SOLTECH
Solution of optical & Network

SFC4000A

L2 + 기가비트 매니지먼트 스위치

사용자 매뉴얼

24포트 100/1000Mbps SFP 매니지먼트 스위치

www.soltech.co.kr

상표

내용물에 관하여 사전 고지 없이 개정 될 수 있습니다.

SOLTECH 은 SOLTECH 기술법인기업의 등록 상표이며 기타 모든 상표는 해당 소유자의 자산입니다.

부인 성명서

SOLTECH 기술제품은 하드웨어가 모든 환경 및 응용 프로그램에서 올바르게 작동 함을 보증하지 않으며 품질, 성능, 상업성 또는 특정 목적에서의 적합성과 관련하여 묵시적이든 개방적이든 어떠한 보증이나 책임을 가하지 않습니다. 솔텍은 사용 설명서가 정확한지 확인하기 위해 모든 노력을 기울였습니다. 솔텍은 발생한 부정확성이나 누락에 대한 책임을 지지 않습니다.

사용 설명서의 정보는 예고없이 변경 될 수 있으며 SOLTECH 의 공식입장을 나타내지 않습니다. SOLTECH 은 이 사용 설명서에 포함 된 정확성에 대해 책임을 지지 않습니다. SOLTECH 은 본 사용 설명서의 정보를 최신 상태로 유지하거나 유지할 의무가 없으며 사전 통보없이 본 사용 설명서나 또는 이 사용 설명서에 기술 된 제품을 개선 할 권리가 있습니다.

본 설명서에 부정확하고 오해의 소지가 있어 정보를 찾을 경우 귀하의 의견과 제안해주시면 감사드립니다.

FCC 주의

이 장비는 테스트 결과 FCC 규정 제 15 조에 따라 클래스 A 디지털 장치에 대한 제한 사항을 준수하는 것으로 판명되었습니다. 상업적 환경에서 장비를 작동 할 때 유해한 접근으로부터 합리적인 보호를 제공하도록 고안되었습니다. 장비는 무선 주파수 에너지를 생성, 사용 및 방출 할 수 있으며, 사용 설명서에 따라 설치 및 사용하지 않을 경우 무선 통신에 유해한 간섭을 유발할 수 있습니다. 주거 지역에서 장비를 작동하면 유해한 간섭이 발생할 가능성이 있으며, 이 경우 사용자는 자비로 간섭을 해결해야합니다.

CE 마크 주의

이제품은 A 클래스 제품이며 국내 환경에 장애를 일으킬 수 있으며, 이경우 사용자는 적절한 조치를 취해야 합니다.

장치의 에너지 효율에 관한 참고사항

이 전력요청장치는 대기모드를 지원하지 않으며 에너지 절약을 위해 전원케이블을 분리하시고 활성화되지 않을 경우 장치의 전원 연결을 제거하는 것이 좋습니다.

WEEE 주의

전자 장비의 유해 물질로 인해 왼쪽 그림의 의미를 이해해야 합니다. WEEE 는 분류되지 않은 일반 폐기 물로 처리하지 않고 별도로 수거해야 합니다.

개정

SOLTECH SFC4000A 사용자 설명서

모델명: SFC4000A

목차

1. 소개

구매해주셔서 감사합니다. SOLTECH SFC4000A 는 관리형 스위치이며 멀티 기가 비트 이더넷과 SFP /SFP+광 섬유 연결 및 튼튼한 2 계층이 제공됩니다. 모델에 대한 설명은 아래와 같습니다.

SFC4000A L2+ 24-포트 100/1000 기반-X SFP + 8 포트 공유형 TP 관리형 스위치

"관리형 스위치"는 이 사용 설명서에 대체이름으로 사용됩니다.

1.1 패킷 내용

관리형 스위치의 상자를 열고 신중하게 포장을 엽니다. 상자에는 다음과 같은 품목이 있어야합니다.

- **관리형 스위치**
- **빠른 설치 가이드**
- **RJ45에 RS232 케이블**
- **고무 피트**
- **전용 나사가 있는 두개의 랙 전용 브래킷**
- **전원코드**
- **SFP 방진 캡**

모델 명	**SFP 방진 캡**
SFC4000A	24

이러한 부품이 누락되거나 손상된 경우 즉시 대리점에 문의하십시오. 가능하면 원래의 포장재를 포함한 상자를 보관하고 수리를 위해 제품을 다시 보내야 할 경우에 대비하여 제품을 다시 포장하십시오.

1.2 제품 설명

SOLTECH SFC4000A 는 L2 관리형 기가비트 이더넷 스위치입니다, 종합적인 백본 또는 대용량 서버에 연결되는 안전한 토폴로지에서 매우 많은 양의 데이터를 처리 가능합니다.

안전하고 유연한 관리를 위한 IPv4 와 IPv6

SFC4000A 스위치는 초고속 전송 성능과 우수한 2 계층 및 4 계층 기술을 제공 할뿐만 아니라 높은 보안과 유연성을 제공하기 위해 여러 VLAN 및 다른 IP 주소를 교차 할 수있는 IPv4 / IPv6 VLAN 라우팅 기능도 제공합니다 관리 및 간단한 네트워킹 응용 프로그램입니다.

3 계층 IPv6 / IPv4 듀얼 스택

SFC4000A 는 계층 3 IPv6 및 IPv4 프로토콜을 모두 지원하므로 IPv6 FTTx 에지 네트워크가 설정된 경우 네트워크 시설을 교체하거나 철저히 조사 할 필요가 없으므로 중소기업이 IPv6 시대에 가장 낮은 투자로 지원할 수 있습니다.

튼튼한 2 계층 특징

SFC4000A 는 동적 포트 링크 집합, Q-in-Q Vlan, 사설 Vlan 다중 스패닝 트리 다중 스패닝 트리 프로토콜 (MSTP), 레이어 2 - 레이어 4 QoS, 대역폭 제어 및 IGMP / MLD 스누핑과 같은 고급 스위치 관리 기능을 위해 프로그래밍 할 수 있습니다. SFC4000A 는 지원 포트의 링크 집계를 통해 고속 트렁크의 작동이 여러 광섬유 포트와 결합되어 장애 조치 (fail-over)를 지원합니다.

강력한 보안

SFC4000A 는 포괄적 인 레이어 2 - 레이어 4 액세스 제어 목록 (ACL)을 제공하여 보안을 에지에 적용합니다. 원본 및 대상 IP 주소, TCP / UDP 포트 또는 정의 된 일반 네트워크 응용 프로그램을 기반으로 패킷을 거부하여 네트워크 액세스를 제한하는 데 사용할 수 있습니다. 이 제품의 보호 메커니즘에는 802.1X 포트 기반 및 MAC 기반 사용자 및 장치 인증도 포함됩니다. 사설 VLAN 기능을 사용하면 에지 포트 간의 통신을 차단하여 사용자의 개인 정보를 보호 할 수 있습니다. 또한 SFC4000A 는 DHCP 스누핑, IP 소스 가드 및 동적 ARP 검사 기능을 제공하여 IP 스누핑 공격을 방지하고 잘못된 MAC 주소로 ARP 패킷을 삭제합니다. 네트워크 관리자는 이전보다 훨씬 적은 시간과 노력으로 고도로 보안 된 기업 네트워크를 구축 할 수 있습니다.

정확한 트래픽 제어

SFC4000A 에는 강력한 트래픽 관리 및 QoS 기능이 탑재되어 SMB 의 연결 서비스를 향상시킵니다. QoS 기능에는 유선 속도의 Layer 4 트래픽 분류기와 대역폭 제한이 포함되어있어 멀티 테넌트 유닛, 멀티 비즈니스 유닛, Telco 또는 네트워크 서비스 제공 업체의 응용 프로그램에 특히 유용합니다. 또한 기업이 제한된 네트워크 리소스를 최대한 활용하고 VoIP 및 화상 회의 전송에서 최고의 성능을 보장 할 수 있습니다.

효과적이고 보안적인 관리형스위치

SFC4000A 관리 형 스위치는 콘솔, 웹 및 SNMP 관리 인터페이스를 갖추고 있습니다. 내장 된 웹 기반 관리 인터페이스를 통해 SFC4000A 는 사용하기 쉽고 플랫폼 독립적 인 관리 및 구성 기능을 제공합니다. SFC4000A 는 표준 SNMP (Simple Network Management Protocol)를 지원하며 SNMP 프로토콜 표준을 기반으로하는 모든 관리 소프트웨어를 통해 관리 할 수 있습니다. 제품 학습 시간을 줄이기 위해 SFC4000A 는 Telnet 또는 콘솔 포트를 통해 Cisco 와 유사한

명령을 제공하므로 고객은 이러한 스위치에서 새로운 명령을 배울 필요가 없습니다. 또한 SFC4000A 는 SSH 및 각 세션에서 패킷 내용을 암호화하는 SNMPv3 연결을 지원하여 안전한 원격 관리를 제공합니다.

유연성 및 확장 솔루션

SFC4000A 에 내장 된 다중 미니 GBIC 슬롯은 100BASE-FX 및 1000BASE-SX / LX SFP (Small Form-factor Pluggable) 광섬유 모듈을 지원하므로 이중 속도를 지원합니다. 이제 관리자는 전송 거리뿐만 아니라 필요한 전송 속도에 따라 적절한 SFP 송수신기를 유연하게 선택할 수 있습니다. 거리는 550m 에서 2km (다중 모드 광섬유)에서 최대 10/20/30/40/50/70/120km (단일 모드 광섬유 또는 WDM 광섬유)까지 확장 할 수 있습니다. 엔터프라이즈 데이터 센터 및 배포판의 응용 프로그램에 매우 적합합니다.

지능형 SFP 진단 메커니즘

SFC4000A 는 네트워크 관리자가 광 출력, 광 입력 전력, 온도, 레이저 바이어스 전류 및 트랜시버 공급 전압과 같은 SFP 의 실시간 매개 변수를 쉽게 모니터링 할 수 있도록 해주는 SFP-DDM (Digital Diagnostic Monitor) 기능을 지원합니다.

1.3 사용자 설명서 사용법

이 사용사 설명서는 다음과 같이 구성됩니다.:

단계 2, 설치

이절에는 관리형 스위치 기능과 관리형 스위치 설치법을 실제로 설명합니다

단계 3, 관리형 스위치

이 절에는 관리 대상 스위치의 소프웨어에 대한 정보가 들어 있습니다.

단계 4, 웹 설정

이 절에서는 웹 인터페이스를 통해 관리허

단계 5, 스위치 작동

이 절에서는 웹 인터페이스를 통해 관리하는 방법에 소개 됩니다.

단계 6, 파워 이상 이더넷 요약

이 장에서는 관리형 대상 스위치의 문제를 해결하는 방법에 대해 설명합니다.

단계 7, 장애처리

이 장에서는 관리형 스위치에 문제를 해결하는 방법에 대하여 설명합니다.

부록 A

이 섹션에서는 관리 스위치의 케이블 정보가 담겨있습니다.

1.4 제품 특징

➢ **물리적인 포트**

- **10/100/1000BASE-T** Gigabit RJ45 copper
- **100/1000BASE-X** mini-GBIC/SFP 슬롯
- 기본 관리와 설치 및 RJ45 콘솔 인터페이스

➢ **2 계층 특징**

- 역행 (반이중) 및 IEEE 802.3x 정지 프레임 흐름 제어 (전이중)로 패킷 손실을 방지합니다.
- 높은 성능의 Store-and-Forward 기술과 runt/CRC 필터링은 오류 패킷을 제거하여 네트워크 대역폭을 최적화합니다.
- Storm Control 지원
  - Broadcast / Unicast / Unknown-unicast
- **VLAN 지원**
  - IEEE 802.1Q tagged VLAN
  - 최대 4,094 개의 VLAN ID 중에서 최대 255 개의 VLAN 그룹
  - (VLAN Q-in-Q) 브릿징 제공 (IEEE 802.1ad) 지원
  - 사설 VLAN Edge (PVE)
  - 포트 기반 VLAN
  - MAC 주소 기반 VLAN
  - IP Subnet 기반 VLAN
  - Voice VLAN
- STP **(Spanning Tree Protocol) 지원**
  - STP, IEEE 802.1D Spanning Tree Protocol
  - RSTP, IEEE 802.1w Rapid Spanning Tree Protocol
  - MSTP, IEEE 802.1s Multiple Spanning Tree Protocol, spanning tree by VLAN
  - BPDU Guard
- **Link Aggregation 지원**
  - 802.3ad Link Aggregation 제어 프로토콜(LACP)
  - Cisco 이더넷 체널(수동 Trunk)
  - 트렁크 그룹당 8 개의 포트 지원
  - 최대 16Gbps 대역폭(full duplex 모드)
- 포트 미러 (다수 대 일 구조)
- 특정포트에서 들어오가 나가는 트래픽을 모니터링 하는 포트 미러링
- 방송 루프를 피하기 위한 루프 보호

➢ **3 계층 IP 라우팅 특징**

- 최대 32 개의 고정 경로 및 경로 요약 지원

➢ **QoS(Quality of Service)**

- 포트 대역폭 제어 출입형태 및 속도 제한

- 모든 스위치 포트에서 8 개의 우선순위 대기열
- 트래픽 분류
  - IEEE 802.1p CoS
  - TOS / DSCP / IPv4/IPv6 패킷들의 우선순위
  - IP TCP/UDP 포트 숫자
  - 전형적인 네트워크 어플라이케이션
- 정확한 우선 순위 및 가중 라우는 로빈(WRR) CoS 정책
- 스위치 포트의 트래픽 정책
- DSCP 표기

➢ **Multicast**

- IGMP-Snooping v1, v2 와 v3 지원
- MLD 절전모드 v1 및 v2 지원
- Querier 형식 지원
- IGMP Snooping 포트 필터링
- MLD Snooping 포트 필터링
- MVR (Multicast VLAN Registration)

➢ **Security**

- 인증
  - IEEE 802.1x 포트-기반/ MAC 기반 네트워크 엑세스 인증
  - IEEE 802.1x 인증과 게스트 VLAN
  - 내장 RADIUS 클라이언트가 RADIUS 서버와 협력
  - RADIUS / TACACS+ 사용자 접근 인증
- 접근 통제 목록
  - IP 기반 접근 제한 리스트 (ACL)
  - MAC 기반 접근 제한 리스트 (ACL)
- 출발지 MAC / IP 주소 결합
- **DHCP Snooping** 는 DHCP 분배를 활성화합니다.
- **유동 ARP 감시** MAC 주소가 잘못된 ARP 패킷과 IP 주소 바인딩을 해제합니다.
- **IP Source Guard** 는 IP 스푸핑으로부터 감시합니다.
- IP 주소에 대하어

➢ **Managemen**

- IPv4 and IPv6 듀얼 스택 관리
- 스위치 관리형 인터페이스
  - 콘솔 / Telnet 명령어 줄 인터페이스
  - 웹 스위치 관리
  - SNMP v1, v2c, 와 v3 관리형 스위치
  - SSH / SSL 보안 접근
- **IPv6** 주소 / NTP 관리
- Built-in Trivial File Transfer Protocol (TFTP) 클라이언트
- BOOTP 와 DHCP for IP 주소 승인

- 시스템 유지
  - 펌웨어 업로드 / 다운로드 via HTTP / TFTP
  - 공장초기화 및 시스템 재부팅을 위한 리셋버튼
  - 듀얼 이미지
- DHCP Relay 와 옵션 82
- 사용자 권한 단계에 따른 통제
- NTP (Network Time Protocol)
- Link Layer Discovery Protocol (LLDP) 과 LLDP-MED
- 네트워크 진단
  - SFP-DDM (Digital Diagnostic Monitor)
  - 케이블 문제에 관한 점진적인 진단 케이블 진단 기술 제공
  - ICMPv6 / ICMPv4 원격 핑
- SMTP / Syslog 원격 알람
- 4 가지 RMON 그룹 (기록, 통계, 알람 및 이벤트)
- 인터페이스 연결 및 연결 중지 알림에 대한 SNMP 트랩
- 시스템 로그
- SOLTECH 똑똑한 유니티 배치관리

➢ 중복 전원 시스템 **(SFC4000A)**

- 100~240V AC / 36-60V DC Dual 파워 여분
- Active-active 중복전원 오류 보호
- 단일 공급 장치에서 치명적인 전원 장애 백업
- 내결함성 및 복원력

1.5 제품 특징

SFC4000A / SFC4000A(DC)

Product	SFC4000A
하드웨어적인 특징	
Copper Ports	8 10/ 100/1000BASE-T RJ45 Auto-MDI/MDI-X ports, shared with Port-1~Port-8
SFP/mini-GBIC Slots	24 100/1000BASE-X Dual Speed SFP interfaces
Console	1 x RS232-to-RJ45 serial port (115200, 8, N, 1)
Switch Architecture	Store-and-Forward
Switch Fabric	48Gbps / non-blocking
Throughput	35.7Mpps@64Bytes
Address 표	16K entries, automatic source address learning and ageing
Share Data Buffer	16M bits
Flow Control	IEEE 802.3x pause frame for full-duplex Back pressure for half-duplex
Jumbo Frame	10K bytes
Reset Button	< 5 sec: System reboot > 5 sec: Factory default
Dimensions (W x D x H)	440 x 200 x 44.5 mm, 1U height
Weight	2745g
Power Requirements – AC	AC 100~240V, 50/60Hz
Power Requirements – DC	---
Power Consumption	45 watts / 153 BTU (max.)
ESD Protection	6KV DC
2 계층 기능	
Port Configuration	Port disable / enable Auto-negotiation 10/100/1000Mbps full and half duplex mode selection Flow control disable / enable
Port Status	Display each port's speed duplex mode, link status, flow control status, auto-negotiation status, trunk status
Port Mirroring	TX / RX / Both Many-to-1 monitor
VLAN	802.1Q agged based VLAN Q-in-Q tunneling Private VLAN Edge (PVE) MAC-based VLAN Protocol-based VLAN Voice VLAN IP Subnet-based VLAN MVR (Multicast VLAN registration) Up to 255 VLAN groups, out of 4094 VLAN IDs
Link Aggregation	IEEE 802.3ad LACP / static trunk 12 groups of 8-port trunk supported
Spanning Tree Protocol	STP, IEEE 802.1D Spanning Tree Protocol RSTP, IEEE 802.1w Rapid Spanning Tree Protocol

	MSTP, IEEE 802.1s Multiple Spanning Tree Protocol
QoS	Traffic classification based, strict priority and WRR 8-Level priority for switching - Port Number - 802.1p priority - 802.1Q VLAN tag - DSCP/TOS field in IP packet
IGMP Snooping	IGMP (v1/v2/v3) snooping, up to 255 multicast groups IGMP querier mode support
MLD Snooping	MLD (v1/v2) snooping, up to 255 multicast groups MLD querier mode support
Access Control List	IP-based ACL / MAC-based ACL Up to 256 entries
Bandwidth Control	Per port bandwidth control Ingress: 100Kbps~1000Mbps Egress: 100Kbps~1000Mbps
3 계층 기능	
IP Interfaces	Max. 128 VLAN interfaces
Routing Table	Max. 32 routing entries
Routing Protocols	IPv4 hardware static routing IPv6 hardware static routing
관리	
Basic Management Interfaces	Console / Telnet / Web browser / SNMP v1, v2c
Secure Management Interfaces	SSH, SSL, SNMP v3
SNMP MIBs	RFC-1213 MIB-II 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 and 9) RFC-2737 Entity MIB RFC-2618 RADIUS Client MIB RFC-2863 IF-MIB RFC-2933 IGMP-STD-MIB RFC-3411 SNMP-Frameworks-MIB RFC-4292 IP Forward MIB RFC-4293 IP MIB RFC-4836 MAU-MIB IEEE 802.1X PAE LLDP
표준 사항	
Regulation Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/100BASE-FX IEEE 802.3z Gigabit 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 802.1X Port Authentication Network Control 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 RFC 2710 MLD version 1 FRC 3810 MLD version 2
환경 설정	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 95% (non-condensing)
Storage	Temperature: -10 ~ 70 degrees C Relative Humidity: 5 ~ 95% (non-condensing)

2. 설치

이 절에서는 데스크탑 또는 랙 마운트에 대한 관리 기능 스위치의 하드웨어 기능 및 설치에 대해 설명합니다. 관리 형 스위치를보다 쉽게 관리하고 제어하려면 디스플레이 표시기 및 포트를 숙지하십시오. 이 장의 전면 패널 그림은 장치 LED 표시등을 표시합니다. 네트워크 장치를 관리 대상 스위치에 연결하기 전에 이 장을 완전히 읽으십시오.

2.1 하드웨어 설명

2.1.1 스위치 전면 패널

전면 패널은 관리형 스위치를 모니터링하는 간단한 인터페이스를 제공합니다. 그림 2-1-1 에서 2-1-5 는 관리형 스위치의 전면 패널을 보여줍니다.

SFC4000A Front Panel

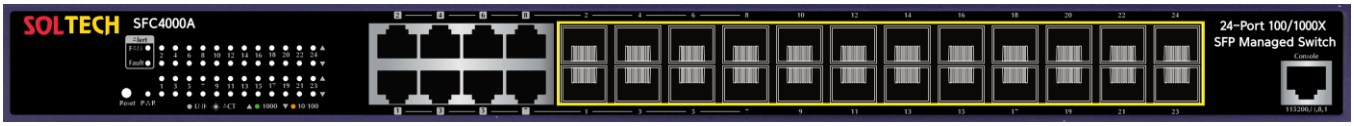


그림 2-1-1: 전면 패널모습 SFC4000A

■ **기가 비트 TP 인터페이스**

10/100/1000BASE-T Copper, RJ45 twisted-pair: 100 미터이상.

■ **SFP 슬롯**

100/1000BASE-X mini-GBIC 슬롯, SFP (Small Factor Pluggable) 송수신기 모듈: From 550m 에서 2km (multi-mode fiber), up to above 10/20/30/40/50/70/120 킬로미터 (single-mode fiber).

■ **콘솔 포트**

콘솔 포트는 RJ45 포트 커넥터입니다. 단말기를 직접 연결하기 위한 인터페이스입니다. 콘솔 포트를 통해 IP 주소 설정, 공정 초기화, 포트 관리 링크 상태 및 시스템 설정 등 다양한 진단 정보를 제공합니다. 사용자는 패키지에서 연결된 DB9-RJ45 콘솔 케이블을 사용하고 장치의 콘솔포트에 연결할 수 있습니다. 연결 후 사용자는 터미널 에뮬레이션 프로그램 (하이퍼 터미널, ProCommPlus, Telix, Winterm 등)을 실행하여 장치의 시작 화면으로 들어갈 수 있습니다..

■ **리셋 버튼**

SFC4000A 전면 패널에는 전원을 껏다 켜지 않고도 관리되는 스위치를 재부팅 할 수 있도록 설계된 재설정버튼이 함께 제공됩니다. 재설정 버튼 기능의 요약 표는 다음과 같습니다.

리셋버튼을 누를경우	기능
5 초 이하: 시스템 재부팅	관리형 스위치 재시작합니다.
5 초 이상: 공장 초기화	관리형스위치를 출고할 경우 기본 구성으로 재설정하시고 관리형 스위치가 재부팅대화 아래와 같이 기본 설정이 로드됩니다.: ◦ 기본 사용자 이름: **admin** ◦ 기본 비밀번호: **admin** ◦ 기본 IP 주소: **192.168.0.100**

	◦ 서브넷 마스크: **255.255.255.0** ◦ 기본 게이트웨이: **192.168.0.254**

SFC4000A-48T4X 의 재설정 버튼은 스위치 측면에 있습니다.

2.1.2 LED 표시등

전면 패널 LED 는 전원 및 시스템 상태, 팬 상태, 포트 링크 / PoE 사용 중 및 데이터 활동의 상태를 나타냅니다. 필요시 모니터링 및 문제 해결에 도움이됩니다. 그림 2-1-6 ~ 그림 2-1-10 은 관리 형 스위치의 LED 표시를 나타냅니다.

SFC4000A / SFC4000A(DC) LED 표시등

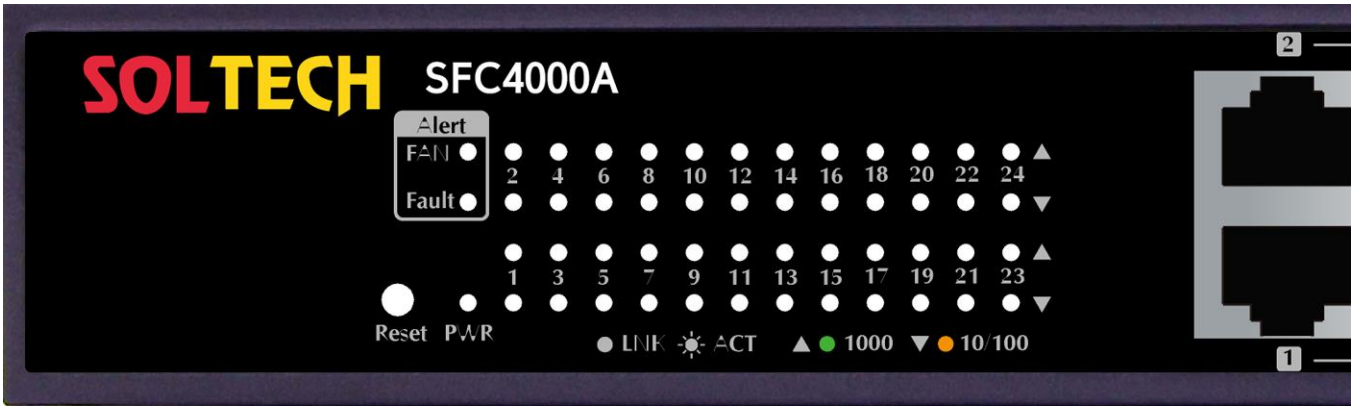


그림 2-1-6: 전면 패널 SFC4000A LED

➢ **시스템**

LED	색상	기능
PWR	**초록**	AC 전원이 입력될 경우 불이 들어옵니다.

➢ **경고등**

LED	색상	기능
FAN	**Green**	팬 장애를 나타내는 표시 등
Fault	**Green**	포트 1 ~ 24 또는 전원 입력 오류를 나타내는 표시 등.

➢ **Per 10/100/1000Mbps RJ45 포트 (포트-1 or 포트-8)**

LED	색상	기능	
1000 LNK/ACT	**Green**	**정상**	포트가 1000Mbps 속도로 실행 중이고 성공적으로 설정되었음을 나타냅니다.
		깜빡임	스위치가 해당 포트를 통해 데이터를 전송 또는 수신 중임을 나타냅니다.
10/100 LNK/ACT	**Orange**	**정상**	포트가 10 / 100Mbps 속도로 성공적으로 설정되었음을 나타냅니다.
		깜빡임	스위치가 해당 포트를 통해 데이터를 전송 또는 수신 중임을 나타냅니다.

➢ **Per 100/1000BASE-X SFP 인터페이스(포트 1 에서 포트 24)**

LED	색상	기능	
1000	**Green**	**정상**	포트가 1000Mbps 에서 성공적으로 설정되었음을 나타냅니다.

LNK/ACT		깜빡임	스위치가 해당 포트를 통해 데이터를 전송하거나 수신 중임을 나타냅니다.
100 LNK/ACT	Orange	정상	포트가 100Mbps 에서 성공적으로 설정되었음을 나타냅니다.
		깜빡임	스위치가 해당 포트를 통해 데이터를 전송하거나 수신 중임을 나타냅니다.

2.1.3 스위치 후면 패널

관리형 스위치의 후면 패널은 AC 입력 전원 소켓으로 구성됩니다. 그림 2-1-11 부터 2-1-15 는 관리형 스위치의 후면 패널을 보여줍니다

SFC4000A 후면 패널

그림 2-1-11: SFC4000A 의 후면 패널

■ **AC 파워소켓**

세계 대부분의 지역에서 관리되는 스위치의 전원 공급 장치는 전기 전압과의 호환성을 위해 100-240VAC 및 50. 60Hz 범위에서 라인 전력을 자동으로 조정할 수 있습니다.

전원 코드의 암 쪽 끝을 관리되는 스위치의 후면 패널에 있는 수신 가능한 부분에 단단히 꽂으면 전원 코드를 콘센트에 꽂을 수 있습니다.

중요: 이 장치는 전원이 필요한 장치이므로 전원이 공급 될 때까지 작동하지 않습니다. 네트워크가 항상 활성화되어 있다면 장치에 UPS (무정전 전원 공급 장치)를 사용하십시오. 네트워크 데이터 손실이나 네트워크 중단을 방지합니다. 일부 지역에서는 서지 억제 장치를 설치하면 스위치 또는 전원 어댑터에 대한 규제되지 않은 서지 또는 전류로 인해 관리 대상 스위치가 손상되지 않도록 보호 할 수 있습니다.

2.2 스위치 설치하기

이 섹션에서는 관리 대상 스위치를 설치하고 관리 대상 스위치에 연결하는 방법에 대해 설명합니다. 다음 주제를 읽고 제시되는 순서대로 절차를 수행하십시오. 데스크탑 또는 선반에 관리형 스위치를 설치하려면 다음 단계를 완료하기 만하면됩니다.

2.2.1 책상에 설치하기

데스크톱 또는 선반에 관리 대상 스위치를 설치하려면 다음 단계를 따르십시오:

1 단계: 고무 다리를 관리스위치 아래쪽에 움푹들어간곳에 부착하시오.

2 단계: 관리형 스위치를 그림 2-2-1 과 같이 AC 전원 근처의 데스크탑이나 선반위에 놓습니다..

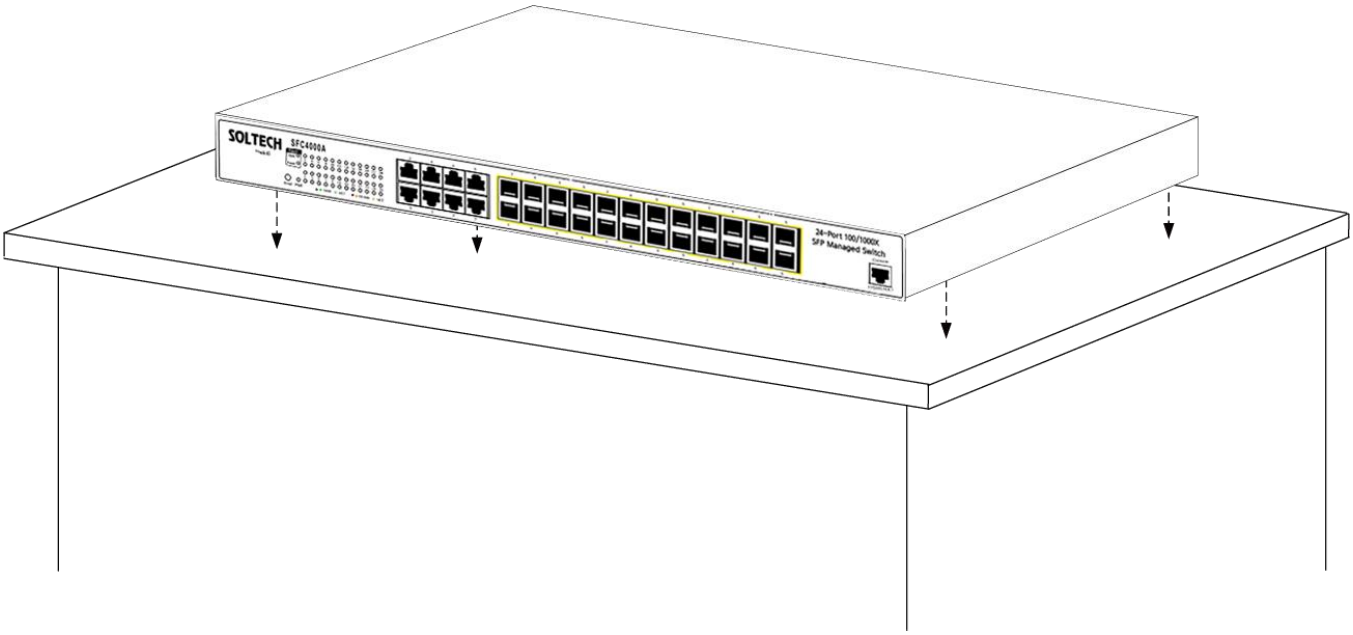


그림 2-2-1: 데스크탑에 관리 스위치 배치

3 단계: 관리형스위치와 주변 물체 사이에는 충분한 환기 공간을 확보하십시오.

Note

위치를 선택할 때는 제 1 장, 4 절에서 설명한 환경 제한 사항 및 사양을 명심하십시오.

4 단계: 관리형 스위치를 네트워크 장치에 연결하십시오.

표준 네트워크 케이블의 한쪽 끝을 관리 스위치 전면의 10/100/1000 RJ45 포트에 연결하십시오.

케이블의 다른 쪽 끝을 프린터 서버, 워크 스테이션 또는 라우터와 같은 네트워크 장치에 연결하십시오.

Note

관리 대상 스위치에 연결하려면 RJ45 팁이있는 UTP 카테고리 5e 네트워크 케이블이 필요합니다. 자세한 내용은 부록 A 의 케이블 연결 사양을 참조하십시오.

5 단계: 관리형 스위치에 전원공급하기

전원 케이블의 한쪽 끝을 관리 스위치에 연결하십시오.

전원 케이블의 전원 플러그를 표준 벽면 콘센트에 연결하십시오.

관리 형 스위치에 전원이 공급되면 전원 LED 는 녹색으로 계속 켜져 있어야합니다.

2.2.2 랙 장착

관리 형 스위치를 19 인치 표준 랙에 설치하려면 아래 설명 된 지침을 따르십시오.

1 단계: 전면 패널을 앞쪽으로 향하게하여 단단한 평면에 관리 스위치를 놓습니다.

2 단계: 패키지에 제공된 나사를 사용하여 랙 장착형 브래킷을 관리 대상 스위치의 각면에 부착하십시오.

그림 2-2-2 관리 대상 스위치의 한쪽에 브래킷을 부착하는 방법을 보여줍니다.

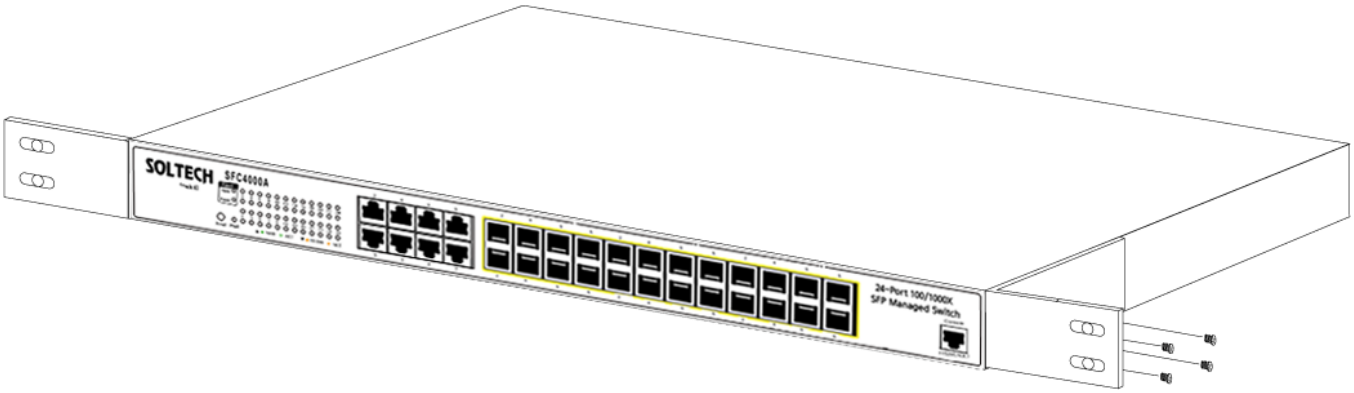


그림 2-2-2: 관리 대상 스위치에 대괄호를 부착하십시오.

장착 브래킷과 함께 제공된 나사를 사용해야합니다. 잘못된 나사를 사용하여 부품이 손상되면 보증이 무효화됩니다.

3 단계: 브래킷을 단단히 고정합니다.

4 단계: 두 번째 브래킷을 반대쪽에 부착하려면 동일한 단계를 따르십시오.

5 단계: 관리 스위치에 브래킷을 부착 한 후 나사를 사용하여 브래킷을 랙에 단단히 고정하십시오 (그림 2-2-3 참조).

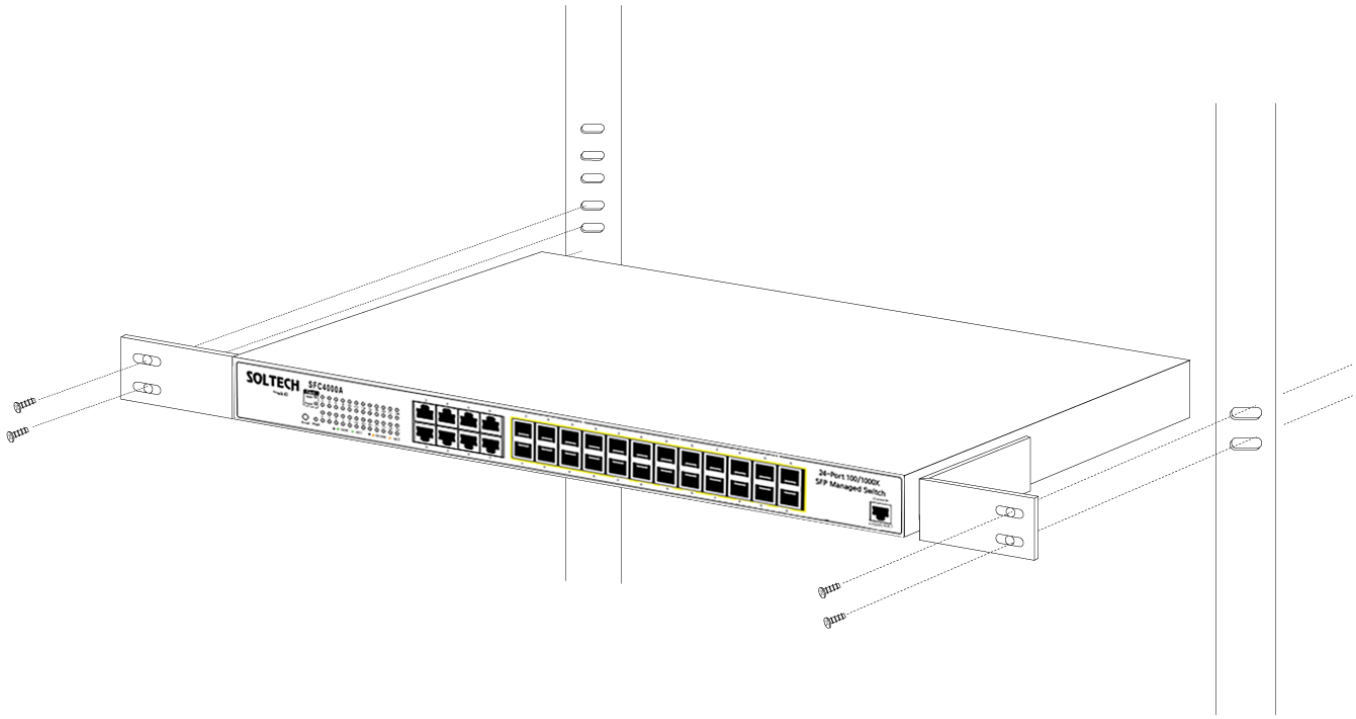


그림 2-2-3: 랙에 관리 스위치 설치

6 단계: 2.2.1 데스크탑 설치의 4 단계와 5 단계를 계속 진행하여 네트워크 케이블을 연결하고 관리 대상 스위치의 전원을 공급하십시오.

2.2.3 SFP / SFP + 송수신기 설치

이 절에서는 SFP / SFP + 송수신기를 SFP / SFP + 슬롯에 삽입하는 방법을 설명합니다. SFP / SFP + 송수신기는 핫 플러그 및 핫 스왑이 가능합니다. 그림 2-2-4 와 같이 관리 대상 스위치의 전원을 끄지 않고도 모든 SFP / SFP + 포트에 송수신기를 연결할 수 있습니다.

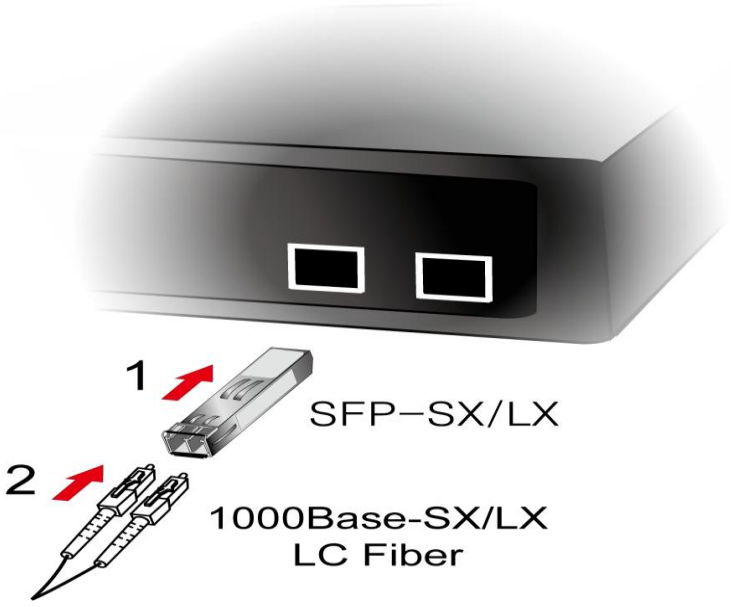


그림 2-2-4: 플러그 인 SFP/SFP+ 송수신기

■ SOLTECH SFP/SFP+ 송수신기 승인

SOLTECH 관리 형 스위치는 단일 모드 및 다중 모드 SFP / SFP + 송수신기를 모두 지원합니다.
승인 된 SOLTECH SFP / SFP + 송수신기 목록은 발행 시점이 정확합니다.

관리 스위치에는 SOLTECH SFP / SFP +를 사용하는 것이 좋습니다. 지원되지 않는 SFP / SFP + 트랜시버를 삽입하면 관리 대상 스위치에서 인식하지 못합니다.

1. SFC4000A 를 다른 네트워크 장치에 연결하기 전에 SFP 송수신 장치의 양면이 동일한 미디어 유형 (예 : 1000BASE-SX - 1000BASE-SX, 1000Bas-LX - 1000BASE-LX)인지 확인해야합니다..
2. 광섬유 케이블 유형이 SFP 송수신기 요구 사항과 일치하는지 확인하십시오.
   - 1000BASE-SX SFP 송수신기에 연결하려면 한 쪽이 male duplex LC 커넥터 유형 인 멀티 모드 광섬유 케이블을 사용하십시오..
   - 1000BASE-SX SFP 송수신기에 연결하려면 한 쪽이 male duplex LC 커넥터 유형 인 단일 모드 광섬유 케이블을 사용하십시오..

■ 광 케이블 연결

1. 양면 LC 커넥터를 SFP / SFP + 송수신기에 끼 웁니다.
2. 케이블의 다른 쪽 끝을 SFP / SFP + 송수신기가 설치된 장치에 연결하십시오..
3. 관리 스위치 전면에있는 SFP / SFP + 슬롯의 LNK / ACT LED 를 확인하십시오. SFP / SFP + 송수신기가 올바르게 작동하는지 확인하십시오..
4. 링크가 실패하면 SFP / SFP + 포트의 링크 모드를 확인하십시오. 일부 fiber-NIC 또는 Media Converters 와 함께 작동하려면 포트 링크 모드를 "1000M Force"또는 "100M Force"로 설정해야합니다.

■ 송수신기 모듈 제거

1. 더 이상 네트워크 활동이 없는지 확인합니다
2. 광섬유 케이블을 부드럽게 제거하십시오.
3. MGB 모듈의 레버를 들어 올리고 수평 위치로 돌립니다..
4. 레버를 통해 모듈을 천천히 잡아 당깁니다.

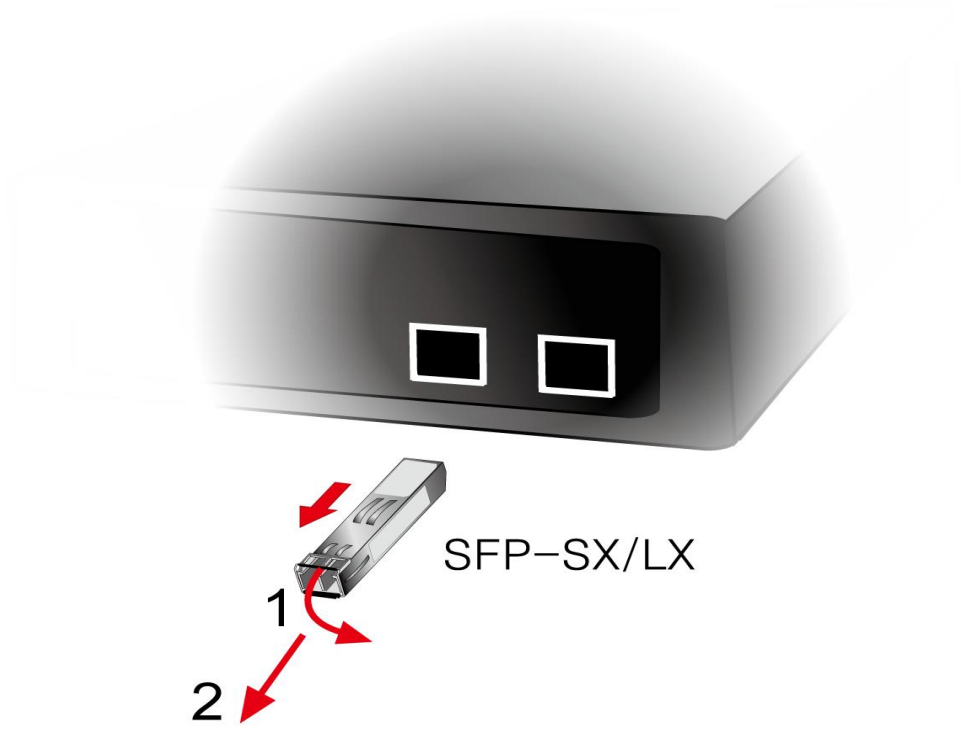


그림 2-2-5: SFP / SFP+ 송수신기 꺼내는법

Note

모듈의 레버를 들어 올리지 않고 수평 위치로 돌리지 말고 모듈을 잡아 당기지 마십시오. 모듈을 직접 잡아 당기면 모듈 및 관리 대상 스위치의 SFP / SFP + 모듈 슬롯이 손상 될 수 있습니다.

3. 관리형 스위치

이 장에서는 관리 대상 스위치에 대한 관리 액세스를 구성하는 데 사용할 수있는 방법을 설명합니다. 관리 응용 프로그램 유형과 관리 장치 (워크 스테이션 또는 개인용 컴퓨터)와 시스템간에 데이터를 전달하는 통신 및 관리 프로토콜에 대해 설명합니다. 포트 연결 옵션에 대한 정보도 들어 있습니다..

이 장에서는 다음 주제를 다룹니다.:

- 요구 사항
- 관리 접근 개요
- 관리 콘솔 엑세스
- 웹기반 관리 엑세스
- SNMP 엑세스
- 표준, 프로토콜 및 관련 리딩

3.1 요구사항

- Windows 2000 / XP, 2003, Vista / 7 / 8, 2008, MAC OS9 이상 또는 TCP / IP 프로토콜과 호환되는 Linux, UNIX 또는 기타 플랫폼을 실행하는 워크 스테이션.
- 워크 스테이션은 이더넷 NIC (Network Interface Card)
- 시리얼 포트 연결 (터미널)
  - 위의 COM 포트 (DB9 / RS-232) 또는 USB-RS-232 변환기가 있는 PC)
- 이더넷 포트 연결
  - 네트워크 케이블 - RJ45 커넥터가있는 표준 네트워크 (UTP) 케이블을 사용하십시오.
- 워크스테이션은 웹브라우저 및 JAVA 런타임 환경 플러그인과 함께 설치됩니다.

관리형스위치에 액세스하려면 Internet Explore 7.0 이상을 사용하는 것이 좋습니다.

3.2 접근관리 개요

관리형 스위치는 다음 방법 중 하나 또는 모두를 사용하여 액세스하고 관리 할 수있는 유연성을 제공합니다.

- 관리용 콘솔
- **웹 브라우저 인터페이스**
- 외부 SNMP 기반 네트워크 관리 응용프로그램

관리 콘솔 및 웹 브라우저 인터페이스 지원은 관리형 스위치 소프트웨어에 내장되어 있으며 즉시 사용할 수 있습니다. 이러한 관리 방법에는 각각 장점이 있습니다. 표 3-1 은 세 가지 관리 방법을 비교합니다..

방법	장점	단점
Console	• IP 와 Subnet 이 필 • 텍스트 기반 • Windows 95 / 98 / NT / 2000 / ME / XP 운영 체제에 내장 된 텔넷 기능 및 하이퍼 터미널 • 보안	• 스위치 근처에 있거나 전화 접속 • 원격 사용자에게는 편리하지 않습니다. • 모뎀 연결이 불안정하거나 느립니다.
Web Browser	• 스위치를 원격으로 구성가능 • 인기있는 브라우저와 호환가능 • 자유로운 로컬위치에서 엑세스가능 • 시각적으로 가장 매력적	• 보안이 손상 될 수 있습니다 (해커는 IP 주소와 서브넷 마스크 만 알면됩니다) • 열악한 연결에서 지연 시간이 발생할 수 있습니다.
SNMP Agent	• MIB 수준에서 스위치 기능과 통신 • 개방형 표준을 기반	• SNMP 관리 소프트웨어 필요성 • 세 가지 방법 모두가 시각적으로 매력적입니다. • 몇몇의 셋팅은 계산을 필요로 합니다 • 보안이 손상 될 수 있습니다 (해커는 커뮤니티 이름 만 알면됩니다)

표 3-1 관리 방법 비교

3.3 웹 관리

관리형 스위치는 Microsoft Internet Explorer 와 같은 표준 브라우저를 통해 네트워크의 어느 곳에서나 관리형 스위치를 관리 할 수있는 관리 기능을 제공합니다. 스위치의 IP 주소를 설정하면 관리 대상 스위치의 IP 주소를 입력하여 웹 브라우저에서 직접 관리 대상 스위치의 웹 인터페이스 응용 프로그램에 액세스 할 수 있습니다.

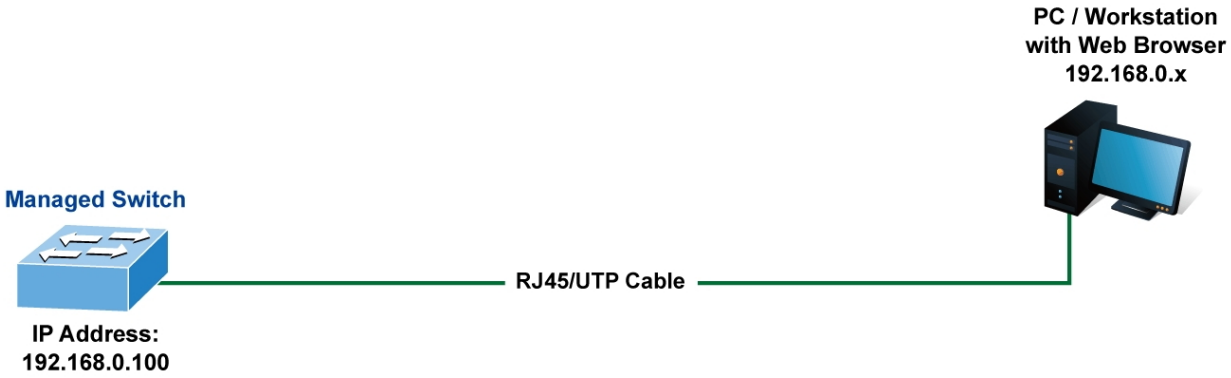


그림 3-1-3: 웹 관리

그런 다음 웹 브라우저를 사용하여 관리 대상 스위치의 콘솔 포트에 직접 연결된 것처럼 중앙 관리 위치에서 관리 대상 스위치 구성 매개 변수를 나열하고 관리 할 수 있습니다. 웹 관리에는 Microsoft Internet Explorer 7.0 이상, Safari 또는 Mozilla Firefox 1.5 이상이 필요합니다.

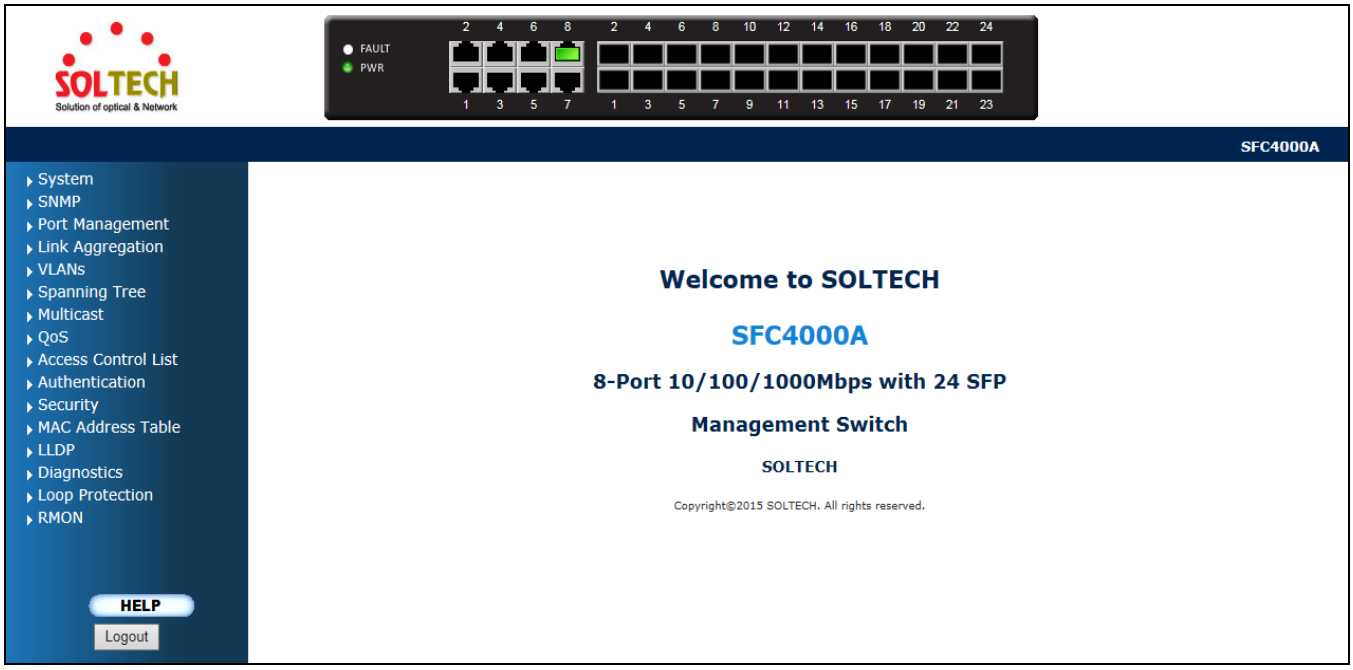
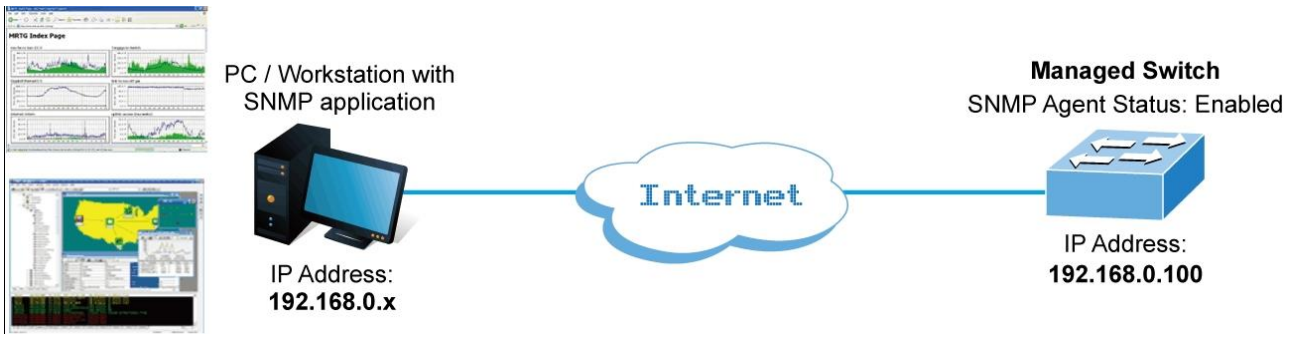


그림 3-1-4: 관리형 스위치의 주요 웹 페이지

3.4 SNMP-기반 네트워크 관리

외부 SNMP 기반 응용 프로그램을 사용하여 SNMP 네트워크 관리자, HP Openview 네트워크 노드 관리 (NNM) 또는 What 's Up Gold 와 같은 관리 대상 스위치를 구성하고 관리 할 수 있습니다. 이 관리 방법을 사용하려면 스위치의 SNMP 에이전트와 SNMP 네트워크 관리 스테이션이 동일한 커뮤니티 문자열을 사용해야합니다. 이 관리 방법은 사실 두 개의 커뮤니티 문자열, get community 문자열과 set community 문자열을 사용합니다. SNMP 네트워크 관리 스테이션이 설정된 커뮤니티 문자열 만 알고 있으면 MIB 에 읽고 쓸 수 있습니다. 그러나 get community 문자열 만 알면 MIB 만 읽을 수 있습니다. 관리형 스위치에 대한 기본 커뮤니티 문자열 가져 오기 및 설정은 공개되어 있습니다.



특징 3-1-5: SNMP 관리

4. 웹페이지 구성

이 절에서는 관리형 스위치에서 웹 기반 관리의 구성 및 기능을 소개합니다..

웹 기반 관리

Managed Switch 는 Microsoft Internet Explorer 와 같은 표준 브라우저를 통해 네트워크의 어느 곳에서나 Managed Switch 를 관리 할 수있는 관리 기능을 제공합니다.

웹 기반 관리는 Internet Explorer 7.0 을 지원합니다. Java 애플릿을 기반으로하여 네트워크 대역폭 소비를 줄이고 액세스 속도를 높이며보기 쉬운 화면을 제공합니다.

> Note
> 기본적으로 IE7.0 이상 버전에서는 Java 애플릿이 소켓을 열 수 없습니다. 사용자는 Java 애플릿이 네트워크 포트를 사용할 수 있도록 브라우저 설정을 명시 적으로 수정해야합니다.

관리 대상 스위치는 이더넷 연결을 통해 구성 할 수 있으므로 관리 대상 PC 를 관리 대상 스위치와 동일한 IP 서브넷 주소로 설정해야합니다.
예를 들어 관리 대상 스위치의 기본 IP 주소는 192.168.0.100 이고 관리자 PC 는 192.168.0.x (여기서 x 는 100 을 제외하고 1 과 254 사이의 숫자 임)로 설정해야하며 기본 서브넷 마스크는 255.255.255.0.
콘솔을 통해 서브넷 마스크 255.255.255.0 을 사용하여 관리 대상 스위치의 기본 IP 주소를 192.168.1.1 로 변경 한 경우 관리자 PC 는 192.168.1.x (여기서 x 는 2 와 254 사이의 숫자 임)에서 관리자 PC 에서 상대 구성을 수행하십시오.

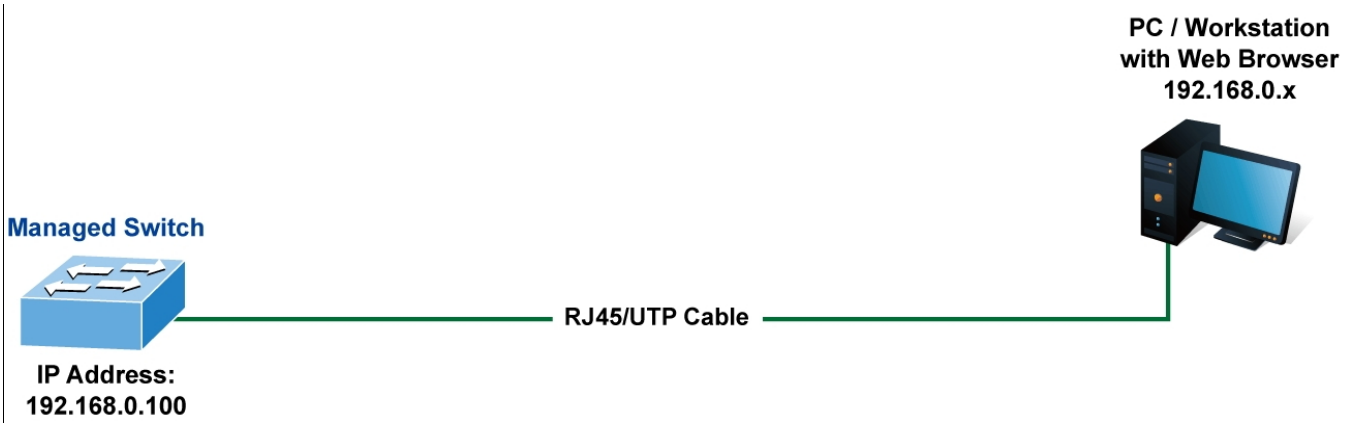


그림 4-1-1: 웹페이지 관리

■ **관리 스위치 로깅**

1. Internet Explorer 7.0 이상의 웹 브라우저를 사용하십시오. 공장 출하시 기본 IP 주소를 입력하여 웹 인터페이스에 액세스하십시오. 공장 출하시 기본 IP 주소는 다음과 같습니다

   http://192.168.0.100

2. 다음 로그인 화면이 나타나면 기본 사용자 이름 "admin"을 암호 "admin"(또는 콘솔을 통해 변경 한 사용자 이름 / 암호)을 입력하여 관리형 스위치 기본 화면에 로그인하십시오. 그림 4-1-2 의 로그인 화면이 나타납니다..

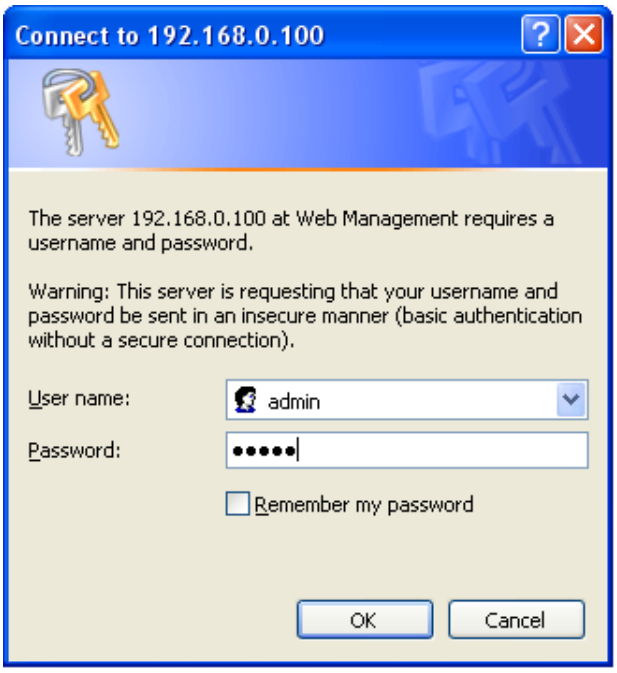


그림 4-1-2: 로그인 화면

기본 User name: **admin**

기본 Password: **admin**

사용자 이름과 암호를 입력하면 메인 화면이 그림 4-1-3 과 같이 나타납니다.

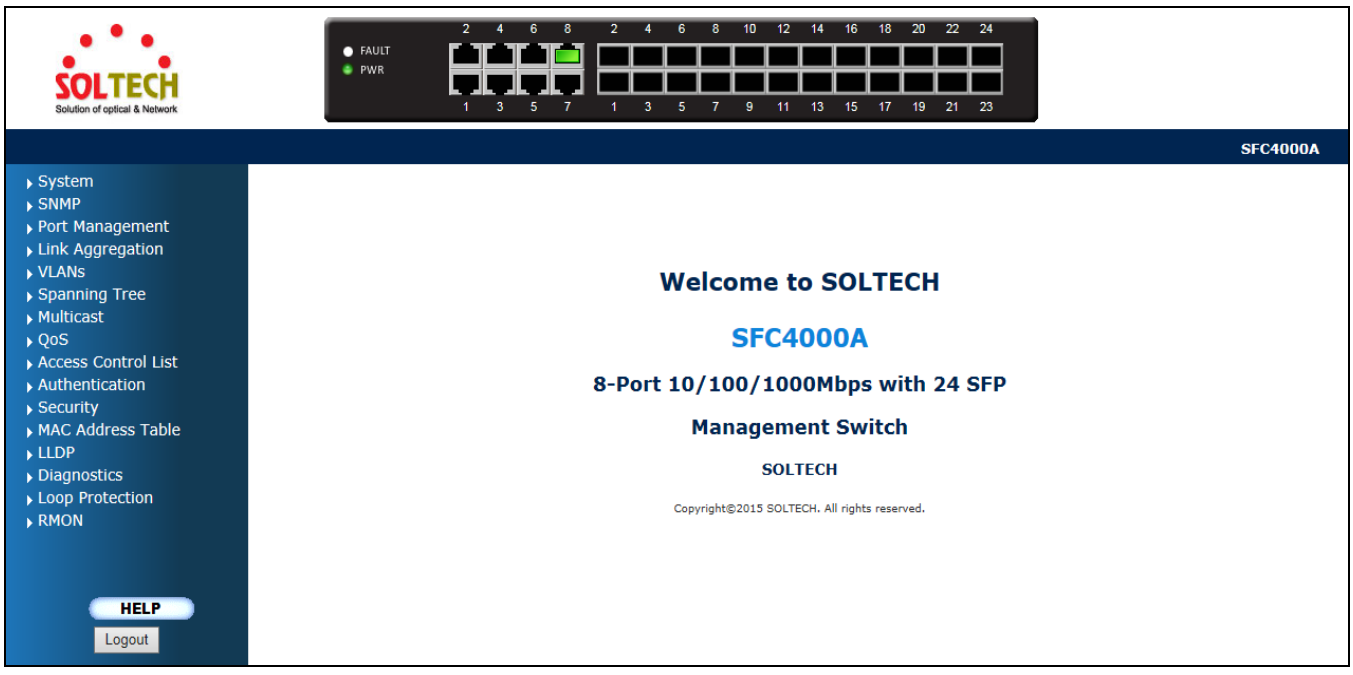


그림 4-1-3: 주요 웹페이지

이제는 웹 관리 인터페이스를 사용하여 스위치 관리를 계속하거나 웹 인터페이스로 관리 대상 스위치를 관리 할 수 있습니다. 웹 페이지의 왼쪽에있는 스위치 메뉴를 통해 관리 스위치가 제공하는 모든 명령과 통계에 액세스 할 수 있습니다..

1. Internet Explorer 7.0 이상을 사용하여 관리형 스위치에 액세스하는 것이 좋습니다..
2. 변경된 IP 주소는 저장 버튼을 클릭 한 즉시 적용됩니다. 새 IP 주소를 사용하여 웹 인터페이스에 액세스해야합니다.
3. 보안상의 이유로이 첫 번째 설정 후에 새 암호를 변경하고 암기하십시오.
4. 웹 인터페이스 아래의 소문자로 된 명령만 수락하십시오.

4.1 주요 웹페이지

관리 형 스위치는 구성 및 관리를위한 웹 기반 브라우저 인터페이스를 제공합니다. 이 인터페이스를 사용하여 원하는 웹 브라우저를 사용하여 관리 대상 스위치에 액세스 할 수 있습니다. 이 장에서는 관리 대상 스위치의 웹 브라우저 인터페이스를 사용하여 구성 및 관리하는 방법에 대해 설명합니다.

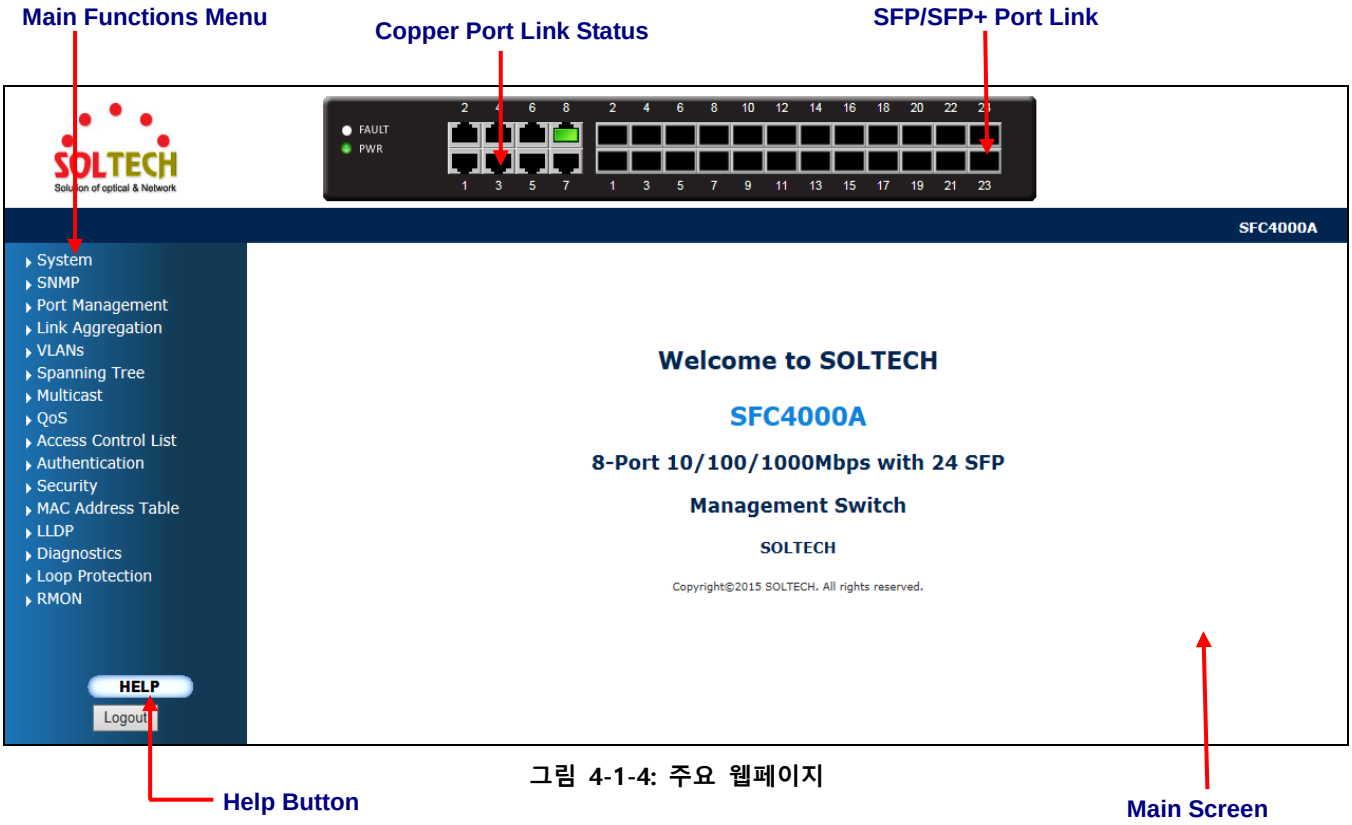


그림 4-1-4: 주요 웹페이지

패널 디스플레이

웹 에이전트는 Managed Switch 의 포트 이미지를 표시합니다. 모드는 링크 업 또는 링크 다운을 포함하여 포트에 대한 다른 정보를 표시하도록 설정할 수 있습니다. 포트의 이미지를 클릭하면 포트 통계 페이지가 열립니다.

포트 상태는 다음과 같이 표시됩니다.

상태	Disabled	Down	Link
RJ45 Ports			
SFP Ports			

주요 메뉴

온보드 웹 에이전트를 사용하여 시스템 매개 변수를 정의하고, 관리 대상 스위치와 모든 포트를 관리 및 제어하거나 네트워크 상태를 모니터링 할 수 있습니다. 관리자는 웹-관리를 통해 주요 기능에 나열된 기능을 선택하여 관리스위치를

설정할 수 있습니다. 그림 4-1-5 의 화면이 나타납니다..

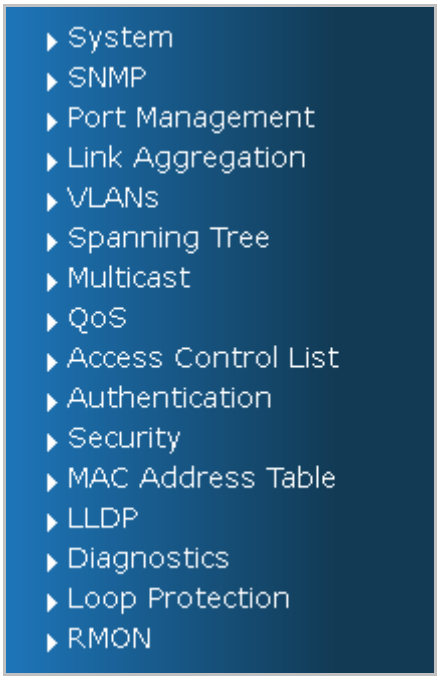


그림 4-1-5: 관리형스위치의 주요 기능

4.2 시스템

시스템 메뉴 항목을 사용하여 관리 대상 스위치의 기본 관리 정보를 표시 및 구성하십시오. 시스템 아래에서 시스템 정보를 구성하고 볼 수있는 다음 항목이 제공됩니다. 이 섹션에는 다음 항목이 있습니다.:

- **System Information** 관리형 스위치 시스템 정보가 여기에 제공됩니다.
- **IP Configuration** 이 페이지에서 관리 대상 스위치에서 관리하는 IPv4 / IPv6 인터페이스와 IP 경로를 구성합니다.
- **IP Status** 이 페이지는 IP 프로토콜 계층의 상태를 표시합니다. 상태는 IP 인터페이스, IP 경로 및 인접 캐시 (ARP 캐시) 상태에 의해 정의됩니다.
- **Users Configuration** 이 페이지는 현재 사용자의 개요를 제공합니다. 현재 웹 서버에서 다른 사용자로 로그인하는 유일한 방법은 브라우저를 닫았다가 다시 열 수 있습니다.
- **Privilege Levels** 이 페이지에서는 권한 수준에 대한 개요를 제공합니다.
- **NTP Configuration** 이 페이지에 NTP 서버를 구성하십시오.
- **Time Configuration** 이 페이지에서 시간 매개 변수를 구성하십시오.
- **UPnP** 이 페이지에서 UPnP 를 구성하십시오.
- **DHCP Relay** 이 페이지에서 DHCP 릴레이를 구성하십시오.
- **DHCP Relay Statistics** 이 페이지는 DHCP 릴레이에 대한 통계를 제공합니다.
- **CPU Load** 이 페이지는 SVG 그래프를 사용하여 CPU 로드를 표시합니다.
- **System Log** 관리형 스위치 시스템 로그 정보가 여기에 제공됩니다.
- **Detailed Log** 관리형 스위치 상세한 로그를 시스템에서 제공합니다.
- **Remote Syslog** 이 페이지에서 원격 syslog 를 구성하십시오
- **SMTP Configuration** 이 페이지에서 SMTP 매개 변수를 구성하십시오.
- **Web Firmware Upgrade** 이 페이지는 관리 대상 스위치를 제어하는 펌웨어의 업데이트를 용이하게합니다.
- **TFTP Firmware Upgrade** TFTP 서버를 통해 펌웨어 업그레이드를 합니다.
- **Save Startup Config** 이렇게하면 running-config 가 startup-config 에 복사되므로 다음 재부팅시 현재 활성 구성이 사용됩니다
- **Configuration Download** 스위치에서 파일을 다운로드 할 수 있습니다.
- **Configuration Upload** 파일을 스위치에 업로드 할 수 있습니다.
- **Configuration Activate** 스위치에 있는 구성 파일을 활성화 할 수 있습니다.
- **Configuration Delete** 플래시에 저장된 쓰기 가능 파일을 삭제할 수 있습니다.
- **Image Select** 이 페이지에서 활성 또는 대체 펌웨어를 구성합니다.
- **Factory Default** 이 페이지에서 관리 대상 스위치의 구성을 재설정 할 수 있습니다. IP 구성만 유지됩니다.
- **System Reboot** 이 페이지에서 관리 대상 스위치를 다시 시작할 수 있습니다. 다시 시작하면 관리 대상 스위치가 정상적으로 부팅됩니다.

4.2.1 시스템 정보

시스템 정보 페이지는 현재 장치 정보에 대한 정보를 제공합니다. 시스템 정보 페이지는 스위치 관리자가 하드웨어 MAC 주소, 소프트웨어 버전 및 시스템 가동 시간을 식별하는 데 도움을줍니다. 그림 4-2-1 의 화면이 나타납니다.

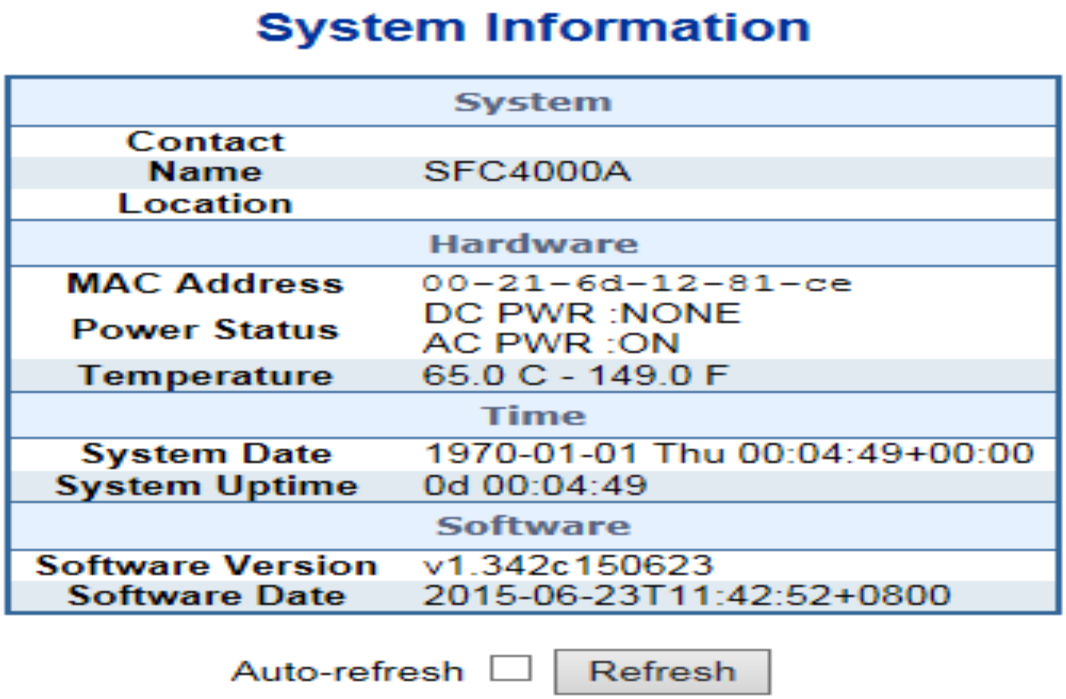


그림 4-2-1: 시스템 정보페이지 화면

이 페이지에서는 다음 필드가 포함됩니다.:

주제	설명
• **Contact**	SNMP 에서 구성된 시스템 문의 | 시스템 정보 | 시스템 문의.
• **Name**	SNMP 에서 구성된 시스템 이름 | 시스템 정보 | 시스템 이름.
• **Location**	SNMP 에서 구성된 시스템 위치 | 시스템 정보 | 시스템 위치.
• **MAC Address**	**관리 대상 스위치의 MAC 주소입니다.**
• **Temperature**	칩셋 온도를 나타냅니다. 현재 (GMT) 시스템 시간과 날짜. 시스템 시간은 구성된 NTP 서버 (있는 경우)를 통해 얻습니다.
• **System Date**	현재 (GMT) 시스템 시간과 날짜. 시스템 시간은 구성된 NTP 서버 (있는 경우)를 통해 얻습니다.
• **System Uptime**	장치가 작동 된 기간입니다.
• **Software Version**	관리되는 스위치의 소프트웨어 버전. 리되는 스위치의 소프트웨어 버전.
• **Software Date**	관리 형 스위치 소프트웨어가 생성 된 날짜입니다.

버튼

자동-새로고침 ☐ :3 초마다 자동으로 체크박스에 확인되어 갱신되어 데이터가 나타납니다..

Refresh : 새로고침을 하고 싶은 경우 수동으로 눌러 갱신 할 수있다.

4.2.2 IP 설정

IP 구성에는 IP 구성, IP 인터페이스 및 IP 라우트가 포함됩니다. 구성된 열은 IP 구성을 보거나 변경 하는 데 사용됩니다. 지원되는 인터페이스의 최대 수는 128 이고 최대 경로 수는 32 입니다. 그림 4-2-2 의 화면 참조.

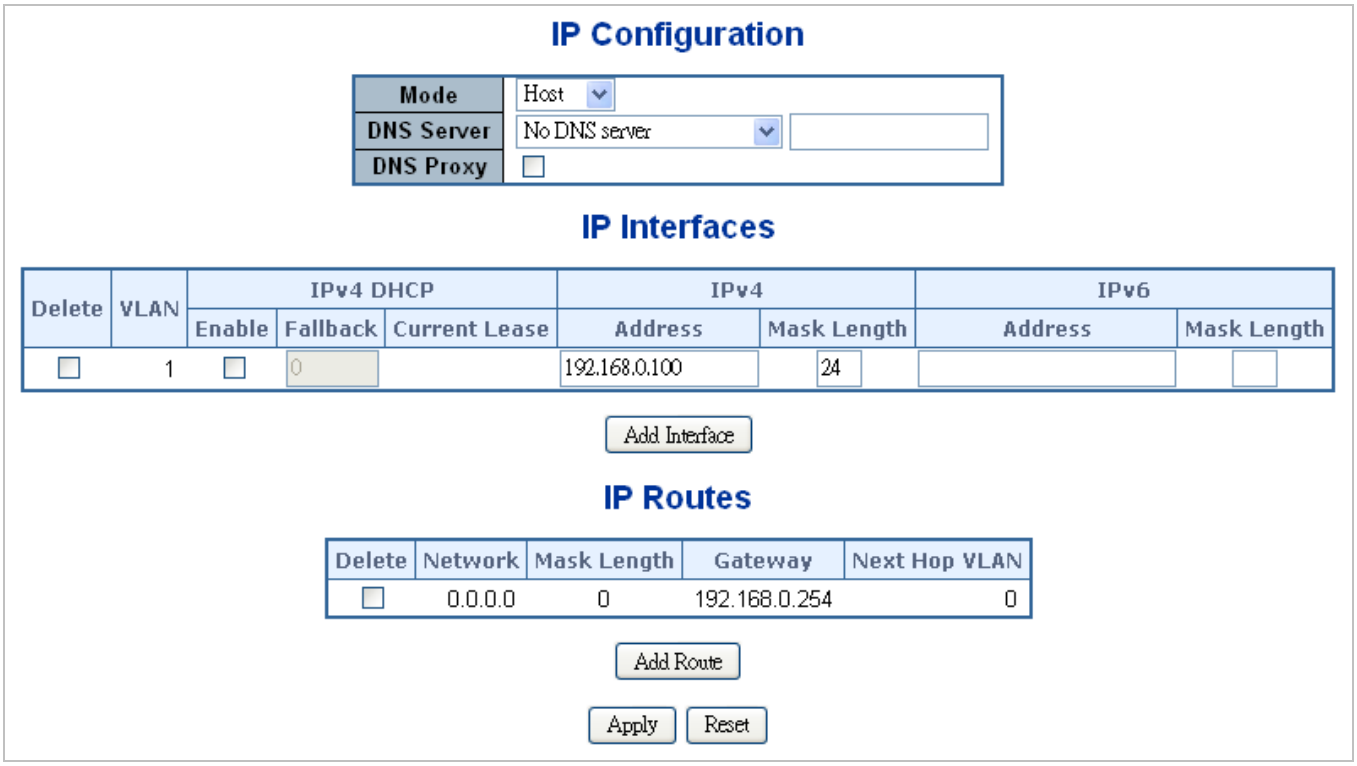


그림 4-2-2: IP 설정페이지 화면

현재의 설정 모습은 다음과 같은 기능을 안내합니다.

목적		설명
• IP Configurations	Mode	IP 스택은 호스트나 라우터로 작동여부를 구성합니다. 호스트 모드에서 인터페이스 간 IP 트래픽은 라우트되지 않으며 라우터모드에서 트래픽은 모든 인터페이스간에 라우팅됩니다.
	DNS Server	이 설정은 스위치로 수행 된 DNS 이름 확인을 제어 합니다. 다음 모드가 지원됩니다. ■ **모든 DHCP 인터페이스** 임의 DHCP 에서 사용가능한 DHCP 가 인터페이스로 제공되는 첫번째 DNS 서버가 사용됩니다.. ■ **DNS 서버가 사용되는 경우** DNS 서버를 사용하지 않습니다.. ■ **설정** 명시적으로 점으로 구분 된 십진수 표기법으로 DNS 서버의 IP

			주소를 제공하십시오.. ■ **DHCP 인터페이스** 제공된 DNS 서버를 이용가능한 DHCP 인터페이스에서 지정해야합니다.
	DNS Proxy		DNS 프록시가 활성화되면 시스템은 DNS 요청을 현재 구성된 DNS 서버로 전달하고 DNS 확인자로 네트워크의 클라이언트 장치에 응답합니다.
• **IP Address**	**Delete**		기존 IP 인터페이스를 삭제하려면 옵션을 선택하십시오.
	VLAN		IP 인터페이스와 연관된 VLAN 입니다. 이 VLAN 의 포트만 IP 인터페이스에 액세스 할 수 있습니다. 이 필드는 새 인터페이스를 작성할 때 입력 할 때만 사용할 수 있습니다.
	IPv4 DHCP	**Enabled**	이 상자를 선택하여 HDCP 클라이언트를 활성화하십시오.
		Fallback	임시 DHCP 를 얻으려고 시도하는 시간(초단위)
		Current Lease	활성화 된 임시 DHCP 인터페이스의 경우 이 열은 HDCP 서버에서 제공 한 현재 인터페이스 주소를 표시합니다.
	IPv4	**Address**	점으로 구분 된 10 진수 표기법으로 관리형 스위치의 IP 주소를 제공합니다.
		Mask Length	IPv4 네트워크 마스크 유효값은 0~30 비트입니다.
	IPv6	**Address**	관리형 스위치의 IP 주소를 제공합니다.
		Mask Length	비트 수 (접두사 길이)로 나타낸 IPv6 네트워크 마스크입니다. 유효한 값은 IPv6 주소의 경우 1 ~ 128 비트입니다..
• **IP Routes**	**Delete**		기존 IP 경로를 삭제하려면이 옵션을 선택하십시오.
	Network		목적지 IP 네트워크 또는이 라우트의 호스트 주소. 올바른 형식은 점으로 구분 된 10 진수 표기법 또는 유효한 IPv6 표기법입니다. 기본 라우트는 0.0.0.0 또는 IPv6 :: notation 값을 사용할 수 있습니다.
	Mask Length		대상 IP 네트워크 또는 호스트 마스크 (비트 수 (접두어 길이)).
	Gateway		IP 게이트웨이의 IP 주소입니다. 올바른 형식은 점으로 구분 된 십진수 표기법 또는 유효한 IPv6 표기법입니다. 게이트웨이와 네트워크는 동일한 유형이어야합니다.
	Next Hop VLAN		게이트웨이와 연관된 특정 IPv6 인터페이스의 VLAN ID (VID)입니다.

버튼

Add Interface: 클릭 하여 모든 인터페이스가 선택됩니다..

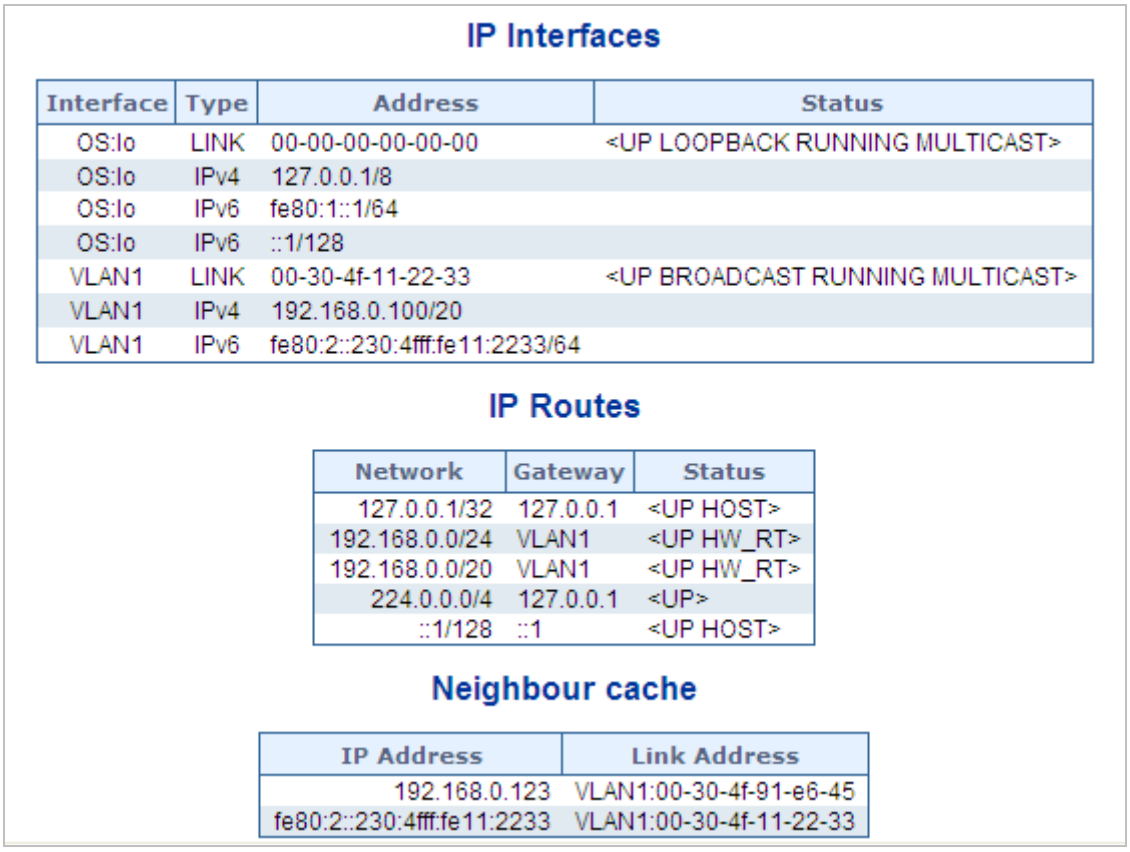
Add Route: 클릭 하여 새로운 라우터를 추가합니다

Apply: 클릭하여 변동내역을 저장합니다.

Reset: 클릭하여 이전에 초기값으로 되돌립니다.

4.2.3 IP 상태

IP 상태에는 IP 프로토콜 계층의 상태를 표시하며 IP 인터페이스, IP 경로 및 인접 캐시(ARP 캐시) 상태에 의해 정의됩니다. 그림 4-2-3 의 화면 참조하시기 바랍니다.



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::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-30-4f-11-22-33	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.100/20	
VLAN1	IPv6	fe80:2::230:4fff:fe11:2233/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
192.168.0.0/24	VLAN1	<UP HW_RT>
192.168.0.0/20	VLAN1	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.0.123	VLAN1:00-30-4f-91-e6-45
fe80:2::230:4fff:fe11:2233	VLAN1:00-30-4f-11-22-33

그림 4-2-3: IP 상태페이지 화면

이페이지에는 다음과 같은 명령어가 포함됩니다.

목표		설명
• **IP Interfaces**	**Interface**	인터페이스의 이름입니다.
	Type	항목의 주소 유형. LINK 또는 IPv4 일 수 있습니다.
	Address	인터페이스의 현재 주소입니다.
	Status	인터페이스 및 주소의 상태 플래그
• **IP Routes**	**Network**	이 경로의 게이트웨이 주소 입니다.
	Gateway	이 경로의 게이트웨이 주소입니다.
	Status	경로의 상태 플래그
• **Neighbor Cache**	**IP Address**	항목의 IP 주소
	Link Address	주어진 IP 주소로의 바인딩이 존재하는 LINK(MAC)주소.

버튼

Auto-refresh ☐ : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Refresh : 페이지를 새로 고칩니다.

4.2.4 사용자 구성

이 페이지는 현재 사용자의 개요를 제공합니다. 현재 웹 서버에서 다른 사용자로 로그인하는 유일한 방법은 브라우저를 닫았다가 다시 열 수 있습니다. 설정이 완료되면 "적용"버튼을 눌러 적용합니다. 새 사용자 이름과 암호로 웹 인터페이스에 로그인하십시오. 그림 4-2-4 의 화면이 나타납니다..

그림 4-2-4: 사용자 설정 페이지 화면

페이지에 포함한 내용:

목적	설명
• **User Name**	사용자의 이름을 정의합니다. 추가하여 변경 및 삭제가 가능합니다.
• **Privilege Level**	사용자의 권한 수준입니다. 허용 범위는 1 에서 15 까지입니다. 권한 수준 값이 15 이면 모든 그룹에 액세스 할 수 있습니다. 즉, 장치의 모든 권한이 부여됩니다. 그러나 다른 사람들은 각 그룹 권한 수준을 참조 할 필요가 있습니다. 사용자 권한은 해당 그룹에 대한 액세스 권한을 가진 그룹 권한 레벨보다 같거나 커야합니다. 기본적으로 대부분의 그룹 권한 수준 5 는 읽기 전용 액세스 권한을 가지며 권한 수준 10 은 읽기 - 쓰기 권한을 갖습니다. 그리고 시스템 유지 보수 (소프트웨어 업로드, 공장 기본값 등)에는 사용자 권한 레벨 15 가 필요합니다. 일반적으로 권한 수준 15 는 관리자 계정, 표준 사용자 계정의 권한 수준 10, 게스트 계정의 권한 수준 5 에 사용할 수 있습니다.

버튼

Add New User : 새로운 사용자를 추가합니다.

사용자 편집 / 추가

이 페이지에 설정된 사용자를 추가하거나 편집 할 수 있습니다..

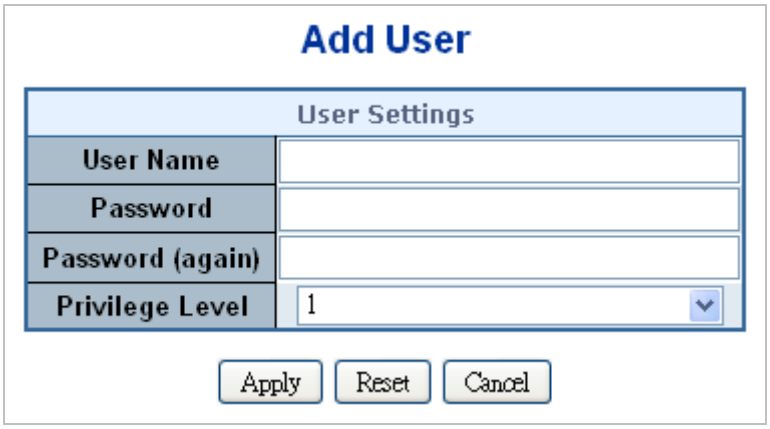


그림 4-2-5: 사용자를 추가하거나 편집하는 화면입니다.

이 페이지에서는 다음을 정의합니다.:

기능	설명
• **Username**	이 항목이 속해야하는 사용자 이름을 식별하는 문자열. 허용되는 문자열 길이는 1 - 31 입니다. 유효한 사용자 이름은 문자, 숫자 및 밑줄의 조합입니다..
• **Password**	사용자의 암호. 허용되는 문자열 길이는 1 에서 31 사이입니다.
• **Password (again)**	확인을 위해 사용자의 새 비밀번호를 다시 입력하십시오.
• **Privilege Level**	사용자의 권한 수준입니다. 허용 범위는 1 에서 15 까지입니다. 권한 수준 값이 15 이면 모든 그룹에 액세스 할 수 있습니다. 즉, 장치의 모든 권한이 부여됩니다. 그러나 다른 사람들은 각 그룹 권한 수준을 참조 할 필요가 있습니다. 사용자 권한은 해당 그룹에 대한 액세스 권한을 가진 그룹 권한 레벨보다 같거나 커야합니다. 기본적으로 대부분의 그룹 권한 수준 5 는 읽기 전용 액세스 권한을 가지며 권한 수준 10 은 읽기 - 쓰기 권한을 갖습니다. 그리고 시스템 유지 보수 (소프트웨어 업로드, 공장 기본값 등)에는 사용자 권한 레벨 15 가 필요합니다. 일반적으로 권한 수준 15 는 관리자 계정, 표준 사용자 계정의 권한 수준 10, 게스트 계정의 권한 수준 5 에 사용할 수 있습니다.

버튼

Apply: 변동사항을 저장합니다.

Reset: 로컬 변경 사항을 실행 취소하고 이전에 저장된 값으로 되돌리려면 클릭하십시오.

Cancel: 현재 사용자를 삭제합니다. 이 버튼은 새 구성에서는 사용할 수 없습니다 (새 사용자 추가).

Delete User: 새 사용자가 추가되면 사용자 구성 페이지에 새 사용자 항목이 표시됩니다.

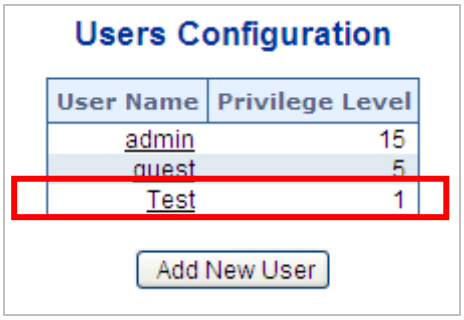


그림 4-2-6: 사용자 구성 페이지 화면

Note

기본 암호를 변경 한 후 새 암호를 잊어버린 경우 관리형 스위치의 전면패널에 "Reset" 버튼을 10 초이상 눌렀다가 놓아주세요. 관리형 스위치가 기본모드로 복원됩니다.

4.2.5 권한 설정

이 페이지에서는 권한에 대한 개요를 제공.합니다.설정이끝나 "Apply" 버튼을 눌러 적용하십시오. 새 사용자 이름과 암호로 웹 인터페이스에 로그인하면 그림 4-2-7 의 화면이 나타납니다.

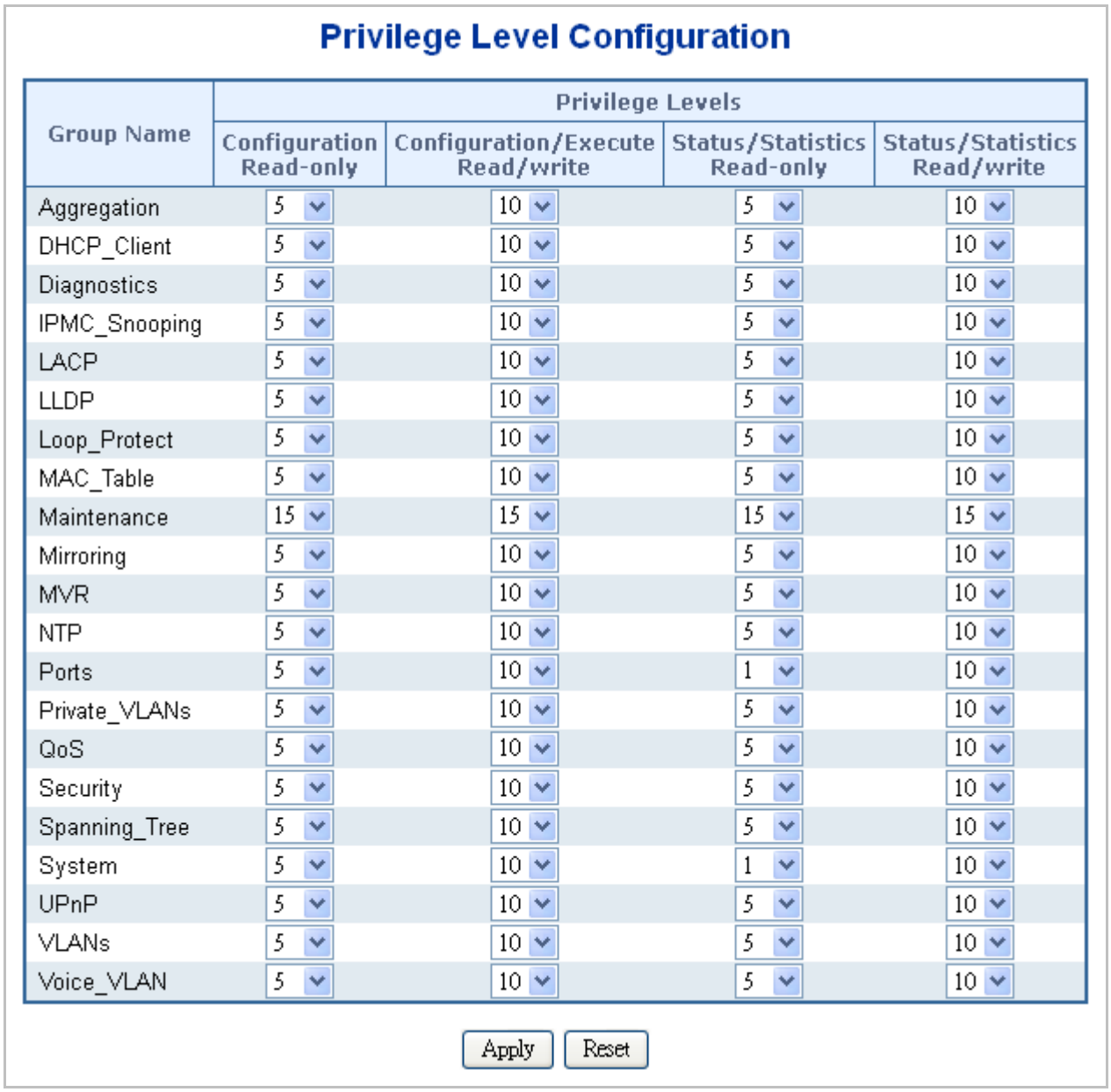


그림 4-2-7: 권한 설정 구성 화면

이 페이지는 다음과 같습니다.

목표	설명
• **Group Name**	권한 그룹을 식별하는 이름. 대부분의 경우 권한 수준 그룹은 단일 모듈 (예 : LACP, RSTP 또는 QoS)로 구성되지만 그 중 일부는 둘 이상을 포함합니다. 다음 설명에서는 이러한 권한 수준 그룹을 세부적으로 정의합니다.:**보안성**:인증, 시스템 접근 관리,포트(Dot1x 포트, MAC 기반 및 MAC 주소 제한 포함), ACL, HTTPS, SSH, ARP 검사 및 IP 소스 가드.

	■ **IP**: '핑(ping)'을 제외한 모든것 ■ **Port**: 'VeriPHY'를 제외한 모든 것. ■ **Diagnostics**: 'ping' 과 'VeriPHY'. ■ **Maintenance**:CLI-시스템 제부팅, 시스템 기본값 복원, 시스템 암호, 구성 저장, 구성 로드, 펌웨어로드. 웹사용자,권한 단계와 모든 것을 유지관리. ■ **Debug**: CLI 에서 만 존재.
• **Privilege Level**	모든 권한 수준 그룹에는 다음 하위 그룹에 대한 권한 단계가 있습니다.: ■ **읽기전용으로 구성** ■ **읽기-쓰기를 실행하여 구성** ■ **상태/통계 읽기 쓰기** ■ **상태/통계 읽기-쓰기** (예: 통계 지우기).

버튼

Apply: 변경사항을 저장하려면 클릭합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.2.6 NTP 설정

이 페이지에서 NTP 를 구성하십시오. NTP 는 컴퓨터 시스템의 시계를 동기화하기위한 네트워크 프로토콜 인 Network Time Protocol 의 머리 글자입니다. NTP 는 UDP (데이터 그램)를 전송 계층으로 사용합니다. NTP 서버를 지정할 수 있습니다. 그림 4-2-8 의 NTP Configuration (NTP 구성) 화면이 나타납니다.

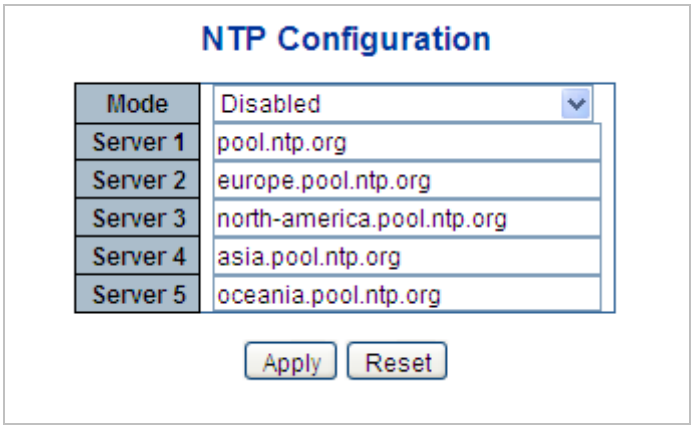


그림 4-2-8: NTP 구성 화면

이 페이지에는 다음을 포함합니다.:

목적	설명
• **Mode**	NTP 모드 작동을 나타냅니다. 가능한 방법은 다음과 같습니다.:

	■ **Enabled**: NTP 모드를 작동합니다. NTP 를 활성화하면 에이전트는 동일한 서브넷 도메인에 있지 않을 경우 클라이언트와 서버간에 전달하고 NTP 메시지를 전송합니다. ■ **Disabled**: NTP 모드의 작동을 중지합니다.
• **Server #**	이 스위치의 NTP IPv4 또는 IPv6 주소를 제공하십시오. IPv6 주소는 콜론 (:)이 각 필드 (:)를 구분하여 최대 네 개의 16 진수로 된 8 개의 필드로 표현되는 128 비트 레코드에 있습니다. 예 : 'fe80 :: 215 : c5ff : fe03 : 4dc7'. '::'기호는 연속 된 0 의 여러 16 비트 그룹을 나타내는 약식 방법으로 사용할 수있는 특수 구문입니다. 그러나 그것은 한 번 나타날 수 있습니다. 또한 다음과 같은 법적 IPv4 주소를 사용했습니다. 예 : ':: 192.1.2.34'..

버튼

Apply: 변경사항을 저장하려면 클릭합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.2.7 시간 설정

이 페이지에서 표준 시간대를 구성하십시오. 시간대는 법적, 상업적 및 사회적 목적을 위해 일정한 표준 시간을 갖는 지역입니다. 긴밀한 상업적 또는 기타 의사 소통의 영역이 동일한 시간을 유지하는 것이 편리하므로 시간대는 국가 및 세분의 경계를 따르는 경향이 있습니다. 그림 4-2-9 의 시간대 구성 화면이 나타납니다.

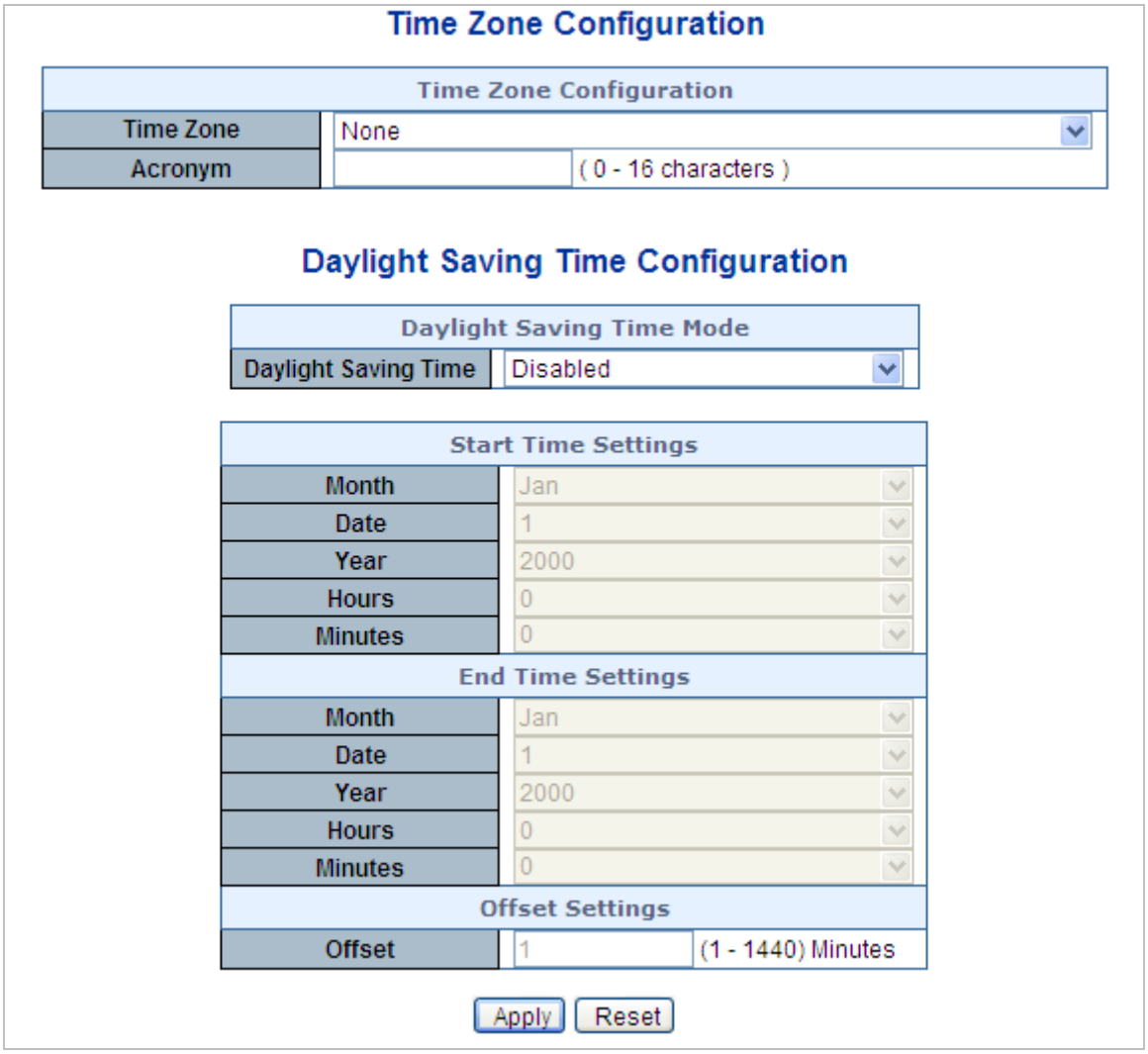


그림 4-2-9: 시간 설정 화면

이 페이지에는 다음을 포함합니다.:

목적	설명
• **Time Zone**	전 세계의 다양한 시간대를 나열합니다. 드롭 다운에서 적절한 시간대를 선택하고 설정 저장을 클릭하십시오.
• **Acronym**	사용자는 시간대의 약어를 설정할 수 있습니다. 이것은 시간대를 식별하기 위해 사용자가 구성 할 수있는 두문자어입니다. (범위 : 최대 16 자)
• **Daylight Saving Time**	이것은 정의 된 일광 절약 시간 동안 아래 설정 한 구성에 따라 시계를 앞으로 또는 뒤로 설정하는 데 사용됩니다. 일광 절약 시간 설정을 사용하지 않으려면 '사용 안 함'을 선택하십시오. '반복'을 선택하고 일광 절약 시간 기간을 구성하여 매년 구성을 반복하십시오. 'Non-Recurring'을 선택하고 일회성 구성을 위해 일광 절약 시간을 설정하십시오. (기본값 : Disabled).
• **Start Time Settings**	• **Week** – 시작 주 번호를 선택합니다. • **Day** – 시작 일을 선택합니다.. • **Month** – 시작 달을 선택합니다..

	• **Hours** – 시작 시간을 선택합니다. • **Minutes** – 시작 분을 선택합니다.
• **End Time Settings**	• **Week** – 한주의 끝번호를 선택합니다. • **Day** – 종료 일을 선택합니다. • **Month** – 종료 달을 선택합니다. • **Hours** – 종료 시간을 선택합니다. • **Minutes** – 종료 분을 선택합니다.
• **Offset Settings**	일광 절약 시간 동안 추가 할 시간 (분)을 입력하십시오. (범위 : 1 ~ 1440)

버튼

Apply: 변경사항을 저장하려면 클릭합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.2.8 UPnP

이 페이지에서 UPnP 를 구성하십시오. UPnP 는 Universal Plug and Play 의 약자입니다. UPnP 의 목표는 장치를 원활하게 연결하고 가정에서의 네트워크 구현 (데이터 공유, 통신 및 엔터테인먼트)을 단순화하고 기업 환경에서 컴퓨터 구성 요소 설치를 단순화하는 것입니다. 그림 4-2-10 의 UPnP Configuration (UPnP 구성) 화면이 나타납니다.

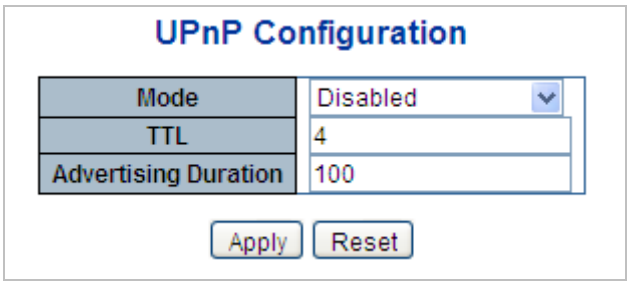


그림 4-2-10: UPnP 설정 화면

이 페이지에는 다음을 포함합니다.

목표	설명
• **Mode**	UPnP 작동 모드를 나타냅니다. 가능한 모드는 다음과 같습니다: ■ **Enabled**: UPnP 모드 작동을 활성화합니다. ■ **Disabled**: UPnP 모드 작동을 비활성화합니다. 모드가 활성화되면 두 개의 ACE 가 자동으로 추가되어 UPnP 관련 패킷을 CPU 에 트랩합니다. 모드가 비활성화되면 ACE 가 자동으로 제거됩니다..

• **TTL**	TTL 값은 SSDP 광고 메시지를 보내기 위해 UPnP 에서 사용됩니다. 유효한 값은 1 - 255 입니다.
• **Advertising Duration**	SSDP 패킷에서 수행되는 지속 시간은 제어 지점 또는 제어 지점에 이 스위치에서 SSDP 광고 메시지를받는 빈도를 알리는 데 사용됩니다. 컨트롤 포인트가 지속 시간 내에 아무런 메시지도 받지 못하면 스위치가 더 이상 존재하지 않는다고 생각할 것입니다. UDP 의 신뢰할 수없는 특성으로 인해 표준에서 광고 지속 시간의 절반 이하에서 광고 새로 고침을 수행하는 것이 좋습니다. 이 구현에서 스위치는 광고 지속 시간에서 30 초를 뺀 간격으로 주기적으로 SSDP 메시지를 보냅니다. 유효한 값은 100 - 86400 입니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

0

그림 4-2-11: UPnP 가 Windows My Network Place 에서 보여지는 모습

4.2.9 DHCP 릴레이

이 페이지에서 DHCP 릴레이를 구성하십시오. DHCP 릴레이는 동일한 서브넷 도메인에 있지 않을 때 클라이언트와 서버간에 DHCP 메시지를 전달하고 전송하는 데 사용됩니다.
DHCP 옵션 82 는 DHCP 릴레이 에이전트가 클라이언트 DHCP 패킷을 DHCP 서버로 전달할 때 DHCP 요청 패킷에 특정 정보를 삽입하고 서버 DHCP 패킷을 DHCP 클라이언트로 전달할 때 DHCP 응답 패킷에서 특정 정보를 제거 할 수있게합니다. DHCP 서버는이 정보를 사용하여 IP 주소 또는 기타 할당 정책을 구현할 수 있습니다. 특히이 옵션은 두 개의 하위 옵션을 설정하여 작동합니다.:

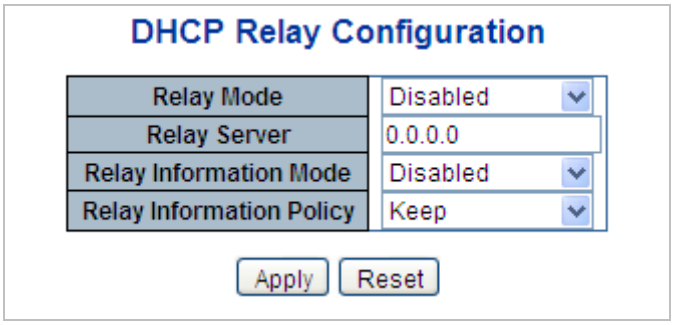
- **순환 ID (option 1)**
- **원격 ID (option2).**

순환 ID 의 하위 옵션에는 요청이 들어온 회로에 대한 정보가 포함되어 있습니다.

원격 ID 의 하위 옵션에는 회로의 원격 호스트 끝과 관련된 정보를 전달하도록 설계되었습니다. .

스위치의 회선 ID 정의는 길이가 4 바이트이고 형식은 "vlan_id" "module_id" "port_no"입니다. "vlan_id"의 매개 변수는 VLAN ID 를 나타내는 처음 두 바이트입니다. "module_id"매개 변수는 모듈 ID 의 세 번째 바이트입니다. "port_no"의 매개 변수는 네 번째 바이트이며 포트 번호를 의미합니다.

원격 ID 의 길이는 6 바이트이며 값은 DHCP 릴레이 에이전트의 MAC 주소와 동일합니다. 그림 4-2-12 의 DHCP Relay Configuration (DHCP 릴레이 구성) 화면이 나타납니다.



화면 4-2-12 DHCP Relay Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Relay Mode**	DHCP 릴레이 모드 작업을 나타냅니다. 가능한 모드는 다음과 같습니다. ■ **Enabled**: DHCP 릴레이 모드 작동을 활성화합니다. DHCP 릴레이 모드 작업을 활성화하면 에이전트는 동일한 서브넷 도메인에 있지 않을 때 클라이언트와 서버간에 DHCP 메시지를 전달하고 전송합니다. 그리고 DHCP 브로드 캐스트 메시지는 고려 된 보안을 위해 범람하지 않을 것입니다. ■ **Disabled**: DHCP 릴레이 모드 작동을 비활성화하십시오.
• **Relay Server**	DHCP 릴레이 서버 IP 주소를 나타냅니다. DHCP 릴레이 에이전트는 동일한 서브넷 도메인에 있지 않을 때 클라이언트와 서버간에 DHCP 메시지를 전달하고 전송하는 데 사용됩니다.
• **Relay Information Mode**	DHCP 릴레이 정보 모드 옵션 작업을 입니다. 가능한 모드는 다음과 같습니다: ■ **Enabled**: DHCP 릴레이 정보 모드 작동을 사용합니다. DHCP 릴레이 정보 모드 작동을 활성화 할 때 에이전트는 DHCP 서버로 전달할 때 DHCP 메시지에 특정 정보 (option82)를 삽입하고 DHCP 클라이언트로 전송할 때 DHCP 메시지에서 제거합니다. DHCP 릴레이 작동 모드에서만 작동합니다. ■ **Disabled**: DHCP 릴레이 정보 모드 작업을 비활성화합니다.
• **Relay Information Policy**	DHCP 릴레이 정보 옵션 정책을 나타냅니다. DHCP 릴레이 정보 모드 작동을 활성화 할 때 에이전트가 이미 릴레이 에이전트 정보가 들어있는 DHCP 메시지를 수신하는 경우. 정책을 집행 할 것입니다. DHCP 릴레이 정보 작동 모드에서만 작동합니다. 가능한 정책은 다음과 같습니다.: ■ **Replace**: 기존 릴레이 정보를 포함하고있는 DHCP 메시지를 받을 때 기존의 릴레이 정보를 교체하십시오. ■ **Keep**: 원래의 릴레이 정보를 이미 포함하고 있는 DHCP 메시지를 받을 때 유지하십시오. ■ **Drop**: 릴레이 정보가 이미 포함 된 DHCP 메시지를 받을 때 패키지를 버립니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.2.10 DHCP 릴레이 통계

이 페이지는 DHCP 릴레이에 대한 통계를 제공합니다. 그림 4-2-13 의 DHCP Relay Statistics 화면이 나타납니다..

