SFC4100 Series 스위치

사용자 설명서

SOLTECH
INFONET INC.

목차

1. 소개

1.1. 제품 소개

1.1.1. 제품 개요

SFC4100T, SFC4100HP 제품은 10/100/1000Mbps TP포트와 100M/1G/10GBase-X를 지원하는 SFP 슬롯이 있는 관리형 10기가 이더넷 스위치입니다.

관리형 10기가 이더넷 스위치는 자동으로 올바른 전송 속도를 식별하고 Port의 전이중/반이중 모드를 결정할 수 있습니다. Backbone 또는 서버로 연결 보안 토폴로지에서는 대용량 데이터 전송을 처리할 수 있습니다. 또한, 낮은 지연 시간 및 높은 데이터 무결성을 보장하기 위해 store-and-forward 전송 방식을 지원하여 불필요한 트래픽을 제거하고 중요한 네트워크 경로에 혼잡을 해소시킵니다.

지능형 주소 인식 알고리즘을 통해 관리형 10기가 이더넷 스위치는 32K의 다른 MAC 주소까지 인식하고 완전한 전송 속도 필터링 및 전달이 가능합니다.

모델명	TP 포트 (1Gbps)	PoE 포트	SFP 슬롯 (10Gbps)	동작온도	비고 (S-Ring, ERPS)
SFC4100T	24 포트	-	4 슬롯	0℃ ~ 60℃	
SFC4100HP	24 포트	24 PoE (af/at) / PoE 400W	4 슬롯	0℃ ~ 50℃	PoE

1.2. 제품 특징

1.2.1. 물리 포트

1.2.1.1. SFC4100T

- 24 10/100/1000BASE-T RJ45 Copper ports with LED
- 4 100/1000/10GBASE-X SFP+ slots
- SFP Slot 상태 LED
- 기본 관리 및 설정을 위한 콘솔 인터페이스

1.2.1.2.SFC4100HP

- 24 10/100/1000BASE-T RJ45 Copper ports with LED
- IEEE 802.3af/at 24 Port(1~24 Port)
- PoE 파워용량 : 400W
- 4 100/1000/10GBASE-X/SFP+ slots
- SFP Slot 상태 LED
- 기본 관리 및 설정을 위한 콘솔 인터페이스

1.2.2. 공통 기능

1.2.2.1. Layer2 기능

- Store-and-Forward architecture의 높은 성능과 runt/CRC filtering은 잘못된 패킷을 제거하여 네트워크 대역폭을 최적화
- Storm Control 지원
  - 브로드캐스트(Broadcast) / 멀티캐스트(Multicast) / 알 수 없는 유니캐스트(Unknown unicast)
- VLAN 지원
  - IEEE 802.1Q tagged VLAN
  - 최대 255개의 VLAN 그룹, 4,094개의 VLAN ID 중에서 선택 가능
  - Provider bridging (VLAN Q-in-Q, IEEE 802.1ad) 지원
  - Private VLAN Edge (PVE)
  - 프로토콜 기반 VLAN
  - MAC 주소 기반 VLAN
  - Voice VLAN
  - GVRP (GARP VLAN Registration Protocol)
- Spanning Tree Protocol 지원
  - IEEE 802.1D Spanning Tree Protocol (STP)
  - IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
  - IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), spanning tree by VLAN
  - BPDU Guard
- Link Aggregation 지원
  - 802.3ad Link Aggregation Control Protocol (LACP)
  - Cisco ether-channel (static trunk)
  - 최대 10개의 Trunk 그룹, 각 Trunk 그룹 당 최대 16개의 포트 지원
- 포트 미러링 제공 (1 : 1 / N : 1)
- 특정 포트의 수신 또는 송신 트래픽을 모니터링 하기 위한 포트 미러링
- 브로드캐스트(Broadcast) 루프를 피하기 위한 루프 보호 기능

1.2.2.2. Power over Ethernet (SFC4100HP)

- IEEE 802.3af/at Power over Ethernet PSE 준수
- 선택 가능한 PoE 모드: IEEE 802.3af/at
- 1~24 포트는 최대 30W 지원
- PoE budget: 400W
- PD(Powered Device) 자동 감지
- 보호 회로로 포트 간의 전원 간섭 방지

1.2.2.3. 서비스 품질 (Quality of Service)

- 포트 당 Ingress Shaper 및 Egress Rate Limit로 대역폭 제어
- 모든 스위치 포트에서 8개의 우선순위 큐(priority queues)
- 트래픽 분류
  - IEEE 802.1p CoS
  - TOS / DSCP / IP Precedence of IPv4/IPv6 packets
  - IP TCP/UDP 포트 번호
  - 일반적인 네트워크 응용 프로그램
- 엄격한 우선 순위 및 Weighted Round Robin (WRR) CoS 정책
- 각 포트에서 QoS 및 In/Out 대역폭 제어 지원
- 스위치 포트에서 Traffic-policing 지원
- DSCP 재표시 지원

1.2.2.4. 멀티캐스트 (Multicast)

- IPv4 IGMP Snooping v1, v2 및 v3 지원
- IPv6 MLD Snooping v1 및 v2 지원
- Querier 모드 지원
- IPv4 IGMP Snooping 포트 필터링
- IPv6 MLD Snooping 포트 필터링
- Multicast VLAN Registration(MVR) 지원

1.2.2.5. 보안

- 인증
  - RADIUS 서버와 같이 동작하는 내장형 RADIUS 클라이언트
  - TACACS+ 로그인 사용자 접속 인증
  - RADIUS / TACACS+ 사용자 접속 인증
  - Guest VLAN은 클라이언트를 서비스가 제한된 VLAN을 할당
- 접근 제어 목록
  - IP 기반의 접근 제어 목록 (ACL)
  - MAC 기반의 접근 제어 목록
- Source MAC / IP 주소 바인딩
- 신뢰할 수 없는 DHCP 메시지 필터링을 위한 DHCP Snooping
- 동적 ARP 검사는 잘못된 MAC 주소와 IP 주소 바인딩을 가진 ARP 패킷을 삭제
- IP Source Guard prevents는 IP spoofing 공격을 방지
- 자동 DoS rule로 DoS 공격을 방어
- 무단으로 접속하는 침입자를 방지하기 위한 IP 주소 액세스 관리

1.2.2.6. 관리

- IPv4 및 IPv6 듀얼 스택 관리
- 스위치 관리 인터페이스
  - Console / Telnet 서비스 Command Line Interface
  - 웹(http/https) 서비스를 통한 스위치 관리
  - SNMP v1, V2c, 및 v3 스위치 관리
  - SSH v2.0 서비스 보안 접속
  - HTTPS SSL/TLS v1.2 서비스 보안 접속
- SNMP 관리
  - 4개의 RMON 그룹 (이력, 통계, 알람 및 이벤트)
  - 인터페이스 링크 업 및 링크 다운 알림을 위한 SNMP 트랩
- IPv6 IP Address / NTP / DNS 관리
- 내장형 Trivial File Transfer Protocol (TFTP) 클라이언트
- IP 주소 할당을 위한 BOOTP 및 DHCP

- 시스템 유지보수
  - HTTP/TFTP를 통한 펌웨어 업로드 / 다운로드
  - 시스템 재부팅 또는 공장 초기화를 위한 리셋 버튼
  - 듀얼 이미지 지원
- DHCP 릴레이
- DHCP Option82
- DHCP 서버
- 사용자 권한 등급 제어
- NTP (Network Time Protocol)
- Link Layer Discovery Protocol (LLDP) and LLDP-MED
- Network 진단
  - ICMPv6 / ICMPv4 원격 Ping
  - 케이블 진단 기술은 잠재적인 케이블 문제를 감지하고 보고하는 메커니즘을 제공
- 원격 알람을 위한 SMTP / Syslog
- 시스템 로그

1.3. 제품 사양

Product	SFC4100T	SFC4100HP
Hardware Specifications		
Copper Ports	24 10/100/1000Mbps RJ45 auto-MDI/MDI-X Ports	
Fiber Slots	4 100/1000/10000Mbps SFP Slots	
Console	1 x RJ45 serial port (Baud Rate : 115200)	
Reset Button	< 2sec : No Action <10sec : Default Reset (keep ip address) >10sec : Factory Reset (All the configurations to default values)	
Power Requirements	AC 100 ~240V, 50/60Hz	
Power Consumption	AC 15.1W / AC 26.9W	AC 36.3W / AC 446.3W (PoE 400W)
Operating Temperature	0℃ ~ 60℃	0℃ ~ 50℃
Size (WxDxH)	440mm(W) x 330mm(D) x 44mm(H)	
Switching Specifications		
Switch Architecture	Store-and-Forward	
Switch Fabric	128Gbps	
Throughput	95.2Mpps	
CPU	CPU MIPS24Kec Core 500MHz (32bit)	
RAM/ Flash Memory	256MB/16MB	
MAC Address Table	32K	
Data Buffer	32Mb	
Flow Control	IEEE 802.3x pause frame for full duplex Back pressure for half duplex	

Jumbo Frame	10K
Software Functions	
Port Configuration	- Port disable / enable - Auto-negotiation 10/100/1000Mbps full and half duplex mode selection - Flow Control disable / enable
Port Status	Display each ports speed duplex mode, link status, flow control status, auto-negotiation status
VLAN	Port-Based / 802.1Q Tagged Based VLAN, Up to 255 VLAN groups Q-in-Q tunneling Private VLAN Edge (PVE) MAC-based VLAN Protocol-based VLAN Voice VLAN MVR (Multicast VLAN Registration) Up to 255 VLAN groups, out of 4096 VLAN ID
Link Aggregation	IEEE 802.3ad LACP / Static Trunk Supports 5 groups of 8-Port trunk
QoS	4 Priority Queue and traffic classification based on 802.1p priority, DSCP field in IP packet
IGMP/MLD snooping	IGMP (v1/v2/v3) Snooping, up to 255 multicast Groups MLD (v1/v2) Snooping, up to 255 multicast Groups
Access Control List	IP-Based ACL / MAC-Based ACL Up to 123 entries
Bandwidth Control	Per port bandwidth control Ingress: 500Kb ~ 1000Mbps Egress: 500Kb ~ 1000Mbps
Port Mirror	One to Multi-port and the monitor mode is RX
SNMP MIBs	RFC-1213 MIB-II IF-MIB RFC-1493 Bridge MIB RFC-1643 Ethernet MIB RFC-2863 Interface MIB RFC-2665 Ether-Like MIB RFC-2819 RMON MIB (Group 1,2,3,9) RFC-2737 Entity MIB RFC-2618 RADIUS Client MIB

	RFC-2933 IGMP-STD_MIB RFC3411 SNMP-Frameworks-MIB LLDP MAU_MIB
Ring Protocol	ERPS, STP, RSTP, MSTP, S-Ring
Inter-VLAN Routing	Supported
Static Routes	128 IPv4 Routes
Standards Conformance	
Network Standards	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX/100Base-FX Fast Ethernet IEEE 802.3z Gigabit Ethernet (SX/LX) IEEE 802.3ab Gigabit 1000T IEEE 802.3x Flow Control and Back pressure IEEE 802.3ad Port trunk with LACP IEEE 802.1D Spanning tree protocol IEEE 802.1w Rapid Spanning Tree protocol IEEE 802.1s Multiple spanning tree protocol IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging IEEE 802.1ab LLDP RFC 768 UDP RFC 793 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP version 1 RFC 2236 IGMP version 2 RFC 3376 IGMP version 3 RFC3590 MLDv1 RFC4604 MLDv2 ITU-T G.8032 Ethernet Ring Protection Switching

1.4. 제품 구성품

	SFC4100T	SFC4100HP
Managed 10G Ethernet Switch	O	O
Rack Mount 브라켓	O	O
고정형 나사	O	O
AC Power 케이블	O	O

이들 중 하나라도 누락되거나 손상되어 수리해야 할 경우 박스에 제품과 부속품을 다시 포장하여 본사나 대리점에 문의하십시오.

2. 외관 설명

2.1. 모델 및 외관

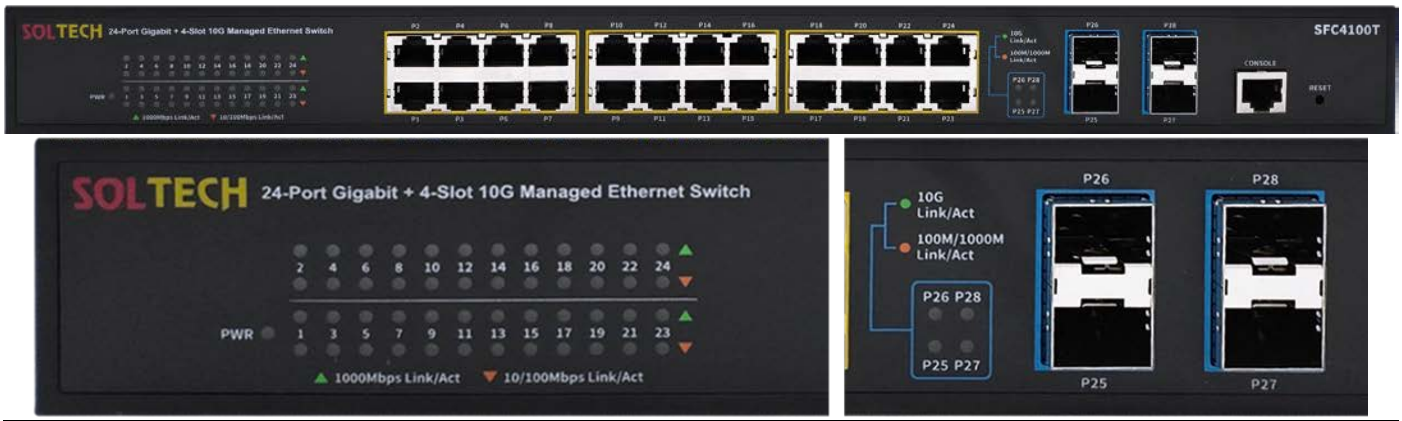
모델	외관	포트정보	크기
SFC4100T		10/100/1000BASE-T 포트 24개 1G/10G SFP 슬롯 4개 콘솔 포트 1개 RESET 스위치 1개 (공장초기화 용도)	440x330x44 (mm)
SFC4100HP		10/100/1000BASE-T 포트 24개 24 PoE(af/at) / PoE 400W 1G/10G SFP 슬롯 4개 콘솔 포트 1개 RESET 스위치 1개 (공장초기화 용도)	440x330x44 (mm)

2.2. LED 동작 상태

전면 패널 LED는 전원, 시스템 상태, 포트 링크/액티브 및 PoE의 즉각적인 상태를 나타내어 연결장치의 잠재적인 문제를 모니터링, 진단 및 해결할 수 있습니다.

아래의 그림은 SFC4100 시리즈 제품에 대한 스위치 LED 표시를 보여줍니다.

2.2.1. SFC4100T



	LED	Color	상태	상태 설명
System	POWER	Green	점등	Switch 전원 On
UTP (1~24)	10/100Mbps Link/ACT	Orange	점등	UTP 포트 연결 상태
			소등	UTP 포트 연결 안 된 상태
	1000Mbps Link/ACT	Green	점멸	데이터 전송 상태
SFP (25~28)	100M/1Gbps Link/ACT	Orange	점등	SFP 슬롯 연결 상태
			소등	SFP 슬롯 연결 안 된 상태
	10Gbps Link/ACT	Green	점멸	데이터 전송 상태

2.2.2.SFC4100HP

	LED	Color	상태	상태 설명
System	POWER	Green	점등	Switch 전원 On
UTP (1~24)	10/100/1000Mbps Link/ACT	Green	점등	UTP 포트 연결 상태
			소등	UTP 포트 연결 안 된 상태
			점멸	데이터 전송 상태
PoE (1~24)	PoE PWR	Orange	점등	포트에 PD가 연결되어 전원을 공급 중
			소등	포트에 PD가 연결되지 않았거나 포트의 전력 한계로 전력이 공급되지 않음
			점멸	PoE 전류가 과부하 되었음
SFP (25~28)	100M/1Gbps Link/ACT	Orange	점등	SFP 슬롯 연결 상태
			소등	SFP 슬롯 연결 안 된 상태
	10Gbps Link/ACT	Green	점멸	데이터 전송 상태

2.3.Power input 연결방법

SFC4100시리즈(SFC4100T, SFC4100HP) 제품의 후면에 전원 입력부가 있으며, 아래의 교류전원을 인가할 수 있습니다.

- SFC4100T, SFC4100HP : AC 전원입력 100~240Vac / 50~60Hz 1개

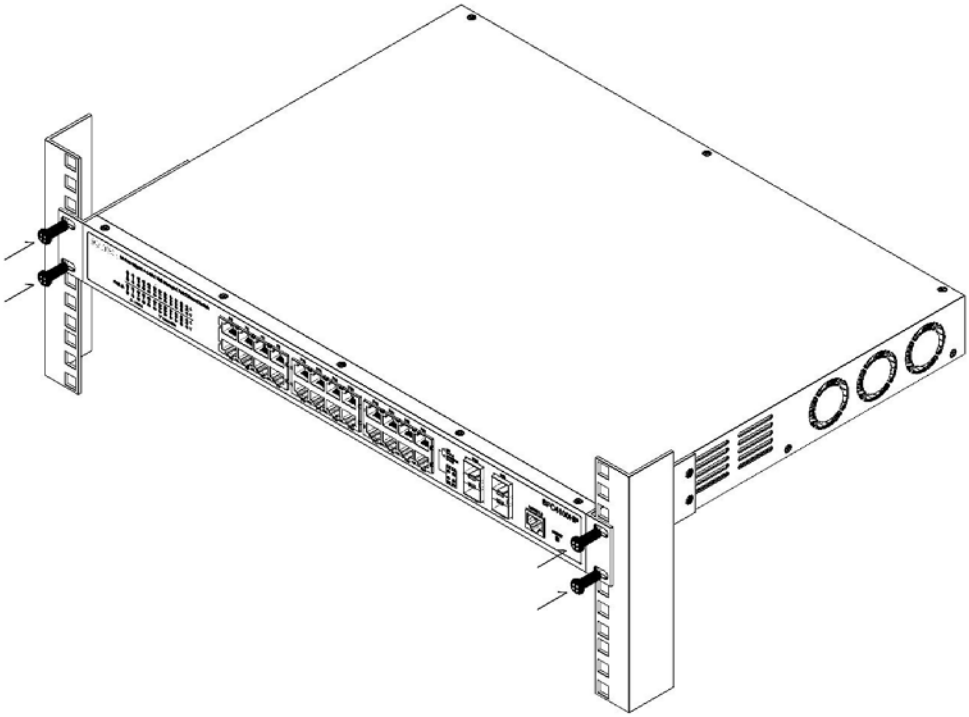
Power Notice :

1. 장치는 전원이 필요한 기기입니다. 전원이 공급되기 전까지는 작동하지 않습니다. 만약 사용자의 네트워크가 항상 활성화되어 있어야 할 경우 UPS(Uninterrupted Power Supply)장치를 사용하는 것을 고려하십시오. 네트워크 데이터 손실 또는 네트워크 정지하는 것을 방지할 수 있습니다.

2. 일부 영역에서 서지 억제 장치를 설치하면 관계없는 서지나 전류에 의해 Switch 또는 전원 어댑터가 손상되지 않도록 하여 Ethernet Switch를 보호할 수 있습니다.

3. 브라켓 장착

SFC4100 Series(SFC4100T, SFC4100HP) 제품의 기본 구성품엔 Rack Mount 브라켓이 동봉되어 있습니다. 이 브라켓을 장착 시 19인치 RACK에 장착이 가능합니다. 브라켓 장착은 아래 그림과 같이 나사 홀을 맞춰준 후 동봉된 나사를 조립하면 장착이 완료됩니다.



SFC4100 Series Rack Mount 장착 모습

4. 제품 설치

이 섹션에서는 Managed 10G Ethernet Switch를 설치하고 Switch를 연결하는 방법에 대해 설명합니다. 다음 항목을 읽고 제시하는 순서의 절차에 따라 수행하십시오. 데스크톱이나 선반에 Managed 10G Ethernet Switch를 설치하려면 다음 단계를 완료하십시오.

4.1. SFC4100 Series 설치 방법

1 단계

SFC4100T/SFC4100HP는 100 ~ 240Vac/50, 60Hz 전원 소스 근처에 놓습니다.

2 단계

Managed 10G Ethernet Switch 와 주변 물체 사이에 충분한 통풍 공간을 유지하십시오.

3 단계

네트워크 장치에 Switch를 연결합니다.

Notice : Managed 10G Ethernet Switch에 대한 연결은 UTP Category 5E 규격 이상의 네트워크 케이블이 필요합니다.

4 단계

Switch 전원 공급

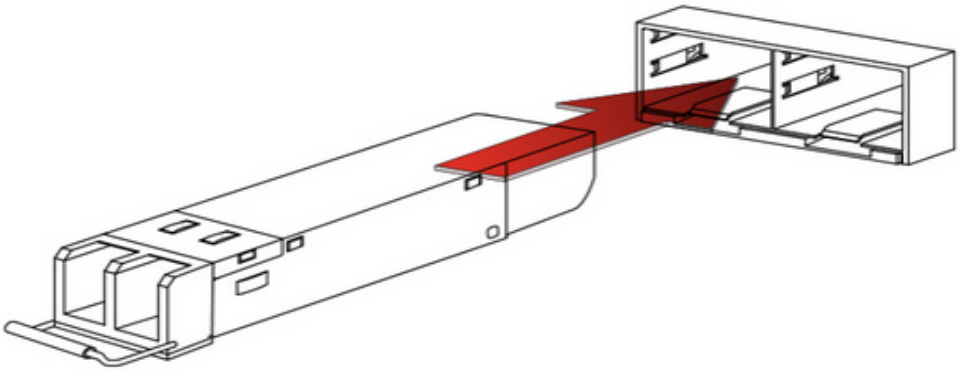
A. Managed 10G Ethernet Switch에 전원 케이블을 연결하십시오.

B. 콘센트에 전원 소스의 전원 케이블을 연결합니다.

Notice : Managed 10G Ethernet Switch는 전원을 받으면 전원 LED(Green)가 항상 켜져 있습니다.

4.2. SFP Transceiver 모듈 설치 방법

SFP 트랜시버 모듈(이하 SFP모듈)은 일반적으로 Hot-pluggable and Hot-swappable 기능을 제공합니다. 사용자는 SFP slot에 모듈을 탈/부착할 때 Managed 10G Ethernet Switch의 전원을 끄지 않아도 됩니다.



Plug-in the SFP Transceiver Module

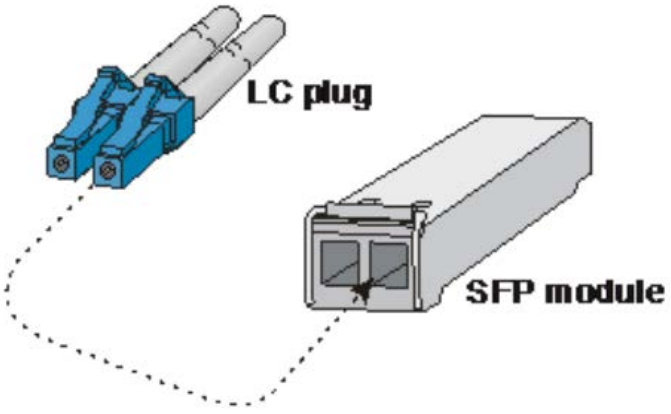
다른 Switch, 워크 스테이션이나 미디어 컨버터를 연결하기 전에 다음 사항을 확인하십시오.

A. 데이터를 전송할 SFP 모듈의 유형이 같은 미디어 유형인지 확인하십시오.
예를 들어 1000BASE-SX에는 1000BASE-SX / 1000BASE-LX에는 1000BASE-LX를 연결해야 합니다.

B. 광섬유 케이블 타입 SFP모듈 유형과 일치하는지 확인하십시오.
1000BASE-SX SFP모듈에 연결하려면 Multi-mode fiber 케이블로 Duplex LC 커넥터 타입을 사용해야 합니다.
1000BASE-LX SFP모듈에 연결하려면 Single-mode fiber 케이블로 Duplex LC 커넥터 타입을 사용해야 합니다.

4.3. 광케이블 연결방법

A. SFP 모듈에 네트워크 케이블 Duplex LC 커넥터를 연결합니다.
B. SFP 모듈이 설치된 fiber NIC(예: Gigabit-이더넷 스위치 또는 미디어 컨버터)에 반대편 케이블을 연결합니다.
C. Switch의 전면에서 SFP slot의 LED LINK/ACT를 이용하여, SFP 모듈이 제대로 작동하는지 확인하십시오.
D. 링크가 실패한 경우에는 SFP slot의 연결모드를 확인하세요.
일부 Fiber NIC는 "1000 Force"로 링크 모드 설정을 할 필요가 있습니다.



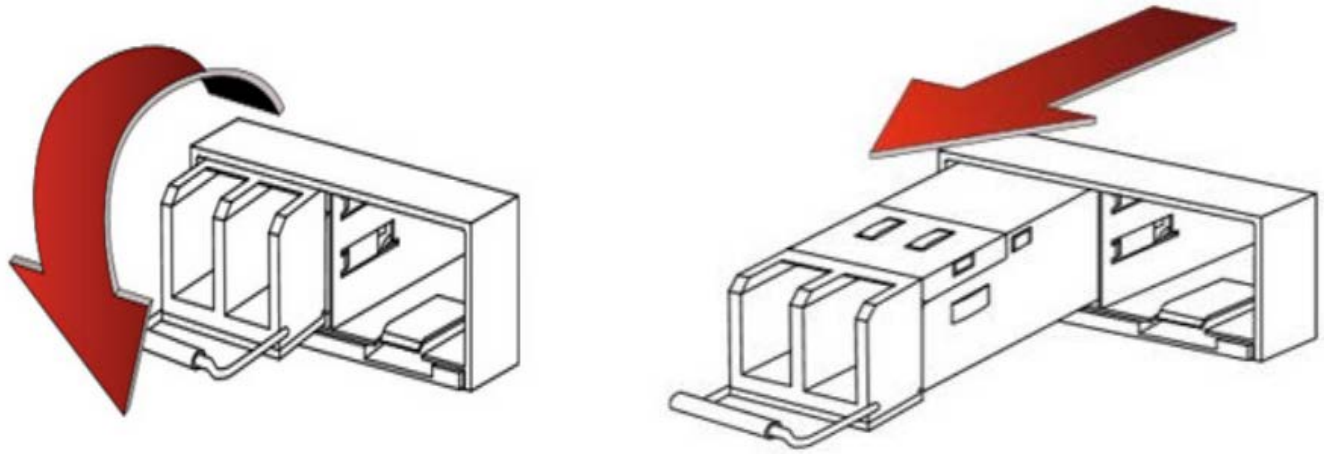
4.4. SFP Transceiver 모듈 제거 방법

A. 사용자가 제거할 SFP 모듈이 있는 포트에 현재 네트워크 활동이 있는지 확인하거나 Switch/컨버터의 관리 인터페이스를 통해 Port를 Disable하십시오.

B. 부드럽게 Fiber 케이블을 제거합니다.

C. 수평으로 SFP 모듈의 손잡이를 잡습니다.

D. 손잡이를 부드럽게 잡아 모듈을 빼냅니다.



Notice : 난폭하게 다루거나 SFP 모듈의 푸쉬 볼트를 잡고 모듈을 끄집어 내지 마십시오. 당길 때 Managed 10G Ethernet Switch 및 SFP 모듈 슬롯을 손상시킬 수 있습니다.

4.5. 운용 환경

본 스위치는 IP카메라, IP전화, PC, 프린터, 저장장치 등의 IT 장비 앞단에 위치하여 각 단말의 패킷을 처리하고, 네트워크 구분을 위하여 여러 개의 2계층의 가상랜(VLAN)을 다른 스위치/라우터로 전달하거나, 서로 다른 3계층 가상랜(VLAN)을 가진 네트워크의 연결 지점에서 가상랜(VLAN) 인터페이스에 서로 다른 대역의 주소를 갖는 네트워크 사이에 IP 패킷을 전달하기 위하여 설치되어 운용됩니다.

스위치 운용환경에서 스위치에서 발생하는 로그의 외부 저장 및 관리를 위하여 로그 서버, 관리자 인증을 위한 인증 서버, 스위치 관리를 위한 SNMP 서버, 시간 동기화를 위한 NTP 서버가 포함될 수 있다. 이외에도, 제품에 따라 스위치에서 제공하는 기능을 사용하기 위하여 필요한 외부 실체가 있는 경우 운용환경에 추가적으로 제시될 수 있다.

제품의 기저 운영체제 버전: RTOS eCoS 3.0

- OpenSSL 버전 1.1.1
- SSH 2.0 – Dropbear_2018.76

5. 스위치 접근 방법

스위치에 접근하는 방법에 대한 간략한 소개입니다.

5.1. 장비 초기 설정 값

장비의 초기 설정 값은 다음과 같습니다.

[초기 설정값]

항목	기본값	비고
관리자 계정	admin	
관리자 비밀번호	admin	
운영모드 변경 비밀번호	admin	기본 관리자 비밀번호
콘솔	활성화	Baud rate : 115200 Data bits : 8 Parity : None Stop bits : 1
SNMP	비활성화	
Telnet	비활성화	
SSH	활성화	
HTTP/HTTPS	활성화	HTTP redirection 활성화
기본 IP주소	192.168.10.100	서브넷 마스크 255.255.255.0(IP/24)
포트 상태	활성화	
감사데이터 생성	활성화	

5.2. WEB 인터페이스

5.2.1. WEB Login

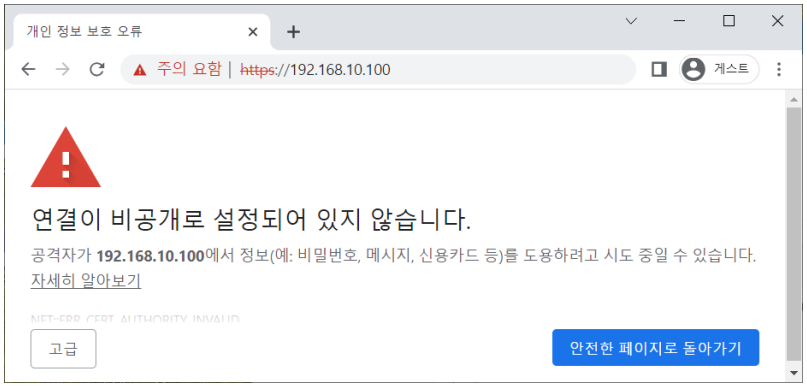
이 페이지에서는 웹 인터페이스에 접속하는 방법을 소개합니다.

1. 사용자는 장비의 IPv4 주소를 알고 있어야 합니다.

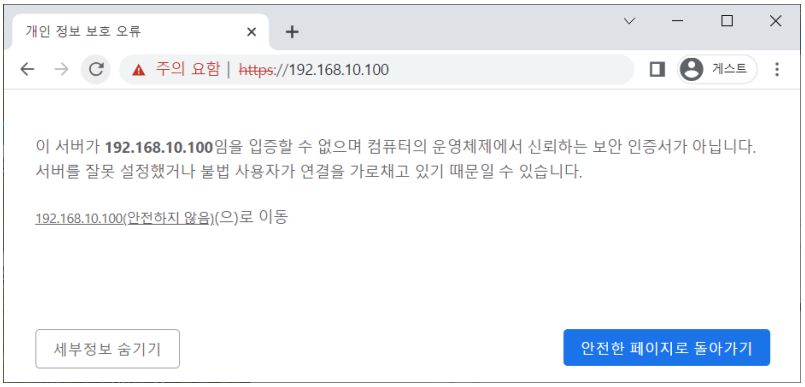
2. 랜 케이블을 사용하여 장비의 LAN 인터페이스와 PC의 랜포트를 연결합니다.

3. 장비의 IPv4 주소로 WEB에서 접속을 시도합니다.(초기IP-192.168.10.100)

정보보호 페이지가 표시됩니다.

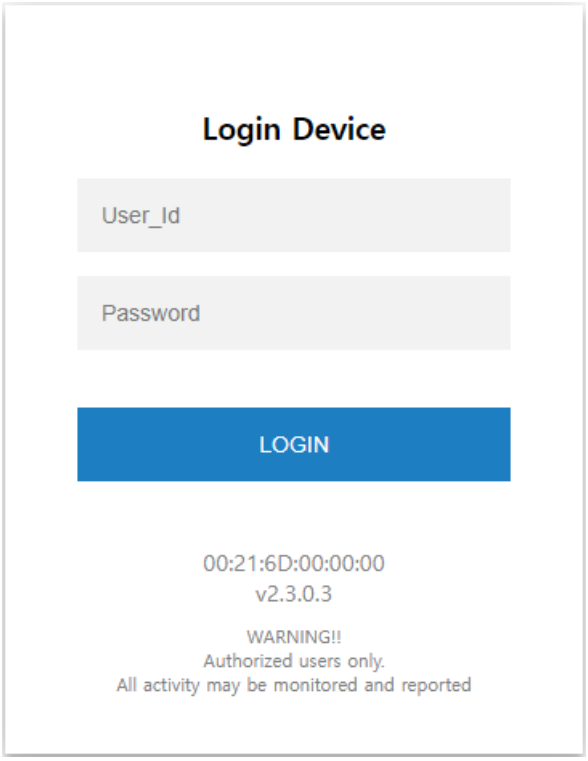


고급을 클릭합니다.



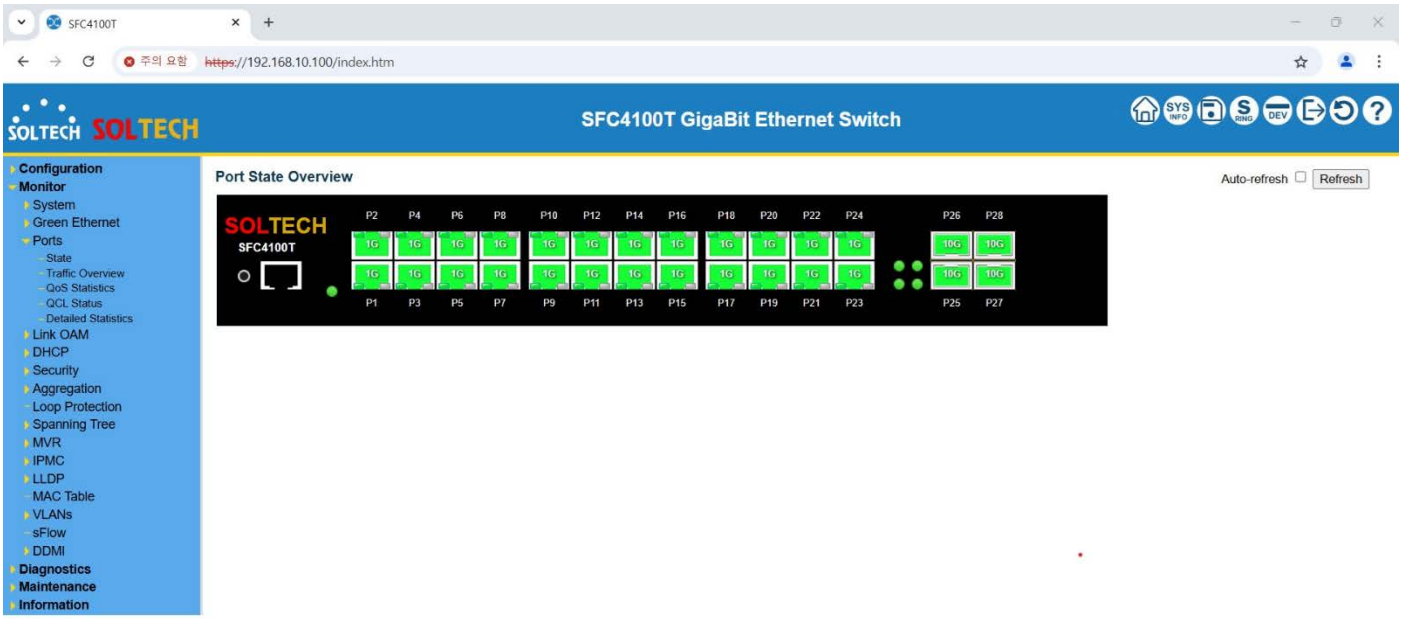
192.168.10.100(안전하지 않음)을 클릭합니다.

로그인 페이지가 나옵니다.



사용자 ID와 Password를 입력하고 로그인 합니다.(초기설정 ID-admin, PW-admin)

4. 장비 웹 인터페이스에 접속되었습니다.



5.3. CLI Interface

5.3.1. CLI 기본 기호

이 페이지는 CLI (Command Line Interface) 명령어에서 자주 사용되는 기호들의 설명을 제공합니다.

기호	설명
< >	값을 직접 입력해야 하는 기호입니다. 영문, 숫자, 특수문자를 넣으세요.
{ }	선택사항을 나타내는 기호입니다. 항목 중 한가지는 선택해야 합니다.
[ ]	선택사항을 나타내는 기호입니다. 전체를 선택하지 않아도 됩니다.
( )	필수적 항목을 표시한 기호입니다. 항목을 꼭 입력하세요.
*	Port 인터페이스에서 사용되는 기호로 포트 전체를 선택할 수 있습니다.
|	구분자로 사용되는 기호로 여러 항목을 나타낼 때 사용됩니다.

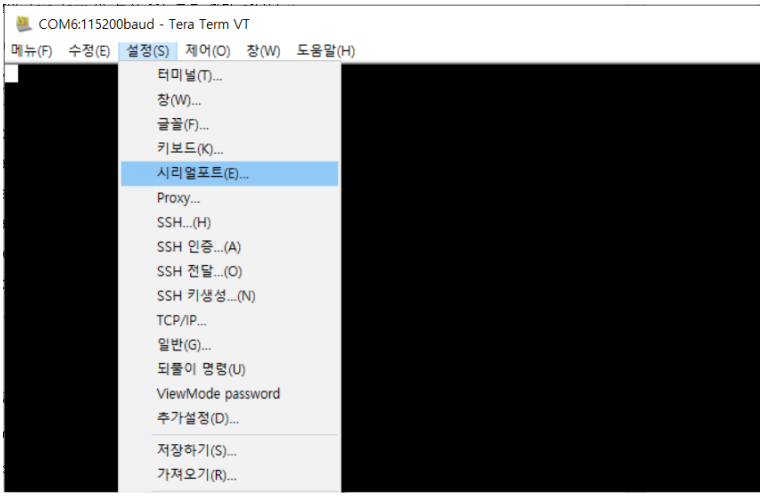
5.3.2. Console(콘솔)

제품의 간단한 셋팅 시 사용되며 장비는 항상 1대1로 연결하여 사용됩니다.

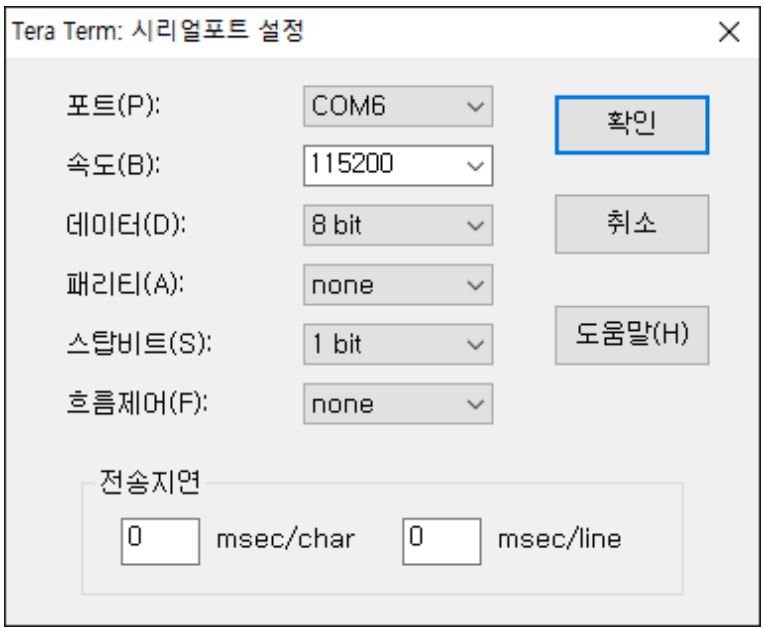
제품의 포함된 Console 케이블을 스위치의 콘솔 포트에 연결하고 PC의 RS-232 포트에 연결합니다.

다음 셋팅 내용은 콘솔 프로그램의 무료 배포 프로그램인 Tera Term을 이용하여 작업한 내용이다.

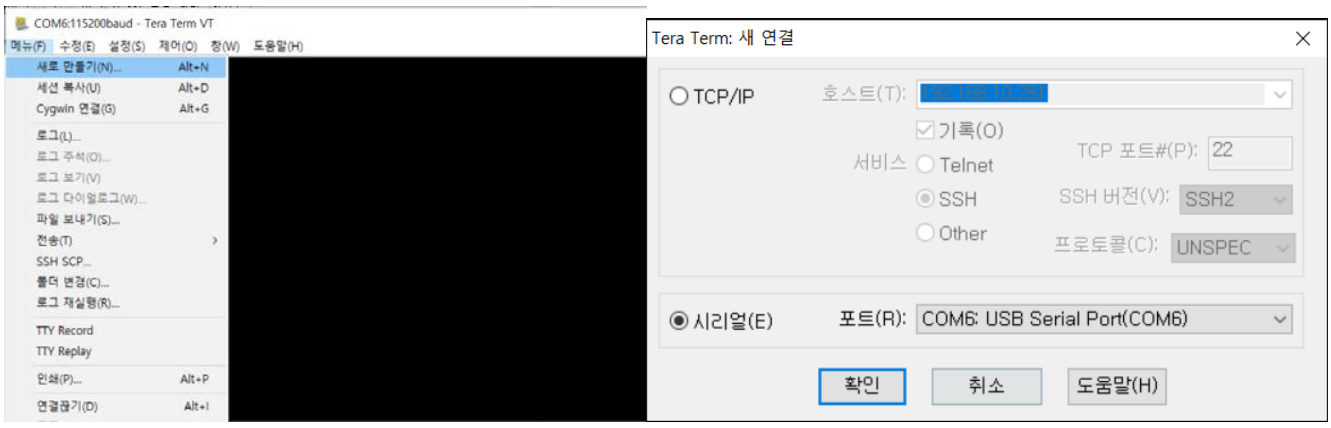
1. 시리얼포트로 진입(설정>시리얼포트)



2. 시리얼포트 설정.(속도 설정을 아래와 같이 115200으로 설정)

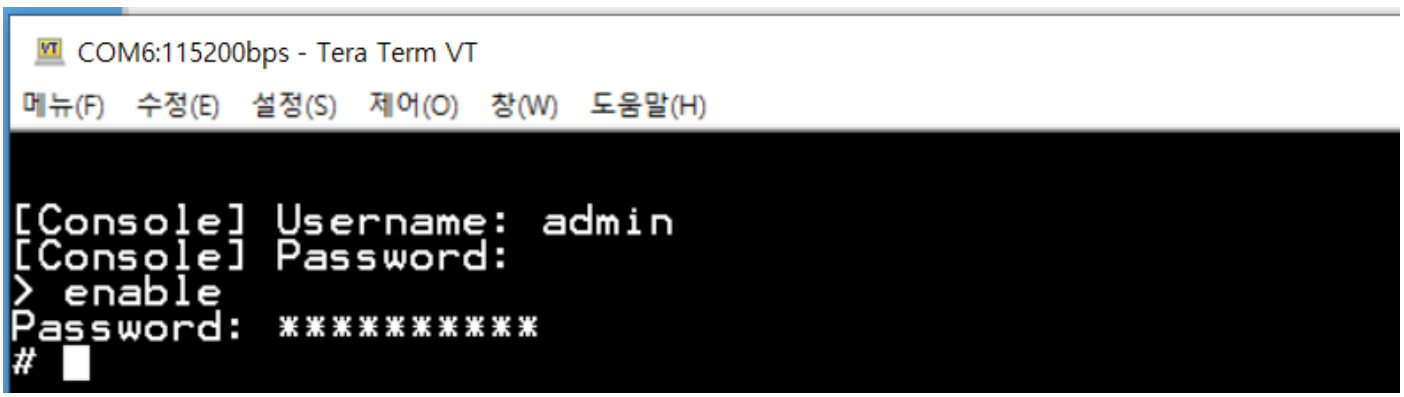


3. 콘솔로 접속합니다.(새로 만들기 필요 Alt+N)



초기 ID와 비밀번호는 admin입니다.

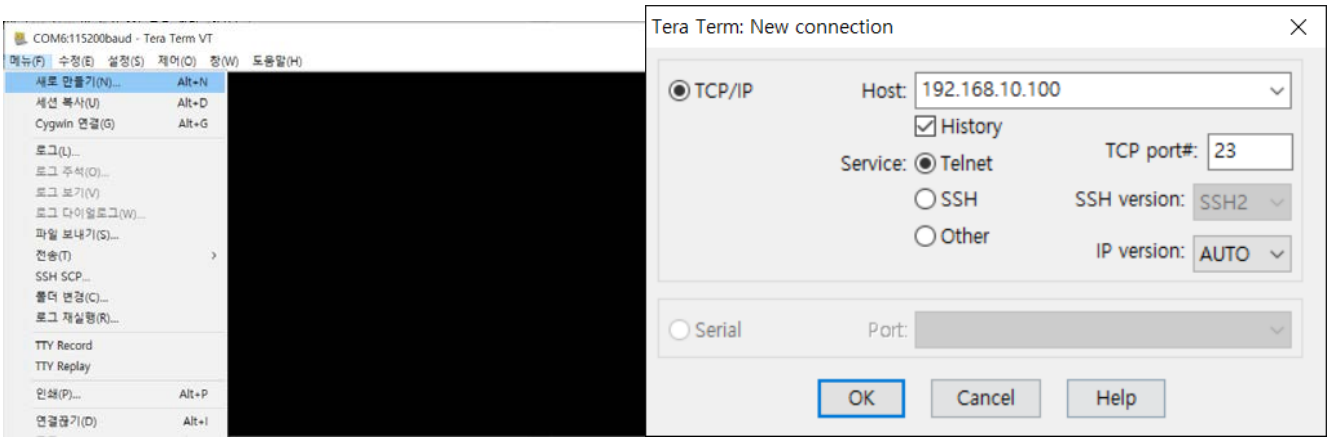
4. Console에 접속된 상태입니다. (ID-admin, PW-admin 또는 이전에 설정한 비밀번호)
패스워드를 입력한 후에 Enable을 입력하여 스위치 운용모드로 진입합니다. (패스워드를 한번 더 확인합니다.)



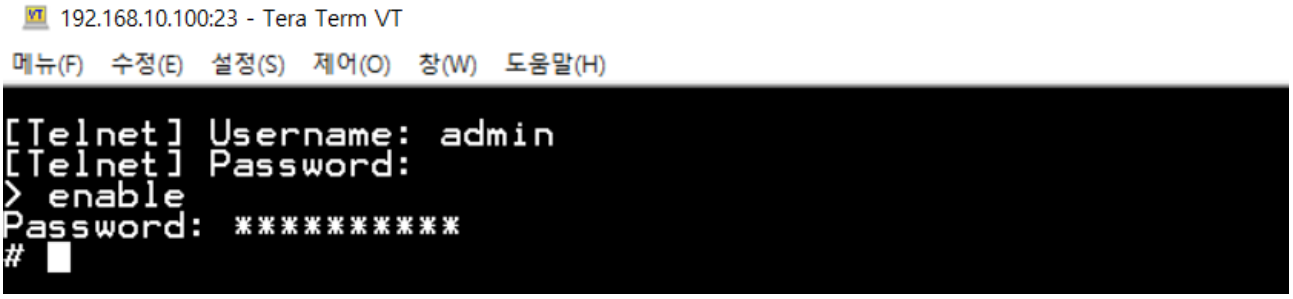
5.3.3. Telnet

이 페이지에서는 Telnet접속을 설명합니다.

콘솔의 2번 항목까지 같은 설정을 진행한 후 아래와 같이 합니다.



Telnet은 같은 네트워크 망 내부에 있는 컴퓨터에서 스위치 접속이 가능합니다.

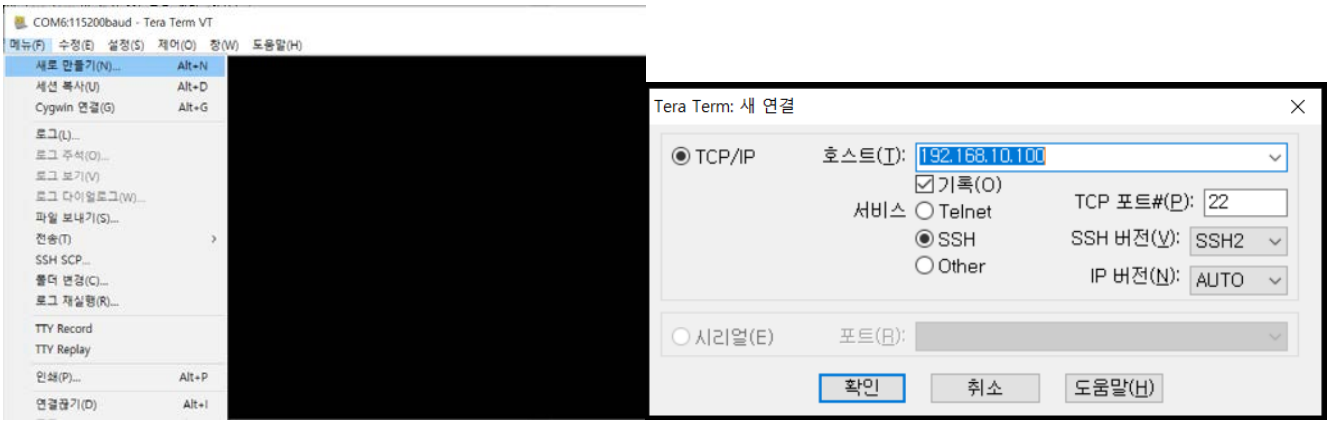


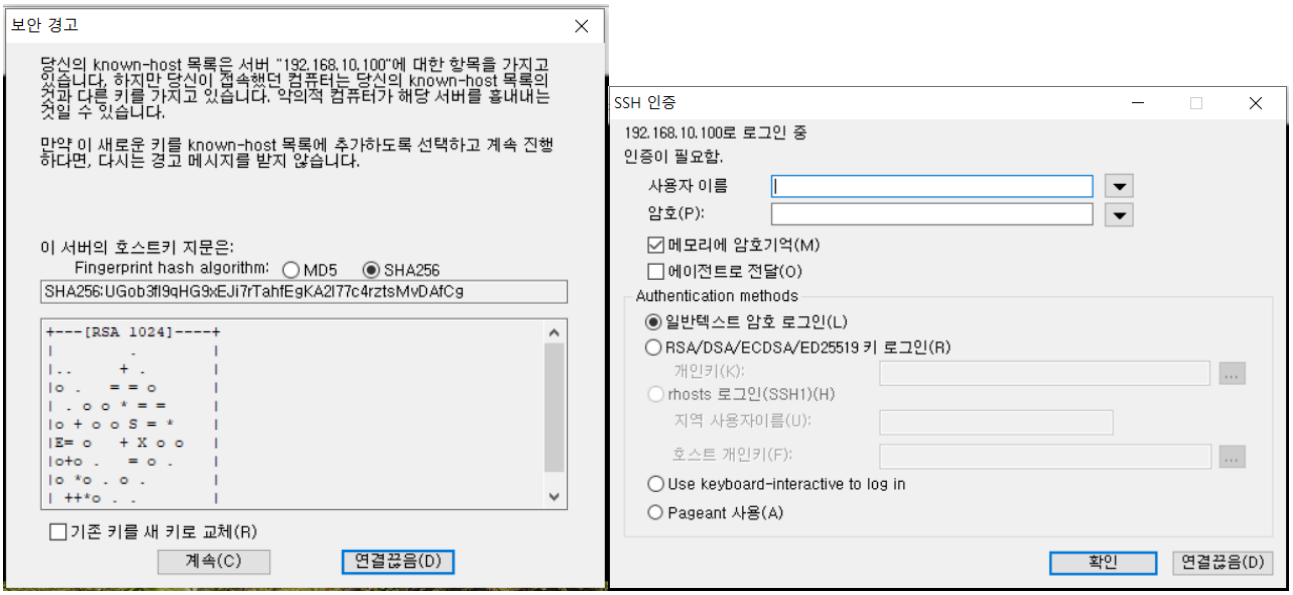
패스워드를 입력한 후에 Enable을 입력하여 스위치 운용모드로 진입합니다. (패스워드를 한번 더 확인합니다.)

5.3.4. SSH

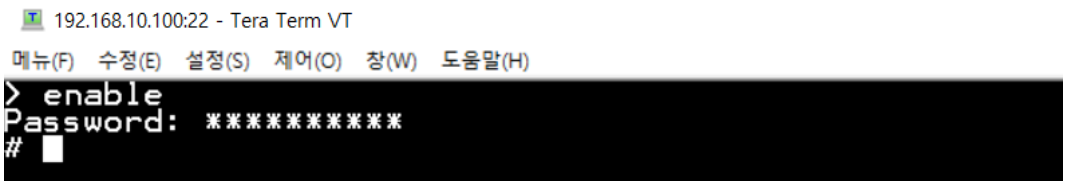
이 페이지에서는 SSH접속을 설명합니다.

콘솔의 2번 항목까지 같은 설정을 진행합니다.





보안 경고 창에서 계속(C)을 클릭 후 SSH 인증 창에서 아이디와 패스워드를 입력



패스워드를 입력한 후에 Enable을 입력하여 스위치 운용모드로 진입합니다. (패스워드를 한번 더 확인합니다.)

5.4. CLI 기본 명령

이 페이지는 Command-Line Interface (CLI)에서 사용되는 기본 명령어에 대한 설명을 제공합니다.

5.4.1. CLI 기본 사용 키

✓ **TAB 키**

명령어를 입력할 때 TAB키를 입력하면 다음에 올 명령어를 보여주거나 혹은 기존 명령어가 완성됩니다.
'<cr>'이 표시되면 CLI상에 해당 명령어 입력이 가능한 것입니다.

✓ **Help**

```
# help
명령어 입력 시 언제든지 물음표 '?'를 입력하여 도움말을 요청할 수 있습니다.
만약 일치하는 항목이 없다면, 도움말 목록은 비어 있으며, 물음표 '?'를 입력해
야 사용 가능한 옵션을 확인할 수 있습니다.
두 가지 유형의 도움말이 제공됩니다:

1. 전체 도움말은 명령 인자를 입력할 준비가 된 경우에 사용 가능하며, 각 가
능한 인자에 대해 설명합니다. (예: 'show ?')

2. 부분 도움말은 줄인 인자가 입력되고 해당 입력과 일치하는 인자를 알고 싶
을 때 제공됩니다. (예: 'show pr?')
```

✓ **'?' 키**

언제든 '?'키를 누르면 입력 가능한 명령어에 대한 도움말이 나옵니다.

```
# ?
clear       Reset functions
configure   Enter configuration mode
copy        Copy from source to destination
delete      Delete one file in flash: file system
dir         Directory of all files in flash: file system
disable     Turn off privileged commands
do          To run exec commands in the configuration mode
enable      Turn on privileged commands
erps        Ethernet Ring Protection Switching
exit        Exit from EXEC mode
firmware    Firmware upgrade/swap
help        Description of the interactive help system
ip          IPv4 commands
ipv6        IPv6 configuration commands
link-oam    Link OAM configuration
logout      Exit from EXEC mode
more        Display file
```

```
no          Negate a command or set its defaults
ping        Send ICMP echo messages
platform    Platform configuration
reload      Reload system.
send        Send a message to other tty lines
show        Show running system information
terminal    Set terminal line parameters
veriphy     VeriPHY keyword
```

✓ **'??' 키**

'??' 키를 입력하면 현재 상태에서 작성 가능한 전체 명령어가 표시됩니다.

5.4.2. CLI 기본사용 모드

CLI는 명령의 성격에 따라 적절한 모드에 모든 명령을 그룹화합니다. CLI 명령 모드의 예시는 아래와 같이 설명됩니다. 각 명령 모드는 특정한 소프트웨어 명령어를 지원합니다.

Command Mode	접근 방법	Prompt에 표시되는 기호	종료 또는 이전모드
User Mode	이것은 접근의 첫 번째 단계입니다. 기본적인 작업을 수행하고 시스템 정보를 나열할 수 있습니다.	**Switch>**	Logout, Exit 명령어
Privileged Mode	사용자 모드(User Mode)에서 "enable" 명령어를 입력하세요.	**Switch#**	Exit, Logout, Disable 명령어.
Global Config Mode	프리빌리지 모드 (Privileged Mode)에서 "configuration terminal" 명령어를 입력하세요.	**Switch (Config)#**	Exit, End 명령어.
Interface Config Mode	글로벌 구성 모드 (Global Config Mode)에서 "interface <포트번호>" "interface <VLAN번호>" 명령어를 입력하세요.	**Switch (config-if)#** **Switch (config-if-vlan)#**	Exit, End 명령어.

5.4.3. CLI 기본 명령어

✓ **Login**

사용자는 처음 로그인할 때 사용자 이름과 비밀번호를 입력해야 합니다.

```
[Console] Username: admin
[Console] Password:
>
```

✓ **Logout**

현재 사용자를 로그아웃 하거나 새로운 사용자로 로그인하려면 로그아웃 합니다.

```
switch# logout
Exit BYE !!!
###: Press ENTER to get started
```

✓ **Enable**

관리자 권한 명령어를 사용하려면, "enable" 명령어를 사용할 수 있습니다.

```
> enable
Password: *******
#
```

✓ **Disable**

관리자 권한 명령어를 사용중지 하려면, "disable" 명령어를 사용할 수 있습니다.

```
# disable
>
```

✓ **Exit**

모드를 종료하려면, "exit" 명령어를 사용할 수 있습니다.

```
> exit
Exit BYE !!!
###: Press ENTER to get started
```

✓ Clear

남은 기록을 삭제하려면, "Clear" 명령어를 사용할 수 있습니다.

```
# clear ?
    access          Access management
    access-list     Access list
    eps             Ethernet Protection Switching.
    erps            Ethernet Ring Protection Switching
    ip              Interface Internet Protocol configuration commands
    ipv6            IPv6 configuration commands
    lacp            Clear LACP statistics
    link-oam        Clear Link OAM statistics
    lldp            Clears LLDP statistics.
    logging         System logging message
    mac             MAC Address Table
    mep             Maintenance Entity Point
    mvr             Multicast VLAN Registration configuration
    sflow           Statistics flow.
    spanning-tree   STP Bridge
    statistics      Clear statistics for one or more given interfaces
```

✓ No

명령을 취소하거나 기본값으로 설정하려면 "no" 명령어를 사용할 수 있습니다.

```
# no ?
    debug           Debugging functions
    port-security   Port security (MAC limiter)
    terminal        Set terminal line parameters
```

✓ Terminal

터미널 라인 매개변수를 설정하려면 "terminal" 명령어를 사용할 수 있습니다.

```
# terminal ?
    editing         Enable command line editing
    exec-timeout    Set the EXEC timeout
    help            Description of the interactive help system
    history         Control the command history function
    length          Set number of lines on a screen
    width           Set width of the display terminal
```

✓ Show

실행 중인 시스템 정보를 확인하려면 "show" 명령어를 사용할 수 있습니다.

```
# show ?
  aaa                 Authentication, Authorization and Accounting methods
  access              Access management
  access-list         Access list
  aggregation         Aggregation port configuration
  audit-log           System Audit Log message
  clock               Configure time-of-day clock
  ddmi                DDMI configuration
  eps                 Ethernet Protection Switching
  erps                Ethernet Ring Protection Switching
  green-ethernet      Shows green Ethernet status for the switch.
  history             Display the session command history
  interface           Interface status and configuration
  ip                  Internet Protocol
  ipmc                IPv4/IPv6 multicast configuration
  ipv6                IPv6 configuration commands
  lacp                LACP configuration/status
  line                TTY line information
  link-oam            Link OAM configuration
  lldp                Display LLDP neighbors information.
  logging             System logging message
  loop-protect        Loop protection configuration
  mac                 Mac Address Table information
  mep                 Maintenance Entity Point
  module-status       Print Modulte Trhead Status
  monitor             Monitoring different system events
  mvr                 Multicast VLAN Registration configuration
  ntp                 Configure NTP
  platform            Platform configuration
  poe                 Power Over Ethernet.
  port-security       Port Security status - Port Security is a module with no
                      direct configuration.
  privilege           Display command privilege
  process             process
  pvlan               PVLAN configuration
  qos                 Quality of Service
```

```
  radius-server      RADIUS configuration
  rmon               RMON statistics
  running-config     Show running system information
  scan-agent         SCAN-AGENT Module
  sflow              Statistics flow.
  snmp               Display SNMP configurations
  spanning-tree      STP Bridge
  sring              SRING Module
  switchport         Display switching mode characteristics
  system             system
  tacacs-server      TACACS+ configuration
  terminal           Display terminal configuration parameters
  user-privilege     Users privilege configuration
  users              Display information about terminal lines
  version            System hardware and software status
  vlan               VLAN status
  voice              Voice appliance attributes
  web                Web
```

✓ Configure

구성 모드로 들어가려면 "configure" 명령을 사용하실 수 있습니다.

```
# configure ?
  terminal    Configure from the terminal
# configure terminal
(config)#
```

✓ Save-config

현재까지 설정한 Config를 Startup-Config에 저장할 때 명령을 사용하실 수 있습니다.
본 명령어는 모드에 관계없이 사용이 가능합니다.

```
# save-config
###: Running-config saved (by:1) !!!
###: Running-config saved !!!
# copy running-config startup-config
Building configuration...
% Saving 930 bytes to flash:startup-config
```

✓ Copy running-config startup-config

현재까지 설정한 Running-Config를 Startup-Config에 저장할 때 명령을 사용하실 수 있습니다.
본 명령어는 Privileged 모드에서만 사용이 가능합니다.

```
# copy running-config startup-config
Building configuration...
% Saving 930 bytes to flash:startup-config
```

✓ Dir

현재 Flash에 저장되어 있는 Config파일을 보려면 "dir" 명령을 사용하실 수 있습니다.

```
# dir
Directory of flash:
    r- 1970-01-01 00:00:00       316 default-config
    rw 1970-01-01 07:43:36      1083 startup-config
2 files, 1399 bytes total.
```

6. 스위치 설정 방법

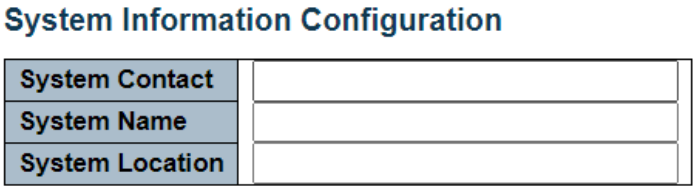
6.1. System

6.1.1. System Configuration

6.1.1.1. Information

웹메뉴 Configuration>System>Information

스위치의 정보(이름,위치등)를 설정합니다.



System Information Configuration

용어	설명
System Contact	스위치 식별정보를 입력합니다. 영문 또는 숫자로 0~255자까지 입력 가능합니다.
System Name	스위치 이름을 입력합니다. 영문 또는 숫자로 0~255자까지 입력 가능하고 (-)기호는 허용됩니다. 공백은 허용되지 않습니다.
System Location	스위치의 위치정보를 입력합니다. 영문 또는 숫자로 0~255자까지 입력 가능합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

✓ **System Contact**

System Information Configuration

System Contact	SOLTECH
System Name	
System Location	

✓ **System Name**

System Information Configuration

System Contact	
System Name	TESTSWITCH
System Location	

✓ **System Location**

System Information Configuration

System Contact	
System Name	
System Location	SOLTECH-LAB

CLI 설정 예시

✓ **System Contact**

```
(config)# snmp-server contact <line255>
(config)# snmp-server contact SOLTECH
```

✓ **System Name**

```
(config)# hostname <host_name>
(config)# hostname TESTSWITCH
```

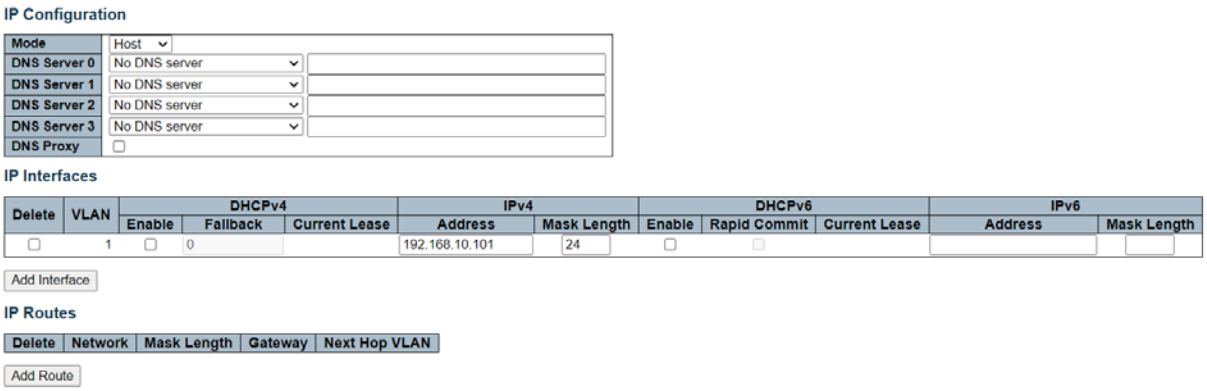
✓ **System Location**

```
(config)# snmp-server location <line255>
(config)# snmp-server location SOLTECH-LAB
```

6.1.1.2. IP

웹메뉴 Configuration>System>IP

IP주소, Subnet Mask, Gateway, DNS, Static IP Route를 설정합니다.



IP Configuration

용어	설명
Mode	IP 스택의 Host, Router로 구성 여부를 설정합니다.
DNS Server	이 설정은 스위치에 의해 수행 된 DNS 이름을 제어합니다.
DNS Proxy	시스템이 현재 구성된 DNS 서버에 DNS 요청을 릴레이하고 네트워크의 클라이언트 장치에 DNS 확인자로 응답합니다.

IP Interfaces

용어	설명
Delete	기존의 IP 인터페이스를 삭제하려면 이 옵션을 선택합니다.
VLAN	IP 인터페이스와 연관된 VLAN입니다. 이 VLAN 포트는 IP 인터페이스에 액세스 할 수 있습니다.
IPv4 DHCP Enabled	이 체크박스를 선택하여 DHCPv4에 클라이언트를 사용합니다.
IPv4 DHCP Fallback Timeout	DHCP 리스를 얻기 위한 시도 시간(초)입니다. 이 기간이 만료되면 구성된 IPv4 주소가 IPv4 인터페이스 주소로 사용됩니다.
IPv4 DHCP Current Lease	활성 Lease와 DHCP 인터페이스의 주소를 표시합니다.
IPv4 Address	점으로 구분 된 십진수 인터페이스의 IPv4 주소 입니다.
IPv4 Mask	IPv4 망 마스크. 유효한 값은 IPv4 주소 0 ~ 30 비트입니다.
DHCPv6 Enable	체크박스를 선택하여 DHCPv6를 클라이언트를 사용합니다.
DHCPv6 Rapid Commit	체크박스를 선택하여 DHCPv6옵션을 선택할 수 있습니다.
DHCPv6 Current Lease	DHCPv6 서버가 제공하는 인터페이스 주소를 보여줍니다.
IPv6 Address	인터페이스의 IPv6 주소입니다.
IPv6 Mask	IPv6 망에서 마스크 비트 (프리픽스 길이). 유효한 값은 IPv6 주소에 대해 1 ~ 128 비트입니다.

IP Routes

용어	설명
Delete	기존 IP 경로를 삭제하려면 이 옵션을 선택합니다.
Network	목적지 IP 네트워크 경로 또는 호스트 주소입니다.
Mask Length	이 노선을 받을 수 있도록 하는 네트워크 주소의 양을 정의합니다. 유효한 값은 0에서 32비트이며, IPv6 경로에 대해 각각 128비트입니다.
Gateway	IP 게이트웨이의 IP 주소입니다.
Next Hop VLAN (Only for IPv6)	게이트웨이와 연관된 특정의 IPv6 인터페이스 VLAN ID (VID)입니다. 주어진 VID는 1 내지 4,095의 범위와 대응하는 IPv6 인터페이스가 유효한 경우에만 유효합니다.

Buttons

Add Interface: 새 IP 인터페이스를 추가합니다. 최대 128 인터페이스가 지원됩니다.

Add Route: 새로운 IP 경로를 추가합니다. 최대 128 개의 노선이 지원됩니다.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

✓ IP Configuration

➢ *Mode*

- Mode Host

IP Configuration

Mode	Host	
DNS Server 0	No DNS server	
DNS Server 1	No DNS server	
DNS Server 2	No DNS server	
DNS Server 3	No DNS server	
DNS Proxy	☐	

- Mode Router

IP Configuration

Mode	Router	
DNS Server 0	No DNS server	
DNS Server 1	No DNS server	
DNS Server 2	No DNS server	
DNS Server 3	No DNS server	
DNS Proxy	☐	

➢ *DNS Server*

- Configured IPv4 or IPv6

IP Configuration

Mode	Host	
DNS Server 0	Configured IPv4 or IPv6	8.8.8.8
DNS Server 1	No DNS server	
DNS Server 2	No DNS server	
DNS Server 3	No DNS server	
DNS Proxy	☐	

IP Configuration

Mode	Host	
DNS Server 0	Configured IPv4 or IPv6	2001:4860:4860::8888
DNS Server 1	No DNS server	
DNS Server 2	No DNS server	
DNS Server 3	No DNS server	
DNS Proxy	☐	

- From any DHCPv4 Interfaces

IP Configuration

Mode	Host	
DNS Server 0	From any DHCPv4 interfaces	
DNS Server 1	No DNS server	
DNS Server 2	No DNS server	
DNS Server 3	No DNS server	
DNS Proxy	☐	

- From this DHCPv4 Interfaces (VLAN1)

IP Configuration

Mode	Host	
DNS Server 0	From this DHCPv4 interface	1
DNS Server 1	No DNS server	
DNS Server 2	No DNS server	
DNS Server 3	No DNS server	
DNS Proxy	☐	

- From any DHCPv6 Interfaces

IP Configuration

Mode	Host	
DNS Server 0	From any DHCPv6 interfaces	
DNS Server 1	No DNS server	
DNS Server 2	No DNS server	
DNS Server 3	No DNS server	
DNS Proxy	☐	

- From this DHCPv6 Interfaces (VLAN1)

IP Configuration

Mode	Host	
DNS Server 0	From this DHCPv6 interface	1
DNS Server 1	No DNS server	
DNS Server 2	No DNS server	
DNS Server 3	No DNS server	
DNS Proxy	☐	

➢ ***DNS Proxy***

IP Configuration

Mode	Host	
DNS Server 0	Configured IPv4 or IPv6	8.8.8.8
DNS Server 1	No DNS server	
DNS Server 2	No DNS server	
DNS Server 3	No DNS server	
DNS Proxy	☑	

✓ IP Interfaces

➢ ***VLAN***(이 필드는 새 인터페이스를 생성할 때만 입력할 수 있습니다.)

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		DHCPv6			IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
☐	1	☐	0		192.168.10.101	24	☐	☐			
Delete	2	☐	0				☐	☐			

➢ ***DHCPv4***

- DHCPv4 폴백 미설정

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		DHCPv6			IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
☐	1	☐	0		192.168.10.101	24	☐	☐			
☐	2	☑	0				☐	☐			

- DHCPv4 폴백 설정(폴백 동안 DHCPv4 서버의 응답이 없으면 IPv4 항목으로 설정)

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		DHCPv6			IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
☐	1	☐	0		192.168.10.101	24	☐	☐			
☐	2	☑	30		2.2.2.2	24	☐	☐			

➢ ***IPv4***

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		DHCPv6			IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
☐	1	☐	0		192.168.10.101	24	☐	☐			
☐	2	☐	0		2.2.2.2	24	☐	☐			

Add Interface

✓ IP Routes

➢ ***Add Route***

- 기본 라우팅을 사용하는 경우

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
☐	0.0.0.0	0	192.168.10.1	0

- 정적 라우팅을 사용하는 경우

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
☐	2.2.2.0	24	192.168.10.1	0

CLI 설정 예시

✓ IP Configuration

➢ ***Mode***

- Mode Host

```
(config)# no ip routing
```

- Mode Router

```
(config)# ip routing
```

➢ ***DNS Server***

- Configured IPv4 or IPv6

```
(config)# ip name-server <0-3> <ipv4_ucast>
(config)# ip name-server 0 8.8.8.8
```

```
(config)# ip name-server <0-3> <ipv6_ucast>
(config)# ip name-server 0 2001:4860:4860::8888
```

- From any DHCPv4 Interfaces

```
(config)# ip name-server <0-3> dhcp ipv4
(config)# ip name-server 0 dhcp ipv4
```

- From this DHCPv4 Interfaces

```
(config)# ip name-server <0-3> dhcp ipv4 interface vlan <vlan_id>
(config)# ip name-server 0 dhcp ipv4 interface vlan 1
```

- From any DHCPv6 Interfaces

```
(config)# ip name-server <0-3> dhcp ipv6
(config)# ip name-server 0 dhcp ipv6
```

- From this DHCPv6 Interfaces

```
(config)# ip name-server <0-3> dhcp ipv6 interface vlan <vlan_id>
(config)# ip name-server 0 dhcp ipv6 interface vlan 1
```

➢ ***DNS Proxy***

```
(config)# ip dns proxy
```

✓ IP Interfaces

➢ ***VLAN***

```
(config)# interface vlan <vlan_list>
(config)# interface vlan 1
```

➢ ***DHCPv4***

- DHCPv4 폴백 미설정

```
(config)# interface vlan <vlan_list>

(config-if-vlan)# ip address dhcp
```

- DHCPv4 폴백 설정.(폴백 동안 DHCPv4 서버의 응답이 없으면 IPv4 항목으로 설정)

```
(config)# interface vlan <vlan_list>
```

```
(config-if-vlan)# ip address dhcp fallback <ipv4_addr> <ipv4_netmask>
timeout <uint>
(config-if-vlan)# ip address dhcp fallback 192.168.10.101 255.255.255.0
timeout 30
```

➢ ***IPv4***

```
(config)# interface vlan <vlan_list>

(config-if-vlan)# ip address <ipv4_addr> <ipv4_netmask>
(config-if-vlan)# ip address 192.168.10.101 255.255.255.0
```

✓ IP Routes

➢ ***Add Route***

- 기본 라우팅을 사용하는 경우(모든 패킷을 게이트웨이로 보냄)

```
(config)# ip route 0.0.0.0 0.0.0.0 <ipv4_addr>
(config)# ip route 0.0.0.0 0.0.0.0 192.168.10.1
```

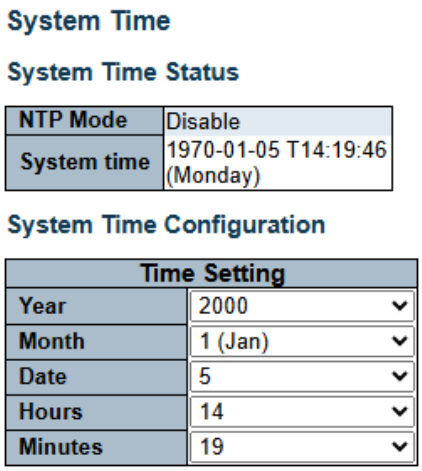
- 정적 라우팅을 사용하는 경우(해당 네트워크 대역의 패킷을 게이트웨이로 보냄)

```
(config)# ip route <ipv4_addr> <ipv4_netmask> <ipv4_addr>
(config)# ip route 2.2.2.0 255.255.255.0 192.168.10.1
```

6.1.1.3. System Time

웹메뉴 Configuration>System>System Time

이 페이지에서 시간을 설정할 수 있습니다.



System Time Status

용어	설명
NTP Mode	NTP 상태를 나타냅니다.
System time	스위치의 현재 시간을 나타냅니다.

'NTP 모드'가 활성화되면 '시간 설정'이 비활성화됩니다.
'시간 설정'을 활성화하려면 NTP 모드를 비활성화로 설정하십시오.

System Time Configuration

용어	설명
Time Setting	이 페이지는 시스템 시간 설정을 구성하는 데 사용됩니다. **Year** 시작 연도를 선택합니다. **Month** 시작 월을 선택합니다. **Date** 시작 날짜를 선택합니다. **Hours** 시작 시간을 선택합니다. **Minutes** 시작 분을 선택합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.
NTP: NTP 설정 페이지로 이동하려면 클릭하세요.
Refresh: 페이지를 새로 고치려면 클릭하세요.

WEB 설정 예시

✓ System Time Configuration

➢ ***Time Setting***

- Year(2000~2037)
- Month(1~12)
- Date(1~31)
- Hours(0~23)
- Minutes(0~59)

Time Setting	
Year	2024
Month	1 (Jan)
Date	1
Hours	0
Minutes	10

Click the Apply button

NTP Mode	Disable
System time	2024-01-01 T00:10:18 (Monday)

CLI 설정 예시

✓ System Time Configuration

➢ ***Time Setting***

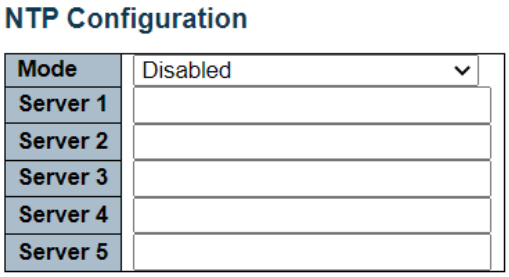
- Year(2000~2037)
- Month(1~12)
- Date(1~31)
- Hours(0~23)
- Minutes(0~59)
- Seconds(0~59)

```
(config)# clock system-time set <d> <t>
<date>    Date yyyy/mm/dd, yyyy=1970-2037, mm=1-12, dd=1-31
<time>    Time HH:mm:ss, HH=0-23, mm=0-59, ss=0-59
(config)# clock system-time set 2024/01/01 00:10:00
```

6.1.1.4. NTP

웹메뉴 Configuration>System>NTP

NTP서버에서 제공하는 시간을 받아오도록 설정합니다.



NTP Configuration

용어	설명
Mode	NTP 동작여부를 설정합니다. Enable: NTP 클라이언트 모드를 활성화합니다. Disable: NTP 클라이언트 모드를 비활성화합니다. (Configuration>System>Time의 Time Zone설정이 필요합니다.)
Server	NTP 서버의 주소를 입력합니다. (DNS를 이용하는 경우 Configuration>System>IP에서 DNS설정이 필요합니다.) NTP서버가 외부 망에 있을경우 Configuration>System>IP에서 IP Routes 기본 게이트웨이 설정이 필요합니다.)

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

✓ NTP Configuration

➢ *Mode*

- Enable(NTP 클라이언트 모드 동작을 사용합니다.)

NTP Configuration

Mode	Enabled
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	

- Disable(NTP 클라이언트 모드 동작을 사용하지 않습니다.)

NTP Configuration

Mode	Disabled
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	

➢ *Server*

- NTP 서버의 IP 주소를 사용(NTP 서버의 IPv4 또는 IPv6 주소를 사용합니다.)

NTP Configuration

Mode	Enabled
Server 1	216.239.35.0
Server 2	
Server 3	
Server 4	
Server 5	

- NTP 서버의 DNS를 사용

NTP Configuration

Mode	Enabled
Server 1	time.google.com
Server 2	
Server 3	
Server 4	
Server 5	

CLI 설정 예시

✓ NTP Configuration

➢ ***Mode***

- Enable(NTP 클라이언트 모드 동작을 사용합니다.)

```
(config)# ntp
```

- Disable(NTP 클라이언트 모드 동작을 사용하지 않습니다.)

```
(config)# no ntp
```

➢ ***Server***

- NTP 서버 설정

```
(config)# ntp server <1-5> ip-address <domain_name> <ipv4_ucast>
<ipv6_ucast>
(config)# ntp server 1 ip-address 216.239.35.0
(config)# ntp server 1 ip-address time.google.com
```

설정 후 확인

✓ 설정 확인

Information Monitor에서 확인이 가능합니다.

➢ ***WEB***

WEB MENU Monitor>System>Information.

➢ ***CLI***

```
# show ntp status

NTP Mode : enabled
Idx   Server IP host address (a.b.c.d) or a host name string
---   ------------------------------------------------

1     time.google.com
2
3
4
5
```

6.1.1.5. Time

웹메뉴 Configuration>System>Time

장비 위치에 따른 시간대를 설정할 수 있습니다.

Time Zone Configuration

Time Zone Configuration	
Time Zone	(UTC+09:00) Seoul
Hours	9
Minutes	0
Acronym	(0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled

Start Time settings	
Month	Jan
Date	1
Year	2014
Hours	0
Minutes	0
End Time settings	
Month	Jan
Date	1
Year	2097
Hours	0
Minutes	0
Offset settings	
Offset	1 (1 - 1439) Minutes

Time Zone Configuration

용어	설명
Time Zone	전 세계적으로 다양한 시간대를 나열합니다. '수동 설정' 옵션은 특정 시간대로 설정이 가능합니다.
Hours	UTC로부터의 편차 시간. 이 필드는 '수동설정' 옵션일 때만 사용 가능합니다.
Minutes	UTC로부터의 편차 시간(분). 이 필드는 '수동설정' 옵션일 때만 사용 가능합니다.
Acronym	사용자 시간대의 약어를 설정할 수 있다.

Daylight Saving Time Configuration

용어	설명
Daylight Saving Time	Daylight Saving Time을 설정합니다. Disabled: 구성을 해제합니다. Recurring: Daylight Saving Time을 매년 구성을 반복하도록 구성합니다. Non-Recurring: Daylight Saving Time을 단일 시간에 고정 구성합니다.
Week	시작하는 주와 종료되는 주를 선택합니다.
Day/Date	시작하는 날과 끝나는 날을 선택합니다.
Month	시작하는 월과 끝나는 월을 선택합니다.

Hours	시작하는 시간과 끝나는 시간을 선택합니다.
Minutes	시작하는 분과 끝나는 분을 선택합니다.
Offset	Daylight Saving Time의 추가 시간 (분)을 입력합니다. (범위 : 1-1439).

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

✓ Time Zone Configuration

➢ *Time Zone*

- (UTC+09:00) Seoul

Time Zone Configuration

Time Zone Configuration	
Time Zone	(UTC+09:00) Seoul
Hours	9
Minutes	0
Acronym	(0 - 16 characters)

- Manual Setting

Time Zone Configuration

Time Zone Configuration	
Time Zone	Manual Setting
Hours	7
Minutes	10
Acronym	(0 - 16 characters)

➢ *Acronym*

Time Zone Configuration

Time Zone Configuration	
Time Zone	(UTC+09:00) Seoul
Hours	9
Minutes	0
Acronym	KOR_SEOUL (0 - 16 characters)

✓ Daylight Saving Time Configuration

➢ *Daylight Saving Time*

- Disable

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled

Start Time settings		
Month	Jan	
Date	1	
Year	2014	
Hours	0	
Minutes	0	
End Time settings		
Month	Jan	
Date	1	
Year	2097	
Hours	0	
Minutes	0	
Offset settings		
Offset	1	(1 - 1439) Minutes

- Recurring

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Recurring

Start Time settings	
Week	1
Day	Mon
Month	Jun
Hours	0
Minutes	0
End Time settings	
Week	4
Day	Mon
Month	Aug
Hours	0
Minutes	0
Offset settings	
Offset	1 (1 - 1439) Minutes

- Non-Recurring

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Non-Recurring

Start Time settings	
Month	May
Date	1
Year	2023
Hours	0
Minutes	0
End Time settings	
Month	Aug
Date	1
Year	2023
Hours	0
Minutes	0
Offset settings	
Offset	1 (1 - 1439) Minutes

CLI 설정 예시

✓ Time Zone Configuration

➢ *Time Zone*

- (UTC+09:00) Seoul

```
(config)# clock timezone '' <-23-23> <0-59> <0-9>
(config)# clock timezone '' 9 0 1
```

- Manual Setting

```
(config)# clock timezone '' <-23-23> <0-59> <0-9>
(config)# clock timezone '' 7 10 0
```

➢ *Acronym*

```
(config)# clock timezone <word16> <-23-23> <0-59> <0-9>
(config)# clock timezone KOR_SEOUL 9 0 1
```

✓ Daylight Saving Time Configuration

➢ *Daylight Saving Time*

- Disable

```
(config)# no clock summer-time
```

- Recurring

```
(config)# clock summer-time '' recurring <1-5> <1-7> <1-12> <hhmm>
<1-5> <1-7> <1-12> <hhmm> <1-1439>
(config)# clock summer-time '' recurring 1 1 6 00:00 4 1 8 00:00 60
```

- Non-Recurring

```
(config)# clock summer-time '' date <1-12> <1-31> <2000097> <hhmm>
<1-12> <1-31> <2000097> <hhmm> <1-1439>
(config)# clock summer-time '' date 5 1 2023 00:00 8 1 2023 00:00 60
```

설정 후 확인

✓ 설정 확인

본 문서 Information Monitor 에서 확인이 가능합니다.

✓ Daylight Saving Time Monitor

➢ ***WEB***

저장 후 동일 페이지에서 확인이 가능합니다.

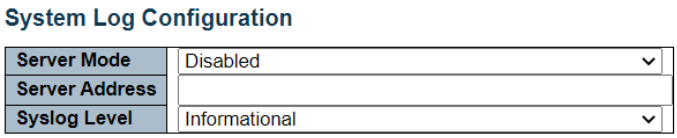
➢ ***CLI***

```
# show clock detail

System Time: 2023-05-17T18:00:58+10:00
Timezone: Timezone Offset : 5401 ( 540 minutes)
Timezone Acronym : KOR_SEOUL
Daylight Saving Time Mode : Non-Recurring.
Daylight Saving Time Start Time Settings :
        Week: 0
        Day: 0
      * Month: 5
      * Date: 1
      * Year: 2023
      * Hour: 0
      * Minute: 0
Daylight Saving Time End Time Settings :
        Week: 0
        Day: 0
      * Month: 8
      * Date: 1
      * Year: 2023
      * Hour: 0
      * Minute: 0
Daylight Saving Time Offset : 60 (minutes)
```

6.1.1.6. Log

웹메뉴 Configuration>System>Log

Log 메시지 및 log Level을 설정합니다.



System Log Configuration

용어	설명
Server Mode	모드 작업을 사용하도록 설정하면 syslog 메시지가 syslog 서버로 전송됩니다. Enabled: 서버 모드 작업을 사용합니다. Disabled: 서버 모드 작업을 사용하지 않습니다.
Server Address	syslog 서버의 IPv4 호스트 주소를 나타냅니다. 스위치가 DNS 기능을 제공하는 경우 도메인 이름일 수도 있습니다.
Syslog Level	syslog 서버로 보낼 메시지의 종류를 나타냅니다. Audit: 감사를 보냅니다. Error: 오류, 감사를 보냅니다. Warning: 경고, 오류, 감사를 보냅니다. Notice: 공지사항, 경고, 오류, 감사를 보냅니다. Informational: 정보, 공지사항, 경고, 오류, 감사를 보냅니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

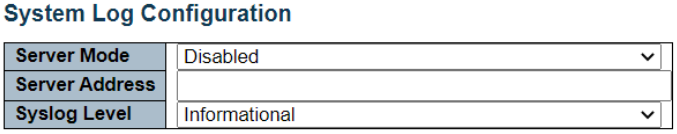
WEB 설정 예시

웹메뉴 Configuration>System>Log

✓ **System Log Configuration**

➢ ***Server Mode***

- Disable



- Enable

System Log Configuration

Server Mode	Enabled
Server Address	
Syslog Level	Informational

➢ ***Server Address***

- IPv4 Address (PC Address)

System Log Configuration

Server Mode	Enabled
Server Address	192.168.10.130
Syslog Level	Informational

➢ ***Syslog Level***

- Audit

System Log Configuration

Server Mode	Enabled
Server Address	192.168.10.130
Syslog Level	Audit

- Error

System Log Configuration

Server Mode	Enabled
Server Address	192.168.10.130
Syslog Level	Error

- Warning

System Log Configuration

Server Mode	Enabled
Server Address	192.168.10.130
Syslog Level	Warning

- Notice

System Log Configuration

Server Mode	Enabled
Server Address	192.168.10.130
Syslog Level	Notice

- Information

System Log Configuration

Server Mode	Enabled
Server Address	192.168.10.130
Syslog Level	Informational

CLI 설정 예시

✓ System Log Configuration

➢ ***Server Mode***

- Disable

```
(config)# no logging on
```

- Enable

```
(config)# logging on
```

➢ ***Server Address***

- IPv4 Address (PC Address)

```
(config)# logging host <ipv4_ucast>
(config)# logging host 192.168.10.130
```

➢ ***Syslog Level***

- Audit

```
(config)# logging level audit
```

- Error

```
(config)# logging level error
```

- Warning

```
(config)# logging level warning
```

- Notice

```
(config)# logging level notice
```

- Information

```
(config)# logging level informational
```

6.1.2. System Monitor

6.1.2.1. Information

웹메뉴 Monitor>System>Information

MAC주소, 시간, 버전등을 확인 할 수 있습니다.

System Information

System	
Contact	
Name	
Location	
Hardware	
MAC Address	00-21-6d-00-00-00
Device Serial	
Time	
System Date	1970-01-02T06:16:20+09:00
System Uptime	0d 21:16:20
Software	
Software Version	
Software Date	2023-07-17T15:20:33+09:00
System Temperature	
Current	42.000 'C (107.600 'F)
Minimum	39.500 'C (103.100 'F)
Maximum	53.500 'C (128.300 'F)
Average	42.000 'C (107.600 'F)

System Information

용어	설명
System	스위치의 시스템 정보를 표시합니다.
Contact	스위치 식별정보를 표시합니다.
Name	스위치 이름을 표시합니다.
Location	스위치 위치정보를 표시합니다.
Hardware	스위치의 하드웨어 정보를 표시합니다.
MAC Address	스위치의 MAC 주소를 표시합니다.
Device Serial	스위치의 Serial 번호를 표시합니다.
Time	스위치의 시간 정보를 표시합니다.
System Date	NTP를 사용할 경우, NTP서버에서 가져온 시간을 보여줍니다. 사용하지 않을 경우에는 스위치가 부팅된 후 "GMT"기준시간(1970년 1월1일 0시 0분0초)으로 경과한 시간을 표시합니다.
System Uptime	장치가 동작하고 있는 시간을 표시합니다.
Software	스위치의 소프트웨어 정보를 표시합니다.
Software Version	스위치의 소프트웨어 버전을 표시합니다.
Software Data	스위치 소프트웨어가 생성 된 날짜를 표시합니다.

System Temperature	스위치의 온도 정보를 표시합니다.
Current	스위치 내부의 현재 온도 값을 표시합니다.
Minimum	스위치 내부의 최소온도 값을 표시합니다.
Maximum	스위치 내부의 최대온도 값을 표시합니다.
Average	스위치 내부의 평균온도 값을 표시합니다.

WEB 확인 예시

웹메뉴 Monitor>System>Information

System Information

System	
Contact	SOLTECH
Name	TESTSWITCH
Location	SOLTECH-LAB
Hardware	
MAC Address	00-21-6d-00-00-00
Device Serial	
Time	
System Date	1970-01-02T05:59:39+09:00
System Uptime	0d 20:59:39
Software	
Software Version	
Software Date	2023-07-17T15:20:33+09:00
System Temperature	
Current	42.000 'C (107.600 'F)
Minimum	39.500 'C (103.100 'F)
Maximum	53.500 'C (128.300 'F)
Average	42.000 'C (107.600 'F)

CLI 확인 예시

✓ **System Information**

```
TESTSWITCH# show version

# show version
MEMORY : Total=208355 KBytes, Free=181987 KBytes, Max=181905 Kbytes
FLASH : 0x40000000-0x40ffffff, 256 x 0x10000 blocks
MAC Address : 00-21-6d-00-00-00
Board Serial :
Previous Restart : Cool
System Contact : SOLTECH
System Name : TESTSWITCH
System Location : SOLTECH-LAB
System Time : 1970-01-02T07:24:10+09:00
```

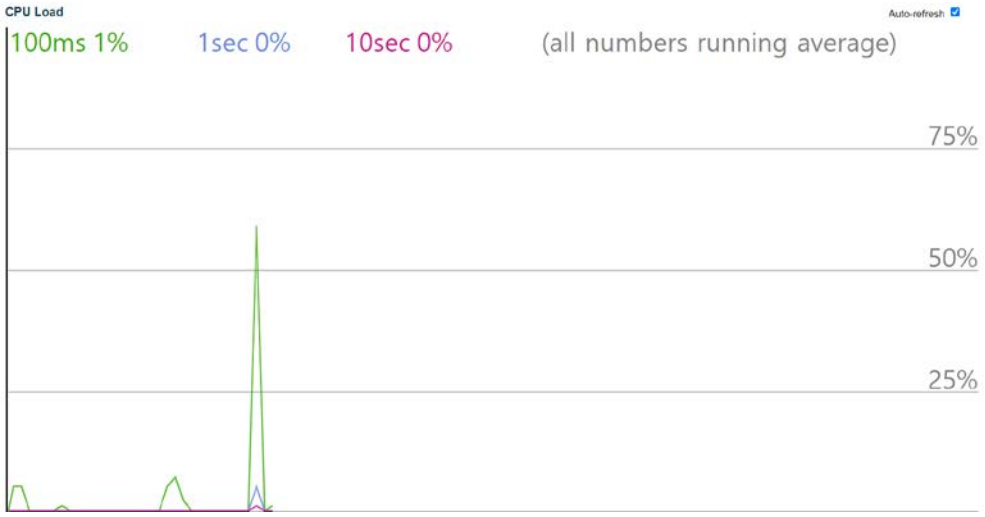
```
System Uptime     : 21:24:10

Image             : SFC4100AB.dat (primary)
Version           : OneImg_JAGUAR2 (standalone) build 5.0.3.0 by Soltech Corp.
Date              : 2023-07-21T14:21:27+09:00
Bank-Index        : Bank1

Alternate Image
---------------
Image             : SFC4100AB.dat (backup)
Version           : OneImg_JAGUAR2 (standalone) build 5.0.1.0 by Soltech Corp.
Date              : 2023-07-17T15:20:33+09:00
Bank-Index        : Bank0
```

```
TESTSWITCH# show system temperature status

   System Temperature Current: 39.500'C (103.100'F)
   System Temperature min: 36.000'C (96.800'F)
   System Temperature Max: 49.500'C (121.100'F)
   System Temperature Average: 39.500'C (103.100'F)
```

6.1.2.2. CPU Load

웹메뉴 Monitor>System>CPU Load

CPU 로드를 SVG 그래프를 이용하여 표시합니다.

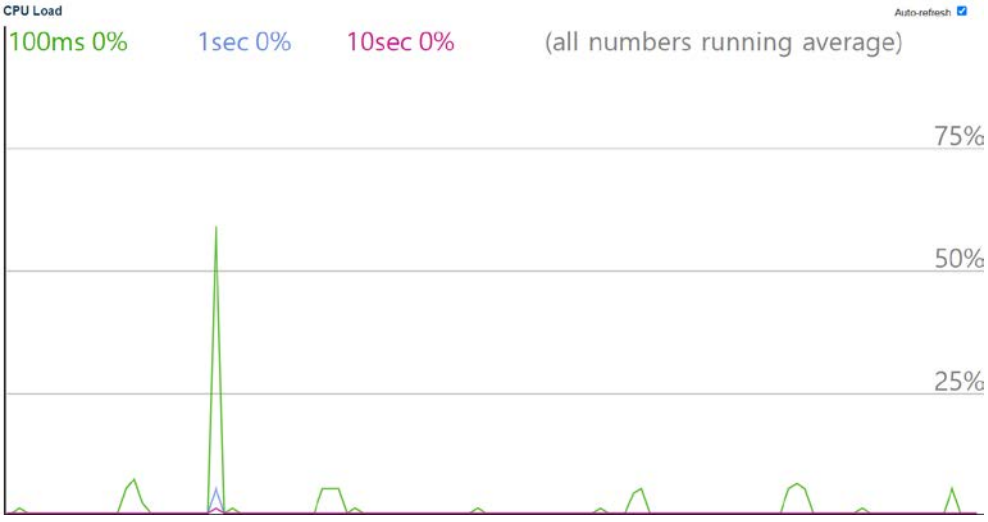


Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다

WEB 확인 예시

웹메뉴 Monitor>System>CPU Load



CLI 확인 예시

```
# show system cpu status

    Average load in 100 ms: 2%
    Average load in 1 sec: 1%
    Average load in 10 sec: 0%
```

6.1.2.3. IP Status

웹메뉴 Monitor>System>IP Status

스위치 정보와 연결된 다른 장비의 정보를 확인할 수 있습니다.

IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-21-6d-00-87-32	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.10.101/24	
VLAN1	IPv6	fe80::221:6dff:fe00:8732/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.10.130	VLAN1:c0-18-50-7e-50-56
fe80::221:6dff:fe00:8732	VLAN1:00-21-6d-00-87-32

IP Interface

용어	설명
Interface	인터페이스의 이름을 표시합니다.
Type	인터페이스의 주소 형식을 표시합니다.
Address	(특정 유형의)인터페이스의 현재 주소를 표시합니다.
Status	인터페이스의 상태를 표시합니다.

IP Routes

용어	설명
Network	Routes의 호스트 주소를 표시합니다.
Gateway	Routes의 게이트 웨이 주소를 표시합니다.
Status	Routes의 상태를 표시합니다.

Neighbour cache

용어	설명
IP Address	Neighbour cache의 IP주소를 표시합니다.
Link Address	Neighbour cache의 Link Address를 표시합니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다

Refresh : 클릭 시 페이지를 새로 고침.

WEB 확인 예시

IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	::1/128	
OS:lo	IPv6	fe80::1/64	
VLAN1	LINK	00-21-6d-00-87-32	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.10.101/24	
VLAN1	IPv6	fe80::221:6dff:fe00:8732/64	
VLAN2	LINK	00-21-6d-00-87-32	<UP BROADCAST RUNNING MULTICAST>
VLAN2	IPv4	2.2.2.2/24	
VLAN2	IPv6	fe80::221:6dff:fe00:8732/64	

IP Routes

Network	Gateway	Status
0.0.0.0/0	192.168.10.1	<UP GATEWAY HW_RT>
3.3.3.0/24	192.168.10.1	<UP GATEWAY HW_RT>
127.0.0.1/32	127.0.0.1	<UP HOST>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.10.130	VLAN1:c0-18-50-7e-50-56
fe80::221:6dff:fe00:8732	VLAN1:00-21-6d-00-87-32
fe80::221:6dff:fe00:8732	VLAN2:00-21-6d-00-87-32

CLI 확인 예시

✓ **IP Interfaces**

```
# show interface vlan

VLAN1
  LINK: 00-21-6d-00-87-32 Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
  IPv4: 192.168.10.101/24 192.168.10.255
  IPv6: fe80::221:6dff:fe00:8732/64 <UP RUNNING>

VLAN2
  LINK: 00-21-6d-00-87-32 Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
  IPv4: 2.2.2.2/24 2.2.2.255
  DHCP: State: FALLBACK
  IPv6: fe80::221:6dff:fe00:8732/64 <UP RUNNING>
```

✓ **IP Routes**

```
# show ip route

0.0.0.0/0 via 192.168.10.1 <UP GATEWAY HW_RT>
2.2.2.0/24 via interface index 2 <UP HW_RT>
3.3.3.0/24 via 192.168.10.1 <UP GATEWAY HW_RT>
127.0.0.1/32 via 127.0.0.1 <UP HOST>
192.168.10.0/24 via interface index 1 <UP HW_RT>
224.0.0.0/4 via 127.0.0.1 <UP>
```

✓ **Neighbour cache**

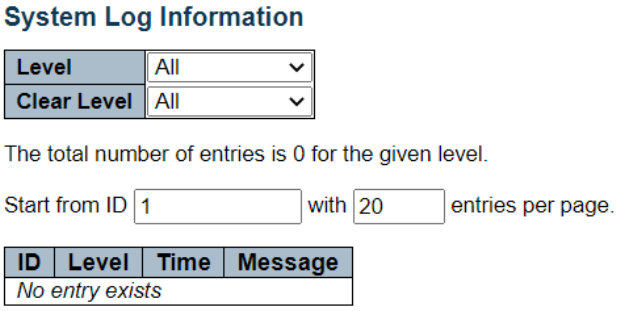
```
# show ip arp

192.168.10.1 (Incomplete)
192.168.10.130 via VLAN1:c0-18-50-7e-50-56
```

```
# show ipv6 neighbor

fe80::221:6dff:fe00:8732 via VLAN1: 00-21-6d-00-87-32
Permanent/REACHABLE
fe80::221:6dff:fe00:8732 via VLAN2: 00-21-6d-00-87-32
Permanent/REACHABLE
```

6.1.2.4. Log

웹메뉴 Monitor>System>Log

Log 메시지 및 log Level을 확인합니다.



System Log Information

용어	설명
Level	시스템 로그 중 해당 레벨 정보만 찾아 보여줍니다
Clear Level	시스템 로그 중 삭제할 레벨을 정합니다.
ID	시스템 로그 항목의 ID를 보여줍니다.
Level	시스템 로그 항목의 레벨을 보여줍니다. Audit: 시스템 로그의 감사 수준. Error: 시스템 로그의 오류 수준. Warning: 시스템 로그의 경고 수준. Notice: 시스템 로그의 공지사항 수준. Informational: 시스템 로그 정보의 수준. All: 모든 레벨.
Time	시스템 로그 항목의 시간을 보여줍니다.
Message	시스템 로그 항목의 메시지를 보여줍니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침. 로컬 변경 사항은 취소합니다.

Clear : 선택한 로그 항목을 삭제합니다.

|<< : 현재 표시되는 마지막 항목에 종료, 시스템 로그 항목을 업데이트 합니다.

<< : 현재 표시되는 마지막 항목에 종료, 시스템 로그 항목을 업데이트 합니다.

>> : 현재 표시되는 마지막 항목에서 시작하여, 시스템 로그 항목을 업데이트 합니다.

>>| : 가능한 마지막 항목의 ID에 종료, 시스템 로그 항목을 업데이트 합니다.

WEB 확인 예시

웹메뉴 Monitor>System>Log

✓ System Log Information

System Log Information

Level	All
Clear Level	All

The total number of entries is 27 for the given level.

Start from ID 1 with 50 entries per page.

ID	Level	Time	Message
1	Audit	1970-01-01T00:00:00+00:00	Audit Log Start, Image:[SFC8100G 5.0.0.4]
2	Info.	1970-01-01T00:00:02+00:00	SYS-BOOTING: Switch just made a cool boot.
3	Audit	1970-01-01T00:00:02+00:00	TELNET server started on port 23.
4	Notice	1970-01-01T00:00:02+00:00	LINK-UPDOWN: Intf. Vlan 1, changed state to down.
5	Audit	1970-01-01T00:00:02+00:00	Intf. Port:1 TEST Ok!!!, (CAP:0x0000303F)
6	Audit	1970-01-01T00:00:02+00:00	Intf. Port:2 TEST Ok!!!, (CAP:0x0000303F)
7	Audit	1970-01-01T00:00:02+00:00	Intf. Port:3 TEST Ok!!!, (CAP:0x0000303F)
8	Audit	1970-01-01T00:00:02+00:00	Intf. Port:4 TEST Ok!!!, (CAP:0x0000303F)
9	Audit	1970-01-01T00:00:02+00:00	Intf. Port:5 TEST Ok!!!, (CAP:0x048E1171)
10	Audit	1970-01-01T00:00:02+00:00	Intf. Port:6 TEST Ok!!!, (CAP:0x048E1171)
11	Audit	1970-01-01T00:00:02+00:00	Intf. Port:7 TEST Ok!!!, (CAP:0x048E1171)
12	Audit	1970-01-01T00:00:02+00:00	Intf. Port:8 TEST Ok!!!, (CAP:0x048E1171)
13	Audit	1970-01-01T00:00:03+00:00	SNMP server Stop.
14	Audit	1970-01-01T00:00:03+00:00	HTTP server started on port 80.
15	Notice	1970-01-01T00:00:06+00:00	LINK-UPDOWN: Intf. GigabitEthernet 1/4, changed state to up.
16	Notice	1970-01-01T00:00:08+00:00	LINK-UPDOWN: Intf. Vlan 1, changed state to up.
17	Audit	1970-01-01T00:00:09+00:00	SSH server started on port 22.
18	Audit	1970-01-01T00:00:10+00:00	HTTPs server started on port 443.
19	Audit	1970-01-01T00:00:13+00:00	User [admin] logged on Console
20	Notice	1970-01-01T00:00:31+00:00	LINK-UPDOWN: Intf. Vlan 1, changed state to up.
21	Audit	1970-01-01T00:00:41+00:00	User [admin] logged on HTTP
22	Notice	1970-01-01T00:01:38+00:00	LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to up.
23	Notice	1970-01-01T00:01:40+00:00	LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to down.
24	Notice	1970-01-01T00:01:47+00:00	LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to up.
25	Notice	1970-01-01T00:01:52+00:00	LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to down.
26	Notice	1970-01-01T00:02:07+00:00	LINK-UPDOWN: Intf. GigabitEthernet 1/1, changed state to up.
27	Notice	1970-01-01T00:02:11+00:00	LINK-UPDOWN: Intf. GigabitEthernet 1/1, changed state to down.

➢ *Level*

- example notice

  선택 Notice> Refresh 버튼 클릭 (공지사항 항목만 확인)

System Log Information

Level	Notice
Clear Level	All

The total number of entries is 10 for the given level.

Start from ID 4 with 50 entries per page.

ID	Level	Time	Message
4	Notice	1970-01-01T00:00:02+00:00	LINK-UPDOWN: Intf. Vlan 1, changed state to down.
15	Notice	1970-01-01T00:00:06+00:00	LINK-UPDOWN: Intf. GigabitEthernet 1/4, changed state to up.
16	Notice	1970-01-01T00:00:08+00:00	LINK-UPDOWN: Intf. Vlan 1, changed state to up.
20	Notice	1970-01-01T00:00:31+00:00	LINK-UPDOWN: Intf. Vlan 1, changed state to up.
22	Notice	1970-01-01T00:01:38+00:00	LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to up.
23	Notice	1970-01-01T00:01:40+00:00	LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to down.
24	Notice	1970-01-01T00:01:47+00:00	LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to up.
25	Notice	1970-01-01T00:01:52+00:00	LINK-UPDOWN: Intf. GigabitEthernet 1/2, changed state to down.
26	Notice	1970-01-01T00:02:07+00:00	LINK-UPDOWN: Intf. GigabitEthernet 1/1, changed state to up.
27	Notice	1970-01-01T00:02:11+00:00	LINK-UPDOWN: Intf. GigabitEthernet 1/1, changed state to down.

➢ *Clear Level*

- example notice

선택 Notice> Clear 버튼 클릭(공지사항 항목만 삭제)

System Log Information

Level	All
Clear Level	Notice

The total number of entries is 18 for the given level.

Start from ID 1 with 50 entries per page.

ID	Level	Time	Message
1	Audit	1970-01-01T00:00:00+00:00	Audit Log Start, Image:[SFC8100G 5.0.0.4]
2	Info.	1970-01-01T00:00:02+00:00	SYS-BOOTING: Switch just made a cool boot.
3	Audit	1970-01-01T00:00:02+00:00	TELNET server started on port 23.
5	Audit	1970-01-01T00:00:02+00:00	Intf. Port:1 TEST Ok!!!, (CAP:0x0000303F)
6	Audit	1970-01-01T00:00:02+00:00	Intf. Port:2 TEST Ok!!!, (CAP:0x0000303F)
7	Audit	1970-01-01T00:00:02+00:00	Intf. Port:3 TEST Ok!!!, (CAP:0x0000303F)
8	Audit	1970-01-01T00:00:02+00:00	Intf. Port:4 TEST Ok!!!, (CAP:0x0000303F)
9	Audit	1970-01-01T00:00:02+00:00	Intf. Port:5 TEST Ok!!!, (CAP:0x048E1171)
10	Audit	1970-01-01T00:00:02+00:00	Intf. Port:6 TEST Ok!!!, (CAP:0x048E1171)
11	Audit	1970-01-01T00:00:02+00:00	Intf. Port:7 TEST Ok!!!, (CAP:0x048E1171)
12	Audit	1970-01-01T00:00:02+00:00	Intf. Port:8 TEST Ok!!!, (CAP:0x048E1171)
13	Audit	1970-01-01T00:00:03+00:00	SNMP server Stop.
14	Audit	1970-01-01T00:00:03+00:00	HTTP server started on port 80.
17	Audit	1970-01-01T00:00:09+00:00	SSH server started on port 22.
18	Audit	1970-01-01T00:00:10+00:00	HTTPs server started on port 443.
19	Audit	1970-01-01T00:00:13+00:00	User [admin] logged on Console
21	Audit	1970-01-01T00:00:41+00:00	User [admin] logged on HTTP
28	Audit	1970-01-01T00:05:36+00:00	User [admin] logouted on Console

CLI 확인 예시

✓ **System Log Information**

```
# show logging

Switch logging host mode is enabled
Switch logging host address is 192.168.10.130
Switch logging level is info.
Number of entries on Switch 1:
Audit: 18
Error: 0
Warning: 0
Notice: 4
Info.: 1
All: 23

ID   Level    Time                      Message
---- -------- ------------------------  -------------------------------

   1 Audit    1970-01-01T00:00:00+00:00 Audit Log Start, Image: [SFC8100G 5.0.0.4]
   2 Info.    1970-01-01T00:00:02+00:00 SYS-BOOTING: Switch just made a cool boot.
   3 Audit    1970-01-01T00:00:02+00:00 TELNET server started on port 23.
   4 Notice   1970-01-01T00:00:02+00:00 LINK-UPDOWN: Intf. Vlan 1, changed state to
down.
   5 Audit    1970-01-01T00:00:02+00:00 Intf. Port:1 TEST Ok!!!, (CAP:0x0000303F)
```

```
 6 Audit     1970-01-01T00:00:02+00:00  Intf. P
                                                  [admin] logged on HTTP
22 Audit     1970-01-01T00:15:30+00:00 User admin logouted on HTTP
23 Audit     1970-01-01T00:15:35+00:00 User [admin] logged on HTTP
```

➢ ***Level***

- example notice

```
# show logging notice

Switch logging host mode is disabled
Switch logging host address is null
Switch logging level is info.

Number of entries on Switch 1:

Audit: 18
Error: 0
Warning: 0
Notice: 4
Info.: 1
All: 23

ID  Level   Time                    Message

---- -------- ------------------------  ------------------------------

4  Notice  1970-01-01T00:00:02+00:00 LINK-UPDOWN: Intf. Vlan 1, changed state to down.
16 Notice  1970-01-01T00:00:06+00:00 LINK-UPDOWN: Intf. GigabitEthernet 1/4, changed state to up.
18 Notice  1970-01-01T00:00:08+00:00 LINK-UPDOWN: Intf. Vlan 1, changed state to up.
20 Notice  1970-01-01T00:00:35+00:00 LINK-UPDOWN: Intf. Vlan 1, changed state to up.
```

➢ ***Clear Level***

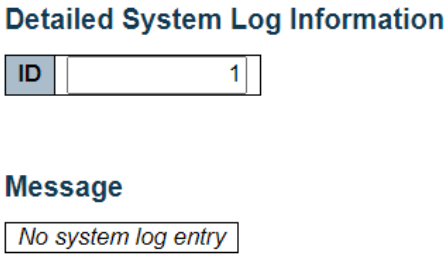
- example notice

```
# clear logging notice

# show logging notice

Switch logging host mode is enabled
Switch logging host address is 192.168.10.130
Switch logging level is info.

Number of entries on Switch 1:
Audit: 18
Error: 0
Warning: 0
Notice: 0
Info.: 1
All: 19
```

6.1.2.5. Detailed Log

웹메뉴 Monitor>System>Detailed Log

스위치 시스템의 상세한 로그 정보를 제공합니다.



Detailed System Log Information

용어	설명
ID	시스템 로그 항목의 ID입니다.
Message	시스템 로그 항목의 메시지입니다.

Buttons

Refresh: 클릭 시 페이지를 새로 고침.

|<<: 현재 표시되는 마지막 항목에 종료, 시스템 로그 항목을 업데이트 합니다.

<<: 현재 표시되는 마지막 항목에 종료, 시스템 로그 항목을 업데이트 합니다.

>>: 현재 표시되는 마지막 항목에서 시작하여, 시스템 로그 항목을 업데이트 합니다.

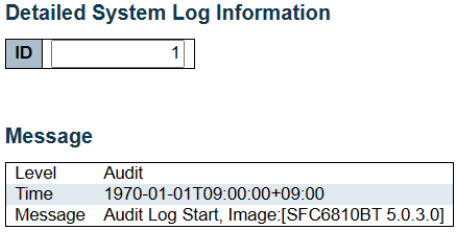
>>|: 가능한 마지막 항목의 ID에 종료, 시스템 로그 항목을 업데이트 합니다.

WEB 확인 예시

웹메뉴 Monitor>System>Detailed Log

✓ **Detailed System Log Information**

➢ ***ID***



CLI 확인 예시

✓ Detailed System Log Information

➢ ***ID***

```
# show logging <1-4294967295>

# show logging 1
Switch : 1
ID     : 1
Level  : Audit
Time   : 1970-01-01T09:00:00+09:00
Message:
Audit Log Start, Image:[SFC8100BT 5.0.3.0]
```

6.2. Green Ethernet

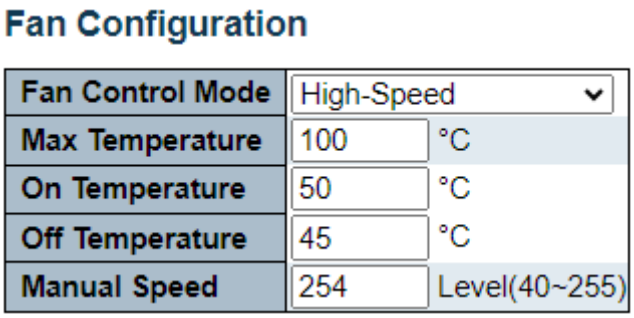
6.2.1. Green Ethernet Configuration

6.2.1.1.Fan

웹메뉴 Configuration>Green Ethernet>Fan

이 페이지는 사용자가 팬을 제어하기 위한 현재 설정을 검사하고 구성할 수 있게 해줍니다.

시스템에 여러 온도 센서가 있으면 가장 높은 온도가 팬을 제어하는 데 사용됩니다.



