사용자 매뉴얼

SOLTECH
Solution of optical & Network

24포트 10/100/1000Mbps + SFP 4 슬롯 기가비트 스위치

▸ SFC4000T

www.soltech.co.kr

목차

소개

The SOLTECH 의 2 계층 Managed Gigabit 스위치 시리즈인 WSGW(Wep 서버 Gateway) 스위치는 모든 멀티 Port 에 기가비트 이더넷 스위치와 2 계층 기능을 가진 SPF 광섬유 연결 기능과 완벽한 2 층계층 기능을 갖춘다.; 다음과 같이 설명 할 수 있다.

SFC4000T : 24-Port 10/100/1000Base-T 와 4 개의 공유 SFP Managed Gigabit 스위치

SFC4000T-DC: 24-Port 10/100/1000Base-T 와 4 개의 공유 SFP Managed Gigabit 스위치 / 중복 전원

" Managed Switch "라는 용어의 의미는 user 메뉴얼 i.e. SFC4000T / SFC4000T-DC.에 언급된 스위치를 의미합니다.

가. 박스 내용물

Managed switch 상자를 열고 주의하여 포장을 풀어야합니다. 다음과 같은 내용물이 박스에 있으니 확인해야합니다.

- ☑ Managed Switch x1
- ☑ user의 매뉴얼 CD x1
- ☑ 빠른 설치 안내책자 x1
- ☑ 스위치 렉 고정 도구 x1
- ☑ 전원 코드 x1
- ☑ 고무제받침용 발 X4
- ☑ RS-232 DB9 Male 콘솔 케이블 x1
- ☑ SFP 더스트 캡 X8

나. 제품 설명

SMB 를위한 효율적인 비용의 IPv6 기가비트 관리형스위치 솔루션

요즘, 많은 전자 제품이나 모바일 장치가 인터넷을 검색 할 수 있으므로 IP 주소가 필요하다는 것을 의미합니다. 그러나 현재 IPv4 네트워크 인프라는 각 단일 user / 클라이언트에 IP 주소를 제공 할만큼 충분한 기능이 없습니다. 이러한 상황 때문에 ISP 는 IPv6 (인터넷 프로토콜 버전 6) 네트워크 인프라를 신속하게 구축해야합니다. 이러한 요구를 충족시키기 위해 솔텍은 IPv6 관리 기가비트 이더넷 스위치 인 SFC4000 시리즈 매니지드 스위치를 출시합니다. IPv4 및 IPv6 관리 기능을 모두 지원합니다. 그것은 원래의 네트워크 구조 (IPv4)와 함께 작동 할 수 있으며 새로운 네트워크 구조 (IPv6)를 미래에도 지원할 수 있습니다. 쉽고 친숙한 관리 인터페이스와 다양한 관리 기능이 포함 된 SFC4000 시리즈 관리 스위치는 ISP 가 IPv6 FTTx 에지 서비스를 구축하고 SMB 를 IPv6 네트워크와 연결하는 최상의 선택입니다.

고성능/ 효과적인 비용/ 기업 데이터 센터나 백본을 위한 기가비트 솔루션 네트워킹

SOLTECH Managed 스위치는 L2 / L4 Managed Gigabit 스위치입니다. 기가비트 네트워크 인터페이스는 48Gbps 스위칭 구조를 갖춘 엔터프라이즈 및 서버의 기본 장비 및 요구 사항이 되었기 때문에, 관리형 스위치는 백본 또는 대용량

서버에 연결된 안전한 토폴로지에서 대용량 데이터를 처리 할 수 있습니다. 강력한 QoS 및 네트워크 보안 기능은 캠퍼스와 엔터프라이즈 모두에서 VoIP, 비디오 스트리밍 및 멀티 캐스트 애플리케이션과 같은 효과적인 데이터 트래픽 제어의 요구를 충족시킵니다.

고성능 기능

관리 형 스위치는 24 개의 10 / 100 / 1000Mbps 기가비트 이더넷 Port 와 4 개의 공유 기가비트 SFP 슬롯을 제공합니다. 스위치 양식에 높은 성능을 자랑하는데 블로킹이 되지 않는 스위치 구조와 와이어 속도를 통한 보다 높은 48Gbps,를 자랑하며 대역폭 증가되는 일에 편리하고 단순한 업그레이드를 하도록 LAN 에 제공한다

안전한 2 계층 기능

관리 형 스위치는 Port 속도 구성 , Port 집합, VLAN, 스패닝 트리 프로토콜, QoS, 대역폭 제어 및 IGMP 스누핑과 같은 기본 스위치 관리 기능을 프로그래밍 할 수 있습니다. 관리 형 스위치는 802.1Q 태그 VLAN, Q-in-Q VLAN, STP 및 Private VLAN 을 제공하므로 관리 형 스위치에서 허용되는 VLAN 그룹은 최대 255 개까지 가능합니다. 관리 형 스위치는 Port 집계를 통해, 트렁킹을 위해 최대 8 개 그룹의 최대 8 개 그룹을 결합한 고속 트렁크이며 장애 극복을 지원한다.

우수한 트래픽 제어

관리 대상에는 강력한 트래픽 관리 및 QoS 기능이 탑재되어 통신 업체가 제공하는 서비스를 향상시킵니다. 이 기능에는 유선 속도의 Layer 4 트래픽 분류기 및 대역폭 제한과 같은 QoS 기능이 포함되어있어 멀티 태넌트, 멀티 비즈니스 유닛, 전기 연결 전송네트워크 서비스 제공 및 여러 프로그램 특히 유용합니다. 또한 기업이 제한된 네트워크 리소스를 최대한 활용하고 VoIP 및 화상 회의 전송시 최고의 성능을 보장 할 수 있습니다..