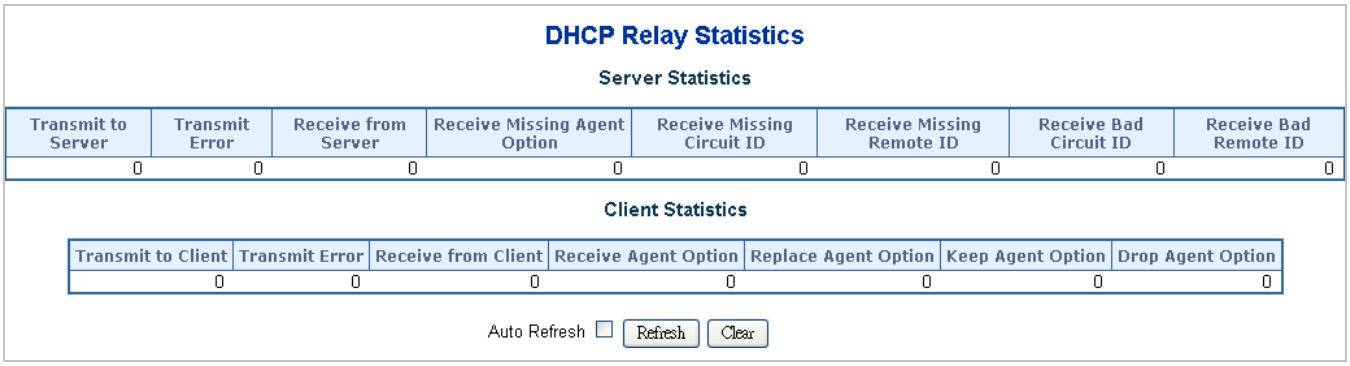


그림 4-2-13: DHCP Relay Statistics 구성화면

이 페이지에서는 다음과 같음을 나타냅니다.:

서버 통계

목적	설명
• **Transmit to Server**	Client 에서 서버로 중계 된 패킷 번호.
• **Transmit Error**	Client 에서 패킷을 보내는 동안 발생하는 오류의 패킷번호 입니다.
• **Receive from Server**	서버로부터 패킷을 수신 한 패킷 수.
• **Receive Missing Agent Option**	에이전트 정보 옵션없이 패킷을 수신 한 패킷 번호입니다.
• **Receive Missing Circuit ID**	연동 ID 옵션이 누락 된 패킷을 수신 한 패킷 번호.
• **Receive Missing Remote ID**	원격 ID 옵션이 누락 된 패킷을 수신 한 패킷 수.
• **Receive Bad Circuit ID**	회로 ID 옵션이 알려진 회로 ID 와 일치하지 않는 패킷 번호입니다.
Receive Bad Remote ID	원격 ID 옵션이 알려진 원격 ID 와 일치하지 않는 패킷 번호.

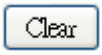
클라이언트 통계

목적	설명
• **Transmit to Client**	서버에서 클라이언트로 패킷을 전달한 패킷 번호입니다.
• **Transmit Error**	패킷을 서버로 잘못 보낸 패킷 번호입니다.
• **Receive from Client**	서버로부터 패킷을 수신 한 패킷 수.
• **Receive Agent Option**	릴레이 에이전트 정보 옵션을 사용하여 패킷을받은 패킷 번호입니다
• **Replace Agent Option**	수신 된 패킷을 릴레이 에이전트 정보 옵션으로 바꾼 패킷 번호.
• **Keep Agent Option**	릴레이 에이전트 정보 옵션을 사용하여 수신 된 패킷을 보존 한 패킷 번호.
• **Drop Agent Option**	릴레이 에이전트 정보 옵션을 사용하여 수신 패킷을 삭제 한 패킷 번호입니다.

버튼

Auto-refresh  : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

: 즉시 페이지를 새로고침합니다.



: 모든 통계 항목을 지웁니다..

4.2.11 CPU 로드

이 페이지는 SVG 그래프를 사용하여 CPU 로드를 표시합니다. 부하는 마지막 100ms, 1sec 및 10 초 간격으로 평균으로 측정됩니다. 마지막 120 개의 samles 가 그래프로 표시되고 마지막 숫자도 텍스트로 표시됩니다. SVG 그래프를 표시하려면 브라우저가 SVG 형식을 지원해야합니다. 브라우저 지원에 대한 자세한 내용은 SVG Wiki 를 참조하십시오. 특히, 작성 당시에는 Microsoft Internet Explorer 에 SVG 를 지원하는 플러그인이 설치되어 있어야합니다. 그림 4-2-14 의 CPU Load 화면이 나타납니다.

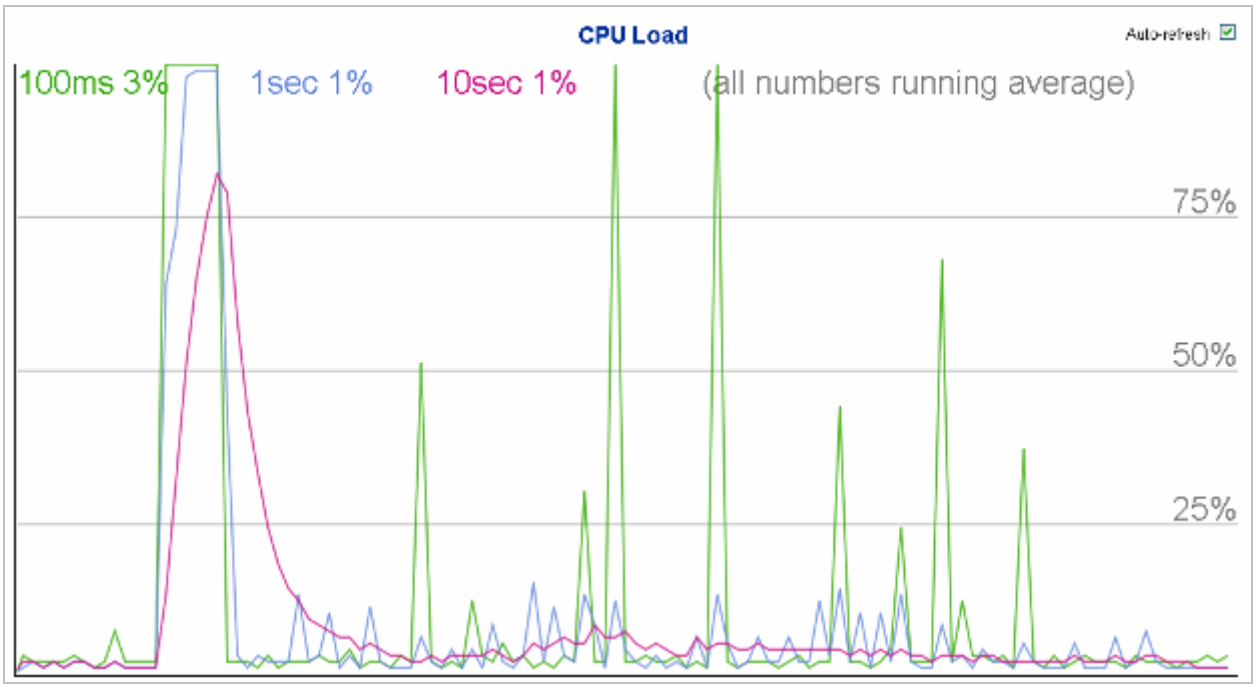


그림 4-2-14: CPU 로드 출력 화면

버튼

Auto-refresh ☐ : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Note

브라우저가이 페이지에 아무 것도 표시 할 수 없으면 Adobe SVG 도구를 다운로드하여 컴퓨터에 설치하십시오.

4.2.12 시스템 로그

관리형 스위치 시스템 로그 정보가 여기에 제공 되며 그림 4-2-15 의 시스템 로그 화면이 나타납니다.

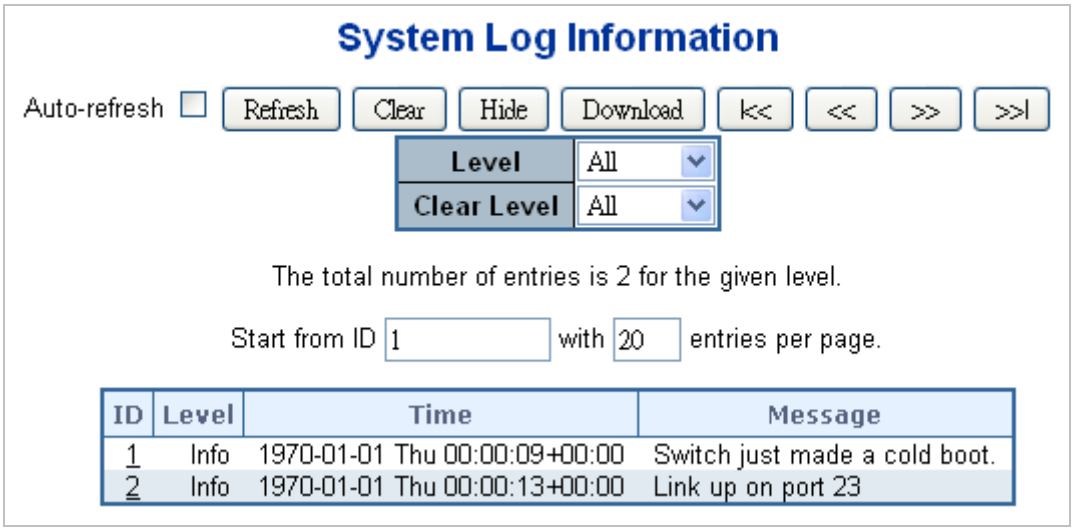


그림 4-2-15: 시스템 로그 정보 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **ID**	시스템 로그 항목의 ID (>=1).
• **Level**	시스템 로그 항목의 단계, 지원 되는 단계 유형은 다음과 같습니다.: ■ **Info**:시스템 로그의 정보 수준. ■ **Warning**:시스템 로그의 경고 수준. ■ **Error**:시스템 로그의 오류 수준. ■ **All**: 모든 단계
• **Clear Level**	시스템 로그 항목의 단계를 지우고 지원레벨 유형은 다음과 같습니다.: ■ **Info**: 시스템 로그의 정보 수준 ■ **Warning**: 시스템 로그의 경고 수준 ■ **Error**: 시스템 로그의 오류 수준 ■ **All**: 모든 수준
• **Time**	시스템 로그 항목의 시간
• **Message**	시스템 로그 항목의 메시지.

버튼

Auto-refresh ☐ : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Refresh : 현재 ID 항목부터 시스템 로그 항목을 업데이트 합니다.

Clear : 전체 로그 항목을 선택하여 초기화합니다

Hide : 선택된 로그 전체 항목을 숨깁니다

Download : 선택된 로그 전체 항목을 다운로드합니다

|<<: 사용 가능한 첫 번째 항목 ID 부터 시스템 로그 항목을 업데이트합니다.

<<: 현재 표시된 마지막 항목에서 끝나는 시스템 로그 항목을 업데이트합니다..

>>: 현재 표시된 마지막 항목부터 시스템 로그 항목을 업데이트합니다.

>>|: 시스템 로그 항목을 업데이트하고 마지막으로 사용 가능한 항목 ID 로 끝납니다.

4.2.13 상세한 로그

관리형 스위치 시스템의 자세한 로그정보는 여기에 나와 있습니다. 그림 4-2-16 의 상세로그 화면이 나타납니다..

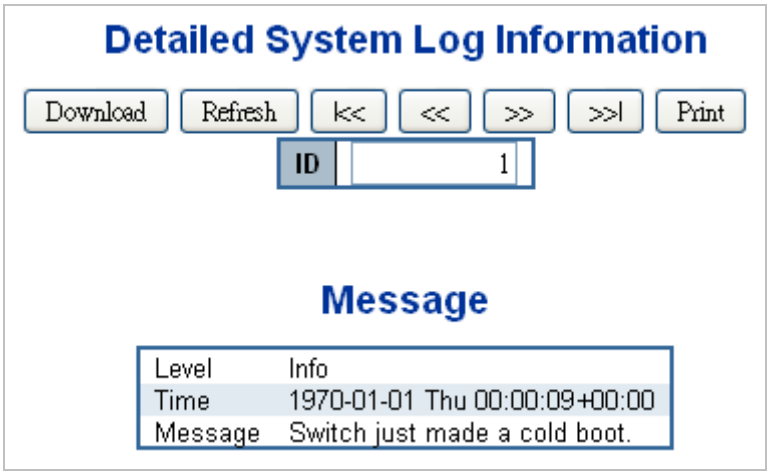


그림 4-2-15: 상세로그 페이지 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **ID**	시스템 로그 항목의 ID (> = 1).
• **Message**	시스템 로그 항목의 메시지

버튼

Download: 시스템 로그 항목을 현재 ID 항목으로 다운로드 하십시오.

Refresh: 시스템 로그 항목을 현재 항목 ID 로 업데이트 합니다.

|<<: 시스템 로그 항목을 사용 가능한 첫 번째 항목 ID 로 업데이트합니다.

<<: 시스템 로그 항목을 이전에 사용 가능한 항목 ID 로 업데이트합니다.

>>: 시스템 로그 항목을 다음 사용 가능한 항목 ID 로 업데이트합니다.

>>|: 시스템 로그 항목을 마지막으로 사용 가능한 항목 ID 로 업데이트합니다.

Print: 시스템 로그 항목을 현재 항목 ID 로 인쇄하십시오.

4.2.14 원격 Syslog

이 페이지에서 원격 syslog 를 구성하십시오. 그림 4-2-17 의 Remote Syslog 화면이 나타납니다..

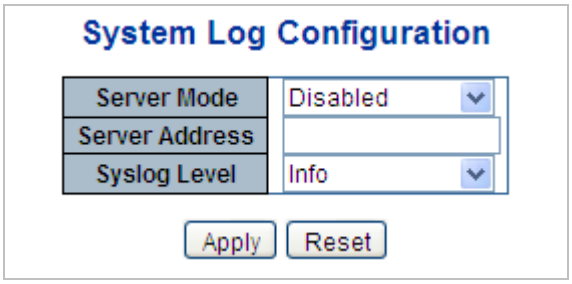


그림 4-2-17: 원격 Syslog 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Mode**	서버 모드 조작을 나타냅니다. 모드 작업이 활성화되면 syslog 메시지가 syslog 서버로 전송됩니다. syslog 프로토콜은 UDP 통신을 기반으로하며 UDP 포트 514 에서 수신되며 UDP 는 연결이없는 프로토콜이고 수신 확인을 제공하지 않으므로 syslog 서버는 수신인에게 다시 응답을 보내지 않습니다. syslog 서버가없는 경우에도 syslog 패킷은 항상 발송됩니다. 가능한 모드는 다음과 같습니다.: ■ **Enabled**: 원격 syslog 모드 작동을 활성화합니다. ■ **Disabled**: 원격 syslog 모드 작동을 비활성화합니다..
• **Syslog Server IP**	syslog 서버의 IPv4 호스트 주소를 나타냅니다. 스위치가 DNS 기능을 제공하면 호스트 이름이 될 수도 있습니다.
• **Syslog Level**	Syslog 서버에 보낼 메시지의 종류를 나타냅니다. 가능한 모드는 다음과 같습니다.: ■ **Info**: 정보와 경고 및 오류를 보냅니다/.. ■ **Warning**: 오류와 경고를 보냅니다 ■ **Error**: 오류를 보냅니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.2.15 SMTP 설정

이 페이지는 스위치의 SMTP 구성을 용이하게합니다. 그림 4-2-18 의 SMTP 구성 화면이 나타납니다..

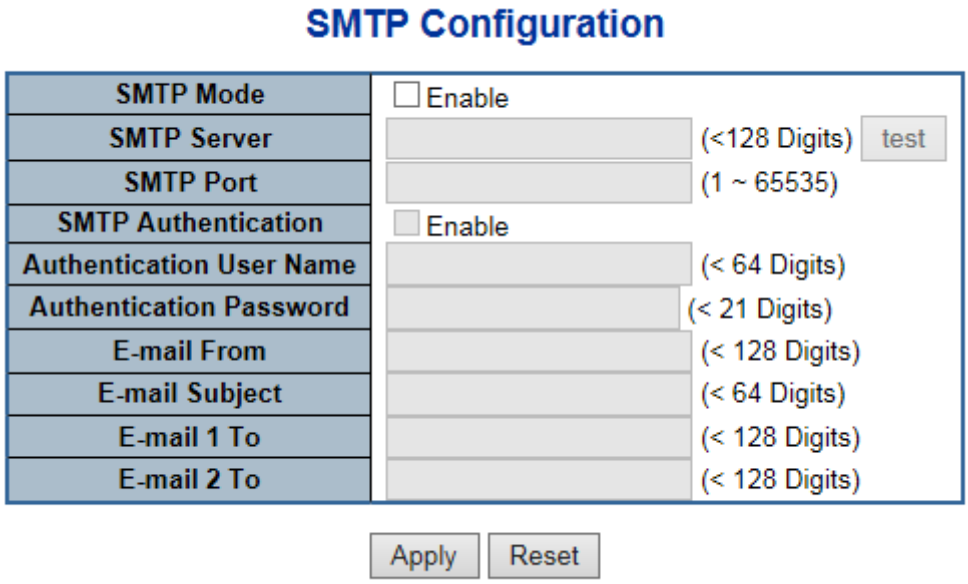


그림 4-2-18: SMTP 설정 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **SMTP Mode**	이 스위치에서 SMTP 를 사용하지 여부를 제어합니다
• **SMTP Server**	SMTP 서버의 SMTP 서버이름 또는 IP,주소를 입력하십시오
• **SMTP Port**	SMTP 서비스의 포트번호를 설정합니다.
• **SMTP Authentication**	SMTP 인증 사용 여부 제어 전자 메일을 보낼 때 인증이 필요한 경우입니다.
• **Authentication User Name**	인증이 되는 경우 SMTP 서버의 사용자 이름을 입력하십시오.
• **Authentication Password**	인증이 되는 경우 SMTP 서버의 암호를 입력하십시오.
• **E-mail From**	보낸 사람의 전자 메일 주소를 입력하십시오. 이주소는 답신에 해당됩니다.
• **E-mail Subject**	전자메일의 주제/제목을 입력하십시오.
• **E-mail 1 To**	수신자의 이메일 주소를 입력하십시오.
• **E-mail 2 To**	

버튼

test: 테스트 메일을 메일 서버로 보내 이계정이 사용가능한지 확인합니다.

Save: 변경사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.2.16 웹 펌웨어 업그레이드

이 페이지는 스위치를 제어하는 펌웨어의 업데이트를 용이하게합니다. 그림 4-2-19 의 웹 펌웨어 업그레이드 화면이 나타납니다..

그림 4-2-19: 웹 펌웨어 업그레이드 화면

펌웨어 업그레이드 화면을 열려면 다음을 수행하십시오:

1. **System 클릭** -> Web **Firmware Upgrade**.
2. Firmware Upgrade 화면이 그림 4-2-19. 처럼 나타날것입니다.
3. 메인페이지에 있는 "Browse" 버튼을 클릭하여 펌웨어를 선택하여 불러옵니다..
4. 불러온 다음 "Upload".를 클릭하면 소프트웨어 업로드 진행 상태가 업로드 상태로 표시합니다.
5. 소프트웨어 시스템에 성공적으로 로드되면 다음화면이 나타납니다. 시스템은 재부팅 후 새 소프트웨어를 로드합니다..

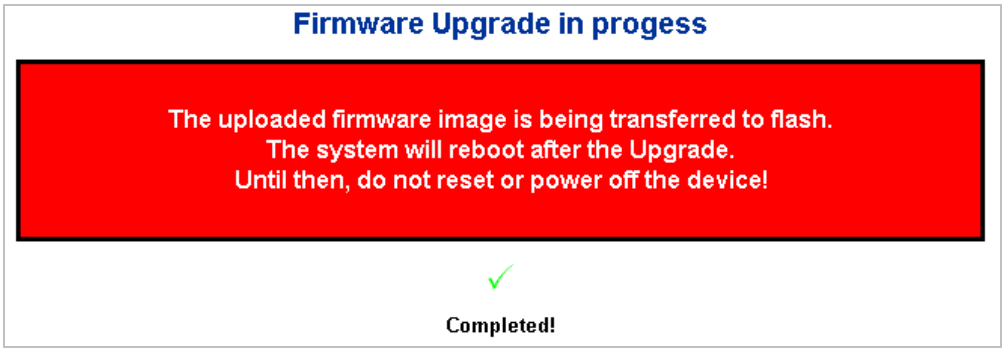


그림 4-2-20: 소프트웨어 로드 성공 알림 화면

Note 소프트웨어를 업그레이드 하는 동안 전원을 끄면 안됩니다.

Note 이미지가 로드 된후 "확인" 버튼을 누르지 않고 펌웨어 업그레이드 페이지를 종료하지 마십시오. 또는 시스템이 새 펌웨어를 적용하지 않습니다. 사용자는 펌웨어 업그레이들 프로세스를 반복해야합니다.

4.2.17 TFTP 펌웨어 업그레이드

펌웨어 업그레이드 페이지는 사용자가 네트워크의 TFTP 서버에서 Managed Switch 펌웨어를 업데이트 할 수있는 기능을 제공합니다. 업데이트하기 전에 TFTP 서버를 준비하고 펌웨어 이미지가 TFTP 서버에 있는지 확인하십시오. 그림 4-2-21 의 TFTP 펌웨어 업그레이드 화면이 나타납니다..

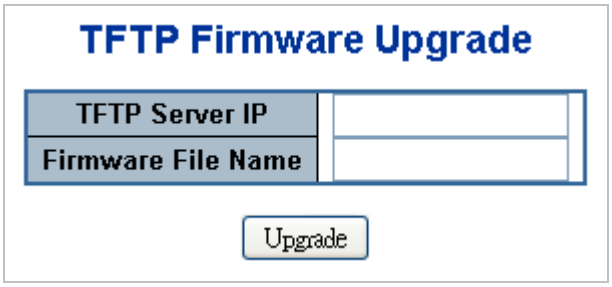


그림 4-2-20: TFTP 펌웨어 업그레이드 페이지 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **TFTP Server IP**	TFTP 서버 IP 주소를 입력하십시오
• **Firmware File Name**	펌웨어 이미지의 이름 (최대 길이 :24 자)

버튼

Upgrade: 클릭하여 업그레이드를 진행합니다.

Note 업데이트 진행이 완료 될 때까지 관리 대상 스위치의 전원을 끄지 마십시오.

Note 이미지가 로드 된 후 "확인"버튼을 누르지 않고 펌웨어 업그레이드 페이지를 종료하지 마십시오. 또는 시스템이 새 펌웨어를 적용하지 않습니다. 사용자는 펌웨어 업그레이드 프로세스를 반복해야합니다.

4.2.18 시작 설정 값 저장

이 기능을 사용하면 현재 구성을 저장할 수 있으므로 그림 4-2-22 의 다음 재부팅 화면에서 현재 활성 구성을 사용할 수 있습니다. 구성을 저장하면 그림 4-2-23 의 화면이 나타납니다..

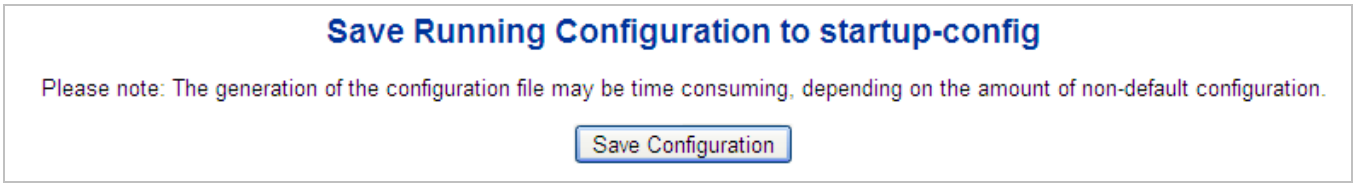


그림 4-2-22: 설정 저장 화면 캡처

그림 4-2-23: 저장이 끝난 화면

4.2.19 다운로드 설정

스위치는 구성을 CLI,형식의 여러 텍스트 파일에 저장합니다. 파일은 가상 (RAM) 이거나 스위치의 플레시에 저장됩니다.

- running-config: 스위치의 현재 활성 구성을 나타내는 가상 파일입니다. 이 파일은 휘발성입니다.
- startup-config. 스위치의 시작 구성이며 부팅시 읽습니다.
- default-config: 공급 업체별 구성을 갖는 읽기 전용 파일입니다. 이 파일은 시스템이 기본 설정으로 복원 될 때 읽습니다.

또한 최대 두 개의 다른 파일을 저장하고 running-config 에 적용하여 구성을 전환 할 수도 있습니다.
Configuration Download 페이지에서는 스위치의 running-config, startup-config 및 default-config 를 다운로드 할 수 있습니다. 아래 그림 4-2-24 를 참조하십시오..

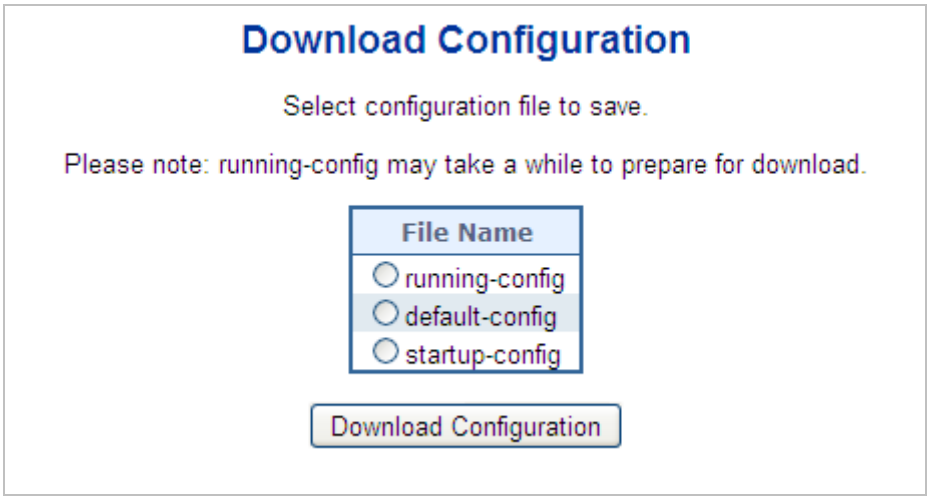


그림 4-2-24: 구성 다운로드 페이지

4.2.20 설정 업로드

구성 업로드 페이지에서 스위치의 running-config 및 startup-config 를 업로드 할 수 있습니다. 아래 그림 4-2-25 를 참조하십시오..

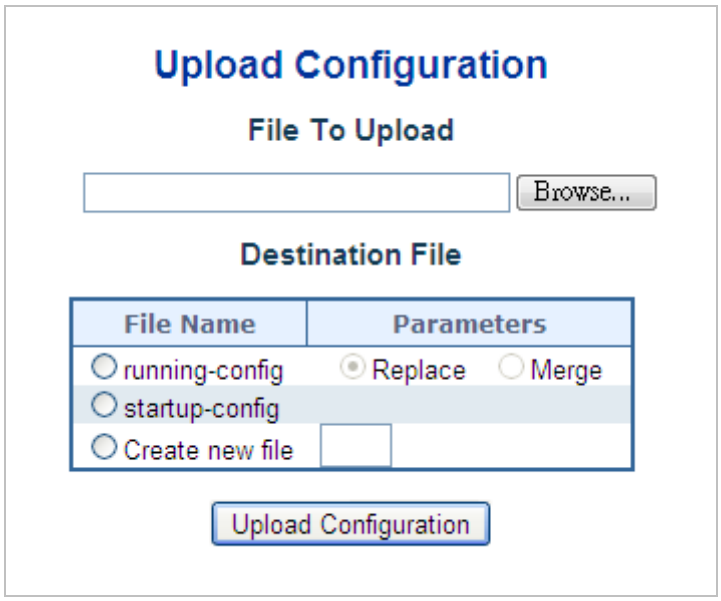


그림 4-2-25: 업로드 설정 화면

대상이 running-config 이면 파일이 스위치 구성에 적용됩니다. 이 작업은 두 가지 방법으로 수행 할 수 있습니다.:

- Replace mode: 현재 구성이 업로드 된 파일의 구성으로 완전히 바뀝니다..
- Merge mode: *running-config*에 업로드 된 파일이 병합됩니다.

파일 시스템이 가득 차면 (위에서 언급 한 세 가지 시스템 파일과 두 개의 다른 파일이 포함 된 경우) 새 파일을 만들 수 없지만 기존 파일을 덮어 쓰거나 다른 파일을 먼저 삭제해야합니다.

4.2.21 활성화 구성

구성 활성화 페이지에서는 스위치에 있는 Startup-config 및 default-config 파일을 활성화 합니다. 아래의 그림 4-2-26 을 참조하십시오.

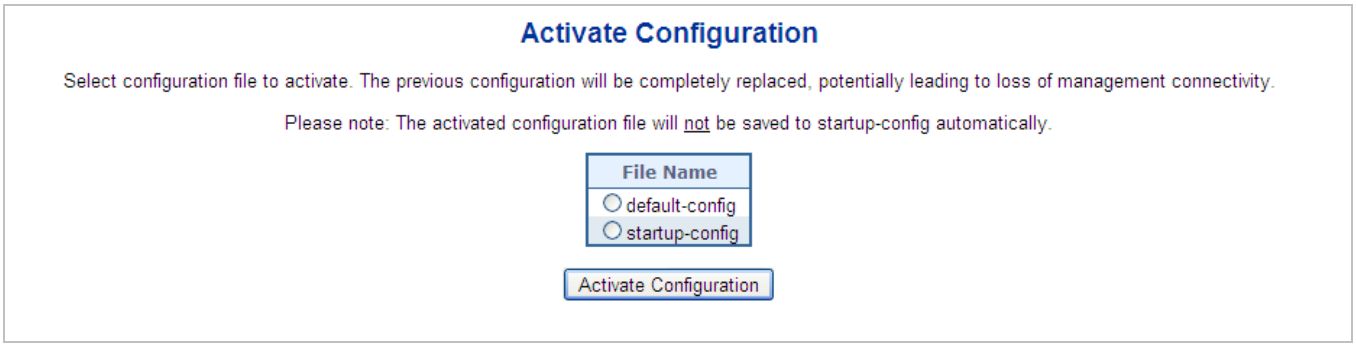


그림 4-2-26: 구성화면 활성화 캡처

현재 활성 구성을 나타내는 running-config 를 제외하고 스위치에있는 구성 파일을 활성화 할 수 있습니다.

활성화 할 파일을 선택하고 Activate Configuration 를 클릭하십시오. 그러면 기존 구성을 선택한 파일의 구성으로 완전히 대체하는 프로세스가 시작됩니다.

4.2.22 구성 삭제

구성 삭제 페이지에서는 FLASH 에 저장된 startup-config 및 default-config 파일을 삭제할 수 있습니다. 이 작업이 완료되고 이전 저장 작업없이 스위치가 재부팅되면 스위치가 기본 구성으로 스위치를 효과적으로 재설정합니다. 아래 그림 4-2-27 을 참조하십시오.

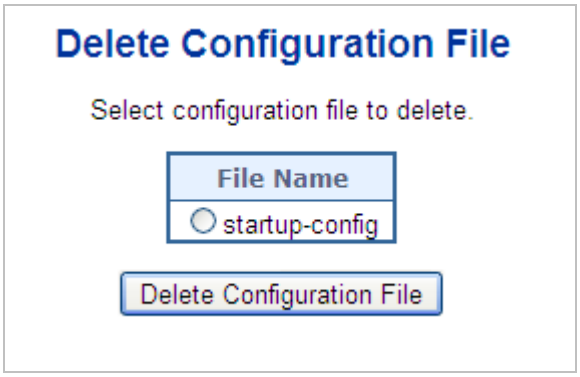


그림 4-2-27: 구성 삭제 화면

4.2.23 이미지 선택하기

이 페이지는 장치의 활성 및 대체 (백업) 펌웨어 이미지에 대한 정보를 제공하며 대체 이미지로 되돌릴 수 있습니다. 웹 페이지는 활성 및 대체 펌웨어 이미지에 대한 정보가있는 두 개의 테이블을 표시합니다. 그림 4-2-28 의 이미지 선택 화면이 나타납니다..

Note

활성 펌웨어 이미지가 대체 이미지 인 경우 "활성 이미지"테이블 만 표시됩니다. 이 경우 대체 이미지 활성화 버튼도 비활성화됩니다.

Note

1. 대체 이미지가 활성화 된 경우 (기본 이미지 손상 또는 수동 개입으로 인해) 장치에 새 펌웨어 이미지를 업로드하면 자동으로 기본 이미지 슬롯이 사용되어 활성화됩니다..
2. 펌웨어 버전 및 날짜 정보는 이전 펌웨어 릴리스의 경우 비어있을 수 있습니다. 이것은 오류를 구성하지 않습니다.

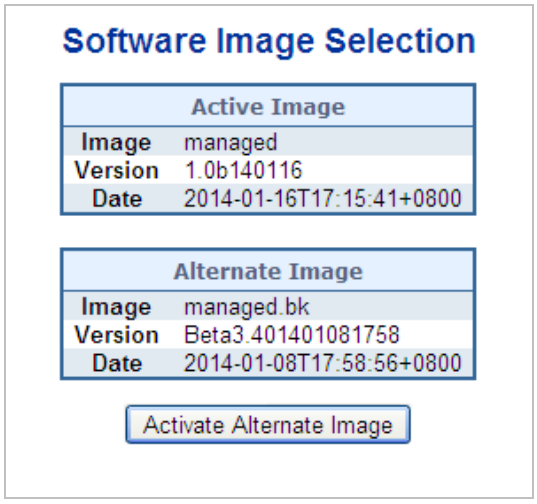


그림 **4-2-28:** Software Image Selection 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Image**	펌웨어 이미지의 플래시 색인 이름입니다. 주 (선호) 이미지의 이름은 image 이며, 대체 이미지의 이름은 image.bk 입니다.
• **Version**	펌웨어 이미지의 버전.
• **Date**	펌웨어가 생성 된 날짜.

버튼

: 대체 이미지를 사용하려면 Activate Alternate Image 클릭하십시오. 이 버튼은 시스템 상태에 따라 비활성화 될 수 있습니다..

4.2.24 공장 초기화

이 페이지에서 관리 대상 스위치의 구성을 재설정 할 수 있습니다. IP 구성 만 유지됩니다. 새로운 구성을 즉시 사용할 수 있으므로 다시 시작할 필요가 없습니다. 그림 4-2-29 의 Factory Default 화면이 나타납니다..

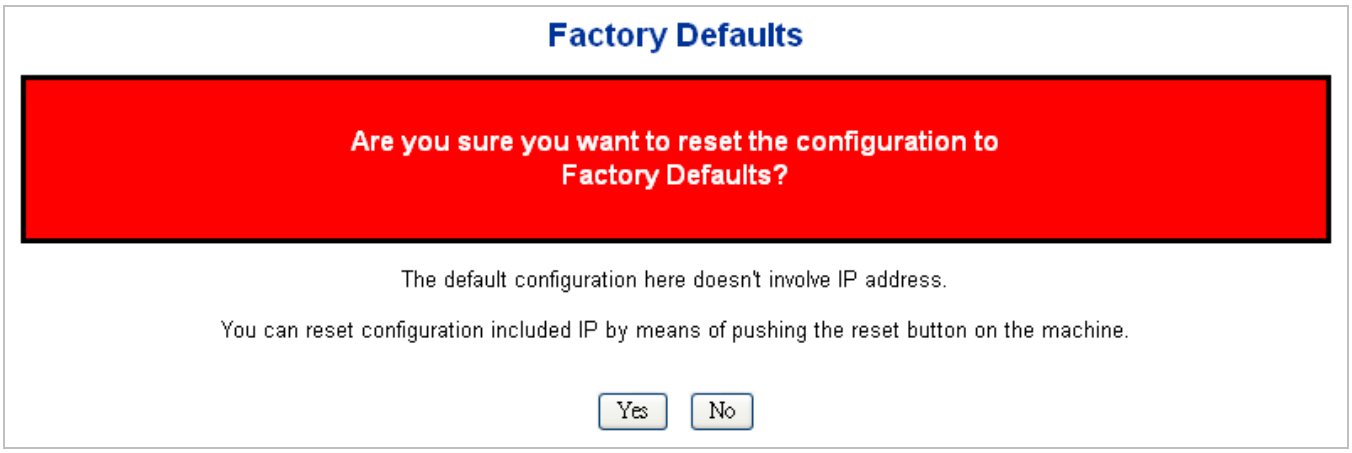


그림 4-2-29: 공장 초기화 화면

버튼

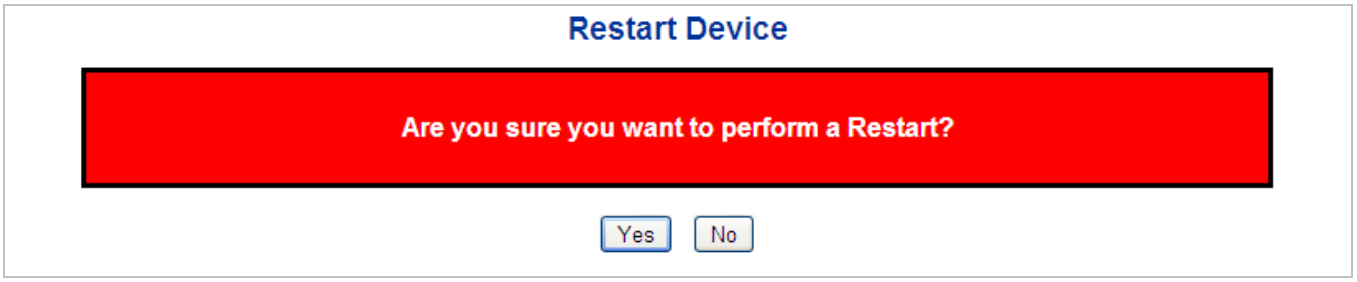
Yes: 공장초기화를 설정하여 리셋하겠습니다.

No: 구성을 재설정 하지 않고 포트상태페이지로 돌아가려면 클릭하십시오.

Note 관리 대상 스위치를 공장 출하시 기본 설정으로 재설정하려면 전면 패널에서 하드웨어 재설정 버튼을 약 10 초 동안 누를 수도 있습니다. 장치가 재부팅 된 후 192.168.0.xx 의 동일한 서브넷에서 관리 웹 인터페이스에 로그인 할 수 있습니다.

4.2.25 시스템 리부팅

재부팅 페이지를 사용하면 원격 위치에서 장치를 재부트 할 수 있습니다. 재부팅 버튼을 누르면 약 60 초 후에 WEB 인터페이스에 다시 로그인해야하며 그림 4-2-30 의 시스템 재부팅 화면이 나타납니다.



화면 4-2-30: 시스템 리부팅 화면

버튼

Yes: 시스템을 리부팅하려면 클릭합니다.

No: 시스템을 재부팅하지 않고 돌아가시려면 클릭하십시오

Note 전면 패널에서 SYS LED 를 확인하여 시스템이 완전히로드되었는지 여부를 확인할 수도 있습니다. SYS LED 가 깜박이면 펌웨어로드 단계에 있습니다. SYS LED 표시등이 켜지면 WEB 브라우저를 사용하여 Managed Switch 에 로그인 할 수 있습니다.

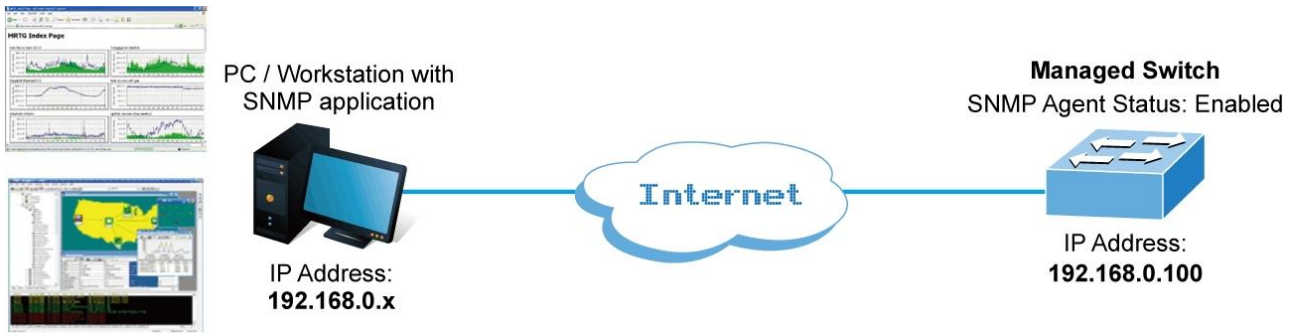
4.3 SNMP(Simple Network Management Protocol)

4.3.1 SNMP 개요

SNMP (Simple Network Management Protocol)는 네트워크 장치간에 관리 정보를 쉽게 교환 할 수있는 응용 프로그램 계층 프로토콜입니다. TCP / IP (Transmission Control Protocol / Internet Protocol) 프로토콜 제품군의 일부입니다. SNMP 를 통해 네트워크 관리자는 네트워크 성능을 관리하고 네트워크 문제를 찾고 해결하며 네트워크 성장을 계획 할 수 있습니다.

SNMP 관리 네트워크는 NMS (Network Management Station), SNMP 에이전트, MIB (Management Information Base) 및 네트워크 관리 프로토콜의 세 가지 핵심 구성 요소로 이루어져 있습니다 :

- **Network management stations (NMSs) : 콘솔이라고도 하는 이 장치는 네트워크 요소를 모니터하고 제어하는 관리 응용 프로그램을 실행합니다. 물리적으로 NMS 는 일반적으로 빠른 CPU, 메가 픽셀 컬러 디스플레이, 상당한 메모리 및 풍부한 디스크 공간을 갖춘 워크 스테이션 용 컴퓨터입니다. 각 관리되는 환경에는 하나 이상의 NMS 가 있어야합니다.**
- **Agents : 에이전트는 네트워크 요소에 상주하는 소프트웨어 모듈입니다. 네트워크 요소가 수신 한 오류 패킷 수와 같은 관리 정보를 수집하고 저장합니다.**
- **Management information base (MIB) : MIB 는 가상 정보 저장소에 상주하는 관리 대상 객체의 모음입니다. 관련 관리 객체의 컬렉션은 특정 MIB 모듈에서 정의됩니다.**
- **Network-management protocol : 관리 프로토콜은 에이전트와 NMS 간에 관리 정보를 전달하는 데 사용됩니다. SNMP 는 인터넷 커뮤니티의 사실상 표준 관리 프로토콜입니다.**



SNMP 운영

SNMP 자체는 간단한 요청 / 응답 프로토콜입니다. NMS 는 응답을받지 않고 여러 요청을 보낼 수 있습니다.

- **Get** -- NMS 가 에이전트에서 개체 인스턴스를 검색 할 수있게합니다.
- **Set** -- NMS 가 에이전트 내의 개체 인스턴스 값을 설정할 수 있습니다.
- **Trap** -- NMS 에 비동기 적으로 이벤트를 알리기 위해 에이전트에서 사용합니다. SNMPv2 트랩 메시지는 SNMPv1 트랩 메시지를 대체하도록 설계되었습니다.

SNMP community

SNMP 커뮤니티는 SNMP 를 실행하는 장치 및 관리 스테이션이 속한 그룹입니다. 정보가 전송되는 위치를 정의하는 데 도움이됩니다. 커뮤니티 이름은 그룹을 식별하는 데 사용됩니다. SNMP 장치 또는 에이전트는 둘 이상의 SNMP

커뮤니티에 속할 수 있습니다. 해당 커뮤니티 중 하나에 속하지 않는 관리 스테이션의 요청에 응답하지 않습니다. SNMP 기본 커뮤니티는 다음과 같습니다.:

- **Write** = 사적허용
- **Read** = 공적허용

SNMP 메뉴를 사용하여 Managed Switch의 SNMP 기능을 표시하거나 구성하십시오. 이 섹션에는 다음 항목이 있습니다.:

■ **System Configuration**	이 페이지에서 SNMP 를 설정합니다.
■ **Trap Configuration**	이 페이지에서 SNMP 트랩을 설정합니다.
■ **System Information**	시스템 정보는 여기서 제공됩니다
■ **SNMPv3 Communities**	SNMPv3 Communities 를 사용합니다.
■ **SNMPv3 Users**	이 페이지에서 SNMPv3 users table 를 설정합니다..
■ **SNMPv3 Groups**	이 페이지에서 SNMPv3 groups table 를 설정합니다.
■ **SNMPv3 Views**	이 페이지에서 SNMPv3 views table 를 설정합니다
■ **SNMPv3 Access**	이 페이지에서 SNMPv3 accesses table 를 설정합니다.

4.3.2 SNMP 시스템 설정

이 페이지에서 SNMP 를 구성하십시오. 그림 4-3-1 의 SNMP System Configuration (SNMP 시스템 구성) 화면이 나타납니다..

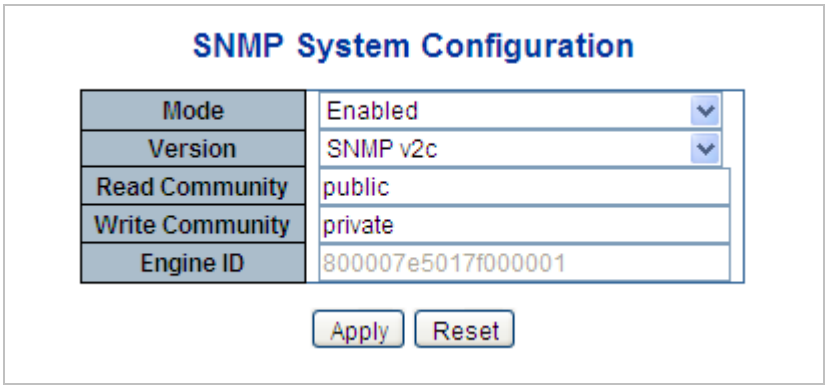


그림 4-3-1: SNMP 시스템 설정 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Mode**	SNMP 모드 작업을 나타냅니다. 가능한 모드는 다음과 같습니다.: ■ **Enabled**: SNMP 모드 작동을 활성화합니다.. ■ **Disabled**: SNMP 모드 작동을 비활성화합니다.
• **Version**	SNMP 를 지원하는 버전을 이야기합니다. ■ **SNMP v1**: SNMP v1 을 지원합니다. ■ **SNMP v2c**: SNMP 2c 를 지원합니다. ■ **SNMP v3**: SNMP 3 를 지원합니다.

• **Read Community**	SNMP 에이전트에 대한 액세스를 허용하는 커뮤니티 읽기 액세스 문자열을 나타냅니다. 허용되는 문자열 길이는 0 에서 255 까지이며 허용되는 내용은 33 에서 126 까지의 ASCII 문자입니다. 이 필드는 SNMP 버전이 SNMPv1 또는 SNMPv2c 인 경우에만 적용됩니다. SNMP 버전이 SNMPv3 인 경우 커뮤니티 문자열이 SNMPv3 커뮤니티 테이블과 연결됩니다. SNMPv1 또는 SNMPv2c 커뮤니티 문자열보다 더 유연하게 보안 이름을 구성 할 수 있습니다. 커뮤니티 문자열 외에 특정 범위의 소스 주소를 사용하여 소스 서브넷을 제한 할 수 있습니다.
• **Write Community**	SNMP 에이전트에 대한 액세스를 허용하는 커뮤니티 쓰기 액세스 문자열을 나타냅니다. 허용되는 문자열 길이는 0 에서 255 까지이며 허용되는 내용은 33 에서 126 까지의 ASCII 문자입니다. 이 필드는 SNMP 버전이 SNMPv1 또는 SNMPv2c 인 경우에만 적용됩니다. SNMP 버전이 SNMPv3 인 경우 커뮤니티 문자열이 SNMPv3 커뮤니티 테이블과 연결됩니다. SNMPv1 또는 SNMPv2c 커뮤니티 문자열보다 더 유연하게 보안 이름을 구성 할 수 있습니다. 커뮤니티 문자열 외에 특정 범위의 소스 주소를 사용하여 소스 서브넷을 제한 할 수 있습니다.
• **Engine ID**	SNMPv3 엔진 ID 를 나타냅니다. 문자열에는 10 에서 64 자의 16 진수 사이의 짝수를 포함해야하지만 모두 0 과 all -F 는 허용되지 않습니다. 엔진 ID 를 변경하면 모든 원래 로컬 사용자가 지워집니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.3.3 SNMP 트랩 설정

이 페이지에서 SNMP 트랩을 구성하십시오. 그림 4-3-2 의 SNMP 트랩 구성 화면이 나타납니다..

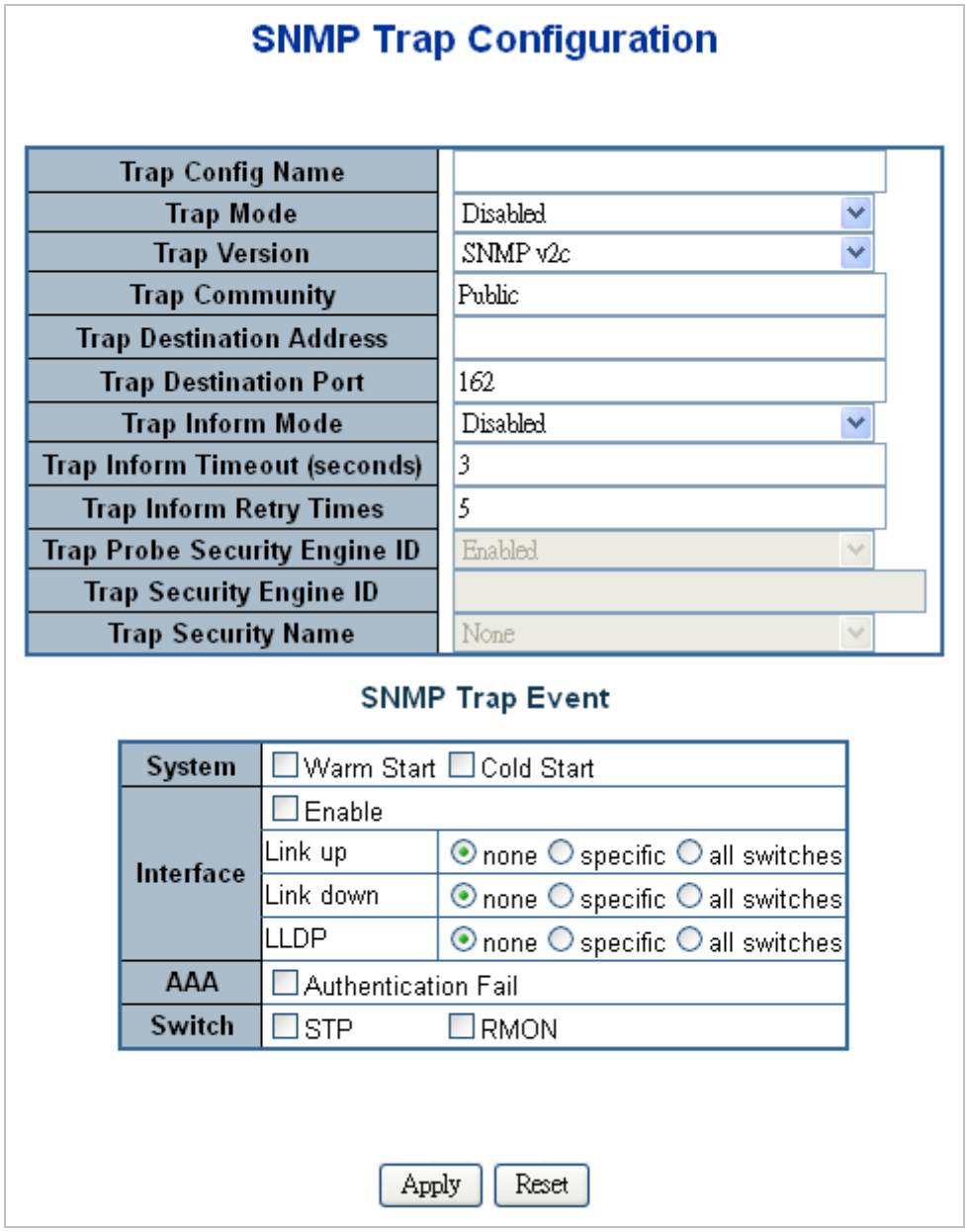


그림 **4-3-2:** SNMP 트랩 구성 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Trap Config**	구성을위한 트랩 구성의 이름을 나타냅니다. 허용되는 문자열 길이는 0 에서 255 까지이며 허용되는 내용은 33 에서 126 까지의 ASCII 문자입니다.
• **Trap Mode**	SNMP 트랩 모드 작동을 나타냅니다. 가능한 모드는 다음과 같습니다.: ■ **Enabled**: SNMP trap 모드 작동을 활성화합니다 ■ **Disabled**: SNMP trap 모드 작동을 비활성화합니다.
• **Trap Version**	SNMP 트랩 지원 버전을 나타냅니다. 가능한 버전은 다음과 같습니다:

	■ **SNMP v1**: SNMP v1 로 설정합니다. ■ **SNMP v2c**: SNMP v2c 로 설정합니다.. ■ **SNMP v3**: SNMPv3 로 설정합니다..
• **Trap Community**	SNMP 트랩 패킷을 보낼 때 커뮤니티 액세스 문자열을 나타냅니다. 허용되는 문자열 길이는 0 에서 255 까지이며 허용되는 내용은 33 에서 126 까지의 ASCII 문자입니다.
• **Trap Destination Address**	SNMP 트랩 대상 주소를 나타냅니다.
• **Trap Destination Port**	SNMP 트랩 목적지 포트를 나타냅니다. SNMP 에이전트가이 포트를 통해 SNMP 메시지를 보내면 포트 범위는 1 ~ 65535 입니다.
• **Trap Inform Mode**	SNMP 트랩 정보 모드 작업을 나타냅니다. 가능한 모드는 다음과 같습니다.: ■ **Enabled**: SNMP 인증 실패를 사용합니다. ■ **Disabled**: SNMP 인증 실패를 비활성화합니다..
• **Trap Inform Timeout (seconds)**	트랩정보에 대한 시간초과를 알립니다 **0** 에서 **2147** 까지의 허용범위가 있습니다..
• **Trap Inform Retry Times**	재 시도 시간을 알리는 SNMP 트랩을 나타냅니다. 허용되는 범위는 0 에서 255 까지입니다.
• **Trap Probe Security Engine ID**	SNMPv3 트랩 프로브 보안 엔진 ID 작동 모드를 나타냅니다. 가능한 값은 다음과 같습니다.: ■ **Enabled**: SNMP 트랩 프로브 보안 엔진 ID 작동 모드를 사용합니다. ■ **Disabled**: SNMP 트랩 프로브 보안 엔진 ID 작동 모드를 비활성화합니다.
• **Trap Security Engine ID**	SNMP 트랩 보안 엔진 ID 를 나타냅니다. SNMPv3 은 인증 및 개인 정보 보호를 위해 USM 을 사용하여 트랩 및 알림을 전송합니다. 이러한 트랩 및 정보에 대한 고유 한 엔진 ID 가 필요합니다. "트랩 프로브 보안 엔진 ID"가 활성화되면 ID 가 자동으로 검색됩니다. 그렇지 않으면이 필드에 지정된 ID 가 사용됩니다. 문자열에는 10 과 64 사이의 자릿수가있는 짝수 (16 진수 형식)가 포함되어야하지만 모두 0 및 all- 'F 는 허용되지 않습니다.
• **Trap Security Name**	SNMP 트랩 보안 이름을 나타냅니다. SNMPv3 은 USM 을 사용하여 인증 및 개인 정보를 보호합니다. 트랩 및 알림을 사용하는 경우 고유 한 보안 이름이 필요합니다.
• **System**	인터페이스 그룹의 트랩을 활성화 / 비활성화합니다. 가능한 함정은 다음과 같습니다. ■ **Warm Start**: Warm Start trap 을 활성화/ 비활성화합니다.. ■ **Cold Start**: Cold Start trap 을 활성화/비활성화합니다..
• **Interface**	인터페이스 그룹의 트랩을 나타냅니다. 가능한 트랩은 다음과 같습니다.: ■ **Link Up**: 링크 업 트랩에 대하여 활성화/비활성화를 합니다. ■ **Link Down**: 링크 업 트랩을 활성화합니다. ■ **LLDP**: LLDP 트랩을 활성화/ 비활성화합니다.
• **AAA**	AAA 그룹의 함정을 나타냅니다. 가능한 함정은 다음과 같습니다.:

	Authentication Fail : SNMP 트랩 인증 실패 트랩을 활성화 / 비활성화합니다.
• **Switch**	스위치 그룹의 트랩을 나타냅니다 가능한 트랩은 이렇습니다.: ■ **STP**: STP 트랩을 활성화/비활성화합니다.. ■ **RMON**: RMON 트랩을 활성화/비활성화합니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.3.4 SNMP 시스템 정보

스위치 시스템 정보는 여기에 나와 있습니다. 그림 4-3-3 의 SNMP System Information 화면이 나타납니다..

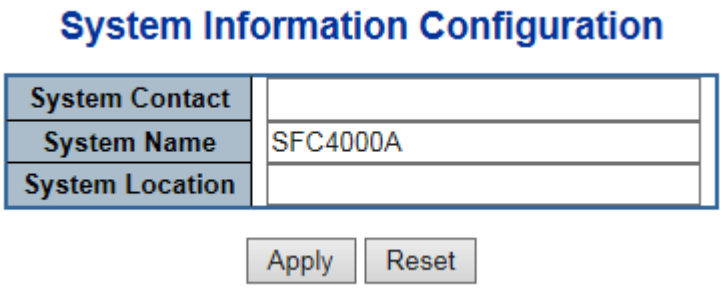


그림 4-3-3: 시스템 정보 설정 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **System Contact**	이 관리 노드에 대한 담당자의 텍스트 식별 정보와 해당 담당자에게 연락하는 방법에 대한 정보. 허용되는 문자열 길이는 0 에서 255 까지이며 허용되는 내용은 32 에서 126 까지의 ASCII 문자입니다.
• **System Name**	이 관리 노드의 관리 상 지정된 이름. 규칙에 따라이 노드의 정규화 된 도메인 이름입니다. 도메인 이름은 알파벳 (A-Za-z), 숫자 (0-9), 빼기 기호 (-)로 그려지는 텍스트 문자열입니다. 공백 문자는 이름의 일부로 사용할 수 없습니다. 첫 번째 문자는 알파 문자 여야합니다. 첫 번째 또는 마지막 문자는 빼기 기호가 아니어야합니다. 허용되는 문자열 길이는 0 에서 255 까지입니다.
• **System Location**	이 노드의 물리적 위치 (예 : 전화 실 3 층). 허용되는 문자열 길이는 0 에서 255 까지이며 허용되는 내용은 32 에서 126 까지의 ASCII 문자입니다.

4.3.5 SNMPv3 설정

4.3.5.1 SNMPv3 Communities

이 페이지에서 SNMPv3 커뮤니티 테이블을 구성하십시오.. 그림 4-3-4 의 SNMPv3 Communities 화면이 나타납니다..

그림 4-3-4: SNMPv3 Communities Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제됩니다.
• **Community**	SNMPv3 에이전트에 대한 액세스를 허용하는 커뮤니티 액세스 문자열을 나타냅니다. 허용되는 문자열 길이는 1 에서 32 이며 허용되는 내용은 33 에서 126 사이의 ASCII 문자입니다. 커뮤니티 문자열은 보안 이름으로 취급되며 SNMPv1 또는 SNMPv2c 커뮤니티 문자열을 매핑합니다.
• **Source IP**	SNMP 액세스 소스 주소를 나타냅니다. 특정 범위의 소스 주소를 사용하여 소스 마스크와 결합 할 때 소스 서브넷을 제한 할 수 있습니다.
• **Source Mask**	SNMP 엑세스 소스 주소 마스크를 나타냅니다.

버튼

Add New Entry: 새 커뮤니티 항목을 추가하려면 클릭하십시오.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.3.5.2 SNMPv3 사용자

이 페이지에서 SNMPv3 사용자 테이블을 구성하십시오. 엔트리 인덱스 키는 엔진 ID 와 사용자 이름입니다. 그림 4-3-5 의 SNMPv3 Users 화면이 나타납니다.

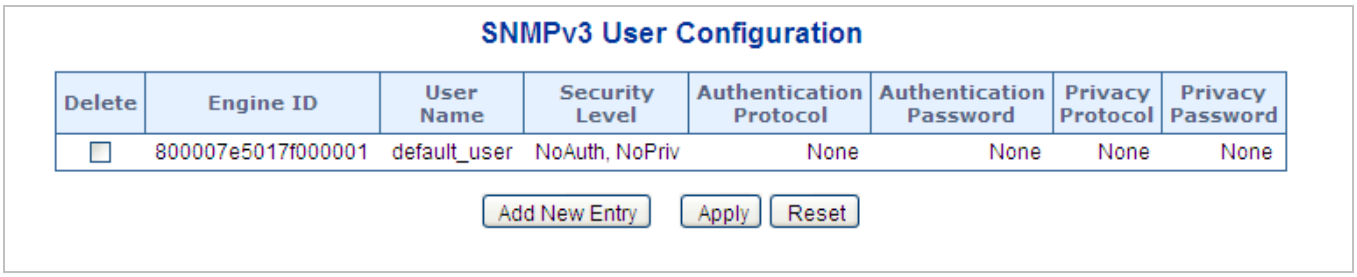


그림 4-3-5: SNMPv3 사용자 설정 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

설정	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제됩니다.
• **Engine ID**	이 항목이 속해야하는 엔진 ID 를 식별하는 8 진수 문자열. 문자열에는 10 과 64 사이의 자릿수가있는 짝수 (16 진수 형식)가 포함되어야하지만 모두 0 및 all- 'F 는 허용되지 않습니다. SNMPv3 아키텍처는 메시지 보안을 위해 사용자 기반 보안 모델 (USM)을 사용하고 액세스 제어를 위해보기 기반 액세스 제어 모델 (VACM)을 사용합니다. USM 항목의 경우 usmUserEngineID 및 usmUserName 이 항목의 키입니다. 간단한 에이전트에서 usmUserEngineID 는 항상 해당 에이전트의 snmpEngineID 값입니다. 이 값은이 사용자가 통신 할 수있는 원격 SNMP 엔진의 snmpEngineID 값을 사용할 수도 있습니다. 즉, 사용자 엔진 ID 가 시스템 엔진 ID 와 같으면 로컬 사용자입니다. 그렇지 않으면 원격 사용자입니다. 이 항목이 속해야하는 사용자 이름을 식별하는 문자열. 허용되는 문자열 길이는 1 에서 32 까지이며 허용되는 내용은 33 에서 126 까지의 ASCII 문자입니다.
• **User Name**	이 항목이 속해야하는 사용자 이름을 식별하는 문자열. 허용되는 문자열 길이는 1 에서 32 까지이며 허용되는 내용은 33 에서 126 까지의 ASCII 문자입니다.
• **Security Level**	이 항목에 속해야하는 보안 모델을 나타내며 가능한 보안 모델은 다음과 같습니다.: ■ **NoAuth, NoPriv**: 인증 및 개인정보가 없습니다.. ■ **Auth, NoPriv**: 인증 및 개인 정보 보호 ■ **Auth, Priv**: 인증 및 개인 정보 보호 항목이 이미있는 경우 보안 레벨의 값을 수정할 수 없습니다. 즉, 먼저 값이 올바르게 설정되어 있는지 확인해야합니다.

• **Authentication Protocol**	이 항목이 속해야하는 인증 프로토콜을 나타냅니다. 가능한 인증 프로토콜은 다음과 같습니다.: ■ **None**: 인증 프로토콜이 없습니다. ■ **MD5**: 이 사용자가 MD5 인증 프로토콜을 사용함을 나타내는 선택적 플래그. ■ **SHA**: 이 사용자가 SHA 인증 프로토콜을 사용함을 나타내는 선택적 플래그. 항목이 이미있는 경우 보안 레벨의 값을 수정할 수 없습니다. 즉, 먼저 값이 올바르게 설정되어 있는지 확인해야합니다.
• **Authentication Password**	인증 암호 구문을 식별하는 문자열입니다. MD5 인증 프로토콜의 경우 허용되는 문자열 길이는 8 ~ 32 입니다. SHA 인증 프로토콜의 경우 허용되는 문자열 길이는 8 ~ 40 입니다. 허용되는 내용은 33 ~ 126 의 ASCII 문자입니다.
• **Privacy Protocol**	이 항목이 속해야하는 개인 정보 보호 프로토콜을 나타냅니다. 가능한 개인 정보 보호 프로토콜은 다음과 같습니다.: ■ **None**: 개인정보 프로토콜이 없습니다. ■ **DES**: 이 사용자가 DES 인증 프로토콜을 사용자가 사용함을 나타내는 플래그 ■ **AES**: 이 사용자가 AES 인증 프로토콜을 나타냅니다..
• **Privacy Password**	프라이버시 암호 구문을 식별하는 문자열입니다. 허용되는 문자열 길이는 8 ~ 32 이며 허용되는 내용은 ASCII 문자 33 ~ 126 입니다.

버튼

Add New Entry: 새로운 사용자 항목을 추가하려면 클릭하십시오.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.3.5.3 SNMPv3 그룹들

이 페이지에서 SNMPv3 그룹 테이블을 구성하십시오. 항목 인덱스 키는 보안 모델 W 보안 이름입니다. 그림 4-3-6 의 SNMPv3 Groups 화면이 나타납니다..

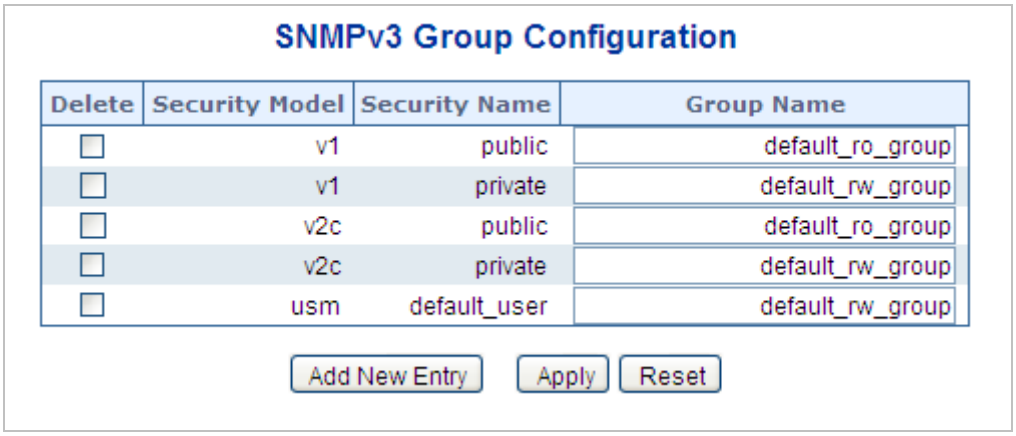


그림 4-3-6: SNMPv3 그룹 설정 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

설정	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제됩니다.
• **Security Model**	: 이 항목이 속해야하는 보안 모델을 나타냅니다. 가능한 보안 모델은 다음과 같습니다. ■ **v1**: SNMPv1. 받습니다 ■ **v2c**: SNMPv2c. 받습니다 ■ **usm**: 사용자 기반의 (USM).
• **Security Name**	이 항목이 속해야하는 보안 이름을 식별하는 문자열. 허용되는 문자열 길이는 1 에서 32 까지이며 허용되는 내용은 33 에서 126 까지의 ASCII 문자입니다.
• **Group Name**	이 항목이 속해야하는 그룹 이름을 식별하는 문자열. 허용되는 문자열 길이는 1 에서 32 까지이며 허용되는 내용은 33 에서 126 까지의 ASCII 문자입니다.

버튼

Add New Entry: 새로운 그룹 엔트리를 만듭니다.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.3.5.4 SNMPv3 Views

이 페이지에서 SNMPv3 보기 테이블을 구성하십시오. 항목 색인 키는보기 이름 W OID 서브 트리입니다. 그림 4-3-7 의 SNMPv3 보기 화면이 나타납니다..

그림 4-3-7: SNMPv3 Views Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제 됩니다.
• **View Name**	이 항목이 속해야하는보기 이름을 식별하는 문자열. 허용되는 문자열 길이는 1 에서 32 까지이며 허용되는 내용은 33 에서 126 까지의 ASCII 문자입니다.
• **View Type**	이 항목이 속해야하는보기 유형을 나타냅니다: ■ **included**:뷰의 하위 트리가 포함 되어야 함을 나타내는 선택적 플래그 ■ **excluded**:뷰의 하위 트리를 제외 해야 함을 나타내는 선택적 플래그 일반적으로보기 항목의보기 유형이 '제외'인 경우보기 유형이 '포함'이고 다른보기 항목이 있어야하며 '제외 된'보기 항목을 초과하는 OID 하위 트리가 있어야합니다.
• **OID Subtree**	이름 첨부 뷰에 추가하는 서브 트리의 루트를 정의하는 OID 입니다. 허용되는 OID 길이는 1 - 128 입니다. 허용되는 문자열 내용은 디지털 번호 또는 별표 (*)입니다.

버튼

Add New Entry: 새로운 view 엔트리를 추가합니다.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.3.5.5 SNMPv3 Access

이 페이지에서 SNMPv3 액세스 테이블을 구성합니다. 항목 색인 키는 그룹 이름, 보안 모델 및 보안 레벨입니다. 그림 4-3-8 의 SNMPv3 Access 화면이 나타납니다..

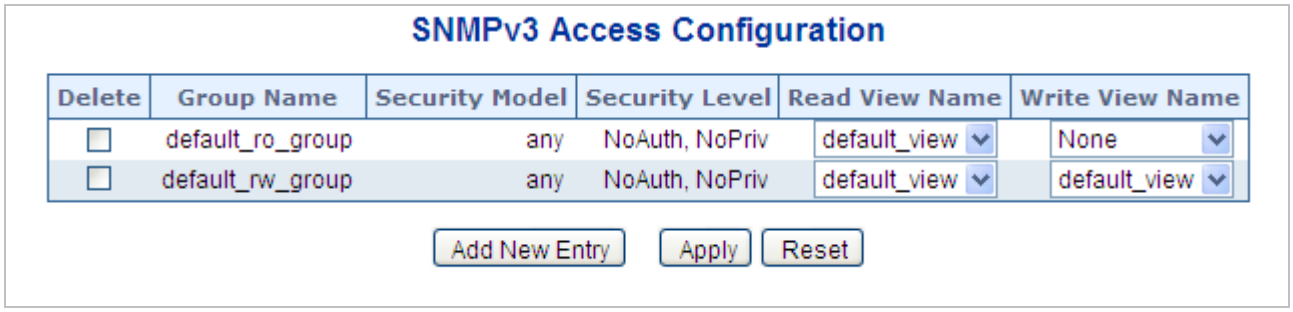


그림 4-3-8: SNMPv3 엑세스 설정 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제됩니다..
• **Group Name**	이 항목이 속해야하는 그룹 이름을 식별하는 문자열. 허용되는 문자열 길이는 1 에서 32 까지이며 허용되는 내용은 33 에서 126 까지의 ASCII 문자입니다.
• **Security Model**	이 항목이 속해야하는 보안 모델을 나타냅니다. 가능한 보안 모델은 다음과 같습니다.: ■ **any**: 보안 모델을 사용합니다. (v1|v2c|usm). ■ **v1**: SNMPv1 용으로 예약되어 있습니다.. ■ **v2c**: SNMPv2c.용으로 예약되어 있습니다. ■ **usm**: 사용자 기반 보안 모델 (USM)
• **Security Level**	이 항목이 속해야하는 보안 모델을 나타냅니다. 가능한 보안 모델은 다음과 같습니다. ■ **NoAuth, NoPriv**:인증 및 개인정보 없음. ■ **Auth, NoPriv**:인증 및 개인 정보 보호.. ■ **Auth, Priv**:인증 및 개인 정보 보호.
• **Read View Name**	이 요청이 현재 값을 요청할 수있는 MIB 개체를 정의하는 MIB 보기의 이름입니다. 허용되는 문자열 길이는 1 에서 32 까지이며 허용되는 내용은 33 에서 126 까지의 ASCII 문자입니다.
• **Write View Name**	이 요청이 잠재적으로 새 값을 설정할 수있는 MIB 객체를 정의하는 MIB 보기의 이름입니다. 허용되는 문자열 길이는 1 에서 32 까지이며 허용되는 내용은 33 에서 126 까지의 ASCII 문자입니다.

버튼

Add New Entry: 새로운 접근방식의 앤트리를 설정합니다.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.4 포트 관리

포트 메뉴를 사용하여 관리형 스위치의 포트를 구성하고 이 부분에는 다음항목이 있습니다.:

- **Port Configuration** 포트 연결 설정 구성
- **Port Statistics Overview** 이더넷 및 RMON 포트 통계를 나열합니다.
- **Port Statistics Detail** 이더넷 및 RMON 포트 통계를 나열합니다.
- **SFP Module Information** SFP 정보 모듈을 나타냅니다.
- **Port Mirror** 미러링을 위한 소스 및 대상 포트 설정

4.4.1 포트 설정

이 페이지에는 현재 포트 구성이 표시됩니다. 포트도 여기서 구성 할 수 있습니다. 그림 4-4-1 의 포트 구성 화면이 나타납니다..

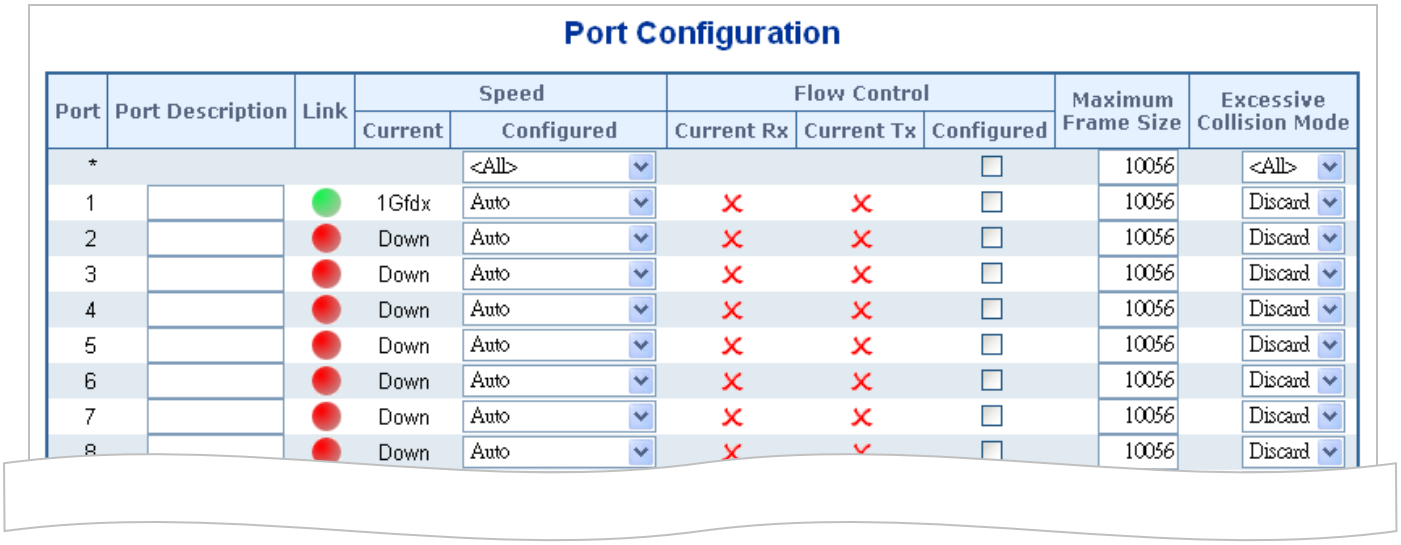


그림 4-4-1: 포트 설정 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	이것은 행의 논리 포트 번호입니다.
• **Port Description**	포트별 설명을 나타냅니다.
• **Link**	현 링크상태가 그래픽으로 표시되며 녹색은 작동중 빨간색은 다운상태를 나타냅니다.
• **Current Link Speed**	포트의 현재 링크속도를 제공합니다.

• **Configured Link Speed**	주어진 스위치 포트에 대해 사용 가능한 링크 속도를 선택하십시오. 메뉴 막대를 그려서 모드를 선택하십시오.. ■ **Auto** - 구리 인터페이스의 자동 협상을 설정합니다. ■ **10Mbps HDX** - 출력 10Mbps / 반이중 모드를 설정합니다. ■ **10Mbps FDX** - 출력 10Mbps / 전이중 모드를 설정합니다. ■ **100Mbps HDX** – 출력 100Mbps/ 반이중 모드를 설정합니다. ■ **100Mbps FDX** – 출력 100Mbps/ 전이중 모드를 설정합니다.. ■ **1Gbps FDX** – 출력 10000Mbps/전이중 모드를 설정합니다.. ■ **Disable** – 포트를 수동으로 종료합니다.
• **Flow Control**	포트에서 자동 속도를 선택하면이 섹션은 링크 파트너에게 알리는 흐름 제어 기능을 나타냅니다. 고정 속도 설정이 선택되면 이것이 사용됩니다. 현재 Rx 열은 포트의 일시 중지 프레임을 따르는 지 여부를 나타내며 현재 Tx 열은 포트의 일시 중지 프레임이 전송되는지 여부를 나타냅니다. Rx 및 Tx 설정은 마지막 자동 협상의 결과에 따라 결정됩니다. 흐름 제어를 사용하도록 구성된 열을 확인하십시오. 이 설정은 구성된 링크 속도 설정과 관련이 있습니다.
• **Maximum Frame Size**	FCS 를 포함하여 스위치 포트에 허용되는 최대 프레임 크기를 입력하십시오. 허용되는 범위는 1518 바이트에서 10056 바이트입니다.
• **Excessive Collision Mode**	포트 전송 충돌 동작을 구성합니다. ■ **Discard**: 16 회의 충돌 후 프레임 폐기(기본값). ■ **Restart**:16 번의 충돌 후에 백오프 알고리즘을 다시 시작합니다.

각 포트가 100M Full, 100M Half, 10M Full 및 10M Half-speed 모드로 실행되도록 설정할 때. Auto-MDIX 기능이 비활성화됩니다.

버튼

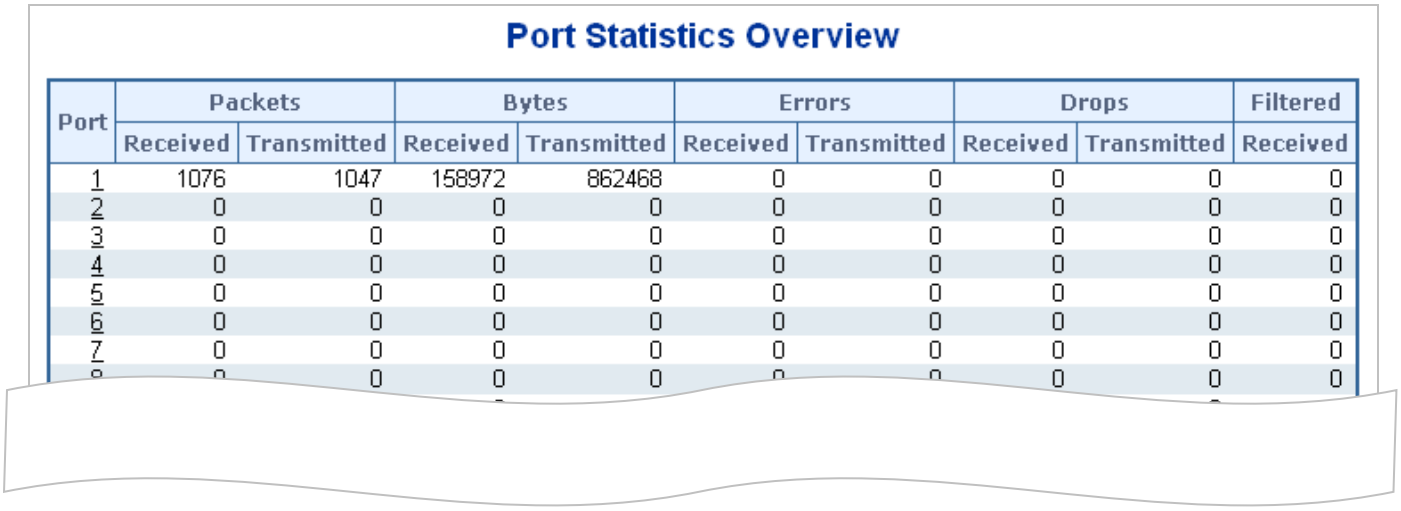
Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

Refresh: 페이지를 새로 고칩니다. 모든 로컬에서 적용됩니다.

4.4.2 포트 통계 개요

이 페이지는 모든 스위치 포트에 대한 일반 트래픽 통계의 개요를 제공합니다. 그림 4-4-2 의 포트 통계 개요 화면이 나타납니다..



Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	1076	1047	158972	862468	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

그림 4-4-2: Port Statistics Overview 화면

위는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	같은 행에 포함 된 설정의 논리 포트 입니다.
• **Packets**	포트당 수신 및 전송 된 패킷의 수를 나타냅니다.
• **Bytes**	포트당 수신 및 전송 된 바이트의 수를 나타냅니다.
• **Errors**	오류로 수신된 프레임의 수와 포트 별 수신된 불안전한 프레임의 수
• **Drops**	진입 또는 송신 혼잡으로 인해 버려진 프레임수입니다.
• **Filtered**	전달 프로세스에 의해 필터링 된 수신 프레임의 수 입니다.

버튼

Download: EXECL 파일로 포트 통계 개요에 관하여 다운받습니다.

Refresh: 즉시 페이지를 새로고침합니다.

Clear: 모든 포트의 카운터를 지웁니다.

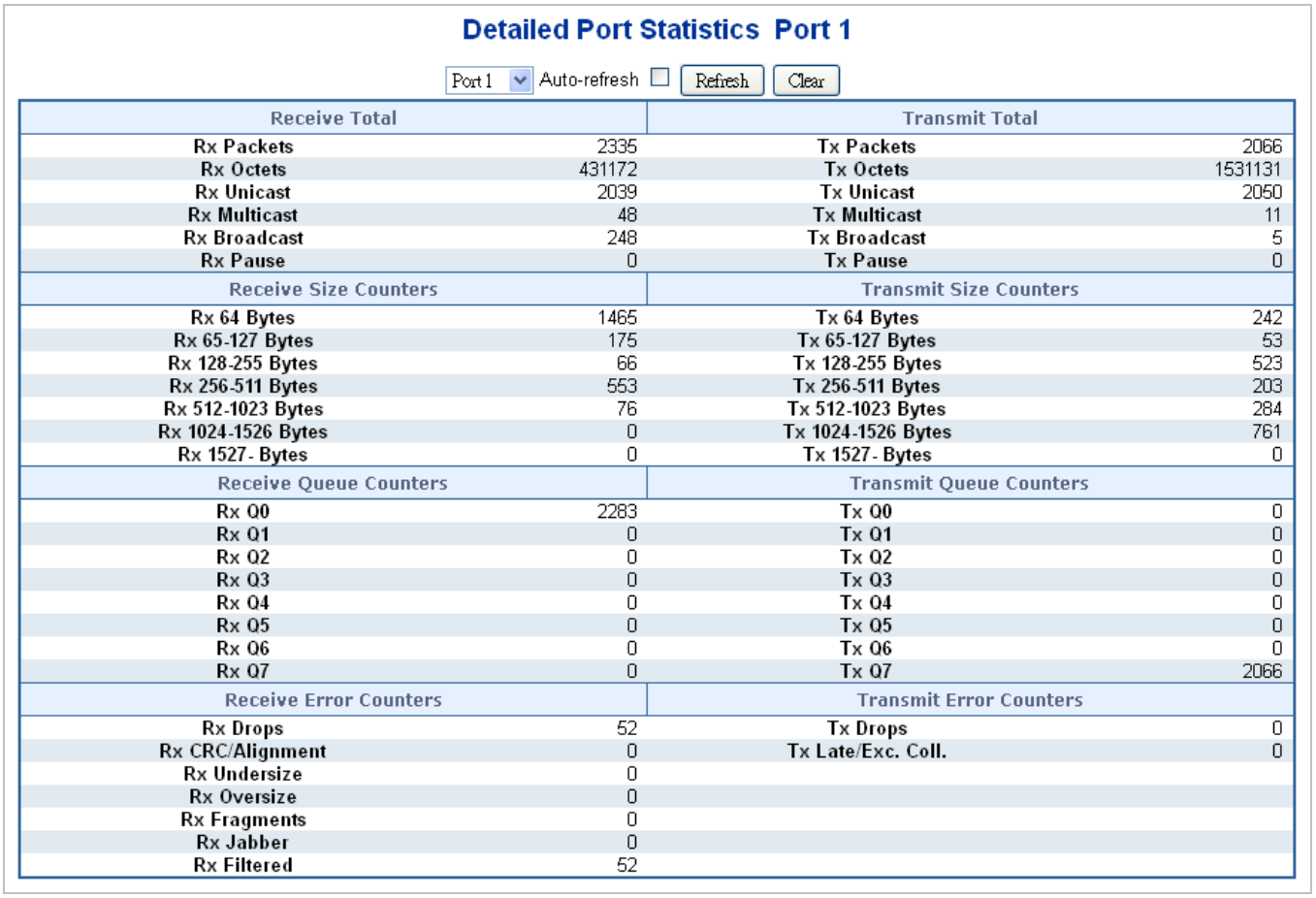
Print: 포트 통계의 결과를 프린트출력합니다.

Auto-refresh : 정기적으로 페이지 자동 새로 고침을 사용하려면 상자를 선택하십시오.

4.4.3 포트 상세 통계

이 페이지는 특정 스위치 포트에 대한 자세한 트래픽 통계를 제공합니다. 포트 선택 상자를 사용하여 표시 할 스위치

포트 세부 정보를 선택하십시오. 표시된 카운터는 수신 및 전송의 합계, 수신 및 전송의 크기 카운터, 수신 및 전송의 오류 카운터입니다. 그림 4-4-3 의 포트 통계 정보 화면이 나타납니다.



Detailed Port Statistics Port 1

Port 1 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	2335	Tx Packets	2066
Rx Octets	431172	Tx Octets	1531131
Rx Unicast	2039	Tx Unicast	2050
Rx Multicast	48	Tx Multicast	11
Rx Broadcast	248	Tx Broadcast	5
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	1465	Tx 64 Bytes	242
Rx 65-127 Bytes	175	Tx 65-127 Bytes	53
Rx 128-255 Bytes	66	Tx 128-255 Bytes	523
Rx 256-511 Bytes	553	Tx 256-511 Bytes	203
Rx 512-1023 Bytes	76	Tx 512-1023 Bytes	284
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	761
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	2283	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	2066
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	52	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	52		

그림 4-4-3: Detailed Port Statistics 포트 1 의 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

수신량과 송신량의 합산

목적	설명
• **Rx and Tx Packets**	수신 및 전송 된 (좋거나 나쁜) 패킷의 수
• **Rx and Tx Octets**	FCS 를 포함하여 수신 및 전송 된 (양호 및 불량) 바이트 수 (프레이밍 비트 제외).
• **Rx and Tx Unicast**	수신 및 전송 된 (양호한 및 나쁜) 유니 캐스트 패킷 수입니다.
• **Rx and Tx Multicast**	수신 및 전송 된 (양호 및 불량) 멀티 캐스트 패킷 수입니다.
• **Rx and Tx Broadcast**	수신 및 전송 된 (좋고 나쁜) 브로드 캐스트 패킷 수입니다.
• **Rx and Tx Pause**	PAUSE 동작을 나타내는 opcode 를 가진이 포트에서 수신되거나 전송 된 MAC 제어 프레임의 수.

수신 및 전송 크기 카운터

수신 및 전송 된 (양호 및 불량) 패킷의 수는 각각의 프레임 크기에 따라 범주로 분리됩니다.

수신 및 송신 큐 카운터

입력 및 출력 큐당 수신 및 송신 된 패킷 수.

오류 카운터 수신

목적	설명
• **Rx Drops**	수신 버퍼 부족 또는 송신 혼잡으로 인해 드롭 된 프레임 수입니다.
• **Rx CRC/Alignment**	CRC 또는 정렬 오류로 수신 된 프레임 수입니다.
• **Rx Undersize**	유효한 CRC 로 수신 된 짧은 프레임 수 입니다..
• **Rx Oversize**	유효한 CRC 로 수신 된 긴 프레임 수입니다.
• **Rx Fragments**	유효하지 않은 CRC 로 수신 된 짧은 프레임 수입니다.
• **Rx Jabber**	유효하지 않은 CRC 로 수신 된 긴 프레임 수입니다.
• **Rx Filtered**	전달 프로세스에 의해 필터링 된 수신 프레임 수입니다. 짧은 프레임은 64 바이트보다 작은 프레임입니다. 긴 프레임은이 포트에 구성된 최대 프레임 길이보다 긴 프레임입니다.

1 짧은 프레임은 64 바이트보다 작은 프레임입니다.
2 긴 프레임은이 포트의 구성된 최대 프레임 길이보다 긴 프레임입니다.

오류 카운터 전송

목적	설명
• **Tx Drops**	출력 버퍼 정체로 인해 드롭 된 프레임 수입니다.
• **Tx Late/Exc. Coll.**	과도하거나 늦은 충돌로 인해 떨어지는 프레임 수입니다.

버튼

Refresh: 즉시 페이지를 새로고침합니다.

Clear: 모든 포트의 카운터를 지웁니다.

Auto-refresh : 정기적으로 페이지 자동 새로 고침을 사용하려면이 상자를 선택하십시오..

4.4.4 SFP 모듈 정보

WGSW-48040HP 는 디지털 진단 모니터링 (DDM) 기능이있는 SFP 모듈을 지원하며이 기능은 디지털 광학 모니터링 (DOM)이라고도합니다. SFP 모듈 정보 페이지를 통해 SFP 모듈의 실제 또는 작동 상태를 점검 할 수 있습니다. 이 페이지는 트랜시버 유형, 속도, 파장, 광 출력 파워, 광 입력 파워, 온도, 레이저 바이어스 전류 및 트랜시버 공급 전압과 같은 작동 상태를 실시간으로 보여줍니다. 포트 번호의 하이퍼 링크를 사용할 수도 있습니다. speficic 인터페이스에서 통계를 확인합니다. 그림 4-4-4 의 SFP 모듈 정보 화면이 나타납니다.

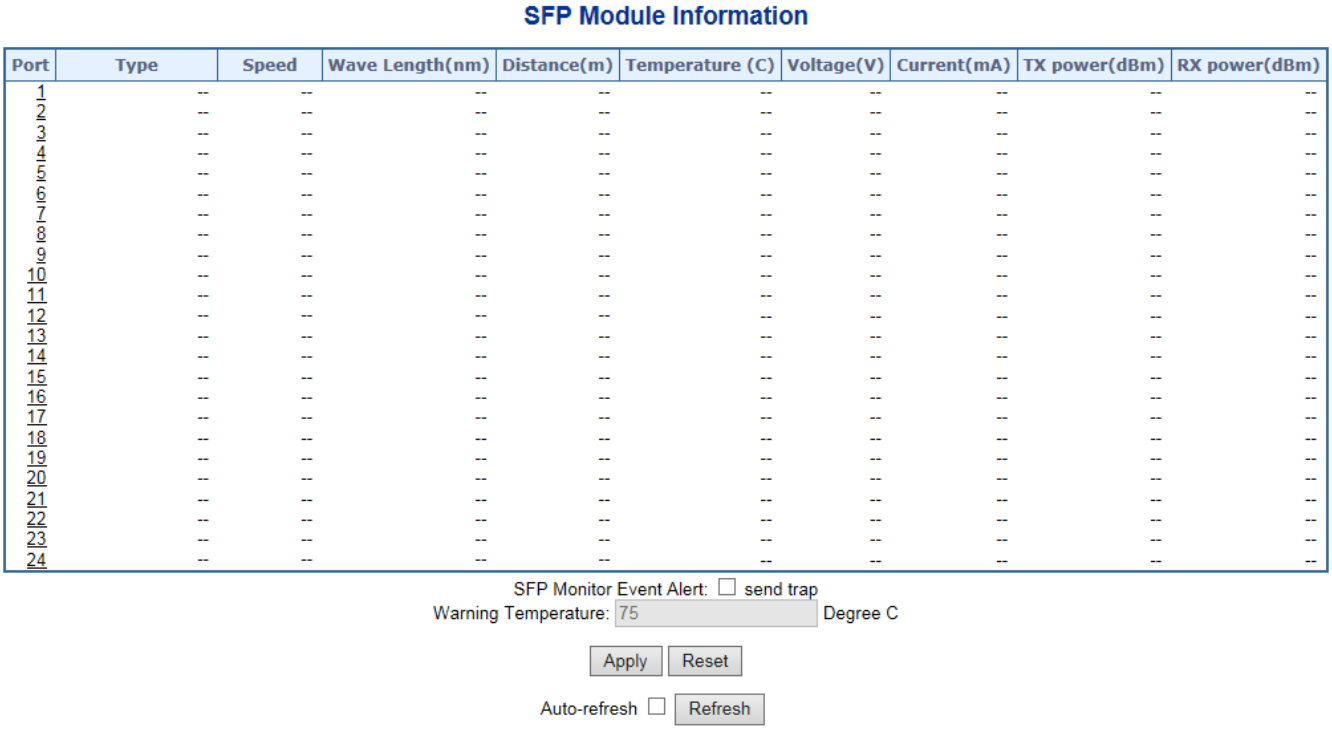


그림 4-4-4: SFP Module Information 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Type**	현재 SFP 모듈의 유형을 표시하십시오. 가능한 유형은 다음과 같습니다.: ■ 1000BASE-SX ■ 1000BASE-LX ■ 100BASE-FX
• **Speed**	현재 SFP 모듈의 속도를 표시합니다. 속도 값 또는 설명은 SFP 모듈에서 가져옵니다. 다른 공급 업체 SFP 모듈은 다른 속도 정보를 표시 할 수 있습니다.
• **Wave Length(nm)**	현재 SFP 모듈의 파장을 표시합니다. 파장 값은 SFP 모듈에서 가져옵니다. 이 열을 사용하여 광섬유 연결이 실패한 동안 두 노드의 파장 값이 일치하는지 확인하십시오.
• **Distance(m)**	현재 SFP 모듈의 지원 거리를 표시하십시오. 거리 값은 SFP 모듈에서 가져옵니다.
• **Temperature(C)** **– SFP DDM Module Only**	현재 SFP DDM 모듈의 온도를 표시합니다. 온도 값은 SFP DDM 모듈에서 가져옵니다.
• **Voltage(V)** **– SFP DDM Module Only**	현재 SFP DDM 모듈의 전압을 표시합니다. 전압 값은 SFP DDM 모듈에서 가져옵니다.
• **Current(mA)** **– SFP DDM Module Only**	현재 SFP DDM 모듈의 Ampere 를 표시합니다. Ampere 값은 SFP DDM 모듈에서 가져옵니다

• **TX power(dBm)** **– SFP DDM Module Only**	현재 SFP DDM 모듈의 TX 전력을 표시합니다. TX 전력 값은 SFP DDM 모듈에서 가져옵니다.
• **RX power(dBm)** **– SFP DDM Module Only**	현재 SFP DDM 모듈의 RX 전원을 표시하십시오. RX 전원 값은 SFP DDM 모듈에서 가져옵니다.

버튼

SFP Monitor Event Alert: ☐ 보내기 트랩

Warning Temperature: 75 'C

Check SFP Monitor Event Alert box; 경고하는 온도 설정에 따라 사용자가 SNMP 트랩을 통해 메시지를 기록 할 수 있습니다.

Auto-refresh ☐ :정기적으로 페이지 자동 새로 고침을 사용하려면이 상자를 선택하십시오..

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

Refresh: 즉시 페이지를 새로고침합니다.

4.4.5 Mirror 포트

이 페이지에서 포트 미러링을 구성하십시오. 이 기능은 패킷을 연구 할 수있는 다른 포트로 네트워크 스위치의 한 포트에서 각 들어 오거나 나가는 패킷의 복사본을 전달하는 네트워크 트래픽을 모니터링하는 데 사용됩니다. 관리자는 스위치 성능을 면밀히 추적하고 필요할 경우이를 변경할 수 있습니다.

- • 네트워크 문제를 디버깅하기 위해 선택한 트래픽을 프레임 분석기가 첨부되어 프레임 흐름을 분석 할 수있는 미러 포트로 복사하거나 미러링 할 수 있습니다.
- • 관리 형 스위치는 모든 포트에서 모니터 포트로가는 트래픽을 눈에 띄지 않게 미러링 할 수 있습니다. 그런 다음이 포트에 프로토콜 분석기 또는 RMON 프로브를 연결하여 트래픽 분석을 수행하고 연결 무결성을 확인할 수 있습니다.

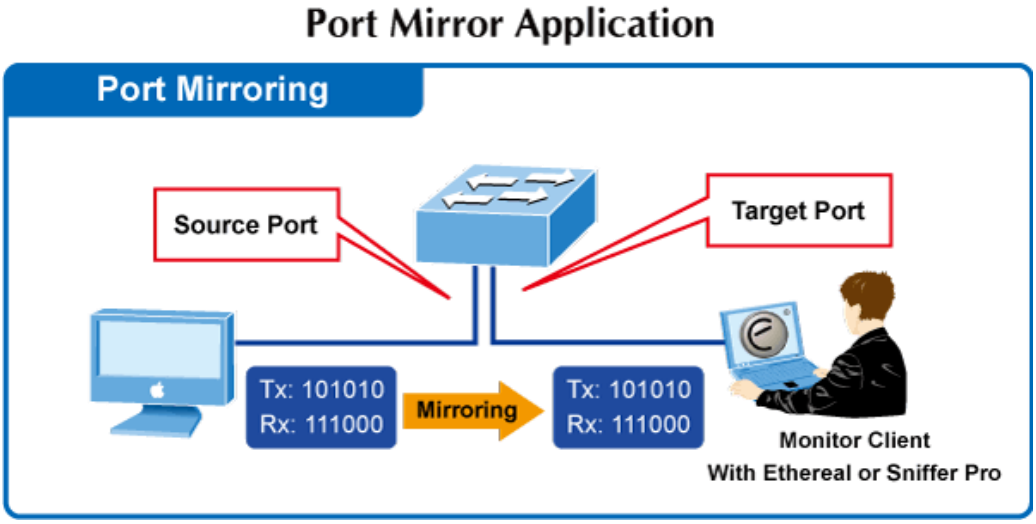


그림 4-4-7: Port Mirror Application

미러 포트에 복사 할 트래픽은 다음과 같이 선택됩니다.

- • 주어진 포트에서 수신 된 모든 프레임 (입력 또는 소스 미러링이라고도 함).
- • 지정된 포트에서 전송되는 모든 프레임 (송신 또는 대상 미러링이라고도 함).

Mirror Port Configuration

그림 4-4-8 의 Port Mirror 화면이 나타납니다..

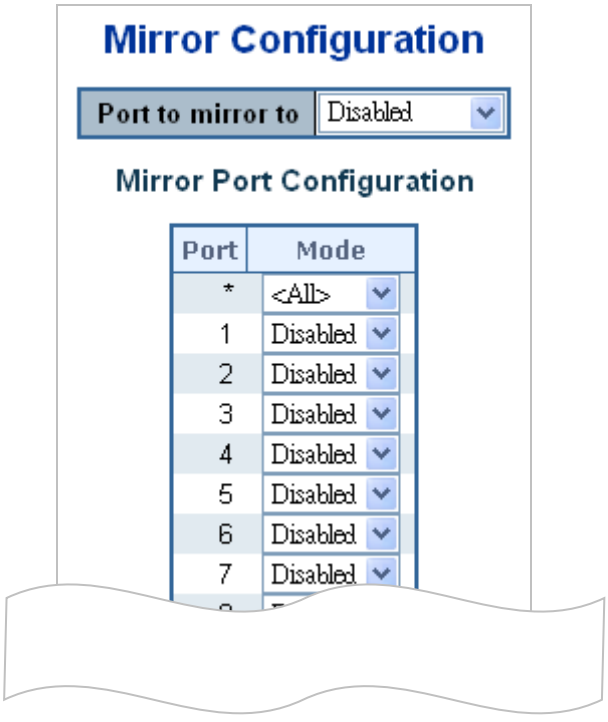


그림 4-4-8: Mirror Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port to mirror on**	소스 (rx) 또는 대상 (tx) 미러링이 활성화 된 포트의 프레임은이 포트에

	미러링됩니다. Disabled 는 미러링을 비활성화합니다.
• **Port**	같은 행에 포함 된 설정의 논리 포트입니다.
• **Mode**	Mirror 방법을 선택하십시오 ■ Rx only: 이 포트에서 수신 된 프레임은 미러링 포트로 미러링됩니다. 전송 된 프레임은 미러링되지 않습니다. ■ Tx only: 이 포트에서 전송 된 프레임은 미러링 포트로 미러링됩니다. 수신 된 프레임은 미러링되지 않습니다. ■ Disabled: 전송 된 프레임이나 수신 된 프레임은 미러링되지 않습니다.. ■ Both: 수신 된 프레임과 전송 된 프레임은 미러 포트로 미러링됩니다.

주어진 포트의 경우 프레임은 한 번만 전송됩니다. 따라서 미러 포트에서 Tx 프레임을 미러링 할 수 없습니다. 이 때문에 선택한 미러 포트의 모드는 Disabled 또는 Rx 로만 제한됩니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.5 Link Aggregation

포트 집합은 포트 그룹을 연결하여 단일 LAG (Link Aggregated Groups)를 형성함으로써 포트 사용을 최적화합니다. 포트 집합은 장치 간 대역폭을 늘리고 포트 유연성을 높이며 링크 중복성을 제공합니다. 각 LAG 는 전이중 작업으로 설정된 동일한 속도의 포트로 구성됩니다. LAG 의 포트는 동일한 속도로 작동하는 경우 서로 다른 미디어 유형 (UTP / 파이버 또는 다른 파이버 유형) 일 수 있습니다.

집계 링크는 수동으로 (포트 트렁크) 또는 관련 링크에서 링크 집계 제어 프로토콜 (LACP)을 활성화하여 자동으로 할당할 수 있습니다. 집계 링크는 시스템에서 단일 논리 포트로 처리됩니다.

특히, 집계 링크는 자동 협상, 속도, 이중 설정 등을 포함하여 비 집합 포트와 유사한 포트 속성을가집니다. 장치는 다음과 같은 집계 링크를 지원합니다.:

- **Static LAGs** (**Port Trunk**) – 선택한 포트를 집계하여 출력 트렁크 그룹으로 만듭니다.
- **Link Aggregation Control Protocol** (**LACP**) LAGs - LACP LAG는 다른 장치에있는 다른 LACP 포트와 집계 포트 링크를 협상합니다. 다른 장치 포트가 LACP 포트 인 경우 장치는 그 장치들 사이에 LAG를 설정합니다.

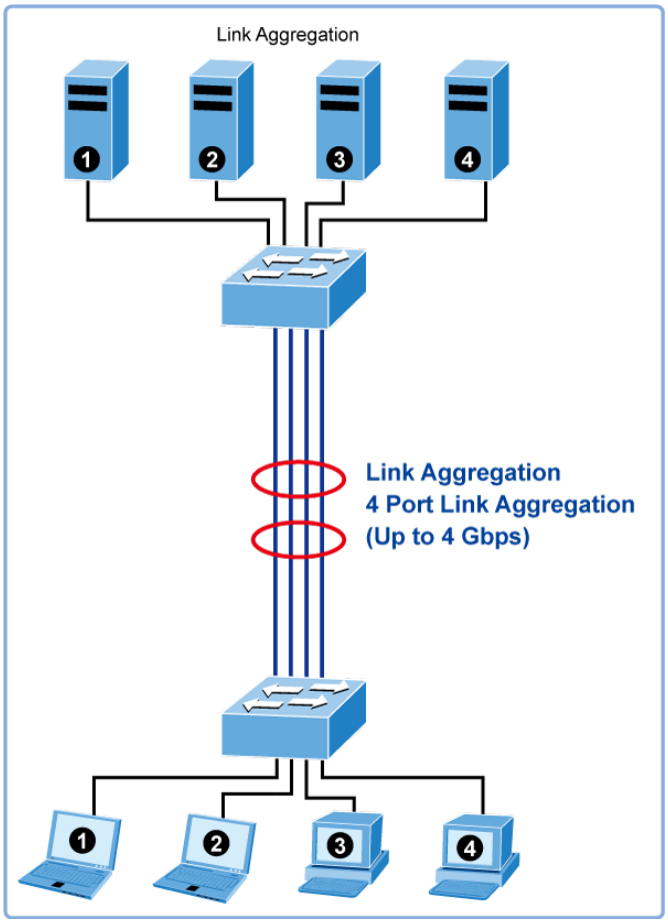


그림 4-5-1: Link Aggregation

링크 집계 제어 프로토콜 (LACP)은 고속 중복 링크가 필요한 파트너 시스템간에 정보를 교환하기위한 표준화 된 방법을 제공합니다. 링크 집합을 사용하면 최대 8 개의 연속 포트를 하나의 전용 연결로 그룹화 할 수 있습니다. 이 기능을 사용하면 네트워크의 장치로 대역폭을 확장 할 수 있습니다. LACP 작동에는 전이중 모드가 필요하며 자세한 정보는 IEEE 802.3ad 표준을 참조하십시오.

포트 링크 집계를 사용하여 네트워크 연결의 대역폭을 높이거나 오류 복구를 보장 할 수 있습니다. Link Aggregation 을 사용하면 최대 4 개의 연속 포트를 스위치 또는 다른 Layer 2 스위치 사이의 단일 전용 연결로 그룹화 할 수 있습니다. 그러나 장치간에 물리적 연결을 설정하기 전에 링크 집계 구성 메뉴를 사용하여 양쪽 장치의 링크 집계를 지정하십시오. 포트 링크 집계를 사용할 때 다음을 참고하십시오.

- 링크 집합에 사용되는 포트는 모두 동일한 미디어 유형 (RJ45, 100Mbps 광섬유)이어야합니다.
- 동일한 링크 집합에 할당 할 수있는 포트에는 다른 제한 사항이 있습니다 (아래 참조).
- 포트는 하나의 링크 집합에만 할당 할 수 있습니다.
- 연결의 양쪽 끝에있는 포트는 링크 집계 포트로 구성되어야합니다.
- 링크 집계의 어느 포트도 미러 소스 포트 또는 미러 대상 포트로 구성 할 수 없습니다.
- 링크 집계의 모든 포트는 VLAN 에서 이동, 추가 또는 삭제 될 때 전체적으로 처리되어야합니다.
- 스패닝 트리 프로토콜은 링크 집계의 모든 포트를 전체적으로 처리합니다.
- 데이터 루프가 생성되지 않도록 스위치 사이에 케이블을 연결하기 전에 링크 집계를 활성화하십시오.
- 데이터 링크가 없도록 링크 집계를 제거하기 전에 모든 링크 케이블의 연결을 끊거나 링크 집계 포트를 비활성화하십시오.

동시에 최대 10 개의 포트를 집계 할 수 있습니다. 관리 형 스위치는 기가비트 이더넷 포트 (최대 5 개 그룹)를 지원합니다. 그룹이 LACP 정적 링크 집계 그룹으로 정의 된 경우 다른 포트 중 하나에 장애가 발생하면 여분의 포트가 대기 모드로 전환되어 중복됩니다. 그룹이 로컬 정적 링크 집계 그룹으로 정의 된 경우 포트 수는 그룹 구성원 포트와 같아야합니다.
집계 코드는 동일한 프레임 흐름 (예 : TCP 연결)에 속한 프레임이 항상 동일한 링크 집계 구성원 포트에서 전달되도록합니다. 따라서 흐름 내의 프레임을 표현하는 것은 불가능합니다. 집계 코드는 다음 정보를 기반으로합니다.:

- **출발지 MAC**
- **목적지 MAC**
- **출발지와 목적지 IPv4 주소.**
- **출발지와 목적지의 IPv4 packets 을 위한 TCP/UTP 포트**

일반적으로 링크 집계 구성원 포트간에 최상의 트래픽 분산을 얻으려면 집계 코드에 5 가지 기여를 모두 사용하도록 설정해야합니다. 각 링크 집합은 최대 10 개의 구성원 포트로 구성 될 수 있습니다. 임의의 양의 링크 집합이 장치에 구성 될 수 있습니다 (장치의 포트 수에 의해서만 제한됩니다). 적절한 트래픽 분산을 구성하려면 링크 집계 내의 포트가 동일한 링크 속도를 사용해야합니다.

4.5.1 Static Aggregation

이 페이지는 집계 해시 모드 및 집계 그룹을 구성하는 데 사용됩니다. 집계 해시 모드 설정은 전역입니다..

Hash Code Contributors

Static Aggeration 은 그림 4-5-2 이 나타냅니다.

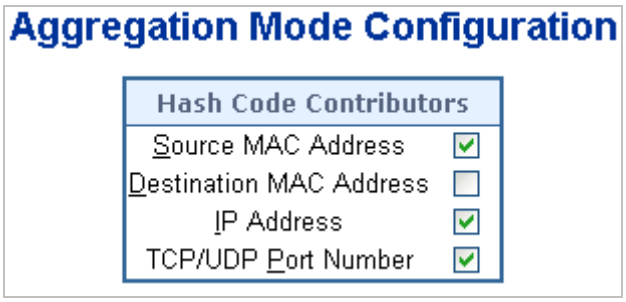


그림 4-5-2 : Aggregation Mode Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Source MAC Address**	소스 MAC 주소는 프레임의 대상 포트를 계산하는 데 사용할 수 있습니다. 소스 MAC 주소의 사용을 활성화하려면 선택하고 비활성화하려면 선택을 취소하십시오. 기본적으로 소스 MAC 주소가 사용됩니다.
• **Destination MAC Address**	대상 MAC 주소는 프레임의 대상 포트를 계산하는 데 사용할 수 있습니다. 확인을 클릭하여 대상 MAC 주소의 사용을 활성화하거나 선택을 취소하여 비활성화하십시오. 기본적으로 대상 MAC 주소는 비활성화되어 있습니다.
• **IP Address**	IP 주소는 프레임의 대상 포트를 계산하는 데 사용할 수 있습니다. IP 주소 사용을 사용하려면 선택하고 사용하지 않으려면 선택을 해제하십시오. 기본적으로 IP 주소가 사용됩니다.
• **TCP/UDP Port Number**	TCP / UDP 포트 번호는 프레임의 대상 포트를 계산하는 데 사용할 수 있습니다. TCP / UDP 포트 번호를 사용하려면 선택하고, 선택하지 않으려면 선택을 취소하십시오. 기본적으로 TCP / UDP 포트 번호가 사용됩니다.

Static Aggregation Group Configuration

그림 4-5-3 의 Aggregation Group Configuration 화면이 나타납니다..

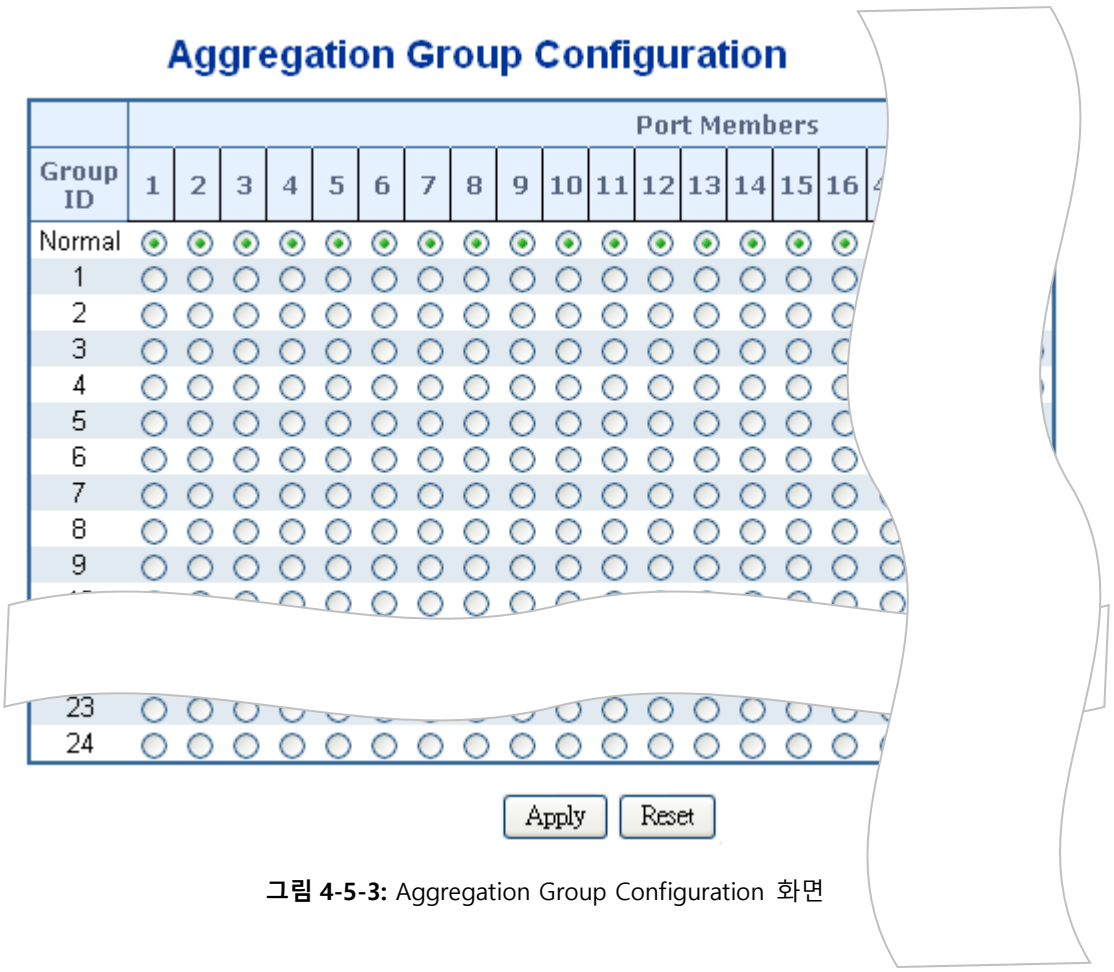


그림 4-5-3: Aggregation Group Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Group ID**	동일한 행에 포함 된 설정의 그룹 ID 를 나타냅니다. 그룹 ID "Normal"은 집계가 없음을 나타냅니다. 포트 당 하나의 그룹 ID 만 유효합니다.
• **Port Members**	스위치 포트는 각 그룹 ID 에 대해 나열됩니다. 집계에 포트를 포함하려면 라디오 버튼을 선택하고 집계에서 포트를 제거하려면 라디오 버튼을 선택 취소하십시오. 기본적으로 모든 집계 그룹에 속한 포트는 없습니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.5.2 LACP Configuration

Link Aggregation Control Protocol (LACP) - LACP LAG 는 다른 장치에있는 다른 LACP 포트와 집계 포트 링크를 협상합니다. LACP 를 사용하면 서로 연결된 포트가 동일한 LAG 에 속하는지 여부를 자동으로 검색 할 수 있습니다.

이 페이지를 통해 사용자는 현재 LACP 포트 구성을 검사 할 수 있으며 변경 가능할 수도 있습니다. 그림 4-5-4 의 LACP Configuration 화면이 나타납니다.

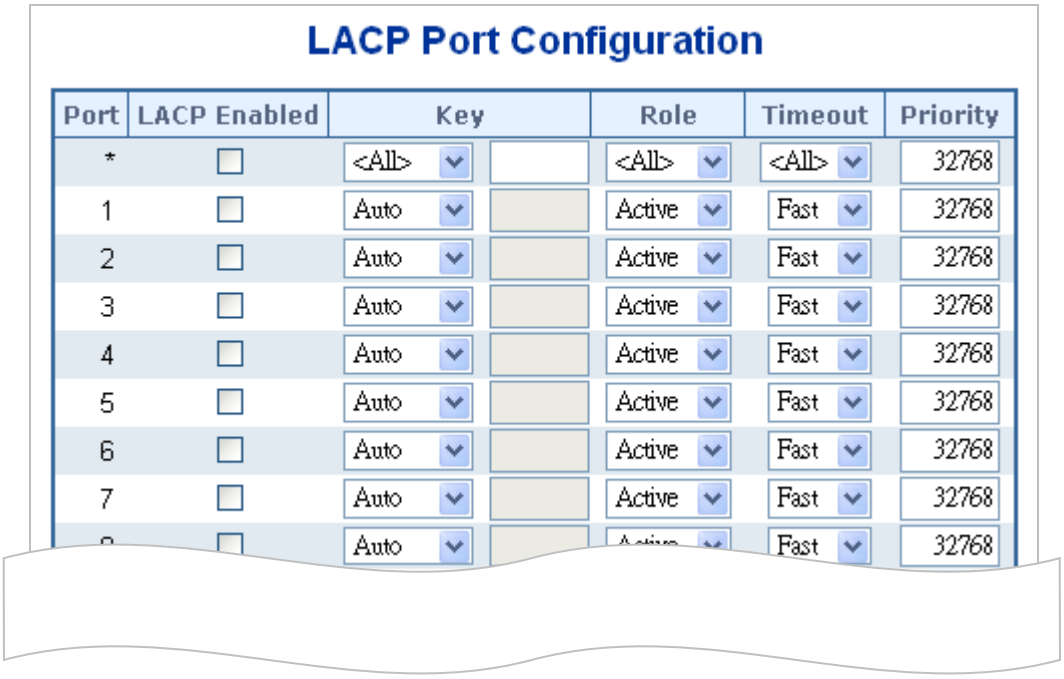


그림 4-5-4 : LACP Port Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	스위치 포트의 숫자
• **LACP Enabled**	이 스위치 포트에서 LACP 를 활성화할지 여부를 제어합니다. LACP 는 2 개 이상의 포트가 동일한 파트너에 연결된 경우 집계를 형성합니다.
• **Key**	포트에서 발생하는 키 값 (범위 : 1-65535) 자동 설정은 물리적 링크 속도 인 10Mb = 1, 100Mb = 2, 1Gb = 3 으로 키를 적절하게 설정합니다. 특정 설정을 사용하여 사용자 정의 값을 입력 할 수 있습니다. 동일한 키 값을 가진 포트는 동일한 집계 그룹에 참여할 수 있지만 다른 키를 가진 포트는 참여할 수 없습니다. 기본 설정은 "자동"입니다.
• **Role**	역할은 LACP 활동 상태를 표시합니다. Active 는 매초마다 LACP 패킷을 전송하고 Passive 는 파트너로부터 LACP 패킷을 기다립니다 (말하면 말하는식).
• **Timeout**	제한 시간은 BPDU 전송 사이의 기간을 제어합니다. Fast 는 매초마다 LACP 패킷을 전송하며, Slow 는 LACP 패킷을 보내기 전에 30 초 동안 대기합니다.
• **Priority**	우선 순위는 포트의 우선 순위를 제어합니다. LACP 파트너가 이 장치에서 지원하는 것보다 큰 그룹을 구성하려는 경우이 매개 변수는 어떤 포트가 활성 상태이고 어느 포트가 백업 역할을 담당 할 것인지를 제어합니다.