Fan Configuration

용어	설명
Fan Control Mode	Fan의 동작모드를 설정합니다. **Fan-off** Fan의 가동을 정지합니다. **Auto (with Temp.)** Fan의 가동을 스위치 내부의 온도센서를 이용하여 동작하는 설정입니다. On Temperature 설정온도에서 Fan이 동작, Off Temperature에서 Fan이 정지합니다. **Low-Speed** Fan Speed가 Max Speed대비 30%의 속도로 고정됩니다. **Medium-Speed** Fan Speed가 Max Speed대비 60%의 속도로 고정됩니다. **High-Speed** Fan Speed가 Max Speed로 고정됩니다. **Manual-Speed** Fan Speed를 수동으로 설정합니다.
Max Temperature	팬이 최고 속도로 작동하는 온도입니다. Max Temperature 설정 값은 On Temperature보다 커야 합니다.
On Temperature	Mode - Auto(with Temp.)설정 시 팬이 켜지는 온도입니다.
Off Temperature	Mode - Auto(with Temp.)설정 시 팬이 꺼지는 온도입니다. Off Temperature 설정 값은 On Temperature보다 작거나 같아야 합니다.
Manual Speed	Mode - Manual-Speed 설정 시 팬의 속도를 설정합니다. 설정 가능한 속도는 40~255 Level입니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

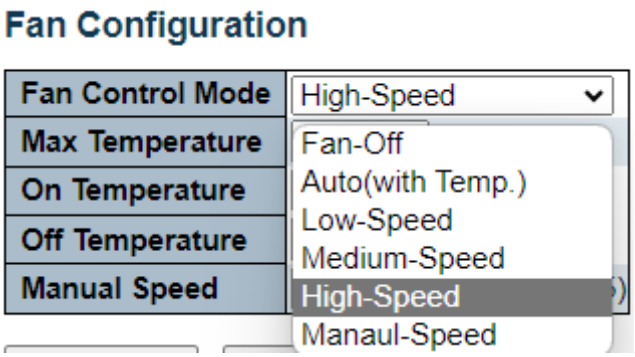
WEB 설정 예시

웹메뉴 Configuration>Green Ethernet>Fan

✓ Fan Configuration

➢ ***Fan Control Mode***

- Fan-Off | Auto(with Temp.) | Low-Speed | Medium-Speed | High-Speed | Manual-Speed



➢ ***Max Temperature***

- ***100℃(-127℃~127℃)***

➢ ***On Temperature***

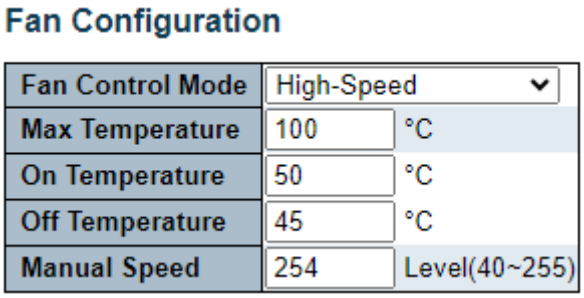
- ***50℃(-127℃~127℃)***

➢ ***Off Temperature***

- ***45℃(-127℃~127℃)***

➢ ***Manual Speed***

- ***254 (40~255)***



CLI 설정 예시

✓ Fan Configuration

➢ *Fan Control Mode*

- Fan-Off | Auto(with Temp.) | Low-Speed | Medium-Speed | High-Speed | Manual-Speed

```
(config)# green-ethernet fan mode { auto | disable | static-low | static-medium |
static-high | { manual-val [ <manual_speed_lvl> ] } }
(config)# green-ethernet fan mode disable
(config)# green-ethernet fan mode auto
(config)# green-ethernet fan mode static-low
(config)# green-ethernet fan mode static-medium
(config)# green-ethernet fan mode static-high
(config)# green-ethernet fan mode manual-val
```

➢ *Max Temperature*

- ***100℃ (-127℃~127℃)***

```
(config)# green-ethernet fan temp-max <new_temp>
(config)# green-ethernet fan temp-max 100
```

➢ *On Temperature*

- ***50℃ (-127℃~127℃)***

```
(config)# green-ethernet fan temp-on <new_temp>
(config)# green-ethernet fan temp-on 50
```

➢ *Off Temperature*

- ***45℃ (-127℃~127℃)***

```
(config)# green-ethernet fan temp-off <new_temp>
(config)# green-ethernet fan temp-off 45
```

➢ *Manual Speed*

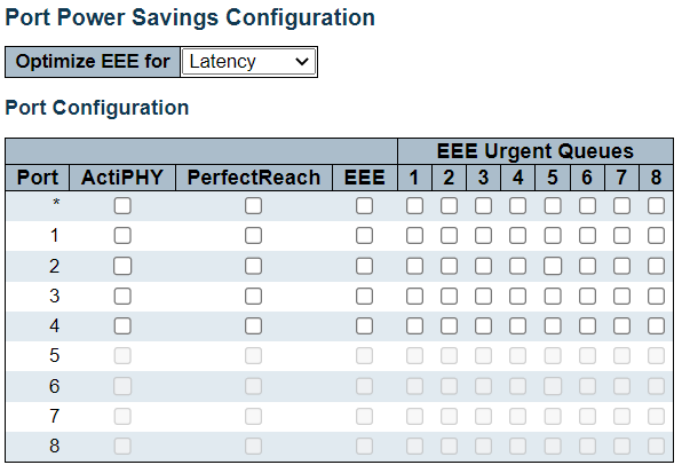
- ***254 (40~255)***

```
(config)# green-ethernet fan mode { auto | disable | static-low | static-medium |
static-high | { manual-val [ <manual_speed_lvl> ] } }
(config)# green-ethernet fan mode manual-val 254
```

6.2.1.2. Port Power Savings

웹메뉴 Configuration>Green Ethernet>Port Power Savings

스위치의 포트 절전기능을 구성 할 수 있습니다.



Port Power Saving Configuration

용어	설명
Optimize EEE for	EEE를 최적화하도록 스위치를 설정하는 옵션입니다. Latency: 트래픽 지연시간을 최소화하도록 하는 옵션 Power: 전력 절약을 최적화하는 옵션

Port Configuration

용어	설명
Port	스위치 포트 번호입니다.
ActiPHY	ActiPHY는 링크가 없을 때 포트의 전원을 낮추는 방식으로 작동합니다.
PerfectReach	짧은 케이블이 있는 포트 전력을 낮추는 방식으로 작동합니다.
EEE	스위치 포트에 대해 EEE를 사용하는 것을 제어합니다. EEE는 이더넷 네트워크에서 실제 트래픽 수요에 따라 네트워크 장치가 비 활동 상태일 때 저전력 수면 모드로 전환하여 전력 소비를 줄이는 기능입니다.
EEE Urgent Queues	체크된 큐는 데이터가 보내질 수 있는 즉시 프레임 전송을 활성화합니다. 체크되지 않으면 데이터가 보내질 수 있어도 프레임버스트 기능을 사용할 때까지 대기하다 보내집니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>Green Ethernet>Port Power Savings

✓ **Port Power Saving Configuration**

➢ ***Optimize EEE for***

- Latency

Port Power Savings Configuration

Optimize EEE for: Latency

Port Configuration

				EEE Urgent Queues							
Port	ActiPHY	PerfectReach	EEE	1	2	3	4	5	6	7	8
*	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

- Power

Port Power Savings Configuration

Optimize EEE for: Power

Port Configuration

				EEE Urgent Queues							
Port	ActiPHY	PerfectReach	EEE	1	2	3	4	5	6	7	8
*	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

➢ ***ActiPHY***

Port Power Savings Configuration

Optimize EEE for: Power

Port Configuration

				EEE Urgent Queues							
Port	ActiPHY	PerfectReach	EEE	1	2	3	4	5	6	7	8
*	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
1	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

➢ ***PerfectReach***

Port Power Savings Configuration

Optimize EEE for: Power

Port Configuration

Port	ActiPHY	PerfectReach	EEE	EEE Urgent Queues 1	2	3	4	5	6	7	8
*	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

➢ ***EEE (Energy-Efficient Ethernet)***

Port Power Savings Configuration

Optimize EEE for: Power

Port Configuration

Port	ActiPHY	PerfectReach	EEE	EEE Urgent Queues 1	2	3	4	5	6	7	8
*	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

➢ ***EEE Urgent Queues***

Port Power Savings Configuration

Optimize EEE for: Power

Port Configuration

Port	ActiPHY	PerfectReach	EEE	EEE Urgent Queues 1	2	3	4	5	6	7	8
*	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☑	☐	☐	☐	☐	☐	☐	☑	☑
3	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☑	☐	☐	☐	☐	☐	☑	☑	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

CLI 설정 예시

✓ Port Power Saving Configuration

➢ *Optimize EEE for*

- Latency

```
(config)# no green-ethernet eee optimize-for-power
```

- Power

```
(config)# green-ethernet eee optimize-for-power
```

➢ *ActiPHY*

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# green-ethernet energy-detect
```

➢ *PerfectReach*

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# green-ethernet short-reach
```

➢ *EEE (Energy-Efficient Ethernet)*

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# green-ethernet eee
```

➢ *EEE Urgent Queues*

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# green-ethernet eee urgent-queues <range_list>
(config-if)# green-ethernet eee urgent-queues 1,7
(config-if)# green-ethernet eee urgent-queues 5-6
```

6.2.2. Green Ethernet Monitor

6.2.2.1. Port Power Savings

웹메뉴 Monitor>Green Ethernet>Port Power Savings

스위치의 포트 절전기능의 현재 상태를 확인할 수 있습니다.

Port Power Savings Status

Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE In power save	ActiPhy Savings	PerfectReach Savings
1		✓	✗	✗	✗	✗	✗
2		✓	✗	✗	✗	✗	✗
3		✓	✗	✗	✗	✗	✗
4		✓	✗	✓	✗	✗	✗
5		✗	✗	✗	✗	✗	✗
6		✗	✗	✗	✗	✗	✗
7		✗	✗	✗	✗	✗	✗
8		✗	✗	✗	✗	✗	✗

Port Power Saving Status

용어	설명
Port	논리적 포트 번호입니다.
Link	포트의 링크 상태를 보여줍니다 (녹색 = 링크 연결됨, 빨강 = 링크 연결 끊김).
EEE cap	포트가 EEE를 지원하는지를 보여줍니다.
EEE Ena	포트 EEE가 활성화되어 있는지를 보여줍니다.
LP EEE cap	링크 파트너가 EEE를 지원하는지를 보여줍니다.
EEE In power save	현재 EEE로 인해 전력을 절약 중인지 상태를 보여줍니다.
Actiphy Savings	현재 ActiPhy로 인해 전력을 절약 중인지 상태를 보여줍니다.
PerfectReach Savings	현재 PerfectReach로 인해 전력을 절약 중인지 상태를 보여줍니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

WEB 확인 예시

✓ Port Power Saving Status

Port Power Savings Status

Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE In power save	ActiPhy Savings	PerfectReach Savings
1	●	✓	✓	✗	✗	✓	✗
2	●	✓	✓	✗	✗	✗	✓
3	●	✓	✓	✗	✗	✓	✗
4	●	✓	✓	✓	✓	✗	✓
5	●	✗	✗	✗	✗	✗	✗
6	●	✗	✗	✗	✗	✗	✗
7	●	✗	✗	✗	✗	✗	✗
8	●	✗	✗	✗	✗	✗	✗

CLI 확인 예시

✓ Port Power Saving Status

```
# show green-ethernet

Interface    Link  Energy-detect  Short-Reach  EEE Capable  EEE Enabled  LP EEE Capable  EEE In Power Save

-------------------- --- -------- ----------- ----------- ----------- --------------- -----------------
GigabitEthernet 1/1   No   Yes      No          Yes          Yes          No              No
GigabitEthernet 1/2   Yes  No       Yes         Yes          Yes          No              No
GigabitEthernet 1/3   No   Yes      No          Yes          Yes          No              No
GigabitEthernet 1/4   Yes  No       Yes         Yes          Yes          Yes             Yes
10GigabitEthernet 1/1 No   N/A      N/A          No           N/A          N/A             N/A
10GigabitEthernet 1/2 No   N/A      N/A          No           N/A          N/A             N/A
10GigabitEthernet 1/3 No   N/A      N/A          No           N/A          N/A             N/A
10GigabitEthernet 1/4 No   N/A      N/A          No           N/A          N/A             N/A
```

6.2.2.2. Fan

웹메뉴 Monitor>Green Ethernet>Fan

팬 제어에 관련된 정보에 대한 개요를 제공하는 페이지입니다.

Fan Status

Fan Status		
Fan Speed	0	RPM
Temperature Sensor No:1	57	°C

Fan Status

용어	설명
Fan Speed	팬이 현재 RPM(분당 회전 수)으로 작동 중인 속도를 보여줍니다.
Temperature Sensor	온도 센서(들)의 온도를 섭씨 온도로 표시합니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

WEB 확인 예시

Fan Status

Fan Status		
Fan Speed	0	RPM
Temperature Sensor No:1	57	°C

CLI 확인 예시

✓ **Fan Status**

```
# show green-ethernet fan
Chip Temp.  Duty cycle  Fan Speed
    57 C         0         0 RPM
```

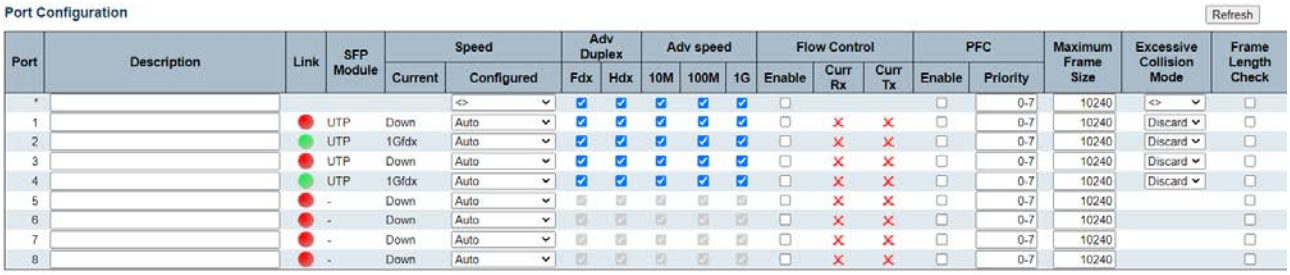
6.3. Ports

6.3.1. Ports Configuration

6.3.1.1. Ports

웹메뉴 Configuration>Ports

현재 포트 구성을 표시합니다. 또한, 각 포트설정도 할 수 있습니다.



Port Configuration

용어	설명
Port	논리적인 포트 번호입니다.
Description	포트의 설명입니다. 최대 256자로 이루어진 문자열입니다.
Link	포트의 링크 상태를 보여줍니다 (녹색 = 링크 연결, 빨강 = 링크 연결 끊기거나 Disable상태 느낌표 = 링크 연결, Speed 설정 불량)
PHY	포트의 물리계층(Physical layer)을 의미합니다. UTP와 SFP 포트로 분류됩니다. SFP 포트의 경우, 삽입된 광모듈의 최대 속도 정보가 표시됩니다.
Speed – Current	포트의 현재 링크 속도를 제공합니다.
Speed – Configured	지정된 스위치 포트에 대해 사용 가능한 링크 속도를 선택합니다. 특정 포트에서 지원되는 속도만 표시됩니다. 가능한 속도는 다음과 같습니다: Disabled - 스위치 포트의 작동을 불가능하게 합니다. Auto - 자동으로 상대방 링크와 호환되는 최고 속도로 포트를 연결합니다. 10Mbps HDX-포트를 10Mbps HDX 모드로만 설정합니다. 10Mbps FDX-포트를 10Mbps FDX 모드로만 설정합니다. 100Mbps HDX-포트를 100Mbps HDX 모드로만 설정합니다. 100Mbps FDX-포트를 100Mbps FDX 모드로만 설정합니다. 1Gbps FDX-포트를 1Gbps FDX 모드로만 설정합니다. 1Gbps C37 - 포트를 1Gbps CLAUSE37 자동 협상 모드로만 설정합니다. 10Gbps FDX–포트를 10Gbps FDX 모드로만 설정합니다. 2.5Gbps FDX - 포트를 2.5Gbps FDX 모드로만 설정합니다. SFP_Auto_AMS - SFP의 속도를 자동으로 결정합니다. 참고: SFP 자동 감지에는 표준화된 방법이 없으므로, 여기에서는 SFP ROM을 읽어 속도를 결정합니다. 표준화된 SFP 자동 감지 방법이 없기

	때문에 일부 SFP는 감지되지 않을 수 있습니다. 포트는 AMS 모드로 설정되며, Cu 포트는 자동 모드로 설정됩니다. 100-FX: 100-FX 속도의 SFP 포트. Cu 포트 비활성화됨. 1000-X: 1000-X 속도의 SFP 포트. Cu 포트 비활성화됨. AMS 모드에서 1000-X 속도를 사용하는 포트는 Cu 포트를 선호함. AMS 모드에서 1000-X 속도를 사용하는 포트는 광섬유 포트를 선호함. AMS 모드에서 100-FX 속도를 사용하는 포트는 광섬유 포트를 선호함.
Advertise Duplex	Duplex를 Auto로 설정하면 포트는 자동 협상을 통해 최선의 듀플렉스 옵션을 선택하고 이를 링크파트너에게 알립니다. Auto가 아닌 다른 값을 설정하면 포트는 해당 값에 해당하는 듀플렉스 옵션만을 알리게 됩니다.
Advertise Speed	속도가 Auto로 설정되면(자동 협상), 포트는 링크 파트너에게 지정된 속도(10M, 100M, 1G)만 알립니다. Auto로 설정된 기본 포트는 지원되는 모든 속도를 알립니다.
Flow Control	Auto가 선택된 경우, 포트는 링크 파트너에게 지원하는 플로우 컨트롤 기능을 알립니다. 즉, 양방향으로 플로우 컨트롤이 가능한지 여부를 알리게 됩니다. 고정 속도 설정이 선택된 경우, 포트는 해당 설정에 따라 플로우 컨트롤을 사용하게 됩니다. Current Rx 열은 포트가 수신한 일시 정지 프레임을 준수하는지 여부를 나타내며, Current Tx 열은 포트가 일시 정지 프레임을 전송하는지 여부를 나타냅니다. Rx 및 Tx 설정은 이전 자동 협상 결과에 따라 결정됩니다. 플로우 컨트롤 설정은 링크 속도 설정과 함께 설정되어야 합니다. 100FX 표준은 자동 협상을 지원하지 않기 때문에, 100FX 모드에서는 플로우 컨트롤 기능이 항상 "비활성화"로 표시됩니다.
PFC	포트에서 PFC(802.1Qbb 우선순위 흐름 제어)가 활성화되면, 우선순위 레벨에서 흐름 제어가 활성화됩니다. 우선순위 필드를 통해 우선순위 범위(하나 또는 그 이상)를 구성할 수 있으며, 예를 들어 '0-3,7'은 '0,1,2,3,7'을 의미합니다. PFC는 자동 협상을 통해 지원되지 않습니다. PFC와 일반 흐름 제어는 동일한 포트에서 동시에 활성화될 수 없습니다.
Maximum Frame Size	FCS(프레임 체크 시퀀스)를 포함한 스위치 포트에서 허용되는 최대 프레임 크기를 입력합니다. (1518~10240bytes)
Excessive Collision Mode	포트 전송 충돌 동작을 구성합니다. Discard: 16번의 충돌 이후 버림 - 충돌이 발생하면 해당 프레임은 버려지고, 새로운 전송을 시도합니다. (기본값) Restart: 16번의 충돌 이후, 백오프 알고리즘을 재시작 합니다. 백오프 알고리즘은 충돌이 발생한 경우 일정 시간 동안 대기한 후 다시 전송을 시도하는 방식입니다.
Frame Length Check	EtherType/Length 필드에 잘못된 프레임 길이가 있는 경우 해당 프레임을 삭제할지 여부를 구성합니다. 이더넷 프레임에는 EtherType 필드가 포함되어 있으며, 이 필드는 값이 1535 이하일 때 프레임 페이로드 크기(바이트 단위)를 나타내는 데 사용될 수 있습니다. EtherType/Length 필드가 1535보다 크면, 이 필드는 EtherType으로 사용되어 프레임의 페이로드에 캡슐화된 프로토콜을 나타냅니다.

	"프레임 길이 확인"이 활성화된 경우, EtherType/Length 필드가 실제 페이로드 길이와 일치하지 않으면 페이로드 크기가 1536 바이트 미만인 프레임은 삭제됩니다. "프레임 길이 확인"이 비활성화된 경우, 프레임 길이 불일치로 인해 프레임이 삭제되지 않습니다. 참고: 프레임 길이 불일치로 삭제된 프레임은 삭제 카운터에 기록되지 않습니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

Refresh: 클릭 시 페이지를 새로 고침. 로컬 변경 사항은 취소합니다.

WEB 설정 예시

✓ Port Configuration

➢ ***Description***

Port Configuration

Refresh

Port	Description	Link	SFP Module	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*	H/W TEAM				<>	☑	☑	☑	☑	☑	☐			☐	0-7	10240	<>	☐
1	H/W TEAM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
2	S/W TEAM	UTP		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
3	LABORATORY	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
4	CONFERENCE ROOM	UTP		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
5	FINANCE TEAM	1G		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
6	SALES TEAM	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
7	PORT_7	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
8	PORT_8	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐

➢ ***Speed Configured***

Auto-negotiation이 기본 값이며, 다른 값은 속도, 듀플렉스가 고정됩니다.

Port Configuration

Port	Description	Link	PHY	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*					<>	☑	☑	☑	☑	☑	☐			☐	0-7	10240	<>	☐
1			UTP	Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
2			UTP	1Gfdx	Disabled	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
3			UTP	Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
4			UTP	Down	10Mbps HDX	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
5			UTP	Down	10Mbps FDX	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
6			UTP	Down	100Mbps HDX	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
7			UTP	Down	100Mbps FDX	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
8			UTP	Down	1Gbps FDX	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
9			-	Down	1Gbps C37	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
10			-	Down		☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐

➢ ***Advertise Duplex***

UTP 포트 – Speed Auto만 설정이 가능하며, Full duplex가 우선적으로 선택되어 링크파트너에 알립니다.

Port Configuration

Refresh

Port	Description	Link	SFP Module	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*	H/W TEAM				<>	☐	☑	☑	☑	☑	☐			☐	0-7	10240	<>	☐
1	H/W TEAM	UTP		1Gfdx	Auto	☐	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
2	S/W TEAM	UTP		1Gfdx	Auto	☑	☐	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
3	LABORATORY	UTP		Down	1Gbps FDX	☐	☐	☐	☐	☐	☐	✗	✗	☐	0-7	10240	Discard	☐
4	CONFERENCE ROOM	UTP		Down	100Mbps FDX	☐	☐	☐	☐	☐	☐	✗	✗	☐	0-7	10240	Discard	☐
5	FINANCE TEAM	1G		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
6	SALES TEAM	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
7	PORT_7	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
8	PORT_8	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐

➢ ***Advertise Speed***

UTP 포트 – Speed Auto만 설정이 가능하며, Speed가 빠른 것이 우선적으로 선택되어 링크파트너에 알립니다.

- Speed – AUTO 모두포함(우선순위에 따라 1Gfdx로 연결)

Port Configuration — Refresh

Port	Description	Link	SFP Module	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*	H/W TEAM				<>	☑	☑	☑	☑	☑	☐			☐	0-7	10240	<>	☐
1	H/W TEAM	UTP		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
2	S/W TEAM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
3	LABORATORY	UTP		Down	10Mbps FDX	☐	☐	☐	☐	☐	☐	✗	✗	☐	0-7	10240	Discard	☐
4	CONFERENCE ROOM	UTP		Down	100Mbps FDX	☐	☐	☐	☐	☐	☐	✗	✗	☐	0-7	10240	Discard	☐
5	FINANCE TEAM	1G		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
6	SALES TEAM	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
7	PORT_7	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
8	PORT_8	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐

- Speed – AUTO 1G 제외(우선순위에 따라 100mfdx로 연결)

Port Configuration — Refresh

Port	Description	Link	SFP Module	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*	H/W TEAM				<>	☑	☑	☑	☑	☐	☐			☐	0-7	10240	<>	☐
1	H/W TEAM	UTP		100fdx	Auto	☑	☑	☑	☑	☐	☐	✗	✗	☐	0-7	10240	Discard	☐
2	S/W TEAM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
3	LABORATORY	UTP		Down	10Mbps FDX	☐	☐	☐	☐	☐	☐	✗	✗	☐	0-7	10240	Discard	☐
4	CONFERENCE ROOM	UTP		Down	100Mbps FDX	☐	☐	☐	☐	☐	☐	✗	✗	☐	0-7	10240	Discard	☐
5	FINANCE TEAM	1G		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
6	SALES TEAM	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
7	PORT_7	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
8	PORT_8	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐

- Speed – AUTO 1G, 100M 제외(우선순위에 따라 10mfdx로 연결)

Port Configuration — Refresh

Port	Description	Link	SFP Module	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*	H/W TEAM				<>	☑	☑	☑	☐	☐	☐			☐	0-7	10240	<>	☐
1	H/W TEAM	UTP		10fdx	Auto	☑	☑	☑	☐	☐	☐	✗	✗	☐	0-7	10240	Discard	☐
2	S/W TEAM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
3	LABORATORY	UTP		Down	10Mbps FDX	☐	☐	☐	☐	☐	☐	✗	✗	☐	0-7	10240	Discard	☐
4	CONFERENCE ROOM	UTP		Down	100Mbps FDX	☐	☐	☐	☐	☐	☐	✗	✗	☐	0-7	10240	Discard	☐
5	FINANCE TEAM	1G		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
6	SALES TEAM	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
7	PORT_7	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
8	PORT_8	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐

➢ ***Flow Control***

- Flow Control Disable(default)

Port Configuration — Refresh

Port	Description	Link	SFP Module	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*	H/W TEAM				<>	☑	☑	☑	☑	☑	☐			☐	0-7	10240	<>	☐
1	H/W TEAM	UTP		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
2	S/W TEAM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
3	LABORATORY	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
4	CONFERENCE ROOM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
5	FINANCE TEAM	1G		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
6	SALES TEAM	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
7	PORT_7	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
8	PORT_8	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐

- Flow Control Enable

Port Configuration

Refresh

Port	Description	Link	SFP Module	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*	H/W TEAM				<>	☑	☑	☑	☑	☑	☑			☐	0-7	10240	<>	☐
1	H/W TEAM	UTP		1Gfdx	Auto	☑	☑	☑	☑	☑	☑	✓	✓	☐	0-7	10240	Discard	☐
2	S/W TEAM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
3	LABORATORY	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
4	CONFERENCE ROOM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
5	FINANCE TEAM	1G		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
6	SALES TEAM	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
7	PORT_7	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
8	PORT_8	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐

➢ ***PFC***

- Enable

Port Configuration

Refresh

Port	Description	Link	SFP Module	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*	H/W TEAM				<>	☑	☑	☑	☑	☑	☐			☑	0-7	10240	<>	☐
1	H/W TEAM	UTP		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☑	0-7	10240	Discard	☐
2	S/W TEAM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
3	LABORATORY	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
4	CONFERENCE ROOM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
5	FINANCE TEAM	1G		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
6	SALES TEAM	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
7	PORT_7	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
8	PORT_8	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐

- Priority

Port Configuration

Refresh

Port	Description	Link	SFP Module	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*	H/W TEAM				<>	☑	☑	☑	☑	☑	☐			☑	0-2	10240	<>	☐
1	H/W TEAM	UTP		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☑	0-2	10240	Discard	☐
2	S/W TEAM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
3	LABORATORY	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
4	CONFERENCE ROOM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
5	FINANCE TEAM	1G		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
6	SALES TEAM	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
7	PORT_7	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
8	PORT_8	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐

Port Configuration

Refresh

Port	Description	Link	SFP Module	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*	H/W TEAM				<>	☑	☑	☑	☑	☑	☐			☑	0-5	10240	<>	☐
1	H/W TEAM	UTP		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☑	0-5	10240	Discard	☐
2	S/W TEAM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
3	LABORATORY	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
4	CONFERENCE ROOM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240	Discard	☐
5	FINANCE TEAM	1G		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
6	SALES TEAM	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
7	PORT_7	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐
8	PORT_8	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐

➢ ***Maximum Frame Size***

(1518~10240bytes)

Port Configuration

Refresh

Port	Description	Link	SFP Module	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*	H/W TEAM				<>	☑	☑	☑	☑	☑	☐			☐	0-7	1518	<>	☐
1	H/W TEAM	UTP		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	1518	Discard	☐
2	S/W TEAM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	2500	Discard	☐
3	LABORATORY	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	3500	Discard	☐
4	CONFERENCE ROOM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	5000	Discard	☐
5	FINANCE TEAM	1G		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	6500		☐
6	SALES TEAM	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	8000		☐
7	PORT_7	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	9500		☐
8	PORT_8	-		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	☐	0-7	10240		☐

➢ ***Excessive Collision Mode(UTP만 설정 가능)***

- Discard(default)

Port Configuration

Refresh

Port	Description	Link	SFP Module	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*	H/W TEAM				<>	☑	☑	☑	☑	☑	☐			☐	0-7	10240	<>	☐
1	H/W TEAM	UTP		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240	Discard	☐
2	S/W TEAM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240	Discard	☐
3	LABORATORY	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240	Discard	☐
4	CONFERENCE ROOM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240	Discard	☐
5	FINANCE TEAM	1G		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240		☐
6	SALES TEAM	-		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240		☐
7	PORT_7	-		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240		☐
8	PORT_8	-		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240		☐

- Restart

Port Configuration

Refresh

Port	Description	Link	SFP Module	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*	H/W TEAM				<>	☑	☑	☑	☑	☑	☐			☐	0-7	10240	<>	☐
1	H/W TEAM	UTP		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240	Restart	☐
2	S/W TEAM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240	Restart	☐
3	LABORATORY	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240	Restart	☐
4	CONFERENCE ROOM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240	Restart	☐
5	FINANCE TEAM	1G		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240		☐
6	SALES TEAM	-		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240		☐
7	PORT_7	-		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240		☐
8	PORT_8	-		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240		☐

➢ ***Frame Length Check***

Port Configuration

Refresh

Port	Description	Link	SFP Module	Speed		Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*	H/W TEAM				<>	☑	☑	☑	☑	☑	☐			☐	0-7	10240	<>	☑
1	H/W TEAM	UTP		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240	Discard	☑
2	S/W TEAM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240	Restart	☑
3	LABORATORY	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240	Restart	☐
4	CONFERENCE ROOM	UTP		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240	Restart	☐
5	FINANCE TEAM	1G		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240		☐
6	SALES TEAM	-		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240		☐
7	PORT_7	-		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240		☐
8	PORT_8	-		Down	Auto	☑	☑	☑	☑	☑	☐	✕	✕	☐	0-7	10240		☐

CLI 설정 예시

✓ Port Configuration

➢ ***Description***

```
(config)# interface 10GigabitEthernet/ GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# description <line>
(config-if) )# description H/W TEAM
```

➢ ***Speed Configured***

Auto-negotiation이 기본 값이며, 다른 값은 설정이 고정됩니다.

```
(config)# interface 10GigabitEthernet/ GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# speed { 10g | 2500 | 1000-c37 | 1000 | 100 | 10 | auto { [ 10 ] [ 100 ]
[ 1000 ] } }
(config-if)# speed auto
(config-if)# speed 100

(config-if)# duplex <auto/full/half>
(config-if)# duplex auto
(config-if)# duplex full
```

➢ ***Advertise Duplex***

UTP 포트 – Speed Auto만 설정이 가능, 설정 상태를 링크파트너에 알립니다.

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# speed auto

(config-if)# duplex auto <full/half/cr>
(config-if)# duplex auto
(config-if)# duplex auto full
```

➢ ***Advertise Speed***

UTP 포트 – Speed Auto만 설정이 가능하며, 설정 상태를 링크파트너에 알립니다.

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# speed auto { [ 10 ] [ 100 ] [ 1000 ] } }
(config-if)# speed auto 10 100
(config-if)# speed auto 1000 100

(config-if)# duplex auto
```

➢ ***Flow Control***

- Flow Control Disable(default)

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# flowcontrol off
```

- Flow Control Enable

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# flowcontrol on
```

➢ ***PFC***

- Enable, Priority

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1
```

```
(config-if)# priority-flowcontrol prio <0~7>
(config-if)# priority-flowcontrol prio 0-7
(config-if)# priority-flowcontrol prio 1,3,7
```

- Disable, Priority

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)#no priority-flowcontrol prio <0~7>
(config-if)#no priority-flowcontrol prio 0-7
(config-if)#no priority-flowcontrol prio 1,3,7
```

➢ ***Maximum Frame Size***

(1518~10240bytes)

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)#mtu 1518-10240
(config-if)#mtu 1518
(config-if)#mtu 10240
```

➢ ***Excessive Collision Mode(UTP만 설정 가능)***

- Discard(default)

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# no excessive-restart
```

- Restart

```
(config)# interface GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# excessive-restart
```

➢ ***Frame Length Check***

- ***Enable***

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# frame-length-check
```

- ***Disable***

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/1

(config-if)# no frame-length-check
```

6.3.2. Ports Monitor

6.3.2.1. State

웹메뉴 Monitor>Ports>State

이 페이지는 현재 스위치 포트 상태에 대한 개요를 제공합니다.

State	Disabled	Down	Link (non-Max Speed)	Link (Max Speed)
RJ-45 Ports				
SFP Ports				

Info. X (Disabled), Out (Module-Out), Down (Link Down), 10M (Link 10m), 100M (Link 100m), 1G (Link 1G), 2.5G (Link 2.5G), 10G (Link 10G), PoE (PoE)

Port State Overview

용어	설명
reset	3초이상 누르면 설정값이 기본값으로 모두 변경됩니다. 10초이상 누르면 모든 설정값이 기본값으로 변경되며, IP도 초기값 (192.168.10.100)으로 변경됩니다.
Power	Power을 연결하면 LED에 불이 들어옵니다.

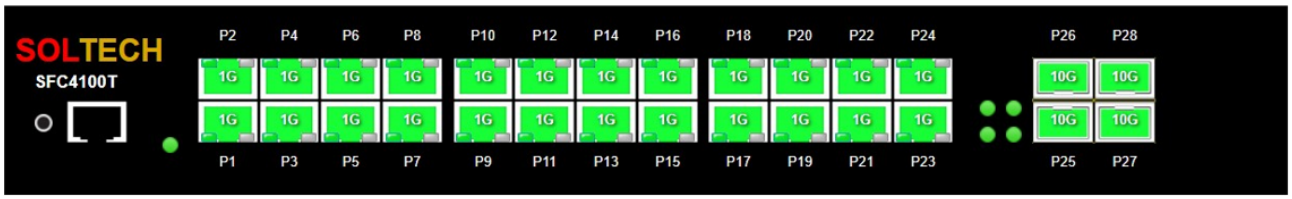
Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

WEB 확인 예시

웹메뉴 Monitor>Ports>State



CLI 확인 예시

✓ **Port State Overview**

```
# show interface * status

Interface          Mode     Speed & Duplex   Flow Control   Max Frame   Excessive   Link      MAC-Addr
---------------------  -------  --------------  ------------  ---------  ---------  ---------  --------
GigabitEthernet 1/1   enabled   Auto      disabled      9600       Discard   1Gfdx     02:21:6D:00:00:00
GigabitEthernet 1/2   enabled   Auto      disabled      9600       Discard   Down      06:21:6D:00:00:00
GigabitEthernet 1/3   enabled   Auto      disabled      9600       Discard   Down      0A:21:6D:00:00:00
GigabitEthernet 1/4   enabled   Auto      disabled      9600       Discard   Down      0E:21:6D:00:00:00
```

6.3.2.2. Traffic Overview

웹메뉴 Monitor>Ports>Traffic Overview

이 페이지는 현재 스위치 포트 상태에 대한 개요를 제공합니다.

Port Statistics Overview

Port	Description	Packets		Bytes		Errors		Drops		Filtered
		Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1		0	0	0	0	0	0	0	0	0
2		0	0	0	0	0	0	0	0	0
3		0	0	0	0	0	0	0	0	0
4		0	0	0	0	0	0	0	0	0
5		0	0	0	0	0	0	0	0	0
6		0	0	0	0	0	0	0	0	0
7		0	0	0	0	0	0	0	0	0
8		0	0	0	0	0	0	0	0	0

Port Statistics Overview

용어	설명
Port	논리 포트입니다. 클릭하면 Detailed Statistics 화면으로 이동합니다.
Description	포트에 대한 설명입니다.
Packets	포트에 수신 및 전송된 패킷 수입니다.
Bytes	포트당 수신 및 전송된 바이트 수입니다.
Errors	오류로 수신된 프레임 수와 불완전한 전송 수입니다.
Drops	수신 또는 송신 혼잡으로 인해 삭제된 프레임 수입니다.
Filtered	전달 프로세스에서 필터링 된 수신 프레임 수입니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

Clear : 클릭 시 모든 포트의 카운터를 지움.

WEB 확인 예시

웹메뉴 Monitor>Ports>Traffic Overview

Port Statistics Overview

Port	Description	Packets		Bytes		Errors		Drops		Filtered
		Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1		1215	486	232396	220964	0	0	0	0	148
2		0	0	0	0	0	0	0	0	0
3		1	4	64	256	0	0	0	0	0
4		0	0	0	0	0	0	0	0	0
5		2561	1	163904	64	0	0	0	0	0
6		1783	4	114112	256	0	0	0	0	0
7		0	0	0	0	0	0	0	0	0
8		545	5	34880	320	0	0	0	0	0

CLI 확인 예시

✓ Port Statistics Overview

```
# show interface GigabitEthernet 1/1-4 statistics packets

Interface              Rx Packets          Tx Packets
---------------------  ------------------  ------------------
GigabitEthernet 1/1    4434                2280
GigabitEthernet 1/2    0                   0
GigabitEthernet 1/3    1                   5
GigabitEthernet 1/4    0                   0

# show interface 10GigabitEthernet 1/1-4 statistics packets

Interface              Rx Packets          Tx Packets
---------------------  ------------------  ------------------
10GigabitEthernet 1/1  6929                43
10GigabitEthernet 1/2  1783                4
10GigabitEthernet 1/3  0                   0
10GigabitEthernet 1/4  545                 5
```

```
# show interface GigabitEthernet 1/1-4 statistics bytes

Interface              Rx Octets           Tx Octets
---------------------  ------------------  ------------------
GigabitEthernet 1/1    1015232             1238992
GigabitEthernet 1/2    0                   0
GigabitEthernet 1/3    64                  320
GigabitEthernet 1/4    0                   0

# show interface 10GigabitEthernet 1/1-4 statistics bytes

Interface              Rx Octets           Tx Octets
---------------------  ------------------  ------------------
10GigabitEthernet 1/1  443456              4008
10GigabitEthernet 1/2  114112              256
10GigabitEthernet 1/3  0                   0
10GigabitEthernet 1/4  34880               320
```

```
# show interface GigabitEthernet 1/1-4 statistics errors

Interface              Rx Errors           Tx Errors
---------------------  ------------------  ------------------
GigabitEthernet 1/1    3                   0
GigabitEthernet 1/2    0                   0
GigabitEthernet 1/3    0                   0
GigabitEthernet 1/4    0                   0

# show interface 10GigabitEthernet 1/1-4 statistics errors

Interface              Rx Errors           Tx Errors
---------------------  ------------------  ------------------
10GigabitEthernet 1/1  0                   0
10GigabitEthernet 1/2  0                   0
10GigabitEthernet 1/3  0                   0
10GigabitEthernet 1/4  0                   0
```

```
# show interface GigabitEthernet 1/1-4 statistics discards

Interface               Rx Discards         Tx Discards
----------------------  ------------------  ------------------
GigabitEthernet 1/1     0                   0
GigabitEthernet 1/2     0                   0
GigabitEthernet 1/3     0                   0
GigabitEthernet 1/4     0                   0

# show interface 10GigabitEthernet 1/1-4 statistics discards

Interface               Rx Discards         Tx Discards
----------------------  ------------------  ------------------
10GigabitEthernet 1/1   0                   0
10GigabitEthernet 1/2   0                   0
10GigabitEthernet 1/3   0                   0
10GigabitEthernet 1/4   0                   0
```

```
# show interface GigabitEthernet 1/1-4 statistics filtered

Interface               Rx Filtered
----------------------  ------------------
GigabitEthernet 1/1     1012
GigabitEthernet 1/2     0
GigabitEthernet 1/3     0
GigabitEthernet 1/4     0

# show interface 10GigabitEthernet 1/1-4 statistics filtered

Interface               Rx Filtered
----------------------  ------------------
10GigabitEthernet 1/1   0
10GigabitEthernet 1/2   0
10GigabitEthernet 1/3   0
10GigabitEthernet 1/4   0
```

6.3.2.3. QoS Statistics

웹메뉴 Monitor>Ports>QoS Statistics

이 페이지는 모든 스위치 포트의 다양한 대기열에 대한 통계를 보여줍니다.

Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Queuing Counters

용어	설명
Port	논리 포트입니다. 클릭하면 Detailed Statistics 화면으로 이동합니다.
Qn	포트당 8개의 QoS 대기열이 있습니다 . Q0은 우선 순위가 가장 낮은 대기열입니다.
Rx/Tx	수신 및 전송된 패킷 수입니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

Clear : 클릭 시 모든 포트의 카운터를 지움.

WEB 확인 예시

웹메뉴 Monitor>Ports>QoS Statistics

Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	494	1	0	0	0	0	0	0	0	0	0	0	0	0	0	309
2	511	1	0	0	0	0	0	0	0	0	0	0	0	0	0	356
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	1	95	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	1323	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	2356	21	0	0	0	0	0	0	0	0	0	0	0	0	0	0

CLI 확인 예시

✓ Queuing Counters

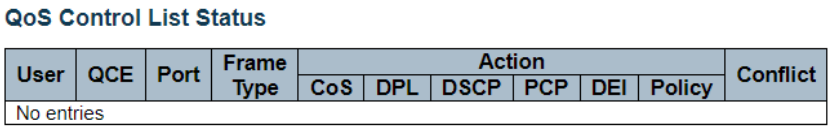
```
#show interface GigabitEthernet 1/1-4 statistics priority

GigabitEthernet 1/1                Rx Priority queue   Tx Priority queue
-----------------------------------  ------------------  ------------------
Priority 0                          930                  1
Priority 1                          0                    0
Priority 2                          0                    0
Priority 3                          0                    0
Priority 4                          0                    0
Priority 5                          0                    0
Priority 6                          0                    0
Priority 7                          0                    378

GigabitEthernet 1/2                Rx Priority queue   Tx Priority queue
-----------------------------------  ------------------  ------------------
Priority 0                          511                  1
Priority 1                          0                    0
Priority 2                          0                    0
Priority 3                          0                    0
Priority 4                          0                    0
Priority 5                          0                    0
Priority 6                          0                    0
Priority 7                          0                    356

GigabitEthernet 1/3                Rx Priority queue   Tx Priority queue
-----------------------------------  ------------------  ------------------
Priority 0                          0                    0
Priority 1                          0                    0
Priority 2                          0                    0
Priority 3                          0                    0
Priority 4                          0                    0
Priority 5                          0                    0
Priority 6                          0                    0
Priority 7                          0                    0

GigabitEthernet 1/4                Rx Priority queue   Tx Priority queue
-----------------------------------  ------------------  ------------------
Priority 0                          1                    95
Priority 1                          0                    0
Priority 2                          0                    0
Priority 3                          0                    0
Priority 4                          0                    0
Priority 5                          0                    0
Priority 6                          0                    0
Priority 7                          0                    0

# show interface 10GigabitEthernet 1/1-4 statistics priority

10GigabitEthernet 1/1              Rx Priority queue    Tx Priority queue
-----------------------------------  ------------------  ------------------
Priority 0                          1323                 12
Priority 1                          0                    0
Priority 2                          0                    0
Priority 3                          0                    0
```

```
Priority 4                              0                0
Priority 5                              0                0
Priority 6                              0                0
Priority 7                              0                0

10GigabitEthernet 1/2                Rx Priority queue     Tx Priority queue
----------------------------------------  ------------------  ------------------
Priority 0                              0                0
Priority 1                              0                0
Priority 2                              0                0
Priority 3                              0                0
Priority 4                              0                0
Priority 5                              0                0
Priority 6                              0                0
Priority 7                              0                0


10GigabitEthernet 1/3                Rx Priority queue     Tx Priority queue
----------------------------------------  ------------------  ------------------
Priority 0                              0                0
Priority 1                              0                0
Priority 2                              0                0
Priority 3                              0                0
Priority 4                              0                0
Priority 5                              0                0
Priority 6                              0                0
Priority 7                              0                0

10GigabitEthernet 1/4                Rx Priority queue     Tx Priority queue
----------------------------------------  ------------------  ------------------
Priority 0                           2356               21
Priority 1                              0                0
Priority 2                              0                0
Priority 3                              0                0
Priority 4                              0                0
Priority 5                              0                0
Priority 6                              0                0
Priority 7                              0                0
```

6.3.2.4. QCL Status

웹메뉴 Monitor>Ports>QCL Status

이 페이지에서는 다른 QCL 사용자별로 QCL 상태를 보여줍니다. 각 행은 정의된 QCE 를 설명합니다. 하드웨어 제한으로 인해 특정 QCE 가 하드웨어에 적용되지 않는 경우 충돌이 발생합니다. 각 스위치에서 지원하는 QCE 의 최대 개수는 256 입니다.



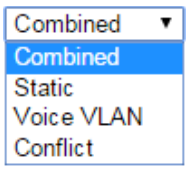
QoS Control List Status

User	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
No entries										

QoS Control List Status

용어	설명
User	QCL 사용자를 나타냅니다.
QCE	QCE ID를 나타냅니다.
Port	QCE와 구성된 포트 목록을 나타냅니다.
Frame Type	프레임의 유형을 나타냅니다 **Any** 모든 프레임 유형에 일치합니다. **Ethernet** EtherType 프레임에 일치합니다. **LLC** LLC(논리 링크 제어) 프레임에 일치합니다. **SNAP** SNAP(서브넷 브릿지 액세스 프로토콜)프레임에 일치합니다. **IPv4** IPv4 프레임에 일치합니다. **IPv6** IPv6 프레임에 일치합니다.
Action	매개변수가 프레임의 내용과 일치하는 경우에 적용되는 인입 프레임의 분류 작업을 나타냅니다. **CoS** 클래스 서비스를 분류합니다. **DPL** 드롭 우선 순위 레벨을 분류합니다. **DSCP** DSCP 값을 분류합니다. **PCP** PCP 값을 분류합니다. **DEI** DEI 값을 분류합니다. **Policy** ACL 정책 번호를 분류합니다.
Conflict	QCL 항목의 충돌 상태를 표시합니다. 하드웨어 리소스는 여러 응용 프로그램에서 공유되기 때문에 QCE를 추가하는 데 필요한 리소스가 사용 불가능할 수 있으므로 충돌 상태를 'Yes'로 표시합니다. 충돌은 '충돌 해결' 버튼을 눌러 하드웨어 리소스를 해제함으로써 해결할 수 있습니다.

Buttons



: 이 드롭 다운 목록에서 QCL 상태를 선택합니다.

Auto-refresh : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

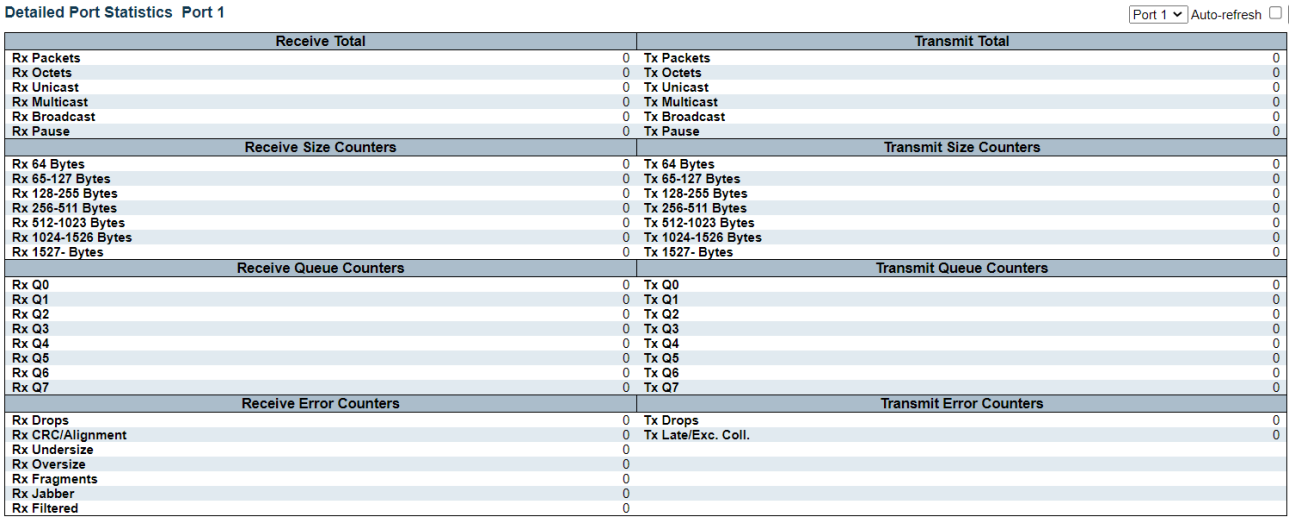
Resolve Conflict: 어떤 QCL 항목에 대한 충돌 상태가 '예'입니다, QCL 항목을 추가하는 데 필요한 리소스를 해제합니다.

Refresh: 클릭 시 페이지를 새로 고침.

6.3.2.5. Detailed Statistics

웹메뉴 Monitor>Ports>Detailed Statistics

이 페이지는 특정 스위치 포트에 대한 자세한 트래픽 통계를 제공합니다.
(포트 선택 상자를 사용하여 표시할 스위치 포트 세부 정보를 선택합니다.)


Detailed Port Statistics Port 1

Port 1 Auto-refresh

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Detailed Port Statistics Port n

용어	설명
Receive and Transmit Total	전체 수신 및 송신된 패킷의 정보를 표시합니다.
Rx and Tx Packets	수신 및 전송 패킷의 수입니다.
Rx and Tx Octets	수신 및 전송 바이트 수입니다.
Rx and Tx Unicast	수신 및 전송 유니 캐스트 패킷의 수입니다.
Rx and Tx Multicast	수신 및 전송 멀티 캐스트 패킷의 수입니다.
Rx and Tx Broadcast	수신 및 전송 브로드 캐스트 패킷의 수입니다.
Rx and Tx Pause	PAUSE 동작을 나타내는 연산 코드가이 포트에서 수신 또는 송신 MAC 제어 프레임 수입니다.
Receive and Transmit Size Counters	수신 및 송신된 패킷을 프레임 크기별로 분류한 수입니다
Receive and Transmit Queue Counters	수신 및 송신된 패킷을 큐별로 분류한 수입니다.
Receive and Transmit Error Counters	수신 및 송신된 패킷 중 에러로 분류된 수입니다.
Rx Drops	수신되어 Drop된 패킷의 수입니다.
Rx CRC/Alignment	CRC 또는 정렬 오류로 수신된 프레임의 개수입니다.
Rx Undersize	수신된 사이즈가 작은 프레임의 수입니다.
Rx Oversize	수신된 사이즈가 초과한 프레임의 수입니다.
Rx Fragments	유효하지 않은 CRC로 수신된 짧은 프레임의 개수입니다.

Rx Jabber	유효하지 않은 CRC로 수신된 긴 프레임의 개수입니다.
Rx Filtered	전달 프로세스에 의해 필터링된 수신된 프레임의 개수입니다.
Tx Drops	출력 버퍼 혼잡으로 인해 드롭된 프레임의 개수입니다.
Tx Late/Exc.	과다한 또는 지연된 충돌로 인해 드롭된 프레임의 개수입니다.

Buttons

Port 1 : 포트를 선택하여 원하는 포트의 정보를 가져옴.

Auto-refresh : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

Clear : 선택한 포트의 카운터를 지웁니다.

WEB 확인 예시

웹메뉴 Monitor>Ports>Detailed Statistics

Detailed Port Statistics Port 1

Port 1 Auto-refresh

Receive Total		Transmit Total	
Rx Packets	2624	Tx Packets	553
Rx Octets	351169	Tx Octets	102221
Rx Unicast	668	Tx Unicast	553
Rx Multicast	693	Tx Multicast	0
Rx Broadcast	1263	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	1673	Tx 64 Bytes	308
Rx 65-127 Bytes	175	Tx 65-127 Bytes	70
Rx 128-255 Bytes	648	Tx 128-255 Bytes	71
Rx 256-511 Bytes	0	Tx 256-511 Bytes	56
Rx 512-1023 Bytes	128	Tx 512-1023 Bytes	26
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	22
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	2624	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	553
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	651		

CLI 확인 예시

✓ Detailed Port Statistics Port

```
#show interface GigabitEthernet <port_type_list> statistics
# show interface GigabitEthernet 1/1 statistics

GigabitEthernet 1/1 Statistics:
Rx Packets:          2693   Tx Packets:          565
Rx Octets:         360643   Tx Octets:         104266
Rx Unicast:          683   Tx Unicast:          565
Rx Multicast:        717   Tx Multicast:          0
Rx Broadcast:       1293   Tx Broadcast:          0
Rx Pause:              0   Tx Pause:              0
Rx 64:              1714   Tx 64:               316
```

```
Rx 65-127:                177    Tx 65-127:                71
Rx 128-255:               672    Tx 128-255:               72
Rx 256-511:                 0    Tx 256-511:               57
Rx 512-1023:              130    Tx 512-1023:              27
Rx 1024-1526:               0    Tx 1024-1526:             22
Rx 1527-    :               0    Tx 1527-    :             0

Rx Priority 0:           2693    Tx Priority 0:             0
Rx Priority 1:              0    Tx Priority 1:             0
Rx Priority 2:              0    Tx Priority 2:             0
Rx Priority 3:              0    Tx Priority 3:             0
Rx Priority 4:              0    Tx Priority 4:             0
Rx Priority 5:              0    Tx Priority 5:             0
Rx Priority 6:              0    Tx Priority 6:             0
Rx Priority 7:              0    Tx Priority 7:           565

Rx Drops:                   0    Tx Drops:                  0
Rx CRC/Alignment:           0    Tx Late/Exc. Coll.:        0
Rx Undersize:               0
Rx Oversize:                0
Rx Fragments:               0
Rx Jabbers:                 0
Rx Filtered:              675
```

#show interface 10GigabitEthernet <port_type_list> statistics

 # show interface 10GigabitEthernet 1/1 statistics

```
10GigabitEthernet 1/1 Statistics:
Rx Packets:              1323    Tx Packets:               12
Rx Octets:              84672    Tx Octets:               768
Rx Unicast:                 0    Tx Unicast:                0
Rx Multicast:            1322    Tx Multicast:              0
Rx Broadcast:               1    Tx Broadcast:             12
Rx Pause:                   0    Tx Pause:                  0

Rx 64:                   1323    Tx 64:                    12
Rx 65-127:                  0    Tx 65-127:                 0
Rx 128-255:                 0    Tx 128-255:                0
Rx 256-511:                 0    Tx 256-511:                0
Rx 512-1023:                0    Tx 512-1023:               0
Rx 1024-1526:               0    Tx 1024-1526:              0
Rx 1527-    :               0    Tx 1527-    :              0

Rx Priority 0:           1323    Tx Priority 0:            12
Rx Priority 1:              0    Tx Priority 1:             0
Rx Priority 2:              0    Tx Priority 2:             0
Rx Priority 3:              0    Tx Priority 3:             0
Rx Priority 4:              0    Tx Priority 4:             0
Rx Priority 5:              0    Tx Priority 5:             0
Rx Priority 6:              0    Tx Priority 6:             0
Rx Priority 7:              0    Tx Priority 7:             0
Rx Drops:                   0    Tx Drops:                  0
Rx CRC/Alignment:           0    Tx Late/Exc. Coll.:        0
Rx Undersize:               0
Rx Oversize:                0
Rx Fragments:               0
Rx Jabbers:                 0
Rx Filtered:                0
```

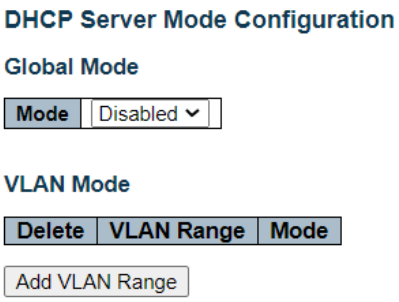
6.4. DHCP

6.4.1. DHCP Configuration

6.4.1.1. Server Mode

웹메뉴 Configuration>DHCP>Server>Mode

이 페이지에서는 시스템 및 VLAN 별로 DHCP 서버를 활성/비활성하기 위해 Global 모드와 VLAN 모드를 구성합니다.



DHCP Server Mode Configuration

Global Mode

용어	설명
Mode	시스템 당 작동 모드를 구성합니다. Enabled: 시스템 당 DHCP 서버를 사용합니다. Disabled: 시스템 당 DHCP 서버를 사용하지 않습니다.

VLAN Mode

용어	설명
VLAN Range	DHCP 서버가 활성화 또는 비활성화 되는 VLAN 범위를 나타냅니다. 첫 번째 VLAN ID는 두 번째 VLAN ID 보다 작거나 같아야 합니다. 단, VLAN 범위에 하나의 VLAN ID만 포함하는 경우, 첫 번째 혹은 두 번째에 한번만 입력하거나 두 번 다 입력할 수 있습니다. 기존 VLAN 범위를 비활성화 하는 방법. 1. 새로운 VLAN 범위를 Add VLAN Range로 추가합니다. 2. 비활성화 VLAN 범위를 입력합니다. 3. Disabled 모드를 선택합니다. 4. Save을 눌러 변경 사항을 적용합니다.
Mode	각 VLAN별 작동 모드를 나타냅니다. Enabled : VLAN별 DHCP 서버를 사용합니다. DIsabled : : VLAN별 DHCP 서버를 사용하지 않습니다.

Buttons

Add VLAN Range: 클릭 시 새로운 VLAN 범위를 지정합니다.

Apply: 클릭 시 변경사항을 적용합니다.

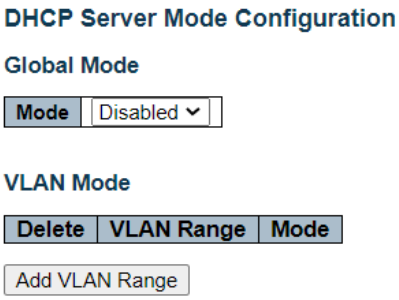
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

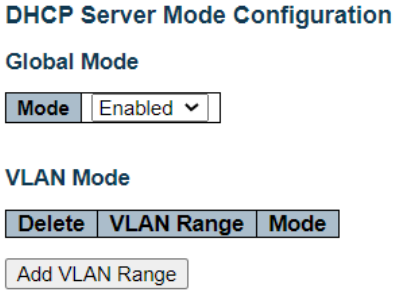
✓ Global Mode

➢ ***Mode***

- ***Disable***



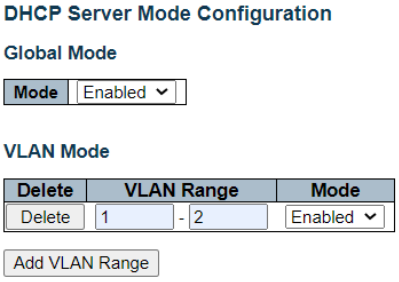
- ***Enable***

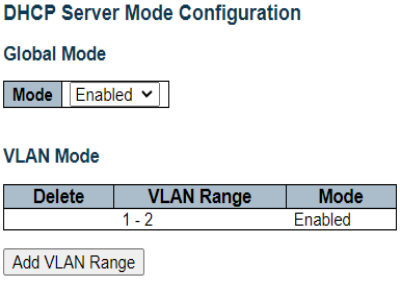


✓ VLAN Mode

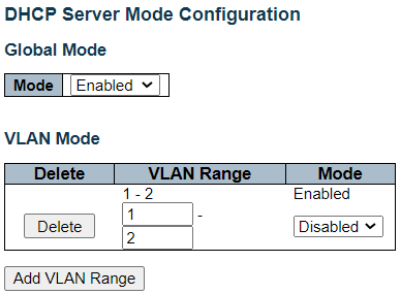
➢ ***Add VLAN Range***

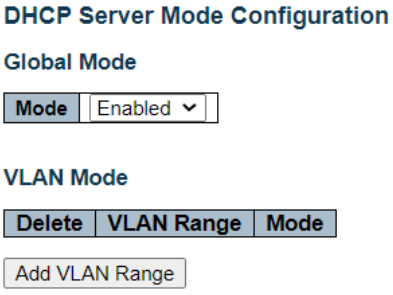
- ***Enable***





- ***Disable***





CLI 설정 예시

✓ Global Mode

➢ *Mode*

- ***Disable***

```
(config)# no ip dhcp server
```

- ***Enable***

```
(config)# ip dhcp server
```

✓ VLAN Mode

➢ *Add VLAN Range*

- ***Enable***

```
(config)# interface vlan <vlan_list>
(config)# interface vlan 1-2

(config-if-vlan)# ip dhcp server
```

- ***Disable***

```
(config)# interface vlan <vlan_list>
(config)# interface vlan 1-2

(config-if-vlan)# no ip dhcp server
```

6.4.1.2. Server Excluded IP

웹메뉴 Configuration>DHCP>Server>Excluded IP

이 페이지는 제외된 IP 주소를 구성합니다.
DHCP 서버는 제외된 IP 주소를 DHCP 클라이언트에 할당하지 않습니다.

DHCP Server Excluded IP Configuration

Excluded IP Address

용어	설명
IP Range	제외할 IP 주소의 범위를 적습니다. 첫 번째 제외된 IP는 두 번째 제외된 IP보다 작거나 같아야 합니다. 단, IP 범위에 제외할 IP가 하나일 경우, 첫 번째와 두 번째 중 하나에만 입력하거나 둘 다 입력하면 됩니다.

Buttons

Add IP Range: 클릭 시 새로운 IP 범위를 지정합니다.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

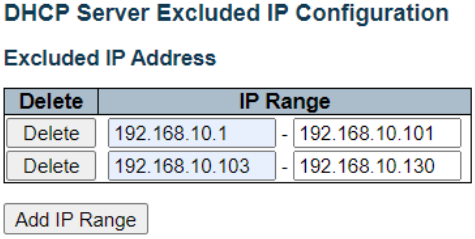
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

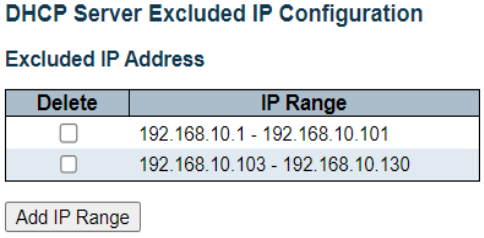
WEB 설정 예시

✓ **Excluded IP Address**

➢ ***Add IP Range***

- ***IP Range***





CLI 설정 예시

✓ Excluded IP Address

➢ *Add IP Range*

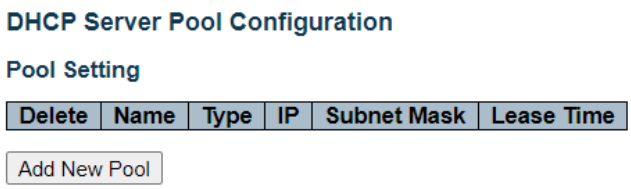
- ***IP Range***

```
(config)# ip dhcp excluded-address <ipv4_addr> <ipv4_addr>
(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.101
(config)# ip dhcp excluded-address 192.168.10.103 192.168.10.130
```

6.4.1.3. Server Pool

웹메뉴 Configuration>DHCP>Server>Pool

이 페이지는 DHCP 풀을 관리합니다.
DHCP 풀에 따라 DHCP 서버는 IP 주소를 할당 클라이언트에게 전달합니다.



DHCP Server Pool Configuration

Pool Setting

용어	설명
Name	풀 이름을 구성하세요. 공백을 제외한 모든 문자를 허용합니다. 자세한 설정을 구성하려면 풀 이름을 클릭하여 구성 페이지로 이동할 수 있습니다.
Type	풀의 유형을 표시합니다. Network: 여러 개의 DHCP 클라이언트에 서비스할 IP 주소 풀을 정의합니다. Host: 클라이언트 식별자 또는 하드웨어 주소로 식별된 특정 DHCP 클라이언트를 위해 서비스합니다.
IP	DHCP 주소 풀의 네트워크 주소를 표시합니다.
Subnet Mask	DHCP 주소 풀의 서브넷 마스크를 표시합니다.
Lease Time	풀의 임대 시간을 표시합니다.

Buttons

Add New Pool: 새로운 DHCP 풀을 추가합니다.

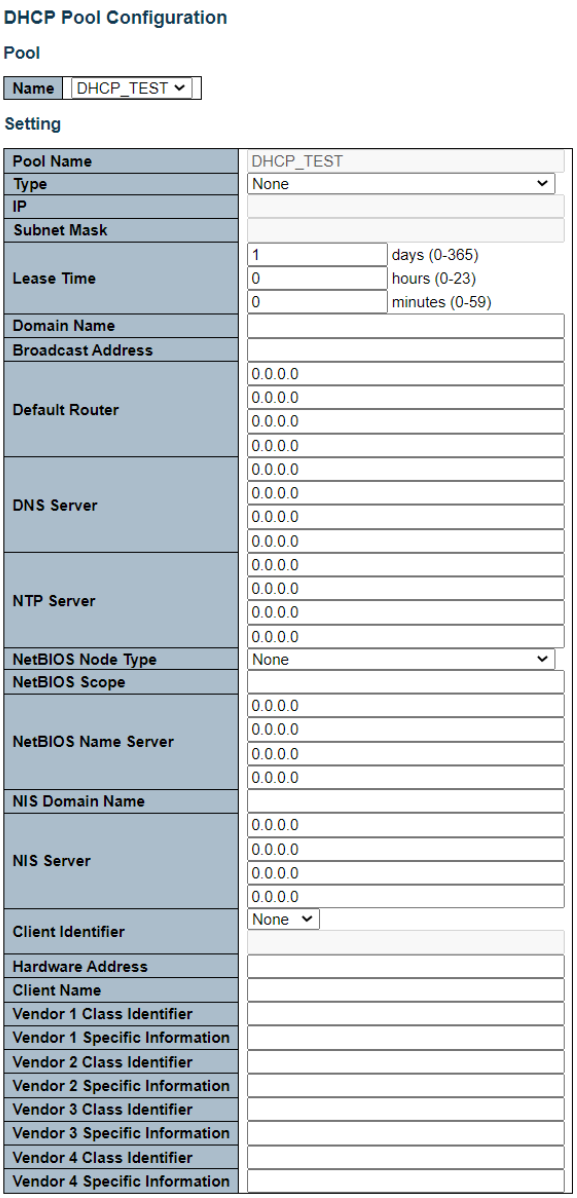
Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

DHCP Pool Configuration

이 페이지는 DHCP 풀의 모든 설정을 구성합니다.



DHCP Pool Configuration

Pool

용어	설명
Name	풀 이름을 사용하여 풀을 선택합니다.

Setting

용어	설명
Pool Name	선택한 풀의 이름을 표시합니다.
Type	풀의 유형을 지정합니다. Network: 여러 개의 DHCP 클라이언트에 서비스할 IP 주소 풀을 정의합니다. Host: 클라이언트 식별자 또는 하드웨어 주소로 식별된 특정 DHCP 클라이언트를 위해 서비스합니다.
IP	DHCP 주소 풀의 네트워크 주소를 지정하세요.

Subnet Mask	DHCP 주소 풀의 서브넷 마스크를 지정하세요.
Lease Time	클라이언트가 IP 주소의 임대 시간을 요청할 수 있는 임대 시간을 지정하세요. (모두 0이면 임대시간 무한대)
Domain Name	클라이언트가 DNS를 통해 호스트 이름을 해석할 때 사용해야 할 도메인 이름을 지정하세요.
Broadcast Address	클라이언트의 서브넷에서 사용 중인 브로드캐스트 주소를 지정하세요.
Default Router	클라이언트의 서브넷에 있는 라우터의 IP 주소 목록을 지정하세요.
DNS Server	클라이언트에 사용 가능한 도메인 이름 시스템(DNS) 네임 서버의 목록을 지정하세요.
NTP Server	클라이언트에 사용 가능한 NTP 서버의 IP 주소 목록을 지정하세요.
NetBIOS Node Type	RFC 1001/1002에 설명된대로 구성 가능한 NetBIOS over TCP/IP 클라이언트를 구성할 수 있도록 NetBIOS 노드 유형 옵션을 지정하세요.
NetBIOS Scope	RFC 1001/1002에 정의된대로 클라이언트의 NetBIOS over TCP/IP 스코프 매개변수를 지정하세요.
NetBIOS Name Server	선호도 순서로 나열된 NBNS 네임 서버 목록을 지정하세요.
NIS Domain Name	클라이언트의 NIS 도메인 이름을 지정하세요.
NIS Server	클라이언트에 사용 가능한 NIS 서버의 IP 주소 목록을 지정하세요.
Client Identifier	풀의 유형이 호스트인 경우 사용할 클라이언트의 고유 식별자를 지정하세요.
Hardware Address	풀의 유형이 호스트인 경우 사용할 클라이언트의 하드웨어(MAC) 주소를 지정하세요.
Client Name	풀의 유형이 호스트인 경우 사용할 클라이언트의 이름을 지정하세요.
Vendor/Class Identifier	DHCP 클라이언트가 벤더 클래스 식별자를 전송하는 경우, DHCP 서버는 DHCP 클라이언트의 벤더 유형 및 구성을 선택적으로 식별하기 위해 지정하세요. DHCP 서버는 해당하는 특정 정보를 클라이언트에게 전달할 것입니다.
Vendor/Specific Information	벤더 클래스 식별자에 따라 벤더별 특정 정보를 지정하세요.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>DHCP>Server>Pool

✓ **DHCP Server Pool Configuration**

➢ ***Add New Pool***

- ***Name***

DHCP Server Pool Configuration

Pool Setting

Delete	Name	Type	IP	Subnet Mask	Lease Time
☐	DHCP_TEST	-	-	-	1 days 0 hours 0 minutes

Add New Pool

✓ DHCP Pool Configuration

➢ *Type*

- ***Network***

DHCP Pool Configuration

Pool

Name DHCP_TEST

Setting

Pool Name	DHCP_TEST
Type	Network
IP	192.168.10.101
Subnet Mask	255.255.255.0
Lease Time	1 days (0-365) 0 hours (0-23) 0 minutes (0-59)
Domain Name	
Broadcast Address	
Default Router	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
DNS Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
NTP Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
NetBIOS Node Type	None
NetBIOS Scope	
NetBIOS Name Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
NIS Domain Name	192.168.10.101
NIS Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Client Identifier	None
Hardware Address	
Client Name	
Vendor 1 Class Identifier	
Vendor 1 Specific Information	
Vendor 2 Class Identifier	
Vendor 2 Specific Information	
Vendor 3 Class Identifier	
Vendor 3 Specific Information	
Vendor 4 Class Identifier	
Vendor 4 Specific Information	

✓ DHCP Server Pool Configuration

➢ *Type*

- ***Network***

DHCP Server Pool Configuration

Pool Setting

Delete	Name	Type	IP	Subnet Mask	Lease Time
☐	DHCP_TEST	Network	192.168.10.101	255.255.255.0	1 days 0 hours 0 minutes

Add New Pool

CLI 설정 예시

✓ DHCP Server Pool Configuration

➢ *Add New Pool*

- ***Name***

```
(config)# ip dhcp pool <word32>
(config)# ip dhcp pool DHCP_TEST
```

✓ DHCP Pool Configuration

➢ *Type*

- ***Network***

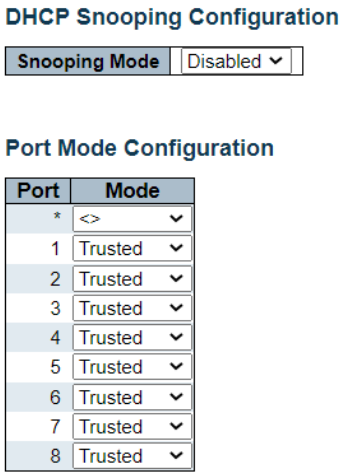
```
(config)# ip dhcp pool <word32>
(config)# ip dhcp pool DHCP_TEST

(config-dhcp-pool)# network <ipv4_ucast> <ipv4_netmask>
(config-dhcp-pool)# network 192.168.10.101 255.255.255.0
```

```
(config)# ip dhcp pool <word32>
(config)# ip dhcp pool DHCP_TEST

(config-dhcp-pool)# nis-domain-name <word128>
(config-dhcp-pool)# nis-domain-name 192.168.10.101
```

6.4.1.4. Snooping

웹메뉴 Configuration>DHCP>Snooping

이 페이지에서 DHCP Snooping 을 설정할 수 있습니다.



DHCP Snooping Configuration

용어	설명
Snooping Mode	DHCP Snooping 모드 작동을 나타냅니다. Enabled: DHCP Snooping 모드 작동을 활성화합니다. DHCP Snooping 모드 작동이 활성화되면 DHCP 요청 메시지는 Trusted 로 설정된 포트로만 송수신이 가능합니다. Disabled: DHCP Snooping 모드 작동을 비활성화합니다.

Port Mode Configuration

용어	설명
Port	논리 포트 번호입니다.
Mode	DHCP Snooping 포트 모드를 나타냅니다. Trusted: 설정된 포트는 DHCP 메시지를 전달할 수 있습니다. Untrusted: 설정된 포트는 DHCP 메시지를 전달할 수 없습니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

✓ **DHCP Snooping Configuration**

➢ ***Snooping Mode***

- ***Disable (Default)***

DHCP Snooping Configuration

Snooping Mode	Disabled

Port Mode Configuration

Port	Mode
*	<>
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted
8	Trusted

- ***Enable***

DHCP Snooping Configuration

Snooping Mode	Enabled

Port Mode Configuration

Port	Mode
*	<>
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted
8	Trusted

✓ Port Mode Configuration

➢ *Mode*

- ***Trusted (Default)***

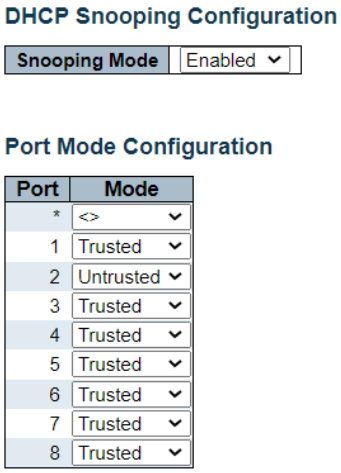
DHCP Snooping Configuration

Snooping Mode	Enabled

Port Mode Configuration

Port	Mode
*	<>
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted
8	Trusted

- ***Untrusted***



CLI 설정 예시

✓ DHCP Snooping Configuration

➢ *Snooping Mode*

- ***Disable (Default)***

```
(config)# no ip dhcp snooping
```

- ***Enable***

```
(config)# ip dhcp snooping
```

✓ Port Mode Configuration

➢ *Mode*

- ***Trusted (Default)***

```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/2

(config-if)# ip dhcp snooping trust
```

- ***Untrusted***

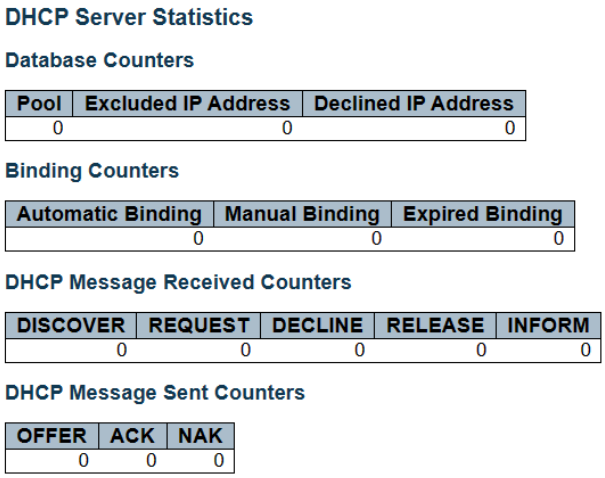
```
(config)# interface 10GigabitEthernet/GigabitEthernet <port_type_list>
(config)# interface GigabitEthernet 1/2

(config-if)# no ip dhcp snooping trust
```

6.4.2. DHCP Monitor

6.4.2.1. Server Statistics

웹메뉴 Monitor>DHCP>Server>Statistics

이 페이지는 데이터베이스 카운터와 DHCP 서버에 의해 전송 및 수신된 DHCP 메시지의 수를 표시합니다.



DHCP Server Statistics

Database Counters

Pool	Excluded IP Address	Declined IP Address
0	0	0

Binding Counters

Automatic Binding	Manual Binding	Expired Binding
0	0	0

DHCP Message Received Counters

DISCOVER	REQUEST	DECLINE	RELEASE	INFORM
0	0	0	0	0

DHCP Message Sent Counters

OFFER	ACK	NAK
0	0	0

DHCP Server Statistics

Database Counters

용어	설명
Pool	풀의 수
Excluded IP Address	제외한 IP 주소 범위의 수.
Declined IP Address	거부된 IP 주소의 수.

Binding Counters

용어	설명
Automatic Binding	네트워크 유형 풀과의 바인딩 수.
Manual Binding	관리자가 클라이언트에게 IP 주소를 할당하는 바인딩 수입니다. 즉, 풀이 호스트 유형인 경우를 말합니다.
Expired Binding	임대 기간이 만료되거나 자동/수동 형식의 바인딩에서 제거된 바인딩의 수입니다.

DHCP Message Received Counters

용어	설명
DISCOVER	수신된 DHCP DISCOVER 메시지의 수입니다.
REQUEST	수신된 DHCP REQUEST 메시지의 수입니다.
DECLINE	수신된 DHCP DECLINE 메시지의 수입니다.
RELEASE	수신된 DHCP RELEASE 메시지의 수입니다.
INFORM	수신된 DHCP INFORM 메시지의 수입니다.

DHCP Message Received Counters

용어	설명
OFFER	전송된 DHCP OFFER 메시지의 수입니다.
ACK	전송된 DHCP ACK 메시지의 수입니다.
NAK	전송된 DHCP NAK 메시지의 수입니다.

Buttons

Auto-refresh : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다

Refresh: 클릭 시 페이지를 새로 고침.

Clear: 클릭 시 DHCP 메시지 수신 카운터 및 DHCP 메시지 보낸 카운터를 지웁니다.

WEB 확인 예시

웹메뉴 Monitor>DHCP>Server>Statistics

DHCP Server Statistics

Database Counters

Pool	Excluded IP Address	Declined IP Address
1	2	0

Binding Counters

Automatic Binding	Manual Binding	Expired Binding
1	0	0

DHCP Message Received Counters

DISCOVER	REQUEST	DECLINE	RELEASE	INFORM
13	1	0	0	0

DHCP Message Sent Counters

OFFER	ACK	NAK
1	1	0

CLI 확인 예시

✓ DHCP Server Statistics

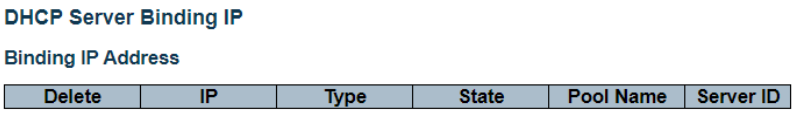
```
# show ip dhcp server statistics

Database Counters
=========================
  POOL                1
  Excluded IP           2
  Declined IP           0
=========================
Binding Counters
=========================
```

```
  Automatic              1
  Manual                 0
  Expired                0
=========================
Message Received Counters
=========================
  DISCOVER              13
  REQUEST                1
  DECLINE                0
  RELEASE                0
  INFORM                 0
=========================
Message Sent Counters
=========================
  OFFER                  1
  ACK                    1
  NAK                    0
=========================
```

6.4.2.2. Server Binding

웹메뉴 Monitor>DHCP>Server>Binding

이 페이지는 DHCP 클라이언트에 대해 생성된 바인딩을 표시합니다.



DHCP Server Binding IP

Binding IP Address

용어	설명
IP	DHCP 클라이언트에 할당된 IP 주소입니다. 클릭하면 상세페이지로 이동합니다.
Type	바인딩의 유형입니다. 가능 유형은 자동(Automatic), 수동(Manual), 만료(Expired)입니다.
State	바인딩의 상태입니다. 가능 상태는 확정(Committed), 할당(Allocated), 만료(Expired)입니다.
Pool Name	바인딩을 생성하는 풀의 이름입니다.
Server ID	바인딩을 서비스하는 서버의 IP 주소입니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다

Refresh : 클릭 시 페이지를 새로 고침.

Clear Selected : 선택한 바인딩을 취소합니다. 선택 결합이 자동 또는 수동이면, 그 만료되도록 변경됩니다. 만료 된 바인딩을 선택하면, 다음은 해제됩니다.

Clear Automatic : 모든 자동 바인딩을 지우고 만료 된 바인딩으로 변경하려면 클릭합니다.

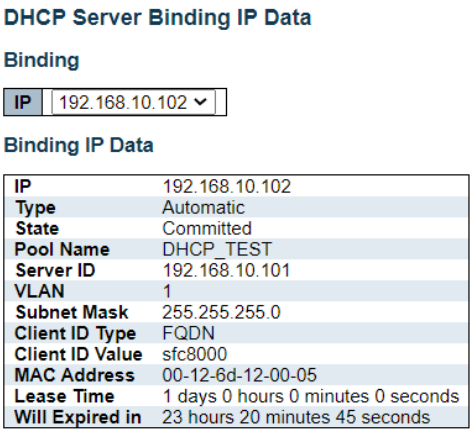
Clear Manual : 모든 수동 바인딩을 취소하고 만료 된 바인딩으로 변경하려면 클릭합니다.

Clear Expired : 모든 만료 된 바인딩을 취소 하려면 클릭합니다.

DHCP Server Binding IP Data

웹메뉴 Monitor>DHCP>Server>Binding

이 페이지는 바인딩의 상세 데이터를 표시합니다.



DHCP Server Binding IP Data

Binding

용어	설명
IP	선택된 바인딩의 IP 주소입니다.

Binding IP Data

용어	설명
IP	DHCP 클라이언트에 할당된 IP 주소입니다.
Type	바인딩의 유형입니다. 가능 유형은 자동(Automatic), 수동(Manual), 만료(Expired)입니다.
State	바인딩의 상태입니다. 가능 상태는 확정(Committed), 할당(Allocated), 만료(Expired)입니다.
Pool Name	바인딩을 생성하는 풀의 이름입니다.
Server ID	바인딩을 서비스하는 서버의 IP 주소입니다.
VLAN ID	DHCP 클라이언트가 속한 인터페이스의 VLAN ID입니다.
Subnet Mask	DHCP 클라이언트가 속한 인터페이스의 넷마스크입니다.
Client ID Type	DHCP 클라이언트 식별자의 유형입니다. 가능 유형은 FQDN, MAC 및 -입니다.
Client ID Value	DHCP 클라이언트 식별자의 값입니다.
MAC Address	DHCP 클라이언트의 하드웨어 주소입니다.
Lease Time	바인딩의 임대 시간입니다.
Will Expired in	바인딩이 만료되기까지 남은 시간입니다.

WEB 확인 예시

웹메뉴 Monitor>DHCP>Server>Binding

DHCP Server Binding IP

Binding IP Address

Delete	IP	Type	State	Pool Name	Server ID
☐	192.168.10.102	Automatic	Committed	DHCP_TEST	192.168.10.101

웹메뉴 Monitor>DHCP>Server>Binding>Click IP

DHCP Server Binding IP Data

Binding

IP 192.168.10.102

Binding IP Data

IP	192.168.10.102
Type	Automatic
State	Committed
Pool Name	DHCP_TEST
Server ID	192.168.10.101
VLAN	1
Subnet Mask	255.255.255.0
Client ID Type	FQDN
Client ID Value	sfc8000
MAC Address	00-12-6d-12-00-05
Lease Time	1 days 0 hours 0 minutes 0 seconds
Will Expired in	23 hours 2 minutes 53 seconds

CLI 확인 예시

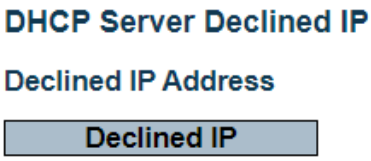
✓ DHCP Server Binding IP

```
# show ip dhcp server binding

IP: 192.168.10.102
--------------------------------------------
  State is committed
  Binding type is automatic
  Pool name is DHCP_TEST
  Server ID is 192.168.10.101
  VLAN ID is 1
  Subnet mask is 255.255.255.0
  Client identifer is type of FQDN that is sfc8000
  Hardware address is 00:12:6d:12:00:05
  Lease time is 1 days 0 hours 0 minutes 0 seconds
  Expiration is in 23 hours 33 minutes 17 seconds
```

6.4.2.3. Server Declined IP

웹메뉴 Monitor>DHCP>Server>Declined IP

이 페이지는 거부된 IP 주소를 표시합니다.



DHCP Server Declined IP

Declined IP Address

용어	설명
Declined IP	거부된 IP 주소의 목록입니다.

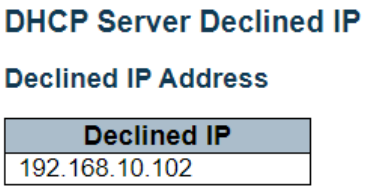
Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다

Refresh : 클릭 시 페이지를 새로 고침.

WEB 확인 예시

웹메뉴 Monitor>DHCP>Server>Declined IP



CLI 확인 예시

✓ **DHCP Server Binding IP**

```
# show ip dhcp server declined-ip

Declined IP Address
      ------------------
0001   192.168.10.102
```

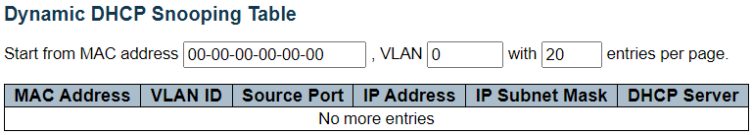
6.4.2.4. Snooping Table

웹메뉴 Monitor>DHCP>Snooping Table

이 페이지는 DHCP 스누핑 모드가 비활성화 된 후 동적 IP 할당 정보를 표시합니다.

DHCP 클라이언트들은 DHCP 서버로부터 동적으로 IP 주소를 획득한 경우에만 이 테이블에 나열됩니다.

(로컬 VLAN 인터페이스 IP 주소는 제외됩니다.)



Dynamic DHCP Snooping Table

용어	설명
MAC Address	사용자 MAC주소 항목입니다..
VLAN ID	VLAN-ID가있는 DHCP 트래픽이 허용됩니다.
Source Port	항목이 표시되는 포트 번호를 전환합니다.
IP Address	항목의 사용자 IP 주소입니다.
IP Subnet Mask	항목의 사용자 IP 서브넷 마스크.
DHCP Server	항목의 DHCP 서버 주소

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

Clear : 클릭 시 카운터 선택을 취소합니다.

|<< : 동적 DHCP 스누핑 테이블의 첫 번째 항목에서 시작하는 테이블을 업데이트합니다.

>> : 현재 표시되는 마지막 항목 후에 항목에서 시작, 테이블을 업데이트합니다.

WEB 확인 예시

웹메뉴 Monitor>DHCP>Snooping Table

Dynamic DHCP Snooping Table

Start from MAC address 00-00-00-00-00-00 , VLAN 0 with 20 entries per page.

MAC Address	VLAN ID	Source Port	IP Address	IP Subnet Mask	DHCP Server
00-21-6d-05-f0-5c	1	1	192.168.10.102	255.255.255.0	192.168.10.101 (Local)

CLI 확인 예시

✓ **Dynamic DHCP Snooping Table**

```
# show ip dhcp snooping table

Entry ID            : 1
MAC Address         : 00-21-6d-05-f0-5c
VLAN ID             : 1
Source Port         : GigabitEthernet 1/1
IP Address          : 192.168.10.102
IP Subnet Mask      : 255.255.255.0
DHCP Server Address: 192.168.10.101 (Local)
Total Entries Number : 1
```

6.4.2.5. Detailed Statistics

웹메뉴 Monitor>DHCP>Detailed Statistics

이 페이지에서 DHCP 스누핑에 대한 통계를 제공합니다.

DHCP Detailed Statistics Port 1

Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

Dynamic Detailed Statistics Port n

용어	설명
Rx and Tx Discover	수신 및 송신된 Discover 패킷의 수를 표시합니다.
Rx and Tx Offer	수신 및 송신된 offer패킷의 수를 표시합니다.
Rx and Tx Request	수신 및 송신된 request패킷의 수를 표시합니다.
Rx and Tx Decline	수신 및 송신된 decline패킷의 수를 표시합니다.
Rx and Tx ACK	수신 및 송신된 ACK 패킷의 수를 표시합니다.
Rx and Tx NAK	수신 및 송신된 NAK 패킷의 수를 표시합니다.
Rx and Tx Release	수신 및 송신된 Release 패킷의 수를 표시합니다.
Rx and Tx Inform	수신 및 송신된 Inform 패킷의 수를 표시합니다.
Rx and Tx Lease Query	수신 및 송신된 Lease Query 패킷의 수를 표시합니다.
Rx and Tx Lease Unassigned	수신 및 송신된 Lease Unassigned 패킷의 수를 표시합니다.
Rx and Tx Lease Unknown	수신 및 송신된 Lease Unknown 패킷의 수를 표시합니다.
Rx and Tx Lease Active	수신 및 송신된 Lease Active 패킷의 수를 표시합니다.
Rx Discarded checksum error	IP / UDP 체크섬 오류로 인한 폐기 패킷의 수입니다.
Rx Discarded from Untrusted	신뢰할 수없는 포트 에서 오는 버려진 패킷의 수입니다.

Buttons

Combined : 버튼을 클릭하여 어떤 유형의 장비를 지정합니다.

Port 1 : 버튼을 클릭하여 포트를 지정하십시오.

Auto-refresh : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

Clear : 클릭 시 카운터 선택을 취소합니다.

WEB 확인 예시

웹메뉴 Monitor>DHCP>Detailed Statistics

✓ DHCP Detailed Statistics Port 1(Client/port1)

DHCP Detailed Statistics Port 1

Receive Packets		Transmit Packets	
Rx Discover	35	Tx Discover	29
Rx Offer	0	Tx Offer	1
Rx Request	28	Tx Request	1
Rx Decline	0	Tx Decline	0
Rx ACK	1	Tx ACK	28
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

CLI 확인 예시

✓ DHCP Detailed Statistics Port 1(Client/port1)

```
# show ip dhcp detailed statistics client/combined/normal-forward/relay/server/snooping
interface 10GigabitEthernet/GigabitEthernet <port_type_list>
# show ip dhcp detailed statistics client interface GigabitEthernet 1/1

GigabitEthernet 1/1 Statistics:
------------------------------
Rx Discover:                0   Tx Discover:                29
Rx Offer:                   0   Tx Offer:                   0
Rx Request:                 0   Tx Request:                 1
Rx Decline:                 0   Tx Decline:                 0
Rx ACK:                     1   Tx ACK:                     0
Rx NAK:                     0   Tx NAK:                     0
Rx Release:                 0   Tx Release:                 0
Rx Inform:                  0   Tx Inform:                  0
Rx Lease Query:             0   Tx Lease Query:             0
Rx Lease Unassigned:        0   Tx Lease Unassigned:        0
Rx Lease Unknown:           0   Tx Lease Unknown:           0
Rx Lease Active:            0   Tx Lease Active:            0
Rx Discarded checksum error:    0
```

6.5. Security

6.5.1. Switch Configuration

제품은 로컬 관리자 및 사용자에 대한 인증 기능을 제공하며 계정별 권한 수준에 따라 사용 권한이 부여됩니다.

사용자 계정 및 권한
사용자 이름과 권한 수준으로 식별되는 스위치에서 여러 사용자를 생성할 수 있습니다.

사용자 허용 범위의 권한 수준은 1~15입니다. 권한 수준 값 15는 모든 그룹에 대한 액세스를 허용하고 장치에 대한 전체 제어 권한을 부여합니다. 사용자 권한은 그룹의 권한 수준과 같거나 높아야 합니다. 기본적으로 권한 수준 5는 읽기 전용 액세스를 제공하고 권한 수준 10은 대부분의 그룹에 대한 읽기-쓰기 액세스를 제공합니다. 소프트웨어 업로드 및 공장 기본 복원과 같은 시스템 유지 관리 작업에는 권한 수준 15가 필요합니다. 일반적으로 관리자 계정에는 권한 수준 15, 일반 사용자 계정에는 권한 수준 10, 게스트 계정에는 권한 수준 5가 사용됩니다.

권한 그룹을 식별하는 이름을 그룹 이름이라고 합니다. 대부분의 경우 권한 수준 그룹은 단일 모듈(예: LACP, RSTP 또는 QoS)로 구성되지만 일부는 둘 이상을 포함합니다.

각 그룹에는 다음 하위 그룹에 대해 1에서 15 사이에서 구성 가능한 인증 권한 수준이 있습니다.

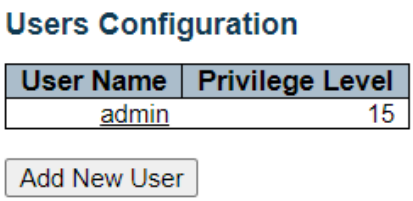
- 구성 읽기 전용
- 구성/실행 읽기-쓰기
- 상태/통계 읽기 전용
- 상태/통계 읽기-쓰기(예: 통계 지우기).

그룹 권한 수준은 웹 인터페이스에서만 사용됩니다. CLI 권한 수준은 각 개별 명령에서 작동합니다. 사용자 권한은 그룹의 권한 수준보다 크거나 같아야 합니다.

6.5.1.1. Users

웹메뉴 Configuration>Security>Switch>Users

이 페이지는 현재 사용자에 대한 개요를 제공합니다.
현재 웹 서버에서 다른 사용자로 로그인하는 방법은 브라우저를 닫은 후 다시 열거나 오른쪽 상단의 Logout 을 사용하면 됩니다.



Users Configuration

용어	설명
User Name	사용자를 식별하는 이름입니다. 이는 사용자 추가/편집으로 이동하는 링크로도 작동합니다.
Privilege Level	사용자의 권한 수준입니다. 허용되는 범위는 0부터 15까지입니다. 권한 수준 값이 15인 경우, 모든 그룹에 액세스할 수 있으며 디바이스를 완전히 제어할 수 있습니다. 그러나 다른 값은 각 그룹의 권한 수준을 참조해야 합니다. 사용자의 권한은 해당 그룹에 액세스하기 위해 동일하거나 그 이상이어야 합니다. 기본 설정에 따르면, 대부분의 그룹의 권한 수준 5는 읽기 전용 액세스를 허용하고, 권한 수준 10은 읽기/쓰기 액세스를 허용합니다. 또한 시스템 유지 관리(소프트웨어 업로드, 공장 초기화 등)에는 사용자 권한 수준 15가 필요합니다. 기본적인 관리자계정은 15레벨입니다.

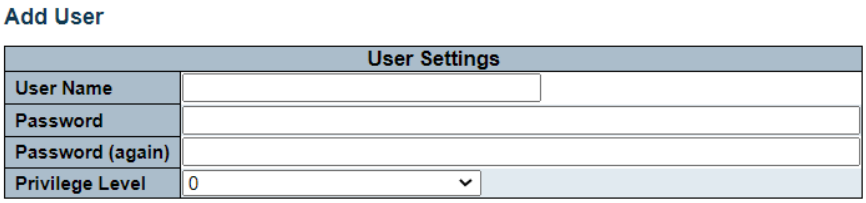
Buttons

Add New User : 새로운 사용자를 추가합니다.

User 추가시 Add New User 버튼을 누르면 Add User설정 페이지가 나옵니다.

Add User

이 페이지는 사용자를 구성하는 페이지입니다.



Add User

용어	설명
User Name	이 항목이 추가할 사용자 이름을 식별하는 문자열입니다. 유효한 사용자 이름은 문자, 숫자 및 밑줄을 허용합니다.(길이 1~31)
Password	사용자의 비밀번호입니다. 허용되는 문자열 길이는 1에서 63까지입니다. 공백을 포함한 모든 출력 가능한 문자가 허용됩니다.
Privilege Level	사용자의 권한 수준입니다. 허용되는 범위는 0부터 15까지입니다. 권한 수준 값이 15인 경우, 모든 그룹에 액세스할 수 있으며 디바이스를 완전히 제어할 수 있습니다. 그러나 다른 값은 각 그룹의 권한 수준을 참조해야 합니다. 사용자의 권한은 해당 그룹에 액세스하기 위해 동일하거나 그 이상이어야 합니다. 기본 설정에 따르면, 대부분의 그룹의 권한 수준 5는 읽기 전용 액세스

	를 허용하고, 권한 수준 10은 읽기/쓰기 액세스를 허용합니다. 또한 시스템 유지 관리(소프트웨어 업로드, 공장 초기화 등)에는 사용자 권한 수준 15가 필요합니다. 기본적인 관리자계정은 15레벨입니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.
Cancel: 로컬 변경 사항을 취소하고 돌아갑니다.
Delete User: 클릭 시 현재 사용자가 삭제 적용합니다.
Delete User Save: 클릭 시 현재 사용자가 삭제 적용 및 저장합니다.

WEB 설정 예시

웹메뉴 Configuration>Security>Switch>Users

✓ Users Configuration

➢ *Add New User*

- ***Add User (Click Add New User)***

Add User

User Settings	
User Name	test
Password	••••••••••
Password (again)	••••••••••
Privilege Level	10

Users Configuration

User Name	Privilege Level
test	10
admin	15

- ***Edit User (Click User Name)***

Edit User

User Settings	
User Name	test
Password	••••••••••
Password (again)	••••••••••
Privilege Level	9

Users Configuration

User Name	Privilege Level
test	9
admin	15

CLI 설정 예시

✓ Users Configuration

➢ *Add New User*

- ***Add User / Edit User***

```
(config)# username <word31> privilege <0-15> password unencrypted
(config)# username test privilege 10 password unencrypted
#: Please input a new password (plain): <line31>
#: Please input the new password AGAIN: <line31>
```

6.5.1.2. Privilege Levels

웹메뉴 Configuration>Security>Switch>Privilege Level

이 페이지는 Privilege Level 에 따른 스위치 접근 권한을 설정합니다.

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
DDMI	15	15	10	15
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	15	15	15	15
EPS	5	10	5	10
ERPS	5	10	5	10
ETH_LINK_OAM	5	10	5	10
Green_Ethernet	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
MEP	5	10	5	10
MVR	5	10	5	10
NTP	5	10	5	10
POE	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10
RMirror	15	15	15	15
Security	15	15	15	15
sFlow	5	10	5	10
Spanning_Tree	5	10	5	10
System	15	15	15	15
VCL	5	10	5	10
VLAN_Translation	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10
XXRP	5	10	5	10

Privilege Level Configuration

용어	설명
Group Name	권한 그룹을 식별하는 이름입니다. 대부분의 경우, 권한 수준 그룹은 단일 모듈로 구성되지만 일부 그룹은 여러 개의 모듈을 포함합니다. 다음 설명은 이러한 권한 수준 그룹을 자세히 정의합니다: **System** Contact, Name, Location, Timezone, Daylight Saving Time, Log. **Security** Authentication, System Access Management, Port (contains MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard. **IP** Ping을 제외한 전체. **Port** VeriPHY를 제외한 전체. **Diagnostics** Ping과 VeriPHY. **Maintenance** CLI에서 System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load.

	Web에서 Users, Privilege Levels과 전체Maintenance. **Debug** CLI에서 해당됨.
Privilege Level	사용자의 권한 수준은 해당 그룹에 대한 권한 수준과 동일하거나 더 높아야 해당 그룹에 대한 액세스 권한을 갖습니다. Configuration Read-Only: 설정을 보기만 할 수 있도록 허용합니다. Configuration/Execute Read-Write: 설정을 읽고 쓸 수 있는 권한을 부여합니다. Status/Statistics Read-Only: 상태 정보와 통계 정보를 읽을 수 있도록 허용합니다. Status/Statistics Read-Write: 상태 정보와 통계 정보를 읽고 쓸 수 있는 권한을 부여합니다. (예:통계를 지울 수 있음)

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>Security>Switch>Privilege Level

✓ Privilege Level Configuration

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
DDMI	15	15	10	15
Debug		15	15	15
DHCP		10	5	10
DHCPv6_Client		10	5	10
Diagnostics		15	15	15
EPS		10	5	10
ERPS		10	5	10
ETH_LINK_OAM		10	5	10
Green_Ethernet		10	5	10
IP		10	5	10
IPMC_Snooping		10	5	10
LACP		10	5	10
LLDP		10	5	10
Loop_Protect		10	5	10
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
MEP	5	10	5	10
MVR	5	10	5	10
NTP	5	10	5	10
POE	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
QoS	5	10	5	10

(0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15)

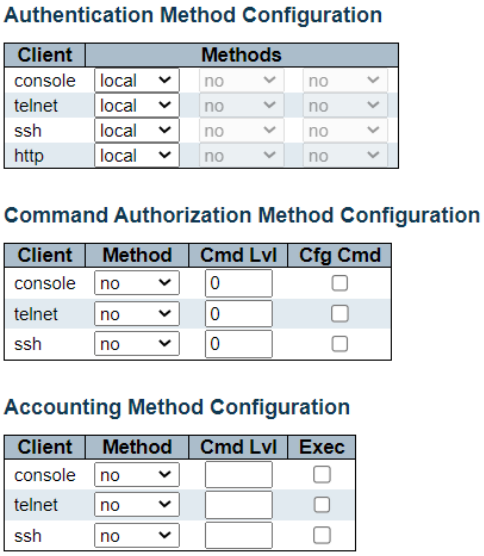
CLI 설정 예시

✓ Privilege Level Configuration

```
(config)# web privilege group {1} level {2} <0-15>
(config)# web privilege group DDMI level configRoPriv 6

{1}
Aggregation      DDMI            DHCP            DHCPv6_Client
Debug            Diagnostics     EPS             ERPS
ETH_LINK_OAM     Green_Ethernet  IP              IPMC_Snooping
LACP             LLDP            Loop_Protect    MAC_Table
MEP              MVR             Maintenance     NTP
POE              Ports           Private_VLANs   QoS
RMirror          Security        Spanning_Tree   System
VCL              VLAN_Translation VLANs          Voice_VLAN
XXRP             sFlow

{2}
configRoPriv  configRwPriv  statusRoPriv  statusRwPriv
```

6.5.1.3. Auth Method

웹메뉴 Configuration>Security>Switch>Auth Method



Authentication Method Configuration

용어	설명
Authentication Method Configuration	사용자가 관리 클라이언트 인터페이스를 통해 스위치에 로그인할 때 어떻게 인증되는지를 구성할 수 있습니다.
Client	해당 관리 클라이언트에 적용됩니다.
Methods	다음 값 중 하나로 설정할 수 있습니다. **no** 인증이 비활성화되어 로그인이 불가능합니다. **local** 인증을 스위치의 로컬 사용자 데이터베이스를 사용합니다. **radius** 원격 RADIUS 서버를 사용하여 인증합니다. **tacacs** 원격 TACACS+ 서버를 사용하여 인증합니다. 원격 서버를 사용하는 방식은 원격 서버가 오프라인인 경우 제한 시간이 있습니다. 이 경우 다음 방식이 시도됩니다. 각 방식은 왼쪽에서 오른쪽으로 시도되며 사용자가 승인 또는 거부될 때까지 계속됩니다. (로컬 설정이 있으면 서버가 작동하지 않아도 직접 설정이 가능)

Command Authorization Method Configuration

용어	설명
Command Authorization Method Configuration	사용자가 사용 가능한 CLI 명령을 제한할 수 있는 기능을 제공합니다.
Client	해당 관리 클라이언트에 적용됩니다.
Method	다음 값 중 하나로 설정할 수 있습니다. **no** 명령어 인가가 비활성화됩니다. 사용자는 권한 수준에 따라 CLI 명령에 대한 액세스 권한이 부여됩니다. **tacacs** 명령어 인가를 위해 원격 TACACS+ 서버를 사용합니다. 모든

	원격 서버가 오프라인인 경우 사용자는 권한 수준에 따라 CLI 명령에 대한 액세스 권한이 부여됩니다.
Cmd Lvl	이 수준보다 높거나 동일한 권한 수준을 가진 모든 명령어를 인가합니다. 유효한 값은 0에서 15 사이입니다.
Cfg Cmd	구성 명령어도 인가합니다.

Accounting Method Configuration

용어	설명
Accounting Method Configuration	명령어 및 exec(로그인) 계정을 구성할 수 있습니다.
Client	해당 관리 클라이언트에 적용됩니다.
Method	다음 값 중 하나로 설정할 수 있습니다: **no** 계정(Accounting)이 비활성화됩니다. **tacacs** 계정을 위해 원격 TACACS+ 서버를 사용합니다.
Cmd Lvl	이 수준보다 높거나 동일한 권한 수준을 가진 모든 명령어의 계정을 활성화합니다. 유효한 값은 0에서 15 사이입니다. 계정을 비활성화하려면 필드를 비워 두세요.
Exec	exec(로그인) 계정을 활성화합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>Security>Switch>Auth Method

✓ Authentication Method Configuration

Authentication Method Configuration

Client	Methods		
console	tacacs	radius	local
telnet	no	no	no
ssh	tacacs	local	no
http	radius	tacacs	local

✓ Command Authorization Method Configuration

Command Authorization Method Configuration

Client	Method	Cmd Lvl	Cfg Cmd
console	tacacs	15	☑
telnet	tacacs	10	☐
ssh	no	0	☐

✓ **Accounting Method Configuration**

Accounting Method Configuration

Client	Method	Cmd Lvl	Exec
console	tacacs	15	☑
telnet	tacacs	10	☐
ssh	no		☐

CLI 설정 예시

✓ **Authentication Method Configuration**

```
(config)# aaa authentication login {1} {2}
(config)# aaa authentication login console tacacs radius local
(config)# aaa authentication login ssh tacacs local
(config)# aaa authentication login http radius tacacs local

(config)# no aaa authentication login {1}
(config)# no aaa authentication login telnet

{1}
Console  http  ssh  telnet

{2}
local  radius  tacacs
```

✓ **Command Authorization Method Configuration**

```
(config)# aaa authorization {1} tacacs commands <0-15> {2}
(config)# aaa authorization console tacacs commands 15 config-commands
(config)# aaa authorization telnet tacacs commands 10

(config)# no aaa authorization {1}
(config)# no aaa authorization ssh

{1}
console   ssh   telnet

{2}
config-commands   <cr>
```

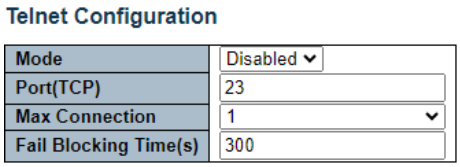
✓ **Accounting Method Configuration**

```
(config)# aaa accounting {1} tacacs {2}
(config)# aaa accounting console tacacs commands 15 exec
(config)# aaa accounting telnet tacacs commands 10

(config)# no aaa accounting {1}
(config)# no aaa accounting ssh

{1}
console   ssh   telnet

{2}
commands <0-15>   exec
```

6.5.1.4. Telnet

웹메뉴 Configuration>Security>Switch>Telnet

이 페이지는 Telnet 을 설정합니다.



Telnet Configuration

용어	설명
Mode	Telnet 모드 동작을 나타냅니다. Enable: Telnet 동작을 활성화합니다 Disable: Telnet 동작을 비활성화합니다.(기본값)
Port(TCP)	Telnet 접속을 위한 TCP 포트를 입력하세요.
Max Connection	스위치에 연결 할 수 있는 클라이언트 수.
Fail Blocking Time(s)	로그인 시도가 여러 번 실패할 경우 차단 시간: 유효한 값은 10초에서 3600초(1시간)로 제한됩니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

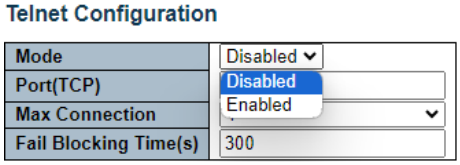
WEB 설정 예시

웹메뉴 Configuration>Security>Switch>Telnet

✓ **Telnet Configuration**

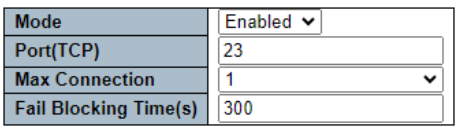
➢ ***Mode***

- ***Enable | Disable***



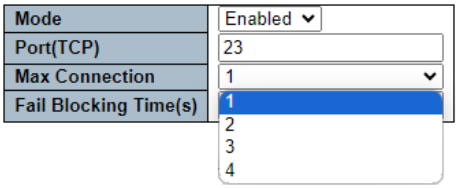
➢ ***Port(TCP)***

- ***Default 23***



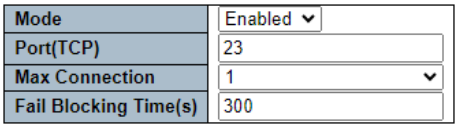
➢ ***Max Connection***

- ***1 | 2 | 3 | 4***



➢ ***Fail Blocking Time(s)***

- ***10~3600sec***



CLI 설정 예시

✓ Telnet Configuration

➢ ***Mode***

- ***Enable | Disable***

```
(config)# ip telnet
(config)# no ip telnet
```

➢ ***Port(TCP)***

- ***Default 23***

```
(config)# ip telnet port { <port> | default }
(config)# ip telnet port 23
(config)# ip telnet port default
```

➢ ***Max Connection***

- ***1 | 2 | 3 | 4***

```
(config)# ip telnet max-connection <connection_cnt>
(config)# ip telnet max-connection 2
(config)# ip telnet max-connection 1
```

➢ ***Fail Blocking Time(s)***

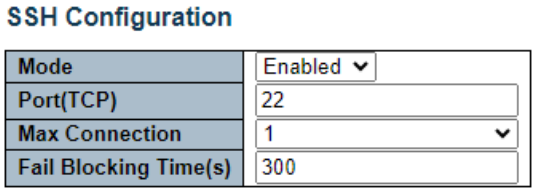
- ***10~3600sec***

```
(config)# ip telnet retry-block-time <block_time>
(config)# ip telnet retry-block-time 300
(config)# ip telnet retry-block-time 10
```

6.5.1.5. SSH

웹메뉴 Configuration>Security>Switch>SSH

이 페이지는 SSH 를 설정합니다.



SSH Configuration

용어	설명
Mode	SSH 모드 동작을 나타냅니다. Enable: SSH 동작을 활성화합니다 Disable: SSH 동작을 비활성화합니다.
Port(TCP)	SSH 서비스의 TCP 포트 번호
Max Connection	스위치에 접근 가능한 클라이언트 수
Fail Blocking Time(s)	로그인 시도가 여러 번 실패할 경우 차단 시간: 유효한 값은 10초에서 3600초(1시간)로 제한됩니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

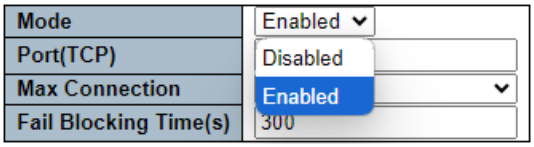
WEB 설정 예시

웹메뉴 Configuration>Security>Switch>SSH

✓ **SSH Configuration**

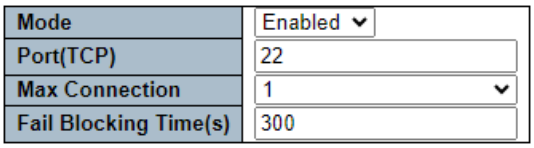
➢ ***Mode***

- ***Enable | Disable***



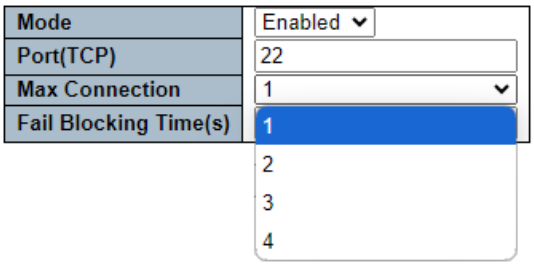
➢ ***Port(TCP)***

- ***1~65534 | 22(default)***



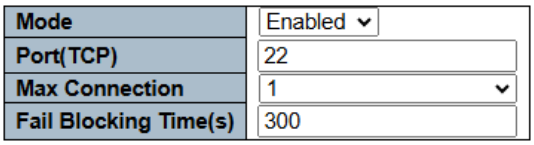
➢ ***Max Connection***

- ***1 | 2 | 3 | 4***



➢ ***Fail Blocking Time(s)***

- ***10~3600sec***



CLI 설정 예시

✓ SSH Configuration

➢ ***Mode***

- ***Enable | Disable***

```
(config)# ip ssh
(config)# no ip ssh
```

➢ ***Port(TCP)***

- ***1~65534 | 22(default)***

```
(config)# ip ssh port { <port> | default }
(config)# ip ssh port 22
(config)# ip ssh port default
```

➢ ***Max Connection***

- ***1 | 2 | 3 | 4***

```
(config)# ip ssh max-connection <connection_cnt>
(config)# ip ssh max-connection 1
(config)# ip ssh max-connection 2
```

➢ ***Fail Blocking Time(s)***

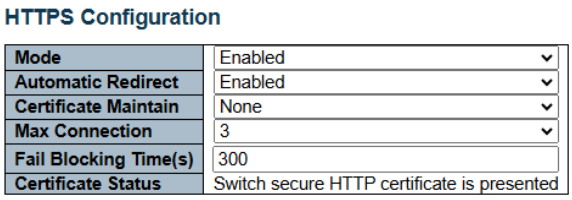
- ***10~3600sec***

```
(config)# ip ssh retry-block-time <block_time>
(config)# ip ssh retry-block-time 10
(config)# ip ssh retry-block-time 300
```

6.5.1.6. HTTPS

웹메뉴 Configuration>Security>Switch>HTTPS

이 페이지에서는 스위치의 HTTPS 설정을 구성하고 현재 인증서에 대한 설정을 할 수 있습니다.



HTTPS Configuration

용어	설명
Mode	HTTPS 모드 동작을 나타냅니다. Enabled: HTTPS동작을 활성화합니다. Disabled: HTTPS동작을 비활성화합니다.
Automatic Redirect	HTTPS 리디렉션 모드 동작을 나타냅니다. 리디렉션 모드는 활성화되면 HTTP 연결은 자동으로 HTTPS로 연결됩니다. (Mode가 Enabled인 경우에만 적용) Enabled: HTTPS 리디렉션 모드 동작을 활성화합니다. Disabled: HTTPS 리디렉션 모드 동작을 비활성화합니다.
Certificate Maintain	인증 유지 작업은 다음과 같은 가능한 작업들을 의미합니다. None: 작업 없음. Delete: 현재 인증서 삭제. Upload: 인증서 PEM 파일 업로드. (웹 브라우저 또는 URL을 통해 업로드할 수 있습니다.) Generate: 새로운 자체 서명 RSA 인증서 생성.
Certificate Pass Phrase	만약 업로드하는 인증서가 특정한 암호구문으로 보호되어 있다면, 해당 암호구문을 이 필드에 입력하세요. (Certificate Maintain 항목에서 Upload를 선택하면 사용 가능합니다.)
Certificate Upload	스위치에 PEM 파일 형식의 인증서를 업로드합니다. 파일에는 인증서와 개인 키가 함께 포함되어야 합니다. 인증서와 개인 키를 따로 저장한 두 개의 파일이 있는 경우 Linux의 cat 명령을 사용하여 하나의 PEM 파일로 결합합니다. RSA 인증서가 권장되며, 대부분의 최신 브라우저 버전에서는 DSA 인증서 지원이 제거되었습니다(예: Firefox v37 및 Chrome v39). 가능한 방법은 다음과 같습니다: Web Browser: 웹 브라우저를 통해 인증서를 업로드합니다. URL: URL을 통해 인증서를 업로드합니다. 지원되는 프로토콜은 HTTP, HTTPS, TFTP, FTP입니다. URL 형식은 <프로토콜>://[<사용자이름>[:<비밀번호>]@]<호스트>[:<포트>][/<경로>]/<파일이름>입니다. *tftp://10.10.10.10/new_image_path/new_image.dat,* *http://username:password@10.10.10.10:80/new_image_path/new_image.dat*

	유효한 파일 이름은 알파벳 (A-Za-z), 숫자 (0-9), 점 (.), 하이픈 (-), 언더스코어(_)로 구성된 텍스트 문자열입니다. 최대 길이는 63자이며, 하이픈은 첫 번째 문자가 될 수 없습니다. '.'만으로 구성된 파일 이름은 허용되지 않습니다.
Certificate Status	스위치의 인증서 현재 상태를 표시합니다. 스위치 보안 HTTPS 인증서가 제시됩니다.(presented) 스위치 보안 HTTPS 인증서가 제시되지 않습니다.(not presented) 스위치 보안 HTTPS 인증서 생성 중입니다.(generating)
Max Connection	스위치에 접근 가능한 클라이언트 수
Fail Blocking Time(s)	로그인 시도가 여러 번 실패할 경우 차단 시간: 유효한 값은 10초에서 3600초(1시간)로 제한됩니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

Refresh: 페이지를 새로 고침을 클릭합니다. 로컬에서의 변경 사항을 취소할 수 있습니다.