효율적인 관리

효율적인 과리를 위해 일련의 관리스위치에는 콘솔과 web 및 snmp 관리 인터페이스가 장착되어 있다. 내장된 웹기반 관리를 통해 사용하기 쉽고 독립적인 플랫폼 관리 및 구성 기능을 제공하고 관리형 스위치는 표준 snmp 를 지원하며 표준기반ㅌ관리 소프트웨어를 통해 관리가 가능하다. 글자 기반 관리의 경우 텔넷 및 콘솔 Port 를 통해 접근이 가능하다.

강화된 보안

관리 형 스위치는 보안을 강화하기위한 다기능 (Access Control List)을 제공합니다. 기계보안 또한 Port 기반 802.1x 및 MAC 기반 user 및 장치 인증도 포함합니다. Port 보안은 클라이언트 수를 제한하는 데 효과적이므로 네트워크 관리자는 이전보다 훨씬 적은 시간과 노력으로 높은수준의 보안된 회사 네트워크를 구축 할수 있습니다 .

유연성과 확장 솔루션

4 개의 mini-GBIC 슬롯은 1000Base-SX / LX 및 WDM SFP (Small Factor Pluggable) 광섬유 모듈과 호환됩니다. 거리는 550 미터 (멀티 방식 섬유) 최대 10/20/30/40/50/70/120 킬로미터 (단일 방식 섬유 또는 WDM 섬유)까지 확장 할 수 있습니다. 기업 데이터 센터 및 배포판 내에서 사용하기에 적합합니다.

연속적인 작동을 약속하는 AC/DC 전원 이중화기능

SFC4000T-DC Managed 스위치는 표준 패키지에 하나의 100 ~ 240V AC 전원 공급 장치와 하나의 DC-48V 전원 공급 장치를 갖추고있어 중복 전원 공급 장치를 제공합니다. 이중 전원 시스템은 또한 100 ~ 240V AC 전원 공급 장치 또는 DC -48V 전원 공급 장치로 신뢰성을 높이기 위해 제공됩니다. 연속 전원 시스템은 가능한 높은 전력 무결성이 요구되는 첨단 시설의 요구 사항을 처리하도록 특별히 설계되었습니다.

다. 메뉴얼 사용법

user 매뉴얼은 다음과같이 구성 되어 있습니다.

Section 2, 설치

이 단계는 관리형 스위치의 물리적인 설치법과 스위치의 기능을 설명하고 있다.

Section 3, 스위치 관리

이 단계는 관리형 스위치의 소프트웨어적인 기능을 포함하여 설명하고 있다.

Section 4, WEB 구성

이 단계는 웹 인터페이스의 관리형 스위치를 사용하는 방법을 설명하고 있다.

Section 5, 인터페이스 명령어 라인

이 단계는 인터페이스 라인 명령어가 어떻게 사용되는지 설명하고 있다.

Section 6, CLI 구성

이 단계는 명령어 라인 인터페이스에 관리형 스위치를 어떻게 사용하는지 설명하고 있다.

Section 7, 스위치 조작

이 단계는 스위치 조작하는 방법에 대해 설명한다.

Section 8, 문제해결

이 단계는 관리형 스위치의 문제해결 방안을 설명한다.

부록 A

이 단계는 관리형 스위치의 케이블 정보를 포함한다.

라. 제품 특징

- 물리적인 Port
  - 24-Port 10/100/1000Base-T RJ-45 구리소재
  - 4 100/1000Base-X mini-GBIC/SFP slots , Port-21 에서 Port-24 까지 공유
  - 기본 설정과 설치를 위한 RS-232 DB9 콘솔 인터페이스

- 2 계층 의 특징

반사 압력 (반이중) 및 IEEE 802.3x PAUSE 프레임 흐름 제어 (전이중) 패킷 손실을 방지합니다.

(Store-and-Forward) 구성 도와 런트/CRC 필터링의 높은성능으로 잘못된 패킷을 삭제하여 네트워크 대역폭을 최적화한다.

Storm Control 기능 지원

- Broadcast / Unicast

VLAN 지원기능

- IEEE 802.1Q 태그 VLAN

최대 4,095 개의 VLAN ID 중에서 최대 256 개의 VLAN 그룹을을 맺을수 있다.

- 제공자로부터 브릿징 (VLAN Q-in-Q) 지원 (IEEE 802.1ad)
- Private VLAN 에지 (PVE)
- 프로토콜 기반 VLAN
- MAC 기반 VLAN
- Voice VLAN

스패닝 트리 프로토콜 지원

- STP, IEEE 802.1d 스패닝 트리 프로토콜
- RSTP, IEEE 802.1w 고속 스패닝 트리 프로토콜
- MSTP, IEEE 802.1s 다중 스패닝 트리 프로토콜, VLAN 별 스패닝 트리
- BPDU Guard

링크 집계 지원

- 802.3ad LACP (링크 집계 제어 프로토콜)
- Cisco 이더넷 채널 (정적 트렁크)
- 최대 14 개의 트렁크 그룹, 트렁크 그룹당 최대 8 개의 Port
- 최대 16Gbps 대역폭 (이중 방식)

Port 미러 제공 (many-to-1)

Port 미러링을 사용하여 특정 Port 에서 들어오는 트래픽이나 나가는 트래픽을 모니터링합니다.