	숫자가 낮을수록 우선 순위가 높아집니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.5.3 LACP 시스템 상태

이 페이지는 모든 LACP 인스턴스에 대한 상태 개요를 제공합니다. LACP Status (LACP 상태) 페이지에는 현재 LACP 집합 그룹 및 LACP 포트 상태가 표시됩니다. 그림 4-5-5 의 LACP System Status 화면이 나타납니다

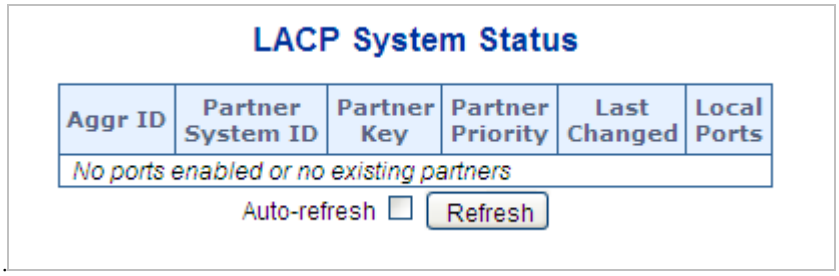


그림 4-5-5: LACP System Status 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Aggr ID**	이 집계 인스턴스와 연결된 집계 ID 입니다. LLAG 의 경우 ID 는 'isid : aggr-id'로 표시되고 GLAG 의 경우 'aggr-id'
• **Partner System ID**	집계 파트너의 시스템 ID (MAC 주소)입니다.
• **Partner Key**	파트너가 이 집계 ID 에 할당 한 키입니다
• **Partner Priority**	집계 파트너의 우선 순위입니다.
• **Last changed**	이 집계가 변경된 이후의 시간.
• **Local Ports**	이 스위치에 대해이 집계의 일부인 포트를 표시합니다.

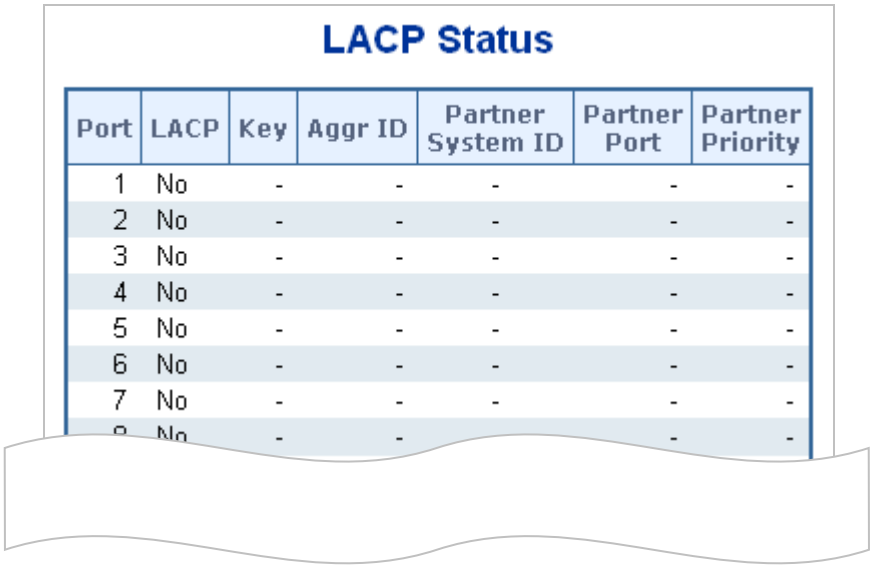
버튼

Refresh: 즉시 페이지를 새로고침합니다.

Auto-refresh : 자동 새로 고침은 3 초마다 발생합니다.

4.5.4 LACP Port Status

이 페이지는 모든 포트의 LACP 상태에 대한 상태 개요를 제공합니다. 그림 4-5-6 의 LACP Port Status 화면이 나타납니다.


LACP Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Priority
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-		-	-

그림 4-5-6: LACP Status 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	스위치 포트 수
• **LACP**	'예'는 LACP 가 활성화되어 있고 포트 링크가 작동 중임을 의미합니다. '아니요'는 LACP 가 활성화되어 있지 않거나 포트 링크가 다운되어 있음을 의미합니다. '백업'은 포트가 집계 그룹에 참여할 수 없지만 다른 포트가 나가면 참여할 수 있음을 의미합니다. LACP 상태는 사용할 수 없습니다.
• **Key**	이 포트에 지정된 키입니다. 동일한 키가있는 포트만 함께 집계 할 수 있습니다.
• **Aggr ID**	이 집계 그룹에 할당 된 집계 ID 입니다.
• **Partner System ID**	파트너의 시스템 ID (MAC 주소)입니다.
• **Partner Port**	이 포트에 연결된 파트너의 포트 번호입니다.
• **Partner Priority**	파트너 포트의 우선 순위입니다.

버튼

Refresh: 즉시 페이지를 새로고침합니다.

Auto-refresh : 3 초마다 새로고침을 자동적.

4.5.5 LACP Port Statistics

이 페이지에서는 모든 포트의 LACP 통계에 대한 개요를 제공합니다. 그림 4-5-7 의 LACP Port Statistics 화면이 나타납니다.

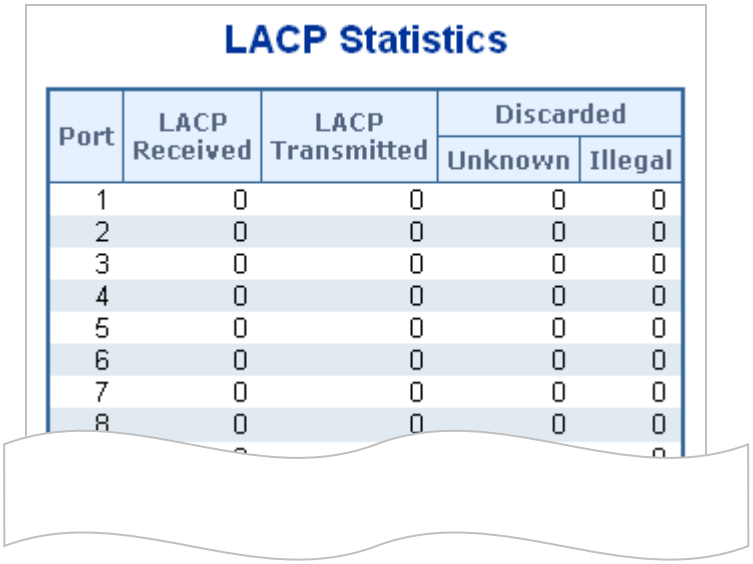


그림 4-5-7: LACP Statistics 화면

• **목적Port**	스위치 포트의 수입니다.
• **LACP Received**	Shows how many LACP frames have been sent from each port.
• **LACP Transmitted**	Shows how many LACP frames have been received at each port.
• **Discarded**	Shows how many unknown or illegal LACP frames have been discarded at each port.

버튼

Auto-refresh :3 간 가만히 둡니다. 자동ㅇㄴ제 할수있븝니 모—

Refresh : 즉시 페이지를 새로고침합니다.

Clear : 모든 태리픽의 정보를 지우고 다시석ㄹ저

4.6 VLAN

4.6.1 VLAN 개요

VLAN (Virtual Local Area Network)은 실제 레이아웃이 아닌 논리적 체계에 따라 구성된 네트워크 토폴로지입니다. VLAN 을 사용하여 모든 LAN 세그먼트 모음을 단일 LAN 으로 나타나는 자치 사용자 그룹으로 결합 할 수 있습니다. VLAN 은 논리적으로 네트워크를 여러 브로드 캐스트 도메인으로 분할하여 패킷이 VLAN 내의 포트간에 만 전달되도록합니다. 일반적으로 VLAN 은 반드시 필요한 것은 아니지만 특정 서브넷에 해당합니다.

VLAN 은 대역폭을 보존하여 성능을 향상시키고 트래픽을 특정 도메인으로 제한하여 보안을 향상시킬 수 있습니다.

VLAN 은 실제 위치 대신 논리로 그룹화 된 최종 노드의 모음입니다. 서로 통신하는 엔드 노드는 물리적으로 네트워크에있는 위치와 상관없이 동일한 VLAN 에 할당됩니다. 브로드 캐스트 패킷은 브로드 캐스트가 시작된 VLAN 의 구성원에게만 전달되기 때문에 논리적으로 VLAN 을 브로드 캐스트 도메인과 동일시 할 수 있습니다..

1. 엔드 노드를 고유하게 식별하고 이들 노드에 VLAN 멤버십을 할당하기 위해 어떤 기준을 사용하는지에 관계없이 네트워크 장치가 VLAN 간에 라우팅 기능을 수행하지 않으면 패킷이 VLAN 을 통과 할 수 없습니다.
2. 관리 형 스위치는 IEEE 802.1Q VLAN 을 지원합니다. 포트 태그 해제 기능을 사용하면 태그 인식되지 않는 장치와의 호환성을 유지하기 위해 패킷 헤더에서 802.1 태그를 제거 할 수 있습니다.

관리 스위치의 기본값은 모든 포트를 DEFAULT_VLAN이라는 단일 802.1Q VLAN에 할당하는 것입니다. 새 VLAN이 만들어지면 새 VLAN에 할당 된 구성원 포트가 DEFAULT_ VLAN 포트 구성원 목록에서 제거됩니다. DEFAULT_VLAN의 VID는 1입니다.

이번 섹션에서는 다음과 같이 소개합니다.

- **VLAN Port Configuration** VLAN 그룹을 활성화합니다
- **VLAN Membership Status** Vlan 멤버쉽 상태를 표시합니다.
- **VLAN Port Status** VALN 포트 상태를 표시합니다
- **Private VLAN** 기본 또는 커뮤니티 Vlan 생성/제거
- **Port Isolation** 포트에서 포트분리를 활성화/비활성화 합니다.
- **MAC-based VLAN** MAC 기반 Vlan 항목을 구성합니다
- **MAC-based VLAN Status** MAC 기반 Vlan 항목을 표시합니다.
- **Protocol-based VLAN** 프로토콜 기반 Vlan 항목을 구성합니다
- **Protocol-based VLAN Membership** 프로토콜 기반 Vlan 항목을 표시합니다.

4.6.2 IEEE 802.1Q VLAN

대규모 네트워크에서 라우터는 각 서브넷의 브로드 캐스트 트래픽을 별도의 도메인으로 격리하는 데 사용됩니다. 이 관리 형 스위치는 VLAN 을 사용하여 네트워크 노드 그룹을 별도의 브로드 캐스트 도메인으로 구성하여 레이어 2 에서 유사한 서비스를 제공합니다. VLAN 은 브로드 캐스트 트래픽을 원래 그룹으로 제한하고 대규모 네트워크에서 브로드 캐스트 스톰을 제거 할 수 있습니다. 또한보다 안전하고 깨끗한 네트워크 환경을 제공합니다..

IEEE 802.1Q VLAN 은 네트워크의 어느 위치 에나있을 수 있지만 동일한 물리적 세그먼트에 속한 것처럼 통신하는 포트 그룹입니다.

VLAN 을 사용하면 물리적 연결을 변경하지 않고도 장치를 새로운 VLAN 으로 이동할 수 있으므로 네트워크 관리가 단순해집니다. VLAN 은 부서별 그룹 (예 : 마케팅 또는 R & D), 사용 그룹 (예 : 전자 메일) 또는 멀티 캐스트 그룹 (화상 회의와 같은 멀티미디어 응용 프로그램에 사용)을 반영하도록 쉽게 구성 할 수 있습니다.

VLAN 은 브로드 캐스트 트래픽을 줄임으로써보다 뛰어난 네트워크 효율성을 제공하며 IP 주소 또는 IP 서브넷을 업데이트 할 필요없이 네트워크를 변경할 수 있습니다. VLAN 은 트래픽이 구성된 Layer 3 링크를 통과하여 다른 VLAN 에 도달해야하므로 본질적으로 높은 수준의 네트워크 보안을 제공합니다.

이 관리형 스위치는 다음 Vlan 기능을 지원합니다.:

- 802.1Q 표준에 기반한 최대 255 개의 Vlan
- 중복포트와 여러 VLAN 에 참여
- 엔드 지역은 여러 Vlan 에 tjhrgkftn
- VLAN 인식 및 VLAN 비 인식 장치간에 트래픽 전달
- 우선순위 태깅

■ IEEE 802.1Q 표준

EEE 802.1Q (태그) VLAN 은 스위치에 구현됩니다. 802.1Q VLAN 에는 태그 지정이 필요하므로 전체 네트워크로 확장 할 수 있습니다 (네트워크상의 모든 스위치가 IEEE 802.1Q 를 준수한다고 가정).

VLAN 을 사용하면 브로드 캐스트 도메인의 크기를 줄이기 위해 네트워크를 세그먼트화할 수 있습니다. VLAN 에 들어가는 모든 패킷은 해당 VLAN 의 구성원 인 스테이션 (IEEE 802.1Q 사용 스위치 이상)으로 만 전달되며 여기에는 알 수없는 소스의 브로드 캐스트, 멀티 캐스트 및 유니 캐스트 패킷이 포함됩니다.

VLAN 은 네트워크 보안 수준을 제공 할 수도 있습니다. IEEE 802.1Q VLAN 은 VLAN 의 구성원 인 스테이션간에 만 패킷을 전달합니다. 모든 포트는 태그 지정 또는 태그 해제로 구성 할 수 있습니다.:

- IEEE 802.1Q VLAN 의 태그 해제 기능을 사용하면 VLAN 을 패킷 헤더의 VLAN 태그를 인식하지 못하는 레거시 스위치와 함께 사용할 수 있습니다..
- 태그 지정 기능을 사용하면 VLAN 을 단일 물리적 연결을 통해 여러 802.1Q 호환 스위치로 확장 할 수 있으며 모든 포트에서 스패닝 트리를 활성화하고 정상적으로 작동 할 수 있습니다..

관련 용어::

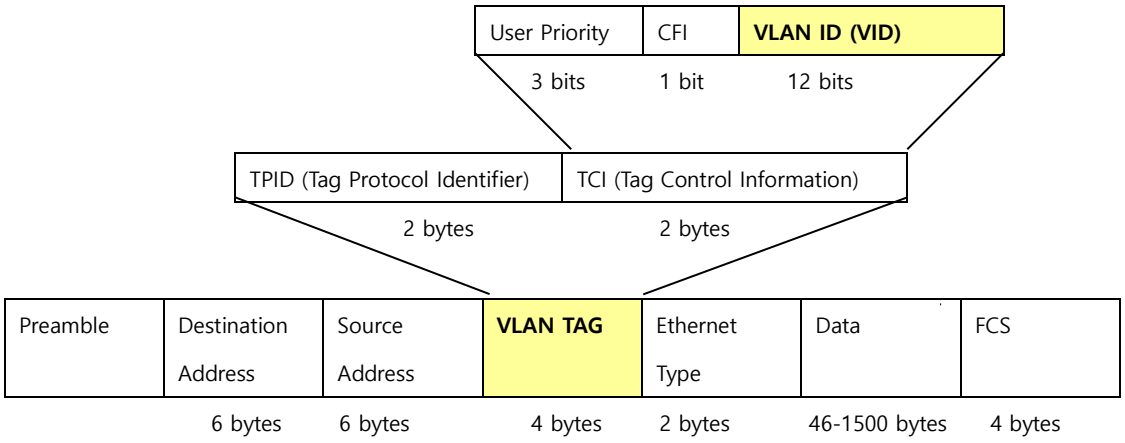
- **Tagging** - 802.1Q VLAN 정보를 패킷의 헤더에 넣는 행위.
- **Untagging** - 패킷 헤더에서 802.1Q VLAN 정보를 제거하는 행위입니다.

■ 802.1Q VLAN Tags

아래의 구성은 802.1Q VLAN 태그를 보여줍니다. 소스 MAC 주소 뒤에 네 개의 추가 8 진수가 삽입됩니다. 그들의 존재 여부는 Ether Type 필드에 0x8100 값으로 표시됩니다. 패킷의 Ether Type 필드가 0x8100 인 경우, 패킷은 IEEE 802.1Q / 802.1p 태그를 전달합니다. 태그는 다음 두 옥텟에 포함되며 3 비트의 사용자 우선 순위, 1 비트의 Canonical Format Identifier (CFI - 토큰 링 패킷을 이더넷 백본을 통해 전달할 수 있도록 캡슐화하는 데 사용됨) 및 12 비트의 VLAN ID VID). 사용자 우선 순위의 3 비트는 802.1p 에서 사용됩니다. VID 는 VLAN 식별자이며 802.1Q 표준에서 사용됩니다. VID 는 12 비트이기 때문에 4094 개의 고유 한 VLAN 을 식별 할 수 있습니다.

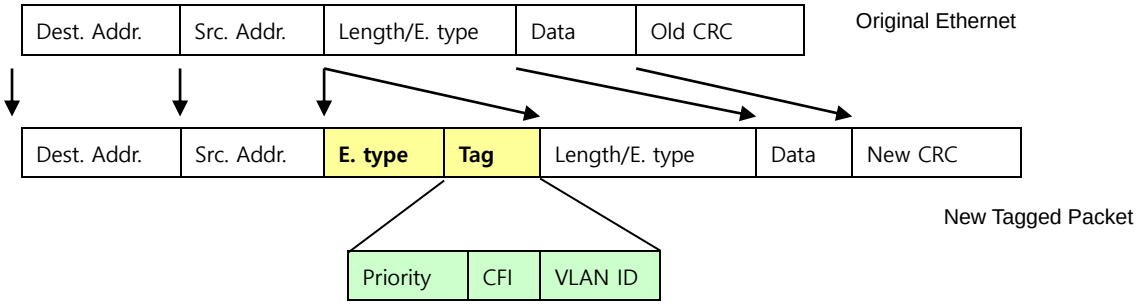
태그는 패킷 헤더에 삽입되어 전체 패킷을 4 옥텟 연장합니다. 원래 패킷에 포함 된 모든 정보가 유지됩니다..

802.1Q Tag



Ether Type 과 VLAN ID 는 원래의 Ether Type / Length 또는 Logical Link Control 이전에 MAC 소스 주소 다음에 삽입됩니다. 패킷이 원래보다 약간 더 길기 때문에 CRC (Cyclic Redundancy Check)를 다시 계산해야합니다..

IEEE802.1Q Tag 추가



■ Port VLAN ID

태그가 지정된 (802.1Q VID 정보를 전달하는) 패킷은 VLAN 정보가 손상되지 않은 한 802.1Q 호환 네트워크 장치에서 다른 장치로 전송할 수 있습니다. 이렇게하면 802.1Q VLAN 이 네트워크 장치 (실제로 모든 네트워크 장치가 802.1Q 와 호환되는 경우 전체 네트워크)를 확장 할 수 있습니다.

스위치의 모든 물리적 포트에는 PVID 가 있습니다. 802.1Q 포트에는 스위치 내에서 사용하기 위해 PVID 가 할당됩니다. 스위치에 VLAN 이 정의되지 않은 경우 모든 포트는 PVID 가 1 인 기본 VLAN 에 할당됩니다. 태그가없는 패킷에는 수신

된 포트의 PVID 가 할당됩니다. 전달 결정은 VLAN 과 관련하여이 PVID 를 기반으로합니다. 태그가 지정된 패킷은 태그에 포함 된 VID 에 따라 전달됩니다. 태그가 지정된 패킷에도 PVID 가 할당되지만 PVID 는 패킷 전달을 결정하는 데 사용되지 않으며 VID 는 결정됩니다.

태그 인식 스위치는 스위치의 PVID 를 네트워크의 VID 와 연관 시키도록 테이블을 유지해야합니다. 스위치는 전송할 패킷의 VID 와 패킷을 전송할 포트의 VID 를 비교합니다. 두 VID 가 다른 경우 스위치는 패킷을 버립니다. 태그없는 패킷에 대한 PVID 와 태그가 지정된 패킷에 대한 VID 의 존재 때문에 태그 인식 및 태그 비 인식 네트워크 장치는 동일한 네트워크에 공존 할 수 있습니다.

스위치 포트는 하나의 PVID 만 가질 수 있지만 VLAN 테이블에 스위치가 저장하는 VID 를 저장할 수있는 VID 를 가질 수 있습니다.

네트워크상의 일부 장치는 태그를 인식하지 못하기 때문에 패킷을 전송하기 전에 태그 인식 장치의 각 포트에서 결정해야합니다 (전송할 패킷에 태그가 있어야하는지 여부). 전송 포트가 태그 비 인식 장치에 연결되어 있으면 패킷에 태그가 없어야합니다. 전송 포트가 태그 인식 장치에 연결되어 있으면 패킷에 태그가 지정되어야합니다..

■ 기본 VLANs

스위치는 초기에 "default"라는 하나의 VLAN 인 VID = 1 을 구성합니다. 공장 출하시의 기본 설정은 스위치의 모든 포트를 "기본값"으로 지정합니다. 새 VLAN 이 포트 기반 모드로 구성되면 해당 구성원 포트가 "기본값"에서 제거됩니다.

■ VLANs 을 포트에 등록하기

스위치에 VLAN 을 활성화하기 전에 먼저 각 포트를 참여시킬 VLAN 그룹에 할당해야합니다. 기본적으로 모든 포트는 태그가없는 포트로 VLAN 1 에 할당됩니다. 하나 이상의 VLAN 에 트래픽을 전달하고 연결의 다른 끝에있는 중간 네트워크 장치 또는 호스트가 VLAN 을 지원하려면 포트를 태그있는 포트로 추가하십시오. 그런 다음 GVRP 를 사용하여 수동 또는 동적으로이 트래픽을 전달할 경로를 따라 다른 VLAN 인식 네트워크 장치의 포트를 동일한 VLAN 에 할당합니다.
그러나이 스위치의 포트를 하나 이상의 VLAN 에 참여 시키되 중간 네트워크 장치 나 연결의 다른 쪽 호스트가 VLAN 을 지원하지 않도록하려면이 포트를 VLAN 에 태그가없는 포트로 추가해야합니다.

VLAN 태그 프레임은 VLAN 인식 또는 VLAN 비 인식 네트워크 상호 연결 장치를 통과 할 수 있지만 VLAN 태그는 VLAN 태깅을 지원하지 않는 엔드 노드 호스트로 전달하기 전에 제거되어야합니다.

■ VLAN Classification

스위치가 프레임을 수신하면 스위치는 다음 두 가지 방법 중 하나로 프레임을 분류합니다. 프레임에 태그가 지정되어 있지 않으면 스위치는 프레임을 관련 VLAN 에 할당합니다 (수신 포트의 기본 VLAN ID 를 기반으로 함). 그러나 프레임에 태그가 지정되면 스위치는 태그가 지정된 VLAN ID 를 사용하여 프레임의 포트 브로드 캐스트 도메인을 식별합니다..

■ Port Overlapping

포트 오버랩은 파일 서버 나 프린터와 같이 서로 다른 VLAN 그룹간에 공통적으로 공유되는 네트워크 리소스에 대한 액세스를 허용하는 데 사용할 수 있습니다. 겹치지 않지만 통신이 필요한 VLAN 을 구현하면이 스위치에서 사용 가능한 라우팅을 통해 연결할 수 있습니다..

■ Untagged VLANs

Untagged (또는 static) VLAN 은 일반적으로 브로드 캐스트 트래픽을 줄이고 보안을 강화하는 데 사용됩니다. VLAN 에 할당 된 네트워크 사용자 그룹은 스위치에 구성된 다른 VLAN 과는 별도로 브로드 캐스트 도메인을 형성합니다. 패킷은 동일한 VLAN 에 지정된 포트 사이에서만 전달됩니다. 태그가없는 VLAN 을 사용하여 사용자 그룹 또는 서브넷을 수동으로 격리 할 수 있습니다..

4.6.3 VLAN 포트 설정

이 페이지는 관리 대상 스위치 포트 VLAN 을 구성하는 데 사용됩니다. 포트 구성 페이지 별 VLAN 에는 VLAN 의 일부인 포트를 관리하기위한 필드가 들어 있습니다. 포트 기본 VLAN ID (PVID)는 VLAN 포트 구성 페이지에서 구성됩니다. 장치에 도착한 모든 태그없는 패킷은 포트 PVID 에 의해 태그가 지정됩니다..

스위치의 명칭의 이해

■ IEEE 802.1Q Tagged 와 Untagged

802.1Q 호환 스위치의 모든 포트는 태그 또는 태그가 지정되지 않은 포트로 구성 될 수 있습니다..

- **Tagged:** 태깅이 활성화 된 포트는 VID 번호, 우선 순위 및 기타 VLAN 정보를 해당 포트로 유입되는 모든 패킷의 헤더에 넣습니다. 패킷에 이전에 태그가 지정되어 있으면 포트가 패킷을 변경하지 않으므로 VLAN 정보가 손상되지 않습니다. 태그의 VLAN 정보는 네트워크의 다른 802.1Q 준수 장치가 패킷 전달 결정을 내리는 데 사용할 수 있습니다.

- **Untagged:** 태그없는 태그가 설정된 포트는 해당 포트로 유입되는 모든 패킷에서 802.1Q 태그를 제거합니다. 패킷에 802.1Q VLAN 태그가 없으면 포트가 패킷을 변경하지 않습니다. 따라서 태그없는 포트가 수신하고 전달하는 모든 패킷에는 802.1Q VLAN 정보가 없습니다. (PVID 는 스위치 내에서만 사용됩니다). Untagging 은 802.1Q 준수 네트워크 장치에서 비 호환 네트워크 장치로 패킷을 보내는 데 사용됩니다..

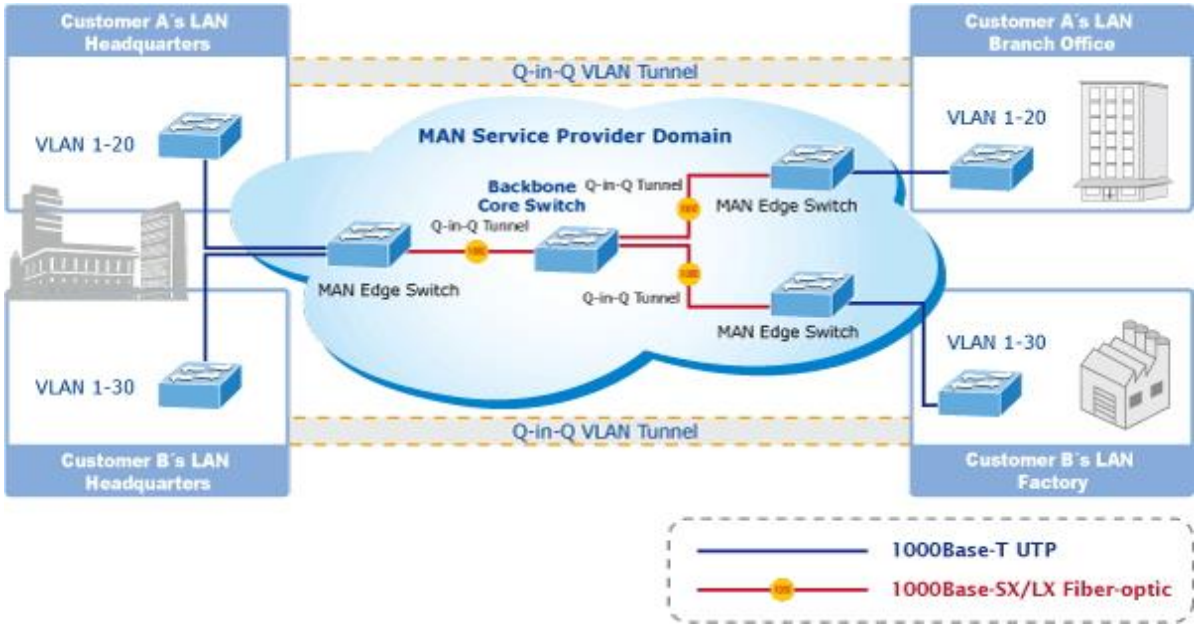
프레임 출입 / 프레임 방출	Tagged 된 출입 프레임	Untagged 된 출입 프레임
Tagged 된 방출 포트	Tagged 인 상태로 있음	태그가 삽입되었다
Untagged 된 방출 포트	태그가 제거되었음	Untagged 인 상태로 있음

표 4-6-1: VLAN VID 태그 / Untag 테이블이있는 입 / 출력 포트

■ IEEE 802.1Q Tunneling (Q-in-Q)

IEEE 802.1Q 터널링 (QinQ)은 네트워크를 통해 여러 고객을 대상으로 트래픽을 전송하는 서비스 제공 업체를 위해 설계되었습니다. QinQ 터널링은 다른 고객이 동일한 내부 VLAN ID 를 사용하는 경우에도 고객 별 VLAN 및 레이어 2 프로토콜 구성을 유지 관리하는 데 사용됩니다. 이것은 서비스 공급자의 네트워크에 들어갈 때 SPVLAN (Service Provider VLAN) 태그를 고객의 프레임에 삽입 한 다음 프레임이 네트워크를 떠날 때 태그를 제거하여 수행됩니다.

서비스 제공 업체의 고객은 내부 VLAN ID 및 지원되는 VLAN 수에 대한 특정 요구 사항을 가질 수 있습니다. 동일한 서비스 제공 업체 네트워크에서 여러 고객이 필요로하는 VLAN 범위는 쉽게 겹칠 수 있으며 인프라를 통과하는 트래픽은 혼합 될 수 있습니다. 각 고객에게 고유 한 VLAN ID 범위를 할당하면 고객 구성이 제한되고 VLAN 매핑 테이블을 집중적으로 처리해야하며 최대 VLAN 한계 인 4096 을 쉽게 초과 할 수 있습니다.



관리형 스위치는 여러 개의 VLAN 태그를 지원하므로 MAN (Metro Access Network) 공간으로 수많은 독립적 인 고객 LAN 의 트래픽을 통합하여 공급자 브리지로 MAN 애플리케이션에서 사용할 수 있습니다. 공급자 브리지의 목적 중 하나는 VLAN 태그를 인식하고 사용하여 MAN 공간의 VLAN 을 고객의 VLAN 과 독립적으로 사용할 수 있도록하는 것입니다. 이는 MAN 에 진입하는 프레임에 대해 MAN 관련 VID 가있는 VLAN 태그를 추가하여 수행됩니다. MAN 을 떠날 때 태그는 제거되고 고객 관련 VID 가있는 원래 VLAN 태그를 다시 사용할 수 있습니다.

이는 VLAN 태그를 간섭하지 않으면 서 일반적인 MAN 공간을 통해 원격 costumer VLAN 을 연결하는 터널링 메커니즘을 제공합니다. 모든 태그는 EtherType 0x8100 또는 0x88A8 을 사용합니다. 여기서 0x8100 은 고객 태그 용이고 0x88A8 은 서비스 공급자 태그 용입니다.

주어진 서비스 VLAN 이 스위치에 2 개의 구성원 포트만있는 경우 특정 VLAN 에 대해 학습을 비활성화 할 수 있으므로 두 포트 간의 포워딩 메커니즘으로 플러딩을 사용할 수 있습니다. 이렇게하면 MAC 테이블 요구 사항이 줄어 듭니다.

Global VLAN Configuration

The Global VLAN Configuration screen in 그림 4-6-1 appears.

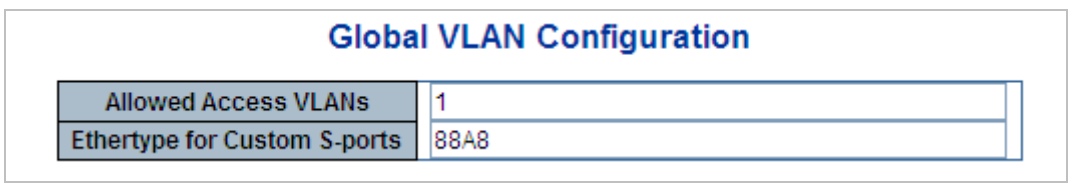


그림 4-6-1 : Global VLAN Configuration Screenshot

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Allowed Access VLANs**	이 필드는 허용 된 액세스 VLAN 을 표시하며 액세스 포트로 구성된 포트에만 영향을줍니다. 다른 모드의 포트는 허용 된 VLAN 필드에 지정된 모든 VLAN 의 구성원입니다. 기본적으로 VLAN 1 만 활성화됩니다. 개별 요소가 쉼표로 구분되는 목록 구문을 사용하면 더 많은 VLAN 을 만들 수 있습니다. 범위는 상한과 하한을 구분하는 대시로 지정됩니다. 다음 예에서는 VLAN 1, 10, 11, 12, 13, 200 및 300 : 1,10-13,200,300 을 만듭니다. 분리 문자 사이에는 공백을 사용할 수 있습니다
• **Ethertype for Custome S-ports**	이 필드는 사용자 정의 S 포트에 사용되는 ethertype / TPID (16 진수로 지정)를 지정합니다. 포트 유형이 S-Custom-Port 로 설정된 모든 포트에 대해 설정이 적용됩니다.

Port VLAN 설정

그림 4-6-2 의 VLAN Port Configuration 화면이 나타납니다..

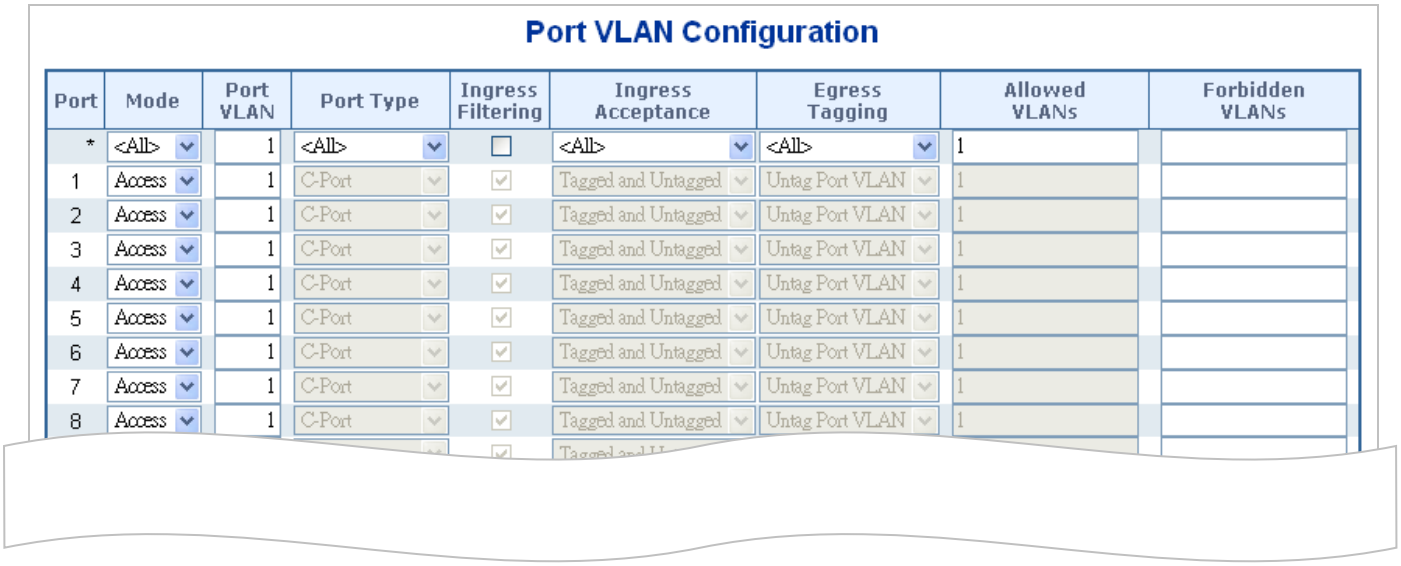


그림 4-6-2 : Port VLAN Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적		설명
• **Port**		이것은이 행의 논리 포트 번호입니다.
• **Mode**	**Access**	액세스 포트는 일반적으로 최종 스테이션에 연결하는 데 사용됩니다. 음성 VLAN 과 같은 다이내믹 기능은 배경에 더 많은 VLAN 에 포트를 추가 할 수

		있습니다. 액세스 포트에는 다음과 같은 특징이 있습니다.: • 정확히 하나의 VLAN 인 포트 VLAN (액세스 VLAN)의 멤버 (기본적으로 1) • 태그없는 및 태그가 지정된 프레임을 허용합니다. • 액세스 VLAN 으로 분류되지 않은 모든 프레임을 폐기합니다. • 송신시 액세스 VLAN 으로 분류 된 모든 프레임은 태그가 없게 전송됩니다. 기타 (동적으로 추가 된 VLAN)는 태그가 첨부 된 상태로 전송됩니다.
	Trunk	트렁크 포트는 여러 VLAN 에서 동시에 트래픽을 전달할 수 있으며 일반적으로 다른 스위치에 연결하는 데 사용됩니다. 트렁크 포트의 특징은 다음과 같습니다.: • 기본적으로 트렁크 포트는 모든 VLAN (1-4095)의 구성원입니다. • 트렁크 포트가 속한 VLAN 은 허용 된 VLAN 을 사용하여 제한 될 수 있습니다 • 포트가 구성원이 아닌 VLAN 으로 분류 된 프레임은 버려집니다. • 기본적으로 Port VLAN (기본 VLAN)으로 분류 된 프레임을 제외한 모든 프레임은 송신시 태그가 지정됩니다. 포트 VLAN 으로 분류 된 프레임은 출구에서 C 태그가 붙지 않습니다. • 외부 태그 지정을 모든 프레임에 태그 지정하도록 변경할 수 있습니다.이 경우 태그가 지정된 프레임 만 수신시 허용됩니다.
	Hybrid	하이브리드 포트는 다양한 방법으로 트렁크 포트와 비슷하지만 추가 포트 구성 기능을 추가합니다. 트렁크 포트에 대해 설명 된 특성 외에도 하이브리드 포트에는 다음과 같은 기능이 있습니다.: • VLAN 태그 비 인식, C- 태그 인식, S- 태그 인식 또는 S- 사용자 정의 태그 인식 가능으로 구성 가능 • 수신 필터링을 제어 가능합니다. • 수신 프레임 및 발신 설정 태깅은 독립적으로 구성 가능합니다.
• **Port VLAN**		포트의 VLAN ID (PVID)를 결정합니다. 허용되는 VLAN 의 범위는 1 ~ 4095 이며 기본값은 1 입니다.. ■ 포트가 VLAN 비 인식으로 구성되거나 프레임이 태그되지 않거나 포트에서 VLAN 인식이 활성화되어 있지만 프레임에 우선 순위 태그가 지정되면 (VLAN ID = 0) 프레임이 포트 VLAN 으로 분류됩니다. ■ 송신시 태그 태그 구성이 태그 VLAN 을 태그 해제로 설정하면 포트 VLAN 으로 분류 된 프레임에 태그가 지정되지 않습니다. 포트 VLAN 은 액세스 모드의 포트에 대해서는 "액세스 VLAN"으로, 트렁크 또는 하이브리드 모드의 포트에 대해서는 기본 VLAN 이라고합니다..
• **Port Type**		하이브리드 모드의 포트는 포트 유형을 변경할 수 있습니다. 즉, 프레임의 VLAN 태그를 사용하여 수신시 프레임을 특정 VLAN 으로 분류하는 데 사용되는지 여부와 특정 TPID 로 응답 할 TPID 를 결정할 수 있습니다. 마찬가지로 출구에서 태그가 필요한 경우 포트 유형이 태그의 TPID 를 결정합니다..

	■ **Unaware:** 진입시 VLAN 태그를 가지고 있든 없든 모든 프레임은 포트 VLAN 으로 분류되며 가능한 태그는 송신시 제거되지 않습니다. ■ **C-Port:** 수신시 TPID 가 0x8100 인 VLAN 태그가있는 프레임은 태그에 포함 된 VLAN ID 로 분류됩니다. 프레임에 태그가 없거나 우선 순위 태그가 지정되면 프레임은 포트 VLAN 으로 분류됩니다. 프레임이 출구에서 태그 지정되어야하는 경우 C 태그로 태그가 지정됩니다.. ■ **S-Port:** 수신시 TPID = 0x8100 또는 0x88A8 인 VLAN 태그가있는 프레임은 태그에 포함 된 VLAN ID 로 분류됩니다. 프레임에 태그가 없거나 우선 순위 태그가 지정되면 프레임은 포트 VLAN 으로 분류됩니다. 프레임이 출구에서 태그 지정되어야하는 경우 S 태그로 태그가 지정됩니다. ■ **S-Custom-Port:** 수신시 TPID = 0x8100 또는 Custom-S 포트에 대해 구성된 Ethertype 과 동일한 VLAN 태그가있는 프레임은 태그에 포함 된 VLAN ID 로 분류됩니다. 프레임에 태그가 없거나 우선 순위 태그가 지정되면 프레임은 포트 VLAN 으로 분류됩니다. 프레임이 출구에서 태그 지정되어야하는 경우 맞춤 S 태그로 태그가 지정됩니다.
• **Ingress Filtering**	하이브리드 포트는 진입 필터링을 변경할 수 있습니다. 액세스 및 트렁크 포트는 항상 수신 필터링을 사용할 수 있습니다.. ■ 수신 필터링이 활성화되어 있으면 (확인란이 선택되어 있음) 포트가 구성원이 아닌 VLAN 으로 분류 된 프레임이 삭제됩니다. ■ 수신 필터링이 비활성화 된 경우 포트가 구성원이 아닌 VLAN 으로 분류 된 프레임이 수락되어 스위치 엔진으로 전달됩니다. 그러나 포트는 구성원이 아닌 VLAN 으로 분류 된 프레임을 절대로 전송하지 않습니다.
• **Ingress Acceptance**	하이브리드 포트를 사용하면 수신시 허용되는 프레임 유형을 변경할 수 있습니다.. ■ **Tagged and Untagged** 태그가 지정된 프레임과 태그가없는 프레임이 모두 허용됩니다.. ■ **Tagged Only** 태그가 지정된 프레임 만 수신시 허용됩니다. 태그없는 프레임은 삭제됩니다.. ■ **Untagged Only** 태그없는 프레임 만 진입시 허용됩니다. 태그가 지정된 프레임은 삭제됩니다..
Egress Tagging	이 옵션은 하이브리드 모드의 포트에서만 사용할 수 있습니다. 트렁크 및 하이브리드 모드의 포트는 송신시 프레임의 태깅을 제어 할 수 있습니다.. ■ **Untag Port VLAN**

	포트 VLAN 으로 분류 된 프레임은 태그가 없게 전송됩니다. 다른 프레임은 관련 태그와 함께 전송됩니다. ■ **Tag All** 포트 VLAN 으로 분류되었는지 여부와 관계없이 모든 프레임이 태그와 함께 전송됩니다.. ■ **Untag All** 포트 VLAN 으로 분류되었는지 여부와 상관없이 모든 프레임은 태그없이 전송됩니다..
• **Allowed VLANs**	트렁크 및 하이브리드 모드의 포트는 구성원이 될 수있는 VLAN 을 제어 할 수 있습니다. 필드의 구문은 사용 가능한 VLAN 필드에 사용 된 구문과 동일합니다. 기본적으로 트렁크 또는 하이브리드 포트는 모든 VLAN 의 구성원이되므로 1-4095 로 설정됩니다. 필드가 비어있을 수 있습니다. 즉, 포트가 VLAN 의 구성원이되지 않음을 의미합니다.
• **Forbidden VLANs**	포트는 하나 이상의 VLAN 의 구성원이되지 않도록 구성 될 수 있습니다. 이는 MVRP 및 GVRP 와 같은 동적 VLAN 프로토콜이 VLAN 에 동적으로 포트를 추가하는 것을 방지해야 할 때 특히 유용합니다. 트릭은 문제의 포트에서 금지 된 VLAN 을 표시하는 것입니다. 구문은 사용 가능한 VLAN 필드에 사용 된 구문과 동일합니다. 기본적으로이 필드는 비워 두어 포트가 모든 가능한 VLAN 의 구성원이 될 수 있음을 의미합니다.

포트는 포트 VLAN ID 와 동일한 VLAN 의 구성원이어야합니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.6.4 VLAN Membership 상태

이 페이지는 VLAN 사용자의 회원 자격 상태에 대한 개요를 제공합니다. 그림 4-6-4 의 VLAN Membership Status 화면이 나타납니다.

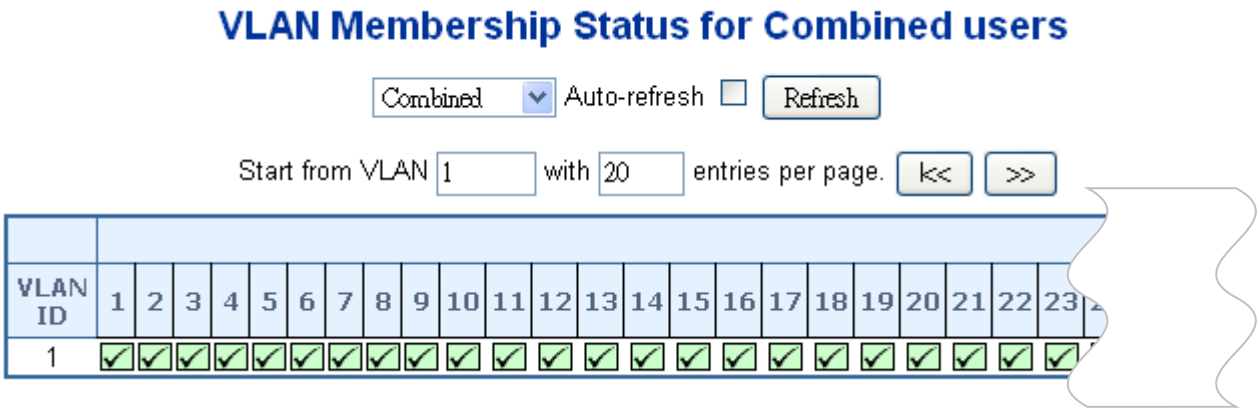


그림 4-6-4: VLAN Membership Status for Static User 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
VLAN User	- **Admin** : 수동값 설정입니다 - **NAS** : NAS 는 포트 기반 인증을 제공합니다.이 인증에는 Supplicant, Authenticator 및 Authentication Server 간의 통신이 포함됩니다. - **GVRP** : GVRP (GARP VLAN 등록 프로토콜 또는 일반 VLAN 등록 프로토콜)는 대규모 네트워크 내에서 VLAN (Virtual Local Area Network)의 제어를 용이하게하는 프로토콜입니다. - **Voice VLAN** : 음성 VLAN 은 일반적으로 IP 전화에서 발생하는 음성 트래픽 용으로 특별히 구성된 VLAN 입니다.. - **MVR** : MVR 은 각 VLAN 의 가입자에 대한 멀티 캐스트 트래픽을 복제 할 필요를 없애기 위해 사용됩니다. 모든 채널의 멀티 캐스트 트래픽은 단일 (멀티 캐스트) VLAN 에서만 전송됩니다.
• **Port Members**	각 Vlan ID 마다 각 포트의 확인란 행이 표시됩니다. 포트가 Vlan 에 포함되어있으면 , ☑ 이미지가 표시 됩니다. 포트가 사용금지를 할경우 ☒ 이미지가 표시됩니다. 금지 된 포트 목록에 포트가 포함되어 있고 동일한 금지 된 포트에 동적 VLAN 사용자 등록 VLAN 이 있으면 충돌 포트가 충돌 포트로 표시됩니다..
• **VLAN Membership**	VLAN Membership Status Page (VLAN 멤버쉽 상태 페이지)는 선택된 VLAN 사용자가 구성한 모든 VLAN 에 대한 현재 VLAN 포트 멤버를 표시합니다 (선택은 콤보 상자에서 허용되어야 함). 모든 VLAN 사용자가 선택되면 모든 VLAN 사용자에 대해이 정보가 표시됩니다. 이는 기본적으로 적용됩니다. VLAN 멤버십을 사용하면 VLAN ID 로 분류 된 프레임을 각 VLAN 멤버 포트에서 전달할 수 있습니다.

버튼

Combined : 이 드롭 다운 목록에서 VLAN Users 를 선택하십시오..

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Refresh : 즉시 페이지를 새로고침합니다.

<< : VLAN 테이블의 첫 번째 항목부터 시작하여 테이블을 업데이트합니다. 즉 가장 낮은 VLAN ID 를 가진 항목을 업데이트합니다.

>> : 현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 갱신합니다.

4.6.5 VLAN Port Status

이 페이지는 VLAN Port Staus 를 제공합니다. 그림 4-6-5 의 VLAN 포트 상태 화면이 나타납니다.

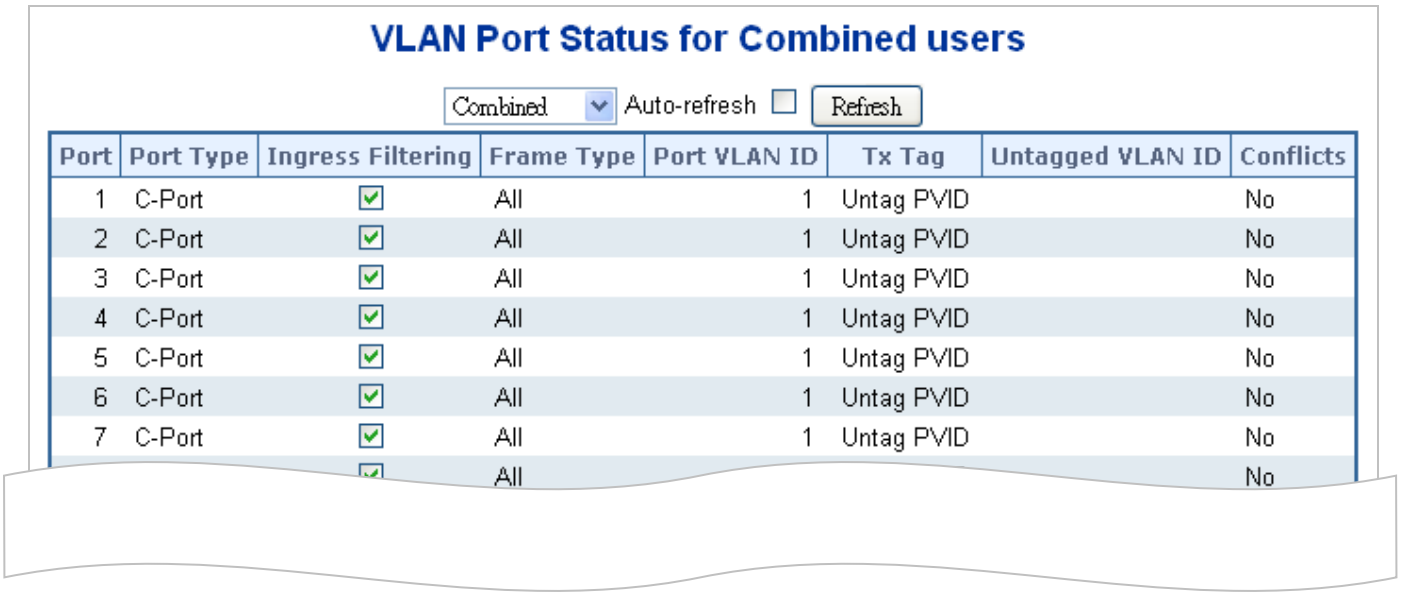


그림 4-6-5: VLAN Port Status for Combined users 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	같은 행에 포함 된 설정의 논리 포트입니다.
• **Port Type**	VLAN 인식이 활성화 된 경우 태그는 포트에서 수신 된 태그가있는 프레임에서 제거됩니다. VLAN 태그 프레임은 태그의 VLAN ID 로 분류됩니다. VLAN 인식을 비활성화하면 모든 프레임이 포트 VLAN ID 로 분류되고 태그는 제거되지 않습니다.
• **Ingress Filtering**	포트에 대한 수신 필터링을 표시합니다. 이 매개 변수는 VLAN 수신 처리에 영향을줍니다. 수신 필터링이 활성화되고 수신 포트가 프레임의 분류 된 VLAN 의 구성원이 아닌 경우 프레임이 삭제됩니다.
• **Frame Type**	포트가 모든 프레임을 허용하는지 태그가 지정된 프레임 만 허용하는지

	표시합니다. 이 매개 변수는 VLAN 수신 처리에 영향을줍니다. 포트가 태그가있는 프레임 만 수신하는 경우 해당 포트에서 수신 된 태그가없는 프레임은 무시됩니다.
• **Port VLAN ID**	포트의 PVID 설정을 표시합니다.
• **Tx Tag**	태그가 지정되었는지 또는 태그가 지정되었는지 여부에 따라 출력 필터링 프레임 상태를 표시합니다.
• **Untagged VLAN ID**	UVID (태그가없는 VLAN ID)를 표시합니다. 포트의 UVID 는 송신 측에서 패킷의 동작을 결정합니다.
• **Conflicts**	존재 여부에 관계없이 충돌 상태를 표시합니다. 휘발성 VLAN 사용자가 VLAN 구성원 또는 VLAN 포트 구성을 설정하도록 요청하면 다음과 같은 충돌이 발생할 수 있습니다.: ■ 기능 간의 기능 충돌. ■ 하드웨어 제한으로 인한 충돌. ■ 사용자 모듈 간의 직접 충돌.

버튼

: Vlan 사용자를 선택하십시오.

Auto-refresh  : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

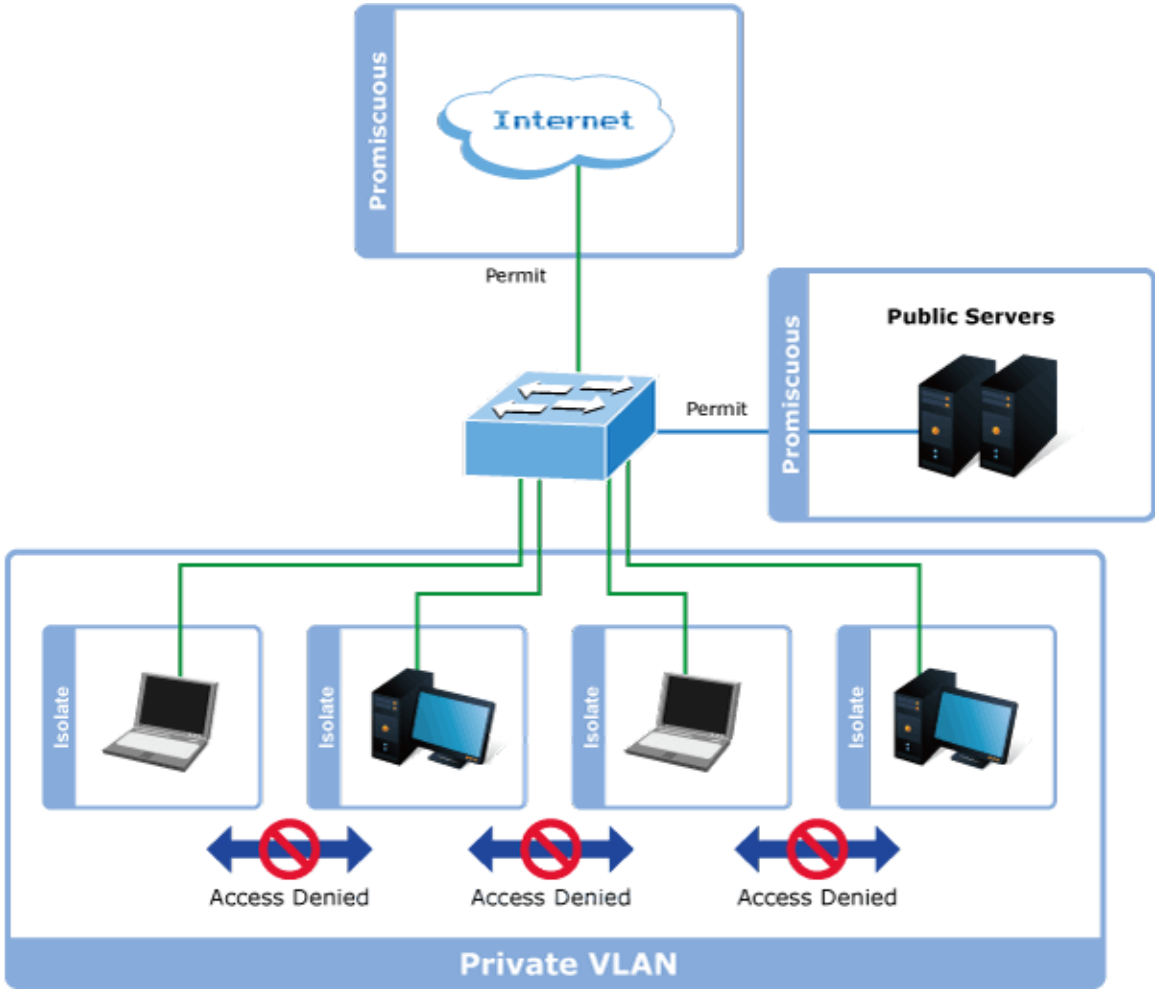
: 즉시 페이지를 새로고침합니다.

4.6.6 Port Isolation

개요

VLAN이 사설 VLAN으로 구성되면 해당 VLAN 내의 포트 간 통신이 차단 될 수 있습니다. 이 섹션에는 두 가지 응용 프로그램 예제가 제공됩니다:

- ISP에 연결된 고객은 동일한 VLAN의 구성원 일 수 있지만 해당 VLAN 내에서 서로 통신 할 수는 없습니다.
- 비무장 지대 (DMZ)의 웹 서버 팜에있는 서버는 외부 세계 및 내부 세그먼트의 데이터베이스 서버와 통신 할 수 있지만 서로 통신 할 수는 없습니다



사설 VLAN 을 적용하려면 먼저 표준 VLAN 작동을 위해 스위치를 구성해야합니다.이 스위치를 배치하면 구성된 VLAN 중 하나 이상을 사설 VLAN 으로 구성 할 수 있습니다. 사설 VLAN 의 포트는 다음 두 그룹 중 하나에 속합니다.

■ **무차별 포트**

— 트래픽을 개인 VLAN의 모든 포트로 전달할 수있는 포트

— 사설 VLAN의 모든 포트에서 트래픽을 수신 할 수있는 포트

■ **독립 포트**

— 트래픽을 전용 VLAN의 무차별 포트로만 전달할 수있는 포트

— 사설 VLAN의 무차별 포트에서만 트래픽을 수신 할 수있는 포트

무차별 및 격리 포트의 구성은 모든 사설 VLAN에 적용됩니다. 트래픽이 사설 VLAN의 무차별 포트로 들어 오면 VLAN

테이블의 VLAN 마스크가 적용됩니다. 격리 된 포트에서 트래픽이 들어 오면 VLAN 테이블의 VLAN 마스크 외에도 사설 VLAN 마스크가 적용됩니다. 이렇게하면 전용 VLAN 내의 무차별 포트로 전달할 수있는 포트가 줄어 듭니다.

이 페이지는 사설 VLAN의 포트에서 포트 격리를 활성화 또는 비활성화하는 데 사용됩니다. VLAN의 포트 구성원은 동일한 VLAN 및 사설 VLAN의 다른 격리 포트로 격리 될 수 있습니다. 그림 4-6-6의 포트 격리 화면이 나타납니다.

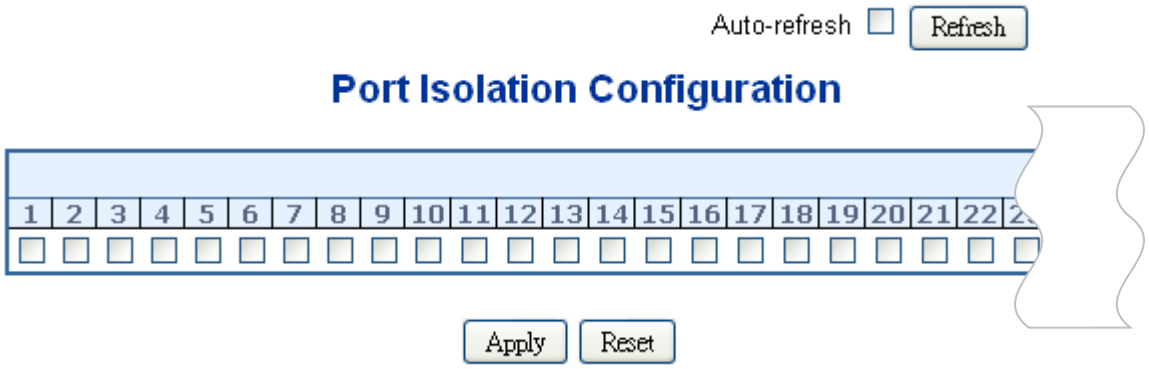


그림 4-6-6: Port Isolation Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port Members**	개인 VLAN 의 각 포트에 대한 확인란이 제공됩니다. 이 옵션을 선택하면 해당 포트에서 포트 격리가 활성화됩니다. 이 옵션을 선택하지 않으면 해당 포트에서 포트 격리가 비활성화됩니다. 기본적으로 포트 격리는 모든 포트에서 비활성화됩니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Refresh: 즉시 페이지를 새로고침합니다.

4.6.7 VLAN 셋팅 예제

- **Separate VLAN**
- **802.1Q VLAN Trunk**
- **Port Isolate**

4.6.7.1 2개의 개별 802.1Q VLANs

이 다이어그램은 Managed Switch 가 두 VLAN 에 대해 Tagged 및 Untagged 트래픽 흐름을 처리하는 방법을 보여줍니다. VLAN 그룹 2 와 VLAN 그룹 3 은 VLAN 으로 구분됩니다. 각 VLAN 은 네트워크 트래픽을 격리하여 VLAN 멤버 만 동일한 VLAN 멤버의 트래픽을 수신합니다. 그림 4-6-7 의 화면이 나타나고 표 4-6-8 은 Managed Switches 의 포트 구성을 설명합니다.

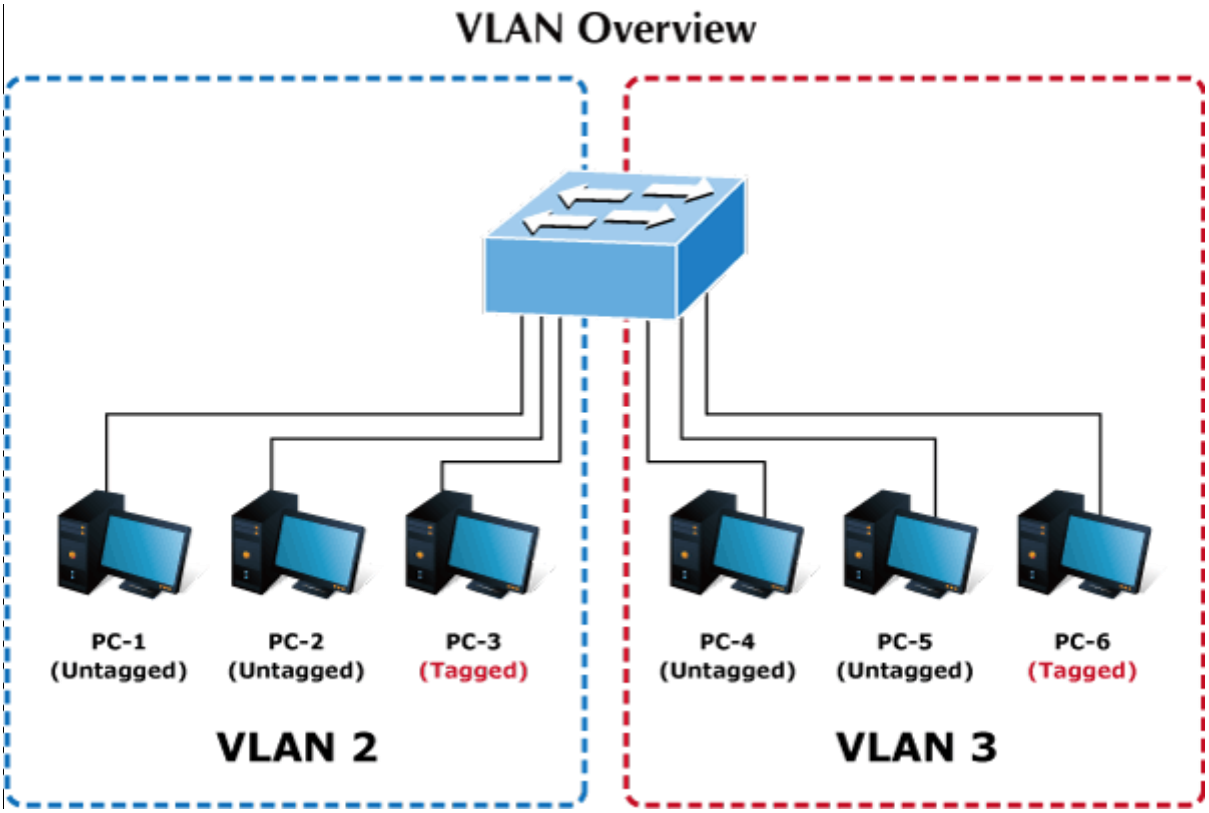


그림 4-6-7: 두 부류의 VLANs 다이아그램

VLAN Group	VID	Untagged Members	Tagged Members
VLAN Group 1	1	Port-7 ~ Port-52	N/A
VLAN Group 2	2	Port-1,Port-2	Port-3
VLAN Group 3	3	Port-4,Port-5	Port-6

표 4-1: VLAN 과 포트설정

다음과 같은 시나리오로 시작합니다.:

- **Untagged 패킷을 VLAN 2 넣습니다.**

1. **[PC-1]에서 허용하는 untagged** 패킷을 **Port-1로 넣고**, 관리형 스위치는 **VLAN Tag=2**.로 태그를 붙일 것입니다. **[PC-2]** 과 **[PC-3]** 은 **Port-2** 와 **Port-3**.를 통해 패킷을 수신합니다.

2. [PC-4],[PC-5] 과 [PC-6]패킷을 받지 않습니다.

3. **Port-2를 패킷이 떠나는 동안 태그**, VLAN Tag=2 **인 태그가 지정된 패킷으로 유지됩니다**

4. **패킷 Port-3을 떠나는 동안 VLAN Tag = 2인 태그가 지정된 패킷으로 유지됩니다.**

■ **Tagged패킷을 VLAN 2에 적용하다.**

5. [PC-3]이 VLAN Tag = 2로 태그 된 패킷을 전송하는 동안 Port-3으로 들어가면 [PC-1]과 [PC-2]는 Port-1과 Port-2를 통해 패킷을 수신합니다.

6. 패킷이 Port-1 및 Port-2를 떠나는 동안 태그가 제거되어 태그가없는 패킷이됩니다.

■ **Untagged 패킷을 넣은 VLAN 3**

1. [PC-4]가 태그가 없는 패킷을 Port-4로 전송하는 동안 스위치는 VLAN 태그 = 3으로 태그를 지정합니다. [PC-5] 및 [PC-6]은 Port-5 및 Port-6을 통해 패킷을 수신합니다.

2. 패킷이 Port-5를 떠나는 동안 태그가 제거되어 태그가 태그가없는 패킷이됩니다..

3. 패킷이 Port-6를 떠나는 동안 VLAN Tag = 3 인 태그가 지정된 패킷으로 유지됩니다.

Note

예에서 VLAN 그룹 1은 기본 VLAN으로 설정되지만 VLAN 2 및 VLAN 3 트래픽 흐름에만 초점을 맞춥니다.

설치 단계

1. VLAN Group 추가

VLANs 2 개 추가 – VLAN 2 과 VLAN 3

Type 1-3 in Allowed Access VLANs column, the 1-3 is including VLAN1 and 2 and 3.

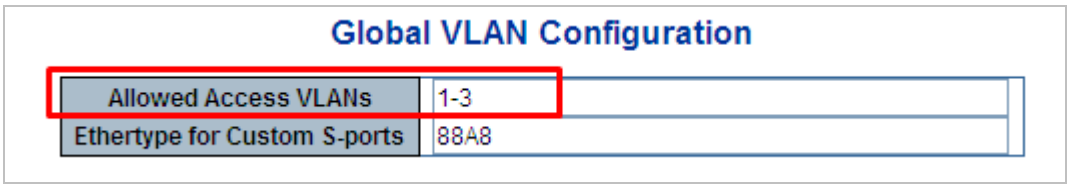


그림 4-6-8: Add VLAN 2 and VLAN 3

2. 각포트에서 Vlan 맴버 할당과 PVID 부여

VLAN 2 : Port-1,Port-2 과 Port-3

VLAN 3 : Port-4, Port-5 과 Port-6

VLAN 1 :모든 다른포트 Port-7~Port-52

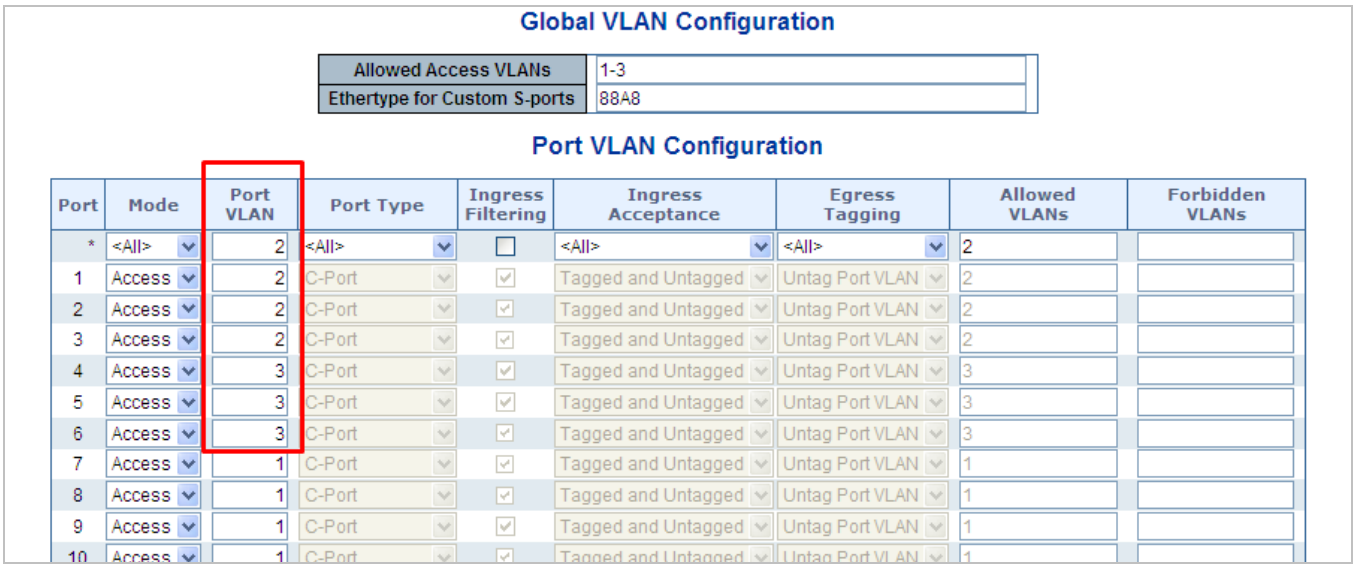


그림 4-6-9: 포트 1 ~ 3 의 포트 VLAN 을 VLAN2 로 변경하고 포트 4 ~ 6 의 포트 VLAN 을 VLAN3 으로 변경

3. 특정 포트에 VLAN 태그 사용

링크 유형: Port-3 (VLAN-2) 과 Port-6 (VLAN-3)

포트 3 모드를 트렁크로 변경하고 허용 된 VLAN 열의 태그 모두 및 유형 2 로 출력 태그 지정을 선택합니다.

포트 6 모드를 트렁크로 변경하고 허용 된 VLAN 열에 태그 모두 및 유형 3 으로 출력 태그 지정을 선택합니다.

그림 4-6-10 의 포트 별 VLAN 구성이 나타납니다..

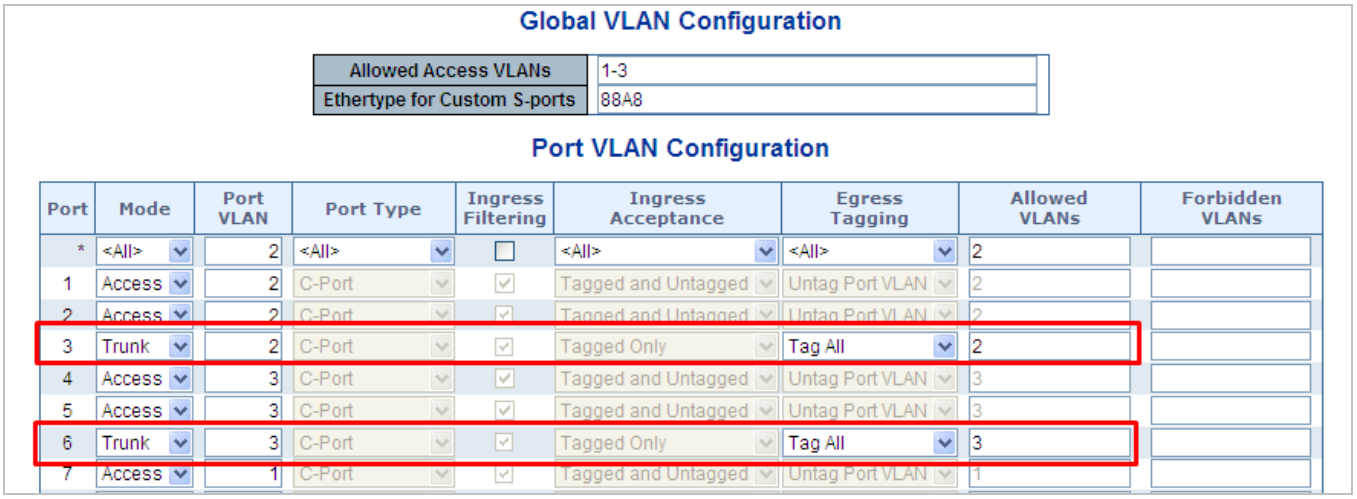


그림 4-6-10: Vlan Membership 페이지에서 Vlan 2 및 3 멤버 확인

4.6.7.2 VLAN 트렁킹 사이에 두개의 802.1Q 를 아는 스위치

부분의 경우는 다른 스위치의 "업 링크"에 사용됩니다. VLAN 은 다른 스위치에서 분리되지만 동일한 VLAN 그룹 내의 다른 스위치로 액세스해야합니다. 그림 4-6-11 의 화면이 나타납니다.

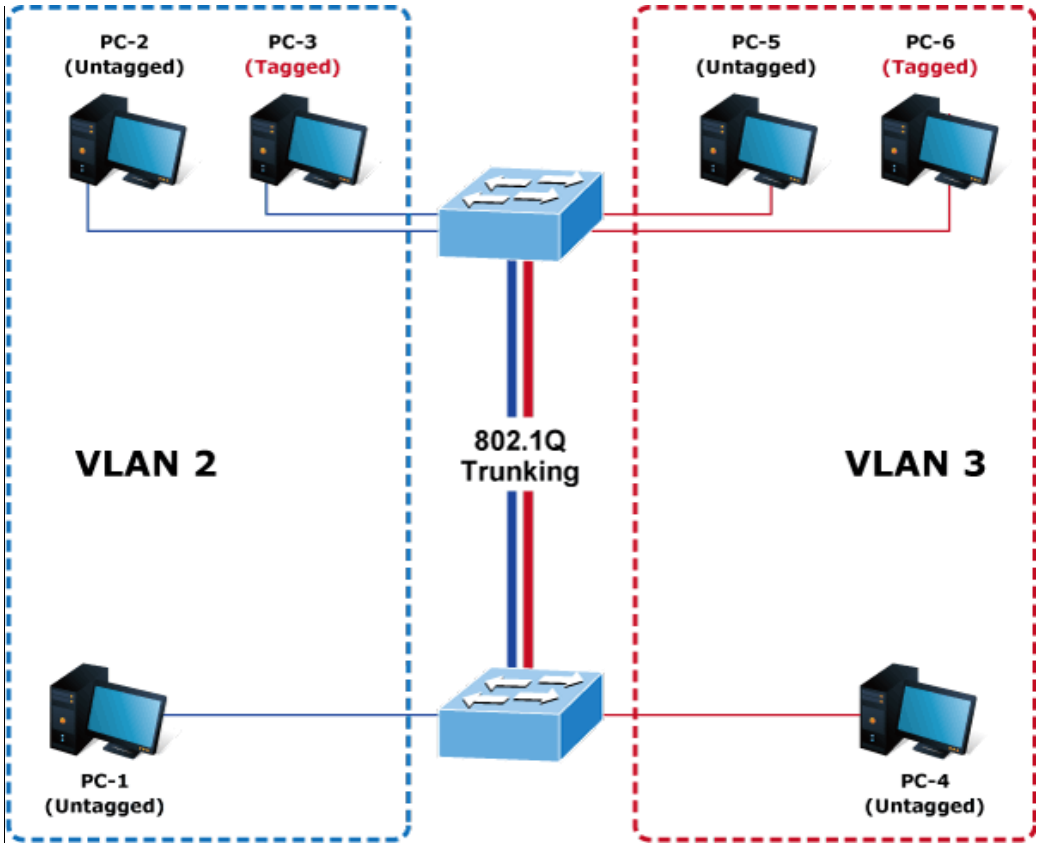


그림 4-6-11: VLAN 트렁킹 다이아그램

설치 단계

1. VLAN Group 추가

VLAN 두개 추가 – VLAN 2 과 VLAN 3

허용 액세스 VLAN 열에 1-3 을 입력하십시오. 1 - 3 은 VLAN1 및 2 와 3 을 포함합니다..

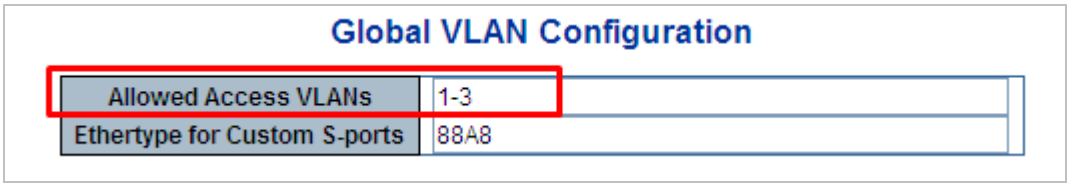


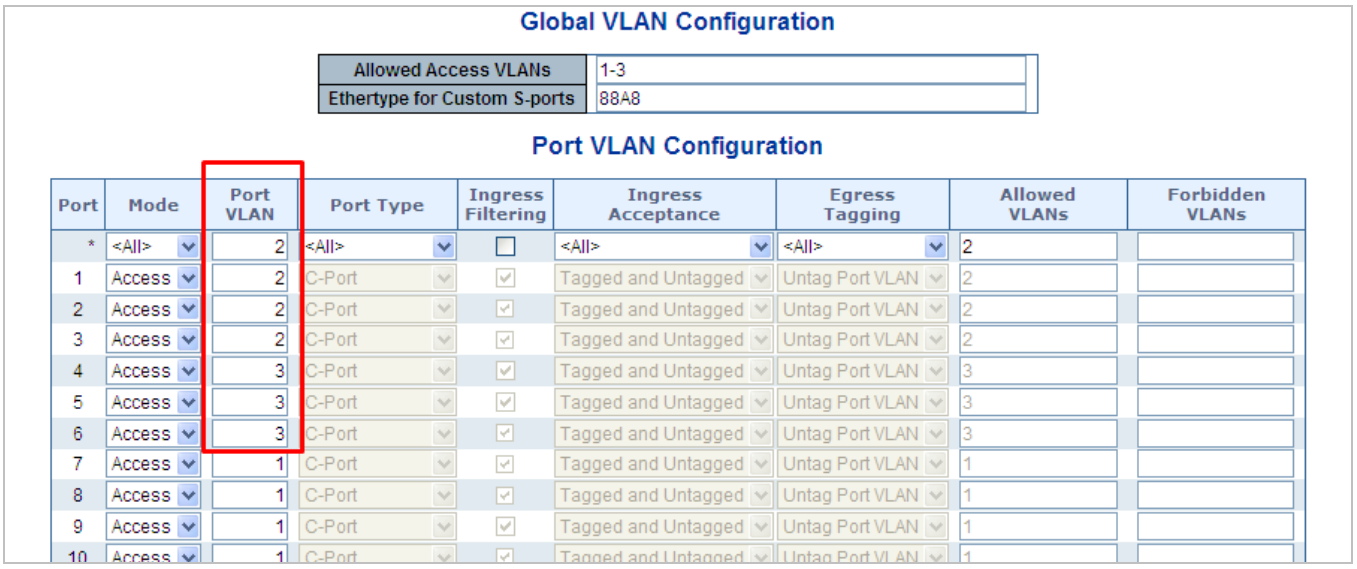
그림 4-6-12: VLAN 2 와 VLAN 3 추가

2. VLAN Member 와 각 PVID 포트의 승인 :

VLAN 2 : Port-1,Port-2 과 Port-3

VLAN 3 : Port-4, Port-5 과 Port-6

VLAN 1 : 모든 다른 포트– Port-7~Port-52



Global VLAN Configuration

Allowed Access VLANs	1-3
Ethertype for Custom S-ports	88A8

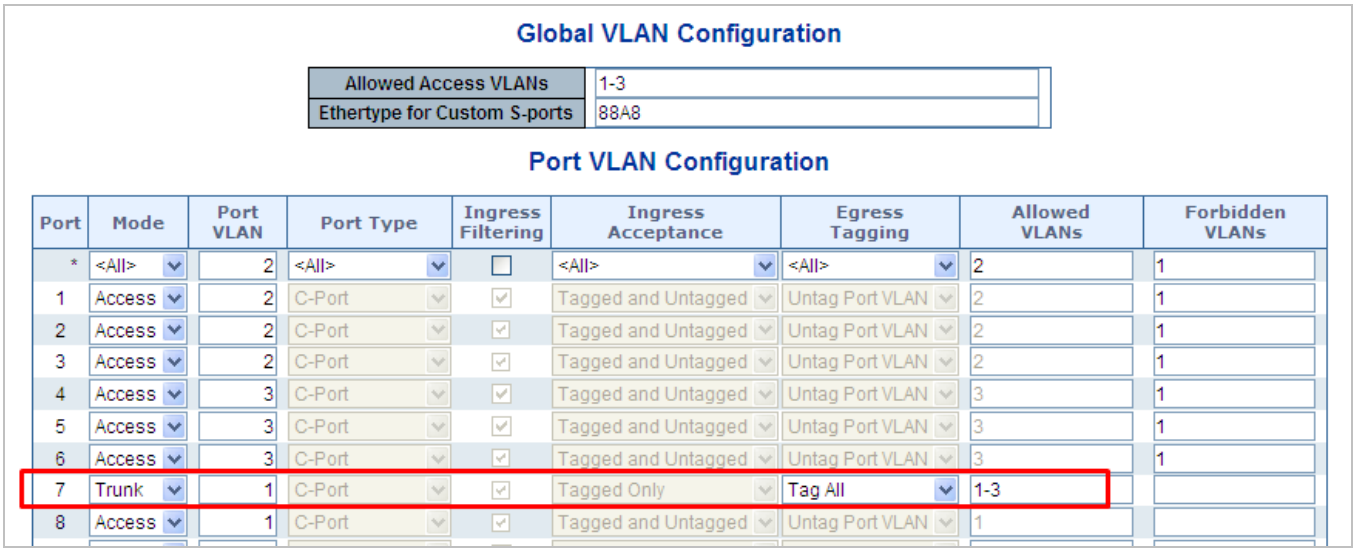
Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<All>	2	<All>	☐	<All>	<All>	2	
1	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
2	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
3	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	
4	Access	3	C-Port	☑	Tagged and Untagged	Untag Port VLAN	3	
5	Access	3	C-Port	☑	Tagged and Untagged	Untag Port VLAN	3	
6	Access	3	C-Port	☑	Tagged and Untagged	Untag Port VLAN	3	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

그림 4-6-13 포트 1 ~ 3 의 포트 VLAN 을 VLAN2 로 변경하고 포트 4 ~ 6 의 포트 VLAN 을 VLAN3 으로 변경합니다.

호스트에 연결하는 VLAN 포트는 4.6.10.1 예제를 참조하십시오. 다음 단계 VLAN 트렁크 포트 구성에 초점을 맞춥니다.

1. 포트 7을 802.1Q VLAN 트렁크 포트로 지정하십시오..
2. VLAN 구성원 구성 페이지에서 Port-7을 VLAN 2와 VLAN 3에 모두 할당합니다..
3. VLAN 1을 VLAN 2 구성원과 VLAN 3 구성원과 겹치는 "공용 영역"으로 정의하십시오..
4. 각 VLAN의 구성원이 될 VLAN 트렁크 포트를 할당합니다. 이 예에서는 Port-7을 VLAN 2 및 VLAN 3 구성원 포트로 추가합니다
5. Port-7을 802.1Q VLAN 트렁크 포트로 지정하고 트렁킹 포트는 나가는 동안 Tagged 포트 여야합니다. Port-7 구성은 그림 4-6-14에 나와 있습니다.



Global VLAN Configuration

Allowed Access VLANs	1-3
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
*	<All>	2	<All>	☐	<All>	<All>	2	1
1	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	1
2	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	1
3	Access	2	C-Port	☑	Tagged and Untagged	Untag Port VLAN	2	1
4	Access	3	C-Port	☑	Tagged and Untagged	Untag Port VLAN	3	1
5	Access	3	C-Port	☑	Tagged and Untagged	Untag Port VLAN	3	1
6	Access	3	C-Port	☑	Tagged and Untagged	Untag Port VLAN	3	1
7	Trunk	1	C-Port	☑	Tagged Only	Tag All	1-3	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

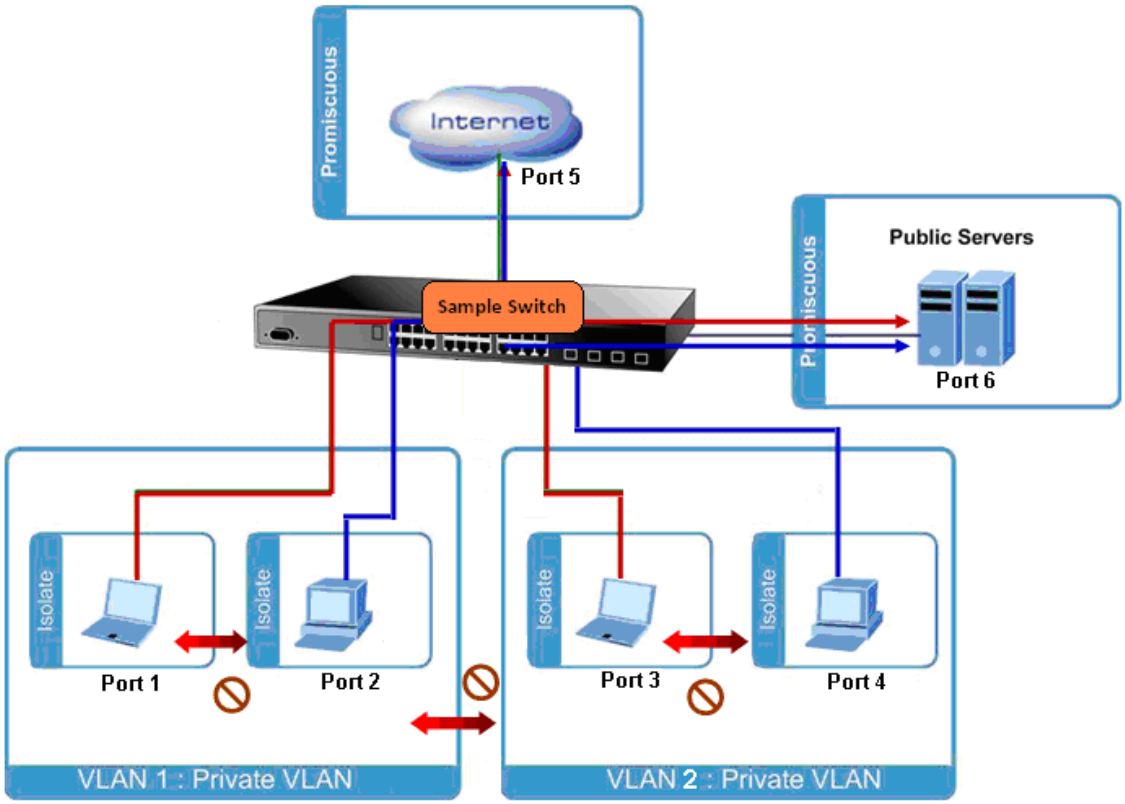
그림 4-6-14: VLAN 중복포트 설정 및 VLAN 1 – 공용 영역 구성원 지정

즉, VLAN 2 구성원 인 Port-1 에서 Port-3 및 VLAN 3 구성원 인 Port-4 에서 Port-6 도 VLAN 1 에 속하지만 다른 PVID 설정을 사용하면 패킷이 VLAN 2 를 형성하거나 VLAN 3 이 불가능합니다. 다른 VLAN 에 액세스합니다..

6. 1 ~ 6 단계를 반복하여 파트너 스위치에서 VLAN 트렁크 포트를 설정하고 VLAN 트렁크에 참가하기 위해 더 많은 VLAN을 추가 한 다음 1 ~ 3 단계를 반복하여 트렁크 포트를 VLAN에 할당합니다..

4.6.7.3 Port Isolate

이 다이어그램은 관리되는 스위치가 격리 포트와 무차별 포트를 처리하는 방법을 보여 주며 각 PC 는 다른 모든 PC 의 격리 포트에 액세스 할 수 없습니다. 하지만 그들은 모두 동일한 서버 / AP / 프린터로 액세스해야합니다. 이 섹션에서는 각 격리 포트에서 액세스 할 수있는 서버 포트를 구성하는 방법을 보여줍니다.



설치 단계

1. 등록 포트 모드

독립포트를 Port-1~Port-4 로 설정합니다.

무속성 포트에 Port5 및 Port-6 을 설정하십시오. 그림 4-6-17 의 화면이 나타납니다..

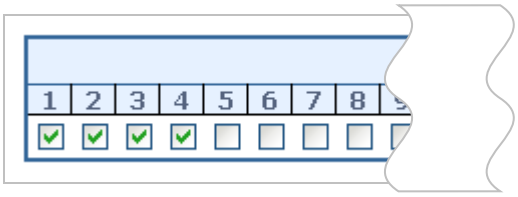


그림 4-6-17: 격리 포트 및 무분별한 포트의 구성

4.6.8 MAC-based VLAN

여기에 MAC 기반 VLAN 엔티티를 구성 할 수 있습니다. 이 페이지에서는 MAC 기반 VLAN 항목을 추가 및 삭제하고 다른 포트에 항목을 할당 할 수 있습니다. 이 페이지에는 정적 항목 만 표시됩니다. 그림 4-6-18 의 MAC 기반 VLAN 화면이 나타납니다..

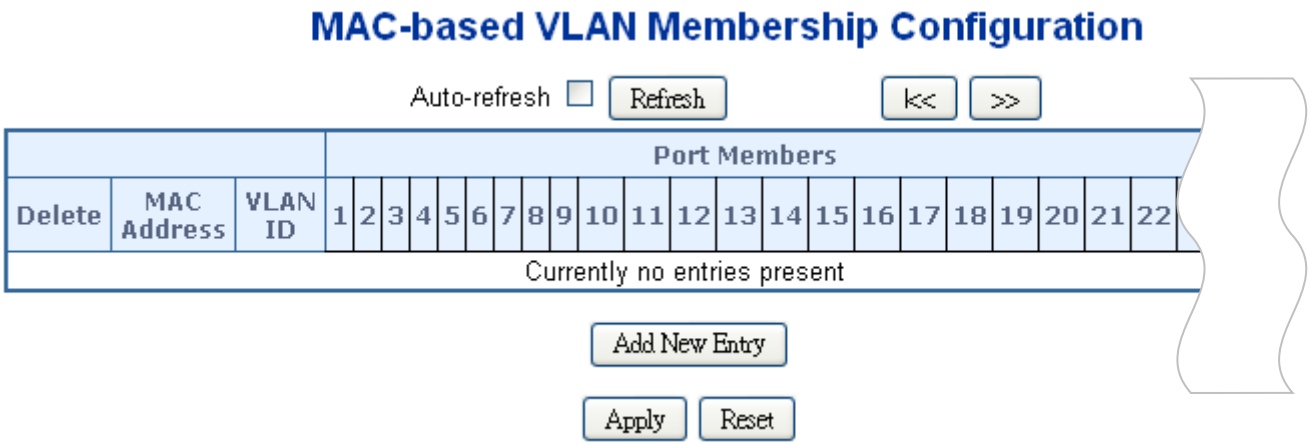


그림 4-6-18: MAC 기반 VLAN 멤버십 설정 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	MAC 기반 VLAN 항목을 삭제하려면이 상자를 선택하고 저장을 누릅니다.
• **MAC Address**	MAC 주소를 나타냅니다.
• **VLAN ID**	VLAN ID 를 나타냅니다.
• **Port Members**	MAC 기반 VLAN 항목마다 각 포트의 확인란 행이 표시됩니다. MAC 기반 VLAN 에 포트를 포함 시키려면 해당 상자를 선택하십시오. MAC 기반 VLAN 에서 포트를 제거하거나 제외하려면 상자가 선택 해제되어 있는지 확인하십시오. 기본적으로 포트는 구성원이 아니며 모든 상자는 선택되지 않습니다.
• **Adding a New MAC-based VLAN**	"Add New Entry (새 항목 추가)"를 클릭하여 새 MAC 기반 VLAN 항목을 추가합니다. 빈 행이 테이블에 추가되고 필요에 따라 MAC 기반 VLAN 항목을 구성 할 수 있습니다. 모든 유니 캐스트 MAC 주소는 MAC 기반 VLAN 항목에 대해 구성 할 수 있습니다. 브로드 캐스트 또는 멀티 캐스트 MAC 주소는 허용되지 않습니다. VLAN ID 의 유효한 값은 1 ~ 4095 입니다. MAC 기반 VLAN 항목은 "저장"을 클릭하면 활성화됩니다. "저장"을 클릭하면 포트 구성원이없는 MAC 기반 VLAN 이 삭제됩니다. "Delete"버튼은 새로운 MAC 기반 VLAN 의 추가를 취소하는 데 사용할 수 있습니다.

버튼

Add New Entry: 새 MAC 기반 VLAN 항목을 추가하려면 누릅니다.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Refresh: 즉시 페이지를 새로고침합니다.

<<: MAC 기반 VLAN 테이블의 첫 번째 항목부터 시작하여 테이블을 업데이트합니다..

>>: 현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 업데이트합니다.

4.6.9 MAC-based VLAN Status

이 페이지는 다양한 MAC 기반 VLAN 사용자가 구성한 MAC 기반 VLAN 항목을 표시합니다. 그림 4-6-19 의 MAC 기반 VLAN 상태 화면이 나타납니다..

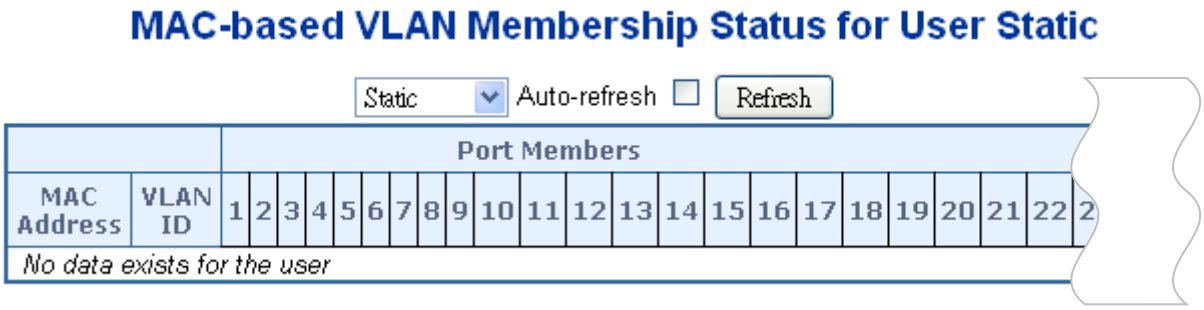


그림 4-6-19: 사용자 정적에 대한 MAC 기반 VLAN 구성원 구성 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **MAC Address**	MAC 주소를 나타냅니다.
• **VLAN ID**	VLAN ID 를 나타냅니다.
• **Port Members**	Vlan 엔트리에 MAC-기반에 Port 멤버를 나타냅니다.

버튼

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Refresh: 즉시 페이지를 새로고침합니다.

4.6.10 프로토콜 기반 VLAN

이 페이지를 사용하면 그룹 이름 (각 그룹에 고유 한) 매핑 항목에 새 프로토콜을 추가 할 수있을뿐 아니라 스위치에 이미 매핑 된 항목을보고 삭제할 수 있습니다. 그림 4-6-20 의 프로토콜 기반 VLAN 화면이 나타납니다.

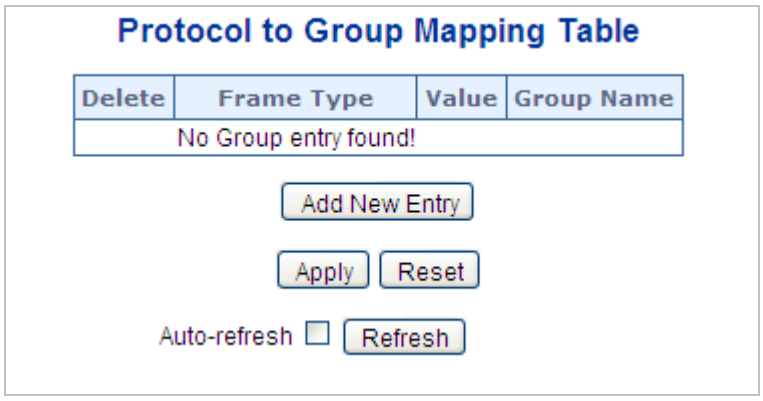


그림 4-6-20: 그룹 매핑 테이블에 대한 프로토콜 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	프로토콜을 그룹 이름 맵 항목을 삭제하려면이 상자를 선택하십시오. 항목은 다음 저장 중에 스위치에서 삭제됩니다.
• **Frame Type**	프레임 유형은 다음 값 중 하나를 가질 수 있습니다.: 1. **Ethernet** 2. **LLC** 3. **SNAP** 참고 : 프레임 유형 필드를 변경하면 다음 텍스트 필드의 유효 값이 선택한 새 프레임 유형에 따라 달라집니다..
• **Value**	이 텍스트 필드에 입력 할 수있는 유효한 값은 이전 프레임 유형 선택 메뉴에서 선택한 옵션에 따라 다릅니다. 아래 세 가지 프레임 유형에 대한 기준이 있습니다.: 1. **For Ethernet**: 이더넷이 프레임 유형으로 선택된 경우 텍스트 필드의 값을 etype 이라고합니다. etype 에 유효한 값은 0x0600-0xffff 범위입니다. 2. **For LLC**: 이 경우 유효한 값은 두 개의 다른 하위 값으로 구성됩니다. a. **DSAP**: 1-바이트 로깅 함 (0x00-0xff) b. **SSAP**: 1-byte long string (0x00-0xff) 3. **For SNAP**: 이 경우 유효한 값은 두 개의 다른 하위 값으로 구성됩니다. a. **OUI**: OUI (Organizationally Unique Identifier) 는 xx-xx-xx 형식의

	값이며 여기서 string 의 각 쌍 (xx)은 0x00-0xff 의 16 진수 값 범위입니다. b. **PID**: OUI 가 16 진수 000000 이면 프로토콜 ID 는 SNAP 상단에서 실행중인 프로토콜의 이더넷 유형 (EtherType) 필드 값입니다. OUI 가 특정 조직의 OUI 인 경우 프로토콜 ID 는 해당 조직에서 SNAP 을 기반으로 실행되는 프로토콜에 할당 된 값입니다.. 다른 말로, OUI 필드의 값이 00-00-00 이면 PID 의 값은 etype (0x0600-0xffff)이고 OUI 의 값이 00-00-00 이 아닌 경우 PID 의 유효한 값은 0x0000 ~ 0xffff.
• **Group Name**	유효한 그룹 이름은 알파벳 (a-z 또는 A-Z)과 정수 (0-9)의 조합으로 구성된 모든 항목에 대해 고유 한 16 자 긴 문자열입니다. 참고 : 특수 문자와 밑줄 (_)은 사용할 수 없습니다.
• **Adding a New Group to VLAN mapping entry**	"새 항목 추가"를 클릭하여 매핑 테이블에 새 항목을 추가하십시오. 빈 행이 테이블에 추가됩니다. 프레임 유형, 값 및 그룹 이름은 필요에 따라 구성 할 수 있습니다. "삭제"버튼을 사용하여 새 항목 추가를 취소 할 수 있습니다.

버튼

Add New Entry: 매핑 테이블에 새 항목을 추가하려면 클릭하십시오.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Refresh: 즉시 페이지를 새로고침합니다.

4.6.11 프로토콜 기반 VLAN

이 페이지에서는 이미 구성된 그룹 이름을 스위치 용 VLAN 에 매핑 할 수 있습니다. 그림 4-6-21 의 Group Name to VLAN Mapping 표 화면이 나타납니다.

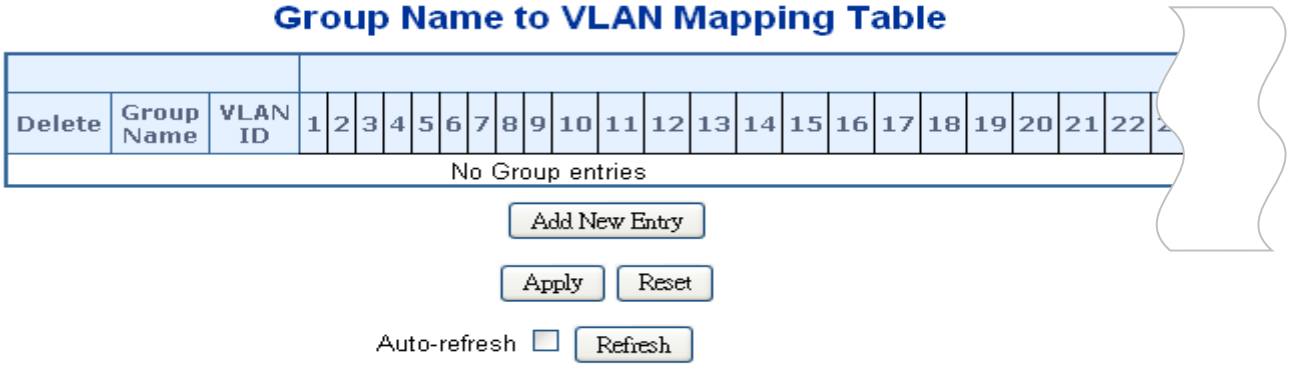


그림 4-6-21: Group Name to VLAN Mapping 표 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	그룹 이름 - VLAN 맵 항목을 삭제하려면이 상자를 선택하십시오. 항목이 다음 저장 중에 스위치에서 삭제됩니다
• **Group Name**	유효한 그룹 이름은 영문자 (a-z 또는 A-Z)와 정수 (0-9)의 조합으로 구성된 최대 16 자의 문자열이며 특수 문자는 사용할 수 없습니다. VLAN 에 매핑하려는 그룹 이름은 프로토콜 대 그룹 매핑 테이블에 있어야하며이 페이지의 다른 기존 매핑 항목에 의해 사용되어서는 안됩니다.
• **VLAN ID**	그룹 이름이 매핑 될 ID 를 나타냅니다. 유효한 VLAN ID 의 범위는 1-4095 입니다.
• **Port Members**	VLAN ID 매핑에 대한 각 그룹 이름에 대해 각 포트의 확인란 행이 표시됩니다. 매핑에 포트를 포함하려면 해당 상자를 선택하십시오. 매핑에서 포트를 제거하거나 제외하려면 상자가 선택 취소되어 있는지 확인하십시오. 기본적으로 포트는 구성원이 아니며 모든 상자는 선택되지 않습니다.
• **Adding a New Group to VLAN mapping entry**	"새 항목 추가"를 클릭하여 매핑 테이블에 새 항목을 추가하십시오. 테이블에 빈 행이 추가되고 필요에 따라 그룹 이름, VLAN ID 및 포트 구성원을 구성 할 수 있습니다. VLAN ID 의 유효한 값은 1 ~ 4095 입니다. "삭제"버튼을 사용하여 새 항목 추가를 취소 할 수 있습니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Refresh: 즉시 페이지를 새로고침합니다.

4.7 Spanning Tree Protocol(STP)

4.7.1 이론

스패닝 트리 프로토콜은 네트워크 루프를 감지 및 비활성화하고 스위치, 브리지 또는 라우터간에 백업 링크를 제공하는 데 사용할 수 있습니다. 이를 통해 스위치는 네트워크의 다른 브리징 장치와 상호 작용하여 네트워크의 두 스테이션간에 단 하나의 경로 만 존재하는지 확인하고 기본 링크가 다운 될 때 자동으로 인계하는 백업 링크를 제공합니다. 이 스위치가 지원하는 스패닝 트리 알고리즘에는 다음 버전이 포함됩니다.

- **STP – Spanning Tree Protocol (IEEE 802.1D)**
- **RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)**
- **MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)**

IEEE 802.1D 스패닝 트리 프로토콜 및 IEEE 802.1w Rapid Spanning Tree Protocol 을 사용하면 네트워크 내에서 루프를 형성하는 스위치 사이의 링크를 차단할 수 있습니다. 스위치 사이에 여러 링크가 감지되면 기본 링크가 설정됩니다. 중복 된 링크는 사용이 차단되고 대기 링크가됩니다. 이 프로토콜을 사용하면 기본 링크가 실패한 경우 복제 링크를 사용할 수 있습니다. 스패닝 트리 프로토콜이 구성되고 활성화되면 기본 링크가 설정되고 복제 된 링크가 자동으로 차단됩니다. 운영자의 개입 없이도 (주 링크 장애시) 차단 된 링크의 재 활성화가 자동으로 수행됩니다.

이 자동 네트워크 재구성은 네트워크 사용자에게 최대 가동 시간을 제공합니다. 그러나 스패닝 트리 알고리즘 및 프로토콜의 개념은 복잡하고 복잡한 주제이므로 완전히 연구하고 이해해야합니다. 스패닝 트리가 잘못 구성된 경우 네트워크 성능이 심각하게 저하 될 수 있습니다. 기본값을 변경하기 전에 다음을 읽어보십시오..

스위치 STP 는 다음을 수행합니다.:

- 스위칭 또는 브리징 요소의 모든 조합에서 단일 스패닝 트리를 생성합니다
- 단일 스위치 내에 포함 된 포트의 조합을 통해 사용자 지정 그룹에 여러 개의 스패닝 트리를 생성합니다..
- 트리의 모든 요소의 오류, 추가 또는 제거를 보완하기 위해 스패닝 트리를 자동으로 재구성합니다..
- 운영자 개입없이 스패닝 트리를 재구성합니다..

Bridge Protocol Data Units

STP 가 안정적인 네트워크 토폴로지에 도달하려면 다음 정보가 사용됩니다:

- 고유 한 스위치 식별자
- 각 스위치 포트와 관련된 루트에 대한 경로 비용
- 포트 식별자

STP 는 브리지 프로토콜 데이터 단위 (BPDU)를 사용하여 네트워크의 스위치간에 통신합니다. 각 BPDU 에는 다음 정보가 들어 있습니다.:

- 송신 스위치가 현재 믿고있는 스위치의 고유 식별자는 루트 스위치입니다
- 송신 포트에서 뿌리까지의 경로 비용
- 송신 포트의 포트 식별자

스위치는 BPDU 를 전송하여 통신하고 스패닝 트리 토폴로지를 구성합니다. 패킷이 전송되는 LAN 에 연결된 모든

스위치는 BPDU 를 수신합니다. BPDU 는 스위치에 의해 직접 전달되지 않지만 수신 스위치는 프레임의 정보를 사용하여 BPDU 를 계산하고 토폴로지가 변경되면 BPDU 전송을 시작합니다.

BPDU 를 통한 스위치 간 통신 결과는 다음과 같습니다.:

- 하나의 스위치가 루트 스위치로 선택됩니다
- 각 스위치에 대해 루트 스위치까지의 최단 거리가 계산됩니다
- 지정된 스위치가 선택됩니다. 이것은 루트 스위치에 가장 가까운 스위치로 패킷을 통해 루트로 전달 됩니다.
- 각 스위치의 포트가 선택됩니다. 이 스위치는 스위치에서 루트 스위치로 가는 최상의 경로를 제공합니다
- STP 에 포함된 포트가 선택됩니다.

안정적인 STP Topology 만들기

루트 포트를 가장 빠른 링크로 만드는 것입니다. 모든 스위치에 STP 가 기본 설정으로 활성화 된 경우 네트워크에서 가장 낮은 MAC 주소를 가진 스위치가 루트 스위치가됩니다. 최상의 스위치의 우선 순위를 높이면 (우선 순위 번호 낮춤) STP 는 루트 스위치로 최상의 스위치를 선택해야합니다.

기본 매개 변수를 사용하여 STP 를 활성화하면 스위치 네트워크의 소스 스테이션과 대상 스테이션 사이의 경로가 이상적이지 않을 수 있습니다. 예를 들어 현재 루트 포트보다 높은 번호를 가진 포트에 고속 링크를 연결하면 루트 포트가 변경 될 수 있습니다..

STP 포트 상태

BPDU 는 네트워크를 통과하는 데 약간의 시간이 걸립니다. 이 전파 지연으로 인해 차단 상태에서 전달 상태로 직접 전환 된 포트가 일시적인 데이터 루프를 만들 수있는 토폴로지 변경이 발생할 수 있습니다. 포트는 패킷 전달을 시작하기 전에 네트워크 전체에 새로운 네트워크 토폴로지 정보가 전파 될 때까지 기다려야합니다. 또한 이전 토폴로지를 기반으로 전달 된 BPDU 패킷의 패킷 수명이 만료 될 때까지 기다려야합니다. 포워드 지연 타이머는 토폴로지가 변경된 후 네트워크 토폴로지가 안정화되도록 허용합니다. 또한 STP 는 토폴로지가 변경된 후 안정적인 네트워크 토폴로지가 생성되도록 포트가 전환해야하는 상태를 지정합니다.

STP 를 사용하는 스위치의 각 포트는 다음 5 가지 상태 중 하나에 있습니다.:

- **Blocking** – 포트가 패킷을 전달하거나 수신하지 못하도록 차단 되는 경우
- **Listening** – 포트가 BPDU 패킷을 수신하기 위해 대기하고 포트를 차단 상태로 되돌릴 수 있음을 알립니다.
- **Learning** – 포트가 전달 데이터베이스에 주소를 추가하고 있지만 아직 패킷을 전달하지 않습니다.
- **Forwarding** – 포트가 패킷을 전달하고 있습니다.
- **Disabled** – 포트는 네트워크 관리 메시지에만 응답하므로 차단 상태로 먼저 복귀해야합니다

포트는 다음과 같이 한 상태에서 다른 상태로 전환합니다.:

- 초기화(스위치 부팅)시에 Blocking
- blocking 에서 listening 나 disabled 상태로 전환
- listening 에서 learning 나 disabled 상태로 전환
- learning 에서 forwarding 나 disabled 상태로 전환
- forwarding 에서 disabled 상태로 전환
- disabled 부터 blocking 상태로 전환

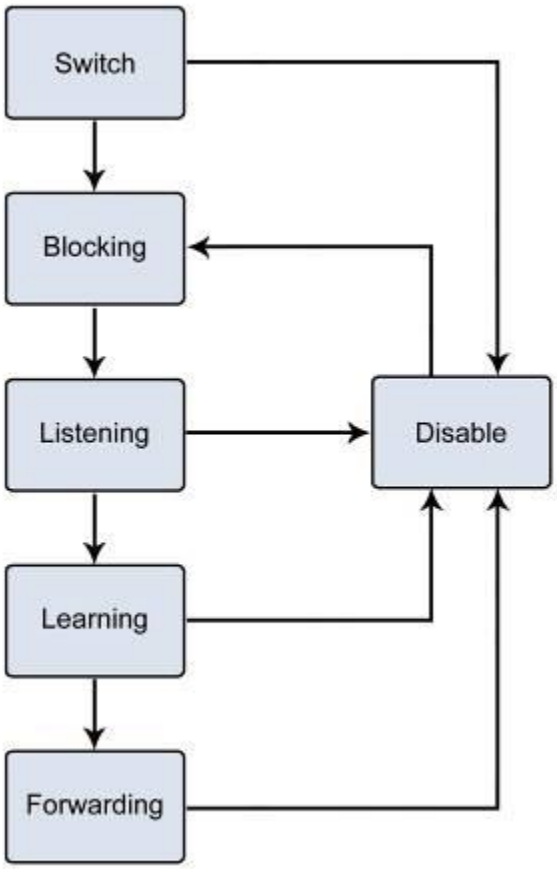


그림 4-7-1: STP 포트 상태로 전환

관리 소프트웨어를 사용하여 각 포트 상태를 수정할 수 있습니다. STP 를 활성화하면 네트워크의 모든 스위치에있는 모든 포트가 차단 상태를 통과 한 다음 전원을 켤 때 청취 및 학습 상태를 통해 전환됩니다. 적절하게 구성된 경우 각 포트는 전달 또는 차단 상태로 안정화됩니다. 해당 포트에 대해 전달 상태가 활성화 될 때까지 BPDU 를 제외한 어떤 패킷도 STP 가능 포트에서 전달되거나 수신되지 않습니다.

2. STP Parameters

STP 진행 수준

스위치는 스위치 레벨과 포트 레벨의 두 가지 작동 레벨을 허용합니다. 스위치 레벨은 하나 이상의 스위치 사이의 링크로 구성된 스패닝 트리를 형성합니다. 포트 수준은 하나 이상의 포트 그룹으로 구성된 스패닝 트리를 구성합니다. STP 는 두 수준 모두에서 동일한 방식으로 작동합니다.

스위치 레벨에서 STP는 각 스위치에 대한 브리지 식별자를 계산 한 다음 루트 브리지와 지정된 브리지를 설정합니다.
포트 수준에서 STP는 루트 포트와 지정된 포트를 설정합니다.

다음은 스위치 레벨에 대해 사용자가 구성 할 수있는 STP 매개 변수입니다.:

파라미터	설명	기본값
Bridge Identifier(Not user configurable except by setting priority below)	사용자 설정 우선 순위와 스위치의 MAC 주소의 조합. Bridge Identifier 는 두 파트로 구성됩니다. 16 비트 우선 순위 및 48 비트 이더넷 MAC 주소 32768 + MAC	32768 + MAC
Priority	각 스위치의 상대적 우선 순위 - 낮은 번호는 우선 순위를 높이며 주어진 스위치가 루트 브리지로 선택 될 확률이 높습니다	32768
Hello Time	스위치의 hello 메시지 broadcast 간 시간	2 초
Maximum Age Timer	포트에 대해 수신 된 BPDU 의 나이를 측정하고 BPDU 의 나이가 최대 나이 타이머의 값을 초과 할 때 BPDU 가 폐기되도록합니다.	20 초
Forward Delay Timer	학습 및 대기 상태에서 포트가 기다리는 시간. 포트를 차단 상태로 되돌릴 수있는 BPDU	15

The following are the user-configurable STP parameters for the port or port group level:

변동	설명	기본
Port Priority	각각에 대한 상대적 우선 순위 포트 - 낮은 포트 번호는 주어진 포트가 루트 포트로 선택 될 확률이 높습니다.	128
Port Cost	경로를 평가하기 위해 STP 에서 사용하는 값 - STP 는 경로 비용을 계산하고 최소 비용의 경로를 활성 경로로 선택합니다.	200,000-100Mbps Fast Ethernet ports 20,000-1000Mbps Gigabit Ethernet ports 0 - 자

기본 STP 설

특징	기본
Enable state	모든 STP 포트 비활성
Port priority	128
Port cost	0
Bridge Priority	32,768

사용자가 변경할 수있는 STA 매개 변수

스위치의 공장 출하시 설정은 대부분의 설치에 적용됩니다. 그러나 기본 설정을 공장 출하 상태로 유지하는 것이 좋습니다. 그렇지 않으면 절대적으로 필요합니다. 스위치의 사용자 변경 가능 매개 변수는 다음과 같습니다.

우선 순위 - 스위치의 우선 순위는 0 에서 65535 까지 설정할 수 있습니다. 0 은 가장 높은 우선 순위와 같습니다..

Hello Time – Hello 시간은 1 ~ 10 초입니다. 이것은 다른 모든 스위치에게 실제로 루트 브리지임을 알리기 위해 루트 브리지에서 전송 한 BPDU 패킷의 두 번 전송 사이의 간격입니다. 스위치에 Hello 시간을 설정하고 루트 브리지가 아닌 경우 스위치가 루트 브리지가 될 때 설정된 Hello 시간이 사용됩니다.

Hello 시간을 최대값보다 크게 할경우 오류가 발생할 수 있습니다.

Max. Age – 최대 Age 은 6 ~ 40 초가 될 수 있습니다. 최대 Age 이 끝나고 BPDU 가 여전히 루트 브리지에서 수신되지 않은 경우 스위치는 루트 브리지가 될 수 있도록 다른 모든 스위치에 자체 BPDU 를 보내기 시작합니다. 스위치의 브리지 식별자가 가장 낮 으면 루트 브리지가됩니다.

Forward Delay Timer – 전달 지연 시간은 4 ~ 30 초입니다. 차단 상태에서 전달 상태로 전환하는 동안 스위치의 모든 포트가 listening 상태로있는 시간입니다.

위의 매개 변수를 설정할 때 다음 공식을 준수하십시오.:

Max. Age _ 2 x (Forward Delay - 1 second)

Max. Age _ 2 x (Hello Time + 1 second)

Port Priority – 포트 우선 순위는 0 부터 240 까지 가능합니다. 숫자가 낮을수록 포트가 루트 포트로 선택 될 확률이 높아집니다.