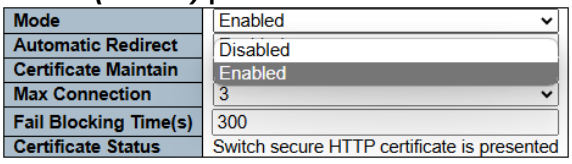
WEB 설정 예시

웹메뉴 Configuration>Security>Switch>HTTPS

✓ **HTTPS Configuration**

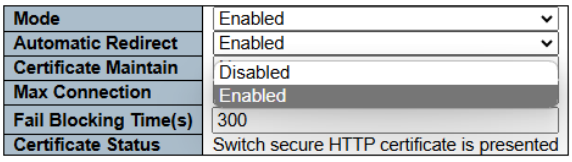
➢ ***Mode***

- ***Enable(default) | Disable***



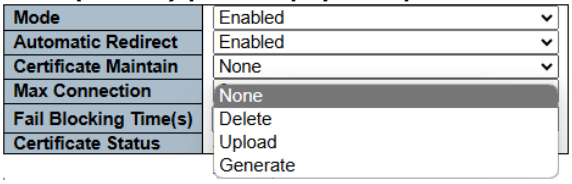
➢ ***Automatic Redirect***

- ***Enable(default) | Disable***

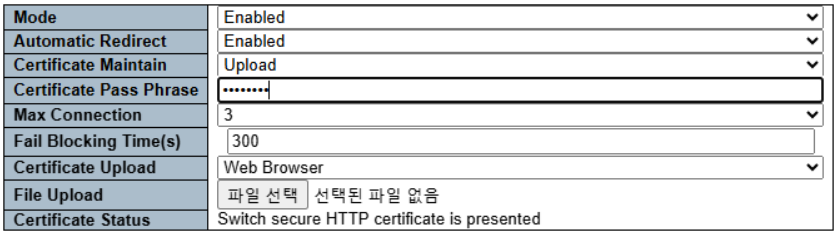


➢ ***Certificate Maintain***

- ***None(default) | Delete | Upload | Generate***

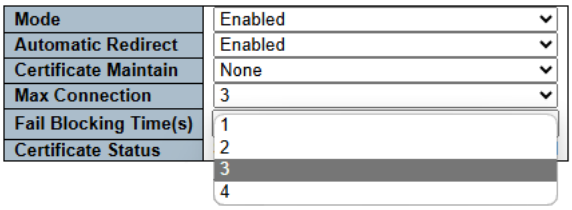


➢ ***Certificate Pass Phrase***



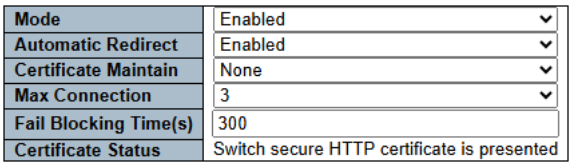
➢ ***Max Connection***

- ***1 | 2 | 3 | 4***



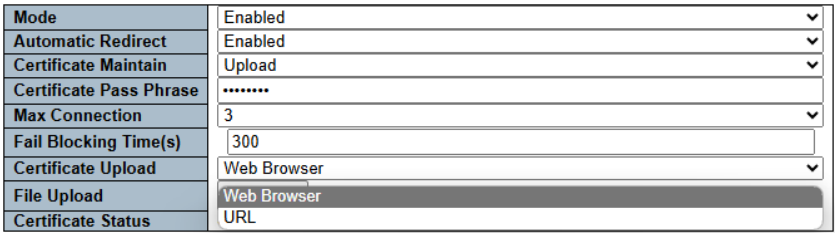
➢ ***Fail Blocking Time(s)***

- ***10~3600sec***

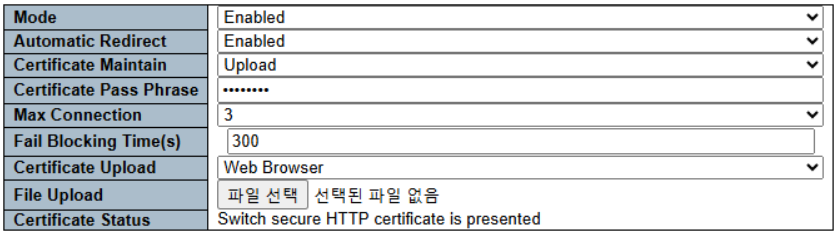


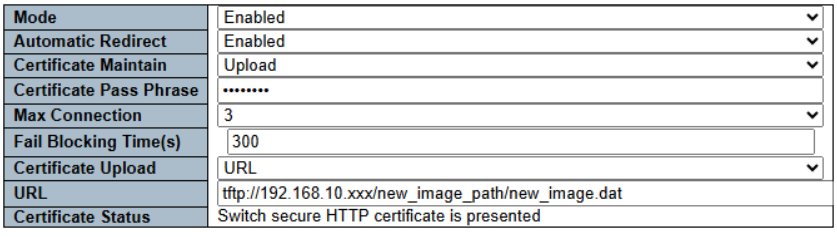
➢ ***Certificate Upload***

- ***Web Browser | URL***



➢ ***File Upload | URL***





CLI 설정 예시

✓ HTTPS Configuration

➢ *Mode*

- ***Enable(default) | Disable***

```
(config)# ip http secure-server
(config)# no ip http secure-server
```

➢ *Automatic Redirect*

- ***Enable(default) | Disable***

```
(config)# ip http secure-redirect
(config)# no ip http secure-redirect
```

➢ *Certificate Maintain*

- ***None | Delete | Generate | Upload***

➢ *Certificate Pass Phrase*

```
(config)# ip http secure-certificate { upload <url_file> [ pass-phrase <pass_phrase> ] |
delete | generate }
(config)# ip http secure-server
(config)# ip http secure-certificate delete
(config)# ip http secure-certificate generate
(config)# ip http secure-certificate upload
tftp://192.168.10.xxx/new_image_path/new_image.dat
(config)# ip http secure-certificate upload
tftp://192.168.10.xxx/new_image_path/new_image.dat pass-phrase password
```

➢ *Max Connection*

- ***1 | 2 | 3 | 4***

```
(config)# ip http max-connection <connection_cnt>
(config)# ip http max-connection 1
(config)# ip http max-connection
```

➢ *Fail Blocking Time(s)*

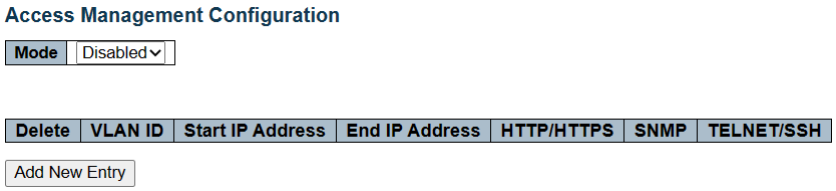
- ***10~3600sec***

```
(config)# ip http retry-block-time <block_time>
(config)# ip http retry-block-time 10
(config)# ip http retry-block-time 300
(config)# ip http retry-block-time 3600
```

6.5.1.7. Access Management

웹메뉴 Configuration>Security>Switch>Access Management

이 페이지에서 액세스 관리 테이블을 구성하세요. 최대 항목 수는 16 개입니다.



Access Management Configuration

용어	설명
Mode	액세스 관리 모드 작동을 나타냅니다. Enable: 액세스 관리 모드를 활성화합니다. Disable: 액세스 관리 모드를 비활성화합니다.
Delete	항목을 삭제합니다. 저장 시 적용 됩니다.
VLAN ID	Access Management Configuration 대한 VLAN ID를 나타냅니다.
Start IP address	Access Management Configuration 의 시작 IP 주소를 나타냅니다.
End IP address	Access Management Configuration 의 끝 IP 주소를 나타냅니다.
HTTP/HTTPS	호스트의 IP 주소가 엔트리 주소 범위에 있는 경우, 호스트는 HTTP/HTTPS 인터페이스를 통해 스위치에 액세스할 수 있다는 것을 나타냅니다.
SNMP	호스트의 IP 주소가 엔트리 주소 범위에 있는 경우, 호스트는 SNMP 인터페이스를 통해 스위치에 액세스할 수 있다는 것을 나타냅니다.
TELNET/SSH	호스트의 IP 주소가 엔트리 주소 범위에 있는 경우, 호스트는 TELNET/SSH 인터페이스를 통해 스위치에 액세스할 수 있다는 것을 나타냅니다.

Buttons

Add New Entry: 새로운 액세스 관리 항목을 추가합니다.
Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>Security>Switch>Access Management

✓ **Access Management Configuration**

➢ ***Mode***

- ***Disable(default)***

Access Management Configuration

Mode	Disabled

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH

- ***Enable***

Access Management Configuration

Mode	Enabled

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH

➢ ***Add New Entry***

Access Management Configuration

Mode	Enabled

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
☐	1	192.168.10.1	192.168.10.135	☑	☐	☑
☐	2	2.2.2.1	2.2.2.100	☐	☑	☐

✓ CLI 설정 예시

✓ Access Management Configuration

➢ ***Mode***

- ***Disable(default)***

```
(config)# no access management
```

- ***Enable***

```
(config)# access management
```

➢ ***Add New Entry***

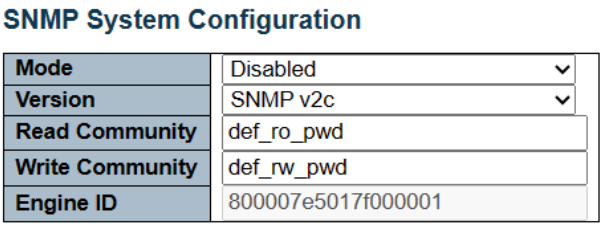
```
(config)# access management <1-16> <1-4095> <ipv4_addr> to <ipv4_addr> [1]
(config)# access management 1 1 192.168.10.1 to 192.168.10.135 web telnet
(config)# access management 2 2 2.2.2.1 to 2.2.2.100 snmp

{1}
all   snmp   telnet   web
```

6.5.1.8. SNMP

6.5.1.8.1. System

웹메뉴 Configuration>Security>SNMP>System

이 페이지에서 SNMP 를 구성하세요.



SNMP System Configuration

용어	설명
Mode	SNMP 모드 작동을 나타냅니다. Enable: SNMP 모드를 활성화합니다. Disable: SNMP 모드를 비활성화합니다.
Version	SNMP 지원 버전을 나타냅니다. SNMP v1: SNMP 지원 버전을 1로 설정합니다. SNMP v2c: SNMP 지원 버전을 2c로 설정합니다. SNMP v3: SNMP 지원 버전을 3으로 설정합니다.
Read Community	SNMP 에이전트에 액세스를 허용하기 위한 읽기 권한 커뮤니티 문자열을 나타냅니다.(영문 또는 숫자, 0~255자) 이 필드는 SNMP 버전이 SNMPv1 또는 SNMPv2c인 경우에만 적용됩니다.
Write Community	SNMP 에이전트에 액세스를 허용하기 위한 쓰기 권한 커뮤니티 문자열을 나타냅니다.(영문 또는 숫자, 0~255자) 이 필드는 SNMP 버전이 SNMPv1 또는 SNMPv2c인 경우에만 적용됩니다.
Engine ID	SNMPv3 엔진 ID를 나타냅니다. 문자열은 짝수 개의 숫자(16진수 형식)를 포함해야 하며, 전체가 0과 F는 허용되지 않습니다.(10~64자) 엔진 ID의 변경은 원래의 로컬 사용자를 모두 지우게 됩니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>Security>SNMP>System

✓ SNMP System Configuration

➢ *Mode*

- ***Disable(default)***

SNMP System Configuration

Mode	Disabled
Version	SNMP v2c
Read Community	def_ro_pwd
Write Community	def_rw_pwd
Engine ID	800007e5017f000001

- ***Enable***

SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	def_ro_pwd
Write Community	def_rw_pwd
Engine ID	800007e5017f000001

➢ *Version*

SNMP System Configuration

Mode	Enabled
Version	SNMP v1
Read Community	def_ro_pwd
Write Community	def_rw_pwd
Engine ID	800007e5017f000001

SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	def_ro_pwd
Write Community	def_rw_pwd
Engine ID	800007e5017f000001

SNMP System Configuration

Mode	Enabled
Version	SNMP v3
Read Community	def_ro_pwd
Write Community	def_rw_pwd
Engine ID	800007e5017f000001

➢ ***Community(v1/v2c)***

- ***Read Community***

SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	test123
Write Community	private
Engine ID	800007e5017f000001

- ***Write Community***

SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	test234
Engine ID	800007e5017f000001

➢ ***Engine ID(v3)***

SNMP System Configuration

Mode	Enabled
Version	SNMP v3
Read Community	public
Write Community	private
Engine ID	800007e5017f000002

CLI 설정 예시

✓ **SNMP System Configuration**

➢ ***Mode***

- ***Disable(default)***

```
(config)# no snmp-server
```

- ***Enable***

```
(config)# snmp-server
```

➢ ***Version***

```
(config)# snmp-server version {1}
(config)# snmp-server version v1

{1}
v1   v2c   v3
```

➢ ***Community(v1/v2c)***

- ***Read Community***

```
(config)# snmp-server community v2c <word255> ro
(config)# snmp-server community v2c test123 ro
```

- ***Write Community***

```
(config)# snmp-server community v2c <word255> rw
(config)# snmp-server community v2c test234 rw
```

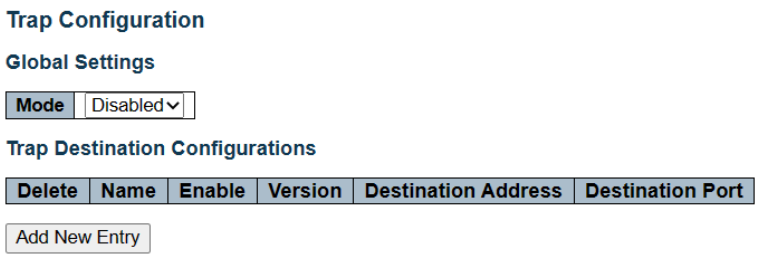
➢ ***Engine ID(v3)***

```
(config)# snmp-server engine-id local <word10-64>
(config)# snmp-server engine-id local 800007e5017f000002
```

6.5.1.8.2. Trap

웹메뉴 Configuration>Security>SNMP>Trap

이 페이지에서 SNMP Trap 를 구성하세요.



Trap Configuration

Global Setting

용어	설명
Mode	Trap 모드 작동을 나타냅니다. Enable: SNMP Trap 모드를 활성화합니다. Disable: SNMP Trap 모드를 비활성화합니다.

Trap Destination Configurations

용어	설명
Name	트랩 구성(대상)의 이름을 나타냅니다.
Enable	트랩 대상 모드 작동을 나타냅니다. Enabled: SNMP 트랩 모드 작동을 활성화합니다. Disabled: SNMP 트랩 모드 작동을 비활성화합니다.
Version	SNMP 트랩 지원 버전을 나타냅니다. SNMPv1: SNMP 트랩 지원 버전을 1로 설정합니다. SNMPv2c: SNMP 트랩 지원 버전을 2c로 설정합니다. SNMPv3: SNMP 트랩 지원 버전을 3으로 설정합니다.
Destination Address	SNMP 트랩 대상 주소를 나타냅니다. 유효한 IPv4 주소는 점으로 구분된 10진 표기법('x.y.z.w')으로 입력할 수 있습니다. 유효한 호스트명도 입력할 수 있습니다. 알파벳(A-Za-z), 숫자(0-9), 점(.), 대시(-)로 이루어진 문자열입니다. 공백은 허용되지 않으며, 첫 번째 문자는 알파벳 문자여야 하고, 첫 번째와 마지막 문자는 점(.)이나 대시(-)가 아니어야 합니다. IPv6도 입력이 가능합니다. IPv6 주소는 콜론(:)으로 구분된 16진수 4자리로 이루어진 8개 필드로 표시되는 128비트 레코드입니다. 예를 들어 'fe80::215:c5ff:fe03:4dc7'입니다. 기호 '::'은 연속된 0의 16비트 그룹을 압축하여 표시하는 특별한 구문이며, 한 번만 나타날 수 있습니다. 또한 일반적인 IPv4 주소를 이용하여 나타낼 수도 있습니다. 예를 들어 '::192.1.2.34'입니다.
Destination port	SNMP 트랩 대상 포트를 나타냅니다. SNMP 에이전트는 이 포트를 통해 SNMP 메시지를 전송합니다. 범위는 1에서 65535까지입니다.

Buttons

Add New Entry: 새로운 사용자를 추가합니다.

(해당 버튼을 클릭하면 SNMP Trap Configuration 창이 열립니다.)

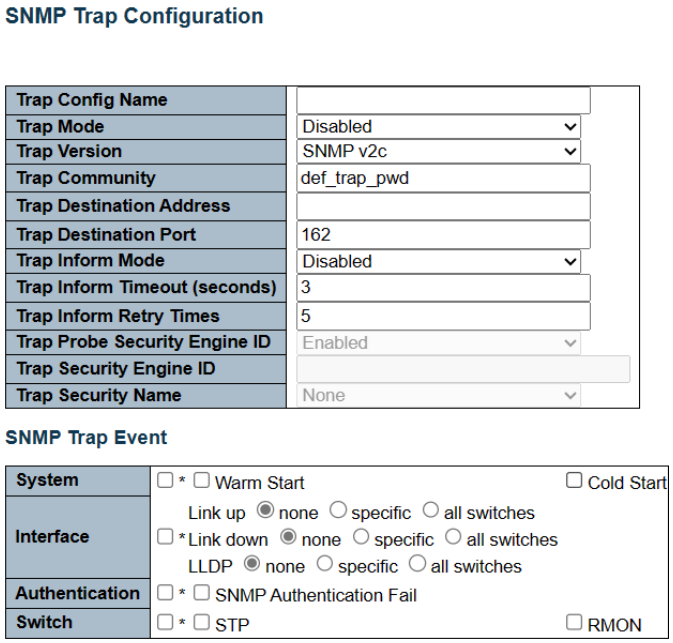
Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

SNMP Trap Detailed Configuration

이 페이지에서 trap 세부 설정을 구성하십시오.



SNMP Trap Configuration

용어	설명
Trap Config Name	Trap 구성의 이름을 나타냅니다.
Trap Mode	SNMP 모드 동작을 나타냅니다. Enabled: SNMP 모드 동작을 사용합니다. Disabled: SNMP 모드 동작을 사용하지 않습니다.
Trap Version	SNMP 트랩 지원되는 버전을 나타냅니다. SNMP v1: 설정 SNMP 트랩 버전 1을 지원합니다. SNMP v2c: 설정 SNMP 트랩 버전 2C을 지원합니다. SNMP v3: 설정 SNMP 트랩은 버전 3을 지원합니다.
Trap Community	SNMP 트랩 패킷을 보낼 때 커뮤니티 액세스 문자열을 나타냅니다. (알파벳, 숫자, 특수문자, 문자열 길이 최대255자가능)
Trap Destination Address	SNMP 트랩 대상 주소를 나타냅니다. 점으로 구분 된 십진수 표기법에 유효한 IP 주소를 ('x.y.z.w')를 사용 할 수 있습니다. 또한 유효한 호스트 이름을 사용 할 수 있습니다. 유효한 호스트 이름은 알파벳 (A-Z), 숫자 (0-9), 점(.), 대시(-)등입니다. 첫 번째 문자는 공백이

	허용될 수 없으며 영문자여야 합니다. 또한 첫 번째와 마지막 문자는 점 또는 대시가 안됩니다.
Trap Destination port	SNMP trap 대상 포트를 나타냅니다. SNMP 에이전트는 이 포트를 통해 SNMP 메시지를 전송합니다. 포트 범위는 1에서 65535까지입니다.
Trap Inform Mode	SNMP trap inform 모드 작업을 나타냅니다. Enabled: SNMP trap inform 모드를 활성화합니다. Disabled: SNMP trap inform 모드를 비활성화합니다.
Trap Inform Timeout	SNMP trap inform 타임아웃을 나타냅니다. 허용되는 범위는 0(초)부터 2147(초)까지입니다.
Trap Inform Retry Times	SNMP trap inform 재시도 횟수를 나타냅니다. 허용되는 범위는 0부터 255까지입니다.
Trap Probe Security Engine ID	SNMP trap probe 보안 엔진 ID 모드 작업을 나타냅니다. Enabled: SNMP trap probe 보안 엔진 ID 모드를 활성화합니다. Disabled: SNMP trap probe 보안 엔진 ID 모드를 비활성화합니다.
Trap Security Engine ID	SNMP trap 보안 엔진 ID를 나타냅니다. SNMPv3는 인증과 개인 정보 보호를 위해 USM을 사용하여 traps 및 informs를 전송합니다. 이러한 traps 및 informs를 위해 고유한 엔진 ID가 필요합니다. "Trap Probe Security Engine ID"가 활성화되어 있을 때는 ID가 자동으로 프로브됩니다. 비활성화 되어있는 경우 이 필드에 지정된 ID가 사용됩니다. 이 문자열은 짝수 개의 16진수 숫자로 구성되어야 하며, 10에서 64 사이의 숫자로 된 자릿수를 가져야 합니다. 다만, 전체가 0 또는 F는 허용되지 않습니다.
Trap Security Name	SNMP trap 보안 이름을 나타냅니다. SNMPv3는 인증과 개인 정보 보호를 위해 USM을 사용하여 traps 및 informs를 전송합니다. traps 및 informs가 활성화되어 있는 경우 고유한 보안 이름이 필요합니다.

SNMP Trap Event

용어	설명
System	인터페이스 그룹의 트랩을 활성화/비활성화합니다. Warm Start: 웜 스타트 트랩을 활성화/비활성화합니다. Cold Start: 콜드 스타트 트랩을 활성화/비활성화합니다.
Interface	인터페이스 그룹의 트랩을 나타냅니다. (SNMP 개체가 인증 실패 트랩을 생성할 수 있는 것을 나타냅니다.) Link Up: 링크 업 트랩을 활성화/비활성화합니다. Link Down: 링크 다운 트랩을 활성화/비활성화합니다. LLDP: LLDP 트랩을 활성화/비활성화합니다.
Authentication	인증 그룹의 트랩을 나타냅니다. SNMP Authentication Fail: SNMP 트랩 인증 실패 트랩을 활성화/비활성화합니다.
Switch	스위치 그룹의 트랩을 나타냅니다. STP: STP 트랩을 활성화/비활성화합니다. RMON: RMON 트랩을 활성화/비활성화합니다.

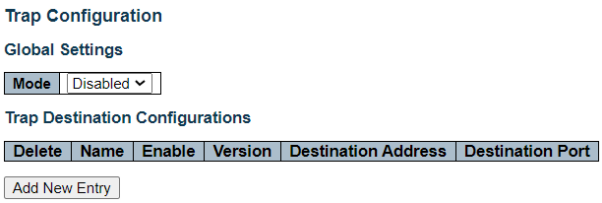
WEB 설정 예시

웹메뉴 Configuration>Security>SNMP>Trap

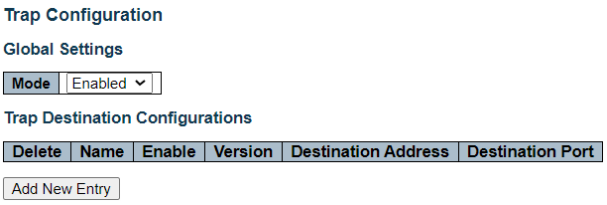
✓ Global Setting

➢ *Mode*

- ***Disable(default)***



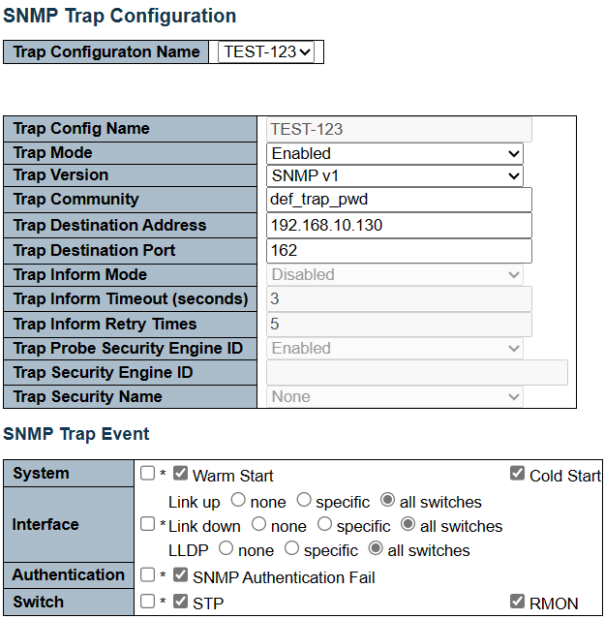
- ***Enable***



✓ Trap Destination Configurations

➢ *Add New Entry*

- ***Use SNMP v1***



Trap Configuration

Global Settings

Mode	Enabled

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port
☐	TEST-123	Enabled	SNMPv1	192.168.10.130	162

- ***Use SNMP v2c***

SNMP Trap Configuration

Trap Configuraton Name	TEST-123

Trap Config Name	TEST-123
Trap Mode	Enabled
Trap Version	SNMP v2c
Trap Community	def_trap_pwd
Trap Destination Address	192.168.10.130
Trap Destination Port	162
Trap Inform Mode	Enabled
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Probe Security Engine ID	Enabled
Trap Security Engine ID	
Trap Security Name	None

SNMP Trap Event

System	☐ * ☑ Warm Start ☑ Cold Start
Interface	Link up ○ none ○ specific ◉ all switches ☐ * Link down ○ none ○ specific ◉ all switches LLDP ○ none ○ specific ◉ all switches
Authentication	☐ * ☑ SNMP Authentication Fail
Switch	☐ * ☑ STP ☑ RMON

Trap Configuration

Global Settings

Mode	Enabled

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port
☐	TEST-123	Enabled	SNMPv2c	192.168.10.130	162

CLI 설정 예시

✓ Global Setting

➢ *Mode*

- ***Disable(default)***

```
(config)# no snmp-server trap
```

- ***Enable***

```
(config)# snmp-server trap
```

✓ Trap Destination Configurations

➢ *Add New Entry*

- ***Use SNMP v1***

(config)# snmp-server host <word32> *(config)# snmp-server host TEST-123* (config-snmps-host)#
(config-snmps-host)# shutdown
(config-snmps-host)# version {v1/v2/v3} <word255> *(config-snmps-host)# version v1 def_trap_pwd*
(config-snmps-host)# host { <v_ipv4_ucast> | <v_word> } [<udp_port>] [traps | informs] *(config-snmps-host)# host 192.168.10.130 162*
(config-snmps-host)# traps [authentication snmp-auth-fail] [system [coldstart] [warmstart]] [switch [stp] [rmon]] *(config-snmps-host)# traps authentication snmp-auth-fail system switch*
(config)# interface (<port_type> [<plist>]) *(config)# interface ** (config-if)# snmp-server host <conf_name> traps [linkup] [linkdown] [lldp] *(config-if)# snmp-server host TEST-123 traps linkup linkdown lldp*

- ***Use SNMP v2***

(config)# snmp-server host <word32> *(config)# snmp-server host TEST-123* (config-snmps-host)#
(config-snmps-host)# shutdown
(config-snmps-host)# version {v1/v2/v3} <word255> *(config-snmps-host)# version v2 def_trap_pwd*
(config-snmps-host)# host { <v_ipv4_ucast> | <v_word> } [<udp_port>] [traps | informs] *(config-snmps-host)# host 192.168.10.130 162 informs*
(config-snmps-host)# traps [authentication snmp-auth-fail] [system [coldstart] [warmstart]] [switch [stp] [rmon]] *(config-snmps-host)# traps authentication snmp-auth-fail system switch*
(config-snmps-host)# informs retries <retries> timeout <timeout> *(config-snmps-host)# informs retries 5 timeout 3(default)*
(config)# interface (<port_type> [<plist>]) *(config)# interface ** (config-if)# snmp-server host <conf_name> traps [linkup] [linkdown] [lldp] *(config-if)# snmp-server host TEST-123 traps linkup linkdown lldp*

6.5.1.8.3. Communities

웹메뉴 Configuration>Security>SNMP>Communities

이 페이지에서 SNMPv3 커뮤니티 테이블을 구성하세요. 항목 인덱스 키는 "Community"입니다.

SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
☐	def_ro_pwd	0.0.0.0	0.0.0.0
☐	def_rw_pwd	0.0.0.0	0.0.0.0

SNMPv3 Community Configuration

용어	설명
Delete	삭제할 항목을 선택하세요. 저장 시 삭제됩니다.
Community	SNMPv3 에이전트에 대한 액세스를 허용하는 커뮤니티 액세스 문자열을 지정합니다. 이 커뮤니티 문자열은 보안 이름으로 처리되며 SNMPv1 또는 SNMPv2c 커뮤니티 문자열에 매핑됩니다. 이 항목은 Groups에 영향을 줍니다.
Source IP	SNMP 액세스 소스 주소를 지정합니다. 소스 마스크와 결합하여 소스 서브넷을 제한하는 데 사용할 수 있는 특정한 범위의 소스 주소입니다.
Source Mask	SNMP 액세스 소스 주소 마스크를 지정합니다.

Buttons

Add New Entry: 새로운 사용자를 추가합니다.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>Security>SNMP>Communities

✓ **SNMPv3 Community Configuration**

➢ ***Add New Entry***

SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
☐	def_ro_pwd	192.168.10.0	255.255.255.0
☐	def_rw_pwd	192.168.10.0	255.255.255.0

CLI 설정 예시

✓ SNMPv3 Community Configuration

➢ *Add New Entry*

```
(config)# snmp-server community v3 <v3_comm> [<v_ipv4_addr> <v_ipv4_netmask>]
(config)# snmp-server community v3 def_ro_pwd 192.168.10.0 255.255.255.0
(config)# snmp-server community v3 def_rw_pwd 192.168.10.0 255.255.255.0
```

6.5.1.8.4. Users

웹메뉴 Configuration>Security>SNMP>Users

이 페이지에서 SNMPv3 사용자 테이블을 구성해주세요. 항목 인덱스 키는 엔진 ID 와 사용자 이름입니다.

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

SNMPv3 User Configuration

용어	설명
Delete	삭제할 항목을 선택하세요. 저장 시 삭제됩니다.
Engine ID	이 항목은 엔진 ID 를 식별하는 옥텟 문자열입니다. 문자열은 16 진수 형식으로 이루어진 짝수 길이여야 하며, 숫자의 자릿수는 10 에서 64 사이여야 합니다. 그러나 모든 0 과 모든 'F'는 허용되지 않습니다. SNMPv3 아키텍처는 메시지 보안을 위해 사용자 기반 보안 모델 (USM)을 사용하고, 액세스 제어를 위해 View 기반 액세스 제어 모델 (VACM)을 사용합니다. USM 항목에서 usmUserEngineID 와 usmUserName 이 항목의 키입니다. 간단한 에이전트에서 usmUserEngineID 는 항상 해당 에이전트의 snmpEngineID 값입니다. 이 값은 또한 이 사용자가 통신할 수 있는 원격 SNMP 엔진의 snmpEngineID 값을 가질 수도 있습니다. 즉, 사용자 엔진 ID 가 시스템 엔진 ID 와 같다면 로컬 사용자이고, 다르다면 원격 사용자입니다.
User Name	이 항목의 이름을 식별하는 문자열입니다. 이 항목은 Groups에 영향을 줍니다. (길이1~32자, 영문 대/소문자, 숫자, 특수문자 사용가능)
Security Level	이 항목의 보안 모델을 나타냅니다. **NoAuth, NoPriv** 인증 및 개인 정보 보호가 없는 모델. **Auth, NoPriv** 인증은 있으나 개인 정보 보호가 없는 모델. **Auth, Priv** 인증과 개인 정보 보호가 있는 모델. 보안 레벨의 값은 이미 항목이 존재하는 경우 수정할 수 없습니다. 따라서 값이 올바르게 설정되었는지 확인되어야 합니다.
Authentication Protocol	이 항목의 인증 프로토콜을 나타냅니다. **None** 인증 프로토콜 없음. **SHA** 사용자가 SHA 인증 프로토콜을 사용하는 것. 보안 레벨의 값은 이미 항목이 존재하는 경우 수정할 수 없습니다. 따라서 값이 올바르게 설정되었는지 먼저 확인해야 합니다.
Authentication Password	인증 암호 구문을 식별하는 문자열입니다. SHA 인증 프로토콜의 경우, 허용되는 문자열 길이는 8에서 40입니다. (영문 대/소문자, 숫자, 특수문자 사용가능)
Privacy Protocol	해당 항목의 개인 정보 보호 프로토콜을 나타냅니다. **None** 개인 정보 보호 프로토콜 없음. **AES** 사용자가 AES 개인 정보 보호 프로토콜을 사용하는 것.

Privacy Password	개인 정보 보호 암호 구문을 식별하는 문자열입니다. (길이8~32자, 영문 대/소문자, 숫자, 특수문자 사용가능)

Buttons

Add New Entry : 새로운 사용자를 추가합니다.

Apply : 클릭 시 변경사항을 적용합니다.

Apply&Save : 클릭 시 변경사항을 적용하고 저장합니다.

Reset : 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>Security>SNMP>Users

✓ **SNMPv3 User Configuration**

➢ ***Add New Entry***

- ***NoAuth, NoPriv***

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☑	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
Delete	800007e5017f000001	TEST-123	NoAuth, NoPriv				

- ***Auth, NoPriv***

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☑	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
Delete	800007e5017f000001	TEST-123	Auth, NoPriv	SHA	••••••••••		

SHA
SHA224
SHA256
SHA384
SHA512

- ***Auth, Priv***

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☑	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
Delete	800007e5017f000001	TEST-123	Auth, Priv	SHA	••••••••••	AES	••••••••••

AES
AES192
AES256

CLI 설정 예시

✓ SNMPv3 User Configuration

➢ *Add New Entry*

- ***NoAuth, NoPriv***

```
(config)# snmp-server user <username> engine-id <engineID>
(config)# snmp user TEST-123 engine-id 800007e5017f000001
```

- ***Auth, NoPriv***

```
(config)# snmp-server user <username> engine-id <engineID> [ { sha | sha224 | sha256 | sha384 | sha512 } <auth_passwd>
(config)# snmp user TEST-123 engine-id 800007e5017f000001 sha **********
```

- ***Auth, Priv***

```
(config)# snmp-server user <username> engine-id <engineID> [ { sha | sha224 | sha256 | sha384 | sha512 } <auth_passwd> [ priv { aes | aes192 | aes256 } <priv_passwd> ] ]
(config)# snmp user TEST-123 engine-id 800007e5017f000001 sha ********** priv aes **********
```

6.5.1.8.5. Groups

웹메뉴 Configuration>Security>SNMP>Groups

SNMPv3 그룹 테이블을 구성합니다. 항목의 인덱스 키는 Security Model과 Security Name입니다.

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
☐	usm	default_user	default_rw_group

SNMPv3 Group Configuration

용어	설명
Delete	삭제할 항목을 선택하세요. 저장 시 삭제됩니다.
Security Model	이 항목의 보안 모델을 선택합니다. **v1** SNMPv1을 선택합니다. **v2c** SNMPv2c를 선택합니다. **usm** User-based Security Model (USM)을 선택합니다.
Security Name	보안 이름을 식별하는 문자열입니다. 이 항목은 Communities, Users의 영향을 받습니다. (길이1~32자, 영문 대/소문자, 숫자, 특수문자 사용가능)
Group Name	그룹을 식별하는 문자열입니다. 이 항목은 Access에 영향을 줍니다. (길이1~32자, 영문 대/소문자, 숫자, 특수문자 사용가능)

Buttons

Add New Entry: 새로운 그룹을 추가합니다.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

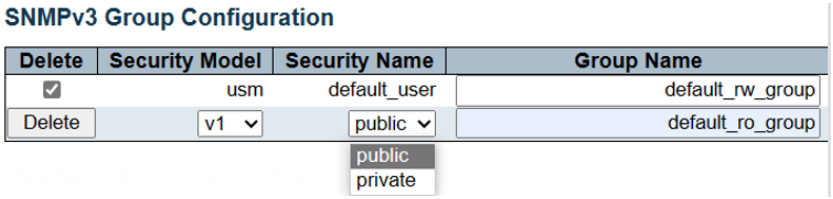
WEB 설정 예시

웹메뉴 Configuration>Security>SNMP>Groups

✓ **SNMPv3 Group Configuration**

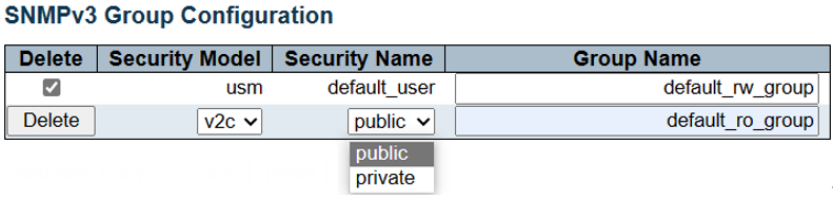
➢ ***Add New Entry***

- ***v1***
  (Security Name은 Communities의 영향을 받습니다.)



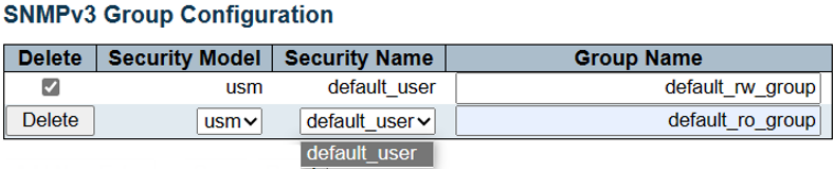
- ***v2c***

  (Security Name은 Communities의 영향을 받습니다.)



- ***usm***

  (Security Name은 Users의 영향을 받습니다.)



CLI 설정 예시

✓ SNMPv3 Group Configuration

➢ *Add New Entry*

- ***v1***

  (Security Name은 Communities의 영향을 받습니다.)

```
(config)# snmp-server security-to-group model { v1 | v2c | v3 } name <security_name>
group <group_name>
(config)# snmp-server security-to-group model v1 name public group default_ro_group
```

- ***v2c***

  (Security Name은 Communities의 영향을 받습니다.)

```
(config)# snmp-server security-to-group model { v1 | v2c | v3 } name <security_name>
group <group_name>
(config)# snmp-server security-to-group model v2c name public group default_ro_group
```

- ***usm***

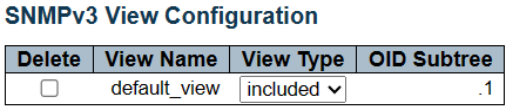
  (Security Name은 Users의 영향을 받습니다.)

```
(config)# snmp-server security-to-group model { v1 | v2c | v3 } name <security_name>
group <group_name>
(config)# snmp-server security-to-group model v3 name default_user group
default_ro_group
```

6.5.1.8.6. Views

웹메뉴 Configuration>Security>SNMP>Views

이 페이지에서 SNMPv3 뷰 테이블을 구성합니다.
항목 인덱스 키는 "뷰 이름(View Name)"과 "OID 서브트리(OID Subtree)"입니다.



SNMPv3 View Configuration

용어	설명
Delete	삭제할 항목을 선택하세요. 저장 시 삭제됩니다.
View Name	이 항목은 속할 뷰의 이름을 식별하는 문자열입니다. 이 항목은 Access 에 영향을 줍니다. (길이 1~32 자, 영문 대/소문자, 숫자, 특수문자 사용가능)
View Type	이 항목은 해당 항목의 뷰 유형을 나타냅니다. **included** 이 뷰 하위 트리가 포함되어야 함을 나타내는 선택. **excluded** 이 뷰 하위 트리가 제외되어야 함을 나타내는 선택. 일반적으로, 뷰 항목의 뷰 유형이 'excluded'인 경우, 뷰 유형이 'included'인 다른 뷰 항목이 있어야 하며, 해당 'excluded' 뷰 항목을 벗어나는 OID 하위 트리를 가져야 합니다.
OID Subtree	지정된 뷰에 추가할 서브트리의 루트를 정의하는 OID입니다. (길이1~128자, 숫자, 별표(*) 사용가능)

Buttons

Add New Entry: 새로운 View를 추가합니다.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

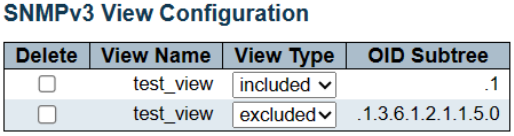
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

✓ **SNMPv3 Group Configuration**

➢ ***Add New Entry***

- ***test_view(excluded SysName)***



CLI 설정 예시

✓ SNMPv3 Group Configuration

➢ *Add New Entry*

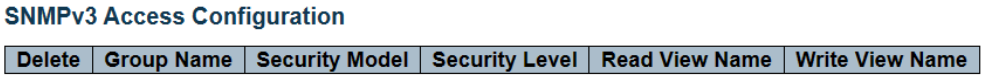
- ***test_view(excluded SysName)***

```
(config)# snmp-server view <view_name> <oid_subtree> { include | exclude }
(config)# snmp-server view test_view .1 include
(config)# snmp-server view test_view .1.3.6.1.2.1.1.5.0 exclude
```

6.5.1.8.7. Access

웹메뉴 Configuration>Security>SNMP>Views

이 페이지에서 SNMPv3 액세스 테이블을 구성합니다. 항목 인덱스 키는 "그룹 이름(Group Name)", "보안 모델(Security Model)", 그리고 "보안 레벨(Security Level)"입니다.



SNMPv3 Access Configuration

용어	설명
Delete	삭제할 항목을 선택하세요. 저장 시 삭제됩니다.
Group Name	이 항목은 해당 항목의 그룹을 식별하는 문자열입니다. 이 항목은 Groups 의 영향을 받습니다. (길이 1~32 자, 영문 대/소문자, 숫자, 특수문자 사용가능)
Security Model	이 항목은 해당 항목의 보안 모델을 나타냅니다. **any** 모든 보안 모델을 혀용pri(v1|v2c|usm). **v1** SNMPv1을 허용. **v2** SNMPv2c을 허용. **usm** User-based Security Model (USM)을 허용.
Security Level	이 항목은 해당 항목의 보안 모델을 나타냅니다. **NoAuth, NoPriv** No authentication and no privacy. **Auth, NoPriv** Authentication and no privacy. **Auth, Priv** Authentication and privacy.
Read View Name	현재 값을 요청할 수 있는 MIB 개체를 정의하는 MIB 뷰의 이름입니다. 이 항목은 Views의 영향을 받습니다. (길이1~32자, 영문 대/소문자, 숫자, 특수문자 사용가능)
Write View Name	새로운 값을 설정할 수 있는 MIB 개체를 정의하는 MIB 뷰의 이름입니다. 이 항목은 Views의 영향을 받습니다. (길이1~32자, 영문 대/소문자, 숫자, 특수문자 사용가능)

Buttons

Add New Entry: 새로운 SNMP 접근을 추가합니다.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

✓ **SNMPv3 Access Configuration**

➢ ***Add New Entry***

- ***default_rw_group(test_view)***

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
☐	default_rw_group	any	Auth, Priv	test_view	test_view

CLI 설정 예시

✓ **SNMPv3 Access Configuration**

➢ ***Add New Entry***

- ***default_rw_group(test_view)***

```
(config)# snmp-server access <group_name> model { v1 | v2c | v3 | any } level { auth | noauth | priv } [ read <view_name> ] [ write <write_name> ]
(config)# snmp-server access default_rw_group model any level priv read test_view write test_view
```

6.5.2. Network Configuration

6.5.2.1. Limit Control

웹메뉴 Configuration>Security>Network>Limit Control

이 페이지를 통해 Port Security Limit Control 시스템과 포트 설정을 구성할 수 있습니다.

시스템별로 포트 보안 제한 에이징을 구성할 수 있습니다.

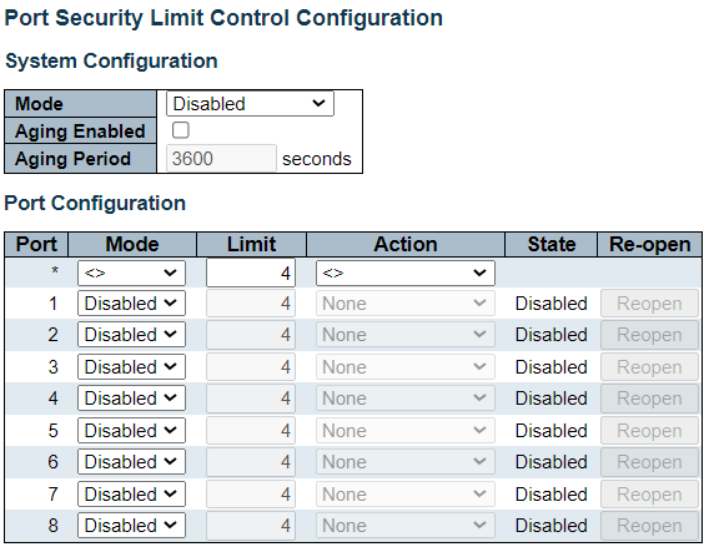
Limit Control 은 특정 포트에서 사용자 수를 제한하는 기능입니다.
사용자는 MAC 주소와 VLAN ID 로 식별됩니다.
포트에서 Limit Control 이 활성화되면, 제한은 포트에 허용되는 최대 사용자 수를 지정합니다.
이 수를 초과하면 특정 동작이 수행됩니다. 동작은 아래 설명된 네 가지 중 하나일 수 있습니다.

• None, Trap, Shutdown, Trap and Shutdown

스위치는 포트 보안이 활성화된 포트에서 새 MAC 주소가 표시될 때 모든 포트가 가져오는 총 MAC 주소 수로 구성됩니다. 모든 포트는 동일한 풀에서 가져오기 때문에 나머지 포트가 이미 사용 가능한 모든 MAC 주소를 사용한 경우 구성된 최대값을 부여할 수 없는 경우가 발생할 수 있습니다.

Limit Control 모듈은 포트에서 학습된 MAC 주소를 관리하는 하위 모듈인 Port Security 모듈을 활용합니다.

Limit Control 구성은 시스템 전체와 포트 전용 두 개의 섹션으로 구성됩니다.



Port Security Limit Control Configuration

System Configuration

용어	설명
Mode	스위치 전체에서 Limit Control 이 활성화되어 있는지 아닌지를 나타냅니다. 전역으로 비활성화된 경우, 제한 확인 및 해당 동작은 비활성화됩니다.
Aging Enabled	체크된 경우, 보안된 MAC 주소는 Aging 기간에 따라 소멸됩니다.
Aging Period	Aging Enabled가 체크되어 있는 경우, 이 입력란을 사용하여 Aging 기간을 제어합니다. 다른 모듈이 MAC 주소를 보호하기 위해 기본 포트 보안을 사용하는 경우, 기능을 사용하는 모든 모듈 중에서 가장 짧은 Aging 기간이 기본 포트 보안에 사용됩니다. (Aging 기간은 10부터 9,999,999까지의 숫자로 설정할 수 있습니다.)

System Configuration

용어	설명
Port	구성이 적용되는 포트 번호입니다.
Mode	이 포트에서 Limit Control이 활성화되어 있는지를 제어합니다. 이 설정과 전역 모드 모두가 활성화되어야 Limit Control이 적용됩니다. 주의해야 할 점은 다른 모듈이 특정 포트에서 Limit Control을 활성화하지 않고도 기본 포트 보안 기능을 사용할 수 있다는 것입니다.
Limit	이 포트에서 보안할 수 있는 최대 MAC 주소 수입니다. 이 수는 1024를 초과할 수 없습니다. 제한을 초과하면 해당하는 동작이 수행됩니다. 스위치는 MAC 주소의 총 수를 가지고 있으며, 모든 포트가 동일한 풀에서 주소를 할당 받기 때문에, 이미 사용 가능한 모든 MAC 주소를 사용한 경우 설정된 최대치를 제공할 수 없을 수 있습니다.
Action	MAC 주소 제한에 도달하면, 스위치는 하나의 동작을 취할 수 있습니다: **None** 해당 포트에서 제한 이상의 MAC 주소를 허용하지 않으며, 추가적인 동작을 취하지 않습니다. **Trap** 해당 포트에서 Limit + 1개의 MAC 주소가 감지되면 SNMP 트랩을 전송합니다. Aging이 비활성 경우, 한 번의 SNMP 트랩만 전송 Aging이 활성화된 경우, 제한을 초과할 때마다 새로운 SNMP 트랩이 전송됩니다. **Shutdown** 해당 포트에서 Limit + 1개의 MAC 주소가 감지되면 포트를 종료합니다. 이로 인해 보안된 모든 MAC 주소가 포트에서 제거되고, 새로운 주소는 학습되지 않습니다. 심지어 포트의 링크가 물리적으로 연결해제, 재결합하더라도, 포트는 종료된 상태로 유지됩니다. 포트를 다시 열려면 세 가지 방법이 있습니다: 1) 스위치를 재부팅합니다. 2) 포트나 스위치에서 Limit Control을 비활성화한 다음 다시 활성화합니다. 3) "Reopen" 버튼을 클릭합니다. **Trap&Shutdown** 해당 포트에서 Limit + 1개의 MAC 주소가 감지되면 위에서 설명한 "Trap" 및 "Shutdown" 동작이 모두 수행됩니다.
State	이 열은 Limit Control의 관점에서 본 현재 포트의 상태를 보여줍니다. 상태는 다음 네 가지 값 중 하나를 가질 수 있습니다:

	Disabled	Limit Control이 Global에서 비활성화되었거나 해당 포트에서 비활성화되었습니다.
	Ready	제한에 도달하지 않았음을 나타냅니다. 모든 Action에 대해 표시될 수 있습니다.
	Limit Reached	해당 포트에서 제한에 도달했음을 나타냅니다. 이 상태는 Action이 None 또는 Trap으로 설정된 경우에만 표시될 수 있습니다.
	Shutdown	Limit Control에 의해 포트가 종료되었음을 나타냅니다. 이 상태는 Action이 Shutdown 또는 Trap & Shutdown으로 설정된 경우에만 표시될 수 있습니다.
Re-open Button	이 모듈에 의해 포트가 종료된 경우, 해당 포트를 다시 열기 위해 이 버튼을 클릭할 수 있습니다. 다시 열기 버튼을 클릭하면 페이지가 새로 고쳐지므로, 아직 적용되지 않은 변경 사항은 손실될 수 있습니다.	

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

Refresh: 클릭 시 페이지를 새로 고침.

WEB 설정 예시

✓ System Configuration

➢ *Mode*

- ***Disabled***

System Configuration

Mode	Disabled
Aging Enabled	☐
Aging Period	3600 seconds

- ***Enabled***

System Configuration

Mode	Enabled
Aging Enabled	☐
Aging Period	3600 seconds

➢ *Aging Enable*

- ***Disabled***

System Configuration

Mode	Enabled
Aging Enabled	☐
Aging Period	3600 seconds

- ***Enabled***

System Configuration

Mode	Enabled
Aging Enabled	☑
Aging Period	3600 seconds

➢ ***Aging Period***
(10 ~ 9,999,999 seconds)

System Configuration

Mode	Enabled
Aging Enabled	☑
Aging Period	9999999 seconds

✓ Port Configuration

➢ ***Mode***

- ***Disabled***

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<>	4	<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen

- ***Enabled***

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<>	4	<>		
1	Enabled	4	None	Ready	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen

➢ ***Limit (1 ~ 1024 MAC address)***

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<>	1024	<>		
1	Enabled	1024	None	Ready	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen

➢ ***Action***

- ***None | Trap | Shutdown | Trap&Shutdown***

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<>	1024	<>		
1	Enabled	1024	Shutdown	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	Trap	Disabled	Reopen
4	Disabled	4	Shutdown	Disabled	Reopen
5	Disabled	4	Trap & Shutdown	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen

CLI 설정 예시

✓ **System Configuration**

➢ ***Mode***

- ***Disabled***

```
(config)# no port-security
```

- ***Enabled***

```
(config)# port-security
```

➢ ***Aging Enable***

- ***Disabled***

```
(config)# no port-security aging
```

- ***Enabled***

```
(config)# port-security aging
```

- ***Aging Period***

(10 ~ 9,999,999 seconds)

```
(config)# port-security aging time <v_10_to_9999999>
(config)# port-security aging time 9999999
```

✓ Port Configuration

➢ *Mode*

- ***Disabled***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# no port-security
```

- ***Enabled***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# port-security
```

➢ *Limit (1 ~ 1024 MAC address)*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# port-security maximum [ <v_1_to_1024> ]
(config-if)# port-security maximum 1024
```

➢ *Action*

- ***None | Trap | Shutdown | Trap&Shutdown***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# port-security violation { protect | trap | trap-shutdown | shutdown }
(config-if)# port-security violation protect
(config-if)# port-security violation trap
(config-if)# port-security violation shutdown
(config-if)# port-security violation trap-shutdown
```

6.5.2.2. ACL

ACL은 프로세스나 프로그램과 같은 특정 트래픽 개체에 대한 액세스가 허용된 개별 사용자 또는 그룹을 지정하는 액세스 제어 항목을 포함하는 ACE 테이블로 구성됩니다. ACE 매개변수는 선택한 프레임 유형에 따라 다릅니다.

액세스 가능한 각 트래픽 개체에는 해당 ACL에 대한 식별자가 포함되어 있습니다. 권한은 특정 트래픽 개체 액세스 권한이 있는지 여부를 결정합니다.

ACL 구현은 예를 들어 다양한 상황에 대해 ACE의 우선 순위가 지정되는 경우 매우 복잡할 수 있습니다. 네트워킹에서 ACL은 호스트 또는 서버에서 사용할 수 있는 서비스 포트 또는 네트워크 서비스 목록을 나타내며, 각 서비스에는 서비스 사용이 허용된 호스트 또는 서버 목록이 있습니다. ACL은 일반적으로 인바운드 트래픽을 제어하도록 구성할 수 있으며 이러한 맥락에서 ACL은 방화벽과 유사합니다.

수동 ACL 구성과 관련된 세 가지 구성 가능한 섹션이 있습니다.

ACL 구성은 가장 높은(상단)에서 가장 낮은(하단) 순으로 우선 순위가 지정된 방식으로 ACE를 표시합니다. 수신 프레임은 일치하는 ACE가 더 많더라도 하나의 ACE에서만 적중됩니다. 일치하는 첫 번째 ACE는 해당 프레임에서 조치(허용/거부)를 수행하고 해당 ACE와 연결된 카운터가 증가합니다. ACE는 수신 포트와 정책(값/마스크 쌍)의 모든 조합과 연결할 수 있습니다. ACE 정책이 생성되면 해당 정책은 ACL 포트 구성의 일부로 포트 그룹과 연결될 수 있습니다. ACE로 구성할 수 있는 여러 매개변수가 있습니다.

ACL 포트 구성은 수신 포트에 정책 ID를 할당하는 데 사용됩니다. 이는 동일한 트래픽 규칙을 따르도록 포트를 그룹화하는 데 유용합니다. 트래픽 정책은 ACL 구성에서 생성됩니다. 각 수신 포트에 대해 다음 트래픽 속성을 설정할 수 있습니다.

- 행동(Action)
- 속도 제한기(Rate Limiter)
- 포트 리디렉션(Port Redirection)
- 미러(Mirror)
- 로깅(Logging)
- 종료(Termination)

관리 인터페이스는 포트에서 포워딩이 허용되는지(Permit) 또는 거부되는지(Deny)를 결정하는 데 사용되는 포트 작업을 허용합니다. 기본 작업은 허용입니다.

ACE는 프레임이 일치하지 않고 ACE 일치를 통과하는 경우에만 적용됩니다. 이 경우 해당 포트와 관련된 카운터가 증가합니다. 16개의 서로 다른 ACL 속도 제한기가 있을 수 있습니다. 속도 제한기 ID는 ACE(들) 또는 수신 포트(들)에 할당될 수 있습니다.

ACE는 여러 매개변수로 구성됩니다. 이러한 매개변수는 선택한 프레임 유형에 따라 다릅니다. 수신 포트는 ACE에 대해 선택한 다음 프레임 유형을 선택해야 합니다. 선택한 프레임 유형에 따라 다른 매개변수 옵션이 표시됩니다. 지원되는 프레임 유형은 다음과 같습니다.

• Any

• 구성 가능한 이더넷 유형

•ARP

•IPv4

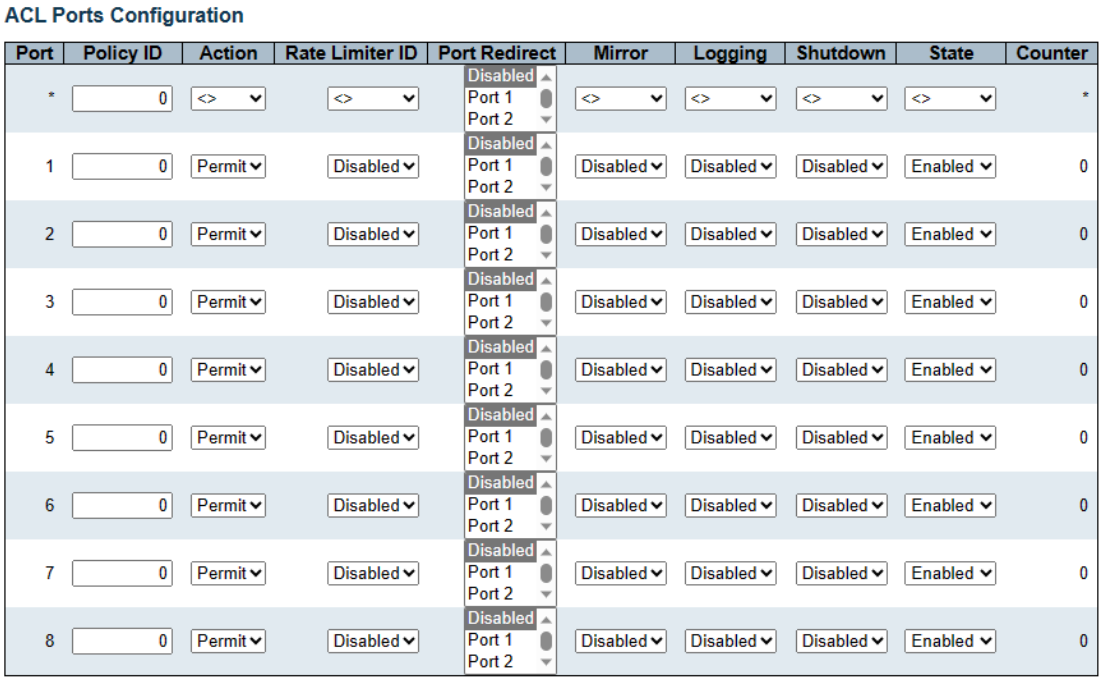
•IPv6

MAC 기반 필터링 및 IP 프로토콜 기반 필터링은 적절한 프레임 유형 선택에 따른 구성으로 달성할 수 있습니다.

6.5.2.2.1. Ports

웹메뉴 Configuration>Security>Network>ACL>Ports

각 스위치 포트의 ACL 매개변수(ACE)를 구성합니다.
이 매개변수는 프레임이 특정 ACE 와 일치하지 않는 한 포트에서 수신된 프레임에 영향을 미칩니다.



ACL Ports Configuration

용어	설명
Port	동일한 행에 포함된 설정에 대한 논리적인 포트입니다.
Policy ID	이 포트에 적용할 정책을 선택합니다. 허용되는 값은 0 부터 255 까지입니다. 기본값은 0 입니다.
Action	전달이 허용되는지 ("Permit") 아니면 거부되는지 ("Deny") 선택합니다. 기본값은 "Permit"입니다.
Rate Limiter ID	이 포트에 적용할 속도 제한기를 선택합니다. 허용되는 값은 "Disabled" 또는 1에서 16까지의 값입니다. 기본값은 "Disabled"입니다.

Port Redirect	프레임이 리디렉션되는 포트를 선택합니다. 허용되는 값은 "Disabled" 또는 특정 포트 번호이며, 기본값은 "Disabled"입니다. (Action 항목의 값이 Permit인 경우 설정이 불가합니다.)
Mirror	이 포트의 Mirroring 작업을 지정합니다. Enabled: 포트에서 수신된 프레임이 Mirroring됩니다. Disabled: 포트에서 수신된 프레임이 Mirroring되지 않습니다. 기본값은 "Disabled"입니다.
Logging	이 포트의 로깅 작업을 지정합니다. 로깅 메시지에는 4바이트 CRC가 포함되지 않습니다. Enabled: 포트에서 수신된 프레임이 시스템 로그에 저장됩니다. Disabled: 포트에서 수신된 프레임이 시스템 로그에 저장되지 않습니다. 기본값은 "Disabled"입니다. 참고: 로깅 기능은 패킷 길이가 1518보다 작을 때(무 VLAN 태그)와 시스템 로그 메모리 크기 및 로깅 속도가 제한되는 경우에만 작동합니다.
Shutdown	이 포트의 포트 종료 동작을 지정합니다. Enabled: 포트에서 프레임을 수신하면 포트가 비활성화됩니다. Disabled: 포트 종료가 비활성화됩니다. 기본값은 "Disabled"입니다. 참고: 포트 종료 기능은 패킷 길이가 1518보다 작을 때(IEEE 802.3 이외의 VLAN 태그 없이)만 작동합니다.
State	이 포트의 포트 상태를 지정합니다. Enabled: ACL 사용자 모듈의 포트 설정을 변경하여 포트를 엽니다. Disabled: ACL 사용자 모듈의 포트 설정을 변경하여 포트를 닫습니다. 기본값은 "Enabled"입니다.
Counter	ACE와 일치하는 프레임의 수를 표시합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

Refresh: 클릭 시 페이지를 새로 고침.

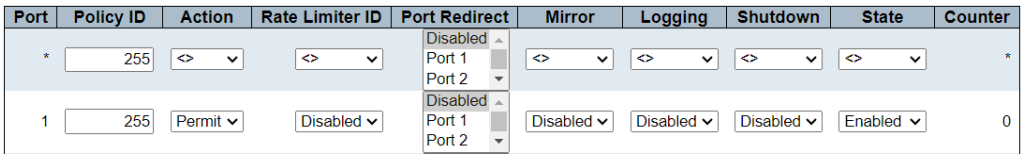
Clear: 클릭 시 카운터 선택을 취소합니다.

WEB 설정 예시

✓ **ACL Ports Configuration**

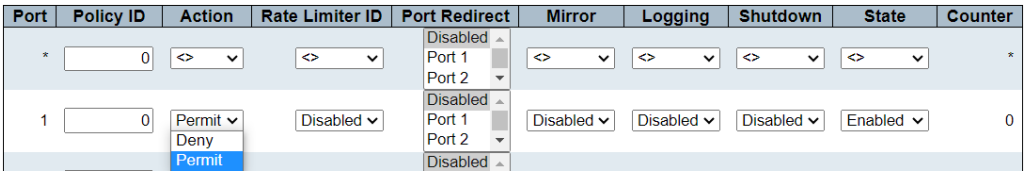
➢ ***Policy ID***

- ***0~255(default 0)***



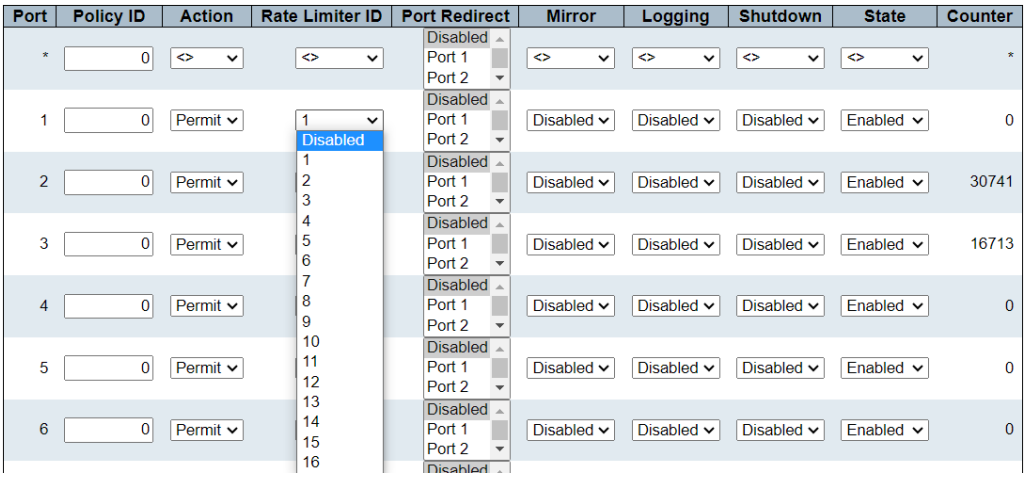
➢ ***Action***

- ***Permit(default) | Deny***



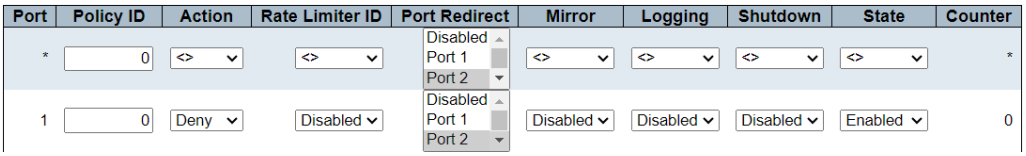
➢ ***Rate Limiter ID***

- ***Disabled | 1~16***



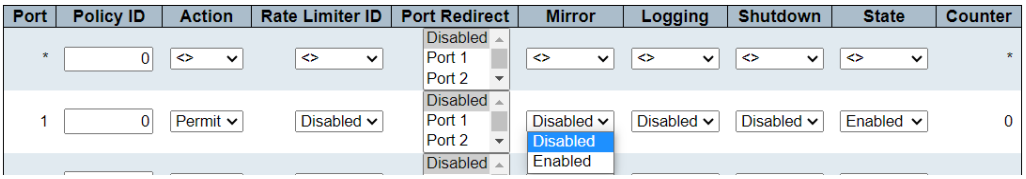
➢ ***Port Redirect (Need Action Deny)***

- ***Disabled(default) | Port Number***



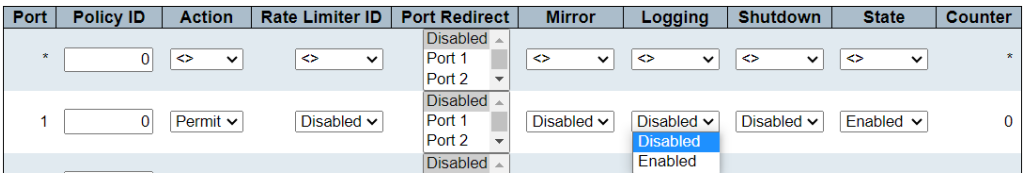
➢ ***Mirror***

- ***Disabled(default) | Enabled***



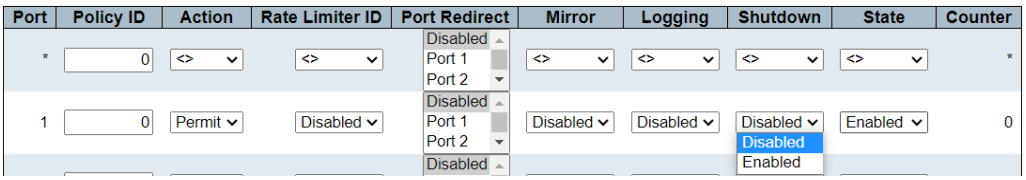
➢ ***Logging***

- ***Disabled(default) | Enabled***



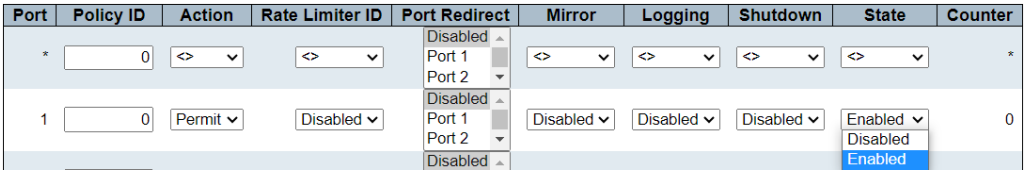
➢ ***Shutdown***

- ***Disabled(default) | Enabled***



➢ ***State***

- ***Enabled(default) | Disabled***



CLI 설정 예시

✓ **ACL Ports Configuration**

➢ ***Policy ID***

- ***0~255(default 0)***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# access-list policy <policy_id>
(config-if)# access-list policy 255
```

➢ ***Action***

- ***Permit(default) | Deny***

```
(config-if)# access-list action { permit | deny }
(config-if)# access-list action deny
```

➢ ***Rate Limiter ID***

- ***Disabled(default) | 1~16***

```
(config-if)# no access-list rate-limiter
```

(config-if)# access-list rate-limiter <rate_limiter_id> *(config-if)# access-list rate-limiter 16* <rate_limiter_id> = <1-16>

➢ ***Port Redirect (Need Action Deny)***

- ***Disabled(default) | Port Number***

(config-if)# no access-list redirect
(config-if)# access-list redirect interface { <port_type> <port_type_id> | (<port_type> [<port_type_list>]) } *(config-if)# access-list redirect interface GigabitEthernet 1/4*

➢ ***Mirror***

- ***Disabled(default) | Enabled***

(config-if)# no access-list mirror
(config-if)# access-list mirror

➢ ***Logging***

- ***Disabled(default) | Enabled***

(config-if)# no access-list logging
(config-if)# access-list logging

➢ ***Shutdown***

- ***Disabled(default) | Enabled***

(config-if)# no access-list shutdown
(config-if)# access-list shutdown

➢ ***State***

- ***Enabled(default) | Disabled***

(config-if)# access-list port-state
(config-if)# no access-list port-state

6.5.2.2.2. Rate Limiters

웹메뉴 Configuration>Security>Network>ACL>Rate Limiters

스위치에 ACL 의 Rate Limiters 구성을 합니다.

ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	10	<>
1	10	pps
2	10	pps
3	10	pps
4	10	pps
5	10	pps
6	10	pps
7	10	pps
8	10	pps
9	10	pps
10	10	pps
11	10	pps
12	10	pps
13	10	pps
14	10	pps
15	10	pps
16	10	pps

ACL Ports Configuration

용어	설명
Rate Limiter ID	동일한 행에 포함된 설정 레이트 리미터 ID 입니다. 1 부터 16 까지의 범위를 가집니다.
Rate	유용한 대역폭은 초당패킷수(pps)의 경우 0 ~ 5,000,000 킬로비트/초(kbps)의 경우 0 ~ 10,000,000 입니다.
Unit	레이트 단위를 지정하세요.(pps: 초당 패킷 수, kbps: 초당 킬로비트 수.)

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

✓ **ACL Rate Limiter Configuration**

➢ ***Rate***

- ***0 ~ 5,000,000pps or 0 ~ 10,000,000kbps***

ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	5000000	<>
1	5000000	pps
2	10000000	kbps
3	10	pps
4	10	pps
5	10	pps
6	10	pps
7	10	pps
8	10	pps
9	10	pps
10	10	pps
11	10	pps
12	10	pps
13	10	pps
14	10	pps
15	10	pps
16	10	pps

CLI 설정 예시

✓ ACL Rate Limiter Configuration

➢ *Rate*

- ***0 ~ 5,000,000pps or 0 ~ 10,000,000kbps***

```
(config)# access-list rate-limiter [ <rate_limiter_list> ] { 10pps <pps10_rate> | 25kbps <kpbs25_rate> }
(config)# access-list rate-limiter <1-16> 10pps <0-500000>
(config)# access-list rate-limiter 1 10pps 500000
```

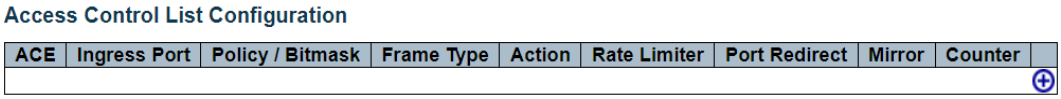
```
(config)# access-list rate-limiter [ <rate_limiter_list> ] { 10pps <pps10_rate> | 25kbps <kpbs25_rate> }
(config)# access-list rate-limiter <1-16> 25kbps <0-400000>
(config)# access-list rate-limiter 2 25kbps 400000
```

6.5.2.2.3. Access Control List Configuration

웹메뉴 Configuration>Security>Network>ACL>Access Control List

이 페이지는 이 스위치에서 정의된 ACE(Access Control Entry)로 구성된 접근 제어 목록(ACL)을 보여줍니다. 각 행은 정의된 ACE를 설명합니다. 각 스위치마다 최대 512개의 ACE를 가질 수 있습니다.

리스트에 새로운 ACE를 추가하려면 가장 아래에 있는 플러스(+) 기호를 클릭하세요. 내부 프로토콜에 사용되는 예약된 ACE는 편집하거나 삭제할 수 없으며, 순서를 변경할 수도 없으며, 우선순위가 가장 높습니다.



Access Control List Configuration

용어	설명
ACE	ACE 의 ID 를 나타냅니다.
Ingress Port	ACE 의 인그레스 포트를 나타냅니다. All: ACE 를 모든 인그레스 포트에 적용합니다. Port: ACE 를 특정 인그레스 포트에 적용합니다.
Policy / Bitmask	ACE의 정책 번호와 비트마스크를 나타냅니다.
Frame Type	ACE의 프레임 유형을 나타냅니다. **Any** ACE는 모든 프레임 유형입니다. **EType** ACE는 이더넷 유형 프레임입니다. **ARP** ACE는 ARP/RARP 프레임입니다. **IPv4** ACE는 모든 IPv4 프레임입니다. **IPv4/ICMP** ACE는 ICMP 프로토콜을 사용하는 IPv4 프레임입니다. **IPv4/UDP** ACE는 UDP 프로토콜을 사용하는 IPv4 프레임입니다. **IPv4/TCP** ACE는 TCP 프로토콜을 사용하는 IPv4 프레임입니다. **IPv4/Other** ACE는 ICMP/UDP/TCP가 아닌 IPv4 프레임입니다. **IPv6** ACE는 모든 IPv6 표준 프레임입니다.
Action	ACE의 전달 동작을 나타냅니다. **Permit** ACE와 일치하는 프레임은 전달하고 학습될 수 있습니다. **Deny** ACE와 일치하는 프레임은 버립니다. **Filter** ACE와 일치하는 프레임은 필터링 됩니다.
Rate Limiter	ACE의 레이트 리미터 번호를 나타냅니다. 허용되는 범위는 1에서 16입니다. "Disabled"로 표시되면 레이트 리미터 기능이 비활성화됩니다.
Port Redirect	ACE의 포트 리다이렉트 동작을 나타냅니다. ACE와 일치하는 프레임은 해당 포트 번호로 리다이렉트됩니다. 허용되는 값은 "Disabled" 또는 특정 포트 번호입니다. "Disabled"로 표시되면 포트 리다이렉트 동작이 비활성화됩니다.
Mirror	이 포트의 미러 동작을 지정합니다. ACE와 일치하는 프레임은 대상 미러 포트로 미러링됩니다. Enabled: 포트에서 수신된 프레임이 미러링됩니다. Disabled: 포트에서 수신된 프레임이 미러링되지 않습니다.

Counter	ACE와 프레임이 매칭된 횟수를 나타냅니다.
Modification Buttons	다음 버튼을 사용하여 테이블의 각 ACE를 수정할 수 있습니다: 현재 행 앞에 새로운 ACE를 삽입합니다. ACE 행을 편집합니다. ACE를 목록에서 위로 이동합니다. (우선순위 상향) ACE를 목록에서 아래로 이동합니다. (우선순위 하향) ACE를 삭제합니다. 가장 아래쪽(+) 기호는 ACE 목록의 가장 아래에 새 항목을 추가합니다.(가장 낮은 우선순위)

Buttons

Auto-refresh : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh: 클릭 시 페이지를 새로 고침.

Clear: 클릭 시 카운터 선택을 취소합니다.

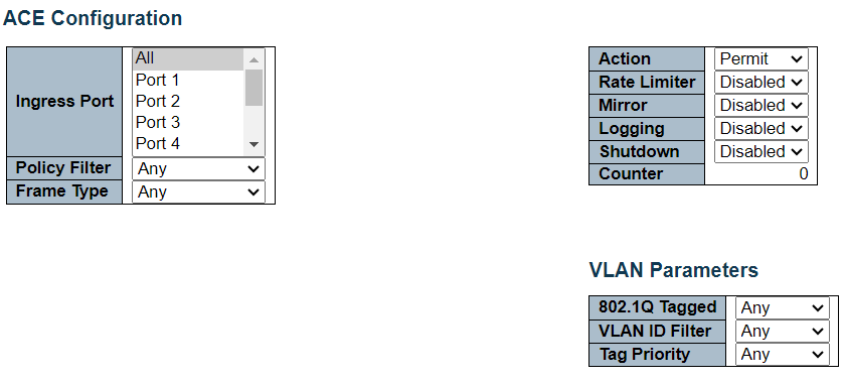
Remove All: 모든 ACE를 제거합니다.

ACE Configuration

이 페이지에서 ACE(접근 제어 항목)를 구성하세요.

ACE는 여러 매개변수로 구성됩니다. 이 매개변수는 선택한 프레임 유형에 따라 다릅니다. 먼저 ACE에 대한 인그레스 포트를 선택한 다음 프레임 유형을 선택하세요. 선택한 프레임 유형에 따라 다른 매개변수 옵션이 표시됩니다.

이 ACE와 일치하는 프레임은 여기에서 정의된 구성과 일치합니다.



ACE Configuration

용어	설명
Ingress Port	이 ACE 가 적용되는 인그레스 포트를 선택하세요. All: ACE 는 모든 포트에 적용됩니다. Port n: ACE 는 해당 포트 번호에 적용됩니다.
Policy Filter	이 ACE 에 대한 정책 번호 필터를 지정하세요. Any: 정책 필터가 지정되지 않았습니다. Specific: 이 ACE 로 특정 정책을 필터링하려면 이 값을 선택하세요. 정책 값과 비트마스크를 입력하는 두 개의 필드가 나타납니다.

Policy Value	정책 필터에 "Specific"이 선택된 경우, 특정 정책 값을 입력할 수 있습니다. 허용되는 범위는 0에서 255입니다.
Policy Bitmask	정책 필터에 "Specific"이 선택된 경우, 특정 정책 비트마스크를 입력할 수 있습니다. 허용되는 범위는 0x0에서 0xff입니다.
Frame Type	이 ACE에 대해 프레임 유형을 선택하세요. **Any** 어떤 프레임이든 ACE와 일치할 수 있습니다. **Ethernet Type** 이더넷 유형 프레임만 ACE와 일치할 수 있습니다. IEEE 802.3에서는 길이/유형 필드의 값이 1536 이상(16진수로 0600이상)이어야 하며, 값이 0x800(IPv4), 0x806(ARP), 0x86DD(IPv6)와 같지 않아야 합니다. **ARP** ARP 프레임만 ACE와 일치할 수 있습니다. (0x806) **IPv4** IPv4 프레임만 ACE와 일치할 수 있습니다. (0x800) **IPv6** IPv6 프레임만 ACE와 일치할 수 있습니다. (0x86DD)
Action	ACE에 일치하는 프레임에 대해 수행할 작업을 지정합니다. **Permit** ACE에 일치하는 프레임은 작업을 허용합니다. **Deny** ACE에 일치하는 프레임은 폐기됩니다. **Filter** ACE에 일치하는 프레임은 필터링됩니다.
Rate Limiter	기본 단위로 된 Rate Limiter를 지정합니다. 허용되는 범위는 1부터 16까지입니다. Disabled는 Rate Limiter 작동이 비활성화됩니다.
Port Redirect	ACE에 일치하는 프레임은 여기에 지정된 포트 번호로 리다이렉트됩니다. Rate limiter는 포트에 영향을 미칩니다. 허용되는 범위는 스위치 포트 번호 범위와 동일합니다. Disabled는 포트 리다이렉트 작업이 비활성화되었음을 나타내며, 동작이 허용될 때 '포트 리다이렉트'의 특정 포트 번호를 설정할 수 없습니다.
Mirror	이 포트의 미러 동작을 지정합니다. ACE와 일치하는 프레임은 대상 미러 포트로 미러링됩니다. Rate limiter는 미러 포트의 프레임에 영향을 주지 않습니다. Enabled: 포트에서 수신된 프레임은 미러링됩니다. Disabled: 포트에서 수신된 프레임은 미러링되지 않습니다.
Logging	ACE의 로깅 동작을 지정합니다. Enabled: ACE와 일치하는 프레임이 시스템 로그에 저장됩니다. Disabled: ACE와 일치하는 프레임이 로깅되지 않습니다. 참고: 로깅 기능은 패킷 길이가 1518 미만이고(VLAN 태그 없음) 시스템 로그 메모리 크기와 로깅 속도가 제한된 경우에만 작동합니다.
Shutdown	ACE의 포트 종료 동작을 지정합니다. Enabled: ACE와 일치하는 프레임이 있을 경우, 인그레스 포트가 비활성화됩니다. Disabled: ACE의 포트 종료 기능이 비활성화됩니다. 참고: 종료 기능은 패킷 길이가 1518 미만이고(VLAN 태그 없음)인 경우에만 작동합니다.
Counter	ACE와 프레임이 매칭된 횟수를 나타냅니다.
MAC Parameters	ACE의 MAC관련 설정을 합니다. (이 프레임 유형이 이더넷 유형 또는 ARP일 때만 표시됩니다.)
SMAC Filter	이 ACE에 대한 소스 MAC 필터를 지정합니다. Any: SMAC 필터가 지정되지 않았습니다. Specific: 이 ACE로 특정 소스 MAC 주소를 필터링하려면이 값을 선택하십시오.
SMAC Value	SMAC 필터에서 "Specific"을 선택하면 특정 소스 MAC 주소를 입력할 수

	있습니다. 유효한 형식은 "xx-xx-xx-xx-xx-xx" 또는 "xx.xx.xx.xx.xx.xx" 또는 "xxxxxxxxxxxx"입니다 (x는 16진수 숫자입니다). 이 ACE에 맞는 프레임은 이 SMAC값을 가집니다.
DMAC Filter	이 ACE에 대한 목적지 MAC 필터를 지정합니다. **Any** DMAC 필터가 지정되지 않았습니다. **MC** 프레임은 멀티캐스트여야 합니다. **BC** 프레임은 브로드캐스트여야 합니다. **UC** 프레임은 유니캐스트여야 합니다. **Specific** 이 ACE로 특정 목적지 MAC 주소를 필터링하려면 이 값을 선택하십시오.
DMAC Value	DMAC 필터의 경우 "Specific"을 선택하면 특정 목적지 MAC 주소를 입력할 수 있습니다. 유효한 형식은 "xx-xx-xx-xx-xx-xx" 또는 "xx.xx.xx.xx.xx.xx" 또는 "xxxxxxxxxxxx"입니다 (x는 16진수 숫자입니다). 이 ACE에 맞는 프레임은 이 DMAC 값을 가집니다.
VLAN Parameters	ACE의 VLAN관련 설정을 합니다.
802.1Q Tagged	802.1Q 태그에 따라 프레임이 액션에 영향을 줄 수 있는지 지정합니다. **Any** 어떤 값이든 허용됩니다 . **Enabled** 태그된 프레임만 허용됩니다. **Disabled** 태그되지 않은 프레임만 허용됩니다.
VLAN ID Filter	이 ACE에 대한 VLAN ID 필터를 지정합니다. **Any** VLAN ID 필터가 지정되지 않습니다. **Specific** 이 ACE로 특정 VLAN ID를 필터링하려면 이 값을 선택하십시오.
VLAN ID	VLAN ID 필터를 "Specific"으로 선택하면 특정 VLAN ID 번호를 입력할 수 있습니다. 허용되는 범위는 1부터 4095까지입니다. 이 ACE와 일치하는 프레임은 이 VLAN ID 값을 가집니다.
Tag Priority	이 ACE에 대한 태그 우선순위를 지정합니다. 이 ACE에 맞는 프레임은 이 태그 우선순위와 일치합니다. 허용되는 숫자 범위는 0부터 7까지이거나 0-1, 2-3, 4-5, 6-7, 0-3, 4-7의 범위입니다. 값 "Any"는 태그 우선순위가 지정되지 않았음을 의미합니다.
ARP Parameters	ACE의 ARP 설정을 구성합니다. (ARP 프레임 유형이 선택되었을 때 ARP 매개변수를 구성할 수 있습니다.)
ARP/RARP	ACE에 대한 사용 가능한 ARP/RARP Opcode(OP) 플래그를 지정합니다. **Any** ARP/RARP OP 플래그가 지정되지 않았습니다. **ARP** 프레임은 ARP Opcode가 ARP로 설정되어야 합니다. **RARP** 프레임은 ARP Opcode가 RARP로 설정되어야 합니다. **Other** 프레임에는 알 수 없는 ARP/RARP Opcode 플래그가 있습니다.
Request/Reply	ACE에 사용 가능한 Request/Reply Opcode (OP) 플래그를 지정합니다. **Any** Request/Reply OP 플래그가 지정되지 않았습니다. **Request** 프레임은 ARP Request 또는 RARP Request OP 플래그가 설정되어야 합니다. **Reply** 프레임은 ARP Reply 또는 RARP Reply OP 플래그가 설정되어야 합니다.
Sender IP Filter	이 ACE에 대한 송신자 IP 필터를 지정합니다. **Any** 송신자 IP 필터가 지정되지 않았습니다. **Host** 송신자 IP 필터가 호스트로 설정되었습니다. **Network** 송신자 IP 필터가 네트워크로 설정되었습니다.
Sender IP Address	송신자 IP 필터로 "Host" 또는 "Network"가 선택되었을 때, 송신자 IP 주소를 점10진 표기법으로 입력할 수 있습니다.

Sender IP Mask	송신자 IP 필터로 "Network"가 선택되었을 때, 점10진 표기법으로 특정 송신자 IP 마스크를 입력할 수 있습니다.
Target IP Filter	특정 ACE에 대한 대상 IP 필터를 지정합니다. **Any** 대상 IP 필터가 지정되지 않았습니다. **Host** 대상 IP 필터가 호스트로 설정되었습니다. **Network** 대상 IP 필터가 네트워크로 설정되었습니다.
Target IP Address	대상 IP 필터로 "Host" 또는 "Network"가 선택되었을 때, 점10진 표기법으로 특정 대상 IP 주소를 입력할 수 있습니다.
Target IP Mask	대상 IP 필터로 "Network"가 선택되었을 때, 점10진 표기법으로 특정 대상 IP 마스크를 입력할 수 있습니다.
ARP Sender MAC Match	프레임이 송신자 하드웨어 주소 필드(SHA) 설정에 따라 액션을 수행할 수 있는지 여부를 지정하세요. **0** SHA가 SMAC 주소와 같지 않은 ARP 프레임. **1** SHA가 SMAC 주소와 같은 ARP 프레임. **Any** 어떤 값이든 허용됩니다.
RARP Target MAC Match	프레임이 대상 하드웨어 주소 필드 (THA) 설정에 따라 액션을 수행할 수 있는지 여부를 지정하세요. **0** THA가 대상 MAC 주소와 같지 않은 RARP 프레임. **1** THA가 대상 MAC 주소와 같은 RARP 프레임. **Any** 어떤 값이든 허용됩니다.
IP/Ethernet Length	프레임이 ARP/RARP 하드웨어 주소 길이 (HLN) 및 프로토콜 주소 길이 (PLN) 설정에 따라 액션을 수행할 수 있는지 여부를 지정하세요. **0** HLN이 이더넷 (0x06)와 같지 않거나 PLN이 IPv4 (0x04)와 같지 않은 ARP/RARP 프레임. **1** HLN이 이더넷 (0x06)와 같고 PLN이 IPv4 (0x04)와 같은 ARP/RARP 프레임. **Any** 어떤 값이든 허용됩니다.
IP	프레임이 ARP/RARP 하드웨어 주소 공간 (HRD) 설정에 따라 액션을 수행할 수 있는지 여부를 지정하세요. **0** HRD가 이더넷 (1)와 같지 않은 ARP/RARP 프레임. **1** HRD가 이더넷 (1)와 같은 ARP/RARP 프레임. **Any** 어떤 값이든 허용됩니다.
Ethernet	프레임이 ARP/RARP 프로토콜 주소 공간 (PRO) 설정에 따라 액션을 수행할 수 있는지 여부를 지정합니다. **0** PRO가 IP (0x800)와 같지 않은 ARP/RARP 프레임입니다. **1** PRO가 IP (0x800)와 같은 ARP/RARP 프레임입니다. **Any** 어떤 값이든 허용됩니다.
IP Parameters	ACE의 IPv4 설정을 구성합니다. 프레임 유형이 "IPv4"로 선택되었을 때 IP 매개변수를 구성할 수 있습니다.
IP Protocol Filter	이 ACE에 대한 IP 프로토콜 필터를 지정하세요. **Any** IP 프로토콜 필터가 지정되지 않음 **Specific**ACE에서 특정 IP 프로토콜을 필터링합니다. **ICMP** IPv4 ICMP 프로토콜 프레임을 필터링합니다. **UDP** IPv4 UDP 프로토콜 프레임을 필터링합니다. **TCP** IPv4 TCP 프로토콜 프레임을 필터링합니다.
IP Protocol Value	IP 프로토콜 값을 지정하기 위해 "Specific"이 선택되었을 때, 특정 값을 입력할 수 있습니다. 허용되는 범위는 0부터 255까지입니다. ACE와 일치하는 프레임은 기입된 IP 프로토콜 값과 일치합니다.

IP TTL	이 ACE의 Time-to-Live 설정을 지정하세요. **zero** Time-to-Live 필드가 0보다 큰 IPv4 프레임은 이 항목과 일치하지 않아야 합니다. **non-zero** Time-to-Live 필드가 0보다 큰 IPv4 프레임은 이 항목과 일치해야 합니다. **Any** 어떤 값이든 허용됩니다.
IP Fragment	이 ACE의 fragment offset 설정을 지정하세요. 이는 IPv4 프레임의 More Fragments (MF) 비트와 Fragment Offset (FRAG OFFSET) 필드에 대한 설정을 포함합니다. **No** MF 비트가 설정되어 있거나 FRAG OFFSET 필드가 0보다 큰 IPv4 프레임은 이 항목과 일치하지 않아야 합니다. **Yes** MF 비트가 설정되어 있거나 FRAG OFFSET 필드가 0보다 큰 IPv4 프레임은 이 항목과 일치해야 합니다. **Any** 어떤 값이든 허용됩니다.
IP Option	이 ACE에 대한 옵션 플래그 설정을 지정하세요. **No** 옵션 플래그가 설정된 IPv4 프레임은 이 항목과 일치하지 않아야 합니다. **Yes** 옵션 플래그가 설정된 IPv4 프레임은 이 항목과 일치해야 합니다. **Any** 어떤 값이든 허용됩니다.
SIP Filter	이 ACE에 대한 소스 IP 필터를 지정하세요. **Any** 소스 IP 필터가 지정되지 않습니다. **Host** 소스 IP 필터가 호스트로 설정됩니다. **Network** 소스 IP 필터가 네트워크로 설정됩니다.
SIP Address	"Host" 또는 "Network"가 소스 IP 필터로 선택된 경우, 점으로 구분된 10진수 표기법으로 특정 SIP 주소를 입력할 수 있습니다.
SIP Mask	소스 IP 필터로 "Network"가 선택된 경우, 점으로 구분된 10진수 표기법으로 특정 SIP 마스크를 입력할 수 있습니다.
DIP Filter	대상 IP 필터에 대한 설정을 지정합니다. **Any** 대상 IP 필터가 지정되지 않습니다. **Host** 대상 IP 필터가 Host로 설정됩니다. **Network** 대상 IP 필터가 Network로 설정됩니다.
DIP Address	대상 IP 필터에 "Host" 또는 "Network"가 선택되면 점으로 구분된 10진법 주소 형식으로 특정 DIP 주소를 입력할 수 있습니다.
DIP Mask	대상 IP 필터에 "Network"가 선택되면 점으로 구분된 10진법 주소 형식으로 특정 DIP 마스크를 입력할 수 있습니다.
IPv6 Parameters	ACE에 대한 IPv6 설정을 구성합니다. "IPv6" 프레임 유형이 선택되었을 때 IPv6 매개변수를 구성할 수 있습니다.
Next Header Filter	IPv6 ACE의 IPv6 헤더 필터를 지정하세요. **Any** IPv6 헤더 필터가 지정되지 않았습니다. **Specific** 이 ACE에서 특정 IPv6 다음 헤더 필터를 필터링합니다. **ICMP** IPv6 ICMP 프로토콜 프레임을 필터링합니다. **UDP** IPv6 UDP 프로토콜 프레임을 필터링합니다. **TCP** IPv6 TCP 프로토콜 프레임을 필터링합니다.
Next Header Value	IPv6 다음 헤더 값에 대해 "Specific"이 선택되었을 때, 특정 값을 입력할 수 있습니다. 허용되는 범위는 0에서 255까지입니다. 이 ACE에 일치하는 프레임은 이 IPv6 프로토콜 값을 가집니다.
SIP Filter	ACE에 대한 소스 IPv6 필터를 지정합니다. **Any** 소스 IPv6 필터가 지정되지 않았습니다.

	Specific 소스 IPv6 필터가 네트워크로 설정되어 있습니다.
SIP Address	소스 IPv6 필터가 "Specific"으로 선택되면 특정한 SIPv6 주소를 입력할 수 있습니다. 이 필드에서는 IPv6 주소의 마지막 32비트만 지원됩니다.
SIP BitMask	소스 IPv6 필터가 "Specific"으로 선택되면 특정한 SIPv6 마스크를 입력할 수 있습니다. 이 필드에서는 IPv6 주소의 마지막 32비트만 지원됩니다. 비트마스크의 사용에 유의하십시오. 이진 비트 값이 "0"이면 해당 비트는 "상관없음"을 의미합니다. 실제로 일치하는 패턴은 [sipv6_address & sipv6_bitmask] (마지막 32비트)입니다. 예를 들어, SIPv6 주소가 2001::3이고 SIPv6 비트마스크가 0xFFFFFFFE(비트 0은 "상관없음" 비트)인 경우, SIPv6 주소 2001::2와 2001::3이 이 규칙에 적용됩니다.
Hop Limit	이 ACE에 대한 홉 제한 설정을 지정하세요. **Zero** 홉 제한 필드가 0보다 큰 IPv6 프레임은 이 항목과 일치하지 않아야 합니다. **non-zero** 홉 제한 필드가 0보다 큰 IPv6 프레임은 이 항목과 일치해야 합니다. **Any** 모든 값이 허용됩니다.
ICMP Parameters	이 ACE에 대한 ICMP 설정을 구성합니다.
ICMP Type Filter	이 ACE에 대한 ICMP 필터를 지정합니다. **Any** ICMP 필터가 지정되지 않았습니다. **Specific** 이 ACE로 특정 ICMP 필터를 필터링하려면 특정 ICMP 값 입력할 수 있습니다.
ICMP Type Value	ICMP 필터가 "Specific"으로 선택된 경우 특정 ICMP 값이 입력될 수 있습니다. 허용되는 범위는 0부터 255까지입니다. 이 ACE에 일치하는 프레임은 해당 ICMP 값을 가집니다.
ICMP Code Filter	이 ACE에 대한 ICMP 코드 필터를 지정합니다. **Any** ICMP 코드 필터가 지정되지 않았습니다. **Specific** 이 ACE로 특정 ICMP 코드 필터를 필터링하려면 특정 ICMP 코드 값을 입력할 수 있습니다.
ICMP Code Value	ICMP 코드 필터가 "Specific"으로 선택된 경우 특정 ICMP 코드 값을 입력할 수 있습니다. 허용되는 범위는 0부터 255까지입니다. 이 ACE에 일치하는 프레임은 해당 ICMP 코드 값을 가집니다.
TCP/UDP Parameters	이 ACE에 대한 TCP/UDP 설정을 구성합니다.
TCP/UDP Source Filter	이 ACE에 대한 TCP/UDP 소스 필터를 지정합니다. **Any** TCP/UDP 소스 필터가 지정되지 않았습니다. **Specific** 이 ACE로 특정 TCP/UDP 소스 필터를 필터링하려면 특정 TCP/UDP 소스 값을 입력할 수 있습니다. **Range** 이 ACE로 특정 TCP/UDP 소스 범위 필터를 필터링하려면 특정 TCP/UDP 소스 범위 값을 입력할 수 있습니다.
TCP/UDP Source No.	TCP/UDP 소스 필터가 "Specific"으로 선택된 경우 특정 TCP/UDP 소스 값을 입력할 수 있습니다. 허용되는 범위는 0부터 65535까지입니다. 이 ACE에 일치하는 프레임은 해당 TCP/UDP 소스 값을 가집니다.
TCP/UDP Source Range	TCP/UDP 소스 필터가 "Range"로 선택된 경우 특정 TCP/UDP 소스 범위 값을 입력할 수 있습니다. 허용되는 범위는 0부터 65535까지입니다. 이 ACE에 일치하는 프레임은 해당 TCP/UDP 소스 값을 가집니다.
TCP/UDP Destination Filter	이 ACE에 대한 TCP/UDP 목적지 필터를 지정합니다. **Any** TCP/UDP 목적지 필터가 지정되지 않았습니다. **Specific** 이 ACE로 특정 TCP/UDP 목적지 필터를 필터링하려면 특정 TCP/UDP 목적지 값을 입력할 수 있습니다.

	Range 이 ACE로 특정 TCP/UDP 목적지 범위 필터를 필터링하려면 특정 TCP/UDP 목적지 범위 값을 입력할 수 있습니다.
TCP/UDP Destination Number	TCP/UDP 목적지 필터가 "Specific"으로 선택된 경우 특정 TCP/UDP 목적지 값을 입력할 수 있습니다. 허용되는 범위는 0부터 65535까지입니다. 이 ACE에 일치하는 프레임은 해당 TCP/UDP 목적지 값을 가집니다.
TCP/UDP Destination Range	TCP/UDP 목적지 필터가 "Range"로 선택된 경우 특정 TCP/UDP 목적지 범위 값을 입력할 수 있습니다. 허용되는 범위는 0부터 65535까지입니다. 이 ACE에 일치하는 프레임은 해당 TCP/UDP 목적지 값을 가집니다.
TCP FIN	이 ACE에 대한 TCP "송신자로부터 더 이상의 데이터 없음" (FIN) 값을 지정합니다. **0** FIN 필드가 설정된 TCP 프레임은 이 항목과 일치하지 않아야 합니다. **1** FIN 필드가 설정된 TCP 프레임은 이 항목과 일치해야 합니다. **Any** 모든 값이 허용됩니다.
TCP SYN	이 ACE에 대한 TCP "시퀀스 번호 동기화" (SYN) 값을 지정합니다. **0** SYN 필드가 설정된 TCP 프레임은 이 항목과 일치하지 않아야 합니다. **1** SYN 필드가 설정된 TCP 프레임은 이 항목과 일치해야 합니다. **Any** 모든 값이 허용됩니다.
TCP RST	이 ACE에 대한 TCP "연결 재설정" (RST) 값을 지정합니다. **0** RST 필드가 설정된 TCP 프레임은 이 항목과 일치하지 않아야 합니다. **1** RST 필드가 설정된 TCP 프레임은 이 항목과 일치해야 합니다. **Any** 모든 값이 허용됩니다.
TCP PSH	이 ACE에 대한 TCP "푸시 기능" (PSH) 값을 지정합니다. **0** PSH 필드가 설정된 TCP 프레임은 이 항목과 일치하지 않아야 합니다. **1** PSH 필드가 설정된 TCP 프레임은 이 항목과 일치해야 합니다. **Any** 모든 값이 허용됩니다.
TCP ACK	이 ACE에 대한 TCP "승인 필드 중요" (ACK) 값을 지정합니다. **0** ACK 필드가 설정된 TCP 프레임은 이 항목과 일치하지 않아야 합니다. **1** ACK 필드가 설정된 TCP 프레임은 이 항목과 일치해야 합니다. **Any** 모든 값이 허용됩니다.
TCP URG	이 ACE에 대한 TCP "긴급 포인터 필드 중요" (URG) 값을 지정합니다. **0** URG 필드가 설정된 TCP 프레임은 이 항목과 일치하지 않아야 합니다. **1** URG 필드가 설정된 TCP 프레임은 이 항목과 일치해야 합니다. **Any** 모든 값이 허용됩니다.
Ethernet Type Parameters	ACE의 Ethernet Type 설정을 구성하세요. Ethernet Type 프레임 유형이 선택된 경우 Ethernet Type 매개변수를 구성할 수 있습니다.
EtherType Filter	이 ACE에 대한 Ethernet 유형 필터를 지정합니다. **Any** EtherType 필터가 지정되지 않았습니다. **Specific** ACE로 특정 EtherType 필터를 필터링하려면 특정 EtherType 값을 입력할 수 있습니다.
Ethernet Type Value	EtherType 필터가 "Specific"으로 선택된 경우 특정 EtherType 값을 입력할 수 있습니다. 허용되는 범위는 0x600부터 0xFFFF까지입니다. 단, 0x800(IPv4), 0x806(ARP) 및 0x86DD(IPv6)는 제외됩니다. 이 ACE에 일치하는 프레임은 해당 EtherType 값을 가집니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset : 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.
Cancel : 이전 페이지로 돌아가려면 클릭하세요.

WEB 설정 예시

웹메뉴 Configuration>Security>Network>ACL>Access Control List

예시) PORT1에서 소스 MAC주소를 이용한 프레임거부

Access Control List Configuration

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
									⊕

✓ Access Control List Configuration

➢ ***Add ACE to end of list***

- ⊕

✓ ACE Configuration

ACE Configuration

Ingress Port	All / Port 1 / Port 2 / Port 3 / Port 4
Policy Filter	Any
Frame Type	Ethernet Type

Action	Deny
Rate Limiter	Disabled
Port Redirect	Disabled / Port 1 / Port 2 / Port 3 / Port 4
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

MAC Parameters

SMAC Filter	Specific
SMAC Value	00-21-6d-05-f0-5c
DMAC Filter	Any

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Ethernet Type Parameters

EtherType Filter	Any

Save Reset Cancel

✓ Access Control List Configuration

Access Control List Configuration

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
1	1	Any	EType	Deny	Disabled	Disabled	Disabled	21	⊕ ⊕ ⊕ ⊗ ⊕

CLI 설정 예시

예시) PORT1에서 소스 MAC주소를 이용한 프레임거부

```
(config)# access-list ace <ace_id> [1]
(config)# access-list ace 1 ingress interface GigabitEthernet 1/1 frame-type etype smac
00-21-6d-05-f0-5c action deny

[1]

action        dmac-type      frame-type     ingress        logging

mirror        next           policy         rate-limiter   redirect

shutdown      tag            tag-priority   vid            <cr>

[ action { permit | deny | filter interface <port_type> <fliter_port_list> } ]

[ dmac-type { unicast | multicast | broadcast | any}

[ ingress { interface ( <port_type> [ <ingress_port_list> ] ) | any } ]

[ logging [ disable ] ]

[ mirror [ disable ] ]

[ next { <ace_id_next> | last } ]

[ policy <policy ID> [ policy-bitmask <policy_bitmask> ] ]

[ rate-limiter { <rate_limiter_id> | disable } ]

[ redirect { interface { ( <port_type> [ <redirect_port_list> ] ) } | disable } ]

[ shutdown [ disable ] ]

[ tag { tagged | untagged | any } ]

[ tag-priority { <tag_priority> | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7 | any } ]

[ vid { <vid> | any } ]

[ shutdown [ disable ] ]

[ frame-type { any | etype [ etype-value { <etype_value> | any } ] [ smac { <etype_smac> |
any } ] [ dmac { <etype_dmac> | any } ] | arp [ sip { <arp_sip> | any } ] [ dip { <arp_dip> |
any } ] [ smac { <arp_smac> | any } ] [ arp-opcode { arp | rarp | other | any } ] [ arp-flag
[ arp-request { <arp_flag_request> | any } ] [ arp-smac { <arp_flag_smac> | any } ] [ arp-
tmac { <arp_flag_tmac> | any } ] [ arp-len { <arp_flag_len> | any } ] [ arp-ip <arp_flag_ip>
| any } ] [ arp-ether { <arp_flag_ether> | any } ] ]
 | ipv4 [ sip { <sipv4> | any } ] [ dip { <dipv4> | any } ] [ ip-protocol { <ipv4_protocol> |
any } ] [ ip-flag [ ip-ttl { <ip_flag_ttl> | any } ] [ ip-options { <ip_flag_options> | any } ]
[ ip-fragment { <ip_flag_fragment> | any } ] ] | ipv4-icmp [ sip { <sipv4_icmp> | any } ]
[ dip { <dipv4_icmp> | any } ] [ icmp-type { <icmpv4_type> | any } ] [ icmp-code
{ <icmpv4_code> | any } ] [ ip-flag [ ip-ttl { <ip_flag_icmp_ttl> | any } ] [ ip-options
{ <ip_flag_icmp_options> | any } ] [ ip-fragment { <ip_flag_icmp_fragment> | any } ] ] |
ipv4-udp [ sip { <sipv4_udp> | any } ] [ dip { <dipv4_udp> | any } ] [ sport
{ <sportv4_udp_start> [ to <sportv4_udp_end> ] | any } ] [ dport { <dportv4_udp_start>
[ to <dportv4_udp_end> ] | any } ] [ ip-flag [ ip-ttl { <ip_flag_udp_ttl> | any } ] [ ip-
options { <ip_flag_udp_options> | any } ] [ ip-fragment { <ip_flag_udp_fragment> |
any } ] ] | ipv4-tcp [ sip { <sipv4_tcp> | any } ] [ dip { <dipv4_tcp> | any } ] [ sport
```

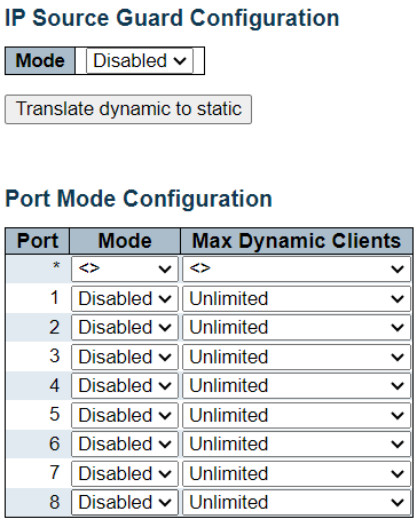
```
{ <sportv4_tcp_start> [ to <sportv4_tcp_end> ] | any } ] [ dport { <dportv4_tcp_start> [ to
<dportv4_tcp_end> ] | any } ] [ ip-flag [ ip-ttl { <ip_flag_tcp_ttl> | any } ] [ ip-options
{ <ip_flag_tcp_options> | any } ] [ ip-fragment { <ip_flag_tcp_fragment> | any } ] ] [ tcp-
flag [ tcp-fin { <tcpv4_flag_fin> | any } ] [ tcp-syn { <tcpv4_flag_syn> | any } ] [ tcp-rst
{ <tcpv4_flag_rst> | any } ] [ tcp-psh { <tcpv4_flag_psh> | any } ] [ tcp-ack
{ <tcpv4_flag_ack> | any } ] [ tcp-urg { <tcpv4_flag_urg> | any } ] ] | ipv6 [ next-header
{ <next_header> | any } ] [ sip { <sipv6> [ sip-bitmask <sipv6_bitmask> ] | any } ] [ hop-
limit { <hop_limit> | any } ] | ipv6-icmp [ sip { <sipv6_icmp> [ sip-bitmask
<sipv6_bitmask_icmp> ] | any } ] [ icmp-type { <icmpv6_type> | any } ] [ icmp-code
{ <icmpv6_code> | any } ] [ hop-limit { <hop_limit_icmp> | any } ] | ipv6-udp [ sip
{ <sipv6_udp> [ sip-bitmask <sipv6_bitmask_udp> ] | any } ] [ sport
{ <sportv6_udp_start> [ to <sportv6_udp_end> ] | any } ] [ dport { <dportv6_udp_start>
[ to <dportv6_udp_end> ] | any } ] [ hop-limit { <hop_limit_udp> | any } ] | ipv6-tcp [ sip
{ <sipv6_tcp> [ sip-bitmask <sipv6_bitmask_tcp> ] | any } ] [ sport { <sportv6_tcp_start>
[ to <sportv6_tcp_end> ] | any } ] [ dport { <dportv6_tcp_start> [ to <dportv6_tcp_end> ]
| any } ] [ hop-limit { <hop_limit_tcp> | any } ] [ tcp-flag [ tcp-fin { <tcpv6_flag_fin> |
any } ] [ tcp-syn { <tcpv6_flag_syn> | any } ] [ tcp-rst { <tcpv6_flag_rst> | any } ] [ tcp-psh
{ <tcpv6_flag_psh> | any } ] [ tcp-ack { <tcpv6_flag_ack> | any } ] [ tcp-urg
{ <tcpv6_flag_urg> | any } ] ] } ]
```

6.5.2.3. IP Source Guard

6.5.2.3.1. Configuration

웹메뉴 Configuration>Security>Network>IP Source Guard>Configuration

이 페이지는 IP 소스 가드 관련 구성을 제공합니다.



IP Source Guard Configuration

용어	설명
Mode of IP Source Guard Configuration	IP 소스 가드를 활성화하거나 비활성화하세요. 모드를 활성화하면 구성된 모든 ACE(액세스 제어 항목)가 손실됩니다.

Port Mode Configuration

용어	설명
Port Mode Configuration	특정 포트에서 IP 소스 가드가 활성화되도록 설정하세요. 주어진 포트의 전역 모드와 포트 모드가 모두 활성화된 경우에만 해당 포트에서 IP 소스 가드가 활성화됩니다.
Max Dynamic Clients	주어진 포트에서 학습할 수 있는 동적 클라이언트의 최대 수를 지정하세요. 이 값은 0, 1, 2 또는 무제한일 수 있습니다. 포트 모드가 활성화되고 최대 동적 클라이언트 값이 0인 경우, 해당 포트의 정적 항목과 일치하는 IP 패킷 전달만 허용됨을 의미합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

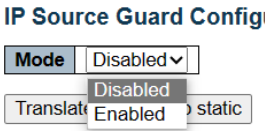
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

Translate dynamic to static: 정적 항목에 모든 동적 항목을 Translate합니다

WEB 설정 예시

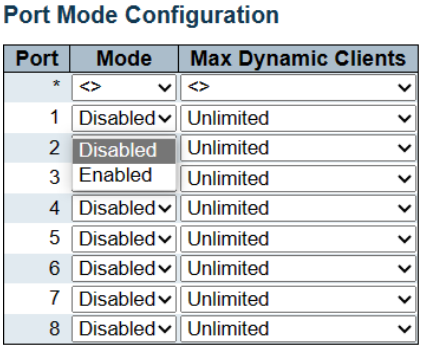
✓ IP Source Guard Configuration

- ➢ ***Mode***
  - ***Disable | Enable***

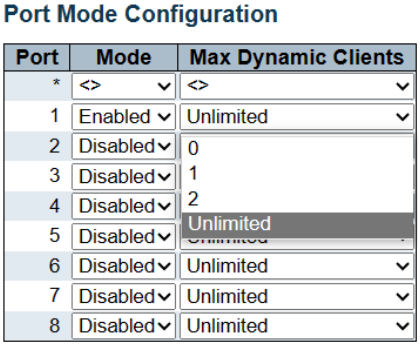


✓ Port Mode Configuration

- ➢ ***Mode***
  - ***Disable | Enable***



- ➢ ***Max Dynamic Clients***
  - ***0 | 1 | 2 | Unlimited***



CLI 설정 예시

✓ IP Source Guard Configuration

- ➢ ***Mode***

- ***Disable | Enable***

(config)# no ip verify source
(config)# ip verify source

✓ Port Mode Configuration

➢ *Mode*

- ***Disable | Enable***

(config)# interface (<port_type> [<plist>]) *(config)# interface GigabitEthernet 1/1* (config-if)# no ip verify source
(config-if)# ip verify source

➢ *Max Dynamic Clients*

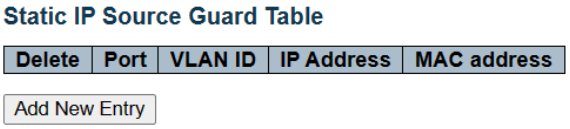
- ***0 | 1 | 2 | Unlimited***

(config-if)# ip verify source limit <cnt_var> (config-if)# ip verify source limit <0-2> *(config-if)# ip verify source limit 0* *(config-if)# ip verify source limit 1* *(config-if)# ip verify source limit 2*
(config-if)# no ip verify source limit

6.5.2.3.2. Static Table

웹메뉴 Configuration>Security>Network>IP Source Guard>Static Table

이 페이지는 스위치의 정적 IP 소스 가드 규칙을 보여줍니다. 규칙의 최대 수는 스위치에서 112개입니다.



Static IP Source Guard Table

용어	설명
Delete	삭제할 항목을 선택하세요. 저장 시 삭제됩니다.
Port	설정 논리 포트.
VLAN ID	설정 VLAN ID.
IP Address	허용된 소스 IP 주소.
MAC address	허용된 소스 MAC 주소.

Buttons

Add New Entry: 정적 IP 소스 가드 테이블에 새 항목을 추가합니다.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

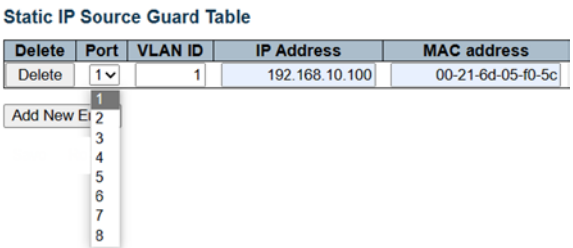
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

✓ **Static IP Source Guard Table**

➢ ***Add New Entry***

- ***Port | VLAN ID(Port VLAN) | IP Address | MAC address***



CLI 설정 예시

✓ Static IP Source Guard Table

➢ ***Add New Entry***

- ***Port | VLAN ID(Port VLAN) | IP Address | MAC address***

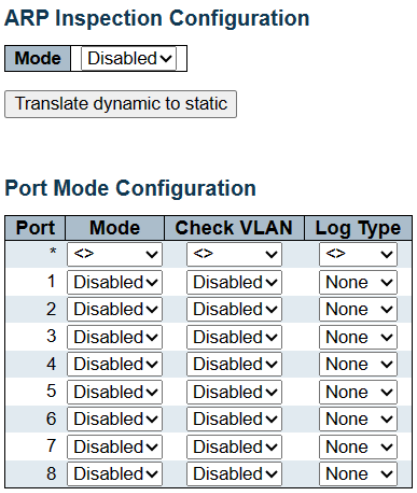
```
(config)# ip source binding interface <port_type> <in_port_type_id> <vlan_var>
<ipv4_var> <mac_var>
(config)# ip source binding interface GigabitEthernet 1/1 1 192.168.10.100 00-21-6D-05-
F0-5C
```

6.5.2.4. ARP Inspection

6.5.2.4.1. Port Configuration

웹메뉴 Configuration>Security>Network>ARP Inspection>Port Configuration

이 페이지는 ARP 검사에 관련된 구성을 제공합니다.



ARP Inspection Configuration

용어	설명
Mode	전체 ARP Inspection을 활성화하거나 비활성화하십시오.

Port Mode Configuration

용어	설명
Port	설정을 위한 논리 포트입니다.
Mode	각 포트에 ARP 검사가 활성화된 경우를 지정하십시오. 특정 포트의 전체 모드와 포트 모드가 모두 활성화된 경우에만 해당 포트에서 ARP Inspection이 활성화됩니다. **Enable** ARP Inspection 작업 활성화. **Disable** ARP Inspection 작업 비활성화.
Check VLAN	VLAN 구성을 검사하려면 "Check VLAN" 설정을 활성화해야 합니다. "Check VLAN"의 기본 설정은 비활성화입니다. (검사할 VLAN 목록은 VLAN Configuration에서 설정하세요.) **Enable** Check VLAN 활성화. ARP 검사의 로그 유형은 VLAN 설정을 참조합니다. **Disable** Check VLAN 비활성화. ARP 검사의 로그 유형은 포트 설정을 참조합니다.
Log Type	주어진 포트의 전역 모드와 포트 모드가 활성화되었고, "Check VLAN" 설정이 비활성화된 경우, ARP 검사의 로그 유형은 포트 설정을 참조합니다. **None** 아무것도 기록하지 않음. **Deny** 거부된 항목 기록. **Permit** 허용된 항목 기록. **All** 모든 항목 기록.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

Translate dynamic to static: 정적 항목에 모든 동적 항목을 Translate합니다.

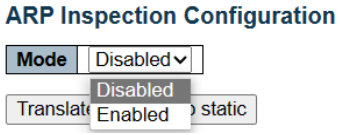
WEB 설정 예시

웹메뉴 Configuration>Security>Network>ARP Inspection>Port Configuration

✓ ARP Inspection Configuration

➢ ***Mode***

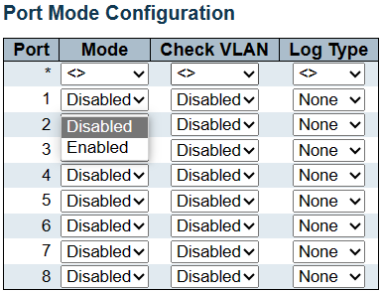
- ***Disable | Enable***



✓ Port Mode Configuration

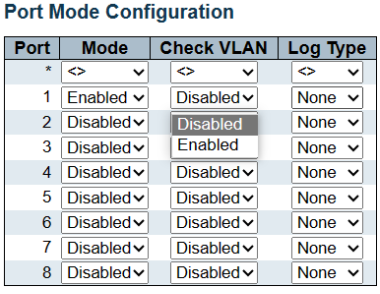
➢ ***Mode***

- ***Disable | Enable***



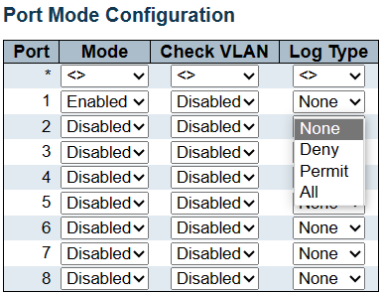
➢ ***Check VLAN***

- ***Disable | Enable***



➢ ***Log Type***

- ***None | Deny | Permit | All***



CLI 설정 예시

✓ ARP Inspection Configuration

➢ ***Mode***

- ***Disable | Enable***