브로드케스트 루프로부터 피해서 루프를 보호한다.

➢ Quality of Service

모든 스위치 Port 에서 8 개의 우선 순위 대기열

트래픽 분류 :

- IEEE 802.1p CoS
- IP TOS / DSCP / IP 우선 순위
- IP TCP / UDP Port 번호
- 일반적인 네트워크 응용 프로그램

엄격한 우선 순위 및 WRR (Weighted Round Robin) CoS 정책

스위치 Port 의 트래픽 폴리싱 정책

DSCP 리마킹

멀티 캐스트

Supports IGMP 스누핑 v1, v2 및 v3

Supports MLD 스누핑 v1 및 v2

Querier 방식 지원

IGMP 스누핑 Port 필터링

MLD 스누핑 Port 필터링

MVR (멀티 캐스트 VLAN 등록)

보안

IEEE 802.1x Port 기반 / MAC 기반 네트워크 접근 인증

RADIUS 서버와 협력 할 수있는 RADIUS 클라이언트 구축

TACACS + 로그인 user 액세스 인증

RADIUS / TACACS + user 인증

IP 기반 액세스 제어 목록 (ACL)

MAC 기반 접근 목록

발신지 MAC / IP 주소 바인딩

신뢰할 수없는 DHCP 메시지를 필터링하는 DHCP 스누핑

동적 ARP 검사는 MAC 주소가 유효하지 않은 ARP 패킷을 IP 주소 바인딩으로 삭제합니다

IP 소스 가드는 IP 스푸핑 공격을 방지합니다.

무단 침입자를 막기위한 IP 주소 접근 관리

관리

인터페이스 관리

- Console / Telnet 명령 라인 인터페이스
- Web switch 관리
- SNMP v1, v2c 및 v3 스위치 관리
- SSH / SSL 보안 접근

네 개의 RMON 그룹 (이력, 통계, 경보 및 이벤트)

IPv6 IP 주소 / NTP / DNS 관리

TFTP (Trivial File Transfer Protocol) 클라이언트 내장

IP 주소 할당을위한 BOOTP 및 DHCP

HTTP / TFTP 를 통한 펌웨어 업로드 / 다운로드

DHCP 릴레이

DHCP Option82

user 특권 수준

NTP (네트워크 시간 프로토콜)

LLDP (Link Layer Discovery Protocol) 프로토콜

케이블 진단 기술은 잠재적 케이블 링 문제를 탐지하고 재발견하는 메커니즘을 제공합니다

시스템 재부팅을위한 리셋 버튼 또는 공장 기본값으로 리셋

배포 관리를위한 SOLTECH Smart Discovery Utility

예비 전원 시스템 (SFC4000T-DC 전용)

■ 100 ~ 240V AC / 48V DC 이중 전원 이중화

■ 활성 - 활성 중복 전원 오류 보호

■ 단일 전원 공급 장치에 치명적인 전원 장애 복구

■ 내결함성 및 복원력.

라 제품 설명서

제품	SFC4000T / SFC4000T-DC
하드웨어 설명	
하드웨어 버전	Version 2
구리 Port	24 10/ 100/1000Base-T RJ-45 Auto-MDI/MDI-X Port
SFP/mini-GBIC Slots	4 100/1000Base-X SFP interfaces, shared with Port-21 에서 Port-24 Compatible with 100Base-FX SFP
콘솔	1 x RS-232 DB9 serial Port (115200, 8, N, 1)
스위치 구성 도	Store-and-Forward
스위치 구조	48Gbps / non-blocking
처리량	35.7Mpps@64Bytes
주소 테이블	16K entries, automatic source 주소 learning and ageing
공유 데이터 버퍼	4Mbits
흐름 통제	IEEE 802.3x Pause Frame for Full-Duplex Back pressure for Half-Duplex
점보 프레임	9Kbytes
초기화 버튼	< 5 sec: 시스템 리부팅 > 5 sec: 공장 초기화
규모 (W x D x H)	440 x 200 x 44.5 mm, 1U high
무게	2740g
LED	Power, , 1000 Link/Act and 10/100 Link/Act for per Gigabit Port, 1000 Speed and Link/Act for per fiber Port
전원 요구사항	100~240V AC, 50/60Hz -48V DC @ 0.6A, Range: -36 ~ -60V (SFC4000T-DC Only)
전원 소비	Max 21.0 watts / 71.652BTU
ESD 보호	6KV DC
Layer 2 기능	
Basic 관리 Interfaces	Console, Telnet, Web Browser, SNMP v1, v2c
Secure 관리 Interfaces	SSH, SSL, SNMP v3
Port 구성	Port disable / enable Auto-Negotiation 10/100/1000Mbps full and half duplex 방식 selection Flow 통제 disable / enable
Port 상태	Display each Port's speed duplex mode, link 상태, Flow 통제 상태, Auto negotiation 상태, trunk 상태
Port Mirroring	TX / RX / Both Many-to-1 monitor
VLAN	802.1Q Tagged Based VLAN, up to 256 VLAN groups