Port Cost – 포트 비용은 0 에서 200000000 까지 설정할 수 있습니다. 숫자가 낮을수록 포트가 패킷을 전달할 확률이 높아집니다

3. STP 실제 예

루프에 연결된 3 개의 스위치에 대한 간단한 그림이 아래 그림에 그려져 있습니다. 이 예에서는 STP 지원이 적용되지 않은 경우 주요 네트워크 문제를 예상 할 수 있습니다.

스위치 A 가 스위치 B 에 패킷을 브로드 캐스트하면 스위치 B 가 스위치 B 로 스위치를 브로드 캐스트하고 스위치 C 가 스위치 A 로 다시 브로드 캐스트합니다. 브로드 캐스트 패킷은 무한 루프로 전달되어 잠재적으로 네트워크 오류를 일으킬 수 있습니다. 이 예에서 STP 는 스위치 B 와 C 사이의 연결을 차단하여 루프를 끊습니다. 특정 연결을 차단하는 결정은 가장 최근의 브리지 및 포트 설정의 STP 계산을 기반으로합니다.

이제 스위치 A 가 스위치 C 에 패킷을 브로드 캐스트하면 스위치 C 가 포트 2 에서 패킷을 버리고 브로드 캐스트가 여기서 끝납니다. 기본값이 아닌 다른 값을 사용하는 STP 설정은 복잡 할 수 있습니다. 따라서 기본 출하시 설정을 유지하는 것이 좋으며 STP 는 자동으로 루트 브리지 / 포트를 할당하고 루프 연결을 차단합니다. STP 가 우선 순위 설정을 사용하여 루트 브리지로 특정 스위치를 선택하도록하거나 포트 우선 순위 및 포트 비용 설정을 사용하여 차단할 특정 포트를 선택하도록 STP 에 영향을주는 것은 비교적 간단합니다..

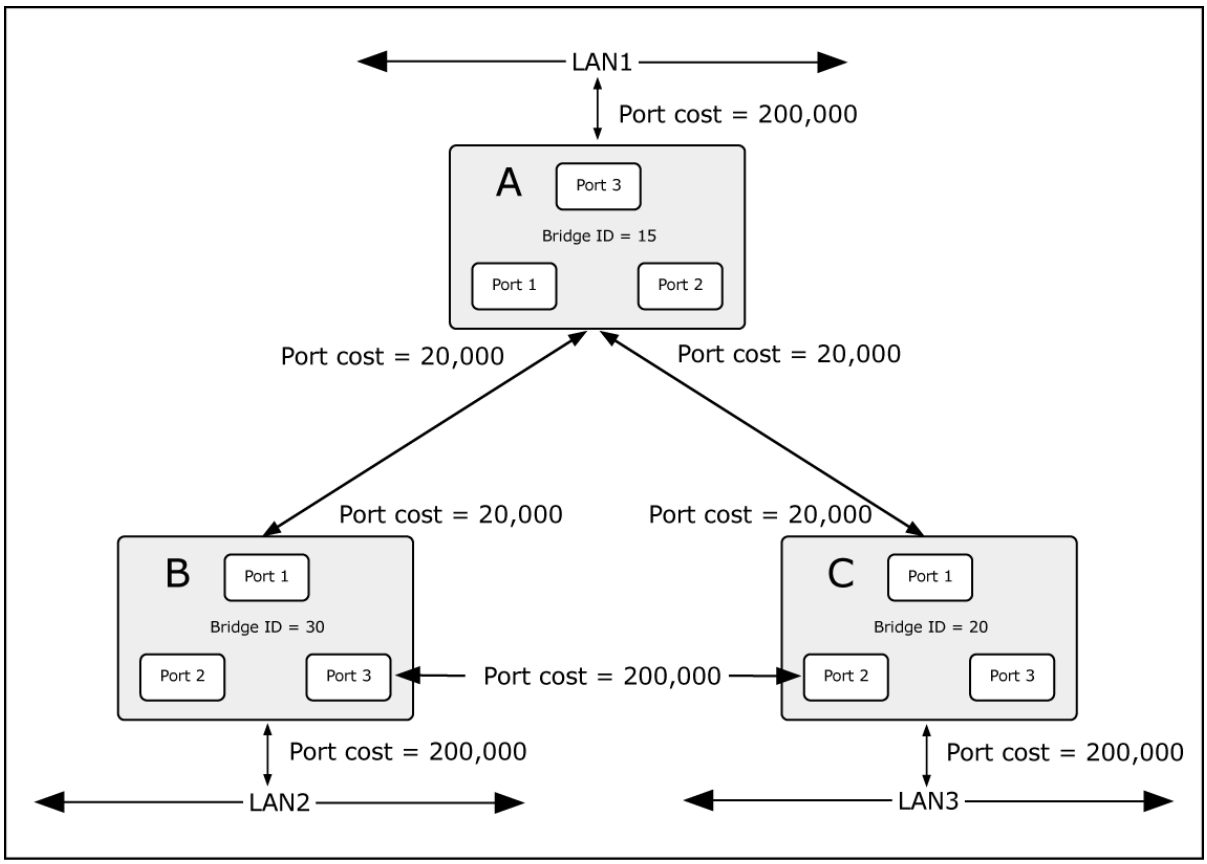


그림 4-7-2: STA 법칙을 적용하기

STP 의 기본값을 설정했을 경우의 예

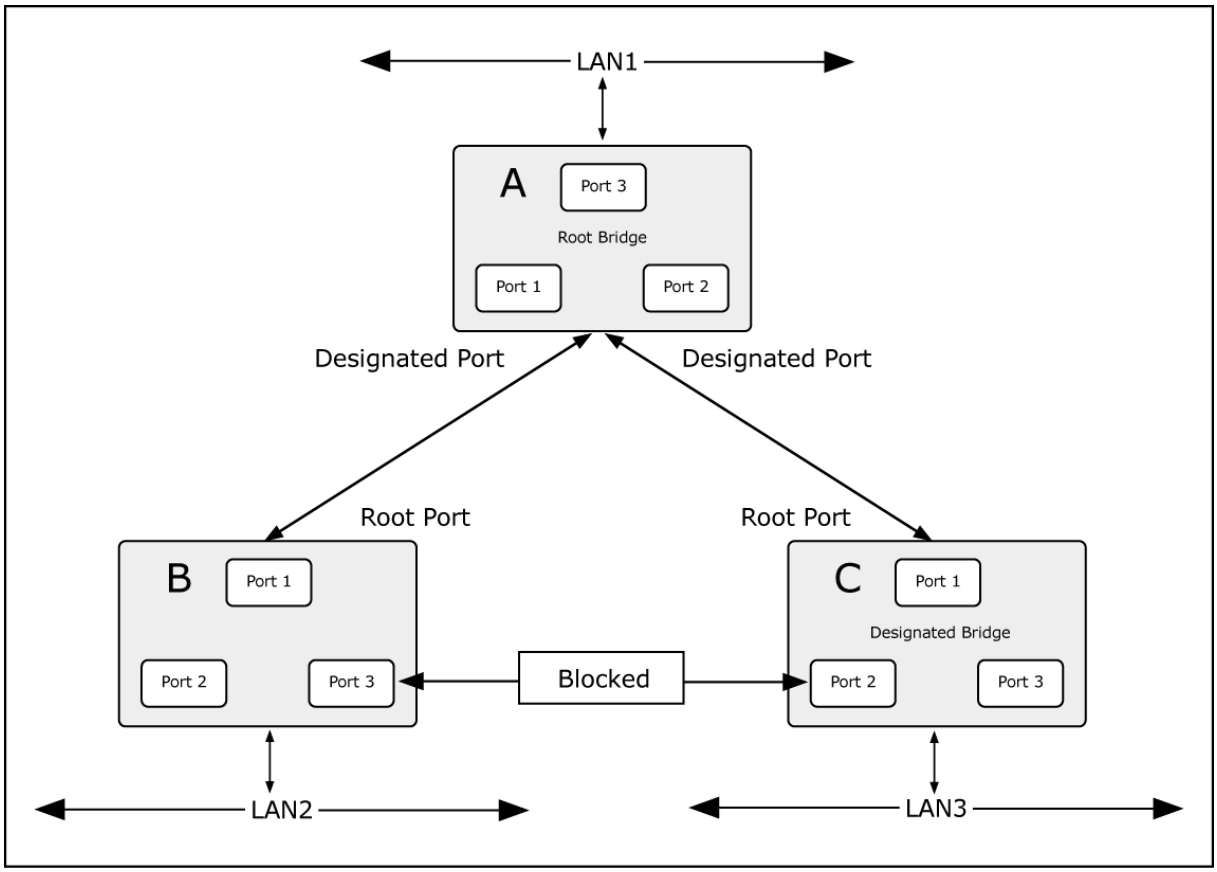


그림 4-7-3: STA 법칙을 적용하고 난 후

가장 낮은 브리지 ID (스위치 C)를 가진 스위치가 루트 브리지로 선출되었으며 스위치 B 와 C 사이에 높은 포트 비용을

제공하도록 포트가 선택되었습니다. 스위치의 두 개의 (선택 사항) 기가비트 포트 (기본 포트 비용 = 20,000) A 는 스위치 B 와 C 모두에서 하나의 (옵션) 기가비트 포트에 연결됩니다. 스위치 B 와 C 사이의 중복 링크는 의도적으로 100Mbps 패스트 이더넷 링크 (기본 포트 비용 = 200,000)로 선택됩니다. 기가비트 포트를 사용할 수 있지만 스위치 B 와 스위치 C 사이의 링크가 차단 된 링크인지 확인하려면 포트 비용을 기본값보다 늘려야합니다.

4.7.2 STP 시스템 설정

이 페이지에서는 시스템 설정을 구성 할 수 있습니다. 이 설정은 스위치의 모든 STP Bridge 인스턴스에서 사용됩니다. 관리 형 스위치는 다음과 같은 스패닝 트리 프로토콜을 지원합니다.:

- **호환성 SPanning Tree Protocol (STP):** 루프를 방지하고 제거하는 엔드 스테이션간에 단일 경로를 제공합니다.
- **일반 Rapid Spanning Tree Protocol (RSTP) :** 전달 루프를 만들지 않고 빠른 스패닝 트리 수렴을 제공하는 네트워크 토폴로지를 감지하고 사용합니다.
- **확장—Multiple Spanning Tree Protocol (MSTP) :** 가상 LAN (VLAN)의 유용성을 더욱 발전시키기 위해 RSTP에 대한 확장을 정의합니다. 이 "VLAN 별"다중 스패닝 트리 프로토콜은 각 VLAN 그룹에 대해 별도의 스패닝 트리를 구성하고 각 스패닝 트리 내에서 가능한 대체 경로 중 하나를 제외하고 모두 차단합니다.

STP 시스템 설정은 그림 4-7-4 에 나타나 있습니다.

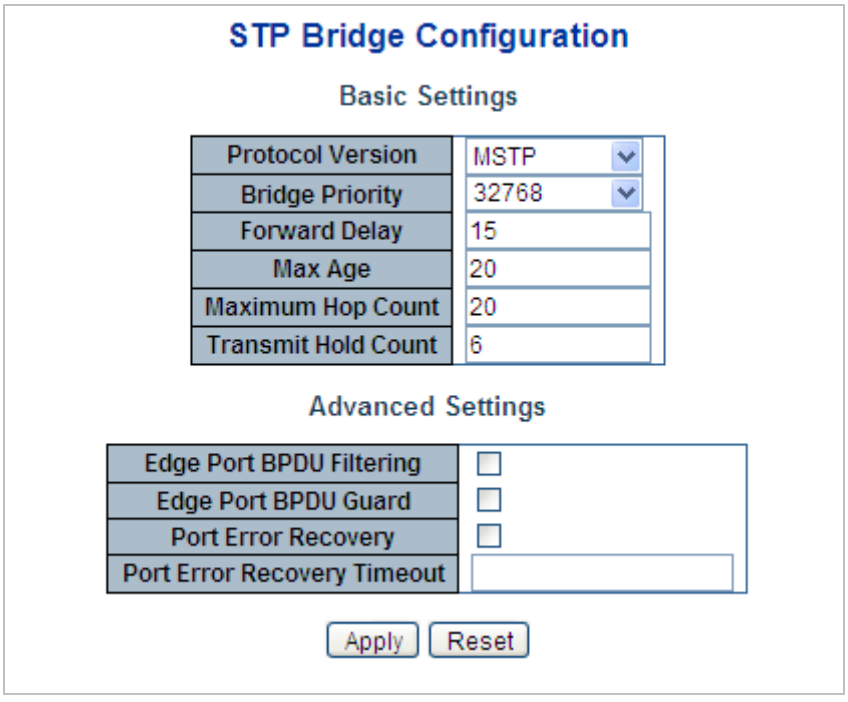


그림 4-7-4: STP 브릿지 설정 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

기본 셋팅

목적	설명
• **Protocol Version**	STP 프로토콜 버전 설정입니다. 유효한 값은 다음과 같습니다.: ■ **STP** (IEEE 802.1D Spanning Tree Protocol) ■ **RSTP** (IEEE 802.2w Rapid Spanning Tree Protocol) ■ **MSTP** (IEEE 802.1s Multiple Spanning Tree Protocol)
• **Bridge Priority**	브리지 우선 순위를 제어합니다. 수치가 낮을수록 우선 순위가 높아집니다. 브리지 우선 순위와 MSTI 인스턴스 번호는 스위치의 6 바이트 MAC 주소와 연결되어 브리지 식별자를 형성합니다. MSTP 작동의 경우 CIST 의 우선 순위입니다. 그렇지 않으면 STP / RSTP 브리지의 우선 순위입니다.
• **Forward Delay**	루트 및 지정된 포트를 전달로 전환하기 위해 STP 브리지가 사용하는 지연시간 (STP 호환 모드에서 사용됨). 유효한 값의 범위는 4 ~ 30 초입니다. -기본값: 15 -최소값: 4 보다 높게 또는 [(최대. 메시지 Age / 2) + 1] -최대값: 30
• **Max Age**	브리지가 루트 브리지 일 때 브리지가 전송하는 정보의 최대 수명입니다. 유효한 값은 6 - 40 초입니다.. -기본값: 20 -최소값: 6 보다 높거나 또는 [2 x (Hello Time + 1)]. -최대값: 40 보다 낮거나 또는 [2 x (Forward Delay -1)]
• **Maximum Hop Count**	이는 MSTI 영역의 경계에서 생성 된 MSTI 정보에 대한 나머지 홉의 초기 값을 정의합니다. 루트 브리지가 BPDU 정보를 배포 할 수있는 브리지의 수를 정의합니다. 유효한 값은 6 ~ 40 홉 범위입니다.
• **Transmit Hold Count**	브리지 포트의 BPDU 수는 초당 보낼 수 있습니다. 초과하면 다음 BPDU 의 전송이 지연됩니다. 유효한 값은 1 - 10 BPDU / 초입니다.

추가 셋팅

목적	설명
• **Edge Port BPDU Filtering**	Edge 로 명시 적으로 구성된 포트가 BPDU 를 전송하고 수신하는지 여부를 제어합니다.
• **Edge Port BPDU Guard**	Edge 로 명시 적으로 구성된 포트가 BPDU 수신시 자체를 비활성화할지 여부를 제어합니다. 포트는 오류 비활성화 상태가되고 활성 토폴로지에서 제거됩니다.
• **Port Error Recovery**	오류가 비활성화 된 상태의 포트가 특정 시간 후에 자동으로 활성화 될지 여부를 제어합니다. 복구가 활성화되어 있지 않으면 정상 STP 작동을 위해 포트를 비활성화하고 다시 활성화해야합니다. 조건은 시스템 재부트로도 지워집니다.
• **Port Error Recovery**	오류 비활성화 상태의 포트가 통과해야하는 시간을 활성화 할 수 있습니다.

Timeout	유효한 값은 30 에서 86400 초 (24 시간)입니다.

Note

관리형 스위치는 Rapid Spanning Tree Protocol 을 기본 스패닝 트리 프로토콜로 구현합니다. "호환"모드를 선택할 때 시스템은 RSTP (802.1w)를 사용하여 다른 STP (802.1D)의 BPDU 제어 패킷과 호환되고 상호 작동합니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.7.3 브릿지 상태

이 페이지는 모든 STP 브리지 인스턴스에 대한 상태 개요를 제공합니다. 표시된 테이블에는 각 STP 브리지 인스턴스에 대한 행이 있으며 여기에는 열에 다음 정보가 표시됩니다. 그림 4-7-5 의 Bridge Status (브리지 상태) 화면이 나타납니다.

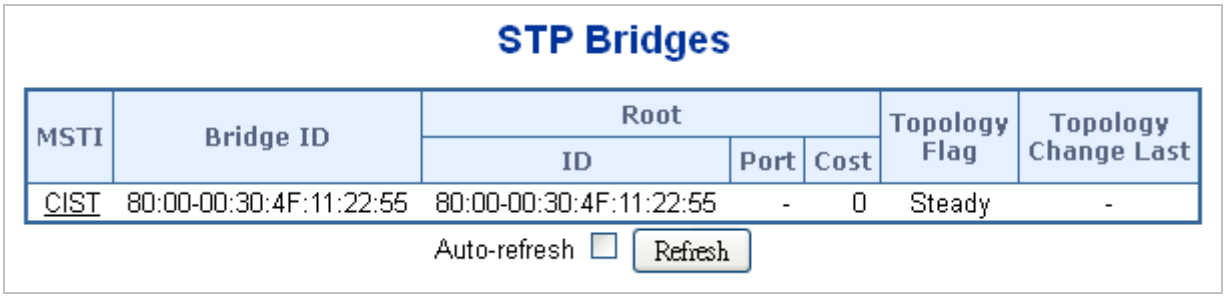


그림 4-7-5: STP Bridge Status 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **MSTI**	브릿지 개체, STP 상세 브릿지 상태에 대한 링크입니다.
• **Bridge ID**	브릿지 개체의 브릿지 ID 입니다.
• **Root ID**	선출 된 루트브릿지의 브릿지 ID 입니다.
• **Root Port**	스위치 포트에 현재 루트포트의 역할이 할당되었습니다.
• **Root Cost**	루트로의 경로 비용. 루트 브릿지의 경우값은 0 입니다. 모든 브릿지의 경우 루트 브릿지에 대한 최소 비용 경로의 포트 경로비용 합계입니다.
• **Topology Flag**	이 브릿지 개체의 토폴로지 변경플레그의 현재 상태입니다.
• **Topology Change Last**	최근 토폴로지 변경이 발생후의 때입니다.

버튼

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Refresh : 즉시 페이지를 새로고침합니다.

4.7.4 CIST 포트 설정

이 페이지에서는 사용자가 현재 STP CIST 포트 구성을 검사 할 수 있으며 가능하면이를 변경할 수도 있습니다. 그림 4-7-6 의 CIST 포트 구성 화면이 나타납니다.

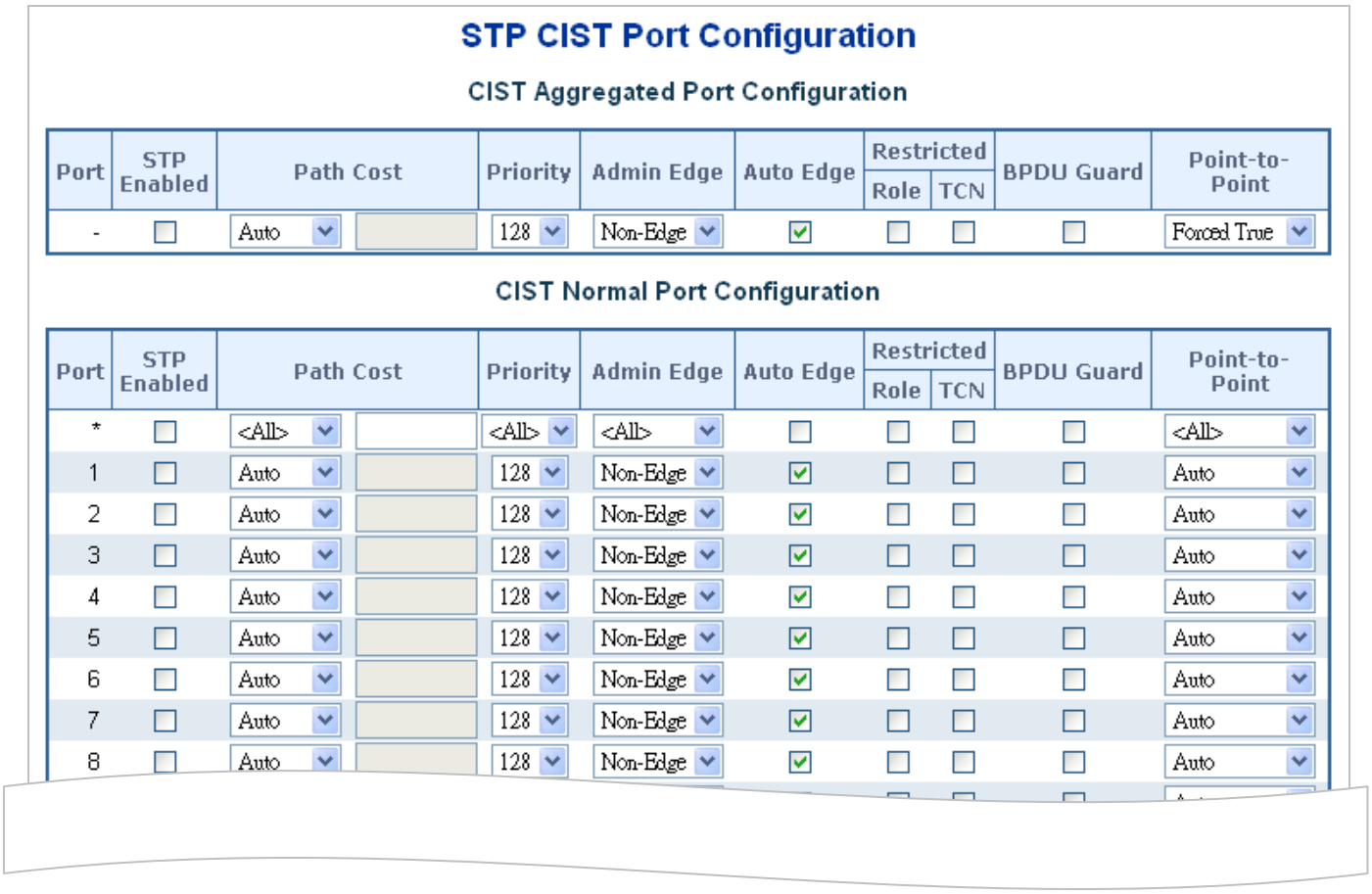


그림 4-7-6 : STP CIST 포트 설정화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	논리적 STP 포트의 스위치 포트 번호입니다.
• **STP Enabled**	이 스위치 포트에서 RSTP 를 활성화할지 여부를 제어합니다.
• **Path Cost**	Auto (자동) 설정은 802.1D 권장 값을 사용하여 물리적 링크 속도로 적절하게 경로 비용을 설정합니다. 특정 설정을 사용하여 사용자 정의 값을 입력 할 수 있습니다. 경로 비용은 네트워크의 활성 토폴로지를 설정할 때 사용됩니다. 낮은 경로 비용 포트가 높은 경로 비용 포트를 위해 전달

	포트로 선택됩니다. 유효한 값은 1 - 200000000 입니다.
• **Priority**	포트 우선 순위를 제어합니다. 이는 동일한 포트 비용을 갖는 포트의 우선 순위를 제어하는 데 사용될 수 있습니다. (위 참조). 기본값 : 128 범위 : 0-240, 16 단계
• **AdminEdge**	operEdge 플래그를 beeing 으로 시작할지 아니면 해제할지 여부를 제어합니다. (포트가 초기화 될 때의 초기 작동 상태).
• **AutoEdge**	브리지가 브리지 포트에서 자동 가장자리 감지를 활성화해야하는지 여부를 제어합니다. 이를 통해 BPDU 가 포트에서 수신되는지 여부에 따라 operEdge 를 파생시킬 수 있습니다
• **Restricted Role**	활성화 된 경우 포트가 최상의 스패닝 트리 우선 순위 벡터를 가지고 있더라도 포트가 CIST 또는 MSTI 의 루트 포트로 선택되지 않도록합니다. 이러한 포트는 루트 포트가 선택된 후에 대체 포트로 선택됩니다. 설정된 경우 스패닝 트리 연결이 부족할 수 있습니다. 네트워크 관리자가 네트워크 코어 영역 외부의 브리지가 스패닝 트리 활성 토폴로지에 영향을 미치지 않도록 설정할 수 있습니다. 브리지가 관리자의 전적인 통제하에 있지 않기 때문일 수 있습니다. 이 기능은 루트 가드라고도합니다.
• **Restricted TCN**	이 옵션을 사용하면 포트가 수신 된 토폴로지 변경 알림 및 토폴로지 변경 사항을 다른 포트로 전파하지 않도록합니다. 설정된 경우 스패닝 트리의 활성 토폴로지가 변경된 후 일시적으로 연결이 끊어 질 수 있습니다. 네트워크 관리자가 네트워크의 코어 영역 외부에 브리지가 생기지 않도록하여 해당 영역에서 주소 플러시를 유발합니다. 그 이유는 해당 브리지가 관리자의 완전한 제어하에 있지 않기 때문이거나 연결된 LAN 의 물리적 링크 상태가 자주 이동하기 때문일 수 있습니다 .
• **BPDU Guard**	활성화 된 경우 유효한 BPDU 를 수신하면 포트가 비활성화됩니다. 비슷한 브리지 설정과 달리 포트 가장자리 상태는이 설정에 영향을주지 않습니다.
• **Point-to-point**	포트가 공유 매체가 아닌 지점 간 LAN 에 연결되는지 여부를 제어합니다. 이것은 자동으로 결정되거나 true 또는 false 로 강제 설정할 수 있습니다. 포워딩 상태로의 전환은 공유 미디어보다 지점 간 LAN 에서 더 빠릅니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

기본적으로 시스템은 각 포트에서 사용되는 속도 및 이중 모드를 자동으로 감지하고 아래 표시된 값에 따라 경로 비용을

구성합니다. 경로 비용 "0"은 자동 구성 모드를 나타내는 데 사용됩니다. 짧은 경로 비용 방법을 선택하고 IEEE 8021w 표준에서 권장하는 기본 경로 비용이 65,535 를 초과하면 기본값은 65,535 로 설정됩니다. .

포트 타입	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

표 4-7-1: 권장 STP 경로 비용 범위

포트 타입	링크 타입	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

표 4-7-2: 권장 STP 경로 비용

포트 타입	링크 타입	IEEE 802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

표 4-7-3: 기본 STP 경로 비용

4.7.5 MSTI 우선순위

이 페이지를 통해 사용자는 현재 STP MSTI 브릿지 우선순위 구성을 검사하고 가능하면 이를 변경합니다. 그림 4-7-7 의 MSTI 우선순위의 화면이 나타납니다.

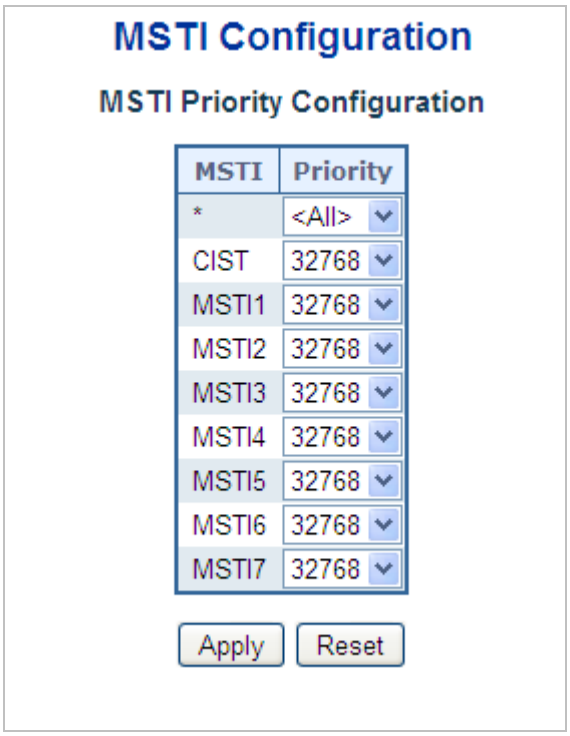


그림 4-7-7: MSTI 우선순위 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **MSTI**	브릿지 개체입니다. CIST 는 항상 활성 상태인 기본 인스턴스입니다.
• **Priority**	브리지 우선 순위를 제어합니다. 수치가 낮을수록 우선 순위가 높아집니다. 브리지 우선 순위와 MSTI 인스턴스 번호는 스위치의 6 바이트 MAC 주소와 연결되어 브리지 식별자를 형성합니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.7.6 MSTI 설정

이 페이지를 통해 사용자는 현재 STP MSTI 브리지 인스턴스 우선 순위 구성을 검사하고 가능하면이를 변경합니다. 그림 4-7-8 의 MSTI 설정화면이 나타납니다..

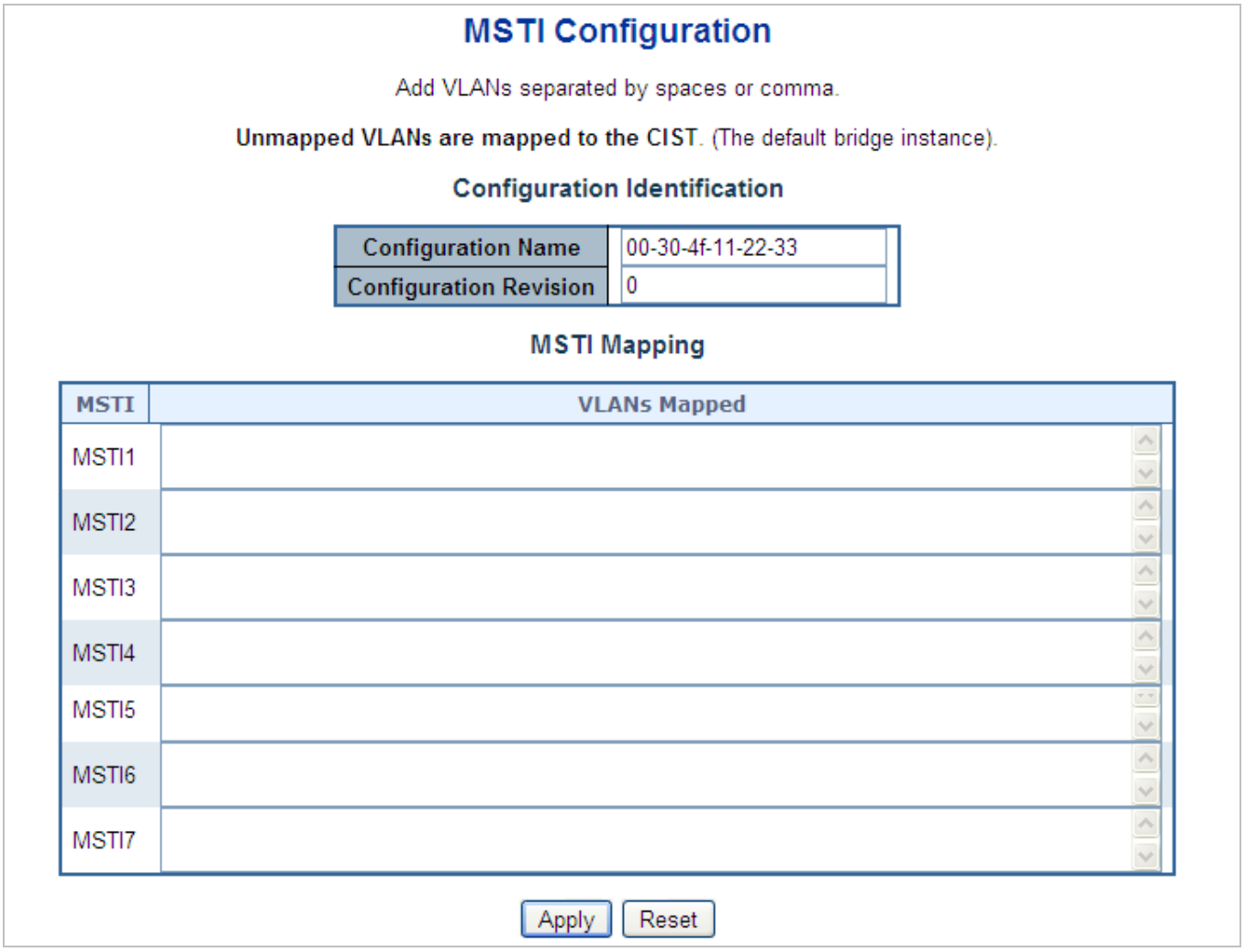


그림 4-7-8: MSTI 설정화면

이 페이지에서는 다음과 같음을 나타냅니다.:

독립 설정

목적	설명
• **Configuration Name**	VLAN 을 MSTI 로 매핑하는 이름입니다. 브리지는 MSTI 의 스패닝 트리를 공유하기 위해 VLAN-MSTI 매핑 구성뿐 아니라 이름과 버전 (아래 참조)을 공유해야합니다. (로컬 내). 이름은 최대 32 자입니다.
• **Configuration Revision**	위에 명명 된 MSTI 구성의 개정판. 0 에서 65535 사이의 정수 여야합니다.

MSTI Mapping

목적	설명
• **MSTI**	브릿지 개체입니다. 명시적으로 매핑되지 않은 Vlan 을 수신하므로 CIST 는 명시적 매핑을 사용할 수 없습니다.
• **VLANs Mapped**	MSTI 에 매핑 된 VLAN 목록입니다. VLAN 은 쉼표 및 / 또는 공백으로 구분해야합니다. VLAN 은 하나의 MSTI 에만 매핑 될 수 있습니다. 사용하지 않는 MSTI 는 그냥 비워 두어야합니다. (즉, 어떤 VLAN 도 매핑되어 있지 않습니다.)

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.7.7 MSTI 포트 설정

이 페이지를 통해 사용자는 현재 STP MSTI 포트 구성을 검사 할 수 있으며 변경 가능할 수도 있습니다. MSTI 포트는 구성되고 각 포트에 적용 가능한 각 MSTI 인스턴스에 대한 각 활성 CIST (실제) 포트에 대해 개별적으로 인스턴스화되는 가상 포트입니다. 실제 MSTI 포트 구성 옵션을 표시하기 전에 MSTI 인스턴스를 선택해야합니다.
이 페이지에는 실제 및 집계 된 포트에 대한 MSTI 포트 설정이 포함되어 있습니다. 집계 설정은 전역입니다. 그림 4-7-9 및 그림 4-7-10 의 MSTI 포트 구성 화면이 나타납니다.

그림 4-7-9 : MSTI 포트 설정 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

MSTI 포트 설정

목적	설명
• **Select MSTI**	브리지 개체를 선택하고 자세한 구성을 설정하십시오.

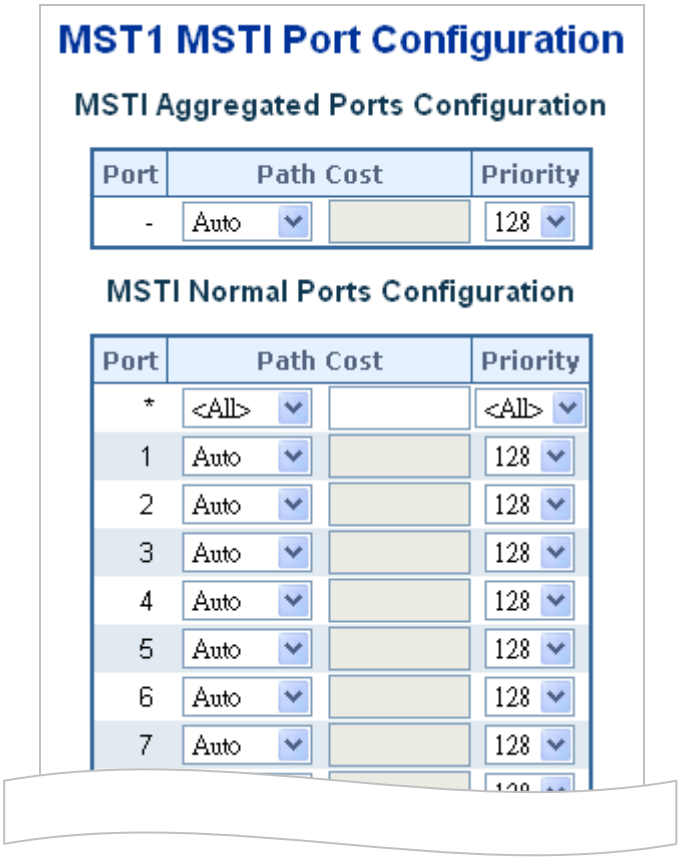


그림 4-7-10 : MST1 MSTI 포트 설정화면

이 페이지에서는 다음과 같음을 나타냅니다.:

MSTx MSTI 포트 설정

목적	설명
• **Port**	해당 STP CIST (및 MSTI) 포트의 스위치 포트 번호입니다.
• **Path Cost**	포트에서 발생하는 경로 비용을 제어합니다. Auto (자동) 설정은 802.1D 권장 값을 사용하여 물리적 링크 속도로 적절하게 경로 비용을 설정합니다. 특정 설정을 사용하여 사용자 정의 값을 입력 할 수 있습니다. 경로 비용은 네트워크의 활성 토폴로지를 설정할 때 사용됩니다. 낮은 경로 비용 포트가 높은 경로 비용 포트를 위해 전달 포트로 선택됩니다. 유효한 값은 1 - 200000000 입니다.
• **Priority**	포트 우선 순위를 제어합니다. 이는 동일한 포트 비용을 갖는 포트의 우선 순위를 제어하는데 사용합니다.

버튼

Get: MSTI 의 MSTx(x=number)를 설정합니다.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.7.8 포트 상태

이 페이지는 현재 선택된 스위치의 포트 물리적 포트에 대한 STP CIST 포트 상태를 표시합니다.

그림 4-7-11 의 STP 포트 상태 화면이 나타납니다.

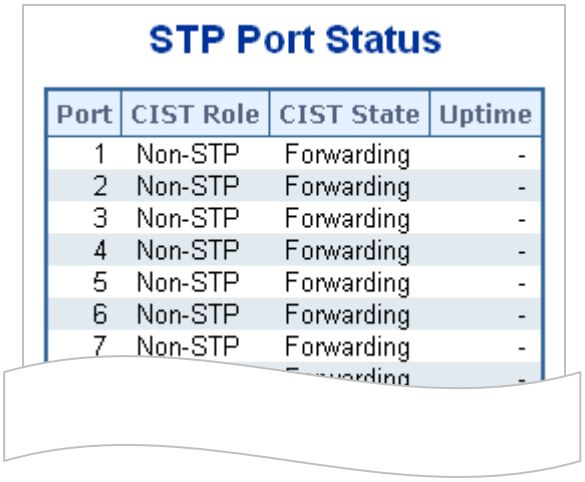


그림 4-7-11: STP Port Status 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	논리적 STP 포트의 스위치 포트 번호입니다.
• **CIST Role**	ICST 포트의 현재 STP 포트 역할. 포트 역할은 다음 값 중 하나 일 수 있습니다.: ■ **AlternatePort** ■ **BackupPort** ■ **RootPort** ■ **DesignatedPort** ■ **Disable**
• **CIST State**	CIST 포트의 현재 STP 포트 상태입니다. 포트 상태는 다음 값 중 하나 일 수 있습니다: ■ **Disabled** ■ **Learning** ■ **Forwarding**
• **Uptime**	브리지 포트가 마지막으로 초기화 된 이후의 시간.

버튼

Refresh: 즉시 페이지를 새로고침합니다.

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다.

4.7.9 포트 통계

STP 포트 통계의 포트 수를 스위치에서 선택된 현재 물리적인 포트들을 나타냅니다. STP 포트 통계는 그림 4-7-12 에 나타냅니다.

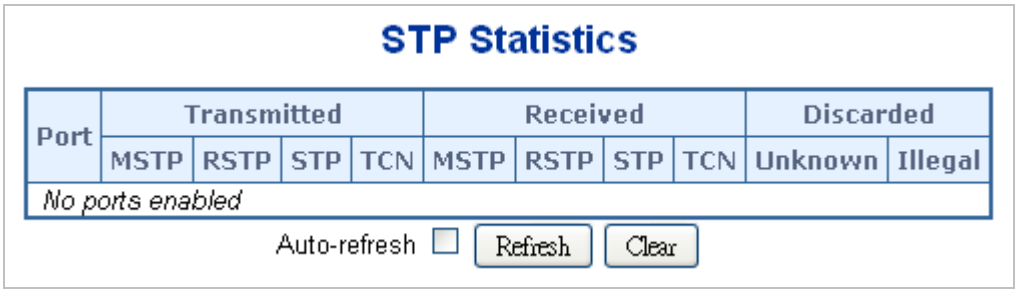


그림 4-7-12: STP 통계 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	논리적 RSTP 포트의 스위치 포트 번호입니다.
• **MSTP**	포트에서 수신 / 전송 된 MSTP 구성 BPDU 의 수.
• **RSTP**	포트에서 수신 / 전송 된 RSTP 구성 BPDU 의 수.
• **STP**	포트에서 수신 / 전송 된 레거시 STP 구성 BPDU 의 수.
• **TCN**	포트에서 수신 / 전송 된 (기존) 토폴로지 변경 알림 BPDU 수입니다.
• **Discarded Unknown**	포트에서 알 수없는 스패닝 트리 BPDU 의 수 (및 버려진 수)입니다.
• **Discarded Illegal**	포트에서 수신 된 (및 삭제 된) 불법 스패닝 트리 BPDU 수입니다.

버튼

Auto-refresh : 모든 정보를 3 초주기로 새로고칩니다.

Refresh : 즉시 페이지를 새로고침합니다.

Clear : 모든 포트의 카운터를 초기화합니다.

4.8 Multicast

4.8.1 IGMP Snooping

IGMP (Internet Group Management Protocol)를 사용하면 호스트와 라우터가 멀티 캐스트 그룹 구성원에 대한 정보를 공유 할 수 있습니다. IGMP 스누핑은 IGMP 메시지 교환을 모니터링하고 기능 처리를 위해 CPU 에 복사하는 스위치 기능입니다. IGMP 스누핑의 전반적인 목적은 멀티 캐스트 프레임의 멀티 캐스트 그룹 구성원 인 포트로의 전달을 제한하는 것입니다..

Internet Group Management Protocol (IGMP)관한 Snooping

멀티 캐스트 전송을 수신하려는 컴퓨터 및 네트워크 장치는 주변 라우터에 멀티 캐스트 그룹의 구성원이 될 것임을 알릴 필요가 있습니다. IGMP (Internet Group Management Protocol)는 이 정보를 전달하는 데 사용됩니다. 또한 IGMP 는 더 이상 활성화되지 않은 구성원에 대한 멀티 캐스트 그룹을 주기적으로 확인하는 데 사용됩니다. 서브 네트워크에 하나 이상의 멀티 캐스트 라우터가있는 경우 하나의 라우터가 '쿼리 됨'으로 선택됩니다. 그런 다음이 라우터는 활성 구성원이있는 멀티 캐스트 그룹의 구성원을 추적합니다. IGMP 로부터 수신 된 정보는 멀티 캐스트 패킷이 주어진 서브 네트워크로 포워딩되어야하는지 여부를 결정하는데 사용됩니다. 라우터는 IGMP 를 사용하여 주어진 서브넷 작업에 적어도 하나의 멀티 캐스트 그룹 구성원이 있는지 확인할 수 있습니다. 하위 네트워크에 구성원이 없으면 패킷은 해당 하위 네트워크로 전달되지 않습니다.

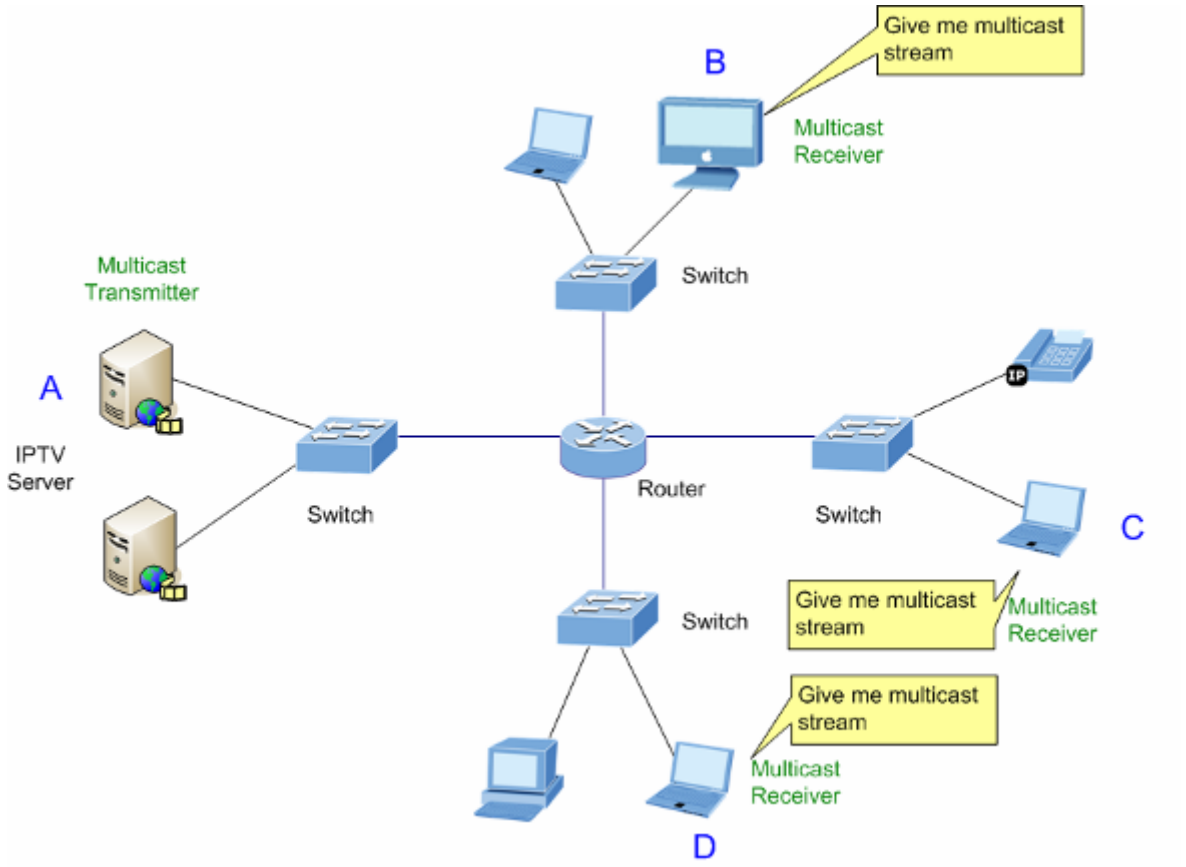


그림 4-8-1: 멀티케스트 서비스

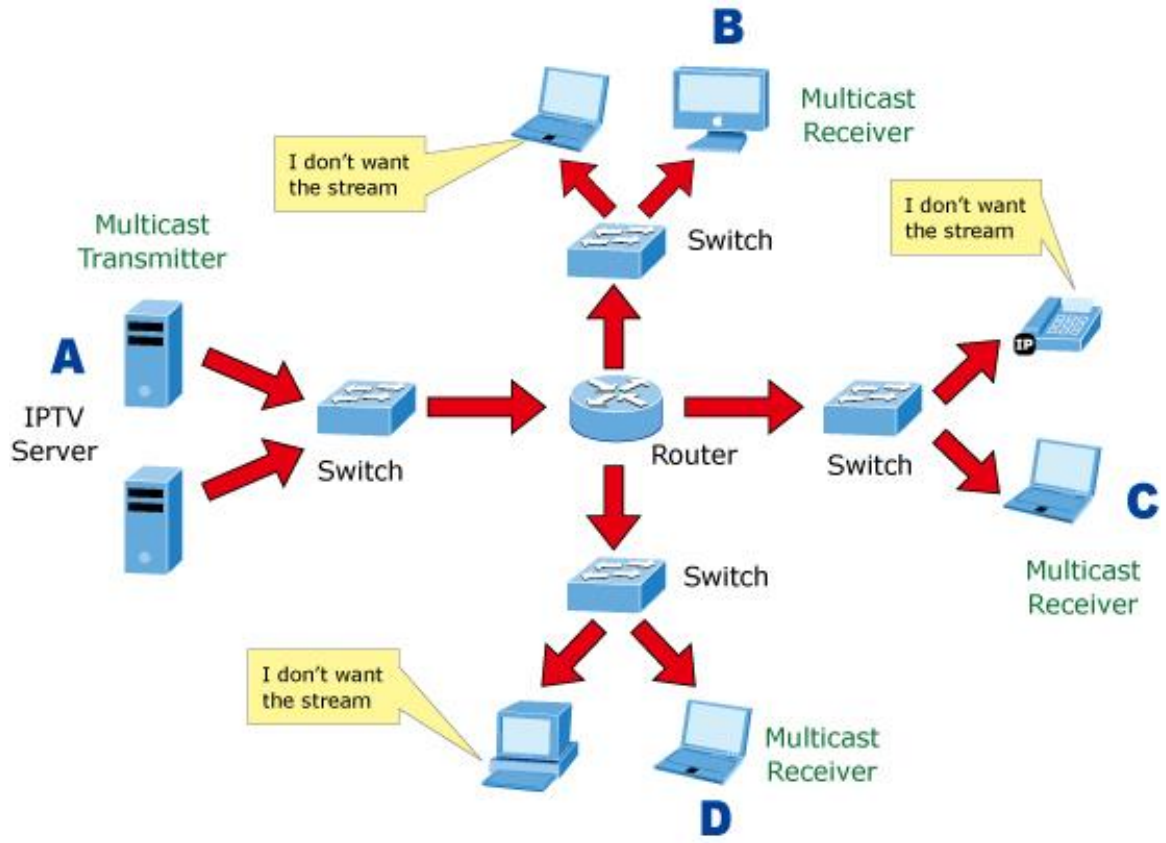


그림 4-8-2: 멀티케스트 플러딩

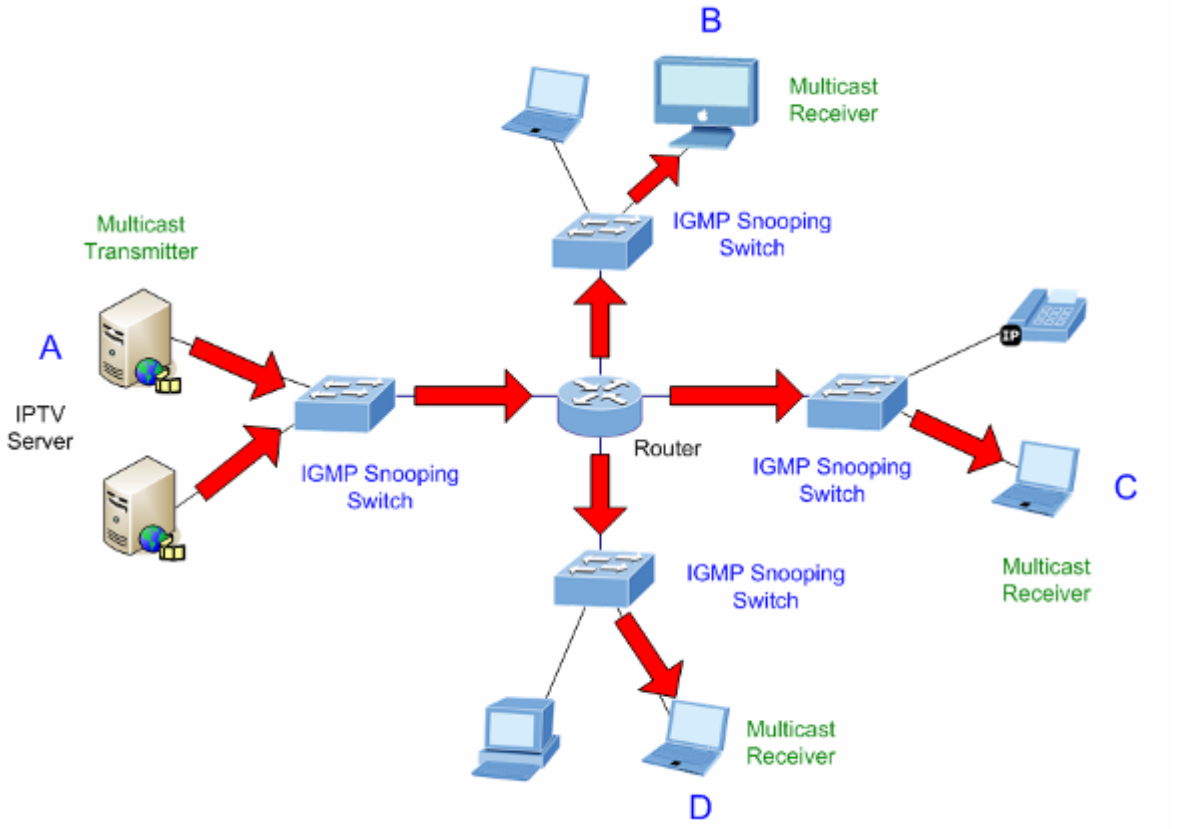


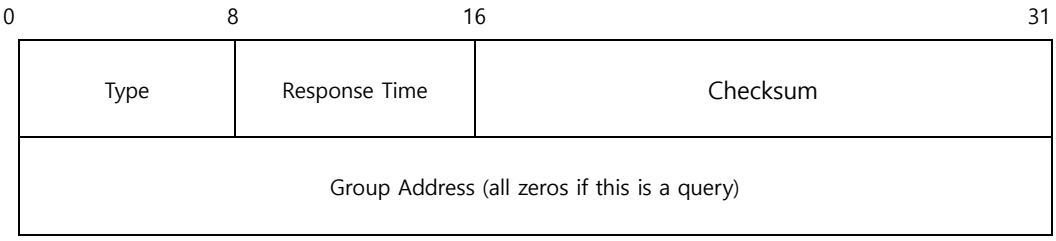
그림 4-8-3: IGMP 멀티케스트 스누핑 스트림 제어

IGMP 버전 1 과 2

멀티 캐스트 그룹을 사용하면 언제든지 회원을 가입하거나 탈퇴 할 수 있습니다. IGMP 는 멀티 캐스트 그룹에 가입하거나 탈퇴 할 때 구성원 및 멀티 캐스트 라우터가 통신하는 방법을 제공합니다. IGMP 버전 1 은 RFC 1112 에 정의되어 있습니다. 패킷 크기는 고정되어 있으며 선택적 데이터는 없습니다. IGMP 패킷의 형식은 다음과 같습니다.:

IGMP 메시지 형태

Octets



IGMP Type 형태 코드는 다음과 같습니다

형태	의미
0x11	멤버쉽 쿼리(만약 그룹주소가 0.0.0.0 일 경우)
0x11	특정 그룹 회원 질의 (그룹 주소가있는 경우)
0x16	**멤버십 보고서 (버전 2)**
0x17	**그룹 탈퇴 (버전 2)**
0x12	**멤버십 보고(버전 1)**

IGMP 패킷을 사용하면 멀티 캐스트 라우터가 해당 서브 네트워크에서 멀티 캐스트 그룹의 구성원을 추적 할 수 있습니다. 다음은 IGMP 를 사용하여 멀티 캐스트 라우터와 멀티 캐스트 그룹 구성원간에 통신되는 내용을 설명합니다.
호스트가 IGMP "보고서"를 보내 그룹에 가입

호스트는 그룹을 떠날 때 보고서를 보내지 않습니다 (버전 1).

호스트는 그룹을 떠날 때 (버전 2) "탈퇴"보고서를 보냅니다.

멀티 캐스트 라우터는 IGMP 쿼리 (모든 호스트 그룹 주소 : 224.0.0.1)를 주기적으로 보내 그룹 구성원이 서브 네트워크에 있는지 확인합니다. 특정 그룹으로부터 응답이 없으면 라우터는 네트워크에 그룹 구성원이 없다고 가정합니다.

쿼리 메시지의 TTL (Time-to-Live) 필드는 쿼리가 다른 하위 네트워크로 전달되지 않도록 1 로 설정됩니다.

IGMP 버전 2 에서는 각 LAN 에 대해 쿼리 된 멀티 캐스트를 선택하는 방법, 명시 적 이탈 메시지 및 특정 그룹에 관련된 쿼리 메시지와 같은 몇 가지 향상된 기능을 소개합니다. 컴퓨터가 멀티 캐스트 그룹에 가입하거나 탈퇴하는 상태는 다음과 같습니다.:

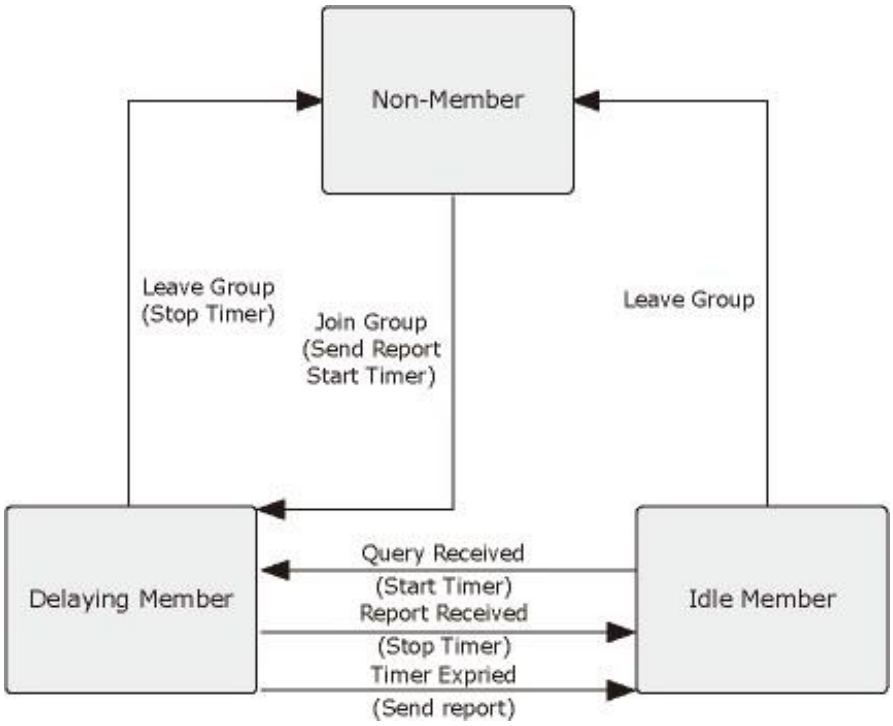


그림 4-8-4: IGMP 전송 상태

■ **IGMP 쿼리어**

라우터 또는 멀티 캐스트 가능 스위치는 주기적으로 호스트에 멀티 캐스트 트래픽을 수신할지 묻습니다. IP 멀티 캐스팅을 수행하는 LAN 에 둘 이상의 라우터 / 스위치가있는 경우, 이들 장치 중 하나는 "쿼리"로 선출되고 그룹 구성원에 대해 LAN 을 쿼리하는 역할을 맡습니다. 그런 다음 서비스 요청을 모든 업스트림 멀티 캐스트 스위치 / 라우터로 전파하여 멀티 캐스트 서비스를 계속 수신하는지 확인합니다.

Note

멀티 캐스트 라우터는이 정보를 DVMRP 또는 PIM 과 같은 멀티 캐스트 라우팅 프로토콜과 함께 사용하여 인터넷에서 IP 멀티 캐스팅을 지원합니다.

4.8.2 개요 표

이 페이지는 IPMC 프로파일 관련 구성을 제공합니다. IPMC 프로필은 IP 멀티 캐스트 스트림에 대한 액세스 제어를 배포하는 데 사용됩니다. 각 프로파일에 대해 최대 128 개의 대응 규칙을 갖는 최대 64 개의 프로파일을 작성할 수 있습니다. 그림 4-8-5 의 프로필 표 화면이 나타납니다.

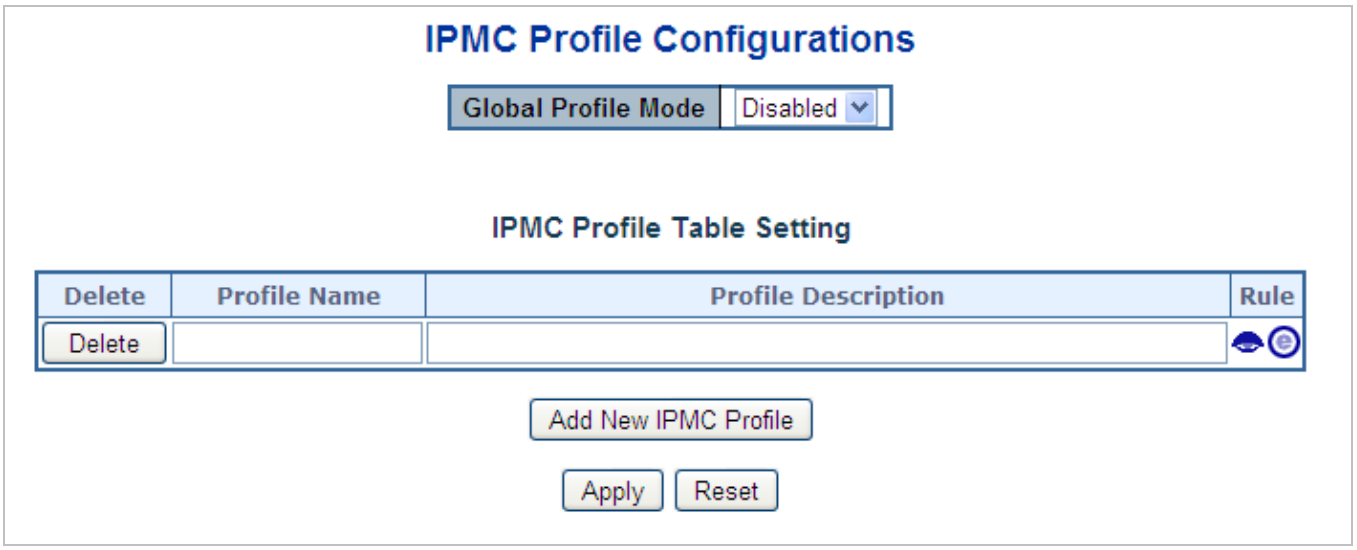


그림 4-8-5: IPMC 개요 설정 페이지

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Global Profile Mode**	글로벌 IPMC 프로필을 활성화 / 비활성화합니다. 글로벌 프로필 모드가 활성화 된 경우에만 프로필 설정을 기반으로 필터링이 시작됩니다.
• **Delete**	항목을 삭제하려면 클릭합니다. 지정된 항목음 다음 저장 중에 삭제됩니다.
• **Profile Name**	프로필 테이블을 인덱싱하는 데 사용되는 이름입니다. 각 항목에는 최대 16 자의 영문자와 숫자로 구성된 고유 한 이름이 있습니다. 하나 이상의 알파벳이 있어야합니다.
• **Profile Description**	프로필에 대한 추가 설명으로, 최대 64 자의 영문자와 숫자로 구성됩니다.
• **Rule**	프로파일이 작성되면 편집 버튼을 클릭하여 지정된 프로파일의 규칙 설정 페이지로 들어갑니다. 보기 버튼을 클릭하면 지정된 프로필에 대한 요약이 표시됩니다. 다음 버튼을 사용하여 지정된 프로필의 규칙을 관리하거나 검사할 수 있습니다. : 지정된 프로필과 연관된 규칙을 나열하십시오. :지정된 프로필과 관련된 규칙을 조정합니다.

버튼

Add New IPMC Profile: 새로운 IPMC 프로파일을 추가하려면 클릭하십시오. 이름을 지정하고 새 항목을 구성하십시오. "저장"을 클릭하십시오.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.8.3 주소 엔트리

이 페이지는 IPMC 프로필에 사용되는 주소 범위 설정을 제공합니다. 주소 항목은 IPMC 프로필과 관련된 주소 범위를 지정하는 데 사용됩니다. 시스템에 최대 128 개의 주소 항목을 작성할 수 있습니다. 그림 4-8-6 의 프로파일 테이블 화면이 나타납니다.

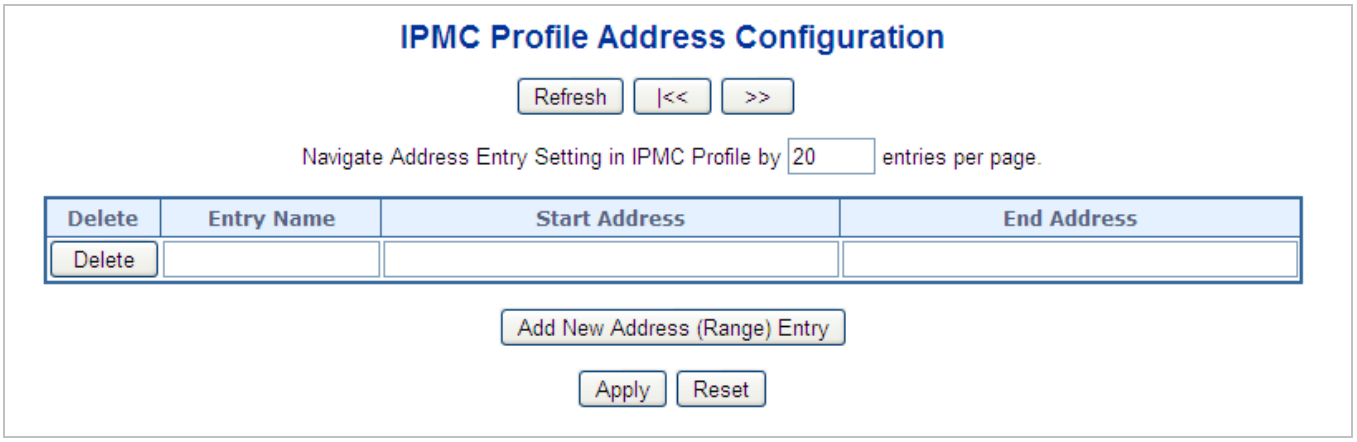


그림 4-8-6: IPMC 프로필 주소 구성 페이지

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 지정된 항목은 다음 저장 중에 삭제됩니다.
• **Entry Name**	주소 입력 테이블 색인에 사용되는 이름입니다. 각 항목에는 최대 16 자의 영문자와 숫자로 구성된 고유 한 이름이 있습니다. 하나 이상의 알파벳이 있어야합니다.
• **Start Address**	주소 범위로 사용될 시작 IPv4 / IPv6 멀티 캐스트 그룹 주소입니다.
• **End Address**	주소 범위로 사용될 끝 IPv4 / IPv6 멀티 캐스트 그룹 주소입니다.

버튼

Add New Address (Range) Entry: 새 주소 범위를 추가하려면 클릭하십시오. 이름을 지정하고 주소를 구성하십시오. "저장"을 클릭하십시오.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

Refresh: 입력 필드에서 표시된 표를 새로 고칩니다.

|<<: IPMC 프로필 주소 구성의 첫 번째 항목부터 시작하여 표를 업데이트합니다.

>>: 현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 업데이트합니다.

4.8.4 IGMP 스누핑 설정

이 페이지는 IGMP 스누핑 관련 구성을 제공합니다. 그림 4-8-7 의 IGMP Snooping 설정 화면이 나타납니다..

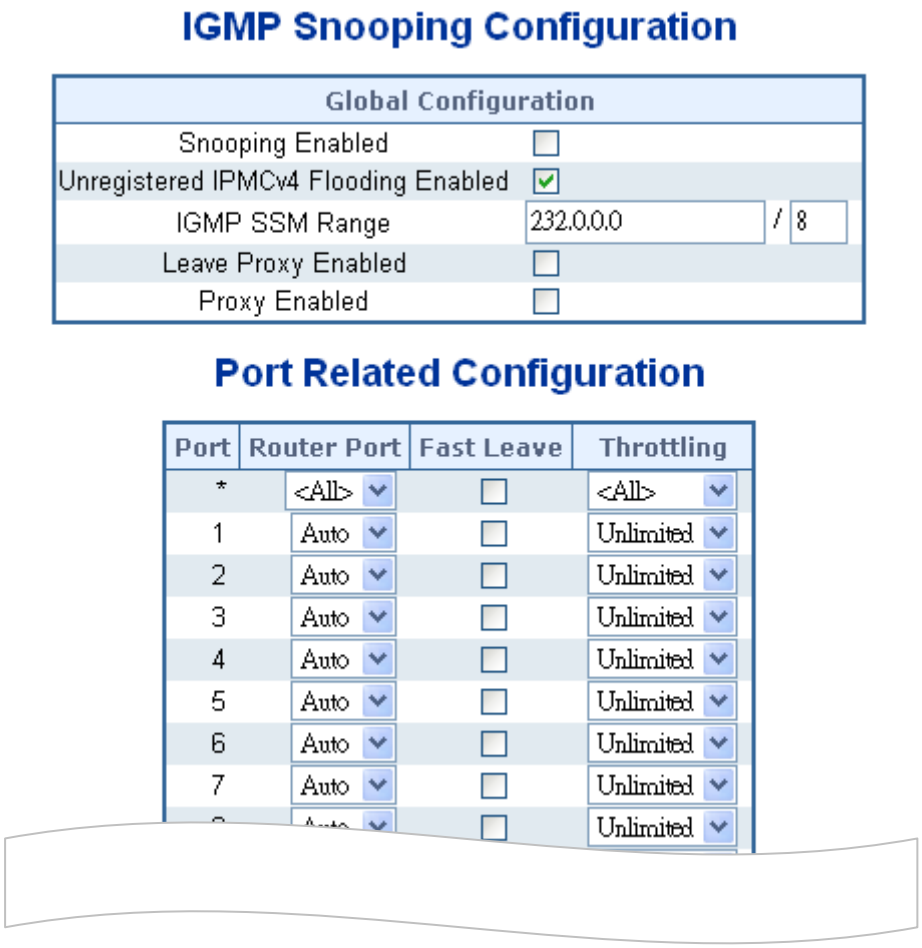


그림 4-8-7: IGMP 스누핑 설정 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Snooping Enabled**	전역 IGMP 스누핑을 활성화합니다.
• **Unregistered IPMCv4 Flooding Enabled**	등록되지 않은 IPMCv4 트래픽 플러딩을 활성화합니다. IGMP 스누핑이 활성화 된 경우에만 플러딩 제어가 적용됩니다. IGMP 스누핑을 사용하지 않으면이 설정에도 불구하고 등록되지 않은

	IPMCv4 트래픽 플러딩이 항상 활성화됩니다.
• **IGMP SSM Range**	SSM (Source-Specific Multicast) Range 를 사용하면 SSM 인식 호스트와 라우터가 주소 범위의 그룹에 대해 SSM 서비스 모델을 실행할 수 있습니다.
• **Leave Proxy Enable**	IGMP Leave Proxy 를 활성화합니다. 이 기능은 불필요한 탈퇴 메시지를 라우터 측으로 전달하는 것을 피하기 위해 사용할 수 있습니다.
• **Proxy Enable**	IGMP 프록시를 활성화합니다. 이 기능은 라우터 측에 불필요한 가입 및 탈퇴 메시지 전달을 방지하는 데 사용할 수 있습니다.
• **Router Port**	IGMP 라우터 포트로 작동하는 포트를 지정하십시오. 라우터 포트는 이더넷 스위치의 레이어 3 멀티 캐스트 장치 또는 IGMP 쿼리 작성기로 연결되는 포트입니다. 스위치는 IGMP 조인을 전달하거나 패킷을 IGMP 라우터 포트에 남겨 둡니다. ■ **자동:** 포트가 IGMP 쿼리 패킷을 수신하는 경우 관리되는 스위치가 자동으로 해당 포트를 IGMP 라우터 포트로 사용하려면 "자동"을 선택합니다. ■ 수정: 관리형 스위치는 항상 지정된 포트를 IGMP 라우터 포트로 사용합니다. 포트에 멀티 캐스트 프로토콜을 적용한 IGMP 멀티 캐스트 서버 또는 IP 카메라를 연결할 때이 모드를 사용하십시오. ■ **없음:** 관리 형 스위치는 지정된 포트를 IGMP 라우터 포트로 사용하지 않습니다. 관리 형 스위치는이 포트에 연결된 IGMP 라우터의 기록을 보관하지 않습니다. 다른 IGMP 멀티 캐스트 서버를 비 쿼리 관리 대상 스위치에 직접 연결하고 IGMP 쿼리 프로그램에 연결된 포트를 통해 멀티 캐스트 스트림이 업 링크로 플러딩되지 않도록하려면이 모드를 사용하십시오.
• **Fast Leave**	포트를 빠르게 빠져 나가십시오
• **Throtting**	스위치 포트가 속할 수있는 멀티 캐스트 그룹 수를 제한합니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.8.5 IGMP Snooping VLAN 구성

각 페이지는 VLAN 테이블에서 최대 99 개의 항목을 표시하며 기본값은 20 이고 "페이지 당 항목 수"입력 필드를 통해 선택됩니다. 처음 방문했을 때, 웹 페이지는 VLAN 표의 처음부터 처음 20 개의 항목을 표시합니다. 가장 먼저 표시되는 VLAN ID 는 VLAN 테이블에 있습니다.

"VLAN"입력 필드는 사용자가 VLAN 테이블에서 시작점을 선택할 수 있도록합니다. 그림 4-8-8 의 IGMP 스누핑 VLAN 구성 화면이 나타납니다.

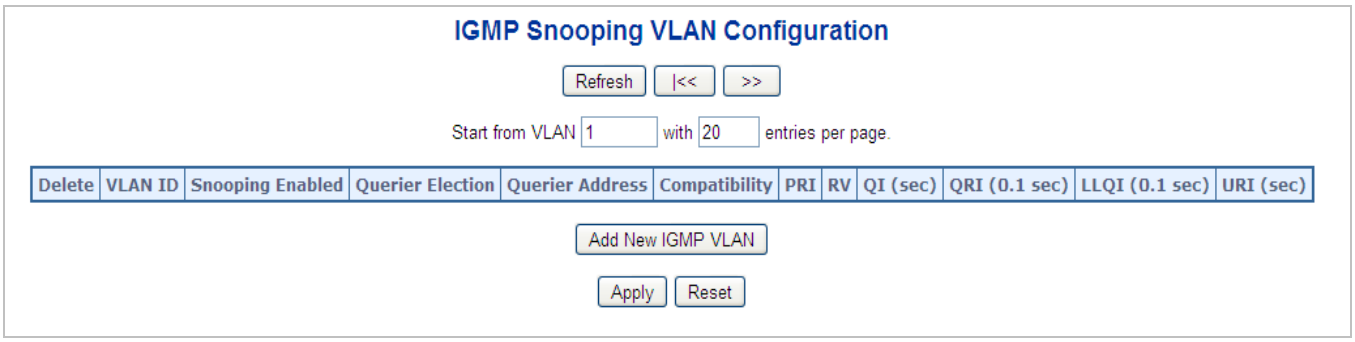


그림 4-8-8: IGMP Snooping VLAN 구성화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 지정된 항목은 다음 저장 중에 삭제됩니다.
• **VLAN ID**	항목의 VLAN ID 입니다.
• **IGMP Snooping Enable**	각- VLAN, IGMP 스누핑을 활성화합니다. 최대 32 개의 VLAN 만 선택할 수 있습니다.
• **Querier Election**	VLAN 에서 IGMP 쿼리 발송기 선택을 사용하도록 설정합니다. IGMP 비 쿼리 발송자로 작동하려면 비활성화합니다.
• **Querier Address**	IGMPQuerier 선택을 위해 IP 헤더에 사용되는 소스 주소로 IPv4 주소를 정의합니다.. ■ Querier 주소가 설정되어 있지 않으면 시스템은이 VLAN 과 연관된 IP 인터페이스의 IPv4 관리 주소를 사용합니다.. ■ IPv4 관리 주소가 설정되어 있지 않으면 시스템은 사용 가능한 첫 번째 IPv4 관리 주소를 사용합니다. 그렇지 않으면 시스템은 미리 정의 된 값을 사용합니다. 기본적으로이 값은 192.0.2.1 입니다.
• **Compatibility**	호환성은 호스트 및 라우터가 네트워크 내의 호스트 및 라우터에서 작동하는 IGMP 버전에 따라 적절한 조치를 취함으로써 유지됩니다. 허용된 선택안은 **IGMP-Auto**, **Forced IGMPv1**, **Forced IGMPv2**, **Forced IGMPv3**. **기본 호환성값은 IGMP-Auto**.입니다.
• **PRI**	인터페이스의 우선 순위. 시스템에서 생성 한 IGMP 제어 프레임 우선

	순위를 나타냅니다. 이 값을 사용하여 서로 다른 트래픽 클래스의 우선 순위를 지정할 수 있습니다. 허용되는 범위는 0 (최선의 노력)에서 7 (가장 높음)이며, 기본 인터페이스 우선 순위 값은 0 입니다
• **RV**	강선성(RV)을 사용하면 네트워크에서 예상되는 패킷 손실을 조정할 수 있습니다. 허용 범위는 1 ~ 255 이며 기본 견고성 변수 값은 2 입니다.
• **QI**	Query Interval 은 Querier 가 보낸 보통 쿼리간의 간격입니다. 허용되는 범위는 1 - 31744 초이며, 기본 쿼리 간격은 125 초입니다.
• **QRI**	정기적 인 일반 쿼리에 삽입 된 Max Resp Code 를 계산하는 데 사용 된 Max Response Time. 허용되는 범위는 0 에서 31744 초까지이며 기본 쿼리 응답 간격은 10 분의 1 초 (10 초) 단위로 100 입니다.
• **LLQI (LMQI for IGMP)**	마지막 구성원 쿼리 시간은 마지막 구성원 쿼리 간격으로 나타내는 시간 값이며 마지막 구성원 쿼리 횟수를 곱한 값입니다. 허용되는 범위는 0 에서 31744 초이며, 기본 구성원 쿼리 간격은 10 분의 1 초 (10 초)입니다.
• **URI**	Unsolicited Report Interval 은 호스트의 그룹 구성원 초기 보고서 반복 간격입니다. 허용되는 범위는 0 ~ 31744 초이며, 기본 원치 않는 보고서 간격은 1 초입니다.

버튼

Refresh: "VLAN"입력 필드에서 시작하여 표시된 표를 새로 고칩니다.

<<: 가장 낮은 VLAN ID 를 가진 항목 인 VLAN 테이블의 첫 번째 항목부터 시작하여 표를 업데이트합니다.

>>: 현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 업데이트합니다.

Add New IGMP VLAN:새 IGMP VLAN 을 추가하려면 클릭하십시오. VID 를 지정하고 새 항목을 구성 후 ."저장"을 클릭하십시오. 특정 VLAN 이 생성 된 후 특정 IGMP VLAN 이 작동하기 시작합니다.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.8.6 IGMP Snooping Port Group Filtering

특정 스위치 응용 프로그램에서 관리자는 최종 사용자가 사용할 수있는 멀티 캐스트 서비스를 제어하려고 할 수 있습니다. 예를 들어, 특정 가입 계획에 기반한 IP / TV 서비스. IGMP 필터링 기능은 스위치 포트에서 지정된 멀티 캐스트 서비스에 대한 액세스를 제한함으로써이 요구 사항을 충족하며 IGMP 스로틀은 포트가 결합 할 수있는 동시 멀티 캐스트 그룹 수를 제한합니다.

IGMP 필터링을 사용하면 포트에서 허용 또는 거부되는 멀티 캐스트 그룹을 지정하는 스위치 포트에 프로필을 할당 할 수 있습니다. IGMP 필터 프로필에는 하나 이상의 멀티 캐스트 주소 또는 범위가 포함될 수 있습니다. 하나의 프로파일에만 포트에 할당 할 수 있습니다. 활성화 된 경우 포트에서 수신 한 IGMP 조인 보고서가 필터 프로필과 비교됩니다. 요청 된 멀티 캐스트 그룹이 허용되면 IGMP 참가 보고서가 정상적으로 전달됩니다. 요청 된 멀티 캐스트 그룹이 거부되면 IGMP 참가 보고서가 삭제됩니다.

IGMP 스로틀은 포트가 동시에 참여할 수있는 멀티 캐스트 그룹의 최대 수를 설정합니다. 한 포트에서 최대 그룹 수에 도달하면 스위치는 다음 두 가지 작업 중 하나를 수행 할 수 있습니다. "거부"또는 "바꾸기". 작업이 거부로 설정된 경우 새 IGMP 참가 보고서가 삭제됩니다. 동작이 바꾸기로 설정되면 스위치는 기존 그룹을 임의로 제거하고이를 새 멀티 캐스트 그룹으로 바꿉니다. 그림 4-8-9 의 IGMP 스누핑 포트 그룹 필터링 구성 화면이 나타납니다..

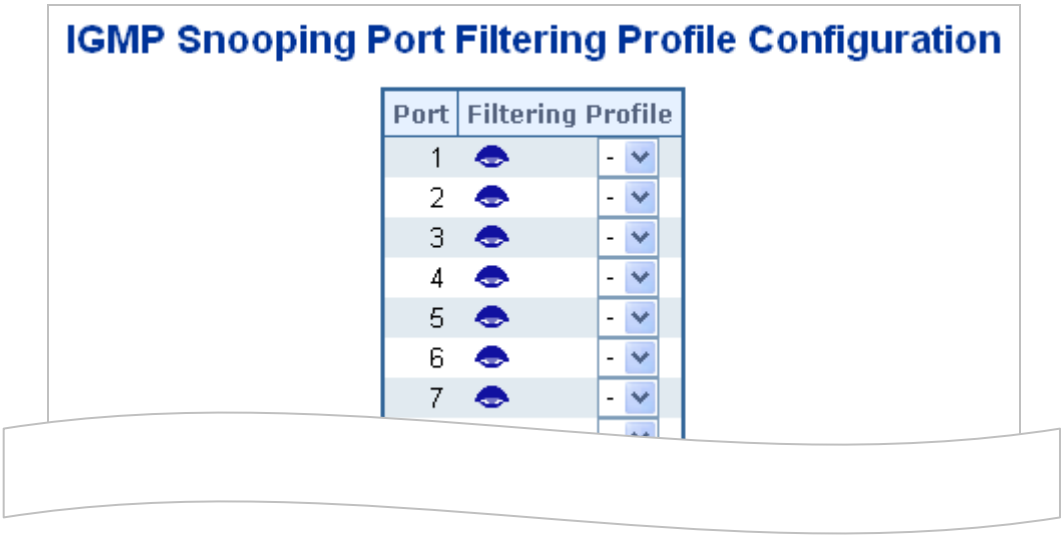


그림 4-8-9: IGMP Snooping Port Filtering Profile 구성 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	설정에 대한 논리 포트 입니다.
• **Filtering Profile**	특정 포트에 대한 필터링 조건으로 IPMC 프로파일을 선택하십시오. 보기 버튼을 클릭하면 지정된 프로필에 대한 요약이 표시됩니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.8.7 IGMP Snooping Status

이 페이지는 IGMP 스누핑 상태를 제공합니다. 그림 4-8-10 의 IGMP Snooping Status 화면이 나타납니다.

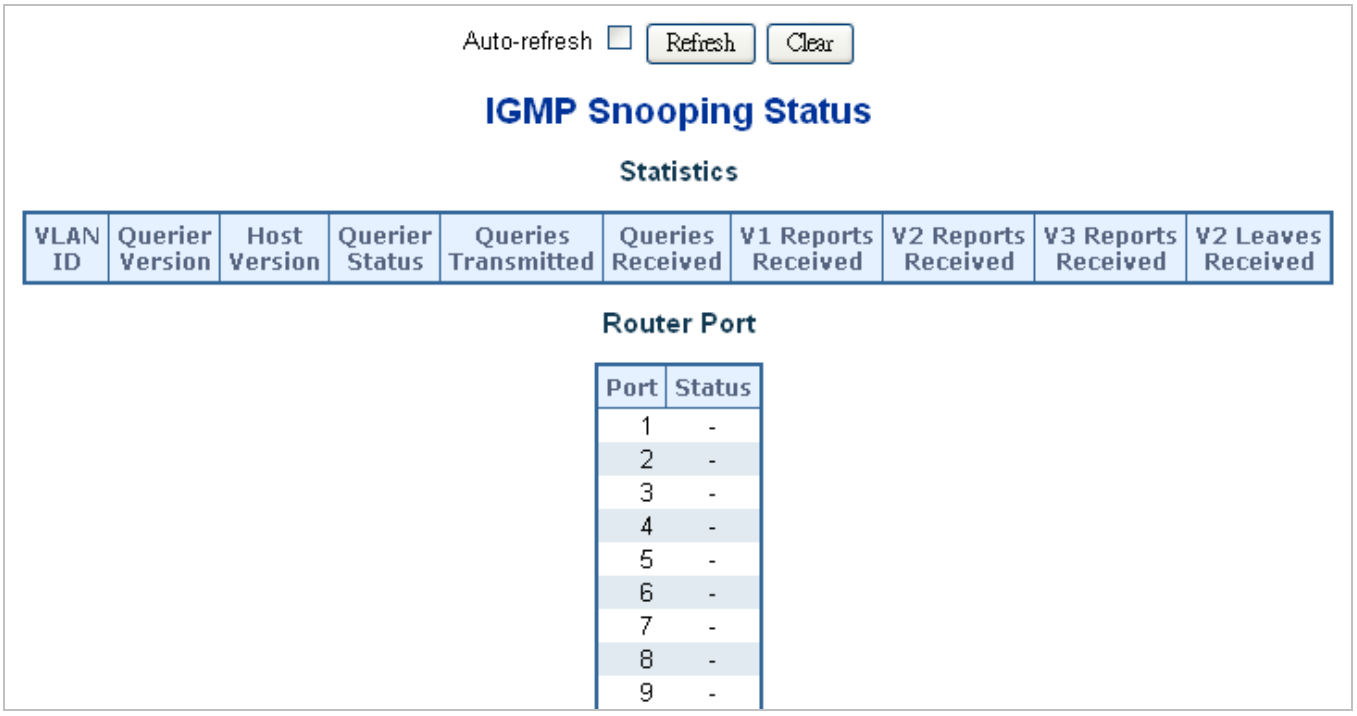


그림 4-8-10: IGMP Snooping Status 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **VLAN ID**	항목의 VLAN ID 입니다.
• **Querier Version**	현재 작동하는 쿼리어의 버전입니다.
• **Host Version**	현재 작업에 호스트 버전입니다.
• **Querier Status**	활성 또는 유휴임을 표시하십시오.
• **Querier Transmitted**	전송 쿼리어의 수
• **Querier Received**	수신 쿼리어의 수
• **V1 Reports Received**	수신 V1 의 보고된 수
• **V2 Reports Received**	수신 V2 의 보고된 수
• **V3 Reports Received**	수신 V3 의 보고된 수
• **V2 Leave Received**	수신된 V2 의 떠나간 수
• **Router Port**	어떤 포트가 라우터 포트로 작동하는지 표시합니다. 라우터 포트는 이더넷 스위치의 레이어 3 멀티 캐스트 장치 또는 IGMP 쿼리 작성기로 연결되는 포트입니다. Static 은 특정 포트가 라우터 포트로 구성되었음을 나타냅니다. Dynamic 은 특정 포트가 라우터 포트로 학습되었음을 나타냅니다. 둘 다 특정 포트가 구성되었거나 라우터 포트로 습득되었음을 나타냅니다.
• **Port**	스위치 포트 번호
• **Status**	특정 포트가 라우터 포트인지 여부를 나타냅니다.

버튼

Refresh: 즉시 페이지를 새로고침합니다.

Clear: 모든 통계 카운터 항목을 지웁니다.

Auto-refresh : 자동적으로 3 초마다 새로고침을 발생합니다.

4.8.8 IGMP 그룹 정보

이 페이지에는 IGMP 그룹 표의 항목이 표시됩니다. IGMP 그룹 표는 먼저 VLAN ID 별로 정렬 된 다음 그룹별로 정렬됩니다. 페이지는 IGMP 그룹 테이블에서 최대 99 개의 항목을 표시하며, 기본값은 20 이고 "페이지 당 항목 수"입력 필드를 통해 선택됩니다. 처음 방문했을 때, 웹 페이지는 IGMP 그룹 표의 처음부터 처음 20 개의 항목을 표시합니다. "Start from VLAN (VLAN 에서 시작)"및 "group (그룹)"입력 필드를 통해 사용자는 IGMP Group Table (IGMP 그룹 테이블)에서 시작점을 선택할 수 있습니다. IGMP 그룹 그림 4-8-11 의 정보 화면이 나타납니다..

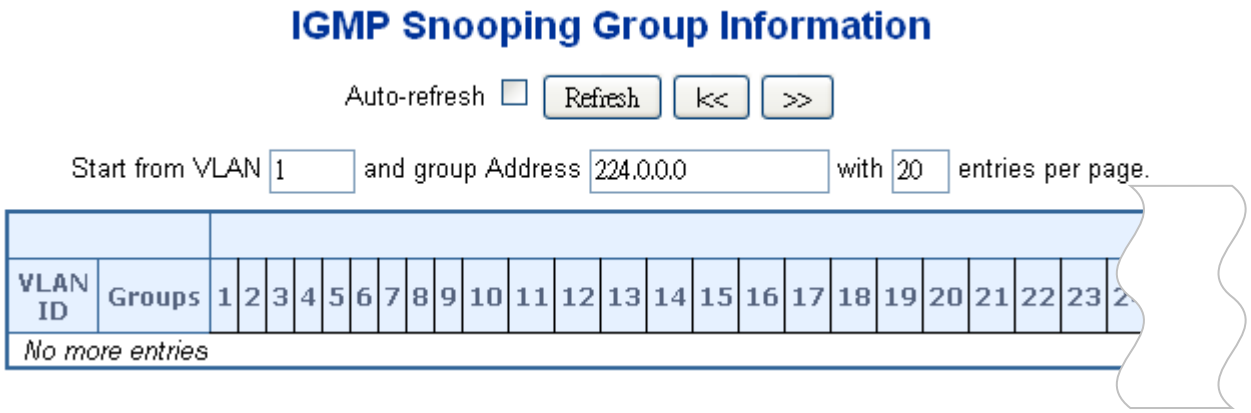


그림 4-8-9: IGMP Snooping 그룹 정보 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **VLAN ID**	그룹의 VLAN ID 입니다.
• **Groups**	표시된 그룹의 그룹 주소.
• **Port Members**	그룹에 속한 포트입니다

버튼

Auto-refresh : 자동으로 3 초마다 새로고침을 합니다..

Refresh: 입력된 각 항목에 대하여 새로고침을 합니다.

<<: IGMP Group Table 의 첫번째 구성화면으로 업데이트합니다.

>>: 가장 마지막의 구성화면을 현재 업데이트합니다.

4.8.9 IGMPv3 안내

이 페이지에는 IGMP SSM 정보 표의 항목이 표시됩니다. IGMP SSM 정보 표는 먼저 VLAN ID 별로 정렬 된 다음 그룹별로 정렬 된 다음 포트 번호별로 정렬됩니다. 동일한 그룹에 속한 차이 원본 주소는 단일 항목으로 처리됩니다.
각 페이지는 IGMP SSM (Source Specific Multicast) 정보 테이블에서 최대 99 개의 항목을 표시하며, 기본값은 20 이고 "페이지 당 항목"입력 필드를 통해 선택됩니다. 처음 방문했을 때, 웹 페이지는 IGMP SSM 정보 표의 처음부터 처음 20 개의 항목을 표시합니다.
"Start from VLAN (VLAN 에서 시작)"및 "Group (그룹)"입력 필드를 통해 사용자는 IGMP SSM 정보 테이블에서 시작점을 선택할 수 있습니다. 그림 4-8-12 의 IGMPv3 Information 화면이 나타납니다.

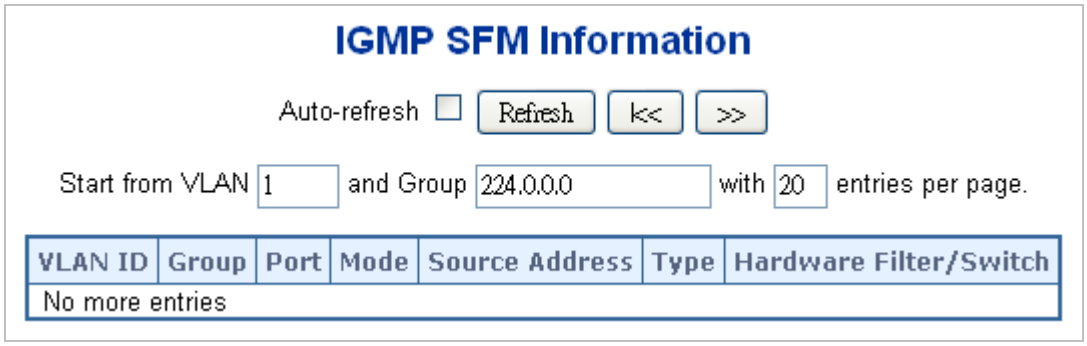


그림 4-8-12: IGMP SSM Information 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **VLAN ID**	그룹의 VLAN ID 입니다.
• **Group**	표시된 그룹의 그룹 주소.
• **Port**	스위치 포트 번호.
• **Mode**	(VLAN ID, 포트 번호, 그룹 주소) 단위로 유지 관리되는 필터링 모드를 나타냅니다. Include 또는 Exclude 중 하나 일 수 있습니다.
• **Source Address**	소스의 IP 주소. 현재 시스템은 필터링 할 IP 원본 주소의 총 수를 128 개로 제한합니다.
• **Type**	유형을 나타냅니다. 허용 또는 거부 중 하나 일 수 있습니다.
• **Hardware Filter/Switch**	소스 IPv4 주소의 특정 그룹 주소를 대상으로하는 데이터 플레인이 칩별로 처리 될 수 있는지 여부를 나타냅니다.

버튼

Auto-refresh : 정기적으로 페이지 자동 새로 고침을 사용하려면이 상자를 선택하십시오.

Refresh : 즉시 페이지를 새로고침합니다.

<< : IGMP 그룹 테이블의 첫 번째 항목부터 표를 업데이트합니다.

>> : 현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 업데이트합니다.

4.8.10 MLD Snooping 구성

이 페이지는 MLD 스누핑 관련 구성을 제공합니다. 그림 4-8-13 의 MLD 스누핑 구성 화면이 나타납니다..

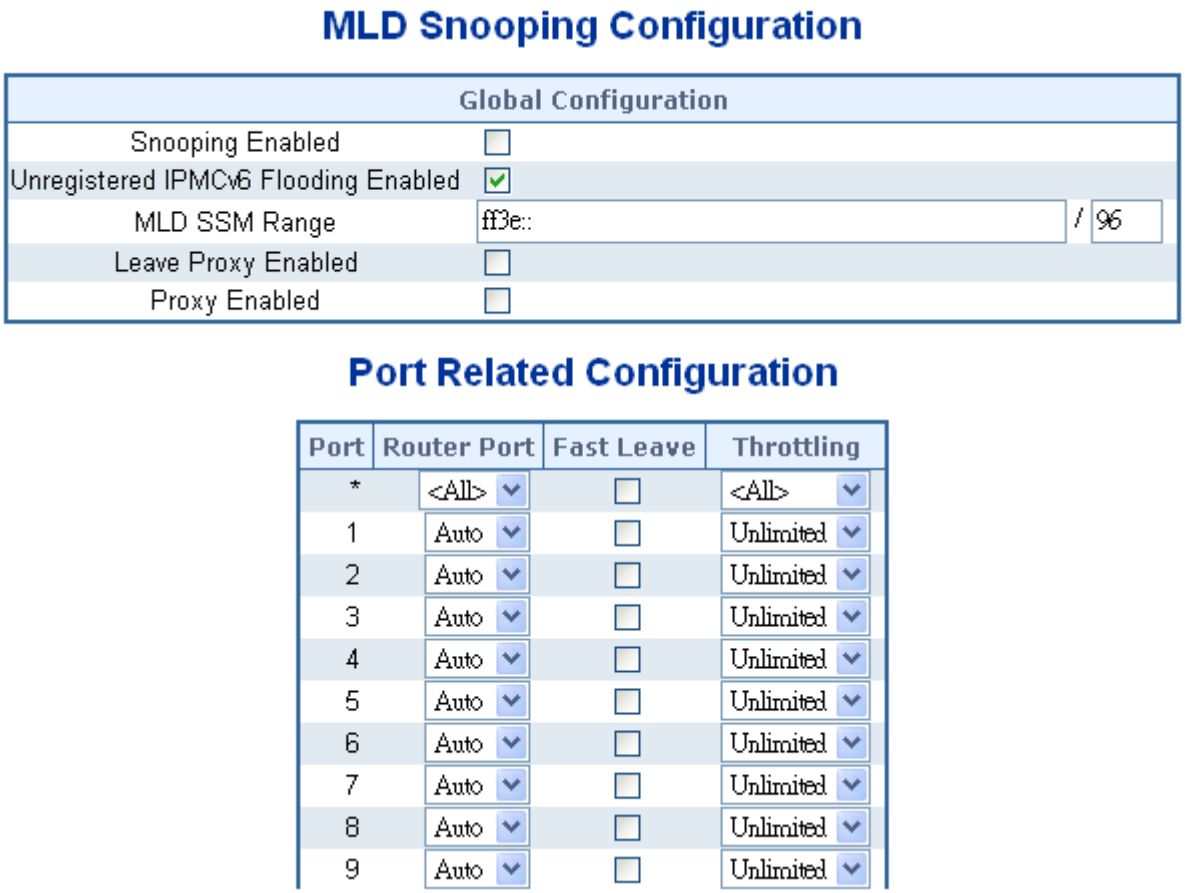


그림 4-8-13: MLD Snooping 설정 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Snooping Enabled**	Global MLD Snooping 을 활성화 합니다..
• **Unregistered IPMCv6 Flooding enabled**	등록되지 않은 IPMCv6 트래픽 플러딩을 사용합니다. MLD 스누핑이 활성화 된 경우에만 플러딩 제어가 적용됩니다. MLD Snooping 이 비활성화되면 미등록 IPMCv6 트래픽 플러딩은이 설정에도 불구하고 항상 활성화됩니다.
• **MLD SSM Range**	SSM (Source-Specific Multicast) Range 를 사용하면 SSM 인식 호스트와 라우터가 주소 범위의 그룹에 대해 SSM 서비스 모델을 실행할 수 있습니다.
• **Leave Proxy Enable**	MLD Leave Proxy 를 활성화합니다. 이 기능은 불필요한 탈퇴 메시지를 라우터 측으로 전달하는 것을 피하기 위해 사용할 수 있습니다.
• **Proxy Enable**	IGMP 프록시를 활성화합니다. 이 기능은 라우터 측에 불필요한 가입 및 탈퇴 메시지 전달을 방지하는 데 사용할 수 있습니다.
• **Router Port**	IGMP 라우터 포트로 작동하는 포트를 지정하십시오. 라우터 포트는 이더넷

	스위치의 레이어 3 멀티 캐스트 장치 또는 IGMP 쿼리 작성기로 연결되는 포트입니다. 스위치는 IGMP 조인을 전달하거나 패킷을 IGMP 라우터 포트에 남겨 둡니다. ■ **Auto:** 포트가 IGMP 쿼리 패킷을 수신하는 경우 관리되는 스위치가 자동으로 해당 포트를 IGMP 라우터 포트로 사용하려면 "자동"을 선택합니다.. ■ **Fix**: 관리형 스위치는 항상 지정된 포트를 IGMP 라우터 포트로 사용합니다. 포트에 멀티 캐스트 프로토콜을 적용한 IGMP 멀티 캐스트 서버 또는 IP 카메라를 연결할 때이 모드를 사용하십시오.. ■ **None:** 관리 형 스위치는 지정된 포트를 IGMP 라우터 포트로 사용하지 않습니다. 관리 형 스위치는이 포트에 연결된 IGMP 라우터의 기록을 보관하지 않습니다. 다른 IGMP 멀티 캐스트 서버를 비 쿼리 관리 대상 스위치에 직접 연결하고 IGMP 쿼리 프로그램에 연결된 포트를 통해 멀티 캐스트 스트림이 업 링크로 플러딩되지 않도록하려면이 모드를 사용하십시오.
• **Fast Leave**	포트를 빠르게 나가도록 활성화합니다.
• **Throtting**	스위치 포트가 속할 수있는 멀티 캐스트 그룹 수를 제한합니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.8.11 MLD Snooping VLAN 설정

각 페이지는 VLAN 테이블에서 최대 99 개의 항목을 표시하며 기본값은 20 이고 "페이지 당 항목 수"입력 필드를 통해 선택됩니다. 처음 방문했을 때, 웹 페이지는 VLAN 표의 처음부터 처음 20 개의 항목을 표시합니다. 가장 먼저 표시되는 VLAN ID 는 VLAN 테이블에 있습니다.

"VLAN"입력 필드는 사용자가 VLAN 테이블에서 시작점을 선택할 수 있도록합니다. 그림 4-8-14 의 MLD Snooping VLAN 설정화면이 나타납니다.

그림 4-8-14: IGMP Snooping VLAN 설정화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 지정된 항목은 다음 저장 중에 삭제됩니다.
• **VLAN ID**	항목의 VLAN ID 입니다.
• **MLD Snooping Enable**	각 VLAN 당 MLD 스누핑을 활성화합니다. MLD 스누핑을 위해 최대 32 개의 VLAN 을 선택할 수 있습니다.
• **Querier Election**	VLAN 에서 MLD Querier 선거에 참여할 수 있습니다. 비활성화 MLD 비 - 쿼리 자 역할을합니다.
• **Compatibility**	호환성은 호스트 및 라우터가 네트워크 내의 호스트 및 라우터에서 작동하는 MLD 버전에 따라 적절한 조치를 취함으로써 유지됩니다. 허용 된 선택은 MLD-Auto, Forece MLDv1, ForceMLDv2 입니다. 기본 호환성 값은 MLD-Auto 입니다.
• **PRI**	(PRI) 인터페이스의 우선 순위. 시스템에 의해 생성 된 MLD 제어 프레임 우선 순위 레벨을 나타냅니다. 이 값을 사용하여 서로 다른 트래픽 클래스의 우선 순위를 지정할 수 있습니다. 허용되는 범위는 0 (최선의 노력)에서 7 (가장 높음)이며, 기본 인터페이스 우선 순위 값은 0 입니다
• **RV**	Robustness Variable 을 사용하면 네트워크에서 예상되는 패킷 손실을 조정할 수 있습니다. 허용 범위는 1 ~ 255 이며 기본 견고성 변수 값은 2 입니다.
• **QI**	Query Interval 은 Querier 가 보낸 General Queries 간의 간격입니다. 허용되는 범위는 1 - 31744 초이며, 기본 쿼리 간격은 125 초입니다.
• **QRI**	정기적 인 일반 쿼리에 삽입 된 Max Resp Code 를 계산하는 데 사용 된 Max Response Time. 허용되는 범위는 0 에서 31744 초까지이며 기본 쿼리 응답 간격은 10 분의 1 초 (10 초) 단위로 100 입니다.
• **LLQI (LMQI for IGMP)**	정기적 인 일반 쿼리에 삽입 된 Max Resp Code 를 계산하는 데 사용 된 Max Response Time. 허용되는 범위는 0 에서 31744 초까지이며 기본 쿼리 응답 간격은 10 분의 1 초 (10 초) 단위로 100 입니다.
• **URI**	기본 구성원 쿼리 간격은 10 분의 1 초 (10 초)입니다.

버튼

Refresh: "VLAN"입력 필드에서 표시된 테이블을 새로 고칩니다.

<<:가장 낮은 VLAN ID 를 가진 항목 인 VLAN 테이블의 첫 번째 항목부터 시작하여 표를 업데이트합니다.

>>: 현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 업데이트합니다.

Add New MLD VLAN: MLD VLAN 을 추가합니다. VID 를 지정하고 새 항목을 구성하십시오. "저장"을 클릭하십시오. 특정 정적 VLAN 이 생성 된 후에 특정 MLD VLAN 이 작동하기 시작합니다.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.8.12 MLD Snooping Port Group 필터링

특정 스위치 응용 프로그램에서 관리자는 최종 사용자가 사용할 수있는 멀티 캐스트 서비스를 제어하려고 할 수 있습니다. 예를 들어, 특정 가입 계획에 기반한 IP / TV 서비스. MLD 필터링 기능은 스위치 포트에서 지정된 멀티 캐스트 서비스에 대한 액세스를 제한함으로써이 요구 사항을 충족하며 MLD 제한은 포트가 결합 할 수있는 동시 멀티 캐스트 그룹 수를 제한합니다.

MLD 필터링을 사용하면 포트에서 허용되거나 거부되는 멀티 캐스트 그룹을 지정하는 스위치 포트에 프로필을 할당 할 수 있습니다. MLD 필터 프로필에는 하나 이상의 멀티 캐스트 주소 또는 범위의 멀티 캐스트 주소가 포함될 수 있습니다. 하나의 프로파일에만 포트에 할당 할 수 있습니다. 활성화 된 경우 포트에서 수신 된 MLD 조인 보고서가 필터 프로필과 비교됩니다. 요청 된 멀티 캐스트 그룹이 허용되면 MLD 가입 보고서가 정상적으로 전달됩니다. 요청 된 멀티 캐스트 그룹이 거부되면 MLD 가입 보고서가 삭제됩니다.

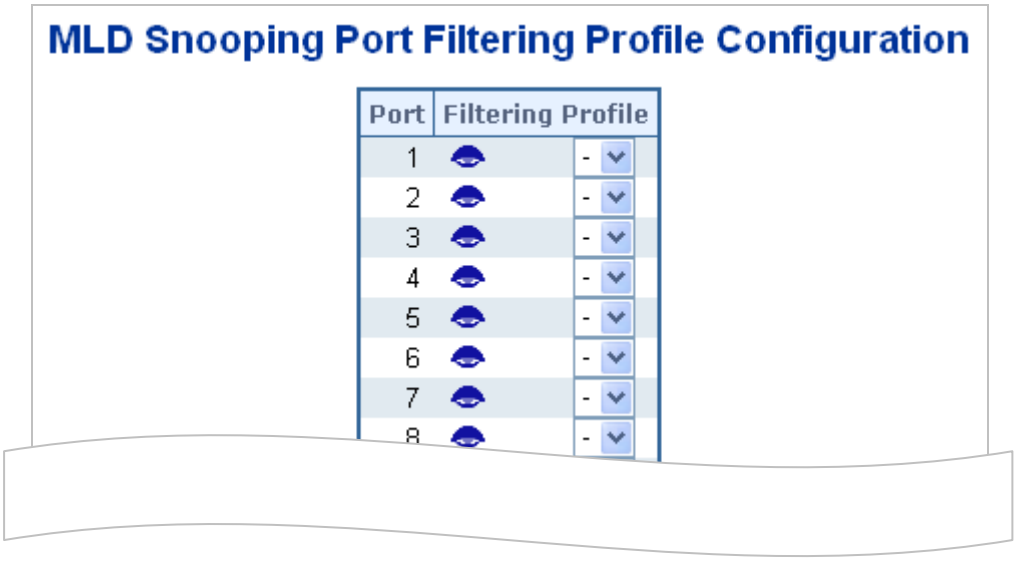


그림 4-8-15: MLD Snooping Port Group Filtering Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	물리적인 포트의 셋팅.
• **Filtering Group**	특정 포트에 대한 필터링 조건으로 IPMC 프로파일을 선택하십시오. 보기 버튼을 클릭하면 지정된 프로필에 대한 요약이 표시됩니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.8.13 MLD Snooping Status

appears.

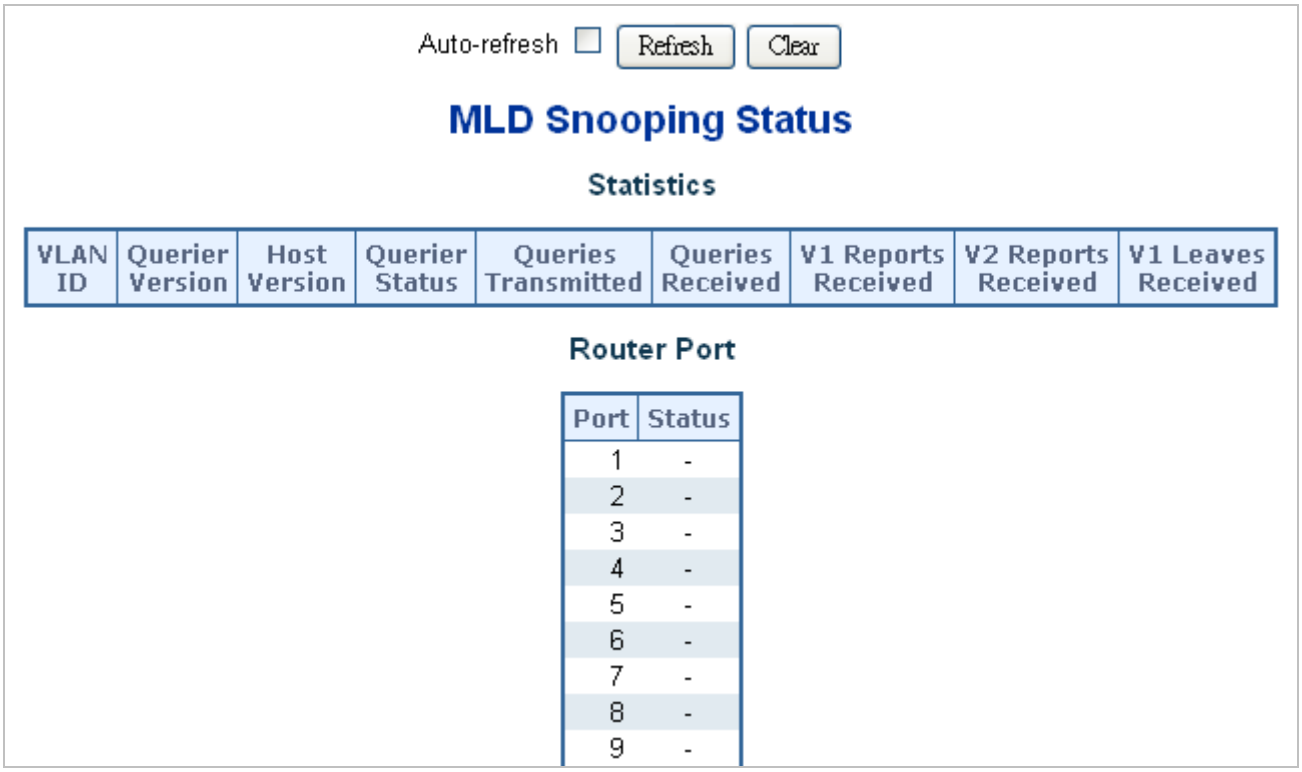


그림 4-8-16: MLD Snooping Status 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **VLAN ID**	항목의 Vlan ID 입니다.
• **Querier Version**	현재 적용되는 쿼리어 버전
• **Host Version**	현재 작업하는 호스트 버전
• **Querier Status**	활성 또는 유휴상태를 보여줍니다. 비활성화에 경우 사용 불가능함을 나타냅니다.

• **Querier Transmitted**	허용 쿼리어의 수를 설정합니다.
• **Querier Received**	받은 쿼리어의 수
• **V1 Reports Received**	수신된 V1 보고서의 수
• **V2 Reports Received**	수신된 V2 의 보고서의 수
• **V1 Leave Received**	송신된 V1 의 보고서의 수
• **Router Port**	어떤 포트가 라우터 포트로 작동하는지 표시합니다. 라우터 포트는 이더넷 스위치의 레이어 3 멀티 캐스트 장치 또는 MLD 쿼리 러쪽으로 연결되는 포트입니다. Static 은 특정 포트가 라우터 포트로 구성되었음을 나타냅니다. Dynamic 은 특정 포트가 라우터 포트로 학습되었음을 나타냅니다. 둘 다 특정 포트가 구성되었거나 라우터 포트로 습득되었음을 나타냅니다.
• **Port**	스위치 포트 수
• **Status**	특정 포트가 라우터 포트인지 여부를 나타냅니다.

버튼

Refresh: 즉시 페이지를 새로고침합니다.

Clear: 모든 통계 항목을 지웁니다. counters.

Auto-refresh : 자동 새로 고침은 3 초마다 발생합니다.

4.8.14 MLD 그룹 안내

이 페이지에는 MLD 그룹 표의 항목이 표시됩니다. MLD 그룹 표는 먼저 VLAN ID 별로 정렬 된 다음 그룹별로 정렬됩니다.

각 페이지는 "페이지 당 입력"입력 필드를 통해 선택된 MLD 그룹 테이블에서 최대 99 개의 항목 (기본값은 20)을 표시합니다. 처음 방문했을 때, 웹 페이지는 MLD 그룹 표의 처음부터 처음 20 개의 항목을 보여줍니다.

"Start from VLAN (VLAN 에서 시작)"및 "group (그룹)"입력 필드를 사용하여 MLD 그룹 테이블에서 시작점을 선택할 수 있습니다. 그림 4-8-17 의 MLD Groups Informatino 화면이 나타납니다..

그림 4-8-17: MLD Snooping Groups Information 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **VLAN ID**	그룹의 Vlan ID 입니다.
• **Groups**	각 그룹의 그룹주소를 나타냅니다
• **Port Members**	그룹에 속한 포트를 나타냅니다

버튼

Auto-refresh : 3 초마다 자동으로 새로 고칩니다.

Refresh : 즉시 페이지를 새로고침합니다.

<< : 표를 업데이트하여 가장 최신의 항목부터 나타냅니다.

>> : 표를 업데이트하여 가장 마지막 항목부터 나타냅니다.

4.8.15 MLDv2 정보

이 페이지에는 MLD SFM 정보 표의 항목이 표시됩니다. MLD SFM (Source-Filtered Multicast) 정보 표에는 SSM (Source-Specific Multicast) 정보도 들어 있습니다. 이 표는 먼저 VLAN ID 별로 정렬 된 다음 그룹별로 정렬 된 다음 포트별로 정렬됩니다. 동일한 그룹에 속하는 다른 소스 주소는 단일 항목으로 처리됩니다. 각 페이지는 MLD SFM 정보 테이블에서 최대 99 개의 항목을 표시하며 기본값은 20 이고 "페이지 당 항목" 입력 필드를 통해 선택됩니다. 처음 방문했을 때, 웹 페이지는 MLD SFM 정보 테이블의 처음부터 처음 20 개의 항목을 보여줍니다..
"Start from VLAN (VLAN 에서 시작)"및 "group (그룹)"입력 필드를 사용하여 MLD SFM 정보 테이블에서 시작점을 선택할 수 있습니다. 그림 4-8-18 의 MLDv2 Information 화면이 나타납니다..

그림 4-8-18: MLD SSM Information 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **VLAN ID**	그룹의 Vlan ID 입니다
• **Group**	각 그룹의 그룹주소를 나타냅니다
• **Port**	스위치 포트 수
• **Mode**	(VLAN ID, 포트 번호, 그룹 주소) 단위로 유지 관리되는 필터링 모드를 나타냅니다. Include 또는 Exclude 중 하나 일 수 있습니다.

• **Source Address**	현재 시스템은 필터링 할 IP 원본 주소의 총 수를 128 개로 제한합니다.
• **Type**	유형을 나타냅니다. 허용 또는 거부 중 하나 일 수 있습니다.
• **Hardware Filter/Switch**	소스 IPv6 주소의 특정 그룹 주소를 대상으로하는 데이터 플레인이 칩별로 처리 될 수 있는지 여부를 나타냅니다.

버튼

Auto-refresh : 자동 새로 고침은 3 초마다 발생합니다..

Refresh : 입력란에서 표시된 표를 새로 고칩니다.

<< : MLD SFM 정보 테이블의 첫 번째 항목부터 시작하여 표를 업데이트합니다.

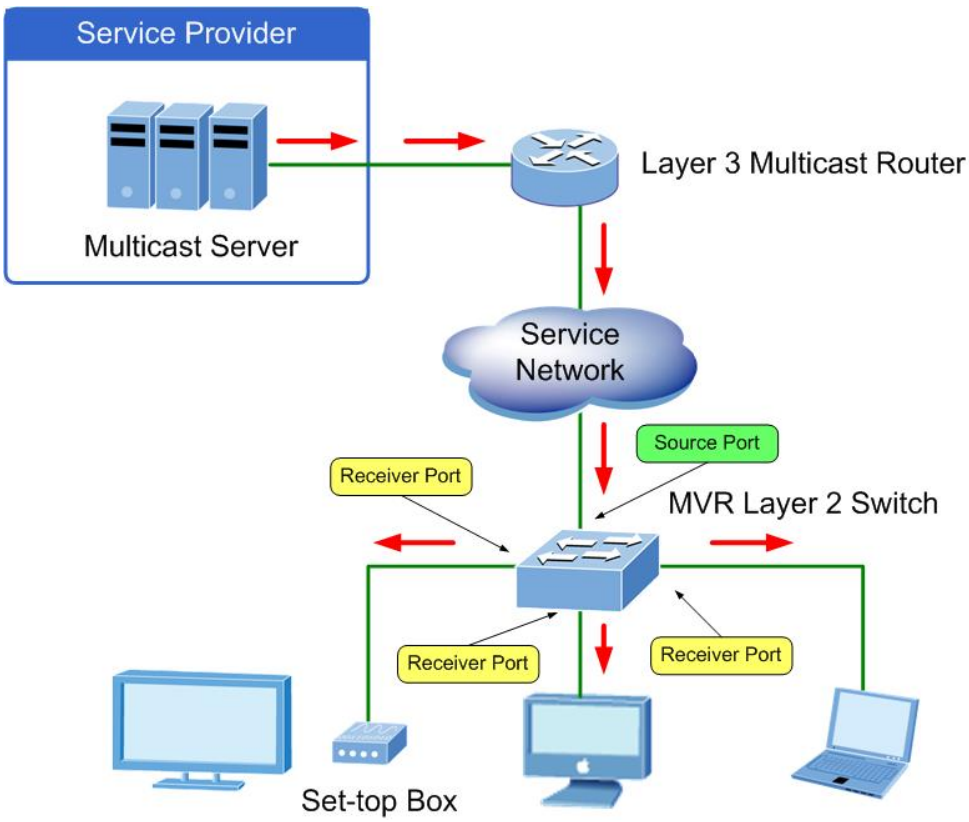
>> : 현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 업데이트합니다.

4.8.16 MVR (Multicast Vlan Register)

MVR 기능을 사용하면 멀티 캐스트 VLAN 에서 멀티 캐스트 트래픽을 전달할 수 있습니다..

- 멀티캐스트 TV 응용 프로그램에서 PC 또는 네트워크 TV 또는 셋톱 박스는 멀티캐스트 스트림을 수신합니다
- 여러 셋톱 박스 또는 PC 를 MVR 수신기 포트로 구성된 스위치 포트 하나의 가입자 포트에 연결할 수 있습니다. 가입자가 채널을 선택하면 셋톱 박스 또는 PC 는 스위치 A 에 IGMP / MLD 보고 메시지를 전송하여 적절한 멀티 캐스트 그룹 주소에 합류합니다.
- 멀티 캐스트 데이터를 멀티 캐스트 VLAN 과주고받는 Up-link 포트를 MVR 소스 포트라고합니다.