```
(config)# no ip arp inspection
```

```
(config)# ip arp inspection
```

✓ Port Mode Configuration

➢ ***Mode***

- ***Disable | Enable***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# ip arp inspection trust
```

```
(config)# no ip arp inspection trust
```

➢ ***Check VLAN***

- ***Disable | Enable***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# no ip arp inspection check-vlan
```

```
(config-if)# ip arp inspection check-vlan
```

➢ ***Log Type***

- ***None | Deny | Permit | All***

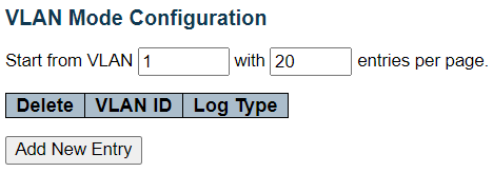
```
(config)# interface ( <port_type> [ <plist> ] )
```

(config)# interface GigabitEthernet 1/1 (config-if)# no ip arp inspection logging
(config-if)# ip arp inspection logging { deny | permit | all } *(config-if)# ip arp inspection logging deny*

6.5.2.4.2. VLAN Configuration

웹메뉴 Configuration>Security>Network>ARP Inspection>VLAN Configuration

이 페이지는 ARP Inspection 관련 구성을 제공합니다.



VLAN Mode Configuration

용어	설명
VLAN Mode Configuration	ARP Inspection 이 어떤 VLAN 에서 활성화되는지 지정합니다. 첫번째, Port Configuration 에서 포트의 설정을 활성화해야 합니다. 이때, 주어진 포트의 전역 모드(Global Mode)와 포트 모드(Port Mode)가 모두 활성화되어야만 해당 포트에서 ARP Inspection 이 활성화됩니다. 두번째, 이 페이지에서 어떤 VLAN 이 검사될지 지정할 수 있습니다. 또한, VLAN 별 기록유형을 달리 할 수 있습니다. **None** 아무 것도 기록하지 않습니다. **Deny** 거부된 항목을 기록합니다. **Permit** 허용된 항목을 기록합니다. **All** 모든 항목을 기록합니다.

Buttons

Refresh: 클릭 시 페이지를 새로 고침.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

<<: 현재 표시되는 마지막 항목에 종료. 시스템 로그 항목을 업데이트 합니다.

>>: 현재 표시되는 마지막 항목에서 시작하여, 시스템 로그 항목을 업데이트 합니다.

Add New Entry: 정적 IP 소스 가드 테이블에 새 항목을 추가합니다.

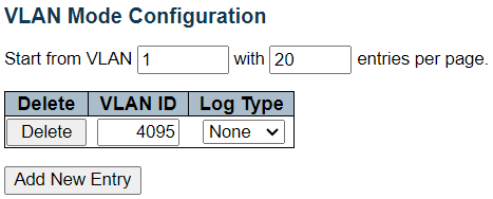
WEB 설정 예시

웹메뉴 Configuration>Security>Network>ARP Inspection>VLAN Configuration

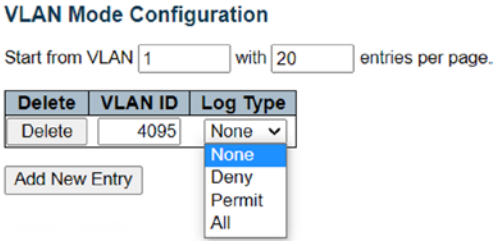
✓ **VLAN Mode Configuration**

➢ ***Add New Entry***

- ***VLAN ID(1~4095)***



- ***Log Type(None | Deny | Permit | All)***



CLI 설정 예시

✓ VLAN Mode Configuration

➢ *Add New Entry*

- ***VLAN ID(1~4095)***

```
(config)# ip arp inspection vlan <in_vlan_list>
(config)# ip arp inspection vlan 4095
```

- ***Log Type(None | Deny | Permit | All)***

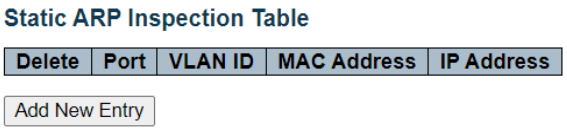
```
(config)# no ip arp inspection vlan <in_vlan_list> logging
(config)# no ip arp inspection vlan 4095 logging
```

```
(config)# ip arp inspection vlan <in_vlan_list> logging { deny | permit | all }
(config)# ip arp inspection vlan 4095 logging deny
(config)# ip arp inspection vlan 4095 logging permit
(config)# ip arp inspection vlan 4095 logging all
```

6.5.2.4.3. Static Table

웹메뉴 Configuration>Security>Network>ARP Inspection>Static Table

이 페이지는 정적 ARP 검사(rule)를 보여줍니다. 스위치에서의 최대 rule 수는 256입니다.



Static ARP Inspection Table

용어	설명
Delete	삭제할 항목을 선택하세요. 저장 시 삭제됩니다.
Port	설정의 논리 포트입니다.
VLAN ID	설정의 VLAN ID 입니다.
MAC Address	ARP 요청 패킷에서 허용된 소스 MAC 주소입니다.
IP Address	ARP 요청 패킷에서 허용된 소스 IP 주소입니다.

Buttons

Add New Entry: 정적 IP 소스 가드 테이블에 새 항목을 추가합니다.
Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

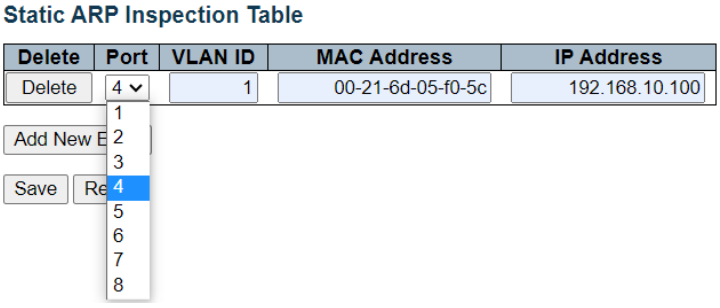
WEB 설정 예시

웹메뉴 Configuration>Security>Network>ARP Inspection>Static Table

✓ **Static ARP Inspection Table**

➢ ***Add New Entry***

- ***Example***



CLI 설정 예시

✓ Static ARP Inspection Table

➢ *Add New Entry*

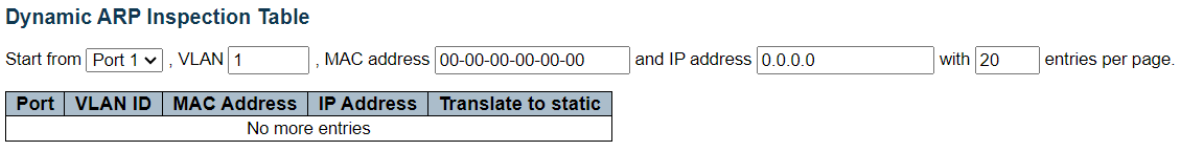
- ***Example***

```
(config)# ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var>
<mac_var> <ipv4_var>
(config)# ip arp inspection entry interface GigabitEthernet 1/4 1 00-21-6d-05-f0-5c
192.168.10.100
```

6.5.2.4.4. Dynamic Table

웹메뉴 Configuration>Security>Network>ARP Inspection>Dynamic Table

이 페이지에는 동적 ARP 검사 테이블의 항목이 표시됩니다.
동적 ARP 검사 테이블은 최대 256개의 항목을 포함하며, 포트, VLAN ID, MAC 주소, IP 주소의 순서로 정렬됩니다. 모든 동적 항목은 DHCP Snooping을 통해 학습됩니다.



Dynamic ARP Inspection Table

용어	설명
Delete	삭제할 항목을 선택하세요. 저장 시 삭제됩니다.
Port	설정의 논리 포트입니다.
VLAN ID	설정의 VLAN ID 입니다.
MAC Address	ARP 요청 패킷에서 허용된 소스 MAC 주소입니다.
IP Address	ARP 요청 패킷에서 허용된 소스 IP 주소입니다.

Buttons

Auto-refresh : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh: 클릭 시 페이지를 새로 고침.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

<<: 현재 표시되는 마지막 항목에 종료. 시스템 로그 항목을 업데이트 합니다.

>>: 현재 표시되는 마지막 항목에서 시작하여, 시스템 로그 항목을 업데이트 합니다.

6.5.3. AAA Configuration

AAA는 Timeout, Retransmit, Secret Key, NAS IP Address, NAS IPv6 Address, NAS Identifier, Dead Time 매개변수를 포함한 공통 서버 구성을 허용합니다. 소프트웨어는 RADIUS 및 TACACS+ 서버의 구성을 지원합니다.

RADIUS 서버는 설계상 신뢰할 수 없는 UDP 프로토콜을 사용합니다. 손실된 프레임에 대처하기 위해 타임아웃 간격은 동일한 길이의 세 개의 하위 간격으로 나뉩니다. 하위 간격 내에 응답이 수신되지 않으면 요청이 다시 전송됩니다. 이 알고리즘을 사용하면 RADIUS 서버가 죽은 것으로 간주되기 전에 최대 세 번 쿼리됩니다.

0~3600초 사이의 숫자로 설정할 수 있는 데드 타임은 스위치가 이전 요청에 응답하지 못한 서버에 새 요청을 보내지 않는 기간입니다.
이렇게 하면 스위치가 이미 죽은 것으로 판단한 서버에 계속해서 연결을 시도하지 않습니다.
데드 타임을 0보다 큰 값으로 설정하면 이 기능이 활성화되지만 둘 이상의 서버가 구성된 경우에만 가능합니다.

인증은 사용자가 스위치의 관리 인터페이스에 액세스할 수 있도록 인증하는 것입니다.

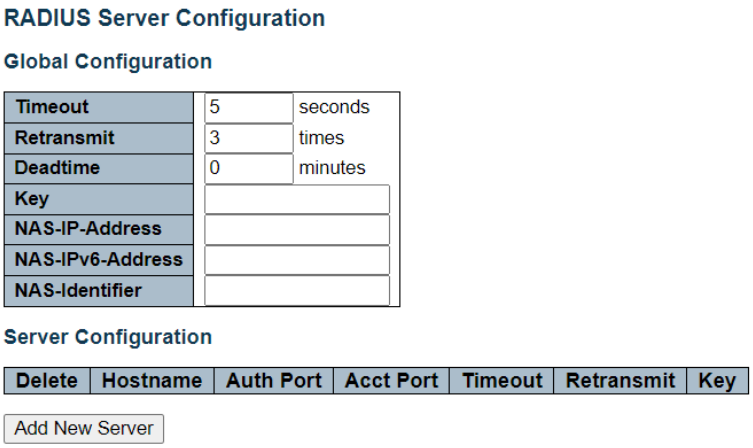
RADIUS 인증 서버는 NAS 모듈과 스위치 관리 인터페이스에 대한 액세스 권한을 부여하는 데 모두 사용됩니다. RADIUS 계정 서버는 NAS 모듈에서만 사용됩니다.

TACACS+는 라우터, 네트워크 액세스 서버 및 기타 네트워크 컴퓨팅 장치를 위한 액세스 제어 네트워크 프로토콜입니다. TACACS+ 인증, 권한 부여 및 계정 관리는 소프트웨어에서 지원됩니다. CLI 인터페이스는 TACACS+ 인증 및 계정 메커니즘 구성을 위한 초기 버전에서만 지원됩니다.

6.5.3.1. RADIUS

웹메뉴 Configuration>Security>AAA>RADIUS

이 페이지에서는 RADIUS 서버를 구성할 수 있습니다.



RADIUS Server Configuration

Global Configuration

용어	설명
Timeout	RADIUS 서버로부터 응답을 받기 위해 재전송하기 전까지 기다리는 시간(1 부터 1000 사이의 초)입니다.
Retransmit	응답이 없는 서버에 대해 RADIUS 요청이 재전송되는 횟수(1 부터 1000 사이)입니다. 마지막 재전송 후에도 서버에서 응답이 없으면 해당 서버는 동작하지 않는 것으로 간주됩니다.
Deadtime	이전 요청에 응답하지 않은 서버에게 새로운 요청을 보내지 않을 기간(0 에서 1440 분 사이)입니다. 스위치가 이미 동작하지 않는 서버에 지속적으로 연락을 시도하는 것을 막을 수 있습니다. Deadtime 을 0 보다 큰 값으로 설정하면 이 기능이 활성화되지만, 여러 개의 서버가 구성되어 있을 때만 적용됩니다.
Key	RADIUS 서버와 스위치 간에 공유되는 최대 63 자의 시크릿 키입니다.
NAS-IP-Address (Attribute 4)	RADIUS Access-Request 패킷의 속성 4 로 사용할 IPv4 주소입니다. 필드를 비워 둘 경우, 발신 인터페이스의 IP 주소가 사용됩니다.
NAS-IPv6-Address (Attribute 95)	RADIUS Access-Request 패킷의 속성 95 로 사용할 IPv6 주소입니다. 필드를 비워 둘 경우, 발신 인터페이스의 IP 주소가 사용됩니다.
NAS-Identifier (Attribute 32)	RADIUS Access-Request 패킷의 속성 32 로 사용될 최대 253 자의 식별자입니다. 필드를 비워 둘 경우, 패킷에 NAS-Identifier 가 포함되지 않습니다.

Server Configuration

용어	설명
Delete	서버 항목을 삭제하려면 선택하세요. 항목은 다음 저장 중에 삭제됩니다.
Hostname	RADIUS 서버의 IP 주소 또는 호스트 이름입니다.
Auth Port	인증을 위해 RADIUS 서버에서 사용할 UDP 포트입니다. 인증을 비활성화하려면 0 으로 설정하세요.
Acct Port	계정 정보를 위해 RADIUS 서버에서 사용할 UDP 포트입니다. 계정을 비활성화하려면 0 으로 설정하세요.
Timeout	이 설정은 전역 타임아웃 값을 덮어씁니다. 비워 둘 경우, 전역 타임아웃 값을 사용합니다.
Retransmit	이 설정은 전역 재전송 값을 덮어씁니다. 비워 둘 경우, 전역 재전송 값이 사용됩니다.
Key	이 선택적인 설정은 전역 키를 덮어씁니다. 비워 둘 경우, 전역 키가 사용됩니다.

Buttons

Add New Server: 새 RADIUS 서버를 추가 할 수 있습니다. 테이블에 빈 행이 추가되며, 필요에 따라 RADIUS 서버를 구성할 수 있습니다. (최대 5개 서버까지 지원)

Delete: 추가한 서버를 취소 합니다.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>Security>AAA>RADIUS

✓ Global Configuration

➢ *Timeout(3sec)*

Global Configuration

Timeout	3	seconds
Retransmit	3	times
Deadtime	0	minutes
Key		
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

➢ *Retransmit(5times)*

Global Configuration

Timeout	3	seconds
Retransmit	5	times
Deadtime	0	minutes
Key		
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

➢ *Deadtime(2minutes)*

Global Configuration

Timeout	3	seconds
Retransmit	5	times
Deadtime	2	minutes
Key		
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

➢ *Key (Radius server secret key)*

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	2	minutes
Key	••••••••••••••••••••••••	
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

➢ *Add New Server*

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
☐	192.168.10.251	1812	1813			

CLI 설정 예시

✓ Global Configuration

➢ ***Timeout(3sec)***

```
(config)# radius-server timeout <seconds>
(config)# radius-server timeout 3
```

➢ ***Retransmit(5times)***

```
(config)# radius-server retransmit <retries>
(config)# radius-server retransmit 5
```

➢ ***Deadtime(2minutes)***

```
(config)# radius-server deadtime <minutes>
(config)# radius-server deadtime 2
```

➢ ***Key (Radius server secret key)***

```
(config)# radius-server key [ <key> ]
(config)# radius-server key radius11
```

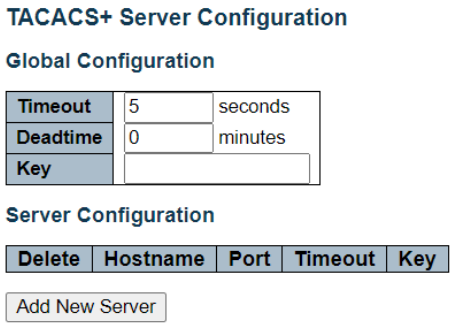
➢ ***Add New Server***

```
(config)# radius-server host <host_name> [ auth-port <auth_port> ] [ acct-port
<acct_port> ] [ timeout <seconds> ] [ retransmit <retries> ] [ key <key> ]
(config)# radius-server host 192.168.10.251 auth-port 1812 acct-port 1813
```

6.5.3.2. TACACS+

웹메뉴 Configuration>Security>AAA>TACACS+

이 페이지에서는 TACACS+ 서버를 구성할 수 있습니다.



TACACS+ Server Configuration

Global Configuration

용어	설명
Timeout	TACACS+ 서버로부터 응답을 받기 위해 기다리는 시간(1~1000 초 범위)을 의미합니다. 응답이 없을 경우 해당 서버가 죽은 것으로 간주됩니다.
Deadtime	이전 요청에 응답하지 않은 서버에게 새로운 요청을 보내지 않을 기간(0 에서 1440 분 사이)입니다. 스위치가 이미 동작하지 않는 서버에 지속적으로 연락을 시도하는 것을 막을 수 있습니다. Deadtime 을 0 보다 큰 값으로 설정하면 이 기능이 활성화되지만, 여러 개의 서버가 구성되어 있을 때만 적용됩니다.
Key	TACACS+ 서버와 스위치 간에 공유되는 최대 63 자 비밀 키입니다. 서버와 스위치 간의 인증 및 통신에 사용됩니다.

Server Configuration

용어	설명
Delete	TACACS+ 서버 항목을 삭제하려면 선택하십시오. 저장 시에 삭제됩니다.
Hostname	TACACS+ 서버의 IP 주소 또는 호스트 이름입니다.
Port	인증에 사용할 TACACS+ 서버의 TCP 포트입니다.
Timeout	이 설정은 전역 타임아웃 값을 덮어씁니다. 비워 둘 경우, 전역 타임아웃 값이 사용됩니다.
Key	이 선택적인 설정은 전역 키를 덮어씁니다. 비워 둘 경우, 전역 키가 사용됩니다.

Buttons

Add New Server : 버튼 클릭 시 새 TACACS + 서버를 추가 할 수 있습니다. 빈 행이 테이블에 추가되고, 필요에 따라 TACACS + 서버가 구성 될 수 있습니다.

Delete : 버튼 클릭 시 새로운 서버의 추가를 취소 할 수 있습니다.

Apply : 클릭 시 변경사항을 적용합니다.

Apply&Save : 클릭 시 변경사항을 적용하고 저장합니다.

Reset : 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>Security>AAA>TACACS+

✓ Global Configuration

- ***Timeout(3sec)***

Global Configuration

Timeout	3	seconds
Deadtime	0	minutes
Key		

- ***Deadtime(2minutes)***

Global Configuration

Timeout	3	seconds
Deadtime	2	minutes
Key		

- ***Key (Tacacs+ server secret key)***

Global Configuration

Timeout	3	seconds
Deadtime	2	minutes
Key	••••••••••••••••••••••••••	

- ***Add New Server***

Server Configuration

Delete	Hostname	Port	Timeout	Key
☐	192.168.10.251	49		

CLI 설정 예시

✓ Global Configuration

- ***Timeout(3sec)***

```
(config)# tacacs-server timeout <seconds>
(config)# tacacs-server timeout 3
```

- ***Deadtime(2minutes)***

```
(config)# tacacs-server deadtime <minutes>
(config)# tacacs-server deadtime 2
```

- ***Key (Tacacs+ server secret key)***

```
(config)# tacacs-server key [ <key> ]
(config)# tacacs-server key tacacs11
```

- ***Add New Server***

```
(config)# tacacs-server host <host_name> [ port <port> ] [ timeout <seconds> ] [ key
<key> ]
(config)# tacacs-server host 192.168.10.251 port 49
```

6.5.4. Access Management Statistics Monitor

웹메뉴 Monitor>Security>Access Management Statistics

Access Management Configuration에 대한 통계정보를 제공합니다.

Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Access Management Statistics

용어	설명
Interface	원격 호스트가 스위치에 액세스 할 수 있는 인터페이스 유형입니다.
Received Packets	Access Management 가 활성화된 인터페이스에서 수신된 패킷의 수입니다.
Allowed Packets	Access Management 가 활성화된 인터페이스에서 허용된 패킷의 수입니다.
Discarded Packets	Access Management 가 활성화된 인터페이스에서 폐기된 패킷의 수입니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

Clear : 선택한 로그 항목을 Clear 합니다.

WEB 확인 예시

웹메뉴 Monitor>Security>Access Management Statistics

Access Management Statistics

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	183	183	0
SNMP	6	0	6
TELNET	122	122	0
SSH	85	85	0

CLI 확인 예시

- ***Access Management Statistics***

```
# show access management statistics
```

```
Access Management Statistics:
------------------------------
HTTP     Receive:      0    Allow:      0    Discard:      0
HTTPS    Receive:    201    Allow:    201    Discard:      0
SNMP     Receive:     26    Allow:      0    Discard:     26
TELNET   Receive:    124    Allow:    124    Discard:      0
SSH      Receive:     89    Allow:     89    Discard:      0
```

6.5.5. Network Monitor

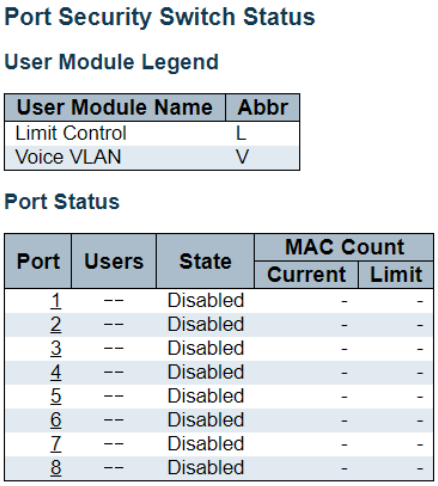
6.5.5.1. Port Security

6.5.5.1.1. Switch

웹메뉴 Monitor>Security>Network>Port Security>Switch

이 페이지는 포트 보안 상태를 보여줍니다. 포트 보안은 직접적인 구성이 없는 모듈입니다. 구성은 다른 모듈, 즉 사용자 모듈에서 간접적으로 이루어집니다. 사용자 모듈이 포트에 포트 보안을 활성화하면 포트는 소프트웨어 기반 학습을 위해 설정됩니다. 이 모드에서는 알 수 없는 MAC 주소의 프레임이 포트 보안 모듈로 전달되며, 이 모듈은 모든 사용자 모듈에게 이 새로운 MAC 주소를 전달할지 차단할지 물어봅니다. MAC 주소가 전달 상태로 설정되려면 모든 활성화된 사용자 모듈이 MAC 주소를 전달해도 괜찮다는 데에 일치해야 합니다. 하나의 모듈만 차단을 선택하면 해당 모듈이 다시 결정할 때까지 차단됩니다.

상태 페이지는 사용자 모듈의 범례와 실제 포트 상태로 나뉘어집니다.



Port Security Switch Status

User Module Legend

User Module Name	Abbr
Limit Control	L
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	--	Disabled	-	-
2	--	Disabled	-	-
3	--	Disabled	-	-
4	--	Disabled	-	-
5	--	Disabled	-	-
6	--	Disabled	-	-
7	--	Disabled	-	-
8	--	Disabled	-	-

Port Security Switch Status

User Module Legend

용어	설명
User Module Legend	범례는 포트 보안 서비스를 요청할 수 있는 모든 사용자 모듈을 보여줍니다.
User Module Name	Port Security 서비스를 요청할 수 있는 모듈의 전체 이름은 다음과 같습니다.
Abbr	사용자 모듈의 한 글자 약어는 포트 상태 테이블의 사용자 열에서 사용됩니다.

User Module Legend

용어	설명
Port Status	이 테이블은 스위치의 각 포트마다 하나의 행과 여러 열이 있습니다.
Port	상태가 적용되는 포트 번호입니다. 이 특정 포트의 상태를 보려면 포트 번호를 클릭하십시오.

Users	각 사용자 모듈마다 해당 모듈이 포트 보안을 활성화했는지 여부를 나타내는 열이 있습니다. '-'은 해당하는 사용자 모듈이 비활성화되었음을 나타내며, 문자는 해당 약어 (Abbr 참조)로 축약된 사용자 모듈이 포트 보안을 활성화했음을 나타냅니다.
State	포트의 현재 상태를 나타냅니다. 다음 네 가지 값 중 하나를 가질 수 있습니다. Disabled: 현재 사용자 모듈이 포트 보안 서비스를 사용하지 않습니다. Ready: 최소한 하나의 사용자 모듈에서 포트 보안 서비스를 사용하고 있으며, 알 수 없는 MAC 주소의 프레임이 도착하기를 기다리고 있습니다. Limit Reached: 적어도 Limit Control 사용자 모듈에서 포트 보안 서비스가 활성화되었으며, 해당 모듈에서 제한에 도달했으며 더 이상 MAC 주소를 수용하지 않아야 함을 나타냅니다. Shutdown: 적어도 Limit Control 사용자 모듈에서 포트 보안 서비스가 활성화되었으며, 해당 모듈에서 제한을 초과했음을 나타냅니다. 포트가 Limit Control 구성 웹 페이지에서 관리적으로 다시 열릴 때까지 해당 포트에서는 MAC 주소를 학습할 수 없습니다.
MAC Count (Current, Limit)	두 개의 열은 현재 학습된 MAC 주소 (전달 및 차단된 주소 모두)의 수와 해당 포트에서 학습할 수 있는 최대 MAC 주소의 수를 각각 나타냅니다. 포트에 사용자 모듈이 활성화되어 있지 않은 경우, "Current" 열은 대시 (-)를 표시합니다. 포트에 "Limit Control" 사용자 모듈이 활성화되어 있지 않은 경우, "Limit" 열은 대시 (-)를 표시합니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

WEB 확인 예시

웹메뉴 Monitor>Security>Network>Port Security>Switch

✓ Port Security Switch Status

Port Security Switch Status

User Module Legend

User Module Name	Abbr
Limit Control	L
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	L-	Limit Reached	5	4
2	--	Disabled	-	-
3	--	Disabled	-	-
4	--	Disabled	-	-
5	--	Disabled	-	-
6	--	Disabled	-	-
7	--	Disabled	-	-
8	--	Disabled	-	-

CLI 확인 예시

✓ Port Security Switch Status

```
# show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security switch

Users:
L = Limit Control
V = Voice VLAN
Interface               Users  State          MAC Cnt
----------------------  -----  -------------  -------
GigabitEthernet 1/1     L-     Limit Reached      5
GigabitEthernet 1/2     --     No users           0
GigabitEthernet 1/3     --     No users           0
GigabitEthernet 1/4     --     No users           0
10GigabitEthernet 1/1   --     No users           0
10GigabitEthernet 1/2   --     No users           0
10GigabitEthernet 1/3   --     No users           0
10GigabitEthernet 1/4   --     No users           0
```

6.5.5.1.2. Port

웹메뉴 Monitor>Security>Network>Port Security>Port

이 페이지는 포트 보안 모듈에 의해 보호되는 MAC 주소를 보여줍니다. 포트 보안은 직접적인 설정이 없는 모듈입니다. 설정은 다른 모듈인 사용자 모듈에서 간접적으로 이루어집니다. 사용자 모듈에서 포트 보안을 활성화한 경우, 포트는 소프트웨어 기반 학습을 위해 설정됩니다. 이 모드에서 알려지지 않은 MAC 주소의 프레임은 포트 보안 모듈로 전달되며, 포트 보안 모듈은 이 새로운 MAC 주소를 전달할지 차단할지 여부에 대해 모든 사용자 모듈에게 요청합니다. MAC 주소가 전달 상태로 설정되기 위해서는 모든 활성화된 사용자 모듈이 MAC 주소를 전달하기로 합의해야 합니다. 하나의 모듈만 차단을 선택하면, 해당 사용자 모듈이 다시 결정할 때까지 차단됩니다.

Port Security Port Status Port 1

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
No MAC addresses attached				

Port Security Port Status Port n

용어	설명
MAC Address & VLAN ID	이 포트에서 보이는 MAC 주소와 VLAN ID 입니다. MAC 주소가 학습되지 않은 경우, "No MAC addresses attached"이라는 단일 행이 표시됩니다.
State	해당 MAC 주소가 차단되었는지 전달 상태인지를 나타냅니다. 차단 상태인 경우, 트래픽을 전송하거나 수신할 수 없습니다.
Time of Addition	해당 MAC 주소가 해당 포트에서 처음으로 확인된 날짜와 시간을 표시합니다.
Age/Hold	적어도 하나의 사용자 모듈이 이 MAC 주소를 차단하기로 결정한 경우, 유지 시간(hold time)이 만료될 때까지 차단 상태로 유지됩니다(초 단위로 측정). 모든 사용자 모듈이 이 MAC 주소를 전달하기로 결정하고 에이징(aging)이 활성화된 경우, 포트 보안 모듈은 주기적으로 이 MAC 주소가 여전히 트래픽을 전달하는지 확인합니다. 에이징 기간(age period)이 만료되고 프레임이 관찰되지 않은 경우, MAC 주소는 MAC 테이블에서 제거됩니다. 그렇지 않으면 새로운 에이징 기간이 시작됩니다. 에이징이 비활성화되었거나 사용자 모듈이 MAC 주소를 영구히 보류하기로 결정한 경우 대시(-)가 표시됩니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

WEB 확인 예시

웹메뉴 Monitor>Security>Network>Port Security>Switch

✓ **Port Security Switch Status**

Port Security Port Status Port 1

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
c0-18-50-d9-aa-2d	1	Blocked	1970-01-01T09:25:21+09:00	85
70-5d-cc-f2-65-66	1	Forwarding	1970-01-01T09:20:21+09:00	-
00-21-6d-00-05-e3	1	Forwarding	1970-01-01T09:20:21+09:00	-
00-12-6d-00-06-04	1	Forwarding	1970-01-01T09:20:21+09:00	-
64-e5-99-68-23-98	1	Forwarding	1970-01-01T09:20:21+09:00	-

CLI 확인 예시

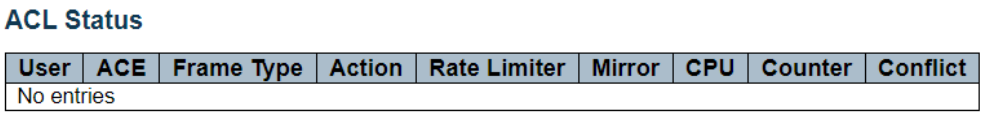
✓ **Port Security Switch Status**

```
# show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security port interface GigabitEthernet 1/1

GigabitEthernet 1/1
-------------------
MAC Address        VID   State       Added                    Age/Hold Time
-----------------  ----  ----------  -------------------------  -------------
58-86-94-f7-2f-79     1  Blocked     1970-01-01T09:30:21+09:00          171
70-5d-cc-f2-65-66     1  Forwarding  1970-01-01T09:20:21+09:00          N/A
00-21-6d-00-05-e3     1  Forwarding  1970-01-01T09:20:21+09:00          N/A
00-12-6d-00-06-04     1  Forwarding  1970-01-01T09:20:21+09:00          N/A
64-e5-99-68-23-98     1  Forwarding  1970-01-01T09:20:21+09:00          N/A
```

6.5.5.2. ACL Status

웹메뉴 Monitor>Security>Network>ACL Status

이 페이지는 다른 ACL 사용자별로 ACL 상태를 보여줍니다. 각 행은 정의된 ACE(액세스 제어 항목)를 설명합니다. 하드웨어 제한으로 인해 특정 ACE 가 하드웨어에 적용되지 않는 경우 충돌이 발생합니다. 각 스위치마다 최대 ACE 수는 512 개입니다.


ACL Status

User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
No entries								

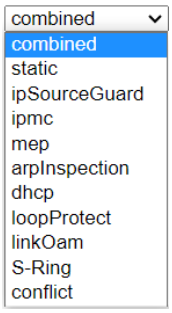
ACL Status

용어	설명
User	ACL 사용자를 나타냅니다.
ACE	로컬 스위치에서의 ACE ID 를 나타냅니다.
Frame Type	ACE 의 프레임 유형을 나타냅니다. **Any** ACE는 모든 프레임 유형과 매칭됩니다. **EType** ACE는 이더넷 타입 프레임과 매칭됩니다. 이더넷 타입 기반 ACE 는 IP와 ARP 프레임과 매칭되지 않습니다. **ARP** ACE는 ARP/RARP 프레임과 매칭됩니다. **IPv4** ACE는 모든 IPv4 프레임과 매칭됩니다. **IPv4/ICMP** ACE는 ICMP 프로토콜을 사용하는 IPv4 프레임과 매칭됩니다. **IPv4/UDP** ACE는 UDP 프로토콜을 사용하는 IPv4 프레임과 매칭됩니다. **IPv4/TCP** ACE는 TCP 프로토콜을 사용하는 IPv4 프레임과 매칭됩니다. **IPv4/Other** ACE는 ICMP/UDP/TCP가 아닌 IPv4 프레임과 매칭됩니다. **IPv6** ACE는 모든 IPv6 표준 프레임과 매칭됩니다.
Action	ACE 의 전달 동작을 나타냅니다. **Permit** ACE와 매칭되는 프레임은 전달되고 학습될 수 있습니다. **Deny** ACE와 매칭되는 프레임은 드롭됩니다. **Filter** ACE와 매칭되는 프레임은 필터링됩니다.
Rate Limiter	ACE 의 속도 제한기 번호를 나타냅니다. 범위는 1 부터 16 까지입니다. "Disabled"가 표시되면 속도 제한기 동작이 비활성화된 것입니다.
CPU	특정 ACE 와 매칭되는 패킷을 CPU 로 전달합니다.
Counter	카운터는 ACE 와 프레임이 몇 번 매칭되었는지를 나타냅니다.
Conflict	특정 ACE 의 하드웨어 상태를 나타냅니다. 하드웨어 제한으로 인해 특정 ACE 가 하드웨어에 적용되지 않습니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.



: 상자를 선택하여 ACL를 선택합니다.

WEB 확인 예시

✓ ACL Status

웹메뉴 Monitor>Security>Network>ACL Status

ACL Status

User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
static	1	EType	Deny	Disabled	Disabled	No	4	No

CLI 확인 예시

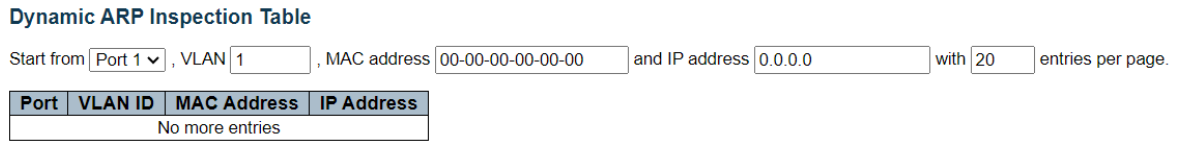
✓ ACL Status

```
# show access-list ace-status [ static ] [ link-oam ] [ loop-protect ] [ dhcp ] [ arp-inspection ] [ mep ] [ ipmc ] [ ip-source-guard ] [ conflicts ]
#  show access-list ace-status

User
----
S    : static
IPSG: ipSourceGuard
IPMC: ipmc
MEP : mep
ARPI: arpInspection
DHCP: dhcp
LOOP: loopProtect
LOAM: linkOam
?    : S-Ring
User ID   Frame   Action Rate L.  Mirror    CPU     Counter Conflict
---- --   -----   ------ -------- --------- ------ -------- --------
S    1    EType   Deny   Disabled Disabled  No           29 No
Switch 1 access-list ace number: 1
```

6.5.5.3. ARP Inspection

웹메뉴 Monitor>Security>Network>ARP Inspection

동적 ARP 인스펙션 테이블의 항목은 이 페이지에 표시됩니다. 동적 ARP 인스펙션 테이블은 최대 256 개의 항목을 포함하며, 먼저 포트로 정렬되고, 다음으로 VLAN ID 로 정렬되며, 그 다음으로 MAC 주소로 정렬되며, 마지막으로 IP 주소로 정렬됩니다. 모든 동적 항목은 DHCP Snooping 으로부터 학습됩니다.



Dynamic ARP Inspection Table

용어	설명
Port	표시된 항목의 스위치 포트 번호
VLAN ID	ARP 트래픽이 허용된 VLAN-ID
MAC Address	해당 항목의 사용자 MAC 주소
IP Address	해당 항목의 사용자 IP 주소

Buttons

Auto-refresh : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh: 클릭 시 페이지를 새로 고침.

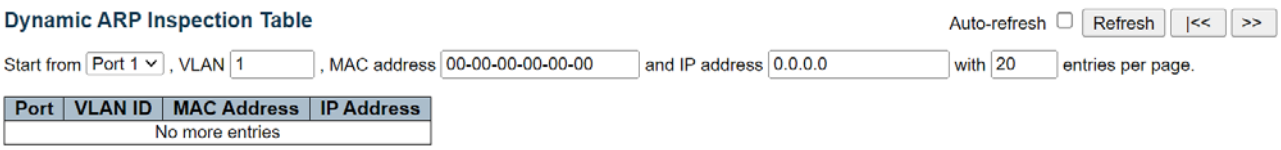
Clear: 모든 정적 항목을 지웁니다.

|<<: 현재 표시되는 마지막 항목에 종료. 시스템 로그 항목을 업데이트 합니다.

>>: 현재 표시되는 마지막 항목에서 시작하여, 시스템 로그 항목을 업데이트 합니다.

WEB 확인 예시

웹메뉴 Monitor>Security>Network>ARP Inspection



CLI 확인 예시

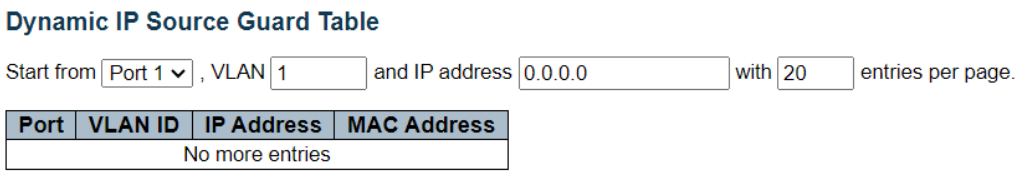
✓ **Dynamic IP Source Guard Table**

```
# show ip arp inspection entry
```

6.5.5.4. IP Source Guard

웹메뉴 Monitor>Security>Network>IP Source Guard

이 페이지에는 동적 IP 출발지 가드 테이블의 항목들이 표시됩니다. 동적 IP 출발지 가드 테이블은 먼저 포트로 정렬되고, 그 다음 VLAN ID 로, 그 다음 IP 주소로, 그리고 마지막으로 MAC 주소로 정렬됩니다.



Dynamic IP Source Guard Table

용어	설명
Port	표시된 항목의 스위치 포트 번호
VLAN ID	IP 트래픽이 허용된 VLAN-ID
MAC Address	해당 항목의 사용자 IP 주소
IP Address	출발지 MAC 주소

Buttons

Auto-refresh : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh: 클릭 시 페이지를 새로 고침.

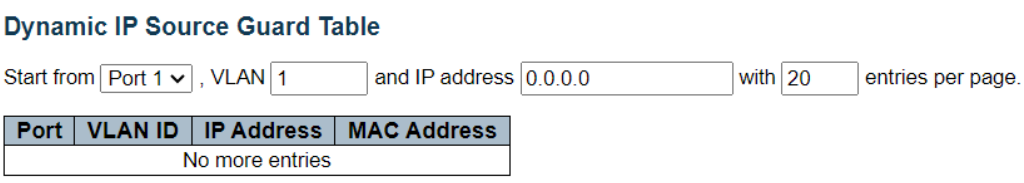
Clear: 모든 동적 항목을 지웁니다.

<<: 현재 표시되는 마지막 항목에 종료. 시스템 로그 항목을 업데이트 합니다.

>>: 현재 표시되는 마지막 항목에서 시작하여, 시스템 로그 항목을 업데이트 합니다.

WEB 확인 예시

웹메뉴 Monitor>Security>Network>IP Source Guard



CLI 확인 예시

✓ **Dynamic IP Source Guard Table**

```
# show ip source binding
```

6.5.6. AAA Monitor

6.5.6.1. RADIUS Overview

웹메뉴 Monitor>Security>AAA>RADIUS Overview

이 페이지는 인증 구성 페이지에서 구성 가능한 RADIUS 서버의 상태에 대한 개요를 제공합니다.

RADIUS Server Status Overview

#	IP Address	Authentication Port	Authentication Status
1			Disabled
2			Disabled
3			Disabled
4			Disabled
5			Disabled

RADIUS Server Status Overview

용어	설명
#	RADIUS 서버 번호입니다. 클릭 시 서버에 대한 상세 통계로 이동합니다.
IP Address	이 서버의 IP 주소입니다.
Authentication Port	인증에 사용되는 UDP 포트 번호입니다.
Authentication Status	서버의 현재 상태입니다. **Disabled** 서버가 비활성화되었습니다. **Not Ready** 서버는 활성화되어 있지만 IP 통신은 아직 작동 중이 아닙니다. **Ready** 서버가 활성화되어 있으며, IP 통신이 작동 중이며, RADIUS 모듈이 액세스 시도를 받을 준비가 되어 있습니다. **Dead (X Seconds left)** 이 서버로 액세스 시도가 있었지만 구성된 시간 초과 내에 응답하지 않았습니다. 서버는 일시적으로 비활성화되었지만, 대기 시간이 만료되면 다시 활성화됩니다. 이러한 상태는 여러 개의 서버가 활성화된 경우에만 발생할 수 있습니다. 괄호 안에는 이 상태가 발생하기까지 남은 시간(초)이 표시됩니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

6.5.6.2. RADIUS Details

웹메뉴 Monitor>Security>AAA>RADIUS Details

이 페이지는 특정 RADIUS 서버에 대한 상세 통계를 제공합니다.

RADIUS Authentication Statistics for Server #1

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address			
State			Disabled
Round-Trip Time			0 ms

RADIUS Server Status Overview

용어	설명
RADIUS Authentication Statistics	이 통계는 RFC4668 - RADIUS 인증 클라이언트 MIB 에서 지정된 내용과 밀접한 관련이 있습니다. 백엔드 서버 사이를 전환하려면 서버 선택 상자를 사용하여 세부 정보를 표시하십시오.
Packet Counters	RADIUS 인증 서버 패킷 카운터입니다. 수신용 카운터는 7 개이고 송신용 카운터는 4 개입니다. **Access Accepts** 서버로부터 수신된 RADIUS Access-Accept 패킷(유효하거나 유효하지 않은)의 개수입니다. **Access Rejects** 서버로부터 수신된 RADIUS Access-Reject 패킷(유효하거나 유효하지 않은)의 개수입니다. **Access Challenges** 서버로부터 수신된 RADIUS Access-Challenge 패킷(유효하거나 유효하지 않은)의 개수입니다. **Malformed Access Responses** 서버로부터 수신된 잘못된 형식의 RADIUS Access-Response 패킷의 개수입니다. 잘못된 패킷에는 유효하지 않은 길이를 가진 패킷이 포함됩니다. 잘못된 액세스 응답으로 인한 부적절한 인증자 또는 메시지 인증자 속성 또는 알 수 없는 유형은 잘못된 형식의 액세스 응답으로 포함되지 않습니다. **Bad Authenticators** 서버로부터 수신된 유효하지 않은 인증자나 메시지 인증자 속성을 포함한 RADIUS Access-Response 패킷의 개수입니다. **Unknown Types** 인증 포트에서 서버로부터 수신된 알 수 없는 유형의 RADIUS 패킷 및 해당 패킷이 삭제된 개수입니다. **Packets Dropped** 인증 포트에서 서버로부터 수신된 RADIUS 패킷 중 다른 이유로 인해 삭제된 패킷의 개수입니다. **Access Requests** 서버로 전송된 RADIUS Access-Request 패킷의 개수입니다. 이는 재전송을 포함하지 않습니다. **Access Retransmissions** RADIUS 인증 서버로 재전송된 RADIUS Access-Request 패킷의 개수입니다. **Pending Requests** 아직 시간 초과되지 않거나 응답을 받지 못한 서버로 향하는 RADIUS Access-Request 패킷의 개수입니다. 이 변수는 Access-Request가 전

		송되면 증가하고, Access-Accept, Access-Reject, Access-Challenge, 시간 초과 또는 재전송으로 인해 감소합니다.
	Timeouts	서버로의 인증 시간 초과 횟수입니다. 시간 초과 후, 클라이언트는 동일한 서버로 재시도하거나 다른 서버로 전송하거나 포기할 수 있습니다. 동일한 서버로의 재시도는 재전송과 시간 초과로 간주됩니다. 다른 서버로의 전송은 요청(Request)과 시간 초과로 간주됩니다.
Other Info	이 섹션에는 서버의 상태와 최신 왕복 시간에 대한 정보가 포함되어 있습니다.	
	IP Address	인증 서버의 IP 주소와 UDP 포트입니다.
	State	서버로부터 수신된 RADIUS Access-Reject 패킷(유효하거나 유효하지 않은)의 개수입니다.
	Round-Trip Time	서버로부터 수신된 RADIUS Access-Challenge 패킷(유효하거나 유효하지 않은)의 개수입니다.

Buttons

Auto-refresh : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh: 클릭 시 페이지를 새로 고침.

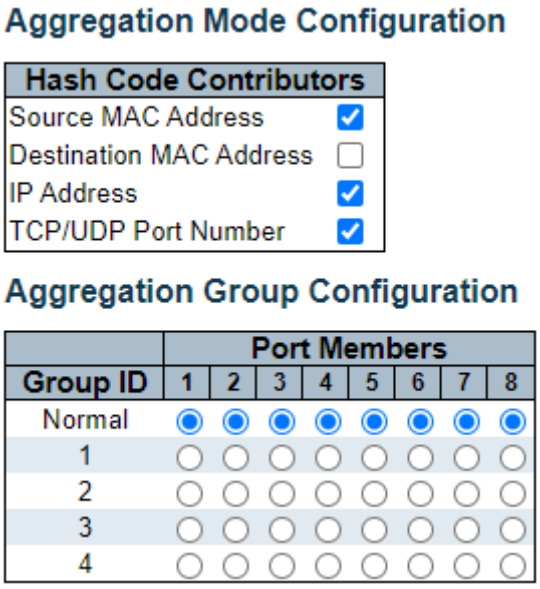
Clear: 선택한 서버의 카운터를 Clear합니다. "대기중인 요청" 카운터는 이 작업에 의해 삭제되지 않습니다.

6.6. Aggregation

6.6.1. Static Configuration

웹메뉴 Configuration>Aggregation>Static

이 페이지는 Aggregation hash mode 와 Aggregation group 을 설정하는 데 사용됩니다.



Aggregation Mode Configuration

Hash Code Contributors

용어	설명
Source MAC Address	Source MAC Address 를 사용하여 프레임의 Destination port 를 계산할 수 있습니다. Source MAC 주소 사용을 활성화하려면 Check 하십시오. Source MAC 주소는 기본적으로 Check 되어 있습니다.
Destination MAC Address	Destination MAC 주소를 사용하여 프레임의 Destination port 를 계산할 수 있습니다. Destination MAC 주소 사용을 활성화하려면 Check 하십시오. Destination MAC 주소는 기본적으로 Uncheck 되어 있습니다.
IP Address	IP Address 를 사용하여 프레임의 Destination port 를 계산할 수 있습니다. IP Address 사용을 활성화하려면 Check 하십시오. IP 주소는 기본적으로 Check 되어 있습니다.
TCP/UDP Port Number	TCP/UDP 포트 번호를 사용하여 프레임의 Destination port 를 계산할 수 있습니다. TCP/UDP 포트 번호 사용을 활성화하려면 Check 하십시오. TCP/UDP 포트 번호는 기본적으로 활성화되어 있습니다.

Aggregation Group Configuration

용어	설명
Group ID	동일한 행에 포함된 설정에 대한 그룹 ID 를 나타냅니다. 그룹 ID "Normal"은 집계가 없음을 나타냅니다. 포트 당 유효한 그룹 ID 는 하나뿐입니다.

Port Members	각 스위치 포트는 각 그룹 ID 에 대해 나열됩니다. 집계에 포트를 포함하려면 라디오 버튼을 선택하고, 포트를 집계에서 제거하려면 라디오 버튼을 선택 해제하십시오. 기본적으로 어떤 포트도 집계 그룹에 속하지 않습니다. 집계에 참여할 수 있는 포트는 전이중(full duplex) 포트뿐이며, 포트는 각 그룹에서 동일한 속도여야 합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>Aggregation>Static

✓ **Aggregation Mode Configuration**

➢ ***Hash Code Contributors***

- ***Source MAC Address(Check)***
- ***Destination MAC Address(Uncheck)***
- ***IP Address(Check)***
- ***TCP/UDP Port Number(Check)***

Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	☑
Destination MAC Address	☐
IP Address	☑
TCP/UDP Port Number	☑

✓ **Aggregation Group Configuration**

➢ ***Group ID***

➢ ***Port Members***

Aggregation Group Configuration

	Port Members							
Group ID	1	2	3	4	5	6	7	8
Normal	○	○	○	○	◉	◉	◉	◉
1	◉	◉	○	○	○	○	○	○
2	○	○	◉	◉	○	○	○	○
3	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○

CLI 설정 예시

✓ Aggregation Mode Configuration

➢ *Hash Code Contributors*

- ***Source MAC Address(Check)***
- ***Destination MAC Address(Uncheck)***
- ***IP Address(Check)***
- ***TCP/UDP Port Number(Check)***

```
(config)# aggregation mode { [ smac ] [ dmac ] [ ip ] [ port ] }*1
(config)# aggregation mode smac ip port
```

✓ Aggregation Group Configuration

➢ *Group ID*

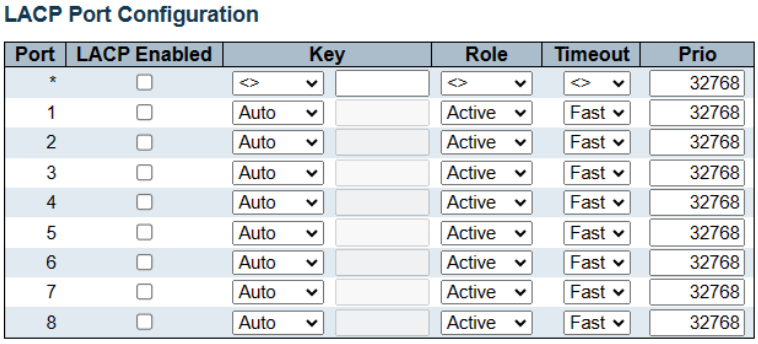
➢ *Port Members*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1-2
(config)# interface GigabitEthernet 1/3-4

(config-if)# aggregation group <v_uint>
(config-if)# aggregation group 1
(config-if)# aggregation group 2
```

6.6.2. LACP Configuration

웹메뉴 Configuration>Aggregation>LACP

이 페이지에서는 사용자가 현재 LACP 포트 구성을 검토하고 변경할 수 있습니다.



LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
1	☐	Auto		Active	Fast	32768
2	☐	Auto		Active	Fast	32768
3	☐	Auto		Active	Fast	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768
6	☐	Auto		Active	Fast	32768
7	☐	Auto		Active	Fast	32768
8	☐	Auto		Active	Fast	32768

LACP Port Configuration

용어	설명
Port	스위치 포트 번호.
LACP Enabled	이 스위치 포트에서 LACP 가 활성화되는지 여부를 제어합니다. 동일한 파트너에 2 개 이상의 포트가 연결되면 LACP 는 집합을 형성합니다.
Key	포트에서 발생하는 키 값은 범위가 1 에서 65535 입니다. 자동 설정은 물리적 링크 속도에 따라 적절한 키를 설정합니다. 예를 들어, 10Mb 의 경우 1, 100Mb 의 경우 2, 1Gb 의 경우 3 입니다. 특정 설정을 사용하여 사용자가 정의한 값으로 입력할 수 있습니다. 동일한 키 값을 갖는 포트는 동일한 집합 그룹에 참여할 수 있지만, 다른 키 값을 갖는 포트는 참여할 수 없습니다.
Role	Role 은 LACP 동작 상태를 보여줍니다. Active" 상태는 매초마다 LACP 패킷을 전송하며, Passive 상태는 파트너로부터 LACP 패킷을 기다립니다. (LACP 패킷을 받았을 때만 채널링이 가능합니다.)
Timeout	타임아웃은 BPDU 전송 간의 기간을 제어합니다. "Fast" 설정은 매초마다 LACP 패킷을 전송하며, "Slow" 설정은 LACP 패킷을 전송하기 전에 30 초를 기다립니다.
Prio	"Prio"는 포트의 우선 순위를 제어합니다. 범위는 1 에서 65535 까지입니다. LACP 파트너가 이 장치에서 지원하는 것보다 큰 그룹을 형성하려는 경우에는 이 매개 변수가 활성 포트와 백업 역할 포트를 제어합니다. 낮은 숫자가 더 높은 우선 순위를 의미합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>Aggregation>LACP

✓ LACP Port Configuration

➢ *LACP Enable*

- ***Enable(1~2 Port)***

LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
1	☑	Auto		Active	Fast	32768
2	☑	Auto		Active	Fast	32768
3	☐	Auto		Active	Fast	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768
6	☐	Auto		Active	Fast	32768
7	☐	Auto		Active	Fast	32768
8	☐	Auto		Active	Fast	32768

➢ *Key*

- ***Auto | Specific(1~65535)***

LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
1	☑	Auto		Active	Fast	32768
2	☑	Auto		Active	Fast	32768
3	☐	Specific		Active	Fast	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768
6	☐	Auto		Active	Fast	32768
7	☐	Auto		Active	Fast	32768
8	☐	Auto		Active	Fast	32768

LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
1	☑	Specific	65535	Active	Fast	32768
2	☑	Specific	65535	Active	Fast	32768
3	☐	Auto		Active	Fast	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768
6	☐	Auto		Active	Fast	32768
7	☐	Auto		Active	Fast	32768
8	☐	Auto		Active	Fast	32768

➢ ***Role***

- ***Active | Passive***

LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
1	☑	Specific	65535	Active	Fast	32768
2	☑	Specific	65535	Passive	Fast	32768
3	☐	Auto		Active	Fast	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768
6	☐	Auto		Active	Fast	32768
7	☐	Auto		Active	Fast	32768
8	☐	Auto		Active	Fast	32768

➢ ***Timeout***

- ***Fast | Slow***

LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
1	☑	Specific	65535	Active	Fast	32768
2	☑	Specific	65535	Active	Fast	32768
3	☐	Auto		Active	Slow	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768
6	☐	Auto		Active	Fast	32768
7	☐	Auto		Active	Fast	32768
8	☐	Auto		Active	Fast	32768

➢ ***Prio***

- ***1~65535***

LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Prio
*	☑	<>	65535	<>	<>	1
1	☑	Specific	65535	Active	Fast	1
2	☑	Specific	65535	Active	Fast	65535
3	☐	Auto		Active	Fast	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768
6	☐	Auto		Active	Fast	32768
7	☐	Auto		Active	Fast	32768
8	☐	Auto		Active	Fast	32768

CLI 설정 예시

✓ LACP Port Configuration

➢ *LACP Enable*

- ***Enable(1~2 Port)***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1-2

(config-if)# lacp
```

➢ *Key*

- ***Auto | Specific(1~65535)***

```
(config-if)# lacp key { <v_1_to_65535> | auto }
(config-if)# lacp key auto
(config-if)# lacp key 65535
```

➢ *Role*

- ***Active | Passive***

```
(config-if)# lacp role { active | passive }
(config-if)# lacp role active
(config-if)# lacp role passive
```

➢ *Timeout*

- ***Fast | Slow***

```
(config-if)# lacp timeout { fast | slow }
(config-if)# lacp timeout fast
(config-if)# lacp timeout slow
```

➢ *Prio*

- ***1~65535***

```
(config-if)# lacp port-priority <v_1_to_65535>
(config-if)# lacp port-priority 1
(config-if)# lacp port-priority 65535
```

6.6.3. Static Monitor

웹메뉴 Monitor>Aggregation>Static

이 페이지에서는 Aggregation group 내 포트의 상태를 확인하는 데 사용됩니다.

Aggregation Status

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports
No aggregation groups					

Aggregation Status

용어	설명
Aggr ID	이 Aggregation 인스턴스와 관련된 Aggregation ID 입니다.
Name	Aggregation group ID 의 이름입니다.
Type	Aggregation group 의 유형(Static 또는 LACP)입니다.
Speed	Aggregation group 의 속도입니다.
Configured ports	집합 그룹의 구성된 구성원 포트입니다.
Aggregated ports	"Prio"는 포트의 우선 순위를 제어합니다. 범위는 1 에서 65535 까지입니다. LACP 파트너가 이 장치에서 지원하는 것보다 큰 그룹을 형성하려는 경우에는 이 매개 변수가 활성 포트와 백업 역할 포트를 제어합니다. 낮은 숫자가 더 높은 우선 순위를 의미합니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

WEB 확인 예시

웹메뉴 Monitor>Aggregation>Static

Aggregation Status

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports
1	LLAG1	Static	1G	GigabitEthernet 1/1-2	none
2	LLAG2	Static	Undefined	GigabitEthernet 1/3-4	none

CLI 확인 예시

✓ **Aggregation Status**

```
# show aggregation
# Aggr ID  Name    Type    Speed  Configured Ports    Aggregated Ports
-------  ------  ------  -------  ------------------------------------------------------------
  1       LLAG1   Static   1G          GigabitEthernet 1/1-2     none
  2       LLAG2   Static   Undefined   GigabitEthernet 1/3-4     none
```

6.6.4. LACP Monitor

6.6.4.1. System Status

웹메뉴 Monitor>Aggregation>LACP>System Status

이 페이지는 모든 LACP 인스턴스에 대한 상태 개요를 제공합니다.

LACP System Status

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
No ports enabled or no existing partners					

LACP System Status

용어	설명
Aggr ID	이 Aggregation 인스턴스와 관련된 Aggregation ID 입니다. LLAG 의 경우 ID 는 'isid:aggr-id'로 표시되고, GLAG 의 경우 'aggr-id'로 표시됩니다.
Partner System ID	Aggregation 파트너의 시스템 ID (MAC 주소)입니다.
Partner Key	Aggregation ID 에 할당된 파트너의 키입니다.
Partner Prio	Aggregation ID 에 할당된 파트너의 우선순위(priority)입니다.
Last changed	이 Aggregation 이 변경된 이후의 시간입니다.
Local Ports	이 스위치의 이 Aggregation 에 속한 포트를 보여줍니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

WEB 확인 예시

웹메뉴 Monitor>Aggregation>LACP>System Status

LACP System Status

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
LLAG1	00-21-6d-00-00-00	3	32768	0d 00:28:57	1,2

CLI 확인 예시

✓ **LACP System Status**

```
# show lacp neighbor
Aggr ID  Partner System ID  Partner Prio  Partner Key  Last Changed
-------  -----------------  ------------  -----------  ------------
1        00:21:6d:00:00:00  32768         3            00:35:08
Port                State     Key    Aggr ID  Partner Port  Partner Port Prio
------------------  --------  -----  -------  ------------  -----------------
Gi 1/1              enabled   3      1        1             32768
Gi 1/2              enabled   3      1        2             32768
```

6.6.4.2. Port Status

웹메뉴 Monitor>Aggregation>LACP>Port Status

이 페이지는 모든 포트의 LACP 상태에 대한 상태 개요를 제공합니다.

LACP Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-

LACP Status

용어	설명
Port	스위치 포트 번호입니다.
LACP	'Yes'는 LACP 가 활성화되어 있고 포트 링크가 열려 있는 것을 의미합니다. 'No'는 LACP 가 비활성화되어 있거나 포트 링크가 닫혀 있는 것을 의미합니다. 'Backup'은 포트가 Aggregation 그룹에 참여하지 못하지만 다른 포트가 떠나면 참여할 수 있다는 것을 의미합니다. 동시에 LACP 상태는 비활성화되어 있습니다.
Key	이 포트에 할당된 키입니다. 동일한 키를 가진 포트만 Aggregation 할 수 있습니다.
Aggr ID	이 Aggregation 그룹에 할당된 Aggregation ID 입니다.
Partner System ID	Aggregation 파트너의 시스템 ID(맥 주소)입니다.
Partner Port	이 포트에 연결된 파트너의 포트 번호입니다.
Partner Prio	파트너의 포트 우선순위입니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

WEB 확인 예시

웹메뉴 Monitor>Aggregation>LACP>Port Status

LACP Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	Yes	3	LLAG1	00-12-6d-00-06-a9	1	32768
2	Yes	3	LLAG1	00-12-6d-00-06-a9	2	32768
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-

CLI 확인 예시

✓ **LACP Status**

```
# show lacp neighbor
Aggr ID  Partner System ID  Partner Prio  Partner Key  Last Changed
-------  -----------------  ------------  -----------  ------------
1        00:21:6d:00:00:00  32768         3            00:35:08
Port                State     Key    Aggr ID  Partner Port  Partner Port Prio
------------------  --------  -----  -------  ------------  -----------------
Gi 1/1              enabled   3      1        1             32768
Gi 1/2              enabled   3      1        2             32768
```

6.6.4.3. Port Statistics

웹메뉴 Monitor>Aggregation>LACP>Port Statistics

이 페이지는 모든 포트에 대한 LACP 통계 개요를 제공합니다.

LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0

LACP Statistics

용어	설명
Port	스위치 포트 번호입니다.
LACP Received	각 포트에서 수신된 LACP 프레임 수를 보여줍니다.
LACP Transmitted	각 포트에서 보낸 LACP 프레임 수를 보여줍니다.
Discarded	각 포트에서 폐기된 알 수 없거나 불법적인 LACP 프레임의 수를 보여줍니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

Clear : 모든 포트의 카운터를 Clear합니다.

WEB 확인 예시

웹메뉴 Monitor>Aggregation>LACP>Port Statistics

LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	113	113	0	0
2	114	113	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0

CLI 확인 예시

✓ **LACP Statistics**

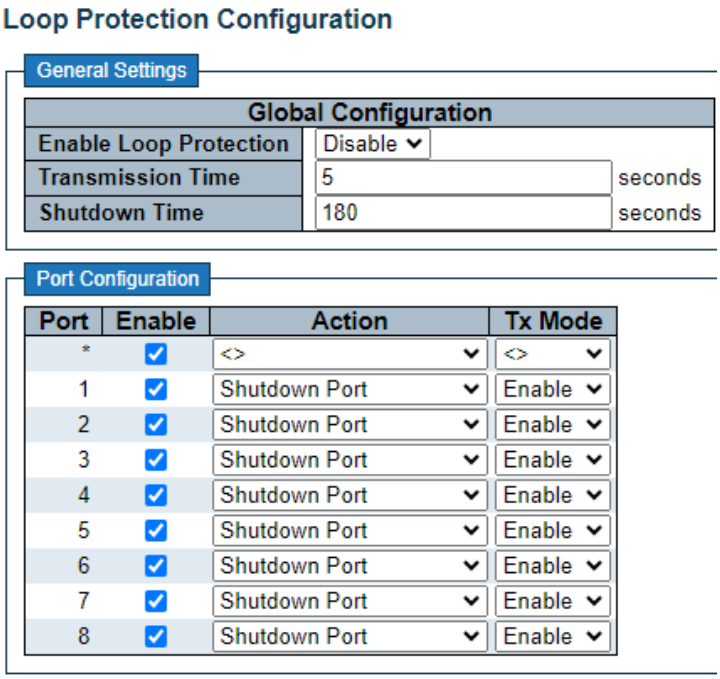
```
# show lacp statistics

Port                Rx Frames   Tx Frames   Rx Unknown   Rx Illegal
------------------- ----------  ----------  ----------   ----------
Gi 1/1              491         491         0            0
Gi 1/2              491         491         0            0
```

6.7. Loop Protection

6.7.1. Loop Protection Configuration

웹메뉴 Configuration>Loop protection

이 페이지에서는 사용자가 현재 Loop Protection 구성을 확인하고 필요한 경우 변경할 수 있습니다.



Loop Protection Configuration

General Settings

Global Configuration

용어	설명
Enable Loop Protection	루프 보호가 전체적으로 활성화되는지를 제어합니다.
Transmission Time	각 포트에서 보내는 각 루프 보호 PDU 사이의 간격입니다. 유효한 값은 1 에서 10 초입니다. 기본값은 5 초입니다.
Shutdown Time	루프가 감지되어 포트 작업이 포트를 종료하는 경우 해당 포트가 비활성화된 상태로 유지되는 기간(초 단위)입니다. 유효한 값은 0 부터 604800 초(7 일)입니다. 값이 0 이면 포트가 비활성화된 상태로 유지됩니다(다음 장치 재시작까지). 기본값은 180 초입니다.

Port Configuration

용어	설명
Port	해당 포트의 스위치 포트 번호입니다.
Enable	이 스위치 포트에서 루프 보호가 활성화되는지를 제어합니다.

Action	포트에서 루프가 감지될 때 수행되는 작업을 구성합니다. 유효한 값은 포트 종료, 포트 종료 및 기록, 기록입니다.
Tx Mode	해당 포트가 루프 보호 PDU 를 활성적으로 생성하는지 또는 루프된 PDU 를 수동으로 찾는지를 제어합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

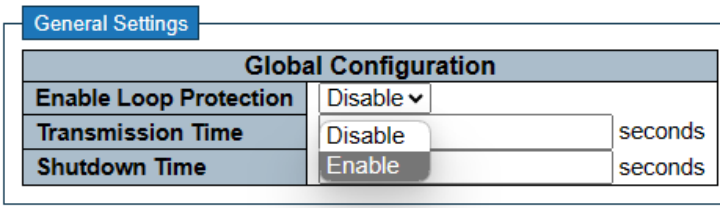
웹메뉴 Configuration>Loop protection

✓ **General Settings**

✓ **Global Configuration**

➢ ***Enable Loop Protection***

- ***Disable | Enable***

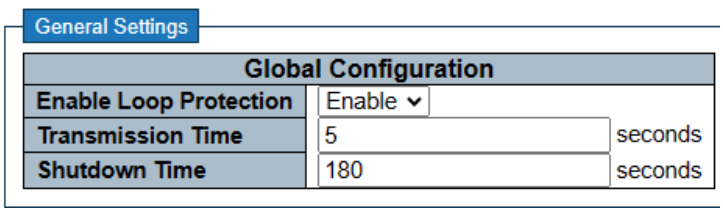


➢ ***Transmission Time***

- ***5sec (1~10)***

➢ ***Shutdown Time***

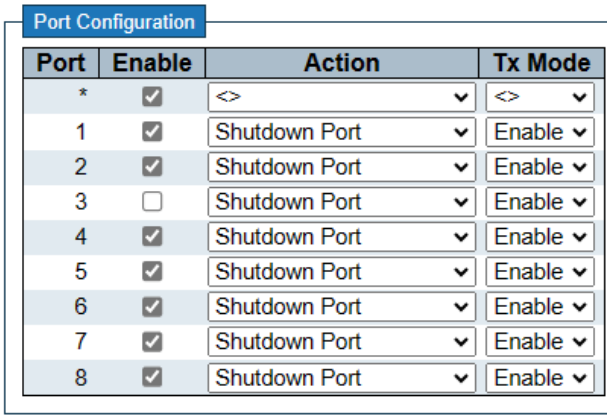
- ***180sec (0~604800)***



✓ Port Configuration

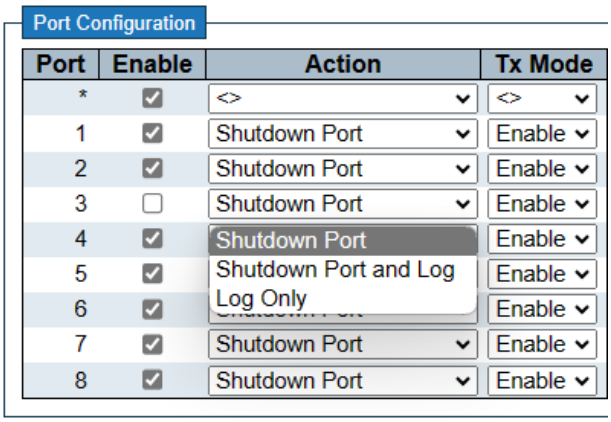
➢ *Enable*

- ***Enable(default) | Disable***



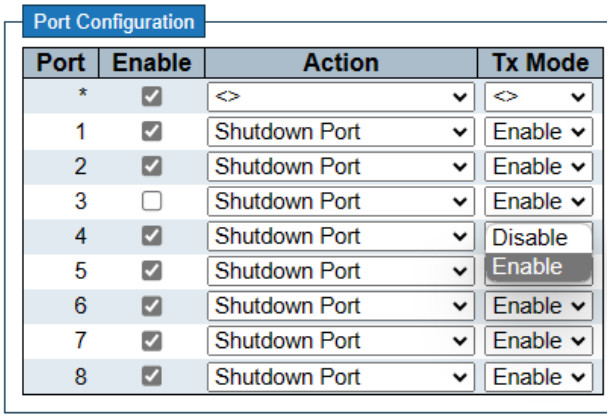
➢ *Action*

- ***Shudown Port(default) | Shutdown Port and Log | Log Only***



➢ *Tx Mode*

- ***Enable(default) | Disable***



CLI 설정 예시

✓ General Settings

✓ Global Configuration

➢ *Enable Loop Protection*

- ***Disable | Enable***

```
(config)# no loop-protect
(config)# loop-protect
```

➢ *Transmission Time*

- ***5sec (1~10)***

```
(config)# loop-protect transmit-time <t>
(config)# loop-protect transmit-time 5
```

➢ *Shutdown Time*

- ***180sec (0~604800)***

```
(config)# loop-protect shutdown-time <t>
(config)# loop-protect shutdown-time 180
```

✓ Port Configuration

➢ *Enable*

- ***Enable(default) | Disable***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/3

(config-if)# loop-protect
(config-if)# no loop-protect
```

➢ *Action*

- ***Shudown Port(default) | Shutdown Port and Log | Log Only***

```
(config-if)# loop-protect action { [ shutdown ] [ log ] }*1
(config-if)# loop-protect action shutdown
(config-if)# loop-protect action shutdown log
(config-if)# loop-protect action log
```

➢ *Tx Mode*

- ***Enable(default) | Disable***

```
(config-if)# loop-protect tx-mode
(config-if)# no loop-protect tx-mode
```

6.7.2. Loop Protection Monitor

웹메뉴 Configuration>Loop Protection

이 페이지는 스위치의 포트별 루프 보호 상태를 표시합니다.

Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Up	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Up	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-

Loop Protection Status

용어	설명
Port	논리 포트의 스위치 포트 번호입니다.
Action	현재 구성된 포트 동작입니다.
Transmit	현재 구성된 포트 전송 모드입니다.
Loops	이 포트에서 감지된 루프의 수입니다.
Status	해당 포트의 현재 루프 보호 상태입니다.
Loop	현재 해당 포트에서 루프가 감지되었는지 여부입니다.
Time of Last Loop	마지막 루프 이벤트가 감지된 시간입니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

WEB 확인 예시

웹메뉴 Monitor>Loop Protection

Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	5	Down	-	1970-01-07T14:20:22+09:00
2	Shutdown	Enabled	17	Down	-	1970-01-07T14:17:30+09:00
3	Shutdown	Enabled	11	Up	-	1970-01-07T14:22:55+09:00
4	Shutdown	Enabled	4	Down	-	1970-01-07T14:14:20+09:00
5	Shutdown	Enabled	1	Down	-	1970-01-07T14:15:43+09:00
6	Shutdown	Enabled	1	Down	-	1970-01-07T14:18:41+09:00
7	Shutdown	Enabled	2	Down	-	1970-01-07T14:20:07+09:00
8	Shutdown	Enabled	3	Down	-	1970-01-07T14:19:49+09:00

CLI 확인 예시

✓ Loop Protection Status

```
# show loop-protect interface *
Loop Protection Configuration
=====================================
Loop Protection    : Enable
Transmission Time : 5 sec
Shutdown Time      : 180 sec


GigabitEthernet 1/1
------------------------------
    Loop protect mode is enabled.
    Action is shutdown.
    Transmit mode is enabled.
    No loop.
    The number of loops is 5.
    Time of last loop is at 1970-01-07T14:20:22+09:00
    Status is down.


GigabitEthernet 1/2
------------------------------
    Loop protect mode is enabled.
    Action is shutdown.
    Transmit mode is enabled.
    No loop.
    The number of loops is 17.
    Time of last loop is at 1970-01-07T14:17:30+09:00
    Status is down.

......
```

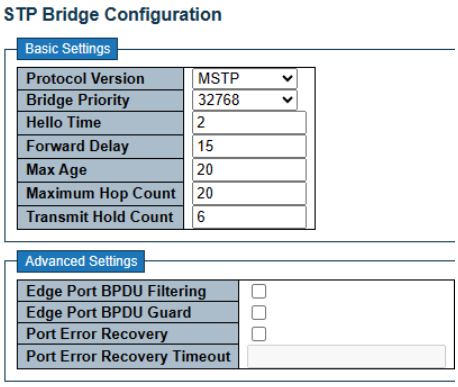
6.8. Spanning Tree

6.8.1. Spanning Tree Configuration

6.8.1.1. Bridge Setting

웹메뉴 Configuration>Spanning Tree>Bridge Setting

이 페이지를 통해 STP(Spanning Tree Protocol) 시스템 설정을 구성할 수 있습니다.
이 설정은 스위치의 모든 STP 브리지 인스턴스에서 사용됩니다.



STP Bridge Configuration

Basic Settings

용어	설명
Protocol Version	MSTP / RSTP / STP 프로토콜 버전 설정합니다. (유효한 값은 STP, RSTP 과 MSTP)
Bridge Priority	브리지 우선순위를 제어합니다. 낮은 숫자 값일수록 우선순위가 더 좋습니다. 브리지 우선순위에 MSTI 인스턴스 번호를 더하고, 스위치의 6 바이트 MAC 주소와 연결하여 브리지 식별자를 형성합니다. MSTP 동작에서는 이것은 CIST(Cumulative Spanning Tree)의 우선순위입니다. 그렇지 않으면 STP/RSTP 브리지의 우선순위입니다.
Hello Time	STP BPDU 를 전송하는 간격입니다. 유효한 값은 1 초에서 10 초 사이이며, 기본값은 2 초입니다. 참고: 기본값에서 이 매개변수를 변경하는 것은 권장되지 않으며, 네트워크에 부정적인 영향을 미칠 수 있습니다.
Forward Delay	STP 브리지가 루트 및 지정 포트를 포워딩으로 전환하는 데 사용하는 지연 시간입니다(STP 호환 모드에서 사용). 유효한 값은 4 초에서 30 초 사이입니다.
Max Age	루트 브리지일 때 브리지가 전송하는 정보의 최대 유지 시간입니다. 유효한 값은 6 초에서 40 초 사이이며, MaxAge 는 (FwdDelay-1)*2 이하여야 합니다.
Maximum Hop Count	이는 MSTI 영역의 경계에서 생성된 MSTI 정보의 남은 홉(initial value)을 정의합니다. 이는 루트 브리지가 BPDU 정보를 배포할 수 있는 브리지 수를 정의합니다. 유효한 값은 6 에서 40 홉 사이입니다.

Transmit Hold Count	한 브리지 포트가 초당 전송할 수 있는 BPDU(Bridge Protocol Data Unit)의 개수입니다. 초과되면 다음 BPDU 의 전송이 지연됩니다. 유효한 값은 초당 1 에서 10 개의 BPDU 입니다.

Advanced Settings

용어	설명
Edge Port BPDU Filtering	Edge 로 명시적으로 구성된 포트가 BPDU 를 전송하고 수신할지 여부를 제어합니다.
Edge Port BPDU Guard	Edge 로 명시적으로 구성된 포트가 BPDU 를 수신하면 자체적으로 비활성화될지 여부를 제어합니다. 해당 포트는 오류 비활성 상태로 전환되고, 활성 토폴로지에서 제거됩니다.
Port Error Recovery	오류 비활성 상태에 있는 포트가 일정 시간 후에 자동으로 활성화될지 여부를 제어합니다. 복구가 비활성화된 경우, 정상적인 STP 동작을 위해 포트를 비활성화하고 다시 활성화해야 합니다. 이 상태는 시스템 재부팅에 의해도 초기화됩니다.
Port Error Recovery Timeout	오류 비활성 상태에 있는 포트를 활성화할 수 있는 시간입니다. 유효한 값은 30 초부터 86400 초(24 시간)까지 입니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

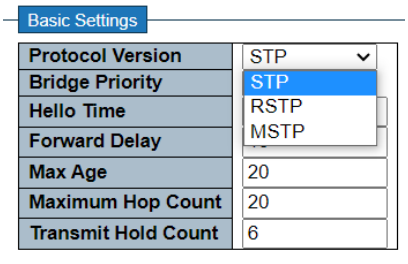
WEB 설정 예시

웹메뉴 Configuration>Spanning Tree>Bridge Setting

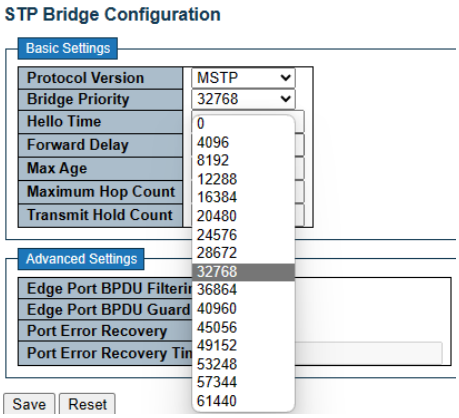
✓ STP Bridge Configuration

➢ *Basic Settings*

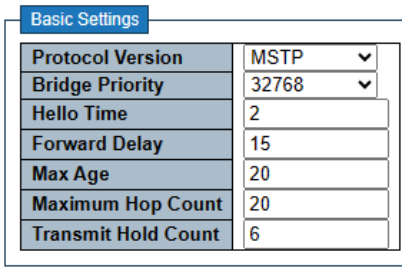
- ***Protocol Version (STP | RSTP | MSTP)***



- ***Bridge Priority (Default 32768)***

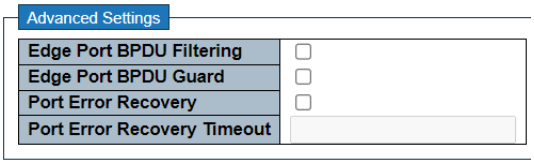


- ***Hello Time(Default 2, 1~10)***
- ***Forward Delay(Default 15, 4~30sec)***
- ***Max Age (Default 20, 6~40sec)***
- ***Maximum Hop Count(Default 20, 6~40sec)***
- ***Transmit Hold Count(Default 6, 1~10sec)***



➢ ***Advanced Settings***

- ***Edge Port BPDU Filtering***
- ***Edge Port BPDU Guard***
- ***Port Error Recovery (30-86400)***



CLI 설정 예시

✓ STP Bridge Configuration

➢ ***Basic Settings***

- ***Protocol Version(STP | RSTP | MSTP)***

```
(config)# spanning-tree mode {stp | rstp | mstp}
(config)# spanning-tree mode stp
```

- ***Bridge Priority(Default 32768)***

```
(config)# spanning-tree mst <instance> priority <prio>
(config)# spanning-tree mst 0 priority 32768
```

- ***Hello Time(Default 2, 1~10)***

```
(config)# spanning-tree mst hello-time <hellotime>
(config)# spanning-tree mst hello-time 2
```

- ***Forward Delay(Default 15, 4~30sec)***

```
(config)# spanning-tree mst forward-time <fwdtime>
(config)# spanning-tree mst forward-time 15
```

- ***Max Age (Default 20, 6~40sec)***

```
(config)# spanning-tree mst max-age <maxage>
(config)# spanning-tree mst max-age 20
```

- ***Maximum Hop Count(Default 20, 6~40sec)***

```
(config)# spanning-tree mst max-hops <maxhops>
(config)# spanning-tree mst max-hops 20
```

- ***Transmit Hold Count(Default 6, 1~10sec)***

```
(config)# spanning-tree transmit hold-count <holdcount>
(config)# spanning-tree transmit hold-count 6
```

➢ ***Advanced Settings***

- ***Edge Port BPDU Filtering***

```
(config)# spanning-tree edge bpdu-filter
```

- ***Edge Port BPDU Guard***

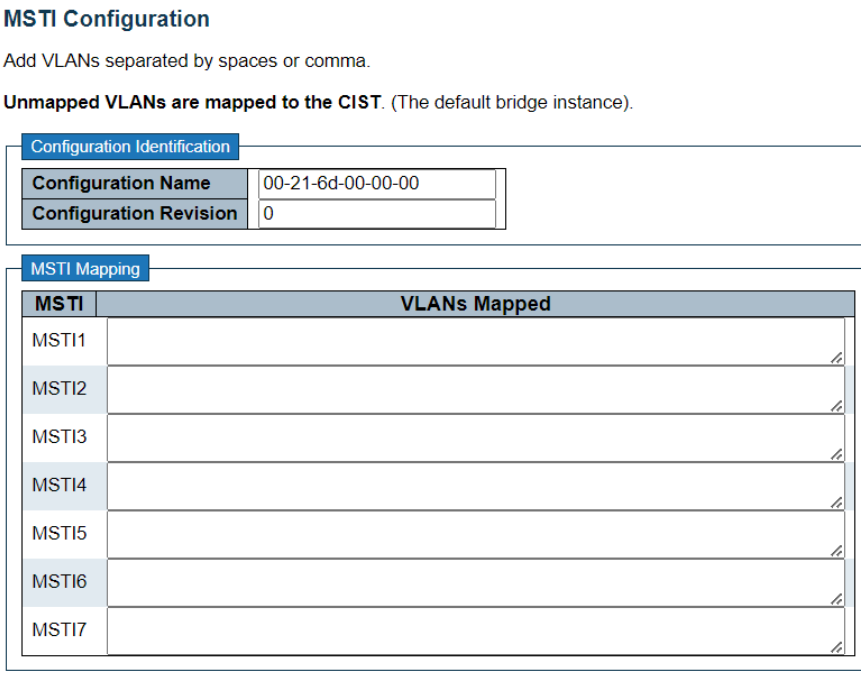
```
(config)# spanning-tree edge bpdu-guard
```

- ***Port Error Recovery (30-86400)***

```
(config)# spanning-tree recovery interval <interval>
```

6.8.1.2. MSTI Mapping

웹메뉴 Configuration>Spanning Tree>MSTI Mapping
이 페이지에서는 현재 STP MSTI 브리지 인스턴스 우선순위 설정을 확인하고 변경할 수 있습니다.



MSTI Configuration

Configuration Identification

용어	설명
Configuration Identification	구성 식별(Configuration Identification)은 MSTP(Multiple Spanning Tree Protocol) 구성의 변경 사항을 식별하는 데 사용되는 값입니다.
Configuration Name	VLAN 에서 MSTI 로의 매핑을 식별하는 이름입니다. 브리지는 MSTI 의 스패닝 트리를 공유하기 위해 이름과 리비전(아래 참조)뿐만 아니라 VLAN-to-MSTI 매핑 구성을 공유해야 합니다. 이 이름은 최대 32 자까지 사용할 수 있습니다.
Configuration Revision	위에서 언급한 MSTI 구성의 리비전입니다. 이 값은 0 과 65535 사이의 정수이어야 합니다.

MSTI Mapping

용어	설명
MSTI Mapping	MSTI Mapping 은 MSTP(Multiple Spanning Tree Protocol)에서 사용되는 VLAN(Virtual LAN)과 MSTI(Multiple Spanning Tree Instance) 간의 매핑을 정의하는 것을 의미합니다.
MSTI	브리지 인스턴스입니다. CIST 는 명시적인 매핑이 불가능하며, 명시적으로 매핑되지 않은 VLAN 을 수신하게 됩니다.
VLANs Mapped	MSTI 에 매핑된 VLAN 목록입니다. VLAN 은 단일 VLAN (1 부터 4094 사이의 값인 xx) 또는 범위 (xx-yy)로 지정할 수 있으며, 각각은 쉼표와/또는 공백으로 구분되어야 합니다. VLAN 은 하나의 MSTI 에만 매핑될 수 있습니다. 사용되지 않는 MSTI 는 비워 두어야 합니다. (즉, 해당 MSTI 에 매핑된 VLAN 이 없는 경우)

Buttons

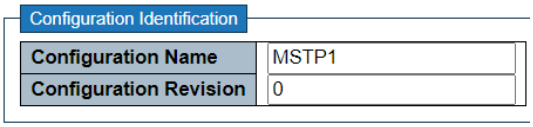
Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

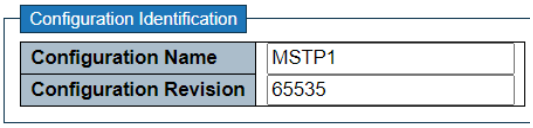
✓ MSTI Configuration

➢ *Configuration Identification*

- ***Configuration Name***

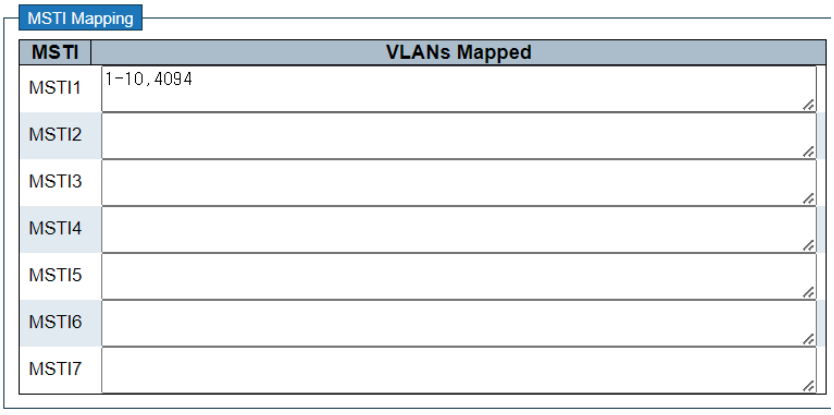


- ***Configuration Revision(0~65535)***



➢ *MSTI Mapping*

- ***VLANs Mapped***



CLI 설정 예시

✓ MSTI Configuration

➢ *Configuration Identification*

- ***Configuration Name | Revision(0~65535)***

```
(config)# spanning-tree mst name <name> revision <v_0_to_65535>
(config)# spanning-tree mst name MSTP1 revision 65535
```

➢ ***MSTI Mapping***

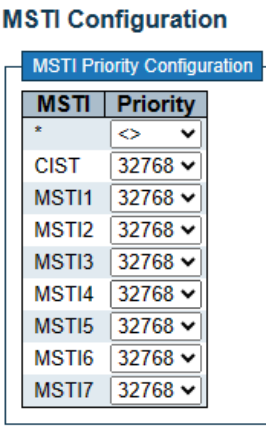
- ***VLANs Mapped***

```
(config)# spanning-tree mst <instance> vlan <v_vlan_list>
(config)# spanning-tree mst 1 vlan 1-10,4094
```

6.8.1.3. MSTI Priorities

웹메뉴 Configuration>Spanning Tree>MSTI Priorities

이 페이지에서는 현재 STP MSTI 브리지 인스턴스 우선순위 설정을 확인하고, 필요한 경우 변경할 수 있습니다.



MSTI Configuration

MSTI Priority Configuration

용어	설명
MSTI	브리지 인스턴스. CIST 는 기본 인스턴스로 항상 활성화되어 있습니다.
Priority	브리지 우선순위를 제어합니다. 숫자가 낮을수록 우선순위가 높습니다. 브리지 우선순위에 MSTI 인스턴스 번호를 더한 후, 스위치의 6 바이트 MAC 주소와 연결하여 브리지 식별자를 형성합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

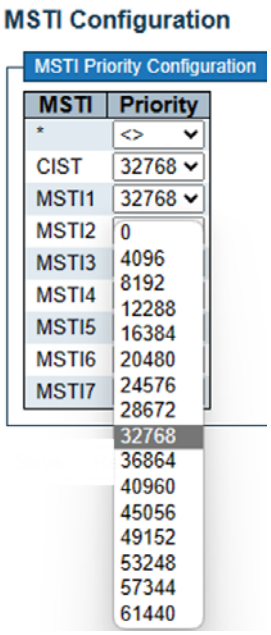
WEB 설정 예시

웹메뉴 Configuration>Spanning Tree>MSTI Priorities

✓ **MSTI Configuration**

➢ ***MSTI Priority Configuration***

- ***MSTI(0-7)***
- ***Priority(Default 32768)***



CLI 설정 예시

✓ MSTI Configuration

➢ ***MSTI Priority Configuration***

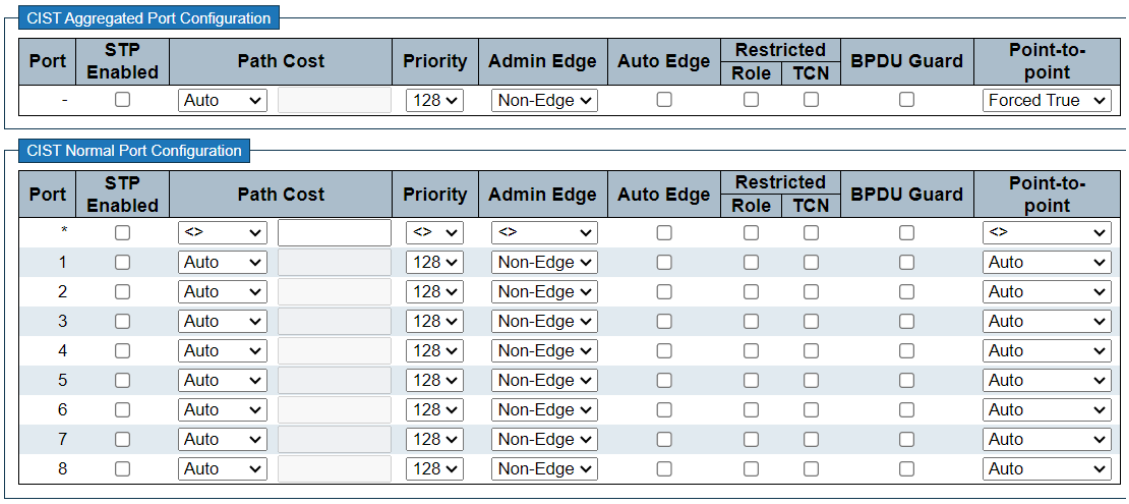
- ***MSTI(0-7)***
- ***Priority(Default 32768)***

```
(config)# spanning-tree mst <instance> priority <prio>
(config)# spanning-tree mst 1 priority 0
(config)# spanning-tree mst 1 priority 61440
```

6.8.1.4. CIST Ports

웹메뉴 Configuration>Spanning Tree>CIST Ports

이 페이지에서는 사용자가 현재 STP CIST 포트 구성을 검토하고 필요에 따라 변경할 수 있습니다.
이 페이지에는 물리적 및 집계된 포트에 대한 설정이 포함되어 있습니다.


CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
-	☐	Auto		128	Non-Edge	☐	☐	☐	☐	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
*	☐	<>		<>	<>	☐	☐	☐	☐	<>
1	☐	Auto		128	Non-Edge	☐	☐	☐	☐	Auto
2	☐	Auto		128	Non-Edge	☐	☐	☐	☐	Auto
3	☐	Auto		128	Non-Edge	☐	☐	☐	☐	Auto
4	☐	Auto		128	Non-Edge	☐	☐	☐	☐	Auto
5	☐	Auto		128	Non-Edge	☐	☐	☐	☐	Auto
6	☐	Auto		128	Non-Edge	☐	☐	☐	☐	Auto
7	☐	Auto		128	Non-Edge	☐	☐	☐	☐	Auto
8	☐	Auto		128	Non-Edge	☐	☐	☐	☐	Auto

STP CIST Port Configuration

CIST Aggregated Port Configuration

CIST Normal Port Configuration

용어	설명
Port	논리적인 STP 포트의 스위치 포트 번호입니다.
STP Enabled	이 스위치 포트에서 STP 를 활성화할지 여부를 제어합니다.
Path Cost	포트에서 발생하는 경로 비용을 제어합니다. Auto 설정은 물리적 링크 속도에 따라 적절한 경로 비용을 설정하며, 802.1D 에서 권장하는 값들을 사용합니다. Specific 설정을 사용하면 사용자가 정의한 값으로 경로 비용을 입력할 수 있습니다. 경로 비용은 네트워크의 활성 토폴로지를 설정할 때 사용됩니다. 경로 비용이 낮은 포트는 경로 비용이 높은 포트보다 전달 포트로 선택됩니다. 유효한 값은 1 에서 200000000 사이입니다.
Priority	포트 우선순위를 제어합니다. 이는 동일한 포트 비용을 가지는 포트의 우선순위를 제어하는 데 사용될 수 있습니다. (위 참조)
operEdge (state flag)	포트가 직접 엣지 장치에 연결되어 있는지를 나타내는 운영 플래그입니다. (브리지가 연결되지 않음). operEdge 가 true 인 엣지 포트는 다른 포트보다 전달 상태로의 전환 속도가 빠릅니다. 이 플래그의 값은 AdminEdge 와 AutoEdge 필드에 기반합니다. 이 플래그는 Monitor->Spanning Tree -> STP Detailed Bridge Status 에서 Edge 로 표시됩니다.
AdminEdge	operEdge 플래그가 설정되거나 해제되어 시작해야 하는지를 제어합니다. (포트가 초기화될 때의 초기 operEdge 상태)
AutoEdge	브리지가 브리지 포트에서 자동 엣지 감지를 활성화해야 하는지를 제어합니다. 이는 포트에서 BPDU 를 수신하는지 여부에 따라 operEdge 를 결정할 수 있게 합니다.

Restricted Role	활성화되면, 포트는 최적의 스패닝 트리 우선순위 벡터를 가지고 있더라도 CIST 또는 MSTI 의 루트 포트로 선택되지 않습니다. 이러한 포트는 루트 포트가 선택된 후에 대체 포트로 선택됩니다. 설정된 경우 스패닝 트리 연결성의 부재를 야기할 수 있습니다. 이는 네트워크 관리자가 네트워크의 핵심 영역 외부의 브리지가 스패닝 트리 활성 토폴로지에 영향을 미치는 것을 방지하기 위해 설정될 수 있습니다. 이 기능은 루트 가드(Root Guard)로도 알려져 있습니다.
Restricted TCN	활성화되면, 포트는 수신된 토폴로지 변경 알림과 토폴로지 변경을 다른 포트로 전파하지 않습니다. 설정된 경우, 지속적으로 잘못된 학습된 스테이션 위치 정보로 인해 스패닝 트리의 활성 토폴로지 변경 후 일시적인 연결 손실이 발생할 수 있습니다. 이는 네트워크 관리자가 네트워크의 핵심 영역 외부의 브리지가 그 영역에서 주소 플러싱을 발생시키지 않도록 설정하기 위해 설정됩니다. 이는 관리자의 완전한 통제가 아니거나 연결된 LAN 의 물리적 링크 상태가 빈번하게 변화하는 경우일 수 있습니다.
BPDU Guard	활성화되면, 유효한 BPDU 를 수신하면 포트 자체를 비활성화 시킵니다. 유사한 브리지 설정과는 달리, 포트 엣지 상태는 이 설정에 영향을 주지 않습니다. 이 설정으로 인해 오류로 인해 오류로 인해 비활성화되는 포트는 브리지 포트 오류 복구 설정에도 영향을 받습니다.
Point-to-Point	포트가 공유 매체가 아닌 포인트 투 포인트 LAN 에 연결되는지를 제어합니다. 이는 자동으로 결정되거나 강제로 true 또는 false 로 설정할 수 있습니다. 포인트 투 포인트 LAN 의 전달 상태로의 전환 속도는 공유 매체보다 빠릅니다.

Buttons

Apply : 클릭 시 변경사항을 적용합니다.
Apply&Save : 클릭 시 변경사항을 적용하고 저장합니다.
Reset : 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

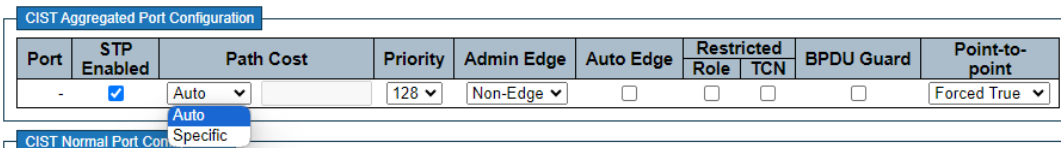
웹메뉴 Configuration>Spanning Tree>CIST Ports

- ✓ **CIST Aggregated Port Configuration**
- ✓ **CIST Normal Port Configuration**
  - ➢ ***STP Enabled***
    - ***Enable | Disable***

CIST Aggregated Port Configuration

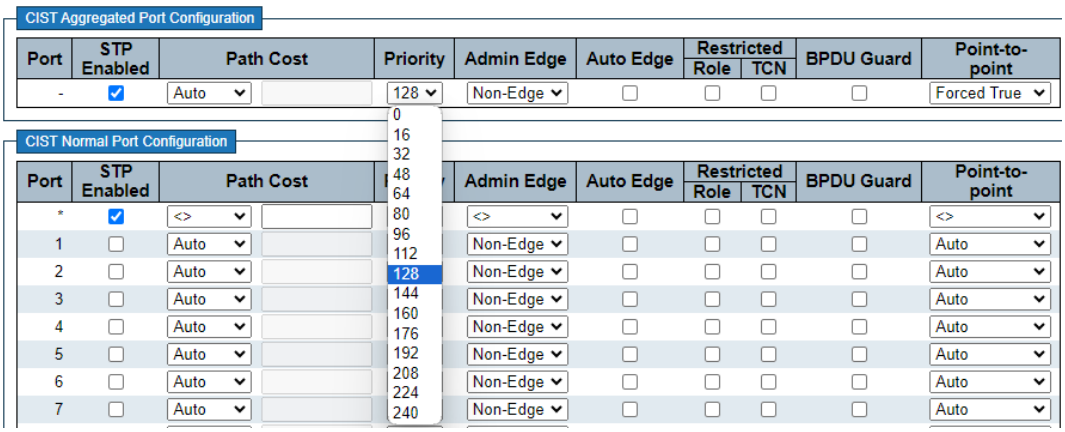
Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
-	☑	Auto		128	Non-Edge	☐	☐	☐	☐	Forced True

  - ➢ ***Path Cost***
    - ***Auto | Specific(1~200,000,000)***



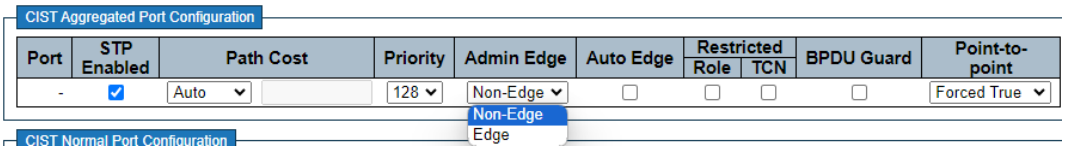
➢ ***Priority***

- ***0|16|32|48|64|80|96|112|128|144|160|176|192|208|224|240***



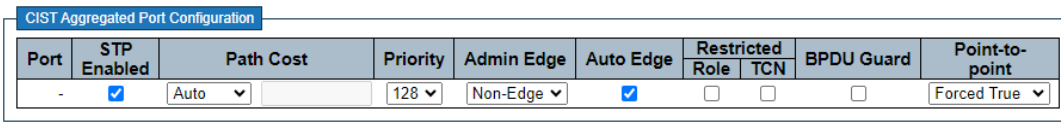
➢ ***Admin Edge***

- ***Non-Edge | Edge***



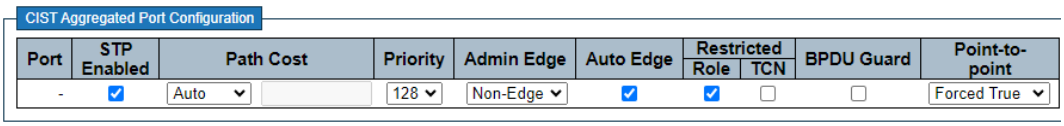
➢ ***Auto Edge***

- ***Enable | Disable***



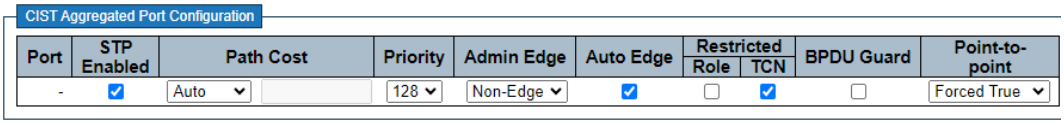
➢ ***Restricted Role***

- ***Enable | Disable***



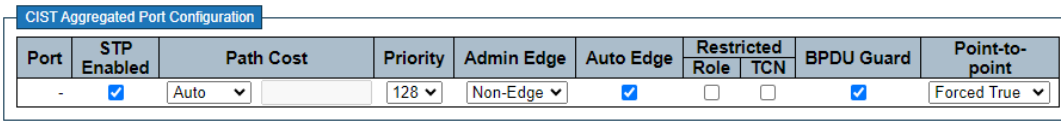
➢ ***Restricted TCN***

- ***Enable | Disable***



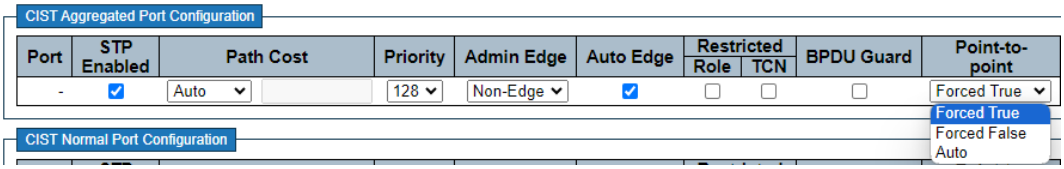
➢ ***BPDU Guard***

- ***Enable | Disable***



➢ ***Point-to-Point***

- ***Forced True | Forced False | Auto***



CLI 설정 예시

✓ **CIST Aggregated Port Configuration**

✓ **CIST Normal Port Configuration**

➢ ***STP Enabled***

- ***Enable | Disable***

```
(config)# spanning-tree aggregation
(config-stp-aggr)# spanning-tree
(config-stp-aggr)# no spanning-tree
```

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface *
(config-if)# spanning-tree
(config-if)# no spanning-tree
```

➢ ***Path Cost***

- ***Auto | Specific(1~200,000,000)***

```
(config-stp-aggr)# spanning-tree mst <instance> cost { <cost> | auto }
(config-stp-aggr)# spanning-tree mst 0 cost auto
(config-stp-aggr)# spanning-tree mst 0 cost 200000000
```

```
(config-if)# spanning-tree mst <instance> cost { <cost> | auto }
(config-if)# spanning-tree mst 0 cost auto
(config-if)# spanning-tree mst 0 cost 200000000
```

➢ ***Priority***

- ***0|16|32|48|64|80|96|112|128|144|160|176|192|208|224|240***

(config-stp-aggr)# spanning-tree mst <instance> port-priority <prio>
(config-stp-aggr)# spanning-tree mst 0 port-priority 128

(config-if)# spanning-tree mst <instance> port-priority <prio>
(config-if)# spanning-tree mst 0 port-priority 128

➢ ***Admin Edge***

- ***Non-Edge | Edge***

(config-stp-aggr)# no spanning-tree edge
(config-stp-aggr)# spanning-tree edge

(config-if)# no spanning-tree edge
(config-if)# spanning-tree edge

➢ ***Auto Edge***

- ***Enable | Disable***

(config-stp-aggr)# spanning-tree auto-edge
(config-stp-aggr)# no spanning-tree auto-edge

(config-if)# spanning-tree auto-edge
(config-if)# no spanning-tree auto-edge

➢ ***Restricted Role***

- ***Enable | Disable***

(config-stp-aggr)# spanning-tree restricted-role
(config-stp-aggr)# no spanning-tree restricted-role

(config-if)# spanning-tree restricted-role
(config-if)# no spanning-tree restricted-role

➢ ***Restricted TCN***

- ***Enable | Disable***

(config-stp-aggr)# spanning-tree restricted-tcn
(config-stp-aggr)# no spanning-tree restricted-tcn

(config-if)# spanning-tree restricted-tcn
(config-if)# no spanning-tree restricted-tcn

➢ ***BPDU Guard***

- ***Enable | Disable***

```
(config-stp-aggr)# spanning-tree bpdu-guard
(config-stp-aggr)# no spanning-tree bpdu-guard
(config-if)# spanning-tree bpdu-guard
(config-if)# no spanning-tree bpdu-guard
```

➢ ***Point-to-Point***

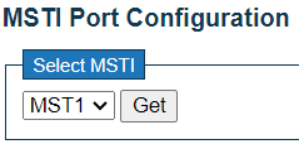
- ***Forced True | Forced False | Auto***

```
(config-stp-aggr)# spanning-tree link-type point-to-point
(config-stp-aggr)# spanning-tree link-type shared
(config-stp-aggr)# spanning-tree link-type auto
(config-if)# spanning-tree link-type point-to-point
(config-if)# spanning-tree link-type shared
(config-if)# spanning-tree link-type auto
```

6.8.1.5. MSTI Ports

웹메뉴 Configuration>Spanning Tree>MSTI Ports

이 페이지는 사용자가 현재 STP MSTI 포트 구성을 검사하고 변경할 수 있는 기능을 제공합니다.
MSTI 포트는 가상 포트로, 포트에 구성된 각 MSTI 인스턴스에 대해 각 활성 CIST(물리적) 포트마다 별도로 인스턴스화됩니다. 실제 MSTI 포트 구성 옵션을 표시하기 전에 MSTI 인스턴스를 선택해야 합니다.
이 페이지에는 물리적 및 집계된 포트에 대한 MSTI 포트 설정이 포함되어 있습니다.



MSTI Port Configuration

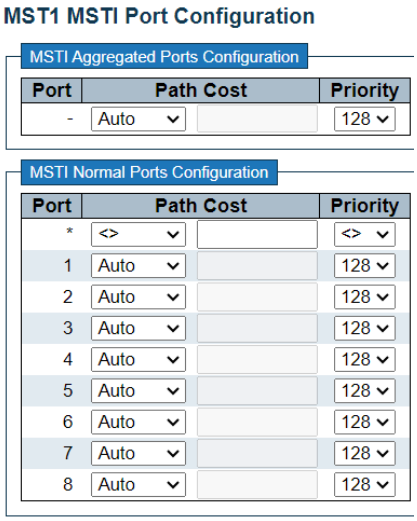
용어	설명
Select MSTI	구성할 MSTI 인스턴스를 선택합니다. 선택 후 GET 버튼을 클릭하면 설정 페이지가 표시됩니다.

Buttons

Get : 특정 MSTI에 대한 설정을 검색합니다.

MSTI Port Configuration

'Get' 버튼을 클릭하면 MSTI 설정을 위한 다음 페이지가 표시됩니다.
이 페이지는 사용자가 현재 STP MSTI 포트 구성을 검사하고 변경할 수 있는 기능을 제공합니다.
MSTI 포트는 각 MSTI 인스턴스에 대해 포트에 구성된 각 활성 CIST(물리적) 포트마다 별도로 인스턴스화 된 가상 포트입니다. 실제 MSTI 포트 구성 옵션을 표시하기 전에 MSTI 인스턴스를 선택해야 합니다.
이 페이지에는 물리적 및 집계된 포트에 대한 MSTI 포트 설정이 포함되어 있습니다.



MSTn MSTI Port Configuration

MSTI Aggregated Ports Configuration

MSTI Normal Ports Configuration

용어	설명
Port	해당하는 STP CIST (그리고 MSTI) 포트의 스위치 포트 번호입니다.
Path Cost	포트에서 발생하는 경로 비용을 제어합니다. Auto 설정은 물리적 링크 속도에 따라 적절한 경로 비용을 설정하며, 802.1D 에서 권장하는 값들을 사용합니다. Specific 설정을 사용하면 사용자가 정의한 값으로 경로 비용을 입력할 수 있습니다. 경로 비용은 네트워크의 활성 토폴로지를 설정하는 데 사용됩니다. 경로 비용이 낮은 포트는 경로 비용이 높은 포트보다 우선하여 전달 포트로 선택됩니다. 유효한 값은 1 에서 200000000 범위에 있습니다.
Priority	포트 우선순위를 제어합니다. 이는 동일한 포트 비용을 가진 포트의 우선순위를 제어하는 데 사용될 수 있습니다. (위 참조)

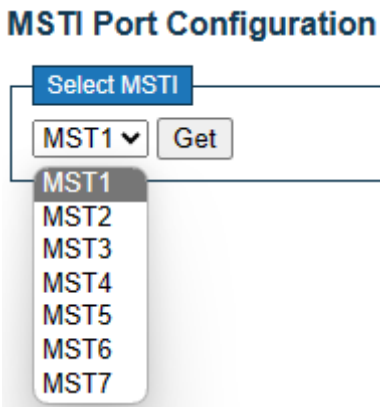
Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>Spanning Tree>MSTI Ports

- ✓ **MSTI Port Configuration**
  - ➢ ***Select MSTI***



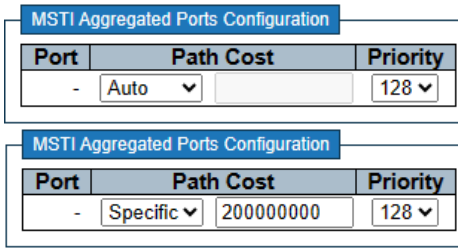
설정할 MST 를 선택한 후 'Get'버튼을 클릭하세요.

- ✓ **MSTn MSTI Port Configuration**
- ✓ **MSTI Aggregated Ports Configuration**

✓ MSTI Normal Ports Configuration

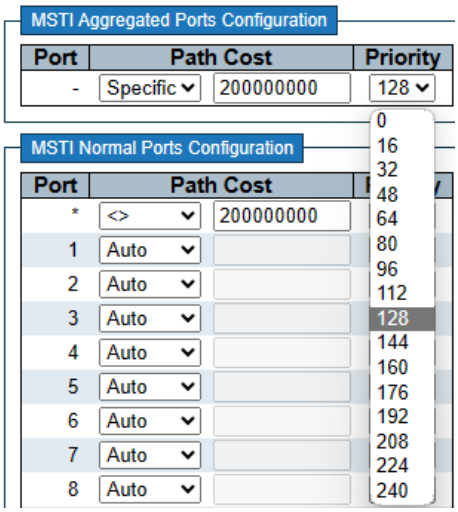
➢ ***Path Cost***

- ***Auto | Specific(1~200,000,000)***



➢ ***Priority***

- ***0|16|32|48|64|80|96|112|128|144|160|176|192|208|224|240***



CLI 설정 예시

✓ MSTI Port Configuration

- ***Select MSTI***

  mst <instance> (CIST=0, MSTI1=1, MSTI2=2, …, MSTI7=7)

✓ MSTn MSTI Port Configuration

✓ MSTI Aggregated Ports Configuration

✓ MSTI Normal Ports Configuration

➢ ***Path Cost***

- ***Auto | Specific(1~200,000,000)***

```
(config)# spanning-tree aggregation

(config-stp-aggr)# spanning-tree mst <instance> cost { <cost> | auto }
(config-stp-aggr)# spanning-tree mst 1 cost auto
(config-stp-aggr)# spanning-tree mst 1 cost 200000000
-----------------------------------------------------------------------
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface *

(config-if)# spanning-tree mst <instance> cost { <cost> | auto }
(config-if)# spanning-tree mst 1 cost auto
(config-if)# spanning-tree mst 1 cost 200000000
```

- ***Priority***
  - ***0\|16\|32\|48\|64\|80\|96\|112\|128\|144\|160\|176\|192\|208\|224\|240***

```
(config-stp-aggr)# spanning-tree mst <instance> port-priority <prio>
(config-stp-aggr)# spanning-tree mst 1 port-priority 128
-----------------------------------------------------------------------
(config-if)# spanning-tree mst <instance> port-priority <prio>
(config-if)# spanning-tree mst 1 port-priority 128
```

6.8.2. Spanning Tree Monitor

6.8.2.1. Bridge Status

웹메뉴 Monitor>Spanning Tree>Bridge Status

이 페이지는 모든 STP 브리지 인스턴스의 상태 개요를 제공합니다.

STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-21-6D-00-00-00	32768.00-21-6D-00-00-00	-	0	Steady	-

표에는 각 STP 브리지 인스턴스에 대한 행이 표시되며, 열은 다음 정보를 표시합니다.

STP Bridges

용어	설명
MSTI	브리지 인스턴스입니다. 또한 STP Detailed Bridge Status 링크입니다.
Bridge ID	이 브리지 인스턴스의 브리지 ID 입니다.
Root ID	현재 선출된 루트 브리지의 브리지 ID 입니다.
Root Port	현재 루트 포트 역할이 할당된 스위치 포트입니다.
Root Cost	루트 경로 비용입니다. 루트 브리지의 경우 0 이며, 다른 모든 브리지의 경우 루트 브리지로의 최소 비용 경로상의 포트 경로 비용의 합입니다.
Topology Flag	이 브리지 인스턴스의 현재 토폴로지 변경 플래그 상태입니다.
Topology Change Last	마지막 토폴로지 변경이 발생한 이후 경과한 시간입니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

STP Detailed Bridge Status

이 페이지는 단일 STP 브리지 인스턴스에 대한 자세한 정보와 관련된 모든 활성 포트의 포트 상태를 제공합니다.

STP Detailed Bridge Status

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-21-6D-00-00-00
Root ID	32768.00-21-6D-00-00-00
Root Cost	0
Root Port	-
Regional Root	32768.00-21-6D-00-00-00
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
No ports or aggregations active							

STP Detailed Bridge Status

용어	설명
STP Bridge Status	이 항목은 STP 브리지 인스턴스의 상태를 보여줍니다.
Bridge Instance	CIST, MST1 등의 브리지 인스턴스입니다.
Bridge ID	이 브리지 인스턴스의 브리지 ID 입니다.
Root ID	현재 선출된 루트 브리지의 브리지 ID 입니다.
Root Port	현재 루트 포트 역할이 할당된 스위치 포트입니다.
Root Cost	루트 경로 비용입니다. 루트 브리지의 경우 0 이며, 다른 모든 브리지의 경우 루트 브리지로의 최소 비용 경로상의 포트 경로 비용의 합입니다.
Regional Root	이 브리지의 MSTP 영역 내에서 현재 선출된 리전 루트 브리지의 브리지 ID 입니다. (CIST 인스턴스에만 해당)
Internal Root Cost	리전 루트 경로 비용입니다. 리전 루트 브리지의 경우 이 값은 0 입니다. 동일한 MSTP 영역 내의 다른 CIST 인스턴스에 대해서는 내부 루트 브리지까지의 최소 비용 경로상의 내부 포트 경로 비용의 합입니다. (CIST 인스턴스에만 해당)
Topology Flag	이 브리지 인스턴스의 토폴로지 변경 플래그의 현재 상태입니다.
Topology Change Count	토폴로지 변경 플래그가 설정된 횟수입니다 (1 초 간격으로 측정).
Topology Change Last	토폴로지 플래그가 마지막으로 설정된 이후 경과한 시간입니다.

STP Detailed Bridge Status

용어	설명
CIST Ports & Aggregations State	이 항목은 CIST (공통 및 내부 스패닝 트리) 포트와 집계의 상태를 보여줍니다.
Port	논리적인 STP 포트의 스위치 포트 번호입니다.
Port ID	STP 프로토콜에서 사용되는 포트 ID 입니다. 이는 브리지 포트의 우선순위 부분과 논리적인 포트 인덱스입니다.
Role	현재 STP 포트 역할입니다. 포트 역할은 다음 값 중 하나일 수 있습니다: 대체 포트, 백업 포트, 루트 포트, 지정 포트.
State	현재 STP 포트 상태입니다. 포트 상태는 다음 값 중 하나일 수 있습니다: 버리는 중(Discarding), 학습 중(Learning), 전달 중(Forwarding).
Path Cost	현재 STP 포트 경로 비용입니다. 이 값은 자동 설정에서 계산된 값이거나 명시적으로 구성된 값일 수 있습니다.
Edge	현재 STP 포트 (운영 중) 엣지 플래그입니다. 엣지 포트는 어떤 브리지에도 연결되지 않은 스위치 포트입니다. 이 플래그는 자동으로 계산되거나 명시적으로 구성될 수 있습니다. 각 엣지 포트는 루프에 참여할 가능성이 없기 때문에 직접 전달 포트 상태로 전환됩니다.
Point-to-Point	현재 STP 포트의 포인트 투 포인트 플래그입니다. 포인트 투 포인트 포트는 공유 LAN 미디어에 연결되지 않은 포트입니다. 이 플래그는 자동으로 계산되거나 명시적으로 구성될 수 있습니다. 포트의 포인트 투 포인트 속성은 포트가 STP 상태로 전환되는 속도에 영향을 미칩니다.
Uptime	브리지 포트가 마지막으로 초기화된 이후 경과한 시간입니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

WEB 확인 예시

웹메뉴 Monitor>Spanning Tree>Bridge Status

✓ **STP Bridges**

STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-21-6D-00-00-00	32768.00-21-6D-00-00-00	-	0	Steady	-
MSTI1	32769.00-21-6D-00-00-00	32769.00-21-6D-00-00-00	-	0	Steady	-

MSTI 를 클릭하면 STP Detailed Bridge Status 창이 열립니다.

✓ **STP Detailed Bridge Status**

✓ **CIST Ports & Aggregations State**

STP Detailed Bridge Status

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.00-21-6D-00-00-00
Root ID	32768.00-21-6D-00-00-00
Root Cost	0
Root Port	-
Regional Root	32768.00-21-6D-00-00-00
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	-

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
2	128:002	DesignatedPort	Forwarding	20000	Yes	Yes	0d 00:46:47

CLI 확인 예시

✓ **STP Bridges**

✓ **STP Detailed Bridge Status**

✓ **CIST Ports & Aggregations State**