	Q-in-Q tunneling Private VLAN Edge (PVE) MAC 기반 VLAN Protocol 기반 VLAN Voice VLAN MVR (Multicast VLAN Registration) Up to 255 VLAN Groups, out of 4094 VLAN IDs
Link Aggregation	IEEE 802.3ad LACP / Static Trunk Support 12 ,그룹 16-Port trunk 지원
QoS	Traffic classification based, Strict priority and WRR 8-Level priority for 스위치 ing - 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 방식 support
MLD Snooping	MLD (v1/v2) Snooping, up to 255 multicast Groups MLD Querier 방식 support
접근 통제 리스트	IP 기반 ACL / MAC 기반 ACL Up to 256 entries
SNMP MIBs	RFC-1213 MIB-II IF-MIB RFC-1493 Bridge MIB RFC-1643 Ethernet MIB RFC-2863 Interface MIB RFC-2665 Ether-Like MIB RFC-2819 RMON MIB (그룹 1, 2, 3 and 9) RFC-2737 Entity MIB RFC-2618 RADIUS Client MIB RFC-2933 IGMP-STD-MIB RFC-3411 SNMP-Frameworks-MIB IEEE 802.1X PAE LLDP MAU-MIB
일반 규격	
규정 준수	FCC Part 15 Class A, CE
일반 준수	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 통제 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 인증 네트워크 통제 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
환경요소	
Operating	Temperature: 0 ~ 50 Degree C Relative Humidity: 20 ~ 95% (non-condensing)
Storage	Temperature: -20 ~ 70 Degree C Relative Humidity: 20 ~ 95% (non-condensing)

1. 설치

이 절에서는 데스크탑 또는 랙 마운트에있는 관리형 스위치 하드웨어 기능 및 설치에 대해 설명합니다. 관리형 스위치를 쉽게 관리 하고 제어하려면 디스플레이 표시기 및 Port 를 숙지하십시오. 이 장의 전면 패널 그림은 장치 LED 표시등을 표시합니다. 네트워크 장치를 관리형 스위치에 연결하기 전에 이 챕터를 완전히 읽으십시오.

1.1 하드웨어 설치

1.1.1 스위치 전면 판낼

유닛 전면 패널은 스위치의 단순 인터페이스 모니터링을 제공합니다. 스위치. 그림 2-1 & 그림 2-2 그림은 관리형 스위에 전면을 보여준다.

SFC4000T Front Panel

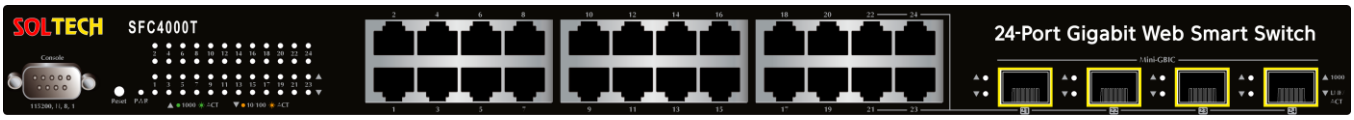


그림 2-1 SFC4000T 전면 패널

SFC4000T-DC Front Panel

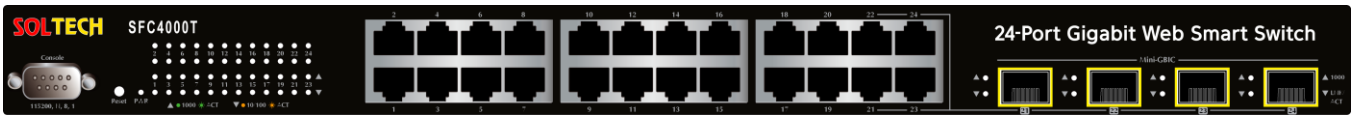


그림 2-2 SFC4000T-DC 전면 패널

■ Gigabit TP interface

10/100/1000Base-T Copper, RJ-45 Twist-Pair: Up to 100 meters.

■ SFP slots

100/1000Base-X mini-GBIC slot, SFP (Small Factor Pluggable) transceiver module: From 550 meters (멀티방식섬유), up to 10/30/50/70/120 kilometers (싱글방식섬유)

■ Reset button

전면 패널 왼쪽의 리셋 버튼은 전원을 끄고 켜지 않고 관리형 스위치를 재부팅 하도록 설계되어있습니다. 다음은 재설정 버튼에대한 요약표를 나타낸것입니다.

Reset Button Pressed and Released	Function
< 5 sec: 시스템 리부	관리형 스위치 재부팅

> 5 sec: 공장초기	관리형 스위치의 공장초기화 구성 은 리부팅하고 로드하는 기본 셋팅은 다음과 같습니다. ◦ Default Username: admin ◦ Default Password: admin ◦ Default IP address: 192.168.0.100 ◦ Subnet mask: 255.255.255.0 ◦ Default Gateway: 192.168.0.254

■ 콘솔 Port

콘솔 Port 는 DB9, RS-232 male 직렬 Port 커넥터입니다. 터미널을 직접 연결하기위한 인터페이스입니다. 콘솔 Port 를 통해 IP 주소 설정, 공장 초기화, Port 관리, 링크 상태 및 시스템 설정과 같은 다양한 진단 정보를 제공합니다. user 는 패키지의 연결된 RS-232 케이블을 사용하여 장치의 콘솔 Port 에 연결할 수 있습니다. 연결이 끝나면 user 는 터미널 에뮬레이션 프로그램 (하이퍼 터미널, ProComm Plus, Telix, Winterm 등)을 실행하여 장치의 시작 화면으로 들어갑니다.

1.1.2 LED 표시.

전면 패널 LED 는 Port 링크 데이터 작동 및 시스템 전원의 순간상태를 나타냅니다. 필요할 때 모니터하고 문제를 해결하는 데 도움이 됩니다. 그림 2-3 은 이러한 관리형 스위치의 LED 상태를 나타내고 있습니다.