각 멀티 캐스트 VLAN 에 대해 해당 채널 설정을 사용하여 최대 8 개의 MVR VLAN 을 생성 할 수 있습니다. 채널 설정에는 최대 256 개의 그룹 주소가 있습니다.



이 페이지는 MVR 관련 구성을 제공합니다. 그림 4-8-19 의 MVR 화면이 나타납니다..

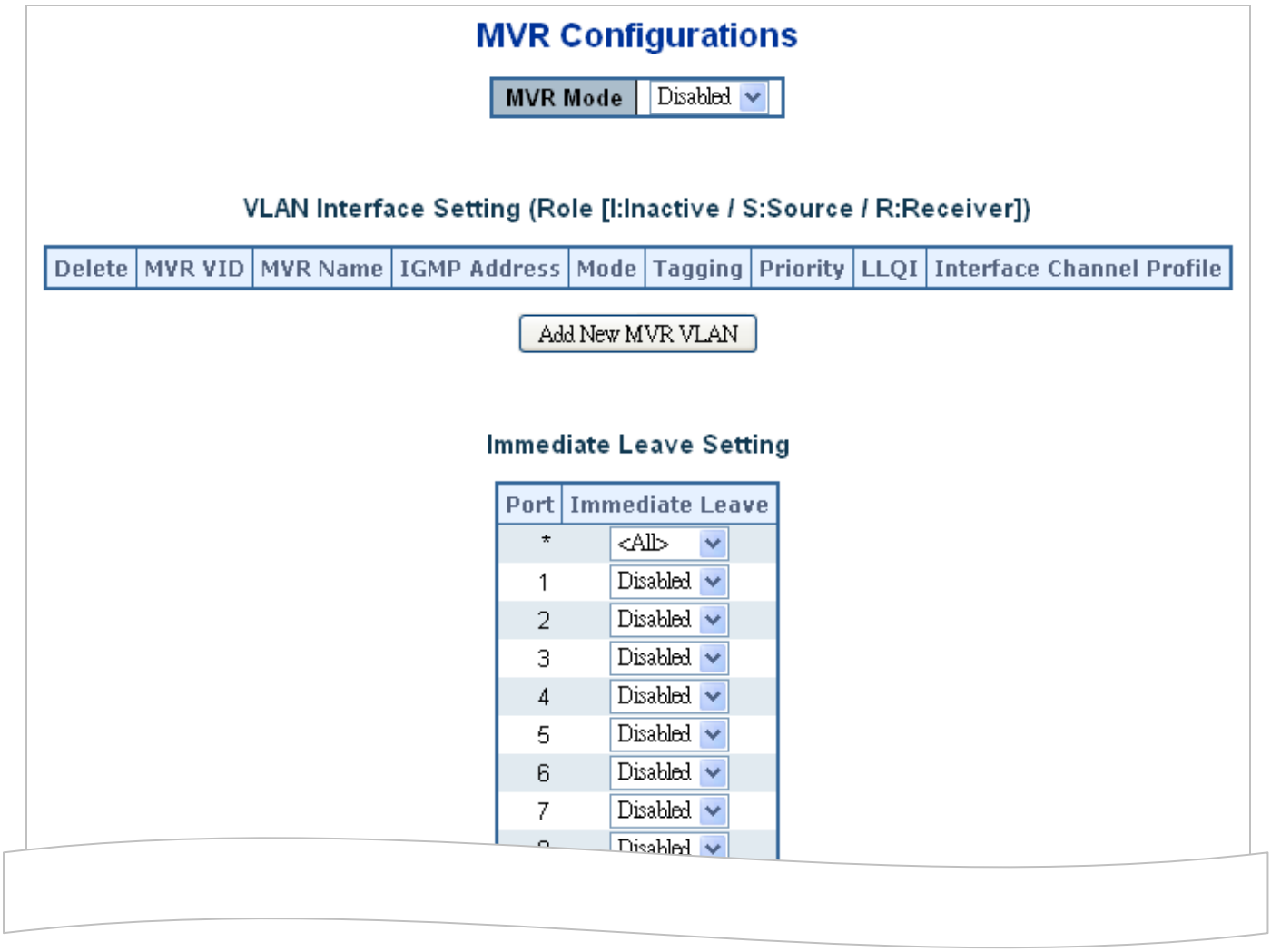


그림 4-8-19: MVR 설정화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **MVR Mode**	전역 MVR 을 활성화 / 비활성화합니다. 미등록 플러딩 제어는 IGMP / MLD 스누핑의 현재 구성에 따라 다릅니다. MVR 그룹 표가 가득 차면 등록되지 않은 플러딩 (Unregistered Flooding) 제어를 활성화하는 것이 좋습니다.
• **Delete**	항목을 삭제하려면 선택하십시오. 지정된 항목은 다음 저장 중에 삭제됩니다.
• **MVR VID**	멀티캐스트 VLAN ID 를 지정하십시오.. 주의: MVR 소스에서 VLAN 포트와 겹치지 않도록 해야합니다..
• **MVR Name**	MVR Name 은 특정 MVR VLAN 의 이름을 나타내는 선택적 속성입니다. MVR VLAN 이름 문자열의 최대 길이는 16 입니다. MVR VLAN 이름에는 영문자 또는 숫자 만 사용할 수 있습니다. 선택적 MVR VLAN 이름이 주어지면 하나 이상의 알파벳이 포함되어야합니다. MVR VLAN 이름은 기존 MVR VLAN

	항목에 대해 편집하거나 새 항목에 추가 할 수 있습니다.
• **IGMP Address**	IGMP 제어 프레임의 IP 헤더에 사용 된 소스 주소로 IPv4 주소를 정의하십시오. 기본 IGMP 주소가 설정되지 않았습니다 (0.0.0.0). IGMP 주소가 설정되어 있지 않으면 시스템은이 VLAN 과 연관된 IP 인터페이스의 IPv4 관리 주소를 사용합니다. IPv4 관리 주소가 설정되어 있지 않으면 시스템은 사용 가능한 첫 번째 IPv4 관리 주소를 사용합니다. 그렇지 않으면 시스템은 미리 정의 된 값을 사용합니다. 기본적으로이 값은 192.0.2.1 입니다.
• **Mode**	MVR 작동 모드를 지정하십시오. 동적 모드에서 MVR 은 소스 포트에 대한 동적 MVR 멤버십 보고서를 허용합니다. 호환 모드에서는 MVR 멤버쉽 보고서가 소스 포트에서 금지됩니다. 기본값은 동적 모드입니다.
• **Tagging**	통과 된 IGMP / MLD 제어 프레임을 Untagged 로 전송할지 또는 MVR VID 로 태그 지정 할지를 지정합니다. 기본값은 Tagged 입니다.
• **Priority**	통과 된 IGMP / MLD 제어 프레임이 우선 순위 방식으로 전송되는 방법을 지정하십시오. 기본 우선 순위는 0 입니다.
• **LLQI**	멀티 캐스트 그룹 구성원에서 포트를 제거하기 전에 수신기 포트에서 IGMP / MLD 보고서 구성원을 기다리는 최대 시간을 정의하십시오. 값은 10 분의 1 초 단위입니다. 범위는 0 에서 31744 까지입니다. 기본 LLQI 는 5 분의 1 초 또는 0.5 초입니다.
• **Interface Channel Setting**	MVR VLAN 을 만들 때 특정 MVR VLAN 에 대한 채널 필터링 조건으로 IPMC 프로필을 선택합니다. 보기 버튼을 클릭하면 MVR VLAN 의 인터페이스 채널 프로파일 링에 대한 요약 정보가 표시됩니다. 지정된 인터페이스 채널에 대해 선택된 프로파일은 허가 그룹 주소를 겹쳐서는 안됩니다.
• **Port**	설정에 대한 논리 포트입니다.
• **Port Role**	지정된 MVR VLAN 의 MVR 포트를 다음 역할 중 하나로 구성합니다.. ■ **Inactive**: 지정된 포트가 MVR 작업에 참여하지 않습니다. ■ **Source**: Multicast 데이터를 송수신하는 UP-link 포트를 구성하고 가입자는 소스에 직접 연결할 수 없습니다. ■ **Receiver**:가입자 포트의 경우 수신 포트로 구성하고 Multicast 데이터를 수신하지 않습니다.. 주의:MVR 소스포트는 관리 Vlan 포트와 중복되지 않도록합니다. 역할 기호를 눌러 포트 역할을 선택하여 설정을 전환하십시오. 나는 비활성을 나타냅니다.; S 는 소스를 나타냅니다.; R 수신지를나타냅니다. 기본 값은 비활성화입니다.
• **Immediate Leave**	포트에서 빠르게 나갑니다.

버튼

Add New MVR VLAN: 새 MVR VLAN 을 추가하고. VID 의 새 항목을 구성하십시오. '저장'을 클릭하십시오.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.8.17 MVR 상태

이 페이지는 MVR 상태를 제공합니다. 그림 4-8-20 의 MVR 상태 화면이 나타납니다..

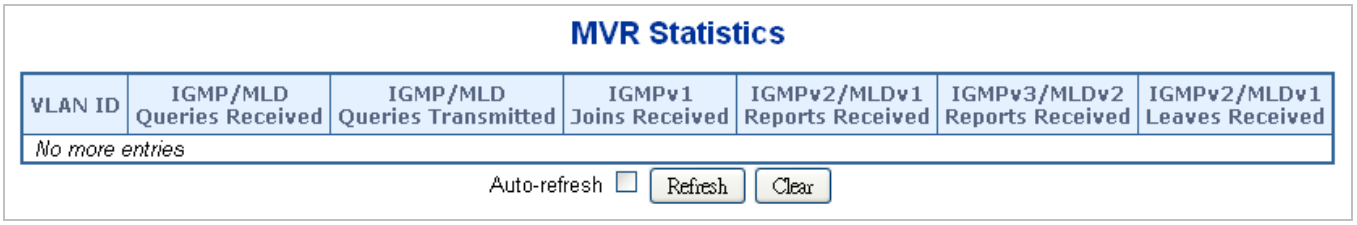


그림 4-8-20: MVR Status 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **VLAN ID**	Multicast Vlan ID 입니다.
• **IGMP/MLD Queries Received**	IGMP 및 MLD 에 대한 각각의 수신 쿼리 수입니다.
• **IGMP/MLD Queries Transmitted**	IGMP 및 MLD 에 대한 Transmitted Queries 의 수입니다.
• **IGMPv1 Joins Received**	수신 된 IGMPv1 조인의 수입니다..
• **IGMPv2/MLDv1 Reports Received**	수신 된 IGMPv2 조인 수 및 MLDv1 보고서 수입니다.
• **IGMPv3/MLDv2 Reports Received**	수신 된 IGMPv1 조인 수 및 MLDv2 보고서 수입니다.
• **IGMPv2/MLDv1 Leaves Received**	수신 된 IGMPv2 Leaves 및 MLDv1 Done 의 수입니다.

버튼

Refresh: 즉시 페이지를 새로고침합니다.

Clear: 모든 통계 카운터 항목을 지웁니다.

Auto-refresh : 자동 새로 고침은 3 초마다 발생합니다..

4.8.18 MVR Groups Information

이 페이지에는 MVR 그룹 표의 항목이 표시됩니다. MVR 그룹 표는 먼저 VLAN ID 별로 정렬 된 다음 그룹별로 정렬됩니다.

각 페이지는 MVR 그룹 테이블에서 최대 99 개의 항목을 표시하며, 기본값은 20 이고 "페이지 당 항목 수"입력 필드를

통해 선택됩니다. 처음 방문했을 때, 웹 페이지는 MVR 그룹 표의 처음부터 처음 20 개의 항목을 보여줍니다.

"Start from VLAN (VLAN 에서 시작)"및 "group (그룹)"입력 필드를 사용하여 MVR Group Table 에서 시작점을 선택할 수 있습니다. 그림 4-8-21 의 MVR 그룹 정보 화면이 나타납니다.

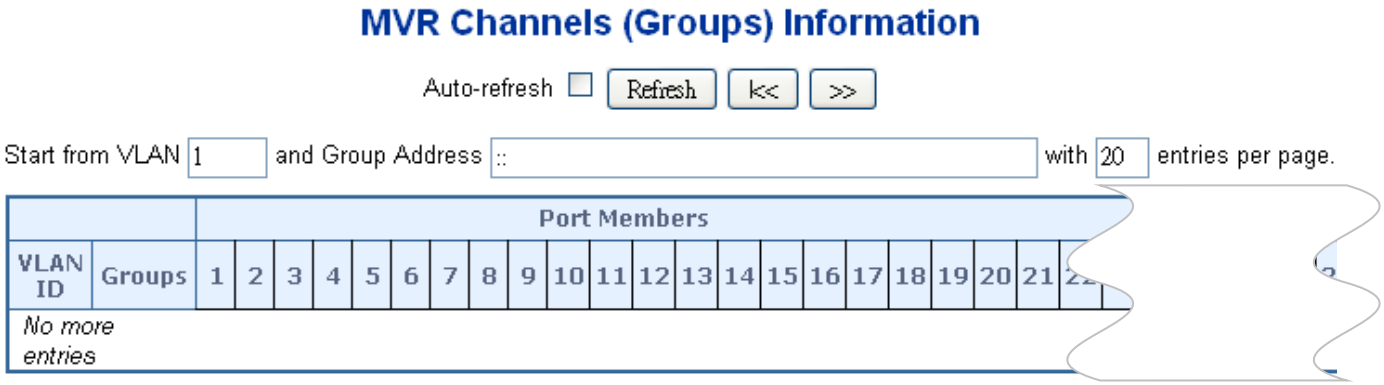


그림 4-8-21: MVR Groups Information 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **VLAN**	그룹의 Vlan ID 입니다.
• **Groups**	각 그룹의 VLAN ID 그룹을 나타냅니다.
• **Port Members**	그룹에 속한 포트를 나타냅니다.

버튼

Auto-refresh : 자동 새로 고침은 3 초마다 발생합니다..

Refresh : 표시 된 입력란에서 표시된 표를 새로 고칩니다.

<< : MVR 채널 (그룹) 정보 표의 첫 번째 항목부터 시작하여 표를 업데이트합니다..

>> : 현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 업데이트합니다..

4.8.19 MVR SFM Information

이 페이지에는 MVR SFM 정보 표의 항목이 표시됩니다. MVR SFM (Source-Filtered Multicast) 정보 표에는 SSM (Source-Specific Multicast) 정보도 들어 있습니다. 이 표는 먼저 VLAN ID 별로 정렬 된 다음 그룹별로 정렬 된 다음 포트별로 정렬됩니다. 동일한 그룹에 속하는 다른 소스 주소는 단일 항목으로 처리됩니다.

각 페이지는 MVR SFM 정보 표 (기본값은 20 임)에서 최대 99 개의 항목을 표시하며 "페이지 당 항목 수"입력 필드를

통해 선택됩니다. 처음 방문했을 때, 웹 페이지는 MVR SFM 정보 표의 처음부터 처음 20 개의 항목을 표시합니다.

"Start from VLAN (VLAN 에서 시작)"및 "Group Address (그룹 주소)"입력 필드를 사용하여 MVR SFM 정보 테이블에서 시작점을 선택할 수 있습니다. 그림 4-8-22 의 MVR SFM 정보 화면이 나타납니다.

그림 4-8-22: MVR SFM Information 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **VLAN ID**	그룹의 Vlan ID 입니다.
• **Group**	그룹의 그룹주소를 나타냅니다.
• **Port**	스위치 포트의 수
• **Mode**	(VLAN ID, 포트 번호, 그룹 주소) 단위로 유지 관리되는 필터링 모드를 나타냅니다. Include 또는 Exclude 중 하나 일 수 있습니다.
• **Source Address**	소스의 IP 주소. 현재 시스템에서는 필터링 할 IP 원본 주소의 총 수를 128 개로 제한합니다. 원본 필터링 주소가 없으면 "없음"이라는 텍스트가 원본 주소 필드에 표시됩니다.
• **Type**	유형을 나타냅니다. 허용 또는 거부 중 하나 일 수 있습니다.
• **Hardware Filter / Switch**	소스 IPv4 / IPv6 주소의 특정 그룹 주소를 대상으로하는 데이터 플레인이 칩별로 처리 될 수 있는지 여부를 나타냅니다.

버튼

Auto-refresh : 자동 새로 고침은 3 초마다 발생합니다..

Refresh : 표시 된 입력란에서 표시된곳을 새로고칩니다.

<< : MVR SFM 정보 테이블의 첫 번째 항목부터 시작하여 표를 업데이트합니다.

4.9 QoS(Quality of Service)

4.9.1 QoS 의 이해

QoS (Quality of Service)는 네트워크 트래픽을 제어 할 수있는 고급 트래픽 우선 순위 지정 기능입니다. QoS 를 사용하면 멀티미디어, 비디오, 프로토콜 특정, 시간 중요 및 파일 백업 트래픽과 같은 다양한 유형의 트래픽에 다양한 등급의 네트워크 서비스를 할당 할 수 있습니다..

QoS 는 대역폭 제한, 지연, 손실 및 지터를 줄입니다. 또한 데이터 전달에 대한 안정성을 높이고 네트워크 전체의 특정 응용 프로그램에 우선 순위를 부여 할 수 있습니다. 스위치가 선택한 응용 프로그램 및 트래픽 유형을 정확하게 처리하도록 정의 할 수 있습니다. 시스템에서 QoS 를 사용하여 다음을 수행 할 수 있습니다.:

- 다음과 같은 방법으로 다양한 네트워크 트래픽을 제어하십시오.:
- 패킷 속성을 기반으로 트래픽을 분류합니다.
- 트래픽에 우선 순위 지정 (예 : 시간이 결정적인 또는 업무에 중요한 응용 프로그램에 우선 순위를 설정).
- 트래픽 필터링을 통한 보안 정책 적용.
- 지연 및 지터를 최소화하여 화상 회의 또는 IP 상의 음성과 같은 멀티미디어 응용 프로그램에 대해 예측 가능한 처리량을 제공합니다..
- 특정 트래픽 유형에 대한 성능을 향상시키고 트래픽 양이 증가 할 때 성능을 보존합니다..
- 네트워크에 지속적으로 대역폭을 추가해야하는 필요성을 줄입니다.
- 네트워크 정체를 관리합니다.

QoS 술어

- **Classifier** - 네트워크의 트래픽을 분류합니다. 트래픽 분류는 프로토콜, 응용 프로그램, 원본, 대상 등으로 결정됩니다. 분류를 작성하고 수정할 수 있습니다. 스위치는 분류 된 트래픽을 그룹화하여 적절한 서비스 수준으로 스케줄링합니다.
- **DiffServ Code Point (DSCP)** - 는 네트워크를 통해 패킷에 필요한 서비스 수준을 나타 내기 위해 특정 애플리케이션 및 / 또는 장치에 의해 인코딩되는 IP 헤더 내의 트래픽 우선 순위 지정 비트입니다..
- **Service Level** - 분류 된 트래픽 집합에 부여 할 우선 순위를 정의합니다. 서비스 레벨을 작성하고 수정할 수 있습니다.
- **Policy** - 네트워크가 비즈니스 요구를 충족 할 수 있도록 네트워크에 적용되는 일련의 "규칙"으로 구성됩니다. 즉, 트래픽은 특정 비즈니스 유형에 대한 중요성에 따라 네트워크 전체에서 우선 순위를 매길 수 있습니다.
- **QoS Profile** - 여러 규칙 집합 (분류 자와 서비스 수준 조합)으로 구성됩니다. QoS 프로파일은 포트에 할당됩니다..
- **Rules** - 스위치가 특정 유형의 트래픽을 처리하는 방법을 정의하는 서비스 수준과 분류자를 포함합니다. 규칙은 QoS 프로파일과 관련됩니다 (위 참조).

네트워크에서 QoS 를 구현하려면 다음 작업을 수행해야합니다.:

1. 서비스 수준을 정의하여 트래픽에 적용될 우선 순위를 결정합니다..
2. 분류기를 적용하여 들어오는 트래픽을 분류하고 스위치에서 처리하는 방법을 결정합니다..
3. 서비스 레벨과 분류자를 연관시키는 QoS 프로파일을 생성합니다..
4. 포트에 QoS 프로파일을 적용하십시오.

4.9.2 Port Policing

모든 스위치 포트에 대한 정책 설정을 구성 할 수 있습니다. 그림 4-9-1 의 포트 폴리싱 화면이 나타납니다.

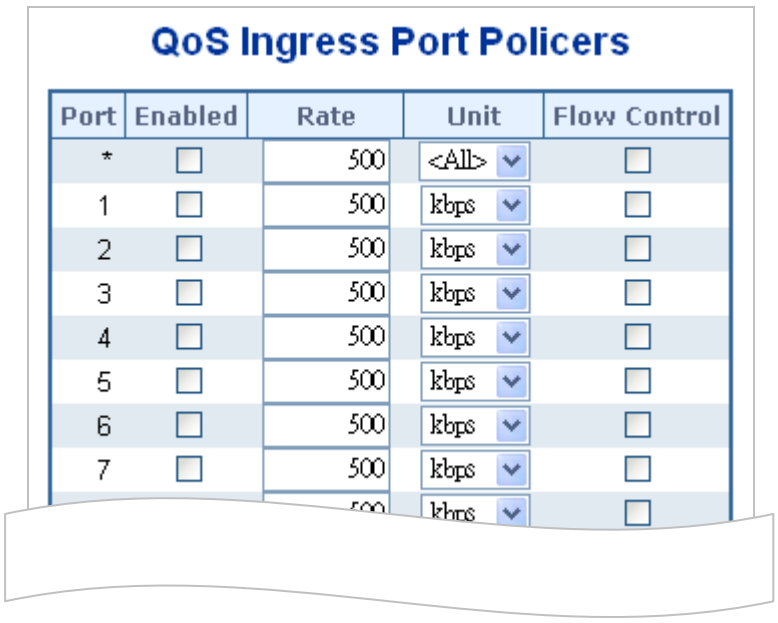


그림 4-9-1: QoS Ingress Port Policers 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	아래 구성이 적용되는 포트 번호입니다.
• **Enable**	이 스위치 포트에서 정책들이 활성화되는지 여부를 제어합니다.
• **Rate**	정책안의 속도를 조정합니다. 이 값은 "단위"가 "kbps"또는 "fps"일 때 100-1000000 으로 제한되며 "단위"가 "Mbps"또는 "kfps"일 때 1-3300 으로 제한됩니다. 기본값은 500 입니다.
• **Unit**	폴리서 속도의 측정 단위를 kbps, Mbps, fps 또는 kfps 로 제어합니다. 기본값은 "kbps"입니다.
• **Flow Control**	흐름 제어가 활성화되고 포트가 흐름 제어 모드 인 경우 프레임을 삭제하는 대신 일시 중지 프레임이 전송됩니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.9.3 Port Classification

이 페이지에서는 모든 스위치 포트에 대한 기본 QoS 수신 등급 설정을 구성 할 수 있습니다. 그림 4-9-2 의 포트 분류 화면이 나타납니다..

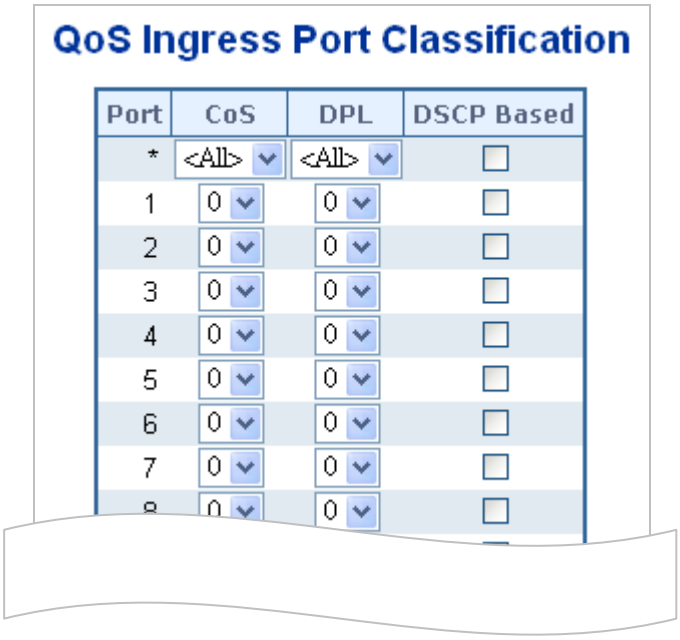


그림 4-9-2 : QoS Ingress Port Classification 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	아래 구성이 적용되는 포트 번호입니다.
• **CoS**	기본 서비스 클래스를 제어합니다. 모든 프레임은 CoS 로 분류됩니다. CoS, 대기열 및 우선 순위간에 일대일 매핑이 있습니다. 0 의 CoS 가 가장 낮은 우선 순위를 갖습니다. 포트가 VLAN 을 인식하고 프레임에 태그가 지정되면 프레임은 아래 표시된 것처럼 태그의 PCP 값을 기반으로하는 CoS 로 분류됩니다. 그렇지 않으면 프레임이 기본 CoS 로 분류됩니다. PCP 값: 0 1 2 3 4 5 6 7 CoS 값: 1 0 2 3 4 5 6 7 분류 된 CoS 는 QCL 항목에 의해 기각 될 수 있습니다. **노트: 기본 CoS 가 동적으로 변경된 경우 구성된 기본 CoS 다음에 괄호 안에 실제 기본 CoS 가 표시됩니다.**
• **DPL**	기본 놓기 우선 순위 수준을 제어합니다. 모든 프레임은 드롭 우선 순위 레벨로 분류됩니다. 포트가 VLAN 을 인식하고 프레임에 태그가 지정되면 프레임은 태그의 DEI 값과 동일한 DPL 로 분류됩니다. 그렇지 않으면 프레임은 기본 DPL 로 분류됩니다. 분류 된 DPL 은 QCL 항목에 의해 폐지 될 수 있습니다.
• **DSCP Based**	DSCP 기반 QoS 수신 포트 분류를 활성화하려면 클릭하십시오.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.9.4 Port Scheduler

이 페이지에서는 모든 스위치 포트에 대한 QoS 출력 포트 스케줄러에 대한 개요를 제공합니다. 그림 4-9-3 의 Port Scheduler 화면이 나타납니다.

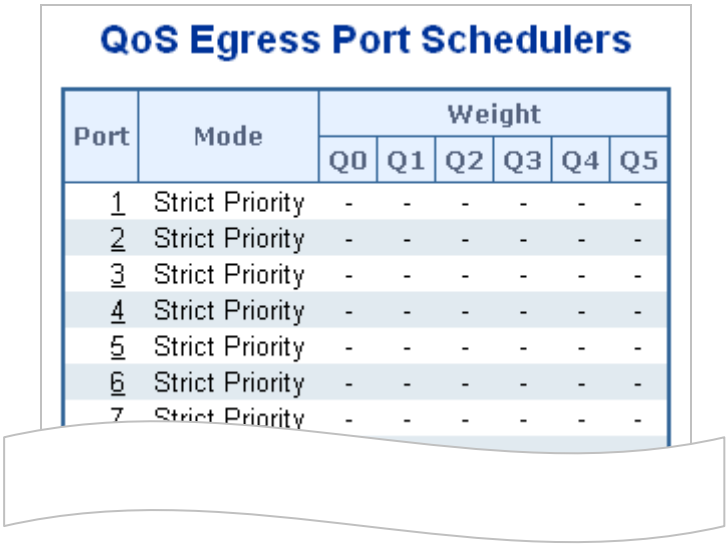


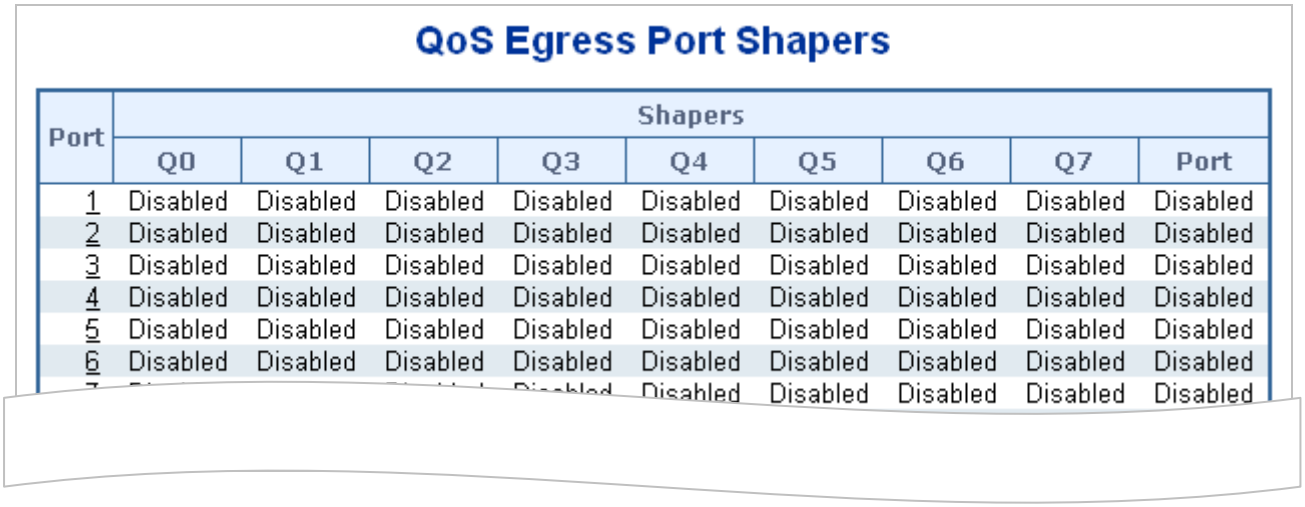
그림 4-9-3: QoS Egress Port Schedule 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	같은 행에 포함 된 설정의 논리 포트입니다. 스케줄러를 구성하려면 포트 번호를 클릭하십시오. 자세한 내용은 4.9.5.1 장을 참조하십시오.
• **Mode**	스케줄러 구성시에 포트번호를 선택합니다.
• **Q0 ~ Q5**	대기열과 포트의 사용감을 나타냅니다.

4.9.5 Port Shaping

이 페이지는 모든 스위치 포트에 대한 QoS 송신 포트 셰이퍼의 개요를 제공합니다. 그림 4-9-4 의 Port Shapping 화면이 나타납니다..



QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
					Disabled	Disabled	Disabled	Disabled	Disabled

그림 4-9-4: QoS Egress Port Shapers 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	같은 행에 포함 된 설정의 논리 포트입니다. 셰이퍼를 구성하려면 포트 번호를 클릭하십시오. 자세한 내용은 4.9.5.1 장을 참조하십시오.
• **Q0 ~Q7**	'사용 중지됨'또는 실제 대기열 셰이퍼 비율을 표시합니다. "800 Mbps".
• **Port**	'사용 중지됨'또는 실제 포트 셰이퍼 속도를 보여줍니다. "800 Mbps".

4.9.5.1 QoS 출력포트 스케줄과 형태

특정 포트의 Port Scheduler 및 Shapers 가이 페이지에서 구성됩니다. 그림 4-9-5 의 QoS 출력 포트 스케줄과 셰이퍼 화면이 나타납니다..

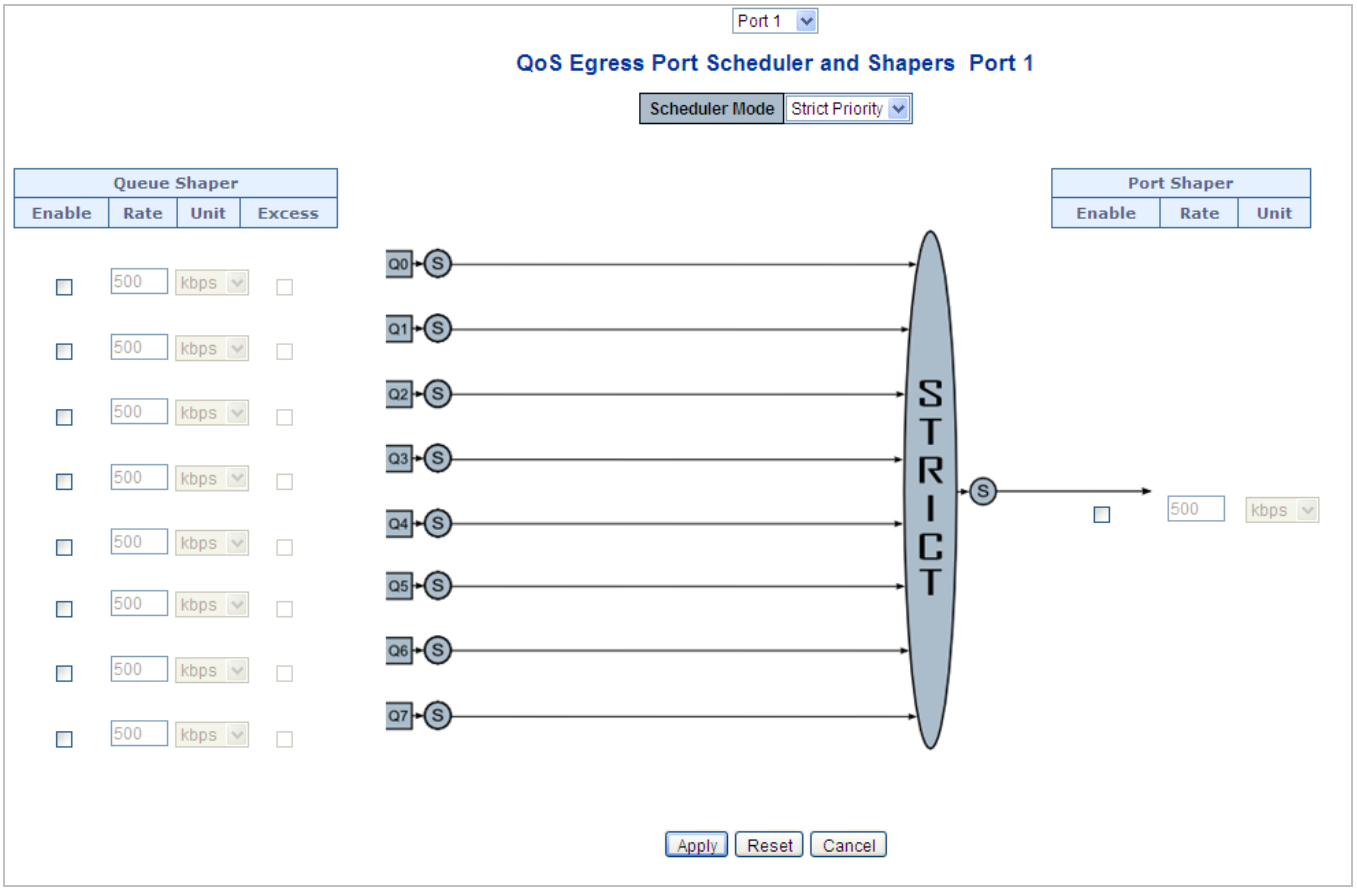


그림 4-9-5: QoS Egress Port Schedule and Shapers 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Schedule Mode**	스위치포트에서 스케줄 모드가 "우선 순위" 나 "가중치" 여부를 제어합니다
• **Queue Shaper Enable**	스위치 포트에서 큐에 대해 큐 형태를 사용할 수 있는지 여부를 제어합니다.
• **Queue Shaper Rate**	큐 셰이퍼의 속도를 제어합니다. 이 값은 "Unit"이 "kbps"인 경우 100-1000000 으로 제한되고 "Unit"가 "Mbps"인 경우 1-13200 으로 제한됩니다. 기본값은 500 입니다.
• **Queue Shaper Unit**	큐 셰이퍼 비율에 대한 측정 단위를 "kbps"또는 "Mbps"로 제어합니다. 기본값은 "kbps"입니다.
• **Queue Shaper Excess**	대기열에서 초과 대역폭을 사용할 수 있는지 여부를 제어합니다.
• **Queue Scheduler**	이 대기열의 가중치를 제어합니다.

Weight	이 값은 1-100 으로 제한됩니다. 이 매개 변수는 "스케줄러 모드"가 "가중치"로 설정된 경우에만 표시됩니다. 기본값은 "17"입니다.
• **Queue Scheduler Percent**	이 대기열에 대한 가중치 (%)를 표시합니다. 이 매개 변수는 "스케줄러 모드"가 "가중치"로 설정된 경우에만 표시됩니다.
• **Port Shaper Enable**	이 스위치 포트에 대해 포트 셰이퍼를 사용할 수 있는지 여부를 제어합니다.
• **Port Shaper Rate**	포트 셰이퍼의 속도를 제어합니다. 이 값은 "Unit"이 "kbps"인 경우 100-1000000 으로 제한되고 "Unit"가 "Mbps"인 경우 1-13200 으로 제한됩니다. 기본값은 500 입니다..
• **Port Shaper Unit**	포트 셰이퍼 속도의 측정 단위를 "kbps"또는 "Mbps"로 제어합니다. 기본값은 "kbps"입니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

Cancel: 클릭하면 로컬에서 변경 한 내용을 취소하고 이전 페이지로 돌아갑니다.

4.9.6 Port Tag Remarking

이 페이지는 모든 스위치 포트에 대한 QoS 출력 포트 태그 리마킹의 개요를 제공합니다. 그림 4-9-6 포트 태그 리마킹 화면이 나타납니다..

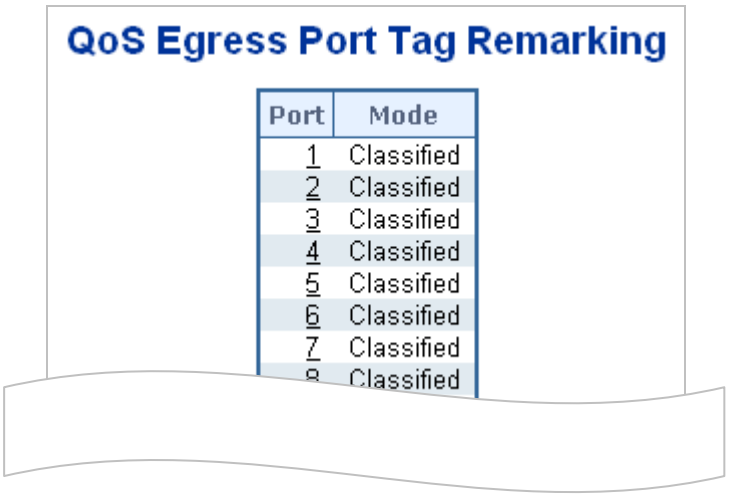


그림 4-9-6: QoS Egress Port Tag Remarking 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	같은 행에 포함 된 설정의 논리 포트입니다. 구성을 확인 하려면 포트 번호를 클릭하십시오. 자세한 내용은 4.9.6.1 장을 참조하십시오.
• **Mode**	포트에 리마킹모드를 사용하여 나타냅니다.. ■ **Classified**: 분류 된 PCP / DEI 값 사용 ■ **Default**: 기본 PCP / DEI 값을 사용하십시오. ■ **Mapped**: QoS 클래스와 DP 레벨의 매핑 된 버전을 사용하십시오.

4.9.6.1 QoS Egress Port Tag Remarking

특정 포트에 대한 QoS 출력 포트 태그 리마킹이이 페이지에서 구성됩니다. 그림 4-9-7 의 QoS Egress Port Tag Remarking sscreen 이 나타납니다.

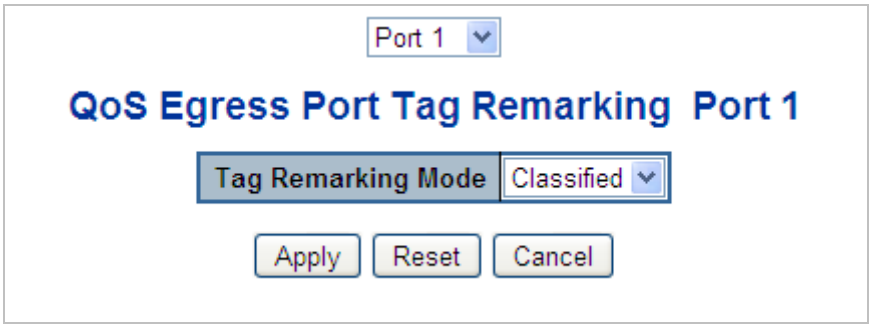


그림 4-9-7: QoS Egress Port Tag Remarking 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Mode**	포트에 태그 리마킹 모드를 나타냅니다.. ■ **Classified**: 분류 된 PCP / DEI 값을 사용하십시오. ■ **Default**: 기본 PCP / DEI 값을 사용합니다.. ■ **Mapped**: 매핑 된 버전의 QoS 클래스 및 DP 수준을 사용합니다.
• **PCP/DEI Configuration**	모드가 Default 로 설정된 경우 사용되는 기본 PCP 및 DEI 값을 조정합니다.
• **(QoS class, DP level) to (PCP, DEI) Mapping**	모드가 맵핑으로 설정된 경우 분류 (QoS 클래스, DP 레벨)에서 (PCP, DEI) 값으로의 매핑을 제어합니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.9.7 Port DSCP

이 페이지에서는 모든 스위치 포트에 대한 기본 QoS 포트 DSCP 구성 설정을 구성 할 수 있습니다. 포트 DSCP 그림 4-9-8 참조.

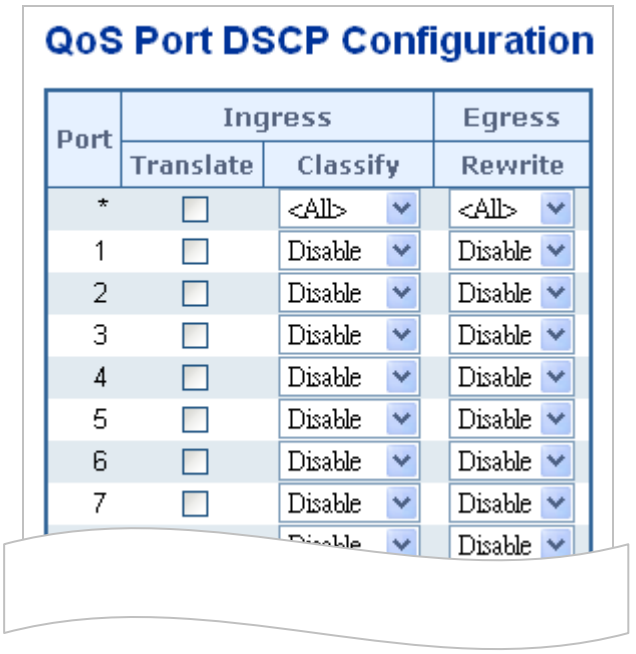


그림 4-9-8: QoS Port DSCP Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	포트 열은 dscp 입구 및 출구 설정을 구성 할 수있는 포트 목록을 표시합니다.
• **Ingress**	Ingress 설정에서 개별 포트에 대한 수신 변환 및 분류 설정을 변경할 수 있습니다. Ingress 에는 두 가지 구성 매개 변수가 있습니다.: ■ **Translate** ■ **Classify**
• **Translate**	입력 변환을 사용하려면 확인란을 클릭합니다.
• **Classify**	포트의 분류에는 4 가지 값이 있습니다. ■ **Disable**: 입력포트에 DSCP 를 분류하지 않습니다. ■ **DSCP=0**: 수신 (또는 사용 가능할 경우 변환) DSCP 가 0 인지 분류합니다. ■ **Selected**: 특정 DSCP 에 대해 DSCP Translation 창에 지정된대로 분류가 활성화 된 선택된 DSCP 만 분류합니다. ■ **All**: 모든 DSCP 를 분류 합니다.
• **Egress**	포트 출력에 덮어쓰는 기록은 다음과 같이 있습니다. - ■ **Disable**: 출력에 덮어쓰지 않음 ■ **Enable**: 매핑없이 다시 작성

	■ **Remap DP Unaware**: 분석기의 DSCP 가 다시 매핑되고 프레임이 재 매핑 된 DSCP 값으로 표시됩니다. 다시 매핑 된 DSCP 값은 항상 'DSCP 변환 -> 출력 다시 매핑 DP0'테이블에서 가져옵니다.. ■ **Remap DP Aware**: 분석기의 DSCP 가 다시 매핑되고 프레임이 재 매핑 된 DSCP 값으로 표시됩니다. 프레임의 DP 수준에 따라 다시 매핑 된 DSCP 값은 'DSCP Translation-> Egress Remap DP0'표 또는 'DSCP Translation-> Egress Remap DP1'표에서 가져옵니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.9.8 DSCP-기반 QoS

이 페이지에서는 모든 스위치에 대한 기본 QoS DSCP 기반 QoS 입력 분류 설정을 구성 할 수 있습니다. 그림 4-9-9 의 DSCP 기반 QoS 화면이 나타납니다.

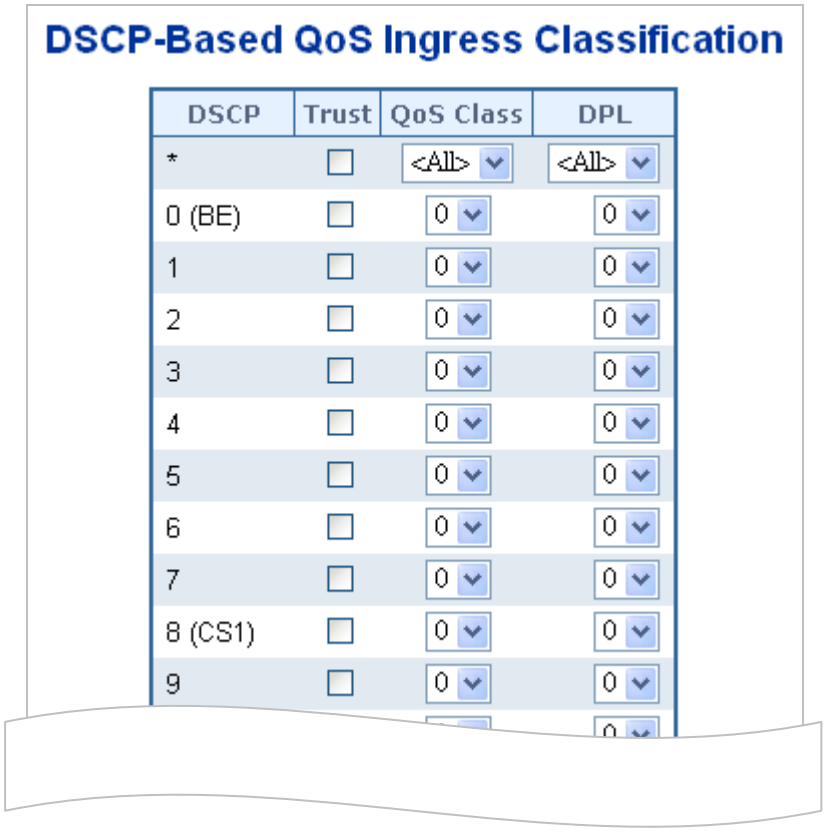


그림 4-9-9: DSCP-based QoS Ingress Classification 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **DSCP**	지원되는 DSCP 값의 최대 수는 64 입니다.
• **Trust**	특정 DSCP 값을 신뢰할 수 있는지 여부를 제어합니다. 신뢰할 수있는 DSCP 값을 가진 프레임 만 특정 QoS 클래스 및 우선 순위 삭제 수준에 매핑됩니다. 신뢰할 수없는 DSCP 값이있는 프레임은 비 IP 프레임으로 처리됩니다.
• **QoS Class**	QoS 클래스 값은 (0-7)
• **DPL**	놓기 우선 순위 (0-1)

4.9.9 DSCP 변환

이 페이지에서는 모든 스위치에 대한 기본 QoS DSCP 변환 설정을 구성 할 수 있습니다. Ingress 또는 Egress 에서 DSCP 변환을 수행 할 수 있습니다. 그림 4-9-10 의 DSCP Translation 화면이 나타납니다.

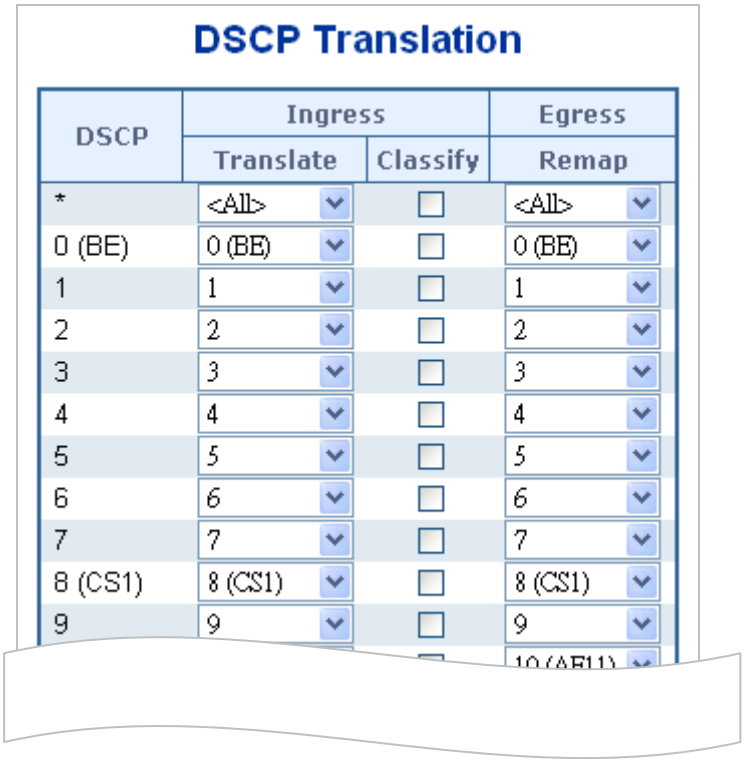


그림 4-9-10: DSCP Translation 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **DSCP**	지원되는 DSCP 값의 최대 수는 64 이며 유효한 DSCP 값의 범위는 0 에서 63 까지입니다.
• **Ingress**	수신 측 DSCP 는 QoS 클래스 및 DPL 맵에 DSCP 를 사용하기 전에 먼저 새 DSCP 로 변환 할 수 있습니다. DSCP Translation 에는 두 가지 구성 매개 변수가 있습니다.– ■ **Translate** ■ **Classify**
• **Translate**	Ingress 쪽의 DSCP 는 (0-63) DSCP 값 중 하나로 변환 할 수 있습니다.
• **Classify**	Ingress 측에서 분류를 사용하려면 클릭하십시오.
• **Egress**	출력면에는 다음과 같은 구성 가능한 매개 변수가 있습니다.- ■ **Remap**
• **Remap DP**	선택 메뉴에서 재 매핑하려는 DSCP 값을 선택하십시오. DSCP 값 범위는 0 에서 63 사이입니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.9.10 DSCP Classification

DSCP 값을 QoS 클래스 및 DPL 값에 매핑 할 수 있습니다. 그림 4-9-11 의 DSCP 분류 화면이 나타납니다.

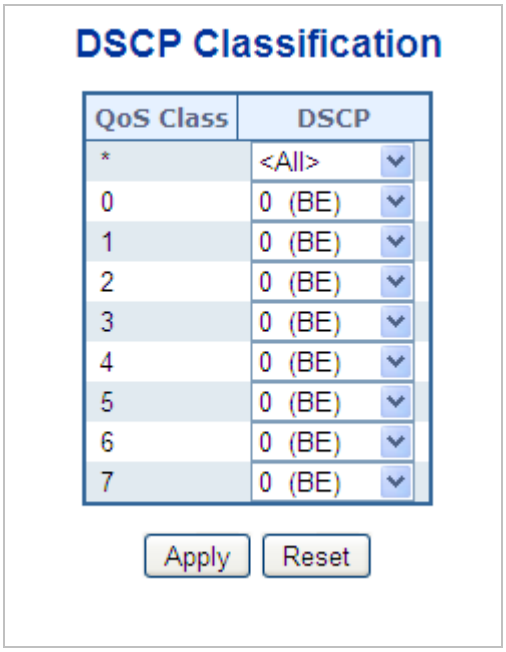


그림 4-9-11: DSCP Classification 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• QoS Class	사용 가능한 QoS 클래스 값의 범위는 0 에서 7 까지입니다. QoS 클래스 (0-7)는 후속 매개 변수에 매핑 될 수 있습니다.
• DPL	실제 놓기 우선 순위 수준.
• DSCP	DSCP 메뉴에서 DSCP 값 (0-63)을 선택하여 DSCP 를 해당 QoS 클래스 및 DPL 값에 매핑합니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.9.11 QoS Control List

이 페이지는 QCE 로 구성된 QoS 제어 목록 (QCL)을 보여줍니다. 각 행은 정의 된 QCE 를 설명합니다. QCE 의 최대 수는 각 스위치에서 256 입니다..

새 QCE 를 목록에 추가하려면 하단의 더하기 기호를 클릭하십시오. 그림 4-9-12 의 QoS 제어 목록 화면이 나타납니다..

그림 4-9-12: QoS Control List Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• QCE#	QCE 의 목차를 나타냅니다.
• Port	QCE 를 해당 포트로 구성된 포트 목록을 나타냅니다..
• DMAC	수신 프레임의 대상 MAC 주소 유형을 지정하십시오. 가능한 값은 다음과 같습니다.: ■ **Any**: 목적지로의 모든 맥주소를 허용합니다. ■ **Unicast**: 유니캐스트 맥주소만 허용합니다 ■ **Multicast**: 멀티캐스트 맥주소만 허용합니다. ■ **Broadcast**: 브로드캐스트 맥주소만 허용합니다.

	기본값은 "Any"로 설정되어 있습니다.
• **SMAC**	발신 MAC 주소의 OUI 필드, 즉 MAC 주소의 처음 3 옥텟 (바이트)을 표시합니다.
• **Tag Type**	태그 유형을 나타냅니다. 가능한 값은 다음과 같습니다.: ■ **Any**: tag 와 Untag 프레임이 일치합니다.. ■ **Untagged:** untagg 프레임만 일치합니다. ■ **Tagged**: tagged 프레임만 일치합니다 기본값은 'Any' 입니다.
• **VID**	특정 VID 또는 VID 범위를 나타내는 VLAN ID 를 나타냅니다. VID 는 1-4095 또는 'Any'
• **PCP**	우선 순위 코드 포인트 : 유효한 값 PCP 는 특정 (0, 1, 2, 3, 4, 5, 6, 7) 또는 범위 (0-1, 2-3, 4-5, 6-7, 0-3, 4 -7) 또는 'Any'.
• **DEI**	삭제 맞춤 지시자 : DEI 의 유효 값은 0, 1 또는 'Any'사이의 값 중 하나 일 수 있습니다.
• **Frame Type**	출입 프레임을 찾을 프레임 유형을 나타냅니다. 가능한 프레임 유형은 다음과 같습니다.: ■ **Any**: QCE 는 모든 프레임 유형과 일치합니다.. ■ **Ethernet**: 이더넷 프레임 (이더넷 유형 0x600-0xFFFF) 만 허용됩니다.. ■ **LLC**: 전용 (LLC) 프레임 허용. ■ **SNAP**: 전용 (SNAP) 프레임 허용. ■ **IPv4**: QCE 는 IPV4 프레임 만 일치시킵니다. ■ **IPv6**: QCE 는 IPV6 프레임 만 일치시킵니다..
• **Action**	구성된 매개 변수가 프레임의 내용과 일치하는 경우 수신 프레임에서 수행되는 분류 작업을 나타냅니다. 세 가지 작업 필드 (클래스, DPL 및 DSCP)가 있습니다. ■ **Class**:QoS 클래스 분류. ■ **DPL**:우선 순위 단계 분류. ■ **DSCP**: DSCP 값에 의 한 분류
• **Modification Button**	QCE 버튼은 다음과 같은 기능들이 있습니다.: ⊕: 현재 행 앞에 새로운 QCE 를 삽입합니다. ⓔ: QCE 를 편집합니다. ⊕: QCE 목록을 위로 이동합니다. ⊕: QCE 목록을 아래로 이동합니다. ⊗: QCE 를 삭제합니다.. ⊕: 하단의 더하기 기호는 QCL 목록 맨 아래에 새 항목을 추가합니다.

4.9.11.1 QoS 전체 제어 설정

그림 4-9-13 의 QCE 설정화면이 나타납니다.

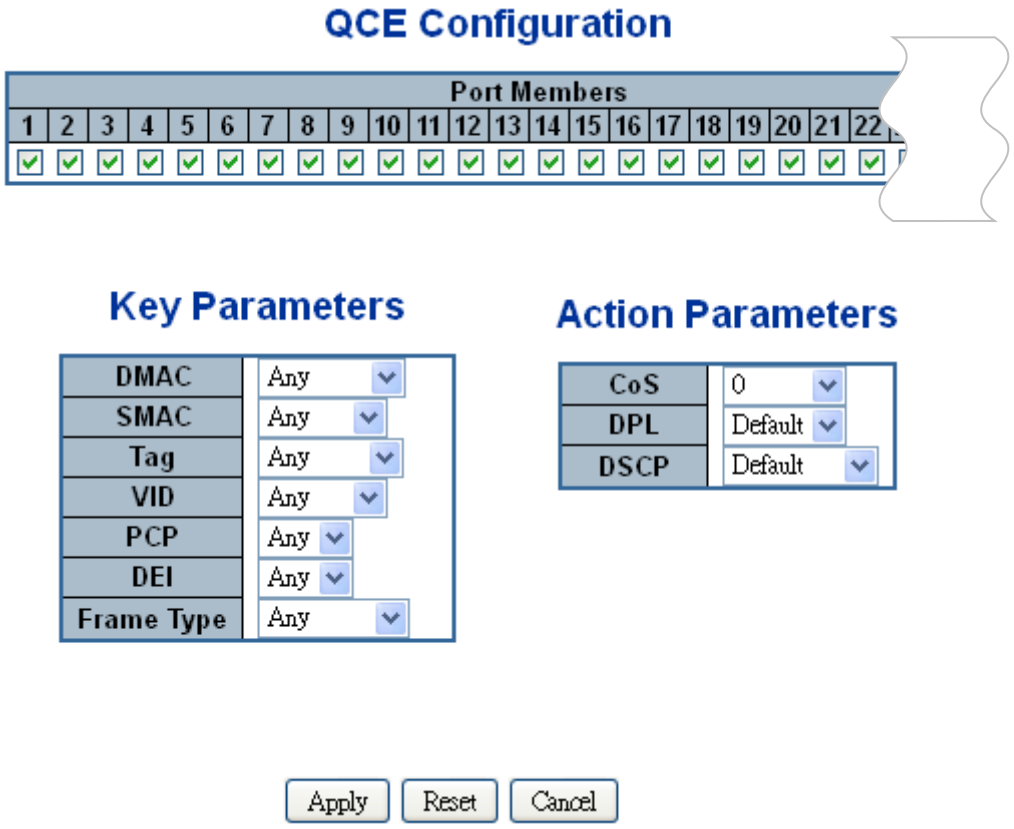


그림 4-9-13: QCE 설정화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port Members**	QCL 항목의 포트 구성원을 만들 경우 확인란을 선택하십시오. 기본적으로 모든 포트가 검사됩니다.
• **Key Parameters**	주요 구성은 다음과 같습니다: ■ **DMAC Type** 가능한 값은 유니 캐스트 (UC), 멀티 캐스트 (MC), 브로드 캐스트 (BC) 또는 'Any' ■ **SMAC** 원본 맥 주소: 24 MS bits (OUI) 또는 'Any' ■ **Tag** 태그 필드의 값은 'Any', 'Untag' 또는'Tag' 일 수 있습니다. ■ **VID** VLAN ID 의 유효한 값은 1-4095 또는 'Any'범위의 값이 될 수 있습니다. 사용자는 특정 값 또는 VID 범위를 입력 할 수 있습니다. ■ **PCP** 우선 순위 코드 포인트 : 유효한 값 PCP 는 특정 (0, 1, 2, 3, 4, 5, 6, 7) 또는 범위 (0-1, 2-3, 4-5, 6-7, 0-3 , 4-7) 또는 'Any' ■ **DEI** Drop Eligible Indicator: DEI 의 유효 값은 0, 1 또는 'Any'사이의 값 중 하나 일 수 있습니다. ■ **Frame Type** 프레임 유형 프레임 유형은 다음 값 중 하나를 가질 수

	있습니다 1. **Any** 2. **Ethernet** 3. **LLC** 4. **SNAP** 5. **IPv4** 6. **IPv6** **Note**: 모든 프레임 유형은 아래에 설명되어 있습니다.
• **Any**	모든 타입의 프레임을 허용합니다.
• **EtherType**	**Ethernet Type** 유효한 이더넷 유형은 0x600-0xFFFF 또는 'Any'이지만 0x800 (IPv4) 및 0x86DD (IPv6)를 제외한 값을 가집니다. 기본값은 'Any'입니다.
• **LLC**	■ **SSAP Address** 유효한 SSAP (Source Service Access Point)은 0x00 에서 0xFF 까지 또는 'Any'로 다양 할 수 있으며, 기본값은 'Any' ■ **DSAP Address** 유효한 DSAP (대상 서비스 액세스 지점)는 0x00 에서 0xFF 까지 또는 'Any', 기본값은 'Any' ■ **Control Address** 유효한 제어 주소는 0x00 에서 0xFF 까지 또는 'Any', 기본값은 'Any'
• **SNAP**	**PID** 유효한 PID (a.k.a 이더넷 유형)는 0x00-0xFFFF 또는 'Any'내에 값을 가질 수 있으며, 기본값은 'Any'
• **IPv4**	■ **Protocol** IP 프로토콜 번호 : (0-255, TCP 또는 UDP) 또는 'Any' ■ **Source IP** 값 / 마스크 형식의 특정 소스 IP 주소 또는 '모두'. IP 와 마스크는 xyzw 형식입니다. 여기서 x, y, z 및 w 는 0 에서 255 사이의 십진수입니다. 마스크가 32 비트 바이너리 문자열로 변환되어 왼쪽에서 오른쪽으로 읽혀지면 첫 번째 0 다음의 모든 비트는 또한 0 일 것 ■ **DSCP** Diffserv 코드 포인트 값 (DSCP) : 특정 값, 값의 범위 또는 'Any'일 수 있습니다. DSCP 값은 BE, CS1-CS7, EF 또는 AF11-AF43 을 포함하여 0-63 범위입니다. ■ **IP Fragment** IPv4 프레임 단편화 된 옵션 : yes | no | any ■ **Sport** 원본 TCP / UDP 포트 : (0-65535) 또는 '모두', 특정 또는 IP 프로토콜에 해당하는 포트 범위 UDP / TCP ■ **Dport** 목적 TCP / UDP 포트 : (0-65535) 또는 '모두', 특정 또는 IP 프로토콜에 해당하는 포트 범위 UDP / TCP
• **IPv6**	**Protocol** IP 프로토콜 번호 : (0-255, TCP 또는 UDP) 또는 'Any' **Source IP** IPv6 소스 주소 : (a.b.c.d) 또는 '모두', 32LSB **DSCP** Diffserv 코드 포인트 값 (DSCP) : 특정 값, 값의 범위 또는 'Any'일 수 있습니다. DSCP 값은 BE, CS1-CS7, EF 또는 AF11-AF43 을 포함하여 0-63 범위입니다. **Sport** 소스 TCP / UDP 포트 : (0-65535) 또는 '모두', 특정 또는 IP 프로토콜에 해당하는 포트 범위 UDP / TCP

	Dport 목적 TCP / UDP 포트 : (0-65535) 또는 '모두', 특정 또는 IP 프로토콜에 해당하는 포트 범위 UDP / TCP
• **Action Parameters**	**Class** QoS 단계: (0-7) 또는 '기본값(Default)'. **DPL** 유효한 삭제 우선 순위 수준은 (0-3) 또는 '기본값'일 수 있습니다. **DSCP** 유효한 DSCP 값은 (0-63, BE, CS1-CS7, EF 또는 AF11-AF43) 또는 '기본값'일 수 있습니다. 'Default'는 기본 분류 된 값이이 QCE 에 의해 수정되지 않는다는 것을 의미합니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 로컬 변경 사항을 실행 취소하고 이전에 저장된 값으로 되돌리려면 클릭하십시오.

Cancel: 구성 변경 사항을 저장하지 않고 이전 페이지로 돌아 가기

4.9.12 QCL 상태

이 페이지는 다른 QCL 사용자에 의한 QCL 상태를 표시합니다. 각 행은 정의 된 QCE 를 설명합니다. 하드웨어 제한으로 인해 특정 QCE 가 하드웨어에 적용되지 않으면 충돌이 발생합니다. QCE 의 최대 수는 각 스위치에서 256 입니다. 그림 4-9-14 의 QoS Control List Status 화면이 나타납니다..

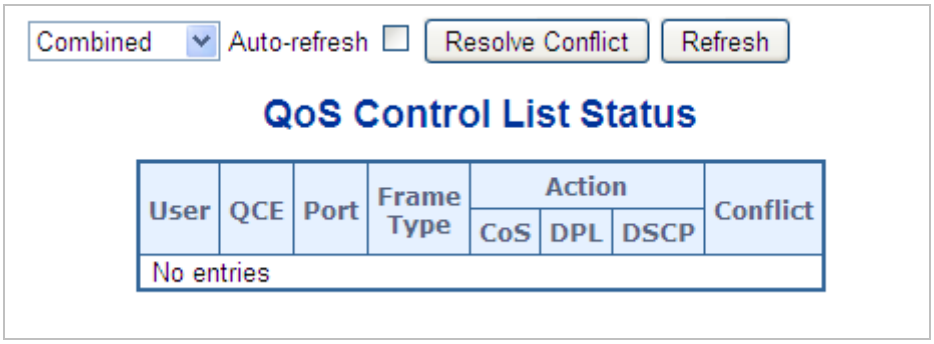


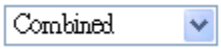
그림 4-9-14: QoS Control List Status 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **User**	QCL 사용자를 나타냅니다.
• **QCE#**	QCE 의 색인을 나타냅니다.
• **Port**	QCE 로 구성된 포트 목록을 나타냅니다.

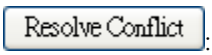
• **Frame Type**	들어오는 프레임을 찾을 프레임 유형을 나타냅니다. 가능한 프레임 유형은 다음과 같습니다.: ■ **Any**: QCE 는 모든 프레임 유형과 일치합니다. ■ **Ethernet**: 이더넷 프레임 (이더넷 유형 0x600-0xFFFF) 만 허용됩니다. ■ **LLC**: (LLC) 프레임만 허용됩니다. ■ **SNAP**: 전용 (SNAP) 프레임 만 허용됩니다.. ■ **IPv4**: QCE 는 IPV4 프레임만 매치합니다. ■ **IPv6**: QCE 는 IPV6 프레임만 매치합니다.
• **Action**	구성된 매개 변수가 프레임의 내용과 일치하는 경우 수신 프레임에서 수행되는 분류 작업을 나타냅니다. 세 가지 작업 필드 (클래스, DPL 및 DSCP)가 있습니다. ■ **Class**: 분류 된 QoS 클래스; 프레임이 QCE 와 일치하면 큐에 놓입니다. ■ **DPL**: 우선 순위 제거 단계; 프레임이 QCE 와 일치하면 DP 레벨은 DPL 열 아래에 표시된 값으로 설정됩니다. ■ **DSCP**: 프레임이 QCE 와 일치하면 DSCP 는 DSCP 열 아래 표시된 값으로 분류됩니다..
• **Conflict**	QCL 항목의 충돌 상태를 표시합니다. H / W 자원은 여러 응용 프로그램에서 공유하므로 QCE 를 추가하는 데 필요한 리소스를 사용할 수 없을 수도 있습니다.이 경우 충돌 상태가 '예'로 표시되고 그렇지 않으면 항상 '아니요'입니다. 'Resolve Conflict (충돌 해결)'버튼을 누르면 QCL 항목을 추가하는 데 필요한 하드웨어 리소스를 해제하여 충돌을 해결할 수 있습니다.

버튼

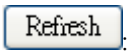


: 이 드롭 다운 목록에서 QCL 상태를 선택하십시오..

Auto-refresh  : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..



: QCL 항목의 충돌 상태가 '예'인 경우 QCL 항목을 추가 시 필요한 자원을 클릭하여 해제하십시오..



: 페이지를 새로 고칩니다.

4.9.13 Storm Control Configuration

스위치에 대한 스톰 제어가이 페이지에서 구성됩니다. 유니 캐스트 스톰 율 제어, 멀티 캐스트 스톰 율 제어 및 브로드 캐스트 스톰 율 제어가 있습니다. 이는 플러딩 된 프레임, 즉 MAC 주소 테이블에 존재하지 않는 (VLAN ID, DMAC) 쌍이있는 프레임에만 영향을줍니다.

구성은 스위치에서 유니 캐스트, 멀티 캐스트 또는 브로드 캐스트 트래픽에 대해 허용 된 패킷 속도를 나타냅니다.

그림 4-9-15 의 Storm Control Configuration 화면이 나타납니다.

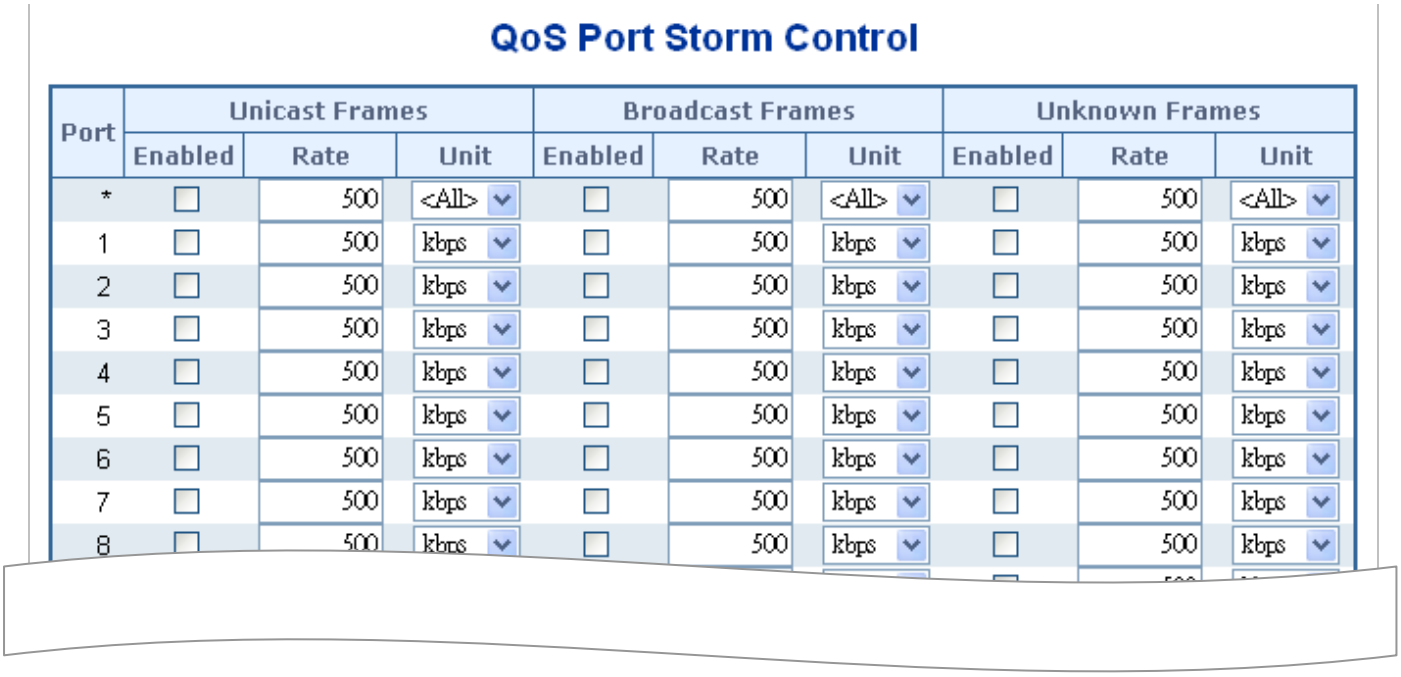


그림 4-9-15: Storm Control Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	아래 구성이 적용되는 포트 번호 입니다.
• **Enable**	이 스위치 포트에서 Storm Control 기능이 활성화되는지 여부를 제어합니다.
• **Rate**	Storm Control 기능의 속도를 제어합니다. 기본값은 500 입니다.이 값은 "Unit"이 "kbps"또는 "fps"일 때 100-1000000 으로 제한되고 "Unit"가 "Mbps"또는 "kfps"일 때 1-13200 으로 제한됩니다.
• **Unit**	Storm rate 에 대한 측정 단위를 kbps, Mbps, fps 또는 kfps 로 제어합니다. 기본값은 "kbps"입니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.9.14 WRED

이 페이지에서는 큐 0 ~ 5 에 RED (Random Early Detection) 설정을 구성 할 수 있습니다. RED 는 큐 6 및 7 에 적용 할 수 없습니다. 큐 (QoS 클래스)에 대해 서로 다른 RED 구성을 통해 가중 임의 조기 발견 WRED) 작업을 수행합니다. 이 설정은 스위치의 모든 포트에 대해 전역입니다. 그림 4-9-16 의 WRED 화면이 나타납니다..

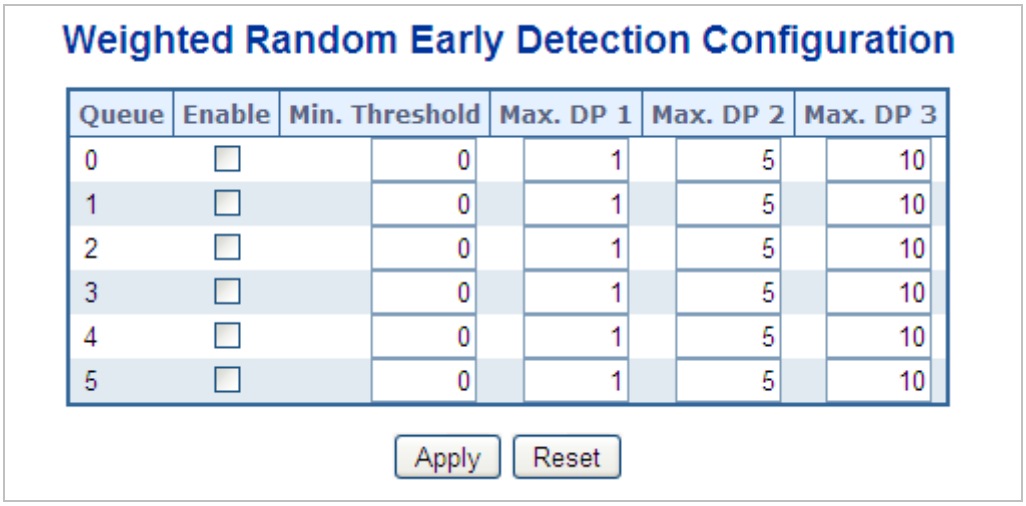


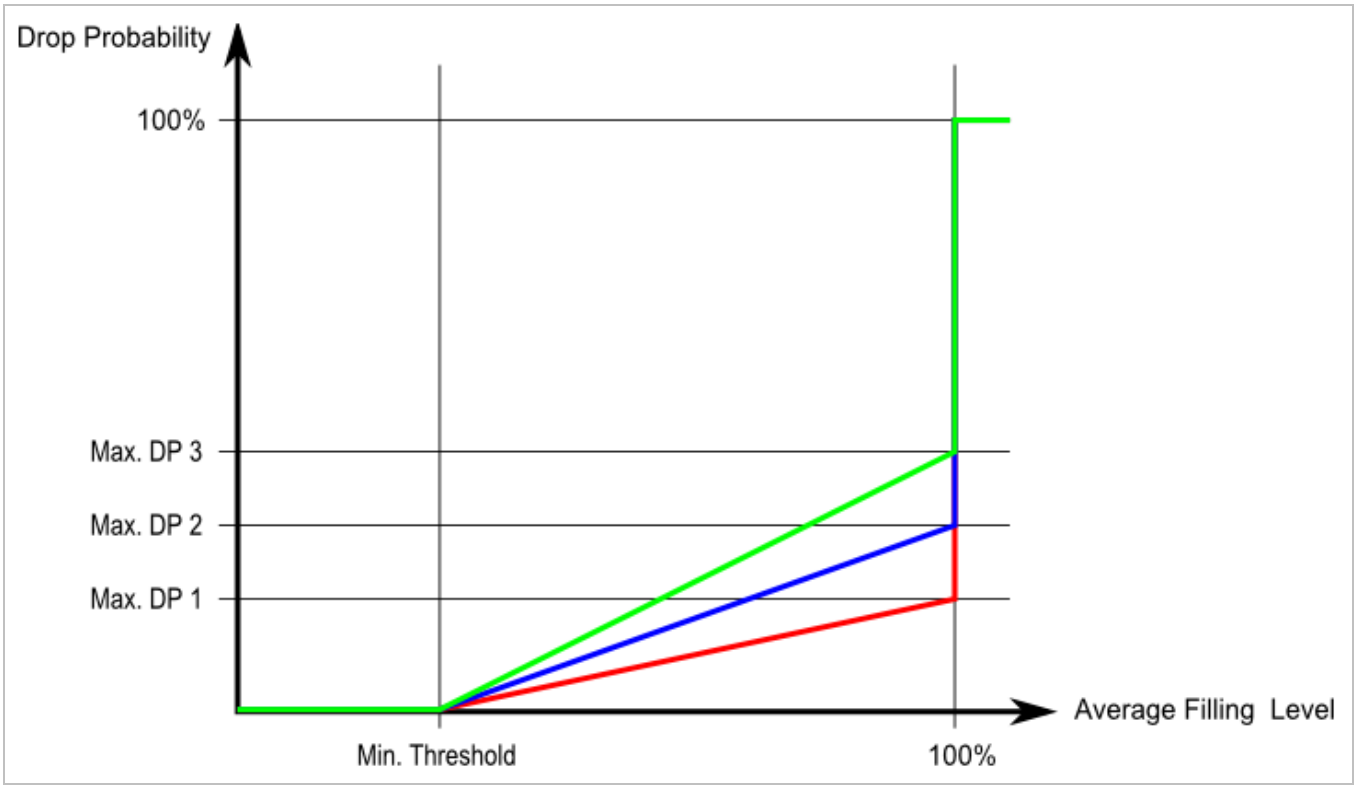
그림 4-9-16 WRED 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Queue**	아래 구성이 적용되는 대기열 번호 (QoS 클래스)입니다.
• **Enable**	이 대기열에 대해 RED 가 활성화되어 있는지 여부를 제어합니다
• **Min. Threshold**	낮은 RED 임계 값을 제어합니다. 평균 대기열 채우기 레벨이이 임계 값보다 낮은 경우, 제거은 0 입니다. 이 값은 0-100 으로 제한됩니다
• **Max. DP 1**	이 값은 0-100 으로 제한됩니다. 평균 대기열 채우기 레벨이 100 % 일 때 놓기 우선 순위 레벨 1 로 표시된 프레임의 충족 속도을 제어합니다.
• **Max. DP2**	평균 대기열 채우기 레벨이 100 % 일 때 놓기 우선 순위 레벨 2 로 표시된 프레임의 놓기 확률을 제어합니다. 이 값은 0-100 으로 제한됩니다.
• **Max. DP3**	평균 대기열 채우기 레벨이 100 % 일 때 놓기 우선 순위 레벨 3 으로 표시된 프레임의 떨어질 확률을 제어합니다. 이 값은 0-100 으로 제한됩니다.

RED Drop Probability Function

다음 그림은 관련 파라미터가 있는 드롭 가능성 함수를 보여 줍니다..



최대치. DP 1-3 은 평균 대기열 채우기 레벨이 100 % 일 때 떨어지는 확률입니다. 놓기 우선 순위 0 으로 표시된 프레임은 절대로 누락되지 않습니다. Min. 임계 값은 대기열에서 임의로 프레임 삭제를 시작하는 평균 대기열 채우기 수준입니다. Drop Precedence Level n 으로 표시된 프레임에 대한 드롭 확률은 0 (최소 임계 값 평균 대기열 채우기 레벨에서)에서 최대로 선형 적으로 증가합니다. DP n (100 % 평균 대기열 채우기 수준).

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.9.15 QoS Statistics

이 페이지는 모든 스위치 포트의 다른 대기열에대한 통계를 입니다. 그림 4-9-17 의 QoS Statistics 화면이 나타납니다..

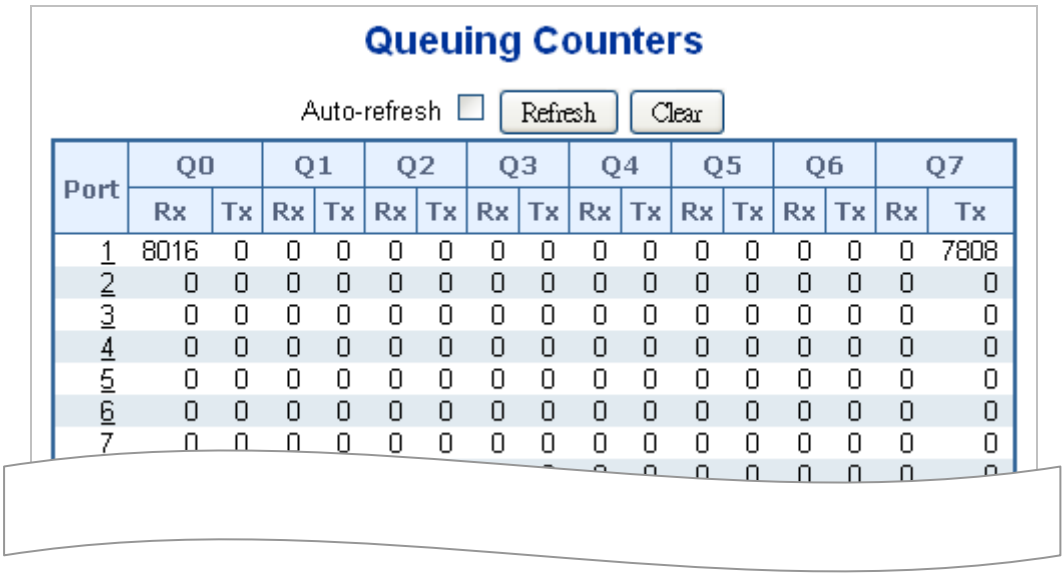


그림 4-9-17: Queuing Counters 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	같은 행에 포함 된 설정의 논리 포트입니다.
• **Q0 ~ Q7**	포트 당 8 개의 QoS 큐가 있습니다. Q0 은 가장 낮은 우선 순위 대기열입니다.
• **Rx/Tx**	큐당 수신 및 전송 된 패킷 수.

버튼

Refresh: 즉시 페이지를 새로고침합니다.

Clear: 모든 포트의 카운터를 지웁니다.

Auto-refresh : 체크박스를 클릭하여 일정시간을 두고 새로고침을 합니다.

4.9.16 Voice VLAN Configuration

음성 VLAN 기능을 사용하면 음성 VLAN 에서 음성 트래픽을 전달할 수 있으며 스위치는 네트워크 트래픽을 분류하고 예약 할 수 있습니다. 한 포트에는 두 개의 VLAN, 즉 음성 및 데이터 용 VLAN 이 권장됩니다.

IP 장비를 스위치에 연결하기 전에 IP 폰은 음성 VLAN ID 를 올바르게 설정해야합니다. 자체 GUI 를 통해 구성해야합니다. 그림 4-9-18 의 음성 VLAN 구성 화면이 나타납니다.

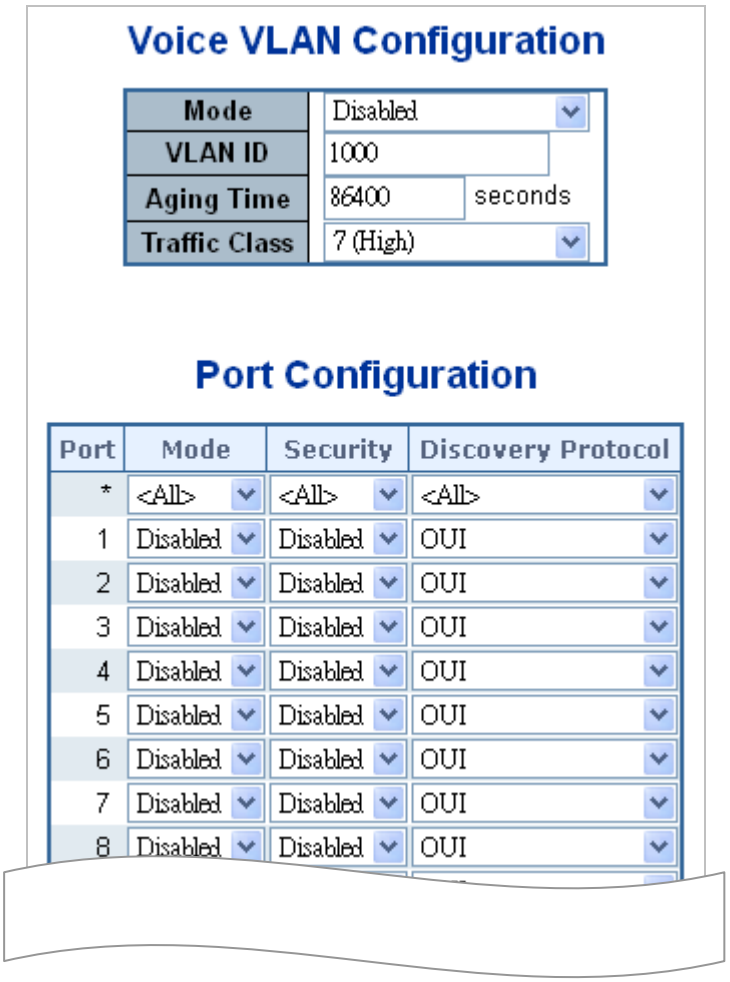


그림 4-9-18: Voice VLAN Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Mode**	음성 VLAN 모드 작동을 나타냅니다. 음성 VLAN 을 활성화하기 전에 MSTP 기능을 비활성화해야합니다. 수신 필터의 충돌을 피할 수 있습니다. 가능한 모드는 다음과 같습니다.: ■ **Enabled**: Voice Vlan 모드를 활성화합니다. ■ **Disabled**: Voice Vlan 모드를 비활성화합니다.
• **VLAN ID**	Voice VLAN ID 를 나타냅니다. 시스템의 고유 한 VLAN ID 여야하며 각 포트 PVID 와 같을 수 없습니다. 가치 관리 VID, MVR VID, PVID 등등과 같은 경우 충돌 구성입니다. 허용되는 범위는 1 ~ 4095 입니다.
• **Aging Time**	Voice VLAN 보안 학습 연령 시간을 나타냅니다. 허용되는 범위는 10 ~ 10000000 초입니다. 보안 모드 또는 자동 감지 모드가 활성화되었을 때 사용됩니다. 다른 경우에는 하드웨어 수명 시간을 기반으로합니다.

	실제 연령대는 [age_time; 2 * age_time] 간격입니다
• **Traffic Class**	Voice Vlan Traffic Class 를 나타냅니다. Voice Vlan 의 모든 트래픽은 class 를 적용합니다.
• **Mode**	Voice VLAN 포트 모드를 나타냅니다. 가능한 포트 모드는 다음과 같습니다. ■ **Disabled**: Voice VLAN.을 사용하지 않습니다. ■ **Auto**: 자동 감지 모드를 사용합니다. 특정 포트에 연결된 VoIP 전화가 있는지 감지하고 음성 VLAN 구성원을 자동으로 구성합니다. ■ **Forced**: Voice VLAN 에 결합합니다..
• **Port Security**	Voice VLAN 포트 보안 모드를 나타냅니다. 이 기능을 사용하면 음성 VLAN 의 모든 비 전화 MAC 주소가 10 초 동안 차단됩니다. 가능한 포트 모드는 다음과 같습니다.: ■ **Enabled**: Enable Voice VLAN security mode operation. ■ **Disabled**: Disable Voice VLAN security mode operation.
• **Port Discovery Protocol**	음성 VLAN 포트 검색 프로토콜을 나타냅니다. 자동 감지 모드가 활성화 된 경우에만 작동합니다. 검색 프로토콜을 "LLDP"또는 "Both"로 구성하기 전에 LLDP 기능을 활성화해야합니다. 검색 프로토콜을 "OUI"또는 "LLDP"로 변경하면 자동 검색 프로세스가 다시 시작됩니다. 가능한 발견 프로토콜은 다음과 같습니다.: ■ **OUI**: OUT 주소로 전화통신 장치를 검색합니다. ■ **LLDP**: LLDP 로 통신장치를 검색합니다.. ■ **Both**: LLDP 와 ■ OUI 를 동시에 적용합니다.

4.9.17 Voice VLAN OUI Table

이 페이지에서 ConfigureVOICE VLAN OUI 표가 있습니다.. 최대 항목 수는 16 입니다. OUI 표를 수정하면 OUI 프로세스 자동 감지가 다시 시작됩니다. 그림 4-9-19 의 음성 VLAN OUI 표 화면이 나타납니다..

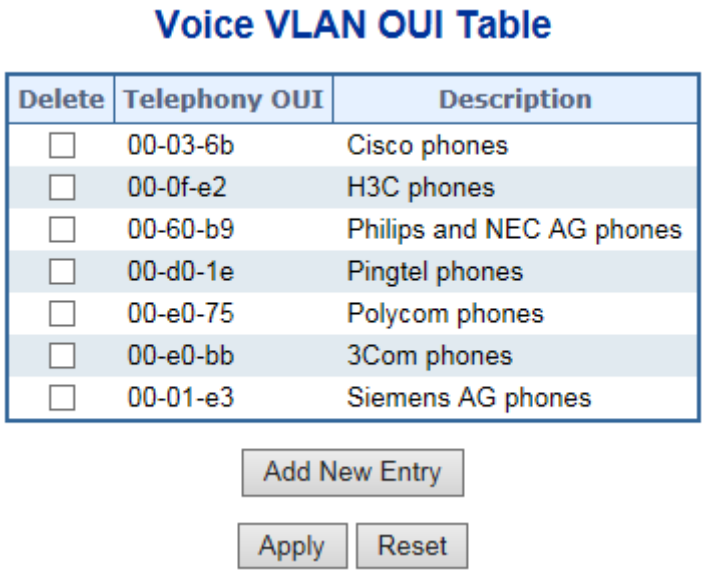


그림 4-9-19: Voice VLAN OUI 표 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제됩니다.
• **Telephony OUI**	전화 통신 OUI 주소는 IEEE 에서 공급 업체에 할당 한 전 세계적으로 고유한 식별자입니다. 6 자 여야하며 입력 형식은 "xx-xx-xx"(x 는 16 진수)입니다.
• **Description**	OUI 주소에 대한 설명. 일반적으로 어떤 벤더 전화 장치가 속해 있는지 설명합니다. 허용되는 문자열 길이는 0 에서 32 사이입니다.

버튼

Add New Entry: 새 액세스 관리 항목을 추가하려면 클릭하십시오.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.10 Access Control Lists

ACL 은 Access Control List (액세스 제어 목록)의 약자입니다. 프로세스 또는 프로그램과 같은 특정 트래픽 목적으로 허용되거나 거부되는 개별 사용자 또는 그룹을 지정하는 액세스 제어 항목을 포함하는 ACE 목록 표입니다.
액세스 가능한 각 트래픽 목적은 ACL 에 대한 식별자를 포함합니다. 권한은 특정 트래픽 액세스 권한이 있는지 여부를 결정합니다.
ACL 구현은 ACE 가 다양한 상황에 우선 순위가 매겨지는 경우와 같이 매우 복잡 할 수 있습니다. 네트워킹에서 ACL 은 호스트 나 서버에서 사용할 수있는 서비스 포트 또는 네트워크 서비스 목록을 말하며 각 목록에는 서비스 사용을 허용 또는 거부 한 호스트 또는 서버 목록이 있습니다. ACL 은 일반적으로 인바운드 트래픽을 제어하도록 구성 될 수 있으며이 내용에서는 방화벽과 유사합니다.

ACE 는 Access Control Entry 의 머리 글자입니다. 특정 ACE ID 와 관련된 액세스 권한을 설명합니다.
세 가지 ACE 프레임 유형 (이더넷 유형, ARP 및 IPv4) 및 두 가지 ACE 작업 (허용 및 거부)이 있습니다. ACE 에는 개별 응용 프로그램에 사용할 수있는 여러 가지 다양한 매개 변수 옵션이 포함되어 있습니다.

4.10.1 Access Control List Status

이 페이지는 여러 ACL 사용자가 ACL 상태를 표시합니다. 각 행은 정의 된 ACE 를 설명합니다. 하드웨어 제한 때문에 특정 ACE 가 하드웨어에 적용되지 않으면 충돌이 발생합니다. 각 ACE 의 최대 수는 512 입니다. 그림 4-10-1 의 음성 VLAN OUI 표 화면이 나타납니다..

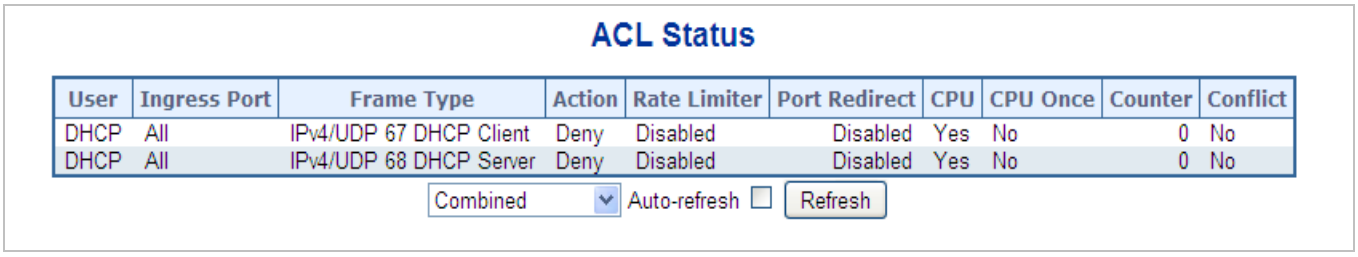


그림 4-10-1: ACL Status 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **User**	ACL 의 사용자를 나타냅니다.
• **Ingress Port**	ACE 의 수신 포트를 나타냅니다. 가능한 값은 다음과 같습니다.: ■ **All**: ACE 가 모든 수신포트와 일치합니다. ■ **Port**: ACE 가 특정 수신포트와 일치합니다.
• **Frame Type**	ACE 의 프레임 유형을 나타냅니다. 가능한 값은 다음과 같습니다.: ■ **Any**: ACE 는 모든 프레임 유형과 일치합니다. ■ **EType**: ACE 는 이더넷 유형 프레임과 일치합니다. 이더넷 유형 기반 ACE 는 IP 및 ARP 프레임과 일치하지 않습니다. ■ **ARP**: ACE 는 ARP / RARP 프레임을 일치시킵니다. ■ **IPv4**: ACE 는 모든 IPv4 프레임과 일치합니다.

	■ **IPv4/ICMP**: ACE 는 IPv4 프레임을 ICMP 프로토콜과 일치시킵니다.. ■ **IPv4/UDP**: ACE 는 IPv4 프레임을 UDP 프로토콜과 일치시킵니다. ■ **IPv4/TCP**: ACE 는 IPv4 프레임을 TCP 프로토콜과 일치시킵니다. ■ **IPv4/Other**: ACE 는 ICMP / UDP / TCP 가 아닌 IPv4 프레임과 일치합니다. ■ **IPv6**: ACE 는 모든 IPv6 표준 프레임과 일치합니다.
• **Action**	ACE 의 전달 작업을 나타냅니다. ■ **Permit**: ACE 와 일치하는 프레임은 전달되고 학습 될 수 있습니다. ■ **Deny**: ACE 와 일치하는 프레임은 삭제됩니다.
• **Rate Limiter**	ACE 의 속도 제한 기 번호를 나타냅니다. 허용 범위는 1 에서 16 까지입니다. Disabled 가 표시되면 속도 제한 기 작동이 비활성화됩니다.
• **Port Redirect**	ACE 의 포트 리디렉션 작업을 나타냅니다. ACE 와 일치하는 프레임은 포트 번호로 리디렉션됩니다. 허용되는 값은 Disabled 또는 특정 포트 번호입니다. Disabled 가 표시되면 포트 재 지정 작업이 비활성화됩니다..
• **Mirror**	이 포트의 미러 작동을 지정하십시오. 허용되는 값은 다음과 같습니다.: ■ **Enabled**: 포트에서 수신 된 프레임이 미러링됩니다. ■ **Disabled**: 포트에서 수신 된 프레임은 미러링되지 않습니다.
• **CPU**	특정 ACE 와 CPU 를 일치시킨 패킷을 전달합니다.
• **CPU Once**	특정 ACE 와 CPU 가 일치하는 첫 번째 패킷을 전달합니다.
• **Counter**	카운터는 ACE 에 프레임이 도달 한 횟수를 나타냅니다.
• **Conflict**	특정 ACE 의 하드웨어 상태를 나타냅니다. 특정 ACE 는 하드웨어 제한으로 인해 하드웨어에 적용되지 않습니다.

버튼

Auto-refresh  : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

: 페이지를 새로 고칩니다.

4.10.2 Access Control List Configuration

이 페이지에는이 스위치에 정의 된 ACE 로 구성된 액세스 제어 목록 (ACL)이 표시됩니다. 각 행은 정의 된 ACE 를 설명합니다. 각 ACE 의 최대 수는 512 입니다.

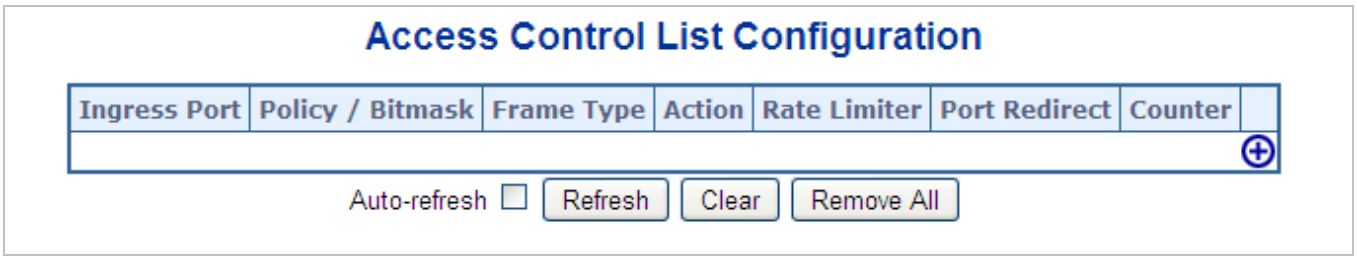


그림 4-10-2: Access Control List Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

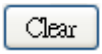
목적	설명
• **Ingress Port**	ACE 의 수신 포트를 나타냅니다. 가능한 값은 다음과 같습니다: ■ **All**: ACE 는 모든 출입포트와 일치합니다 ■ **Port**: ACE 는 특정 출입포트와 일치합니다.
• **Policy / Bitmask**	ACE 는 bit 마스크와 정책을 일치시켜야합니다.
• **Frame Type**	ACE 의 프레임 유형을 나타냅니다. 가능한 값은 다음과 같습니다.: ■ **Any**: ACE 는 모든 프레임 유형과 일치합니다. ■ **EType**: ACE 는 이더넷 유형 프레임과 일치합니다. 이더넷 유형 기반 ACE 는 IP 및 ARP 프레임과 일치하지 않습니다. ■ **ARP**: ACE 는 ARP / RARP 프레임을 일치시킵니다. ■ **IPv4**: ACE 가 모든 IPv4 프레임과 일치합니다. ■ **IPv4/ICMP**: IPv4 프레임을 ICMP 프로토콜과 일치시킵니다. ■ **IPv4/UDP**: ACE 는 IPv4 프레임을 UDP 프로토콜과 일치시킵니다. ■ **IPv4/TCP**: ACE 는 IPv4 프레임을 TCP 프로토콜과 일치시킵니다 ■ **IPv4/Other**: ACE 는 ICMP / UDP / TCP 가 아닌 IPv4 프레임과 일치합니다. ■ **IPv6**: ACE 는 모든 IPv6 표준 프레임과 일치합니다.
• **Action**	ACE 의 전달 작업을 나타냅니다. ■ **Permit**: ACE 와 일치하는 프레임을 전달하고 학습 할 수 있습니다. ■ **Deny**: ACE 와 일치하는 프레임이 삭제됩니다.
• **Rate Limiter**	ACE 의 속도 제한 기 번호를 나타냅니다. 허용 범위는 1 에서 16 까지입니다. Disabled 가 표시되면 속도 제한 기 작동이 비활성화됩니다.
• **Port Redirect**	ACE 의 포트 리디렉션 작업을 나타냅니다. ACE 와 일치하는 프레임은 포트 번호로 리디렉션됩니다. 허용되는 값은 Disabled 또는 특정 포트 번호입니다. Disabled (비활성화)가 표시되면 포트 재 지정 작업이 비활성화됩니다.

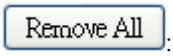
• **Counter**	카운터로 ACE 에 프레임이 도달 한 횟수를 나타냅니다.
• **Modification Button**	다음 버튼을 사용하여 표의 각 ACE (액세스 제어 항목)를 수정할 수 있습니다:  : 현재 행 앞에 새 ACE 를 삽입합니다.  : ACE 행을 편집합니다.  : ACE 를 목록 위로 이동합니다.  : ACE 를 목록 아래로 이동합니다.  : ACE 를 삭제합니다.  : 하단의 더하기 기호는 ACE 목록 맨 아래에 새 항목을 추가합니다.

버튼

Auto-refresh  : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

 : 미완성된 목록을 지우고 다시 새로 고침합니다.

 : 카운터 기록을 모두 제거합니다.

 : ACE 기능으 모두 제거합니다.

4.10.3 ACE Configuration

이 페이지에서 ACE (액세스 제어 항목)를 구성하십시오. ACE 는 여러 매개 변수로 구성됩니다. 이 매개 변수는 선택한 프레임 유형에 따라 다릅니다. 먼저 ACE 의 수신 포트를 선택한 다음 프레임 유형을 선택하십시오. 선택한 프레임 유형에 따라 다른 매개 변수 옵션이 표시됩니다. 이 ACE 에 도달하는 프레임은 여기에 정의 된 구성과 일치합니다. 그림 4-10-3 의 ACE Configuration 화면이 나타납니다.

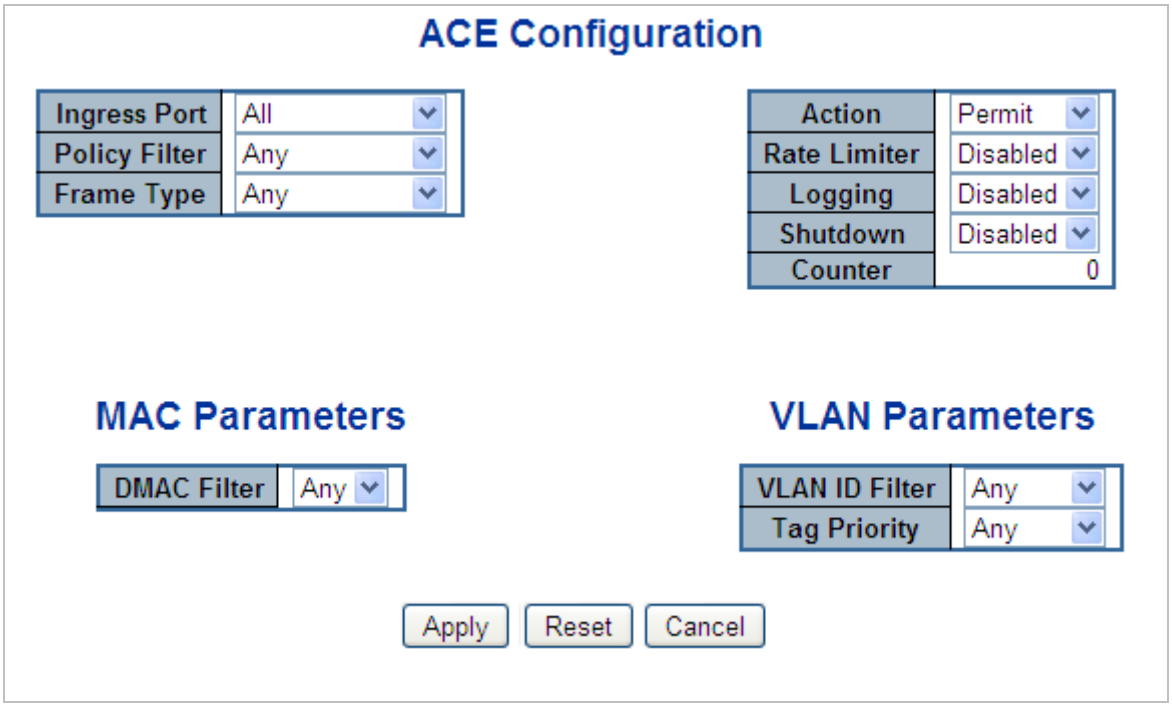


그림 4-10-3: ACE Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Ingress Port**	이 ACE 가 적용되는 수신 포트를 선택하십시오. ■ **Any**: 어떤 포트에도 ACE 가 적용됩니다. ■ **Port n**: ACE 는이 포트 번호에 적용됩니다. 여기서 n 은 스위치 포트의 번호입니다.
• **Policy Filter**	이 ACE 에 대한 지정 정책 번호를 필터합니다. ■ **Any**: 필터하지 않습니다.('유후"상태입니다) ■ **Specific**: 이 ACE 로 특정 정책을 필터링하려면이 값을 선택하십시오. 정책 값을 입력하기위한 두 개의 필드와 비트 마스크가 나타납니다.
• **Policy Value**	정책 필터에 대해 "Specific"을 선택한 경우 특정 정책 값을 입력 할 수 있습니다. 허용되는 범위는 0 에서 255 까지입니다.
• **Policy Bitmask**	정책 필터에 대해 "Specific"을 선택한 경우 특정 정책 비트 마스크를 입력 할 수 있습니다. 허용되는 범위는 0x0 에서 0xff 입니다.
• **Frame Type**	이 ACE 의 프레임 유형을 선택하십시오. 이 프레임 유형은 상호 배타적입니다.. ■ **Any**: 모든 프레임은이 ACE 와 일치 할 수 있습니다..

	■ **Ethernet Type**: 이더넷 유형 프레임 만이 ACE 와 일치 할 수 있습니다. IEEE 802.3 은 길이 / 유형 필드 사양의 값이 1536 십진수 (1600 16 진수)와 같거나 크다고 설명합니다. ■ **ARP**: ARP 프레임 만이 ACE 와 일치 할 수 있습니다. ARP 프레임은 이더넷 유형의 ACE 와 일치하지 않습니다. ■ **IPv4**: IPv4 프레임 만이 ACE 와 일치 할 수 있습니다. IPv4 프레임은 이더넷 유형의 ACE 와 일치하지 않습니다. ■ **IPv6**: IPv6 프레임 만이 ACE 와 일치 할 수 있습니다. IPv6 프레임이 ACE 를 이더넷 유형과 일치시키지 않습니다.
• **Action**	이 ACE 에 도달하는 프레임에서 수행 할 동작을 지정하십시오.. ■ **Permit**: ACE 에 도달하는 프레임에 ACE 작업에 대한 권한이 부여됩니다. ■ **Deny**: 이 ACE 에 도달하는 프레임이 삭제됩니다.
• **Rate Limiter**	속도 제한기를 기본 단위 수로 지정하십시오. 허용되는 범위는 1 - 16 입니다. Disabled 는 속도 제한 기 작동이 비활성화됨을 나타냅니다.
• **Port Redirect**	ACE 에 도달 한 프레임은 여기에 지정된 포트 번호로 리디렉션됩니다. 허용되는 범위는 스위치 포트 번호 범위와 동일합니다. Disabled 는 포트 리디렉션 작업이 비활성화되었음을 나타냅니다.
• **Logging**	ACE 의 로깅 작업을 지정하십시오. 허용되는 값은 다음과 같습니다: ■ **Enabled**: ACE 와 일치하는 프레임은 시스템 로그에 저장됩니다. ■ **Disabled**: ACE 와 일치하는 프레임은 기록되지 않습니다. **노트** : 로깅 기능은 패킷 길이가 1518 미만 (VLAN 태그 없음)이고 시스템 로그 메모리 크기 및 로깅 속도가 제한되어있는 경우에만 작동합니다
• **Shutdown**	ACE 의 포트 종료 작동을 지정하십시오. 허용되는 값은 다음과 같습니다.: ■ **Enabled**: 프레임이 ACE 와 일치하면 수신 포트가 비활성화됩니다. ■ **Disabled**: 포트 종료는 ACE 에 대해 비활성화됩니다. **Note**: 종료 기능은 패킷 길이가 1518 미만 (VLAN 태그 없음) 인 경우에만 작동합니다.
• **Counter**	카운터는 ACE 에 프레임이 도달 한 횟수를 나타냅니다.

■ **MAC Parameters**

목적	설명
• **SMAC Filter**	(프레임 유형이 이더넷 유형 또는 ARP 인 경우에만 표시됨) 이 ACE 에 대한 소스 MAC 필터를 지정하십시오. ■ **Any**: SMAC 필터가 지정되지 않았습니다. (SMAC 상태는 "유후"입니다.) ■ **Specific**: 이 ACE 로 특정 소스 MAC 주소를 필터링하려면이 값을 선택하십시오. SMAC 값을 입력하는 필드가 나타납니다.
• **SMAC Value**	SMAC 필터에 대해 "Specific"을 선택한 경우 특정 소스 MAC 주소를 입력 할 수 있습니다. 유효한 형식은 "xx-xx-xx-xx-xx-xx"또는 "xx.xx.xx.xx.xx.xx"또는 "xxxxxxxxxxxx"입니다 (x 는 16 진수입니다). 이 ACE 를 치는 프레임이이 SMAC 값과 일치합니다.
• **DMAC Filter**	이 ACE 에 대한 대상 MAC 필터를 지정하십시오.. ■ **Any**: DMAC 필터가 지정되지 않습니다. (DMAC 필터 상태는 "유후" ■ **MC**:프레임이 멀티케스트되어야 합니다. ■ **BC**:프레임이 브로드 캐스트되어야 합니다 ■ **UC**: 프레임이 유니캐스트이어야 합니다. ■ **Specific**: 이 ACE 로 특정 대상 MAC 주소를 필터링하려면이 값을 선택하십시오. DMAC 값을 입력하는 필드가 나타납니다.
• **DMAC Value**	DMAC 필터에 대해 "Specific"을 선택한 경우 특정 대상 MAC 주소를 입력 할 수 있습니다. 유효한 형식은 "xx-xx-xx-xx-xx-xx"또는 "xx.xx.xx.xx.xx.xx"또는 "xxxxxxxxxxxx"입니다 (x 는 16 진수입니다). 이 ACE 를 치는 프레임이이 DMAC 값과 일치합니다.

■ **VLAN Parameters**

목적	설명
• **VLAN ID Filter**	ACE 에 Vlan ID 필터링을 지정하십시오. ■ **Any**: Vlan ID 필터링을 지정하지 않습니다. ■ **Specific**: ACE 로 특정 VLAN ID 를 필터링하려면이 값을 선택하십시오. VLAN ID 번호를 입력하는 필드가 나타납니다.
• **VLAN ID**	VLAN ID 필터에 대해 "Specific"을 선택한 경우 특정 VLAN ID 번호를 입력 할 수 있습니다. 허용되는 범위는 1 ~ 4095 입니다.이 ACE 에 도달하는 프레임은이 VLAN ID 값과 일치합니다.
• **Tag Priority**	이 ACE 의 태그 우선 순위를 지정하십시오. 이 ACE 를 치는 프레임이이 태그 우선 순위와 일치합니다. 허용되는 숫자 범위는 0 에서 7 까지입니다. 값은 태그 우선 순위가 지정되지 않음을 의미합니다 (태그 우선 순위는 "신경 쓰지 않음"입니다).

■ ARP Parameters

프레임 유형 "ARP"가 선택되면 ARP 매개 변수를 구성 할 수 있습니다..

목적	설명
• **ARP/RARP**	ACE 에 대해 사용 가능한 ARP / RARP opcode (OP) 플래그를 지정하십시오. ■ **Any**: ARP / RARP OP 플래그가 지정되지 않았습니다. ■ **ARP**: ARP / RARP opcode 가 ARP 로 설정되어 있어야합니다. ■ **RARP**: ARP / RARP opcode 가 RARP 로 설정되어 있어야합니다. ■ **Other**: 알 수없는 ARP / RARP Opcode 플래그가 있습니다.
• **Request/Reply**	사용 가능한 ARP / RARP opcode (OP) 플래그를 지정하십시오. ■ **Any**: ARP / RARP OP 플래그가 지정되지 않습니다. (OP 는 "신경 쓰지 않아"입니다.) ■ **Request**: 프레임에 ARP 요청 또는 RARP 요청 OP 플래그가 설정되어 있어야합니다.. ■ **Reply**: 응답 : 프레임에 ARP 응답 또는 RARP 응답 OP 플래그가 있어야합니다.
• **Sender IP Filter**	ACE 에 대한 보낸 사람 IP 필터를 지정하십시오.. ■ **Any**: 보낸 사람 IP 필터가 지정되지 않습니다. ■ **Host**: 보낸 사람 IP 필터가 호스트로 설정됩니다. 나타나는 SIP 주소 필드에 보낸 사람 IP 주소를 지정하십시오. ■ **Network**: 보낸 사람 IP 필터가 네트워크로 설정됩니다. 나타나는 SIP 주소 및 SIP 마스크 필드에 IP 주소와 마스크를 지정하십시오.
• **Sender IP Address**	보낸 사람 IP 필터에 대해 "호스트"또는 "네트워크"를 선택한 경우 특정 보낸 사람 IP 주소를 점으로 구분 된 십진수 표기법으로 입력 할 수 있습니다.
• **Sender IP Mask**	보낸 사람 IP 필터에 대해 "네트워크"를 선택한 경우 특정 보낸 사람 IP 마스크를 점으로 구분 된 10 진수 표기법으로 입력 할 수 있습니다.
• **Target IP Filter**	이 특정 ACE 에 대한 대상 IP 필터를 지정하십시오. ■ **Any**: 대상 IP 필터가 지정되지 않습니다. ■ **Host**: 대상 IP 필터가 호스트로 설정됩니다. 나타나는 Target IP Address 필드에 대상 IP 주소를 지정하십시오. ■ **Network**: 대상 IP 필터가 네트워크로 설정됩니다. 나타나는 대상 IP 주소 및 대상 IP 마스크 필드에 대상 IP 주소와 대상 IP 마스크를 지정하십시오.
• **Target IP Address**	대상 IP 필터에 대해 "호스트"또는 "네트워크"를 선택한 경우 특정 대상 IP 주소를 점으로 구분 된 십진수 표기법으로 입력 할 수 있습니다.
• **Target IP Mask**	대상 IP 필터에 대해 "네트워크"를 선택한 경우 특정 대상 IP 마스크를 점으로 구분 된 십진수 표기법으로 입력 할 수 있습니다.
• **ARP Sender MAC Match**	프레임이 보낸 사람 하드웨어 주소 필드 (SHA) 설정에 따라 동작을 수행 할 수 있는지 여부를 지정합니다.

	■ **0**: SHA 가 SMAC 주소와 같지 않은 ARP 프레임. ■ **1**: SHA 가 SMAC 주소와 동일한 ARP 프레임. ■ **Any**: 모든 값은 허용됩니다.
• **RARP Target MAC Match**	프레임이 대상 하드웨어 주소 필드 (THA) 설정에 따라 동작을 수행 할 수 있는지 여부를 지정합니다. ■ **0**: THA 가 SMAC 주소와 같지 않은 RARP 프레임 ■ **1**: THA 가 SMAC 주소와 동일한 RARP 프레임. ■ **Any**: 모든 값은 허용됩니다
• **IP/Ethernet Length**	프레임이 ARP / RARP 하드웨어 주소 길이 (HLN) 및 프로토콜 주소 길이 (PLN) 설정에 따라 동작을 수행 할 수 있는지 여부를 지정합니다. ■ **0**: HLN 이 이더넷 (0x06)이고 (PLN)이 IPv4 (0x04) 인 ARP / RARP 프레임. ■ **1**: HLN 이 이더넷 (0x06)이고 (PLN)이 IPv4 (0x04) 인 ARP / RARP 프레임. ■ **Any**: 모든 값은 허용됩니다.
• **IP**	프레임이 ARP / RARP 하드웨어 주소 공간 (HRD) 설정에 따라 동작을 수행 할 수 있는지 여부를 지정합니다. ■ **0**: HLD 가 이더넷 (0) 인 ARP / RARP 프레임. ■ **1**: HLD 가 이더넷 (1) 인 ARP / RARP 프레임. ■ **Any**: 모든 값은 허용됩니다.
• **Ethernet**	프레임이 ARP / RARP 프로토콜 주소 공간 (PRO) 설정에 따라 동작을 수행 할 수 있는지 여부를 지정합니다. ■ **0**: PRO 가 IP (0x800)와 다른 ARP / RARP 프레임 ■ **1**: PRO 가 IP (0x800)와 동일한 ARP / RARP 프레임 ■ **Any**: 모든값은 허용됩니다.

■ IP Parameters

프레임 유형 "IPv4"가 선택되면 IP 매개 변수를 구성 할 수 있습니다.

목적	설명
• **IP Protocol Filter**	ACE 에 대한 IP 프로토콜 필터를 지정하십시오. ■ **Any**: IP 프로토콜 필터가 지정되어 있지 않습니다. ■ **Specific**: ACE 로 특정 IP 프로토콜 필터를 필터링하려면이 값을 선택하십시오. IP 프로토콜 필터 입력 필드가 나타납니다. ■ **ICMP**: ICMP 를 선택하여 IPv4 ICMP 프로토콜 프레임을 필터링합니다. ICMP 매개 변수를 정의하기위한 추가 필드가 나타납니다. 이 필드는이 도움말 파일의 뒷부분에서 설명합니다. ■ **UDP**: IPv4 UDP 프로토콜 프레임을 필터링하려면 UDP 를 선택하십시오. UDP 매개 변수를 정의하기위한 추가 필드가 나타납니다. 이 필드는이 도움말 파일의 뒷부분에서 설명합니다.