```
# show spanning-tree

CIST Bridge STP Status
Bridge ID    : 32768.00-21-6D-00-00-00
Root ID      : 32768.00-21-6D-00-00-00
Root Port    : -
Root PathCost: 0
Regional Root: 32768.00-21-6D-00-00-00
Int. PathCost: 0
Max Hops     : 20
TC Flag      : Steady
TC Count     : 0
TC Last      : -

Port       Port Role       State       Pri  PathCost  Edge  P2P  Uptime
---------  --------------  ----------  ---  --------  ----  ---  -------------
Gi 1/2     DesignatedPort  Forwarding  128     20000  Yes   Yes  0d 01:32:52

MSTI1 Bridge STP Status
Bridge ID    : 32769.00-21-6D-00-00-00
Root ID      : 32769.00-21-6D-00-00-00
Root Port    : -
Root PathCost: 0
TC Flag      : Steady
TC Count     : 0
TC Last      : -
Gi 1/2     DesignatedPort  Forwarding  128     20000  Yes   Yes  0d 01:31:56
```

6.8.2.2. Port Status

웹메뉴 Monitor>Spanning Tree>Port Status

이 페이지는 스위치의 물리적인 포트에 대한 STP CIST 포트 상태를 표시합니다.

STP Port Status

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-

STP Port Status

용어	설명
Port	논리적인 STP 포트의 스위치 포트 번호입니다.
CIST Role	CIST 포트의 현재 STP 포트 역할입니다. 포트 역할은 다음 값 중 하나입니다: 대체 포트(Alternate Port), 백업 포트(Backup Port), 루트 포트(Root Port), 지정 포트(Designated Port), 비활성화됨(Disabled).
CIST State	CIST 포트의 현재 STP 포트 상태입니다. 포트 상태는 다음 값 중 하나입니다: 버리는 중(Discarding), 학습 중(Learning), 전달 중(Forwarding).
Uptime	브리지 포트가 마지막으로 초기화된 이후 경과한 시간입니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

WEB 확인 예시

웹메뉴 Monitor>Spanning Tree>Port Status

✓ **STP Port Status**

STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	DesignatedPort	Forwarding	0d 01:55:34
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	Disabled	Discarding	-
11	Disabled	Discarding	-
12	Disabled	Discarding	-

CLI 확인 예시

✓ STP Port Status

```
# show spanning-tree mst 0 int *

Mst    Port       Port Role       State       Pri  PathCost  Edge  P2P  Uptime
-----  ---------  --------------  ----------  ---  --------  ----  ---  -------------
CIST   Gi 1/2     DesignatedPort  Forwarding  128     20000  Yes   Yes  0d 02:49:51
```

6.8.2.3. Port Statistics

웹메뉴 Monitor>Spanning Tree>Port Statistics

이 페이지는 스위치의 브리지 포트의 STP 포트 통계 카운터를 표시합니다.

STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

STP Statistics

용어	설명
Port	논리적인 STP 포트의 스위치 포트 번호입니다.
MSTP	포트에서 수신/전송된 MSTP BPDU 의 개수입니다.
RSTP	포트에서 수신/전송된 RSTP BPDU 의 개수입니다.
STP	포트에서 수신/전송된 레거시 STP 구성 BPDU 의 개수입니다.
TCN	포트에서 수신/전송된 (레거시) 토폴로지 변경 알림 BPDU 의 개수입니다.
Discarded Unknown	포트에서 수신된(및 버려진) 알 수 없는 스패닝 트리 BPDU 의 개수입니다.
Discarded Illegal	포트에서 수신된(및 버려진) 부적절한 스패닝 트리 BPDU 의 개수입니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

Clear : 클릭 시 카운터 선택을 취소합니다.

WEB 확인 예시

웹메뉴 Monitor>Spanning Tree>Port Statistics

✓ **STP Statistics**

STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
2	5666	0	0	0	0	0	0	0	0	0

CLI 확인 예시

✓ **STP Port Status**

```
# show spanning-tree detailed interface *

Port       Rx MSTP   Tx MSTP   Rx RSTP   Tx RSTP   Rx STP    Tx STP    Rx TCN    Tx TCN    Rx Ill.  Rx Unk.
---------- --------- --------- --------- --------- --------- --------- --------- --------- -------- -------
  Gi 1/2          0      6668         0         0         0         0         0         0        0       0
```

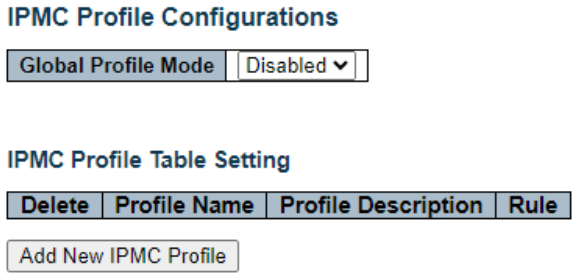
6.9. IPMC Profile

6.9.1. Profile Table Configuration

웹메뉴 Configuration>IPMC Profile>Profile Table

이 페이지에서는 IPMC 프로필 관련 구성을 제공합니다.

IPMC 프로필은 IP 멀티캐스트 스트림에 대한 액세스 제어를 배포하는 데 사용됩니다. 최대 64개의 프로필을 생성할 수 있으며 각각에 최대 128개의 해당 규칙을 생성할 수 있습니다.



IPMC Profile Configurations

용어	설명
Global Profile Mode	전역 IPMC 프로필을 활성화/비활성화합니다. 시스템은 전역 프로필 모드가 활성화된 경우에만 프로필 설정을 기반으로 필터링을 시작합니다.

IPMC Profile Table Setting

용어	설명
Delete	항목을 삭제하려면 체크하십시오. 다음 저장 시 지정된 항목이 삭제됩니다.
Profile Name	프로필 테이블의 색인에 사용되는 이름입니다. 각 항목은 최대 16 자의 알파벳과 숫자로 구성된 고유한 이름을 가집니다. 항목은 하나의 알파벳은 포함되어야 합니다.
Profile Description	프로필에 대한 최대 64 자의 알파벳과 숫자로 구성된 추가 설명입니다. 설명에 공백이나 스페이스 문자는 허용되지 않습니다. 설명 문장을 구분할 때는 "_" 또는 "-"를 사용하십시오.
Rule	프로필이 생성되면 지정된 프로필의 규칙 설정 페이지로 이동하려면 편집 버튼을 클릭하십시오. 지정된 프로필에 대한 요약 정보는 보기 버튼을 클릭하여 표시됩니다. 다음 버튼을 사용하여 지정된 프로필의 규칙을 관리하거나 검사할 수 있습니다. : 지정된 프로필과 관련된 규칙을 나열합니다. : 지정된 프로필과 관련된 규칙을 조정합니다.

Buttons

Add New IPMC Profile: 새 IPMC 프로필을 추가하려면 클릭하세요. 새 항목의 이름을 지정하고 구성하세요.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

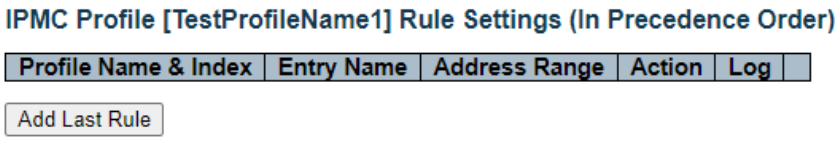
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

IPMC Profile Rule Settings Table

버튼을 클릭하면 목록 페이지가 나옵니다.

버튼을 클릭하면 설정 페이지가 나옵니다.

이 페이지는 특정 IPMC 프로필에 대한 필터링 규칙 설정을 제공합니다. 구성된 규칙 항목들을 선행 순서로 표시합니다. 첫 번째 규칙 항목은 조회에서 가장 높은 우선순위를 갖고 있으며, 마지막 규칙 항목은 조회에서 가장 낮은 우선순위를 갖습니다.



IPMC Profile [Profile Name] Rule Settings (In precedence Order)

용어	설명
Profile Name	지정된 프로필의 이름을 지정합니다. 이 필드는 편집할 수 없습니다.
Entry Name	이 규칙에 사용되는 주소 범위를 지정하는 데 사용되는 이름입니다. 선택된 상자에서는 기존의 프로필 주소 항목만 선택됩니다. 이 필드는 규칙 설정 테이블이 커밋되는 동안 "none"("-")으로 선택이 허용되지 않습니다.
Address Range	선택된 프로필 항목의 해당 주소 범위입니다. 이 필드는 편집할 수 없으며, 선택된 프로필 항목에 따라 자동으로 조정됩니다.
Action	규칙의 주소 범위와 일치하는 그룹 주소를 포함하는 Join/Report 프레임을 수신할 때의 학습 동작을 나타냅니다. Enable: 규칙에 지정된 범위와 일치하는 그룹 주소는 학습됩니다. Disable: 규칙에 지정된 범위와 일치하는 그룹 주소는 삭제됩니다.
Log	규칙의 주소 범위와 일치하는 그룹 주소를 포함하는 Join/Report 프레임을 수신할 때의 로깅 기본값을 나타냅니다. Enable: 규칙에 지정된 범위와 일치하는 그룹 주소의 해당 정보가 로깅됩니다. Disable: 규칙에 지정된 범위와 일치하는 그룹 주소의 해당 정보가 로깅되지 않습니다.
Rule Management Buttons	다음 버튼을 사용하여 규칙 및 해당 우선 순서를 관리할 수 있습니다: : 현재 규칙 항목 앞에 새로운 규칙을 삽입합니다. : 현재 규칙 항목을 삭제합니다. : 규칙 항목을 위로 이동합니다. : 규칙 항목을 아래로 이동합니다.

Buttons

Add Last Rule: 지정된 프로필의 규칙 목록 끝에 새로운 규칙을 추가하려면 클릭하세요. 주소 항목을 지정하고 새 항목을 구성하세요.

Commit: 지정된 프로필의 규칙 변경 사항을 커밋하려면 클릭하세요.

Reset: 로컬에서 수행한 모든 변경 사항을 취소하고 이전에 저장된 값으로 되돌리려면 클릭하세요.

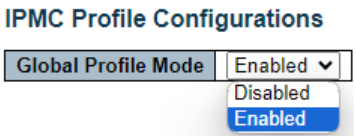
WEB 설정 예시

웹메뉴 Configuration>IPMC Profile>Profile Table

✓ IPMC Profile Configuration

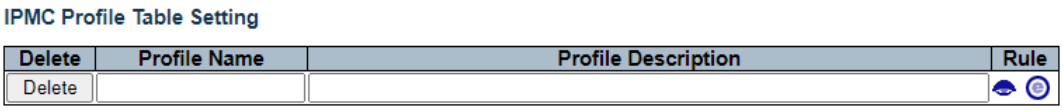
➢ *Global Profile Mode*

- ***Enable*** **|** *Disable*



✓ IPMC Profile Table Setting

➢ *Add New IPMC Profile*

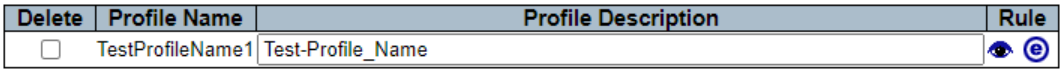


➢ *Profile Name*

- *Maximum 16 alphabetic and numeric characters.*

➢ *Profile Description*

- *Maximum 64 alphabetic and numeric characters.*



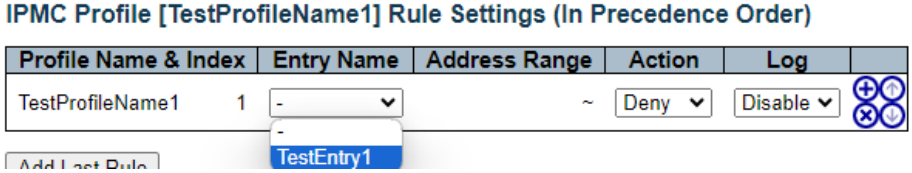
Click  button for setting Edit Profile [Profile Name] Rule

✓ IPMC Profile [Profile Name] Rule Settings (In precedence Order)

➢ *Add Last Rule*

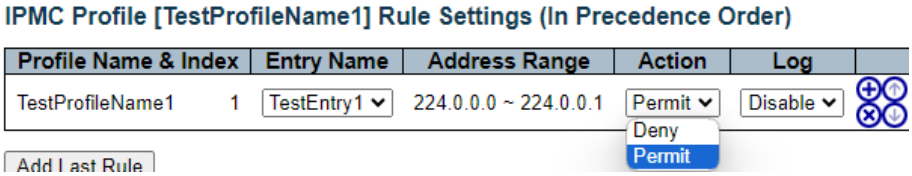
➢ *Entry Name*

- Select Entry (Settings required in the Address Entry.)



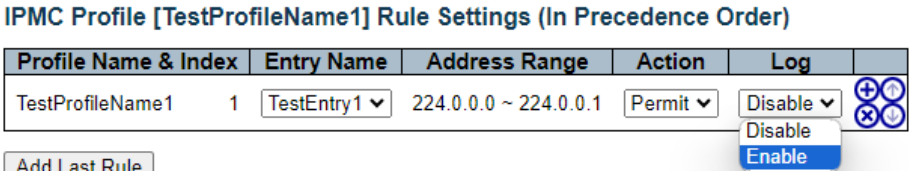
➢ ***Action***

- Deny | **Permit**



➢ ***Log***

- Disable | **Enable**



Click Commit button to commit rule changes for the designated profile.

Click button to view Profile [Profile Name] Rule

IPMC Profile [TestProfileName1] Rule Settings (In Precedence Order)

Profile Name & Index		Entry Name	Address Range	Action	Log
TestProfileName1	1	TestEntry1	224.0.0.0 ~ 224.0.0.1	Permit	Enable

EXAMPLE CLI CONFIGURATION

✓ IPMC Profile Configuration

➢ ***Global Profile Mode***

- ***Enable*** **|** *Disable*

```
(config)# ipmc profile
(config)# no ipmc profile
```

✓ IPMC Profile Table Setting

➢ ***Add New IPMC Profile***

➢ ***Profile Name***

- *Maximum 16 alphabetic and numeric characters.*

```
(config)# ipmc profile <word16>
(config)# ipmc profile TestProfileName1
```

➢ ***Profile Description***

- *Maximum 64 alphabetic and numeric characters.*

```
(config)# ipmc profile <word16>
(config)# ipmc profile TestProfileName1

(config-ipmc-profile)# description <line64>
(config-ipmc-profile)# description Test-Profile_Name
```

✓ **IPMC Profile [Profile Name] Rule Settings (In precedence Order)**

➢ ***Add Last Rule***

➢ ***Entry Name***

- Select Entry (Settings required in the Address Entry.)

➢ ***Action***

- Deny | **Permit**

➢ ***Log***

- Disable | **Enable**

```
(config)# ipmc profile <word16>
(config)# ipmc profile TestProfileName1
(config-ipmc-profile)# range <entry_name> { permit | deny } [ log ] [ next <next_entry> ]
(config-ipmc-profile)# range TestEntry1 permit log
(config-ipmc-profile)# range TestEntry1 permit
(config-ipmc-profile)# range TestEntry1 deny log
(config-ipmc-profile)# range TestEntry1 deny
```

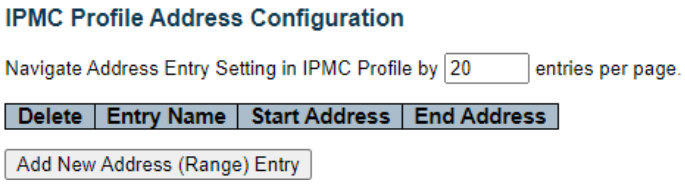
Click button to view Profile [Profile Name] Rule

```
# show ipmc profile [ <profile_name> ] [ detail ]
# show ipmc profile
IPMC Profile is now enabled to start filtering.
Profile: TestProfileName1 (In IGMP Mode)
Description: Test-Profile_Name
HEAD-> TestEntry1 (Permit the following range and log the matched entry)
Start Address: 224.0.0.0
End Address  : 224.0.0.1

# show ipmc profile detail
IGMP will permit and log matched address between [224.0.0.0 <-> 224.0.0.1]
IGMP will deny matched address between [224.0.0.2 <-> 239.255.255.255]
MLD will deny matched address between [ff00:: <-> ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff]
```

6.9.2. Address Entry Configuration

웹메뉴 Configuration>IPMC Profile>Address Entry

이 페이지는 IPMC 프로필에서 사용되는 주소 범위 설정을 제공합니다.
주소 항목은 IPMC 프로필과 관련된 주소 범위를 지정하는 데 사용됩니다.
시스템에서는 최대 128개의 주소 항목을 생성할 수 있습니다.



IPMC Profile Address Configuration

용어	설명
Delete	해당 항목을 삭제하려면 체크하세요. 지정된 항목은 저장 시 삭제됩니다.
Entry Name	주소 항목 테이블을 색인화하는 데 사용되는 이름입니다. 각 항목은 최대 16 자의 알파벳과 숫자로 구성된 고유한 이름을 가지고 있습니다. 적어도 하나의 알파벳이 있어야 합니다. 이 항목은 Profile Table 에서 사용됩니다.
Start Address	주소 범위로 사용될 시작 IPv4/IPv6 멀티캐스트 그룹 주소입니다.
End Address	주소 범위로 사용될 끝 IPv4/IPv6 멀티캐스트 그룹 주소입니다.

Buttons

Add New Address (Range) Entry: 새 주소 범위를 추가하려면 클릭하세요. 이름을 지정하고 주소를 구성하세요.

Apply: 변경 사항을 적용하려면 클릭하세요.

Apply&Save: 변경 사항을 적용하고 저장하려면 클릭하세요.

Reset: 로컬에서 수행한 모든 변경 사항을 취소하고 이전에 저장된 값으로 되돌리려면 클릭하세요.

Refresh: 입력 필드부터 표시된 테이블을 새로 고칩니다.

|<<: IPMC 프로필 주소 구성의 첫 번째 항목부터 테이블을 업데이트합니다.

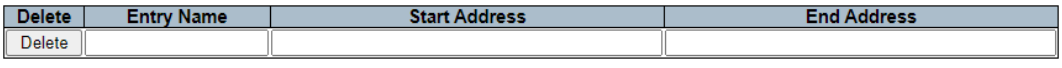
>>: 테이블을 업데이트합니다. 현재 표시된 마지막 항목 다음 항목부터 시작합니다.

WEB 설정 예시

웹메뉴 Configuration>IPMC Profile>Address Entry

✓ **IPMC Profile Address Configuration**

➢ ***Add New Address(Range) Entry***



➢ ***Entry Name***

- *Maximum 16 alphabetic and numeric characters*

➢ ***Start Address***

- *IPv4/IPv6 Multicast Group Address(ex IPv4-224.0.0.0~239.255.255.255)*

➢ ***End Address***

- *IPv4/IPv6 Multicast Group Address(ex IPv4-224.0.0.0~239.255.255.255)*

Delete	Entry Name	Start Address	End Address
☐	TestEntry1	224.0.0.0	224.0.0.1

CLI 설정 예시

✓ IPMC Profile Address Configuration

➢ ***Add New Address(Range) Entry***

➢ ***Entry Name***

- *Maximum 16 alphabetic and numeric characters*

➢ ***Start Address***

- *IPv4/IPv6 Multicast Group Address(ex IPv4-224.0.0.0~239.255.255.255)*

➢ ***End Address***

- *IPv4/IPv6 Multicast Group Address(ex IPv4-224.0.0.0~239.255.255.255)*

```
(config)# ipmc range <entry_name> { <v_ipv4_mcast> [ <v_ipv4_mcast_1> ] | <v_ipv6_mcast>
[ <v_ipv6_mcast_1> ] }
(config)# ipmc range TestEntry1 224.0.0.0 224.0.0.1
```

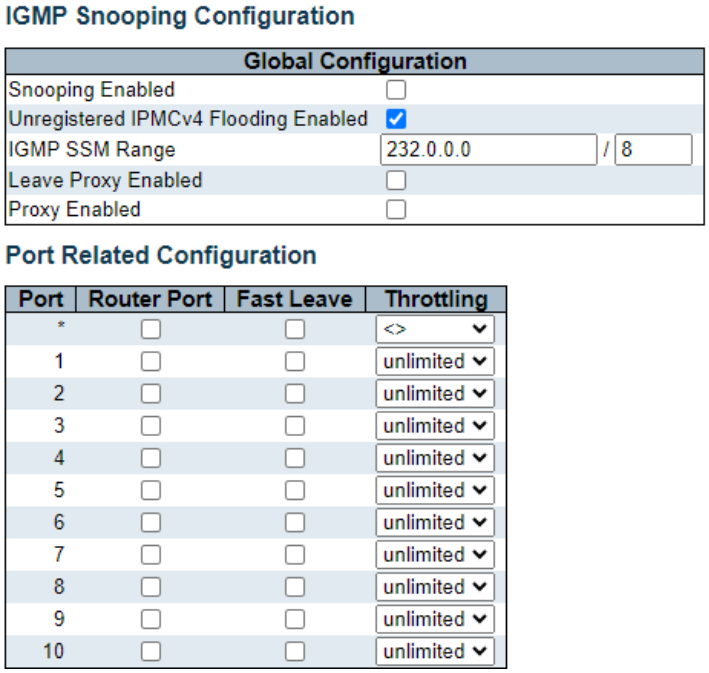
6.10. IPMC

6.10.1. IGMP Snooping Configuration

6.10.1.1. Basic Configuration

웹메뉴 Configuration>IPMC>IGMP Snooping>Basic Configuration

이 페이지는 IGMP 스누핑 관련 구성을 제공합니다.



IGMP Snooping Configuration

Global Configuration

용어	설명
Snooping Enabled	Global IGMP Snooping 을 활성화합니다.
Unregistered IPMCv4 Flooding Enabled	미 등록된 IPMCv4 트래픽 플러딩을 활성화합니다. 플러딩 제어는 IGMP 스누핑이 활성화된 경우에만 작동합니다. IGMP 스누핑이 비활성화된 경우에는 이 설정과 관계없이 미등록 IPMCv4 트래픽 플러딩이 항상 활성화됩니다.
IGMP SSM Range	SSM (Source-Specific Multicast) 범위는 SSM-aware 호스트와 라우터가 주소 범위 내의 그룹에 대해 SSM 서비스 모델을 실행할 수 있도록 합니다. 범위에 대해 유효한 IPv4 멀티캐스트 주소를 접두사로 할당하고, 범위에 대한 접두사 길이(4 에서 32 까지)를 설정하십시오.
Leave Proxy Enabled	IGMP Leave Proxy 를 활성화합니다. 이 기능은 불필요한 나가기 메시지를 라우터 측으로 전달하지 않도록 할 때 사용할 수 있습니다.
Proxy Enabled	IGMP Proxy 를 활성화합니다. 이 기능을 사용하면 불필요한 조인 및 나가기 메시지를 라우터 측으로 전달하지 않을 수 있습니다.

Port Related Configuration

용어	설명
Router Port	라우터 포트로 작동할 포트를 지정합니다. 라우터 포트는 Ethernet 스위치의 포트 중 레이어 3 멀티캐스트 장치 또는 IGMP 쿼리어 쪽으로 이어지는 포트입니다. Aggregation 구성 포트가 라우터 포트로 선택된 경우, 전체 Aggregation 이 라우터 포트로 작동합니다.
Fast Leave	포트에서 빠른 나가기를 활성화합니다. 시스템은 나가기 메시지를 받으면 마지막 멤버 쿼리 메시지를 보내지 않고 그룹 레코드를 제거하고 데이터 전달을 중지합니다. 이 기능은 특정 포트에 단일 IGMPv2 호스트만 연결된 경우에만 활성화하는 것이 권장됩니다.
Throttling	스위치 포트가 속할 수 있는 멀티캐스트 그룹 수를 제한합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>IPMC>IGMP Snooping>Basic Configuration

- ✓ **IGMP Snooping Configuration**
- ✓ **Global Configuration**
  - ➢ ***Snooping Enabled***
    - ***Enable*** **|** *Disable*
  - ➢ ***Unregistered IPMCv4 Flooding Enabled***
    - *Enable* **|** ***Disable***
  - ➢ ***IGMP SSM Range***
    - ***224.0.0.0~239.255.255.255 / 4~32***
  - ➢ ***Leave Proxy Enable***
    - ***Enable*** **|** *Disable*
  - ➢ ***Proxy Enable***
    - *Enable* **|** ***Disable***

IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	☑
Unregistered IPMCv4 Flooding Enabled	☐
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	☑
Proxy Enabled	☐

✓ **Port Related Configuration**

➢ ***Router Port***

- ***Checked*** **|** *Unchecked*

➢ ***Fast Leave***

- ***Checked*** **|** *Unchecked*

➢ ***Throttling***

- ***Unlimited(default)*** **|** *1~10*

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	☑	☑	<>
1	☑	☑	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
4	☐	☐	unlimited
5	☐	☐	unlimited
6	☐	☐	unlimited
7	☐	☐	unlimited
8	☐	☐	unlimited
9	☐	☐	unlimited
10	☐	☐	unlimited

CLI 설정 예시

✓ **IGMP Snooping Configuration**

✓ **Global Configuration**

➢ ***Snooping Enabled***

- ***Enable*** **|** *Disable*

```
(config)# ip igmp snooping
(config)# no ip igmp snooping
```

➢ ***Unregistered IPMCv4 Flooding Enabled***

- *Enable* **|** ***Disable***

```
(config)# ip igmp unknown-flooding
(config)# no ip igmp unknown-flooding
```

➢ ***IGMP SSM Range***

- ***224.0.0.0~239.255.255.255 / 4~32***

```
(config)# ip igmp ssm-range <v_ipv4_mcast> <ipv4_prefix_length>
(config)# ip igmp ssm-range 232.0.0.0 8
```

➢ ***Leave Proxy Enable***

- ***Enable*** **|** *Disable*

```
(config)# ip igmp host-proxy leave-proxy
(config)# no ip igmp host-proxy leave-proxy
```

➢ ***Proxy Enable***

- *Enable* **|** ***Disable***

```
(config)# ip igmp host-proxy
(config)# no ip igmp host-proxy
```

✓ **Port Related Configuration**

➢ ***Router Port***

- ***Checked*** **|** *Unchecked*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# ip igmp snooping mrouter
(config-if)# no ip igmp snooping mrouter
```

➢ ***Fast Leave***

- ***Checked*** **|** *Unchecked*

```
(config-if)# ip igmp snooping immediate-leave
(config-if)# no ip igmp snooping immediate-leave
```

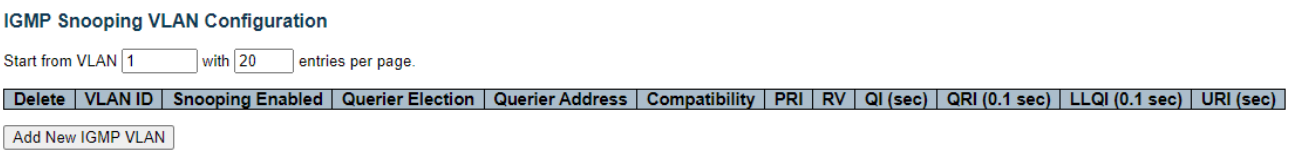
➢ ***Throttling***

- ***Unlimited(default)*** **|** *1~10*

```
(config-if)# no ip igmp snooping max-groups
(config-if)# ip igmp snooping max-groups <throttling>
(config-if)# ip igmp snooping max-groups 10
```

6.10.1.2. VLAN Configuration

웹메뉴 Configuration>IPMC>IGMP Snooping>VLAN Configuration



IGMP Snooping VLAN Configuration

Navigating the IGMP Snooping VLAN Table

각 페이지는 VLAN 테이블에서 최대 99 개의 항목을 보여줍니다. 기본값은 20 으로, "페이지 당 항목" 입력 필드를 통해 선택됩니다. 처음 방문할 때 웹 페이지는 VLAN 테이블의 처음 20 개 항목을 보여줍니다. 표시되는 첫 번째 항목은 VLAN 테이블에서 발견된 가장 낮은 VLAN ID 를 가진 항목입니다.

"VLAN" 입력 필드를 사용하면 사용자가 VLAN 테이블에서 시작점을 선택할 수 있습니다. Refresh 버튼을 클릭하면 해당 위치나 다음으로 가까운 VLAN 테이블 일치 항목부터 표시된 테이블이 업데이트됩니다.

>> 버튼은 현재 표시된 항목을 기반으로 다음 조회를 수행합니다. 끝에 도달하면 "더 이상 항목이 없음"이라는 텍스트가 표시됩니다. 처음부터 다시 시작하려면 |<< 버튼을 사용하세요.

IGMP Snooping VLAN Table Columns

용어	설명
Delete	체크한 항목을 삭제합니다. 지정된 항목은 다음 저장 시 삭제됩니다.
VLAN ID	해당 항목의 VLAN ID 입니다.
IGMP Snooping Enabled	각 VLAN 별 IGMP Snooping 을 활성화합니다. 최대 32 개의 VLAN 을 IGMP Snooping 에 선택할 수 있습니다.
Querier Election	해당 VLAN 에서 IGMP 쿼리어 선출에 참여하도록 활성화합니다. IGMP 비-쿼리어로 작동하려면 비활성화하세요.
Querier Address	IGMP 쿼리어 선출을 위해 IPv4 헤더에서 사용되는 소스 주소를 IPv4 주소로 정의합니다. 쿼리어 주소가 설정되지 않은 경우 시스템은 이 VLAN 에 연결된 IP 인터페이스의 IPv4 관리 주소를 사용합니다. IPv4 관리 주소가 설정되지 않은 경우 시스템은 첫 번째로 사용 가능한 IPv4 관리 주소를 사용합니다. 그렇지 않으면, 시스템은 사전에 정의된 값을 사용합니다. 기본적으로 이 값은 192.0.2.1 입니다.
Compatibility	호스트와 라우터가 네트워크 내에서 호스트 및 라우터의 IGMP 버전에 따라 적절한 조치를 취함으로써 호환성을 유지합니다. 허용되는 선택은 IGMP-Auto, 강제 IGMPv1, 강제 IGMPv2, 강제 IGMPv3 이며, 기본 호환성 값은 IGMP-Auto 입니다.
PRI	Priority of Interface. 인터페이스 우선순위는 시스템에서 생성된 IGMP 제어 프레임의 우선순위 수준을 나타냅니다. 이러한 값은 서로 다른 클래스의 트래픽에 우선순위를 부여하는 데 사용될 수 있습니다. 허용되는 범위는 0(최선의 노력)부터 7(최고)까지이며, 기본 인터페이스 우선순위 값은 0 입니다.
RV	Robustness Variable.

	Robustness 변수는 네트워크에서 예상되는 패킷 손실에 대한 조정을 허용합니다. 허용되는 범위는 1 에서 255 이며, 기본 Robustness 변수 값은 2 입니다.
QI	Query Interval. 쿼리 간격은 쿼리어에 의해 보내진 일반 쿼리들 사이의 간격입니다. 허용되는 범위는 1 부터 31744 초이며, 기본 쿼리 간격은 125 초입니다.
QRI	Query Response Interval. 쿼리 응답 간격은 주기적인 일반 쿼리에 삽입되는 최대 응답 지연 코드를 계산하는 데 사용되는 최대 응답 지연입니다. 허용되는 범위는 0 에서 31744 까지이며, 기본 쿼리 응답 간격은 10 초 (초단위로 10 을 곱한 값)입니다.
LLQI (LMQI for IGMP)	Last Member Query Interval. 마지막 멤버 쿼리 간격은 마지막 멤버 쿼리 시간을 나타내는 값으로, 마지막 멤버 쿼리 간격과 마지막 멤버 쿼리 카운트를 곱한 값입니다. 허용되는 범위는 0 에서 31744 까지이며, 기본 마지막 멤버 쿼리 간격은 1 초를 의미하는 10 의 정수로 표시된 값입니다.
URI	Unsolicited Report Interval. 미요청 보고 간격은 호스트의 그룹 멤버십에 대한 초기 보고 간의 반복 시간입니다. 허용되는 범위는 0 에서 31744 초이며, 기본 미요청 보고 간격은 1 초입니다.

Buttons

Refresh: 테이블을 새로고침 합니다.

|<<: 첫 번째 테이블로 돌아갑니다. 가장 낮은 VLAN ID를 가진 항목부터 테이블이 업데이트 됩니다.

>>: 다음 테이블이 표시됩니다. 현재 표시된 마지막 항목 다음 항목부터 테이블이 업데이트 됩니다.

Add New IGMP VLAN: 새로운 IGMP VLAN을 추가하려면 클릭하세요. VID를 지정하고 새 항목을 구성하세요. "저장"을 클릭하세요. 해당 정적 VLAN이 생성된 후에도 특정 IGMP VLAN이 작동을 시작합니다.

Apply: 클릭 시 변경 사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

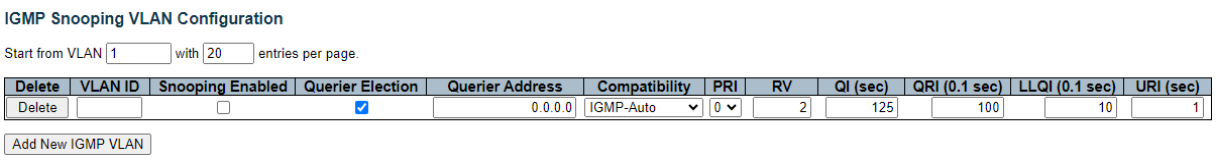
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>IPMC>IGMP Snooping>VLAN Configuration

✓ IGMP Snooping VLAN Configuration

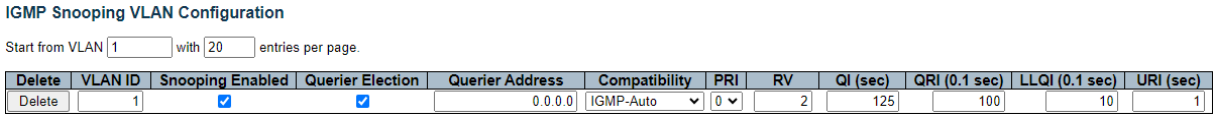
➢ *Add New IGMP VLAN*



➢ *VLAN ID*

- ***VLAN ID 1****(1~4095)*

- ***Snooping Enabled***
  - ***Enable*** | *Disable*
- ***Querier Election***
  - ***Enable*** | *Disable*
- ***Querier Address***
  - *0.0.0.0(no setting)* | *192.168.10.1(setting)*
- ***Compatibility***
  - ***IGMP-Auto*** | *Forced IGMPv1* | *Forced IGMPv2* | *Forced IGMPv3*
- ***PRI***
  - ***0****(0~7)*
- ***RV***
  - ***2****(1~255)*
- ***QI(sec)***
  - ***125****(1~31744)*
- ***QRI(0.1sec)***
  - ***100****(0~31744)*
- ***LLQI(0.1sec)***
  - ***10****(0~31744)*
- ***URI(sec)***
  - ***1****(0~31744)*



CLI 설정 예시

✓ IGMP Snooping VLAN Configuration

➢ *VLAN ID*

- ***VLAN ID 1****(1~4095)*

```
(config)# ip igmp snooping vlan <v_vlan_list>
(config)# ip igmp snooping vlan 1
```

➢ *Snooping Enabled*

- ***Enable*** | *Disable*

```
(config)# interface vlan <vlist>
(config)# interface vlan 1

(config-if-vlan)# ip igmp snooping
(config-if-vlan)# no ip igmp snooping
```

➢ *Querier Election*

- ***Enable*** | *Disable*

```
(config-if-vlan)# ip igmp snooping querier election
(config-if-vlan)# no ip igmp snooping querier election
```

➢ *Querier Address*

- *0.0.0.0(no setting)* | *192.168.10.100(setting)*

```
(config-if-vlan)# ip igmp snooping querier address <v_ipv4_ucast>
(config-if-vlan)# no ip igmp snooping querier address
(config-if-vlan)# ip igmp snooping querier address 192.168.10.1
```

➢ *Compatibility*

- ***IGMP-Auto*** | *Forced IGMPv1* | *Forced IGMPv2* | *Forced IGMPv3*

```
(config-if-vlan)# ip igmp snooping compatibility { auto | v1 | v2 | v3 }
(config-if-vlan)# ip igmp snooping compatibility auto
(config-if-vlan)# ip igmp snooping compatibility v1
(config-if-vlan)# ip igmp snooping compatibility v2
(config-if-vlan)# ip igmp snooping compatibility v3
```

➢ *PRI*

- ***0****(0~7)*

```
(config-if-vlan)# ip igmp snooping priority <cos_priority>
(config-if-vlan)# ip igmp snooping priority 0
```

➢ ***RV***

- ***2****(1~255)*

```
(config-if-vlan)# ip igmp snooping robustness-variable <ipmc_rv>
(config-if-vlan)# ip igmp snooping robustness-variable 2
```

➢ ***QI(sec)***

- ***125****(1~31744)*

```
(config-if-vlan)# ip igmp snooping query-interval <ipmc_qi>
(config-if-vlan)# ip igmp snooping query-interval 125
```

➢ ***QRI(0.1sec)***

- ***100****(0~31744)*

```
(config-if-vlan)# ip igmp snooping query-max-response-time <ipmc_qri>
(config-if-vlan)# ip igmp snooping query-max-response-time 100
```

➢ ***LLQI(0.1sec)***

- ***10****(0~31744)*

```
(config-if-vlan)# ip igmp snooping last-member-query-interval <ipmc_lmqi>
(config-if-vlan)# ip igmp snooping last-member-query-interval 10
```

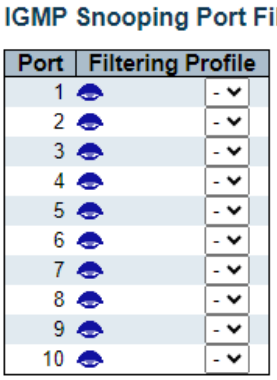
➢ ***URI(sec)***

- ***1****(0~31744)*

```
(config-if-vlan)# ip igmp snooping unsolicited-report-interval <ipmc_uri>
(config-if-vlan)# ip igmp snooping unsolicited-report-interval 1
```

6.10.1.3. Port Filtering Profile

웹메뉴 Configuration>IPMC>IGMP Snooping>Port Filtering Profile



IGMP Snooping Port Filtering Profile Configuration

용어	설명
Port	설정을 위한 논리적 포트입니다.
Filtering Profile	지정된 포트에 대한 필터링 조건으로 IPMC 프로필을 선택하십시오. 보기 버튼을 클릭하여 해당 프로필에 대한 요약을 표시할 수 있습니다.
Profile Management Button	지정된 프로필의 규칙을 확인하려면 다음 버튼을 사용할 수 있습니다. : 지정된 프로필과 관련된 규칙을 나열하십시오.

Buttons

Apply: 클릭 시 변경 사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>IPMC>IGMP Snooping>Port Filtering Profile

✓ **IGMP Snooping Port Filtering Profile Configuration**

➢ ***Filtering Profile***

- *Select the IPMC Profile*

IGMP Snooping Port Filtering Profile Configuration

Port	Filtering Profile
1	-
2	-
3	TestProfileName1
4	-
5	-
6	-
7	-
8	-
9	-
10	-

➢ ***Profile Management Button***

- *Click* button to view Profile [Profile Name] Rule

IPMC Profile [TestProfileName1] Rule Settings (In Precedence Order)

Profile Name & Index		Entry Name	Address Range	Action	Log
TestProfileName1	1	TestEntry1	224.0.0.0 ~ 224.0.0.1	Permit	Enable

CLI 설정 예시

✓ IGMP Snooping Port Filtering Profile Configuration

➢ ***Filtering Profile***

- *Select the IPMC Profile*

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# ip igmp snooping filter <profile_name>
(config-if)# ip igmp snooping filter TestProfileName1
```

➢ ***Profile Management Button***

- *Click* button to view Profile [Profile Name] Rule

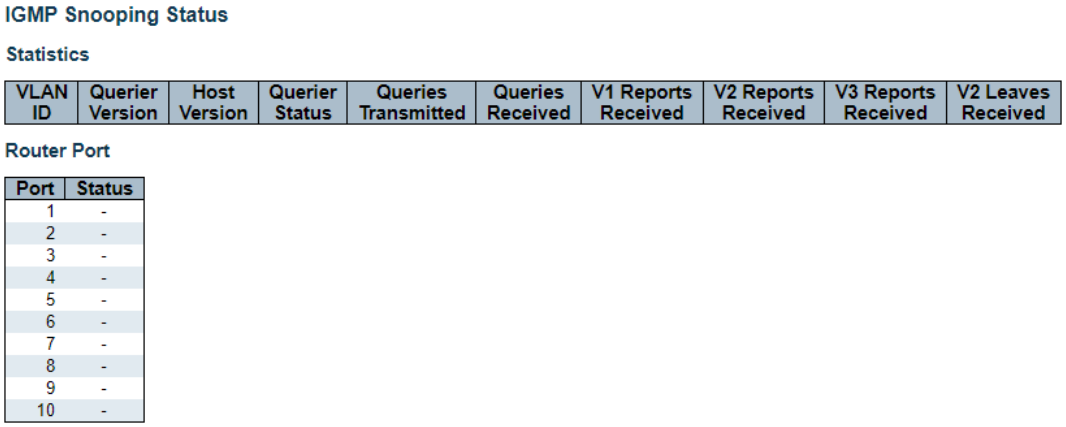
```
# show ipmc profile [ <profile_name> ] [ detail ]
# show ipmc profile
IPMC Profile is now enabled to start filtering.
Profile: TestProfileName1 (In IGMP Mode)
Description: Test-Profile_Name
HEAD-> TestEntry1 (Permit the following range and log the matched entry)
Start Address: 224.0.0.0
End Address  : 224.0.0.1

# show ipmc profile detail
IGMP will permit and log matched address between [224.0.0.0 <-> 224.0.0.1]
IGMP will deny matched address between [224.0.0.2 <-> 239.255.255.255]
MLD will deny matched address between [ff00:: <-> ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff]
```

6.10.2. IGMP Snooping Monitor

6.10.2.1. Status

웹메뉴 Monitor>IPMC>IGMC Snooping>Status

이 페이지는 IGMP 스누핑 상태를 제공합니다.


IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-

IGMP Snooping Status

Statistics

용어	설명
VLAN ID	항목의 VLAN ID 입니다.
Querier Version	현재 작동 중인 쿼리어 버전입니다.
Host Version	현재 작동 중인 호스트 버전입니다.
Querier Status	쿼리어 상태가 "ACTIVE" 또는 "IDLE"을 나타냅니다. "DISABLE"는 특정 인터페이스가 관리적으로 비활성화된 것을 나타냅니다.
Queries Transmitted	전송된 쿼리의 수입니다.
Queries Received	수신된 쿼리의 수입니다.
V1 Reports Received	받은 V1 리포트의 수입니다.
V2 Reports Received	받은 V2 리포트의 수입니다.
V3 Reports Received	받은 V3 리포트의 수입니다.
V2 Leaves Received	받은 V2 Leave 수입니다.

Router Port

라우터 포트로 작동하는 포트를 표시합니다. 라우터 포트는 이더넷 스위치의 포트 중 레이어 3 멀티캐스트 장치 또는 IGMP 쿼리어로 이어지는 포트입니다.

Static 은 특정 포트가 라우터 포트로 구성되어 있는 것을 나타냅니다.

Dynamic 은 특정 포트가 라우터 포트로 학습된 것을 나타냅니다.

Both 는 특정 포트가 라우터 포트로 구성되거나 학습된 것을 나타냅니다.

용어	설명

Port	스위치 포트 번호
Status	특정 포트가 라우터 포트인지를 나타냅니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침. 로컬 변경 사항은 취소합니다.

Clear : 모든 통계 카운터를 초기화합니다.

WEB 확인 예시

웹메뉴 Monitor>IPMC>IGMC Snooping>Status

- ✓ **IGMP Snooping Status**
- ✓ **Statistics**
- ✓ **Router Port**

IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
1	v3	v3	ACTIVE	1	0	0	0	0	0

Router Port

Port	Status
1	Static
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-

CLI 확인 예시

- ✓ **IGMP Snooping Status**
- ✓ **Statistics**

```
# show ip igmp snooping
IGMP Snooping is enabled to start snooping IGMP control plane.
Switch-1 IGMP Interface Status
IGMP snooping VLAN 1 interface is enabled.
Querier status is ACTIVE
RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:5 V2Leave:0
TX IGMP Query:6 / (Source) Specific Query:0
Compatibility:IGMP-Auto / Querier Version:Default / Host Version:Version 3
```

- ✓ **Router Port**

```
# show ip igmp snooping mrouter
IGMP Snooping is enabled to start snooping IGMP control plane.
Switch-1 IGMP Router Port Status
Gi 1/1: Static Router Port
```

6.10.2.2. Groups Information

웹메뉴 Monitor>IPMC>IGMC Snooping>Groups Information

이 페이지에는 IGMP 그룹 테이블의 항목이 표시됩니다.
IGMP 그룹 테이블은 먼저 VLAN ID 로 정렬되고 그런 다음 그룹으로 정렬됩니다.

IGMP Snooping Group Information

Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.

		Port Members									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10
No more entries											

IGMP Snooping Group Information

용어	설명
VLAN ID	그룹의 VLAN ID 입니다.
Groups	표시된 그룹의 그룹 주소입니다.
Port Members	이 그룹에 속한 포트들입니다.

Buttons

Auto-refresh : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh: 입력 필드부터 표시된 테이블을 새로고침 합니다.

|<<: IGMP 그룹 테이블의 첫 번째 항목부터 테이블을 업데이트합니다.

>>: 표시된 마지막 항목 다음 항목부터 테이블을 업데이트합니다.

WEB 확인 예시

웹메뉴 Monitor>IPMC>IGMC Snooping>Groups Information

✓ **IGMP Snooping Group Information**

IGMP Snooping Group Information

Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.

		Port Members									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10
1	239.255.255.250		✓								

CLI 확인 예시

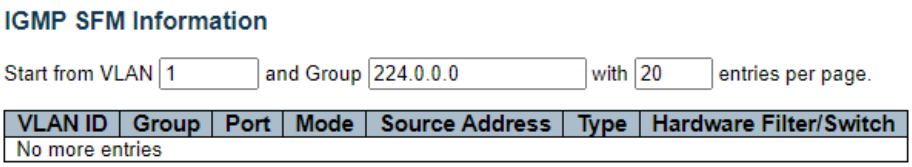
✓ **IGMP Snooping Group Information**

```
# show ip igmp snooping group-database
IGMP Snooping is enabled to start snooping IGMP control plane.
IGMP Group Database
Switch-1 IGMP Group Table
239.255.255.250 is registered on VLAN 1
Port Members: Gi 1/2
Switch-1 IGMP Group Count: 1
```

6.10.2.3. IPv4 SFM Information

웹메뉴 Monitor>IPMC>IGMC Snooping>IPv4 SFM Information

이 페이지에는 IGMP SFM(소스 필터링 멀티캐스트) 정보 테이블의 항목이 표시됩니다. IGMP SFM 정보 테이블에는 SSM(소스별 멀티캐스트) 정보도 포함됩니다. 이 테이블은 먼저 VLAN ID 로 정렬되고, 그룹으로 정렬된 후에 포트로 정렬됩니다. 같은 그룹에 속하는 다른 소스 주소는 단일 항목으로 처리됩니다.



IGMP SFM Information

용어	설명
VLAN ID	그룹의 VLAN ID 입니다.
Group	표시된 그룹의 그룹 주소입니다.
Port	스위치 포트 번호
Mode	VLAN ID, 포트 번호, 그룹 주소 기준으로 유지되는 필터링 모드를 나타냅니다. 이는 Include 또는 Exclude 중 하나일 수 있습니다.
Source Address	소스의 IP 주소입니다. 현재, 필터링할 수 있는 IPv4 소스 주소의 최대 수(그룹당)는 8 개입니다. 소스 주소 필터링이 없는 경우 "None"이라는 텍스트가 소스 주소 필드에 표시됩니다.
Type	유형을 나타냅니다. 허용(Allow) 또는 거부(Deny) 중 하나일 수 있습니다.
Hardware Filter/Switch	지정된 그룹 주소에서 소스 IPv4 주소로 향하는 데이터 평면을 칩이 처리할 수 있는지 여부를 나타냅니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 입력 필드부터 표시된 테이블을 새로고침 합니다.

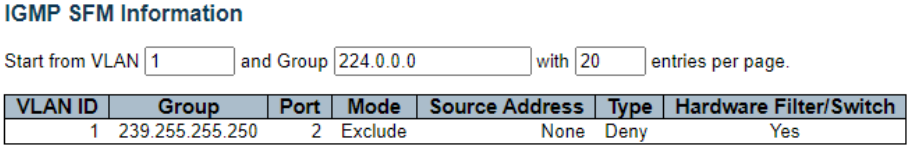
|<< : IGMP SFM 정보 테이블의 첫 번째 항목부터 테이블을 업데이트합니다.

>> : 표시된 마지막 항목 다음 항목부터 테이블을 업데이트합니다.

WEB 확인 예시

웹메뉴 Monitor>IPMC>IGMC Snooping>IPv4 SFM Information

✓ IGMP SFM Information



CLI 확인 예시

✓ IGMP SFM Information

```
# show ip igmp snooping group-database sfm-information detail
IGMP Snooping is enabled to start snooping IGMP control plane.
(IGMP proxy for LEAVE mechanism is active)
Multicast streams destined to unregistered IGMP groups will be flooding.
Groups in range 232.0.0.0/8 follow IGMP SSM registration service model.
IGMP Group Database
Switch-1 IGMP Group Table
239.255.255.250 is registered on VLAN 1
Port Members: Gi 1/2
Hardware Switch: Yes
Gi 1/2 Mode is Exclude (Filter Timer: 151)
Deny Source Address: None
Switch-1 IGMP Group Count: 1
```

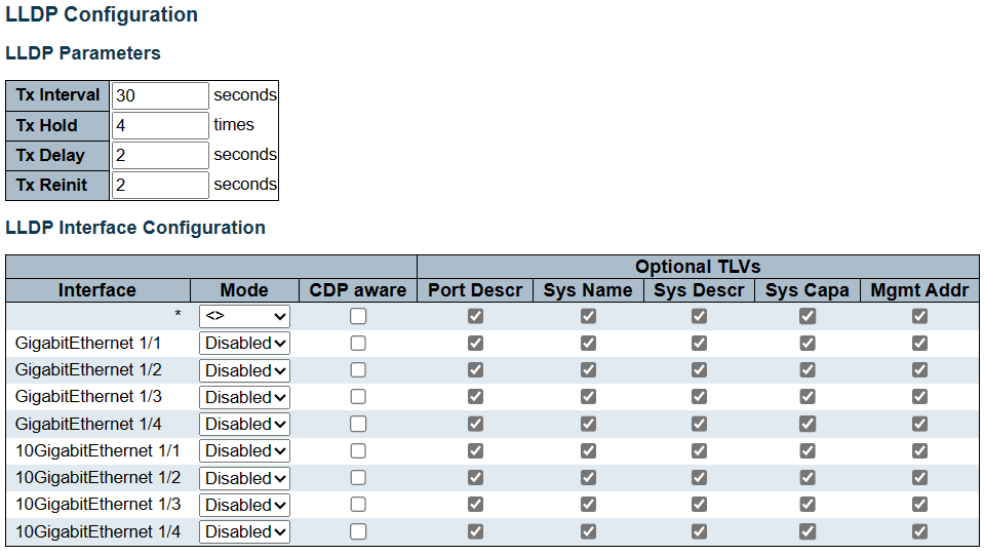
6.11. LLDP

6.11.1. LLDP Configuration

6.11.1.1. LLDP

웹메뉴 Configuration>LLDP>LLDP

이 페이지는 사용자가 현재 LLDP 인터페이스 설정을 검사하고 구성할 수 있도록 합니다.



LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

LLDP Interface Configuration

			Optional TLVs				
Interface	**Mode**	**CDP aware**	**Port Descr**	**Sys Name**	**Sys Descr**	**Sys Capa**	**Mgmt Addr**
*	<>	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/1	Disabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/2	Disabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/3	Disabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/4	Disabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/1	Disabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/2	Disabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/3	Disabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/4	Disabled	☐	☑	☑	☑	☑	☑

LLDP Configuration

LLDP Parameters

용어	설명
Tx Interval	스위치는 네트워크 검색 정보를 최신 상태로 유지하기 위해 이웃에게 주기적으로 LLDP 프레임을 전송합니다. 각 LLDP 프레임 사이의 간격은 Tx 간격 값에 의해 결정됩니다. 유효한 값은 5 에서 32768 초로 제한됩니다.
Tx Hold	각 LLDP 프레임에는 LLDP 프레임의 정보가 유효한 기간이 포함됩니다. LLDP 정보의 유효 기간은 Tx Hold 에 Tx Interval 초를 곱한 값으로 설정됩니다. 유효한 값은 2 에서 10 배로 제한됩니다.
Tx Delay	만약 구성이 변경되었을 경우 (예: IP 주소 변경), 새로운 LLDP 프레임이 전송되지만 LLDP 프레임 사이의 시간은 항상 Tx Delay 초 이상이어야 합니다. Tx Delay 는 Tx Interval 값의 1/4 보다 크지 않아야 합니다. 유효한 값은 1 에서 8192 초로 제한됩니다.
Tx Reinit	인터페이스가 비활성화되거나 LLDP 가 비활성화되었거나 스위치가 될 때 LLDP 종료 프레임이 이웃 장치로 전송되어 LLDP 정보가 더 이상 유효하지 않음을 알립니다. Tx Reini 은 종료 프레임과 새로운 LLDP 초기화 사이의 시간(초)을 제어합니다. 유효한 값은 1 에서 10 초로 제한됩니다.

LLDP Interface Configuration

용어	설명
Interface	논리적인 LLDP 인터페이스의 스위치 인터페이스 이름입니다.
Mode	LLDP 모드를 선택하세요. **Rx only** 스위치는 LLDP 정보를 보내지 않지만 이웃 장치로부터 수신한 LLDP 정보를 분석합니다. **Tx only** 스위치는 이웃 장치로부터 수신한 LLDP 정보를 버리지만 LLDP 정보를 보냅니다. **Disabled** 스위치는 LLDP 정보를 보내지 않으며 이웃 장치로부터 수신한 LLDP 정보를 버립니다. **Enabled** 스위치는 LLDP 정보를 보내며 이웃 장치로부터 수신한 LLDP 정보를 분석합니다.
CDP Aware	CDP 인식을 선택하세요. CDP 작업은 수신된 CDP 프레임의 분석으로 제한됩니다 (스위치는 CDP 프레임을 전송하지 않음). CDP 프레임은 인터페이스의 LLDP 가 활성화된 경우에만 분석됩니다. LLDP 이웃 테이블의 해당 필드에 매핑될 수 있는 CDP TLV 만 분석됩니다. 다른 모든 TLV 는 버려집니다 (인식되지 않은 CDP TLV 와 버려진 CDP 프레임은 LLDP 통계에 표시되지 않음). CDP TLV 는 아래에 표시된 대로 LLDP 이웃 테이블로 매핑됩니다. CDP TLV "장치 ID"는 LLDP "시스템 ID" 필드로 매핑됩니다. CDP TLV "주소"는 LLDP "관리 주소" 필드로 매핑됩니다. CDP 주소 TLV 에는 여러 주소가 포함될 수 있지만 LLDP 이웃 테이블에는 첫 번째 주소만 표시됩니다. CDP TLV "포트 ID"는 LLDP "포트 ID" 필드로 매핑됩니다. CDP TLV "버전 및 플랫폼"은 LLDP "시스템 설명" 필드로 매핑됩니다. CDP 와 LLDP 모두 "시스템 기능"을 지원하지만 CDP 기능은 LLDP 의 일부가 아닌 기능을 포함합니다. 이러한 기능은 LLDP 이웃 테이블에서 "기타"로 표시됩니다. 모든 인터페이스에서 CDP 인식이 비활성화되어 있는 경우 스위치는 이웃 장치로부터 수신된 CDP 프레임을 전달합니다. 적어도 하나의 인터페이스에서 CDP 인식이 활성화된 경우 스위치에서는 모든 CDP 프레임이 종료됩니다. 참고: 인터페이스의 CDP 인식이 비활성화된 경우 CDP 정보는 즉시 제거되지 않고 보유 시간이 초과될 때 제거됩니다.
Port Descr	선택한 경우 "포트 설명"이 전송되는 LLDP 정보에 포함됩니다.
Sys Name	선택한 경우 "시스템 이름"이 전송되는 LLDP 정보에 포함됩니다.
Sys Descr	선택한 경우 "시스템 설명"이 전송되는 LLDP 정보에 포함됩니다.
Sys Capa	선택한 경우 "시스템 기능"이 전송되는 LLDP 정보에 포함됩니다.
Mgmt Addr	선택한 경우 "관리 주소"가 전송되는 LLDP 정보에 포함됩니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>LLDP>LLDP

- ✓ **LLDP Configuration**
- ✓ **LLDP Parameters**
  - ➢ ***Tx Interval***
    - ***5~32768 sec(30sec)***
  - ➢ ***Tx Hold***
    - ***2~10 times(4times)***
  - ➢ ***Tx Delay***
    - ***1~8192 sec(2sec)***
  - ➢ ***Tx Delay***
    - ***1~10 sec(2sec)***

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

- ✓ **LLDP Interface Configuration**
  - ➢ ***Mode***
    - ***Disabled | Enabled(default) | Rx Only | Tx Only***

LLDP Interface Configuration

			Optional TLVs				
Interface	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/1	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/2	Disabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/3	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/4	Rx only	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/5	Tx only	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/6	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/7	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/8	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/1	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/2	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/3	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/4	Enabled	☐	☑	☑	☑	☑	☑

  - ➢ ***CDP aware***
    - ***Disabled(default) | Enabled***

LLDP Interface Configuration

			Optional TLVs				
Interface	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/1	Enabled	☑	☑	☑	☑	☑	☑
GigabitEthernet 1/2	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/3	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/4	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/5	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/6	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/7	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/8	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/1	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/2	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/3	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/4	Enabled	☐	☑	☑	☑	☑	☑

➢ ***Optional TLVs***

➢ ***Port Descr***

- ***Disabled | Enabled(default)***

LLDP Interface Configuration

			Optional TLVs				
Interface	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/1	Enabled	☐	☐	☑	☑	☑	☑
GigabitEthernet 1/2	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/3	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/4	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/5	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/6	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/7	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/8	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/1	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/2	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/3	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/4	Enabled	☐	☑	☑	☑	☑	☑

➢ ***Sys Name***

- ***Disabled | Enabled(default)***

LLDP Interface Configuration

			Optional TLVs				
Interface	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/1	Enabled	☐	☑	☐	☑	☑	☑
GigabitEthernet 1/2	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/3	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/4	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/5	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/6	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/7	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/8	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/1	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/2	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/3	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/4	Enabled	☐	☑	☑	☑	☑	☑

➢ ***Sys Descr***

- ***Disabled | Enabled(default)***

LLDP Interface Configuration

Interface	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/1	Enabled	☐	☑	☑	☐	☑	☑
GigabitEthernet 1/2	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/3	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/4	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/5	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/6	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/7	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/8	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/1	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/2	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/3	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/4	Enabled	☐	☑	☑	☑	☑	☑

➢ ***Sys Capa***

- ***Disabled | Enabled(default)***

LLDP Interface Configuration

Interface	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/1	Enabled	☐	☑	☑	☑	☐	☑
GigabitEthernet 1/2	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/3	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/4	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/5	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/6	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/7	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/8	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/1	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/2	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/3	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/4	Enabled	☐	☑	☑	☑	☑	☑

➢ ***Mgmt Addr***

- ***Disabled | Enabled(default)***

LLDP Interface Configuration

Interface	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/1	Enabled	☐	☑	☑	☑	☑	☐
GigabitEthernet 1/2	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/3	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/4	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/5	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/6	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/7	Enabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/8	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/1	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/2	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/3	Enabled	☐	☑	☑	☑	☑	☑
10GigabitEthernet 1/4	Enabled	☐	☑	☑	☑	☑	☑

CLI 설정 예시

✓ **LLDP Configuration**

✓ **LLDP Parameters**

➢ ***Tx Interval***

- ***5~32768 sec(30sec)***

```
(config)# lldp timer <val>
(config)# lldp timer 30
```

➢ ***Tx Hold***

- ***2~10 times(4times)***

```
(config)# lldp holdtime <val>
(config)# lldp holdtime 4
```

➢ ***Tx Delay***

- ***1~8192 sec(2sec)***

```
(config)# lldp transmission-delay <val>
(config)# lldp transmission-delay 2
```

➢ ***Tx Delay***

- ***1~10 sec(2sec)***

```
(config)# lldp transmission-delay <val>
(config)# lldp reinit 2
```

✓ **LLDP Interface Configuration**

➢ ***Mode***

- ***Disabled | Enabled(default) | Rx Only | Tx Only***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# lldp receive
(config-if)# lldp transmit
Enabled
(config-if)# lldp receive
(config-if)# lldp transmit
Disabled
(config-if)# no lldp receive
(config-if)# no lldp transmit
Rx Only
(config-if)# lldp receive
(config-if)# no lldp transmit
Tx Only
(config-if)# no lldp receive
(config-if)# lldp transmit
```

➢ ***CDP aware***

- ***Disabled(default) | Enabled***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# lldp cdp-aware
```

- ***Optional TLVs***
- ***Port Descr***
  - ***Disabled | Enabled(default)***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# lldp tlv-select port-description
```

- ***Sys Name***
  - ***Disabled | Enabled(default)***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# lldp tlv-select system-name
```

- ***Sys Descr***
  - ***Disabled | Enabled(default)***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# lldp tlv-select system-description
```

- ***Sys Capa***
  - ***Disabled | Enabled(default)***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# lldp tlv-select system-capabilities
```

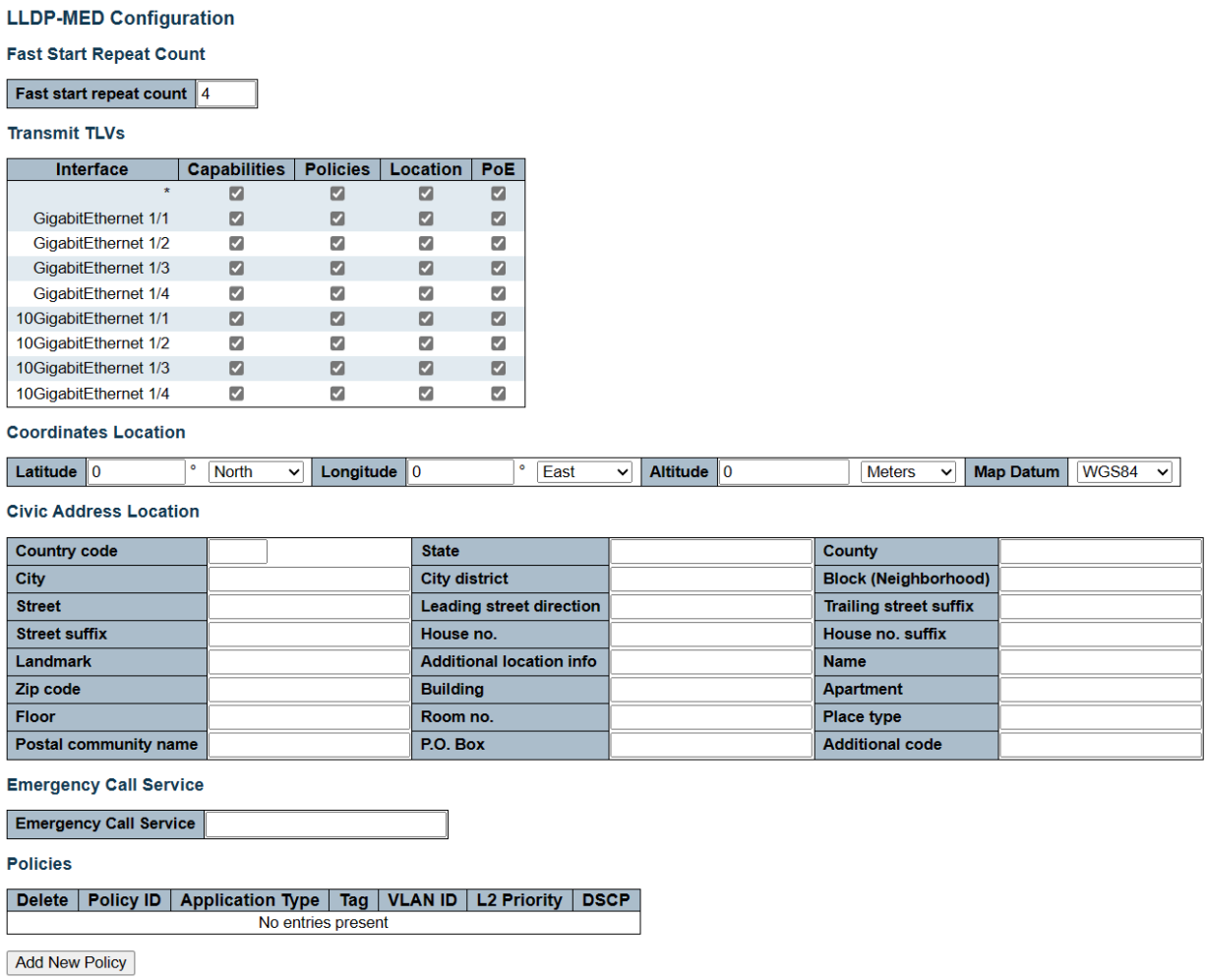
- ***Mgmt Addr***
  - ***Disabled | Enabled(default)***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# lldp tlv-select management-address
```

6.11.1.2. LLDP-MED

웹메뉴 Configuration>LLDP>LLDP-MED

이 페이지에서는 LLDP-MED 를 구성할 수 있습니다. 이 기능은 LLDP-MED 를 지원하는 VoIP 장치에 적용됩니다.



LLDP-MED Configuration

Fast Start Repeat Count

용어	설명
Fast start repeat count	일반적으로 VoIP 시스템에서는 엔드포인트의 신속한 시작 및 긴급 호출 서비스 위치 식별을 위한 LLDP-MED(LINK LAYER DISCOVERY PROTOCOL - MEDIA ENDPOINT DISCOVERY)가 매우 중요한 측면입니다. 또한, 네트워크 정책과 관련된 특정 엔드포인트 유형에 대해서만 관련 정보를 알리는 것이 좋습니다 (예: 허용된 음성 기능 장치에만 음성 네트워크 정책을 알리도록 한정). 이는 제한된 LLDPU 공간을 보존하고 부적절한 네트워크 정책에 대한 알림으로 인한 보안 및 시스템 무결성 문제를 감소시키기 위함입니다. 이러한 목표를 달성하기 위해 LLDP-MED 는 프로토콜과 프로토콜 상위의 응용 계층 간에 LLDP-MED Fast Start 상호작용을 정의합니다. 초기에는 네트워크 연결 장치는 LLDP TLV 를 LLDPDU 에서만 전송합니다. LLDP-MED 엔드포인트 장치가 감지되면, LLDP-

	MED 기능을 갖춘 네트워크 연결 장치는 관련 인터페이스의 외부 LLDPDU 에서 LLDP-MED TLV 를 알리기 시작합니다. LLDP-MED 애플리케이션은 새로운 LLDP-MED 이웃이 감지되면 LLDPDU 전송 속도를 일시적으로 1 초 이내로 가속화하여 새 이웃에게 가능한 빠르게 LLDP-MED 정보를 공유하기 위해 시작됩니다. 이웃간의 LLDP 프레임 전송 중 프레임이 손실될 위험이 있으므로, Fast start 반복 횟수를 지정하여 Fast start 전송을 여러 번 반복하는 것이 권장됩니다. 권장되는 값은 4 회이며, 새로운 정보가 포함된 LLDP 프레임을 수신할 때 1 초 간격으로 4 개의 LLDP 프레임이 전송됩니다. LLDP-MED 및 LLDP-MED Fast Start 메커니즘은 LLDP-MED 네트워크 연결 장치와 엔드포인트 장치 사이의 링크에서만 실행되도록 설계되었으며, 네트워크 연결 장치를 포함한 LAN 인프라 요소 또는 다른 유형의 링크에는 적용되지 않음에 유의해야 합니다.

Transmit TLVs

용어	설명
Transmit TLVs	이웃에게 전송할 LLDP-MED 정보를 선택할 수 있습니다. 체크박스가 선택되면 해당 정보가 이웃에게 전송되는 프레임에 포함됩니다.
Interface	구성이 적용되는 인터페이스 이름입니다.
Capabilities	체크하면 스위치의 기능이 LLDP-MED 정보에 포함됩니다.
Policies	체크하면 인터페이스에 대한 구성된 정책이 LLDP-MED 정보에 포함됩니다.
Location	체크하면 스위치에 대한 구성된 위치 정보가 LLDP-MED 정보에 포함됩니다.
PoE	체크하면 인터페이스에 대한 구성된 PoE (Power Over Ethernet) 정보가 LLDP-MED 정보에 포함됩니다.

Coordinates Location

용어	설명
Coordinates Location	이 섹션은 스위치의 좌표를 설정할 수 있습니다.
Latitude	위도는 적도를 기준으로 남쪽으로 내려갈 때 음수로, 북쪽으로 올라갈 때 양수로 표현되며, 0 부터 90 도 사이의 값으로 설정합니다. 최대 소수점 4 자리까지 설정할 수 있습니다.
Longitude	경도는 본초 자오선을 기준으로 동쪽으로 갈 때 양수로, 서쪽으로 갈 때 음수로 표현되며, 0 부터 180 도 사이의 값으로 설정합니다. 최대 소수점 4 자리까지 설정할 수 있습니다.
Altitude	고도는 -2097151.9 에서 2097151.9 사이의 값으로 설정하며, 최대 소수점 1 자리까지 설정할 수 있습니다. 또한, 두 가지 고도 유형(층 또는 미터) 중에서 선택할 수 있습니다. 미터(Meters): 수직 기준으로 정의된 높이로써 미터로 표시됩니다. 층(Floors): 건물 내에서 보다 관련성 있는 형태로 고도를 나타냅니다. 층 간 차원이 다른 건물에서 유용합니다. 고도 0.0 은 건물 외부에서도 의미가 있으며, 주어진 위도와 경도에서의 지면 높이를 나타냅니다. 건물 내부에서는 0.0 은 주 출입구의 지면 수준에 해당하는 층을 나타냅니다.
Map Datum	이러한 옵션에서 제공되는 좌표에는 지도 데이터가 사용됩니다: WGS84: (지리적 3D) - 1984 년 세계 기구계(WGS84), CRS 코드 4327, 본초 자오선 이름: 그리니치. NAD83/NAVD88: 1983 년 북아메리카 기준점(NAD83), CRS 코드 4269, 본초 자오선 이름: 그리니치; 관련 수직 기준점은 1988 년 북아메리카 수직 기준점(NAVD88)입니다. 이 기준점 쌍은 해변가 근처가 아닌 땅 위의 위치를 참조할 때 사용됩니다(해양 기준점 = NAD83/MLLW). NAD83/MLLW: 1983 년 북아메리카 기준점(NAD83), CRS 코드 4269, 본초 자오선 이름:

	그리니치; 관련 수직 기준점은 평균 하부 저조 수위(Mean Lower Low Water, MLLW)입니다. 이 기준점 쌍은 물/해/양 위치를 참조할 때 사용됩니다.

Civic Address Location

용어	설명
Civic Address Location	IETF Geopriv Civic Address 기반 위치 구성 정보(Civic Address LCI)의 경우, 결합된 도시 주소 정보의 총 문자 수는 250 자를 초과해서는 안 됩니다. 250 자 제한에 대한 몇 가지 주의 사항이 있습니다. 1. 비어 있지 않은 도시 주소 위치는 도시 주소 위치 텍스트에 추가로 2 개의 문자를 사용합니다. 2. 2 자리 국가 코드는 250 자 제한에 포함되지 않습니다.
Country code	대문자 ASCII 글자로 된 ISO 3166 국가 코드는 2 자리로 구성되며, 예를 들어 DK(덴마크), DE(독일), US(미국) 등이 있습니다.
State	국가의 하위 지역구분(주(State), 칸톤(Canton), 지역(Region), 도(Province), 현(Prefecture))을 말합니다.
County	군(County), 교구(Parish), 군(Gun), 구(District)입니다.
City	도시(City), 시(시군구), 예를 들어 서울(Seoul)입니다.
City district	시구(City division), 자치구(Borough), 도시 구역(City district), 와드(Ward)입니다.
Block (Neighborhood)	동네(Neighborhood), 블록(Block)입니다.
Street	거리(Street) - 예시: Poppelvej (포펠베이)
Leading street direction	선행 거리 방향(Leading street direction) - 예시: N (북)
Trailing street suffix	뒤따르는 거리 접미사(Trailing street suffix) - 예시: SW (남서)
Street suffix	거리 접미사(Street suffix) - 예시: Ave (번지), Platz (광장)
House no.	건물 번호(House number) - 예시: 21
House no. suffix	건물 번호 접미사(House number suffix) - 예시: A (에이), 1/2 (일 분의 이)
Landmark	랜드마크 또는 대표 주소(Landmark or vanity address) - 예시: Columbia University (콜롬비아 대학교)
Additional location info	추가 위치 정보(Additional location info) - 예시: South Wing (남쪽 윙)
Name	이름 (거주 및 사무실 사용자) - 예시: Flemming Jahn (플레밍 얀)
Zip code	우편 번호/우편 코드 (Postal/zip code) - 예시: 2791
Building	건물 (구조) - 예시: Low Library (로우 도서관)
Apartment	유닛 (아파트, 스위트) - 예시: Apt 42 (42 호 아파트)
Floor	층수 (Floor) - 예시: 4 층
Room no.	호실 번호 (Room number) - 예시: 450F (450F 호)
Place type	장소 유형 (Place type) - 예시: 사무실
Postal community name	우편 커뮤니티 이름 (Postal community name) - 예시: Leonia (레오니아)
P.O. Box	우편 사서함 (P.O. BOX) - 예시: 12345
Additional code	추가 코드 (Additional code) - 예시: 1320300003

Emergency Call Service

용어	설명
Emergency Call Service	비상 호출 서비스(E911 및 기타)는 TIA 또는 NENA 에 의해 정의된 것과 같이, 비상 호출 서비스를 의미합니다. ELIN 식별자 데이터 형식은 전통적인 CAMA 또는 ISDN 트렁크 기반 PSAP 로의 비상 호출 설정 중 사용되는 ELIN 식별자를 전달하기 위해 정의됩니다. 이 형식은 비상 호출에 사용되는 ELIN 에 해당하는 숫자로 이루어진 숫자 문자열로 구성됩니다.

Policies

용어	설명
Policies	네트워크 정책 탐색(Network Policy Discovery)은 VLAN 구성과 관련된 불일치 문제의 효율적인 발견과 진단을 가능하게 합니다. 이는 특정 프로토콜 응용 프로그램에 대해 적용되는 관련 Layer 2 및 Layer 3 속성과 함께 작동합니다. 부적절한 네트워크 정책 설정은 음성 품질 저하나 서비스 중단과 같은 VoIP 환경에서 매우 중요한 문제입니다. 정책은 주로 대화식 음성 및/또는 비디오 서비스와 같은 '실시간' 네트워크 정책 요구사항이 있는 응용 프로그램에 사용됩니다. 광고된 네트워크 정책 속성은 다음과 같습니다: 1. Layer 2 VLAN ID (IEEE 802.1Q003) 2. Layer 2 priority value (IEEE 802.1D004) 3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474) 이 네트워크 정책은 특정 포트에서 지원되는 여러 응용 프로그램 유형 집합과 연결될 수 있습니다. 구체적으로 다루는 응용 프로그램 유형은 다음과 같습니다: 1. 음성 2. 게스트 음성 3. 소프트 폰 음성 4. 비디오 회의 5. 스트리밍 비디오 6. 제어/신호 (위의 미디어 유형에 대해 별도의 네트워크 정책을 조건적으로 지원) 대규모 네트워크에서는 조직 전체에 걸쳐 여러 VoIP 정책을 지원하며, 응용 프로그램 유형별로 다른 정책을 사용할 수 있습니다. LLDP-MED 는 각각 다른 응용 프로그램 유형에 해당하는 여러 정책을 포트당 광고할 수 있도록 합니다. 동일한 네트워크 연결 장치의 다른 포트는 인증된 사용자 식별 또는 포트 구성에 따라 다른 정책 집합을 광고할 수 있습니다. LLDP-MED 는 네트워크 연결 장치와 엔드 포인트 간의 링크 외에 다른 링크에서 실행되지 않으며, 따라서 LAN 내부에서 빈번히 실행되는 다양한 네트워크 정책을 광고할 필요가 없습니다.
Delete	정책을 삭제할 것인지 체크하세요. 다음 저장 시에 정책이 삭제될 것입니다.
Policy ID	해당 정책을 선택하여 특정 인터페이스에 매핑할 때 사용할 ID 는 자동으로 생성되며, 이를 사용해야 합니다.
Application Type	다음은 각 응용 프로그램 유형의 의도적인 사용 사례입니다: 1. 음성 - 전용 IP 전화기 및 대화형 음성 서비스를 지원하는 유사한 장치에서 사용합니다. 이러한 장치는 일반적으로 데이터 응용 프로그램과 격리되어 배치 및 보안이 향상되도록 별도의 VLAN 에 배치됩니다. 2. 음성 신호 (조건적) - 음성 신호와 음성 미디어에 대해 서로 다른 정책이 필요한 네트워크 토폴로지에서 사용합니다. 음성 응용 프로그램 정책으로 광고되는 것과 동일한 네트워크 정책이 적용되는 경우에는 이 응용 프로그램 유형을 광고하지 않아야 합니다.

	3. 게스트 음성 - 게스트 사용자 및 방문자를 위한 별도의 '제한된 기능 집합' 음성 서비스를 지원합니다. 이들은 자체 IP 전화기 및 대화형 음성 서비스를 지원하는 유사한 장치를 사용합니다. 4. 게스트 음성 신호 (조건적) - 게스트 음성 신호와 게스트 음성 미디어에 대해 서로 다른 정책이 필요한 네트워크 토폴로지에서 사용합니다. 게스트 음성 응용 프로그램 정책으로 광고되는 것과 동일한 네트워크 정책이 적용되는 경우에는 이 응용 프로그램 유형을 광고하지 않아야 합니다. 5. 소프트 폰 음성 - 일반적인 데이터 중심 장치(예: PC 또는 노트북)에서 소프트 폰 응용 프로그램을 사용합니다. 이 종류의 엔드 포인트는 종종 여러 VLAN 을 지원하지 않거나 지원하지 않을 수 있으며 일반적으로 '태그되지 않은' VLAN 이나 단일 '태그된' 데이터 전용 VLAN 을 사용하도록 구성됩니다. '태그되지 않은' VLAN 에 대해 네트워크 정책이 정의된 경우 (아래의 '태그 여부' 플래그 참조), L2 우선순위 필드는 무시되고 DSCP 값만 관련이 있습니다. 6. 비디오 회의 - 전용 비디오 회의 장비 및 실시간 대화형 비디오/오디오 서비스를 지원하는 유사한 장치에서 사용합니다. 7. 스트리밍 비디오 - 방송이나 멀티캐스트 기반의 비디오 콘텐츠 배포 및 특정 네트워크 정책 처리를 지원하는 유사한 응용 프로그램에서 사용합니다. 버퍼링을 위해 TCP 를 사용하는 비디오 응용 프로그램은 이 응용 프로그램 유형의 의도된 사용 사례가 아닙니다. 8. 비디오 신호 (조건적) - 비디오 신호와 비디오 미디어에 대해 별도의 정책이 필요한 네트워크 토폴로지에서 사용합니다. 비디오 회의 응용 프로그램 정책으로 광고되는 것과 동일한 네트워크 정책이 적용되는 경우에는 이 응용 프로그램 유형을 광고하지 않아야 합니다.
Tag	지정된 응용 프로그램 유형이 '태그된(tagged)' VLAN 을 사용하는지 아니면 '태그되지 않은(untagged)' VLAN 을 사용하는지를 나타내는 태그입니다. '태그되지 않은(untagged)' VLAN 을 사용하는 경우, 장치는 IEEE 802.1Q003 에서 정의한 태그 헤더를 포함하지 않은 태그되지 않은 프레임 형식을 사용합니다. 이 경우, VLAN ID 와 Layer 2 우선순위 필드는 무시되고 DSCP 값만이 관련이 있습니다. 반면 '태그된(tagged)' VLAN 을 사용하는 경우, 장치는 IEEE 802.1Q 태그 프레임 형식을 사용하며, VLAN ID 와 Layer 2 우선순위 값만이 아닌 DSCP 값도 사용됩니다. 태그된 형식에는 추가적인 필드인 태그 헤더가 포함됩니다. 태그된 프레임 형식은 또한 IEEE 802.1Q003 에서 정의한 우선순위 태그된 프레임도 포함합니다.
VLAN ID	IEEE 802.1Q003 에서 정의된 인터페이스의 VLAN 식별자(VLAN ID)입니다.
L2 Priority	지정된 응용 프로그램 유형에 사용할 Layer 2 우선순위(L2 Priority)입니다. L2 우선순위는 IEEE 802.1D004 에서 정의된 0 부터 7 까지의 여덟 개의 우선순위 수준 중 하나를 지정할 수 있습니다. 값 0 은 IEEE 802.1D004 에서 정의된 기본 우선순위를 사용함을 나타냅니다.
DSCP	지정된 응용 프로그램 유형에 대한 Diffserv 노드 동작을 제공하기 위해 사용할 DSCP(Differentiated Services Code Point) 값입니다. 이는 IETF RFC 2474 에서 정의된 대로 0 부터 63 까지의 64 개 코드 포인트 값 중 하나를 포함할 수 있습니다. 값 0 은 RFC 2475 에서 정의된 기본 DSCP 값을 사용함을 나타냅니다.

Adding a new policy

용어	설명
Adding a new policy	새 정책을 추가하려면 " Add New Policy"를 클릭하십시오. 새 정책에 대해 응용 프로그램 유형, 태그, VLAN ID, L2 우선순위 및 DSCP 를 지정하십시오. 그런 다음 "저장"을 클릭하십시오. 지원되는 정책 수는 32 개입니다.
Policies Interface	인증된 사용자 식별 정보 또는 인터페이스 구성에 따라 각 인터페이스는 고유한 네트워크 정책 집합 또는 동일한 네트워크 정책에 대한 다른 속성을 알릴 수 있습니다.

Configuration	
Interface	이 구성이 적용되는 인터페이스의 이름입니다.
Policy Id	특정 인터페이스에 적용되는 정책 집합입니다. 정책 집합은 해당 정책에 해당하는 체크박스를 선택하여 선택됩니다.

Buttons

Add New Policy: 클릭시 새 Policy을 추가 할 수 있습니다.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

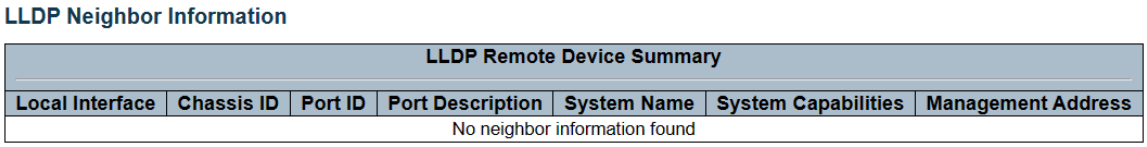
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

6.11.2. LLDP Monitor

6.11.2.1. Neighbors

웹메뉴 Monitor>LLDP>Neighbors

이 페이지는 모든 LLDP 이웃에 대한 상태 개요를 제공합니다.


LLDP Neighbor Information

LLDP Remote Device Summary						
Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
No neighbor information found						

LLDP Neighbor Information

표에는 LLDP 이웃이 감지된 각 인터페이스에 대한 행이 표시됩니다. 열에는 다음과 같은 정보가 포함됩니다.

용어	설명
Local Interface	LLDP 프레임을 수신한 인터페이스입니다.
Chassis ID	Chassis ID 는 이웃의 LLDP 프레임의 식별자입니다.
Port ID	Port ID 는 이웃 포트의 식별자입니다.
Port Description	Port Description 은 이웃 장치에서 알리는 포트 설명입니다.
System Name	시스템 이름은 이웃 장치에서 알리는 이름입니다.
System Capabilities	시스템 기능은 이웃 장치의 기능을 설명합니다. 1. 기타 (Other) 2. 중계기 (Repeater) 3. 브리지 (Bridge) 4. WLAN 액세스 포인트 (WLAN Access Point) 5. 라우터 (Router) 6. 전화기 (Telephone) 7. DOCSIS 케이블 장치 (DOCSIS cable device) 8. 스테이션 전용 (Station only) 9. 예약됨 (Reserved) 기능이 활성화된 경우, 기능 뒤에 (+)가 붙습니다. 기능이 비활성화된 경우, 기능 뒤에 (-)가 붙습니다.
Management Address	관리 주소는 네트워크 관리를 지원하기 위해 상위 계층 개체에서 사용되는 이웃 장치의 주소입니다. 예를 들어, 이웃의 IP 주소를 포함할 수 있습니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh: 클릭 시 페이지를 새로 고침.

WEB 확인 예시

웹메뉴 Monitor>LLDP>Neighbors

✓ LLDP Neighbor Information

LLDP Neighbor Information

LLDP Remote Device Summary						
Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
GigabitEthernet 1/8	00-21-6D-01-02-03	5	GigabitEthernet 1/5	SFC8000GHP	Bridge(+)	172.30.1.30 (IPv4)

CLI 확인 예시

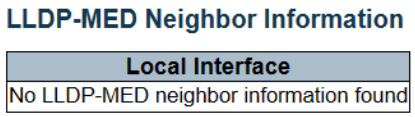
✓ LLDP Neighbor Information

```
# show lldp neighbors
Local Interface     : GigabitEthernet 1/8
Chassis ID          : 00-21-6D-01-02-03
Port ID             : 5
Port Description    : GigabitEthernet 1/5
System Name         : SFC8000GHP
System Description  : SFC8000GHP 2.4.0.1 2023-10-11T11:11:42+09:00
System Capabilities : Bridge(+)
Management Address  : 172.30.1.30 (IPv4)
PoE Type            : PSE Device
PoE Source          : Primary Power Source
PoE Power           : 0.0 [W]
PoE Priority        : Low Priority
```

6.11.2.2. LLDP-MED Neighbors

웹메뉴 Monitor>LLDP>LLDP-MED Neighbors

이 페이지는 모든 LLDP-MED 이웃의 상태 개요를 제공합니다.



LLDP-MED Neighbor Information

표에는 LLDP 이웃이 감지된 각 인터페이스에 대한 행이 표시됩니다. 이 기능은 LLDP-MED 를 지원하는 VoIP 장치에 적용됩니다. 열에는 다음과 같은 정보가 포함됩니다.

용어	설명
Interface	LLDP 프레임을 수신한 인터페이스입니다.
Device Type	LLDP-MED 장치는 두 가지 주요 장치 유형으로 구성됩니다: 네트워크 연결 장치(Network Connectivity Devices)와 엔드포인트 장치(Endpoint Devices). LLDP-MED 네트워크 연결 장치 정의 TIA-1057 에 정의된 LLDP-MED 네트워크 연결 장치는 LLDP-MED 엔드포인트 장치에 대한 IEEE 802 기반 LAN 인프라 접근을 제공합니다. LLDP-MED 네트워크 연결 장치는 다음 기술을 기반으로 하는 LAN 액세스 장치입니다: 1.LAN 스위치/라우터 2.IEEE 802.1 브리지 3.IEEE 802.3 중계기 (역사적인 이유로 포함됨) 4.IEEE 802.11 무선 액세스 포인트 5.IEEE 802 프레임을 어떤 방법으로든 중계할 수 있는 TIA-1057 에서 정의한 IEEE 802.1AB 및 MED 확장을 지원하는 장치 LLDP-MED 엔드포인트 장치 정의 TIA-1057 에 정의된 LLDP-MED 엔드포인트 장치는 IEEE 802 LAN 네트워크 가장자리에 위치하며, LLDP-MED 프레임워크를 사용하여 IP 통신 서비스에 참여합니다. LLDP-MED 엔드포인트 장치 범주 내에서 LLDP-MED 체계는 다음과 같이 추가적인 엔드포인트 장치 클래스로 분류됩니다. 각 LLDP-MED 엔드포인트 장치 클래스는 이전 엔드포인트 장치 클래스에 정의된 기능을 기반으로 구축됩니다. 예를 들어, 미디어 엔드포인트(Class II)로 규정된 LLDP-MED 엔드포인트 장치는 일반 엔드포인트(Class I)에 해당하는 TIA-1057 의 모든 측면을 지원하며, 커뮤니케이션 장치(Class III)로 규정된 LLDP-MED 엔드포인트 장치는 미디어 엔드포인트(Class II)와 일반 엔드포인트(Class I)에 해당하는 TIA-1057 의 모든 측면을 지원합니다. LLDP-MED 일반 엔드포인트 (Class I)

	LLDP-MED 일반 엔드포인트 (Class I) 정의는 TIA-1057 에서 정의된 기본 LLDP 검색 서비스가 필요한 모든 엔드포인트 제품에 적용됩니다. 그러나 IP 미디어를 지원하지 않거나 최종 사용자 통신 장치로 작동하지 않는 장치에 해당합니다. 이러한 장치에는 (하지만 이에 국한되지 않음) IP 통신 컨트롤러, 기타 통신 관련 서버 또는 TIA-1057 에서 정의한 기본 서비스를 필요로하는 장치가 포함될 수 있습니다. 이 클래스에서 정의된 검색 서비스에는 LAN 구성, 장치 위치, 네트워크 정책, 전력 관리 및 재고 관리가 포함됩니다. LLDP-MED 미디어 엔드포인트 (Class II) LLDP-MED 미디어 엔드포인트 (Class II) 정의는 IP 미디어 기능을 갖춘 모든 엔드포인트 제품에 적용됩니다. 그러나 특정 사용자와 관련이 있을 수도 있고 없을 수도 있습니다. 이전의 일반 엔드포인트 클래스(Class I)에 정의된 모든 기능을 포함하며, 미디어 스트리밍과 관련된 측면을 추가로 포함합니다. 이 클래스에 준수하는 예상 제품 범주에는 (하지만 이에 국한되지 않음) 음성/미디어 게이트웨이, 회의 다리, 미디어 서버 등이 있습니다. 이 클래스에서 정의된 검색 서비스에는 미디어 유형별 네트워크 계층 정책 검색이 포함됩니다. LLDP-MED 커뮤니케이션 엔드포인트 (Class III) LLDP-MED 커뮤니케이션 엔드포인트 (Class III) 정의는 IP 미디어를 지원하는 최종 사용자 통신 장치로 작동하는 모든 엔드포인트 제품에 적용됩니다. 이전의 일반 엔드포인트(Class I) 및 미디어 엔드포인트(Class II) 클래스에 정의된 모든 기능을 포함하며, 최종 사용자 장치와 관련된 측면을 추가로 포함합니다. 이 클래스에 준수하는 예상 제품 범주에는 (하지만 이에 국한되지 않음) IP 전화기, PC 기반 소프트폰 또는 최종 사용자를 직접 지원하는 기타 통신 장치 등이 있습니다. 이 클래스에서 정의된 검색 서비스에는 위치 식별자 제공 (ECS / E911 정보 포함), 내장형 L2 스위치 지원, 재고 관리가 포함됩니다.
LLDP-MED Capabilities	LLDP-MED 기능은 이웃 장치의 LLDP-MED 기능을 설명합니다. 가능한 기능은 다음과 같습니다: 1. LLDP-MED 기능 2. 네트워크 정책 3. 위치 식별 4. 확장된 전원 (MDI-PSE 를 통한) 5. 확장된 전원 (MDI-PD 를 통한) 6. 재고 7. 예약됨
Application Type	네트워크 정책에서 정의된 애플리케이션의 주요 기능을 나타내는 애플리케이션 유형입니다. Endpoint 또는 Network Connectivity 장치에 의해 알려진 가능한 애플리케이션 유형은 다음과 같습니다. 1. 음성 - 전용 IP 전화기 및 대화식 음성 서비스를 지원하는 유사한 기기에서 사용합니다. 이러한 기기는 일반적으로 데이터 애플리케이션으로부터 격리되어 배치의 편의성과 보안을 향상시키기 위해 별도의 VLAN 에 배치됩니다. 2. 음성 신호 - 음성 신호 및 음성 미디어에 대해 별도의 정책이 필요한 네트워크 토폴로지에서 사용합니다. 3. 게스트 음성 - 게스트 사용자와 방문자를 위한 별도의 제한된 기능 집합의 음성

	서비스를 지원하기 위해 사용합니다. 게스트는 자체 IP 전화기 및 대화식 음성 서비스를 지원하는 유사한 기기를 사용합니다. 4. 게스트 음성 신호 - 게스트 음성 신호 및 게스트 음성 미디어에 대해 별도의 정책이 필요한 네트워크 토폴로지에서 사용합니다. 5. 소프트폰 음성 - 일반적인 데이터 중심 장치인 PC 나 노트북에서 소프트폰 애플리케이션에 사용합니다. 6. 비디오 컨퍼런싱 - 전용 비디오 컨퍼런싱 장비 및 실시간 대화식 비디오/오디오 서비스를 지원하는 유사한 기기에 사용합니다. 7. 스트리밍 비디오 - 방송이나 다중 캐스트를 기반으로 하는 비디오 콘텐츠 배포 및 스트리밍 비디오 서비스를 지원하는 유사한 응용 프로그램에 사용됩니다. 버퍼링과 TCP 에 의존하는 비디오 애플리케이션은 이 애플리케이션 유형의 의도된 사용이 아닙니다. 8. 비디오 신호 - 비디오 신호 및 비디오 미디어에 대해 별도의 정책이 필요한 네트워크 토폴로지에서 사용합니다.
Policy	Policy 는 Endpoint Device 가 해당 정책이 장치에서 요구되는 것임을 명시적으로 알리고자 함을 나타냅니다. Unknown: 지정된 애플리케이션 유형의 네트워크 정책이 현재 알려지지 않았습니다. Defined: 알려진 네트워크 정책이 정의되었습니다.
TAG	TAG 는 지정된 애플리케이션 유형이 태그가 있는 VLAN 또는 태그가 없는 VLAN 을 사용하는지를 나타냅니다. Untagged: 장치는 IEEE 802.1Q003 에 정의된 대로 태그 헤더가 포함되지 않은 태그 없는 프레임 형식을 사용합니다. Tagged: 장치는 IEEE 802.1Q 태그된 프레임 형식을 사용합니다.
VLAN ID	VLAN ID 는 IEEE 802.1Q003 에서 정의된 인터페이스의 VLAN 식별자 (VID)입니다. 유효한 VLAN ID 를 정의하기 위해 1 부터 4094 까지의 값이 사용됩니다. 장치가 IEEE 802.1Q003 에 정의된 우선 순위 태그가 지정된 프레임을 사용하는 경우 (우선 순위 태그가 있음), 값 0 (우선 순위 태그 지정)이 사용됩니다. 이 경우에는 IEEE 802.1D 우선 순위 레벨만 중요하며, 인입 인터페이스의 기본 PVID 가 대신 사용됩니다.
Priority	Priority 는 지정된 애플리케이션 유형에 사용되는 Layer 2 우선 순위를 나타냅니다. 0 부터 7 까지의 여덟 개의 우선 순위 레벨 중 하나를 사용할 수 있습니다.
DSCP	DSCP 는 지정된 애플리케이션 유형에 대해 Diffserv 노드 동작을 제공하기 위해 사용할 DSCP 값입니다. 이 값은 IETF RFC 2474 에서 정의된 대로 0 부터 63 까지의 64 개의 코드 포인트 값 중 하나를 포함합니다.
Auto-negotiation	자동 협상은 링크 파트너가 MAC/PHY 자동 협상을 지원하는지 여부를 식별합니다.
Auto-negotiation status	자동 협상 상태는 현재 링크 파트너에서 자동 협상이 활성화되어 있는지 여부를 나타냅니다. 자동 협상이 지원되지만 자동 협상 상태가 비활성화된 경우, 802.3 PMD 동작 모드는 자동 협상이 아닌 운용 MAU 유형 필드 값에 의해 결정됩니다.
Auto-negotiation Capabilities	자동 협상 기능은 링크 파트너의 MAC/PHY 기능을 나타냅니다.

Buttons

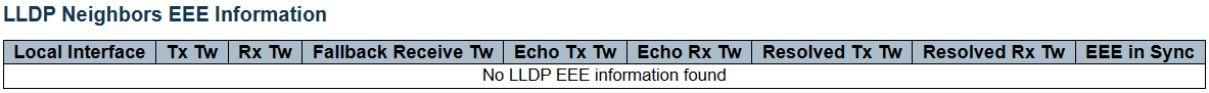
Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh: 클릭 시 페이지를 새로 고침.

6.11.2.3. EEE

웹메뉴 Monitor>LLDP>EEE

EEE(Energy-Efficient Ethernet)를 사용함으로써 전력 절약이 가능하지만 트래픽 지연이 발생할 수 있습니다. 이러한 지연은 전력 절약을 위해 회로의 EEE(Energy-Efficient Ethernet)가 꺼져 있어 트래픽을 전송하기 전에 부팅하는 시간이 필요하기 때문입니다. 이 시간을 "웨이크업 시간"이라고 합니다. 최소한의 지연을 달성하기 위해 장치는 LLDP 를 사용하여 각각의 송신 및 수신 "웨이크업 시간"에 대한 정보를 교환하여 필요한 최소 웨이크업 시간에 동의하는 방식으로 사용할 수 있습니다.
이 페이지는 LLDP 에 의해 교환되는 EEE 정보에 대한 개요를 제공합니다.



LLDP Neighbors EEE Information

Local Interface	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
No LLDP EEE information found								

LLDP Neighbors EEE Information

표에는 각 인터페이스마다 한 줄이 표시됩니다.
인터페이스가 EEE 를 지원하지 않는 경우 "EEE not supported for this interface"으로 표시됩니다.
특정 인터페이스에서 EEE 가 활성화되지 않은 경우 "EEE not enabled for this interface"으로 표시됩니다.
링크 파트너가 EEE 를 지원하지 않는 경우 "Link partner is not EEE capable"으로 표시됩니다.
열에는 다음과 같은 정보가 포함됩니다.

용어	설명
Local Interface	LLDP 프레임을 수신 또는 송신하는 인터페이스.
Tx Tw	링크 파트너가 LPI(Low Power Idle)를 해제한 후 데이터 전송을 지연시킬 수 있는 최대 시간.
Rx Tw	수신기가 수면 모드에서 깨어나는 데 필요한 시간 동안 전송자가 기다려야 하는 시간입니다.
Fallback Receive Tw	링크 파트너의 대체 수신 Tw(Tw_sys_rx)입니다. 수신 링크 파트너는 전송자에게 대체로 원하는 Tw_sys_tx 를 알릴 수 있습니다. 수신 링크 파트너는 일반적으로 절전을 위한 Discrete levels(이산 수준)을 가지고 있기 때문에, 이는 전송자가 더 효율적인 할당을 위해 사용할 수 있는 추가 정보를 제공합니다. 이 옵션을 구현하지 않은 시스템은 기본값으로 수신 Tw_sys_tx 와 동일한 값을 사용합니다.
Echo Tx Tw	링크 파트너의 Echo Tx Tw 값입니다. 해당 Echo 값은 로컬 링크 파트너가 원격 링크 파트너의 해당 값에 대한 반사(Echo)로 정의됩니다. 로컬 링크 파트너는 원격 링크 파트너로부터 에코된 값을 받으면 원격 링크 파트너가 가장 최근의 값을 수신, 등록 및 처리했는지 여부를 판단할 수 있습니다. 예를 들어, 로컬 링크 파트너가 에코된 매개변수를 받았는데 이 값이 로컬 MIB 의 값과 일치하지 않는다면, 로컬 링크 파트너는 원격 링크 파트너의 요청이 오래된 정보에 기반한 것임을 추론할 수 있습니다.
Echo Rx Tw	링크 파트너의 Echo Rx Tw 값입니다.
Resolved Tx Tw	이 링크에 대한 해결된 Tx Tw 입니다. 참고: 링크 파트너가 아닙니다.

	이 값은 LLDP 를 통해 교환된 EEE 정보를 기반으로 실제로 사용되는 "tx wakeup time"입니다.
Resolved Rx Tw	이 링크에 대한 해결된 Rx Tw 입니다. 참고: 링크 파트너가 아닙니다. 이 값은 LLDP 를 통해 교환된 EEE 정보를 기반으로 실제로 사용되는 "tx wakeup time"입니다.
EEE in Sync	스위치와 링크 파트너가 wakeup 시간에 동의했는지를 나타냅니다. 빨강색 - 스위치와 링크 파트너가 wakeup 시간에 동의하지 않았습니다. 초록색 - 스위치와 링크 파트너가 wakeup 시간에 동의했습니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

WEB 확인 예시

웹메뉴 Monitor>LLDP>EEE

✓ LLDP Neighbors EEE Information

LLDP Neighbors EEE Information

Local Interface	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
GigabitEthernet 1/8	EEE not enabled for this interface							

CLI 확인 예시

✓ LLDP Neighbors EEE Information

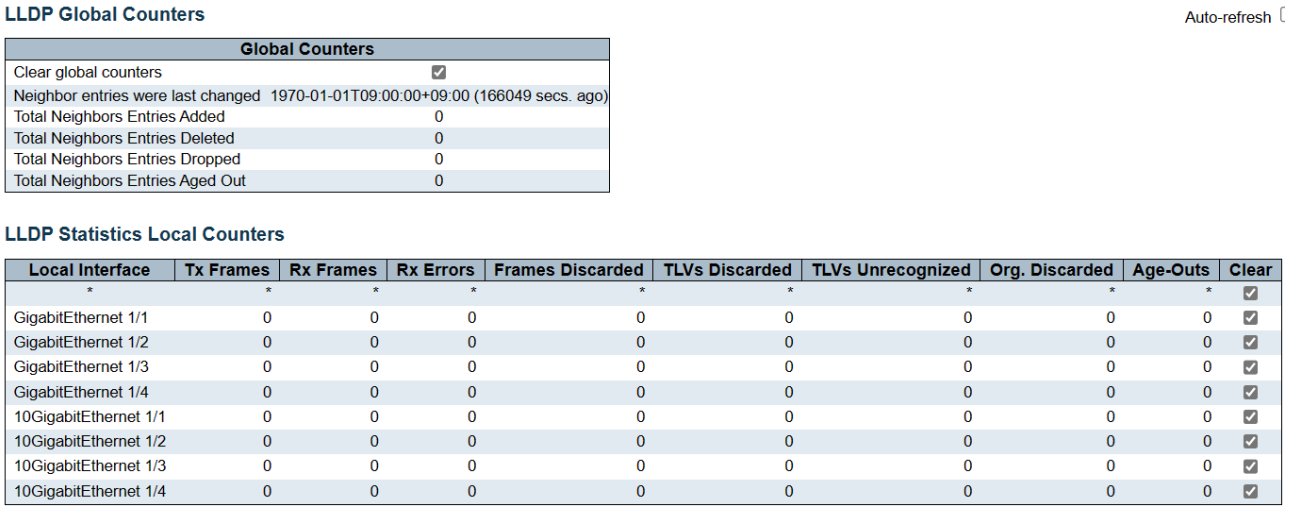
```
# show lldp eee
Local Interface     : GigabitEthernet 1/8
EEE not enabled for this interface
```

6.11.2.4. Port Statistics

웹메뉴 Monitor>LLDP>Port Statistics

이 페이지는 LLDP 트래픽에 대한 개요를 제공합니다.

전역 카운터는 전체 스위치에 대한 카운터를 나타내며, 로컬 카운터는 현재 선택된 스위치의 각 인터페이스별 카운터를 나타냅니다.


LLDP Global Counters

Auto-refresh

Global Counters	
Clear global counters	☑
Neighbor entries were last changed	1970-01-01T09:00:00+09:00 (166049 secs. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
*	*	*	*	*	*	*	*	*	☑
GigabitEthernet 1/1	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/2	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/3	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/4	0	0	0	0	0	0	0	0	☑
10GigabitEthernet 1/1	0	0	0	0	0	0	0	0	☑
10GigabitEthernet 1/2	0	0	0	0	0	0	0	0	☑
10GigabitEthernet 1/3	0	0	0	0	0	0	0	0	☑
10GigabitEthernet 1/4	0	0	0	0	0	0	0	0	☑

LLDP Global Counters

용어	설명
Global Counters	전역 카운터는 전체 스위치에 대한 카운터를 나타냅니다.
Clear global counters	체크하면 전역 카운터는 "클리어" 버튼을 누를 때 초기화됩니다.
Neighbor entries were last changed	마지막 항목이 삭제되거나 추가된 시간을 보여줍니다. 또한 마지막 변경이 감지된 이후 경과된 시간을 보여줍니다.
Total Neighbors Entries Added	스위치 재부팅 이후 추가된 새 항목의 수를 보여줍니다.
Total Neighbors Entries Deleted	스위치 재부팅 이후 삭제된 새 항목의 수를 보여줍니다.
Total Neighbors Entries Dropped	항목 테이블이 가득 차서 LLDP 프레임이 삭제된 경우의 수를 보여줍니다.
Total Neighbors Entries Aged Out	수명이 만료되어 항목이 삭제된 경우의 수를 보여줍니다.

LLDP Statistics Local Counters

용어	설명
Local Counters	로컬 카운터는 현재 선택된 스위치의 각 인터페이스별 카운터를 나타냅니다.
Local Interface	LLDP 프레임이 수신 또는 송신되는 인터페이스입니다.
Tx Frames	해당 인터페이스에서 송신된 LLDP 프레임의 개수입니다.
Rx Frames	해당 인터페이스에서 수신된 LLDP 프레임의 개수입니다.

Rx Errors	해당 인터페이스에서 수신된 오류를 포함한 LLDP 프레임의 개수입니다.
Frames Discarded	인터페이스에서 LLDP 프레임을 수신하고 스위치의 내부 테이블이 가득 찬 경우, LLDP 프레임은 계수되고 폐기됩니다. 이 상황은 LLDP 표준에서 "Too Many Neighbors"로 알려져 있습니다. LLDP 프레임은 Chassis ID 또는 Remote Port ID 가 테이블에 이미 포함되어 있지 않은 경우 새로운 항목이 테이블에 추가되어야 합니다. 특정 인터페이스의 링크가 끊어지거나 LLDP 종료 프레임이 수신되거나 항목이 시간이 지나면 항목이 테이블에서 제거됩니다.
TLVs Discarded	각 LLDP 프레임은 "Type Length Value"의 약자인 TLV(TLV)라고 불리는 여러 정보를 포함할 수 있습니다. TLV 가 형식에 맞지 않는 경우, 해당 TLV 는 계수되고 폐기됩니다.
TLVs Unrecognized	알맞은 형식을 갖춘 TLV 지만 알 수 없는 유형 값이 있는 경우의 개수입니다.
Org. Discarded	LLDP 프레임이 조직적인 TLV 를 포함하고 있지만 해당 TLV 가 지원되지 않는 경우, 해당 TLV 는 버려지고 개수가 세어집니다.
Age-Outs	각 LLDP 프레임은 LLDP 정보의 유효 기간(만료 시간)에 대한 정보를 포함합니다. 만약 만료 시간 내에 새로운 LLDP 프레임이 수신되지 않으면, LLDP 정보가 제거되고 Age-Out 카운터가 증가합니다.
Clear	체크하면 특정 인터페이스에 대한 카운터가 “클리어" 버튼을 누를 때 초기화됩니다.

Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

Clear : 클릭 시 카운터 선택을 취소합니다.

WEB 확인 예시

웹메뉴 Monitor>LLDP>Port Statistics

LLDP Global Counters

Global Counters	
Clear global counters	☑
Neighbor entries were last changed	1970-01-01T13:44:54+09:00 (89711 secs. ago)
Total Neighbors Entries Added	23
Total Neighbors Entries Deleted	22
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	8

LLDP Statistics Local Counters

Local Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
*	*	*	*	*	*	*	*	*	☑
GigabitEthernet 1/1	135	2668	0	0	0	0	0	0	☑
GigabitEthernet 1/2	263	0	0	0	0	0	0	0	☑
GigabitEthernet 1/3	1470	0	0	0	0	0	0	0	☑
GigabitEthernet 1/4	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/5	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/6	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/7	19	25	0	0	0	0	0	2	☑
GigabitEthernet 1/8	3300	3054	0	0	0	0	0	4	☑
10GigabitEthernet 1/1	0	0	0	0	0	0	0	0	☑
10GigabitEthernet 1/2	0	0	0	0	0	0	0	0	☑
10GigabitEthernet 1/3	0	0	0	0	0	0	0	0	☑
10GigabitEthernet 1/4	0	0	0	0	0	0	0	0	☑

CLI 확인 예시

✓ **LLDP Global Counters**

✓ **LLDP Statistics Local Counters**

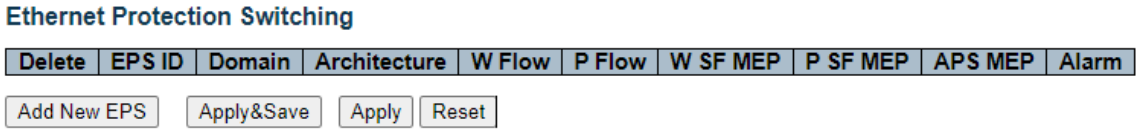
```
# show lldp statistics
LLDP global counters
Neighbor entries was last changed at 1970-01-01T13:44:54+09:00  (90116 secs. ago).
Total Neighbors Entries Added    23.
Total Neighbors Entries Deleted  22.
Total Neighbors Entries Dropped  0.
Total Neighbors Entries Aged Out 8.

LLDP local counters
                        Rx          Tx          Rx          Rx          Rx TLV      Rx TLV      Rx TLV
Interface               Frames      Frames      Errors      Discards    Errors      Unknown     Organiz.    Aged
---------               ------      ------      ------      --------    ------      -------     --------    ----

GigabitEthernet 1/1     2668        135         0           0           0           0           0           0
GigabitEthernet 1/2     0           263         0           0           0           0           0           0
GigabitEthernet 1/3     0           1483        0           0           0           0           0           0
GigabitEthernet 1/4     0           0           0           0           0           0           0           0
GigabitEthernet 1/5     0           0           0           0           0           0           0           0
GigabitEthernet 1/6     0           0           0           0           0           0           0           0
GigabitEthernet 1/7     25          19          0           0           0           0           0           2
GigabitEthernet 1/8     3067        3314        0           0           0           0           0           4
10GigabitEthernet 1/1   0           0           0           0           0           0           0           0
10GigabitEthernet 1/2   0           0           0           0           0           0           0           0
10GigabitEthernet 1/3   0           0           0           0           0           0           0           0
10GigabitEthernet 1/4   0           0           0           0           0           0           0           0
```

6.12. EPS

6.12.1. EPS Configuration

웹메뉴 Configuration>EPS

Ethernet (Linear) Protection Switch 인스턴스는 여기서 구성됩니다.



Ethernet Protection Switching

용어	설명
Delete	EPS 를 삭제하려면 선택하세요. 다음 저장시 삭제됩니다.
EPS ID	EPS 의 ID 입니다. 범위는 1-100 입니다. 설정 페이지로 이동하려면 EPS 의 ID 를 클릭하세요.
Domain	Port: 이는 포트 도메인에서 EPS 를 생성합니다. 'W/P Flow'는 포트입니다.
Architecture	**1+1** 1+1 EPS를 생성합니다. **1:1** 1:1 EPS를 생성합니다.
W Flow	EPS의 작업 Flow – Domain을 참조하세요.
P Flow	EPS의 보호 Flow – Domain을 참조하세요.
W SF MEP	작업 신호 실패 보고 MEP.
P SF MEP	보호 신호 실패 보고 MEP.
APS MEP	APS PDU 처리 MEP.
Alarm	EPS 활성 알람입니다.

Buttons

Add New EPS: 새 EPS 항목을 추가하려면 클릭하세요.

Refresh: 클릭 시 페이지를 새로 고침. 로컬 변경 사항은 취소합니다.

Apply: 클릭 시 변경사항을 적용합니다.

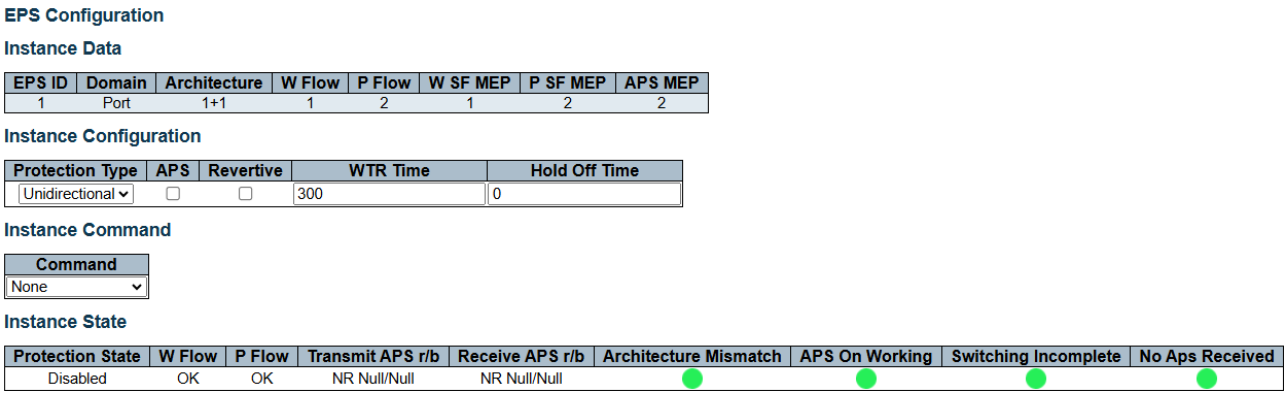
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

EPS Configuration

EPS ID를 클릭하면 설정 페이지로 이동합니다.

이 페이지는 사용자가 현재 EPS 인스턴스를 검사하고 구성할 수 있게 합니다.