SFC4000T / SFC4000T-DC LED indication

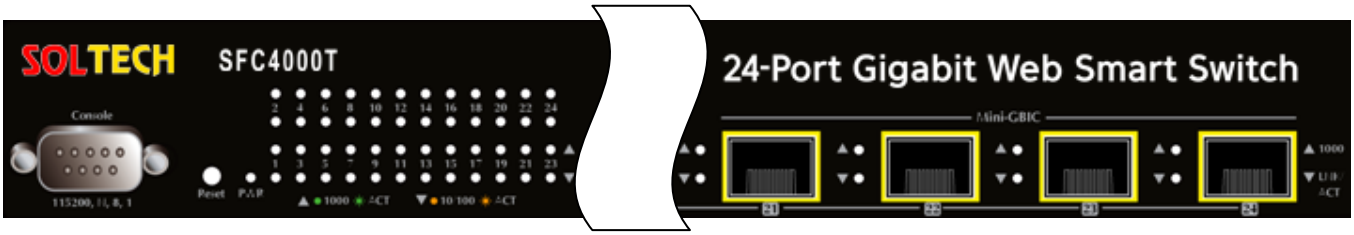


그림 2-3 SFC4000T / SFC4000T-DC LED for Front Panel

■ 시스템

LED	Color	Function
PWR	Green	스위치의 파워가 들어올경우 불이 들어온다 .

■ Per 10/100/1000Mbps Port

LED	Color	Function
1000 LNK/ACT	Green	Lights 성공적으로 설정었음을 나타내는 표시등 입니다. 1000mbps 속도로 실행중 ed. 깜박임 : 스위치가 해당 Port 를 통해 데이터를 전송하거나 수신 중임을 나타냅니다
10/100 LNK/ACT	Orange	Port 가 10 / 100Mbps 속도로 성공적으로 설정되었음을 나타내는 표시등입니다. 깜박임 : 스위치가 해당 Port 를 통해 데이터를 전송하거나 수신 중임을 나타냅니다.

■ Per 100/1000Base-X SFP Interfaces

LED	Color	Function
1000	Green	Port 가 1000Mbps 에서 작동 중임을 나타내는 표시등입니다. 꺼짐은 Port 가 100Mbps 에서 작동 중이거나 링크가 없음을 나타냅니다.
LNK/ACT	Orange	Port 가 성공적으로 설정되었음을 나타내는 표시등 깜박임 : 스위치가 해당 Port 를 통해 데이터를 전송하거나 수신 중임을 나타냅니다.

1.1.3 스위치 후면

관리형 스위치의 후면 패널은 100-240V AC, 50-60Hz 의 입력 전원을 수용하는 전원 소켓을 나타냅니다 다음 그림들은 이러한 관리되는 스위치 후면 패널은 보여줍니다.

SFC4000T Rear Panel

그림 2-4 Rear panel of SFC4000T (후면)

SFC4000T-DC Rear Panel

그림 2-5 Rear panel of SFC4000T-DC (후면)

■ AC 전원 콘센트

세계 대부분의 지역에서 전기 서비스와의 호환성을 위해 관리형 스위치의 전원 공급 장치는 100-240VAC 및 50/60 Hz 의 범위에서 자동으로 조정됩니다.

전원 코드의 암 끝 부분을 관리 스위치의 후면 패널에있는 소켓에 단단히 꽂습니다. 전원 코드의 다른 쪽 끝을 전기 서비스 콘센트에 연결하면 전원이 공급됩니다.

전원 알림 : 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 서억제 장치를 설치하면 스위치 또는 전원 어댑터에 대한 조절되지 않은 서지 또는 전류로 인해 관리되는 스위치가 손상되는 것을 방지하는 데 도움이 될 수 있습니다.

■ DC 전원 커넥터

SFC4000T-DC 의 후면 패널에는 전원 스위치와 -36V ~ -60V DC 의 DC 전원 입력 전압을 수용하는 DC 전원 커넥터가 있습니다. 전원 케이블을 입력 단자 블록의 관리 대상 스위치에 연결하십시오. 터미널 블록에있는 두 개의 나사의 크기는 M3.5 입니다.

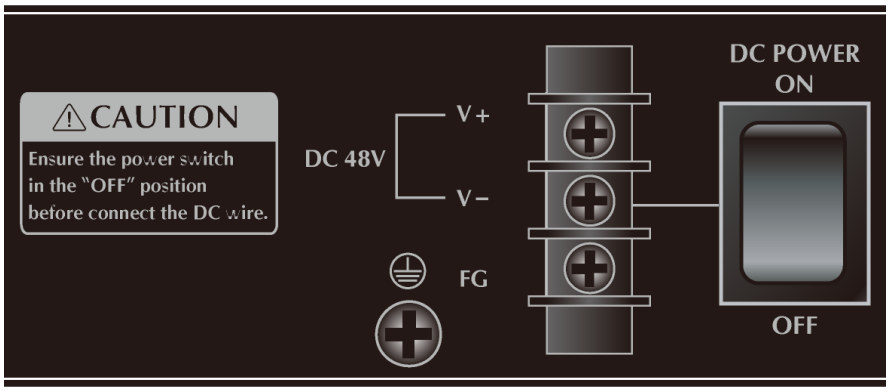


그림 2-6 SFC4000T-DC 후방 패널

경고

DC 전원 케이블을 SFC4000T-DC 의 입력 단자 블록에 연결하기 전에 전원 스위치가 "OFF"위치에 있고 DC 전원이 꺼져 있는지 확인하십시오

1.2 스위치 설치

이 단계에서는 관리형 스위치를 설치하고 관리형 스위치에 연결하는 방법을 설명합니다. 다음 주제를 읽고 제시되는 순서대로 절체를 수행하십시오. 데스크탑 또는 선반에 Managed 스위치를 설치하려면 다음 단계를 완료하기 만하면됩니다.