	■ **TCP**: IPv4 TCP 프로토콜 프레임을 필터링하려면 TCP 를 선택하십시오. TCP 매개 변수를 정의하기위한 추가 필드가 나타납니다. 이 필드는이 도움말 파일의 뒷부분에서 설명합니다
• **IP Protocol Value**	IP 프로토콜 값으로 "Specific"을 선택한 경우 특정 값을 입력 할 수 있습니다. 허용되는 범위는 0 에서 255 까지입니다.이 ACE 에 도달하는 프레임이이 IP 프로토콜 값과 일치합니다.
• **IP TTL**	이 ACE 의 TTL (Time-To-Live) 설정.. ■ **zero**: TTL 필드가 0 보다 큰 IPv4 프레임은이 항목과 일치 할 수 없어야합니다. ■ **non-zero**: 0 보다 큰 TTL (Time to Live) 필드가있는 IPv4 프레임이이 항목과 일치 할 수 있어야합니다. ■ **Any**: 모든 값을 허용합니다.
• **IP Fragment**	이 ACE 에 대한 조각 오프셋 설정을 지정합니다. 여기에는 IPv4 프레임의 MF (More Fragments) 비트 및 Fragment Offset (FRAG OFFSET) 필드에 대한 설정이 포함됩니다. ■ **No**: MF 비트가 설정되거나 FRAG OFFSET 필드가 0 보다 큰 IPv4 프레임은이 항목과 일치 할 수 없어야합니다. ■ **Yes**: MF 비트가 설정되거나 FRAG OFFSET 필드가 0 보다 큰 IPv4 프레임은이 항목과 일치 할 수 있어야합니다.. ■ **Any**: 값을 모두 허용합니다.
• **IP Option**	ACE 에 대한 옵션 플래그 설정을 지정하십시오. ■ **No**: 옵션 플래그가 설정된 IPv4 프레임은이 항목과 일치 할 수 없어야합니다. ■ **Yes**: 옵션 플래그가 설정된 IPv4 프레임은이 항목과 일치 할 수 있어야합니다. ■ **Any**: 모든 값을 허용합니다.
• **SIP Filter**	ACE 에 대한 원본 IP 필터를 지정하십시오. ■ **Any**: 소스 IP 필터가 지정되지 않습니다. ■ **Host**: 소스 IP 필터가 호스트로 설정됩니다. 나타나는 SIP 주소 필드에 원본 IP 주소를 지정하십시오.. ■ **Network**: 소스 IP 필터가 네트워크로 설정됩니다. 나타나는 SIP 주소 및 SIP 마스크 필드에 원본 IP 주소와 원본 IP 마스크를 지정하십시오.
• **SIP Address**	소스 IP 필터에 대해 "호스트"또는 "네트워크"를 선택한 경우 특정 SIP 주소를 점으로 구분 된 십진수 표기법으로 입력 할 수 있습니다.
• **SIP Mask**	소스 IP 필터에 대해 "네트워크"가 선택되면 점으로 구분 된 10 진수 표기법으로 특정 SIP 마스크를 입력 할 수 있습니다.
• **DIP Filter**	ACE 에 대한 대상 IP 필터를 지정하십시오.. ■ **Any**: IP 필터를 지정하지 않습니다. ■ **Host**: 목적 IP 필터가 호스트로 설정됩니다. 나타나는 DIP 주소 필드에

	대상 IP 주소를 지정하십시오. ■ **Network**: 목적 IP 필터가 네트워크로 설정됩니다. 나타나는 DIP 주소 및 DIP 마스크 필드에 대상 IP 주소 및 대상 IP 마스크를 지정하십시오.
• **DIP Address**	목적지 IP 필터에 대해 "호스트"또는 "네트워크"를 선택한 경우 특정 DIP 주소를 점으로 구분 된 십진수 표기법으로 입력 할 수 있습니다.
• **DIP Mask**	목적 IP 필터에 대해 "네트워크"를 선택한 경우 점으로 구분 된 10 진수 표기법으로 특정 DIP 마스크를 입력 할 수 있습니다.

■ **IPv6 Parameters**

목적	설명
• **Next Header Fliter**	ACE 에 대한 IPv6 다음 헤더 필터를 지정하십시오.. ■ **Any**: IPv6 헤더필터를 지정하지 않습니다. ■ **Specific**: ACE 와 함께 특정 IPv6 다음 헤더 필터를 필터링하려면이 값을 선택하십시오. IPv6 다음 머리글 필터를 입력하기위한 필드가 나타납니다. ■ **ICMP**: ICMP 를 선택하여 IPv6 ICMP 프로토콜 프레임을 필터링합니다. ICMP 매개 변수를 정의하기위한 추가 필드가 나타납니다. 이 필드는이 도움말 파일의 뒷부분에서 설명합니다 ■ **UDP**: IPv6 UDP 프로토콜 프레임을 필터링하려면 UDP 를 선택하십시오. UDP 매개 변수를 정의하기위한 추가 필드가 나타납니다. 이 필드는이 도움말 파일의 뒷부분에서 설명합니다. ■ **TCP**: IPv6 TCP 프로토콜 프레임을 필터링하려면 TCP 를 선택하십시오. TCP 매개 변수를 정의하기위한 추가 필드가 나타납니다. 이 필드는이 도움말 파일의 뒷부분에서 설명합니다
• **Next Header Value**	IPv6 다음 헤더 값으로 "특정"을 선택한 경우 특정 값을 입력 할 수 있습니다. 허용되는 범위는 0 에서 255 까지입니다.이 ACE 에 도달하는 프레임은이 IPv6 프로토콜 값과 일치합니다
• **SIP Filter**	ACE 에 대한 소스 IPv6 필터를 지정하십시오. ■ **Any**: 소스 IPv6 필터가 지정되지 않습니다. ■ **Specific**: 소스 IPv6 필터가 네트워크로 설정됩니다. 표시되는 SIP 주소 필드에 소스 IPv6 주소와 소스 IPv6 마스크를 지정하십시오.
• **SIP Address**	소스 IPv6 필터에 대해 "Specific"을 선택한 경우 특정 SIPv6 주소를 입력 할 수 있습니다. 이 필드는 IPv6 주소의 마지막 32 비트 만 지원했습니다.
• **SIP BitMask**	소스 IPv6 필터에 대해 "특정"을 선택한 경우 특정 SIPv6 마스크를 입력 할 수 있습니다. 필드는 IPv6 주소의 마지막 32 비트 만 지원했습니다. 비트 마스크의 사용법을 확인합니다. 값이 "0"이면 유후상태를 의미합니다. 실제 일치 패턴은 [sipv6_address & sipv6_bitmask] (마지막 32 비트)입니다. 예를 들어, SIPv6 주소가 2001 :: 3 이고 SIPv6 비트 마스크가 0xFFFFFFFE 인

	경우 (비트 0 이 "신경 쓰지 않음"비트 인 경우) SIPv6 주소 2001 :: 2 및 2001 :: 3 이이 규칙에 적용됩니다.
• **Hop Limit**	ACE 에 대한 홉 한계 설정을 지정하십시오.. ■ **zero**: 홉 한계 필드가 0 보다 큰 IPv6 프레임은이 항목과 일치 할 수 없어야합니다. ■ **non-zero**: 0 보다 큰 홉 수 제한 필드가있는 IPv6 프레임은이 항목과 일치 할 수 있어야합니다.. ■ **Any**: 모든 값을 허용합니다.

■ **ICMP Parameters**

목적	설명
• **ICMP Type Filter**	ACE 에 대한 ICMP 필터를 지정하십시오. ■ **Any**: ICMP 필터가 지정되지 않습니다. ■ **Specific**: ACE 로 특정 ICMP 필터를 필터링하려면 특정 ICMP 값을 입력하면됩니다. ICMP 값 입력 필드가 나타납니다.
• **ICMP Type Value**	ICMP 필터에 대해 "특정"을 선택하면 특정 ICMP 값을 입력 할 수 있습니다. 허용되는 범위는 0 에서 255 까지입니다.이 ACE 에 도달하는 프레임이이 ICMP 값과 일치합니다.
• **ICMP Code Filter**	ACE 에 대한 ICMP 코드 필터를 지정하십시오. ■ **Any**: ICMP 코드 필터가 지정되지 않습니다. ■ **Specific**: ACE 로 특정 ICMP 코드 필터를 필터링하려면 특정 ICMP 코드 값을 입력 할 수 있습니다. ICMP 코드 값을 입력하는 필드가 나타납니다.
• **ICMP Code Value**	ICMP 코드 필터에 대해 "특정"이 선택되면 특정 ICMP 코드 값을 입력 할 수 있습니다. 허용되는 범위는 0 에서 255 까지입니다.이 ACE 에 도달하는 프레임이이 ICMP 코드 값과 일치합니다.

■ **TCP/UDP Parameters**

목적	설명
• **TCP/UDP Source Filter**	ACE 에 대한 TCP / UDP 원본 필터를 지정하십시오. ■ **Any**: TCP / UDP 원본 필터가 지정되지 않았습니다 ■ **Specific**: ACE 로 특정 TCP / UDP 원본 필터를 필터링하려면 특정 TCP / UDP 원본 값을 입력 할 수 있습니다. TCP / UDP 소스 값을 입력하는 필드가 나타납니다.. ■ **Range**: ACE 로 특정 TCP / UDP 원본 범위 필터를 필터링하려면 특정

	TCP / UDP 원본 범위 값을 입력 할 수 있습니다. TCP / UDP 소스 값을 입력하는 필드가 나타납니다.
• **TCP/UDP Source No.**	TCP / UDP 소스 필터에 대해 "특정"이 선택되면 특정 TCP / UDP 소스 값을 입력 할 수 있습니다. 허용되는 범위는 0 ~ 65535 입니다.이 ACE 에 도달하는 프레임이이 TCP / UDP 원본 값과 일치합니다.
• **TCP/UDP Source Range**	TCP / UDP 소스 필터에 대해 "Range"가 선택되면 특정 TCP / UDP 소스 범위 값을 입력 할 수 있습니다. 허용되는 범위는 0 ~ 65535 입니다.이 ACE 에 도달하는 프레임이이 TCP / UDP 원본 값과 일치합니다.
• **TCP/UDP Destination Filter**	ACE 에 대한 TCP / UDP 대상 필터를 지정하십시오.. ■ **Any**: TCP / UDP 대상 필터가 지정되지 않습니다 (TCP / UDP 대상 필터 상태는 "주의하지 않음"). ■ **Specific**: ACE 와 함께 특정 TCP / UDP 대상 필터를 필터링하려면 특정 TCP / UDP 대상 값을 입력 할 수 있습니다. TCP / UDP 대상 값을 입력하는 필드가 나타납니다. ■ **Range**: ACE 와 함께 특정 범위의 TCP / UDP 대상 필터를 필터링하려면 특정 TCP / UDP 대상 범위 값을 입력 할 수 있습니다. TCP / UDP 대상 값을 입력하는 필드가 나타납니다.
• **TCP/UDP Destination Number**	TCP / UDP 대상 필터에 대해 "특정"을 선택한 경우 특정 TCP / UDP 대상 값을 입력 할 수 있습니다. 허용되는 범위는 0 ~ 65535 입니다.이 ACE 에 도달하는 프레임이이 TCP / UDP 대상 값과 일치합니다
• **TCP/UDP Destination Range**	TCP / UDP 대상 필터에 대해 "범위"를 선택한 경우 특정 TCP / UDP 대상 범위 값을 입력 할 수 있습니다. 허용되는 범위는 0 ~ 65535 입니다.이 ACE 에 도달하는 프레임이이 TCP / UDP 대상 값과 일치합니다.
• **TCP FIN**	ACE 에 대해 TCP "전송자로부터 데이터가 없습니다"(FIN) 값을 지정하십시오.. ■ **0**: FIN 필드가 설정된 TCP 프레임은이 항목과 일치 할 수 없어야합니다. ■ **1**: FIN 필드가 설정된 TCP 프레임은이 항목과 일치 할 수 있어야합니다 ■ **Any**: 모든 값을 허용합니다.
• **TCP SYN**	ACE 의 TCP "Synchronize sequence numbers"(SYN) 값을 지정하십시오. ■ **0**: SYN 필드가 설정된 TCP 프레임은 이 항목과 일치하지 않습니다.. ■ **1**: SYN 필드가 설정된 TCP 프레임은 이 항목과 일치해야 합니다. ■ **Any**: 모든 값을 허용합니다.
• **TCP RST**	ACE 에 대한 TCP "초기 연결(RST)" 값을 지정하십시오. ■ **0**: RST 필드가 설정된 TCP 프레임은 이 항목과 일치하지 않습니다 ■ **1**: RST 필드가 설정된 TCP 프레임은 이 항목과 일치해야 합니다. ■ **Any**: 모든 값을 허용합니다.
• **TCP PSH**	ACE 에 대한 TCP "푸시 기능"(PSH) 값을 지정하십시오.. ■ **0**: PSH 필드가 설정된 TCP 프레임은 이 항목과 일치하지 않습니다. ■ **1**: PSH 필드가 설정된 TCP 프레임은 이 항목과 일치해야 합니다.

	■ **Any**: 모든 값을 허용합니다.
• **TCP ACK**	ACE 에 대한 TCP "전송신호"(ACK) 값을 지정하십시오. ■ **0**: ACK 필드가 설정된 TCP 프레임은 이 항목과 일치하지 않습니다. ■ **1**: ACK 필드가 설정된 TCP 프레임은 이 항목과 일치해야 합니다. ■ **Any**: 모든 값을 허용합니다.
• **TCP URG**	ACE 에 대한 TCP "Urgent Pointer field significant"(URG) 값을 지정하십시오. ■ **0**: URG 필드가 설정된 TCP 프레임은 이 항목과 일치하지 않습니다. ■ **1**: URG 필드가 설정된 TCP 프레임은 이 항목과 일치해야 합니다. ■ **Any**: 모든 값을 허용합니다.

■ Ethernet Type Parameters

이더넷 유형 매개 변수는 프레임 유형 "이더넷 유형"이 선택 될 때 구성 될 수 있습니다.

목적	설명
• **EtherType Filter**	ACE 에 이더넷 유형 필터를 지정하십시오. ■ **Any**: EtherType 필터가 지정되지 않습니다 (EtherType 필터 상태는 "주의하지 않음"). ■ **Specific**: ACE 로 특정 EtherType 필터를 필터링하려면 특정 EtherType 값을 입력 할 수 있습니다. EtherType 값을 입력하는 필드가 나타납니다.
• **Ethernet Type Value**	EtherType 필터에 대해 "Specific"을 선택한 경우 특정 EtherType 값을 입력 할 수 있습니다. 허용되는 범위는 0x600 에서 0xFFFF 까지이지만 0x800 (IPv4), 0x806 (ARP) 및 0x86DD (IPv6)는 제외됩니다. 이 ACE 를 치는 프레임이이 EtherType 값과 일치합니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

Cancel: 이전 페이지로 되돌아갑니다.

4.10.4 ACL Ports Configuration

각 스위치 포트의 ACL 매개 변수 (ACE)를 구성하십시오. 이 매개 변수는 프레임이 특정 ACE 와 일치하지 않으면 포트에서 수신 된 프레임에 영향을줍니다. 그림 4-10-4 의 ACL Ports Configuration 화면이 나타납니다.

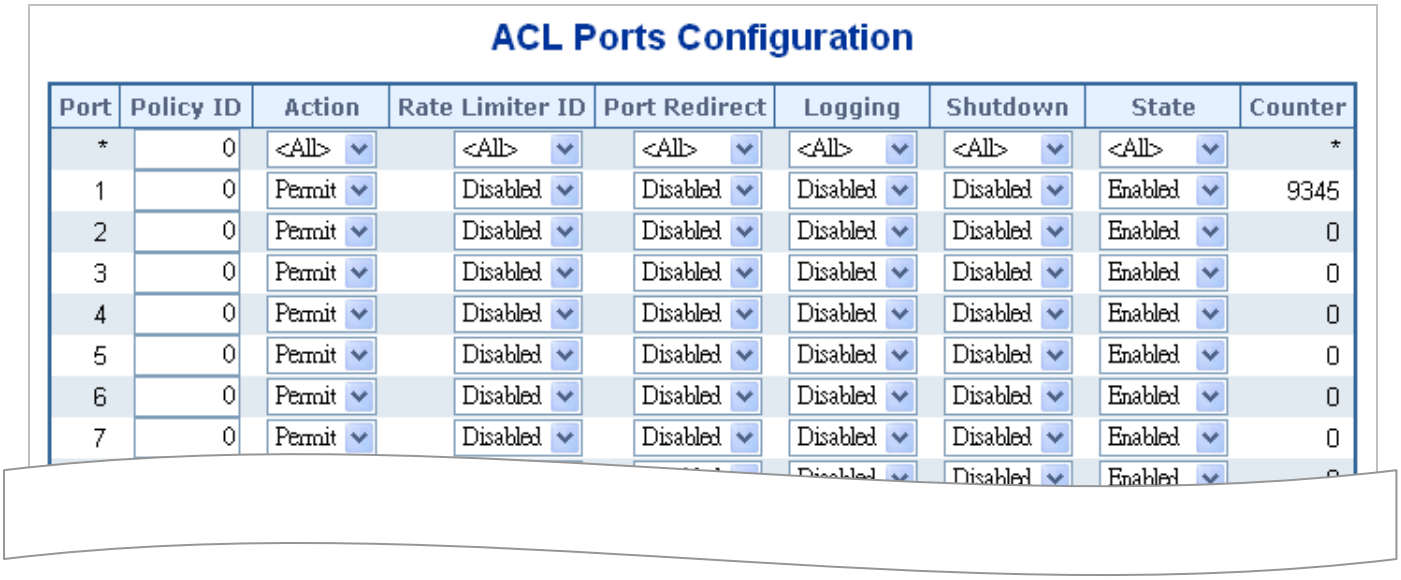


그림 4-10-4: ACL Ports Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	같은 행에 포함 된 설정의 논리 포트입니다.
• **Policy ID**	포트에 적용 할 정책을 선택하십시오. 허용되는 값은 0 에서 255 까지입니다. 기본값은 0 입니다.
• **Action**	전달 허용 ("Permit") 또는 거부 ("Deny") 여부를 선택하십시오. 기본값은 “Permit”다
• **Rate Limiter ID**	포트에 적용 할 속도 제한기를 선택하십시오. 허용되는 값은 Disabled 또는 1 에서 16 사이의 값입니다. 기본값은 "사용 안 함"입니다.
• **Port Redirect**	리디렉션 할 포트 프레임을 선택하십시오. 허용되는 값은 Disabled 또는 특정 포트 번호이며 작업이 허용 될 때 설정할 수 없습니다. 기본값은 "사용 안 함"입니다.
• **Logging**	이 포트의 로그 작업을 지정하십시오. 허용되는 값은 다음과 같습니다.: ■ **Enabled**: 시스템 로그에 저장된 프레임을 받아옵니다. ■ **Disabled**: 포트에서 수신 된 프레임은 기록되지 않습니다. 기본값은 “Disabled”입니다. 시스템 로그 메모리 크기 및 로깅 속도는 제한됩니다.
• **Shutdown**	포트의 포트 종료 작동을 지정하십시오. 허용되는 값은 다음과 같습니다: ■ **Enabled**: 포트에서 프레임을 수신하면 포트에 비활성화됩니다.

	■ **Disabled**: 포트에서 프레임을 수신하면 포트에 활성화됩니다. 기본값은 Disable 입니다.
• **State**	포트의 포트 상태를 지정하십시오. 허용되는 값은 다음과 같습니다: ■ **Enabled**: ACL 사용자 모듈의 휘발성 포트 구성을 변경하여 포트를 다시 열 수 있습니다. ■ **Disabled**: ACL 사용자 모듈의 휘발성 포트 구성을 변경하여 포트를 닫습니다. 기본값은 "Enable"입니다.
• **Counter**	ACE 와 일치하는 프레임 수를 기록합니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

Refresh: 클릭하여 로컬단의 값을 새로고침합니다.

Clear: 클릭하여 숫자값을 초기화합니다.

4.10.5 ACL Rate Limiter Configuration

스위치의 ACL 에 대한 속도 제한기를 구성하십시오.

그림 4-10-5 의 ACL Rate Limiter Configuration 화면이 나타납니다..

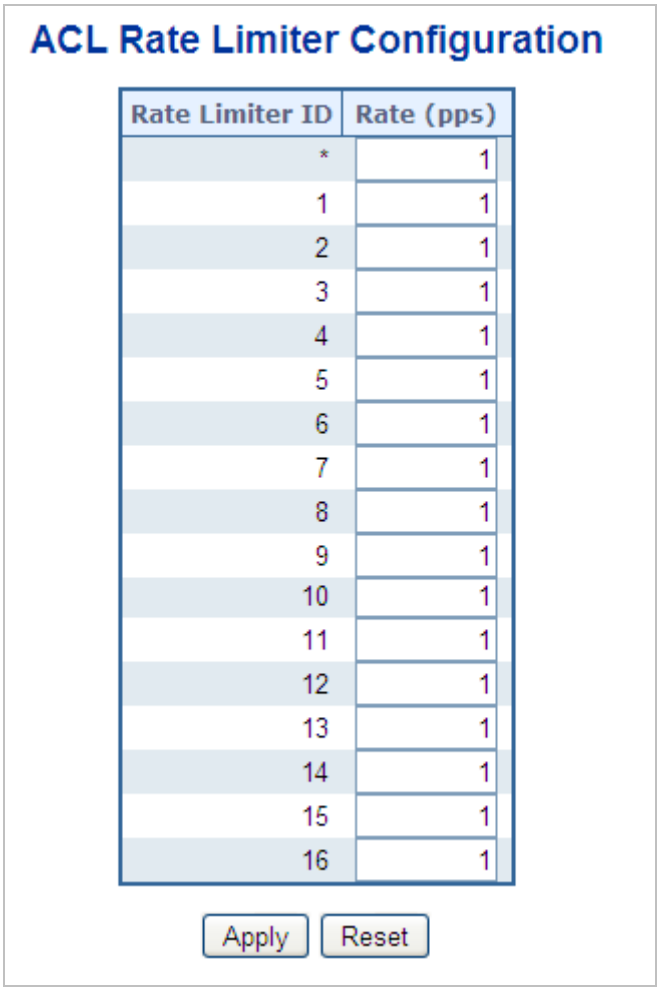


그림 4-10-5: ACL Rate Limiter Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Rate Limiter ID**	같은 행에 포함 된 설정의 속도 제한 기 ID 입니다.
• **Rate (pps)**	허용되는 값은 0-3276700 (pps) 또는 0, 100, 200, 300, ..., 1000000 (kbps)입니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.11 Authentication

이 섹션에서는 사용자 액세스 및 관리 제어를 포함하여 관리 대상 스위치의 액세스를 제어합니다.
인증 섹션에는 다음 주요 주제에 대한 링크가 있습니다.

- **IEEE 802.1X 포트 기반 망 접근 통제**
- **MAC-기반 인증**
- **사용자 인증**

802.1X (Port-Based) 인증 개요

802.1X 환경에서 사용자는 요청자, 스위치는 인증 자, RADIUS 서버는 인증 서버입니다. 스위치는 중간자 (man-in-the-middle) 역할을하여 요청자와 인증 서버간에 요청 및 응답을 전달합니다. 요청자와 스위치간에 전송되는 프레임은 EAPOL (EAP over LANs) 프레임으로 알려진 특수한 802.1X 프레임입니다. EAPOL 프레임은 EAP PDU 를 캡슐화합니다 (RFC3748). 스위치와 RADIUS 서버간에 전송되는 프레임은 RADIUS 패킷입니다. 또한 RADIUS 패킷은 스위치의 IP 주소, 이름 및 요청자의 포트 번호와 같은 다른 속성과 함께 EAP PDU 를 캡슐화합니다. EAP 는 MD5-Challenge, PEAP 및 TLS 와 같은 다양한 인증 방법을 허용한다는 점에서 매우 유연합니다. 중요한 점은 인증 자 (스위치)가 서 플리 컨트 및 인증 서버가 사용하는 인증 방법이나 특정 방법에 필요한 정보 교환 프레임 수를 알 필요가 없다는 것입니다. 스위치는 프레임의 EAP 부분을 관련 유형 (EAPOL 또는 RADIUS)으로 캡슐화하고 전달합니다. 인증이 완료되면 RADIUS 서버는 성공 또는 실패 표시가 포함 된 특수 패킷을 전송합니다. 이 결정을 요청자에게 전달하는 것 외에도 스위치는이를 사용하여 요청자와 연결된 스위치 포트에서 트래픽을 열거 나 차단합니다.

Overview of MAC-Based Authentication

802.1X 와는 달리 MAC 기반 인증은 표준이 아니며 업계에서 채택한 최상의 방법입니다. MAC 기반 인증에서 사용자는 클라이언트라고하며 스위치는 클라이언트를 대신하여 요청자 역할을합니다. 클라이언트가 보낸 초기 프레임 (모든 종류의 프레임)은 스위치에 의해 스누핑되며, 스위치는 RADIUS 서버와의 후속 EAP 교환에서 사용자의 MAC 주소를 사용자 이름과 암호로 사용합니다. 6 바이트 MAC 주소는 "xx-xx-xx-xx-xx-xx"형식의 문자열로 변환됩니다. 즉, 대시 (-)가 하위 케이스의 16 진수 사이의 구분 기호로 사용됩니다. 스위치는 MD5-Challenge 인증 방법 만 지원하므로 RADIUS 서버를 적절하게 구성해야합니다. 인증이 완료되면 RADIUS 서버는 MAC 테이블에 정적 항목을 사용하여 성공 또는 실패 표시를 보내 스위치가 특정 클라이언트에 대한 트래픽을 열거 나 차단하도록합니다. 그래야만 클라이언트의 프레임이 스위치로 전달됩니다. 이 인증에는 EAPOL 프레임이 포함되어 있지 않으므로 MAC 기반 인증은 802.1X 표준과 아무 관련이 없습니다.

802.1X 를 통한 MAC 기반 인증의 이점은 여러 클라이언트를 동일한 포트 (예 : 타사 스위치 또는 허브)에 연결하여 개별 인증이 필요하며 클라이언트가 특정 인증 자 소프트웨어를 필요로하지 않는다는 점입니다 인증. 단점은 MAC 주소가 악의적 인 사용자에 의해 스푸핑 될 수 있으며 MAC 주소가 유효한 RADIUS 사용자 인 장비가 누구에게나 사용될 수 있으며 MD5-Challenge 방법 만 지원된다는 것입니다.
802.1X 및 MAC 기반 인증 구성은 시스템 및 포트와 같은 두 섹션으로 구성됩니다.

텔넷 및 웹 브라우저와 같은 로컬 또는 원격 인증 방법을 사용하여 관리 액세스를 위해 시스템에 로그인하는 사용자를 인증하도록 Managed Switch 를 구성 할 수 있습니다. 이 관리 스위치는 다음 옵션을 사용하여 안전한 네트워크 관리 액세스를 제공합니다.:

- **Remote Authentication Dial-in User Service (RADIUS)**
- **Terminal Access Controller Access Control System Plus (TACACS+)**
- **Local user name 과 Priviledge Level control**

RADIUS 와 **TACACS+는**중앙 서버에서 실행되는 소프트웨어를 사용하여 네트워크에서 RADIUS 인식 또는 TACACS 인식 장치에 대한 액세스를 제어하는 로그온 인증 프로토콜입니다. 인증 서버에는 관리 대상 스위치에 대한 관리 액세스가 필요한 각 사용자에 대한 관련 권한 수준이있는 여러 사용자 이름 / 암호 쌍의 데이터베이스가 있습니다.

4.11.1 IEEE 802.1X 포트기반 인증의 이해

IEEE 802.1X 표준은 권한이없는 클라이언트가 공개적으로 액세스 할 수있는 포트를 통해 LAN 에 연결하는 것을 제한하는 클라이언트 - 서버 기반 액세스 제어 및 인증 프로토콜을 정의합니다. 인증 서버는 스위치 또는 LAN 이 제공하는 서비스를 사용 가능하게하기 전에 스위치 포트에 연결된 각 클라이언트를 인증합니다.

클라이언트가 인증 될 때까지 802.1X 액세스 제어는 클라이언트가 연결된 포트를 통해 EAPOL (Extensible Authentication Protocol over LAN) 트래픽 만 허용합니다. 인증이 성공하면 정상 트래픽이 포트를 통과 할 수 있습니다.

이 섹션에는 다음과 같은 개념 정보가 포함되어 있습니다.

- 장비의 규칙들
- 인증 시작 및 메시지 교환
- 허가 및 허가되지 않은 국가의 항구

■ 장비의 규칙들

802.1X 포트 기반 인증을 사용하면 네트워크의 장치가 아래와 같이 특정 역할을 수행합니다..

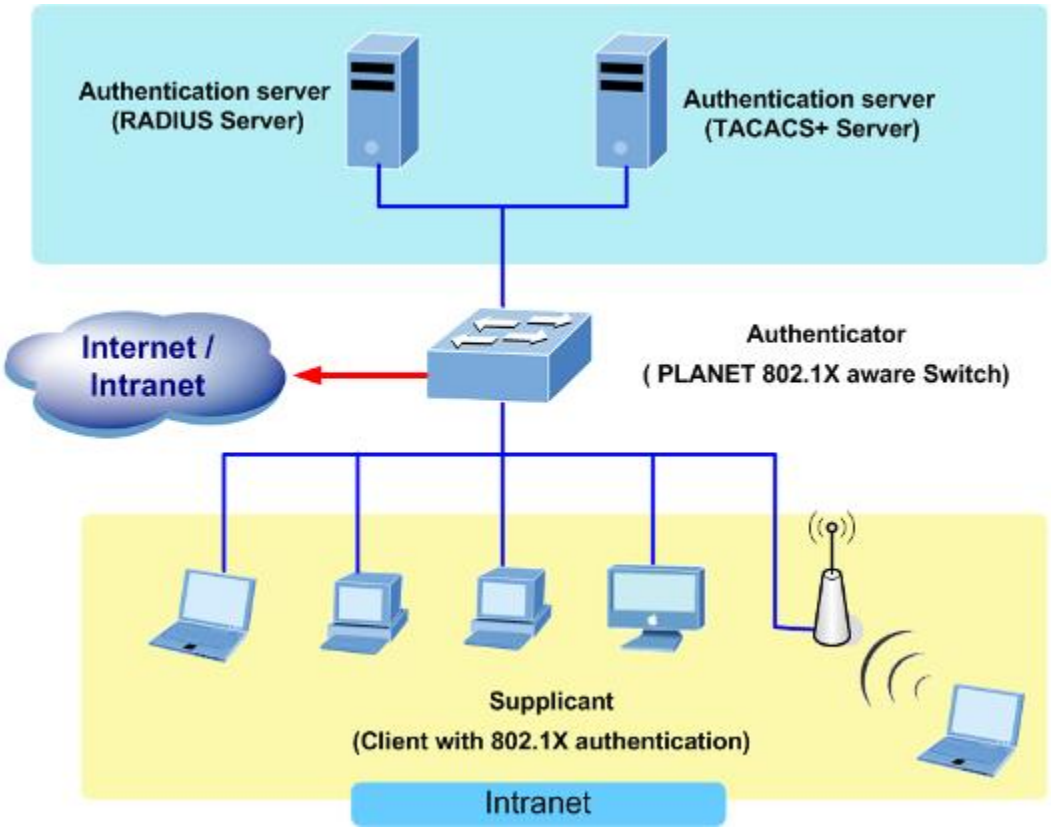


그림 4-11-1

- **Client**— LAN 에 대한 액세스를 요청하고 서비스를 전환하고 스위치의 요청에 응답하는 장치 (워크 스테이션). 워크 스테이션은 Microsoft Windows XP 운영 체제와 같은 802.1X 호환 클라이언트 소프트웨어를 실행하고 있어야합니다. 클라이언트는 IEEE 802.1X 사양의 요청자입니다.

- **Authentication server**— 클라이언트의 실제 인증을 수행합니다. 인증 서버는 클라이언트의 신원을 확인하고 클라이언트가 LAN 에 액세스하고 서비스를 전환 할 권한이 있는지 여부를 스위치에 알립니다. 스위치는 프록시 역할을하기 때문에 인증 서비스는 클라이언트에게 투명합니다. 이 릴리스에서는 EAP (Extensible Authentication Protocol) 확장을 사용하는 RADIUS (Remote Authentication Dial-In User Service) 보안 시스템이 유일하게 지원되는 인증 서버입니다. Cisco Secure Access Control Server 버전 3.0 에서 사용할 수 있습니다. RADIUS 는 RADIUS 서버와 하나 이상의 RADIUS 클라이언트간에 보안 인증 정보가 교환되는 클라이언트 / 서버 모델에서 작동합니다.

- **Switch (802.1X device)**— 클라이언트의 인증 상태를 기반으로 네트워크에 대한 물리적 액세스를 제어합니다. 이 스위치는 클라이언트와 인증 서버 간의 중간 (프록시) 역할을하며 클라이언트로부터 신원 정보를 요청하고 인증 서버와 정보를 확인한 다음 클라이언트에 응답을 중계합니다. 스위치에는 EAP (Extensible Authentication Protocol) 프레임을 캡슐화 및 캡슐 해제하고 인증 서버와 상호 작용하는 RADIUS 클라이언트가 포함됩니다. 스위치가 EAPOL 프레임을 수신하고 인증 서버로 릴레이하면 이더넷 헤더가 제거되고 나머지 EAP 프레임은 RADIUS 형식으로 다시 캡슐화됩니다. EAP 프레임은 캡슐화 중에 수정되거나 검사되지 않으며 인증 서버는 기본 프레임 형식으로 EAP 를 지원해야합니다. 스위치가 인증 서버에서 프레임을 수신하면 서버의 프레임 헤더가 제거되고 EAP 프레임은 이더넷 용으로 캡슐화되어 클라이언트로 전송됩니다.

■ **Authentication Initiation and Message Exchange**

스위치 또는 클라이언트가 인증을 시작할 수 있습니다. dot1x port-control auto interface configuration 명령을 사용하여 포트에서 인증을 사용하는 경우 스위치는 포트 링크 상태가 아래에서 위로 전환 될 때 인증을 시작해야합니다. 그런 다음 EAP 요청 / 신원 프레임을 클라이언트에 보내 신원을 요청합니다 (일반적으로 스위치는 초기 신원 / 요청 프레임을 보내고이어서 인증 정보에 대한 하나 이상의 요청을 보냅니다). 프레임을 수신하면 클라이언트는 EAP- 응답 / 신원 프레임으로 응답합니다.

그러나 부팅 중에 클라이언트가 스위치에서 EAP 요청 / ID 프레임을받지 못하면 클라이언트는 EAPOL 시작 프레임을 전송하여 인증을 시작할 수 있습니다.이 프레임은 클라이언트의 ID 를 요청하도록 스위치에 프롬프트합니다

802.1X 가 네트워크 액세스 장치에서 활성화되거나 지원되지 않으면 클라이언트의 EAPOL 프레임이 삭제됩니다. 세 번 시도한 인증 시도 후에 클라이언트가 EAP 요청 / 신원 프레임을받지 못하면 클라이언트는 포트가 승인 된 상태 인 것처럼 프레임을 전송합니다. 허가 된 상태의 포트는 클라이언트가 성공적으로 인증되었음을 의미합니다.

클라이언트가 ID 를 제공하면 스위치는 중개 역할을 시작하여 인증이 성공하거나 실패 할 때까지 클라이언트와 인증 서버간에 EAP 프레임을 전달합니다. 인증에 성공하면 스위치 포트가 인증됩니다..

EAP 프레임의 특정 교환은 사용되는 인증 방법에 따라 다릅니다. "그림 4-11-2"는 RADIUS 서버에서 OTP (One-Time-Password) 인증 방법을 사용하여 클라이언트가 시작한 메시지 교환을 보여줍니다..

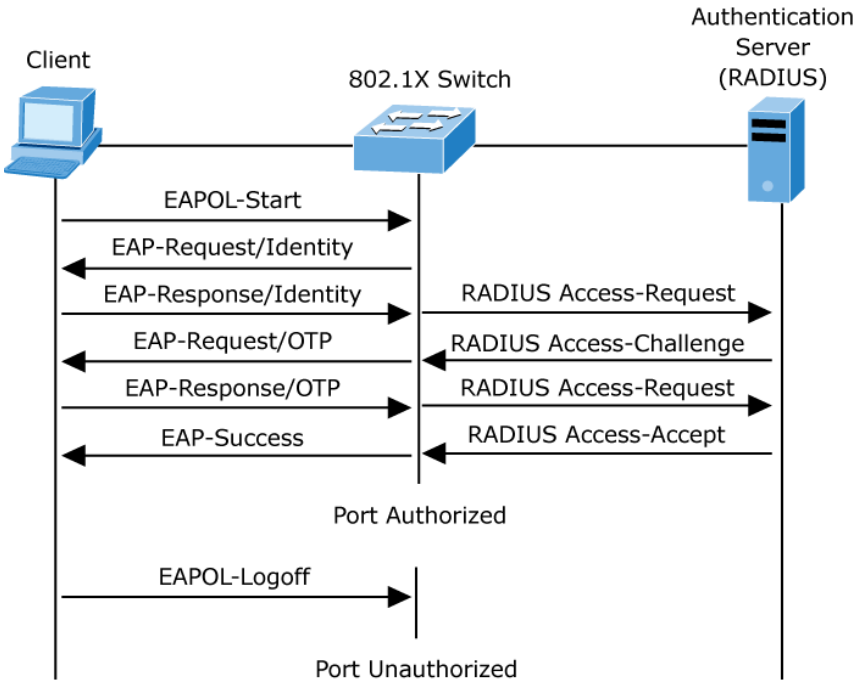


그림 4-11-2: EAP 메시지 교환

■ **비허용 상태와 허용 상태의 장비**

스위치 포트 상태는 클라이언트가 네트워크에 액세스 할 수 있는지 여부를 결정합니다. 포트가 인증되지 않은 상태에서 시작됩니다. 이 상태에서 포트는 802.1X 프로토콜 패킷을 제외한 모든 입구 및 출구 트래픽을 허용하지 않습니다. 클라이언트가 성공적으로 인증되면 포트는 승인 된 상태로 전환되어 클라이언트의 모든 트래픽이 정상적으로

흐르게합니다.

802.1X 를 지원하지 않는 클라이언트가 인증되지 않은 802.1X 포트에 연결된 경우 스위치는 클라이언트의 ID 를 요청합니다. 이 경우 클라이언트는 요청에 응답하지 않고 포트는 허가되지 않은 상태를 유지하며 클라이언트는 네트워크에 대한 액세스 권한이 부여되지 않습니다.

반대로 802.1X 지원 클라이언트가 802.1X 프로토콜을 실행하지 않는 포트에 연결하면 클라이언트는 EAPOL 시작 프레임을 보내 인증 프로세스를 시작합니다. 응답이 수신되지 않으면 클라이언트는 정해진 횟수만큼 요청을 보냅니다. 응답이 수신되지 않으므로 클라이언트는 포트가 승인 된 상태 인 것처럼 프레임 전송을 시작합니다

클라이언트가 성공적으로 인증되면 (인증 서버로부터 Accept 프레임 수신) 포트 상태가 권한 부여로 변경되고 인증 된 클라이언트의 모든 프레임이 포트를 통해 허용됩니다. 인증에 실패하면 포트가 승인되지 않은 상태로 유지되지만 인증을 다시 시도 할 수 있습니다. 인증 서버에 도달 할 수 없으면 스위치는 요청을 재전송 할 수 있습니다. 지정한 횟수만큼 시도한 후 서버에서 응답을받지 못하면 인증이 실패하고 네트워크 액세스가 허용되지 않습니다.

클라이언트가 로그 오프하면 EAPOL 로그 오프 메시지가 전송되어 스위치 포트가 무단 상태로 전환됩니다.

포트의 링크 상태가 위쪽에서 아래쪽으로 전환되거나 EAPOL- 로그 오프 프레임이 수신되면 포트는 승인되지 않은 상태로 돌아갑니다..

4.11.2 Authentication Configuration

이 페이지에서는 관리 클라이언트 인터페이스 중 하나를 통해 스위치에 로그인 할 때 사용자가 인증되는 방식을 구성 할 수 있습니다. 그림 4-11-3 의 인증 방법 구성 화면이 나타납니다.

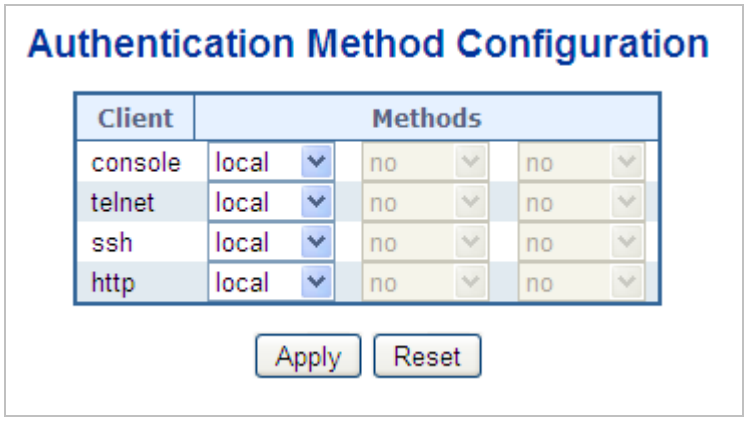


그림 4-11-3: Authentication Method Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Client**	아래 구성이 적용되는 관리 클라이언트.
• **Authentication Method**	인증 방법은 다음 값 중 하나로 설정할 수 있습니다. ■ **None**: 인증이 비활성화되고 로그인 할 수 없습니다.. ■ **Local**: 인증에 스위치의 로컬 사용자 데이터베이스를 사용합니다.. ■ **RADIUS**: 인증에 원격 RADIUS 서버를 사용합니다. ■ **TACACS+**: 인증에 원격 TACACS + 서버를 사용합니다. 원격 서버가 포함 된 방법은 원격 서버가 오프라인 인 경우 시간 초과됩니다. 이 경우 다음 방법이 시도됩니다. 각 메소드는 왼쪽에서 오른쪽으로 시도되고 메소드가 사용자를 승인하거나 거부 할 때까지 계속됩니다. 원격 서버를 기본 인증에 사용하는 경우 보조 인증을 '로컬'로 구성하는 것이 좋습니다. 구성된 인증 서버가없는 경우 관리 클라이언트가 로컬 사용자 데이터베이스를 통해 로그인 할 수 있습니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.11.3 Network Access Server Configuration

이 페이지에서는 IEEE 802.1X 및 MAC 기반 인증 시스템 및 포트 설정을 구성 할 수 있습니다.

IEEE 802.1X 표준은 사용자가 인증을위한 자격 증명을 먼저 제출하도록하여 네트워크에 대한 무단 액세스를 방지하는 포트 기반 액세스 제어 절차를 정의합니다. 하나 이상의 중앙 서버 인 백엔드 서버는 사용자가 네트워크에 액세스 할 수 있는지 여부를 결정합니다. 이 백엔드 (RADIUS) 서버는 "구성 → 보안 → AAA"페이지에서 구성됩니다. IEEE802.1X 표준은 포트 기반 동작을 정의하지만 비표준 변형은 아래에서 살펴볼 보안 제한 사항을 극복합니다.

MAC 기반 인증을 사용하면 동일한 포트에서 둘 이상의 사용자를 인증 할 수 있으므로 사용자가 자신의 시스템에 특수한 802.1X 인증 자 소프트웨어를 설치하지 않아도됩니다. 스위치는 사용자의 MAC 주소를 사용하여 백엔드 서버를 인증합니다. 침입자는 MAC 기반 인증을 802.1X 인증보다 덜 안전하게 만드는 위장 된 MAC 주소를 만들 수 있습니다. NAS 구성은 시스템 및 포트와 같은 두 섹션으로 구성됩니다. 그림 4-11-4 의 네트워크 액세스 서버 구성 화면이 나타납니다..

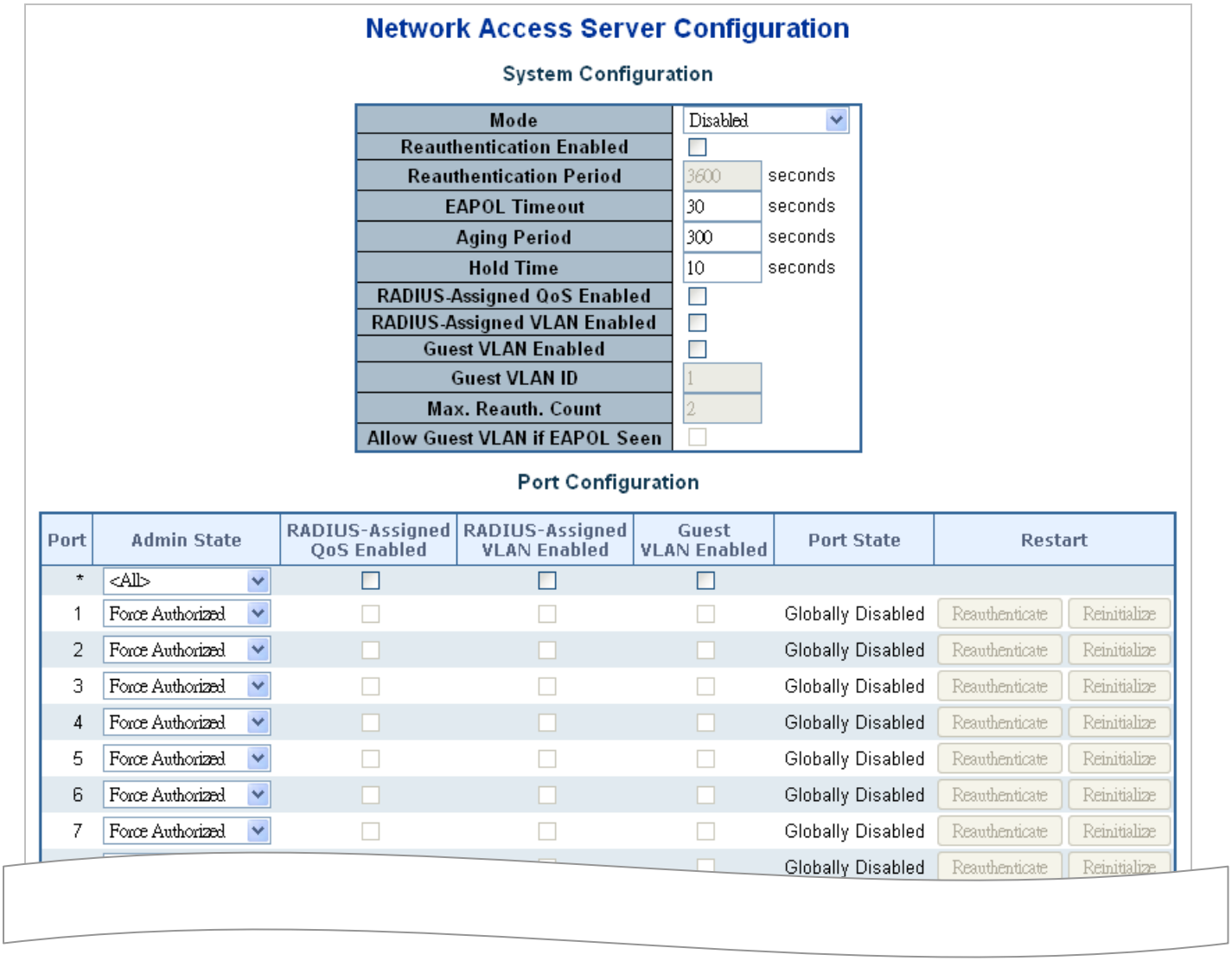


그림 4-11-4: Network Access Server Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

시스템 설정

목적	설명
• **Mode**	스위치에서 NAS 가 전체적으로 활성화 또는 비활성화되었는지 나타냅니다. 전역 적으로 사용할 수없는 경우 모든 포트에서 프레임 전달이 허용됩니다.
• **Reauthentication Enabled**	이 옵션을 선택하면 재 인증 기간에 지정 간격 후에 성공적으로 인증 된 요청자 / 클라이언트가 재 인증됩니다. 802.1X 지원 포트 재 인증은 새 장치가 스위치 포트에 연결되어 있는지 또는 요청자가 더 이상 연결되어 있지 않은지 여부를 감지하는 데 사용할 수 있습니다. AC 기반 포트의 경우 재 인증은 RADIUS 서버 구성이 변경된 경우에만 유용합니다. 스위치와 클라이언트 간의 통신을 포함하지 않으므로 포트에 클라이언트가 여전히

	있음을 의미하지는 않습니다.
• **Reauthentication Period**	연결된 클라이언트를 재 인증해야하는 기간 (초)을 결정합니다. Reauthentication Enabled 확인란을 선택한 경우에만 활성화됩니다. 유효한 값은 1 - 3600 초입니다.
• **EAPOL Timeout**	요청 신원 EAPOL 프레임의 재전송 시간을 결정합니다. 유효한 값은 1 - 65535 초입니다. 이것은 MAC 기반 포에는 영향을 미치지 않습니다.
• **Aging Period**	이 설정은 포트 보안 기능을 사용하여 MAC 주소를 보호하는 모드와 같은 다음 모드에 적용됩니다. ■ **Single 802.1X** ■ **Multi 802.1X** ■ **MAC-Based Auth**. NAS 모듈이 포트 보안 모듈을 사용하여 MAC 주소를 보호 할 때 포트 보안 모듈은 해당 MAC 주소에서 일정한 간격으로 활동을 확인하고 주어진 시간 내에 활동이없는 경우 사용 가능한 자원을 확보해야합니다. 이 매개 변수는이 기간을 정확하게 제어하며 10 ~ 1000000 초 사이의 숫자로 설정할 수 있습니다. 재 인증이 활성화되어 있고 포트가 802.1X 기반 모드 인 경우 포트에 더 이상 연결되지 않은 요청자가 다음 재 인증시 제거되어 실패 할 것이므로 이는 그리 중요하지 않습니다. 그러나 재 인증을 사용할 수 없는 경우 자원을 비울 수있는 유일한 방법은 항목을 에이징하는 것입니다. MAC 기반 인증의 포트 모드에서 재 인증은 스위치와 클라이언트간에 직접 통신을 일으키지 않으므로 클라이언트가 여전히 연결되어 있는지 여부를 감지 할 수 없으며 모든 리소스를 비울 수있는 유일한 방법은 항목을 오래되게하는 것입니다.
• **Hold Time**	이 설정은 포트 보안 기능을 사용하여 MAC 주소를 보호하는 모드와 같은 다음 모드에 적용됩니다.: ■ **Single 802.1X** ■ **Multi 802.1X** ■ **MAC-Based Auth**. RADIUS 서버가 클라이언트 액세스를 거부했거나 RADIUS 서버 요청이 ("구성 → 보안 → AAA"페이지에 지정된 시간 초과에 따라) 시간 초과되어 클라이언트가 액세스를 거부 한 경우 - 클라이언트가 승인되지 않은 상태. 보류 타이머는 진행중인 인증 중에 계산되지 않습니다. MAC 기반 인증에서 모드에서 스위치는 보류 시간 동안 클라이언트에서 오는 새 프레임을 무시합니다. Hold Time 은 10 ~ 1000000 초 사이의 숫자로 설정할 수 있습니다.
• **RADIUS-Assigned QoS**	RADIUS 할당 QoS 는 성공적으로 인증 된 요청자로부터 들어오는 트래픽이

Enabled	스위치에 할당되는 트래픽 클래스를 중앙에서 제어 할 수있는 방법을 제공합니다. 이 기능을 사용하려면 RADIUS 서버가 특수 RADIUS 특성을 전송하도록 구성되어야합니다. "RADIUS 할당 QoS 활성화 됨"확인란은 RADIUS 서버에 할당 된 QoS 클래스 기능을 전체적으로 활성화 / 비활성화하는 빠른 방법을 제공합니다. 이 옵션을 선택하면 개별 포트의 Ditto 설정에 따라 해당 포트에 RADIUS 할당 QoS 클래스가 사용되는지 여부가 결정됩니다. 이 옵션을 선택하지 않으면 RADIUS 서버에서 할당 된 QoS 클래스가 모든 포트에 대해 비활성화됩니다.
• **RADIUS-Assigned VLAN Enabled**	RADIUS 할당 QoS 는 성공적으로 인증 된 요청자로부터 들어오는 트래픽이 스위치에 할당되는 트래픽 클래스를 중앙에서 제어 할 수있는 방법을 제공합니다. 이 기능을 사용하려면 RADIUS 서버가 특수 RADIUS 특성을 전송하도록 구성되어야합니다. "RADIUS 할당 QoS 활성화 됨"확인란은 RADIUS 서버에 할당 된 QoS 클래스 기능을 전체적으로 활성화 / 비활성화하는 빠른 방법을 제공합니다. 이 옵션을 선택하면 개별 포트의 Ditto 설정에 따라 해당 포트에 RADIUS 할당 QoS 클래스가 사용되는지 여부가 결정됩니다. 이 옵션을 선택하지 않으면 RADIUS 서버에서 할당 된 QoS 클래스가 모든 포트에 대해 비활성화됩니다.
• **Guest VLAN Enabled**	게스트 VLAN 은 일반적으로 네트워크 액세스가 제한적인 특수 VLAN 으로, 네트워크 관리자가 정의한 시간 초과 후 802.1X 비 인식 클라이언트가 배치됩니다. 스위치는 아래 나열된대로 게스트 VLAN 에 들어가고 나가기위한 일련의 규칙을 따릅니다. "게스트 VLAN 사용"확인란은 게스트 VLAN 기능을 전체적으로 활성화 / 비활성화하는 빠른 방법을 제공합니다. 이 옵션을 선택하면 개별 포트의 Ditto 설정에 따라 포트를 게스트 VLAN 으로 이동할 수 있는지 여부가 결정됩니다. 이 옵션을 선택하지 않으면 게스트 VLAN 으로 이동하는 기능이 모든 포트에서 비활성화됩니다.
• **Guest VLAN ID**	이 값은 포트가 게스트 VLAN 으로 이동 된 경우 포트의 포트 VLAN ID 가 설정되는 값입니다. Guest VLAN 옵션이 전역 적으로 활성화 된 경우에만 변경 가능합니다. 유효한 값은 [1; 4095].
• **Max. Reauth. Count**	이 설정으로 스위치가 게스트 VLAN 을 입력하기 전에 응답없이 EAPOL 요청 ID 프레임을 전송하는 횟수가 조정됩니다. Guest VLAN 옵션이 전역 적으로 활성화 된 경우에만 값을 변경할 수 있습니다. 유효한 값은 [1; 255].
• **Allow Guest VLAN if EAPOL Seen**	스위치는 포트의 수명 동안 포트에서 EAPOL 프레임을 수신했는지 기억합니다. 스위치가 게스트 VLAN 에 입장할지 여부를 고려하면이 옵션이 활성화 또는 비활성화되었는지 먼저 확인합니다. 포트를 사용하지 않는 경우

	(선택 안 함, 기본값) 스위치는 포트의 수명 동안 포트에서 EAPOL 프레임을 수신하지 않은 경우에만 게스트 VLAN 으로 들어갑니다. 활성화 (선택)되어있는 경우 스위치는 포트의 수명 동안 포트에서 EAPOL 프레임을 수신하더라도 게스트 VLAN 입력을 고려합니다. Guest VLAN 옵션이 전역 적으로 활성화 된 경우에만 값을 변경할 수 있습니다.

Port Configuration

표에는 각 포트에 대해 하나의 행과 여러 열이 있습니다.:

목적	설명
• **Port**	아래 구성이 적용되는 포트 번호입니다.
• **Admin State**	NAS 에 전역모드에서 포트의 인증 모드를 선택하여 통제하려면 다음과 같은 방법을 이용합니다. **인증 강화** 이 모드에서 스위치는 포트 링크가 올라 오면 하나의 EAPOL 성공 프레임을 보내고 포트의 클라이언트는 인증없이 네트워크 액세스를 허용합니다. **비허가 강화** 이 모드에서 스위치는 포트 링크가 올라 오면 하나의 EAPOL 실패 프레임을 보내고 포트의 클라이언트는 네트워크 액세스를 허용하지 않습니다. **포트기반 802.1X** 802.1X 환경에서 사용자는 요청자, 스위치는 인증 자, RADIUS 서버는 인증 서버입니다. 인증자는 중간자 (man-in-the-middle) 역할을하여 요청자와 인증 서버간에 요청 및 응답을 전달합니다. 요청자와 스위치간에 전송되는 프레임은 EAPOL (EAP over LANs) 프레임으로 알려진 특수한 802.1X 프레임입니다. EAPOL 프레임은 EAP PDU 를 캡슐화합니다 (RFC3748). 스위치와 RADIUS 서버간에 전송되는 프레임은 RADIUS 패킷입니다. 또한 RADIUS 패킷은 스위치의 IP 주소, 이름 및 요청자의 포트 번호와 같은 다른 속성과 함께 EAP PDU 를 캡슐화합니다. EAP 는 MD5-Challenge, PEAP 및 TLS 와 같은 다양한 인증 방법을 허용한다는 점에서 매우 유연합니다. 중요한 점은 인증 자 (스위치)가 서 플리 컨트 및 인증 서버가 사용하는 인증 방법이나 특정 방법에 필요한 정보 교환 프레임 수를 알 필요가 없다는 것입니다. 스위치는 프레임의 EAP 부분을 관련 유형 (EAPOL 또는 RADIUS)으로 캡슐화하고 전달합니다.

인증이 완료되면 RADIUS 서버는 성공 또는 실패 표시가 포함 된 특수 패킷을 전송합니다. 이 결정을 요청자에게 전달하는 것 외에도 스위치는이를 사용하여 요청자와 연결된 스위치 포트에서 트래픽을 열거 나 차단합니다.

Note: 2 개의 백엔드 서버가 활성화되어 있고 AAA 구성 페이지를 사용하여 서버 시간 초과가 X 초로 구성되어 있고 목록의 첫 번째 서버가 현재 다운되었지만 죽은 것으로 간주되지 않는다고 가정합니다. 이제 Supplicant 가 X 초보다 빠른 속도로 EAPOL Start 프레임을 재전송하면 인증자가 획득되지 않습니다. 왜냐하면 스위치가 요청자로부터 새로운 EAPOL Start 프레임을 수신 할 때마다 스위치가 진행중인 백엔드 인증 서버 요청을 취소하기 때문입니다. 서버가 아직 실패하지 않았으므로 (X 초가 만료되지 않았으므로) 스위치의 다음 백엔드 인증 서버 요청시 동일한 서버에 연결됩니다. 이 시나리오는 영원히 반복됩니다. 따라서 서버 시간 제한은 요청자의 EAPOL 시작 프레임 재전송 속도보다 작아야합니다.

단일 802.1X

포트 기반 802.1X 인증에서 요청자가 포트에서 성공적으로 인증되면 네트워크 트래픽을 위해 전체 포트가 열립니다. 이렇게하면 포트에 연결된 다른 클라이언트 (예 : 허브를 통해)가 성공적으로 인증 된 클라이언트를 피기 백하고 실제로 인증되지 않은 경우에도 네트워크 액세스를 얻을 수 있습니다. 이 보안 위반을 극복하려면 Single 802.1X 변형을 사용하십시오.

단일 802.1X 는 실제로 IEEE 표준은 아니지만 포트 기반 802.1X 와 동일한 특성을 제공합니다. Single 802.1X 에서는 한 번에 하나의 인증 요청자가 포트에서 인증을받을 수 있습니다. 일반적인 EAPOL 프레임은 요청자와 스위치 간의 통신에 사용됩니다. 둘 이상의 요청자가 포트에 연결되어있는 경우 포트 연결이 시작될 때 가장 먼저 오는 포트가 가장 먼저 고려됩니다. 해당 요청자가 일정 기간 내에 유효한 자격 증명을 제공하지 않으면 다른 요청자에게 기회가 주어집니다. 일단 서 플리 컨트가 성공적으로 인증되면 해당 서 플리 컨트 만 액세스가 허용됩니다. 이것은 모든 지원되는 모드 중에서 가장 안전합니다. 이 모드에서는 포트 보안 모듈을 사용하여 인증이 완료되면 요청자의 MAC 주소를 보호합니다.

다중 802.1X

다중 802.1X 는 IEEE 802.1X 와 유사하지만 IEEE 표준이 아니지만 동일한 특성을 많이 사용하는 변형입니다. 다중 802.1X 에서 하나 이상의 인증 요청자가 동일한 포트에서 동시에 인증받을 수 있습니다. 각 요청자는 개별적으로 인증되며 포트 보안 모듈을 사용하여 MAC 표에 보안됩니다.

멀티 802.1X 에서 멀티 캐스트 BPDU MAC 주소를 스위치에서 요청자 방향으로 보낸 EAPOL 프레임의 대상 MAC 주소로 사용할 수 없습니다.

	그러면 포트에 연결된 모든 요청자가 스위치에서 보낸 요청에 응답하게됩니다. 대신 스위치는 요청자가 보낸 첫 번째 EAPOL 시작 또는 EAPOL 응답 ID 프레임에서 가져온 요청자의 MAC 주소를 사용합니다. 예외는 요청자가 첨부되지 않은 경우입니다. 이 경우 스위치는 BPDU 멀티캐스트 MAC 주소를 대상으로 사용하여 EAPOL 요청 ID 프레임을 보내 포트에있는 요청자를 깨 웁니다. 포트 보안 제한 기능을 사용하여 포트에 연결할 수있는 최대 요청자 수를 제한 할 수 있습니다. **MAC-기반 인증** 포트 기반 802.1X 와는 달리 MAC 기반 인증은 표준이 아니라 업계에서 채택한 모범 사례 방법입니다. MAC 기반 인증에서 사용자는 클라이언트라고하며 스위치는 클라이언트를 대신하여 요청자 역할을합니다. 클라이언트가 보낸 초기 프레임 (모든 종류의 프레임)은 스위치에 의해 스누핑되며, 스위치는 RADIUS 서버와의 후속 EAP 교환에서 사용자의 MAC 주소를 사용자 이름과 암호로 사용합니다. 6 바이트 MAC 주소는 "xx-xx-xx-xx-xx-xx"형식의 문자열로 변환됩니다. 즉, 대시 (-)가 하위 케이스의 16 진수 사이의 구분 기호로 사용됩니다. 스위치는 MD5-Challenge 인증 방법 만 지원하므로 RADIUS 서버를 적절하게 구성해야합니다. 인증이 완료되면 RADIUS 서버는 성공 또는 실패 표시를 보내고 포트 보안 모듈을 사용하여 특정 클라이언트의 트래픽을 열거 나 차단합니다. 그래야만 클라이언트의 프레임이 스위치로 전달됩니다. 이 인증에는 EAPOL 프레임이 포함되어 있지 않으므로 MAC 기반 인증은 802.1X 표준과 아무 관련이 없습니다. 포트 기반 802.1X 를 통한 MAC 기반 인증의 이점은 여러 클라이언트가 동일한 포트 (예 : 타사 스위치 또는 허브를 통해)에 연결될 수 있으며 여전히 개별 인증이 필요하며 클라이언트가 특별한 필요가 없음을 의미합니다 인증 자 소프트웨어. 802.1X 기반 인증을 통한 MAC 기반 인증의 이점은 클라이언트가 인증을위한 특정 인증 자 소프트웨어가 필요 없다는 것입니다. 단점은 악의적 인 사용자가 MAC 주소를 스푸핑 할 수 있다는 것입니다. MAC 주소가 유효한 RADIUS 사용자 인 장비는 누구든지 사용할 수 있습니다. 또한 MD5-Challenge 메서드 만 지원됩니다. 포트 보안 제한 기능을 사용하여 포트에 연결할 수있는 최대 클라이언트 수를 제한 할 수 있습니다.
• **RADIUS-Assigned QoS Enabled**	주어진 포트에 대해 RADIUS 할당 QoS 가 전체적으로 활성화되고 활성화 (확인)되면 스위치는 요청자가 성공적으로 인증 될 때 RADIUS 서버가 전송한 RADIUS 액세스 수락 패킷에 포함 된 QoS 클래스 정보에 반응합니다. 존재하고 유효한 경우 요청자의 포트에서 수신 된 트래픽은 주어진 QoS

	클래스로 분류됩니다. (재) 인증이 실패하거나 RADIUS 액세스 수락 패킷이 더 이상 QoS 클래스를 운반하지 않거나 유효하지 않은 경우 또는 요청자가 포트에 더 이상 존재하지 않으면 포트의 QoS 클래스는 원래 QoS 클래스로 즉시 되돌아갑니다 그 동안에 RADIUS 가 할당 된 것에 영향을 미치지 않고 관리자가 변경할 수 있습니다.. 이 옵션은 단일 클라이언트 모드에서만 사용할 수 있습니다.. ■ **Port-based 802.1X** ■ **Single 802.1X** QoS 식별에 사용되는 RADIUS 속성 클래스 : RFC4675 에 정의 된 User-Priority-Table 속성은 Access-Accept 패킷에서 QoS 클래스를 식별하기위한 기초를 형성합니다. 패킷에있는 속성의 첫 번째 항목 만 고려되고 유효하도록하려면이 규칙을 따라야합니다.: ● 속성 값의 모든 8 옥텟은 동일해야하며 '0'- '7'범위의 ASCII 문자로 구성되어야합니다. 이는 범위 [0; 0]의 원하는 QoS 클래스로 변환됩니다. 7].
• **RADIUS-Assigned VLAN Enabled**	주어진 포트에 대해 RADIUS 할당 VLAN 을 전역 적으로 활성화하고 활성화 (선택)하면 스위치는 요청자가 성공적으로 인증되면 RADIUS 서버가 전송 한 RADIUS 액세스 수락 패킷에 포함 된 VLAN ID 정보에 응답합니다. 존재하고 유효한 경우 포트의 포트 VLAN ID 가이 VLAN ID 로 변경되고 포트가 해당 VLAN ID 의 구성원으로 설정되며 포트는 VLAN 비 인식 모드로 강제 설정됩니다. 일단 할당되면 포트에 도착한 모든 트래픽은 분류되고 RADIUS 할당 VLAN ID 로 전환됩니다.. (재) 인증이 실패하거나 RADIUS 액세스 수락 패킷이 더 이상 VLAN ID 를 전달하지 않거나 유효하지 않은 경우 또는 요청자가 포트에 더 이상 존재하지 않으면 포트의 VLAN ID 가 원래 VLAN ID 로 즉시 되돌아갑니다 그 동안에 RADIUS 가 할당 된 것에 영향을 미치지 않고 관리자가 변경할 수 있습니다. 이 옵션은 단일 클라이언트 모드에서만 사용할 수 있습니다.. ■ **Port-based 802.1X** ■ **Single 802.1X** VLAN 할당 문제를 해결하려면 "모니터 → VLANs → VLAN 구성원 및 VLAN 포트"페이지를 사용하십시오. 이 페이지는 현재 포트 VLAN 구성을 (일시적으로) 덮어 쓰는 모듈을 보여줍니다 VLAN ID 식별에 사용되는 RADIUS 속성: RFC2868 과 RFC3580 은 Access-Accept 패킷에서 VLAN ID 를 식별하는 데 사용되는 속성의 기초를 형성합니다. 다음과 같은 기준이 사용됩니다.:

	● Tunnel-(Type, Medium-Type, Tunnel-private-Group-ID) 속성은 모두 Access-Accept 패킷에 적어도 한 번 있어야합니다. ● 스위치는 동일한 태그 값을 갖고 다음 요구사항을 충족하는 첫 번째 속성 집합을 찾습니다(Tag == 0 을 사용하면 Tunnel-Private-Group-Id 에 태그를 포함 하지 않음): ● Tunnel-Mudium-Type 의 값은 "IEEE-802"(서수는 6) ● Tunnel-Type 의 값은 "VLAN"에 반드시 설정되어야한다. (서수는 13). ● Value of Tunnel-Private-Group-ID 는 VLAN ID 나타내는 10 진수 문자열로 해석되는 '0' – '9' 범위의 ASCII 문자로 된 문자열이며 읽어온 0 표시는 버리며 최종값은[1;4095].
• **Guest VLAN Enabled**	**주어진 포트에 대해 게스트 VLAN 이 전역 적으로 활성화되고 활성화 (확인)되면 스위치는 아래에 설명 된 규칙에 따라 포트를 게스트 VLAN 으로 이동하는 것을 고려합니다.** **이 옵션은 EAPOL 기반 모드에서만 사용할 수 있습니다. 즉,Port-based 802.1X** ■ **Single 802.1X** ■ **Multi 802.1X** **게스트 VLAN 협력:** 게스트 VLAN 지원 포트의 링크가 올라 오면 스위치는 EAPOL 요청 신원 프레임 전송을 시작합니다. 그러한 프레임의 전송 횟수가 Max 를 초과하면 재가동. 카운트 및 EAPOL 프레임이 수신되지 않은 동안 스위치는 게스트 VLAN 을 입력하는 것으로 간주합니다. EAPOL 요청 식별 프레임의 전송 간격은 EAPOL 시간 초과로 구성됩니다. EAPOL 이 활성화 된 경우 게스트 VLAN 허용을 선택하면 포트가 이제 게스트 VLAN 에 배치됩니다. 비활성화 된 경우 스위치는 먼저 포트에서 EAPOL 프레임을 수신했는지 확인합니다 (포트 링크가 다운되거나 포트의 Admin 상태가 변경되면이 기록이 지워짐). 그렇지 않은 경우 포트는 게스트 VLAN 에 배치해야합니다. 그렇지 않으면 게스트 VLAN 으로 이동하지 않지만 EAPOL 시간 초과로 지정된 속도로 EAPOL 요청 ID 프레임을 계속 전송합니다. 게스트 VLAN 에서 포트는 인증 된 것으로 간주되며 포트의 연결된 모든 클라이언트는이 VLAN 에서 액세스가 허용됩니다. 스위치는 게스트 VLAN 을 입력 할 때 EAPOL 성공 프레임을 전송하지 않습니다. 게스트 VLAN 에서 스위치는 EAPOL 프레임에 대한 링크를 모니터링하고 이러한 프레임 중 하나가 수신되면 스위치는 즉시 게스트 VLAN 에서 포트를 가져와 포트 모드에 따라 요청자를 인증하기 시작합니다. EAPOL 프레임이 수신되면 "EAPOL 이 표시된 경우 게스트 VLAN 허용"이 비활성화 된 경우

	포트는 게스트 VLAN 으로 되돌아 갈 수 없습니다.
• **Port State**	포트의 현재 상태입니다. 다음 값 중 하나를 수행 할 수 있습니다. ■ **Globally Disabled**: NAS 가 전역적으로 사용되지 않습니다. ■ **Link Down**: NAS 가 전역적으로 활성화되고 포트에 링크는 다운됩니다. ■ **Authorized**: 포트에 강제 인증또는 단일 요청지원모드이고 요청자를 인증합니다. ■ **Unauthorized**: 포트가 강제 비인증되거나 단일 요청자 모드에 있으며 RADIUS 서버에서 요청자가 성공적으로 승인되지 않습니다. ■ **X Auth/Y Unauth**: 포트가 다중 사용자 모드입니다. 현재 X 클라이언트는 권한이 부여되며 Y 는 권한이 없음을 나타냅니다.
• **Restart**	각 행에 대해 두 개의 버튼을 사용할 수 있습니다. 이 단추는 인증이 전역적으로 활성화되고 포트의 Admin State 가 EAPOL 기반 또는 MAC 기반 모드인 경우에만 활성화됩니다. 이 버튼을 누를 경우에도 변경한 설정이 적용되지 않습니다.. ■ **Reauthenticate**: 포트의 조용한 기간이 만료 될 때마다 (EAPOL 기반 인증) 재 인증을 예약합니다. MAC 기반 인증의 경우 재 인증이 즉시 시도됩니다. 이 단추는 포트에서 성공적으로 인증 된 클라이언트에 대한 효과 만 가지며 클라이언트가 일시적으로 무단으로되지 않게합니다. ■ **Reinitialize**: 포트에서 클라이언트의 재 초기화를 강제하므로 재 인증이 즉시 이루어집니다. 클라이언트는 재 인증이 진행되는 동안 허가되지 않은 상태로 전환합니다.

버튼

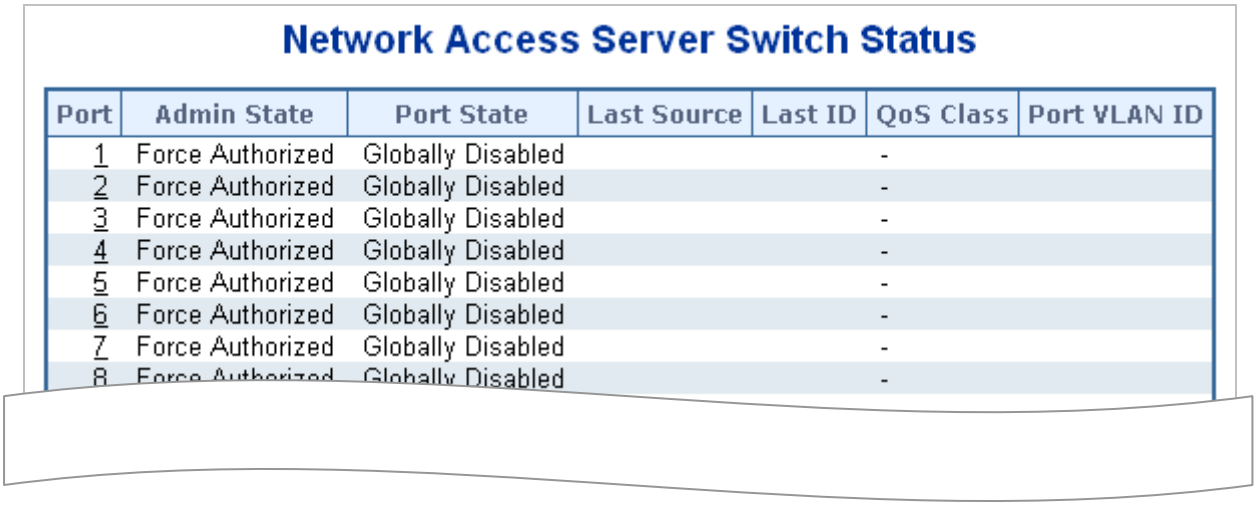
Refresh: 페이지를 새로 고칩니다.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.11.4 Network Access Overview

이 페이지는 선택된 스위치의 현재 NAS 포트 상태에 대한 개요를 제공합니다. 그림 4-11-5 의 네트워크 액세스 개요 화면이 나타납니다.



Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	
7	Force Authorized	Globally Disabled			-	
8	Force Authorized	Globally Disabled			-	

그림 4-11-5: Network Access Server Switch 상태 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	스위치 포트 번호. 이 포트에 대한 자세한 NAS 통계를 탐색하려면 누릅니다.
• **Admin State**	포트의 현재 관리 상태입니다. 가능한 값에 대한 설명은 NAS Admin State 를 참조하십시오.
• **Port State**	포트의 현재 상태입니다. 개별 상태에 대한 설명은 NAS Port State (NAS 포트 상태)를 참조하십시오.
• **Last Source**	EAPOL 기반 인증을 위해 가장 최근에 수신 한 EAPOL 프레임에서 전송 된 소스 MAC 주소와 MAC 기반 인증을 위해 새 클라이언트에서 가장 최근에 수신 된 프레임입니다.
• **Last ID**	EAPOL 기반 인증을 위해 가장 최근에 수신 한 Response Identity EAPOL 프레임에서 전달 된 사용자 이름 (요청자 신원) 및 MAC 기반 인증을 위해 새 클라이언트에서 가장 최근에 수신 된 프레임의 원본 MAC 주소.
• **QoS Class**	QoS 사용하도록 설정된 경우 RADIUS 서버가 포트에 할당 한 클래스입니다
• **Port VLAN ID**	NAS 가 포트를 넣은 VLAN ID. 포트 VLAN ID 가 NAS 에 의해 무시되지 않으면이 필드는 비어 있습니다. VLAN ID 가 RADIUS 서버에 의해 할당되면 "(RADIUS 가 할당 됨)"이 VLAN ID 에 추가됩니다. RADIUS 할당 VLAN 에 대한 자세한 내용은 여기를 참조하십시오. 포트가 게스트 VLAN 으로 이동되면 "(게스트)"가 VLAN ID 에 추가됩니다. 여기에 게스트 VLAN 에 대해 자세히 읽어보십시오

버튼

Refresh: 즉시 페이지를 새로고침합니다.

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

4.11.5 Network Access Statistics

이 페이지는 EAPOL 기반 IEEE 802.1X 인증을 실행하는 특정 스위치 포트에 대한 자세한 NAS 통계를 제공합니다. MAC 기반 포트의 경우 선택한 백엔드 서버 (RADIUS 인증 서버) 통계 만 표시합니다. 포트 선택 상자를 사용하여 표시 할 포트 세부 정보를 선택하십시오. 그림 4-11-6 의 네트워크 액세스 통계 화면이 나타납니다.

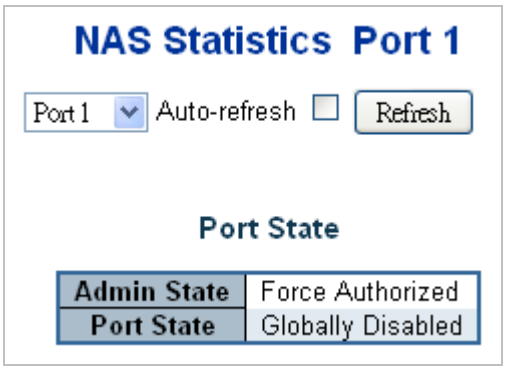


그림 4-11-6: Network Access Statistics 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

Port State

목적	설명
• **Admin State**	포트의 현재 관리 상태입니다. 가능한 값에 대한 설명은 NAS Admin State 를 참조하십시오.
• **Port State**	포트의 현재 상태입니다. 개별 상태에 대한 설명은 NAS Port State (NAS 포트 상태)를 참조하십시오.
• **QoS Class**	RADIUS 서버가 할당 한 QoS 클래스 QoS 클래스가 지정되지 않으면이 필드는 공백입니다.
• **Port VLAN ID**	AS 가 포트를 넣은 VLAN ID. 포트 VLAN ID 가 NAS 에 의해 무시되지 않으면이 필드는 비어 있습니다. VLAN ID 가 RADIUS 서버에 의해 할당되면 "(RADIUS 가 할당 됨)"이 VLAN ID 에 추가됩니다. RADIUS 할당 VLAN 에 대한 자세한 내용은 여기를 참조하십시오. 포트가 게스트 VLAN 으로 이동되면 "(게스트)"가 VLAN ID 에 추가됩니다. 여기에 게스트 VLAN 에 대해 자세히 읽어보십시오.

Port Counters

목적	설명
• EAPOL Counters	이러한 요청자 프레임 카운터는 다음 관리 상태에서 사용할 수 있습니다.: ■ **Force Authorized** ■ **Force Unauthorized** ■ **Port-based 802.1X** ■ **Single 802.1X** ■ **Multi 802.1X**

방향	이름	IEEE 이름	설명
Rx	**Total**	dot1xAuthEapolFramesRx	스위치가 수신 한 모든 유형의 유효한 EAPOL 프레임 수입니다.
Rx	**Response ID**	dot1xAuthEapolRespIdFramesRx	스위치가 수신 한 유효한 EAPOL 응답 ID 프레임 수입니다.
Rx	**Responses**	dot1xAuthEapolRespFramesRx	스위치가 수신 한 유효한 EAPOL 응답 프레임 (응답 ID 프레임 제외)의 수.
Rx	**Start**	dot1xAuthEapolStartFramesRx	스위치가 수신 한 EAPOL 시작 프레임 수.
Rx	**Logoff**	dot1xAuthEapolLogoffFramesRx	스위치가 수신 한 유효한 EAPOL 로그 오프 프레임 수입니다.
Rx	**Invalid Type**	dot1xAuthInvalidEapolFramesRx	프레임 유형이 인식되지 않는 스위치에서 수신 한 EAPOL 프레임 수입니다.
Rx	**Invalid Length**	dot1xAuthEapLengthErrorFramesRx	패킷 본문 길이 필드가 유효하지 않은 스위치에 의해 수신 된 EAPOL 프레임 수입니다.
Tx	**Total**	dot1xAuthEapolFramesTx	스위치가 전송 한 모든 유형의 EAPOL 프레임 수입니다.

	Tx	**Request ID**	dot1xAuthEapolReqIdFramesTx	스위치가 전송 한 EAPOL 요청 ID 프레임 수입니다
	Tx	**Requests**	dot1xAuthEapolReqFramesTx	스위치가 전송 한 유효한 EAPOL 요청 프레임 (요청 ID 프레임 제외)의 수.

- **Backend Server Counters**

이러한 백엔드 (RADIUS) 프레임 카운터는 다음 관리 상태에서 사용할 수 있습니다.:

- **Port-based 802.1X**
- **Single 802.1X**
- **Multi 802.1X**
- **MAC-based Auth**.

방향	이름	IEEE이름	설명
Rx	**Access Challenges**	dot1xAuthBackendAccessChallenges	**802.1X-기반**: 스위치가 요청자의 첫 번째 응답 다음에 백엔드 서버로부터 첫 번째 요청을 수신 한 횟수를 계산합니다. 백엔드 서버가 스위치와 통신하고 있음을 나타냅니다. **MAC-기반**: 이 포트 (맨 왼쪽 테이블) 또는 클라이언트 (맨 오른쪽 테이블)에 대해 백엔드 서버에서받은 모든 액세스 챌린지를 계산합니다.
Rx	**Other Requests**	dot1xAuthBackendOtherRequestsToSupplicant	**802.1X-기반**: 스위치가 첫 번째 요청자 다음에 요청자에게 EAP 요청 패킷을 보내는 횟수를 계산합니다. 백엔드 서버가 EAP 방법을 선택했음을 나타냅니다. **MAC-기반**: 해당 사항 없음.
Rx	**Auth. Successes**	dot1xAuthBackendAuthSuccesses	**802.1X- 및 MAC-기반**: 스위치가 성공 표시를 수신 한 횟수를 계산합니다. 요청자 / 클라이언트가

				백엔드 서버에 성공적으로 인증되었음을 나타냅니다
	Rx	**Auth. Failures**	dot1xAuthBackendAuthFails	**802.1X- 및 MAC-기반**: 스위치가 오류 메시지를 수신한 횟수를 계산합니다. 이는 요청자 / 클라이언트가 백엔드 서버에 대해 인증하지 않았 음을 나타냅니다
	Tx	**Responses**	dot1xAuthBackendResponses	**802.1X-기반:** 스위치가 요청자의 첫 번째 응답 패킷을 백엔드 서버로 보내려고 시도하는 횟수를 계산합니다. 스위치가 백엔드 서버와 통신을 시도했음을 나타냅니다. 가능한 재전송은 계산되지 않습니다. **MAC-based:** 주어진 포트 (맨 왼쪽 테이블) 또는 클라이언트 (맨 오른쪽 테이블)에 대해 스위치에서 백엔드 서버로 보낸 모든 백엔드 서버 패킷을 센다. 가능한 재전송은 계산되지 않습니다.

- **Last Supplicant/Client Info**

인증을 시도한 최종 요청자 / 클라이언트에 대한 정보. 이 정보는 다음 관리 상태에서 사용할 수 있습니다.:

- **Port-based 802.1X**
- **Single 802.1X**
- **Multi 802.1X**
- **MAC-based Auth**.

이름	IEEE 이름	설명
MAC Address	dot1xAuthLastEapolFrameSource	최근 사용한 MAC 주소.
VLAN ID	-	가장 최신의 수신 된 Vlan ID 입니다.
Version	dot1xAuthLastEapolFrameVersion	**802.1X-based**: 가장 최근에 수신 한 응답 ID EAPOL 프레임에서 전달 된 사용자 이름 (요청자

		신원)입니다.. **MAC-based**: 적용 불가능
Identity	-	**802.1X-based**: 가장 최근에 수신 한 응답 ID EAPOL 프레임에서 전달 된 사용자 이름 (요청자 신원)입니다.. **MAC-based**: 적용 불가능

Selected Counters

목적	설명
• **Selected Counters**	포트가 다음 관리 상태 중 하나 일 때 선택된 카운터 표가 표시됩니다.: ■ **Multi 802.1X** ■ **MAC-based Auth**. 이 표는 포트 카운터 테이블과 동일하며 포트 카운터 테이블 옆에 배치되며 MAC 주소가 현재 선택되지 않은 경우 비어있게됩니다. 표를 채우려면 아래 표에서 첨부 된 MAC 주소 중 하나를 선택하십시오.

Attached MAC Address

목적	설명
• **Identity**	응답 ID EAPOL 프레임에서받은 요청자 ID 를 표시합니다. 링크를 클릭하면 요청자의 EAPOL 및 백엔드 서버 카운터가 선택된 카운터 테이블에 표시됩니다. 요청자가 첨부되지 않은 경우 요청 된 요청자가 표시되지 않습니다. MAC 기반 인증에는이 열을 사용할 수 없습니다.
• **MAC Address**	Multi 802.1X 의 경우이 열에는 연결된 요청자의 MAC 주소가 저장됩니다. MAC 기반 인증의 경우이 열에는 연결된 클라이언트의 MAC 주소가 저장됩니다. 링크를 클릭하면 클라이언트의 백엔드 서버 카운터가 선택된 카운터 테이블에 표시됩니다. 연결되어있는 클라이언트가없는 경우 No clients attached 가 표시됩니다.
• **VLAN ID**	이 열은 포트 보안 모듈을 통해 현재 해당 클라이언트가 보호하고있는 VLAN ID 를 보유합니다..
• **State**	클라이언트는 인증되거나 인증되지 않을 수 있습니다. 인증 된 상태에서는 포트에서 프레임을 전달할 수 있으며 인증되지 않은 상태에서는 차단됩니다. 백엔드 서버가 클라이언트를 성공적으로 인증하지 않으면 인증되지 않습니다. 하나 또는 다른 이유로 인증에 실패하면 클라이언트는 보류 시간 (초) 동안 인증되지 않은 상태를

	유지합니다.
• **Last Authentication**	클라이언트의 마지막 인증 날짜 및 시간을 표시합니다 (성공적 일뿐만 아니라 성공하지 못했습니다).

버튼

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Refresh: 즉시 페이지를 새로고침합니다.

Clear: 이 버튼은 다음과은 방법에 사용할수 있습니다.

- 승인 된 권한 부여
- 비허가 권한
- 포트-기반 802.1X
- 단일 802.1X

선택한 포트에 대한 카운터를 지우려면 클릭하십시오.

Clear All: 이 버튼은 다음과 같은 방법으로 사용할 수 있습니다.

- 다중 802.1X
- MAC-기반 Auth.X

포트 카운터와 연결된 모든 클라이언트 카운터를 모두 지우려면 클릭하십시오. 그러나 "마지막 클라이언트"는 지워지지 않습니다..

Clear This: 이 버튼은 다음과 같은 방법으로 사용할 수 있습니다.

- 다중 802.1X
- MAC-기반 Auth.X

현재 선택된 클라이언트의 카운터 만 지우려면 클릭하십시오..

4.11.6 RADIUS

이 페이지에서는 RADIUS 서버를 구성 할 수 있습니다. 그림 4-11-7 의 RADIUS Configuration 화면이 나타납니다.

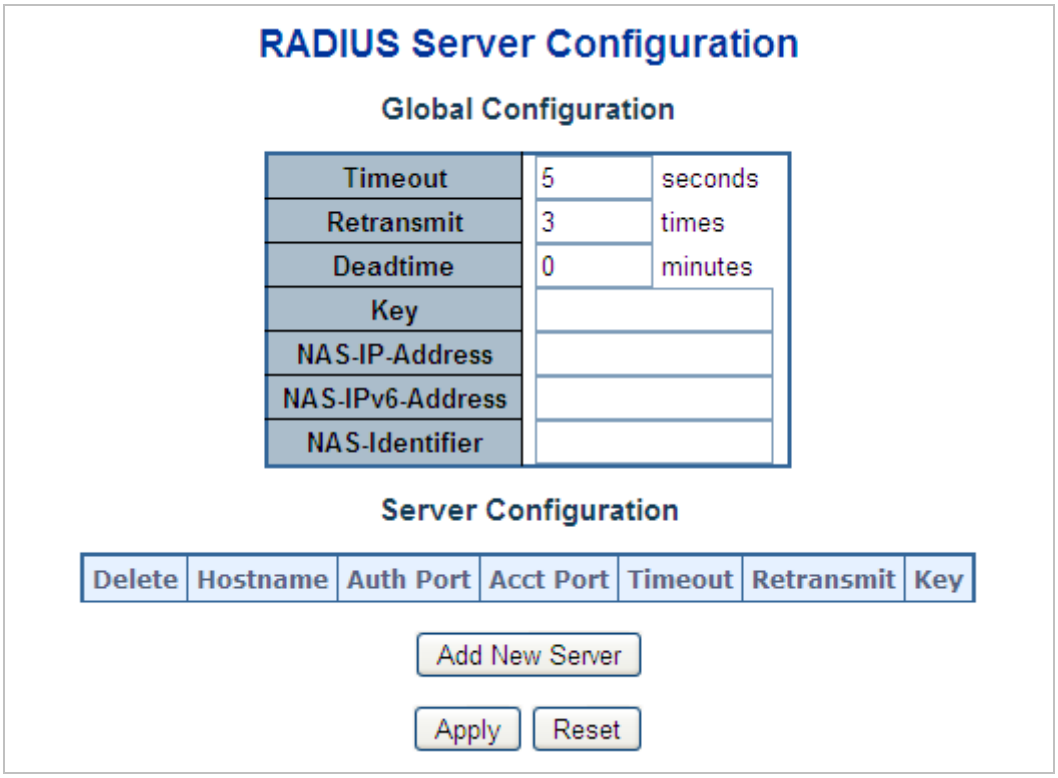


그림 4-11-7: RADIUS Server Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

Global Configuration

이 설정은 모든 RADIUS 서버에 공통입니다.

목적	설명
• **Timeout**	시간 초과는 요청을 다시 전송하기 전에 RADIUS 서버의 응답을 기다리는 시간 (1 - 1000 초)입니다.
• **Retransmit**	Retransmit 은 RADIUS 요청이 응답하지 않는 서버로 재전송되는 횟수 (1 - 1000 범위)입니다. 마지막 재전송 후 서버가 응답하지 않으면 죽은 것으로 간주됩니다.
• **Dead Time**	0 에서 3600 초 사이의 숫자로 설정할 수있는 데드 타임은 스위치가 이전 요청에 응답하지 못한 서버에 새 요청을 보내지 않는 기간입니다. 이렇게하면 스위치가 이미 죽은 것으로 판별 한 서버에 지속적으로 접속하지 못하게됩니다.

	데드 타임을 0 보다 큰 값으로 설정하면이 기능을 사용할 수 있지만 둘 이상의 서버가 구성된 경우에만 가능합니다.
• **Key**	RADIUS 서버와 스위치간에 공유되는 비밀 키 - 최대 63 자.
• **NAS-IP-Address**	RADIUS 액세스 요청 패킷의 특성 4 로 사용될 IPv4 주소입니다. 이 필드를 비워두면 나가는 인터페이스의 IP 주소가 사용됩니다.
• **NAS-IPv6-Address**	RADIUS 액세스 요청 패킷의 특성 95 로 사용될 IPv6 주소입니다. 이 필드를 비워두면 나가는 인터페이스의 IP 주소가 사용됩니다.
• **NAS-Identifier**	253 자의 식별자 - RADIUS 액세스 요청 패킷의 특성 32 로 사용됩니다. 이 필드를 비워두면 NAS 식별자가 패킷에 포함되지 않습니다.

Server Configuration

표에는 각 RADIUS 서버에 대한 행과 여러 열이 있습니다.:

목적	설명
• **Delete**	RADIUS 서버 항목을 삭제하려면이 상자를 선택하십시오. 항목은 다음 저장 중에 삭제됩니다.
• **Hostname**	RADIUS 서버의 IP 주소 또는 호스트 이름.
• **Auth Port**	RADIUS 서버에서 인증에 사용할 UDP 포트입니다.
• **Acct Port**	계정을 위해 RADIUS 서버에서 사용할 UDP 포트입니다.
• **Timeout**	이 선택적 설정은 전역 시간 초과 값을 무시합니다. 공백으로두면 전역 시간 초과 값이 사용됩니다.
• **Retransmit**	이 선택적 설정은 전역 재전송 값을 무시합니다. 공백으로두면 전역 재전송 값이 사용됩니다.
• **Key**	이 선택적 설정은 전역 키를 무시합니다. 비워두면 전역 키가 사용됩니다.

버튼

Add New Server: 새 RADIUS 서버를 추가하려면 누릅니다. 빈 행이 테이블에 추가되고 필요에 따라 RADIUS 서버를 구성 할 수 있습니다. 최대 5 개의 서버가 지원됩니다.

Delete : 새 서버의 추가를 취소하려면 누릅니다..

Apply : 변동사항을 클릭하여 저장합니다.

Reset : 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.11.7 TACACS+

이 페이지에서는 TACACS + 서버를 구성 할 수 있습니다. 그림 4-11-8 의 TACACS + Configuration 화면이 나타납니다.

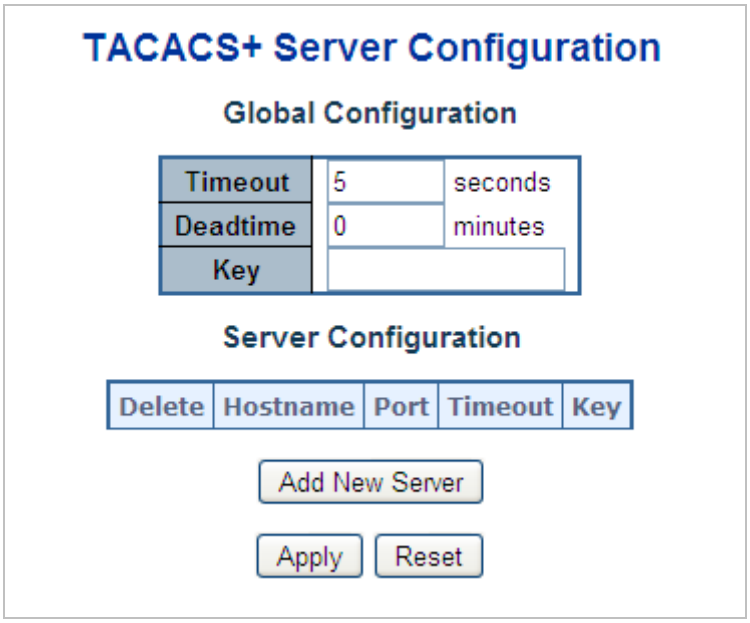


그림 4-11-8: TACACS+ Server Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

Global Configuration

이러한 설정은 모든 TACACS + 서버에 공통적으로 적용됩니다.

목적	설명
• **Timeout**	시간 초과는 TACACS + 서버가 응답하지 않을 때까지 기다리는 시간 (초)입니다 (범위 : 1 - 1000).
• **Dead Time**	Dead Time 은 0 ~ 1440 분 사이의 숫자로 설정할 수 있습니다.이 시간은 스위치가 이전 요청에 응답하지 않은 서버에 새 요청을 보내지 않는 기간입니다. 이렇게하면 스위치가 이미 죽은 것으로 판별 한 서버에 지속적으로 접속하지 못하게됩니다. Deadtime 을 0 보다 큰 값으로 설정하면 둘 이상의 서버가 구성된

	경우에만이 기능을 사용할 수 있습니다.
• **Key**	비밀 키 - 최대 63 자 길이 - TACACS + 서버와 스위치간에 공유됩니다.

Server Configuration

표에는 각 TACACS + 서버에 대해 하나의 행과 여러 열이 있습니다.:

목적	설명
• **Delete**	TACACS + 서버 항목을 삭제하려면이 상자를 선택하십시오. 항목은 다음 저장 중에 삭제됩니다.
• **Hostname**	TACACS + 서버의 IP 주소 또는 호스트 이름.
• **Port**	인증을 위해 TACACS + 서버에서 사용할 TCP 포트입니다.
• **Timeout**	이 선택적 설정은 전역 시간 초과 값을 무시합니다. 공백으로두면 전역 시간 초과 값이 사용됩니다.
• **Key**	이 선택적 설정은 전역 키를 무시합니다. 비워두면 전역 키가 사용됩니다.

버튼

Add New Server: 새 TACACS + 서버를 추가하려면 누릅니다. 빈 행이 테이블에 추가되고 필요에 따라 TACACS + 서버를 구성 할 수 있습니다. 최대 5 개의 서버가 지원됩니다.

Delete: 새 서버의 추가를 취소하려면 누릅니다.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.11.8 RADIUS Overview

이 페이지에서는 인증 구성 페이지에서 구성 할 수있는 RADIUS 서버의 상태에 대한 개요를 제공합니다. 그림 4-11-9 의 RADIUS 인증 / 계정 서버 개요 화면이 나타납니다.

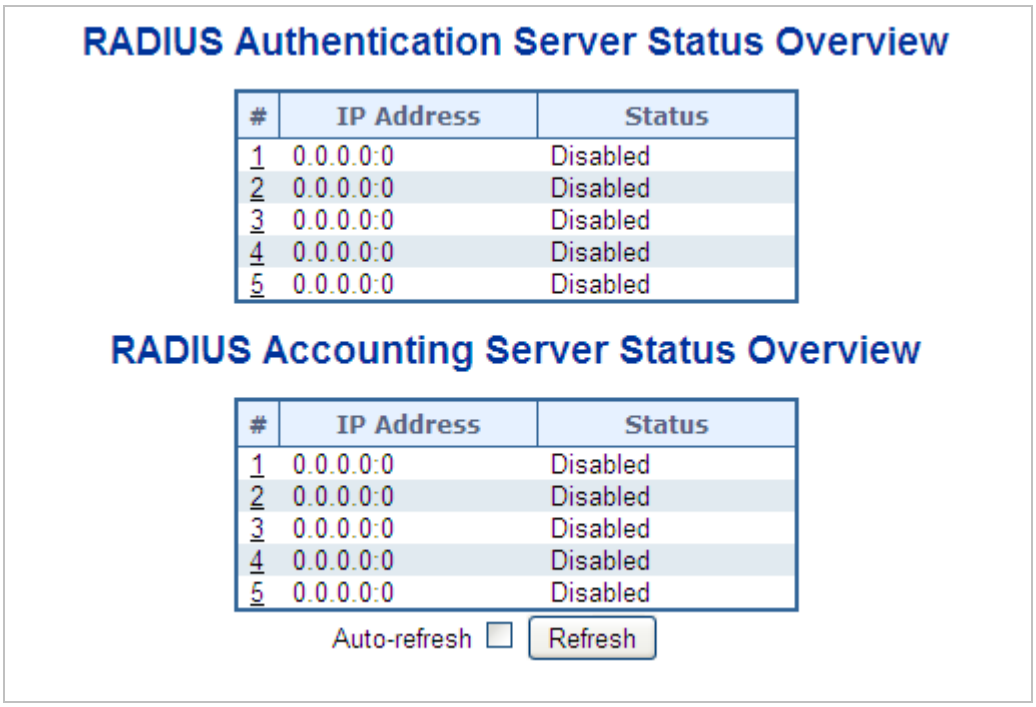


그림 4-11-9: RADIUS Authentication/Accounting Server Overview 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

RADIUS Authentication Server Status Overview

목적	설명
• #	RADIUS 서버 번호. 이 서버에 대한 자세한 통계로 이동하려면 클릭하십시오.
• IP Address	이 서버의 IP 주소 및 UDP 포트 번호 (<IP 주소> : <UDP 포트> 표기법)
• Status	서버의 현재 상태. 이 필드에는 다음 값 중 하나가 사용됩니다.: ■ **Disabled**: 서버가 비활성화되었습니다. ■ **Not Ready**: 서버가 활성화되어 있지만 IP 통신이 아직 시작 및 실행되지 않습니다.. ■ **Ready**: 서버가 활성화되고 IP 통신이 시작되어 실행되며 RADIUS 모듈은 액세스 시도를 수락 할 준비가됩니다. ■ **Dead (X seconds left)**: 이 서버에 대한 액세스가 시도되었지만 구성된 제한 시간 내에 응답하지 않았습니다. 서버는 일시적으로 비활성화되었지만 불감 시간이 만료되면 다시 활성화됩니다. 이 발생하기 전에 남은 시간 (초)은 괄호 안에 표시됩니다. 이 상태는 둘 이상의 서버가 사용 가능할 때만 도달 할 수 있습니다..

RADIUS Accounting Server Status Overview

목적	설명
• #	RADIUS 서버 번호. 이 서버에 대한 자세한 통계로 이동하려면 클릭하십시오.

• **IP Address**	이 서버의 IP 주소 및 UDP 포트 번호 (<IP 주소> : <UDP 포트> 표기법)
• **Status**	서버의 현재 상태. 이 필드에는 다음 값 중 하나가 사용됩니다.: ■ **Disabled**: 서버가 비활성화되었습니다. ■ **Not Ready**: 서버가 활성화되어 있지만 IP 통신이 아직 시작 및 실행되지 않습니다.. ■ **Ready**: 서버가 활성화되고 IP 통신이 시작되어 실행되며 RADIUS 모듈은 계정 시도를 수락 할 준비가됩니다. 죽음현상 (X seconds left): 이 서버에 대한 계정을 시도했지만 구성된 제한 시간 내에 응답하지 않았습니다. 서버는 일시적으로 비활성화되었지만 비활성 시간이 만료되면 다시 활성화됩니다. 이 발생하기 전에 남은 시간 (초)은 괄호 안에 표시됩니다. 이 상태는 둘 이상의 서버가 사용 가능할 때만 도달 할 수 있습니다.

버튼

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Refresh : 즉시 페이지를 새로고침합니다.

4.11.9 RADIUS Details

이 페이지는 특정 RADIUS 서버에 대한 자세한 통계를 제공합니다. 그림 4-11-10 의 서버 개요 RADIUS 인증 / 계정 화면이 나타납니다..

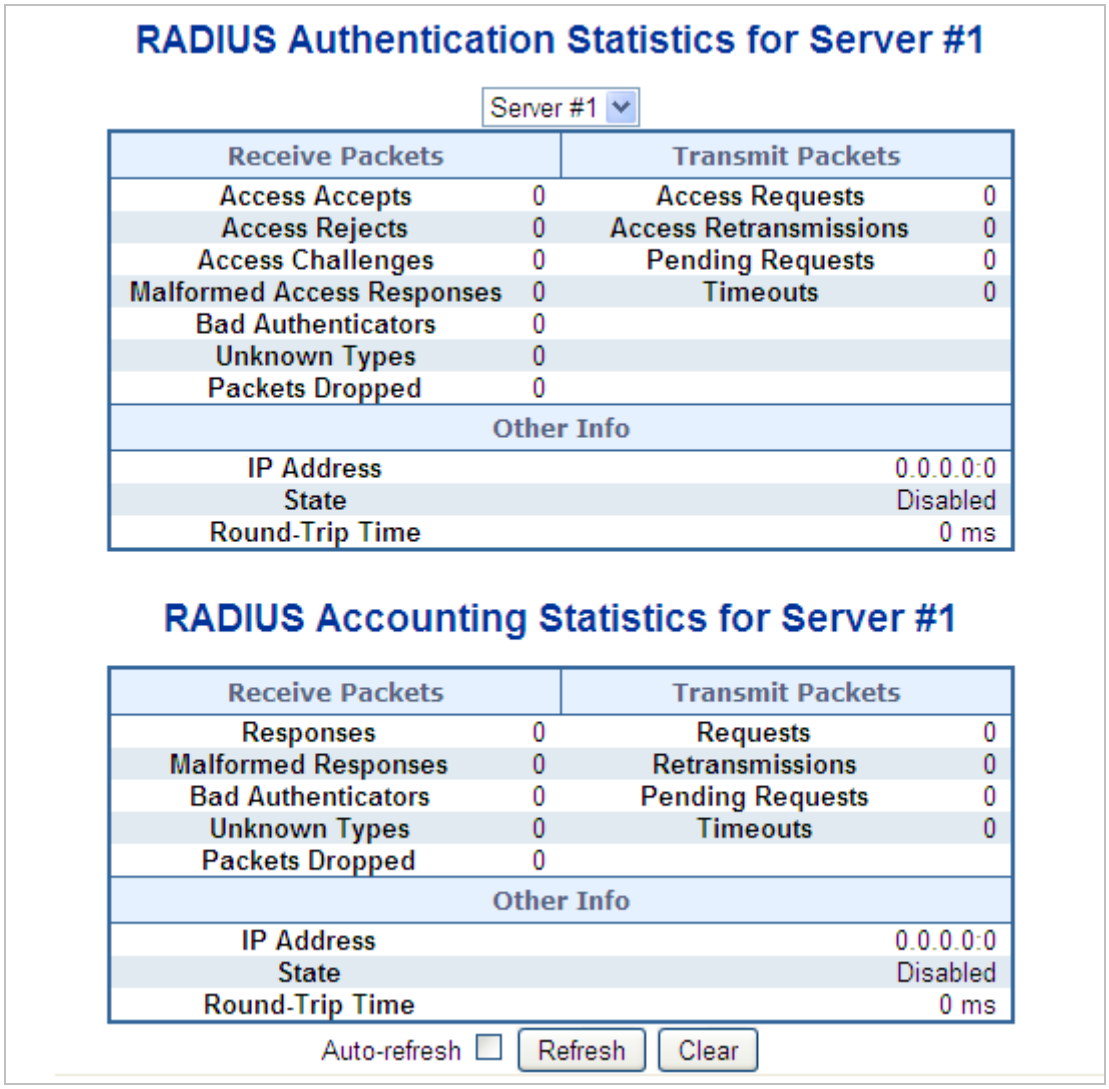


그림 4-11-10: RADIUS Authentication/Accounting for Server Overview 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

RADIUS Authentication Statistics

통계는 RFC4668 - RADIUS 인증 클라이언트 MIB 에 지정된 것과 밀접하게 매핑됩니다. 세부 사항을 표시 할 백엔드 서버 사이를 전환하려면 서버 선택 상자를 사용하십시오.

목적	설명			
• **Packet Counters**	RADIUS 인증 서버 패킷 카운터. 7 개의 수신 카운터와 4 개의 송신 카운터가 있습니다.			
	방향	**이름**	**RFC4668 이름**	**설명**
	Rx	**Access Accepts**	radiusAuthClientExtA	서버로부터 수신 한 RADIUS

		ccessAccepts	액세스 허용 패킷 (유효 또는 무효)의 수.
Rx	**Access Rejects**	radiusAuthClientExtAccessRejects	서버에서 수신 한 RADIUS 액세스 거부 패킷 수 (유효 또는 무효).
Rx	**Access Challenges**	radiusAuthClientExtAccessChallenges	서버로부터 수신 한 RADIUS 액세스 - 챌린지 패킷 (유효 또는 무효)의 수.
Rx	**Malformed Access Responses**	radiusAuthClientExtMalformedAccessResponses	서버에서 수신 한 잘못된 RADIUS 액세스 - 응답 패킷 수입니다. 잘못된 패킷에는 길이가 잘못된 패킷이 포함됩니다. 잘못된 인증 자나 메시지 인증 자 속성 또는 알 수없는 유형은 잘못된 형식의 응답으로 포함되지 않습니다..
Rx	**Bad Authenticators**	radiusAuthClientExtBadAuthenticators	서버에서 수신 한 유효하지 않은 인증 자 또는 Message Authenticator 특성을 포함하는 RADIUS 액세스 - 응답 패킷 수입니다.
Rx	**Unknown Types**	radiusAuthClientExtUnknownTypes	인증 포트에서 서버로부터 수신되고 다른 이유로 인해 삭제 된 RADIUS 패킷 수.
Rx	**Packets Dropped**	radiusAuthClientExtPacketsDropped	인증 포트에서 서버로부터 수신되고 다른 이유로 인해 삭제 된 RADIUS 패킷 수.
Tx	**Access Requests**	radiusAuthClientExtAccessRequests	서버에 보낸 RADIUS 액세스 요청 패킷 수입니다. 여기에는 재전송이 포함되지 않습니다.
Tx	**Access Retransmissions**	radiusAuthClientExtAccessRetransmissions	RADIUS 인증 서버에 재전송 된 RADIUS 액세스 요청 패킷 수입니다

	Tx	**Pending Requests**	radiusAuthClientExtPendingRequests	아직 시간 초과되지 않았거나 응답을받지 못한 서버를 대상으로하는 RADIUS 액세스 요청 패킷 수입니다. 이 변수는 Access-Accept, Access-Reject, Access-Challenge, 시간 초과 또는 재전송의 수신으로 인해 액세스 요청이 보내고 감소 될 때 증가합니다.
	Tx	**Timeouts**	radiusAuthClientExtTimeouts	서버에 대한 인증 시간 초과 횟수입니다. 시간 초과 후 클라이언트는 동일한 서버로 다시 시도하거나 다른 서버로 보내거나 포기할 수 있습니다. 동일한 서버에 대한 재시도는 재전송과 시간 초과로 계산됩니다. 다른 서버로 보내지는 요청은 시간 제한과 함께 계산됩니다.

- **Other Info**

이 절에는 서버 상태 및 최신 왕복 시간에 대한 정보가 들어 있습니다.

Name	RFC4668 Name	설명
IP Address	-	해당 인증 서버의 IP 주소 및 UDP 포트 서버의 상태를 표시합니다.
State	-	다음 중 하나의 값이 적용됩니다.: ■ **Disabled**: 선택 된 서버는 비활성화됩니다. ■ **Not Ready**: 서버가 활성화되어 있지만 IP 통신이 아직 시작 및 실행되지 않습니다. ■ **Ready**: 서버가 활성화되고 IP 통신이 시작되어 실행되며 RADIUS 모듈은 액세스 시도를 수락할 준비가됩니다. ■ **Dead (X seconds left)**: 이 서버에 대한 액세스가 시도되었지만 구성된 제한 시간 내에 응답하지 않았습니다. 서버는 일시적으로 비활성화되었지만 불감 시간이 만료되면 다시 활성화됩니다.
Round-Trip	radiusAuthClient	발생하기 전에 남은 시간 (초)은 괄호 안에

	Time	ExtRoundTripTime	표시됩니다. 이 상태는 둘 이상의 서버가 사용 가능할 때만 도달 할 수 있습니다. 가장 최근의 Access-Reply / Access-Challenge 와 RADIUS 인증 서버에서 일치 한 Access-Request 간의 시간 간격 (밀리 초 단위). 이 측정의 입도는 100ms 입니다. 0ms 의 값은 서버와의 왕복 통신이 아직 없음을 나타냅니다.

RADIUS Accounting Statistics

통계는 RFC4670 - RADIUS Accounting Client MIB 에 지정된 것과 밀접하게 매핑됩니다. 세부 사항을 표시 할 백엔드 서버 사이를 전환하려면 서버 선택 상자를 사용하십시오..

목적	설명			
• **Packet Counters**	RADIUS 계정 서버 패킷 카운터. 5 개의 수신 카운터와 4 개의 송신 카운터가 있습니다.			
	방향	**이름**	**RFC4670 이름**	**설명**
	Rx	**Responses**	radiusAccClientExtResponses	서버에서 수신 한 RADIUS 패킷 수 (유효 또는 무효).
	Rx	**Malformed Responses**	radiusAccClientExtMalformedResponses	서버에서 수신 한 잘못된 RADIUS 패킷 수입니다. 잘못된 패킷에는 길이가 잘못된 패킷이 포함됩니다. 잘못된 인증 자 또는 알 수없는 유형은 잘못된 형식의 액세스 응답으로 포함되지 않습니다.
	Rx	**Bad Authenticators**	radiusAcctClientExtBadAuthenticators	서버에서 수신 한 유효하지 않은 인증자를 포함하는 RADIUS 패킷의 수.
	Rx	**Unknown Types**	radiusAccClientExtUnknownTypes	계정 포트에서 서버로부터 수신 된 알 수없는 유형의 RADIUS 패킷 수입니다.
	Rx	**Packets Dropped**	radiusAccClientExtPacketsDropped	계정 포트에서 서버로부터 수신 된 RADIUS 패킷 수. 다른 이유로 인해

				삭제되었습니다.
	Tx	**Requests**	radiusAccClientExtRequests	서버로 보낸 RADIUS 패킷 수. 여기에는 재전송이 포함되지 않습니다.
	Tx	**Retransmissions**	radiusAccClientExtRetransmissions	RADIUS 계정 서버에 재전송 된 RADIUS 패킷 수입니다.
	Tx	**Pending Requests**	radiusAccClientExtPendingRequests	아직 시간 초과되지 않았거나 응답을받지 못한 서버를 대상으로하는 RADIUS 패킷 수입니다. 이 변수는 응답, 시간 초과 또는 재전송의 수신으로 인해 요청이 보내고 감소 될 때 증가합니다.
	Tx	**Timeouts**	radiusAccClientExtTimeouts	서버에 대한 계정 시간 종료 횟수. 시간 초과 후 클라이언트는 동일한 서버로 다시 시도하거나 다른 서버로 보내거나 포기할 수 있습니다. 동일한 서버에 대한 재시도는 재전송과 시간 초과로 계산됩니다. 다른 서버로 보내지는 요청은 시간 제한과 함께 계산됩니다

- **Other Info**

이 절에는 서버 상태 및 최신 왕복 시간에 대한 정보가 들어 있습니다.

이름	RFC4670 이름	설명
IP Address	-	해당 카운팅 서버의 IP 주소 및 UDP 포트
State	-	서버의 상태를 표시합니다. 다음 값 중 하나를 취합니다.: ■ **Disabled**: 선택한 서버가비활성화됩니다. ■ **Not Ready**: 서버가 활성화되어 있지만 IP 통신이 아직 시작 및 실행되지 않습니다.. ■ **Ready**: 서버가 활성화되고 IP 통신이 시작되어 실행되며 RADIUS 모듈은 계정 시도를 수락 할 준비가됩니다.. ■ **Dead (X seconds left)**: 이 서버에 대한

			계정 시도가 이루어졌지만 구성된 제한 시간 내에 응답하지 않았습니다. 서버는 일시적으로 비활성화되었지만 불감 시간이 만료되면 다시 활성화됩니다. 이 발생하기 전에 남은 시간 (초)은 괄호 안에 표시됩니다. 이 상태는 둘 이상의 서버가 사용 가능할 때만 도달 할 수 있습니다.
Round-Trip Time	radiusAccClientExtRoundTripTime	■	가장 최근의 응답과 RADIUS 계정 서버에서 일치시킨 요청 간의 시간 간격 (밀리 초 단위). 이 측정의 입도는 100ms 입니다. 0ms 의 값은 서버와의 왕복 통신이 아직 없음을 나타냅니다

버튼

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Refresh : 즉시 페이지를 새로고침합니다.

Clear : 선택한 서버의 카운터를 지 웁니다. "보류중인 요청"카운터는이 작업으로 지워지지 않습니다.

4.11.10 Windows Platform RADIUS Server Configuration

RADIUS 서버를 설정하고 클라이언트 IP 주소를 관리형 스위치에 할당하십시오. 이 경우 192.168.0.100 의 관리 대상 스위치의 기본 IP 주소에있는 필드. 또한 공유 비밀 키가 관리형 스위치의 802.1x 시스템 구성 (이 경우 12345678)에서 설정 한 것과 같아야합니다.

1. 원격 RADIUS 서버 및 비밀 키의 IP 주소를 구성하십시오.

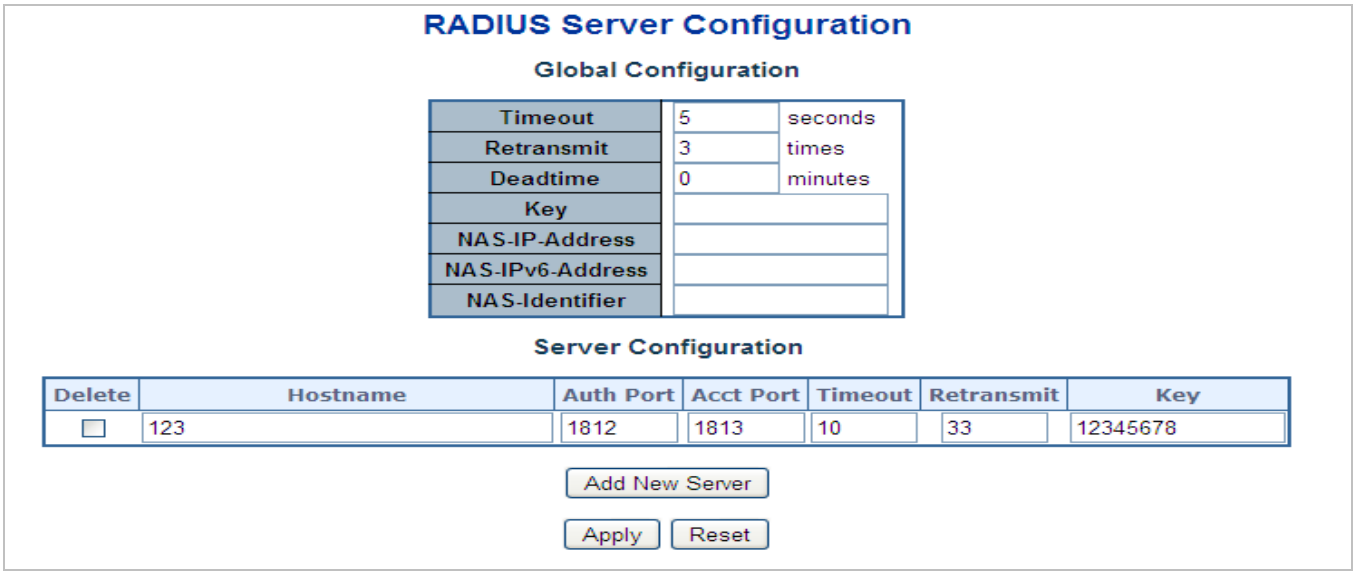


그림 4-11-11: RADIUS Server 설정 화면

2. Windows 2003 서버에 새 RADIUS Cleint 를 추가하십시오.

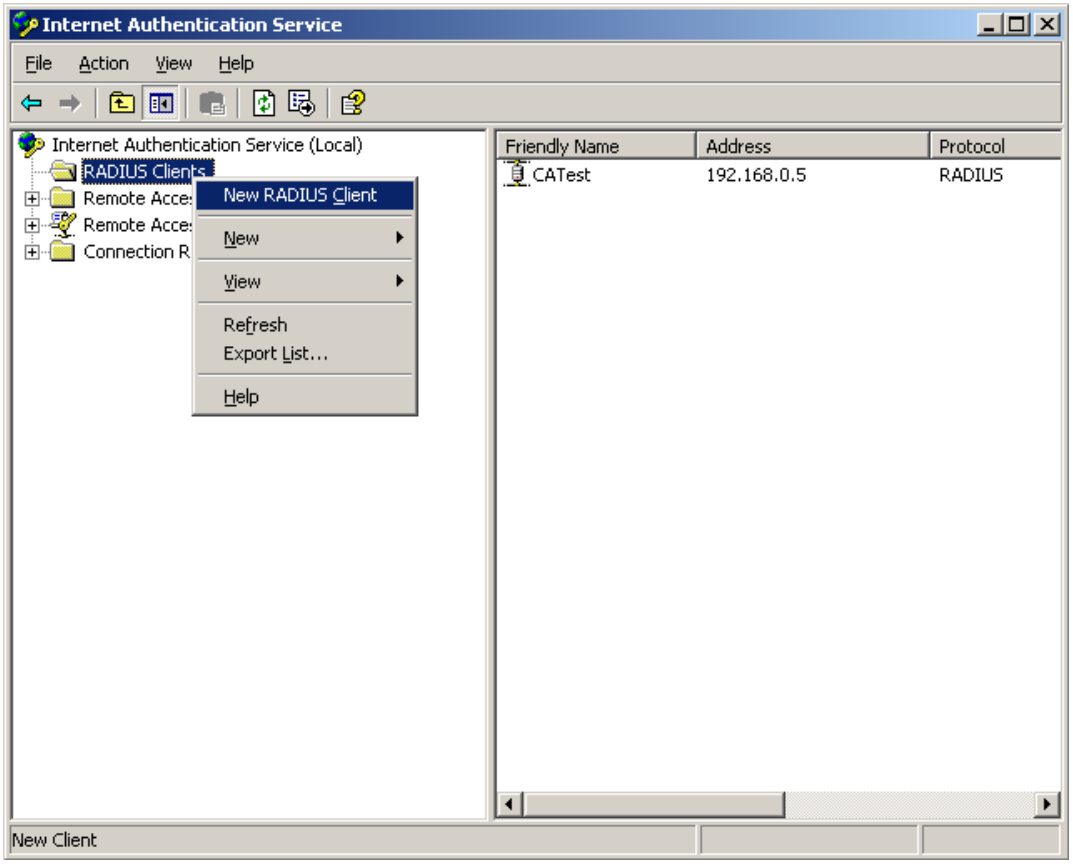


그림 4-11-12: Windows 서버 - 새 RADIUS 클라이언트 설정 추가

3. 관리 대상 스위치에 클라이언트 IP 주소 할당

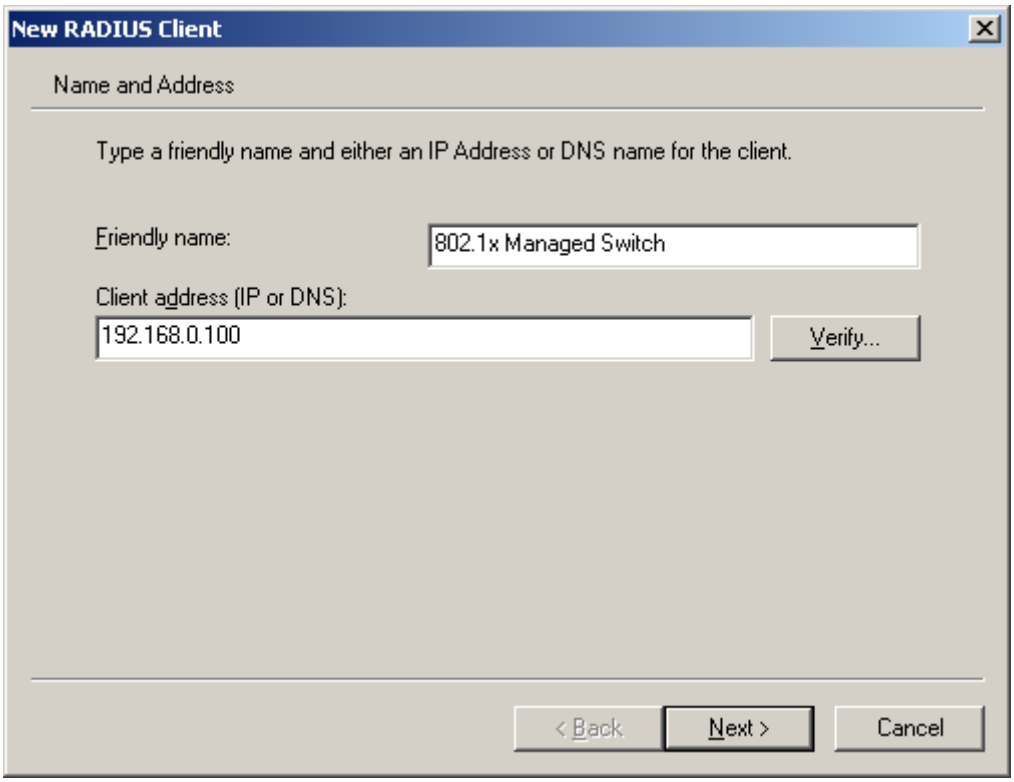


그림 4-11-13: Windows Server RADIUS 서버 설정

4. 공유 비밀 키는 관리형스위치에 구성된 키와 같아야합니다.