EPS Configuration

Instance Data

EPS ID	Domain	Architecture	W Flow	P Flow	W SF MEP	P SF MEP	APS MEP
1	Port	1+1	1	2	1	2	2

Instance Configuration

Protection Type	APS	Revertive	WTR Time	Hold Off Time
Unidirectional	☐	☐	300	0

Instance Command

Command
None

Instance State

Protection State	W Flow	P Flow	Transmit APS r/b	Receive APS r/b	Architecture Mismatch	APS On Working	Switching Incomplete	No Aps Received
Disabled	OK	OK	NR Null/Null	NR Null/Null	●	●	●	●

EPS Configuration

Instance Data

용어	설명
EPS ID	EPS 의 ID 입니다.
Domain	EPS 생성 웹의 도움말을 참조하세요.
Architecture	EPS 생성 웹의 도움말을 참조하세요.
W Flow	EPS 생성 웹의 도움말을 참조하세요.
P Flow	EPS 생성 웹의 도움말을 참조하세요.
W SF MEP	EPS 생성 웹의 도움말을 참조하세요.
P SF MEP	EPS 생성 웹의 도움말을 참조하세요.
APS MEP	EPS 생성 웹의 도움말을 참조하세요.

Instance Configuration

용어	설명	
Protection Type	Unidirectional	EPS의 양 끝은 서로 다른 Working/Protection Flow에서 트래픽을 선택할 수 있습니다. 이는 1+1의 경우에만 설정이 가능합니다.
	Bidirectional	EPS의 양 끝은 동일한 Working/Protection Flow에서 트래픽을 선택합니다. 이는 APS가 활성화되어야 합니다. 1:1의 경우 필수입니다.
APS	APS 프로토콜을 활성화/비활성화할 수 있습니다. 1:1의 경우 필수입니다.	
Revertive	Working Flow로의 복귀 전환을 활성화/비활성화할 수 있습니다.	
WTR Time	복귀 전환 시 사용할 대기 시간을 설정합니다. 범위는 1에서 720초입니다.	
Hold Off Time	전환하기 전에 신호 실패를 지속적으로 확인하기 위해 사용할 시간 값을 설정합니다. 이 값은 100밀리초 단위이며 최대 값은 100(10초)입니다.	

Instance Command

용어	설명	
Command	None	이 인스턴스에 활성화된 로컬 명령이 없습니다.
	Clear	활성화된 로컬 명령이 제거됩니다.
	Lock Out	이 EPS는 Working에 잠겨 있습니다(활성화되지 않음). 1:N의 경우(동일한 보호 흐름을 가진 여러 EPS가 있는 경우) - 하나의 EPS가 Protection Flow으로 전환되면 다른 EPS는 이 명령이 강제 적용됩니다.
	Forced Switch	강제 Protection로 전환합니다.
	Manual Switch P	수동으로 Protection로 전환합니다.
	Manual Switch W	수동으로 Working로 전환합니다. 이는 '비복귀' 모드에서만 허용됩니다.

	Exercise	프로토콜 연습 - 트래픽에 영향을 미치지 않음. 이는 'Bidrectional' Protection 유형에서만 허용됩니다.
	Freeze	이 EPS는 로컬에서 동결되었습니다 - 모든 입력을 무시합니다.
	Lock Out Local	이 EPS는 로컬에서 "잠겨" 있으며, 작업에서 감지된 로컬 SF를 무시합니다.

Instance State

용어	설명	
Protection State	EPS 상태는 G.8031 의 상태 전환 테이블에 따릅니다.	
W Flow	OK	Working Flow의 상태가 정상입니다.
	SF	Working Flow의 상태가 신호 실패입니다.
	SD	Working Flow의 상태가 신호 저하입니다.
P Flow	OK	Protection Flow의 상태가 정상입니다.
	SF	Protection Flow의 상태가 신호 실패입니다.
	SD	Protection Flow의 상태가 신호 저하입니다.
Transmit APS r/b	G.8031의 상태 전환 테이블에 따른 전송된 APS입니다.	
Receive APS r/b	G.8031의 상태 전환 테이블에 따른 수신된 APS입니다.	
Architecture Mismatch	수신된 APS에서 나타난 아키텍처가 로컬에서 구성된 것과 일치하지 않습니다.	
APS on working	APS가 Protection Flow에서 수신되었습니다.	
Switching Incomplete	트래픽이 EPS의 양 끝에서 동일한 Flow로 선택되지 않았습니다.	
No APS Received	반대 끝에서 APS PDU가 수신되지 않았습니다.	

Buttons

Refresh: 클릭 시 페이지를 새로 고침. 로컬 변경 사항은 취소합니다.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

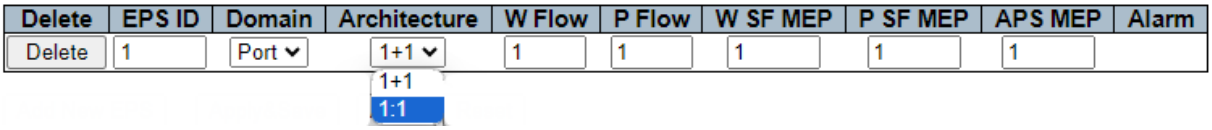
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

✓ **Ethernet Protection Switching**

➢ ***Add New EPS***

Ethernet Protection Switching



- ***EPS ID (1~100)***
- ***Domain(Port)***
- ***Architecture(1+1 | 1:1)***
- ***W Flow(MEP instance number)***

- ***P Flow(MEP instance number)***
- ***W SF MEP(MEP instance number)***
- ***P SF MEP(MEP instance number)***
- ***APS MEP(MEP instance number | Not W Flow)***
- ***Alarm***

Delete	EPS ID	Domain	Architecture	W Flow	P Flow	W SF MEP	P SF MEP	APS MEP	Alarm
☐	1	Port	1:1	1	2	1	2	2	●

Click EPS ID

✓ **EPS Configuration**

✓ **Instance Data**

EPS ID	Domain	Architecture	W Flow	P Flow	W SF MEP	P SF MEP	APS MEP
1	Port	1:1	1	2	1	2	2

✓ **Instance Configuration**

- ***Protection Type (Unidirectional | Bidirectional)***

  1+1 Unidirectional
  1+1 Bidirectional
- ***APS***
- ***Revertive***
- ***WTR Time(1~720)***
- ***Hold Off Time(0~100 10sec)***

Protection Type	APS	Revertive	WTR Time	Hold Off Time
Unidirectional	☐	☐	300	0

Unidirectional
Bidirectional

1+1 Bidirectional

Protection Type	APS	Revertive	WTR Time	Hold Off Time
Bidirectional	☑	☑	300	0

1:1

Protection Type	APS	Revertive	WTR Time	Hold Off Time
Bidirectional	✓	☑	300	0

✓ **Instance Command**

- ***None | Clear | Lock Out | Forced Switch | Manual Switch P | Manual Switch W | Exercise | Freeze | Lock Out Local***

Command
None

None
Clear
Lock Out
Forced Switch
Manual Switch P
Manual Switch W
Exercise
Freeze
Lock Out Local

✓ **Instance State**

- ***Protection State***
- ***W Flow***
- ***P Flow***
- ***Transmit APS r/b***
- ***Receive APS r/b***
- ***Architecture Mismatch***
- ***APS On Working***
- ***Switching Incomplete***
- ***No APS Received***

Protection State	W Flow	P Flow	Transmit APS r/b	Receive APS r/b	Architecture Mismatch	APS On Working	Switching Incomplete	No Aps Received
SfW	SF	OK	SFw Normal/Normal	SFw Normal/Normal	●	●	●	●

CLI 설정 예시

✓ **Ethernet Protection Switching**

➢ ***Add New EPS***

- ***EPS ID (1~100)***
- ***Domain(Port)***
- ***Architecture(1+1 | 1:1)***
- ***W Flow(MEP instance number)***
- ***P Flow(MEP instance number)***

```
(config)# eps <inst> domain { port | tunnel-tp | pw } architecture { 1plus1 | 1for1 } work-flow
{ <flow_w> | <port_type> <port_w> } protect-flow { <flow_p> | <port_type> <port_p> }
(config)# eps 1 domain port architecture 1for1 work-flow GigabitEthernet 1/1 protect-flow
GigabitEthernet
```

- ***W SF MEP(MEP instance number)***
- ***P SF MEP(MEP instance number)***
- ***APS MEP(MEP instance number | Not W Flow)***

```
(config)# eps <inst> mep-work <mep_w> mep-protect <mep_p> mep-aps <mep_aps>
(config)# eps 1 mep-work 1 mep-protect 2 mep-aps 2
```

✓ **EPS Configuration**

✓ **Instance Configuration**

- ***Protection Type (Unidirectional | Bidirectional)***

1+1 Unidirectional
1+1 Bidirectional

- ***APS***

```
(config)# eps <inst> 1plus1 { bidirectional | { unidirectional [ aps ] } }
(config)# eps 1 1plus1 bidirectional
(config)# eps 1 1plus1 unidirectional
(config)# eps 1 1plus1 unidirectional aps
```

- ***Revertive***

- ***WTR Time(1~720)***

```
(config)# eps <inst> revertive { 10s | 30s | 5m | 6m | 7m | 8m | 9m | 10m | 11m | 12m | { wtr-value
<wtr_value> } }
(config)# eps 1 revertive 10s
(config)# eps 1 revertive wtr-value 10
(config)# eps 1 revertive 12m
(config)# eps 1 revertive wtr-value 720
```

- ***Hold Off Time(0~100 10sec)***

```
(config)# eps <inst> holdoff <hold>
(config)# eps 1 holdoff 100
(config)# eps 1 holdoff 1
(config)# eps 1 holdoff 0
```

✓ **Instance Command**

- ***None | Clear | Lock Out | Forced Switch | Manual Switch P | Manual Switch W | Exercise | Freeze | Lock Out Local***

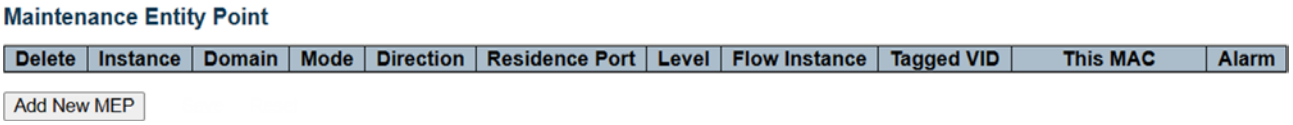
```
(config)# eps <inst> command { lockout | forced | manualp | manualw | exercise | freeze |
lockoutlocal }
(config)# no eps 1 command
(config)# eps 1 command lockout
```

6.13. MEP

6.13.1. MEP Configuration

웹메뉴 Configuration>MEP

이곳에서 Maintenance Entity Point 인스턴스가 구성됩니다.



Maintenance Entity Point

용어	설명
Delete	MEP(Maintenance Entity Point)를 삭제하려면 선택하세요. 다음 저장시 삭제됩니다.
Instance	MEP 의 ID 입니다. MEP 의 ID 를 클릭하면 구성 페이지로 이동할 수 있습니다. 범위는 1 부터 100 까지입니다.
Domain	Port: 이것은 Port 도메인에 속한 MEP 입니다.
Mode	MEP: Maintenance Entity 의 종단점(Maintenance Entity End Point)입니다. MIP: Maintenance Entity 의 중간점(Maintenance Entity Intermediate Point)입니다.
Direction	Down: 이것은 다운 MEP(Down MEP)입니다 - 'Residence Port'에서 Ingress OAM 및 트래픽을 모니터링합니다. Up: 이것은 업 MEP(Up MEP)입니다 - 'Residence Port'에서 Egress OAM 및 트래픽을 모니터링합니다.
Residence Port	MEP 가 모니터링하는 포트입니다 - 'Direction'을 참조하십시오. EVC MEP 의 경우 포트는 EVC 의 포트여야 합니다. VLAN MEP 의 경우 포트는 VLAN 멤버여야 합니다.
Level	이 MEP 의 MEG 레벨입니다.
Flow Instance	이 MEP 는 이 플로우와 관련이 있습니다. '도메인'을 참조하세요. 포트 MEP 의 경우에는 관련성이 없으며 표시되지 않습니다.
Tagged VID	Port MEP: 외부 C/S 태그(포트 유형에 따라)가 이 VID 와 함께 추가됩니다 '0'을 입력하면 TAG 가 추가되지 않은 것을 의미합니다. EVC MEP: 사용되지 않습니다. VLAN MEP: 사용되지 않습니다. EVC MIP: Serval 에서는 이것은 MIP 가 활성화된 이 EVC 에서 구독자 플로우를 식별하는 구독자 VID 입니다.
This MAC	이 MEP 의 MAC 주소입니다. 유니캐스트가 선택된 경우 다른 MEP 에서 사용될 수 있습니다. (정보 제공용)
Alarm	이 MEP 에는 활성화된 알람이 있습니다.

Buttons

Add New MEP : 새 MEP 항목을 추가합니다.

Refresh: 클릭 시 페이지를 새로 고침. 로컬 변경 사항은 취소합니다.

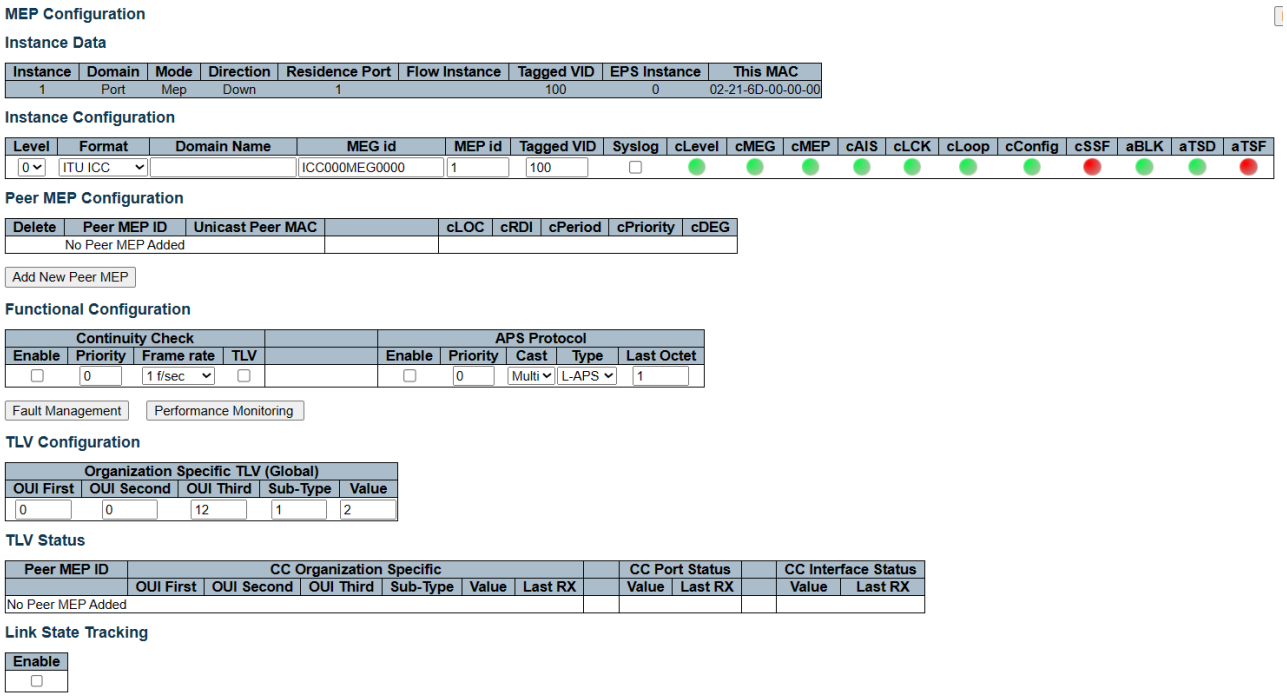
Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

MEP Configuration

이 페이지에서는 사용자가 현재 MEP 인스턴스를 검토하고 구성할 수 있습니다.



Instance Data

용어	설명
MEP Instance	MEP 의 ID 입니다.
Domain	MEP 생성 웹의 도움말을 참조하세요.
Mode	MEP 생성 웹의 도움말을 참조하세요.
Direction	MEP 생성 웹의 도움말을 참조하세요.
Residence Port	MEP 생성 웹의 도움말을 참조하세요.
Flow Instance	MEP 생성 웹의 도움말을 참조하세요.
Tagged VID	MEP 생성 웹의 도움말을 참조하세요.
This MAC	MEP 생성 웹의 도움말을 참조하세요.

Instance Configuration

용어	설명
Level	MEP 생성 웹의 도움말을 참조하세요.
Format	두 가지 가능한 유지 관리 연합 식별자 형식의 구성입니다. **ITU ICC**: 이는 ITU 에 의해 정의됩니다 (Y1731 Fig. A3). '도메인 이름'은 사용되지 않습니다. 'MEG ID'는 최대 13 자까지여야 합니다. **IEEE String**: 이는 IEEE 에 의해 정의됩니다 (802.1ag Section 21.6.5). '도메인 이름'은 최대 16 자까지 사용할 수 있습니다. 'MEG ID' (짧은 MA 이름)는 최대 16 자까지 사용할 수 있습니다. **ITU CC ICC**: 이는 ITU 에 의해 정의됩니다 (Y1731 Fig. A5). '도메인 이름'은 사용되지 않습니다. 'MEG ID'는 최대 15 자까지여야 합니다.

Domain Name	이것은 IEEE 유지 보수 도메인 이름이며 'IEEE String' 형식의 경우에만 사용됩니다. 이 문자열은 비어 있을 수 있으며 유지 보수 도메인 이름 형식 1 - 없음을 나타낼 수 있습니다. 이 문자열은 최대 16 자까지 사용할 수 있습니다.
MEG Id	이는 '형식'에 따라 ITU MEG ID 또는 IEEE Short MA Name 입니다. '형식'을 참조하세요. ITU ICC 형식의 경우 최대 13 자여야 합니다. ITU CC ICC 형식의 경우 최대 15 자여야 합니다. IEEE String 형식의 경우 최대 16 자까지 사용할 수 있습니다.
MEP Id	이 값은 전송되는 2 바이트 CCM MEP ID 가 됩니다.
Tagged VID	이 값은 OAM PDU 에 추가된 태그의 VID 가 됩니다.
VOE	이는 MEP 구현을 위해 VOE(Hardware OAM Engine)를 사용하려고 시도할 것입니다. 모든 플랫폼이 VOE 를 지원하는 것은 아닙니다.
cLevel	Fault Cause 는 이 MEP 에 대해 구성된 것보다 낮은 수준의 CCM 을 수신한 것을 나타냅니다.
cMEG	Fault Cause 는 이 MEP 에 대해 구성된 것과 다른 MEG ID 를 가진 CCM 을 수신한 것을 나타냅니다.
cMEP	Fault Cause 는 이 MEP 에 대해 구성된 모든 'Peer MEP ID'와 다른 MEP ID 를 가진 CCM 을 수신한 것을 나타냅니다.
cAIS	Fault Cause 는 AIS PDU 가 수신된 경우를 나타냅니다.
cLCK	Fault Cause 는 LCK PDU 가 수신된 경우를 나타냅니다.
cDEG	Fault Cause 는 서버 레이어가 신호 저하를 나타내는 경우를 나타냅니다.
cSSF	Fault Cause 는 서버 레이어가 신호 실패를 나타내는 경우를 나타냅니다.
aBLK	이 플로우에서 서비스 프레임 차단 작업이 활성화되었습니다.
aTSD	트레일 신호 저하를 나타내는 작업은 계산됩니다.
aTSF	보호 대상으로 트레일 신호 실패를 나타내는 작업이 활성화되었습니다.

Peer MEP Configuration

용어	설명
Delete	Peer MEP 를 삭제하기 위해 체크하세요. 다음 저장 시에 삭제됩니다.
Peer MEP ID	이 값은 수신된 CCM 에서 예상되는 MEP ID 가 될 것입니다. 'cMEP'을 참조하세요.
Unicast Peer MAC	Peer MEP 와 함께 유니캐스트가 선택된 경우 이 MAC 주소가 사용됩니다. 또한 이 MAC 주소는 이 peer MEP 로부터 수신되는 CCM PDU 의 HW 체크 (LOC 검출)에 사용됩니다.
cLOC	Peer MEP 로부터 CCM 이 수신되지 않은 경우 (3.5 기간 동안)를 나타내는 Fault Cause 입니다.
cRDI	Peer MEP 로부터 수신된 CCM 에 원격 결함 표시가 포함된 경우를 나타내는 Fault Cause 입니다.
cPeriod	Peer MEP 로부터 수신된 CCM 의 주기가 이 MEP 에 대해 구성된 값과 다른 경우를 나타내는 Fault Cause 입니다.
cPriority	Peer MEP 로부터 수신된 CCM 의 우선순위가 이 MEP 에 대해 구성된 값과 다른 경우를 나타내는 Fault Cause 입니다.

Functional Configuration

Continuity Check

용어	설명
Enable	CCM PDU 를 기반으로 한 연속성 확인은 CCM PDU 의 송수신 여부에 따라 활성화 또는 비활성화할 수 있습니다. CCM PDU 는 항상 멀티캐스트 클래스 1 로 전송됩니다.

Priority	TAG 에 삽입될 PCP 비트로 사용될 우선 순위입니다 (있는 경우). 연속성 확인 및 손실 측정이 소프트웨어 기반 CCM 에서 모두 구현되는 경우 '우선순위'는 동일해야 합니다.
Frame rate	CCM PDU 의 프레임 속도를 선택합니다. 이 값은 Y.1731 에서 설명하는 송신 주기의 역수입니다. 이 값은 다음과 같은 용도로 사용됩니다: *CCM PDU 의 송신 속도를 결정합니다. *3.5 주기 이내에 CCM PDU 를 수신하지 못한 경우 cLOC 오류 원인이 선언됩니다. 'cLOC'를 참조하세요. *다른 주기로 CCM PDU 를 수신한 경우 cPeriod 오류 원인이 선언됩니다. -'cPeriod'를 참조하세요. 300f/초 또는 100f/초를 선택하면 가능한 경우 하드웨어 기반 CCM 이 구성됩니다. 다른 프레임 속도를 선택하면 소프트웨어 기반 CCM 이 구성됩니다. 연속성 확인과 손실 측정이 모두 소프트웨어 기반 CCM 에 구현된 경우, '프레임 속도'는 동일해야 합니다.
TLV	CCM PDU 에서 TLV 삽입을 활성화/비활성화합니다.

APS Protocol

용어	설명
Enable	송수신하는 R-APS/L-APS PDU 를 기반으로 하는 자동 보호 전환 프로토콜 정보 전달을 활성화/비활성화할 수 있습니다. APS 를 구현하는 ERPS/ELPS 를 지원하려면 이 기능을 활성화해야 합니다. 하나의 Peer MEP 만 구성된 경우에만 유효합니다.
Priority	(해당되는 경우) TAG 에 PCP 비트로 삽입될 우선순위입니다.
Cast	유니캐스트 또는 멀티캐스트로 전송되는 APS PDU 를 선택합니다. 유니캐스트 MAC 은 '유니캐스트 Peer MAC' 구성에서 가져옵니다. 유니캐스트는 L-APS 에만 유효하며, '유형'을 참조하십시오. R-APS PDU 는 G.8032 에서 설명한 멀티캐스트 MAC 으로 항상 전송됩니다.
Type	R-APS: APS PDU 는 R-APS 로 전송됩니다. 이는 ERPS 에 사용됩니다. L-APS: APS PDU 는 L-APS 로 전송됩니다. 이는 ELPS 에 사용됩니다.
Last Octet	이 값은 전송 및 예상되는 RAPS 멀티캐스트 MAC 의 마지막 옥텟입니다. G.8031 (03/2010)에서 RAPS 멀티캐스트 MAC 은 01-19-A7-00-00-XX 로 정의됩니다. 현재 표준에서는 이 마지막 옥텟의 값으로 '01'이 사용되며, 다른 값의 사용은 추가 연구를 위한 것입니다.

TLV Configuration

OAM PDU TLV 의 구성입니다. 현재는 CCM 에만 TLV 가 지원됩니다.

용어	설명
Organization Specific - OUI First	OS TLV OUI 필드에서 전송되는 첫 번째 값입니다.
- OUI Second	OS TLV OUI 필드에서 전송되는 두 번째 값입니다.
- OUI Third	OS TLV OUI 필드에서 전송되는 세 번째 값입니다.
- Sub-Type	OS TLV 의 Sub-Type 필드에서 전송되는 값입니다.
- Value	OS TLV 의 Value 필드에서 전송되는 값입니다.

TLV Status

마지막으로 수신된 TLV의 표시입니다. 현재는 CCM의 TLV만 지원됩니다.

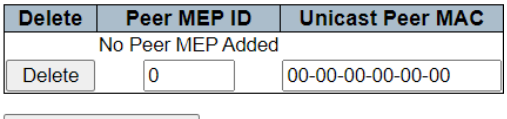
용어	설명
CC Organization Specific - OUI First	마지막으로 수신된 OS TLV OUI 필드의 첫 번째 값입니다.
- OUI Second	마지막으로 수신된 OS TLV OUI 필드의 두 번째 값입니다.
- OUI Third	마지막으로 수신된 OS TLV OUI 필드의 세 번째 값입니다.
- Sub-Type	OS TLV Sub-Type 필드에서 마지막으로 수신된 값입니다.
- Value	OS TLV 값 필드에서 마지막으로 수신된 값입니다.
- Last RX	마지막으로 수신된 CCM PDU 에는 OS TLV 가 포함되었습니다.
CC Port Status - Value	PS TLV 의 Value 필드에서 마지막으로 수신된 값입니다.
- Last RX	PS TLV 가 마지막으로 수신된 CCM PDU 에 포함되었습니다.
CC Interface Status - Value	IS TLV 가 마지막으로 수신된 CCM PDU 에 포함되었습니다.
- Last RX	마지막으로 수신된 CCM PDU 에 IS TLV 가 포함되었습니다.

Link State Tracking

용어	설명
Enable	LST 가 인스턴스에서 활성화되면, 로컬 SF 또는 수신된 CCM 인터페이스 상태 TLV 에서 'isDown'이 감지되면 소속 포트가 중단됩니다. 이 기능은 Up-MEP 에서만 유효합니다. CCM 전송 속도는 1 f/s 이상이어야 합니다.

Buttons

Add New Peer MEP : 버튼누르게 되면 다음과 같이 입력상자가 나타납니다. 새로운 Peer Mep를 추가합니다.



Fault Management : 장애 관리 페이지로 이동합니다.

Performance Monitoring : 성능 모니터링 페이지로 이동합니다.

Refresh : 클릭 시 페이지를 새로 고침. 로컬 변경 사항은 취소합니다.

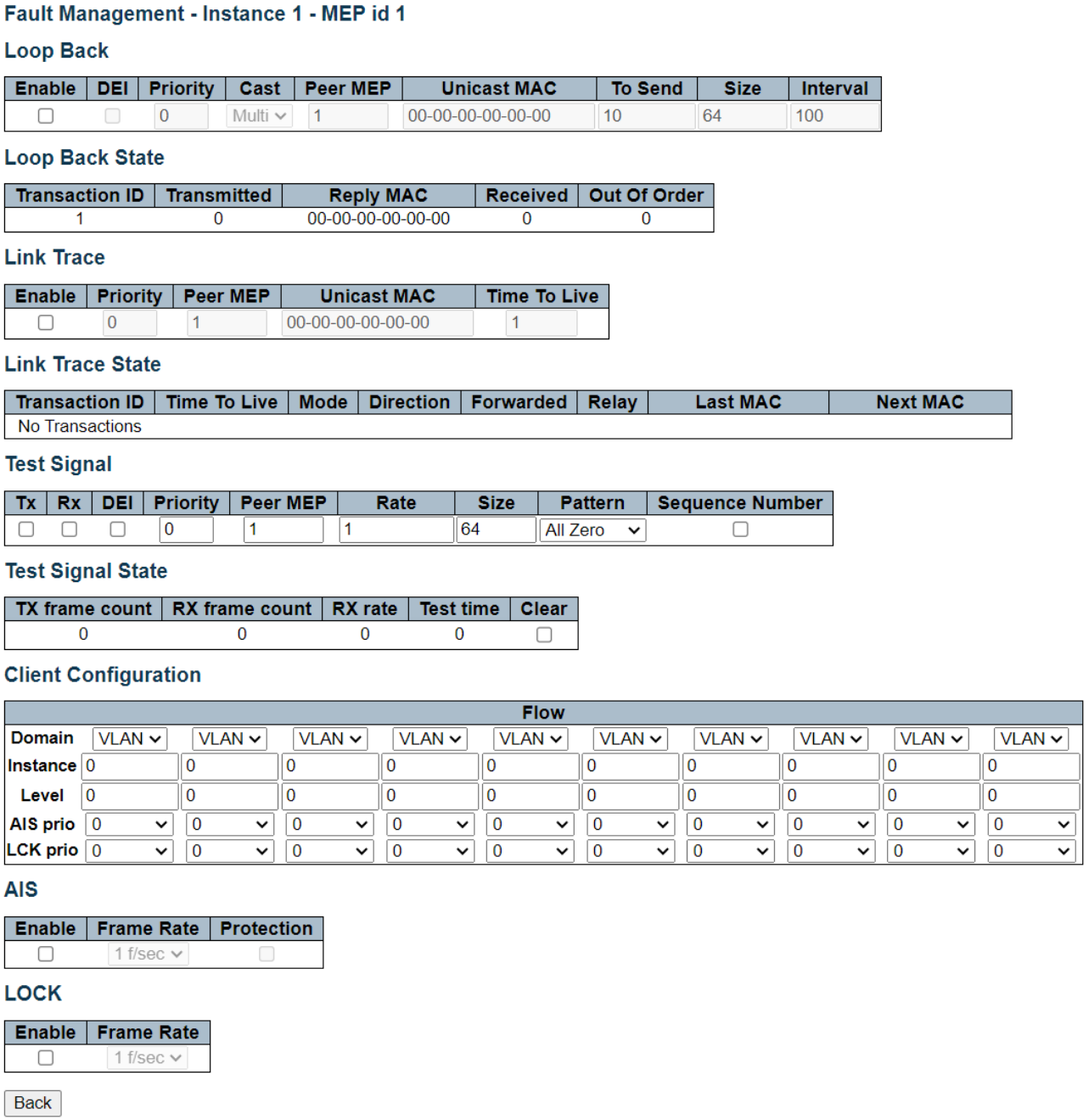
Apply : 클릭 시 변경사항을 적용합니다.

Apply&Save : 클릭 시 변경사항을 적용하고 저장합니다.

Reset : 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

Fault Management - Instance 1 - MEP id 1

This page allows the user to inspect and configure the Fault Management of the current MEP Instance.



Fault Management - Instance 1 - MEP id 1

Loop Back

Enable	DEI	Priority	Cast	Peer MEP	Unicast MAC	To Send	Size	Interval
☐	☐	0	Multi	1	00-00-00-00-00-00	10	64	100

Loop Back State

Transaction ID	Transmitted	Reply MAC	Received	Out Of Order
1	0	00-00-00-00-00-00	0	0

Link Trace

Enable	Priority	Peer MEP	Unicast MAC	Time To Live
☐	0	1	00-00-00-00-00-00	1

Link Trace State

Transaction ID	Time To Live	Mode	Direction	Forwarded	Relay	Last MAC	Next MAC
No Transactions							

Test Signal

Tx	Rx	DEI	Priority	Peer MEP	Rate	Size	Pattern	Sequence Number
☐	☐	☐	0	1	1	64	All Zero	☐

Test Signal State

TX frame count	RX frame count	RX rate	Test time	Clear
0	0	0	0	☐

Client Configuration

Flow										
Domain	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN
Instance	0	0	0	0	0	0	0	0	0	0
Level	0	0	0	0	0	0	0	0	0	0
AIS prio	0	0	0	0	0	0	0	0	0	0
LCK prio	0	0	0	0	0	0	0	0	0	0

AIS

Enable	Frame Rate	Protection
☐	1 f/sec	☐

LOCK

Enable	Frame Rate
☐	1 f/sec

Back

Loop Back

용어	설명
Enable	LBM/LBR PDU 를 전송/수신하여 루프백을 기반으로 한 활성화/비활성화가 가능합니다. 모든 '전송 대상' LBM PDU 가 전송된 후에는 자동으로 루프백이 비활성화됩니다. 이때는 끝에서부터 모든 LBR 을 기다리며, 5 초 동안 대기합니다.
DEI	DEI (Drop Eligible Indicator)는 필요한 경우 PCP 비트로 TAG 에 삽입됩니다.
Priority	우선순위는 필요한 경우 PCP 비트로 TAG 에 삽입됩니다.

Cast	LBM PDU 의 전송 방식을 유니캐스트 또는 멀티캐스트로 선택합니다. 유니캐스트 MAC 은 'Peer MEP' 또는 '유니캐스트 Peer MAC'을 통해 구성됩니다. MIP 로 전달되는 경우 유니캐스트 루프백만 가능합니다.
Peer MEP	만약 '유니캐스트 MAC'이 모두 0 으로 구성된 경우에만 사용됩니다. LBM 유니캐스트 MAC 은 해당 피어의 '유니캐스트 Peer MAC' 구성에서 가져옵니다.
Unicast MAC	이 값은 모두 0 으로 구성되지 않은 경우에만 사용됩니다. 이 값은 LBM PDU 유니캐스트 MAC 로 사용됩니다. 이는 MIP 에 대한 루프백을 구성하는 유일한 방법입니다.
To Send	한 번의 루프 테스트에서 전송할 LBM PDU 의 수입니다. 값이 0 이면 무한 전송을 나타냅니다 (테스트 동작). 이는 하드웨어 기반의 LBM/LBR 이며, VOE 가 필요합니다.
Size	LBM 프레임 크기는 바이트 단위로 입력되며, LBM OAM PDU 와 CRC(4 바이트)를 포함한 태그되지 않은 프레임의 원하는 크기를 의미합니다. 예를 들어, 'Size'가 64 일 때, 태그되지 않은 프레임 크기는 다음과 같습니다: DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 바이트 태그가 추가될 때마다 전송된 프레임은 4 바이트씩 더 길어집니다. 터널 EVC 의 경우 8 바이트가 추가됩니다. 고려해야 할 두 가지 최대 프레임 크기가 있습니다. 스위치 RX 프레임 최대 크기: 스위치 포트에서 허용되는 최대 프레임 크기는 10240 바이트입니다. CPU RX 프레임 최대 크기: CPU 로 복사할 수 있는 최대 프레임 크기는 1526 바이트입니다. 선택한 프레임 크기가 CPU RX 프레임 최대 크기를 초과하는 경우 경고가 표시됩니다. 프레임 최소 크기는 64 바이트입니다.
Interval	LBM PDU 전송 간격은 10ms 입니다. 'To Send'가 0 이 아닌 경우(최대 100 - '0'은 가능한 한 빠른 속도), 10ms 간격으로 전송됩니다. 'To Send'가 0 인 경우(최대 10,000), 1us(마이크로초) 간격으로 전송됩니다.

Loop Back State

용어	설명
Transaction ID	첫 번째 전송된 LBM 의 트랜잭션 ID 는 초기값으로 설정됩니다. 각 LBM 이 전송될 때마다 PDU 내의 트랜잭션 ID 가 증가합니다.
Transmitted	전송된 총 LBM PDU 의 수를 나타냅니다.
Reply MAC	응답하는 MEP/MIP 의 MAC 주소입니다. 멀티캐스트 LBM 의 경우, 그룹 내 모든 피어 MEP 로부터 응답을 받을 수 있습니다. 'To Send'가 0 인 경우에는 이 MAC 주소가 표시되지 않습니다.
Received	이 'Reply MAC'로부터 수신된 총 LBR PDU 의 수입니다.
Out Of Order	이 'Reply MAC'로부터 수신된 LBR PDU 중에서 'Transaction ID'가 잘못된 것의 수입니다.

Link Trace

용어	설명
Enable	LTM/LTR PDU 의 전송/수신에 따라 링크 추적(Link Trace)이 활성화/비활성화될 수 있습니다. 모든 5 개의 트랜잭션이 5 초 간격으로 완료되고 마지막에 모든 LTR 에 대해 5 초간 대기할 경우, 링크 추적은 자동으로 비활성화됩니다. LTM PDU 는 항상 멀티캐스트 Class 2 로 전송됩니다.
Priority	PCP 비트로 TAG 에 삽입될 우선순위 (있는 경우)입니다.
Peer MEP	이는 'Unicast MAC'가 모두 0 으로 구성된 경우에만 사용됩니다. 링크 추적 대상 MAC 은 이 피어의 'Unicast Peer MAC' 구성에서 가져옵니다.

Unicast MAC	이는 모두 0 으로 구성되지 않은 경우에만 사용됩니다. 이는 링크 추적 대상 MAC 으로 사용됩니다. 이는 MIP 를 대상 MAC 으로 구성하는 유일한 방법입니다.
Time To Live	이 값은 Y.1731 에서 설명된 LTM PDU 의 TTL(TimetoLive) 값입니다. 이 값은 MIP 에 의해 전달될 때마다 감소합니다. TTL 값이 0 에 도달하면 더 이상 전달되지 않습니다.

Link Trace State

용어	설명
Transaction ID	각 LTM 전송마다 트랜잭션 ID 가 증가합니다. 이 값은 전송된 LTM PDU 에 삽입되며, LTR PDU 에서 수신되기를 기대합니다. 잘못된 트랜잭션 ID 를 가진 LTR 은 무시됩니다. 한 개의 활성화된 링크 추적에서는 다섯 개의 트랜잭션이 있습니다.
Time To Live	이 값은 이 LTR 을 전송하는 MIP/MEP 가 수신한 LTM 에서 가져온 TTL 값입니다. 전달된 것처럼 감소됩니다.
Mode	이 LTR 을 보낸 것이 MEP 인지 MIP 인지를 나타냅니다.
Direction	MEP/MIP 가 이 LTR 을 보낸 것이 Ingress/egress 인지 나타내는 경우입니다.
Forwarded	MEP/MIP 가 이 LTR 를 전달했는지 여부를 나타내는 경우입니다.
Relay	릴레이 동작은 다음 중 하나일 수 있습니다. MAC: LT 대상 MAC 주소에 대한 일치가 발생했습니다. FDB: 필터링 DB 에서 일치에 기반하여 LTM 이 전달되었습니다. MFDB: MIP CCM DB 에서 일치에 기반하여 LTM 이 전달되었습니다.
Last MAC	이 LTR 을 일으킨 LBM 의 마지막 발신자를 식별하는 MAC 는 MEP 를 시작하거나 이전 MIP 전달을 의미합니다.
Next MAC	이 LTR 을 일으킨 LBM 의 다음 발신자를 식별하는 MAC 는 MIP 전달 또는 종료 MEP 를 의미합니다.

Test Signal

용어	설명
Enable	TEST PDU 를 전송하는 것에 기반한 테스트 신호는 활성화/비활성화될 수 있습니다.
DEI	PCP 비트로 삽입될 DEI (Destination Ethernet Identifier)입니다.
Priority	PCP 비트로 삽입될 우선순위입니다.
Peer MEP	TEST 프레임의 대상 MAC 은 이 피어의 '유니캐스트 피어 MAC' 구성에서 가져옵니다.
Rate	TEST 프레임의 전송 속도입니다.
Size	TEST 프레임의 크기입니다. 이는 TEST OAM PDU 를 포함하는 태그가 없는 프레임의 원하는 크기(바이트 단위)로 입력됩니다. CRC(4 바이트)를 포함합니다. 예를 들어, '크기(Size)'가 64 인 경우 => 태그가 없는 프레임 크기 = DMAC(6) + SMAC(6) + TYPE(2) + TEST PDU 길이(46) + CRC(4) = 64 바이트 각 태그가 추가될 때마다 전송된 프레임은 4 바이트 더 길어집니다. 터널 EVC 의 경우 8 바이트가 됩니다. 고려해야 할 두 가지 프레임 최대 크기가 있습니다. 스위치 RX 프레임 최대 크기: 스위치 포트에서 수락되는 최대 프레임 크기(모두 포함)는 10240 바이트입니다. CPU RX 프레임 최대 크기: CPU 로 복사 가능한 최대 프레임 크기(모두 포함)는 1526 바이트입니다. 선택한 프레임 크기가 CPU RX 프레임 최대 크기를 초과하는 경우 경고가 표시됩니다. 프레임 최소 크기는 64 바이트입니다.

Pattern	'Empty' TEST PDU 의 크기는 12 바이트입니다. 구성된 프레임 크기를 달성하기 위해 데이터 TLV(TLV 데이터 유형)가 패턴과 함께 추가됩니다. 예를 들어, '크기(Size)'가 64 인 경우 => 태그가 없는 프레임 크기 = DMAC(6) + SMAC(6) + TYPE(2) + TEST PDU 길이(46) + CRC(4) = 64 바이트 TEST PDU 의 길이는 46 바이트이므로 46-12=34 바이트의 패턴이 추가됩니다. All Zero: 패턴은 '00000000'입니다. All One: 패턴은 '11111111'입니다. 10101010: 패턴은 '10101010'입니다.

Test Signal State

용어	설명
TX frame count	'클리어(Clear)' 이후 전송된 TEST 프레임의 수입니다.
RX frame count	'클리어(Clear)' 이후 수신된 TEST 프레임의 수입니다.
RX rate	'클리어(Clear)' 이후 첫 번째 수신된 TEST 프레임을 기준으로 계산된 현재 수신된 TEST 프레임 비트 속도(Kbps)입니다. 이 계산은 1 초 단위로 이루어지며, '클리어' 이후 첫 번째 TEST 프레임을 수신한 시점부터 시작됩니다. 이 계산에 사용되는 프레임 크기는 '클리어' 이후 처음 수신된 프레임의 크기입니다.
Test time	'클리어(Clear)' 이후 첫 번째 TEST 프레임을 수신한 이후 경과한 시간(초)입니다.
Clear	이로 인해 모든 테스트 신호 상태가 초기화됩니다. TEST 프레임의 전송이 다시 시작됩니다. 'Rx frame count', 'RX rate', 'Test time'의 계산은 첫 번째 TEST 프레임을 수신할 때부터 시작됩니다.

Client Configuration

포트 MEP만이 플로우 구성을 갖는 서버 MEP가 될 수 있습니다. 클라이언트 플로우의 우선순위는 항상 EVC에 구성된 가장 높은 우선순위입니다.

용어	설명
Domain	클라이언트 레이어 플로우의 도메인입니다.
Instance	클라이언트 레이어 플로우 인스턴스 번호입니다.
Level	이 클라이언트 레이어 플로우에서 전송되는 AIS 및 LCK PDU 는 이 레벨에 있을 것입니다.
AIS Prio	각 클라이언트 플로우에서 AIS 를 전송할 때 사용할 우선순위입니다. 가능한 가장 높은 PCP 를 가져오는 우선순위를 선택할 수 있습니다.t
LCK Prio	각 클라이언트 플로우에서 LCK 를 전송할 때 사용할 우선순위입니다. 가능한 가장 높은 PCP 를 가져오는 우선순위를 선택할 수 있습니다.

AIS

용어	설명
Enable	클라이언트 레이어 플로우에 AIS 신호 (AIS PDU 전송)를 삽입하는 것은 활성화/비활성화할 수 있습니다.
Frame Rate	AIS PDU 의 프레임 속도를 선택합니다. 이는 Y.1731 에서 설명된 전송 주기의 역수입니다.
Protection	이를 선택하면 첫 번째 3 개의 AIS PDU 가 가능한 한 빠르게 전송됩니다. 이는 종단점에서 보호 용도로 사용하는 경우입니다.

LOCK

용어	설명
Enable	클라이언트 레이어 플로우에 LOCK 신호 (LCK PDU 전송)를 삽입하는 것은 활성화/비활성화할 수 있습니다.
Frame Rate	LCK PDU 의 프레임 속도를 선택합니다. 이는 Y.1731 에서 설명된 전송 주기의 역수입니다.

Buttons

Back : 다시 MEP 인스턴스 메인 페이지로 이동 합니다.

Refresh: 클릭 시 페이지를 새로 고침. 로컬 변경 사항은 취소합니다.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

Performance Monitor - Instance 1 - MEP id 1

This page allows the user to inspect and configure the performance monitor of the current MEP Instance.

Performance Monitor - Instance 1 - MEP id 1 Refresh

Performance Monitoring Data Set

Enable
☐

Loss Measurement

Tx	Rx	Priority	Cast	Peer MEP	Rate	Size	Synthetic	Ended	FLR Interval	Meas. Interval	Loss Threshold	SLM Test ID
☐	☐	0	Multi	1	1 f/sec	64	☐	Single	5	1000	0	0

Loss Measurement State

Peer MEP ID	Tx	Rx	Near End Loss Count	Far End Loss Count	Interval Elapsed	Interval Near End Loss Ratio	Interval Far End Loss Ratio	Total Near End Loss Ratio	Total Far End Loss Ratio	Clear
No Peer MEP Added										

Loss Measurement Availability

Enable	Interval	FLR Threshold	Maintenance
☐	10	10	☐

Loss Measurement Availability State

Peer MEP ID	Near Availability Count	Far Availability Count	Near Unavailability Count	Far Unavailability Count	Near State	Far State
No Peer MEP Added						

Loss Measurement High Loss Interval

Enable	FLR Threshold	Consecutive Interval
☐	100	100

Loss Measurement High Loss Interval State

Peer MEP ID	Near Count	Far Count	Near Consecutive Count	Far Consecutive Count
No Peer MEP Added				

Loss Measurement Signal Degrade

Enable	TX Minimum	FLR Threshold	Bad Threshold	Good Threshold
☐	0	10	10	10

Delay Measurement

Enable	Priority	Cast	Peer MEP	Ended	Tx Mode	Calc	Gap	Count	Unit	Synchronized	Counter Overflow Action
☐	0	Multi	1	Single	Standardize	Flow	10	10	us	☐	Keep

Delay Measurement State

	Tx	Rx	Rx Timeout	Rx Error	Av Delay Tot	Av Delay last N	Delay Min.	Delay Max.	Av Delay-Var Tot	Av Delay-Var last N	Delay-Var Min.	Delay-Var Max.	Overflow	Clear
One-way														
F-to-N	0	0	0	0	0	0	0	0	0	0	0	0	0	
N-to-F	0	0	0	0	0	0	0	0	0	0	0	0	0	
Two-way	0	0	0	0	0	0	0	0	0	0	0	0	0	☐

Delay Measurement Bins

Measurement Bins for FD	Measurement Bins for IFDV	Measurement Threshold
3	3	5000

Delay Measurement Bins for FD

	bin0	bin1	bin2
One-way			
F-to-N	0	0	0
N-to-F	0	0	0
Two-way	0	0	0

Delay Measurement Bins for IFDV

	bin0	bin1	bin2
One-way			
F-to-N	0	0	0
N-to-F	0	0	0
Two-way	0	0	0

F-to-N :Far-end-to-near-end

N-to-F :Near-end-to-far-end

Back

Performance Monitoring Data Set

용어	설명
Enable	이 MEP 인스턴스를 활성화하면 PM 세션에서 수집한 'PM 데이터 세트'에 기여할 것입니다.

Loss Measurement

용어	설명
Tx	손실 측정 이니셔에이터가 활성화/비활성화되었습니다. 이니셔에이터는 CCM 또는 LMM/LMR 또는 SLM/SLR/1SL PDU 를 전송/수신합니다 - '합성' 및 '종료'를 참조하십시오. 서비스 프레임 LM(합성이 아님)은 하나의 Peer MEP 만 구성된 경우에만 허용됩니다. 합성 프레임 LM 은 여러 개의 Peer MEP 가 구성된 경우 허용됩니다.
Rx	LM PDUs (LMM/SLM/1SL)를 수신할 때 손실 계산을 활성화합니다. 이 설정은 LM 이니셔에이터가 활성화되어 있는 경우 무시됩니다.
Priority	PCP 비트로 삽입될 우선순위 (있는 경우)는 'Priority'입니다. 연속성 체크 및 손실 측정이 SW 기반 CCM 에서 모두 구현된 경우 'Priority'는 동일해야 합니다.
Cast	LM PDU 의 전송 방식을 유니캐스트 또는 멀티캐스트로 선택할 수 있습니다. 유니캐스트 MAC 은 '유니캐스트 피어 MAC' 데이터베이스에서 가져옵니다. 연속성 체크 및 이중 종단 손실 측정이 SW 기반 CCM 에서 모두 구현된 경우 'Cast'는 동일해야 합니다.
Peer MEP	유니캐스트 LM 의 피어 MEP-ID 입니다. MAC 은 '유니캐스트 피어 MAC' 데이터베이스에서 가져옵니다. 여러 피어('합성' LM)의 경우에만 사용됩니다.
Rate	LM PDU 의 프레임 속도를 선택합니다. 이는 Y.1731 에서 설명하는 전송 주기의 역수입니다. '합성' LM 의 경우, 100f/sec 를 선택하는 것이 유효합니다. 이중 종단 '서비스 프레임' LM (CCM PDU 기반)의 경우, 6f/min 을 선택하는 것은 유효하지 않습니다. 연속성 체크와 손실 측정이 모두 SW 기반 CCM 에서 구현된 경우, '프레임 속도'는 동일해야 합니다.
Size	'합성' SLM/1SL 프레임의 크기입니다. 이는 LM OAM PDU 가 포함된 태그되지 않은 프레임의 원하는 크기(바이트 단위)로 입력됩니다. 이 크기에는 CRC(4 바이트)도 포함됩니다. 예를 들어 'Size' = 64 인 경우, 태그되지 않은 프레임 크기는 DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 바이트가 됩니다. 전송되는 프레임은 각 태그마다 4 바이트씩 길어집니다. 터널 EVC 의 경우 8 바이트가 추가됩니다. 고려해야 할 두 가지 최대 프레임 크기가 있습니다. 스위치 RX 프레임 최대 크기: 스위치 포트에서 수용되는 최대 프레임 크기(모든 포함 요소 포함) (바이트 단위) CPU RX 프레임 최대 크기: CPU 로 복사할 수 있는 최대 프레임 크기(모든 포함 요소 포함) (바이트 단위) 선택한 프레임 크기가 CPU RX 프레임 최대 크기를 초과하는 경우 경고가 표시됩니다. 프레임 최소 크기는 64 바이트입니다.
Synthetic	합성 프레임 LM 이 활성화되었습니다. 이는 SLM/SLR/1SL PDU 를 기반으로 하는 LM 입니다.
Ended	Single: LMM/LMR 또는 SLM/SLR 을 기반으로 한 단일 종단 손실 측정. Dual: SW 기반 CCM 이나 1SL 을 기반으로 한 이중 종단 손실 측정.
FLR Interval	이는 측정 간격 프레임 손실 비율이 계산되는 측정 간격 수입니다.

Meas Interval	이는 '합성' LM 의 측정 간격을 밀리초 단위로 나타낸 것입니다. 이 값은 LM PDU 전송 간격('Rate'의 역수)의 정수배여야 합니다. 이 간격은 SL OAM PDU 의 수를 기반으로 손실 및 프레임 손실 비율(FLR)을 계산하는 데 사용됩니다. 계산된 FLR 은 가용성, 높은 손실 및 저하된 FLR 임계 값과 비교하는데 사용됩니다. 예시: 'Rate' = 100f/sec => 'Meas Interval' = N * 10 밀리초 예시: 'Rate' = 10f/sec => 'Meas Interval' = N * 100 밀리초 서비스 프레임 기반 LM 의 경우 이 속성은 사용되지 않으며, 측정 간격은 항상 LM PDU 전송 간격과 동일합니다.
Loss Threshold	손실 측정이 임계 값을 초과하는 경우, 원격 측의 손실 임계 값 카운트가 증가됩니다.
SLM Test ID	SLM PDU 에서 사용할 테스트 ID 값입니다 (G.8013 의 9.22.1 절 참조). 기본값은 0 입니다.

Loss Measurement State

용어	설명
Peer MEP	다음 상태와 관련된 Peer MEP ID 입니다.
Tx	마지막 '클리어' 이후 누적 전송된 LM PDU 의 수입니다.
Rx	마지막 '클리어' 이후 누적 수신된 LM PDU 의 수입니다.
Near End Loss Count	마지막 '클리어' 이후 누적된 근접 측의 프레임 손실 횟수입니다.
Far End Loss Count	마지막 '클리어' 이후 누적된 원격 측의 프레임 손실 횟수입니다.
Interval Elapsed	마지막 '클리어' 이후 경과한 'FLR 간격'의 누적 횟수입니다.
Interval Near End Loss Ratio	근접 측의 프레임 손실 횟수와 원격 측에서 전송한 프레임 수를 기반으로 최신 'FLR 간격'에서 계산된 근접 측 프레임 손실 비율입니다. 이 값은 (손실/전송)*10000 으로 표시됩니다. 1/100 백분율과 동일합니다.
Interval Far End Loss Ratio	원격 측의 프레임 손실 횟수와 근접 측에서 전송한 프레임 수를 기반으로 최신 'FLR 간격'에서 계산된 원격 측 프레임 손실 비율입니다. 이 값은 (손실/전송)*10000 으로 표시됩니다. 1/100 백분율과 동일합니다.
Total Near End Loss Ratio	마지막 '클리어' 이후 근접 측의 프레임 손실 횟수와 원격 측에서 전송한 프레임 수를 기반으로 계산된 근접 측 프레임 손실 비율입니다. 이 값은 (손실/전송)*10000 으로 표시됩니다. 1/100 백분율과 동일합니다.
Interval Far End Loss Ratio	마지막 '클리어' 이후 원격 측의 프레임 손실 횟수와 근접 측에서 전송한 프레임 수를 기반으로 계산된 원격 측 프레임 손실 비율입니다. 이 값은 (손실/전송)*10000 으로 표시됩니다. 1/100 백분율과 동일합니다.
Clear	이 체크 및 저장 세트는 누적 카운터를 지우고 비율 계산을 다시 시작합니다.

Loss Measurement Availability

용어	설명
Enable	손실 측정 가능성의 활성화/비활성화 여부입니다.
Interval	가용성 상태를 변경하기 위해 동일한 가용성을 가진 측정 횟수입니다. 유효한 범위는 1 에서 1000 까지입니다.
FLR Threshold	프레임 손실 비율에 대한 가용성 임계 값을 per mille(1000 분의 1) 단위로 나타냅니다.
Maintenance	손실 측정 가용성 유지의 활성화/비활성화 여부입니다.

Loss Measurement Availability Status

용어	설명
Near Avail Count	근접 측이 "Avail" 상태일 때 수행된 측정 횟수입니다.
Far Avail Count	원격 측이 "Avail" 상태일 때 수행된 측정 횟수입니다.
Near Unavail Count	근접 측이 "Unavail" 상태일 때 수행된 측정 횟수입니다.
Far Unavail Count	원격 측이 "Unavail" 상태일 때 수행된 측정 횟수입니다.
Near Window Curr	현재 근접 측의 가용성 윈도우 크기입니다. 근접 상태가 "Avail"일 때, 이 값은 정의된 프레임 손실 비율 임계 값을 초과하는 연속된 측정의 현재 개수를 나타냅니다. 근접 상태가 "Unavail"일 때, 이 값은 정의된 프레임 손실 비율 임계 값과 동일하거나 이하인 연속된 측정의 현재 개수를 나타냅니다. 이 값이 정의된 "Interval" 값(또는 "윈도우 크기"로도 알려짐)에 도달하면 가용성 상태가 변경됩니다.
Far Window Curr	현재 원격 측의 가용성 윈도우 크기입니다. 자세한 내용은 근접 측 윈도우 현재 값을 위한 설명을 참조하십시오.
Near State	현재 근접 측의 가용성 상태입니다.
Far State	현재 원격 측의 가용성 상태입니다.

Loss Measurement High Loss Interval

용어	설명
Enable	손실 측정 고 손실 간격의 활성화/비활성화 여부입니다.
FLR Threshold	고 손실 간격의 프레임 손실 비율 임계 값을 per mille(1000 분의 1) 단위로 나타냅니다.
Consecutive Interval	고 손실 간격의 연속된 측정 횟수입니다.

Loss Measurement High Loss Interval Status

용어	설명
Near Count	근접 측의 고 손실 간격 횟수입니다. 이는 가용성 상태가 "가용"이고 FLR 이 고 손실 간격 FLR 임계 값을 초과하는 측정 횟수를 나타냅니다.
Far Count	원격 측의 고 손실 간격 횟수입니다. 이는 가용성 상태가 "가용"이고 FLR 이 고 손실 간격 FLR 임계 값을 초과하는 측정 횟수를 나타냅니다.
Near Consecutive Count	근접 측의 고 손실 간격 연속 횟수입니다.
Far Consecutive Count	원격 측의 고 손실 간격 연속 횟수입니다.

Loss Measurement Signal Degrade

용어	설명
Enable	손실 측정 신호 저하의 활성화/비활성화 여부입니다.
TX Minimum	측정 이전에 프레임 손실 비율을 손실 비율 임계 값과 비교하기 전에 전송되어야 하는 최소 프레임 수입니다.
FLR Threshold	per mille(1000 분의 1) 단위로 표시된 신호 저하된 프레임 손실 비율 임계 값입니다.
Bad Threshold	저하 상태를 설정하기 위해 연속적으로 나쁜 간격 측정의 수입니다.
Good Threshold	저하 상태를 해제하기 위해 연속적으로 좋은 간격 측정의 수입니다.

Delay Measurement

용어	설명
Enable	1DM/DMM PDU 를 전송하여 지연 측정을 활성화/비활성화할 수 있습니다. 1DM/DMR PDU 를 수신하고 처리하여 지연 측정을 하는 것은 항상 활성화되어 있습니다.
Priority	태그에 PCP 비트로 삽입될 우선순위입니다 (있는 경우).
Cast	1DM/DMM PDU 의 전송 방식을 유니캐스트 또는 멀티캐스트로 선택할 수 있습니다. 유니캐스트 MAC 은 'Peer MEP'를 통해 구성될 것입니다.
Peer MEP	이 설정은 'Cast'가 Uni 로 구성된 경우에만 사용됩니다. 1DM/DMR 유니캐스트 MAC 은 해당 피어의 '유니캐스트 피어 MAC' 구성에서 가져옵니다.
Ended	Single: DMM/DMR 을 기반으로 한 단일 종단 지연 측정. Dual: 1DM 을 기반으로 한 이중 종단 지연 측정.
Tx Mode	Standardize: 1DM/DMR 을 전송하기 위한 Y.1731 표준화 방식입니다. Proprietary: Vitesse 의 고유한 방식으로, 1DM/DMR 을 전송하기 위해 후속 패킷을 사용합니다.
Calc	이 설정은 'Ended'가 단일 종단으로 구성된 경우에만 사용됩니다. Round trip: 초기화자의 전송 및 수신 타임스탬프에 의해 계산된 프레임 지연입니다. 프레임 지연 = RxTimeb - TxTimeStampf Flow: 초기화자와 원격의 전송 및 수신 타임스탬프에 의해 계산된 프레임 지연입니다. 프레임 지연 = (RxTimeb - TxTimeStampf) - (TxTimeStampb - RxTimeStampf)
Gap	10ms 간격으로 1DM/DMM PDU 를 전송하는 간격입니다. 범위는 10 에서 65535 까지입니다.
Count	계산할 최근 레코드의 개수입니다. 범위는 10 에서 2000 까지입니다.
Unit	시간 해상도입니다.
Synchronized	이중 종단 DM 을 계산하기 위해 DMM/DMR 패킷을 사용하는 기능을 활성화합니다. 이 옵션이 활성화된 경우 다음 동작이 수행됩니다. DMR 을 수신하면 왕복 지연(라운드트립 또는 플로우) 및 근접 측에서 원격 측으로의 단방향 지연과 원격 측에서 근접 측으로의 단방향 지연이 모두 계산됩니다. DMM 또는 1DM 을 수신하면 원격 측에서 근접 측으로의 단방향 지연만 계산됩니다.
Counter Overflow Action	오버플로우가 발생할 때 수행할 동작입니다.

Delay Measurement State

용어	설명
Tx	마지막 '클리어' 이후 누적된 전송 횟수입니다.
Rx	마지막 '클리어' 이후 누적된 수신 횟수입니다.
Rx Timeout	마지막 '클리어' 이후 누적된 양방향 수신 타임아웃 횟수입니다.
Rx Error	마지막 '클리어' 이후 누적된 수신 오류 횟수입니다. 이는 프레임 지연이 1 초보다 크거나 원격 측의 체류 시간이 왕복 시간보다 큰 경우에 계산됩니다.
Av Delay Tot	마지막 '클리어' 이후 평균 총 지연 시간입니다.
Av Delay last N	마지막 '클리어' 이후 마지막 n 개 패킷의 평균 지연 시간입니다.
Delay Min.	마지막 '클리어' 이후 최소 지연 시간입니다.
Delay Max.	마지막 '클리어' 이후 최대 지연 시간입니다.
Av Delay-Var Tot	마지막 '클리어' 이후 평균 총 지연 변동입니다.
Av Delay-Var last N	마지막 '클리어' 이후 마지막 n 개 패킷의 평균 지연 변동입니다.

Delay-Var Min.	마지막 '클리어' 이후 최소 지연 변동입니다.
Delay-Var Max.	마지막 '클리어' 이후 최대 지연 변동입니다.
Overflow	마지막 '클리어' 이후 카운터 오버플로우 횟수입니다.
Clear	이 체크 및 저장 설정은 누적된 카운터를 초기화합니다.
Far-end-to-near-end one-way delay	단방향 지연은 원격 장치에서 로컬 장치로의 지연입니다. 다음은 이 지연을 계산하는 조건입니다. 1. 1DM 수신. 2. 동기화가 활성화된 DMM 수신. 3. 동기화가 활성화된 DMR 수신.
Near-end-to-far-end one-way delay	단방향 지연은 로컬 장치에서 원격 장치로의 지연입니다. 이 지연을 계산하는 유일한 경우는 다음과 같습니다: 동기화가 활성화된 DMR 수신.

Delay Measurement Bins

Measurement Bin은 지정된 범위 내에 속하는 지연 측정의 수를 Measurement Interval 동안에 저장하는 카운터입니다.

용어	설명
Measurement Bins for FD	Measurement Interval 당 구성 가능한 프레임 지연 Measurement Bins 의 수입니다. 지원되는 Measurement Interval 당 최소 FD Measurement Bin 수는 2 입니다. 지원되는 Measurement Interval 당 최대 FD Measurement Bin 수는 10 입니다. 지원되는 Measurement Interval 당 기본 FD Measurement Bin 수는 3 입니다.
Measurement Bins for IFDV	Measurement Interval 당 구성 가능한 프레임 지연 변동 Measurement Bins 의 수입니다. 지원되는 Measurement Interval 당 최소 FD Measurement Bin 수는 2 입니다. 지원되는 Measurement Interval 당 최대 FD Measurement Bin 수는 10 입니다. 지원되는 Measurement Interval 당 기본 FD Measurement Bin 수는 2 입니다.
Measurement Threshold	각 Measurement Bins 에 대해 구성 가능한 측정 임계 값입니다. 측정 임계 값의 단위는 마이크로초 (us)입니다. 측정 구간의 기본 구성된 측정 임계 값은 5000 us 의 증가입니다.

Delay Measurement Bins for FD

Measurement Bin은 Measurement Interval 동안 지정된 범위 내에 속하는 지연 측정의 수를 저장하는 카운터입니다. 측정 임계 값이 5000 마이크로초(us)이고 Measurement Bin의 총 개수가 네 개인 경우, 다음과 같은 예를 들 수 있습니다.

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us(0 이상 5000 미만의 지연 측정 수)
bin1	5,000 us	5,000 us <= measurement < 10,000 us(5000 이상 10000 미만의 지연 측정 수)
bin2	10,000 us	10,000 us <= measurement < 15,000 us(10000 이상 15000 미만의 지연 측정 수)
bin3	15,000 us	15,000 us <= measurement < infinite us(15000 이상 무한대의 지연 측정 수)

Delay Measurement Bins for IFDV

Measurement Bin은 Measurement Interval 동안 지정된 범위 내에 속하는 지연 측정의 수를 저장하는 카운터 입니다. 측정 임계 값이 5000 마이크로초(us)이고 Measurement Bin의 총 개수가 네 개인 경우, 다음과 같은 예를 들 수 있습니다.

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us(0 이상 5000 미만의 지연 측정 수)
bin1	5,000 us	5,000 us <= measurement < 10,000 us(5000 이상 10000 미만의 지연 측정 수)
bin2	10,000 us	10,000 us <= measurement < 15,000 us(10000 이상 15000 미만의 지연 측정 수)
bin3	15,000 us	15,000 us <= measurement < infinite us(15000 이상 무한대의 지연 측정 수)

Buttons

Back : 다시 MEP 인스턴스 메인 페이지로 이동 합니다.

Refresh: 클릭 시 페이지를 새로 고침. 로컬 변경 사항은 취소합니다.

Apply: 클릭 시 변경사항을 적용합니다.

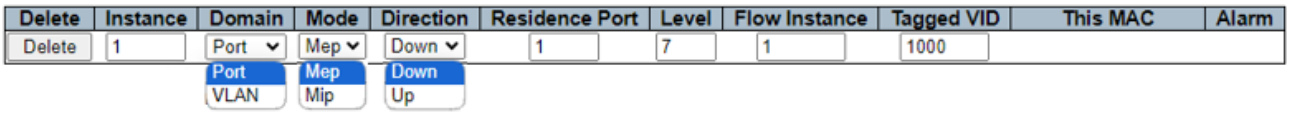
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>MEP

- ✓ **Maintenance Entity Point**
  - ➢ ***Add New MEP***
    - ***Instance(1~100)***
    - ***Domain(Port | VLAN)***
    - ***Mode(Mep | Mip)***
    - ***Direction(Down | Up)***
    - ***Residence Port(Port Number | VLAN ID)***
    - ***Level(0~7)***
    - ***Flow Instance***
    - ***Tagged VID***



Maintenance Entity Point

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
☐	1	Port	Mep	Down	1	7		1000	02-21-6D-44-44-44	
☐	2	Port	Mep	Down	2	7		1000	06-21-6D-44-44-44	

인스턴스 번호를 클릭하세요.

✓ MEP Configuration

✓ Instance Data

Instance	Domain	Mode	Direction	Residence Port	Flow Instance	Tagged VID	EPS Instance	This MAC
1	Port	Mep	Down	1		1000	0	02-21-6D-44-44-44

✓ Instance Configuration

Level	Format	Domain Name	MEG id	MEP id	Tagged VID	Syslog
7	ITU ICC		ICC000MEG0000	1	1000	☐

- ***Level(0~7)***
- ***Format(ITU ICC | IEEE String | ITU CC ICC)***
- ***Domain Name(IEEE String 만 해당됩니다.)***
  - *이 항목은 비어있거나, 최대 16자까지 사용 가능합니다.*
- ***MEG ID***
  - *ITU ICC는 13자까지 가능합니다.*
  - *ITU CC ICC는 15자까지 가능합니다.*
  - *IEEE String은 16자까지 가능합니다.*
- ***MEP ID***
  - ***0~8191***
- ***Tagged VID***
  - ***0~4095***
- ***Syslog(Enable | Disable)***

✓ Peer MEP Configuration

Delete	Peer MEP ID	Unicast Peer MAC
No Peer MEP Added		

Click Add New Peer MEP

Delete	Peer MEP ID	Unicast Peer MAC
No Peer MEP Added		
Delete	0	00-00-00-00-00-00

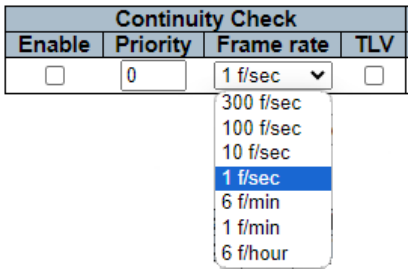
- ***Peer MEP ID (Input Peer MEP ID)***
- ***Unicast Peer MAC (Auto | Manual)***

- ***MEP ID를 입력하면 MAC이 자동으로 검색됩니다.***
- ***Unicast Peer MAC 은 수동으로도 입력 가능합니다.***

✓ Functional Configuration

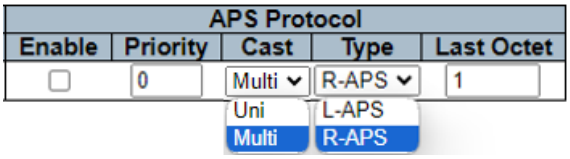
➢ *Continuity Check*

- ***Enable***
- ***Priority(0~7)***
- ***Frame rate(300f/sec | 100f/sec | 10f/sec | 1f/sec | 6f/min | 1f/min | 6f/hour)***
- ***TLV***



➢ *APS Protocol*

- ***Enable***
- ***Priority(0~7)***
- ***Cast(Uni | Multi)***
- ***Type(L-APS | R-APS)***
- ***Last Octet(0~255)***



✓ TLV Configuration

➢ *Organization Specific TLV(Global)*

- ***OUI First(0~255)***
- ***OUI Second(0~255)***
- ***OUI Third(0~255)***
- ***Sub-Type(0~255)***
- ***Value(0~255)***

Organization Specific TLV (Global)				
OUI First	OUI Second	OUI Third	Sub-Type	Value
0	0	12	1	2

✓ **Link State Tracking**

➢ ***Enable***

Enable
☐

✓ **MEP Status Alarm**

➢ ***Instance Configuration***

- ***cLevel, cMEG, cMEP, cAIS, cLCK, cLoop, cConfig, cSSF, aBLK, aTSD, aTSF***

cLevel	cMEG	cMEP	cAIS	cLCK	cLoop	cConfig	cSSF	aBLK	aTSD	aTSF
●	●	●	●	●	●	●	●	●	●	●

➢ ***Peer MEP Configuration***

- ***cLOC, cRDI, cPeriod, cPriority, cDEG***

cLOC	cRDI	cPeriod	cPriority	cDEG
●	●	●	●	●

✓ **TLV Status**

➢ ***Peer MEP ID***

➢ ***CC Organization Specific***

- ***OUI First, OUI Second, OUI Third, Sub-Type, Value, Last RX***

➢ ***CC Port Status***

- ***Value, Last RX***

➢ ***CC Interface Status***

- ***Value, Last RX***

Peer MEP ID	CC Organization Specific							CC Port Status			CC Interface Status	
	OUI First	OUI Second	OUI Third	Sub-Type	Value	Last RX		Value	Last RX		Value	Last RX
2	0	0	0	0	0	●		0	●		0	●

EXAMPLE CLI CONFIGURATION

✓ **Ethernet Protection Switching**

➢ ***Add New EPS***

- ***Instance(1~100)***
- ***Domain(Port | VLAN)***
- ***Mode(Mep | Mip)***

- ***Direction(Down | Up)***
- ***Residence Port(Port Number | VLAN ID)***
- ***Level(0~7)***
- ***Flow Instance***
- ***Tagged VID***

```
(config)# mep <inst> [ mip ] { up | down } domain { port | evc | vlan | tp-link | tunnel-tp | pw | lsp }
[ vid <vid> ] [ flow <flow> ] level <level> [ interface <port_type> <port> ]
(config)# mep 1 down domain port vid 1000 level 7 interface GigabitEthernet 1/1
(config)# mep 2 down domain port vid 1000 level 7 interface GigabitEthernet 1/2
```

✓ **MEP Configuration**

✓ **Instance Data**

✓ **Instance Configuration**

➢ ***Level(0~7)***

```
(config)# mep <inst> level <level>
(config)# mep 1 level 1
```

➢ ***Format(ITU ICC | IEEE String | ITU CC ICC)***

➢ ***Domain Name(Use only IEEE String)***

- *이 항목은 비어있거나, 최대 16자까지 사용 가능합니다.*

➢ ***MEG ID***

- ***ITU ICC는 13자까지 가능합니다.***
- ***ITU CC ICC는 15자까지 가능합니다.***
- ***IEEE String은 16자까지 가능합니다.***

```
(config)# mep <inst> meg-id <megid> { itu | itu-cc | { ieee [ name <name> ] } }
(config)# mep 1 meg-id example itu
(config)# mep 1 meg-id example itu-cc
(config)# mep 1 meg-id example ieee name example1
```

➢ ***MEP ID***

- ***0~8191***

```
(config)# mep <inst> mep-id <mepid>
(config)# mep 1 meg-id example itu
(config)# mep 1 meg-id example itu-cc
(config)# mep 1 meg-id example ieee name example1
```

➢ ***Tagged VID***

- ***0~4095***

```
(config)# mep <inst> vid <vid>
(config)# mep 1 vid 1000
```

➢ ***Syslog(Enable | Disable)***

```
(config)# mep <inst> syslog
(config)# mep 1 syslog
```

✓ **Peer MEP Configuration**

➢ ***Peer MEP ID (Input Peer MEP ID)***

➢ ***Unicast Peer MAC (Auto | Manual)***

- ***MEP ID를 입력하면 MAC이 자동으로 검색됩니다.***
- ***Unicast Peer MAC 은 수동으로도 입력 가능합니다.***

```
(config)# mep <inst> peer-mep-id <mepid> [ mac <mac> ]
(config)# mep 1 peer-mep-id 2
(config)# mep 1 peer-mep-id 2 mac 00-21-6d-00-00-00
```

✓ **Functional Configuration**

➢ ***Continuity Check***

- ***Enable***
- ***Priority(0~7)***
- ***Frame rate(300f/sec | 100f/sec | 10f/sec | 1f/sec | 6f/min | 1f/min | 6f/hour)***

```
(config)# mep <inst> cc <prio> [ fr300s | fr100s | fr10s | fr1s | fr6m | fr1m | fr6h ]
(config)# mep 1 cc 7 fr1s
(config)# mep 1 cc 0
```

- ***TLV***

```
(config)# mep <inst> ccm-tlv
(config)# mep 1 ccm-tlv
```

➢ ***APS Protocol***

- ***Enable***
- ***Priority(0~7)***
- ***Cast(Uni | Multi)***
- ***Type(L-APS | R-APS)***
- ***Last Octet(0~255)***

```
(config)# mep <inst> aps <prio> [ multi | uni ] { laps | { raps [ octet <octet> ] } }
(config)# mep 1 aps 0 raps octet 1
(config)# mep 2 aps 7 raps octet 255
(config)# mep 1 aps 7 laps
```

✓ TLV Configuration

- ➢ ***Organization Specific TLV(Global)***
  - ***OUI First, OUI Second, OUI Third(0-0xffffff)***
  - ***Sub-Type(0-0xff)***
  - ***Value(0-0xff)***

```
(config)# mep os-tlv oui <oui> sub-type <subtype> value <value>
(config)# mep os-tlv oui 0xffffff sub-type 0xff value 0xff
(config)# mep os-tlv oui 0xC sub-type 0x1 value 0x2
```

✓ Link State Tracking

- ➢ ***Enable***

```
(config)# (config)# mep 1 link-state-tracking
```

✓ MEP Status Alarm

- ➢ ***Instance Configuration***
  - ***cLevel, cMEG, cMEP, cAIS, cLCK, cLoop, cConfig, cSSF, aBLK, aTSD, aTSF***
- ➢ ***Peer MEP Configuration***
  - ***cLOC, cRDI, cPeriod, cPriority, cDEG***

```
# show mep

MEP state is:
  Inst  cLevel  cMeg  cMep  cAis  cLck  cLoop cConf  cSsf  aBlk  aTsd  aTsf  Peer MEP  cLoc  cRdi
     1  False   False  False  False False  False  False  True  False  False  True        2     False False

cPeriod cPrio  cDeg
False   False  False
```

✓ TLV Status

- ➢ ***Peer MEP ID***
- ➢ ***CC Organization Specific***
  - ***OUI First, OUI Second, OUI Third, Sub-Type, Value, Last RX***
- ➢ ***CC Port Status***
  - ***Value, Last RX***
- ➢ ***CC Interface Status***
  - ***Value, Last RX***

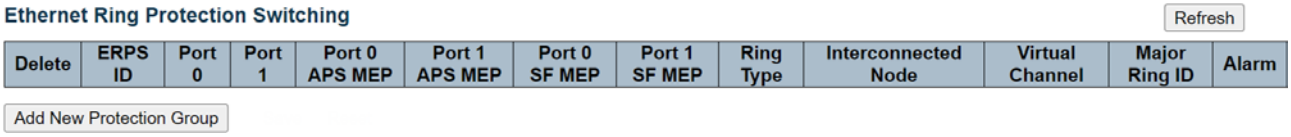
```
# show mep tlv
MEP CCM TLV Status is:
    Inst  Peer MEP    OS OUI    OS Sub    OS Value    PS Value    IS Value    OS RX    PS RX    IS RX
       1         2    00-00-00         0           0           0           0    False    False    False
```

6.14. ERPS

6.14.1. ERPS Configuration

웹메뉴 Configuration>ERPS

여기에서 ERPS 인스턴스를 구성할 수 있습니다.



Ethernet Ring Protection Switching

용어	설명
Delete	이 상자는 다음 저장 작업에서 ERPS 를 삭제할 때 사용됩니다.
ERPS ID	생성된 보호 그룹의 ID 입니다. 1 부터 64 까지의 정수 값이어야 합니다. 생성할 수 있는 ERPS 보호 그룹의 최대 개수는 64 입니다. 보호 그룹의 ID 를 클릭하여 구성 페이지로 이동할 수 있습니다.
Port 0	이는 링 내의 스위치의 포트 0 을 생성합니다.
Port 1	이는 링 내의 스위치의 "포트 1"을 생성합니다. 상호 연결된 하위 링은 하나의 링 포트만을 가지므로 "포트 1"은 상호 연결된 하위 링을 위해 "0"으로 구성됩니다. 이 필드의 "0"은 해당 인스턴스에 "포트 1"이 연결되어 있지 않음을 나타냅니다.
Port 0 SF MEP	포트 0 신호 장애를 보고하는 MEP 입니다.
Port 1 SF MEP	포트 1 신호 장애를 보고하는 MEP 입니다. 가상 채널이 없는 상호 연결된 하위 링에는 하나의 SF MEP 만이 연관되므로 해당 링 인스턴스에는 "0"으로 구성됩니다. 이 필드의 "0"은 해당 인스턴스에 포트 1 SF MEP 가 연결되어 있지 않음을 나타냅니다.
Port 0 APS MEP	포트 0 APS PDU 처리 MEP 입니다.
Port 1 APS MEP	포트 1 APS PDU 처리 MEP 입니다. 가상 채널이 없는 상호 연결된 하위 링에는 하나의 APS MEP 만이 연관되므로 해당 링 인스턴스에는 "0"으로 구성됩니다. 이 필드의 "0"은 해당 인스턴스에 포트 1 APS MEP 가 연결되어 있지 않음을 나타냅니다.
Ring Type	보호 링의 유형입니다. 주요 링 또는 하위 링으로 설정할 수 있습니다.
Interconnected Node	"Interconnected Node"은 링 인스턴스가 상호 연결되었음을 나타냅니다. 구성하려면 해당 확인란을 클릭하십시오. "예"는 이 인스턴스에 대해 상호 연결된 노드임을 나타냅니다. "아니오"는 구성된 인스턴스가 상호 연결되지 않은 것을 나타냅니다.
Virtual Channel	하위 링은 상호 연결된 노드에서 가상 채널을 가질 수 있거나 가지지 않을 수 있습니다. 이는 "가상 채널" 확인란을 사용하여 구성됩니다. "예"는 가상 채널을 가진 하위 링임을 나타냅니다. "아니오"는 하위 링이 가상 채널을 가지지 않음을 나타냅니다.
Major Ring ID	상호 연결된 하위 링의 주요 링 그룹 ID 입니다. 이는 주요 링에서 토폴로지 변경 업데이트를 보내는 데 사용됩니다. 링이 주요 링인 경우, 이 값은 해당 링의 보호 그룹 ID 와 동일합니다.
Alarm	ERPS 에 활성화된 알람이 있습니다.

Buttons

Add New Protection Group : 새로운 보호 그룹 항목을 추가합니다.

Refresh: 클릭 시 페이지를 새로 고침. 로컬 변경 사항은 취소합니다.

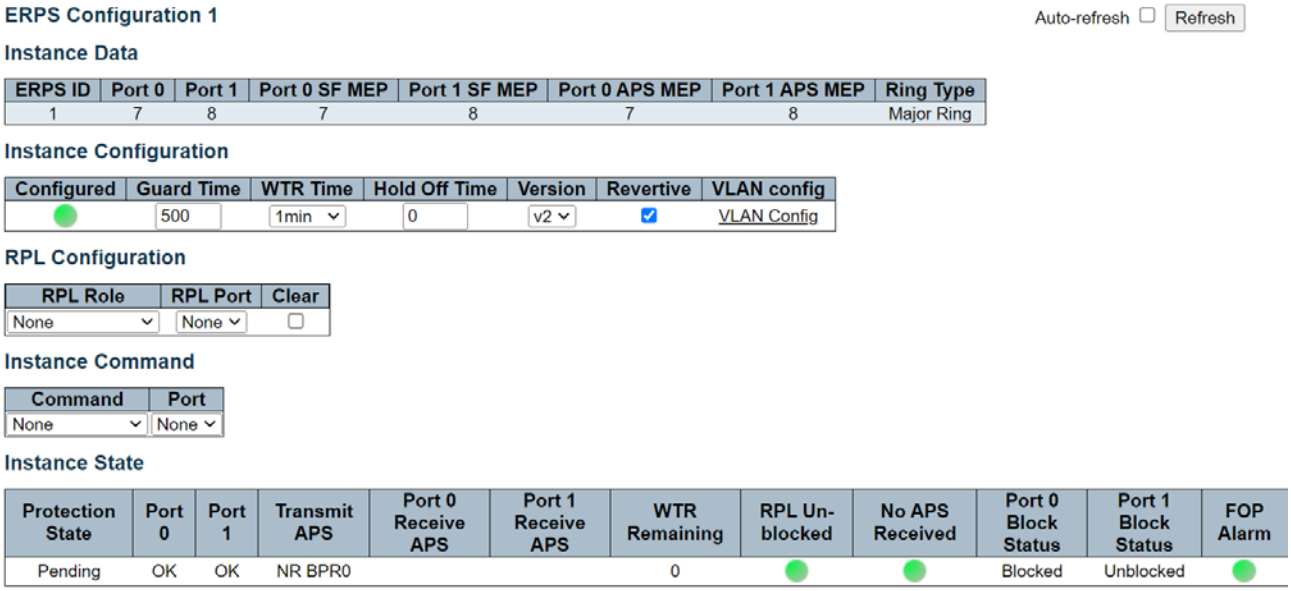
Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

ERPS Configuration 1

이 페이지는 사용자가 현재 ERPS 인스턴스를 검사하고 구성할 수 있도록 합니다.



ERPS Configuration 1

Instance Data

용어	설명
ERPS ID	보호 그룹의 ID 입니다.
Port 0	ERPS 웹 생성에 대한 도움말을 참조하십시오.
Port 1	ERPS 웹 생성에 대한 도움말을 참조하십시오.
Port 0 SF MEP	ERPS 웹 생성에 대한 도움말을 참조하십시오.
Port 1 SF MEP	ERPS 웹 생성에 대한 도움말을 참조하십시오.
Port 0 APS MEP	ERPS 웹 생성에 대한 도움말을 참조하십시오.
Port 1 APS MEP	ERPS 웹 생성에 대한 도움말을 참조하십시오.
Ring Type	보호 링의 유형입니다. 주요 링 또는 하위 링으로 설정할 수 있습니다.

Instance Configuration

용어	설명
Configured	빨간색: 이 ERPS 는 생성되었지만 아직 구성되지 않았으며 비활성화되어 있습니다.

	초록색: 이 ERPS 는 구성되었으며 활성화되어 있습니다.
Guard Time	오래된 R-APS 메시지 수신을 방지하기 위해 사용되는 가드 타임아웃 값입니다. 가드 타이머의 기간은 10ms 단위로 구성할 수 있으며, 최소값은 10ms 이고 최대값은 2 초입니다. 기본값은 500ms 입니다.
WTR Time	복원 전환에서 사용되는 복원 대기 시간(Wait To Restore) 값입니다. WTR 시간의 기간은 1 분 단위로 운영자에 의해 구성할 수 있으며, 최소값은 5 분에서 최대값은 12 분입니다. 기본값은 5 분입니다.
Hold Off Time	스위칭 전에 Signal Fail 에 대한 지속적인 확인을 수행하는 데 사용되는 타이밍 값입니다. 홀드 오프 타이머의 범위는 0 에서 10 초이며, 100ms 단위로 구성할 수 있습니다.
Version	ERPS 프로토콜 버전 - v1 또는 v2
Revertive	Revertive 모드에서는 보호 전환을 발생시키는 조건이 해결된 후에 트래픽 채널이 작동 중인 전송 엔티티로 복원되며, 즉 RPL 에서 차단됩니다. Non-Revertive 모드에서는 보호 전환 조건이 해결된 후에도 트래픽 채널은 RPL 을 사용하며, RPL 이 실패하지 않은 경우에 계속 사용됩니다.
VLAN config	보호 그룹의 VLAN 구성입니다. "VLAN 구성" 링크를 클릭하여 이 보호 그룹의 VLAN 을 구성할 수 있습니다.

RPL Configuration

용어	설명
RPL Role	이는 RPL 소유자 또는 RPL 이웃으로 설정할 수 있습니다.
RPL Port	이를 통해 동쪽 포트 또는 서쪽 포트를 RPL 블록으로 선택할 수 있습니다.
Clear	소유자를 변경해야 하는 경우, 클리어 확인란을 선택하여 해당 ERPS 링의 RPL 소유자를 지울 수 있습니다.

Sub-Ring Configuration

용어	설명
Topology Change	이 확인란을 선택하면 하위 링의 토폴로지 변경이 주요 링에 전파되는 것을 나타냅니다.

Instance Command

용어	설명
Command	관리 명령입니다. 포트는 수동 전환 또는 강제 전환 상태 중 하나로 관리적으로 구성될 수 있습니다.
Forced Switch	강제 전환 명령은 해당 명령이 발행된 링 포트에 차단을 강제로 적용합니다.
Manual Switch	장애 또는 FS 가 없는 경우, 수동 전환 명령은 해당 명령이 발행된 링 포트에 차단을 강제로 적용합니다.
Clear	Clear 명령은 활성 로컬 관리 명령 (예: 강제 전환 또는 수동 전환)을 지우는 데 사용됩니다.
Port	포트 선택 - 해당 명령이 적용되는 보호 그룹의 Port0 또는 Port1 입니다.

Instance State

용어	설명
Protection State	G.8032 의 상태 전이 테이블에 따른 ERPS 상태입니다.
Port 0	OK: 동쪽 포트의 상태가 정상입니다. SF: 동쪽 포트의 상태가 Signal Fail 입니다.

Port 1	OK: 서쪽 포트의 상태가 정상입니다. SF: 서쪽 포트의 상태가 Signal Fail 입니다.
Transmit APS	G.8032 의 상태 전이 테이블에 따른 전송된 APS 입니다.
Port 0 Receive APS	G.8032 의 상태 전이 테이블에 따른 Port 0 에서 수신된 APS 입니다.
Port 1 Receive APS	G.8032 의 상태 전이 테이블에 따른 Port 1 에서 수신된 APS 입니다.
WTR Remaining	WTR (Wait To Restore) 타임아웃이 남은 시간(밀리초)입니다.
RPL Un-blocked	워킹 플로우에서 APS 가 수신되었습니다.
No APS Received	다른쪽에서 RAPS PDU 를 수신하지 못했습니다.
Port 0 Block Status	포트 0 의 차단 상태 (트래픽과 R-APS 차단 상태 모두). 가상 채널이 없는 하위 링에서는 R-APS 채널이 절대로 차단되지 않습니다.
Port 1 Block Status	포트 1 의 차단 상태 (트래픽과 R-APS 차단 상태 모두). 가상 채널이 없는 하위 링에서는 R-APS 채널이 절대로 차단되지 않습니다.
FOP Alarm	프로토콜 결함(FOP) 상태의 실패. FOP 가 감지되면 빨간색 LED 가 켜지고, 그렇지 않으면 녹색 LED 가 켜집니다.

Buttons

Refresh: 클릭 시 페이지를 새로 고침. 로컬 변경 사항은 취소합니다.

Auto-refresh : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

ERPS VLAN Configuration n

ERPS VLAN Configuration n

용어	설명
Delete	VLAN 항목을 삭제하려면 이 상자를 선택하세요. 항목은 다음 저장 시 삭제됩니다.
VLAN ID	이 특정 VLAN 의 ID 를 나타냅니다.
Adding a New VLAN	새로운 VLAN ID 를 추가하려면 Add New Entry 를 "클릭"하세요. VLAN ID 의 유효한 값은 1 부터 4095 까지입니다. "저장"을 클릭하면 VLAN 이 활성화됩니다. 포트 멤버가 없는 VLAN 은 "저장"을 클릭할 경우 삭제됩니다. Delete 버튼은 새로운 VLAN 추가를 되돌리는 데 사용할 수 있습니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

Back : 이 MEP 인스턴스의 메인 페이지로 돌아가려면 클릭하세요.

Refresh: "VLAN ID" 입력 필드부터 시작하여 표시된 테이블을 새로고침 하려면 클릭하세요.

WEB 설정 예시

웹메뉴 Configuration>ERPS

✓ **Ethernet Ring Protection Switching**

➢ ***Add New Protection Group***

- ***ERPS ID(1~64)***
- ***Port 0(Enter Port Number)***
- ***Port 1(Enter Port Number)***
- ***Port 0 APS MEP(Enter MEP Instance Number)***
- ***Port 1 APS MEP(Enter MEP Instance Number)***
- ***Port 0 SF MEP(Enter MEP Instance Number)***
- ***Port 1 SF MEP(Enter MEP Instance Number)***
- ***Ring Type(Major | Sub)***
- ***Interconnected Node(Enable | Disable)***
- ***Virtual Channel(can be set on the sub ring)***
- ***Major Ring ID(can be set when it is both an Interconnected Node and a sub ring)***

Ethernet Ring Protection Switching

Delete	ERPS ID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	Ring Type	Interconnected Node	Virtual Channel	Major Ring ID	Alarm
Delete	1	1	2	1	2	1	2	Major	☐	☐	0	

Delete	ERPS ID	Port 0	Port 1	Port 0 APS MEP	Port 1 APS MEP	Port 0 SF MEP	Port 1 SF MEP	Ring Type	Interconnected Node	Virtual Channel	Major Ring ID	Alarm
☐	1	1	2	1	2	1	2	Major	No	No	1	

ERPS ID를 클릭

✓ **ERPS Configuration n**

✓ **Instance Data**

➢ ***ERPS ID***

➢ ***Port 0***

➢ ***Port 1***

➢ ***Port 0 SF MEP***

➢ ***Port 1 SF MEP***

➢ ***Port 0 APS MEP***

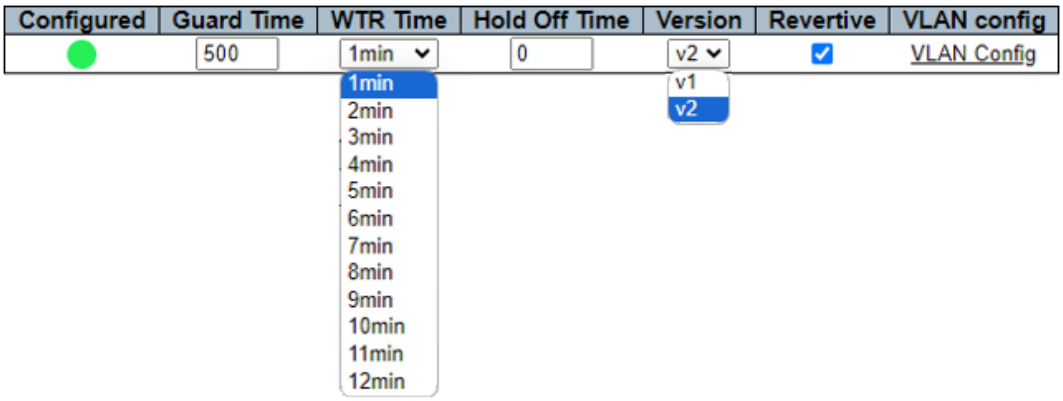
➢ ***Port 1 APS MEP***

➢ ***Ring Type***

ERPS ID	Port 0	Port 1	Port 0 SF MEP	Port 1 SF MEP	Port 0 APS MEP	Port 1 APS MEP	Ring Type
1	1	2	1	2	1	2	Major Ring

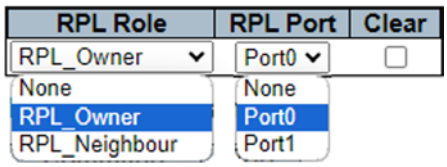
✓ Instance Configuration

- ➢ ***Configured***
- ➢ ***Guard Time***
  - ***10~2000(msec)***
- ➢ ***WTR Time***
  - ***1min | 2min | 3min | 4min | 5min | 6min | 7min | 8min | 9min | 10min | 11min | 12min***
- ➢ ***Hold Off Time***
  - ***0~10000(msec)***
- ➢ ***Version***
  - ***v1 | v2***
- ➢ ***Revertive***
  - ***Enable | Disable***
- ➢ ***VLAN config***
  - ***VLAN Config (ERPS VLAN Configuration 페이지로 이동합니다.)***



✓ RPL Configuration

- ➢ ***RPL Role***
  - ***None | RPL_Owner | RPL_Neighbour***
- ➢ ***RPL Port***
  - ***None | Port0 | Port1***
- ➢ ***Clear***
  - ***Check Box***
    (RPL 설정을 리셋하고 싶으면 체크설정 후 Apply 하세요.)



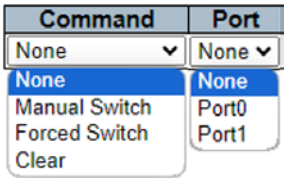
✓ **Instance Command**

➢ ***Command***

- ***None | Manual Switch | Forced Switch | Clear***

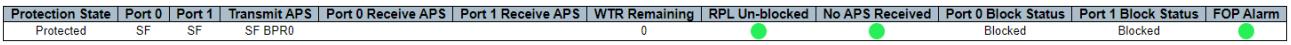
➢ ***Port***

- ***None | Port0 | Port1***



✓ **Instance State**

➢ ***Protection State | Port 0 | Port 1 | Transmit APS | Port 0 Receive APS | Port 1 Receive APS | WTR Remaining | RPL Un-blocked | No APS Received | Port 0 Block Status | Port 1 Block Status | FOP Alarm***

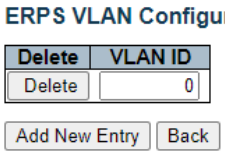


VLAN Config 를 클릭

✓ **ERPS VLAN Configuration n**

➢ ***Add New Entry***

- ***VLAN ID(1~4095)***



CLI 설정 예시

✓ **Ethernet Ring Protection Switching**

➢ ***Add New Protection Group***

- ***ERPS ID(1~64)***
- ***Port 0(Enter Port Number)***
- ***Port 1(Enter Port Number)***
- ***Interconnected Node(Enable | Disable)***

- ***Ring Type(Major | Sub)***
- ***Virtual Channel(can be set on the sub ring)***
- ***Major Ring ID(can be set when it is both an Interconnected Node and a sub ring)***

```
(config)# erps <group> major port0 interface <port_type> <port0> port1 interface <port_type> <port1> [ interconnect ]
(config)# erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet 1/2
(config)# erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet 1/2 interconnect
```

```
(config)# erps <group> sub port0 interface <port_type> <port0> { { port1 interface <port_type> <port1> } | { interconnect <major_ring_id> } } [ virtual-channel ]
(config)# erps 1 sub port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet 1/2 virtual-channel
(config)# erps 1 sub port0 interface GigabitEthernet 1/1 interconnect 1 virtual-channel
```

- ***Port 0 APS MEP(Enter MEP Instance Number)***
- ***Port 1 APS MEP(Enter MEP Instance Number)***
- ***Port 0 SF MEP(Enter MEP Instance Number)***
- ***Port 1 SF MEP(Enter MEP Instance Number)***

```
(config)# erps <group> mep port0 sf <p0_sf> aps <p0_aps> port1 sf <p1_sf> aps <p1_aps>
(config)# erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
(config)# erps 1 mep port0 sf 1 aps 1
```

✓ Instance Configuration

➢ *Guard Time*

- ***10~2000(msec)***

```
(config)# erps <group> guard <guard_time_ms>
(config)# erps 1 guard 500
```

➢ *WTR Time*

- ***1min | 2min | 3min | 4min | 5min | 6min | 7min | 8min | 9min | 10min | 11min | 12min***

➢ *Revertive*

- ***Enable | Disable***

```
(config)# erps <group> revertive <wtr_time_minutes>
(config)# erps 1 revertive 12
(config)# no erps 1 revertive
```

➢ *Hold Off Time*

- ***0~10000(msec)***

```
(config)# erps <group> holdoff <holdoff_time_ms>
(config)# erps 1 holdoff 10000
(config)# erps 1 holdoff 0
```

➢ ***Version***

- ***v1 | v2***

```
(config)# erps <group> version { 1 | 2 }
(config)# erps 1 version 1
(config)# erps 1 version 2
```

✓ **RPL Configuration**

➢ ***RPL Role***

- ***None | RPL_Owner | RPL_Neighbour***

➢ ***RPL Port***

- ***None | Port0 | Port1***

```
(config)# erps <group> rpl { owner | neighbor } { port0 | port1 }
(config)# erps 1 rpl owner port0
(config)# erps 1 rpl neighbor port0
```

➢ ***Clear***

```
(config)# no erps <group> rpl
```

✓ **Instance Command**

➢ ***Command***

- ***None | Manual Switch | Forced Switch | ClearPort***

- ***None | Port0 | Port1***

```
# erps <group> command { force | manual | clear } { port0 | port1 }
# erps 1 command manual port0
# erps 1 command force port1
# erps 1 command clear port1
```

✓ **Instance State**

- ***Protection State | Port 0 | Port 1 | Transmit APS | Port 0 Receive APS | Port 1 Receive APS | WTR Remaining | RPL Un-blocked | No APS Received | Port 0 Block Status | Port 1 Block Status | FOP Alarm***

```
# show erps 1 detail
Grp#  Port 0      Port 1      RPL:Role   Port    Blocking
  1   Gi 1/1      Gi 1/2      Owner      Port 0  Blocked

   Protected VLANS:      None

   Protection Group State          :Active
   Port 0 SF MEP                   :1
   Port 1 SF MEP                   :2
   Port 0 APS MEP                  :1
   Port 1 APS MEP                  :2
   WTR Timeout                     :1
   WTB Timeout                     :5500
```

```
Hold-Off Timeout                :0
Guard Timeout                   :500
Node Type                       :Major
Reversion                       :Revertive
Version                         :2
ERPSv2 Administrative Command   :None


FSM State                       :IDLE
Port 0 Link Status              :Link Down
Port 1 Link Status              :Link Down
Port 0 Block Status             :BLOCKED
Port 1 Block Status             :UNBLOCKED
R-APS Transmission              :NR RB DNF BPR 0
R-APS Port 0 Reception          :NONE
R-APS Port 1 Reception          :NONE
FOP Alarm                       :OFF
```

✓ ERPS VLAN Configuration n

➢ *Add New Entry*

- ***VLAN ID(1~4095)***

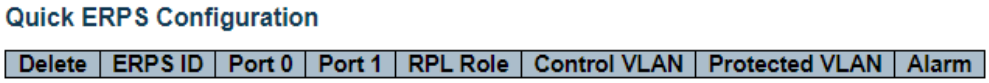
```
(config)# erps <group> vlan { none | [ add | remove ] <vlans> }
(config)# erps 1 vlan 1
(config)# erps 1 vlan add 1
(config)# erps 1 vlan remove 1
```

6.15. Q-ERPS

6.15.1. Q-ERPS Configuration

웹메뉴 Configuration>Q-ERPS

해당 페이지는 단일 Major ERPS를 쉽고 빠르게 설정할 수 있도록 만든 페이지입니다. 해당 페이지에서 설정한 값은 MEP와 ERPS에 자동으로 대입되어 설정이 됩니다. 기본 설정(ERPS 프로토콜의 Major 단일링의 구동)이 가능하도록 설계되었으며, 세부적인 설정은 MEP와 ERPS 설정에서 변경이 가능합니다.



Quick ERPS Configuration

용어	설명
Delete	이 상자는 다음 적용 작업에서 ERPS 와 MEP 를 삭제 대상으로 표시하는 데 사용됩니다.
ERPS ID	생성된 보호 그룹의 ID 는 1 에서 64 사이의 정수 값이어야 합니다. 생성할 수 있는 ERPS 보호 그룹의 최대 수는 64 개입니다. 보호 그룹의 ID 를 클릭하여 구성 페이지로 이동하세요.
Port 0	이 작업은 링 내에서 스위치의 포트 0 을 생성합니다. (MEP 가 동시 생성됩니다)
Port 1	이 작업은 링 내에서 스위치의 포트 1 을 생성합니다. (MEP 가 동시 생성됩니다)
RPL Role	Owner Node 를 설정하세요. Owner Node 의 RPL 은 0 번 포트로 설정됩니다.
Control VLAN	ERPS 의 Control VLAN 을 설정하세요.
Protected VLAN	ERPS 로 보호할 Protected-VLAN (Data VLAN)을 설정하세요.
Alarm	ERPS 의 현재 상태를 보여줍니다.

Buttons

Add New Protection Group: 새로운 보호항목그룹을 추가합니다.

Refresh: 클릭 시 페이지를 즉시 새로고침 합니다.

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>Q-ERPS

✓ **Quick ERPS Configuration**

➢ ***Add New Protection Group***

- ***ERPS ID(1~64)***
- ***Port 0***

- ***Port 1***
- ***RPL Role***
- ***Control Vlan***
- ***Protected Vlan***

Delete	ERPS ID	Port 0	Port 1	RPL Role	Control VLAN	Protected VLAN	Alarm
Delete	1	1	2	RPL_Owner	100	1-10,12,15	

None
RPL_Owner

Delete	ERPS ID	Port 0	Port 1	RPL Role	Control VLAN	Protected VLAN	Alarm
☐	1	1	2	RPL_Owner	100	VLAN Config	

Click ERPS ID(ERPS 설정 페이지를 참조하세요.)

Click VLAN Config(ERPS 설정 페이지를 참조하세요.)

EXAMPLE CLI CONFIGURATION

✓ Quick ERPS Configuration

➢ *Add New Protection Group*

- ***ERPS ID(1~64)***
- ***Port 0(Enter Port Number)***
- ***Port 1(Enter Port Number)***
- ***RPL Role(None | RPL_Owner)***
- ***Control VLAN(1~4095)***
- ***Protected VLAN(1~4095)***

```
(config)# quick-erps <group> port0 <port_type> <port0> port1 <port_type> <port1> role { owner | ordinary } control <control_vlan> protected <protected_vlans>
(config)# quick-erps 1 port0 GigabitEthernet 1/1 port1 GigabitEthernet 1/2 role owner control 100 protected 1-10,12,15
```

6.16. S-Ring

6.16.1. S-Ring Configuration

웹메뉴 Configuration>S-Ring

S-Ring은 Ring Protocol의 일환으로 Master 노드의 2nd Port에서 송신한 패킷이 1st Port로 수신되는지 여부로 Ring을 관리하는 프로토콜입니다.
설정된 시간동안 패킷이 수신되는 경우 1st Port를 Blocking 상태로 유지합니다.

이 페이지는 Sring 그룹을 구성하는 데 사용됩니다. S-Ring을 지원하는 장비가 3대 이상일 때 사용 가능합니다.

Sring Configuration & Status

Sring Configuration									
ID	Mode	Status	Alarm	1st Port	2nd Port	Robustness	Master ID	Order	Reordering
1	Disable	-		10	9	2	-	-	Refresh
2	Disable	-		8	7	2	-	-	Refresh

Sring Configuration & Status

용어	설명
Ring Number	링 번호입니다. 각 장비에서 최대 2 개 Ring 까지 동시 설정이 가능합니다.
Mode	S-Ring 사용 여부, S-Ring 모드 표시: Disabled: S-Ring 비사용. Slave: S-Ring 의 Slave 모드 설정. Master: S-Ring 의 Master 모드 설정.
Status	S-Ring 의 상태를 표시합니다. (-): S-Ring 이 설정되지 않은 상태입니다. Failover: 링이 끊어진 상태를 나타냅니다. Ring: 정상적인 링 상태를 나타냅니다.
Alarm	S-Ring 의 상태를 색으로 표시합니다. : Disable 상태 : 링 형태가 아닐 경우(Failover 상태) : 링 형태일 경우(Ring 상태)
1st Port	S-Ring 을 구성하기 위해 포트를 설정하세요. (S-Ring #1 포트)
2nd Port	S-Ring 을 구성하기 위해 포트를 설정하세요. (S-Ring #2 포트)
Robustness	설정 값 1 당 시간(10ms)을 나타내며, 설정 시간동안 해당 패킷이 수신되지 못하면 Ring 상태가 Failover 됩니다. 주로 연결이 불안할 때 값을 변경합니다. * 해당 값이 높으면 Ring 에서 Failover 로 변경될 때 노드가 끊기는 시간이 증가합니다.
Master ID	이 값은 링의 마스터 ID 번호를 나타냅니다. 마스터의 이 값은 링 ID 와 동일합니다.
Order	이 값은 노드가 마스터로부터 얼마나 떨어져 있는지를 나타냅니다. 마스터는 이 값으로 시작하므로 항상 '1'이며, 마스터의 2 번 포트에서 시작합니다.
ReOrdering	Ordering 패킷을 전송합니다. Ordering 패킷 전송은 '마스터'만 가능합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.
Refresh: 페이지를 새로고침 하려면 클릭하세요.

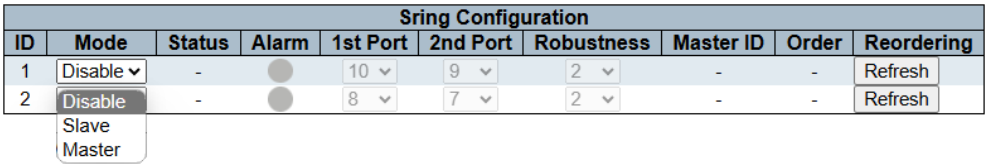
WEB 설정 예시

웹메뉴 Configuration>S-Ring

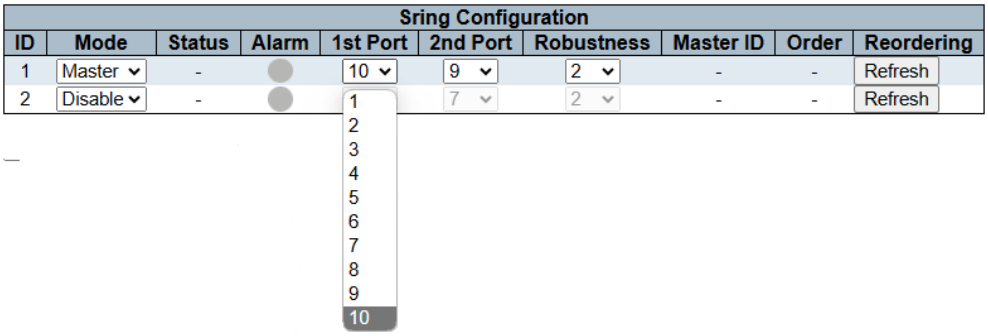
✓ Sring Configuration & Status

➢ ***Mode***

- ***Disable | Slave | Master***

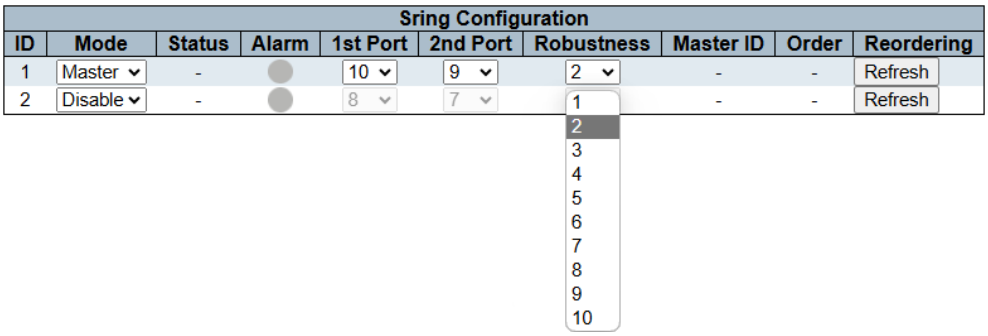


➢ ***1st Port | 2nd Port***



➢ ***Robustness***

- ***1~10***



➢ ***Reordering***

- ***Refresh***

Sring Configuration									
ID	Mode	Status	Alarm	1st Port	2nd Port	Robustness	Master ID	Order	Reordering
1	Master	Failover		10	9	2	1	1	Refresh
2	Disable	-		8	7	2	-	-	Refresh

CLI 설정 예시

✓ Sring Configuration & Status

- ➢ ***Mode***
  - ***Disable | Slave | Master***
- ➢ ***1st Port | 2nd Port***
- ➢ ***Robustness***
  - ***1~10***

```
(config)# sring id <v_id> [ mode { disable | { master | slave } 1st-port <v_ingressPort>
2nd-port <v_egressPort> } ] [ robustness <v_robustnessValue> ]
(config)# sring id 1 mode disable
(config)# sring id 1 mode master 1st-port 12 2nd-port 11 robustness 2
(config)# sring id 2 mode slave 1st-port 10 2nd-port 9 robustness 2
(config)# sring id 2 robustness 2
(config)# no sring
(config)# no sring id 1
```

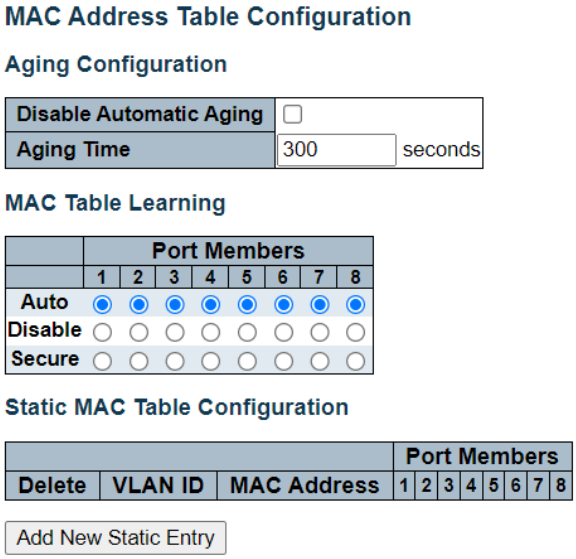
6.17. MAC Table

6.17.1. MAC Table Configuration

웹메뉴 Configuration>MAC Table

이 페이지에서 MAC 주소 테이블을 구성합니다.

Dynamic MAC 테이블 항목의 타임아웃을 설정하고 Static MAC 테이블을 여기에서 구성하세요.



Aging Configuration

기본적으로, 동적 항목은 MAC 테이블에서 300초 후에 제거됩니다. 이 제거는 에이징(aging)이라고도 합니다.

에이징 시간을 설정하려면 여기에 초 단위로 값을 입력하세요. 예를 들어, Age time [ ]초입니다.

허용되는 범위는 10에서 1000000초입니다.

□ 자동 에이징 비활성화를 선택하여 동적 항목의 자동 에이징을 비활성화하세요.

MAC Table Learning

만약 특정 포트의 학습 모드가 회색으로 표시되어 있다면, 다른 모듈이 해당 모드를 제어하므로 사용자가 변경할 수 없습니다. 각 포트는 다음 설정에 따라 학습을 수행할 수 있습니다.

용어	설명
Auto	알 수 없는 SMAC(출발지 MAC 주소)를 포함한 프레임이 수신되는 즉시 학습이 자동으로 수행됩니다.
Disable	학습은 수행되지 않습니다.
Secure	정적 MAC 항목만 학습되며, 다른 모든 프레임은 삭제됩니다. 참고: 안전한 학습 모드로 변경하기 전에 스위치를 관리하는 데 사용되는 링크를 정적 MAC 테이블에 추가해야 합니다. 그렇지 않으면 관리 링크가 손실되고 다른 비안전한 포트를 사용하거나 시리얼 인터페이스를 통해 스위치에 연결하여 복원해야 합니다.

Static MAC Table Configuration

정적 MAC 테이블의 항목은 이 테이블에서 표시됩니다. 정적 MAC 테이블은 최대 64개의 항목을 포함할 수 있습니다.

MAC 테이블은 먼저 VLAN ID로 정렬되고, 그 다음에 MAC 주소로 정렬됩니다.

용어	설명
Delete	삭제하려면 항목을 확인하세요. 다음 저장 시 삭제됩니다.
VLAN ID	해당 항목의 VLAN ID 입니다.
MAC Address	해당 항목의 MAC 주소입니다.
Port Members	체크 표시는 해당 항목의 포트 멤버를 나타냅니다. 필요에 따라 체크 또는 체크 해제하여 항목을 수정하세요.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

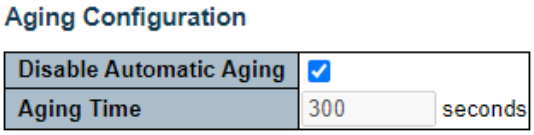
Add New Static Entry: 정적 MAC 테이블에 새 항목을 추가 할 수 있습니다. 새 항목에 대한 VLAN의 ID, MAC 주소 및 포트 멤버를 지정합니다. 그 후, "저장"을 클릭합니다.