1.2.1 데스크탑 설치

데스크톱 또는 선반에 관리 대상 스위치를 설치하려면 다음 단계를 따르십시오.

1 단계 : 고무 다리를 관리 스위치의 아래쪽에있는 움푹 들어간 부분에 부착하십시오.

2 단계 : 관리되는 스위치를 그림 2-7 과 같이 AC 전원 근처의 데스크탑이나 선반 위에 놓습니다.

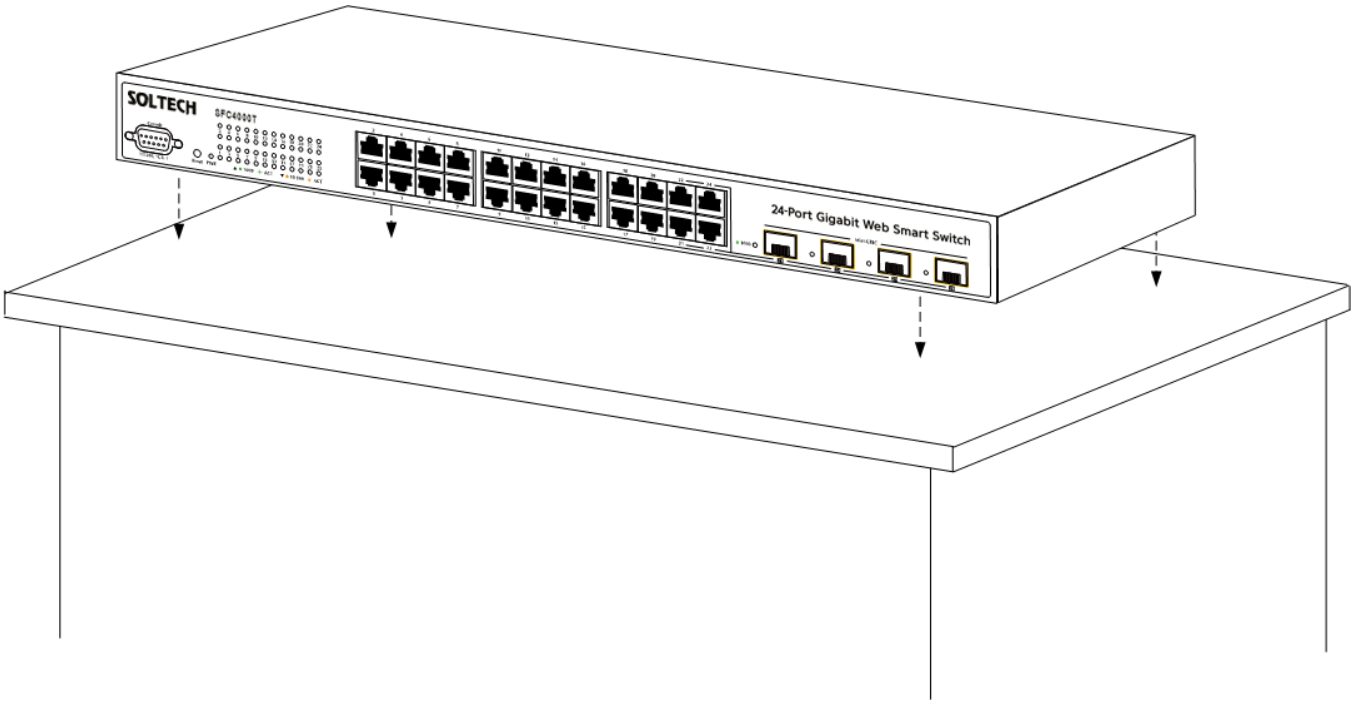


그림 2-7 책상에 관리형스위치를 둔 모습

Step3: 관리형 스위치와 주변 물체사이에 충분한 환기 공간을 확보해야한다

Note

위치를 선택할 때는 1 장, 4 절 및 사양에서 설명한 환경 제한 사항을 명심하십시오.

Step4: 관리형 스위치를 네트워크 장치에 연결합니다.

표준 네트워크 케이블의 한쪽 끝을 관리 스위치 전면의 10/100/1000 RJ-45 Port 에 연결하십시오

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

Note

관리형 스위치에 연결하려면 RJ-45 팁이있는 UTP 카테고리 5 네트워크 케이블이 필요합니다. 자세한 내용은 부록 A 의 케이블 연결 사양을 참조하십시오.

Step5: 관리형 스위치에 전원을 공급합니다.

전원 케이블의 한쪽 끝을 관리 대상 스위치에 연결하십시오.

전원 케이블의 전원 플러그를 표준 벽면 콘센트에 연결하십시오.

관리형 스위치에 전원이 공급되면 전원 LED 가 녹색으로 계속 켜져야 합니다

1.2.2 랙 연결

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

단계 1: : 관리 스위치를 단단한 평면 위에 놓고 전면 패널을 전면쪽으로 배치합니다.

단계 2:. 패키지에 제공된 나사를 사용하여 관리 대상 스위치의 양쪽에 랙 마운트 브래킷을 부착하십시오.