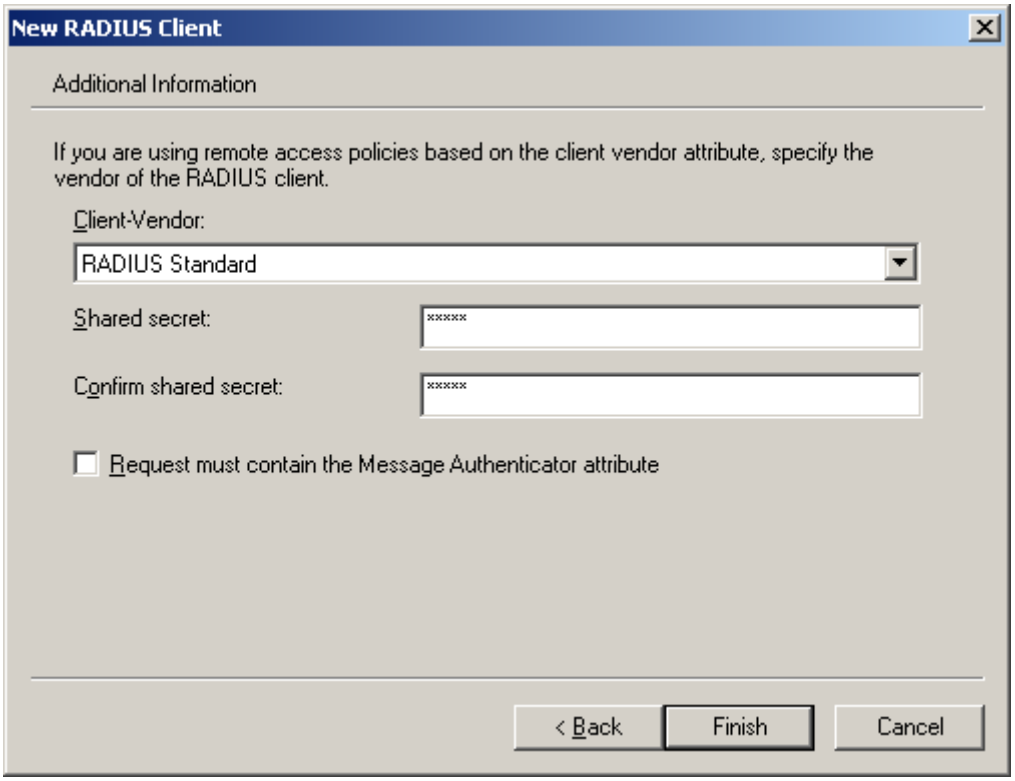


그림 4-11-14: Windows Server RADIUS 서버 셋팅

5. "802.1X Port Configuration"과 같은 속성 802.1X 을 구성합니다.

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
1	Port-based 802.1X	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
2	Port-based 802.1X	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize

그림 4-11-15: 802.1x 포트 설정

6. 사용자 데이터를 만듭니다. 사용자 데이터 설정은 Radius Server PC 에서 만들어야합니다. 예를 들어 Radius Server 는 Win2003 Server 에 기반을두고 다음을 수행합니다.:

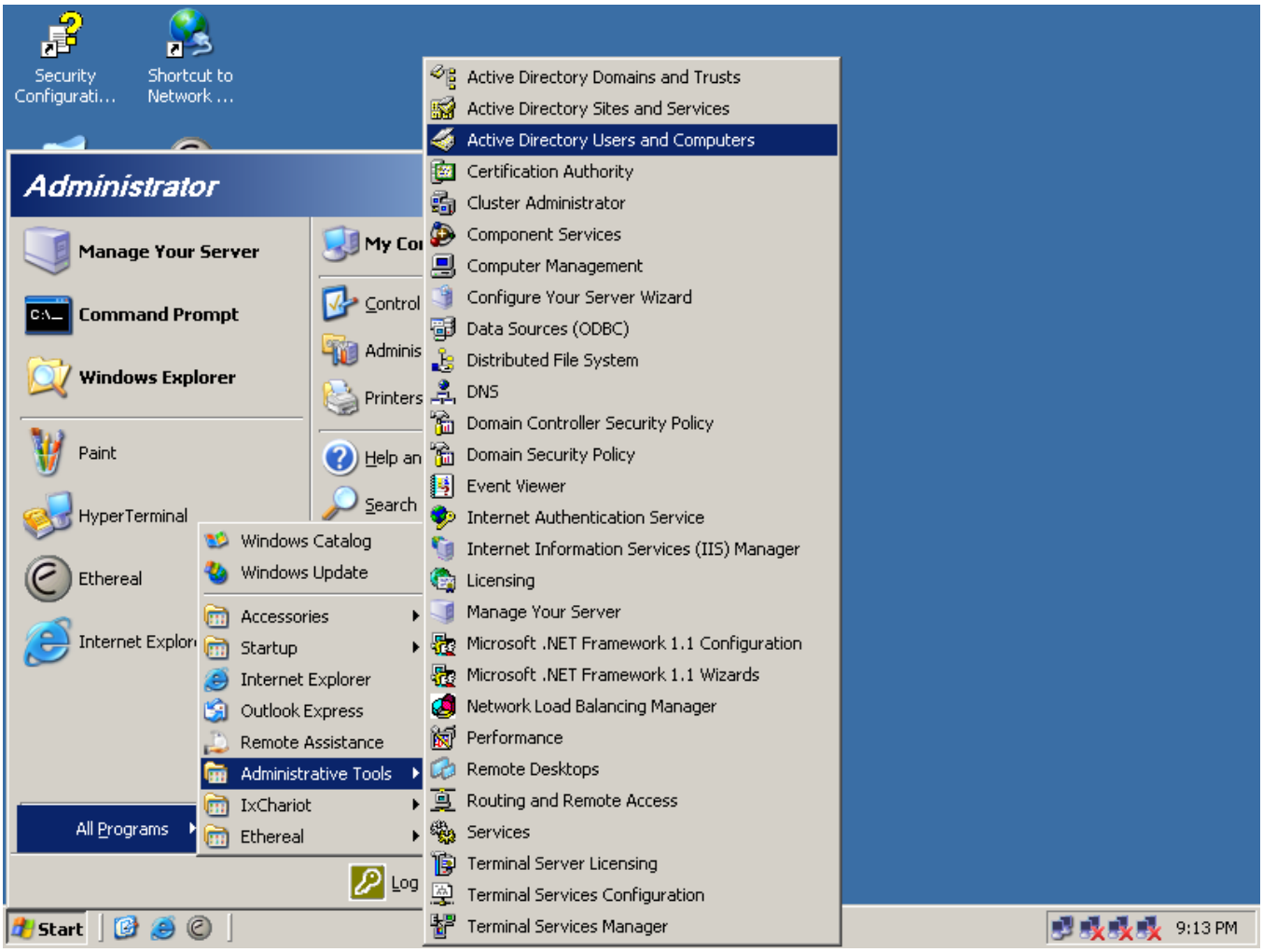


그림 4-11-16: Windows 2003 AD Server Setting Path

7. "Active Directory 사용자 및 컴퓨터"를 입력하고 합법적 인 사용자 데이터를 만듭니다. 다음으로 속성을 입력하기 위해 생성 한 사용자를 마우스 오른쪽 단추로 클릭하고 주목할 대상을 선택합니다.:

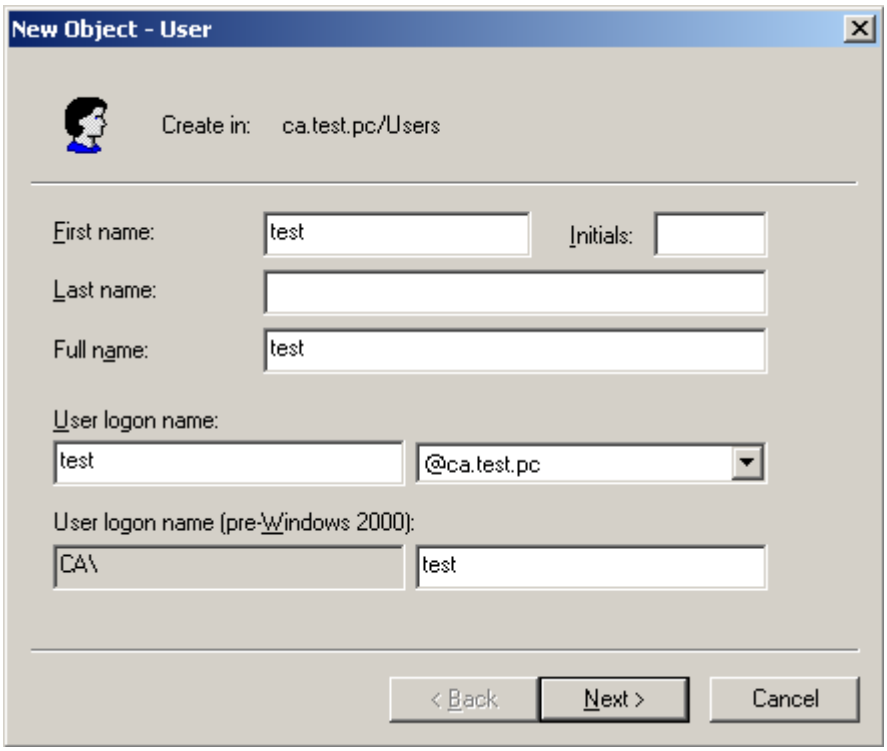


그림 4-11-17: 사용자 추가 설정화면

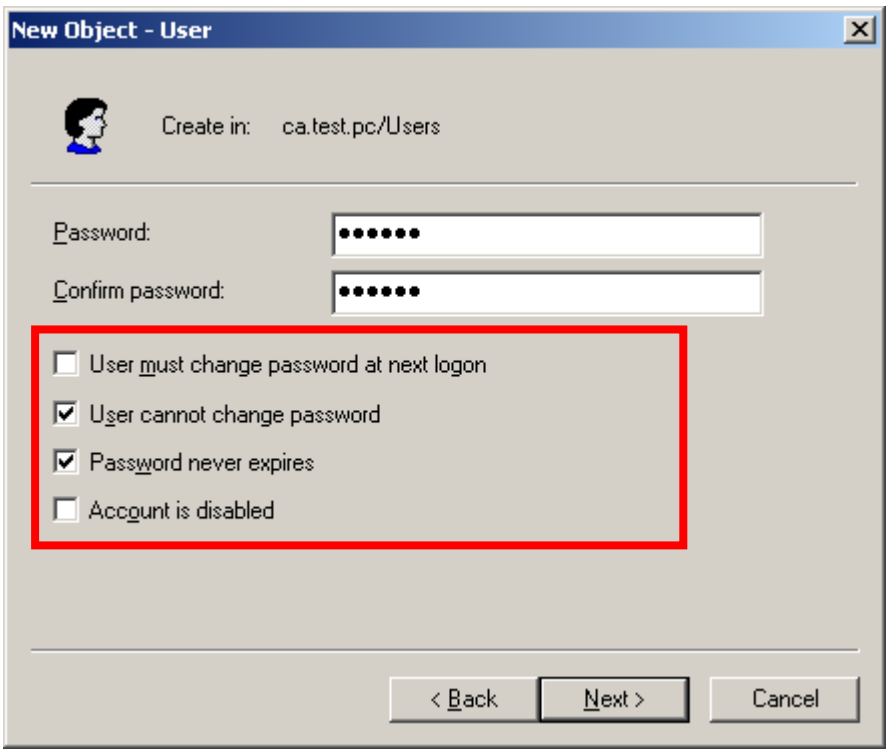


그림 4-11-18: 사용자 옵션 구성화면

Note

포트가 RADIUS 서버에 연결되어 있거나 포트가 다른 스위치에 연결된 업 링크 포트 인 경우 포트 인증 상태를 "인증 된 포트"로 설정합니다. 또는 802.1X 가 작동하기 시작하면 스위치가 RADIUS 서버에 액세스하지 못할 수 있습니다.

4.11.11 802.1X Client Configuration

Windows XP 는 원래 802.1X 를 지원합니다. 다른 운영 체제 (Windows 98SE, ME, 2000)의 경우 802.1X 클라이언트 유틸리티가 필요합니다. 다음 절차에서는 Windows XP 에서 802.1x 인증을 구성하는 방법을 보여줍니다.
무선 클라이언트의 802.1x 인증 유형을 변경하려는 경우 (예 : EAP-MD5 에서 EAP-TLS 로 전환하려는 경우) 먼저 기존 연결에서 기존의 기존 무선 네트워크를 제거한 다음 다시 추가해야합니다..

■ 구성예제: EAP-MD5 인증

1. 시작에서> 제어판에서 "네트워크 연결".을 더블클릭합니다.
2. 오른쪽마우스로 로컬네트워크 연결을 클릭합니다
3. 윈도우 설정에 속성(Properties)을 누릅니다.

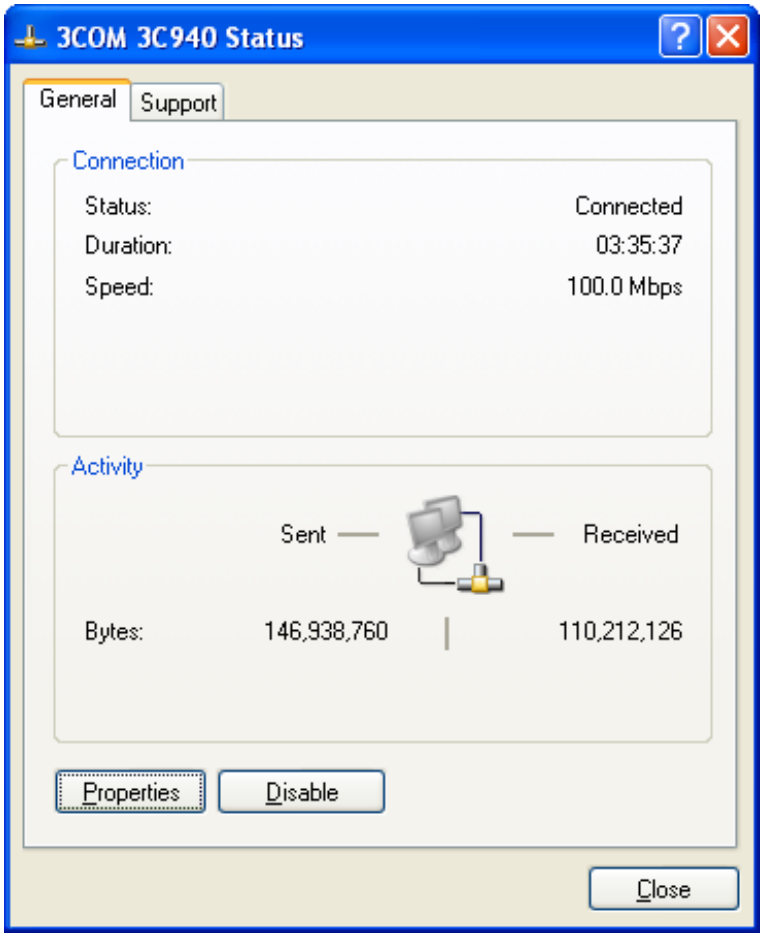


그림4-11-19

4. 메뉴에 "**Authentication**" 선택하합니다.
5. "**Enable network access control using IEEE 802.1X**" 을 선택하여, IEEE 802.1x authentication 활성화시킵니다.
6. EAP 유형의 드롭 다운 목록 상자에서. "**MD-5 Challenge**"을 선택합니다.

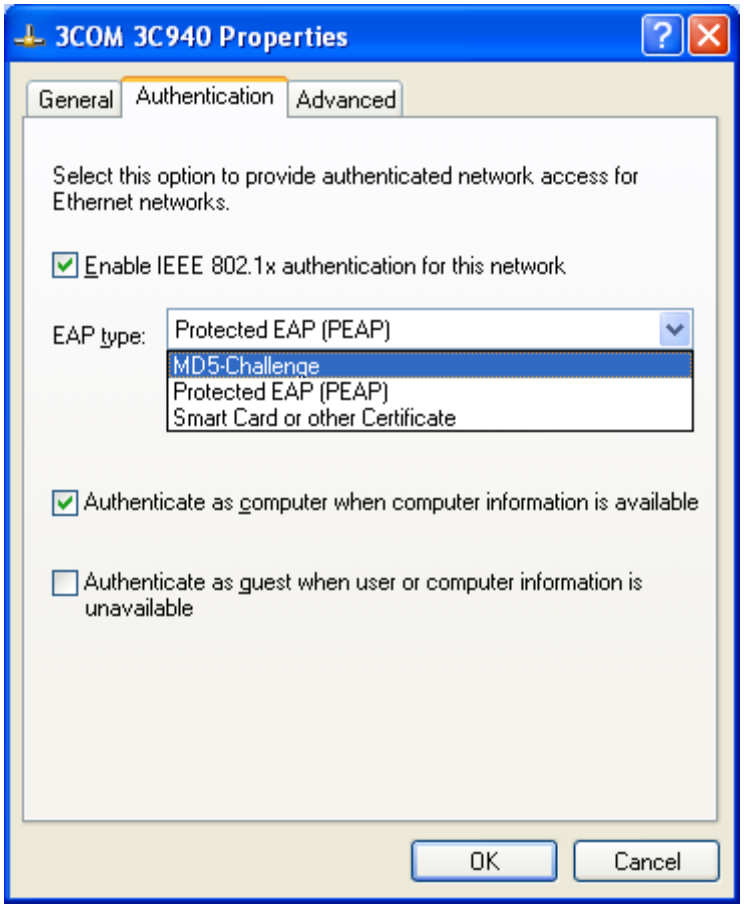


그림4-11-20

7. "**OK(확인)**"을 선택합니다..
8. 클라이언트가 관리형 스위치와 연결되면 사용자 인증 고지가 시스템 트레이에 나타납니다. 계속하려면 알림을 클릭하십시오..

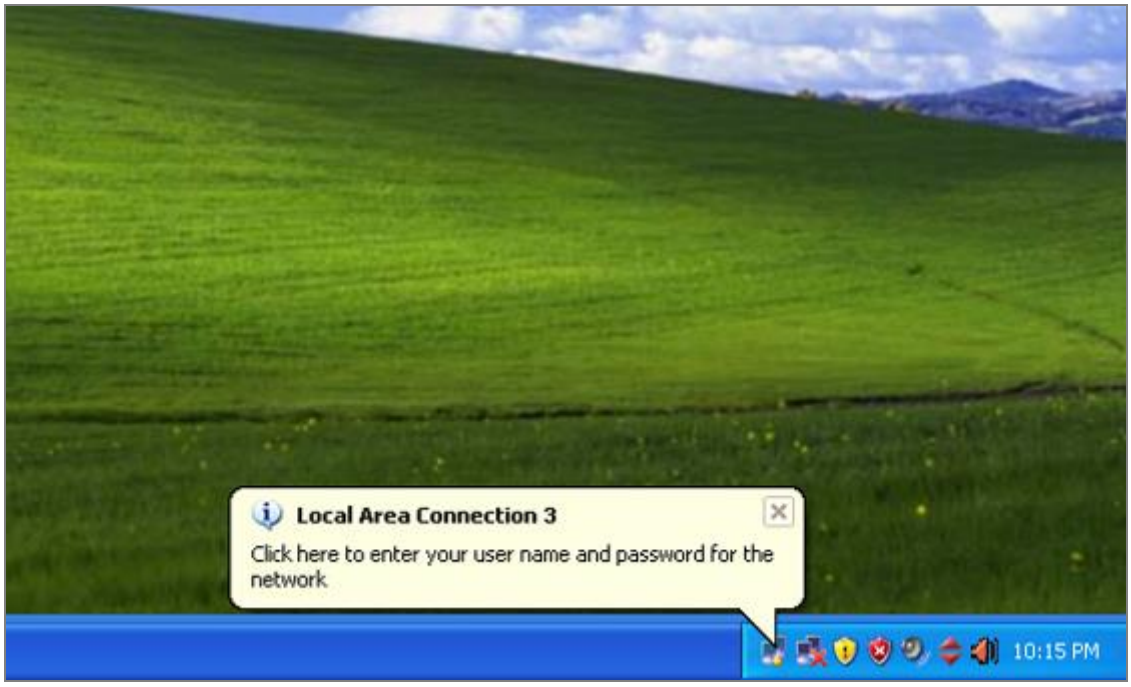


그림4-11-21: Windows 클라이언트 팝업 로그인 요청 메시지

9. 계정이 속한 사용자 이름, 암호 및 로그온 도메인을 입력하십시오..
10. "확인"을 클릭하여 유효성 검사 프로세스를 완료하십시오.

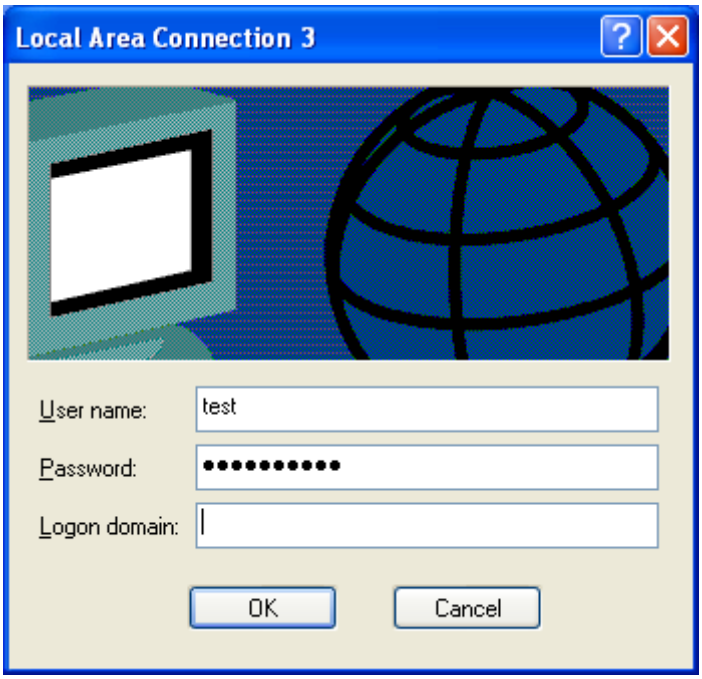


그림4-11-22

4.12 Security(보안)

이 섹션에서는 사용자 액세스 및 관리 제어를 포함하여 관리 대상 스위치의 액세스를 제어합니다.
보안 페이지에는 다음 기본 주제에 대한 링크가 있습니다.:

- **Port Limit Control**
- **Access Management**
- **HTTPs / SSH**
- **DHCP Snooping**
- **IP Source Guard**
- **ARP Inspection**

4.12.1 Port Limit Control

이 페이지에서는 포트 보안 제한 제어 시스템 및 포트 설정을 구성 할 수 있습니다. 제한 제어는 주어진 포트에서 사용자 수를 제한 할 수있게합니다. 사용자는 MAC 주소 및 VLAN ID 로 식별됩니다. 제한 제어가 포트에서 활성화되면 제한은 포트의 최대 사용자 수를 지정합니다. 이 수가 초과되면 조치가 취해집니다. 조치는 아래 설명 된 4 가지 조치 중 하나 일 수 있습니다.
제한 제어 모듈은 포트에서 학습 한 MAC 주소를 관리하는 포트 보안 모듈 인 하위 계층 모듈을 사용합니다. 제한 제어 구성은 시스템 및 포트와 같은 두 섹션으로 구성됩니다. 그림 4-12-1 의 포트 제한 제어 구성 화면이 나타납니다..

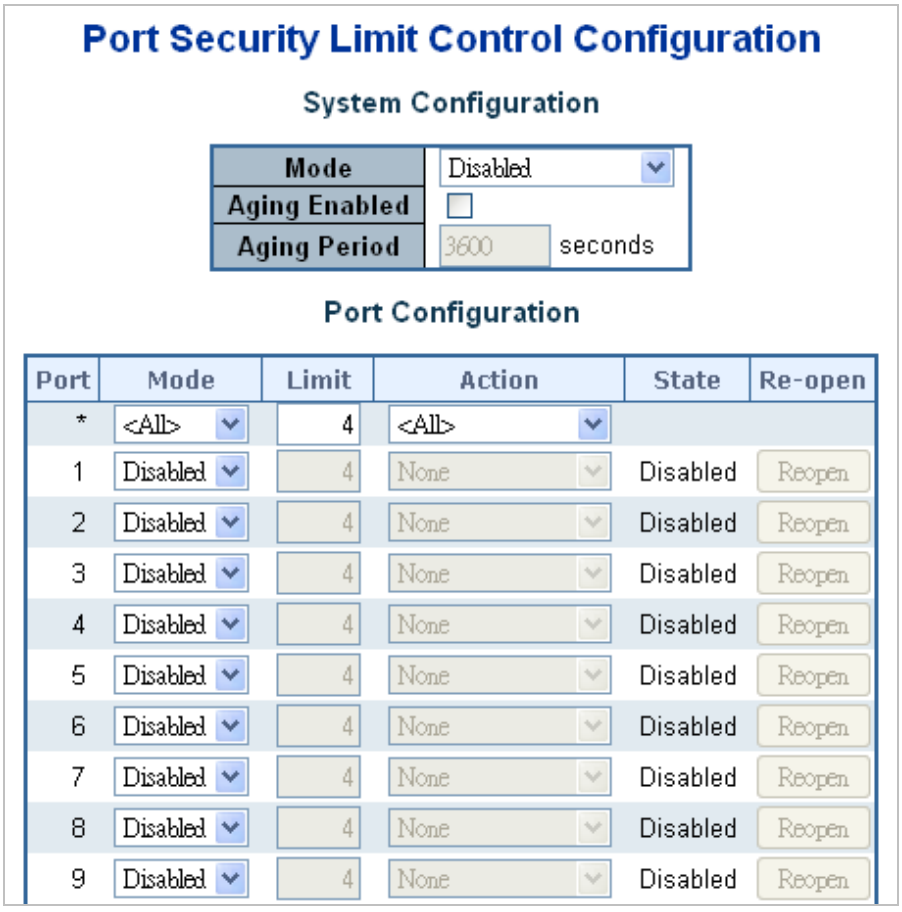


그림 4-12-1: Port Limit Control Configuration 개요 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

System Configuration

목적	설명
• **Mode**	제한 제어가 스위치에서 전체적으로 활성화 또는 비활성화되었는지 나타냅니다. 전역 적으로 사용할 수없는 경우 다른 모듈에서도 여전히 기본 기능을 사용할 수 있지만 제한 검사 및 해당 작업은 사용할 수 없습니다.
• **Aging Enabled**	옵션을 선택하면 에이징 기간에 설명 된대로 보안 MAC 주소가 고갈 될 수 있습니다.
• **Aging Period**	Aging Enabled 가 선택되면 에이징 기간이이 입력으로 제어됩니다. 다른 모듈이 기본 포트 보안을 사용하여 MAC 주소를 보호하는 경우 에이징 기간에 대한 다른 요구 사항이있을 수 있습니다. 기본 포트 보안은 기능을 사용하는 모든 모듈의 요구 된 더 짧은 에이징 기간을 사용합니다. 에이징 기간은 10 에서 10,000,000 초 사이의 숫자로 설정할 수 있습니다. 노후화가 필요한 이유를 이해하려면 다음 시나리오를 고려하십시오. 최종 호스트가 타사 스위치 또는 허브에 연결되어 있고이 포트가 제한 제어가 활성화 된이 스위치의 포트에 연결되어 있다고 가정합니다. 최종 호스트는 제한을 초과하지 않으면 전달할 수 있습니다. 이제 최종 호스트가 로그 오프하거나 전원이 꺼 졌다고 가정 해보십시오. 고령화가 아니라면 최종 호스트는이 스위치로 자원을 계속 사용하고 전달할 수 있습니다. 이 상황을 극복하기 위해 노화를 활성화하십시오. 에이징을 사용하도록 설정하면 최종 호스트가 보호되면 타이머가 시작됩니다. 타이머가 만료되면 스위치는 최종 호스트에서 프레임을 찾기 시작하고 이러한 프레임이 다음 에이징 기간 내에 표시되지 않으면 최종 호스트는 연결이 해제 된 것으로 간주되어 해당 리소스가 스위치에서 해제됩니다.

Port Configuration

다음 표는 아래와 같은 기능과 설명이 있습니다.:

목적	설명
• **Port**	아래 구성이 적용되는 포트 번호입니다.
• **Mode**	Limit Control 기능이 포트에서 활성화되었는지 여부를 제어합니다. Limit Control 을 적용하려면 이 모드와 Global Mode 를 모두 Enabled 로 설정해야합니다. 다른 모듈은 주어진 포트에서 제한 제어를 활성화하지 않고 기본 포트 보안 기능을 계속 사용할 수 있습니다.
• **Limit**	이 포트에서 보호 할 수있는 최대 MAC 주소 수입니다. 이 수는 1024 를

	초과 할 수 없습니다. 한계를 초과하면 해당 조치가 수행됩니다. 스위치는 포트 보안이 활성화 된 포트에 새로운 MAC 주소가 표시 될 때마다 모든 포트가 그려지는 전체 MAC 주소 수와 함께 "발생"합니다. 모든 포트가 동일한 풀에서 가져 오므로 나머지 포트가 이미 사용 가능한 모든 MAC 주소를 사용하고 있으면 구성된 최대 값을 부여 할 수 없습니다.
• **Action**	한도에 도달하면 스위치는 다음 작업 중 하나를 수행 할 수 있습니다.: ■ **None**: 포트에서 MAC 주소를 제한하지 않고 더 이상 허용하지 마십시오. ■ **Trap**: 포트에 Limit + 1 MAC 주소가 표시되면 SNMP 트랩을 보냅니다. 에이징을 사용하지 않으면 하나의 SNMP 트랩 만 전송되지만 에이징을 사용하면 한계를 초과 할 때마다 새 SNMP 트랩이 전송됩니다... ■ **Shutdown**: 포트에 Limit + 1 MAC 주소가 표시되면 포트를 종료하십시오. 이것은 모든 보안 MAC 주소가 포트에서 제거되고 새로운 것이 배워지지 않는다는 것을 의미합니다. 포트에서 물리적으로 연결이 끊어지고 다시 연결 되더라도 (케이블을 분리하여) 포트는 계속 종료됩니다. 포트를 다시 열려면 세 가지 방법이 있습니다. 1) 스위치를 부팅하고 2) 포트 또는 스위치의 제한 제어를 비활성화한 다음 다시 활성화합니다. 3) Re-open 버튼을 클릭하십시오. ■ **Trap & Shutdown**: 포트에 제한값+1 을 MAC 주소가 표시되면 위에서 설명한 "Trap" 및 "Shutdown" 동작이 사용합니다..
• **State**	다음 열은 Limit Control 의 관점에서 본 포트의 현 상태를 보여줍니다. 다음 4 가지 성격중 한가지를 가집니다. ■ **Disabled**: Limit Control 에서 전역에 비활성화가 되거나 포트에서 비활성화됩니다. ■ **Ready**: 한도에 아직 도달하지 못했습니다. 이것은 모든 작업에 대해 표시 될 수 있습니다 ■ **Limit Reached**: 이 포트에서 한도에 도달했음을 나타냅니다. 이 상태는 동작이 없음 또는 트랩으로 설정된 경우에만 표시 될 수 있습니다. ■ **Shutdown**: 포트가 제한 제어 모듈에 의해 종료되었음을 나타냅니다. 이 상태는 동작이 종료 또는 트랩 및 종료로 설정된 경우에만 표시 될 수 있습니다.
• **Re-open Button**	이 모듈에 의해 포트가 종료 된 경우이 버튼을 클릭하여 다시 열 수 있습니다.이 경우이 경우에만 활성화됩니다. 다른 방법에 대해서는 동작 절의

	종료를 참조하십시오. 다시 열 버튼을 클릭하면 페이지가 새로 고쳐 지므로 커밋되지 않은 변경 사항이 손실됩니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

Refresh: 페이지를 새로 고칩니다. 적용되지 않은 변경사항은 손실됩니다.

4.12.2 Access Management

이 페이지에서 액세스 관리 표를 구성하십시오. 최대 항목 수는 16 입니다. 응용 프로그램의 유형이 액세스 관리 항목 중 하나와 일치하면 스위치에 대한 액세스가 허용됩니다. 그림 4-12-2 의 Access Management Configuration 화면이 나타납니다..

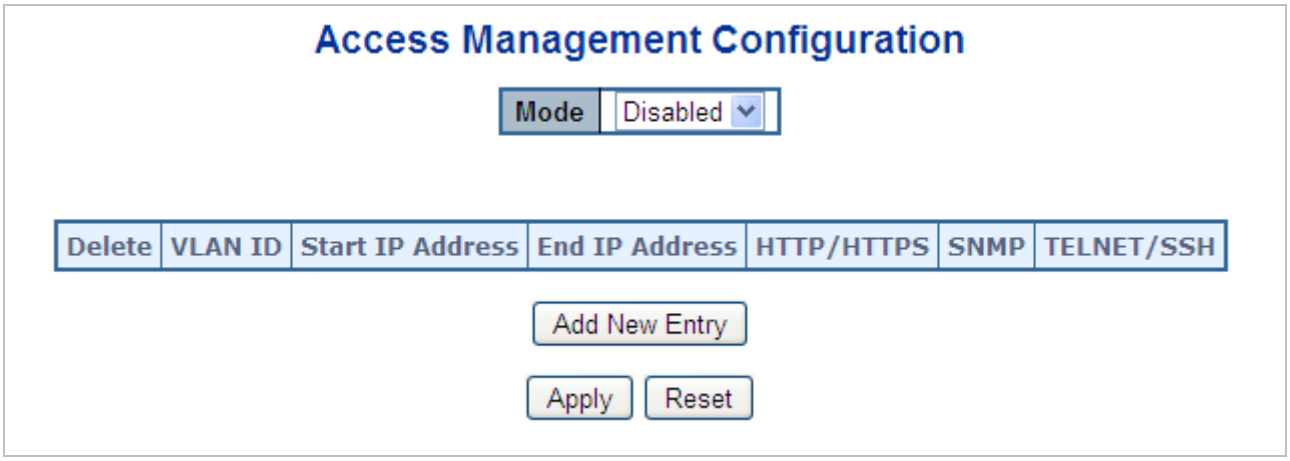


그림 4-12-2: Access Management Configuration Overview 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Mode**	액세스 관리 모드 조작을 나타냅니다. 가능한 모드는 다음과 같습니다.: Enabled: 액세스 관리 모드 조작을 사용 가능하게하십시오. Disabled: 액세스 관리 모드 작업을 비활성화합니다.
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 적용시 삭제됩니다
• **VLAN ID**	액세스 관리 항목의 VLAN ID 를 나타냅니다
• **Start IP address**	액세스 관리 항목의 시작 IP 주소를 나타냅니다.
• **End IP address**	액세스 관리 항목의 끝 IP 주소를 나타냅니다.
• **HTTP/HTTPS**	호스트가 호스트 IP 주소가 항목과 일치하는 HTTP / HTTPS 인터페이스에서 스위치에 액세스 할 수 있음을 나타냅니다.
• **SNMP**	호스트가 호스트 IP 주소가 항목과 일치하는 SNMP 인터페이스에서 스위치에 액세스 할 수 있음을 나타냅니다.
• **TELNET/SSH**	호스트가 호스트 IP 주소가 항목과 일치하는 TELNET / SSH 인터페이스에서 스위치에 액세스 할 수 있음을 나타냅니다.

버튼

Add New Entry: 새 액세스 관리 항목을 추가하려면 클릭하십시오.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.12.3 Access Management Statistics

이 페이지는 액세스 관리에 대한 통계를 제공합니다. 그림 4-12-3 의 액세스 관리 통계 화면이 나타납니다..

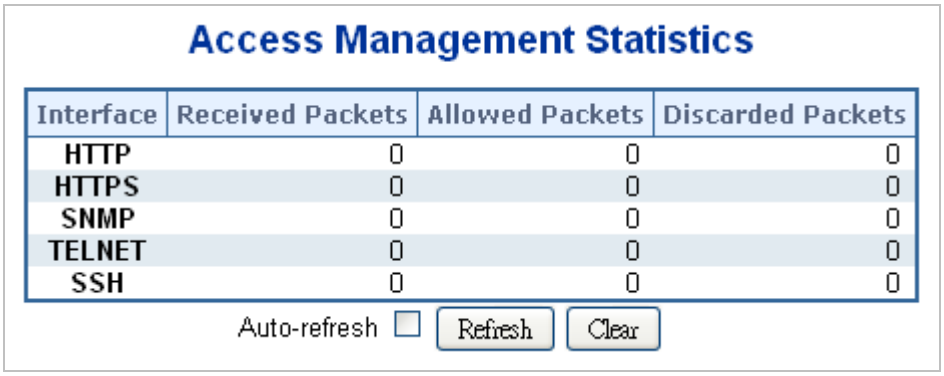


그림 4-12-3: Access Management Statistics Overview 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Interface**	원격 호스트를 허용 한 인터페이스가 스위치에 액세스 할 수 있습니다.
• **Receive Packets**	액세스 관리 모드에서 인터페이스로부터 수신 된 패킷 번호가 사용 가능합니다.
• **Allow Packets**	액세스 관리 모드에서 인터페이스에서 허용 된 패킷 수를 사용할 수 있습니다.
• **Discard Packets**	액세스 관리 모드에서 인터페이스에서 버려진 패킷 번호가 사용 가능합니다.

버튼

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Refresh: 즉시 페이지를 새로고침합니다.

Clear: 모든 통계 항목을 지웁니다..

4.12.4 HTTPs

이 페이지에서 HTTPS 를 구성하십시오. 그림 4-12-4 의 HTTPS 구성 화면이 나타납니다..

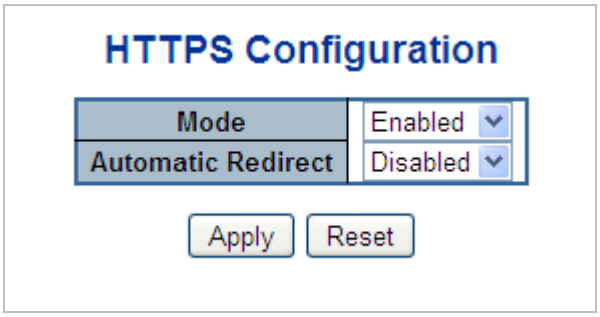


그림 4-12-4: HTTPS Configuration Screen 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Mode**	HTTPS 모드 작업을 나타냅니다. 현재 연결이 HTTPS 인 경우 HTTPS 사용 안 함 모드를 적용하면 웹 브라우저가 자동으로 HTTP 연결로 리디렉션됩니다. 가능한 모드는 다음과 같습니다.: ■ **Enabled**: HTTPS 모드를 작동시켜 활성화합니다. ■ **Disabled**: HTTPS 모드를 작동시켜 활성화합니다.
• **Automatic Redirect**	HTTPS 리디렉션 모드 작업을 나타냅니다. HTTPS 모드 "Enabled"가 선택된 경우에만 중요합니다. HTTPS 모드와 자동 리디렉션이 모두 활성화 된 경우 자동으로 웹 브라우저를 HTTPS 연결로 리디렉션하거나 둘 다 사용할 수없는 경우 웹 브라우저를 HTTP 연결로 리디렉션합니다. 가능한 모드는 다음과 같습니다.: ■ **Enabled**: HTTPS 리디렉션 모드로 활성화합니다.. ■ **Disabled**: HTTPS 리디렉션 모드로 비활성화합니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.12.5 SSH

이 페이지에서 SSH 를 구성하십시오. 이 페이지는 포트 보안 상태를 표시합니다. 포트 보안은 직접 구성이없는 모듈입니다. 구성은 다른 모듈 (사용자 모듈)에서 간접적으로 발생합니다. 사용자 모듈이 포트에서 포트 보안을 활성화하면 포트는 소프트웨어 기반 학습용으로 설정됩니다. 이 모드에서는 알 수없는 MAC 주소의 프레임이 포트 보안 모듈로 전달되며, 포트 보안 모듈은 모든 사용자 모듈에게이 새 MAC 주소가 전달되거나 차단 될지 여부를 묻습니다. 포워딩 상태로 설정할 MAC 주소의 경우, 활성화 된 모든 사용자 모듈은 MAC 주소 전달을 허용하는 만장일치로 동의해야합니다. 오직 하나만 차단하도록 선택하면 사용자 모듈이 다르게 결정할 때까지 차단됩니다.
상태 페이지는 두 개의 섹션으로 나뉩니다. 하나는 범례 사용자 모듈이 있고 다른 하나는 실제 포트 상태입니다. 그림 4-12-5 의 SSH Configuration 화면이 나타납니다..

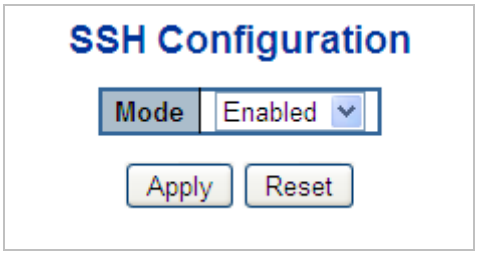


그림 4-12-5: SSH Configuration Screen 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Mode**	SSH 모드 작동을 나타냅니다. 가능한 모드는 다음과 같습니다.: ■ **Enabled**: SSH Mode 를 활성화합니다.. ■ **Disabled**: SSH Mode 를 비활성화합니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.12.6 Port Security Status

이 페이지는 포트 보안 상태를 표시합니다. 포트 보안은 직접 구성이 없는 모듈입니다. 구성은 다른 모듈 (사용자 모듈)에서 간접적으로 발생합니다. 사용자 모듈이 포트에서 포트 보안을 활성화하면 포트가 다음과 같이 설정됩니다. 소프트웨어 기반 학습. 이 모드에서는 알 수없는 MAC 주소의 프레임이 포트 보안 모듈로 전달되며, 포트 보안 모듈은 모든 사용자 모듈에게이 새 MAC 주소가 전달되거나 차단 될지 여부를 묻습니다. 포워딩 상태로 설정할 MAC 주소의 경우, 활성화 된 모든 사용자 모듈은 MAC 주소 전달을 허용하는 만장일치로 동의해야합니다. 오직 하나만 차단하도록 선택하면 사용자 모듈이 다르게 결정할 때까지 차단됩니다.

상태 페이지는 두 개의 섹션으로 나뉩니다. 하나는 범례 사용자 모듈이 있고 다른 하나는 실제 포트 상태입니다.
그림 4-12-6 의 포트 보안 상태 화면을 나타냅니다...

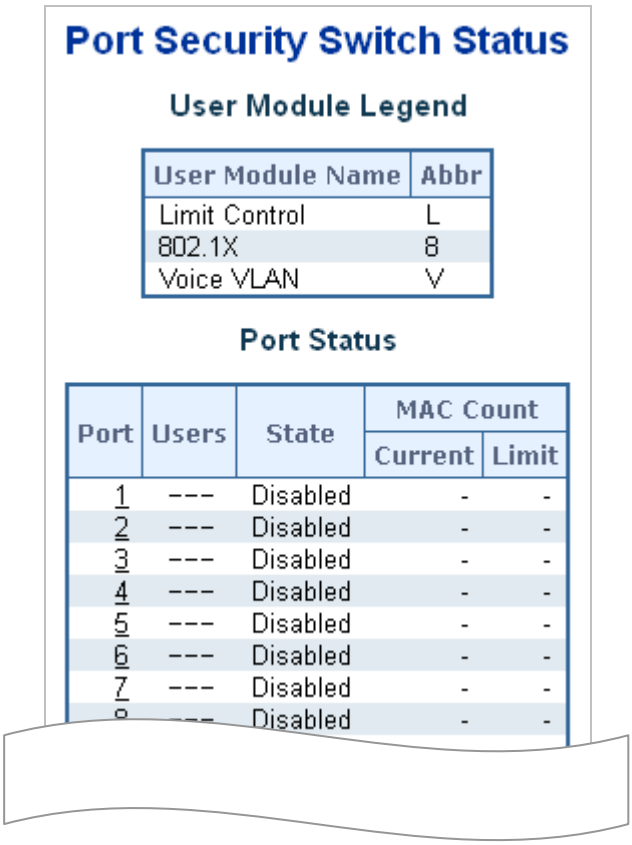


그림 4-12-6: Port Security Status Screen 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

User Module Legend

범례에는 포트 보안 서비스를 요청할 수있는 모든 사용자 모듈이 표시됩니다..

목적	설명
• **User Module Name**	포트 보안 서비스를 요청할 수있는 모듈의 전체 이름입니다.
• **Abbr**	사용자 모듈의 한 글자 약어. 이 값은 포트 상태 테이블의 Users 열에서 사용됩니다.

Port Status

표에는 스위치의 선택된 스위치에있는 각 포트에 대해 하나의 행과 여러 개의 열이 있습니다.:

목적	설명
• **Port**	상태가 적용되는 포트 번호. 이 특정 포트의 상태를 보려면 포트 번호를 클릭하십시오.

• **Users**	각 사용자 모듈에는 해당 모듈이 포트 보안을 사용하는지 여부를 나타내는 열이 있습니다. '-'는 해당 사용자 모듈이 활성화되지 않았음을 나타내는 반면 문자는 해당 문자로 축약 된 사용자 모듈이 포트 보안을 사용함을 나타냅니다.
• **State**	포트의 현재 상태를 표시합니다. 다음 네 가지 값 중 하나를 취할 수 있습니다.: ■ **Disabled**: 현재 포트 보안 서비스를 사용중인 사용자 모듈이 없습니다.. ■ **Ready**: 포트 보안 서비스가 적어도 하나의 사용자 모듈에서 사용되고 있으며 알 수없는 MAC 주소의 프레임이 도착하기를 기다리고 있습니다. ■ **Limit Reached**: 포트 보안 서비스가 적어도 제한 제어 사용자 모듈에 의해 활성화되고 해당 모듈이 한계에 도달했으며 더 이상 MAC 주소를 가져 오지 못한다고 표시했습니다.. ■ **Shutdown**: 포트 보안 서비스가 적어도 제한 제어 사용자 모듈에 의해 활성화되고 해당 모듈이 한계를 초과했음을 나타냅니다. 제한 제어 구성 웹 페이지에서 관리 상 다시 열릴 때까지 포트에서 MAC 주소를 학습 할 수 없습니다.
• **MAC Count (Current, Limit)**	두 열은 현재 학습 된 MAC 주소 (전달 및 차단됨) 및 포트에서 학습 할 수있는 최대 MAC 주소 수를 나타냅니다. 포트에서 사용자 모듈이 활성화되어 있지 않으면 현재 열에 대시 (-)가 표시됩니다. 제한 제어 사용자 모듈이 포트에서 활성화되어 있지 않으면 제한 열에 대시 (-)가 표시됩니다.

버튼

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Refresh : 즉시 페이지를 새로고침합니다.

4.12.7 Port Security Detail

이 페이지는 포트 보안 모듈에 의해 보호 된 MAC 주소를 표시합니다. 포트 보안은 직접 구성이없는 모듈입니다. 구성은 다른 모듈 (사용자 모듈)에서 간접적으로 발생합니다. 사용자 모듈이 포트에서 포트 보안을 활성화하면 포트는 소프트웨어 기반 학습용으로 설정됩니다. 이 모드에서는 알 수없는 MAC 주소의 프레임이 포트 보안 모듈로 전달되며, 포트 보안 모듈은 모든 사용자 모듈에게이 새 MAC 주소가 전달되거나 차단 될지 여부를 묻습니다. 포워딩 상태로 설정할 MAC 주소의 경우, 활성화 된 모든 사용자 모듈은 MAC 주소 전달을 허용하는 만장일치로 동의해야합니다. 오직 하나만 차단하도록 선택하면 사용자 모듈이 다르게 결정할 때까지 차단됩니다. 그림 4-12-7 의 포트 보안 상세 화면이 나타납니다..

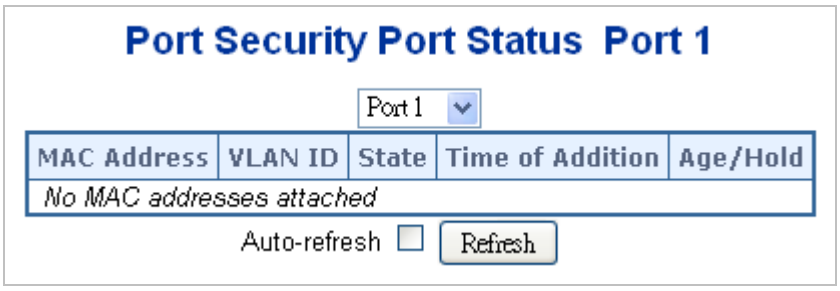


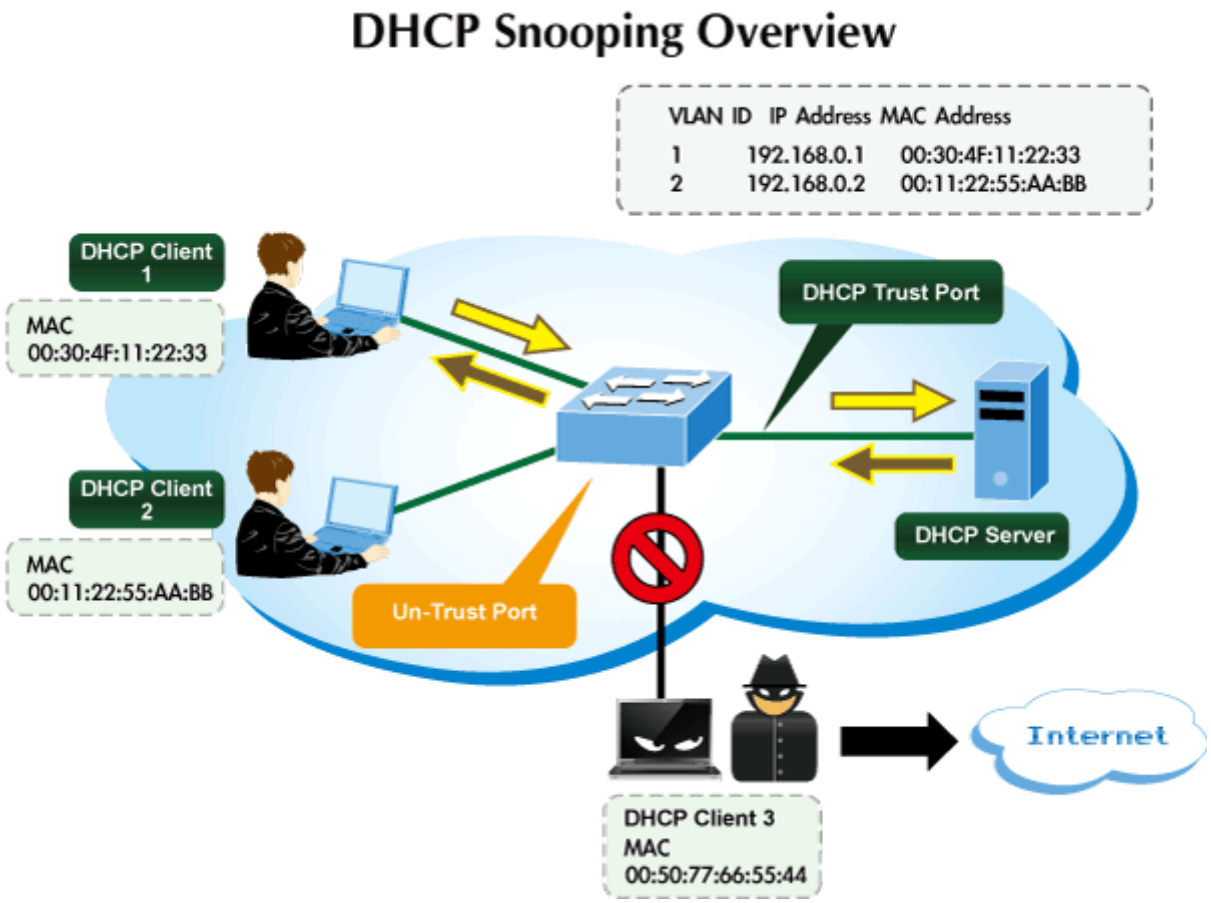
그림 4-12-7: Port Security Detail Screen 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **MAC Address & VLAN ID**	이 포트에 표시되는 MAC 주소 및 VLAN ID 입니다. 학습 된 MAC 주소가 없으면 "MAC 주소를 붙이지 않음"이라는 단일 행이 표시됩니다.
• **State**	해당 MAC 주소가 차단되었는지 또는 전달 중인지 여부를 나타냅니다. 차단 된 상태에서는 트래픽을 전송하거나 수신 할 수 없습니다.
• **Time of Addition**	이 MAC 주소가 포트에서 처음으로 표시 된 날짜와 시간을 표시합니다.
• **Age/Hold**	(-)가 표시됩니다 노화가 비활성화 또는 사용자 모듈이 무기한 해결 대시를 MAC 를 개최하기로 결정했다 경우

4.12.8 DHCP Snooping

DHCP 스누핑은 DHCP 클라이언트와 서버 간의 합법적 인 대화에 가짜 DHCP 응답 패킷을 주입하여 간섭을 시도 할 때 DUT 의 신뢰할 수없는 포트에서 침입자를 차단하는 데 사용됩니다.



페이지에서 DHCP 스누핑을 구성하십시오. 그림 4-12-8 의 DHCP Snooping Configuration 화면이 나타납니다..

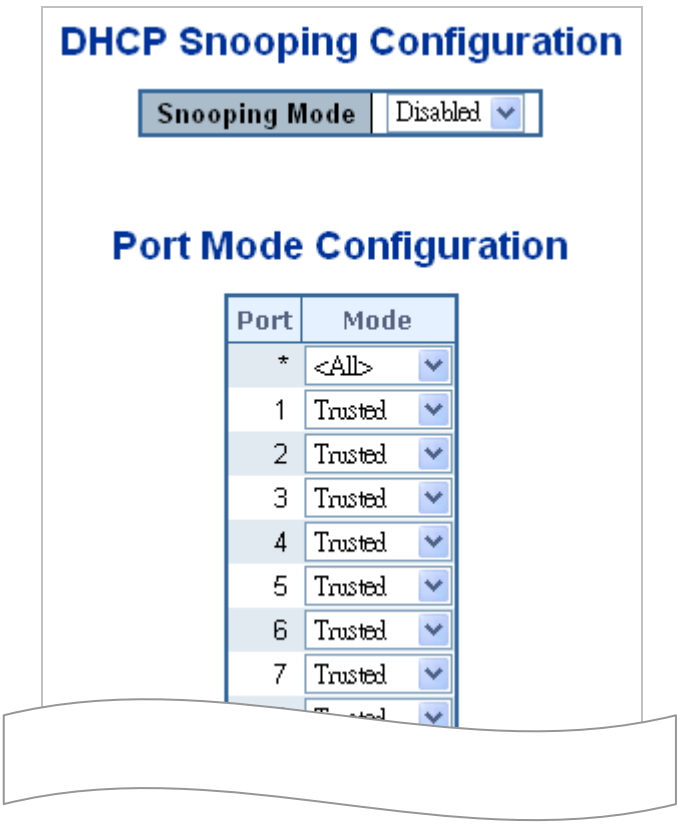


그림 4-12-8: DHCP Snooping Configuration Screen 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Snooping Mode**	DHCP 스누핑 모드 작업을 나타냅니다. 가능한 모드는 다음과 같습니다.: ■ **Enabled**: DHCP 스누핑 모드 작동을 활성화합니다. DHCP 스누핑 모드 작동을 활성화하면 요청 DHCP 메시지가 트러스트 된 포트로 전달되고 트러스트 된 포트의 응답 패킷 만 허용됩니다.. ■ **Disabled**: DHCP 스누핑 모드 작동을 비활성화합니다.
• **Port Mode Configuration**	DHCP 스누핑 포트 모드를 나타냅니다. 가능한 포트 모드는 다음과 같습니다.: ■ **Trusted**: 포트를 DHCP 메시지의 신뢰할 수있는 출처로 구성합니다. ■ **Untrusted**: 포트를 DHCP 메시지의 신뢰할 수없는 소스로 구성합니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.12.9 Snooping Table

이 페이지는 DHCP 스누핑 모드가 비활성화 된 후 동적 IP 할당 정보를 표시합니다. DHCP 서버에서 가져온 모든 DHCP 클라이언트는 로컬 VLAN 인터페이스 IP 주소를 제외하고이 표에 나열됩니다. 동적 DHCP 스누핑 표의 항목이이 페이지에 표시됩니다. 그림 4-12-9 의 동적 DHCP 스누핑 표 화면이 나타납니다..

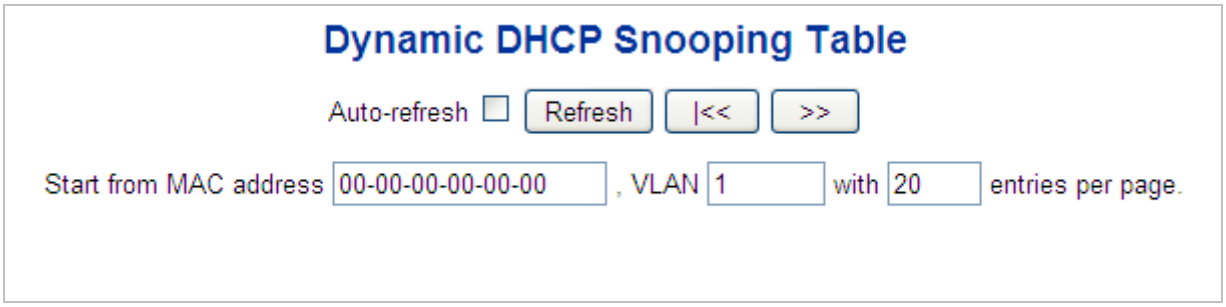


그림 4-12-9: Dynamic DHCP Snooping 표 Screen 화면

버튼

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

>>: 다음 조회의 기초로 현재 표시된 표의 마지막 항목을 사용합니다. 마지막에 도달하면 표시된 테이블에 "No more entries"텍스트가 표시됩니다

|<<: 처음화면으로 돌아갑니다.

4.12.10 IP Source Guard Configuration

IP 소스 가드는 DHCP 스누핑 표 또는 수동으로 구성된 IP 소스 바인딩을 기반으로 트래픽을 필터링하여 DHCP 스누핑 신뢰할 수없는 포트에서 IP 트래픽을 제한하는 데 사용되는 보안 기능입니다. 호스트가 다른 호스트의 IP 주소를 스푸핑하고 사용할 때 IP 스푸핑 공격을 방지하는 데 도움이됩니다. 이 페이지는 IP 소스 가드 관련 구성을 제공합니다. 그림 4-12-10 의 IP Source Guard Configuration 화면이 나타납니다.

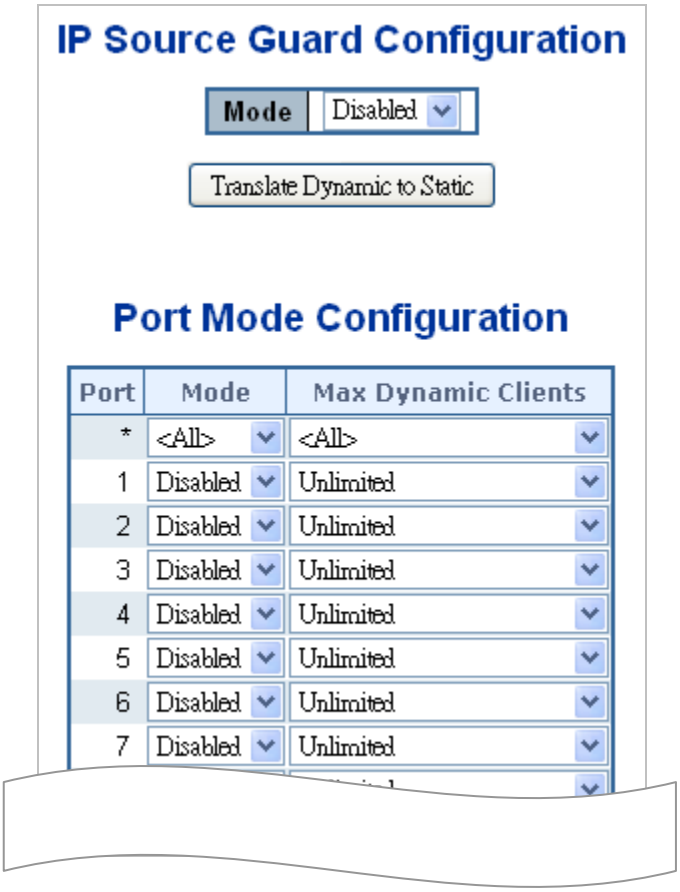


그림 4-12-10: IP Source Guard Configuration Screen 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Mode of IP Source Guard Configuration**	글로벌 IP 소스 가드를 활성화하거나 글로벌 IP 소스 가드를 비활성화하십시오. 모드가 활성화되면 구성된 모든 ACE 가 손실됩니다.
• **Port Mode Configuration**	IP 소스 가드 지정은 포트에서 활성화됩니다. 주어진 포트의 글로벌 모드와 포트 모드가 모두 활성화되어있을 때만이 주어진 포트에서 IP 소스 가드가 활성화됩니다.
• **Max Dynamic Clients**	주어진 포트에서 학습 할 수있는 동적 클라이언트의 최대 수를

	지정하십시오. 이 값은 0, 1, 2 및 무제한 일 수 있습니다. 포트 모드가 활성화되어 있고 max dynamic 클라이언트의 값이 0 인 경우 특정 포트의 정적 항목과 일치하는 IP 패킷 전달 만 허용한다는 의미입니다.

버튼

Translate Dynamic to Static: 모든 동적 항목을 정적 항목으로 변환하려면 클릭하십시오..

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.12.11 IP Source Guard Static Table

이 페이지는 정적 IP 소스 가드 테이블을 제공합니다. 그림 4-12-11 의 정적 IP 소스 가드 표 화면이 나타납니다.

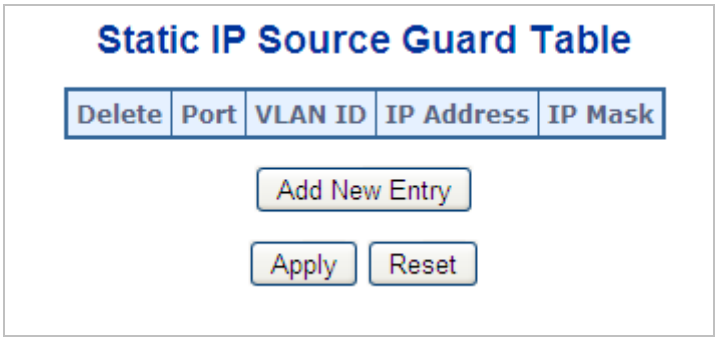


그림 4-12-11: Static IP Source Guard 표 Screen 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제됩니다.
• **Port**	설정에 대한 논리 포트입니다.
• **VLAN ID**	설정에 대한 VLAN ID 입니다.
• **IP Address**	허용 된 소스 IP 주소.
• **MAC Address**	허용 된 소스 MAC 주소

버튼

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

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.12.12 ARP Inspection

ARP 검사는 보안 기능입니다. ARP 캐시를 "중독 (poisoning)"하여 Layer 2 네트워크에 연결된 호스트 나 장치에 대해 여러 유형의 공격을 시작할 수 있습니다. 이 기능은 이러한 공격을 차단하는 데 사용됩니다. 유효한 ARP 요청 및 응답만 DUT 를 통과 할 수 있습니다. 이 페이지는 ARP 검사 관련 설정을 제공합니다. 그림 4-12-12 의 ARP Inspection Configuration 화면이 나타납니다.

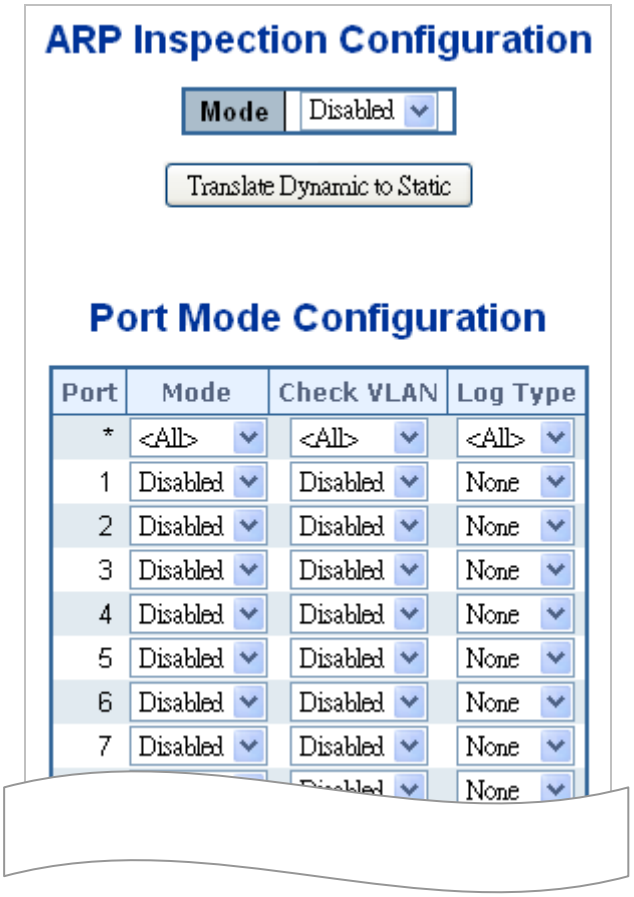


그림 4-12-12: ARP Inspection Configuration Screen 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Mode of ARP Inspection Configuration**	전역 ARP 검사를 활성화하거나 전역 ARP 검사를 비활성화하십시오.
• **Port Mode Configuration**	ARP 검사 지정은 포트에서 활성화됩니다. 주어진 포트의 글로벌 모드와 포트 모드가 활성화 된 경우에만이 주어진 포트에서 ARP 검사가 활성화됩니다. 가능한 모드는 다음과 같습니다.: ■ **Enabled**: ARP 검사기능 작동을 활성화합니다. ■ **Disabled**: ARP 검사기능 작동을 비활성화합니다. VLAN 구성을 검사하려면 "Check VLAN"설정을 활성화해야합니다. 기본

	설정 인 "Check VLAN"은 비활성화되어 있습니다. "Check VLAN"설정을 사용하지 않으면 ARP 검사의 로그 유형이 포트 설정을 참조합니다. 그리고 "Check VLAN"설정이 활성화되면 ARP 검사의 로그 유형이 VLAN 설정을 참조합니다. "Check VLAN"의 가능한 설정은 다음과 같습니다. ■ **Enabled**: check VLAN 작동을 활성화합니다. ■ **Disabled**: check VLAN 작동을 활성화합니다. 주어진 포트의 글로벌 모드 및 포트 모드 만 활성화되고 "VLAN 확인"설정이 비활성화되어 있으면 ARP 검사의 로그 유형은 포트 설정을 참조합니다. 네 가지 로그 유형과 가능한 유형은 다음과 같습니다.: ■ **None**: 아무것도 기록하지 않습니다. ■ **Deny**: 거부된 항목을 기록합니다. ■ **Permit**: 허용 된 항목을 기록합니다. ■ **ALL**:모든 로그 항목을 기록합니다.

버튼

Translate Dynamic to Static: 모든 동적 항목을 정적 항목으로 변환하려면 클릭하십시오.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.12.13 ARP Inspection Static Table

이 페이지는 정적 ARP 검사 표를 제공합니다. 그림 4-12-13 의 정적 ARP 검사 표 화면이 나타납니다.

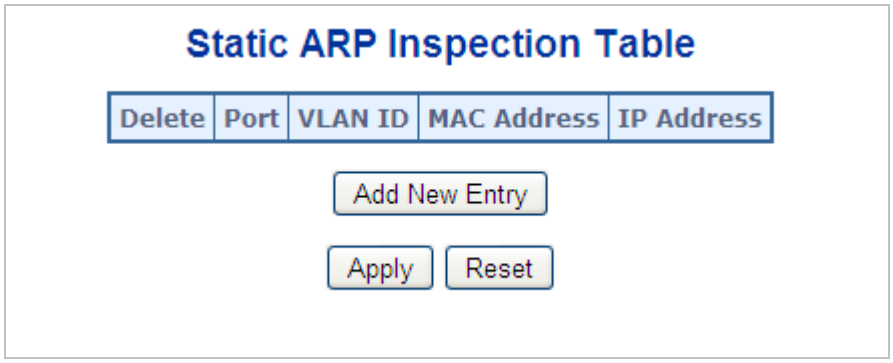


그림 4-12-13: Static ARP Inspection 표 Screen 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 저장항목중 다음에 삭제됩니다
• **Port**	설정값에 대한 논리적인 포트입니다.

• **VLAN ID**	설정값에 대한 Vlan ID 입니다.
• **MAC Address**	ARP 요청 패킷의 소스 MAC 주소를 허용합니다.
• **IP Address**	허용 된 소스 IP 주소는 ARP 요청 패킷입니다.

버튼

Add New Entry: Static ARP Inspection (정적 ARP 검사) 표에 새 항목을 추가하려면 누릅니다.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.12.14 Dynamic ARP Inspection Table

동적 ARP 검사 표의 항목은이 페이지에 표시됩니다. Dynamic ARP Inspection (동적 ARP 검사) 표는 최대 1024 개의 항목을 포함하며 포트별로 먼저 정렬 된 다음 VLAN ID, MAC 주소 및 IP 주소 순으로 정렬됩니다. 그림 4-12-14 의 동적 ARP 검사 표 화면이 나타납니다.

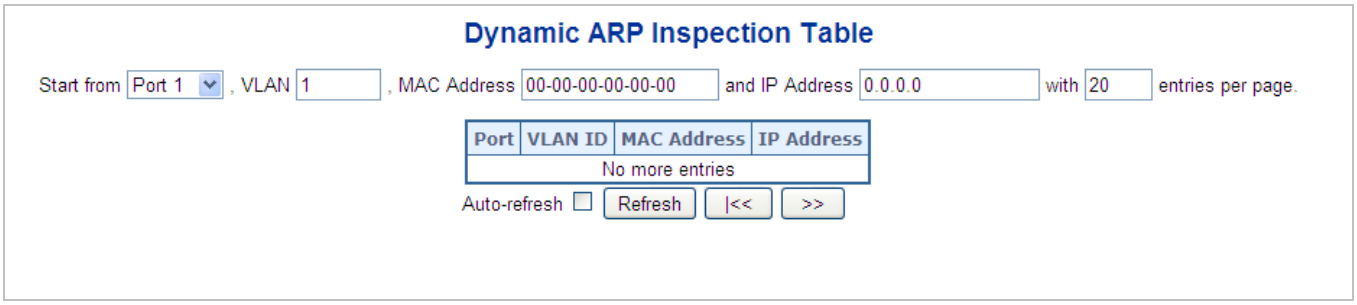


그림 4-12-14: Dynamic ARP Inspection 표 화면

ARP Inspection Table 탐색

각 페이지는 Dynamic ARP Inspection (동적 ARP 검사) 표에서 최대 99 개의 항목을 표시하며, 기본값은 20 이고 "페이지 당 항목"입력 필드를 통해 선택됩니다. 처음 방문했을 때, 웹 페이지는 동적 ARP 검사 표의 처음부터 처음 20 개의 항목을 표시합니다.

"포트 주소에서 시작", "VLAN", "MAC 주소"및 "IP 주소"입력 필드를 사용하여 동적 ARP 검사 표에서 시작점을 선택할 수 있습니다. "Refresh (새로 고침)"버튼을 클릭하면 표시된 표 또는 가장 가까운 다음 동적 ARP 검사 표 일치 항목이 업데이트됩니다. 또한 두 개의 입력 필드는 "새로 고침"버튼을 클릭 할 때 첫 번째 표시된 항목의 값을 취합니다. 동일한 시작 주소로 계속 새로 고침 할 수 있습니다.

">>"는 다음 조회를 위해 현재 표시된 항목의 마지막 항목을 사용합니다. 마지막에 도달하면 표시된 테이블에 "No more entries"텍스트가 표시됩니다. 다시 시작하려면 "| <<"버튼을 사용하십시오.. 이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	상태가 적용되는 포트 번호. 이 특정 포트의 상태를 보려면 포트 번호를 클릭하십시오.
• **VLAN ID**	항목의 Vlan ID 입니다.
• **MAC Address**	항목의 Mac 주소입니다.
• **IP Address**	항목이 IP 주소입니다.

버튼

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

Refresh : 상태가 적용되는 포트 번호. 이 특정 포트의 상태를 보려면 포트 번호를 클릭하십시오.

Clear : 모든 동적 항목을 새로고침합니다.

<< : 가장 낮은 VLAN ID 및 MAC 주소를 갖는 항목 인 MAC 테이블의 첫 번째 항목부터 시작하여 표를 업데이트합니다.

>> : 현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 업데이트합니다.

4.13 Address Table

프레임 전환은 프레임에 포함 된 DMAC 주소를 기반으로합니다. 관리 형 스위치는 MAC 주소를 스위치 포트에 매핑하여 프레임이 어느 포트로 이동해야하는지 (프레임의 DMAC 주소를 기반으로)를 파악하는 표를 작성합니다. 이 표에는 정적 및 동적 항목이 모두 들어 있습니다. 정적 항목은 관리자가 DMAC 주소와 스위치 포트간에 고정 매핑을 원할 경우 네트워크 관리자가 구성합니다.

프레임에는 MAC 주소 (SMAC 주소)가 포함되어있어 프레임을 전송하는 장비의 MAC 주소를 표시합니다. SMAC 주소는 스위치가 자동으로 MAC 표를 이러한 동적 MAC 주소로 업데이트하는 데 사용됩니다. 구성 가능한 에이징 시간 후에 해당 SMAC 주소가있는 프레임이 표시되지 않으면 동적 항목이 MAC 표에서 제거됩니다..

4.13.1 MAC 표 Configuration

이 페이지에 MAC 주소 표가 구성되어 있습니다. 동적 MAC 표의 항목에 대한 시간 초과를 설정하고 여기서 정적 MAC 표를 구성하십시오. 그림 4-13-1 의 MAC Address Table Configuration 화면이 나타납니다.

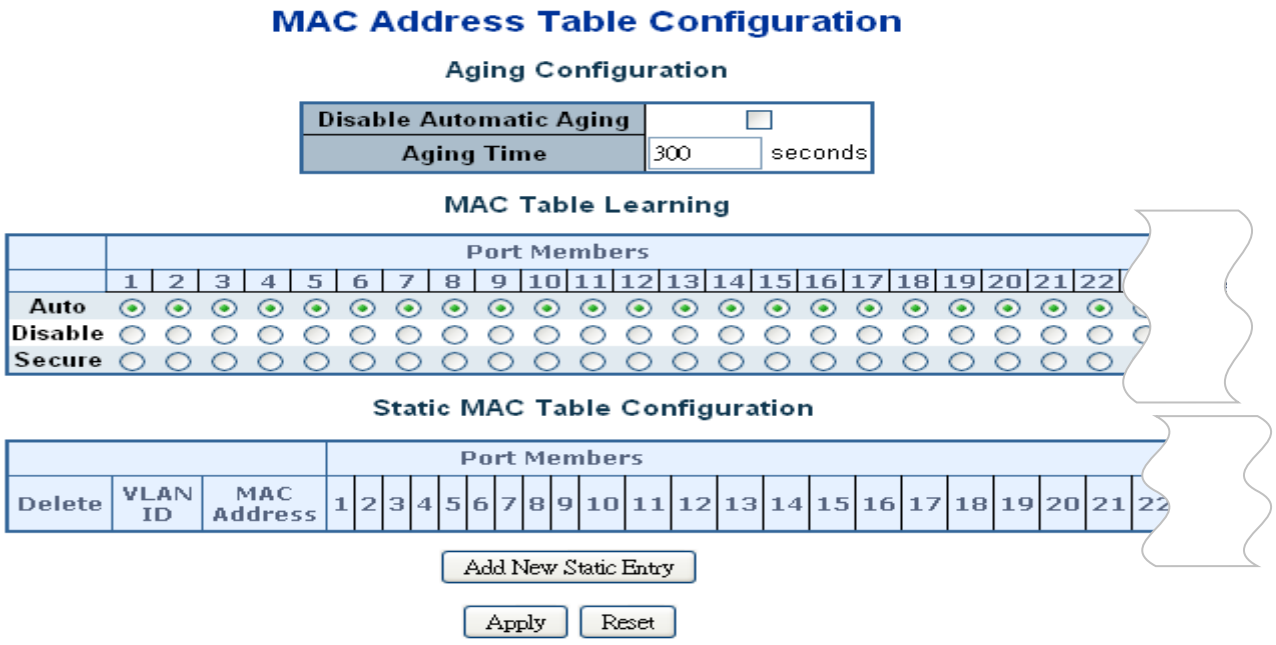


그림 4-13-1: MAC Address 표 Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

Aging Configuration

기본적으로 동적 항목은 300 초 후에 MAC 표에서 제거됩니다. 이 제거는 에이징라고도합니다.

목적	설명
• **Disable Automatic Aging**	동적 항목의 자동 에이징을 활성화 / 비활성화합니다.
• **Aging Time**	학습 된 항목이 삭제 된 이후의 시간입니다. 기본적으로 동적 항목은 300 초 후에 MAC 에서 제거됩니다. 이 제거는 노화라고도합니다. (범위 : 10-10000000 초, 기본값 : 300 초)

MAC 표 Learning

주어진 포트에 대한 학습 모드가 회색으로 표시되면 다른 모듈이 모드를 제어하므로 사용자가 변경할 수 없습니다. 이러한 모듈의 예로 802.1X 에서의 MAC 기반 인증이 있습니다

목적	설명
• **Auto**	학습은 SMAC 가 알려지지 않은 프레임이 수신되는 즉시 자동으로 수행됩니다.
• **Disable**	아무런 학습도 이루어지지 않습니다.
• **Secure**	정적 MAC 항목 만 학습되고 다른 모든 프레임은 삭제됩니다. 참고 : 보안 학습 모드로 변경하기 전에 스위치 관리에 사용 된 링크가 Static Mac 표에 추가되었는지 확인하십시오. 그렇지 않으면 관리 링크가 손실되고 다른 비보안 포트를 사용하거나 스위치에 연결해야만 복원 할 수 있습니다 직렬 인터페이스를 통해.

Static MAC 표 Configuration

MAC 표의 정적 항목은이 표에 나와 있습니다. 정적 MAC 표는 64 개의 항목을 포함 할 수 있습니다. MAC 표는 먼저 VLAN ID 와 MAC 주소 순으로 정렬됩니다.

목적	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제됩니다.
• **VLAN ID**	항목의 Vlan ID 입니다.
• **MAC Address**	항목의 MAC 주소입니다.
• **Port Members**	체크 표시는 항목의 구성원 인 포트를 나타냅니다. 필요에 따라 항목을 수정하거나 선택을 취소하십시오.
• **Adding a New Static Entry**	Add New Static Entry 를 클릭하여 정적 MAC 테이블에 새항목을 추가하고 Vlan ID 와 MAC 주소 및 포트 구성원을 지정하십시오. "저장"을 클릭하십시오.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.13.2 MAC Address 표 Status

Dynamic MAC Table

이 페이지에는 MAC 표의 항목이 표시됩니다. MAC 표는 최대 8192 개의 항목을 포함하며 VLAN ID, MAC 주소 순서로 먼저 정렬됩니다. 그림 4-13-2 의 MAC Address Table 화면이 나타납니다.

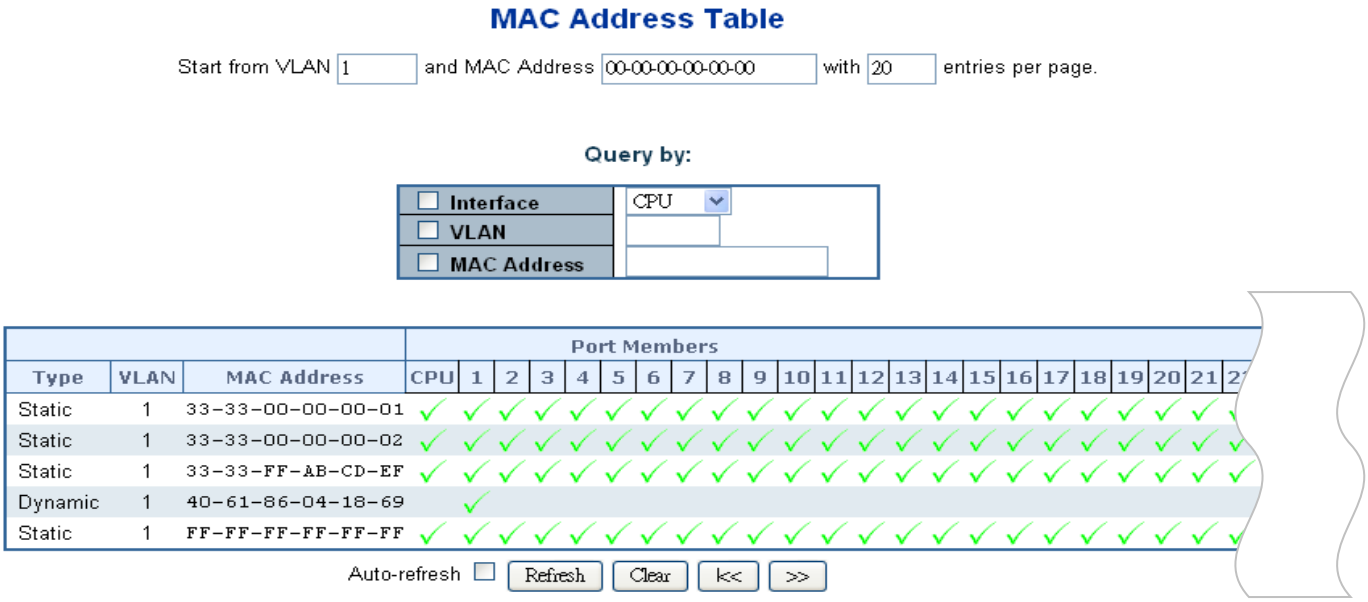


그림 4-13-2: MAC Address 표 Status 화면

Navigating the MAC Table

각 페이지는 MAC 테이블에서 최대 999 개의 항목을 표시하며 기본값은 20 이고 "페이지 당 항목 수"입력 필드를 통해 선택됩니다. 처음 방문했을 때, 웹 페이지는 MAC 표의 처음부터 처음 20 개의 항목을 보여줍니다. 가장 먼저 표시되는 것은 VLAN ID 가 가장 낮고 MAC 테이블에서 가장 낮은 MAC 주소가 표시됩니다.

"MAC 주소에서 시작"및 "VLAN"입력 필드를 사용하여 MAC 테이블에서 시작점을 선택할 수 있습니다. "Refresh (새로 고침)"버튼을 클릭하면 표시되는 표가 바로 또는 가장 가까운 다음 MAC 표 일치에서부터 업데이트됩니다.

또한 두 개의 입력 필드는 "새로 고침"버튼을 클릭 할 때 첫 번째 표시된 항목의 값을 취합니다. 동일한 시작 주소로 계속 새로 고침 할 수 있습니다.

">>"는 현재 조회 된 VLAN / MAC 주소 쌍 중 마지막 항목을 다음 조회의 기준으로 사용합니다. 끝에 도달하면 표시된 테이블에 "더 이상의 항목이 없습니다"라는 텍스트가 표시됩니다. 다시 시작하려면 "| <<"버튼을 사용하십시오..

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Type**	항목이 정적 항목인지 또는 동적 항목인지 나타냅니다.
• **VLAN**	항목의 VLAN ID 입니다.
• **MAC Address**	항목의 MAC 주소입니다.

• **Port Members**	항목의 구성원 인 포트

버튼

Auto-refresh : 자동 새로 고침은 3 초마다 발생합니다..

Refresh: "MAC 주소에서 시작"및 "VLAN"입력 필드에서 표시된 표를 새로 고칩니다.

Clear: 모든 동적 항목을 플러시합니다.

<<: 가장 낮은 VLAN ID 및 MAC 주소를 갖는 항목 인 MAC 테이블의 첫 번째 항목부터 시작하여 표를 업데이트합니다.

>>: 현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 업데이트합니다.

4.14 LLDP

4.14.1 Link Layer Discovery Protocol

LLDP (Link Layer Discovery Protocol)는 로컬 브로드 캐스트 도메인의 인접 장치에 대한 기본 정보를 검색하는 데 사용됩니다. LLDP 는 정기적 인 브로드 캐스트를 사용하여 전송 장치에 대한 정보를 알리는 Layer 2 프로토콜입니다. 광고 정보는 IEEE 802.1ab 표준에 따라 TLV (Type Length Value) 형식으로 표시되며 장치 식별, 기능 및 구성 설정과 같은 세부 정보를 포함 할 수 있습니다. 또한 LLDP 는 발견 한 인접 네트워크 노드에 대해 수집 된 정보를 저장하고 유지 관리하는 방법을 정의합니다.

링크 계층 검색 프로토콜 - LLDP-MED (Media Endpoint Discovery)는 IP 전화기 및 네트워크 스위치와 같은 끝점 장치를 관리하기위한 LLDP 의 확장 기능입니다. LLDP-MED TLV 는 네트워크 정책, 전원, 인벤토리 및 장치 위치 세부 정보와 같은 정보를 알립니다. SNMP 응용 프로그램에서 LLDP 및 LLDP-MED 정보를 사용하여 문제 해결을 단순화하고 네트워크 관리를 향상 시키며 정확한 네트워크 토폴로지를 유지 관리 할 수 있습니다..

4.14.2 LLDP Configuration

이 페이지에서는 사용자가 현재 LLDP 포트 설정을 검사하고 구성 할 수 있습니다. LLDP 구성 화면 그림 4-14-1 에 나타납니다.

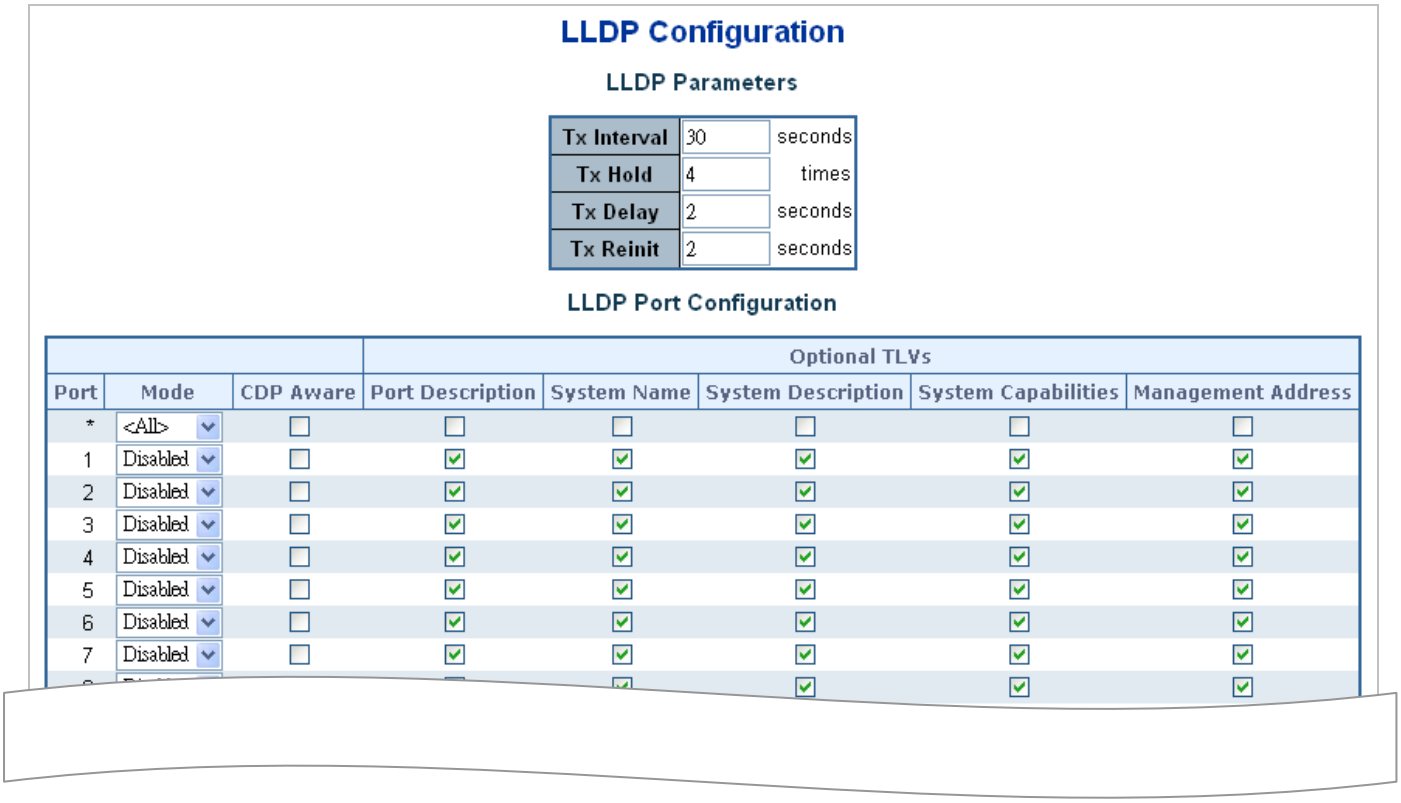


그림 4-14-1: LLDP Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

LLDP Parameters

목적	설명
• **Tx Interval**	스위치는 네트워크 검색 정보를 최신 상태로 유지하기 위해 정기적으로 LLDP 프레임을 이웃 라우터로 전송합니다. 각 LLDP 프레임 사이의 간격은 Tx 간격 값에 의해 결정됩니다. 유효한 값은 5 - 32768 초로 제한됩니다. 기본값 : 30 초 이 속성은 다음 규칙을 준수해야합니다. (전송 간격 * 대기 시간의 배율) ≤65536 및 전송 간격> = (4 * 지연 간격)
• **Tx Hold**	각 LLDP 프레임은 LLDP 프레임의 정보가 유효한 것으로 간주되는 기간에 대한 정보를 포함합니다. LLDP 정보 유효 기간은 Tx Hold 에 Tx Interval seconds 를 곱한 값으로 설정됩니다. 유효한 값은 2 - 10 로 제한됩니다. 초 단위의 TTL 은 다음 규칙을 기반으로합니다.: (전송 간격 *대기 시간 배율) ≤ 65536. 따라서 기본 TTL 은 4 * 30 = 120 초입니다.
• **Tx Delay**	일부 구성이 변경되면 (예 : IP 주소) 새 LLDP 프레임이 전송되지만 LLDP 프레임 간의 시간은 항상 적어도 Tx 지연 초의 값이됩니다. Tx 지연은 Tx 간격 값의 1/4 보다 클 수 없습니다. 유효한 값은 1 - 8192 초로 제한됩니다. 이 속성은 규칙을 준수해야합니다. (4 *지연간격) ≤ 전송간격
• **Tx Reinit**	포트가 비활성화 된 경우 LLDP 가 비활성화되거나 스위치가 재부팅됩니다. LLDP 종료 프레임이 인접 장치로 전송되어 LLDP 정보가 더 이상 유효하지 않음을 알립니다. Tx Reinit 은 종료 프레임과 새 LLDP 초기화 사이의 시간 (초)을 제어합니다. 유효한 값은 1 - 10 초로 제한됩니다.

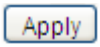
LLDP Port Configuration

LLDP 포트 설정은 페이지 헤더에 반영된 스위치와 관련이 있습니다.

목적	설명
• **Port**	논리적 LLDP 포트의 스위치 포트 번호입니다.
• **Mode**	LLDP mode 를 선택합니다. ■ **Rx only** 스위치는 LLDP 정보를 전송하지 않지만 인접 장치의 LLDP 정보는 분석됩니다. ■ **Tx only** 스위치는 이웃 라우터로부터 수신 한 LLDP 정보를 삭제하지만 LLDP 정보를 전송합니다. ■ **Disabled** 라우터로부터 수신 한 LLDP 정보를 삭제합니다. ■ **Enabled** 스위치는 LLDP 정보를 전송하고 이웃으로부터 수신 한 LLDP 정보를 분석합니다.

• **CDP Aware**	CDP 인식을 선택하십시오. CDP 작업은 들어오는 CDP 프레임을 디코딩하는 것으로 제한됩니다 (스위치는 CDP 프레임을 전송하지 않습니다). CDP 프레임은 포트의 LLDP 가 활성화 된 경우에만 디코딩됩니다. LLDP 인접 장치의 표에서 해당 필드에 매핑 될 수있는 CDP TLV 만 디코딩됩니다. 다른 모든 TLV 는 삭제됩니다 (인식 할 수없는 CDP TLV 및 삭제 된 CDP 프레임은 LLDP 통계에 표시되지 않습니다). CDP TLV 는 아래와 같이 LLDP 인접 항목의 표에 매핑됩니다. CDP TLV "장치 ID"는 LLDP "샤시 ID"필드에 매핑됩니다. CDP TLV "주소"는 LLDP "관리 주소"필드에 매핑됩니다. CDP 주소 TLV 는 여러 주소를 포함 할 수 있지만 첫 번째 주소 만 LLDP 인접 항목 표에 표시됩니다. CDP TLV "포트 ID"는 LLDP "포트 ID"필드에 매핑됩니다. CDP TLV "버전 및 플랫폼"은 LLDP "시스템 설명"필드에 매핑됩니다. CDP 와 LLDP 는 모두 "시스템 기능"을 지원하지만 CDP 기능은 LLDP 의 일부가 아닌 기능을 포함합니다. 이러한 기능은 LLDP 인접 테이블에 "기타"로 표시됩니다. 모든 포트에서 CDP 인식이 비활성화 된 경우 스위치는 인접 장치에서 수신한 CDP 프레임을 전달합니다. 하나 이상의 포트에 CDP 인식이 활성화되어 있으면 모든 CDP 프레임이 스위치에 의해 종료됩니다. 참고 : 포트의 CDP 인식이 비활성화되면 CDP 정보는 즉시 제거되지 않지만 보류 시간이 초과되면 제거됩니다.
• **Port description**	Optional TLV: 옵션을 선택하면 전송 된 LLDP 정보에 "포트 설명"이 포함됩니다.
• **System Name**	Optional TLV: 옵션을 선택하면 "시스템 이름"이 전송 된 LLDP 정보에 포함됩니다
• **System description**	Optional TLV: 옵션을 선택하면 "시스템 설명"이 전송 된 LLDP 정보에 포함됩니다.
• **System Capabilites**	Optional TLV: 선택하면 "시스템 기능"이 전송 된 LLDP 정보에 포함됩니다.
• **Management Address**	Optional TLV: 선택하면 "관리 주소"가 전송 된 LLDP 정보에 포함됩니다..

버튼



: 변동사항을 클릭하여 저장합니다.

: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.14.3 LLDP MED Configuration

이 페이지에서는 LLDP-MED 를 구성 할 수 있습니다. 그림 4-14-2 의 LLDPMED Configuration 화면이 나타납니다.

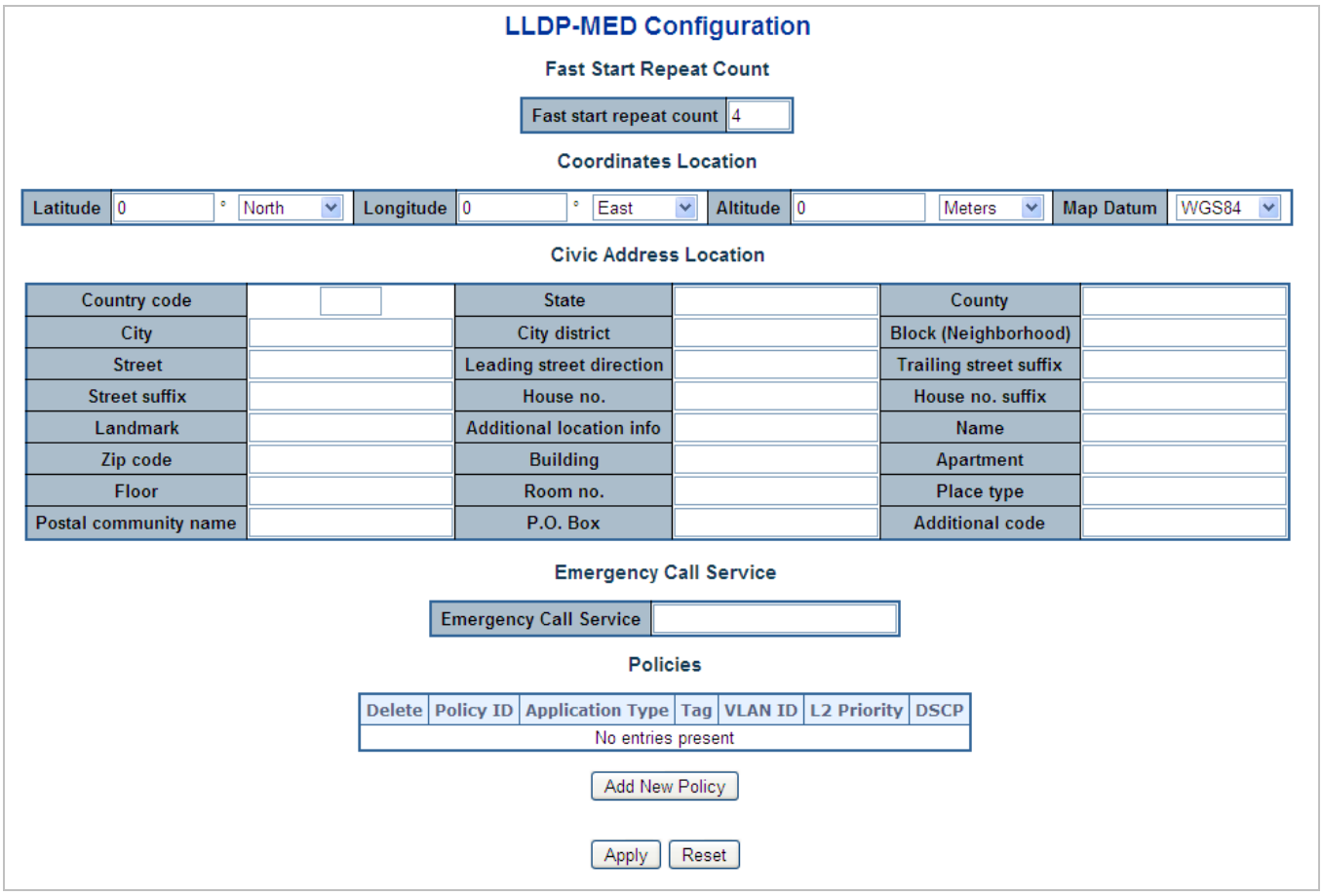


그림 4-14-2: LLDPMED Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

Fast start repeat count

목적	설명
• **Fast start repeat count**	신속한 시동 및 긴급 통화 서비스 위치 확인 엔드 포인트의 발견은 일반적으로 VoIP 시스템에서 매우 중요한 부분입니다. 또한, 제한된 LLDPU 공간을 보존하고 음성을 줄이려면 특정 종점 유형과 관련이있는 정보 (예 : 음성 네트워크 정책을 허용 된 음성 지원 장치에만 보급하는 등)를 광고하는 것이 가장 좋습니다 보안 및 시스템 무결성 문제로 인해 네트워크 정책에 대한 부적절한 지식이 발생할 수 있습니다. 이를 염두에두고 LLDP-MED 는 이러한 관련 속성을 달성하기 위해 프로토콜과 프로토콜 상단의 응용 프로그램 계층간에 LLDP-MED Fast Start 상호 작용을 정의합니다. 처음에는 네트워크 연결 장치가 LLDPDU 에 LLDP TLV 만 전송합니다. LLDP-MED 종단점 장치가 감지 된 후에 만 LLDP-MED 지원 네트워크 연결 장치가 관련 포트에서 나가는 LLDPDU 에 LLDP-MED TLV 를 보급하기 시작합니다. LLDP-MED 응용 프로그램은 새로운 LLDP-MED

	이웃이 감지되어 LLDP-MED 정보를 가능한 한 빨리 새로운 이웃에게 공유할 수 있도록 LLDPDU 의 전송 속도를 1 초 이내로 일시적으로 높입니다. 이웃 간의 전송 중에 LLDP 프레임이 손실 될 위험이 있기 때문에 이웃들이 LLDP 프레임을 수신 할 가능성을 높이기 위해 빠른 시작 전송을 여러 번 반복하는 것이 좋습니다. 빠른 시작 반복 카운트를 사용하면 빠른 시작 전송이 반복되는 횟수를 지정할 수 있습니다. 새로운 정보가있는 LLDP 프레임이 수신 될 때 1 초 간격의 4 LLDP 프레임이 전송되므로 권장 값은 4 배입니다. LLDP-MED 및 LLDP-MED Fast Start 메커니즘은 LLDP-MED 네트워크 연결 장치와 종단 장치 간의 링크에서만 실행되며 네트워크 연결을 비롯한 LAN 인프라 요소 간의 링크에는 적용되지 않습니다. 장치 또는 기타 유형의 링크가 있어야합니다.

Coordinates Location

목적	설명
• **Latitude**	Latitude 는 0 ~ 90 도 범위 내에서 최대 4 자리까지 정규화되어야합니다. 적도의 북쪽 또는 적도의 남쪽 방향을 지정할 수 있습니다
• **Longitude**	경도는 최대 4 자리 숫자로 0-180 도 이내로 정규화되어야합니다. 본초 자오선의 동쪽 또는 본 자오선의 서쪽 방향을 지정할 수 있습니다.
• **Altitude**	Altitude 는 최대 4 자릿수 인 -32767 ~ 32767 범위 내로 표준화되어야합니다. 두 고도 유형 (층 또는 미터) 중에서 선택할 수 있습니다. Meters : 지정된 세로 데이터로 정의 된 고도 미터를 나타냅니다. Floors (바닥) : 바닥에서 바닥까지의 치수가 다른 건물에서보다 관련성 높은 형태로 고도를 나타냅니다. 고도 = 0.0 은 건물 외부에서도 의미가 있으며 주어진 위도와 경도에서 지표면을 나타냅니다. 건물 내부에서 0.0 은 정문 입구의지면 수준을 나타냅니다.
• **Map Datum**	이 Option 에서 주어진 좌표에 사용 된 Map Datum ■ **WGS84**: (Geographical 3D) - 세계 측지 시스템 1984, CRS 코드 4327, 본초 자오선 이름 : 그리니치. ■ **NAD83/NAVD88**: North American Datum 1983, CRS Code 4269, 본초 자오선 이름 : Greenwich; 관련 수직 데이터는 1988 년 북미 수직 데이터 (NAVD88)입니다. 이 데이텀 쌍은 육지의 위치를 참조 할 때 사용되며 조수 (Datum = NAD83 / MLLW)를 사용하지는 않습니다. ■ **NAD83/MLLW**: North American Datum 1983, CRS Code 4269, 본초 자오선 이름 : Greenwich; 관련 수직 자료는 평균 저수위 (MLLW)입니다. 이 데이텀 쌍은 물 / 바다 / 바다에서 위치를 참조 할 때 사용됩니다.

도시 로컬 주소

IETF Geopriv Civic Address 기반의 위치 구성 정보 (Civic Address LCI).

목적	설명
• **Country code**	두 자로 된 ISO 3166 국가 코드 (대문자 ASCII 문자) - 예 : DK, DE 또는 US.
• **State**	국가에 대한 세분화 (state, canton, region, province, prefecture).
• **County**	County, parish, gun (일본), district.
• **City**	도시, 군구, 시(일본) – 예: 코펜하겐
• **City district**	분지역, , city district, ward, chou (일본)
• **Block (Neighborhood)**	이웃, 블록
• **Street**	길거리-예제: Poppelv
• **Leading street direction**	선도 방향 - 예제 : N
• **Trailing street suffix**	Trailing street suffix -예제: SW
• **Street suffix**	거리 접미사-예제: Ave, Platz
• **House no.**	집 번호– 하우스 번호: 21
• **House no. suffix**	집 번호 접미사-예제: A, 1/2
• **Landmark**	랜드 마크 또는 베니티 주소-예제: Columbia University
• **Additional location info**	추가 위치 정보 -예제 : South Wing
• **Name**	이름(거주지 및 사무실 거주자) -예제: Flemming Jahn
• **Zip code**	우편/우편 번호 -예제: 2791
• **Building**	건물 (구조) -예제: 낮은 도서관
• **Apartment**	단위(Apartment, suite) -예제: Apt 42
• **Floor**	층-예제: 4
• **Room no.**	방번호- 예제: 450F
• **Place type**	장소 유형-예제 : 사무실
• **Postal community name**	우편 커뮤니티 이름 - 예제 Leonia
• **P.O. Box**	사서함 (P.O. BOX) -예제: 12345
• **Additional code**	추가 코드- 예시: 1320300003

Emergency Call Service

TIA 또는 NENA 에서 정의한 비상 전화 서비스 (예 : E911 및 기타).

목적	설명
• **Emergency Call Service**	**Emergency Call Service** ELIN 식별자 데이터 형식은 비상 호출 설정 중에 사용되는 ELIN 식별자를 일반 CAMA 또는 ISDN 트렁크 기반 PSAP 에 전달하도록 정의됩니다. 이 형식은 긴급 통화에 사용할 ELIN 에 해당하는 숫자 숫자 문자열로 구성됩니다.

Policies

네트워크 정책 검색을 사용하면 해당 포트에서 특정 프로토콜 응용 프로그램 집합에 적용되는 관련 Layer 2 및 Layer 3 특성과 함께 VLAN 구성의 불일치 문제를 효율적으로 검색하고 진단 할 수 있습니다. VoIP 환경에서 부적절한 네트워크 정책 구성은 음성 품질 저하 또는 서비스 손실을 초래하는 매우 중요한 문제입니다.

정책은 대화 형 음성 및 / 또는 비디오 서비스와 같은 특정 '실시간' 네트워크 정책 요구 사항이있는 응용 프로그램에만 사용해야합니다..

광고되는 네트워크 정책 속성은 다음과 같습니다.

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 우선순위 값 (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) 값(IETF RFC 2474)

네트워크 정책은 잠재적으로 알려지며 주어진 포트에서 지원되는 여러 유형의 응용 프로그램과 연관됩니다. 특별히 다루는 응용 프로그램 유형은 다음과 같습니다.:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signaling (위의 미디어 유형에 대한 별도의 네트워크 정책을 조건부로 지원합니다.)

대규모 네트워크는 전체 조직의 여러 VoIP 정책과 애플리케이션 유형별 정책을 지원할 수 있습니다. LLDP-MED 는 포트별로 여러 정책을 광고 할 수 있으며 각 정책은 서로 다른 응용 프로그램 유형에 해당합니다. 동일한 네트워크 연결 장치의 다른 포트는 인증 된 사용자 ID 또는 포트 구성을 기반으로 다른 정책 집합을 알릴 수 있습니다.

LLDP-MED 는 네트워크 연결 장치와 끝점 이외의 링크에서 실행되지 않으므로 LAN 내부의 집계 된 링크 내부에서 자주 실행되는 많은 네트워크 정책을 알릴 필요가 없습니다.

목적	설명
• **Delete**	정책을 삭제하려면 선택하십시오. 다음 저장이 되기전에 삭제됩니다.
• **Policy ID**	정책의 ID 입니다. 이것은 자동으로 생성되며 특정 포트에 매핑 될 정책을 선택할 때 사용됩니다.
• **Application Type**	응용 프로그램 유형의 의도 된 사용: ■ **Voice** -대화 형 음성 서비스를 지원하는 전용 IP 텔레포니 핸드셋 및 기타 유사한 어플라이언스에서 사용할 수 있습니다. 이러한 장치는 일반적으로 별도의 VLAN 에 배포되어 데이터 응용 프로그램과의 격리로 보안을 강화하고 쉽게 설치할 수 있습니다.. ■ **Voice Signaling (조건부)** - 음성 시그널링과는 다른 정책이 필요한 네트워크 토폴로지에서 사용하기위한 것입니다. 이 응용 프로그램

	유형은 음성 응용 프로그램 정책에 보급 된 것과 동일한 네트워크 정책이 모두 적용되는 경우 보급해서는 안됩니다. ■ **Guest Voice** - 자체 IP 텔레포니 핸드셋 및 대화 형 음성 서비스를 지원하는 기타 유사한 어플라이언스를 사용하여 게스트 사용자 및 방문객을위한 별도의 '제한된 기능 세트'음성 서비스를 지원합니다.. ■ **Guest Voice Signaling (조건부)** - 게스트 음성 미디어보다 게스트 음성 시그널링에 대해 다른 정책이 필요한 네트워크 토폴로지에서 사용합니다. 이 응용 프로그램 유형은 Guest Voice 응용 프로그램 정책에 보급 된 정책과 동일한 네트워크 정책이 모두 적용되는 경우 보급해서는 안됩니다. ■ **Softphone Voice** - PC 또는 랩톱과 같은 일반적인 데이터 중심 장치의 소프트 폰 응용 프로그램에서 사용합니다. 이 엔드 포인트 클래스는 종종 여러 개의 VLAN 을 지원하지 않으며, 일반적으로 '태그없는'VLAN 또는 단일 '태그 지정된'데이터 특정 VLAN 을 사용하도록 구성됩니다. 네트워크 정책이 '태그없는'VLAN (아래의 태그 지정 플래그 참조)과 함께 사용하도록 정의 된 경우 L2 우선 순위 필드는 무시되고 DSCP 값만 관련성을 갖습니다. ■ **Video Conferencing** - 전용 화상 회의 장비 및 실시간 대화 형 비디오 / 오디오 서비스를 지원하는 기타 유사한 장비에 사용됩니다. ■ **Streaming Video** - 브로드 캐스트 또는 멀티 캐스트 기반 비디오 컨텐츠 배포 및 특정 네트워크 정책 처리가 필요한 스트리밍 비디오 서비스를 지원하는 기타 유사한 응용 프로그램에 사용됩니다. 버퍼링을 사용하여 TCP 를 사용하는 비디오 응용 프로그램은이 응용 프로그램 유형을 의도 한 용도로 사용하지 않습니다. ■ **Video Signaling (조건부)** - 비디오 신호보다는 비디오 신호에 대해 별도의 정책이 필요한 네트워크 토폴로지에서 사용합니다. 화상 회의 응용 프로그램 정책에서 보급 된 것과 동일한 네트워크 정책이 모두 적용되는 경우이 응용 프로그램 유형을 보급해서는 안됩니다.
• **Tag**	지정된 애플리케이션 유형이 '태그가 추가됨'또는 '태그없는'VLAN 을 사용하는지 여부를 나타내는 태그입니다. ■ **Untagged** 장치가 태그없는 프레임 형식을 사용하고 있으며 IEEE 802.1Q-2003 에 정의 된 태그 머리글을 포함하지 않음을 나타냅니다. 이 경우 VLAN ID 및 레이어 2 우선 순위 필드는 모두 무시되며 DSCP 값만 관련성을 갖습니다. ■ **Tagged** 장치가 IEEE 802.1Q 태그가 지정된 프레임 형식을 사용 중이며 VLAN ID 와 계층 2 우선 순위 값이 DSCP 값과 함께 사용되고 있음을 나타냅니다. 태그가 지정된 형식에는 태그

	머리글이라고하는 추가 필드가 포함됩니다. 태그가 추가 된 프레임 형식에는 IEEE 802.1Q-2003 에 정의 된 우선 순위 태그가 지정된 프레임도 포함됩니다
• **VLAN ID**	IEEE 802.1Q-2003 에 정의 된 포트의 VLAN 식별자 (VID)
• **L2 Priority**	L2 우선 순위는 지정된 응용 프로그램 유형에 사용되는 계층 2 우선 순위입니다. L2 우선 순위는 IEEE 802.1D-2004 에 정의 된대로 8 개의 우선 순위 레벨 (0-7) 중 하나를 지정할 수 있습니다. 값 0 은 IEEE 802.1D-2004 에 정의 된 기본 우선 순위 사용을 나타냅니다.
• **DSCP**	IETF RFC 2474 에 정의 된 지정된 응용 프로그램 유형에 대해 Diffserv 노드 동작을 제공하는 데 사용되는 DSCP 값입니다. DSCP 에는 64 개의 코드 포인트 값 (0 ~ 63) 중 하나가 포함될 수 있습니다. 값 0 은 RFC 2475 에 정의 된 기본 DSCP 값의 사용을 나타냅니다.
• **Adding a new policy**	새 정책을 추가하려면 ck [Add New Policy] 클릭하십시오. 새 정책에 대해 응용 프로그램 유형, 태그, VLAN ID, L2 우선 순위 및 DSCP 를 지정하십시오. "저장"을 클릭하십시오. 지원되는 정책 수는 32 개입니다.

Port Policies Configuration

모든 포트는 인증 된 사용자 ID 또는 포트 구성을 기반으로 동일한 네트워크 정책에 대해 고유 한 네트워크 정책 집합이나 다른 특성을 광고 할 수 있습니다..

목적	설명
• **Port**	구성이 적용되는 포트 번호입니다.
• **Policy ID**	특정 포트에 적용되는 정책 집합입니다. 정책 집합은 정책에 해당하는 확인란을 선택하여 선택합니다.

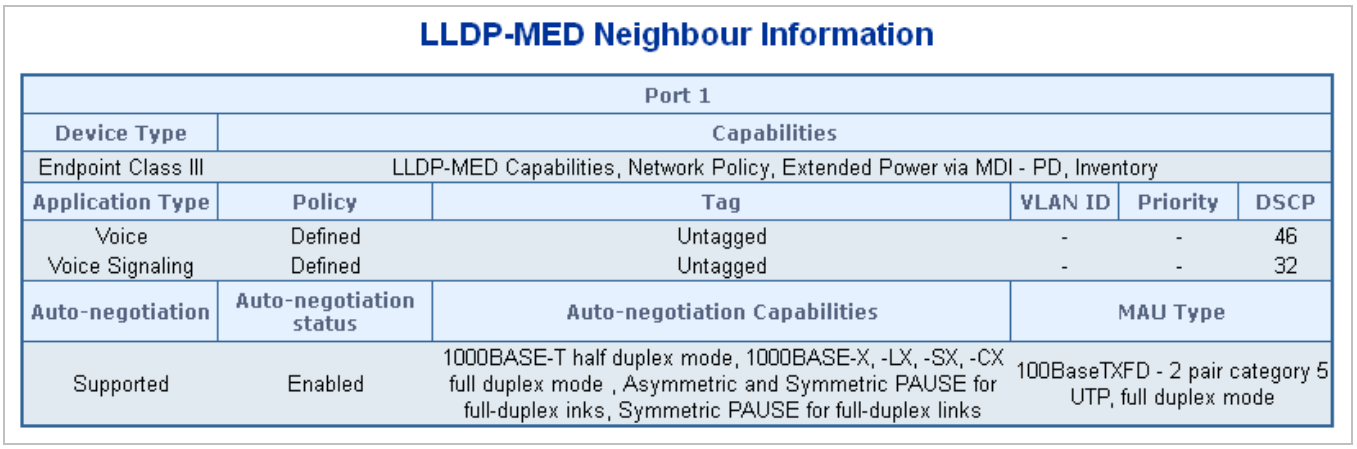
버튼

[Apply]: 변동사항을 클릭하여 저장합니다.