WEB 설정 예시

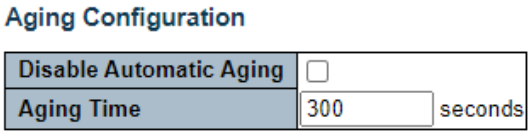
웹메뉴 Configuration>MAC Table

✓ **Aging Configuration**

➢ ***Disable Automatic Aging***

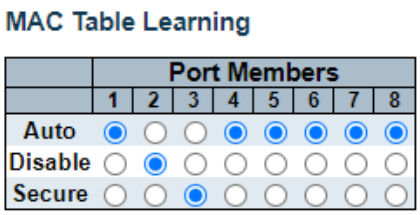


➢ ***Aging Time(Enable Automatic Aging | Aging Time 300)***



✓ **Mac Table Learning**

➢ ***Auto | Disable | Secure***



✓ Static MAC Table Configuration

➢ ***Add New Static Entry***

Static MAC Table Configuration

			Port Members							
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8
Delete	1	00-21-6d-00-00-01	☐	☐	☑	☐	☐	☐	☐	☐

Static MAC Table Configuration

			Port Members							
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8
☐	1	00-21-6D-00-00-01	☐	☐	☑	☐	☐	☐	☐	☐

CLI 설정 예시

✓ Aging Configuration

➢ ***Disable Automatic Aging***

```
(config)# mac address-table aging-time <v_0_10_to_1000000>
(config)# mac address-table aging-time 0
```

➢ ***Aging Time(Enable Automatic Aging | Aging Time 300)***

```
(config)# mac address-table aging-time <v_0_10_to_1000000>
(config)# mac address-table aging-time 300
```

✓ Mac Table Learning

➢ ***Auto***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1
(config-if)# mac address-table learning
```

➢ ***Disable***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/2
(config-if)# no mac address-table learning
```

➢ ***Secure***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/3
(config-if)# mac address-table learning secure
```

✓ Static MAC Table Configuration

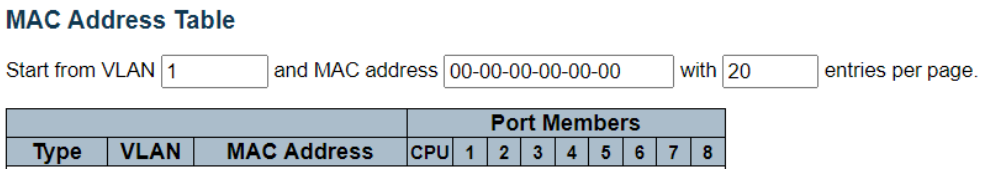
➢ ***Add New Static Entry***

```
(config)# mac address-table static <v_mac_addr> vlan <v_vlan_id> [ interface
( <port_type> [ <v_port_type_list> ] ) ]
(config)# mac address-table static 00-21-6d-00-00-01 vlan 1 interface GigabitEthernet 1/3
```

6.17.2. MAC Table Monitor

웹메뉴 Monitor>MAC Table

MAC 테이블의 항목은 이 페이지에서 표시됩니다. MAC 테이블은 최대 8192개의 항목을 포함할 수 있으며, VLAN ID로 먼저 정렬되고 그 다음에 MAC 주소로 정렬됩니다.



MAC Table Columns

용어	설명
Type	해당 항목이 Static 인지 Dynamic 인지를 나타냅니다.
MAC address	해당 항목의 MAC 주소입니다.
VLAN	해당 항목의 VLAN ID 입니다.
Port Members	해당 항목의 포트 멤버입니다.

Buttons

Auto-refresh : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh: 클릭 시 페이지를 새로 고침.

Clear: 모든 동적 항목을 클리어 합니다.

<<: 현재 표시되는 마지막 항목에 종료. 시스템 로그 항목을 업데이트 합니다.

>>: 현재 표시되는 마지막 항목에서 시작하여, 시스템 로그 항목을 업데이트 합니다.

WEB 확인 예시

웹메뉴 Monitor>MAC Table

✓ MAC Address Table

MAC Address Table

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

			Port Members								
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8
Static	1	00-21-6D-00-00-01				✓					
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-AE-DA-82	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic	1	C0-18-50-7E-50-56		✓							
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓

CLI 확인 예시

✓ MAC Address Table

```
# show mac address-table

Type      VID   MAC Address        Ports
Static    1     00:21:6d:00:00:01  GigabitEthernet 1/3
Static    1     33:33:00:00:00:01  GigabitEthernet 1/1-4 10GigabitEthernet 1/1-4 CPU
Static    1     33:33:00:00:00:02  GigabitEthernet 1/1-4 10GigabitEthernet 1/1-4 CPU
Static    1     33:33:ff:ae:da:82  GigabitEthernet 1/1-4 10GigabitEthernet 1/1-4 CPU
Dynamic   1     c0:18:50:7e:50:56  GigabitEthernet 1/1
Static    1     ff:ff:ff:ff:ff:ff  GigabitEthernet 1/1-4 10GigabitEthernet 1/1-4 CPU
```

6.18. VLANs

6.18.1. VLAN Configuration

웹메뉴 Configuration>VLANs

이 페이지는 스위치에서 VLAN 구성을 제어하는 데 사용됩니다.

이 페이지는 전역 섹션과 포트별 구성 섹션으로 나뉩니다.

Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Global VLAN Configuration

용어	설명
Allowed Access VLANs	이 필드는 허용된 Access VLAN 을 나타냅니다. 즉, Access 포트로 구성된 포트에만 영향을 미칩니다. 다른 모드의 포트는 "허용된 VLAN" 필드에 지정된 VLAN 의 멤버입니다. 기본적으로 VLAN 1 만 활성화되어 있습니다. 쉼표로 구분된 목록 구문을 사용하여 더 많은 VLAN 을 생성할 수 있습니다. 범위는 하한과 상한을 대시(-)로 구분하여 지정됩니다. 다음 예시는 VLAN 1, 10, 11, 12, 13, 200, 300 을 생성합니다: 1,10-13,200,300. 구분자 사이에 공백을 사용할 수 있습니다.
Ethertype for Custom S-ports	이 필드는 사용자 정의 S-포트에 사용되는 이더타입/TPID(16 진수로 지정)을 지정합니다. 이 설정은 포트 유형이 S-Custom-Port 로 설정된 모든 포트에 적용됩니다.

Port VLAN Configuration

용어	설명
Port	이는 행의 논리적인 포트 번호입니다.
Mode	포트 모드(기본값은 Access)는 해당 포트의 기본 동작을 결정합니다. 한 포트는 다음과 같은 세 가지 모드 중 하나에 있을 수 있습니다. 특정 모드가 선택될 때, 해당 행의 나머지 필드는 해당 모드에 따라 회색으로 표시되거나 변경 가능하게 됩니다. 회색으로 표시된 필드는 해당 모드가 적용될 때 포트가 받게 될 값을 나타냅니다. **Access** — Access 포트는 일반적으로 엔드 스테이션에 연결하는 데 사용됩니다. 음성 VLAN과 같은 동적 기능은 포트를 뒷단에서 더 많은 VLAN에 추가할 수 있습니다. Access 포트는 다음과 같은 특징을 가지고 있습니다: 1. 정확히 하나의 VLAN, 포트 VLAN(또는 Access VLAN)의 구성원입니다. 기본값은 1입니다. 2. 태그되지 않은 프레임과 C-태그된 프레임을 수락합니다.

		3. Access VLAN에 분류되지 않은 모든 프레임은 삭제됩니다. 4. 퇴출시에 모든 프레임은 태그되지 않은 상태로 전송됩니다.
	Trunk	트렁크 포트는 여러 VLAN의 트래픽을 동시에 전송할 수 있으며, 일반적으로 다른 스위치에 연결하는 데 사용됩니다. 트렁크 포트는 다음과 같은 특성을 가지고 있습니다: 1. 기본적으로 트렁크 포트는 모든 VLAN(1-4095)의 구성원입니다. 2. 트렁크 포트의 구성원이 될 수 있는 VLAN은 허용된 VLAN의 사용에 의해 제한될 수 있습니다. 3. 포트의 구성원이 아닌 VLAN에 분류된 프레임은 삭제됩니다. 4. 기본적으로 Port VLAN(또는 Native VLAN)에 분류되지 않은 모든 프레임은 퇴출 시에 태그가 추가됩니다. Port VLAN에 분류된 프레임은 퇴출 시에 C-태그가 추가되지 않습니다. 5. 퇴출 태깅은 모든 프레임에 태그를 추가하도록 변경될 수 있으며, 이 경우에는 인그레스에서 태그가 있는 프레임만 수락됩니다.
	Hybrid	하이브리드 포트는 트렁크 포트와 많은 면에서 유사하지만 추가적인 포트 구성 기능을 가지고 있습니다. 트렁크 포트에 대한 설명에 추가하여 하이브리드 포트는 다음과 같은 기능을 가지고 있습니다: 1. VLAN 태그 비인식, C-태그 인식, S-태그 인식 또는 S-사용자-태그 인식으로 구성할 수 있습니다. 2. 인그레스 필터링을 제어할 수 있습니다. 3. 프레임의 인그레스 수용 및 퇴출 태깅 구성을 독립적으로 구성할 수 있습니다.
Port VLAN		포트의 VLAN ID(PVID)를 결정합니다. 허용된 VLAN 은 1 부터 4095 까지의 범위에 있으며, 기본값은 1 입니다. 인그레스 시, 포트가 VLAN 비인식으로 구성되었거나 프레임이 태그되지 않은 경우 또는 포트에 VLAN 인식이 활성화되어 있지만 프레임이 우선순위 태그(VLAN ID = 0)인 경우 프레임은 포트 VLAN 로 분류됩니다. 이그레스 시, 포트 VLAN 에 분류된 프레임은 이그레스 태깅 구성이 포트 VLAN 에 태그를 하지 않도록 설정되어 있다면 태그가 추가되지 않습니다. 포트 VLAN 은 Access 모드의 포트에 대해 "Access VLAN"이라고도 하며, Trunk 또는 Hybrid 모드의 포트에 대해 "Native VLAN"이라고도 합니다.
Port Type		하이브리드 모드의 포트는 포트 유형을 변경할 수 있습니다. 즉, 프레임의 VLAN 태그를 사용하여 프레임을 인그레스 시 특정 VLAN 에 분류할지 여부 및 그렇다면 어떤 TPID 로 반응할지를 결정합니다. 마찬가지로 이그레스(Egress) 시에도 포트 유형은 필요한 경우 태그의 TPID 를 결정합니다. Unaware: 인그레스 시에는 VLAN 태그의 여부에 관계없이 모든 프레임이 포트 VLAN 로 분류되며, 태그가 있는 경우에도 태그가 제거되지 않습니다. C-Port: 인그레스 시에는 TPID = 0x8100 인 VLAN 태그가 있는 프레임이 태그에 포함된 VLAN ID 로 분류됩니다. 프레임이 태그되지 않았거나 우선순위 태그인 경우 프레임은 포트 VLAN 로 분류됩니다. 이그레스(Egress) 시에 프레임에 태그가 필요한 경우, C-태그가 사용됩니다. S-Port: 이그레스(Egress) 시에 프레임에 태그가 필요한 경우, S-태그가 사용됩니다. 인그레스 시에는 TPID = 0x88A8 인 VLAN 태그가 있는 프레임이 태그에 포함된 VLAN ID 로 분류됩니다. 우선순위 태그된 프레임은 포트 VLAN 로 분류됩니다.

	포트가 "Tagged Only" 프레임을 수용하도록 구성되어 있고, 이 TPID 를 갖지 않은 프레임은 삭제됩니다. S-Custom-Port: 이그레스(Egress) 시에 프레임에 태그가 필요한 경우, 사용자 정의 S-태그가 사용됩니다. 인그레스 시에는 사용자 정의 S-포트에 구성된 이더타입과 동일한 TPID 를 갖는 VLAN 태그가 있는 프레임이 태그에 포함된 VLAN ID 로 분류됩니다. 우선순위 태그된 프레임은 포트 VLAN 로 분류됩니다. 포트가 "Tagged Only" 프레임을 수용하도록 구성되어 있고, 이 TPID 를 갖지 않은 프레임은 삭제됩니다.
Ingress Filtering	하이브리드 포트는 인그레스 필터링을 변경할 수 있습니다. Access 및 Trunk 포트는 항상 인그레스 필터링이 활성화되어 있습니다. 인그레스 필터링이 활성화된 경우(체크박스가 선택된 경우), 포트의 구성원이 아닌 VLAN 에 분류된 프레임은 삭제됩니다. 인그레스 필터링이 비활성화된 경우, 포트의 구성원이 아닌 VLAN 에 분류된 프레임은 수락되어 스위치 엔진으로 전달됩니다. 그러나 포트는 해당 VLAN 의 프레임을 전송하지 않습니다.
Ingress Acceptance	하이브리드 포트는 인그레스에서 수용되는 프레임 유형을 변경할 수 있습니다. **Tagged and Untagged**: 태그가 있는 프레임과 언태그된 프레임 모두 수용됩니다. 프레임이 태그되었는지 여부에 대한 설명은 포트 유형을 참조하십시오. **Tagged Only**: 인그레스 시 해당 포트 유형 태그가 있는 프레임만 수락됩니다. **Untagged Only**: 인그레스 시에는 언태그된 프레임만 수락됩니다. 프레임이 언태그된 것으로 간주되는 경우에 대한 설명은 포트 유형을 참조하십시오.
Egress Tagging	트렁크 및 하이브리드 모드의 포트는 퇴출 시 프레임의 태깅을 제어할 수 있습니다. **Untag Port VLAN**: 포트 VLAN에 분류된 프레임은 태그 없이 전송됩니다. 다른 프레임은 관련된 태그와 함께 전송됩니다. **Tag All**: 포트 VLAN에 분류되었는지 여부에 상관없이 모든 프레임은 태그와 함께 전송됩니다. **Untag All**: 포트 VLAN에 분류되었는지 여부에 상관없이 모든 프레임은 태그 없이 전송됩니다. 이 옵션은 하이브리드 모드의 포트에만 사용할 수 있습니다.
Allowed VLANs	트렁크 및 하이브리드 모드의 포트는 자신이 구성원이 될 수 있는 VLAN 을 제어할 수 있습니다. Access 포트는 Access VLAN 하나의 구성원만 될 수 있습니다. 이 필드의 구문은 "Enabled VLANs" 필드에서 사용하는 구문과 동일합니다. 기본적으로 트렁크 또는 하이브리드 포트는 모든 VLAN 의 구성원이 되므로 1-4095 로 설정됩니다. 이 필드를 비워 둘 수도 있으며, 이 경우 포트는 어떤 VLAN 의 구성원도 되지 않습니다.
Forbidden VLANs	포트는 하나 이상의 VLAN 의 구성원이 되지 않도록 구성할 수 있습니다. 이는 MVRP 와 GVRP 와 같은 동적 VLAN 프로토콜이 포트를 동적으로 VLAN 에 추가하는 것을 방지해야 할 때 특히 유용합니다. 해당 포트에서 이러한 VLAN 을 금지된 VLAN 으로 표시하는 것이 핵심입니다. 구문은 "Enabled VLANs" 필드에서 사용하는 구문과 동일합니다. 기본적으로 이 필드는 비워져 있으며, 이는 포트가 모든 가능한 VLAN 의 구성원이 될 수 있다는 것을 의미합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

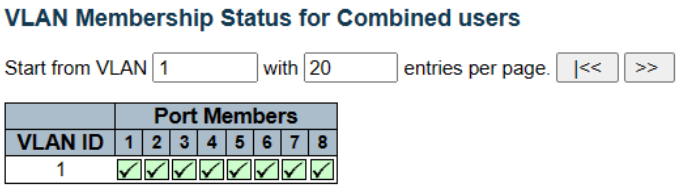
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

6.18.2. VLAN Monitor

6.18.2.1. Membership

웹메뉴 Monitor>VLANs>Membership

이 페이지는 VLAN 사용자의 멤버십 상태를 개요로 제공합니다.



VLAN Membership Status for Combined users

용어	설명
VLAN User	다양한 내부 소프트웨어 모듈은 VLAN 서비스를 사용하여 VLAN 멤버십을 동적으로 구성할 수 있습니다. 오른쪽의 드롭다운 목록을 사용하여 관리자가 구성한 VLAN 멤버십(Admin) 또는 이러한 내부 소프트웨어 모듈 중 하나가 구성한 멤버십을 선택할 수 있습니다. "Combined" 항목은 관리자와 내부 소프트웨어 모듈의 구성을 결합하여 하드웨어에 실제로 구성된 내용을 반영합니다.
VLAN ID	포트 구성원이 표시되는 VLAN ID 입니다.
Port Members	각 VLAN ID 에 대해 포트의 체크 박스 행이 표시됩니다. 포트가 VLAN 에 포함된 경우 다음 이미지가 표시됩니다: ✓. 포트가 금지된 포트 목록에 있는 경우 다음 이미지가 표시됩니다: ✗. 포트가 금지된 포트 목록에 있으면서 동시에 VLAN 에 포함되려고 하는 경우 다음 이미지가 표시됩니다: ✗. 이 경우 포트는 VLAN 의 구성원이 되지 않습니다.

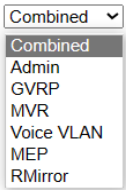
Buttons

Auto-refresh ☐ : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh : 클릭 시 페이지를 새로 고침.

|<< : 현재 표시되는 마지막 항목에 종료. 시스템 로그 항목을 업데이트 합니다.

>> : 현재 표시되는 마지막 항목에서 시작하여, 시스템 로그 항목을 업데이트 합니다.



: 이 Drop 다운 목록에서 VLAN 사용자를 선택합니다.

6.18.2.2. Ports

웹메뉴 Monitor>VLANs>Ports

이 페이지는 VLAN 포트 상태를 제공합니다.

VLAN Port Status for Combined users

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag All		No
2	C-Port	☑	All	1	Untag All		No
3	C-Port	☑	All	1	Untag All		No
4	C-Port	☑	All	1	Untag All		No
5	C-Port	☑	All	1	Untag All		No
6	C-Port	☑	All	1	Untag All		No
7	C-Port	☑	All	1	Untag All		No
8	C-Port	☑	All	1	Untag All		No

VLAN Port Status for Combined users

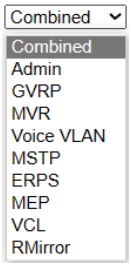
용어	설명
VLAN User	다양한 내부 소프트웨어 모듈은 VLAN 서비스를 사용하여 VLAN 포트 구성을 실시간으로 구성할 수 있습니다. 오른쪽의 드롭다운 목록을 사용하여 관리자가 구성한 VLAN 멤버십 (Admin) 또는 이러한 내부 소프트웨어 모듈 중 하나가 구성한 멤버십을 선택할 수 있습니다. "Combined" 항목은 관리자와 내부 소프트웨어 모듈의 구성을 결합하여 실제 하드웨어에 구성된 내용을 기본적으로 반영합니다. 특정 소프트웨어 모듈이 포트 설정 중 하나도 재정의하지 않은 경우, 테이블에 "선택한 사용자에 대한 데이터가 없음"이라는 텍스트가 표시됩니다.
Port	같은 행에 포함된 설정의 논리적인 포트입니다.
Port Type	지정된 사용자가 포트에서 구성하려는 포트 유형(Unaware, C-Port, S-Port, S-Custom-Port)을 나타냅니다. 선택한 사용자에 의해 재정의되지 않은 경우 해당 필드는 비어 있습니다.
Ingress Filtering	지정된 사용자가 인그레스 필터링을 활성화하는지 여부를 나타냅니다. 선택한 사용자에 의해 재정의되지 않은 경우 해당 필드는 비어 있습니다.
Frame Type	지정된 사용자가 포트에서 구성하려는 허용 프레임 유형(All, Tagged, Untagged)을 나타냅니다. 선택한 사용자에 의해 재정의되지 않은 경우 해당 필드는 비어 있습니다.
Port VLAN ID	지정된 사용자가 포트에 설정하려는 포트 VLAN ID (PVID)를 나타냅니다. 선택한 사용자에 의해 재정의되지 않은 경우 해당 필드는 비어 있습니다.
Tx Tag	지정된 사용자가 포트에서 가지는 전송 태그 요구 사항 (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID)을 나타냅니다. 선택한 사용자에 의해 재정의되지 않은 경우 해당 필드는 비어 있습니다.
Untagged VLAN ID	선택한 사용자에 의해 Tx 태그가 재정의되어 Tag 또는 Untag UVID 로 설정되고 있다면, 이 필드에는 사용자가 이그레스 시 태그 또는 언태그하려는 VLAN ID 가 표시됩니다. 선택한 사용자에 의해 재정의되지 않은 경우 해당 필드는 비어 있습니다.
Conflicts	두 사용자가 포트의 구성에 대해 충돌하는 요구 사항을 가질 수 있습니다. 예를 들어, 한 사용자는 이그레스 시 모든 프레임에 태그를 요구하는 반면 다른 사용자는 이그레스 시 모든 프레임에 언태그를 요구할 수 있습니다.

	두 사용자 모두 이길 수는 없으므로, 이는 우선순위가 있는 방식으로 충돌을 해결합니다. 관리자의 우선순위가 가장 낮습니다. 다른 소프트웨어 모듈은 드롭다운 목록에서의 위치에 따라 우선순위가 결정됩니다. 목록에서 높을수록 높은 우선순위를 가집니다. 충돌이 있는 경우, "Combined" 사용자와 충돌이 발생한 소프트웨어 모듈에 대해 "Yes"로 표시됩니다. "Combined" 사용자는 실제로 하드웨어에 구성된 내용을 반영합니다.

Buttons

Auto-refresh : 체크박스 체크 시 주기적으로 페이지 자동 새로 고침을 사용합니다.

Refresh: 클릭 시 페이지를 새로 고침.



: 이 Drop 다운 목록에서 선택 VLAN 사용자.

6.19. QoS

6.19.1. QoS Configuration

6.19.1.1. Port Classification

웹메뉴 Configuration>QoS>Port Classification

이 페이지에서는 모든 스위치 포트에 대한 기본 QoS 인그레스 분류 설정을 구성할 수 있습니다.

QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	WRED Group
*	<>	<>	<>	<>			<>
1	0	0	0	0	Disabled		1
2	0	0	0	0	Disabled		1
3	0	0	0	0	Disabled		1
4	0	0	0	0	Disabled		1
5	0	0	0	0	Disabled		1
6	0	0	0	0	Disabled		1
7	0	0	0	0	Disabled		1
8	0	0	0	0	Disabled		1

QoS Ingress Port Classification

용어	설명
Port	아래 설정이 적용되는 포트 번호입니다.
CoS	기본 서비스 클래스를 제어합니다. 모든 프레임은 서비스 클래스(CoS)에 분류됩니다. CoS, 큐 및 우선순위 간에는 일대일 매핑이 있습니다. CoS 0 (제로)은 가장 낮은 우선순위를 가집니다. 포트가 VLAN 을 인식하고 프레임이 태그 되며 Tag Class.이 활성화된 경우, 프레임은 태그의 PCP 및 DEI 값을 기반으로 한 CoS 로 분류됩니다. 그렇지 않은 경우 프레임은 기본 CoS 로 분류됩니다. 분류된 CoS 는 QCL 항목에 의해 무시될 수 있습니다. 참고: 기본 CoS 가 동적으로 변경된 경우, 구성된 기본 CoS 의 괄호 안에 실제 기본 CoS 가 표시됩니다.
DPL	기본 드롭 우선순위(DPL) 레벨을 제어합니다. 모든 프레임은 드롭 우선순위 레벨에 따라 분류됩니다. 포트가 VLAN 을 인식하고 프레임이 태그 되며 Tag Class.이 활성화된 경우, 프레임은 태그의 PCP 및 DEI 값을 기반으로 한 DPL 로 분류됩니다. 그렇지 않은 경우 프레임은 기본 DPL 로 분류됩니다. 분류된 DPL 은 QCL 항목에 의해 무시될 수 있습니다.
PCP	기본 PCP(PCP 우선순위) 값을 제어합니다. 모든 프레임은 PCP 값을 기준으로 분류됩니다. 포트가 VLAN 을 인식하고 프레임이 태그 된 경우, 프레임은 태그의 PCP 값으로 분류됩니다. 그렇지 않은 경우 프레임은 기본 PCP 값으로 분류됩니다.
DEI	기본 DEI(DEI 비트) 값을 제어합니다. 모든 프레임은 DEI 값을 기준으로 분류됩니다. 포트가 VLAN 을 인식하고 프레임이 태그 된 경우, 프레임은 태그의 DEI 값으로 분류됩니다. 그렇지 않은 경우 프레임은 기본 DEI 값으로 분류됩니다.

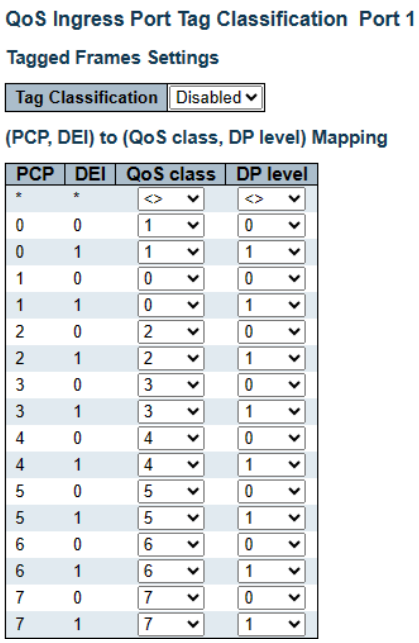
Tag Class	이 포트의 태그 된 프레임에 대한 분류 모드를 표시합니다. 비활성화: 태그 된 프레임에는 기본 CoS 와 DPL 을 사용합니다. 활성화: 태그 된 프레임에는 PCP 와 DEI 의 매핑 된 버전을 사용합니다. 모드를 구성하거나/또는 매핑을 설정하려면 해당 모드를 클릭하세요. 참고: 이 설정은 포트가 VLAN 을 인식하지 않는 경우에는 영향을 미치지 않습니다. VLAN 을 인식하지 않는 포트에 수신된 태그 된 프레임은 항상 기본 CoS 와 DPL 로 분류됩니다.
DSCP Based	DSCP 기반 QoS 인그레스 포트 분류를 활성화하려면 클릭하세요.
WRED Group	WRED 그룹 멤버십을 제어합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

QoS Ingress Port Tag Classification Port n

'Tag Class.'를 클릭하면 설정 페이지가 열립니다.
태그된 프레임에 대한 분류 모드가 이 페이지에서 구성됩니다.



Tagged Frames Settings

용어	설명
Tag Classification	이 포트에서 태그된 프레임의 분류 모드를 제어합니다. **Disabled** 태그된 프레임에 대한 기본 QoS 클래스 및 드롭 우선 순위를 사용합니다. **Enabled** 태그된 프레임에 대한 PCP와 DEI의 매핑 버전을 사용합니다.

(PCP, DEI) to (QoS class, DP level) Mapping

용어	설명
Tag Classification	태그 분류가 활성화된 경우 (PCP, DEI)에서 (QoS 클래스, DP 레벨) 값의 매핑을 제어합니다.

WEB 설정 예시

웹메뉴 Configuration>QoS>Port Classification

✓ QoS Ingress Port Classification

➢ *CoS*

- 0~7 (0 – The Lowest Priority)

QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	WRED Group
*	<>	<>	<>	<>		☑	<>
1	0	0	0	0	Disabled	☑	1
2	0	0	0	0	Disabled	☑	1
3	0	0	0	0	Disabled	☑	1
4	0	0	0	0	Disabled	☑	1
5	0	0	0	0	Disabled	☑	1
6	0	0	0	0	Disabled	☑	1
7	0	0	0	0	Disabled	☑	1
8	0	0	0	0	Disabled	☑	1
9	0	0	0	0	Disabled	☑	1
10	0	0	0	0	Disabled	☑	1
11	0	0	0	0	Disabled	☑	1
12	0	0	0	0	Disabled	☑	1

CoS 드롭다운: 0, 1, 2, 3, 4, 5, 6, 7

➢ *DPL*

- 0~3 (0 – Low drop probability)

QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	WRED Group
*	<>	<>	<>	<>		☑	<>
1	0	0	0	0	Disabled	☑	1
2	0	0	0	0	Disabled	☑	1
3	0	0	0	0	Disabled	☑	1
4	0	0	0	0	Disabled	☑	1
5	0	0	0	0	Disabled	☑	1
6	0	0	0	0	Disabled	☑	1
7	0	0	0	0	Disabled	☑	1
8	0	0	0	0	Disabled	☑	1
9	0	0	0	0	Disabled	☑	1
10	0	0	0	0	Disabled	☑	1
11	0	0	0	0	Disabled	☑	1
12	0	0	0	0	Disabled	☑	1

DPL 드롭다운: 0, 1, 2, 3

➢ ***PCP***

- 0~7 (0 - The Lowest Priority)

QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	WRED Group
*	<>	<>	<>	<>		☑	<>
1	0	0	0	0	Disabled	☑	1
2	0	0	0	0	Disabled	☑	1
3	0	0	1	0	Disabled	☑	1
4	0	0	2	0	Disabled	☑	1
5	0	0	3	0	Disabled	☑	1
6	0	0	4	0	Disabled	☑	1
7	0	0	5	0	Disabled	☑	1
8	0	0	6	0	Disabled	☑	1
9	0	0	7	0	Disabled	☑	1
10	0	0	0	0	Disabled	☑	1
11	0	0	0	0	Disabled	☑	1
12	0	0	0	0	Disabled	☑	1

➢ ***DEI***

- 0~1 (0 – Low drop probability)

QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	WRED Group
*	<>	<>	<>	<>		☑	<>
1	0	0	0	0	Disabled	☑	1
2	0	0	0	0	Disabled	☑	1
3	0	0	0	1	Disabled	☑	1
4	0	0	0	0	Disabled	☑	1
5	0	0	0	0	Disabled	☑	1
6	0	0	0	0	Disabled	☑	1
7	0	0	0	0	Disabled	☑	1
8	0	0	0	0	Disabled	☑	1
9	0	0	0	0	Disabled	☑	1
10	0	0	0	0	Disabled	☑	1
11	0	0	0	0	Disabled	☑	1
12	0	0	0	0	Disabled	☑	1

➢ ***Tag Class***

- Disabled

QoS Ingress Port Tag Classification Port n

Tagged Frames Settings

➢ ***Tag Classification***

- Disabled | Enabled

Tagged Frames Settings

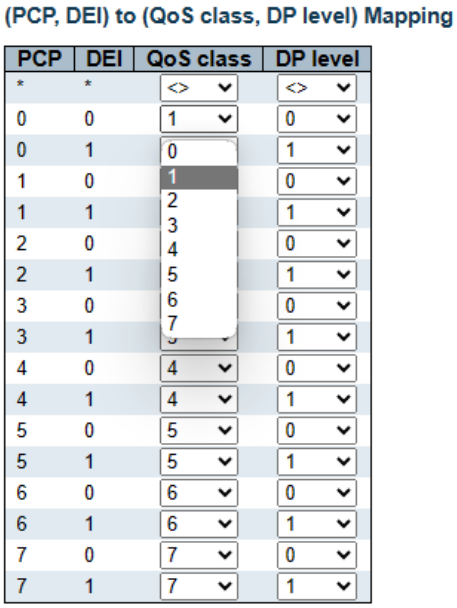
Tag Classification	Disabled

(PCP, DEI) to (QoS Disabled / Enabled)

(PCP, DEI) to (QoS class, DP level) Mapping

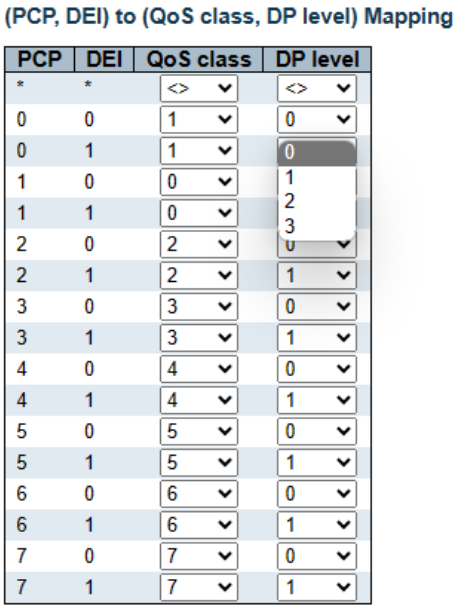
➢ ***QoS class***

- 0~7 (0 - The Lowest Priority)



➢ ***DP level***

- 0~3 (0 – Low drop probability)



➢ ***DSCP Based***

- Enabled | Disabled

QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	WRED Group
*	<>	<>	<>	<>		☐	<>
1	0	0	0	0	Disabled	☐	1
2	0	0	0	0	Disabled	☑	1
3	0	0	0	0	Disabled	☑	1
4	0	0	0	0	Disabled	☑	1
5	0	0	0	0	Disabled	☑	1
6	0	0	0	0	Disabled	☑	1
7	0	0	0	0	Disabled	☑	1
8	0	0	0	0	Disabled	☑	1
9	0	0	0	0	Disabled	☑	1
10	0	0	0	0	Disabled	☑	1
11	0	0	0	0	Disabled	☑	1
12	0	0	0	0	Disabled	☑	1

➢ ***WRED Group***

- 1~3 (WRED group)

QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	WRED Group
*	<>	<>	<>	<>		☑	<>
1	0	0	0	0	Disabled	☑	1
2	0	0	0	0	Disabled	☑	1
3	0	0	0	0	Disabled	☑	2
4	0	0	0	0	Disabled	☑	3
5	0	0	0	0	Disabled	☑	1
6	0	0	0	0	Disabled	☑	1
7	0	0	0	0	Disabled	☑	1
8	0	0	0	0	Disabled	☑	1
9	0	0	0	0	Disabled	☑	1
10	0	0	0	0	Disabled	☑	1
11	0	0	0	0	Disabled	☑	1
12	0	0	0	0	Disabled	☑	1

CLI 설정 예시

✓ QoS Ingress Port Classification

➢ ***CoS***

- 0~7 (0 – The Lowest Priority)

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos cos <cos>
(config-if)# qos cos 0
```

➢ ***DPL***

- 0~3 (0 – Low drop probability)

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos dpl <dpl>
(config-if)# qos dpl 0
```

➢ ***PCP***

- 0~7 (0 – The Lowest Priority)

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos pcp <pcp>
(config-if)# qos pcp 0
```

➢ ***DEI***

- 0~1 (0 – Low drop probability)

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos dei <dei>
(config-if)# qos dei 0
```

➢ ***Tag Class***

- Disabled

QoS Ingress Port Tag Classification Port n

Tagged Frames Settings

➢ ***Tag Classification***

- Disabled | Enabled

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos trust tag
```

(PCP, DEI) to (QoS class, DP level) Mapping

➢ ***QoS class***

- 0~7 (0 - The Lowest Priority)

➢ ***DP level***

- 0~3 (0 – Low drop probability)

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl>
(config-if)# qos map tag-cos pcp 0 dei 0 cos 1 dpl 0
```

➢ ***DSCP Based***

- Enabled | Disabled

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos trust dscp
(config-if)# no qos trust dscp
```

➢ ***WRED Group***

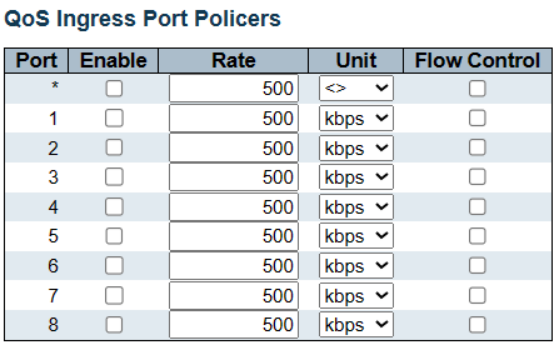
- 1~3 (WRED group)

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos wred-group <wred_group>
(config-if)# qos wred-group 1
```

6.19.1.2. Port Policing

웹메뉴 Configuration>QoS>Port Policing

이 페이지에서는 모든 스위치 포트에 대한 폴리서 설정을 구성할 수 있습니다.



QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	☐	500	<>	☐
1	☐	500	kbps	☐
2	☐	500	kbps	☐
3	☐	500	kbps	☐
4	☐	500	kbps	☐
5	☐	500	kbps	☐
6	☐	500	kbps	☐
7	☐	500	kbps	☐
8	☐	500	kbps	☐

QoS Ingress Port Policers

용어	설명
Port	아래 설정이 적용되는 포트 번호입니다.
Enable	이 스위치 포트에 대한 포트 폴리서를 활성화 또는 비활성화합니다.
Rate	포트 폴리서의 속도를 제어합니다. "단위"가 kbps 또는 fps 일 때 이 값은 10-13128147 로 제한되며, "단위"가 Mbps 또는 kfps 일 때 이 값은 1-13128 로 제한됩니다. 속도는 포트 폴리서에서 지원하는 가장 가까운 값으로 내부적으로 반올림됩니다.
Unit	포트 폴리서 속도의 측정 단위를 kbps, Mbps, fps 또는 kfps 로 제어합니다.
Flow Control	플로우 컨트롤이 활성화되고 포트가 플로우 컨트롤 모드에 있는 경우, 프레임을 폐기하는 대신 일시 중지 프레임이 전송됩니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>QoS>Port Policing

✓ **QoS Ingress Port Policers**

➢ ***Enable***

- Enabled | Disabled

QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	☐	1	<>	☐
1	☑	1	Mbps	☐
2	☐	1	Mbps	☐
3	☐	1	Mbps	☐
4	☐	1	Mbps	☐
5	☐	1	Mbps	☐
6	☐	1	Mbps	☐
7	☐	1	Mbps	☐
8	☐	1	Mbps	☐
9	☐	1	Mbps	☐
10	☐	1	Mbps	☐
11	☐	1	Mbps	☐
12	☐	1	Mbps	☐

➢ ***Rate***

- 10-13128147(kbps, fps) or 1-13128(Mbps, kfps)

QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	☐	1	<>	☐
1	☑	1	Mbps	☐
2	☐	1	Mbps	☐
3	☐	1	Mbps	☐
4	☐	1	Mbps	☐
5	☐	1	Mbps	☐
6	☐	1	Mbps	☐
7	☐	1	Mbps	☐
8	☐	1	Mbps	☐
9	☐	1	Mbps	☐
10	☐	1	Mbps	☐
11	☐	1	Mbps	☐
12	☐	1	Mbps	☐

➢ ***Unit***

- kbps, Mbps, fps, kfps

QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	☑	1	<>	☐
1	☑	1	Mbps	☐
2	☐	1	kbps	☐
3	☐	1	Mbps	☐
4	☐	1	fps	☐
5	☐	1	kfps	☐
6	☐	1	Mbps	☐
7	☐	1	Mbps	☐
8	☐	1	Mbps	☐
9	☐	1	Mbps	☐
10	☐	1	Mbps	☐
11	☐	1	Mbps	☐
12	☐	1	Mbps	☐

➢ ***Flow Control***

- Enabled | Disabled

QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	☑	1	<>	☐
1	☑	1	Mbps	☑
2	☐	1	Mbps	☐
3	☐	1	Mbps	☐
4	☐	1	Mbps	☐
5	☐	1	Mbps	☐
6	☐	1	Mbps	☐
7	☐	1	Mbps	☐
8	☐	1	Mbps	☐
9	☐	1	Mbps	☐
10	☐	1	Mbps	☐
11	☐	1	Mbps	☐
12	☐	1	Mbps	☐

CLI 설정 예시

✓ QoS Ingress Port Policers

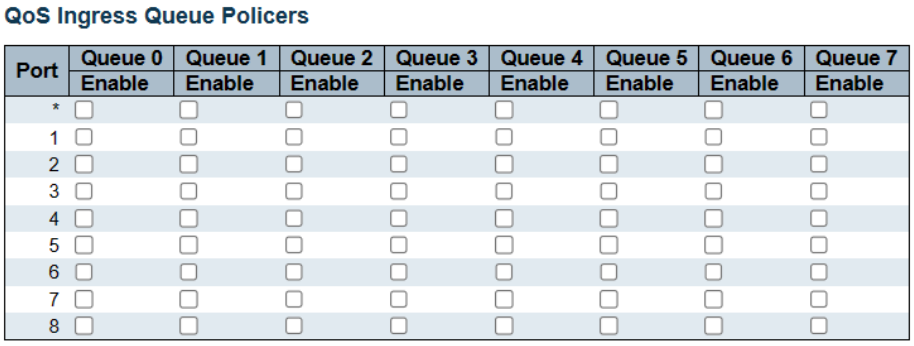
- ***Enable***
  - Enabled | Disabled
- ***Rate***
  - 10-13128147(kbps, fps) or 1-13128(Mbps, kfps)
- ***Unit***
  - kbps, Mbps, fps, kfps
- ***Flow Control***
  - Enabled | Disabled

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos policer <rate> [ kbps | mbps | fps | kfps ] [ flowcontrol ]
(config-if)# qos policer 1 mbps flowcontrol
(config-if)# qos policer 1 mbps
(config-if)# qos policer 10 kbps
(config-if)# no qos policer
```

6.19.1.3. Queue Policing

웹메뉴 Configuration>QoS>Queue Policing

이 페이지에서는 모든 스위치 포트에 대한 큐 폴리서 설정을 구성할 수 있습니다.



QoS Ingress Queue Policers

Port	Queue 0 Enable	Queue 1 Enable	Queue 2 Enable	Queue 3 Enable	Queue 4 Enable	Queue 5 Enable	Queue 6 Enable	Queue 7 Enable
*	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐

QoS Ingress Queue Policers

용어	설명
Port	아래 설정이 적용되는 포트 번호입니다.
Enable (E)	이 스위치 포트에 대한 큐 폴리서를 활성화 또는 비활성화합니다.
Rate	큐 폴리서의 속도를 제어합니다. "단위"가 kbps 인 경우 이 값은 25-13128147 로 제한되고, "단위"가 Mbps 인 경우 이 값은 1-13128 로 제한됩니다. 속도는 큐 폴리서에서 지원하는 가장 가까운 값으로 내부적으로 반올림됩니다. 이 필드는 적어도 하나의 큐 폴리서가 활성화된 경우에만 표시됩니다.
Unit	큐 폴리서 속도의 측정 단위를 kbps 또는 Mbps 로 제어합니다. 이 필드는 적어도 하나의 큐 폴리서가 활성화된 경우에만 표시됩니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>QoS>Queue Policing

✓ **QoS Ingress Queue Policers**

- ***Queue n (n, 0~7)***
- ***Enable (E)***
  - Enabled | Disabled

QoS Ingress Queue Policers

Port	Queue 0			Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	E	Rate	Unit	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	☐	1	<>	☐	☐	☐	☐	☐	☐	☐
1	☑	1	Mbps	☐	☐	☐	☐	☐	☐	☐
2	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
3	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
4	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
5	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
6	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
7	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
8	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
9	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
10	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
11	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
12	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐

➢ ***Rate***

- 25-13128147(kbps) or 1-13128(Mbps)

QoS Ingress Queue Policers

Port	Queue 0			Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	E	Rate	Unit	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	☑	25	<>	☐	☐	☐	☐	☐	☐	☐
1	☑	25	kbps	☐	☐	☐	☐	☐	☐	☐
2	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
3	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
4	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
5	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
6	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
7	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
8	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
9	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
10	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
11	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
12	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐

➢ ***Unit***

- kbps, Mbps

QoS Ingress Queue Policers

Port	Queue 0			Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	E	Rate	Unit	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	☑	1	<>	☐	☐	☐	☐	☐	☐	☐
1	☑	1	Mbps	☐	☐	☐	☐	☐	☐	☐
2	☐	1	kbps	☐	☐	☐	☐	☐	☐	☐
3	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
4	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
5	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
6	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
7	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
8	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
9	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
10	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
11	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐
12	☐	1	Mbps	☐	☐	☐	☐	☐	☐	☐

CLI 설정 예시

✓ QoS Ingress Queue Policers

- ➢ ***Queue n (n, 0~7)***
- ➢ ***Enable (E)***
  - Enabled | Disabled
- ➢ ***Rate***
  - 25-13128147(kbps) or 1-13128(Mbps)
- ➢ ***Unit***
  - kbps, Mbps

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# qos queue-policer queue <queue> <rate> [ kbps | mbps ]
(config-if)# qos queue-policer queue 0 1 mbps
(config-if)# qos queue-policer queue 0 25 kbps
(config-if)# no qos queue-policer queue 0
```

6.19.1.4. Port Scheduler

웹메뉴 Configuration>QoS>Port Scheduler

이 페이지는 모든 스위치 포트에 대한 QoS Egress Port 스케줄러의 개요를 제공합니다.

QoS Egress Port Schedulers

Port	Mode	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	Strict Priority	-	-	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-	-	-

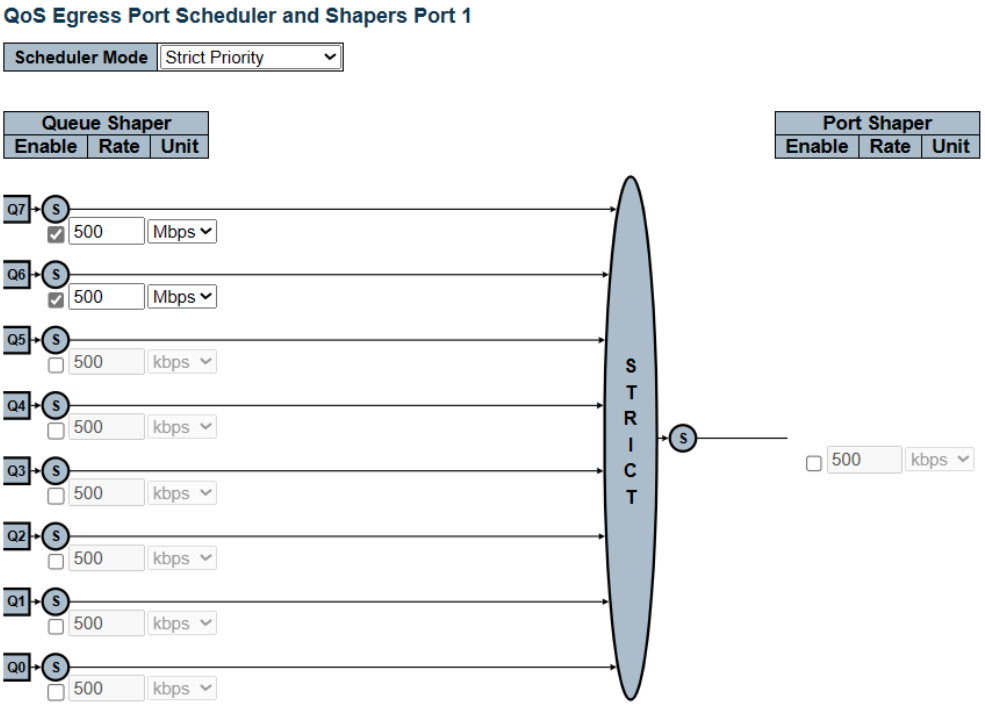
QoS Egress Port Schedulers

용어	설명
Port	동일한 행에 포함된 설정에 대한 논리적인 포트입니다. 스케줄러를 구성하려면 포트 번호를 클릭하세요.
Mode	이 포트의 스케줄링 모드를 보여줍니다.
Qn	이 큐와 포트에 대한 가중치를 보여줍니다.

QoS Egress Port Scheduler and Shapers Port n

Scheduler를 구성하기 위해 포트 번호를 클릭하세요.

이 페이지에서는 특정 포트의 스케줄러와 셰이퍼를 구성할 수 있습니다.



QoS Egress Port Schedulers and Shapers Port n

용어	설명
Scheduler Mode	이 스위치 포트에서 얼마나 많은 큐가 엄격하게 스케줄 되고 얼마나 많은 큐가 가중치로 스케줄 되는지를 제어합니다.
Queue Shaper Enable	이 스위치 포트에서 이 큐에 대해 큐 셰이퍼를 활성화할지 여부를 제어합니다.
Queue Shaper Rate	큐 셰이퍼의 속도를 제어합니다. "Unit"이 kbps 인 경우 이 값은 100-13107100 으로 제한되고, "Unit"이 Mbps 인 경우 1-13107 로 제한됩니다. 속도는 큐 셰이퍼에서 지원하는 가장 가까운 값으로 내부적으로 반올림됩니다.
Queue Shaper Unit	큐 셰이퍼의 속도를 측정하는 단위를 kbps 또는 Mbps 로 제어합니다.
Queue Scheduler Weight	이 큐에 대한 가중치를 제어합니다. 이 값은 1-100 으로 제한됩니다. 이 매개변수는 "스케줄러 모드"가 "가중치"로 설정된 경우에만 표시됩니다.
Queue Scheduler Percent	이 큐에 대한 가중치를 백분율로 표시합니다. 이 매개변수는 "스케줄러 모드"가 "가중치"로 설정된 경우에만 표시됩니다.
Port Shaper Enable	이 스위치 포트에 대해 포트 셰이퍼를 활성화/비활성화합니다.
Port Shaper Rate	포트 셰이퍼의 속도를 제어합니다. 이 값은 "Unit"이 kbps 인 경우 100 에서 13107100 까지, Mbps 인 경우 1 에서 13107 까지 제한됩니다. 속도는 내부적으로 포트 셰이퍼에서 지원하는 가장 가까운 값으로 반올림됩니다.
Port Shaper Unit	포트 셰이퍼 속도의 측정 단위를 kbps 또는 Mbps 로 제어합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

Back: 로컬 변경 사항을 취소하고 이전 페이지로 돌아갑니다.

WEB 설정 예시

웹메뉴 Configuration>QoS>Port Scheduler

✓ **QoS Egress Port Schedulers**

QoS Egress Port Schedulers

Port	Mode	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	Strict Priority	-	-	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-	-	-

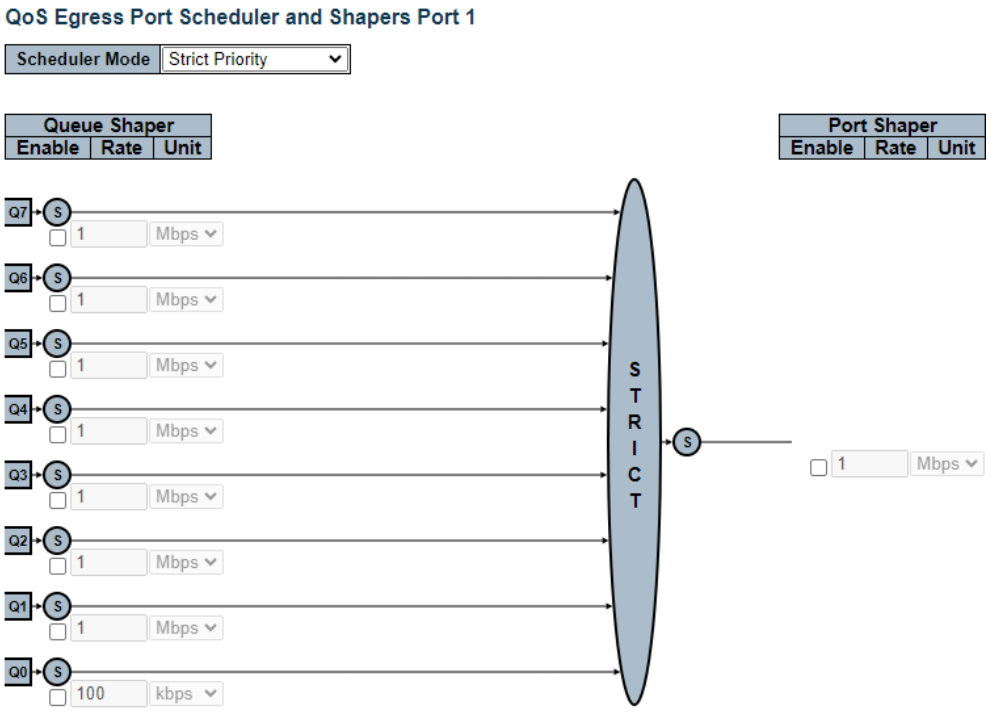
➢ ***Port***

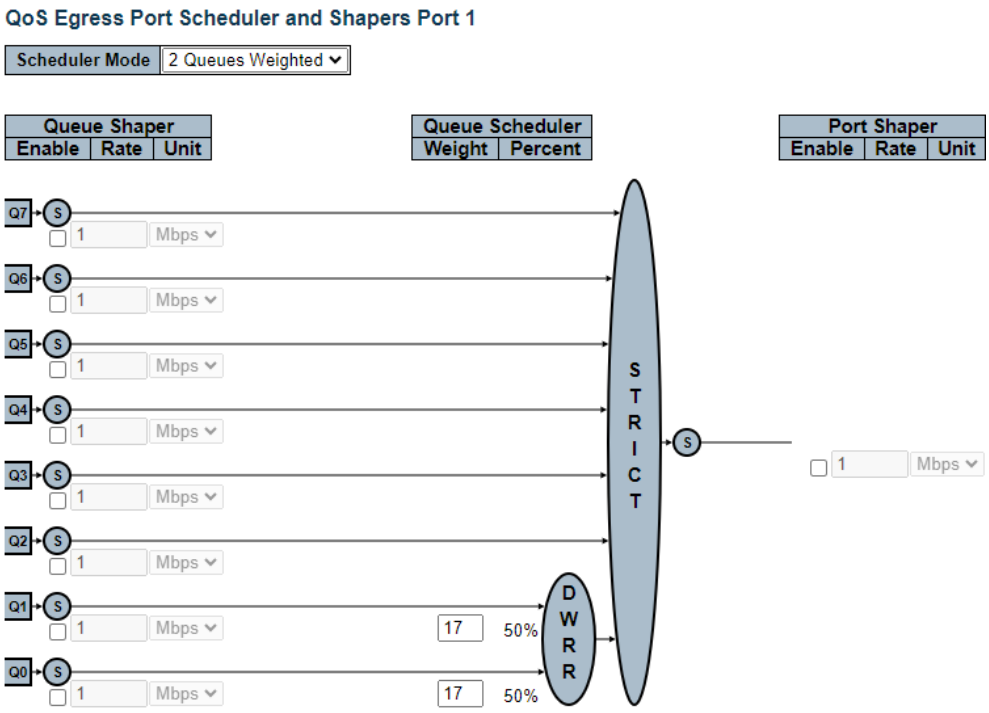
스케줄러를 구성하려면 포트 번호를 클릭하세요.

✓ QoS Egress Port Schedulers and Shapers Port n

➢ *Scheduler Mode*

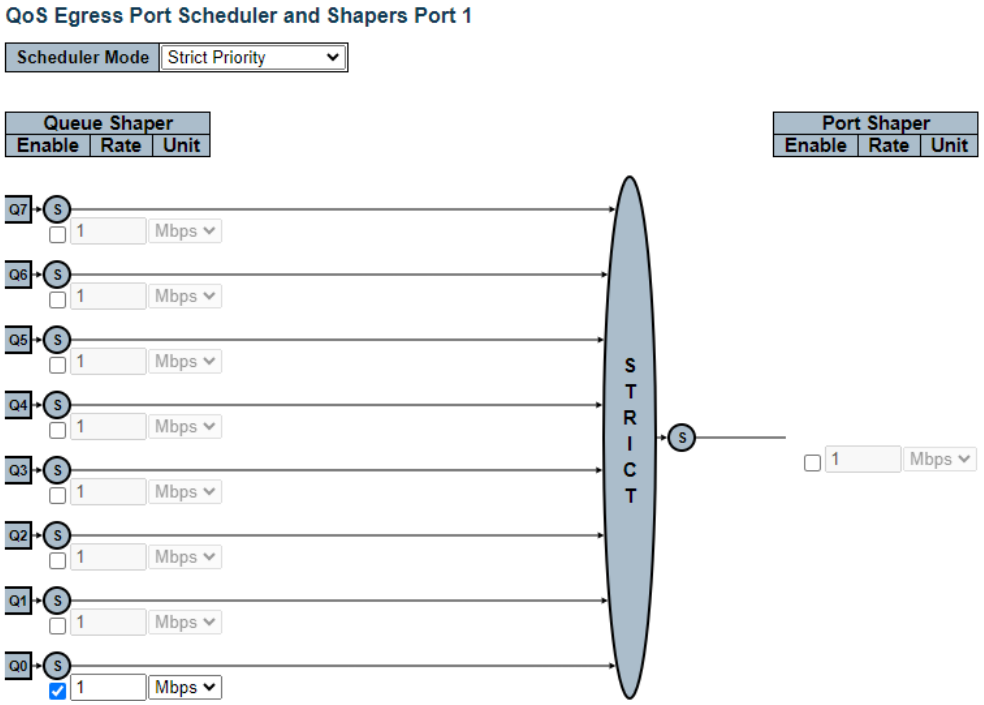
- Strict Priority | Queues Weighted





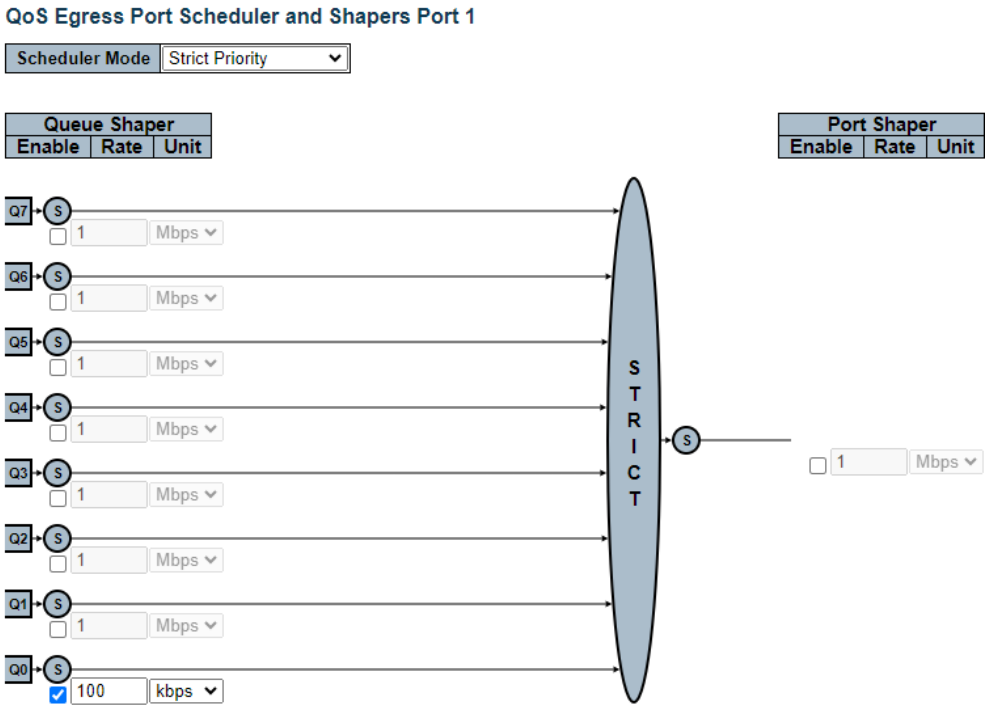
➢ ***Queue Shaper Enable***

- Enabled | Disabled



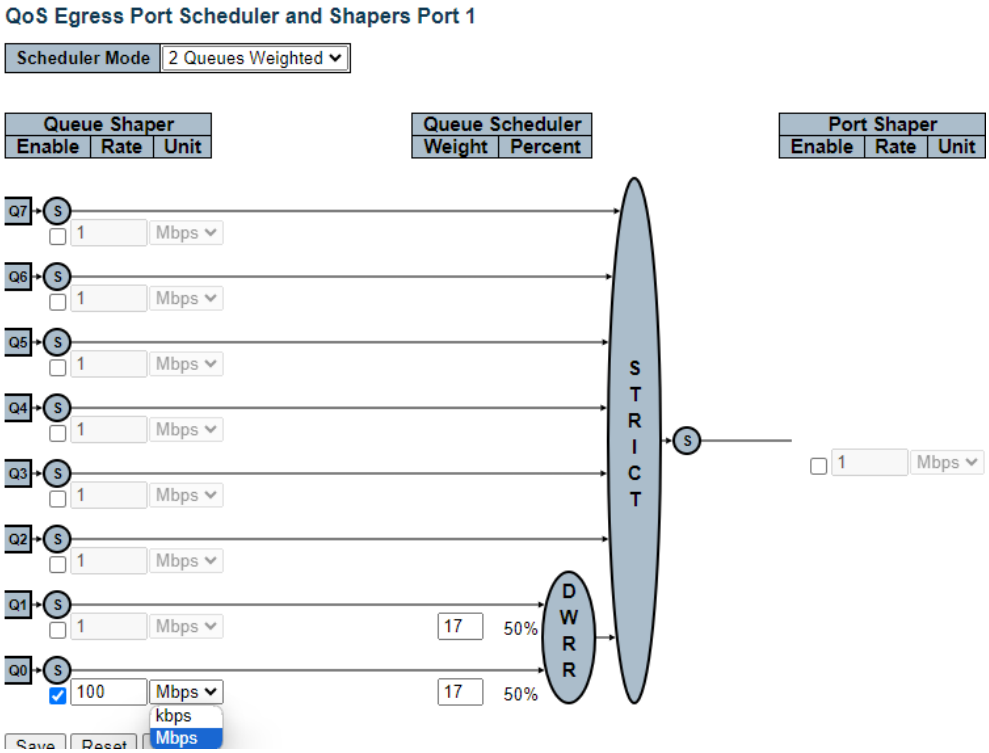
➢ ***Queue Shaper Rate***

- 100-13107100(kbps) or 1-13107(Mbps)



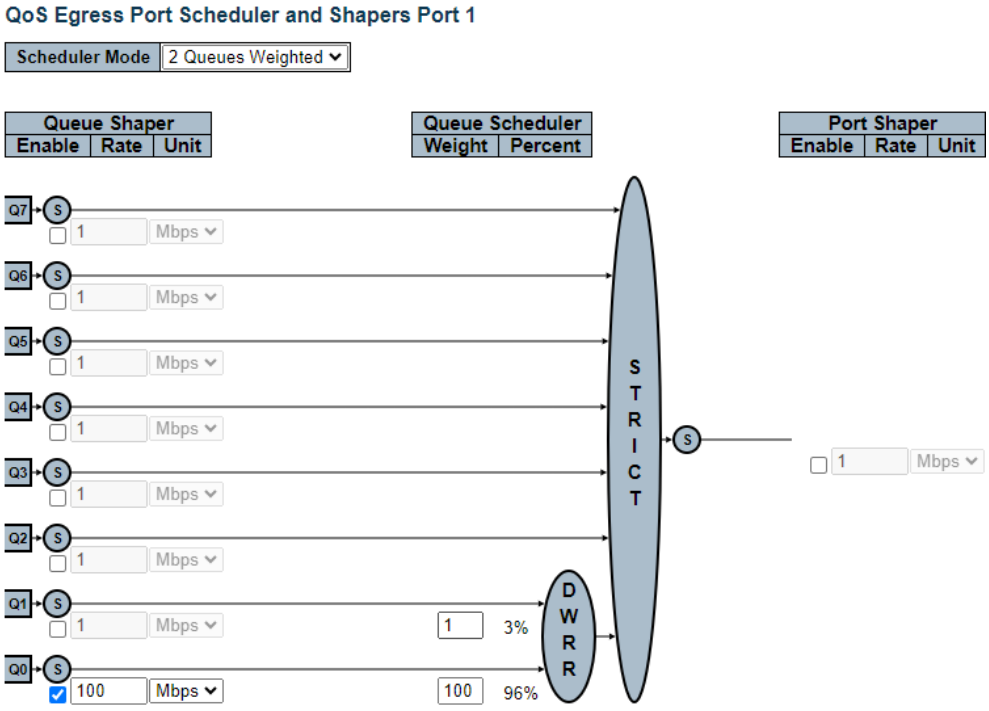
➢ ***Queue Shaper Unit***

- kbps or Mbps



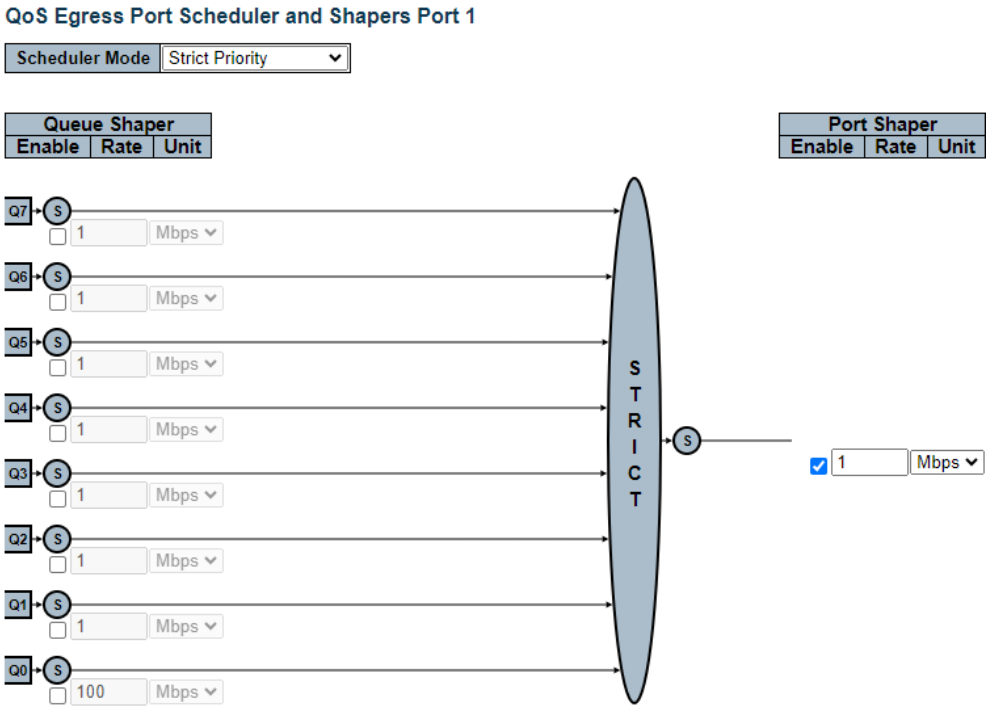
➢ ***Queue Scheduler Weight***

- 1~100(Scheduler Mode should be set to 'Weighted')



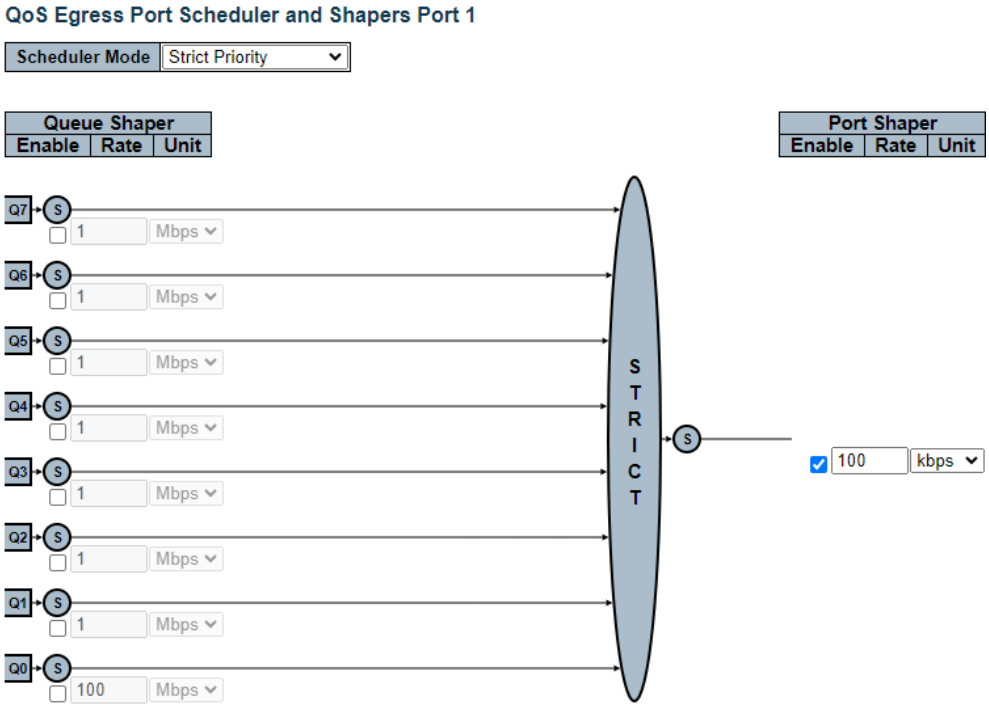
➢ ***Port Shaper Enable***

- Enabled | Disabled



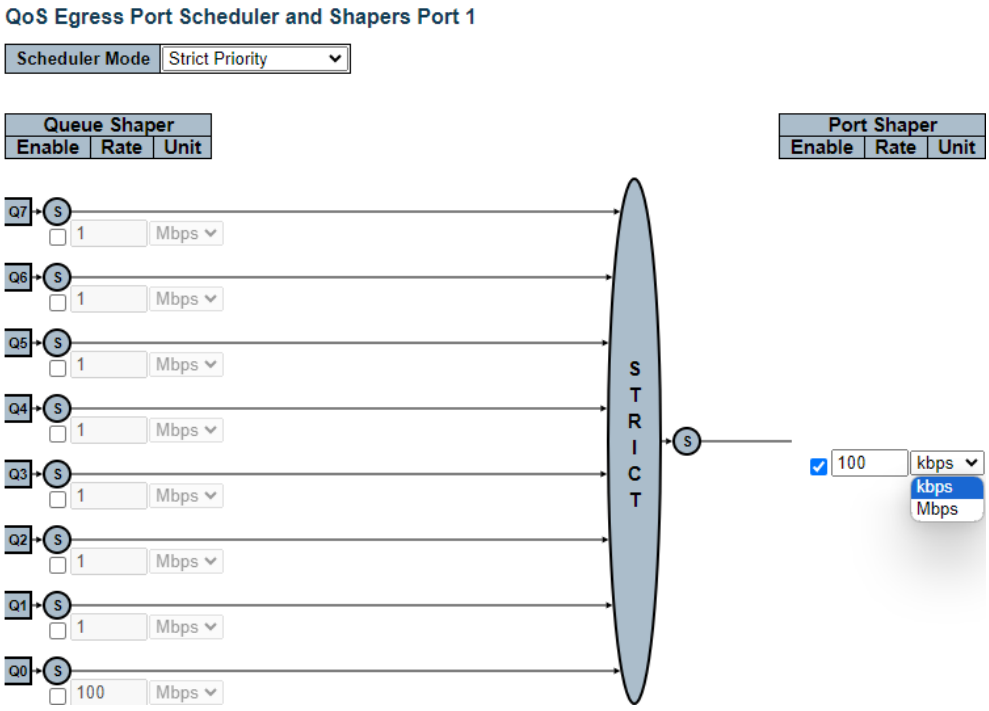
➢ ***Port Shaper Rate***

- 100-13107100(kbps) or 1-13107(Mbps)



➢ ***Port Shaper Unit***

- kbps or Mbps



CLI 설정 예시

✓ QoS Egress Port Schedulers

- ***Port***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1
```

✓ QoS Egress Port Schedulers and Shapers Port n

- ***Scheduler Mode***
  - Strict Priority | Queues Weighted

```
(config-if)# no qos wrr

(config-if)# qos wrr <w0> <w1> [ <w2> [ <w3> [ <w4> [ <w5> [ <w6> [ <w7> ] ] ] ] ] ]
(config-if)# qos wrr 17 17
```

- ***Queue Shaper Enable***
  - Enabled | Disabled
- ***Queue Shaper Rate***
  - 100-13107100(kbps) or 1-13107(Mbps)
- ***Queue Shaper Unit***
  - kbps or Mbps

```
(config-if)# qos queue-shaper queue <queue> <rate> [ kbps | mbps ] [ excess ] [ rate-type { line | data } ]
(config-if)# no qos queue-shaper queue 0
(config-if)# qos queue-shaper queue 0 1 mbps
(config-if)# qos queue-shaper queue 0 100 kbps
```

- ***Queue Scheduler Weight***
  - 1~100(Scheduler Mode should be set to 'Weighted')

```
(config-if)# qos wrr <w0> <w1> [ <w2> [ <w3> [ <w4> [ <w5> [ <w6> [ <w7> ] ] ] ] ] ]
(config-if)# qos wrr 100 1
```

- ***Port Shaper Enable***
  - Enabled | Disabled
- ***Port Shaper Rate***
  - 100-13107100(kbps) or 1-13107(Mbps)
- ***Port Shaper Unit***
  - kbps or Mbps

```
(config-if)# qos shaper <rate> [ kbps | mbps ] [ rate-type { line | data } ]
(config-if)# no qos shaper
(config-if)# qos shaper 1 mbps
(config-if)# qos shaper 100 kbps
```

6.19.1.5. Port Shaping

웹메뉴 Configuration>QoS>Port Shaping

이 페이지는 모든 스위치 포트에 대한 QoS 이그레스 포트 셰이퍼의 개요를 제공합니다.

QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-

QoS Egress Port Shapers

용어	설명
Port	같은 행에 포함된 설정에 대한 논리 포트입니다. 셰이퍼를 구성하려면 포트 번호를 클릭하십시오.
Qn	해당 포트의 큐 셰이퍼 속도를 나타냅니다. 비활성화된 경우 "-"로 표시되거나 실제 큐 셰이퍼 속도가 표시됩니다. 예를 들어 "800 Mbps"와 같이 표시될 수 있습니다.
Port	해당 포트의 포트 셰이퍼 속도를 나타냅니다. 비활성화된 경우 "-"로 표시되거나 실제 포트 셰이퍼 속도가 표시됩니다. 예를 들어 "800 Mbps"와 같이 표시될 수 있습니다.

6.19.1.6. Port Tag Remarking

웹메뉴 Configuration>QoS>Port Tag Remarking

이 페이지는 모든 스위치 포트에 대한 QoS Egress 포트 태그 리마킹 설정 개요를 제공합니다.

QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified

QoS Egress Port Tag Remarking

용어	설명
Port	같은 행에 있는 설정에 대한 논리 포트가 표시됩니다. 태그 리마킹을 구성하려면 포트 번호를 클릭하세요.
Mode	해당 포트의 태그 리마킹 모드가 표시됩니다. Classified: 분류된 PCP/DEI 값을 사용합니다. Default: 기본 PCP/DEI 값을 사용합니다. Mapped: QoS 클래스 및 DP 레벨의 매핑 된 버전을 사용합니다.

QoS Egress Port Tag Remarking Port

특정 포트에 대한 QoS Egress Port Tag Remarking이 이 페이지에서 구성됩니다..

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode	Classified

QoS Egress Port Tag Remarking Port n

용어	설명
Mode	이 포트의 태그 리마킹 모드를 제어합니다. Classified: 분류된 PCP/DEI 값을 사용합니다. Default: 기본 PCP/DEI 값을 사용합니다. Mapped: QoS 클래스와 DP 레벨의 매핑 된 버전을 사용합니다.
PCP/DEI Configuration	모드가 Default 로 설정된 경우에 사용되는 기본 PCP 와 DEI 값을 제어합니다.
(QoS class, DP level) to (PCP, DEI) Mapping	모드가 Mapped 로 설정된 경우, 분류된 (QoS 클래스, DP 레벨) 값과 (PCP, DEI) 값 사이의 매핑을 제어합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.
Cancel: 로컬 변경 사항을 취소하고 돌아갑니다.

WEB 설정 예시

웹메뉴 Configuration>QoS>Port Tag Remarking

✓ QoS Egress Port Tag Remarking

➢ ***Port(***태그 리마킹을 구성하려면 포트 번호를 클릭하세요.***)***

QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified

✓ QoS Egress Port Tag Remarking Port n

➢ ***Tag Remarking Mode***

- Classified

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode	Classified

- Default

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode	Default

PCP/DEI Configuration

Default PCP	0
Default DEI	0

- Mapped

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode	Mapped

(QoS class, DP level) to (PCP, DEI) Mapping

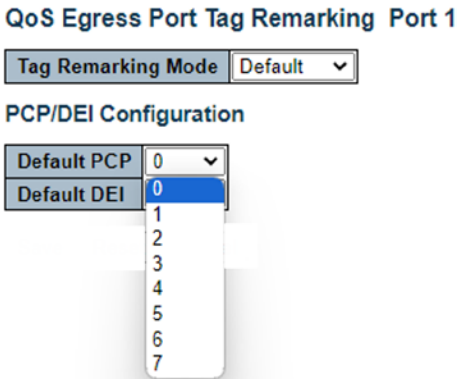
QoS class	DP level	PCP	DEI
*	*	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

✓ PCP/DEI Configuration

아래 항목은 Mode가 Default일 때 표시됩니다.

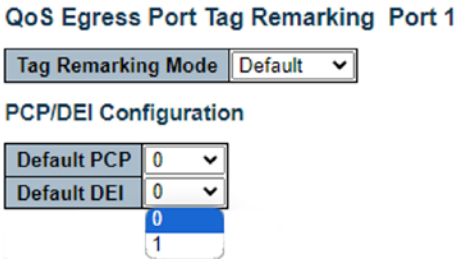
➢ ***Default PCP***

- 0~7



➢ ***Default DEI***

- 0~1

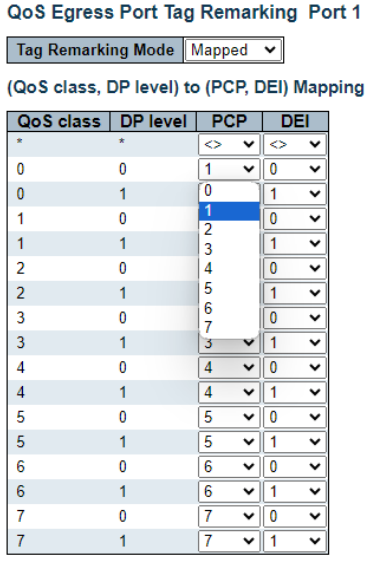


✓ (QoS class, DP level) to (PCP, DEI) Mapping

아래 항목은 Mode가 Mapped일 때 표시됩니다.

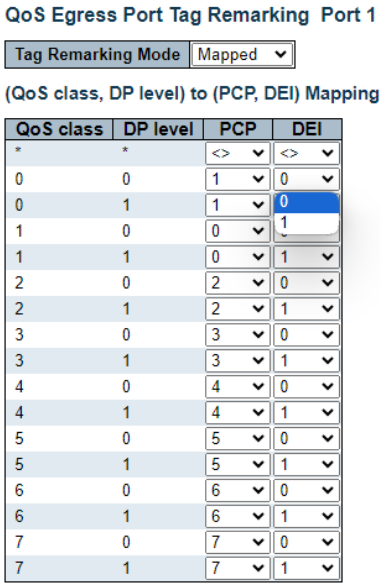
➢ ***PCP***

- 0~7



➢ ***DEI***

- 0~1



CLI 설정 예시

✓ QoS Egress Port Tag Remarking

➢ ***Port***

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1
```

✓ QoS Egress Port Tag Remarking Port n

➢ ***Tag Remarking Mode***

- Classified

```
(config-if)# no qos tag-remark
```

- Default

```
(config-if)# qos tag-remark { pcp <pcp> dei <dei> | mapped }
(config-if)# qos tag-remark pcp <pcp> dei <dei>
```

- Mapped

```
(config-if)# qos tag-remark { pcp <pcp> dei <dei> | mapped }
(config-if)# qos tag-remark mapped
```

✓ PCP/DEI Configuration

➢ ***Default PCP***

- 0~7

➢ ***Default DEI***

- 0~1

```
(config-if)# qos tag-remark pcp <pcp> dei <dei>
(config-if)# qos tag-remark pcp 0 dei 0
```

✓ **(QoS class, DP level) to (PCP, DEI) Mapping**

➢ ***PCP***

- 0~7

➢ ***DEI***

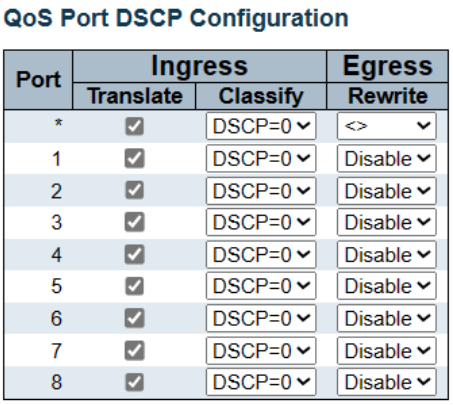
- 0~1

```
(config-if)# qos map cos-tag cos <cos> dpl <dpl> pcp <pcp> dei <dei>
(config-if)# qos map cos-tag cos 0 dpl 0 pcp 1 dei 0
```

6.19.1.7. Port DSCP

웹메뉴 Configuration>QoS>Port DSCP

이 페이지에서는 스위치의 모든 포트에 대한 기본 QoS 포트 DSCP 구성 설정을 구성할 수 있습니다.



QoS Port DSCP Configuration

용어	설명
Port	Port 열에는 DSCP 인그레스 및 이그레스 설정을 구성할 수 있는 포트 목록이 표시됩니다.
Ingress	Ingress 설정에서는 개별 포트에 대한 인그레스 translation and classification 설정을 변경할 수 있습니다.
1. Translate	인그레스 변환을 활성화하려면 체크 박스를 선택하세요.
2. Classify	포트의 분류에는 4 가지 다른 값이 있습니다. 1. 비활성화: 인그레스 DSCP 분류 없음. 2. DSCP=0: 들어오는 (또는 활성화된 경우 변환된) DSCP 가 0 이면 분류합니다. 3. 선택된: 특정 DSCP 에 대해 활성화된 분류가 DSCP 번역 창에 지정된 경우에만 선택된 DSCP 를 분류합니다. 4. 모두: 모든 DSCP 를 분류합니다.
Egress	포트 Egress Rewriting 은 다음 중 하나일 수 있습니다: 1. 비활성화: Egress 재작성 없음. 2. 활성화: 재작성이 활성화되어 있지만 재매핑은 없음. 3. 재매핑: 분석기로부터의 DSCP 가 재매핑되고 프레임은 재매핑 된 DSCP 값으로 다시 표시됩니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>QoS>Port DSCP

✓ **QoS Port DSCP Configuration**

➢ ***Ingress Translate***

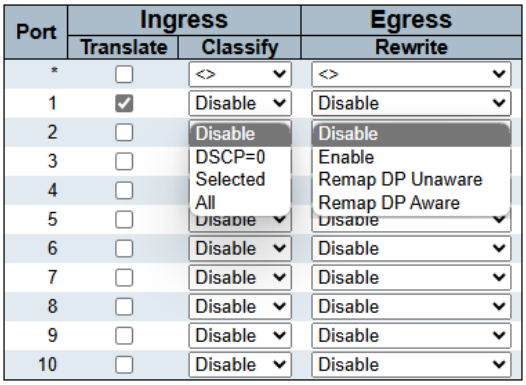
- Enable | Disable

➢ ***Ingress Classify***

- Disable | DSCP=0 | Slected | All

➢ ***Egress Rewrite***

- Disable | Enable | Remap DP Unaware | Remap DP Aware
- Disable | Enable | Remap



CLI 설정 예시

✓ **QoS Port DSCP Configuration**

➢ ***Ingress Translate***

- Enable | Disable

```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1
```

```
(config-if)# qos dscp-translate
(config-if)# no qos dscp-translate
```

➢ ***Ingress Classify***

- Disable | DSCP=0 | Slected | All

```
(config-if)# qos dscp-classify { zero | selected | any }
(config-if)# no qos dscp-classify
(config-if)# qos dscp-classify zero
(config-if)# qos dscp-classify selected
(config-if)# qos dscp-classify any
```

➢ ***Egress Rewrite***

- Disable | Enable | Remap DP Unaware | Remap DP Aware
- Disable | Enable | Remap

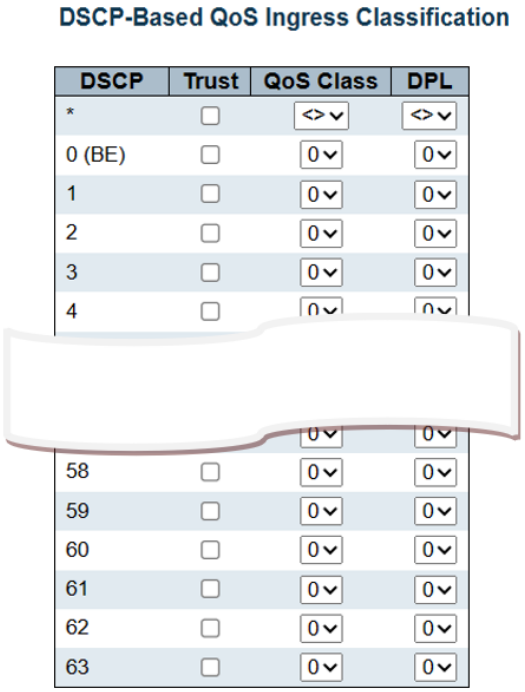
```
(config-if)# qos dscp-remark { rewrite | remap | remap-dp }
(config-if)# no qos dscp-remark
```

(config-if)# qos dscp-remark rewrite *(config-if)# qos dscp-remark remap* *(config-if)# qos dscp-remark remap-dp*
(config-if)# qos dscp-remark { rewrite | remap | remap-dp } *(config-if)# no qos dscp-remark* *(config-if)# qos dscp-remark rewrite* *(config-if)# qos dscp-remark remap*

6.19.1.8. DSCP-Based QoS

웹메뉴 Configuration>QoS>DSCP-Based QoS

이 페이지에서는 모든 스위치에 대한 기본 QoS DSCP 기반 인그레스 분류 설정을 구성할 수 있습니다.



DSCP-Based QoS Ingress Classification

용어	설명
DSCP	지원되는 최대 DSCP 값의 수는 64 입니다.
Trust	특정 DSCP 값을 신뢰할지 여부를 제어합니다. 신뢰할 수 있는 DSCP 값만이 특정한 QoS 클래스와 Drop Precedence Level 로 매핑됩니다. 신뢰할 수 없는 DSCP 값을 가진 프레임은 비-IP 프레임으로 처리됩니다.
QoS Class	QoS 클래스 값은 0 부터 7 까지의 값을 가질 수 있습니다.
DPL	드롭 우선 순위 레벨은 0 부터 3 까지의 값을 가질 수 있습니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>QoS>DSCP-Based QoS

✓ **DSCP-Based QoS Ingress Classification**

➢ ***DSCP***

➢ ***Trust***

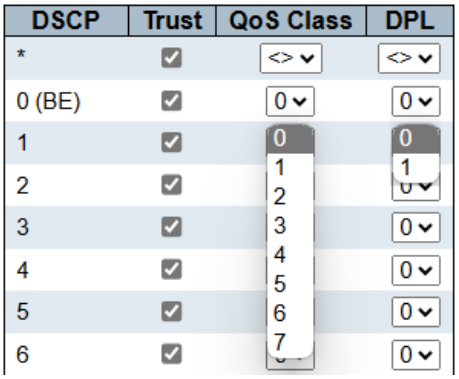
- Trusted | Untrusted

➢ ***QoS Class***

- 0~7

➢ ***DPL***

- 0~1



CLI 설정 예시

✓ DSCP-Based QoS Ingress Classification

➢ ***DSCP***

➢ ***Trust***

- Trusted | Untrusted

➢ ***QoS Class***

- 0~7

➢ ***DPL***

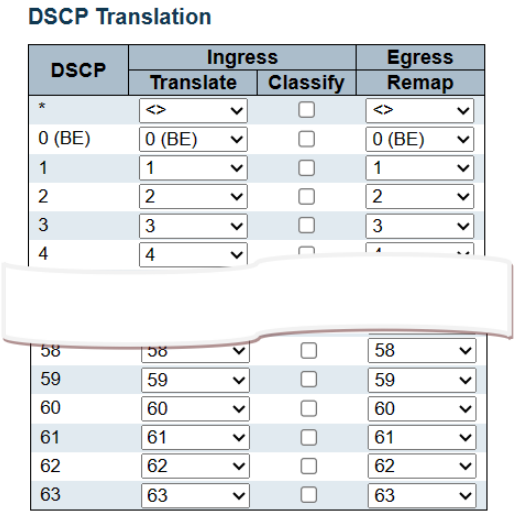
- 0~1

```
(config)# qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 |
af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } cos <cos> dpl <dpl>
(config)# no qos map dscp-cos 0
(config)# qos map dscp-cos 0 cos 0 dpl 0
(config)# qos map dscp-cos 63 cos 7 dpl 1
(config)# qos map dscp-cos cs1 cos 7 dpl 1
```

6.19.1.9. DSCP Translation

웹메뉴 Configuration>QoS>DSCP Translation

이 페이지에서는 모든 스위치에 대한 기본적인 QoS DSCP 변환 설정을 구성할 수 있습니다.
DSCP 변환은 Ingress 또는 Egress에서 수행할 수 있습니다.



DSCP Translation

용어	설명
DSCP	지원되는 DSCP 값의 최대 개수는 64 개이며, 유효한 DSCP 값의 범위는 0 부터 63 까지입니다.
Ingress	입력 측의 DSCP 는 QoS 클래스와 DPL 맵에 사용되기 전에 먼저 새로운 DSCP 로 번역될 수 있습니다. DSCP 번역을 위한 두 가지 구성 매개변수가 있습니다. 1. 번역 (Translate) 2. 분류 (Classify)
1. Translate	입력 측의 DSCP 는 (0-63)의 DSCP 값 중 하나로 번역될 수 있습니다.
2. Classify	클릭하여 입력 측에서의 분류를 활성화하세요.
Egress	Egress 측에는 다음과 같이 구성 가능한 매개변수가 있습니다. Remap(재매핑)
Remap	0 에서 63 까지의 DSCP 값 중에서 재매핑하려는 DSCP 값을 선택하십시오.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>QoS>DSCP Translation

✓ **DSCP Translation**

➢ ***DSCP***

➢ ***Ingress Translate***

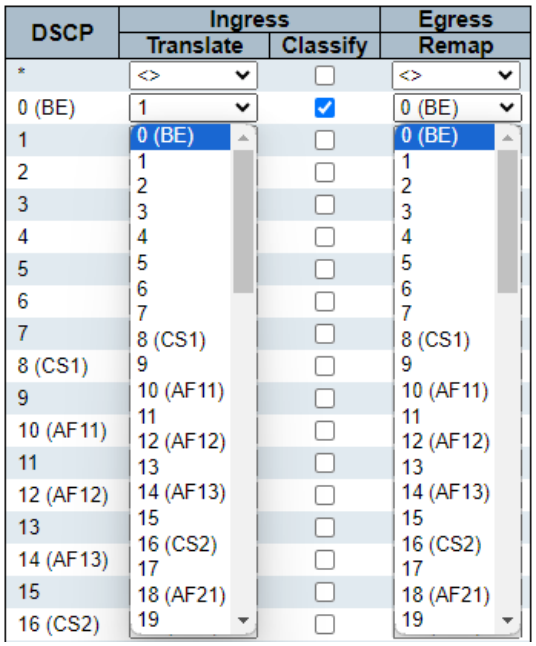
- 0~63

➢ ***Ingress Classify***

- Enable | Disable

➢ ***Egress Remap***

- 0~63



CLI 설정 예시

✓ **DSCP Translation**

➢ ***DSCP***

➢ ***Ingress Translate***

- 0~63

```
(config)# qos map dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } to { <dscp_num_tr> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }
(config)# qos map dscp-ingress-translation 0 to 1
(config)# qos map dscp-ingress-translation 60 to 63
(config)# qos map dscp-ingress-translation be to 1
```

➢ ***Ingress Classify***

- Enable | Disable

```
(config)# qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 |
af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }
(config)# qos map dscp-classify 0
(config)# qos map dscp-classify 63
(config)# qos map dscp-classify be
(config)# no qos map dscp-classify 0
```

➢ ***Egress Remap***

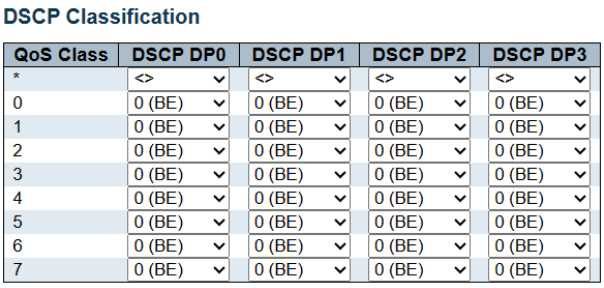
- 0~63

```
(config)# qos map dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 |
af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } <dpl> to { <dscp_num_tr> |
{ be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 |
cs6 | cs7 | ef | va } }
(config)# qos map dscp-egress-translation 0 to 1
(config)# qos map dscp-egress-translation 60 to 63
(config)# qos map dscp-egress-translation be to 1
```

6.19.1.10. DSCP Classification

웹메뉴 Configuration>QoS>DSCP Classification

이 페이지에서는 QoS 클래스와 Drop Precedence Level을 DSCP 값으로 매핑할 수 있습니다.


DSCP Classification

QoS Class	DSCP DP0	DSCP DP1	DSCP DP2	DSCP DP3
*	<>	<>	<>	<>
0	0 (BE)	0 (BE)	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)	0 (BE)	0 (BE)
5	0 (BE)	0 (BE)	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)	0 (BE)	0 (BE)

DSCP Classification

용어	설명
QoS Class	실제 QoS 클래스입니다.
DSCP DP0	Drop Precedence Level 0 에 대해 분류된 DSCP 값 (0-63)을 선택합니다.
DSCP DP1	Drop Precedence Level 1 에 대해 분류된 DSCP 값 (0-63)을 선택합니다.
DSCP DP2	Drop Precedence Level 2 에 대해 분류된 DSCP 값 (0-63)을 선택합니다.
DSCP DP3	Drop Precedence Level 3 에 대해 분류된 DSCP 값 (0-63)을 선택합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>QoS>DSCP Classification

✓ **DSCP Classification**

➢ ***QoS Class***

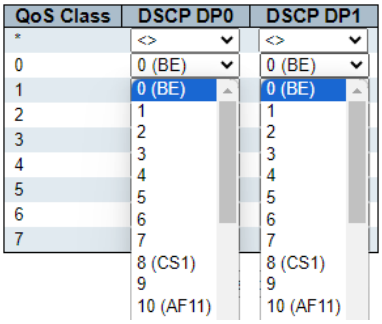
- 0~7

➢ ***DP***

- 0~1, 0~3

➢ ***DSCP***

- 0~63



CLI 설정 예시

- ***QoS Class***
  - 0~7
- ***DP***
  - 0~1 or 0~3
- ***DSCP***
  - 0~63

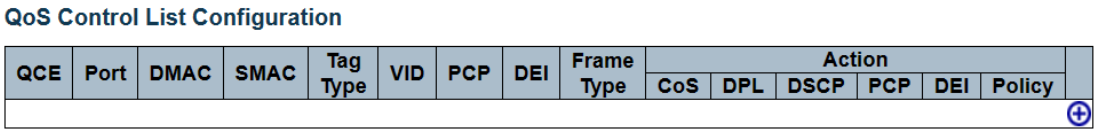
```
(config)# qos map cos-dscp <cos> dpl <dpl> dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }
(config)# qos map cos-dscp 0 dpl 0 dscp 0
(config)# qos map cos-dscp 7 dpl 1 dscp 63
(config)# qos map cos-dscp 7 dpl 1 dscp be
```

6.19.1.11. QoS Control List

웹메뉴 Configuration>QoS>QoS Control List

이 페이지는 QoS 제어 목록(QCL)을 표시합니다. 이 목록은 QCE(QoS Classification Entry)들로 구성됩니다. 각 행은 정의된 QCE를 설명합니다. 각 스위치마다 최대 256개의 QCE를 설정할 수 있습니다.

리스트에 새로운 QCE를 추가하려면 가장 아래에 있는 더하기(+) 기호를 클릭하세요.



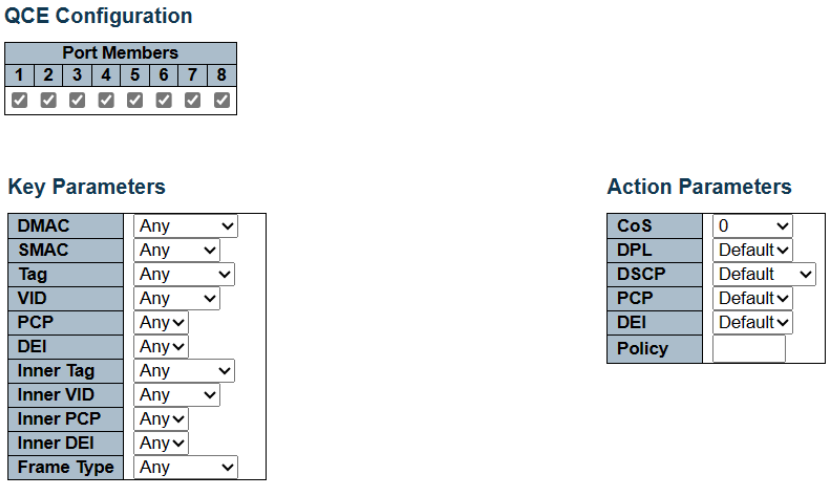
QoS Control List Configuration

용어	설명
QCE	QCE ID 를 나타냅니다.
Port	QCE 와 구성된 포트 목록 또는 'Any'를 나타냅니다.
DMAC	수신 프레임의 목적지 MAC 주소를 나타냅니다. Any: 모든 DMAC 주소가 일치합니다. Unicast: 유니캐스트 DMAC 주소가 일치합니다. Multicast: 멀티캐스트 DMAC 주소가 일치합니다. Broadcast: 브로드캐스트 DMAC 주소가 일치합니다. <MAC>: 특정 DMAC 주소가 일치합니다. 기본값은 'Any'입니다.
SMAC	특정 소스 MAC 주소나 'Any' 가 일치합니다.
Tag Type	태그 유형을 나타냅니다. 가능한 값은 다음과 같습니다: Any: 태그된 및 언태그된 프레임과 일치합니다. Untagged: 언태그된 프레임과 일치합니다. Tagged: 태그된 프레임과 일치합니다. C-Tagged: C-태그가 있는 프레임과 일치합니다. S-Tagged: S-태그가 있는 프레임과 일치합니다. 기본값은 'Any'입니다.
VID	(VLAN ID)는 특정한 VID 또는 VID 범위를 나타냅니다. VID 는 1 에서 4095 까지의 범위에 있거나 'Any'일 수 있습니다.
PCP	Priority Code Point (PCP): PCP 의 유효한 값은 특정한 값(0, 1, 2, 3, 4, 5, 6, 7)이나 범위(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) 또는 'Any'입니다.
DEI	Drop Eligible Indicator (DEI): DEI 의 유효한 값은 0, 1 또는 'Any'입니다.
Frame Type	프레임 유형을 나타냅니다. 가능한 값은 다음과 같습니다: Any: 모든 프레임 유형과 일치합니다. Ethernet: EtherType 프레임과 일치합니다. LLC: (LLC) 프레임과 일치합니다. SNAP: (SNAP) 프레임과 일치합니다. IPv4: IPv4 프레임과 일치합니다. IPv6: IPv6 프레임과 일치합니다.
Action	매개변수가 프레임의 내용과 일치하는 경우 인그레스 프레임에 대해 수행되는 분류 동작을 나타냅니다.

	가능한 동작은 다음과 같습니다: CoS: 서비스 등급(Class of Service)을 분류합니다. DPL: 드롭 우선 순위(Drop Precedence Level)를 분류합니다. DSCP: DSCP 값(DSCP value)을 분류합니다. PCP: PCP 값(PCP value)을 분류합니다. DEI: DEI 값(DEI value)을 분류합니다. Policy: ACL 정책 번호(Access Control List Policy number)를 분류합니다.
Modification Buttons	다음 버튼을 사용하여 테이블에서 각 QCE (QoS 제어 항목)를 수정할 수 있습니다: : 현재 행 앞에 새로운 QCE 를 삽입합니다. : QCE 를 편집합니다. : QCE 를 위로 이동시킵니다. : QCE 를 아래로 이동시킵니다. : QCE 를 삭제합니다. : 최하단의 플러스 기호는 QCE 목록의 가장 아래에 새 항목을 추가합니다.

QCE Configuration

이 페이지에서는 한 번에 하나의 QoS 제어 항목(QCE)을 편집하거나 삽입할 수 있습니다. QCE는 여러 매개변수로 구성됩니다. 이 매개변수는 선택한 프레임 유형에 따라 다양합니다.



QCE Configuration

	용어	설명
	Port Members	포트를 QCL 항목에 포함시키려면 체크 박스 버튼을 선택하십시오. 기본적으로 모든 포트가 포함됩니다.
	Key Parameters	주요 설정은 다음과 같이 설명됩니다: DMAC: 가능한 값은 '유니캐스트(Unicast)', '멀티캐스트(Multicast)', '브로드캐스트(Broadcast)', '특정(Specific)' (xx-xx-xx-xx-xx-xx 형식) 또는 '모두(Any)'입니다. SMAC: 출발지 MAC 주소: xx-xx-xx-xx-xx-xx 형식이거나 '모두(Any)'입니다. Tag: Tag 필드의 값은 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' 또는 '모두(Any)'일 수 있습니다. VID: VLAN ID의 유효한 값은 1에서 4095까지의 범위에 있는 모든 값이거나 '모두(Any)'일 수 있습니다. 사용자는 특정한 값이나

		VID의 범위를 입력할 수 있습니다.	
		PCP	PCP의 유효한 값은 특정한 값(0, 1, 2, 3, 4, 5, 6, 7) 또는 범위(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) 또는 '모두(Any)'일 수 있습니다.
		DEI	DEI의 유효한 값은 '0', '1' 또는 '모두(Any)'입니다.
		Inner Tag	내부 태그 필드의 값은 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' 또는 '모두(Any)'일 수 있습니다.
		Inner VID	내부 VLAN ID의 유효한 값은 1에서 4095까지의 범위 내의 모든 값이거나 '모두(Any)'일 수 있습니다. 사용자는 특정 값이나 VID 범위를 입력할 수 있습니다.
		Inner PCP	내부 PCP의 유효한 값은 특정 값 (0, 1, 2, 3, 4, 5, 6, 7) 또는 범위 (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) 또는 '모두(Any)'입니다.
		Inner DEI	내부 DEI의 유효한 값은 '0', '1' 또는 '모두(Any)'입니다.
		Frame Type	프레임 유형은 다음과 같은 값 중 하나를 가질 수 있습니다: 1.Any, 2,EtherType, 3.LLC, 4.SNAP, 5.IPv4, 6.IPv6
	1. Any	모든 유형의 프레임을 허용합니다.	
	2. EtherType	Ether Type	유효한 이더타입은 0x600-0xFFFF 중에서 0x800(IPv4)와 0x86DD(IPv6)을 제외하거나 'Any'입니다.
	3. LLC	DSAP Address	유효한 DSAP(Destination Service Access Point)은 0x00에서 0xFF까지의 값이거나 'Any'입니다.
		SSAP Address	유효한 SSAP(Source Service Access Point)은 0x00에서 0xFF까지의 값이거나 'Any'입니다.
		Control	유효한 제어 필드(Control field)는 0x00에서 0xFF까지의 값이거나 'Any'입니다.
	4. SNAP	PID	유효한 PID(또는 이더타입)은 0x0000에서 0xFFFF까지의 값이거나 'Any'입니다.
	5. IPv4	Protocol	IP 프로토콜 번호는 0에서 255까지의 값 또는 'TCP', 'UDP', 'Any'일 수 있습니다.
		Source IP	특정 소스 IP 주소는 값/마스크 형식이거나 'Any'일 수 있습니다. IP와 마스크는 x.y.z.w 형식이며, 여기서 x, y, z, w는 0에서 255 사이의 10진수입니다. 마스크를 32비트 이진 문자열로 변환하여 왼쪽에서 오른쪽으로 읽을 때, 첫 번째 0 다음의 모든 비트는 0이어야 합니다.
		Destination IP	특정 대상 IP 주소는 값/마스크 형식이거나 'Any'일 수 있습니다.
		IP Fragment	IPv4 프레임 분할 옵션은 'Yes', 'No', 또는 'Any'일 수 있습니다.
		DSCP	DSCP(Diffserv Code Point) 값은 특정 값, 값의 범위 또는 'Any'일 수 있습니다. DSCP 값은 BE, CS1-CS7, EF 또는 AF11-AF43을 포함하여 0-63의 범위에 있습니다.
		Sport	출발지 TCP/UDP 포트는 0-65535 또는 'Any'로 설정할 수 있으며, IP 프로토콜 UDP/TCP에 적용되는 특정 포트 또는 포트 범위를 지정할 수 있습니다.
		Dport	목적지 TCP/UDP 포트는 0-65535 또는 'Any'로 설정할 수 있으며, IP 프로토콜 UDP/TCP에 적용되는 특정 포트 또는 포트 범위를 지정할 수 있습니다.
	6. IPv6	Protocol	IP 프로토콜 번호는 0에서 255까지의 값 또는 'TCP', 'UDP', 'Any'로

		설정할 수 있습니다.	
		Source IP: IPv6 소스 주소의 하위 32비트를 값/마스크 형식으로 지정하거나 'Any'로 설정할 수 있습니다.	
		Destination IP: 특정 대상 IPv6 주소를 값/마스크 형식으로 지정하거나 'Any'로 설정할 수 있습니다.	
		DSCP: Diffserv Code Point(DSCP) 값은 특정 값, 값의 범위 또는 'Any'로 설정할 수 있습니다. DSCP 값은 0-63 범위 내에 있으며, BE, CS1-CS7, EF 또는 AF11-AF43과 같은 값이 포함됩니다.	
		Sport: 소스 TCP/UDP 포트는 0부터 65535까지의 값 또는 'Any'로 설정할 수 있으며, IP 프로토콜 UDP/TCP에 적용될 수 있는 특정 포트 또는 포트 범위를 지정할 수 있습니다.	
		Dport: 목적지 TCP/UDP 포트는 0부터 65535까지의 값 또는 'Any'로 설정할 수 있으며, IP 프로토콜 UDP/TCP에 적용될 수 있는 특정 포트 또는 포트 범위를 지정할 수 있습니다.	
	Action Parameters	CoS: Class of Service는 0부터 7까지의 값 또는 'Default'로 설정할 수 있습니다.	
		DP: Drop Precedence Level은 0부터 3까지의 값 또는 'Default'로 설정할 수 있습니다.	
		DSCP: DSCP는 0부터 63까지의 값 또는 'BE', 'CS1-CS7', 'EF' 또는 'AF11-AF43'으로 설정할 수 있습니다. 또는 'Default'로 설정할 수도 있습니다.	
		PCP: PCP는 0부터 7까지의 값 또는 'Default'로 설정할 수 있습니다. 참고: PCP와 DEI는 개별적으로 설정할 수 없습니다.	
		DEI: DEI는 0 또는 1의 값 또는 'Default'로 설정할 수 있습니다.	
		Policy: ACL 정책 번호는 0부터 255까지의 값 또는 'Default' (빈 필드)로 설정할 수 있습니다.	
		'Default'는 이 QCE 에 의해 기본 분류 값이 수정되지 않음을 의미합니다.	

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.
Cancel: 변경된 설정을 저장하지 않고 이전 페이지로 돌아가려면 클릭하세요.

WEB 설정 예시

웹메뉴 Configuration>QoS>QoS Control List

✓ **QoS Control List Configuration**

- ***QCE***
- ***Port***
- ***DMAC***
- ***SMAC***
- ***Tag Type***

- ***VID***
- ***PCP***
- ***DEI***
- ***Frame Type***
- ***Action***
  - CoS
  - DPL
  - DSCP
  - PCP
  - DEI
  - Policy

QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action					
									CoS	DPL	DSCP	PCP	DEI	Policy
														⊕

Click ⊕ Button

✓ QCE Configuration

- ***Port Members***
  - Select Port

Port Members									
1	2	3	4	5	6	7	8	9	10
☑	☑	☐	☐	☑	☑	☐	☐	☑	☑

✓ Key Parameters

- ***DMAC***
  - Any | Unicast | Multicast | Broadcast

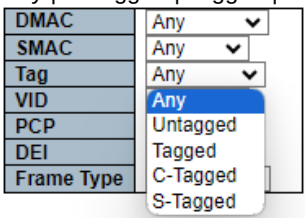
DMAC	Any
SMAC	Any (Any / Unicast / Multicast / Broadcast)
Tag	
VID	
PCP	
DEI	Any
Frame Type	Any

- ***SMAC***
  - Any | Specific(이 옵션을 선택하면 추가 구성 옵션이 생성됩니다.)

DMAC	Any	
SMAC	Specific	00-00-00-00-00-00
Tag	Any	
VID	Specific	
PCP	Any	
DEI	Any	
Frame Type	Any	

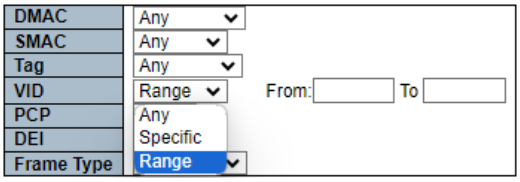
- ***Tag***

- Any | Untagged | Tagged | C-Tagged | S-Tagged



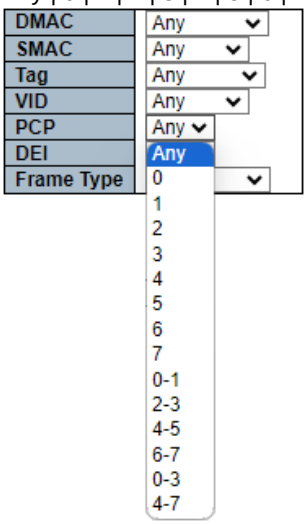
➢ ***VID***

- Any | Specific(추가 구성 옵션) | Range(추가 구성 옵션)



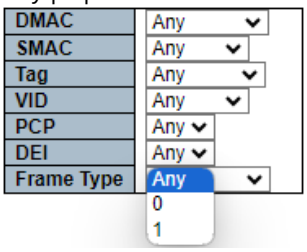
➢ ***PCP***

- Any | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7



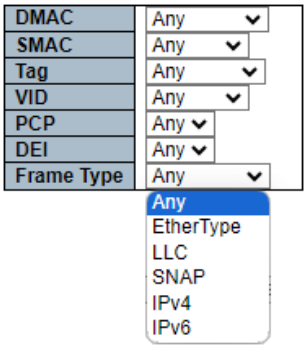
➢ ***DEI***

- Any | 0 | 1



➢ ***Frame Type***(추가 구성 옵션)

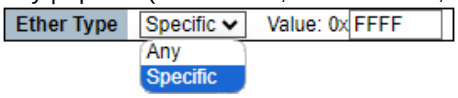
- Any | EtherType | LLC | SNAP | IPv4 | IPv6



✓ EtherType Parameters

➢ *Ether Type*

- Any | Specific(0x600-0x7ff,0x801-0x86dc,0x86de-0xffff)



✓ LLC Parameters

➢ *DSAP Address*

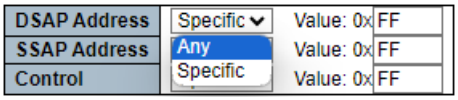
- Any | Specific(추가 구성 옵션)

➢ *SSAP Address*

- Any | Specific(추가 구성 옵션)

➢ *Control*

- Any | Specific(추가 구성 옵션)



✓ SNAP Parameters

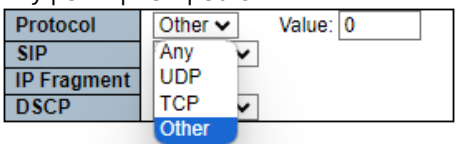
➢ *PID*

- Any | Specific(추가 구성 옵션)

✓ IPv4 Parameters

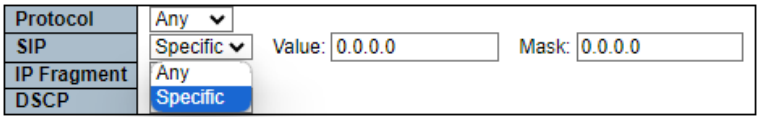
➢ ***Protocol***(추가 구성 옵션)

- Any | UDP | TCP | Other



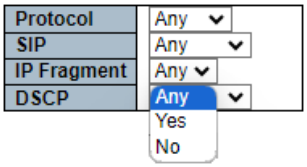
➢ *SIP*

- Any | Specific(추가 구성 옵션)



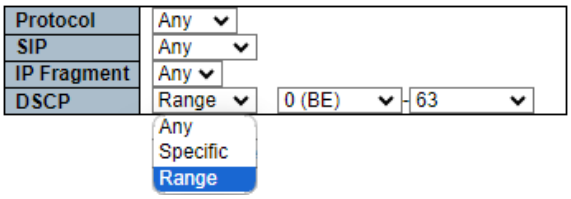
➢ *IP Fragment*

- Any | Yes | No



➢ ***DSCP***

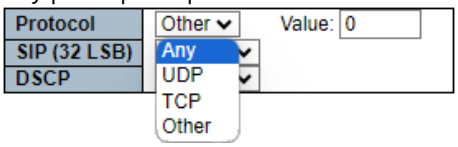
- Any | Specific(추가 구성 옵션) | Range(추가 구성 옵션)



✓ IPv6 Parameters

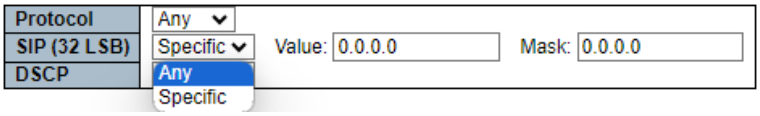
➢ ***Protocol***(추가 구성 옵션)

- Any | UDP | TCP | Other



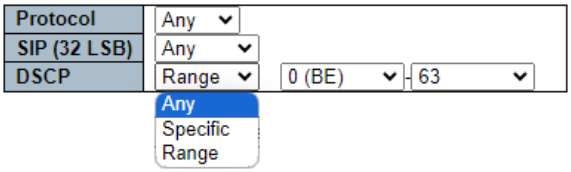
➢ ***SIP (32LSB)***

- Any | Specific(추가 구성 옵션)



➢ ***DSCP***

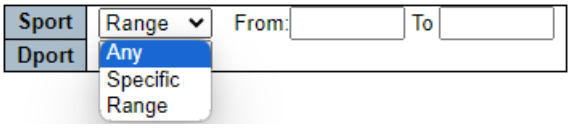
- Any | Specific(추가 구성 옵션) | Range(추가 구성 옵션)



✓ UDP Parameters

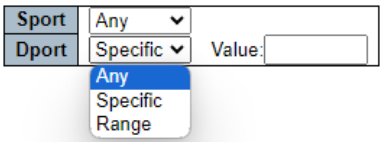
➢ ***Sport***

- Any | Specific(추가 구성 옵션) | Range(추가 구성 옵션)



➢ ***Dport***

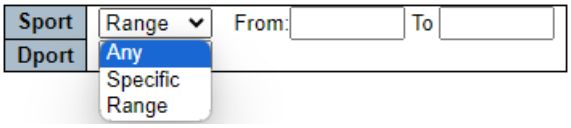
- Any | Specific(추가 구성 옵션) | Range(추가 구성 옵션)



✓ TCP Parameters

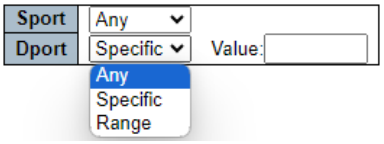
➢ ***Sport***

- Any | Specific(추가 구성 옵션) | Range(추가 구성 옵션)



➢ ***Dport***

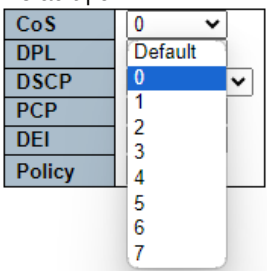
- Any | Specific(추가 구성 옵션) | Range(추가 구성 옵션)



✓ Action Parameters

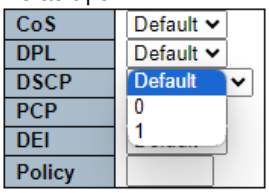
➢ ***CoS***

- Default | 0~7



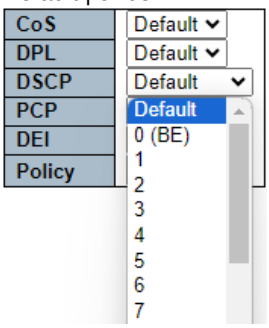
➢ ***DPL***

- Default | 0~1



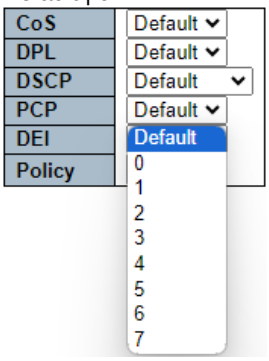
➢ ***DSCP***

- Default | 0~63



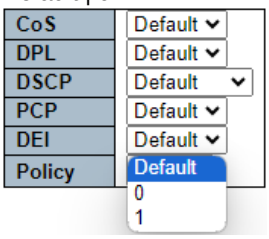
➢ ***PCP***

- Default | 0~7



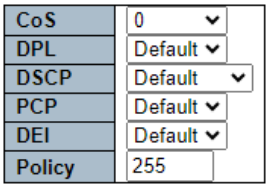
➢ ***DEI***

- Default | 0~1



➢ ***Policy***

- Default(빈 필드) | 0~255



CLI 설정 예시

✓ QCE Configuration

```
(config)# qos qce { [ update ] } <qce_id> [ { next <qce_id_next> } | last ] [ interface (<port_type>
[ <port_list> ] ) ] [ smac { <smac> | <smac_24> | any } ] [ dmac { <dmac> | unicast | multicast | broadcast |
any } ] [ tag { [ type { untagged | tagged | c-tagged | s-tagged | any } ] [ vid { <ot_vid> | any } ] [ pcp
{ <ot_pcp> | any } ] [ dei { <ot_dei> | any } ] }*1 ] [ inner-tag { [ type { untagged | tagged | c-tagged | s-
tagged | any } ] [ vid { <it_vid> | any } ] [ pcp { <it_pcp> | any } ] [ dei { <it_dei> | any } ] }*1 ] [ frame-type
{ any | { etype [ { <etype_type> | any } ] } | { llc [ dsap { <llc_dsap> | any } ] [ ssap { <llc_ssap> | any } ]
[ control { <llc_control> | any } ] } | { snap [ { <snap_data> | any } ] } | { ipv4 [ proto { <pr4> | tcp | udp |
any } ] [ sip { <sip4> | any } ] [ dip { <dip4> | any } ] [ dscp { <dscp4> | { be | af11 | af12 | af13 | af21 | af22
| af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any } ]
 fragment { yes | no | any } ] [ sport { <sp4> | any } ] [ dport { <dp4> | any } ] } | { ipv6 [ proto { <pr6> | tcp
| udp | any } ] [ sip { <sip6> | any } ] [ dip { <dip6> | any } ] [ dscp { <dscp6> | { be| af11 | af12 | af13 | af21
| af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any } ]
[ sport { <sp6> | any } ] [ dport { <dp6> | any } ] } } ] [ action { [ cos { <action_cos> | default } ] [ dpl
{ <action_dpl> | default } ] [ pcp-dei { <action_pcp> <action_dei> | default } ] [ dscp { <action_dscp_dscp> |
{ be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 |
cs6 | cs7 | ef | va } | default } ] [ policy { <action_policy> | default } ] }*1 ]
```

➢ ***Port Members***

- Select Port

```
(config)# qos qce 1 interface *
(config)# qos qce 1 GigabitEthernet 1/1
(config)# qos qce 1 interface 2.5GigabitEthernet 1/1
```

✓ Key Parameters

➢ ***DMAC***

- Any | Unicast | Multicast | Broadcast

```
(config)# qos qce 1 dmac any
(config)# qos qce 1 dmac unicast
(config)# qos qce 1 dmac multicast
(config)# qos qce 1 dmac broadcast
```

➢ ***SMAC***

- Any | Specific

```
(config)# qos qce 1 smac any
(config)# qos qce 1 smac 00-21-6d-00-00-00
```

➢ ***Tag***

- Any | Untagged | Tagged | C-Tagged | S-Tagged