그림 2-8 은 관리 형 스위치의 한쪽에 브래킷을 부착하는 방법을 보여줍니다.

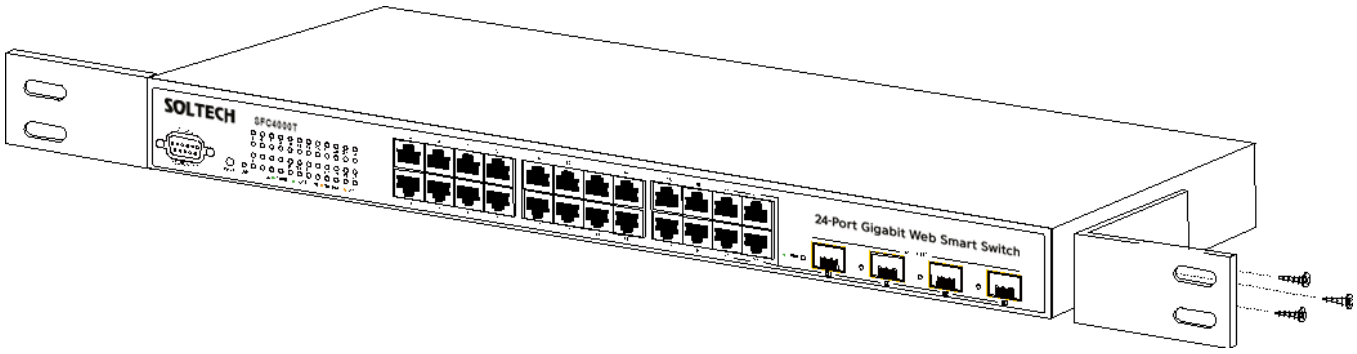


그림 2-8 관리형 스위치에 브래킷을 부착하는그림

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

단계 3: 브래킷을 단단히 고정시킵니다.

단계 4: 두번째 브래킷도 반대쪽에 부착합니다.

단계 5: 관리 장치에 브래킷을 부착한후 나사를 사용하여 브래킷을 랙에 단단히 고정하십시오 (그림 2-9 참조)

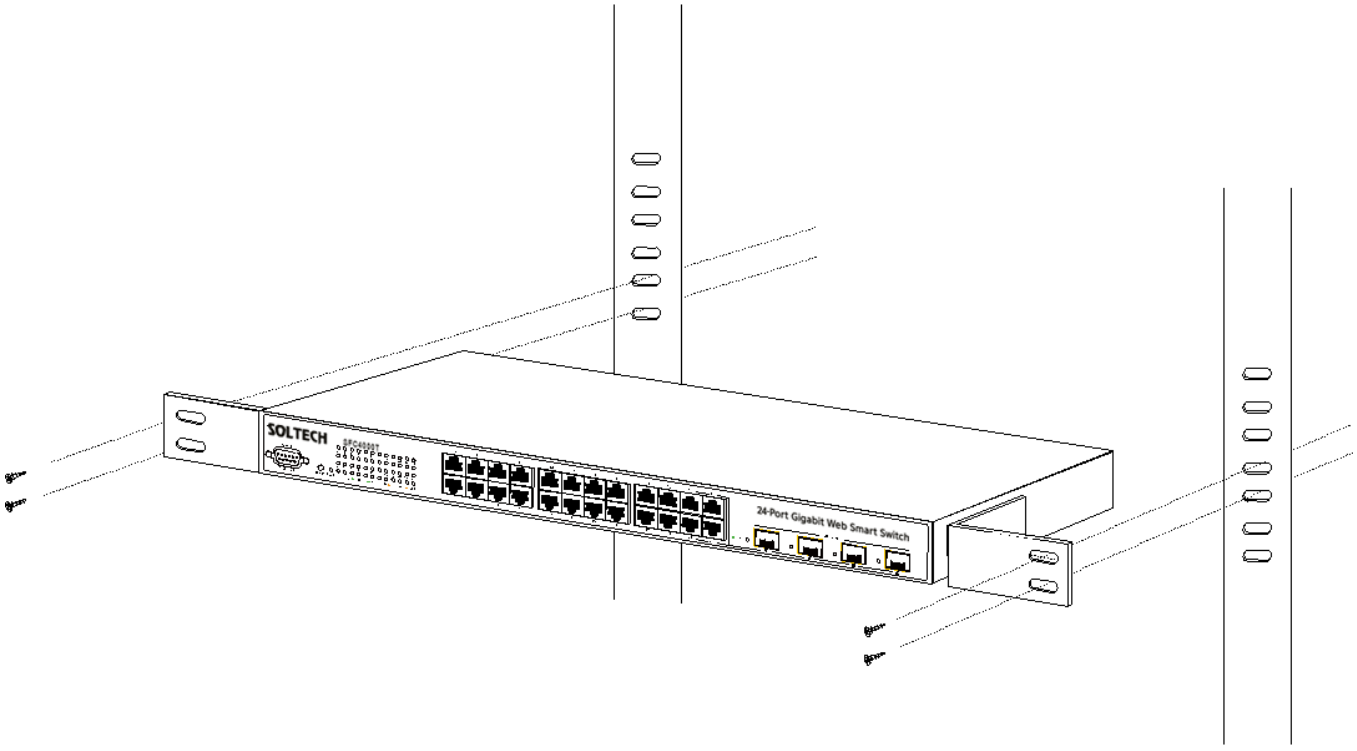


그림 2-9 렉에 스위치를 장착하는 모습

단계 6: 데스크탑 설치의 4 단계와 5 단계를 수행하여 네트워크 케이블을 연결하고 전원을 관리형 스위치에 공급합니다.