[Reset]: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.14.4 LLDP-MED Neighbor

이 페이지는 모든 LLDP-MED 이웃에 대한 상태 개요를 제공합니다. 표시된 표에는 LLDP 인접 항목이 감지 된 각 포트에 대한 행이 있습니다. 그림 4-14-3 의 LLDP-MED Neighbor Information 화면이 나타납니다. 열에는 다음 정보가 있습니다.:



LLDP-MED Neighbour Information

Port 1					
Device Type	**Capabilities**				
Endpoint Class III	LLDP-MED Capabilities, Network Policy, Extended Power via MDI - PD, Inventory				
Application Type	**Policy**	**Tag**	**VLAN ID**	**Priority**	**DSCP**
Voice	Defined	Untagged	-	-	46
Voice Signaling	Defined	Untagged	-	-	32
Auto-negotiation	**Auto-negotiation status**	**Auto-negotiation Capabilities**	**MAU Type**		
Supported	Enabled	1000BASE-T half duplex mode, 1000BASE-X, -LX, -SX, -CX full duplex mode , Asymmetric and Symmetric PAUSE for full-duplex inks, Symmetric PAUSE for full-duplex links	100BaseTXFD - 2 pair category 5 UTP, full duplex mode		

그림 4-14-3: LLDP-MED Neighbor Information 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

Fast start repeat count

목적	설명
• **Port**	LLDP 프레임을 수신 한 포트입니다.
• **Device Type**	LLDP-MED 장치는 네트워크 연결 장치 및 종단 장치라는 두 가지 기본 장치 유형으로 구성됩니다. **LLDP-MED 네트워크 연결 장치 정의** LLDP-MED 네트워크 연결 장치는 TIA-1057 에 정의 된대로 LLDP-MED 종단 장치 용 IEEE 802 기반 LAN 인프라에 대한 액세스를 제공합니다. LLDP-MED 네트워크 연결 장치는 다음 기술 중 하나를 기반으로 한 LAN 액세스 장치입니다.: 1. LAN 스위치/라우터 2. IEEE 802.1 브릿지 3. IEEE 802.3 중계기 (역사적 이유로 포함) 4. IEEE 802.11 Wireless Access Point 5. TIA-1057 에 의해 정의 된 IEEE 802.1AB 및 MED 확장을 지원하고 임의의 방법을 통해 IEEE 802 프레임을 중계 할 수있는 모든 장치. **LLDP-MED 엔드포인트 장치 정의** LLDP-MED 종단점 장치 범주에서 LLDP-MED 체계는 다음에서 정의 된대로 추가 종단점 장치 클래스로 분리됩니다. 각 LLDP-MED 종단점 장치 클래스는 이전 종단점 장치 클래스에 대해 정의 된 기능을 기반으로 정의됩니다. 예를 들어 미디어 종단점 (클래스 II)으로서의 준수를 주장하는 LLDP-MED 종단점 장치는 일반 종단점 (클래스 I)에 적용 할 수있는 TIA-1057 의 모든 측면과 통신 장치로서의 적합성을 주장하는 LLDP-MED 종단점 장치를 모두 지원합니다 (Class III)은 Media Endpoints (Class II)와 Generic Endpoints (Class I) 모두에 적용 할 수있는 TIA-1057 의 모든 측면을 지원합니다. **LLDP-MED 일반적인 엔드포인트(Class I)**

	LLDP-MED 일반 종단점 (클래스 I) 정의는 TIA-1057 에 정의 된 기본 LLDP 검색 서비스를 필요로하는 모든 종단점 제품에 적용되지만 IP 미디어를 지원하지 않거나 최종 사용자 통신 기기로 작동하지 않습니다. 이러한 장치에는 IP 통신 컨트롤러, 기타 통신 관련 서버 또는 TIA-1057 에 정의 된 기본 서비스가 필요한 장치가 포함될 수 있습니다 (단, 이에 국한되지는 않음). 이 클래스에 정의 된 검색 서비스에는 LAN 구성, 장치 위치, 네트워크 정책, 전원 관리 및 재고 관리가 포함됩니다. **LLDP-MED 미디어 엔드포인트 (Class II)** LDP-MED 미디어 엔드 포인트 (클래스 II) 정의는 IP 미디어 기능을 가진 모든 엔드 포인트 제품에 적용 할 수 있지만 특정 최종 사용자와 관련이있을 수도 있고 그렇지 않을 수도 있습니다. 기능에는 이전 일반 종점 클래스 (클래스 I)에 대해 정의 된 모든 기능이 포함되며 미디어 스트리밍과 관련된 요소가 포함되도록 확장됩니다. 이 클래스를 준수해야하는 제품 카테고리에는 음성 / 미디어 게이트웨이, 컨퍼런스 브리지, 미디어 서버 등이 포함됩니다 (이에 국한되지 않음). 이 클래스에 정의 된 검색 서비스에는 미디어 유형별 네트워크 계층 정책 검색이 포함됩니다.. **LLDP-MED 소통 엔드포인트 (Class III)** LLDP-MED 통신 엔드포인트 (클래스 III) 정의는 IP 미디어를 지원하는 최종 사용자 통신 기기로 작동하는 모든 종단 제품에 적용됩니다. 기능에는 이전 일반 종점 (클래스 I) 및 미디어 종점 (클래스 II) 클래스에 대해 정의 된 모든 기능이 포함되며 최종 사용자 장치와 관련된 측면을 포함하도록 확장됩니다. 이 클래스를 준수해야하는 제품 카테고리에는 IP 폰, PC 기반 소프트 폰 또는 최종 사용자를 직접 지원하는 기타 통신 장비와 같은 최종 사용자 통신 기기가 포함됩니다 (이에 국한되지 않음). 이 클래스에서 정의 된 검색 서비스에는 위치 식별자 (ECS / E911 정보 포함) 제공, 내장형 L2 스위치 지원, 재고 관리
• **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 확인 4. MDI – PSE 를 통한 확장된 전력 5. MDI – PD 를 통한 확장된 전력 6. 재고 7. 예약
• **Application Type**	응용 프로그램 엔드 포인트 또는 네트워크 연결 장치에서 보급 한이 네트워크 정책에 대해 정의 된 응용 프로그램의 기본 기능을 나타내는 유형입니다. 보잘것없는 응용 프로그램 유형이 아래에 나와 있습니다.

	■ **Voice** - 대화 형 음성 서비스를 지원하는 전용 IP 텔레포니 핸드셋 및 기타 유사한 어플라이언스에서 사용할 수 있습니다. 이러한 장치는 일반적으로 별도의 VLAN 에 배포되어 데이터 응용 프로그램과의 격리로 보안을 강화하고 쉽게 설치할 수 있습니다. ■ **Voice Signaling** - 음성 신호보다 음성 신호에 대해 다른 정책이 필요한 네트워크 토폴로지에서 사용. ■ **Guest Voice** - 대화 형 음성 서비스를 지원하는 자체 IP 텔레포니 핸드셋 및 기타 유사한 어플라이언스를 사용하여 게스트 사용자 및 방문객을위한 별도의 제한된 기능 세트 음성 서비스를 지원합니다. ■ **Guest Voice Signaling** - 게스트 음성 메시징과 게스트 음성 메시징에 대해 다른 정책이 필요한 네트워크 토폴로지에서 사용하기. ■ **Softphone Voice** - PC 또는 랩톱과 같은 일반적인 데이터 중심 장치에서 소프트 폰 응용 프로그램에 사용. ■ **Video Conferencing** - 실시간 대화 형 비디오 / 오디오 서비스를 지원하는 전용 화상 회의 장비 및 기타 유사한 장비에 사용. ■ **Streaming Video** - 브로드 캐스트 또는 멀티 캐스트 기반 비디오 컨텐츠 배포 및 특정 네트워크 정책 처리가 필요한 스트리밍 비디오 서비스를 지원하는 기타 유사한 응용 프로그램에 사용됩니다. 버퍼링을 사용하여 TCP 를 사용하는 비디오 응용 프로그램은이 응용 프로그램 유형을 의도한 용도로 사용하지 않습니다. ■ **Video Signaling** - 비디오 신호보다 비디오 신호에 대한 별도의 정책이 필요한 네트워크 토폴로지에서 사용하기위한 것입니다.
• **Policy**	**Policy** 엔드 포인트 장치가 정책이 장치에 필요하다는 것을 명시 적으로 알리고 싶다는 것을 나타냅니다. 정의 또는 알 수 없음 ■ **Unknown**: 지정된 응용 프로그램 유형에 대한 네트워크 정책은 현재 알 수 없습니다. ■ **Defined**: 네트워크 정책이 정의됩니다.
• **TAG**	TAG 는 지정된 응용 프로그램 유형이 태그가 붙어 있거나 태그가없는 VLAN 을 사용하고 있는지 여부를 나타냅니다. 태그없는 태그가 붙을 수 있음 ■ **Untagged**: 장치가 태그없는 프레임 형식을 사용하고 있으며 IEEE 802.1Q-2003 에 정의 된대로 태그 머리글을 포함하지 않습니다. ■ **Tagged**: 장치가 IEEE 802.1Q 태그가 지정된 프레임 형식을 사용하고 있습니다.
• **VLAN ID**	VLAN ID 는 IEEE 802.1Q-2003 에 정의 된 포트의 VLAN 식별자 (VID)입니다. 유효한 VLAN ID 를 정의하는 데는 1 에서 4094 사이의 값이 사용됩니다. 장치가 IEEE 802.1Q-2003 에 정의 된대로 우선 순위 태그가 지정된 프레임을 사용하는 경우 IEEE 802.1D 우선 순위 수준 만 중요하고 대신 입력 포트의 기본 PVID 가 사용되는 경우 값 0 (우선 순위 태그 지정)이 사용됩니다.
• **Priority**	우선 순위는 지정된 응용 프로그램 유형에 사용되는 2 계층 우선 순위입니다.

	우선 순위 8 개 중 하나 (0-7)까지 있음
• **DSCP**	DSCP 는 IETF RFC 2474 에 정의 된대로 지정된 응용 프로그램 유형에 대해 Diffserv 노드 동작을 제공하는 데 사용되는 DSCP 값입니다. 64 개의 코드 포인트 값 (0 ~ 63) 중 하나를 포함합니다.
• **Auto-negotiation**	**Auto-negotiation** 링크 파트너가 MAC / PHY 자동 협상을 지원하는지 식별합니다.
• **Auto-negotiation status**	**Auto-negotiation status** 링크 파트너에서 현재 자동 협상이 활성화되어 있는지 여부를 나타냅니다. 자동 협상이 지원되고 자동 협상 상태가 비활성화 된 경우 802.3 PMD 작동 모드는 자동 협상이 아닌 작동 가능한 MAU 유형 필드 값으로 결정됩니다.
• **Auto-negotiation Capabilities**	**Auto-negotiation Capabilities** 링크 파트너 MAC / PHY 기능을 보여줍니다.

버튼

Refresh: 즉시 페이지를 새로고침합니다.

Auto-refresh ☐: 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

4.14.5 Neighbor

이 페이지는 모든 LLDP 이웃에 대한 상태 개요를 제공합니다. 표시된 표에는 LLDP 인접 항목이 감지 된 각 포트에 대한 행이 있습니다. 그림 4-14-4 의 LLDP Neighbor Information 화면이 나타납니다.

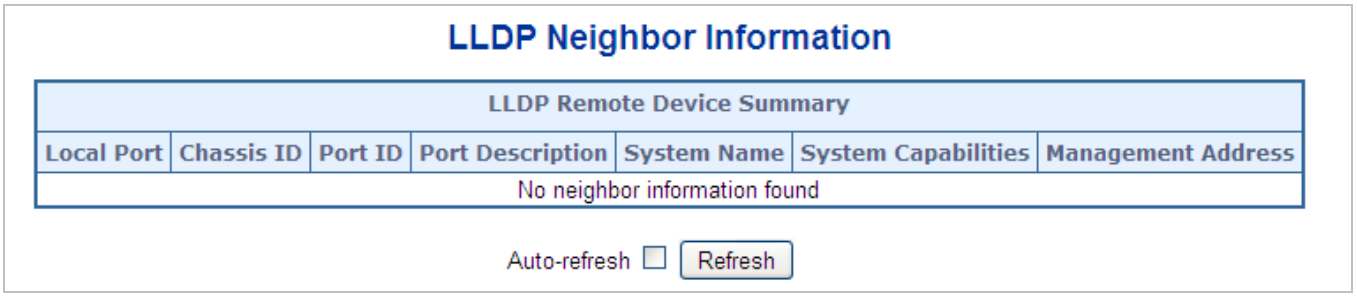


그림 4-14-4: LLDP Neighbor Information 화면

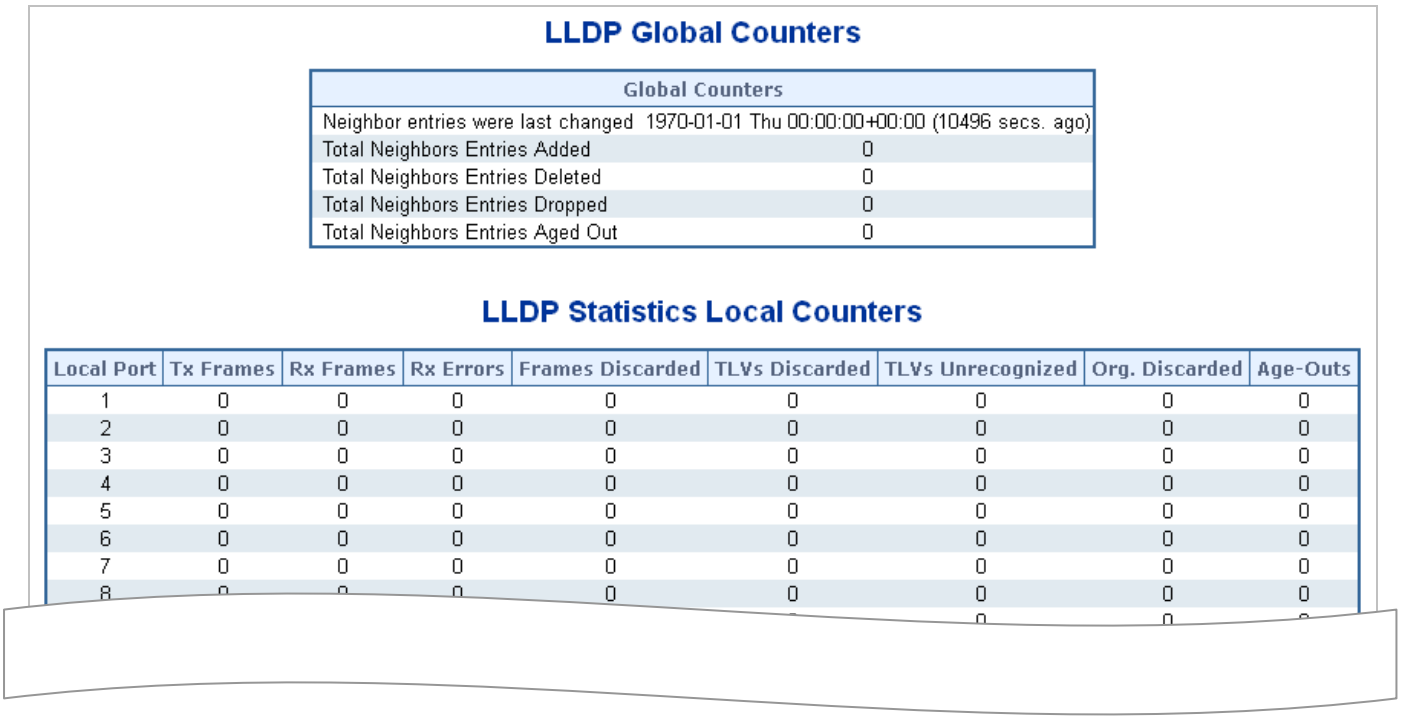
이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Local Port**	LLDP 프레임을 수신 한 포트입니다.
• **Chassis ID**	Shassis ID 는 이웃한의 LLDP 프레임을 식별합니다.
• **Port ID**	포트 ID 는 인접한 포트의 ID 입니다.

• **Port Description**	Port **Description 은** 인접한 장치가 보급 한 포트 설명입니다.
• **System Name**	시스템 이름은 이웃 장치가 알리는 이름입니다.
• **System Capabilities**	시스템 기능은 이웃 장치의 기능을 설명합니다. 가능한 기능은 다음과 같습니다: 1. 기타 2. 리피터 3. 브릿지 4. WLAN Access Point 5. 라우터 6. 전화기 7. DOCSIS 케이블 장치 8. 전용 지점 9. 예약 기능이 활성화되면 기능 뒤에 (+)가옵니다. 기능이 비활성화 된 경우 기능 뒤에 (-)가옵니다.
• **Management Address**	관리 주소는 네트워크 관리에 의한 검색을 돕기 위해 상위 계층 엔티티에 사용되는 인접 장치의 주소입니다. 이것은 예를 들어 이웃의 IP 주소를 보유할 수 있습니다.

4.14.6 Port Statistics

이 페이지는 모든 LLDP 트래픽의 개요를 제공합니다. 두 종류의 카운터가 표시됩니다. 글로벌 카운터는 전체 스위치를 참조하는 카운터이며 로컬 카운터는 현재 선택된 스위치의 카운터를 나타냅니다. 그림 4-14-5 의 LLDP Statistics (LLDP 통계) 화면이 나타납니다.



LLDP Global Counters

Global Counters	
Neighbor entries were last changed	1970-01-01 Thu 00:00:00+00:00 (10496 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 Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

그림 4-14-5: LLDP Statistics 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

Global Counters

목적	설명
• **Neighbor entries were last changed**	마지막 항목이 마지막으로 삭제되거나 추가 된 시간도 표시됩니다. 마지막 변경이 감지 된 이후 경과 된 시간도 표시합니다.
• **Total Neighbors Entries Added**	스위치 재부트 이후 추가 된 새 항목 수를 표시합니다.
• **Total Neighbors Entries Deleted**	스위치 재부팅 후 삭제 된 새 항목 수를 표시합니다
• **Total Neighbors Entries Dropped**	항목이 가득 찼기 때문에 삭제 된 LLDP 프레임 수를 나타냅니다.
• **Total Neighbors Entries Aged Out**	TTL (Time-To-Live) 만료로 인해 삭제 된 항목 수를 표시합니다.

LLDP Statistics Local Counters

표시된 표에는 각 포트에 대한 행이 들어 있습니다. 열에는 다음 정보가 있습니다.:

목적	설명
• **Local Port**	LLDP 프레임이 수신되거나 전송되는 포트입니다
• **Tx Frames**	포트에서 전송 된 LLDP 프레임 수입니다.
• **Rx Frames**	포트에서 수신 한 LLDP 프레임 수입니다.
• **Rx Errors**	어떤 종류의 오류가 포함 된 수신 된 LLDP 프레임 수입니다.
• **Frames Discarded**	LLDP 프레임이 포트에서 수신되고 스위치의 내부 표가 가득 차게 실행 된 경우 LLDP 프레임은 계수되고 폐기됩니다. 이 상황을 LLDP 표준에서 "너무 많은 이웃"이라고합니다. 섀시 ID 또는 원격 포트 ID 가 테이블에 아직 포함되어 있지 않으면 LLDP 프레임에 표에 새 항목이 필요합니다. 주어진 포트가 연결될 때, LLDP 셧다운 프레임이 수신 될 때 또는 엔트리가 오래 될 때, 엔트리는 표에서 제거됩니다.
• **TLVs Discarded**	각 LLDP 프레임은 TLV (TLV 는 "유형 길이 값"의 약자)로 알려진 여러 정보를 포함 할 수 있습니다. TLV 의 형식이 잘못되면 카운트되어 폐기됩니다.
• **TLVs Unrecognized**	올바른 형식의 TLV 수는 알 수없는 유형 값입니다.
• **Org. Discarded**	받은 조직적 TLV 수입니다.
• **Age-Outs**	각 LLDP 프레임에는 LLDP 정보가 유효한 시간 (에이지 아웃 시간)에 대한 정보가 들어 있습니다. 에이지 아웃 시간 내에 새로운 LLDP 프레임이

	수신되지 않으면 LLDP 정보가 제거되고 에이지 아웃 카운터가 증가된다.

버튼

Refresh: 즉시 페이지를 새로고침합니다.

Clear: 로컬 카운터를 지 웁니다. 모든 카운터 (글로벌 카운터 포함)는 재부팅시 지워집니다.

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

4.15 Network Diagnostics

이 섹션에서는 문제 해결을 위해 실제 레이어 및 IP 레이어 네트워크 진단 도구를 제공합니다. 진단 도구는 네트워크 관리자가 포인트 투 포인트 (point to point)와 더 나은 서비스 고객 간의 문제를 신속하게 진단 할 수 있도록 설계되었습니다.
진단 메뉴 항목을 사용하여 관리 대상 스위치의 기본 관리 세부 정보를 표시 및 구성하십시오. 시스템 아래에서 시스템 정보를 구성하고 볼 수있는 다음 항목이 제공됩니다.
이 섹션에는 다음 항목이 있습니다.:

- **Ping**
- **IPv6 Ping**
- **원격 IP Ping**
- **케이블 진단**

PING

.ping 및 IPv6 ping 을 사용하면 ICMP PING 패킷을 실행하여 IP 연결 문제를 해결할 수 있습니다. Managed Switch 는 ICMP 패킷을 전송하고 회신을 받으면 순번과 왕복 시간이 표시됩니다.

Cable Diagnostics

케이블 진단은 구리 케이블에서 테스트를 수행합니다. 이 기능은 케이블 길이 및 작동 조건을 식별하고 Cat5 연선 케이블에서 발생할 수있는 다양한 일반 결함을 격리 할 수 있습니다. 다음과 같은 두 가지 상태가있을 수 있습니다.:

- 1000BASE-T 모드에서 트위스트 페어 인터페이스에 링크가 설정된 경우 링크 또는 데이터 전송을 중단하지 않고도 케이블 진단을 실행할 수 있습니다..
- 링크가 100BASE-TX 또는 10BASE-T 로 설정된 경우 진단이 실행되는 동안 케이블 진단을 통해 링크가 끊어집니다.

진단이 끝나면 링크가 다시 설정됩니다. 그리고 다음과 같은 기능을 사용할 수 있습니다.

- 케이블 링크 간의 결합
- 케이블 간 종단
- 케이블 길이

4.15.1 Ping

이 페이지에서는 ICMP PING 패킷을 실행하여 IP 연결 문제를 해결할 수 있습니다.

"시작"을 누르면 5 개의 ICMP 패킷이 전송되고 회신을 받으면 순번과 왕복 시간이 표시됩니다. 모든 패킷에 대한 응답이 수신되거나 시간이 초과 될 때까지 페이지가 자동으로 새로 고침됩니다. 그림 4-15-1 의 ICMP Ping 화면이 나타납니다.

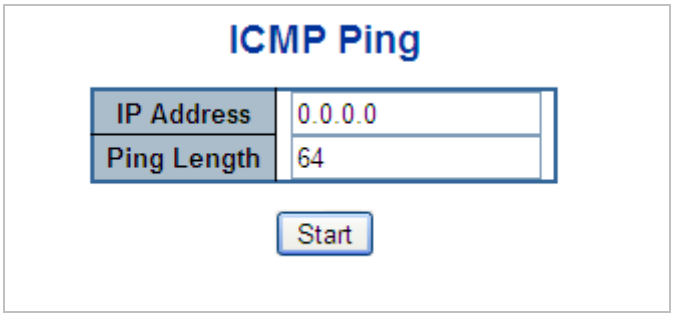


그림 4-15-1: ICMP Ping 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **IP Address**	IP 주소 도착지
• **Ping Length**	ICMP 패킷의 페이로드 크기입니다. 값의 범위는 2 바이트에서 1452 바이트입니다.

Note

대상 IP 주소가 Managed Switch의 동일한 네트워크 서브넷 내에 있거나 올바른 게이트웨이 IP 주소를 설정했는지 확인하십시오.

버튼

Start: ICMP 패킷을 전송하려면 클릭하십시오.

New Ping: PING 을 사용하여 진단을 다시 시작하려면 클릭하십시오.

4.15.2 IPv6 Ping

이 페이지에서는 ICMPv6 PING 패킷을 실행하여 IPv6 연결 문제를 해결할 수 있습니다.

"시작"을 누르면 5 개의 ICMPv6 패킷이 전송되고 응답을 받으면 순번과 왕복 시간이 표시됩니다. 모든 패킷에 대한 응답이 수신되거나 시간이 초과 될 때까지 페이지가 자동으로 새로 고침됩니다. 그림 4-15-2 의 ICMPv6 Ping 화면이 나타납니다..

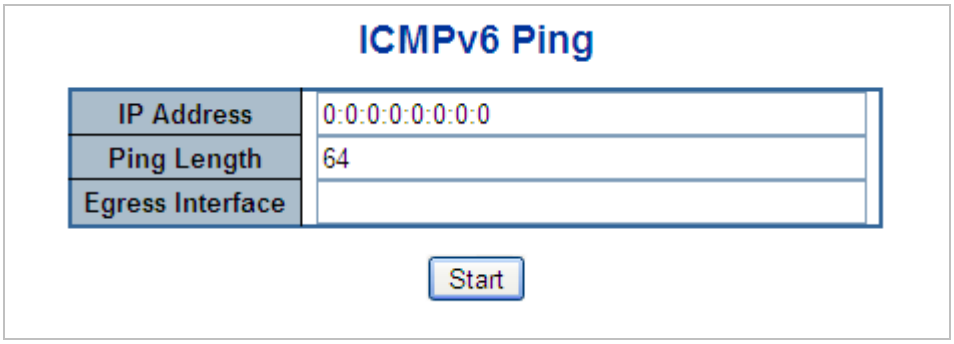


그림 4-15-2: ICMPv6 Ping 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **IP Address**	IP 주소의 도착지입니다.
• **Ping Length**	ICMP 패킷의 페이로드 크기입니다. 값의 범위는 2 바이트에서 1452 바이트입니다.
• **Egress Interface**	ICMP 패킷이 전송되는 특정 송신 IPv6 인터페이스의 VLAN ID (VID)입니다. 주어진 VID 의 범위는 1 - 4094 이며 해당 IPv6 인터페이스가 유효한 경우에만 유효합니다. 인터페이스의 출구가 주어지지 않을 때, PING6 은 목적지에 가장 잘 맞는 인터페이스를 찾습니다. 루프백 주소에 대해 송신 인터페이스를 지정하지 마십시오. 링크 로컬 또는 멀티 캐스트 주소에 대해 출력 인터페이스를 지정하십시오.

버튼

Start: ICMP 패킷을 전송합니다.

New Ping: PING 을 사용하여 진단을 다시 시작하려면 클릭하십시오..

4.15.3 Remote IP Ping Test

.

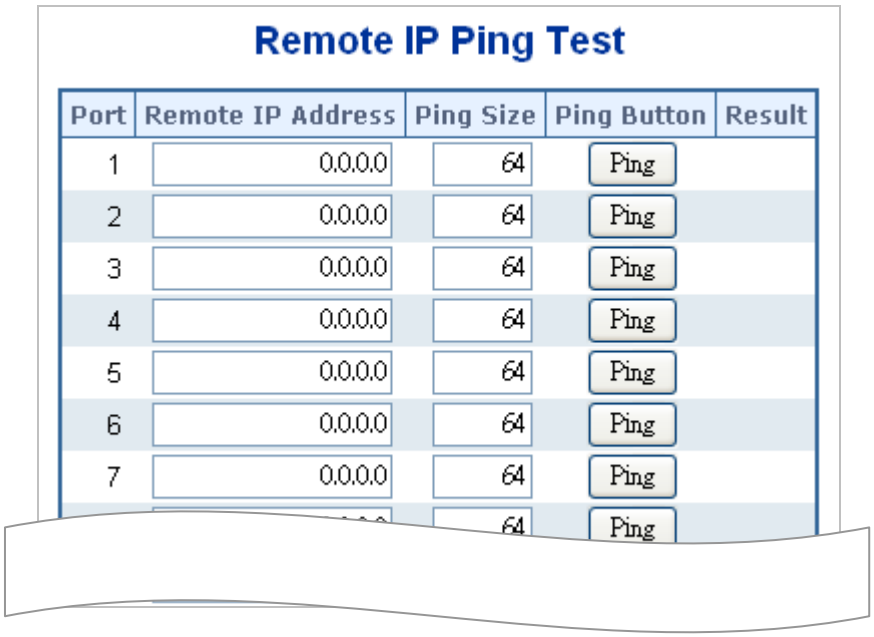


그림 4-15-3: Remote IP Ping Test 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	설정에 관한 논리포인트
• **Remote IP Address**	목적지 IP 주소
• **Ping Size**	ICMP 패킷의 페이로드 크기입니다. 값의 범위는 8 바이트에서 1400 바이트입니다.
• **Result**	핑결과를 표시합니다

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

Clear: IP 주소로 출력된 Ping 값을 지웁니다.

4.15.4 Cable Diagnostics

이 페이지는 케이블 진단을 실행하는 데 사용됩니다.

진단을 실행하려면를 누르십시오. 약 5 초가 소요됩니다. 모든 포트를 선택하면 약 15 초가 걸릴 수 있습니다. 완료되면

페이지가 자동으로 새로 고쳐지고 케이블 상태 표에서 케이블 진단 결과를 볼 수 있습니다. 케이블 진단은 길이가 7 - 140 미터 인 케이블에 대해서만 정확합니다.

10 및 100 Mbps 포트는 케이블 진단을 실행하는 동안 연결됩니다. 따라서 10 또는 100 Mbps 관리 포트에서 케이블 진단을 실행하면 VeriPHY 가 완료 될 때까지 스위치가 응답을 중지하게됩니다. 그림 4-15-4 의 VeriPHY 케이블 진단 화면이 나타납니다..

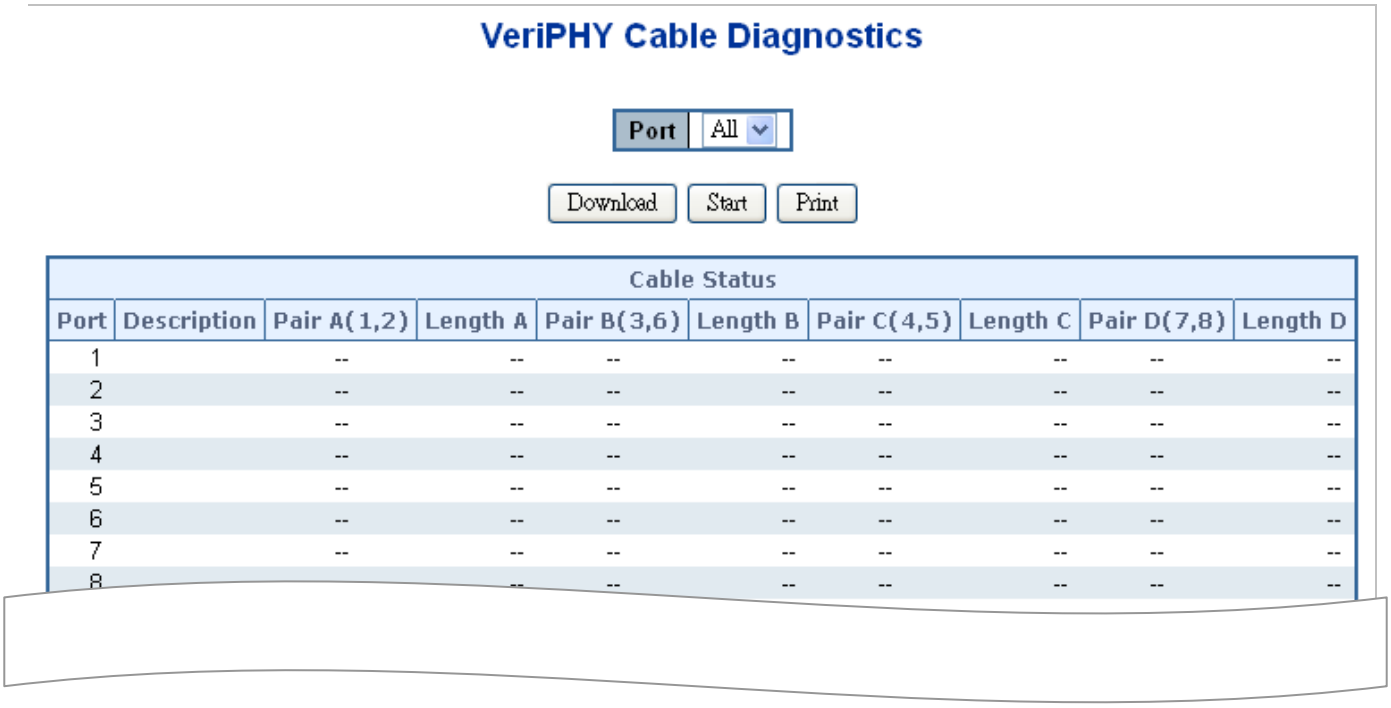


그림 4-15-4: VeriPHY Cable Diagnostics 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	케이블 진단을 요청하는 포트.
• **Description**	포트 별 표시 설명.

• Cable Status	**Port**: 포트 번호. **Pair**: 케이블 쌍의 상태. **OK** – 올바르게 종료 된 한 쌍 **Open** – 한 쌍 열기 **Short** – 쇼트가 된 한 쌍 **Short A** - 페어 A 에 교차 단쌍 **Short B** - 페어 B 에 교차 단쌍 **Short C** – 페어 C 에 교차 단쌍 **Short D** - 페어 D 에 교차 단쌍 **Cross A** – 페어 A 와의 비정상적인 크로스 결합 **Cross B** - 페어 B 와의 비정상적인 크로스 결합 **Cross C** - 페어 C 와의 비정상적인 크로스 결합 **Cross D** - 페어 D 와의 비정상적인 크로스 결합 **Length**: 케이블 쌍의 길이 (미터). 최대거리값은 3 미터입니다.

버튼

Start: 진단 모드를 클릭하여 시작합니다.

4.16 Loop Protection

이 장에서는 관리 스위치에서 브로드 캐스트 루프를 방지하는 루프 보호 기능을 제공하는 루프 보호 기능을 사용하는 방법을 설명합니다.

4.16.1 Configuration

이 페이지에서는 사용자가 현재 Loop Protection 구성을 검사 할 수 있으며, 가능하면이를 변경할 수도 있습니다. 그림 4-17-1 의 화면이 나타납니다..

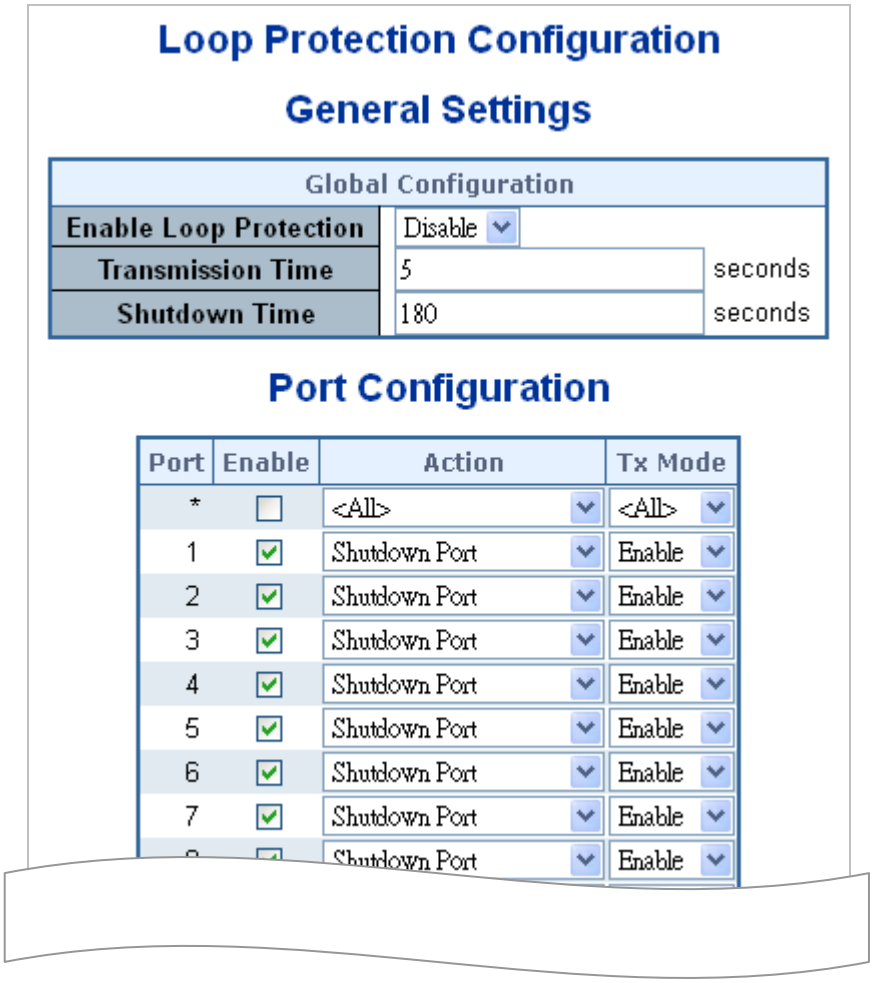


그림 4-17-1: Loop Protection Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

General Settings

목적	설명
• **Enable Loop Protection**	루프 보호를 활성화할지 여부를 제어합니다 (전체적으로).
• **Transmission Time**	포트에서 전송 된 루프 보호 PDU 사이의 간격. 유효한 값은 1 - 10 초입니다.

• **Shutdown Time**	루프가 발생했을 때 포트가 비활성화 된 상태로 유지되는 기간 (초)은 감지되며 포트 동작은 포트를 종료합니다. 유효한 값은 0 - 604800 초 (7 일)입니다. 0 값은 포트를 비활성화 된 상태로 유지합니다

Port Configuration

목적	설명
• **Port**	포트의 스위치 포트 번호입니다.
• **Enable**	이 스위치 포트에서 루프 보호를 활성화할지 여부를 제어합니다
• **Action**	포트에서 루프 감지 시 작업을 구성합니다. 유효한 값은 Shutdown Port, Shutdown Port (종료 포트) 및 Log or Log Only (로그 또는 로그 전용)입니다.
• **Tx Mode**	포트가 루프 보호 PDU 를 적극적으로 생성하는지 또는 루프 된 PDU 를 수동적으로 찾는 지 여부를 제어합니다.

버튼

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.16.2 Loop Protection Status

이 페이지는 스위치의 루프 보호 포트 상태를 표시합니다. 그림 4-17-2 의 화면이 나타납니다.

그림 4-17-2: Loop Protection Status 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Port**	논리 포트의 관리형 스위치 포트 번호입니다.
• **Action**	현재 구성된 동작하는 포트입니다.
• **Transmit**	현재 구성된 포트 전송 모드입니다.

• **Loops**	포트에서 감지 된 루프 수입니다
• **Status**	포트의 현재 루프 보호 상태입니다.
• **Loop**	루프가 현재 포트에서 감지되는지 여부.
• **Time of Last Loop**	마지막 루프 이벤트가 감지 된 시간입니다

버튼

Refresh: 즉시 페이지를 새로고침합니다.

Auto-refresh : 정기적으로 페이지 자동 새로 고침을 사용하려면이 상자를 선택하십시오.

4.17 RMON

RMON 은 표준 SNMP 의 가장 중요한 확장입니다. RMON 은 표준 네트워크 모니터 기능 및 인터페이스를 정의하고 SNMP 관리 단말기와 원격 모니터 간의 통신을 가능하게하는 MIB 정의 세트입니다. RMON 은 서브넷 내부의 작업을 모니터링하는 매우 효율적인 방법을 제공합니다.

RMON 의 MID 는 10 개의 그룹으로 구성됩니다. 스위치는 가장 자주 사용되는 그룹 1, 2, 3 및 9 를 지원합니다.:

- **Statistics:** 에이전트가 모니터링하는 각 서브넷에 대한 기본 사용 및 오류 통계를 유지 관리합니다.
- **History:** Statistics (통계)에서 사용 가능한 정기 통계 샘플을 기록합니다.
- **Alarm:** 관리 콘솔 사용자가 RMON 에이전트 레코드에 대한 샘플 간격 및 경고 임계 값에 대해 개수 또는 정수를 설정할 수 있습니다.
- **Event:** RMON 에이전트가 생성 한 모든 이벤트의 목록입니다.

알람은 Event 구현에 따라 다릅니다. 통계 및 히스토리는 현재 또는 히스토리 서브넷 통계를 표시합니다. 알람 및 이벤트는 네트워크의 정수 데이터 변경을 모니터링하고 비정상적인 이벤트 (트랩 전송 또는 로그 기록)에 대한 경고를 제공하는 방법을 제공합니다.

4.17.1 RMON Alarm Configuration

이 페이지에서 RMON 알람 표를 구성하십시오. 엔트리 인덱스 키는 ID 입니다.; 그림 4-18-1 의 화면이 나타납니다..

그림 4-18-1: RMON Alarm Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제됩니다.
• **ID**	항목의 색인을 나타냅니다. 범위는 1 에서 65535 사이입니다.
• **Interval**	샘플링 및 상승 및 하강 임계 값 비교를위한 간격 (초)을 나타냅니다. 범위는 1 ~ 2 ^ 31-1 입니다.
• **Variable**	샘플링 할 특정 변수를 나타냅니다. 가능한 변수는 다음과 같습니다: ■ **InOctets**: 구성한 문자를 포함하여 인터페이스에서 수신 한 총 8 진수. ■ **InUcastPkts**: 상위 계층 프로토콜에 전달되는 유니 캐스트 패킷 수. ■ **InNUcastPkts**: 상위 계층 프로토콜로 전달되는 브로드 캐스트 및 멀티 캐스트 패킷 수입니다. ■ **InDiscards**: 패킷이 정상적이더라도 버려지는 인바운드 패킷 수..

	■ **InErrors**: 상위 계층 프로토콜로 전달할 수없는 오류가있는 인바운드 패킷 수. ■ **InUnknownProtos**: 알 수 없거나 지원되지 않는 프로토콜로 인해 버려진 인바운드 패킷 수. ■ **OutOctets**: 구상된 문자를 포함하여 인터페이스에서 전송 된 옥텟의 수. ■ **OutUcastPkts**: 전송을 요구하는 유니 캐스트 (uni-cast) 패킷의 수.. ■ **OutNUcastPkts**: 전송을 요청하는 브로드 캐스트 및 멀티 캐스트 패킷 수입니다. ■ **OutDiscards**: 패킷이 정상적인 경우 폐기되는 아웃 바운드 패킷 수입니다 ■ **OutErrors**: 오류로 인해 전송할 수 없었던 아웃 바운드 패킷 수 ■ **OutQLen**: 출력 패킷 대기열의 길이 (패킷 단위).
• **Sample Type**	선택한 변수를 샘플링하고 임계 값과 비교할 값을 계산하는 방법은 가능한 샘플 유형입니다.: ■ **Absolute**: 셈플을 직접 가져옵니다. ■ **Delta**: 샘플 간의 차이를 계산합니다 (기본값).
• **Value**	마지막 샘플링 기간 동안의 통계 값.
• **Startup Alarm**	선택한 변수를 샘플링하고 임계 값과 비교할 값을 계산하는 방법은 가능한 샘플 유형입니다.: ■ **RisingTrigger alarm** 첫 번째 값이 상승 임계 값보다 클 때 ■ **FallingTrigger alarm**. 첫 번째 값이 하강 임계 값보다 작은 경우 ■ **RisingOrFallingTrigger alarm** 첫 번째 값이 상승 임계 값보다 크거나 하강 임계 값보다 작은 경우 (기본값)
• **Rising Threshold**	상위 임계 값 (-2147483648-2147483647)
• **Rising Index**	상위 이벤트 색인 (1-65535).
• **Falling Threshold**	하위 임계 값 (-2147483648-2147483647)
• **Falling Index**	이벤트 지수 하락 (1-65535).

버튼

Add New Entry: 새로운 개체의 엔트리를 추가합니다.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.17.2 RMON Alarm Status

페이지는 RMON 알람 항목의 개요를 제공합니다. 각 페이지는 알람 테이블의 항목을 99 개까지 표시하며 기본값은 20 개이며 "페이지 당 항목 수"입력 필드를 통해 선택됩니다. 처음 방문했을 때, 웹 페이지는 알람 테이블의 처음부터 처음 20 개의 항목을 보여줍니다. 가장 먼저 표시되는 ID 는 Alarm 테이블에서 가장 낮은 ID 로 표시됩니다. 그림 4-18-2 의

화면이 나타납니다.

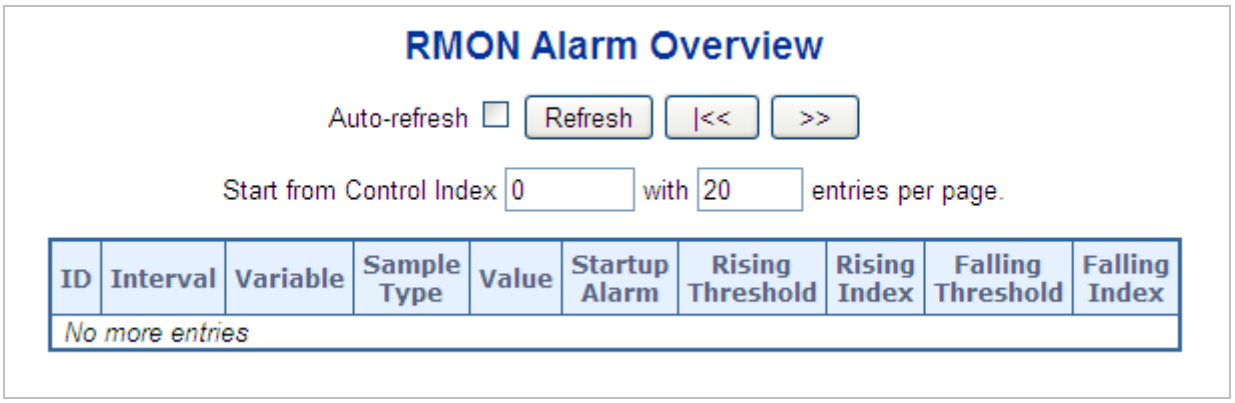


그림 4-18-2: RMON Alarm Overview 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **ID**	경보 제어 항목의 색인을 나타냅니다
• **Interval**	샘플링 및 상승 및 하강 임계 값 비교를위한 간격 (초)을 나타냅니다.
• **Variable**	샘플링 할 특정 변수를 나타냅니다.
• **Sample Type**	선택한 변수를 샘플링하고 임계 값과 비교할 값을 계산하는 방법.
• **Value**	마지막 샘플링 기간 동안의 통계 값.
• **Startup Alarm**	이 항목이 처음 유효한 것으로 설정된 경우 보낼 수있는 알람입니다.
• **Rising Threshold**	상승하는 임계 값.
• **Rising Index**	상승하는 이벤트 인덱스.
• **Falling Threshold**	떨어지는 임계 값.
• **Falling Index**	떨어지는 이벤트 색인.

버튼

Refresh: 즉시 페이지를 새로고침합니다.

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

<<: 알람 테이블의 첫 번째 항목, 즉 가장 낮은 ID 를 가진 항목부터 테이블을 업데이트합니다.

>>:현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 업데이트합니다..

4.17.3 RMON Event Configuration

이 페이지에서 RMON 이벤트 표를 구성하십시오. 엔트리 인덱스 키는 ID 입니다. 그림 4-18-3 의 화면이 나타납니다.

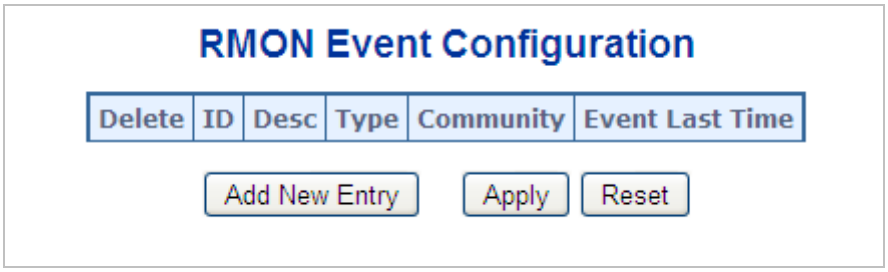


그림 4-18-4: RMON Event Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제됩니다.
• **ID**	항목의 색인을 나타냅니다. 범위는 1 에서 65535 사이입니다.
• **Desc**	문자열의 길이는 0 ~ 127 이며, 디폴트는 Null 값 입니다
• **Type**	이벤트의 공지를 나타냅니다. 가능한 타입은 다음과 같습니다.: ■ **none**: 구성 된문자를 포함하여 인터페이스에서 수신 한 총 8 진수. ■ **log**: 상위 계층 프로토콜에 전달되는 유니 캐스트 (uni-cast) 패킷의 수. ■ **snmptrap**: 상위 계층 프로토콜로 전달되는 브로드 캐스트 및 멀티 캐스트 패킷 수입니다 ■ **logandtrap**: 패킷이 정상적 일지라도 버려지는 인바운드 패킷 수.
• **Community**	트랩을 보낼 때 커뮤니티를 지정하고, 문자열 길이는 0 에서 127 까지이며, 기본값은 "public"입니다.
• **Event Last Time**	이벤트 항목이 마지막으로 이벤트를 생성 할 때의 sysUpTime 값을 나타냅니다.

버튼

Add New Entry: 새 커뮤니티 항목을 추가하려면 클릭하십시오.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.17.4 RMON Event Status

이 페이지는 RMON 이벤트 표 항목에 대한 개요를 제공합니다. 각 페이지는 "표당 입력 수"입력란을 통해 선택된 이벤트 표의 최대 99 개 항목 (기본값은 20)을 표시합니다. 처음 방문했을 때, 웹 페이지는 이벤트 테이블의 처음부터 처음 20 개의 항목을 보여줍니다. 가장 먼저 표시되는 이벤트 색인 및 로그 색인은 이벤트 표에 있습니다. 그림 4-18-5 의 화면이 나타납니다..

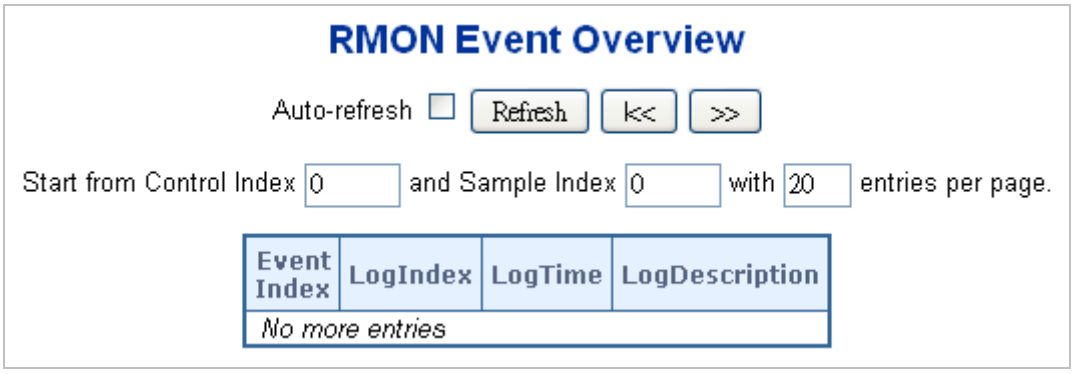


그림 4-18-5: RMON Event Overview 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Event Index**	이벤트 항목의 색인을 나타냅니다.
• **Log Index**	로그 항목의 색인을 나타냅니다.
• **LogTime**	이벤트 로그 시간을 나타냅니다.
• **Log설명**	이벤트 설명을 나타냅니다.

버튼

Refresh: 즉시 페이지를 새로고침합니다.

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

<<.알람테이블의 첫 번째 항목부터 시작하여 테이블을 업데이트합니다. 즉 가장 낮은 ID 를 가진 항목을 업데이트합니다.

>>: 현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 업데이트합니다.

<<: 현재 표시된 처음 항목 이전의 항목으로 시작하여 표를 업데이트합니다.

4.17.5 RMON History Configuration

이 페이지의 RMON History 표를 구성하십시오. 엔트리 인덱스 키는 ID 입니다. 그림 4-18-6 의 화면이 나타납니다.

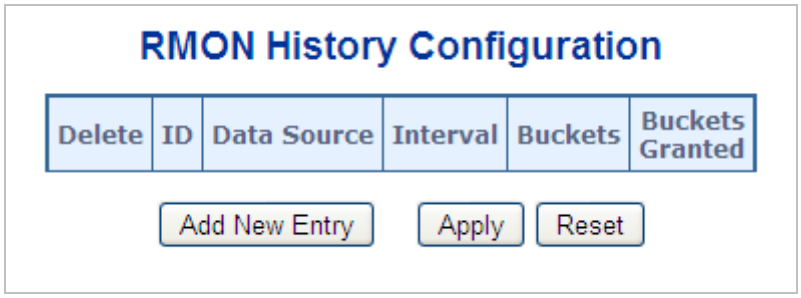


그림 4-18-6: RMON History Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제됩니다.
• **ID**	항목의 색인을 나타냅니다. 범위는 1 에서 65535 사이입니다.
• **Data Source**	모니터 할 포트 ID 를 나타냅니다.
• **Interval**	기록 통계 데이터를 샘플링하는 간격을 초 단위로 나타냅니다. 범위는 1 - 3600 이며, 기본값은 1800 초입니다
• **Buckets**	RMON 에 저장된이 History 제어 항목과 관련된 최대 데이터 항목을 나타냅니다. 범위는 1 - 3600 이며, 기본값은 50 입니다.
• **Buckets Granted**	데이터의 갯수는 RMON 에 저장됩니다.

버튼

Add New Entry: 새 커뮤니티 항목을 추가하려면 클릭하십시오.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.17.6 RMON History Status

이 페이지는 RMON 기록 항목에 대한 세부 정보를 제공합니다. 그림 4-18-7 의 화면이 나타납니다.

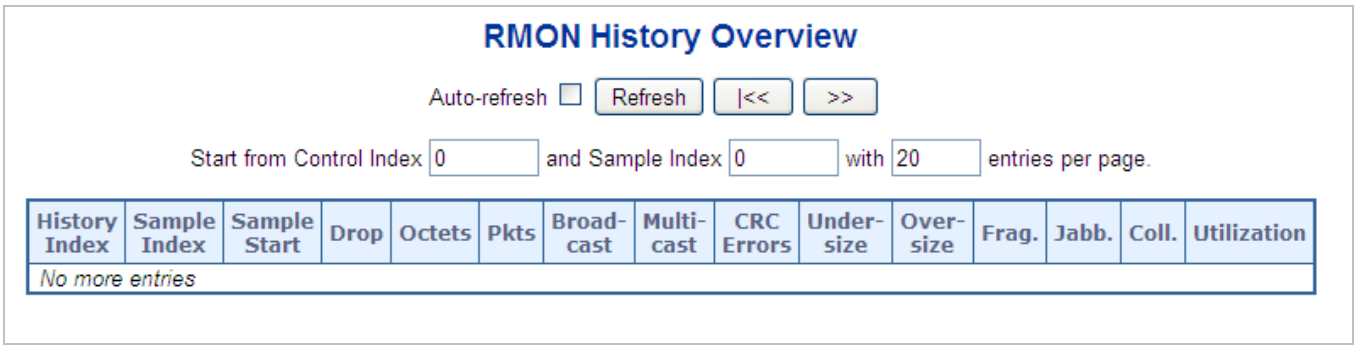


그림 4-18-7: RMON History Overview 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **History Index**	기록 제어 항목의 색인을 나타냅니다.
• **Sample Index**	컨트롤 항목과 연결된 데이터 항목의 인덱스를 나타냅니다.
• **Sample Start**	샘플을 측정 한 간격의 시작 부분에있는 sysUpTime 의 값입니다
• **Drop**	자원 부족으로 인해 프로브가 패킷을 삭제 한 총 이벤트 수입니다.
• **Octets**	네트워크에서 수신 한 데이터의 총 옥텟 수 (불량 패킷 포함).
• **Pkts**	수신 된 총 패킷 수 (불량 패킷, 브로드 캐스트 패킷 및 멀티 캐스트 패킷 포함).
• **Broadcast**	브로드 캐스트 주소로 향하는 수신 된 양호한 패킷의 총 수
• **Multicast**	멀티 캐스트 주소로 향하는 수신 된 양호한 패킷의 총 수.
CRC Errors	64 ~ 1518 옥텟 (포함하지만 프레이밍 비트는 제외하고 FCS 옥텟 포함)을 포함하지만 옥텟 수 (FCS 오류)가 포함 된 불량 프레임 검사 시퀀스 (FCS)를 포함하여 수신 된 총 패킷 수 또는 정수가 아닌 수의 8 진수를 갖는 잘못된 FCS (정렬 오류).
• **Undersize**	64 옥텟보다 적게 수신 된 총 패킷 수입니다.
• **Oversize**	수신 된 총 패킷 수는 1518 옥텟보다 긴 경우입니다.
• **Frag.**	크기가 유효하지 않은 CRC 로 수신 된 64 옥텟보다 작은 프레임 수입니다.
• **Jabb.**	크기가 유효하지 않은 CRC 로 수신 된 64 옥텟보다 큰 프레임 수입니다.
• **Coll.**	이더넷 세그먼트의 총 충돌 수를 가장 잘 예측 한 것입니다.
• **Utilization**	이 샘플링 간격 동안이 인터페이스에서 평균 물리 계층 네트워크 사용률을 가장 잘 예측 한 값입니다 (단위 : 백분율).

버튼

Refresh: 즉시 페이지를 새로고침합니다.

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

<<: 히스토리 테이블의 첫 번째 항목, 즉 가장 낮은 히스토리 인덱스 및 샘플 인덱스가있는 항목부터 테이블을 업데이트합니다.

>>: 현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 업데이트합니다.

4.17.7 RMON Statistics Configuration

이 페이지에서 RMON 통계 표를 구성하십시오. 엔트리 인덱스 키는 ID 입니다. 그림 4-18-8 의 화면이 나타납니다.

그림 4-18-8: RMON Statistics Configuration 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제됩니다.
• **ID**	항목의 색인을 나타냅니다. 범위는 1 에서 65535 사이입니다.
• **Data Source**	모니터 할 포트 ID 를 나타냅니다.

버튼

Add New Entry: 새 커뮤니티 항목을 추가하려면 클릭하십시오.

Apply: 변동사항을 클릭하여 저장합니다.

Reset: 변동사항을 취소하고 이전 저장상태로 되돌리려면 클릭합니다.

4.17.8 RMON Statistics Status

이 페이지는 RMON 통계 항목의 개요를 제공합니다. 각 페이지는 통계 테이블에서 최대 99 개의 항목을 표시하며

기본값은 20 이고 "페이지 당 항목 수"입력 필드를 통해 선택됩니다. 처음 방문했을 때 웹 페이지는 통계 표의 처음부터 처음 20 개의 항목을 표시합니다. 가장 먼저 표시되는 ID 는 통계표에서 가장 낮은 ID 로 표시됩니다. 그림 4-18-9 의 화면이 나타납니다..

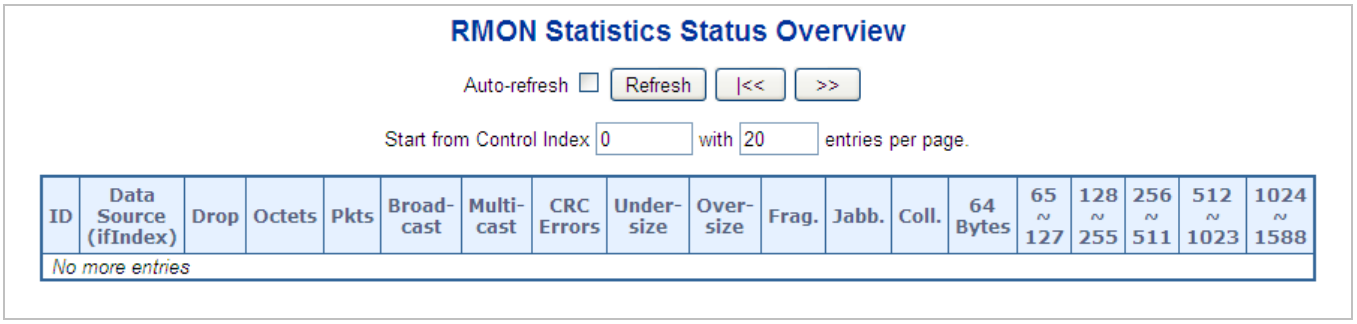


그림 4-18-9: RMON Statistics Status Overview 화면

이 페이지에서는 다음과 같음을 나타냅니다.:

목적	설명
• **ID**	통계 항목 색인을 나타냅니다.
• **Data Source (ifIndex)**	모니터 할 포트 ID 입니다.
• **Drop**	자원 부족으로 인해 프로브가 패킷을 삭제 한 총 이벤트 수입니다.
• **Octets**	네트워크에서 수신 한 데이터의 총 옥텟 수 (불량 패킷 포함).
• **Pkts**	수신 된 총 패킷 수 (불량 패킷, 브로드 캐스트 패킷 및 멀티 캐스트 패킷 포함).
• **Broadcast**	브로드 캐스트 주소로 향하는 수신 된 양호한 패킷의 총 수.
• **Multicast**	멀티 캐스트 주소로 향하는 수신 된 양호한 패킷의 총 수.
• **CRC Errors**	64 옥텟과 1518 옥텟 사이의 길이 (프레이밍 비트 제외, FCS 옥텟 포함)를 가진 수신 된 총 패킷 수.
• **Undersize**	64 옥텟보다 적게 수신 된 총 패킷 수입니다.
• **Oversize**	수신 된 총 패킷 수는 1518 옥텟보다 길었습니다.
• **Frag.**	크기가 유효하지 않은 CRC 로 수신 된 64 옥텟보다 작은 프레임 수입니다.
• **Jabb.**	크기가 유효하지 않은 CRC 로 수신 된 64 옥텟보다 큰 프레임 수입니다.
• **Coll.**	이더넷 세그먼트의 총 충돌 수를 가장 잘 예측 한 것입니다.
• **64 Bytes**	길이가 64 옥텟 인 총 패킷 수 (불량 패킷 포함).
• **65~127**	길이가 65 에서 127 옥텟 사이 인 총 패킷 수 (불량 패킷 포함).
• **128~255**	길이가 128 에서 255 옥텟 사이 인 수신 된 패킷 (불량 패킷 포함)의 총 수.
• **256~511**	길이가 256 에서 511 옥텟 사이 인 총 패킷 수 (불량 패킷 포함).

• **512~1023**	수신 한 길이가 512 에서 1023 옥텟 인 불량 패킷을 포함한 총 패킷 수입니다.
• **1024~1518**	길이가 1024 에서 1518 옥텟 사이 인 총 패킷 수 (불량 패킷 포함).

버튼

Refresh: 즉시 페이지를 새로고침합니다.

Auto-refresh : 페이지를 자동으로 새로 고치며 3 초마다 새로고침이 발생합니다..

<<: 알람 테이블의 첫 번째 항목, 즉 가장 낮은 ID 를 가진 항목부터 테이블을 업데이트합니다.

>>: 현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 업데이트합니다.

5. SWITCH OPERATION

5.1 Address Table

관리되는 스위치는 주소 테이블로 구현됩니다. 이 주소 표는 여러 항목으로 구성됩니다. 각 항목은 MAC 주소, 포트 번호 등을 포함하여 네트워크에있는 일부 노드의 주소 정보를 저장하는 데 사용됩니다.

5.2 Learning

하나의 패킷이 어떤 포트에서 들어 오면, 관리되는 스위치는 소스 주소 인 포트 번호를 기록합니다. 그리고 주소 테이블에있는 다른 관련 정보. 이 정보는 향후 패킷에 대한 전달 또는 필터링을 결정하는 데 사용됩니다.

5.3 Forwarding & Filtering

하나의 패킷이 관리형 스위치의 일부 포트에서 오면 소스 주소를 배우는 것 외에도 목적지 주소를 확인합니다. 관리형 스위치는 대상 주소에 대한 주소테이블을 검색합니다. 이 패킷이 없으면이 패킷은이 패킷이 들어오는 포트를 제외한 다른 모든 포트로 전달됩니다.이 포트는이 패킷을 연결된 네트워크로 전송합니다. 검색된 경우이 패킷과 다른 포트에 대상 주소가있는 경우 관리형 스위치는 이 패킷을 주소 테이블의 정보에 따라이 대상 주소가있는 포트로 전달합니다. 그러나 목적지 주소가이 패킷과 같은 포트에 있으면이 패킷이 필터링됩니다. 따라서 네트워크 처리량 및 가용성이 향상됩니다.

5.4 Store-and-Forward

Store-and-Forward 는 패킷 포워딩 기술의 한 유형입니다. 저장 - 전달 관리 스위치는 수신 프레임을 내부 버퍼에 저장하고, 전송 전에 완전한 오류 검사를 수행합니다. 따라서 오류 패킷이 발생하지 않아 네트워크가 효율성과 안정성을 필요로 할 때 최상의 선택입니다.
관리형 스위치는 패킷 헤더에서 목적지 주소를 스캔하고 들어오는 포트에 대해 라우팅 표를 검색하여 필요한 경우에만 패킷을 전달합니다. 고속 포워딩은 스위치를 서버를 네트워크에 직접 연결하여 처리량과 가용성을 향상시키는 데 유용합니다. 그러나 스위치는 존재하는 허브를 분류하는 데 사용되며 거의 항상 전체 성능을 향상시킵니다. 모든 이더넷 네트워크 환경에서 이더넷 스위칭을 쉽게 구성하여 기존 케이블 및 어댑터를 사용하여 대역폭을 크게 높일 수 있습니다. 관리 형 스위치의 학습 기능으로 인해 각 수신 및 발신 패킷의 소스 주소와 해당 포트 번호가 라우팅 테이블에 저장됩니다. 이 정보는 이후 목적지 주소가 소스 주소와 동일한 세그먼트에있는 패킷을 필터링하는 데 사용됩니다. 이로 인해 네트워크 트래픽이 해당 도메인에 국한되며 네트워크의 전반적인로드가 줄어 듭니다.
관리형스위치는 "Store and Forward"를 수행하므로 오류 패킷이 발생하지 않습니다. 보다 신뢰성있게, 재전송 속도를 감소시킨다. 패킷 손실은 발생하지 않습니다..

5.5 Auto-Negotiation

스위치의 STP 포트에는 내장 된 "자동 협상"포트가 있습니다. 이 기술은 다른 네트워크 장치와의 연결이 설정 될 때 (일반적으로 전원 켜기 또는 재설정시) 최상의 대역폭을 자동으로 설정합니다. 이것은 두 장치의 두 번째 장치가 연결되어 있고 가능한 모드 및 속도를 감지하여 수행됩니다. 10BASE-T 및 100BASE-TX 장치는 모두 Half 또는 Full-Duplex 모드로 포트에 연결할 수 있습니다. 1000BASE-T 는 전이중 모드에서만 연결할 수 있습니다..

부록 A : 용어집

A

ACE

ACE 는 Access Control Entry 의 머리 글자입니다. 특정 ACE ID 와 관련된 액세스 권한을 설명합니다.

세 가지 ACE 프레임 유형 (이더넷 유형, ARP 및 IPv4) 및 두 가지 ACE 작업 (허용 및 거부)이 있습니다. ACE 에는 개별 응용 프로그램에 사용할 수있는 여러 가지 다양한 매개 변수 옵션이 포함되어 있습니다..

ACL

ACL 은 Access Control List (액세스 제어 목록)의 약자입니다. 프로세스 또는 프로그램과 같은 특정 트래픽 목적으로 허용되거나 거부되는 개별 사용자 또는 그룹을 지정하는 액세스 제어 항목을 포함하는 ACE 목록 표입니다.

각각의 액세스 가능한 트래픽 목적은 ACL 에 대한 식별자를 포함합니다. 권한은 특정 트래픽 용도 액세스 권한이 있는지 여부를 결정합니다.
ACL 구현은 ACE 가 다양한 상황에 우선 순위가 매겨지는 경우와 같이 매우 복잡 할 수 있습니다. 네트워킹에서 ACL 은 호스트 나 서버에서 사용할 수있는 서비스 포트 또는 네트워크 서비스 목록을 말하며 각 목록에는 서비스 사용을 허용 또는 거부 한 호스트 또는 서버 목록이 있습니다. ACL 은 일반적으로 인바운드 트래픽을 제어하도록 구성 될 수 있으며이 컨텍스트에서는 방화벽과 유사합니다.

수동 ACL 구성과 관련된 3 개의 웹 페이지가 있습니다.
ACL|Access Control List: 웹 페이지는 ACE 를 가장 높은 우선 순위에서 가장 낮은 우선 순위로 표시합니다. 기본값은 표가 비어 있습니다. 입구 프레임은 ACE 가 더 일치하더라도 하나의 ACE 에서만 히트를 얻습니다. 첫 번째 일치하는 ACE 는 해당 프레임에서 조치 (허가 / 거부)를 취하고 해당 ACE 와 연관된 카운터가 증가합니다. ACE 는 정책, 1 입구 포트 또는 모든 입구 포트 (전체 스위치)와 연관 될 수 있습니다. ACE 정책이 생성되면 해당 정책은 "포트"웹 페이지 아래에있는 포트 그룹과 연관 될 수 있습니다. ACE 로 구성 할 수있는 많은 매개 변수가 있습니다. 웹 페이지 도움말 텍스트를 읽고 각각에 대한 추가 정보를 얻으십시오. ACE 의 최대 수는 64 입니다..
ACL|Ports: ACL 포트 구성은 수신 포트에 정책 ID 를 할당하는 데 사용됩니다. 이는 포트를 그룹화하여 동일한 트래픽 규칙을 따르는 데 유용합니다. 트래픽 정책은 "액세스 제어 목록"- 페이지 아래에 생성됩니다. 각 진입 포트에 대해 특정 트래픽 등록 정보 (작업 / 속도 제한 기 / 포트 복사 등)를 설정할 수도 있습니다. 프레임은 일치하지 않고 일치하는 ACE 를 지나칠 경우에만 적용됩니다. 이 경우 해당 포트와 연관된 카운터가 증가합니다. 특정 포트 등록 정보에 대한 웹 페이지 도움말 텍스트를 참조하십시오.
ACL|Rate Limiters: 이 페이지에서 속도 제한기를 구성 할 수 있습니다. 초당 1-1024K 패킷 범위의 15 가지 속도 제한 기가있을 수 있습니다. "포트"및 "액세스 제어 목록"웹 페이지에서 ACE (들) 또는 수신 포트에 속도 제한 기 ID 를 지정할 수 있습니다.

AES

AES 는 Advanced Encryption Standard 의 머리 글자입니다. 암호화 키 프로토콜은 802.1i 표준에 적용되어 WLAN 보안을 향상시킵니다. DES 및 3DES 를 대체 할 미국 정부의 암호화 표준입니다. AES 는 128 비트의 고정 블록 크기와 128, 192 또는 256 비트의 키 크기를 가지고 있습니다..

AMS

AMS 는 Auto Media Select 의 약자입니다. AMS 는 이중 매체 포트 (구리 (구리) 및 광섬유 (SFP) 케이블을 모두 지원하는 포트)에 사용됩니다 .AMS 는 SFP 또는 CU 케이블이 삽입되어 해당 미디어로 전환되는지 자동으로 결정합니다 .SFP 및 cu 케이블이 모두 삽입 된 경우, 포트가 원하는 미디어를 선택합니다.

APS

APS 는 Automatic Protection Switching 의 약자입니다. 이 프로토콜은 G.8031 에 정의 된대로 보호 그룹의 두 끝에서 양방향으로 스위칭이 수행되도록 보장하는 데 사용됩니다

Aggregation

여러 포트를 병렬로 사용하여 포트의 한계를 초과하는 링크 속도를 높이고 가용성을 높이기 위해 중복을 늘립니다. (Port Aggregation, Link Aggregation).

ARP

ARP 는 Address Resolution Protocol 의 약자입니다. IP 주소를 이더넷 주소와 같은 실제 주소로 변환하는 데 사용되는 프로토콜입니다. ARP 를 사용하면 인접 호스트의 인터넷 주소 만 알면 호스트가 다른 호스트와 통신 할 수 있습니다. IP 를 사용하기 전에 호스트는 원하는 대상 시스템의 인터넷 주소를 포함하는 브로드 캐스트 ARP 요청을 전송합니다.

ARP Inspection

ARP 검사는 보안 기능입니다. ARP 캐시를 "중독 (poisoning)"하여 Layer 2 네트워크에 연결된 호스트 나 장치에 대해 여러 유형의 공격을 시작할 수 있습니다. 이 기능은 이러한 공격을 차단하는 데 사용됩니다. 유효한 ARP 요청 및 응답 만 스위치 장치를 통과 할 수 있습니다.

Auto-Negotiation

자동 협상은 두 개의 서로 다른 장치가 작동 모드와 링크를 위해 해당 장치에서 공유 할 수있는 속도 설정을 설정하는 프로세스입니다.

C

CC

CC 는 연속성 검사 (Continuity Check)의 머리 글자입니다. 피어 MEP 에 CCM 프레임을 전송하여 네트워크의 연속성 손실을 감지 할 수있는 MEP 기능입니다.

CCM

CCM 은 Continuity Check Message 의 머리 글자입니다. 이것은 MEP 에서 피어 MEP 로 전송되어 CC 기능을 구현하는 데 사용되는 OAM 프레임입니다.

CDP

CDP 는 Cisco Discovery Protocol 의 약자입니다.

D

DEI

DEI 는 Drop Eligible Indicator 의 약자입니다. VLAN 태그의 1 비트 필드입니다..

DES

DES 는 Data Encryption Standard 의 약자입니다. 이진 코딩 정보를 암호화 (암호화) 및 해독 (암호 해독)하는 수학 알고리즘에 대한 완전한 설명을 제공합니다.

데이터를 암호화하면 cipher 라고하는 이해할 수없는 형식으로 변환됩니다. 해독 암호는 데이터를 다시 일반 텍스트라고하는 원래 형식으로 변환합니다. 이 표준에서 설명하는 알고리즘은 키라고하는 이진수를 기반으로하는 암호화 및 암호 해독 작업을 지정합니다..

DHCP

DHCP 는 Dynamic Host Configuration Protocol 의 머리 글자 어입니다. 동적 IP 주소를 네트워크의 장치에 할당하는 데 사용되는 프로토콜입니다.

네트워크 컴퓨터 (클라이언트)가 DHCP 서버에서 IP 주소 및 기본 게이트웨이, 서브넷 마스크 및 DNS 서버의 IP 주소와 같은 기타 매개 변수를 얻기 위해 사용하는 DHCP.

DHCP 서버는 모든 IP 주소가 고유한지 확인합니다. 예를 들어 첫 번째 클라이언트의 할당이 유효하고 (임대가 만료되지 않은 경우) IP 주소가 두 번째 클라이언트에 할당되지 않습니다. 따라서 IP 주소 풀 관리는 사람 네트워크 관리자가 아닌 서버에서 수행합니다.

동적 주소 지정은 관리자가 작업을 관리해야하는 대신 소프트웨어가 IP 주소를 추적하기 때문에 네트워크 관리를 단순화합니다. 즉, 고유 한 IP 주소를 수동으로 할당하는 번거 로움없이 새 컴퓨터를 네트워크에 추가 할 수 있습니다..

DHCP Relay

DHCP 릴레이는 동일한 서브넷 도메인에 있지 않을 때 클라이언트와 서버간에 DHCP 메시지를 전달하고 전송하는 데 사용됩니다.

DHCP 옵션 82 는 DHCP 릴레이 에이전트가 클라이언트 DHCP 패킷을 DHCP 서버로 전달할 때 DHCP 요청 패킷에 특정 정보를 삽입하고 서버 DHCP 패킷을 DHCP 클라이언트로 전달할 때 DHCP 응답 패킷에서 특정 정보를 제거 할 수있게합니다. DHCP 서버는이 정보를 사용하여 IP 주소 또는 기타 할당 정책을 구현할 수 있습니다. 특히이 옵션은 회로 ID (옵션 1)와 원격 ID (옵션 2)의 두 가지 하위 옵션을 설정하여 작동합니다. 회로 ID 하위 옵션에는 요청이 들어온 회로에 대한 정보가 포함되어 있습니다. 원격 ID 하위 옵션은 회로의 원격 호스트 끝과 관련된 정보를 전달하도록 설계되었습니다.

스위치의 회선 ID 정의는 길이가 4 바이트이고 형식은 "vlan_id" "module_id" "port_no"입니다. "vlan_id"매개 변수는 VLAN ID 를 나타내는 처음 두 바이트입니다. "module_id"매개 변수는 모듈 ID 의 세 번째 바이트입니다. "port_no"의 매개 변수는 네 번째 바이트이며 포트 번호를 의미합니다.

원격 ID 의 길이는 6 바이트이며 값은 DHCP 릴레이 에이전트 MAC 주소와 동일합니다.

DHCP Snooping

DHCP 스누핑은 DHCP 클라이언트와 서버 간의 합법적 인 대화에 가짜 DHCP 응답 패킷을 삽입하여 간섭을 시도 할 때 스위치 장치의 신뢰할 수없는 포트에서 침입자를 차단하는 데 사용됩니다..

DNS

DNS 는 Domain Name System 의 머리 글자입니다. 다양한 유형의 정보를 도메인 이름과 함께 저장하고 연결합니다. 무엇보다도 DNS 는 인간 친화적 인 도메인 이름과 컴퓨터 호스트 이름을 컴퓨터 친숙한 IP 주소로 변환합니다. 예를 들어 www.example.com 이라는 도메인 이름은 192.168.0.1 로 번역 될 수 있습니다

DoS

DoS 는 DoS (Denial of Service)의 약자입니다. DoS (서비스 거부) 공격에서 공격자는 합법적 인 사용자가 정보 나 서비스에 액세스하지 못하도록 시도합니다. 네트워크 사이트 또는 네트워크 연결을 대상으로 공격자는 네트워크 사용자가 영향을받는 컴퓨터에 의존하는 전자 메일, 웹 사이트, 온라인 계정 (은행 등) 또는 기타 서비스에 액세스하지 못하게 할 수 있습니다.

Dotted Decimal Notation

점 십진수 표기법은 십진수와 점을 구분 기호로 사용하여 IP 주소를 작성하는 방법입니다.
IPv4 점 분리 10 진수 주소의 형식은 x.y.z.w 입니다. 여기서 x, y, z 및 w 는 0 과 255 사이의 십진수입니다

DSCP

DSCP 는 Differentiated Services Code Point 의 약자입니다. 패킷 분류를 위해 IP 패킷의 헤더에있는 필드입니다.

E

EEE

EEE 는 IEEE 802.3az 에 정의 된 Energy Efficient Ethernet 의 약자입니다.

EPS

EPS 는 ITU / T G.8031 에 정의 된 Ethernet Protection Switching 의 약자입니다.

Ethernet Type

Ethernet Type 또는 EtherType 은 이더넷 네트워킹 표준에 의해 정의 된 이더넷 MAC 헤더의 필드입니다. 이 프로토콜은 이더넷 프레임에서 전송되는 프로토콜을 나타내는 데 사용됩니다.

F

FTP

FTP 는 File Transfer Protocol (파일 전송 프로토콜)의 약자입니다. 전송 제어 프로토콜 (TCP)을 사용하고 파일 쓰기 및 읽기를 제공하는 전송 프로토콜입니다. 또한 디렉토리 서비스 및 보안 기능을 제공합니다.

Fast Leave

IGMP 스누핑 고속 대기 처리를 사용하면 스위치가 그룹 관련 쿼리를 먼저 인터페이스에 전송하지 않고도 포워딩 테이블 항목에서 인터페이스를 제거 할 수 있습니다. VLAN 인터페이스는 원래의 탈퇴 메시지에 지정된 멀티 캐스트 그룹의 멀티 캐스트 트리에서 제거됩니다. 빠른 탈퇴 처리는 여러 멀티 캐스트 그룹이 동시에 사용되는 경우에도 스위치 네트워크의 모든 호스트에 대해 최적의 대역폭 관리를 보장합니다.

H

HTTP

HTTP 는 Hypertext Transfer Protocol 의 약자입니다. WWW (World Wide Web)에서 정보를 전송하거나 전달하는 데 사용되는 프로토콜입니다.

HTTP 는 메시지가 형식화되고 전송되는 방법과 다양한 명령에 대한 응답으로 웹 서버와 브라우저가 취해야 할 조치를 정의합니다. 예를 들어 브라우저에 URL 을 입력하면 실제로 웹 서버에 HTTP 명령을 전송하여 요청한 웹 페이지를 가져오고 전송하도록 지시합니다. World Wide Web 의 작동 방식을 제어하는 다른 주요 표준은 HTML 로, Web Pages 의 형식과 표시 방법을 설명합니다.

모든 웹 서버 시스템에는 웹 페이지 파일 외에도 HTTP 데몬을 기다릴 수있는 프로그램이 있습니다. HTTP 데몬은 HTTP 요청을 기다리고 도착한 후 처리하도록 설계된 프로그램입니다. 웹 브라우저는 HTTP 클라이언트이며 서버 시스템에 요청을 보냅니다. HTTP 클라이언트는 원격 호스트 (기본적으로 포트 80)의 특정 포트에 TCP (Transmission Control Protocol) 연결을 설정하여 요청을 시작합니다. 해당 포트에서 수신 대기하는 HTTP 서버는 클라이언트가 요청 메시지를 보낼 때까지 기다립니다.

HTTPS

HTTPS 는 Secure Socket Layer 를 통한 Hypertext Transfer Protocol 의 약자입니다. 보안 HTTP 연결을 나타내는 데 사용됩니다.

HTTPS 는 인증 및 암호화 된 통신을 제공하며 지불 트랜잭션 및 회사 로그온과 같은 보안에 민감한 통신을 위해 World Wide Web 에서 널리 사용됩니다.

HTTPS 는 실제로 정규적인 HTTP 응용 프로그램 계층화에서 Netscape 의 SSL (Secure Socket Layer)을 하위 계층으로 사용하는 것입니다. (HTTPS 는 TCP / IP 와의 상호 작용에서 HTTP 포트 80 대신 포트 443 을 사용합니다.) SSL 은 상용 교환을위한 적절한 수준의 암호화로 간주되는 RC4 스트림 암호화 알고리즘에 40 비트 키 크기를 사용합니다.

I

ICMP

ICMP 는 Internet Control Message Protocol 의 머리 글자 어입니다. 이것은 오류 응답, 진단 또는 라우팅 목적을 생성 한 프로토콜입니다. ICMP 메시지에는 일반적으로 라우팅 문제 또는 타임 스탬프 또는 반향 트랜잭션과 같은 간단한 교환에 대한 정보가 들어 있습니다. 예를 들어, PING 명령은 ICMP 를 사용하여 인터넷 연결을 테스트합니다.

IEEE 802.1X

IEEE 802.1X 는 포트 기반 네트워크 액세스 제어를위한 IEEE 표준입니다. LAN 포트에 연결된 장치에 인증을 제공하고 인증이 실패 할 경우 지점 간 연결을 설정하거나 해당 포트에서 액세스하지 못하도록합니다. 802.1X 를 사용하면 모든 스위치 포트에 대한 액세스를 서버에서 중앙 집중식으로 제어 할 수 있습니다. 즉, 인증 된 사용자는 네트워크 내의 모든 지점에서 인증을 위해 동일한 자격 증명을 사용할 수 있습니다.

IGMP

IGMP 는 Internet Group Management Protocol 의 머리 글자 어입니다. 이것은 인터넷 프로토콜 멀티 캐스트 그룹의 구성원을 관리하는 데 사용되는 통신 프로토콜입니다. IGMP 는 IP 호스트와 인접한 멀티 캐스트 라우터에서 멀티 캐스트 그룹 멤버십을 설정하는 데 사용됩니다. 이것은 유니 캐스트 연결을위한 ICMP 와 같은 IP 멀티 캐스트 사양의 핵심 부분입니다. IGMP 는 온라인 비디오 및 게임에 사용될 수 있으며 이러한 용도를 지원할 때 자원을보다 효율적으로 사용할 수 있습니다.

IGMP Querier

라우터가 IGMP 쿼리 메시지를 특정 링크로 보냅니다. 이 라우터를 Querier 라고합니다.

IMAP

IMAP 은 Internet Message Access Protocol (인터넷 메시지 액세스 프로토콜)의 약자입니다. 전자 메일 클라이언트가 메일 서버에서 전자 메일 메시지를 검색하기위한 프로토콜입니다.

IMAP 은 IMAP 클라이언트가 서버와 통신하는 데 사용하는 프로토콜이며 SMTP 는 IMAP 서버로 메일을 전송하는 데 사용되는 프로토콜입니다.

인터넷 메시지 액세스 프로토콜의 현재 버전은 IMAP4 입니다. POP3 (Post Office Protocol version 3)와 비슷하지만 더 복잡하고 복잡한 기능을 제공합니다. 예를 들어, IMAP4 프로토콜은 전자 메일 메시지를 컴퓨터에 다운로드하지 않고 서버에 남겨 둡니다. 서버에서 메시지를 제거하려면 메일 클라이언트를 사용하여 로컬 폴더를 생성하고 로컬 하드 드라이브에 메시지를 복사 한 다음 서버에서 메시지를 삭제하고 영구 삭제해야합니다..

IP

P 는 인터넷 프로토콜의 약자입니다. 이것은 인터넷 네트워크를 통해 데이터를 통신하는 데 사용되는 프로토콜입니다.

IP 는 "최선형"시스템입니다. 즉, 전송 된 정보의 패킷이 보낸 것과 동일한 조건에서 대상에 도달하지 못합니다. LAN (Local Area Network) 또는 WAN (Wide Area Network)에 연결된 각 장치에는 인터넷 프로토콜 주소가 부여되며이 IP 주소는 확장 네트워크에 연결된 다른 모든 장치 중에서 장치를 고유하게 식별하는 데 사용됩니다.

인터넷 프로토콜의 현재 버전은 32 비트 인터넷 프로토콜 주소를 갖는 IPv4 로 40 억 개의 고유 주소를 허용합니다. 이 숫자는 큰 블록으로 주소를 취하는 웹 마스터의 관행으로 급격히 줄어들며 그 대부분은 사용되지 않고 있습니다. 128 비트 인터넷 프로토콜 주소를 갖는 새로운 버전의 인터넷 프로토콜 (IPv6)을 채택하는 다소 실질적인 움직임이 있습니다. 이 숫자는 대략 39 개의 0 이있는 3 개의 숫자로 대략 표현할 수 있습니다. 그러나 IPv4 는 여전히 인터넷의 대부분의 프로토콜입니다.

IPMC

IPMC 는 IP MultiCast 의 머리 글자입니다.

IP Source Guard

IP 소스 가드는 DHCP 스누핑 표 또는 수동으로 구성된 IP 소스 바인딩을 기반으로 트래픽을 필터링하여 DHCP 스누핑 신뢰할 수없는 포트에서 IP 트래픽을 제한하는 데 사용되는 보안 기능입니다. 호스트가 다른 호스트의 IP 주소를 스푸핑하고 사용할 때 IP 스푸핑 공격을 방지하는 데 도움이됩니다.

L

LACP

LACP 는 IEEE 802.3ad 표준 프로토콜입니다. 링크 집계 제어 프로토콜 (Link Aggregation Control Protocol)은 여러 물리적 포트를 함께 묶어 단일 논리 포트를 형성 할 수있게합니다

LLDP

LLDP 는 IEEE 802.1ab 표준 프로토콜입니다.
이 표준에 명시된 LLDP (Link Layer Discovery Protocol)는 IEEE 802 LAN 에 연결된 스테이션이 동일한 IEEE 802 LAN 에 연결된 다른 스테이션에 해당 스테이션을 통합하는 시스템에서 제공하는 주요 기능, 관리 주소 해당

기능의 관리를 제공하는 엔터티 또는 해당 관리 엔티티가 필요로하는 IEEE 802 LAN 에 대한 스테이션 연결 지점의 식별. 이 프로토콜을 통해 배포 된 정보는 수신자가 표준 MIB (Management Information Base)에 저장하므로 NMS (Network Management System)에서 단순 네트워크 관리 프로토콜 (SNMP)과 같은 관리 프로토콜을 사용하여 정보에 액세스 할 수 있습니다. SNMP).

LLDP-MED

LLDP-MED 는 IEEE 802.1ab 의 확장이며 전기 통신 산업 협회 (TIA-1057)에서 정의합니다.

LOC

LOC 는 Loss Of Connectivity 의 머리 글자이며 MEP 가 감지하고 네트워크의 연결이 끊어 졌음을 나타냅니다. EPS 별로 스위치 기준으로 사용할 수 있습니다.

M

MAC Table

프레임 전환은 프레임에 포함 된 DMAC 주소를 기반으로합니다. 스위치는 MAC 주소를 스위치 포트에 매핑하는 표를 작성하여 프레임이 이동해야하는 포트 (프레임의 DMAC 주소를 기반으로 함)를 알 수 있습니다. 이 표에는 정적 및 동적 항목이 모두 들어 있습니다. 정적 항목은 관리자가 DMAC 주소와 스위치 포트간에 고정 매핑을 원할 경우 네트워크 관리자가 구성합니다. 프레임에는 MAC 주소 (SMAC 주소)가 포함되어있어 프레임을 전송하는 장비의 MAC 주소를 표시합니다. SMAC 주소는 스위치가 자동으로 MAC 표를 이러한 동적 MAC 주소로 업데이트하는 데 사용됩니다. 구성 가능한 에이징 시간 후에 해당 SMAC 주소가있는 프레임이 표시되지 않으면 동적 항목이 MAC 표에서 제거됩니다.

MEP

MEP 는 Maintenance Entity Endpoint 의 약자이며 유지 관리 엔티티 그룹 (ITU-T Y.1731)의 끝점입니다.

MD5

MD5 는 Message-Digest 알고리즘 5 의 머리 글자입니다. MD5 는 128 비트 해시 값이있는 암호화 해시 함수를 사용하는 메시지 다이제스트 알고리즘입니다. 1991 년 Ron Rivest 에 의해 설계되었습니다. MD5 는 RFC 1321 - MD5 Message-Digest Algorithm 에 공식적으로 정의되어 있습니다.

Mirroring

네트워크 문제를 디버깅하거나 네트워크 트래픽을 모니터링하기 위해 스위치 시스템을 여러 포트의 프레임을 미러 포트로 미러링하도록 구성 할 수 있습니다. 이 경우 프레임을 미러링하는 것은 프레임을 복사하는 것과 같습니다. 들어오는 (원본) 프레임과 나가는 (대상) 프레임을 모두 미러 포트로 미러링 할 수 있습니다

MLD

MLD 는 IPv6 에 대한 Multicast Listener Discovery 의 약자입니다. MLD 는 IPv6 라우터에서 IPv4 에 IGMP 가 사용되는 것과 마찬가지로 직접 연결된 링크에서 멀티 캐스트 수신기를 검색하는 데 사용됩니다. 이 프로토콜은 별도의 프로토콜을 사용하는 대신 ICMPv6 에 포함됩니다.

MVR

Multicast VLAN Registration (MVR)은 소스 VLAN 의 멀티 캐스트 트래픽을 가입자 VLAN 과 공유 할 수있게 해주는 레이어 2 (IP) 네트워크 용 프로토콜입니다.
MVR 을 사용하는 주된 이유는, 코어 네트워크에서 전송되는 중복 된 멀티 캐스트 스트림을 방지하여 대역폭을 절약하는 대신 스트림 (들) (위키 백과)에 MVR-VLAN 에 수신 호스트가 /을 요청한 VLAN 에 전달되는 것입니다.

N

NAS

NAS 는 네트워크 액세스 서버 (Network Access Server)의 머리 글자입니다. NAS 는 보호 된 소스에 대한 액세스를 보호하는 게이트웨이 역할을합니다. 클라이언트가 NAS 에 연결하고 NAS 가 클라이언트의 제공된 자격 증명이 유효한 지 묻는 다른 리소스에 연결합니다. 그 답을 바탕으로 NAS 는 보호 된 리소스에 대한 액세스를 허용하거나 허용하지 않습니다. NAS 구현의 예는 IEEE 802.1X 입니다.

NetBIOS

NetBIOS 는 Network Basic Input / Output System 의 머리 글자입니다. 이것은 별도의 컴퓨터에있는 응용 프로그램이 LAN (Local Area Network) 내에서 통신 할 수있게 해주는 프로그램이며 WAN (Wide Area Network)에서 지원되지 않습니다.

네트워크의 각 컴퓨터에 NetBIOS 이름과 다른 호스트 이름에 해당하는 IP 주소를 제공하는 NetBIOS 는 OSI (Open Systems Interconnection) 모델에 설명 된 세션 및 전송 서비스를 제공합니다..

NFS

NFS 는 Network File System 의 약자입니다. 호스트가 원격 시스템에 파티션을 마운트하여 로컬 파일 시스템 인 것처럼 사용할 수 있습니다.

NFS 를 사용하면 시스템 관리자는 네트워크의 중앙 위치에 리소스를 저장할 수 있으므로 승인 된 사용자가 파일에 지속적으로 액세스 할 수 있습니다. NFS 는 파일, 프린터 및 기타 리소스를 컴퓨터 네트워크를 통해 영구 저장 장치로 공유 할 수 있도록 지원합니다

NTP

NTP 는 컴퓨터 시스템의 시계를 동기화하기위한 네트워크 프로토콜 인 Network Time Protocol 의 머리 글자입니다. NTP 는 UDP (데이터 그램)를 전송 계층으로 사용합니다.

O

OAM

OAM 은 운영 관리 및 유지 관리의 머리 글자입니다.(Operation Administration and Maintenance)

캐리어 이더넷 기능을 구현하는 데 사용되는 ITU-T Y.1731 에 설명 된 프로토콜입니다. CC 및 RDI 와 같은 MEP 기능은이 기능을 기반으로합니다.

Optional TLVs.

LLDP 프레임에는 여러 개의 TLV 가 있습니다.
일부 TLV 의 경우, 스위치가 LLDP 프레임에 TLV 를 포함해야하는 경우 구성 가능합니다. 이러한 TLV 는 선택적 TLV 로 알려져 있습니다. 선택적 TLV 가 비활성화 된 경우 해당 정보가 LLDP 프레임에 포함되지 않습니다..

OUI

OUI 는 조직적으로 고유 한 식별자입니다. OUI 주소는 IEEE 가 공급 업체에 할당 한 전 세계적으로 고유 한 식별자입니다. MAC 주소의 처음 24 비트를 구성하는 OUI 주소에 따라 장치가 속한 공급 업체를 결정할 수 있습니다.

P

PCP

PCP 는 Priority Code Point 의 약자입니다. 802.1Q 프레임의 우선 순위 레벨을 저장하는 3 비트 필드입니다. 사용자 우선 순위라고도합니다.

PD

PD 는 Powered Device 의 머리 글자입니다. PoE> 시스템에서 전력은 PSE (전력 소싱 장비)에서 원격 장치로 전달됩니다. 원격 장치를 PD 라고합니다.

PHY

PHY 는 Physical Interface Transceiver 의 약자이며 이더넷 물리적 계층 (IEEE-802.3)을 구현하는 장치입니다.

PING

Ping 은 해당 컴퓨터에서 응답을 생성하기 위해 네트워크 또는 인터넷을 통해 특정 컴퓨터로 패킷을 보내는 프로그램입니다. 다른 컴퓨터는 패킷을 수신했다는 확인 응답을 보냅니다. Ping 은 네트워크 또는 인터넷상의 특정 컴퓨터가 존재하고 연결되어 있는지 확인하기 위해 만들어졌습니다.

ping 은 ICMP (Internet Control Message Protocol) 패킷을 사용합니다. PING 요청은 원본 컴퓨터의 패킷이며 PING 응답은 대상의 패킷 응답입니다.

Policer

Policer 는 수신 된 프레임의 대역폭을 제한 할 수 있습니다. 입구 쪽 큐 앞에 위치합니다.

POP3

POP3 는 Post Office Protocol 버전 3 의 약자입니다. 전자 메일 클라이언트가 메일 서버에서 전자 메일 메시지를 검색하기위한 프로토콜입니다.

POP3 는 사용자가 다운로드 한 즉시 서버에서 메일을 삭제하도록 설계되었습니다. 그러나 일부 구현에서는 사용자 또는 관리자가 일정 기간 동안 메일을 저장하도록 지정할 수 있습니다. POP 는 "저장 후 전달"서비스로 생각할 수 있습니다.

다른 프로토콜은 인터넷 메시지 액세스 프로토콜 (IMAP)입니다. IMAP 은 서버에 전자 메일을 보관하고 서버의 폴더에 전자 메일을 구성 할 수있는 더 많은 기능을 사용자에게 제공합니다. IMAP 은 원격 파일 서버로 생각할 수 있습니다.

POP 및 IMAP 은 전자 메일 수신을 처리하며 SMTP (Simple Mail Transfer Protocol)와 혼동하지 마십시오. SMTP 를 사용하여 전자 메일을 보내면 받는 사람을 대신하여 메일 처리기에서이를받습니다. 그런 다음 POP 또는 IMAP 을 사용하여 메일을 읽습니다. IMAP4 및 POP3 은 전자 메일 검색을 위한 가장 널리 보급 된 두 가지 인터넷 표준 프로토콜입니다. 사실상 모든 최신 전자 메일 클라이언트와 서버는이 두 가지를 모두 지원합니다.

PPPoE

PPPoE 는 이더넷을 통한 지점 간 프로토콜 (Point-to-Point Protocol)의 머리 글자입니다.
이더넷 프레임 내에 PPP (Point-to-Point Protocol) 프레임을 캡슐화하기위한 네트워크 프로토콜입니다. 주로 개별 사용자가 이더넷과 일반 메트로 이더넷 네트워크 (Wikipedia)를 통해 ADSL 트랜시버 (모뎀)에 연결하는 ADSL 서비스에 사용됩니다.

Private VLAN

사설 VLAN 에서 사설 VLAN 의 포트 간 통신은 허용되지 않습니다. VLAN 은 사설 VLAN 으로 구성 될 수 있습니다.

PTP

PTP 는 컴퓨터 시스템의 시계를 동기화하기위한 네트워크 프로토콜 인 Precision Time Protocol 의 약자입니다.

Q

QCE

QCE 는 QoS Control Entry 의 머리 글자입니다. 특정 QCE ID 와 연관된 QoS 클래스를 설명합니다.

QCE 프레임 유형에는 이더넷 유형, VLAN, UDP / TCP 포트, DSCP, TOS 및 태그 우선 순위가 있습니다. 프레임은 개별 애플리케이션에 대해 "낮음", "보통", "보통"및 "높음"의 4 가지 QoS 클래스 중 하나로 분류 할 수 있습니다.

QCL

QCL 은 QoS 제어 목록의 약자입니다. 특정 트래픽 개체의 특정 QoS 클래스로 분류되는 QoS 제어 항목을

포함하는 QCE 의 목록 표입니다.

각각의 액세스 가능한 트래픽 객체는 그 QCL 에 식별자를 포함한다. 특권은 특정 QoS 클래스에 대한 특정 트래픽의 목적을 결정합니다.

QL

QL SyncE 에서 이것은 주어진 클럭 소스의 품질 레벨입니다. 이것은 포트에서 수신 된 클록의 품질을 나타내는 SSM 의 포트에서 수신됩니다.

QoS

QoS 는 Quality of Service 의 약자입니다. 이것은 개별 응용 프로그램이나 프로토콜 간의 대역폭 관계를 보장하는 방법입니다.

통신 네트워크는 고품질 비디오 및 실시간 음성과 같은 지연에 민감한 데이터를 비롯하여 다양한 응용 프로그램 및 데이터를 전송합니다. 네트워크는 안전하고 예측 가능하며 측정 가능하고 때로는 보장되는 서비스를 제공해야합니다.

필요한 QoS 를 달성하는 것이 성공적인 종단 간 비즈니스 솔루션의 비결입니다. 따라서 QoS 는 네트워크 리소스를 관리하는 기술 집합입니다.

QoS class

모든 들어오는 프레임은 해당 특정 QoS 클래스에 대해 구성된 내용에 따라 프레임에 대한 큐잉, 스케줄링 및 혼잡 제어 보장을 제공하기 위해 장치 전체에 사용되는 QoS 클래스로 분류됩니다. QoS 클래스, 대기열 및 우선 순위 사이에는 일대일 매핑이 있습니다. QoS 클래스 0 (영)이 가장 낮은 우선 순위를 갖습니다.

R

RARP

이더넷 주소와 같은 지정된 하드웨어 주소에 대한 IP 주소를 얻는 데 사용되는 프로토콜입니다. RARP 는 ARP 의 보완물입니다.

RADIUS

RADIUS 는 Remote Authentication Dial In User Servic 의 약자입니다. 네트워크 서비스를 연결하고 사용하는 사람이나 컴퓨터를 위한 중앙 집중식 액세스, 권한 부여 및 계정 관리를 제공하는 네트워킹 프로토콜입니다.

RDI

RDI 는 Remote Defect Indication 의 머리 글자입니다. 이것은 원격 피어 MEP 에 감지 된 결함을 나타 내기 위해 MEP 에서 사용하는 OAM 기능입니다

Router Port

라우터 포트는 스위치를 Layer 3 멀티 캐스트 장치쪽으로 연결하는 이더넷 스위치의 포트입니다.

RSTP

1998 년 IEEE 802.1w 문서는 토폴로지가 변경된 후 빠른 스패닝 트리 컨버전스를 제공하는 Rapid Spanning Tree Protocol 인 STP 의 발전을 소개했습니다. 표준 IEEE 802.1D-2004 는 이제 STP 와 역 호환되는 동시에 RSTP 와 STP 를 통합합니다.

S

SAMBA

Samba 는 UNIX 와 유사한 운영 체제에서 실행되는 프로그램으로 UNIX 와 Microsoft Windows 컴퓨터 간의 완벽한 통합을 제공합니다. Samba 는 Microsoft Windows, IBM OS / 2 및 기타 SMB 클라이언트 컴퓨터의 파일 및 인쇄 서버 역할을합니다. Samba 는 SMB (Server Message Block) 프로토콜과 CIFS (Common Internet File System)를 사용합니다.이 프로토콜은 Microsoft Windows 네트워킹에서 사용되는 기본 프로토콜입니다.

Samba 는 Linux, 가장 일반적인 Unix 플랫폼, OpenVMS 및 IBM OS / 2 를 포함한 다양한 운영 체제 플랫폼에 설치할 수 있습니다.

Samba 는 네트워크의 마스터 브라우저에 자신을 등록 할 수 있으므로 Microsoft Windows "Neighborhood Network"의 호스트 목록에 표시됩니다.

SHA

SHA 는 Secure Hash Algorithm 의 머리 글자입니다. 국가 안보국 (NSA)에서 설계하고 NIST 에서 미국 연방 정보 처리 표준 (Federal Information Processing Standard)으로 발행 한 것입니다. 해시 알고리즘은 임의의 길이의 입력 데이터 시퀀스 (메시지)의 고정 길이 디지털 표현 (메시지 요약으로 알려짐)을 계산합니다.

Shaper

셰이퍼는 전송 된 프레임의 대역폭을 제한 할 수 있습니다. 수신 대기열 다음에 위치합니다.

SMTP

SMTP 는 SMTP (Simple Mail Transfer Protocol)의 약자입니다. TCP (Transmission Control Protocol)를 사용하고 FTP 파일 전송 서비스를 모델로하는 메일 서비스를 제공하는 텍스트 기반 프로토콜입니다. SMTP 는 시스템과 수신 메일 관련 알림간에 메일 메시지를 전송합니다.

SNAP

SNAP (SubNetwork Access Protocol)은 IEEE 802.2 LLC 를 사용하는 네트워크에서 8 비트 802.2 서비스 액세스 지점 (SAP) 필드로 구별 할 수있는 것보다 많은 프로토콜을 멀티플렉싱하는 메커니즘입니다. SNAP 은 이더넷 유형 필드 값별로 프로토콜 식별을 지원합니다. 벤더 - 프라이빗 프로토콜 식별자도 지원합니다.

SNMP

SNMP 는 SNMP (Simple Network Management Protocol)의 약자입니다. 이는 네트워크 관리를위한 TCP / IP (Transmission Control Protocol / Internet Protocol) 프로토콜의 일부입니다. SNMP 를 통해 다양한 네트워크 개체가

네트워크 관리 아키텍처에 참여할 수 있습니다. 이를 통해 네트워크 관리 시스템은 SNMP 를 구현하는 네트워크 장치에서 트랩이나 변경 사항 알림을 수신하여 네트워크 문제를 학습 할 수 있습니다.

SNTP

SNTP 는 컴퓨터 시스템의 시계를 동기화하기위한 네트워크 프로토콜 인 Simple Network Time Protocol 의 머리 글자입니다. SNTP 는 UDP (데이터 그램)를 전송 계층으로 사용합니다..

SPROUT

라우팅 기술을 사용한 스택 프로토콜. 마스터 스위치의 선거뿐 아니라 스택 내의 토폴로지 변경을 거의 즉각적으로 검색하는 고급 프로토콜. 또한 SPROUT 은 스택 내에서 최단 경로 전달을 수행하도록 각 스위치를 설정하기위한 매개 변수를 계산합니다..

SSID

Service Set Identifier 는 사용자가 부착하려는 특정 802.11 무선 LAN 을 식별하는 데 사용되는 이름입니다. 클라이언트 장치는 해당 SSID 를 알리는 범위 내의 모든 액세스 지점에서 브로드 캐스트 메시지를 수신하고 사전 구성을 기반으로 연결하거나 SSID 목록을 표시하고 사용자에게 하나 (위키피디아)를 선택하도록 요청하여 연결할 수 있습니다.

SSH

SSH 는 Secure SHell 의 머리 글자입니다. 두 개의 네트워크 장치간에 보안 채널을 사용하여 데이터를 교환 할 수있는 네트워크 프로토콜입니다. SSH 에서 사용되는 암호화는 안전하지 않은 네트워크에서 데이터의 기밀성과 무결성을 제공합니다. SSH 의 목표는 이전의 rlogin 인 TELNET 및 rsh 프로토콜을 대체하는 것이 었습니다.이 프로토콜은 강력한 인증이나 기밀성을 보장하지 않습니다 (Wikipedia).

SSM

SSM SyncE 에서 이것은 Synchronization Status Message 의 약자이며 QL 표시를 포함합니다.

STP

스패닝 트리 프로토콜은 모든 브리지 된 LAN 에 루프없는 토폴로지를 보장하는 OSI 계층 -2 프로토콜입니다. 원래 STP 프로토콜은 이제 RSTP 에 의해 폐기되었습니다.

SyncE

SyncE Synchronous Ethernet 의 약자입니다. 이 기능은 네트워크 '클럭 주파수'를 동기화하는 데 사용됩니다. 실시간 클록 동기화 (IEEE 1588)와 혼동하지 마십시오.

T

TACACS+

TACACS +는 터미널 액세스 컨트롤러 액세스 제어 시스템 플러스의 약자입니다. 하나 이상의 중앙 집중식 서버를 통해 라우터, 네트워크 액세스 서버 및 기타 네트워크 컴퓨팅 장치에 대한 액세스 제어를 제공하는 네트워킹 프로토콜입니다. TACACS +는 별도의 인증, 권한 부여 및 회계 서비스를 제공합니다.

Tag Priority

Tag Priority 는 802.1Q 프레임의 우선 순위 레벨을 저장하는 3 비트 필드입니다..

TCP

TCP 는 Transmission Control Protocol 의 약어입니다. IP (인터넷 프로토콜)를 사용하여 컴퓨터간에 메시지를 교환하는 통신 프로토콜입니다.

TCP 프로토콜은 송신자에서 수신자로의 안정적이고 순차적 인 데이터 전달을 보장하며 동일한 호스트에서 실행되는 동시 응용 프로그램 (예 : 웹 서버 및 전자 메일 서버)에 의한 여러 연결의 데이터를 구별합니다.

네트워크 호스트의 응용 프로그램은 TCP 를 사용하여 서로 연결을 만들 수 있습니다. 이는 연결 지향 프로토콜로 알려져 있습니다. 즉, 각 끝에있는 응용 프로그램이 교환 할 메시지가 교환 될 때까지 연결이 설정되고 유지된다는 것을 의미합니다. TCP 는 메시지가 IP 가 관리하는 패킷으로 분할되고 패킷을 다른 끝에 완전한 메시지로 다시 어셈블하도록 보장합니다.

TCP 를 사용하는 일반적인 네트워크 응용 프로그램에는 World Wide Web (WWW), 전자 메일 및 파일 전송 프로토콜 (FTP)이 있습니다.

TELNET

TELNET 은 TELetype NETwork 의 머리 글자입니다. TCP (Transmission Control Protocol)를 사용하고 TELNET 서버와 TELNET 클라이언트 사이에 가상 연결을 제공하는 터미널 에뮬레이션 프로토콜입니다.

TELNET 은 클라이언트가 서버를 제어하고 네트워크의 다른 서버와 통신 할 수있게합니다. 텔넷 세션을 시작하려면 클라이언트 사용자는 유효한 사용자 이름과 암호를 입력하여 서버에 로그인해야합니다. 그런 다음 클라이언트 사용자는 텔넷 프로그램을 통해 서버 콘솔에 직접 명령을 입력하는 것처럼 명령을 입력 할 수 있습니다..

TFTP

TFTP 는 Trivial File Transfer Protocol 의 머리 글자입니다. UDP (User Datagram Protocol)를 사용하고 파일 쓰기 및 읽기를 제공하는 전송 프로토콜이지만 디렉토리 서비스 및 보안 기능은 제공하지 않습니다.

ToS

ToS 는 Type of Service 의 약자입니다. IPv4 ToS 우선 순위 제어로 구현됩니다. IP 헤더의 6 비트 ToS 필드에서 우선 순위를 결정하기 위해 완전히 디코딩됩니다. ToS 필드의 최상위 6 비트는 64 개의 가능성으로 완전히 디코딩되며 그 결과 인 특이 코드는 IPv4 ToS 우선 순위 제어 비트 (0 ~ 63)의 해당 비트와 비교됩니다.

TLV

TLV 는 유형 길이 값의 머리 글자입니다. LLDP 프레임은 여러 정보를 포함 할 수 있습니다. 이러한 각 정보는 TLV 로 알려져 있습니다..

TKIP

TKIP 는 임시 키 무결성 프로토콜 (Temporal Key Integrity Protocol)의 머리 글자입니다. WPA 에서 WEP 를 새로운

암호화 알고리즘으로 대체하는 데 사용되었습니다. TKIP 는 WEP 에 대해 정의 된 동일한 암호화 엔진과 RC4 알고리즘으로 구성됩니다. TKIP 의 암호화에 사용되는 키는 128 비트이며 각 패킷에 사용되는 키를 변경합니다.

U

UDP

UDP 는 User Datagram Protocol (사용자 데이터 그램 프로토콜)의 머리 글자 어입니다. IP (인터넷 프로토콜)를 사용하여 컴퓨터간에 메시지를 교환하는 통신 프로토콜입니다.

UDP는 인터넷 프로토콜 (IP)을 사용하는 TCP (전송 제어 프로토콜) 대신 사용할 수 있습니다. TCP와 달리 UDP는 메시지를 패킷 데이터 그램으로 나누는 서비스를 제공하지 않으며 UDP 는 패킷을 다시 어셈블 및 시퀀싱하지 않습니다. 즉, UDP 를 사용하는 응용 프로그램은 전체 메시지가 도착했는지, 올바른 순서인지 확인 할 수 있어야합니다. 교환 할 데이터 단위가 매우 작기 때문에 처리 시간을 절약하려는 네트워크 응용 프로그램은 UDP 를 TCP 보다 선호 할 수 있습니다.

UDP 는 IP 계층에서 제공하지 않는 두 가지 서비스를 제공합니다. 이 도구는 포트 번호를 제공하여 여러 사용자 요청을 구별하고 선택적으로 체크섬 기능을 사용하여 데이터가 손상되지 않았는지 확인합니다.

UDP 를 사용하는 일반적인 네트워크 응용 프로그램에는 DNS (Domain Name System), IPTV, VoIP (Voice over IP) 및 TFTP (Trivial File Transfer Protocol)와 같은 스트리밍 미디어 응용 프로그램이 포함됩니다.

UPnP

UPnP 는 Universal Plug and Play 의 약자입니다. UPnP 의 목표는 장치를 원활하게 연결하고 가정에서의 네트워크 구현 (데이터 공유, 통신 및 엔터테인먼트)을 단순화하고 기업 환경에서 컴퓨터 구성 요소 설치를 단순화하는 것입니다

User Priority

User Priority 는 802.1Q 프레임의 우선 순위 레벨을 저장하는 3 비트 필드입니다.

V

VLAN

가상 LAN. 스위치 포트 간의 통신을 제한하는 방법. VLAN 은 다음 애플리케이션에 사용될 수 있습니다:

VLAN 미인식 스위칭: 이것은 기본 구성입니다. 모든 포트는 포트 VLAN ID 1 및 VLAN 1 구성원과 VLAN 을 인식하지 못합니다. 즉, VLAN 1 에서 MAC 주소를 인식하고 스위치는 VLAN 태그를 제거하거나 삽입하지 않습니다.

VLAN 인식 스위칭: IEEE 802.1Q 표준을 기반으로합니다. 모든 포트는 VLAN 을 인식합니다. VLAN 인식 스위치에 연결된 포트는 여러 VLAN 의 멤버이며 태그가 지정된 프레임을 전송합니다. 다른 포트는 하나의 VLAN 의 구성원이며이 포트 VLAN ID 로 설정되며 태그없는 프레임을 전송합니다.

발송자 스위칭 : Q-in-Q 전환이라고도합니다. 가입자에게 연결된 포트는 VLAN 을 인식하지 못하고 하나의 VLAN 멤버이며이 고유 한 포트 VLAN ID 로 설정됩니다. 서비스 공급자에 연결된 포트는 VLAN 을 인식하고 여러 VLAN 의 구성원이며 모든 프레임을 태그 지정하도록 설정됩니다. 구독자 포트에서 수신 된 태그가없는 프레임은 단일 VLAN 태그를 사용하여 발송자 포트로 전달됩니다. 발송자 포트에서 수신 된 태그가 지정된 프레임은 이중 VLAN 태그가있는 발송자 포트로 전달됩니다.

VLAN ID

VLAN ID 는 프레임이 속하는 VLAN 을 지정하는 12 비트 필드입니다.

Voice VLAN

음성 VLAN 은 음성 트래픽을 위해 특별히 구성된 VLAN 입니다. 음성 VLAN 에 음성 장치가 연결된 포트를 추가함으로써 음성 데이터에 대한 QoS 관련 구성을 수행하여 음성 트래픽 및 음성 품질의 전송 우선 순위를 보장 할 수 있습니다.

W

WEP

WEP 은 **W**ired **E**quivalent **P**rivacy 의 약자입니다. WEP 는 IEEE 802.11 무선 네트워크를 보호하기 위해 사용되지 않는 알고리즘입니다. 무선 네트워크는 라디오를 사용하여 메시지를 브로드 캐스트하므로 유선 네트워크보다 도청에 더 취약합니다. 1999 년에 소개되었을 때 WEP 는 전통적인 유선 네트워크 (Wikipedia)와 비교할 수있는 기밀성을 제공하기위한 것이 었습니다.

WiFi

WiFi 는 Wireless Fidelity 의 약자입니다
802.11b, 802.11a, 듀얼 밴드 등 모든 유형의 802.11 네트워크를 언급 할 때 일반적으로 사용하기위한 것입니다.이 용어는 Wi-Fi Alliance 에서 발표 한 것입니다..

WPA

WPA 는 Wi-Fi Protected Access 의 약자입니다. 이는 이전 시스템 인 Wired Equivalent Privacy (WEP)에서 발견 된 몇 가지 심각한 약점에 대한 응답으로 작성되었습니다. WPA 는 대부분의 IEEE 802.11i 표준을 구현했으며 802.11i 가 준비되는 동안 WEP 대신 사용할 수있는 중간 측정 수단으로 사용되었습니다. WPA 는 특히 펌웨어 업그레이드를 통해 사전 WPA 무선 네트워크 인터페이스 카드와 함께 작동하도록 설계되었지만 1 세대 무선 액세스 지점과 반드시 일치하지는 않습니다. WPA2 는 전체 표준을 구현하지만 이전 네트워크 카드 (Wikipedia)에서는 작동하지 않습니다..

WPA-PSK

WPA-PSK 는 Wi-Fi Protected Access - Pre Shared Key 의 약자입니다. WPA 는 무선 네트워크의 보안을 강화하도록 설계되었습니다. WPA 에는 기업용 및 개인용의 두 가지 맛이 있습니다. 엔터프라이즈는 각 사용자에게 서로 다른 키를 배포하는 IEEE 802.1X 인증 서버와 함께 사용하기위한 것입니다. 개인 WPA 는 확장 성이 낮은 'PSK (pre-shared key)'모드를 사용하며 허용 된 모든 컴퓨터에 동일한 암호문이 제공됩니다. PSK 모드에서 보안은 암호 구문의 강도와 기밀성에 따라 다릅니다. WPA 의 디자인은 IEEE 802.11i 표준 (Wikipedia)의 초안 3 을 기반으로합니다.

WPA-Radius

WPA-Radius 는 Wi-Fi Protected Access - Radius (802.1X 인증 서버)의 머리 글자입니다. WPA 는 무선 네트워크의 보안을 강화하도록 설계되었습니다. WPA 에는 기업용 및 개인용의 두 가지 맛이 있습니다. 엔터프라이즈는 각 사용자에게 서로 다른 키를 배포하는 IEEE 802.1X 인증 서버와 함께 사용하기위한 것입니다. 개인 WPA 는 확장성이 낮은 'PSK (pre-shared key)'모드를 사용하며 허용 된 모든 컴퓨터에 동일한 암호문이 제공됩니다. PSK 모드에서 보안은 암호 구문의 강도와 기밀성에 따라 다릅니다. WPA 의 디자인은 IEEE 802.11i 표준 (Wikipedia)의 초안 3 을 기반으로 합니다.

WPS

WPS 는 Wi-Fi Protected Setup 의 약자입니다. 무선 홈 네트워크를 쉽고 안전하게 구축하기위한 표준입니다. WPS 프로토콜의 목표는 모든 가정용 장치를 무선 네트워크 (Wikipedia)에 연결하는 프로세스를 단순화하는 것입니다.

WRED

WRED 은 **W**eighted **R**andom **E**arly **D**etection 의 약자입니다. 트래픽이 대기열 내에 쌓일 때 우선 순위가 높은 프레임을 우대 적으로 처리하는 능동적 인 대기열 관리 메커니즘입니다. 프레임의 DP 레벨은 WRED 의 입력으로 사용됩니다. 프레임에 할당 된 DP 레벨이 높으면 정체 시간 동안 프레임이 드롭 될 확률이 높아집니다.

WTR

WTR 은 **W**ait **T**o **R**estore 의 약자입니다.. 이것은 자원에 대한 실패가 이전에 실패한 자원으로의 복원이 완료되기 전에 '활성 상태가 아니어야'하는 시간입니다.