```
(config)# qos qce 1 tag type any
(config)# qos qce 1 tag type untagged
(config)# qos qce 1 tag type tagged
(config)# qos qce 1 tag type c-tagged
(config)# qos qce 1 tag type s-tagged
```

➢ ***VID***

- Any | Specific | Range

```
(config)# qos qce 1 tag vid any
(config)# qos qce 1 tag vid 1
(config)# qos qce 1 tag vid 1-2
```

➢ ***PCP***

- Any | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7

```
(config)# qos qce 1 tag pcp any
(config)# qos qce 1 tag pcp 0
(config)# qos qce 1 tag pcp 0-1
(config)# qos qce 1 tag pcp 0-3
```

➢ ***DEI***

- Any | 0 | 1

```
(config)# qos qce 1 tag dei any
(config)# qos qce 1 tag dei 0
(config)# qos qce 1 tag dei 1
```

➢ ***Frame Type***

- Any | EtherType | LLC | SNAP | IPv4 | IPv6

```
(config)# qos qce 1 frame-type any
(config)# qos qce 1 frame-type etype
(config)# qos qce 1 frame-type ipv4
(config)# qos qce 1 frame-type ipv6
(config)# qos qce 1 frame-type llc
(config)# qos qce 1 frame-type snap
```

✓ **EtherType Parameters**

➢ ***Ether Type***

- Any | Specific(<0x600-0x7ff,0x801-0x86dc,0x86de-0xffff>)

```
(config)# qos qce 1 frame-type etype any
(config)# qos qce 1 frame-type etype 0x600
```

✓ **LLC Parameters**

➢ ***DSAP Address***

- Any | Specific(<0-0xff>)

```
(config)# qos qce 1 frame-type llc dsap any
(config)# qos qce 1 frame-type llc dsap 0xff
```

➢ ***SSAP Address***

- Any | Specific(<0-0xff>)

```
(config)# qos qce 1 frame-type llc ssap any
(config)# qos qce 1 frame-type llc ssap 0xff
```

➢ ***Control***

- Any | Specific(<0-0xff>)

```
(config)# qos qce 1 frame-type llc control any
(config)# qos qce 1 frame-type llc control 0xff
```

✓ **SNAP Parameters**

➢ ***PID***

- Any | Specific(<0-0xffff>)

```
(config)# qos qce 1 frame-type snap any
(config)# qos qce 1 frame-type snap 0xffff
```

✓ **IPv4 Parameters**

➢ ***Protocol***

- Any | UDP | TCP | Other(<0-255>)

```
(config)# qos qce 1 frame-type ipv4 proto any
(config)# qos qce 1 frame-type ipv4 proto udp
(config)# qos qce 1 frame-type ipv4 proto tcp
(config)# qos qce 1 frame-type ipv4 proto 255
```

➢ ***SIP***

- Any | Specific(<ipv4_subnet>)

```
(config)# qos qce 1 frame-type ipv4 sip any
(config)# qos qce 1 frame-type ipv4 sip 192.168.10.100/255.255.255.0
```

➢ ***IP Fragment***

- Any | Yes | No

```
(config)# qos qce 1 frame-type ipv4 fragment any
(config)# qos qce 1 frame-type ipv4 fragment yes
(config)# qos qce 1 frame-type ipv4 fragment no
```

➢ ***DSCP***

- Any | Specific(0-63, BE, CS1-CS7, EF or AF11-AF43) | Range(0-63)

```
(config)# qos qce 1 frame-type ipv4 dscp any
(config)# qos qce 1 frame-type ipv4 dscp 0
(config)# qos qce 1 frame-type ipv4 dscp be
(config)# qos qce 1 frame-type ipv4 dscp 62-63
```

✓ **IPv6 Parameters**

➢ ***Protocol***(additional configuration options.)

- Any | UDP | TCP | Other(<0-255>)

```
(config)# qos qce 1 frame-type ipv6 proto any
(config)# qos qce 1 frame-type ipv6 proto udp
(config)# qos qce 1 frame-type ipv6 proto tcp
(config)# qos qce 1 frame-type ipv6 proto 255
```

➢ ***SIP (32LSB)***

- Any | Specific(<ipv4_subnet>)

```
(config)# qos qce 1 frame-type ipv6 sip any
(config)# qos qce 1 frame-type ipv6 sip 192.168.10.100/255.255.255.0
```

➢ ***DSCP***

- Any | Specific(0-63, BE, CS1-CS7, EF or AF11-AF43) | Range(0-63)

```
(config)# qos qce 1 frame-type ipv6 dscp any
(config)# qos qce 1 frame-type ipv6 dscp 0
(config)# qos qce 1 frame-type ipv6 dscp be
(config)# qos qce 1 frame-type ipv6 dscp 62-63
```

✓ UDP Parameters

➢ *Sport*

- Any | Specific(0~65535) | Range(0-65535)

```
(config)# qos qce 1 frame-type ipv4 proto udp sport any
(config)# qos qce 1 frame-type ipv4 proto udp sport 100
(config)# qos qce 1 frame-type ipv4 proto udp sport 0-65535
(config)# qos qce 1 frame-type ipv6 proto udp sport any
(config)# qos qce 1 frame-type ipv6 proto udp sport 100
(config)# qos qce 1 frame-type ipv6 proto udp sport 0-65535
```

➢ *Dport*

- Any | Specific(0~65535) | Range(0-65535)

```
(config)# qos qce 1 frame-type ipv4 proto udp dport any
(config)# qos qce 1 frame-type ipv4 proto udp dport 100
(config)# qos qce 1 frame-type ipv4 proto udp dport 0-65535
(config)# qos qce 1 frame-type ipv6 proto udp dport any
(config)# qos qce 1 frame-type ipv6 proto udp dport 100
(config)# qos qce 1 frame-type ipv6 proto udp dport 0-65535
```

✓ TCP Parameters

➢ *Sport*

- Any | Specific | Range

```
(config)# qos qce 1 frame-type ipv4 proto tcp sport any
(config)# qos qce 1 frame-type ipv4 proto tcp sport 100
(config)# qos qce 1 frame-type ipv4 proto tcp sport 0-65535
(config)# qos qce 1 frame-type ipv6 proto tcp sport any
(config)# qos qce 1 frame-type ipv6 proto tcp sport 100
(config)# qos qce 1 frame-type ipv6 proto tcp sport 0-65535
```

➢ *Dport*

- Any | Specific | Range

```
(config)# qos qce 1 frame-type ipv4 proto tcp dport any
(config)# qos qce 1 frame-type ipv4 proto tcp dport 100
(config)# qos qce 1 frame-type ipv4 proto tcp dport 0-65535
(config)# qos qce 1 frame-type ipv6 proto tcp dport any
(config)# qos qce 1 frame-type ipv6 proto tcp dport 100
(config)# qos qce 1 frame-type ipv6 proto tcp dport 0-65535
```

✓ Action Parameters

➢ *CoS*

- Default | 0~7

```
(config)# qos qce 1 action cos default
(config)# qos qce 1 action cos 7
```

➢ *DPL*

- Default | 0~1

```
(config)# qos qce 1 action dpl default
(config)# qos qce 1 action dpl 0
```

➢ *DSCP*

- Default | 0~63

```
(config)# qos qce 1 action dscp default
(config)# qos qce 1 action dscp 0
(config)# qos qce 1 action dscp be
(config)# qos qce 1 action dscp 63
```

- ***PCP***
  - Default | 0~7
- ***DEI***
  - Default | 0~1

```
(config)# qos qce 1 action pcp-dei default
(config)# qos qce 1 action pcp-dei 7 1
(config)# qos qce 1 action pcp-dei 0 0
```

- ***Policy***
  - Default | 0~255

```
(config)# qos qce 1 action policy default
(config)# qos qce 1 action policy 255
(config)# qos qce 1 action policy 0
```

6.19.1.12. Storm Policing

웹메뉴 Configuration>QoS>Storm Policing

이 페이지에서는 스위치의 전역 스톰 폴리서를 구성할 수 있습니다.

Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unknown Unicast	☑	1	kfps
Multicast	☑	1	kfps
Broadcast	☑	1	kfps

Port Storm Policer Configuration

Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit
*	☐	1	<>	☑	1	<>	☐	1	<>
1	☐	1	kfps	☑	1	kfps	☐	1	kfps
2	☐	1	kfps	☑	1	kfps	☐	1	kfps
3	☐	1	kfps	☑	1	kfps	☐	1	kfps
4	☐	1	kfps	☑	1	kfps	☐	1	kfps
5	☐	1	kfps	☑	1	kfps	☐	1	kfps
6	☐	1	kfps	☑	1	kfps	☐	1	kfps
7	☐	1	kfps	☑	1	kfps	☐	1	kfps
8	☐	1	kfps	☑	1	kfps	☐	1	kfps
9	☐	1	kfps	☑	1	kfps	☐	1	kfps
10	☐	1	kfps	☑	1	kfps	☐	1	kfps
11	☐	1	kfps	☑	1	kfps	☐	1	kfps
12	☐	1	kfps	☑	1	kfps	☐	1	kfps

Global Storm Policer Configuration

유니캐스트 스톰 폴리서, 멀티캐스트 스톰 폴리서 및 브로드캐스트 스톰 폴리서가 있습니다.

이러한 폴리서는 플러딩 된 프레임에만 영향을 미칩니다. 즉, MAC 주소 테이블에 없는 (VLAN ID, DMAC) 쌍을 가진 프레임에 영향을 미칩니다. 표시된 설정은 다음과 같습니다:

용어	설명
Frame Type	아래는 설정 지원되는 프레임 유형입니다.
Enable	프레임 유형에 대한 글로벌 스톰 폴리서를 활성화 또는 비활성화합니다.
Rate	글로벌 스톰 폴리서의 속도를 제어합니다. "Unit"이 fps 또는 kbps 인 경우 이 값은 10-13128147 로 제한되며, kfps 또는 Mbps 인 경우 1-13128 로 제한됩니다. 속도는 내부적으로 글로벌 스톰 폴리서가 지원하는 가장 가까운 값으로 반올림됩니다.
Unit	글로벌 스톰 폴리서의 속도를 측정하는 단위를 선택합니다. 이 단위는 fps(프레임/초), kfps(천 프레임/초), kbps(킬로비트/초), Mbps(메가비트/초) 중에서 선택할 수 있습니다.

Port Storm Policer Configuration

포트 스톰 폴리서는 스위치의 모든 포트에 대해 구성됩니다.

유니캐스트 프레임, 브로드캐스트 프레임, 언노운프레임(플러딩)을 위한 스톰 폴리서가 있습니다.

표시된 설정은 다음과 같습니다.

용어	설명
Port	아래 구성이 적용되는 포트 번호입니다.

Enable	이 스위치 포트의 스톰 폴리서를 활성화하거나 비활성화합니다.
Rate	포트 스톰 폴리서의 속도를 제어합니다. "단위"가 fps 또는 kbps 인 경우에는 10 에서 13128147 까지의 값을, kfps 또는 Mbps 인 경우에는 1 에서 13128 까지의 값을 입력할 수 있습니다. 속도는 포트 스톰 폴리서가 지원하는 가장 가까운 값으로 내림 처리됩니다.
Unit	포트 스톰 폴리서의 속도 단위를 설정합니다. "fps", "kfps", "kbps", "Mbps" 중에서 선택할 수 있습니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

WEB 설정 예시

웹메뉴 Configuration>QoS>Storm Policing

✓ Global Storm Policer Configuration

- ***Frame Type***
  - Unknown Unicast | Multicast | Broadcast
- ***Enable***
  - Enable | Disable
- ***Rate***
  - 10-13128147(fps|kbps)
  - 1-13128(kfps|Mbps)
- ***Unit***
  - fps | kfps | kbps | Mbps

Frame Type	Enable	Rate	Unit
Unknown Unicast	☑	13128147	kbps
Multicast	☑	13128	Mbps
Broadcast	☑	10	fps

✓ Port Storm Policer Configuration

- ***Port***
- ***Enable***
  - Enable | Disable
- ***Rate***
  - 10-13128147(fps|kbps)
  - 1-13128(kfps|Mbps)

➢ ***Unit***

- fps | kfps | kbps | Mbps

Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit
*	☑	10	<>	☑	1	<>	☐	1	<>
1	☑	10	fps	☑	1	kfps	☐	1	kfps
2	☑	13128147	kbps	☑	1	kfps	☐	1	kfps
3	☑	1	kfps	☑	1	kfps	☐	1	kfps
4	☑	13128	Mbps	☑	1	kfps	☐	1	kfps
5	☐	1	kfps	☑	1	kfps	☐	1	kfps
6	☐	1	kfps	☑	1	kfps	☐	1	kfps
7	☐	1	kfps	☑	1	kfps	☐	1	kfps
8	☐	1	kfps	☑	1	kfps	☐	1	kfps
9	☐	1	kfps	☑	1	kfps	☐	1	kfps
10	☐	1	kfps	☑	1	kfps	☐	1	kfps
11	☐	1	kfps	☑	1	kfps	☐	1	kfps
12	☐	1	kfps	☑	1	kfps	☐	1	kfps

CLI 설정 예시

✓ Global Storm Policer Configuration

➢ ***Frame Type***

- Unknown Unicast | Multicast | Broadcast

➢ ***Enable***

- Enable | Disable

➢ ***Rate***

- 10-13128147(fps|kbps)
- 1-13128(kfps|Mbps)

➢ ***Unit***

- fps | kfps | kbps | Mbps

```
(config)# qos storm { unicast | multicast | broadcast } <rate> [ fps | kfps | kbps | mbps ]
(config)# qos storm unicast 13128 kfps
(config)# qos storm multicast 13128147 fps
(config)# qos storm broadcast 1 mbps
```

✓ Port Storm Policer Configuration

➢ ***Port***

➢ ***Enable***

- Enable | Disable

➢ ***Rate***

- 10-13128147(fps|kbps)

- 1-13128(kfps|Mbps)

➢ ***Unit***

- fps | kfps | kbps | Mbps

(config)# interface interface (<port_type> [<plist>]) *(config)# interface GigabitEthernet 1/1*
(config-if)# qos storm { unicast | multicast | broadcast } <rate> [fps | kfps | kbps | mbps] *(config-if)# qos storm unicast 13128 kfps* *(config-if)# qos storm multicast 13128147 fps* *(config-if)# qos storm broadcast 1 mbps* *(config-if)# qos storm multicast 10 kbps*

6.19.1.13. WRED

웹메뉴 Configuration>QoS>WRED

이 페이지에서는 랜덤 조기 탐지(Random Early Detection, RED) 설정을 구성할 수 있습니다.

Weighted Random Early Detection Configuration

Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	☐	0	50	Drop Probability
1	0	2	☐	0	50	Drop Probability
1	0	3	☐	0	50	Drop Probability
1	1	1	☐	0	50	Drop Probability
1	1	2	☐	0	50	Drop Probability
1	1	3	☐	0	50	Drop Probability
1	2	1	☐	0	50	Drop Probability
1	2	2	☐	0	50	Drop Probability
1	2	3	☐	0	50	Drop Probability
1	3	1	☐	0	50	Drop Probability
3	5	2	☐	0	50	Drop Probability
3	5	3	☐	0	50	Drop Probability
3	6	1	☐	0	50	Drop Probability
3	6	2	☐	0	50	Drop Probability
3	6	3	☐	0	50	Drop Probability
3	7	1	☐	0	50	Drop Probability
3	7	2	☐	0	50	Drop Probability
3	7	3	☐	0	50	Drop Probability

Weighted Random Early Detection Configuration

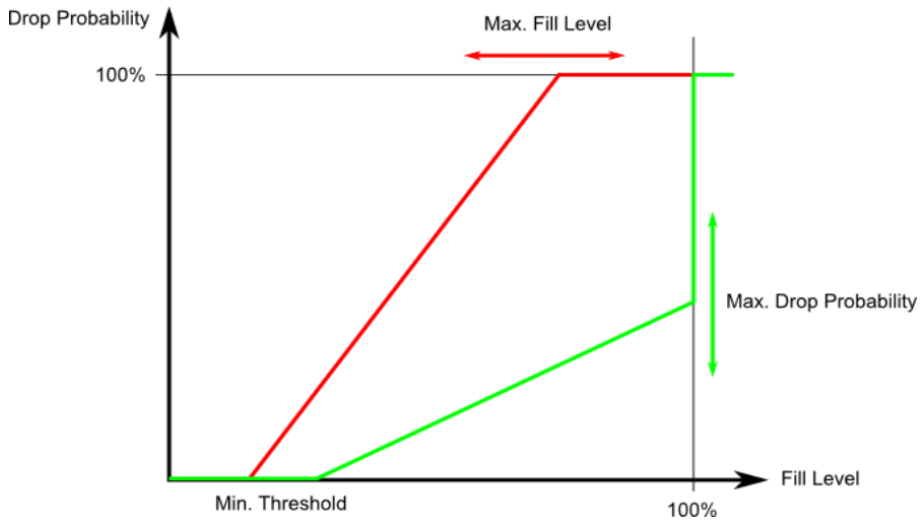
다양한 RED 구성을 통해 큐(QoS 클래스) 간에 가중 랜덤 조기 탐지(Weighted Random Early Detection, WRED) 작업을 수행할 수 있습니다.

이 설정은 스위치의 모든 포트에 대해 전역적으로 적용됩니다.

용어	설명
Group	설정이 적용되는 WRED 그룹 번호입니다.
Queue	설정이 적용되는 큐 번호 (QoS 클래스)입니다.
DPL	설정이 적용되는 Drop Precedence Level 입니다.
Enable	이 항목을 통해 해당 엔트리에 대해 RED 를 활성화 또는 비활성화할 수 있습니다.
Min	RED 의 하한으로, 큐 채움 수준이 이 임계 값 아래로 떨어지면 드롭 확률은 0 입니다. 이 값은 0-100%로 제한됩니다.
Max	Drop Precedence Level > 0 (노란색 프레임)에 대한 상한 RED 드롭 확률 또는 채움 수준 임계 값을 제어합니다. 이 값은 1-100%로 제한됩니다.
Max Unit	Max 에 대한 단위를 선택합니다. Drop Probability Max는 채움 수준이 거의 100%인 경우 드롭 확률을 제어합니다. Fill Level Max는 드롭 확률이 100%에 도달하는 채움 수준을 제어합니다.

RED Drop Probability Function

다음 그림은 연관된 매개변수와 함께 드롭 확률과 채움 수준 간의 관계를 보여주는 그림입니다.



Min 은 Drop Precedence Level > 0 (노란색 프레임)으로 표시된 프레임이 무작위로 드롭되기 시작하는 채움 수준입니다.

만약 Max Unit 이 'Drop Probability'인 경우(녹색 선), Max 는 채움 수준이 100% 바로 아래일 때의 드롭 확률을 제어합니다.

만약 Max Unit 이 'Fill Level'인 경우(빨간색 선), Max 는 드롭 확률이 100%에 도달하는 채움 수준을 제어합니다. 이 구성을 통해 드롭 우선 순위 레벨 0(녹색 프레임)으로 표시된 프레임을 전용으로 유지할 수 있습니다. 예약된 부분은 (100 - Max) %로 계산됩니다.

드롭 우선 순위 레벨 0(녹색 프레임)으로 표시된 프레임은 절대로 드롭되지 않습니다.

프레임의 드롭 확률은 평균 큐 채우기 수준(Min)에서 0 으로부터 시작하여 Max Drop Probability 또는 Fill Level 까지 선형적으로 증가합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

6.20. Mirroring

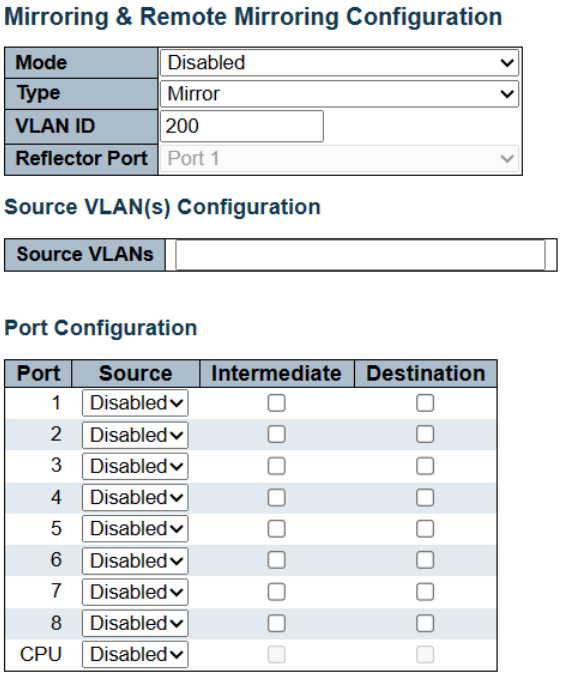
6.20.1. Mirroring Configuration

웹메뉴 Configuration>Mirroring

Mirroring 은 스위치 포트 분석기의 기능입니다. 관리자는 Mirroring 을 사용하여 네트워크 문제를 디버깅할 수 있습니다. 선택한 트래픽은 미러링되거나 복사되어 네트워크 트래픽을 분석할 수 있는 네트워크 분석기가 연결된 대상 포트로 전달됩니다.

원격 미러링은 Mirroring 의 확장 기능입니다. 다른 스위치에서 대상 포트를 확장할 수 있습니다. 따라서 관리자는 다른 스위치에서 네트워크 트래픽을 분석할 수 있습니다.

태그된 미러링 트래픽을 받으려면 반사 포트에서 VLAN 출발지 태깅을 "Tag All"로 설정해야 합니다. 반대로, 태그되지 않은 미러링 트래픽을 받으려면 반사 포트에서 VLAN 출발지 태깅을 "Untag All"로 설정해야 합니다.



Mirroring & Remote Mirroring Configuration

용어	설명
Mode	이 페이지에서는 미러링 기능을 활성화/비활성화할 수 있습니다.
Type	스위치 유형을 선택하세요. Mirror: 스위치는 미러 모드로 실행 중입니다. 소스 포트(들)와 대상 포트는 이 스위치에 위치합니다. Source: 스위치는 모니터링 플로우에 대한 소스 노드입니다. 소스 포트(들), 리플렉터 포트 및 중간 포트(들)는 이 스위치에 위치합니다. Intermediate: 스위치는 모니터링 플로우에 대한 전달 노드이며, 스위치는 옵션

	노드입니다. 목표는 소스 스위치에서 대상 스위치로 트래픽을 전달하는 것입니다. 중간 포트(들)는 이 스위치에 위치합니다. Destination: 스위치는 모니터링 플로우에 대한 종단 노드입니다. 대상 포트(들)과 중간 포트(들)는 이 스위치에 위치합니다.
VLAN ID	VLAN ID 는 모니터 패킷이 복사될 위치를 가리킵니다. 기본 VLAN ID 는 200 입니다.
Reflector Port	리플렉터 포트는 트래픽을 원격 미러링 VLAN 으로 리다이렉트하는 방법입니다. 리플렉터 포트로 설정된 포트에 연결된 장치는 원격 미러링이 비활성화될 때까지 연결이 끊어집니다. 스택 모드에서는 올바른 장치를 선택하기 위해 스위치 ID 를 선택해야 합니다. 포트를 종료하면 리플렉터 포트로 지정할 수 없습니다. 리플렉터 포트인 포트를 종료하면 원격 미러 기능이 작동하지 않습니다. 참고 1: 리플렉터 포트는 소스 스위치 유형에서만 mo 선택해야 합니다. 참고 2: 리플렉터 포트는 MAC 테이블 학습과 STP 를 비활성화해야 합니다. 참고 3: 리플렉터 포트는 순수한 구리 포트에서만 지원됩니다.

Source VLAN(s) Configuration

스위치는 VLAN 기반 미러링을 지원할 수 있습니다. 스위치에서 특정 VLAN을 모니터링하려면 이 필드에서 선택한 VLAN을 설정할 수 있습니다.

참고1: 미러링 세션은 포트 또는 VLAN 중 하나만 소스로 가져야 하며 둘 다 사용할 수 없습니다.

Port Configuration

다음 테이블은 포트 역할 선택에 사용됩니다.

용어	설명
Port	같은 행에 있는 설정에 대한 논리 포트입니다.
Source	미러 모드를 선택합니다. Disabled: 프레임 전송 및 수신 모두 미러링되지 않습니다. Both: 중간/목적지 포트에서 수신된 프레임과 전송된 프레임이 미러링됩니다. Rx only: 이 포트에서 수신된 프레임은 중간/목적지 포트에서 미러링됩니다. 전송된 프레임은 미러링되지 않습니다. Tx only: 이 포트에서 전송된 프레임은 중간/목적지 포트에서 미러링됩니다. 수신된 프레임은 미러링되지 않습니다.
Intermediate	중간 포트를 선택하세요. 이 체크박스는 원격 미러링을 위해 설계되었습니다. 중간 포트는 다른 스위치에 연결하기 위한 스위치 포트입니다. 참고: 중간 포트는 MAC 테이블 학습을 비활성화해야 합니다.
Destination	목적지 포트를 선택하세요. 이 체크박스는 미러 또는 원격 미러링을 위해 설계되었습니다. 목적지 포트는 소스 포트에서의 트래픽 복사본을 수신하는 스위치 포트입니다. 노트 1: 미러 모드에서는 해당 장치는 하나의 목적지 포트만 지원합니다. 노트 2: 목적지 포트는 MAC 테이블 학습을 비활성화해야 합니다.

Configuration Guideline for All Features

스위치가 원격 미러링 모드에서 실행되는 경우, 관리자는 다른 기능이 활성화되거나 비활성화되어 있는지 확인해야 합니다.

예를 들어, 관리자는 반사 포트의 MSTP를 비활성화하지 않습니다.
모든 모니터 트래픽은 반사 포트에서 차단됩니다.

권장 설정에 대해서는 도움말 페이지를 참조해 주세요.

Buttons

Apply : 클릭 시 변경사항을 적용합니다.
Apply&Save : 클릭 시 변경사항을 적용하고 저장합니다.
Reset : 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

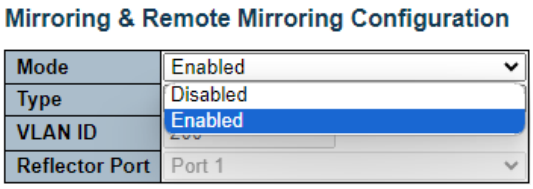
WEB 설정 예시

웹메뉴 Configuration>Mirroring

✓ **Mirroring & Remote Mirroring Configuration**

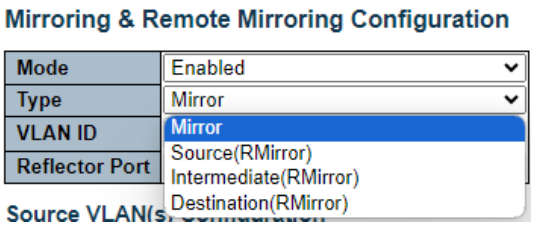
➢ ***Mode***

- Disabled | Enabled



➢ ***Type***

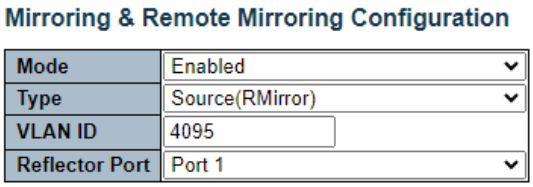
- Mirror | Source | Intermediate | Destination



➢ ***VLAN ID***

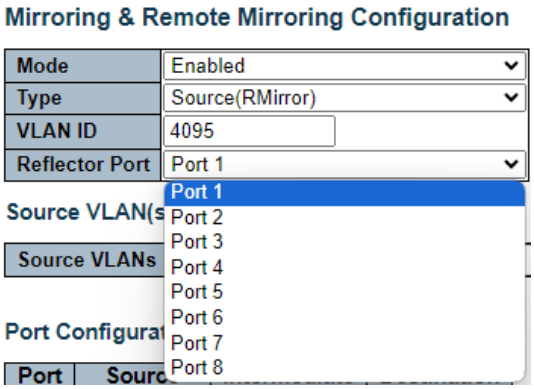
Source | Intermediate | Destination(RMirror) 타입만 설정이 가능합니다.

- 1~4095



➢ ***Reflector Port***

Source(RMirror) 타입만 설정이 가능합니다.

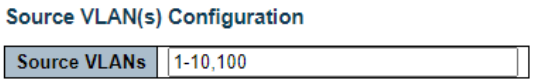


✓ Source VLAN(s) Configuration

➢ ***Source VLANs***

Mirror, Source(RMirror) 타입만 설정이 가능합니다.

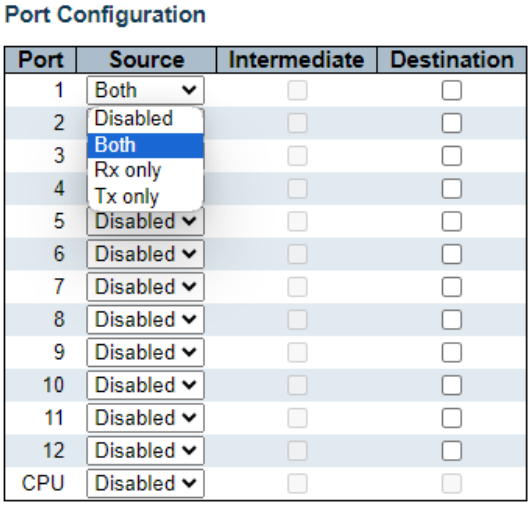
- 1~4095(설정하면 Port Configuration의 소스에 영향을 줍니다.)



✓ Port Configuration

➢ ***Source***

- Disabled | Both | Rx Only | Tx Only



➢ ***Intermediate***

Source | Intermediate | Destination(RMirror) 타입만 설정이 가능합니다.

Port Configuration

Port	Source	Intermediate	Destination
1	Disabled	☐	☐
2	Disabled	☐	☐
3	Disabled	☑	☐
4	Disabled	☑	☐
5	Disabled	☐	☐
6	Disabled	☐	☐
7	Disabled	☐	☐
8	Disabled	☐	☐
9	Disabled	☐	☐
10	Disabled	☐	☐
11	Disabled	☐	☐
12	Disabled	☐	☐
CPU	Disabled	☐	☐

➢ ***Destination***

Mirror, Destination(RMirror) 타입만 설정이 가능합니다.

Port Configuration

Port	Source	Intermediate	Destination
1	Disabled	☐	☐
2	Disabled	☐	☑
3	Disabled	☐	☐
4	Disabled	☐	☐
5	Disabled	☐	☐
6	Disabled	☐	☐
7	Disabled	☐	☐
8	Disabled	☐	☐
9	Disabled	☐	☐
10	Disabled	☐	☐
11	Disabled	☐	☐
12	Disabled	☐	☐
CPU	Disabled	☐	☐

CLI 설정 예시

✓ Mirroring & Remote Mirroring Configuration

➢ ***Mode***

- Disabled | Enabled

```
(config)# no monitor session 1
(config)# monitor session 1
```

➢ ***Type***

- Mirror(Default) | Source | Intermediate | Destination

➢ ***VLAN ID***

Source | Intermediate | Destination(RMirror) 타입만 설정이 가능합니다.

- 1~4095

➢ ***Reflector Port***

Source(RMirror) 타입만 설정이 가능합니다.

```
(config)# monitor session <session_number> [ destination { interface ( <port_type>
[ <di_list> ] ) | remote vlan <drvid> reflector-port <port_type> <rportid> } | source
{ interface ( <port_type> [ <si_list> ] ) [ both | rx | tx ] | remote vlan <srvid> | vlan
<source_vlan_list> | cpu [ both | rx | tx ] } | intermediate { interface ( <port_type>
[ <ii_list> ] ) | remote vlan <irvid> } ]

(config)# monitor session 1 destination remote vlan 4095 reflector-port
GigabitEthernet 1/1
(config)# monitor session 1 intermediate remote vlan 4095
(config)# monitor session 1 source remote vlan 4095
```

✓ **Source VLAN(s) Configuration**

➢ ***Source VLANs***

Mirror, Source(RMirror) 타입만 설정이 가능합니다.

- 1~4095(설정하면 Port Configuration의 소스에 영향을 줍니다.)

```
(config)# monitor session <session_number> [ destination { interface ( <port_type>
[ <di_list> ] ) | remote vlan <drvid> reflector-port <port_type> <rportid> } | source
{ interface ( <port_type> [ <si_list> ] ) [ both | rx | tx ] | remote vlan <srvid> | vlan
<source_vlan_list> | cpu [ both | rx | tx ] } | intermediate { interface ( <port_type>
[ <ii_list> ] ) | remote vlan <irvid> } ]

(config)# monitor session 1 source vlan 1-10
(config)# monitor session 1 source vlan 100
```

✓ **Port Configuration**

➢ ***Source***

- Disabled | Both | Rx Only | Tx Only

```
(config)# monitor session <session_number> [ destination { interface ( <port_type>
[ <di_list> ] ) | remote vlan <drvid> reflector-port <port_type> <rportid> } | source
{ interface ( <port_type> [ <si_list> ] ) [ both | rx | tx ] | remote vlan <srvid> | vlan
<source_vlan_list> | cpu [ both | rx | tx ] } | intermediate { interface ( <port_type>
[ <ii_list> ] ) | remote vlan <irvid> } ]

(config)# monitor session 1 source interface GigabitEthernet 1/1 both
(config)# monitor session 1 source interface GigabitEthernet 1/1 rx
(config)# monitor session 1 source interface GigabitEthernet 1/1 tx
(config)# monitor session 1 source cpu both
```

➢ ***Intermediate***

Source | Intermediate | Destination(RMirror) 타입만 설정이 가능합니다.

```
(config)# monitor session <session_number> [ destination { interface ( <port_type>
[ <di_list> ] ) | remote vlan <drvid> reflector-port <port_type> <rportid> } | source
{ interface ( <port_type> [ <si_list> ] ) [ both | rx | tx ] | remote vlan <srvid> | vlan
<source_vlan_list> | cpu [ both | rx | tx ] } | intermediate { interface ( <port_type>
[ <ii_list> ] ) | remote vlan <irvid> } ]

(config)# monitor session 1 intermediate interface GigabitEthernet 1/3-4
```

➢ ***Destination***

Mirror, Destination(RMirror) 타입만 설정이 가능합니다.

```
(config)# monitor session <session_number> [ destination { interface ( <port_type>
[ <di_list> ] ) | remote vlan <drvid> reflector-port <port_type> <rportid> } | source
{ interface ( <port_type> [ <si_list> ] ) [ both | rx | tx ] | remote vlan <srvid> | vlan
<source_vlan_list> | cpu [ both | rx | tx ] } | intermediate { interface ( <port_type>
[ <ii_list> ] ) | remote vlan <irvid> } ]

(config)# monitor session 1 destination interface GigabitEthernet 1/2
```

예시

✓ **Example**

➢ ***Mirror***

Source - CPU, Mirror Port - Gigabit Ethernet 1/1

Mirroring & Remote Mirroring Configuration

Mode	Enabled
Type	Mirror
VLAN ID	200
Reflector Port	Port 1

Source VLAN(s) Configuration

Source VLANs	

Port Configuration

Port	Source	Intermediate	Destination
1	Disabled	☐	☑
2	Disabled	☐	☐
3	Disabled	☐	☐
4	Disabled	☐	☐
5	Disabled	☐	☐
6	Disabled	☐	☐
7	Disabled	☐	☐
8	Disabled	☐	☐
9	Disabled	☐	☐
10	Disabled	☐	☐
11	Disabled	☐	☐
12	Disabled	☐	☐
CPU	Both	☐	☐

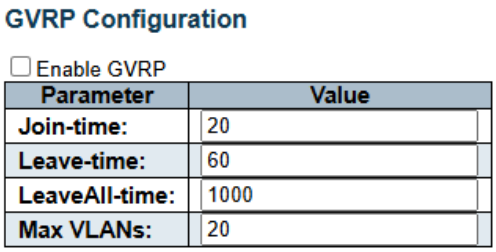
```
(config)# monitor session 1
(config)# monitor session 1 source cpu both
(config)# monitor session 1 destination interface GigabitEthernet 1/1
```

6.21. GVRP

6.21.1. Global config

웹메뉴 Configuration>GVRP>Global config

이 페이지에서는 모든 GVRP 활성화 포트에 일반적으로 적용되는 Global GVRP 구성 설정을 할 수 있습니다.



GVRP Configuration

용어	설명
Enable GVRP globally	체크박스에 있는 GVRP 활성화를 체크하고 저장 버튼을 눌러 GVRP 기능을 전역적으로 활성화합니다.
GVRP protocol timers	Join-time: 1-20cs 범위의 값, 즉 1cs는 1/100초입니다. 기본값은 20cs입니다. Leave-time: 60-300cs 범위의 값, 즉 1cs는 1/100초입니다. 기본값은 60cs입니다. LeaveAll-time: 1000-5000cs 범위의 값, 즉 1cs는 1/100초입니다. 기본값은 1000cs입니다.
Max number of VLANs	GVRP 가 활성화되면, GVRP 가 지원하는 최대 VLAN 수가 지정됩니다. 기본값은 20 입니다. 이 숫자는 GVRP 가 꺼져 있을 때만 변경할 수 있습니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

Refresh: 클릭 시 페이지를 새로고침 합니다. 로컬에서 변경된 사항은 취소됩니다.

WEB 설정 예시

웹메뉴 Configuration>GVRP>Global config

✓ **GVRP Configuration**

➢ ***Enable GVRP globally***

- Enabled | Disable

➢ ***GVRP protocol timers***

- Join-time(1~20csec)

- Leave-time(60~300csec)
- *Leave All-time(1000~5000csec)*

➢ ***Max number of VLANs***

- 1~4095(변경하려면 GVRP를 Disable하십시오.)

☑ Enable GVRP

Parameter	Value
Join-time:	20
Leave-time:	60
LeaveAll-time:	1000
Max VLANs:	20

CLI 설정 예시

✓ GVRP Configuration

➢ ***Enable GVRP globally***

- Enabled | Disable

```
(config)# gvrp
(config)# no gvrp
```

➢ ***GVRP protocol timers***

- Join-time(1~20csec)
- Leave-time(60~300csec)
- *Leave All-time(1000~5000csec)*

```
(config)# gvrp time { [ join-time <jointime> ] [ leave-time <leavetime> ] [ leave-all-time
<leavealltime> ] }
(config)# gvrp time join-time 20 leave-time 60 leave-all-time 1000
```

➢ ***Max number of VLANs***

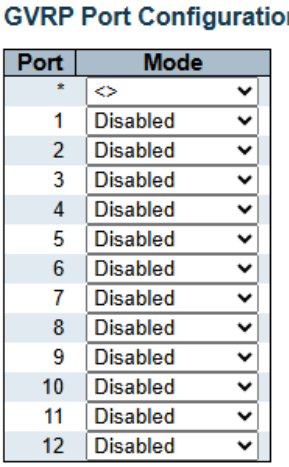
- 1~4095(변경하려면 GVRP를 Disable하십시오.)

```
(config)# gvrp max-vlans <maxvlans>
(config)# gvrp max-vlans 20
```

6.21.2. Port config

웹메뉴 Configuration>GVRP>Port config

이 페이지에서는 GVRP 작동을 위해 포트를 활성화하거나 비활성화할 수 있습니다.
이 설정은 GVRP가 전역적으로 구성되기 전이나 후에 수행할 수 있으며, 프로토콜 작동은 동일합니다.



GVRP Port Configuration

용어	설명
Mode	DDMI 모드 동작을 나타냅니다. 가능한 모드는 다음과 같습니다: Enabled DDMI 모드 동작을 활성화합니다. Disabled DDMI 모드 동작을 비활성화합니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.
Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.
Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

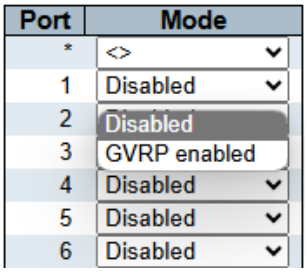
WEB 설정 예시

웹메뉴 Configuration>DDMI

✓ **GVRP Port Configuration**

➢ ***Mode***

- Disabled | GVRP Enabled



CLI 설정 예시

✓ GVRP Port Configuration

➢ *Mode*

- Disabled | GVRP Enabled

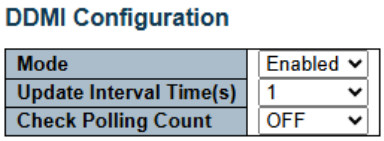
```
(config)# interface ( <port_type> [ <plist> ] )
(config)# interface GigabitEthernet 1/1

(config-if)# gvrp
```

6.22. DDMI

6.22.1. DDMI Configuration

웹메뉴 Configuration>DDMI

DDMI를 이 페이지에서 구성합니다.



DDMI Configuration

용어	설명
Mode	DDMI 모드 동작을 나타냅니다. 가능한 모드는 다음과 같습니다: Enabled DDMI 모드 동작을 활성화합니다. Disabled DDMI 모드 동작을 비활성화합니다.
Update Interval Time(s)	DDMI 의 업데이트 시간 간격입니다. 단위는 초이며, 최소 1 초에서 최대 12 초까지 설정할 수 있습니다.
Check Polling Count	DDMI 간격의 Polling 횟수입니다. 이것은 DDMI 정보를 자동으로 업데이트하는 횟수입니다. Polling 횟수는 OFF 상태이며 최소 1, 최대 10 까지 설정할 수 있습니다. 기본 값은 OFF 입니다.

Buttons

Apply: 클릭 시 변경사항을 적용합니다.

Apply&Save: 클릭 시 변경사항을 적용하고 저장합니다.

Reset: 클릭 시 변경사항을 취소하고 이전 값으로 되돌립니다.

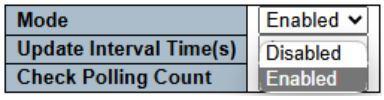
WEB 설정 예시

웹메뉴 Configuration>DDMI

✓ **DDMI Configuration**

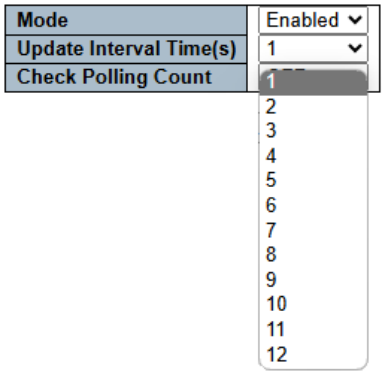
➢ ***Mode***

- Enabled | Disabled



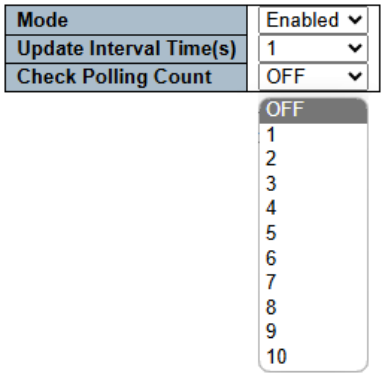
➢ ***Update Interval Time(s)***

- 1~12



➢ ***Check Polling Count***

- OFF | 1~10



CLI 설정 예시

✓ DDMI Configuration

➢ ***Mode***

- Enabled | Disabled

```
(config)# ddmi
(config)# no ddmi
```

➢ ***Update Interval Time(s)***

- 1~12

```
(config)# ddmi update-interval <interval_time>
(config)# ddmi update-interval 1
```

➢ ***Check Polling Count***

- 0~10 (0:OFF)

```
(config)# ddmi check-polling-count <polling_cnt>
(config)# ddmi check-polling-count 0
(config)# ddmi check-polling-count 10
```

6.22.2. DDMI Monitor

6.22.2.1. Overview

웹메뉴 Configuration>DDMI>Overview

이 페이지에서 DDMI(Digital Diagnostic Monitoring Interface) 개요 정보를 표시합니다.

DDMI Overview

Port	Vendor	Part Number	Serial Number	Revision	Data Code	Transceiver
5	-	-	-	-	-	-
6	-	-	-	-	-	-
7	-	-	-	-	-	-
8	-	-	-	-	-	-

DDMI Overview

용어	설명
Port	DDMI 포트입니다. (포트 번호를 누르면 Detail 페이지로 갑니다.)
Vendor	SFP 공급 업체의 이름을 나타냅니다.
Part Number	SFP 공급 업체가 제공한 부품 번호를 나타냅니다.
Serial Number	공급 업체가 제공한 일련 번호를 나타냅니다.
Revision	공급 업체가 제공한 부품 번호의 개정 수준을 나타냅니다.
Data Code	공급 업체의 제조 일련 번호를 나타냅니다.
Transeiver	트랜시버의 호환성을 나타냅니다.

WEB 확인 예시

웹메뉴 Configuration>DDMI>Overview

✓ **DDMI Overview**

DDMI Overview

Port	Vendor	Part Number	Serial Number	Revision	Data Code	Transceiver
5	Soltech	GP-3148-L2CD	S2005136619	1.0	2020-05-19	2G5
6	OEM	SFP-LX	S1231240320176	A0	2014-03-09	1000BASE_LX
7	soltech	SFP-10G-LR	S1804239531	A	2018-05-07	10G
8	OEM	SFP-SM	S0131241120202	A0	2014-11-12	100BASE_LX

CLI 확인 예시

✓ **DDMI Overview**

```
# show interface ( <port_type> [ <plist> ] ) transceiver
# show interface 10GigabitEthernet 1/1-4 transceiver

10GigabitEthernet 1/1
```

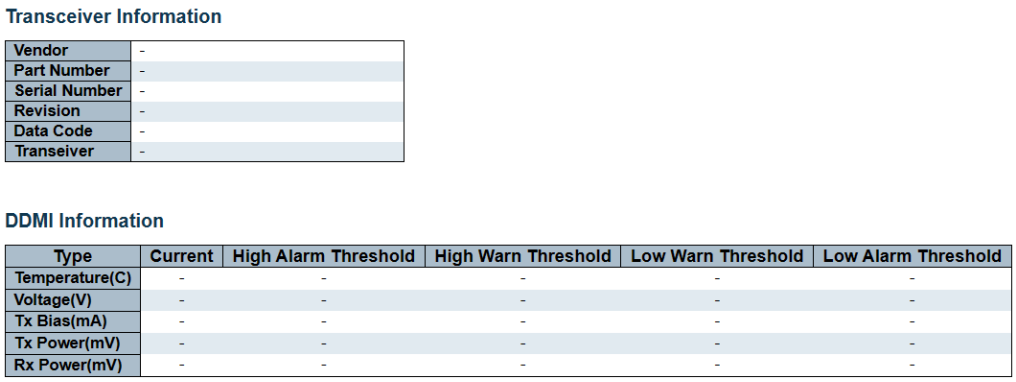
```
------------------------------
Tranceiver Information
============================================================
Vendor             : Soltech
Part Number        : GP-3148-L2CD
Serial Number      : S2005136619
Revision           : 1.0
Data Code          : 2020-05-19
Transceiver        : 2G5

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
============================================================
             current   High Alarm   High Warn    Low Warn      Low Alarm
                        Threshold    Threshold    Threshold     Threshold
-------------  --------  ----------   ----------   ----------    --------

Temperature(C)
Voltage(V)
Tx Bias(mA)
Tx Power(mW)
Rx Power(mW)


10GigabitEthernet 1/2
------------------------------
Tranceiver Information
============================================================
Vendor             : OEM
Part Number        : SFP-LX
Serial Number      : S1231240320176
Revision           : A0
Data Code          : 2014-03-09
Transceiver        : 1000BASE_LX

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
============================================================

% SFP module doesn't support DDMI


10GigabitEthernet 1/3
------------------------------
Tranceiver Information
============================================================
Vendor             : soltech
Part Number        : SFP-10G-LR
Serial Number      : S1804239531
Revision           : A
Data Code          : 2018-05-07
Transceiver        : 10G

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
```

```
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
============================================================

              current   High Alarm   High Warn    Low Warn      Low Alarm
                          Threshold   Threshold    Threshold      Threshold
-------------  --------  ----------   ----------   ----------    --------
Temperature(C)
Voltage(V)
Tx Bias(mA)
Tx Power(mW)
Rx Power(mW)


10GigabitEthernet 1/4
-----------------------------
Tranceiver Information
============================================================
Vendor              : OEM
Part Number         : SFP-SM
Serial Number       : S0131241120202
Revision            : A0
Data Code           : 2014-11-12
Transceiver         : 100BASE_LX

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.

Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.

============================================================

% SFP module doesn't support DDMI
```

6.22.2.2. Detailed

웹메뉴 Configuration>DDMI>Detailed

DDMI(Digital Diagnostic Monitoring Interface) 상세 정보를 이 페이지에서 표시합니다.



Transceiver Information

Vendor	-
Part Number	-
Serial Number	-
Revision	-
Data Code	-
Transeiver	-

DDMI Information

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	-	-	-	-	-
Voltage(V)	-	-	-	-	-
Tx Bias(mA)	-	-	-	-	-
Tx Power(mV)	-	-	-	-	-
Rx Power(mV)	-	-	-	-	-

Transceiver Information

DDMI의 상세 정보를 이 페이지에서 표시합니다.

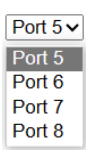
용어	설명
Vendor	SFP 공급업체 이름을 나타냅니다.
Part Number	SFP 공급업체가 제공한 부품 번호를 나타냅니다.
Serial Number	공급업체가 제공한 일련번호입니다.
Revision	제조업체가 제공한 부품 번호의 개정 수준을 나타냅니다.
Data Code	제조업체의 제조일자 코드를 나타냅니다.
Transeiver	광모듈의 호환성을 나타냅니다.

DDMI Information

이 페이지에서 DDMI 정보를 표시합니다.

용어	설명
Current	현재 온도, 전압, 송신 바이어스, 송신 출력 및 수신 출력의 값입니다.
High Alarm Threshold	온도, 전압, 송신 바이어스, 송신 출력 및 수신 출력의 심각한 경보입니다.
High Warn Threshold	온도, 전압, 송신 바이어스, 송신 출력 및 수신 출력의 고 경보 임계 값입니다.
Low Warn Threshold	온도, 전압, 송신 바이어스, 송신 출력 및 수신 출력의 저 경보 임계 값입니다.
Low Alarm Threshold	온도, 전압, 송신 바이어스, 송신 출력 및 수신 출력의 심각한 경보입니다.

Buttons



: 포트 번호를 선택하세요. 선택한 포트의 상세 정보 페이지가 표시됩니다.

Auto-refresh : 이 상자를 체크하면 페이지가 자동으로 새로고침됩니다.

Refresh: 페이지를 즉시 새로고침하려면 클릭하세요.

WEB 확인 예시

웹메뉴 Configuration>DDMI>Detailed

✓ **Transceiver Information**

✓ **DDMI Information**

Transceiver Information

Vendor	Soltech
Part Number	GP-3148-L2CD
Serial Number	S2005136619
Revision	1.0
Data Code	2020-05-19
Transeiver	2G5

DDMI Information

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)					
Voltage(V)					
Tx Bias(mA)					
Tx Power(mV)					
Rx Power(mV)					

CLI 확인 예시

✓ **Transceiver Information**

✓ **DDMI Information**

```
# show interface ( <port_type> [ <plist> ] ) transceiver
# show interface 10GigabitEthernet 1/1-4 transceiver

10GigabitEthernet 1/1
------------------------------
Tranceiver Information
============================================================
Vendor              : Soltech
Part Number         : GP-3148-L2CD
Serial Number       : S2005136619
Revision            : 1.0
Data Code           : 2020-05-19
Transceiver         : 2G5

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
============================================================
                current   High Alarm   High Warn    Low Warn      Low Alarm
                          Threshold    Threshold    Threshold     Threshold
-------------  --------  ----------  ----------  ----------   --------

Temperature(C)
Voltage(V)
Tx Bias(mA)
Tx Power(mW)
```

```
Rx Power(mW)


10GigabitEthernet 1/2
------------------------------
Tranceiver Information
============================================================
Vendor              : OEM
Part Number         : SFP-LX
Serial Number       : S1231240320176
Revision            : A0
Data Code           : 2014-03-09
Transceiver         : 1000BASE_LX

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
============================================================

% SFP module doesn't support DDMI


10GigabitEthernet 1/3
------------------------------
Tranceiver Information
============================================================
Vendor              : soltech
Part Number         : SFP-10G-LR
Serial Number       : S1804239531
Revision            : A
Data Code           : 2018-05-07
Transceiver         : 10G

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
============================================================

              current   High Alarm   High Warn    Low Warn      Low Alarm
                          Threshold    Threshold     Threshold       Threshold
-------------  --------  ----------   ----------   ----------    --------
Temperature(C)
Voltage(V)
Tx Bias(mA)
Tx Power(mW)
Rx Power(mW)


10GigabitEthernet 1/4
------------------------------
Tranceiver Information
============================================================
Vendor              : OEM
Part Number         : SFP-SM
Serial Number       : S0131241120202
Revision            : A0
Data Code           : 2014-11-12
```

```
Transceiver          : 100BASE_LX

DDMI Information

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.

Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.

============================================================

% SFP module doesn't support DDMI
```

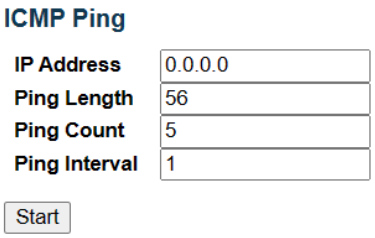
7. 스위치 상태 진단

7.1. Diagnostics

7.1.1. Ping

웹메뉴 Diagnostics>Ping

이 페이지는 ICMP PING 패킷을 발송하여 IP 연결 문제를 해결할 수 있게 해줍니다.



ICMP Ping

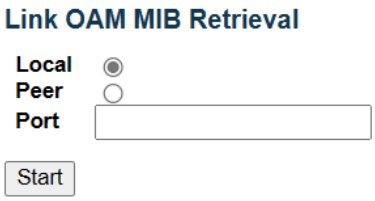
'시작'을 누르면 ICMP 패킷이 전송되고, 응답을 받으면 순서 번호와 왕복 시간이 표시됩니다. ICMP ECHO_REPLY 타입의 IP 패킷 안에 수신된 데이터의 양은 항상 요청된 데이터 공간(ICMP 헤더)보다 8 바이트 더 많습니다. 모든 패킷에 대한 응답을 받거나 타임아웃이 발생할 때까지 페이지가 자동으로 새로고침됩니다.

7.1.2. Link OAM

7.1.2.1. MIB Retrieval

웹메뉴 Diagnostics>Link OAM>MIB Retrieval

이 페이지는 특정 포트에서 로컬 또는 원격 OAM MIB 변수 데이터를 검색할 수 있게 해줍니다.



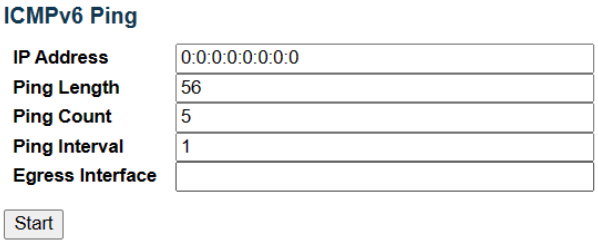
Link OAM MIB Retrieval

관심 있는 내용을 검색하기 위해 적절한 라디오 버튼을 선택하고 스위치의 포트 번호를 입력하세요. 내용을 검색하려면 '시작'을 클릭하세요. 다른 관심 있는 내용을 검색하려면 '새로운 검색'을 클릭하세요.

7.1.3. Ping6

웹메뉴 Diagnostics>Ping6

이 페이지는 ICMPv6 PING 패킷을 발송하여 IPv6 연결 문제를 해결할 수 있게 해줍니다.



ICMPv6 Ping

'시작'을 누르면 ICMPv6 패킷이 전송되고, 응답을 받으면 순서 번호와 왕복 시간이 표시됩니다. 모든 패킷에 대한 응답을 받거나 타임아웃이 발생할 때까지 페이지가 자동으로 새로고침됩니다.

발송된 ICMP 패킷의 다음과 같은 속성을 설정할 수 있습니다:

용어	설명
IP Address	목적지 IP 주소.
Ping Length	ICMP 패킷의 페이로드 크기. 값은 2 바이트에서 1452 바이트까지입니다.
Ping Count	ICMP 패킷의 개수. 값은 1 번에서 60 번까지입니다.
Ping Interval	ICMP 패킷의 간격. 값은 0 초에서 30 초까지입니다.
Egress Interface (Only for IPv6)	ICMP 패킷이 나가는 특정 출구 IPv6 인터페이스의 VLAN ID (VID). VID 는 1 에서 4094 까지이며, 해당 IPv6 인터페이스가 유효할 때만 적용됩니다. 출구 인터페이스가 주어지지 않으면, PING6 은 목적지에 가장 적합한 인터페이스를 찾습니다. 루프백 주소의 경우 출구 인터페이스를 지정하지 마세요. 링크 로컬 또는 멀티캐스트 주소의 경우 출구 인터페이스를 지정하세요.

Buttons

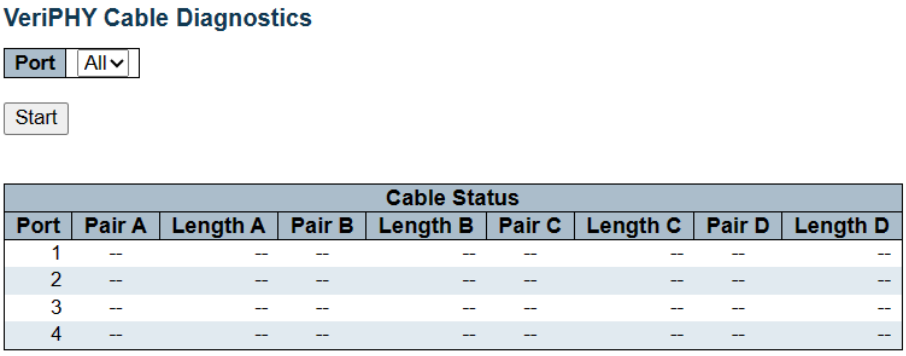
Start: ICMP 패킷을 전송하기 시작합니다.

New Ping: 새로운 PING으로 다시 시작하려면 클릭하세요.

7.1.4. VeriPHY

웹메뉴 Diagnostics>VeriPHY

이 페이지는 10/100 및 1G 구리 포트에 대한 VeriPHY 케이블 진단을 실행하는 데 사용됩니다.



VeriPHY Cable Diagnostics

진단을 실행하려면 '시작'을 누르세요. 이 작업은 약 5초 정도 걸립니다. 모든 포트를 선택하면 약 15초 정도 걸릴 수 있습니다. 완료되면 페이지가 자동으로 새로고침되고, 케이블 상태 테이블에서 케이블 진단 결과를 확인할 수 있습니다. VeriPHY는 7 - 140 미터 길이의 케이블에 대해서만 정확하다는 점을 유의하세요.

VeriPHY를 실행하는 동안 10 및 100 Mbps 포트는 연결이 끊어집니다. 따라서 10 또는 100 Mbps 관리 포트에서 VeriPHY를 실행하면 VeriPHY가 완료될 때까지 스위치가 응답하지 않게 됩니다.

용어	설명	
Port	VeriPHY 케이블 진단을 요청하는 포트 번호입니다.	
Cable Status	**Port**	포트 번호입니다.
	Pair	케이블 Pair 의 상태입니다. OK - 케이블이 올바르게 종결되어 있는 상태입니다. Open - 케이블이 연결이 되지 않은 상태입니다. Short – 케이블이 짧은 상태로 연결된 상태입니다. Short A - Pair A 에 대한 교차 단락 상태입니다. Short B - Pair B 에 대한 교차 단락 상태입니다. Short C - Pair C 에 대한 교차 단락 상태입니다. Short D – Pair D 에 대한 교차 단락 상태입니다. Cross A - Pair A 와의 비정상적인 교차 결합 상태입니다. Cross B - Pair B 와의 비정상적인 교차 결합 상태입니다. Cross C - Pair C 와의 비정상적인 교차 결합 상태입니다. Cross D - Pair D 와의 비정상적인 교차 결합 상태입니다.
	Length	케이블의 길이(미터 단위)입니다. 분석 가능 거리는 3미터입니다.

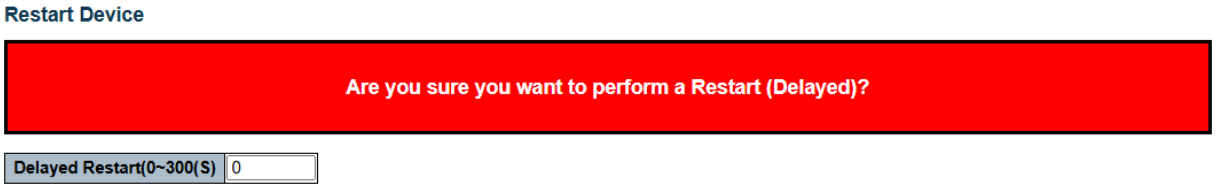
8. 스위치 유지

8.1. Maintenance

8.1.1. Restart Device

웹메뉴 Maintenance>Restart Device

이 페이지에서 스위치를 재시작 할 수 있습니다. 재시작 후 스위치는 정상적으로 부팅됩니다.
재시작시 Startup-config를 불러오게 됩니다. (저장하지 않고 재시작시 설정이 없어집니다.)



용어	설명
Delayed Restart	지정된 대기 시간이 지난 후 재시작이 시작됩니다. (0 초에서 300 초까지 지연 시간을 설정할 수 있습니다. 0: 즉시 재시작)

Buttons

Restart : 클릭시 장비를 재시작합니다.

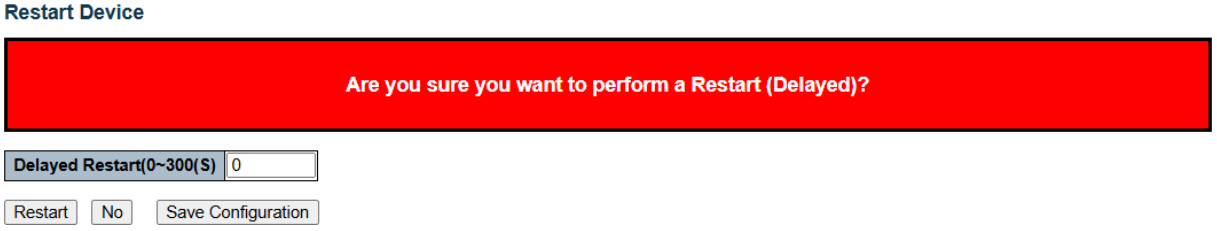
No : 클릭시 장비 재시작을 하지않고 첫화면(Port State)으로 갑니다.

Save Configuration : 이 명령어는 현재 실행 중인 설정을 시작 설정으로 복사하여, 다음 재부팅 시 현재 활성화된 설정이 사용되도록 보장합니다.

WEB 실행 예시

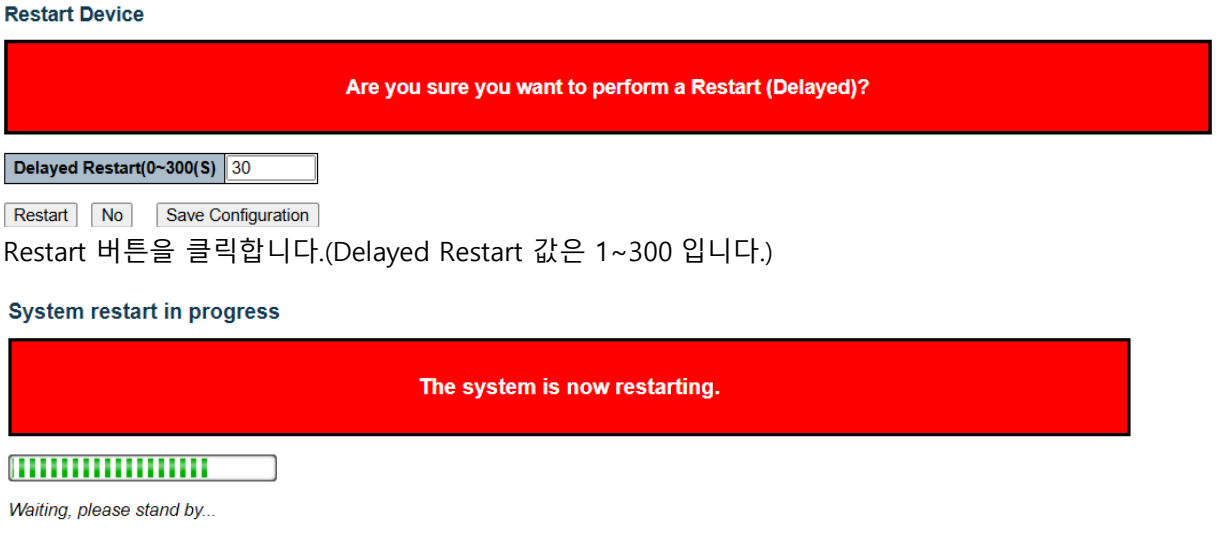
웹메뉴 Maintenance>Restart Device

1. 즉시 재시작



Restart 버튼을 클릭합니다.(Delayed Restart 값은 0 입니다.)

2. 딜레이 후 재시작



Restart 버튼을 클릭합니다.(Delayed Restart 값은 1~300 입니다.)

수 분을 기다리면 로그인 화면이 출력되며 재시작이 완료됩니다.

CLI 실행 예시

✓ Restart Device(Load Startup-Config and Restart)

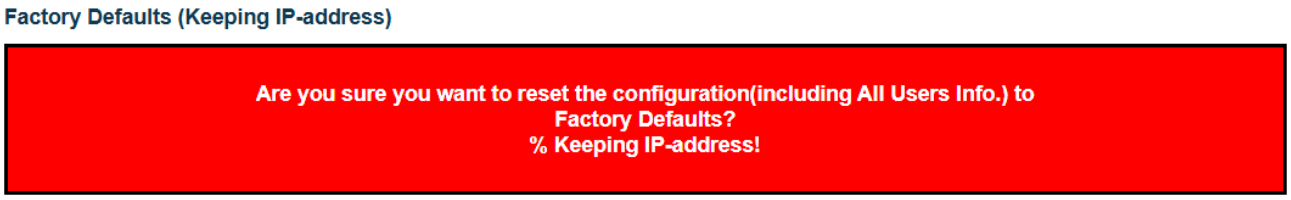
```
# reload { { { cold [ <delay_sec> | now ]
# reload cold
# reload cold now
# reload cold 300

% Cold reload in progress, please stand by.
################################################
###: Start SOLTECH_boot_v1_1                ###
################################################
###: CPU    Test.....................PASS!
###: TCAM   Test.....................PASS!
###: DRAM   Test.....................PASS!
###: Flash Test.....................PASS!
###: Loading flash: IMG.bin .....
###: Verifying firmware image integrity.....
###: IMG-KEY:7F80C36F18AA01DA22999FE8EDE2B57B
            AAD7096D8EC4D49840B026A19C9766E4
###: CAL-KEY:7F80C36F18AA01DA22999FE8EDE2B57B
            AAD7096D8EC4D49840B026A19C9766E4
###: SHA256 hash verified: SUCCESS !!!
###: Start Decompress Image .....
###: Please wait system up .....


###: Dev MAC addr: [00:21:6D:00:00:00]
###: Dev-Name:모델명

###: Board Serial: 모델 시리얼
###: Board Name: 모델명
###: Port Info: Port:12[UTP:8(PoE:8),SFP:4]

###: Press ENTER to get started
```

8.1.2. Factory Defaults

WEB MENU Maintenance>Factory Defaults

이 페이지에서 스위치의 구성을 재설정할 수 있습니다. IP 구성만 유지됩니다.

새로운 구성은 즉시 적용되며, 재시작 하지 않습니다.



Buttons

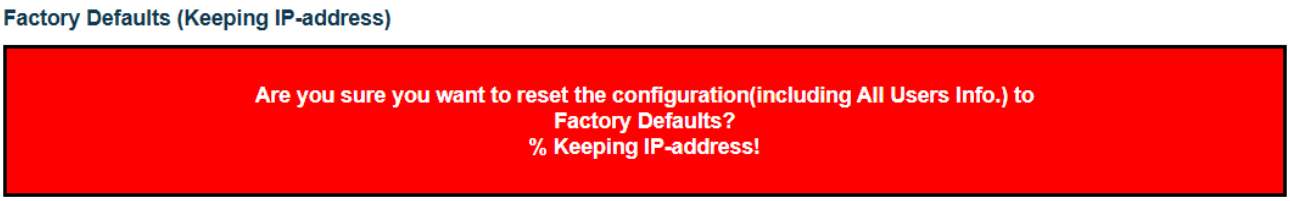
FactoryDefaults & Save : 클릭하여 구성을 공장 기본값으로 재설정합니다. (IP 설정은 유지됩니다)

FactoryDefaults : 클릭하여 구성을 공장 기본값으로 재설정합니다. (구성을 플래시에 저장하지 않음!!)

☐ Keeping IP-address : 체크박스를 선택하면 IP 주소는 유지한 채로 공장 초기화가 됩니다.

WEB 실행 예시

WEB MENU Maintenance>Factory Defaults



✓ **Factory Defaults**

➢ ***Factory Defaults & Save***

웹에서 Factory Defaults를 실행하면 IP 구성을 유지한 상태로 나머지 설정들이 초기화 됩니다.

버튼을 클릭하면 현재 저장되어 있는 Startup-config가 동시에 초기화 됩니다. (IP는 현재 IP로 유지됨)

➢ ***Factory Defaults***

웹에서 Factory Defaults를 실행하면 IP 구성을 유지한 상태로 나머지 설정들이 초기화 됩니다.

버튼을 클릭하면 현재 저장되어 있는 Startup-config는 유지됩니다. (재시작시 Startup-Config를 불러옴)

➢ ***Keeping IP-address***

웹에서 Factory Defaults를 실행할 때 IP구성을 포함할 것인지를 설정합니다. 체크를 해제하고 초기화를 진행하면 완전한 공장초기화가 되며, 초기 IP인 192.168.10.100으로 초기화 됩니다.

CLI 실행 예시

✓ Factory Defaults

➢ ***Defaults***

CLI에서 Defaults를 실행하면 IP설정을 포함하여 초기화 됩니다.(Startup-config초기화)

```
# reload defaults

% Reloading defaults (Update startup-config). Please stand by.
Config Factory-Default applied! (Update startup-confg, By CLI)

###: Press ENTER to get started
```

➢ ***Defaults keep-ip***

CLI에서 Defaults를 실행하면 IP설정을 제외하여 초기화 됩니다.

(Startup-config는 IP가 덮어쓰기 됩니다.)

```
# reload defaults keep-ip

% Reloading defaults, attempting to keep VLAN 1 IP address (Update startup-config).
Please stand by.
Config Factory-Default applied! (Update startup-confg, Keeping IP-addr, By CLI)

###: Press ENTER to get started
```

➢ ***Defaults no-save***

CLI에서 Defaults를 실행하면 IP설정을 포함하여 초기화 됩니다.

(Startup-config는 기존대로 유지됩니다. 보안 모델은 초기 패스워드를 Flash에 저장하지 마세요.)

설정 후 재시작 시 기존에 저장했던 Startup-config를 그대로 불러옵니다.

```
# reload defaults-no-save

% Reloading defaults . Please stand by.
Config Factory-Default applied! (By CLI)
###: Press ENTER to get started

#: Please input a new admin password:**********
#: Please input the new password AGAIN:**********
#: Save admin password to flash now ? (yes/no):no

#
```

➢ ***Defaults no-save keep-ip***

CLI에서 Defaults를 실행하면 IP설정을 제외하여 초기화 됩니다.

(Startup-config는 기존대로 유지됩니다. 보안 모델은 초기 패스워드를 Flash에 저장하지 마세요.)

설정 후 재시작 시 기존에 저장했던 Startup-config를 그대로 불러옵니다.

```
# reload defaults-no-save keep-ip

% Reloading defaults, attempting to keep VLAN 1 IP address . Please stand by.

Config Factory-Default applied! (By CLI)
###: Press ENTER to get started


#: Please input a new admin password:**********
#: Please input the new password AGAIN:**********
#: Save admin password to flash now ? (yes/no):no

#
```

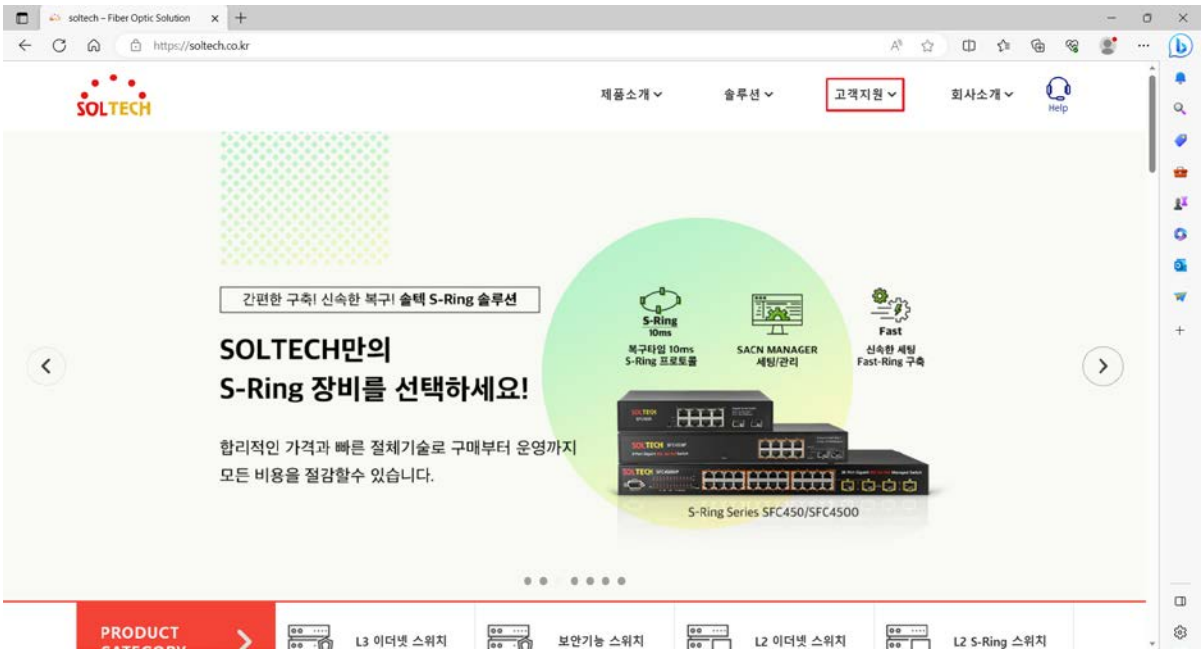
8.1.3. Software

8.1.3.1. Firmware Download

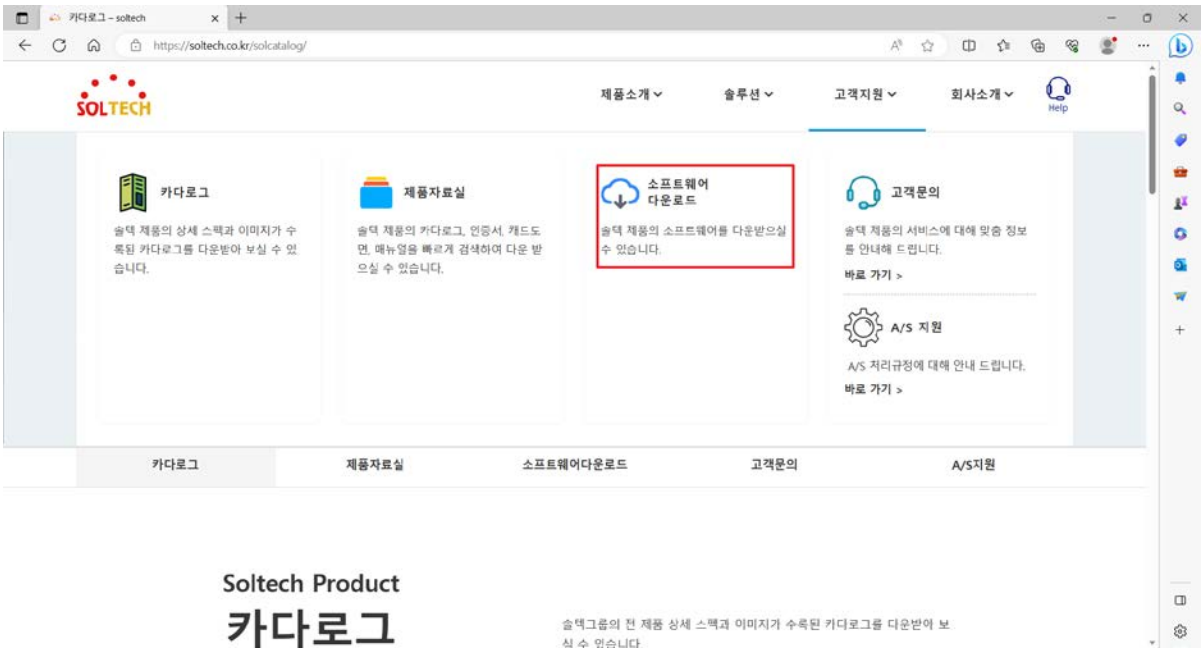
이 페이지에서는 장비의 펌웨어를 다운로드 받을 수 있는 방법에 대하여 설명합니다.

회사 홈페이지 www.soltech.co.kr로 접속합니다.

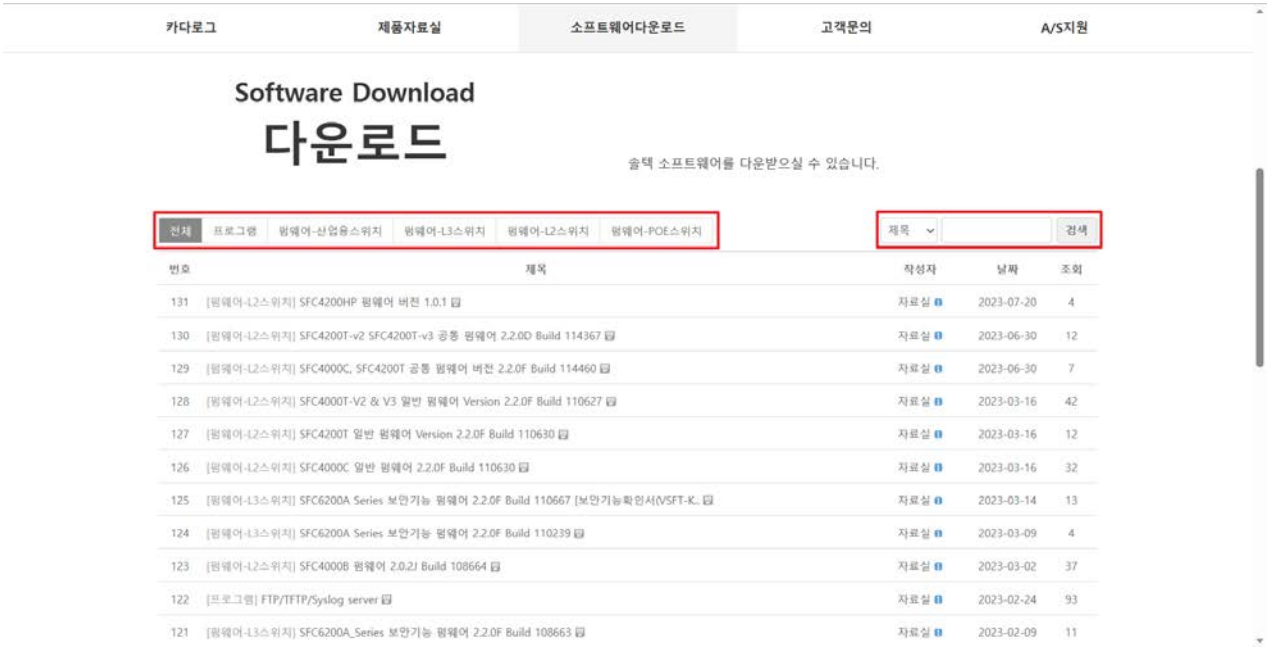
고객지원>소프트웨어 다운로드>제품명 검색 또는 제품군을 클릭하세요.



고객지원을 클릭



소프트웨어 다운로드 클릭



제품군 분류를 이용하거나 제품명을 검색하여 해당 제품의 최신 펌웨어를 받으실 수 있습니다.

8.1.3.2. Upload

WEB MENU Maintenance>Software>Upload

이 페이지는 스위치를 제어하는 펌웨어의 업데이트를 합니다.

Buttons

파일 선택: 이 버튼을 클릭하면 업로드할 소프트웨어 이미지를 찾을 수 있습니다.

Upload: 이 버튼을 클릭하여 선택한 소프트웨어 이미지를 업로드하세요.

Disable Automatic Restart After Updates : 이 버튼이 체크되어 있으면, 업데이트 후 시스템이 자동으로 재시작하지 않습니다. (업로드만 진행되며, 펌웨어가 적용되려면 장비 재시작이 필요합니다.)

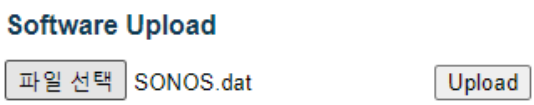
소프트웨어 이미지가 업로드 된 후, 페이지에서 펌웨어 업데이트가 시작되었다고 알립니다. 몇 분 후에 펌웨어가 업데이트되고 스위치가 재시작 됩니다.

주의: 이 시점에서 장치를 재시작하거나 전원을 끄지 마십시오. 스위치가 이후에 작동하지 않을 수 있습니다.

경고: 펌웨어가 업데이트되는 동안 웹 접속은 비활성화됩니다. 펌웨어 업데이트가 진행 중인 동안 전면 LED 는 초당 10Hz 의 주기로 녹색 l 꺼짐으로 깜박입니다. 이 시기에 장치를 재시작하거나 전원을 끄지 마십시오. 그렇게 할 경우 스위치가 이후에 작동하지 않을 수 있습니다.

WEB 실행 예시

✓ **Software Upload**



파일 선택을 클릭 후 이미지가 있는 폴더를 찾아 선택하면 위와 같이 파일명이 표시됩니다.

이 때 필요한 파일은 확장자 (.dat)파일입니다. 업로드 버튼을 클릭하면 업데이트가 진행됩니다.

Upload 를 진행하면 Upload 이후 장비가 자동으로 재시작 합니다. (기본값)

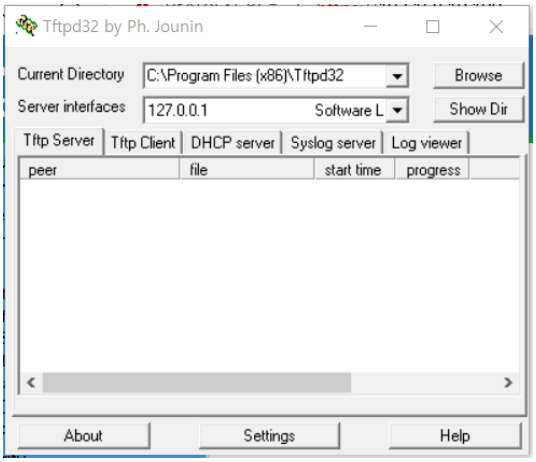
장비가 자동으로 재시작 하는 것을 방지하려면 Disable Automatic Restart After Updates 를 선택하시면 됩니다. (업로드만 진행되며, 펌웨어가 적용되려면 장비 재시작이 필요함.)

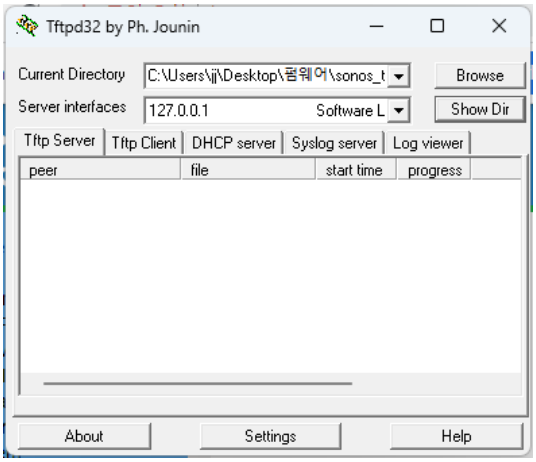
CLI 실행 예시

콘솔(TFTP 활용)을 이용한 소프트웨어 업그레이드 방법입니다.

✓ Software Upload

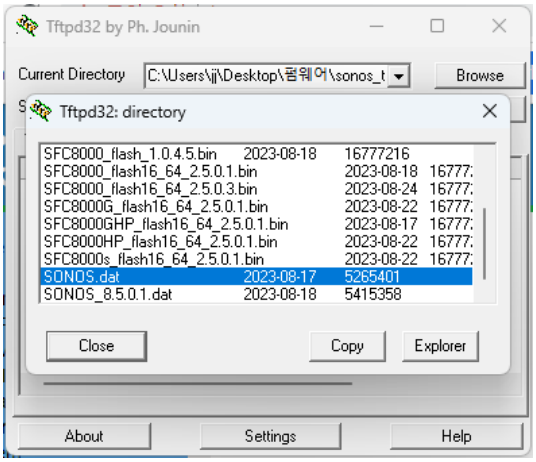
1. Tftpd32 프로그램을 실행한다.





2. Browse 를 클릭하여 업데이트 하고자 하는 파일 위치를 찾습니다.

3. Show Dir 을 클릭하여 파일을 선택하고 Copy 를 클릭 후 Close 를 클릭하여 창을 닫습니다.



4. Console 창으로 돌아와 다음을 입력합니다.

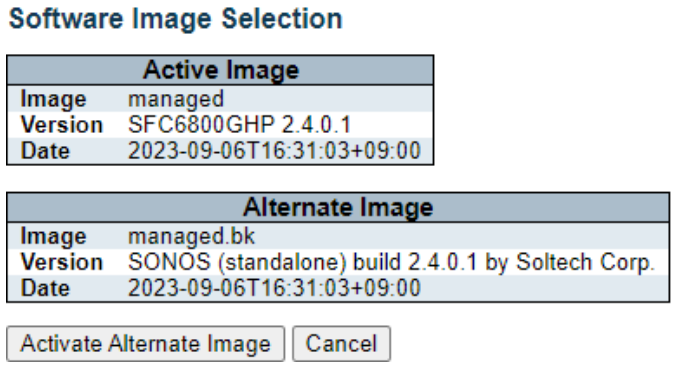
```
# firmware upgrade <url_file> [ forced ] [ not-reboot ]
# firmware upgrade tftp://192.168.10.130/SONOS.dat
# firmware upgrade tftp://192.168.10.130/SONOS.dat not-reboot

Downloaded "SONOS.dat", 5799906 bytes
TFTP Host:192.168.10.130 Upgrade Start (Download:5799906 Bytes)
###: Verifying firmware image integrity .....
IMG-KEY:3D5801C74658E0DA4C0AEDC28ABCF896D0C46331A1843DC7A930787659122861
CAL-KEY:3D5801C74658E0DA4C0AEDC28ABCF896D0C46331A1843DC7A930787659122861
SHA256 hash verified: SUCCESS
```

8.1.3.3. Image Select

WEB MENU Maintenance>Software>Image Select

이 페이지는 장치에 있는 활성 및 대체(백업) 펌웨어 이미지에 대한 정보를 제공하며, 대체 이미지로 되돌릴 수 있도록 합니다.

웹 페이지는 활성 및 대체 펌웨어 이미지에 대한 정보를 포함한 두 개의 테이블을 표시합니다.



참고:

1. 활성 펌웨어 이미지가 대체 이미지인 경우 "활성 이미지" 테이블만 표시됩니다. 이 경우 "대체 이미지 활성화" 버튼도 비활성화됩니다.
2. 대체 이미지가 활성 상태인 경우 (주 이미지의 손상 또는 수동 개입으로 인해), 장치에 새 펌웨어 이미지를 업로드하면 자동으로 주 이미지 슬롯을 사용하여 활성화됩니다.
3. 펌웨어 버전 및 날짜 정보는 오래된 펌웨어 버전의 경우 비어 있을 수 있습니다. 이는 오류를 나타내는 것이 아닙니다.

Software Image Selection

용어	설명
Image	마지막으로 업데이트된 시점의 펌웨어 이미지 파일 이름입니다.
Version	펌웨어 이미지 파일의 버전입니다.
Date	펌웨어가 생성된 날짜입니다.

Buttons

Activate Alternate Image :대체 이미지를 사용하려면 클릭하십시오. 시스템 상태에 따라 이 버튼이 비활성화 될 수 있습니다.

Cancel : 백업 이미지의 활성화를 취소합니다. 이 페이지를 벗어납니다.

WEB 실행 예시

WEB MENU Maintenance>Software>Image Select

Software Image Selection

Active Image	
Image	managed
Version	SFC6800GHP 2.4.0.1
Date	2023-09-06T16:31:03+09:00

Alternate Image	
Image	managed.bk
Version	SONOS (standalone) build 2.4.0.1 by Soltech Corp.
Date	2023-09-06T16:31:03+09:00

Activate Alternate Image Cancel

Activate Alternate Image: 을 클릭하면 대체 이미지가 활성화됩니다. 기존 이미지에 문제가 발생한 경우 사용하세요.

System restart in progress

The system is now restarting.

Waiting, please stand by...

CLI 실행 예시

✓ Software Image Selection

```
# firmware swap

... Erase from 0x40fd0000-0x40fdffff: .
... Program from 0x8ffdfffc-0x8ffefffc to 0x40fd0000: .
... Program from 0x8ffe0006-0x8ffe0008 to 0x40fd000a: .
Alternate image activated, now rebooting.
#
```

8.1.4. Configuration

스위치는 CLI 형식의 여러 텍스트 파일에 구성 정보를 저장합니다. 이 파일들은 가상(RAM 기반) 파일이거나 스위치의 플래시에 저장될 수 있습니다.

1. running-config: 스위치에서 현재 활성화된 구성을 나타내는 가상 파일입니다. 이 파일은 휘발성입니다.

2. startup-config: 스위치의 부팅 시에 읽히는 시작 구성입니다. 이 파일이 부팅 시에 존재하지 않으면 스위치는 기본 구성으로 시작됩니다.

3. default-config: 공급 업체별 구성을 담고 있는 읽기 전용 파일입니다. 이 파일은 시스템을 기본 설정으로 복원할 때 읽힙니다.

최대 31개의 다른 파일: 주로 구성 백업이나 대체 구성에 사용되는 파일입니다.

8.1.4.1. CLI dir

이 페이지에서는 CLI에서 현재 Flash에 저장되어 있는 Config 파일을 보는 방법을 소개합니다.

WEB의 경우 해당기능이 이미 필요한 페이지에 구현되어 있습니다.

CLI 실행 예시

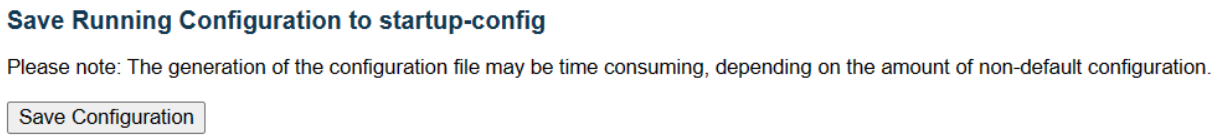
✓ **Dir Command in CLI**

```
# dir
Directory of flash:
    r- 1970-01-01 00:00:00      316 default-config
    rw 1970-01-01 07:43:36     1083 startup-config
2 files, 1399 bytes total.
```

Flash에 저장할 수 있는 파일은 총 32개입니다. Upload 항목을 이용하여 생성 가능합니다.

8.1.4.2. Save startup-config

웹메뉴 Maintenance>Configuration>Save startup-config



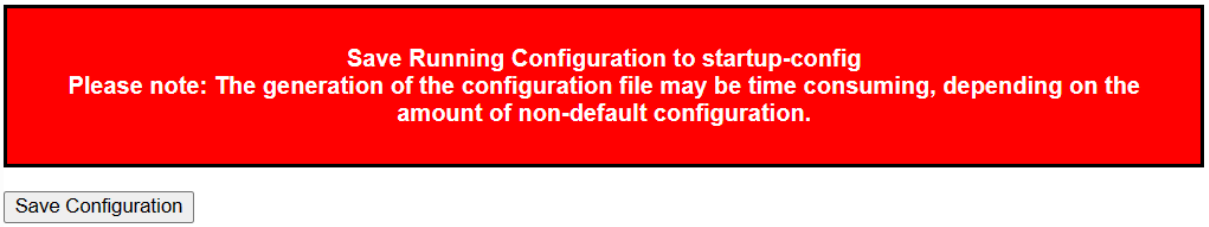
이 작업은 running-config를 startup-config로 복사하여 다음 재부팅 시에 현재 활성화된 구성이 사용되도록 합니다.

Buttons

Save Configuration : "Save Configuration"을 클릭하여 running-config를 startup-config로 복사하세요.

WEB 실행 예시

웹메뉴 Maintenance>Configuration>Save startup-config



Save Configuration을 클릭하여 현재 설정 상태를 저장해 둡니다. 재시작 후에도 현재 설정 상태를 그대로 가져옵니다.

CLI 실행 예시

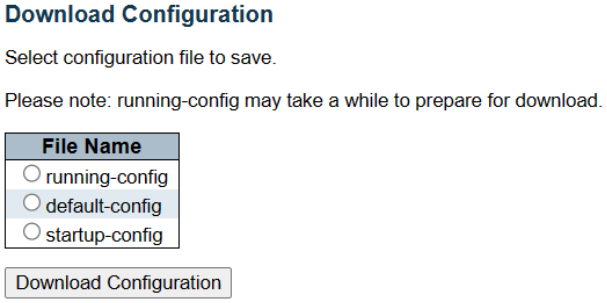
✓ **Copy running-config to start-config**

```
# copy running-config startup-config

Building configuration...
% Saving 1083 bytes to flash:startup-config
#
```

8.1.4.3. Download

웹메뉴 Maintenance>Configuration>Download

스위치의 파일 중 어떤 파일이든 웹 브라우저로 다운로드할 수 있습니다.

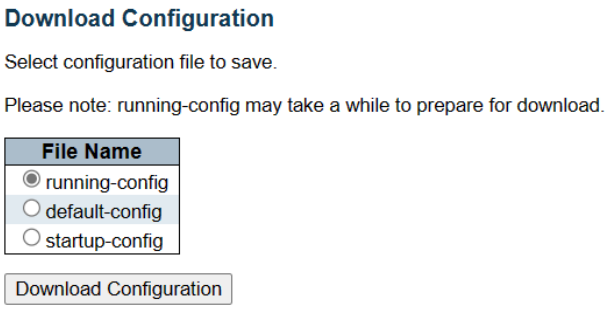


파일을 선택하고 'Download Configuration'를 클릭하세요.

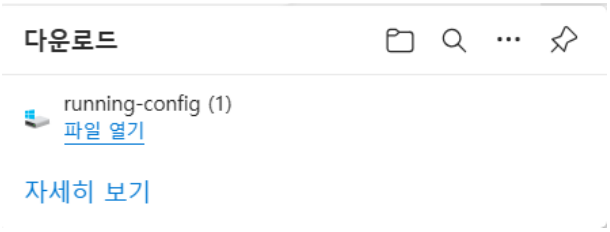
running-config의 다운로드는 준비 작업이 필요하기 때문에 완료까지 약간의 시간이 소요될 수 있습니다.

WEB 실행 예시

웹메뉴 Maintenance>Configuration>Download



파일을 선택하고 'Download Configuration'를 클릭하세요.

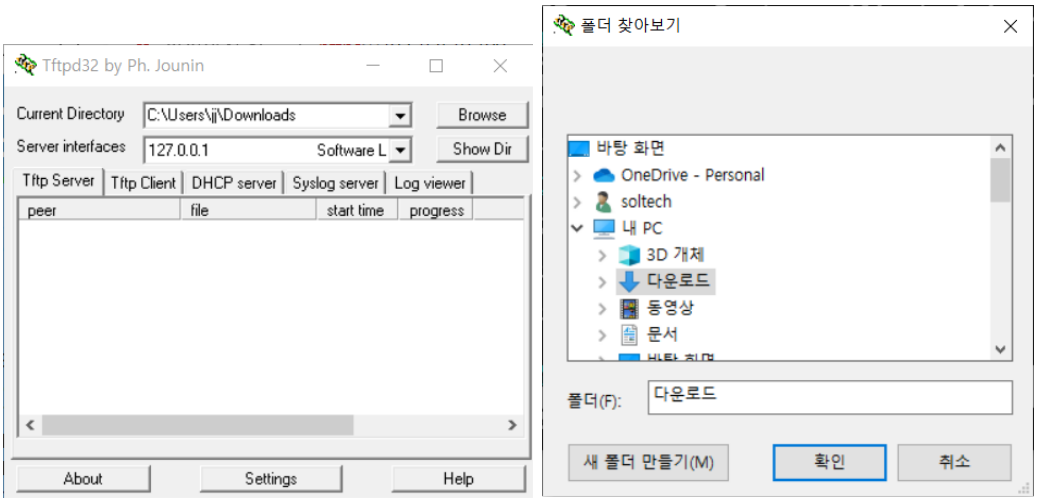


다운로드 된 파일이 표시됩니다.

CLI 실행 예시

✓ Download Configuration

Tftpd32 를 실행하여 파일을 저장할 위치를 정합니다.



Browse 를 클릭하여 파일이 저장될 위치를 설정합니다.

이후 CLI 명령어를 입력합니다.

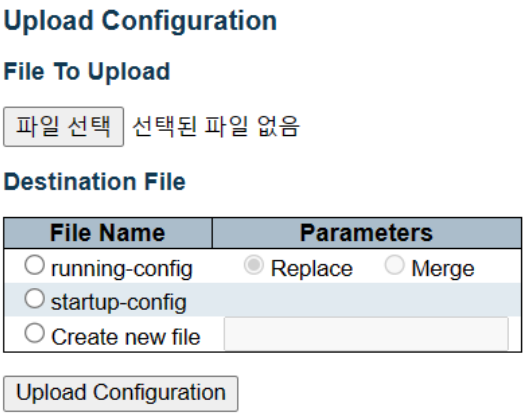
```
# copy 플래시파일명 tftp://PC IPv4주소/저장파일명
# copy running-config tftp://192.168.10.130/running-config
Building configuration...
% Saving 1083 bytes to TFTP server 192.168.10.130: running-config
```

해당 폴더에 파일이 저장되었는지 확인하세요.

8.1.4.4. Upload

웹메뉴 Maintenance>Configuration>Upload

웹 브라우저에서 스위치의 모든 파일에 파일을 업로드할 수 있습니다. 단, 읽기 전용인 default-config은 제외됩니다.



업로드 할 파일을 선택하고 대상 파일을 선택한 후 "Upload Configuration"을 클릭하세요.

File To Upload

Buttons

파일 선택 : 클릭하여 업로드 파일을 선택하세요.

Destination File

장치의 업로드 대상 파일을 선택하세요.

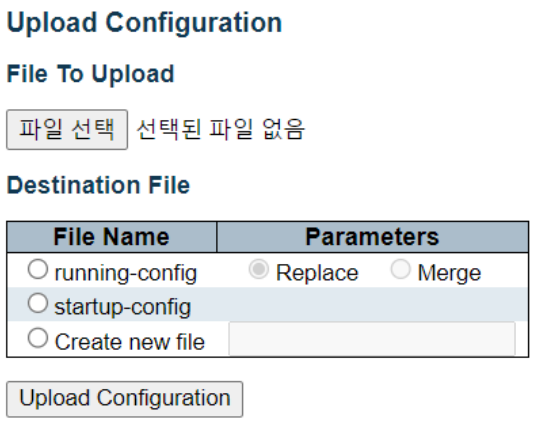
용어	설명
Running-config	파일 내용이 Running-config 에 적용됩니다. 이는 두 가지 방식으로 수행될 수 있습니다: **Replace mode** 현재 구성이 업로드한 파일의 구성으로 완전히 대체됩니다. **Merge mode** 업로드한 파일이 running-config 에 병합됩니다.
Startup-config	파일 내용이 Startup-config 에 저장됩니다. 장비 재시작 후 적용됩니다.
Create new file	플래시 파일 시스템이 가득 찬 경우 (즉, default-config와 시작 구성을 포함한 32개의 파일이 있는 경우), 새 파일을 생성할 수 없습니다. 대신 기존 파일을 덮어쓰거나 다른 파일을 삭제해야 합니다.

Buttons

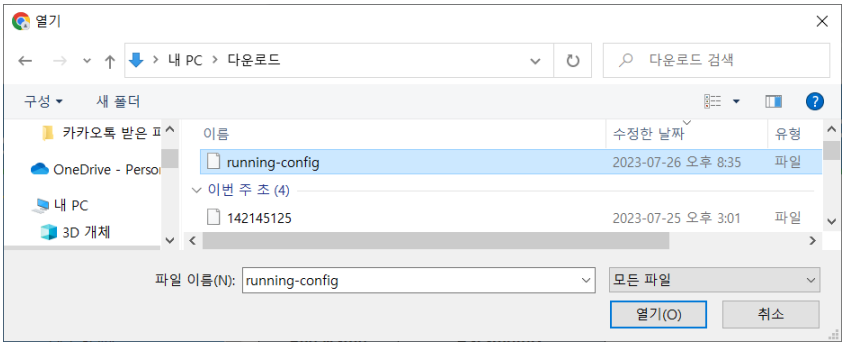
Upload Configuration : 해당 설정 파일을 목적지 파일에 업로드 하려면 클릭하세요.

WEB 실행 예시

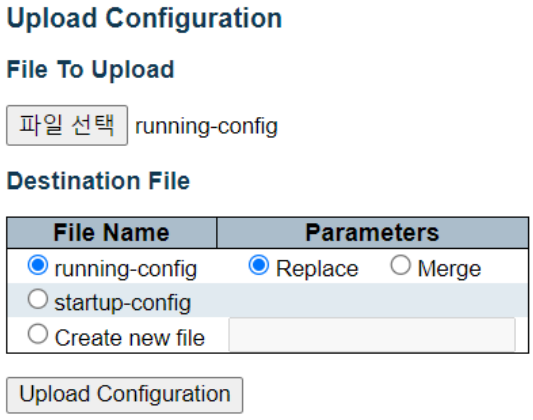
웹메뉴 Maintenance>Configuration>Upload



1. 파일 선택 을 클릭하여 저장한 Config를 불러옵니다.



2. 원하는 파일을 선택한 후 열기 버튼을 클릭합니다.



3. 원하는 파일을 선택하고 Upload Configuration 을 클릭합니다.

(Running-config의 경우 대체하거나(Replace) Config를 결합하는 것(Merge)을 선택할 수 있습니다.)

Activating New Configuration

Please note: If the configuration changes IP settings, management connectivity may be lost.

Status

Activation completed successfully.

Output

```
10GigabitEthernet 1/1 does not have PoE support
10GigabitEthernet 1/2 does not have PoE support
10GigabitEthernet 1/3 does not have PoE support
10GigabitEthernet 1/4 does not have PoE support
```

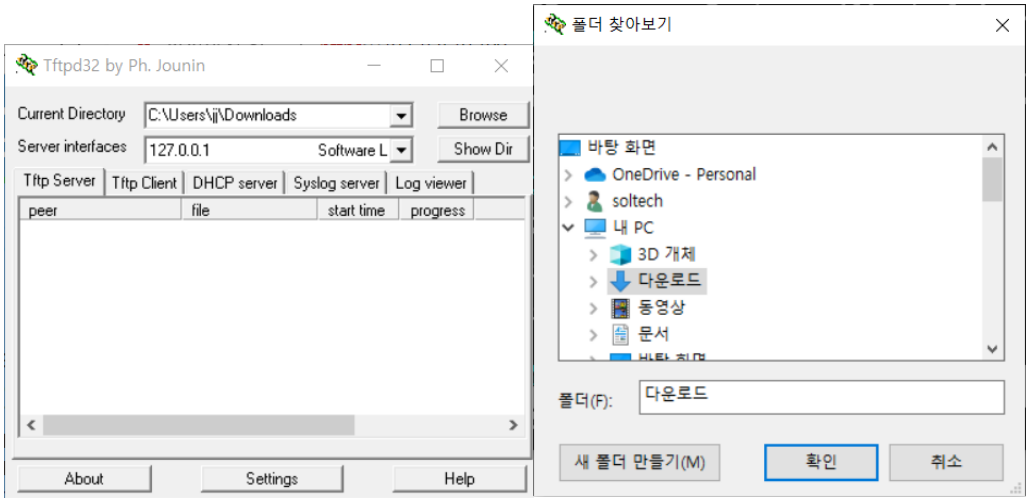
해당 화면이 출력되며 Config가 Upload됩니다.

CLI 실행 예시

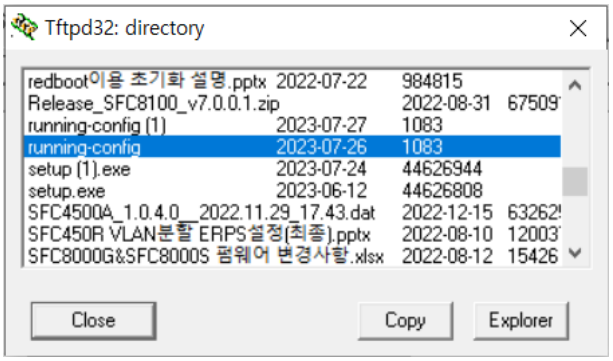
✓ Upload Configuration

Running-Config 에 바로 업로드 하는 것이 현재 불가하여 다른 방법으로 소개합니다.

1. tftp32 에서 Browse 를 클릭하여 경로를 설정해 줍니다.



2. Show Dir 을 클릭하여 파일을 선택하고 Copy 를 클릭 후 Close 를 클릭하여 창을 닫습니다.

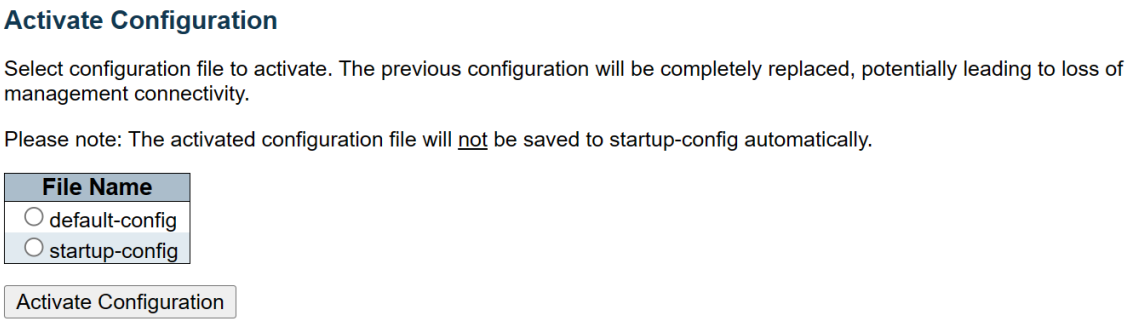


3. Console 창으로 돌아와 다음을 입력합니다.

```
# copy tftp://<PC IPv4 Address>/<upload_filename> startup-config
# copy tftp://192.168.10.130/running-config startup-config
% Loading 123 from TFTP server 192.168.10.130
% Saving 1083 bytes to flash:startup-config

# reload cold
```

8.1.4.5. Activate

웹메뉴 Maintenance>Configuration>Activate



Activate Configuration

활성화할 구성 파일을 선택하세요. 이전 구성은 완전히 대체되며, 관리 연결성이 손실될 수 있습니다.

참고: 활성화된 구성 파일은 자동으로 startup-config에 저장되지 않습니다.

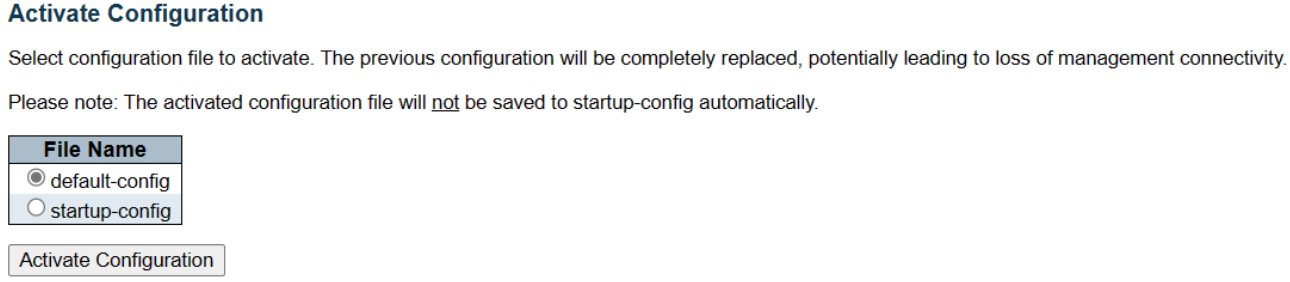
용어	설명
Default-config	Running-config 를 제외하고, Default-config 가 활성화됩니다.
Startup-config	Running-config 를 제외하고, Startup-config 가 활성화됩니다.

Buttons

Activate Configuration : 클릭 시 running-config를 선택한 파일로 대체합니다.

WEB 실행 예시

웹메뉴 Maintenance>Configuration>Activate



원하는 구성 파일을 선택하고 Activate Configuration 을 클릭합니다.

아래 화면이 출력되며, 장비의 현재 Config가 대체됩니다.

Activating New Configuration

Please note: If the configuration changes IP settings, management connectivity may be lost.

Status

Activation completed successfully.

Output

```
(No output was generated.)
```

CLI 실행 예시

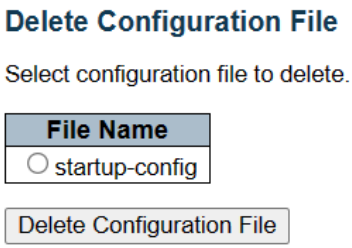
✓ Activate Configuration

```
# copy <flash 파일> running-config
# copy flash:default-config running-config
```

8.1.4.6. Delete

웹메뉴 Maintenance>Configuration>Delete

스타트업 구성을 포함하여 플래시에 저장된 쓰기 가능한 파일을 삭제할 수 있습니다. 이를 수행하고 이전에 구성을 저장하지 않은 채 스위치를 재부팅하면 스위치가 사실상 기본 구성으로 재설정됩니다.



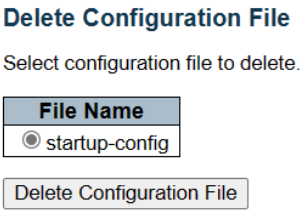
Buttons

Delete Configuration File : 클릭하면 선택한 파일이 지워집니다.

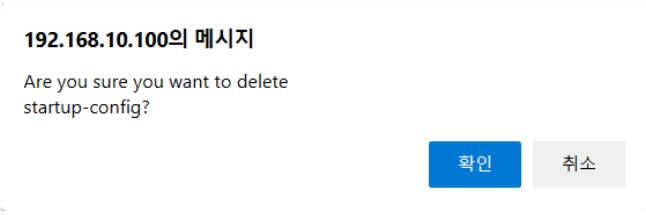
WEB 실행 예시

웹메뉴 Maintenance>Configuration>Delete

✓ **Delete Configuration File**



지울 파일을 선택하고 Delete Configuration File 을 클릭하세요.



위와 같은 경고창이 나옵니다.(해당 파일을 삭제할 것인지를 묻는 경고창)

startup-config successfully deleted. (삭제가 완료되었습니다. 재시작 시 Defaults설정으로 갑니다.)

CLI 실행 예시

✓ Delete Configuration File

```
# delete <url_file>
# delete flash:startup-config
```

9. 문제 해결 방법

9.1. Emergency Recovery

9.1.1. 3seconds Reset

장비가 작동되지 않거나 설정을 잘못한 경우 하드웨어적으로 빠르게 장비초기화를 하는 버튼이 있습니다.

전면부에 Reset이라고 쓰여 있는 부분을 얇고 긴 클립이나 펜으로 3초 정도 눌러주면 Port Led가 깜박이며 초기화 됩니다.

이 때 IP만 그대로 유지되고 장비의 설정이 모두 Factory Defaults 되므로 주의하세요.

(재설정하거나 기존에 저장했던 Config를 업로드하여 사용하세요)

9.1.2. 10seconds Reset

장비가 작동되지 않거나 설정을 잘못한 경우 하드웨어적으로 빠르게 장비초기화를 하는 버튼이 있습니다.

전면부에 Reset이라고 쓰여 있는 부분을 얇고 긴 클립이나 펜으로 10초 정도 눌러주면 Port Led가 깜박이며 초기화 됩니다. (3초 리셋과 다르게 LED 깜박임이 변화됩니다 확인하세요.)

이 때 장비의 설정이 IP를 포함하여 모두 Factory Defaults 되므로 주의하세요.

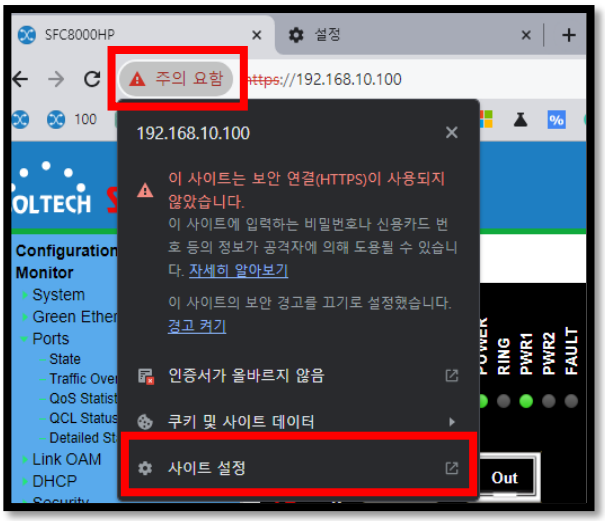
(장비의 초기 IP는 192.168.10.100입니다. 재설정하거나 기존에 저장했던 Config를 업로드하여 사용하세요)

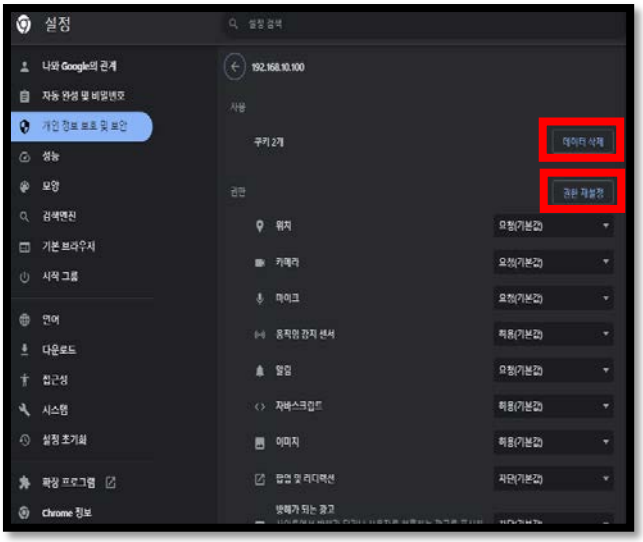
9.2. WEB Interface 접속 오류

WEB 접속에서 간헐적으로 로그인 접속이 안되거나 유지가 안될 경우, 다음과 같이 진행 부탁드립니다.

기본적으로 문제 발생 시, 모든 웹브라우저를 닫고 재실행 시 문제가 해결되며,
지속적으로 문제 발생 시에는 아래 절차로 진행 해주십시요.

9.2.1. Google Chrome Browser





1. 장비 URL 옆에 주의 요함 "클릭"
2. 사이트 설정 "클릭"
3. 해당 장비 IP 확인 후 "데이터 삭제" / "권한 재설정"
4. 설정 완료 이후 웹 브라우저를 닫고 해당 장비 다시 접속

9.2.2. Microsoft Edge Browser

1. 장비 URL 옆에 안전하지 않음 "클릭"

2. 쿠키 "클릭" 후 쿠키 삭제 후 장비 다시 접속

3. 사이트에 대한 사용권한 "클릭"

4. 해당 장비 IP 확인 후 "사용 권한 초기화"

10. 품질보증 및 고객지원

10.1. 품질보증

- **본 제품에 대한 보증기간은 1년입니다.**

- **정상적으로 사용 중 수리 시**
  - **보증기간 내: 무상수리**
  - **보증기간 경과 후: 유상수리**

  ☞ **소비자의 과실 및 천재지변에 의한 고장 시에도 유상수리**

10.2. 고객지원

제품의 구입처와 본사에서 편리한 고객서비스(A/S)를 받으실 수 있습니다.

수리를 의뢰할 때는 제품을 임의 분리하거나 손상되지 않도록 유의 바랍니다.

A/S 연락처 **주소: 서울시 영등포구 당산로41길 11 SK V1 CENTER 215호**
Tel: 070-4106-6200 **E-mail: as@soltech.co.kr**