1.2.3 SFP 송수신기 설치

이번 단계 에서는 SFP 송수신기를 SFP 슬롯에 삽입하는 방법을 설명합니다.
SFP 송수신기는 핫 플러그 및 핫 스왑이 가능합니다. 관리 형 스위치의 전원을 끄지 않고도 모든 SFP Port 에서 송수신기를 플러그 인 및 플러그 아웃 할 수 있습니다. 그림 2-10 과 같이 나타납니다.

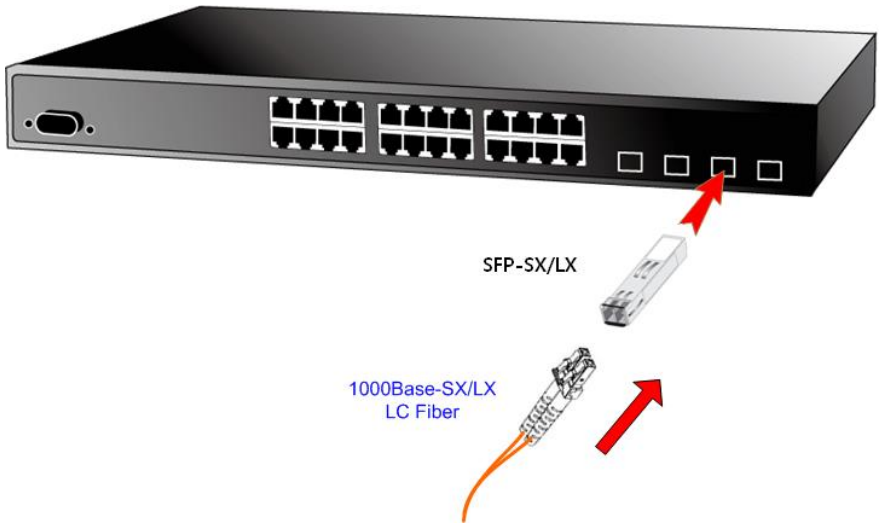


그림 2-10 송수신기 플러그인

■ 승인 된 soltech SFP 송수신기

SOLTECH 관리형 스위치는 단일 방식 및 다중 방식 SFP 송수신 장치를 모두 지원합니다. 승인 된 SOLTECH SFP 송수신기 목록은 발행 시점에 정확합니다.

- SFP-SX SFP (1000BASE-SX SFP 송수신기 / 다중 방식 / 850nm / 220m ~ 550m)
- SFP-LX SFP (1000BASE-LX SFP 송수신기 / 단일 방식 / 1310nm / 10km)
- SFP-LXWA SFP (1000BASE-LX SFP 송수신기 / WDM 단일 방식 / TX : 1550nm, RX : 1310nm / 20km)
- SFP-LXWB SFP (1000BASE-LX SFP 송수신기 / WDM 단일 방식 / TX : 1310nm, RX : 1550nm / 20km)

Note

관리 스위치에서 SOLTECH SFP 를 사용할 것을 권장합니다. 지원되지 않는 SFP 송수신 장치를 삽입하면 관리 장치는이를 인식하지 못합니다

다른 Managed 스위치, 워크 스테이션 또는 미디어 컨버터를 연결하기 전에.

1. SFP 송수신 장치의 양면이 동일한 미디어 유형 (예 : 1000Base-SX - 1000Base-SX, 1000Bas-LX - 1000Base-LX)인지 확인하십시오.
2. SFP 송수신기 방식 I 과 일치하는 광섬유 케이블 유형을 확인하십시오.

1000Base-SX SFP 송수신기에 연결하려면 멀티 방식 광섬유 케이블을 사용하십시오. 한 쪽은 male duplex LC 커넥터 유형이어야합니다.

1000Base-LX SFP 송수신기에 연결하려면 단일 방식 광섬유 케이블을 사용하십시오. 한 쪽은 male duplex LC 커넥터 유형이어야합니다.

■ 광 케이블 연결

1. 네트워크 케이블의 이중 LC 커넥터를 SFP 송수신기에 연결하십시오.

2. 케이블의 다른 쪽 끝을 장치에 연결합니다. - SFP 가 설치되어 있고 광섬유 NIC 가 워크 스테이션에 있거나 Media Converter 에 연결되어 있습니다.

3. 관리 스위치 전면에있는 SFP 슬롯의 LNK / ACT LED 를 확인하십시오. SFP 송수신기가 올바르게 작동하는지 확인하십시오.

4. 링크가 실패한 경우 SFP Port 의 링크 방식을를 확인합니다.o 는 일부 fiber-NIC 또는 Media Converters 와 함께 작동하며 링크 방식을를 "1000 Force"또는 "100 Force"로 설정해야합니다.

트랜시버 모듈을 제거하십시오

1. 문의하거나 네트워크 관리자에게 문의하여 네트워크 활동이 없는지 확인하십시오. 또는 스위치 / 컨버터 (사용 가능한 경우)의 관리 인터페이스를 통해 사전에 Port 를 비활성화하십시오.

2. 광섬유 케이블을 부드럽게 제거합니다.

3. MGB 모듈의 핸들을 수평으로 돌립니다.

4. 핸들을 통해 모듈을 부드럽게 잡아 당깁니다.

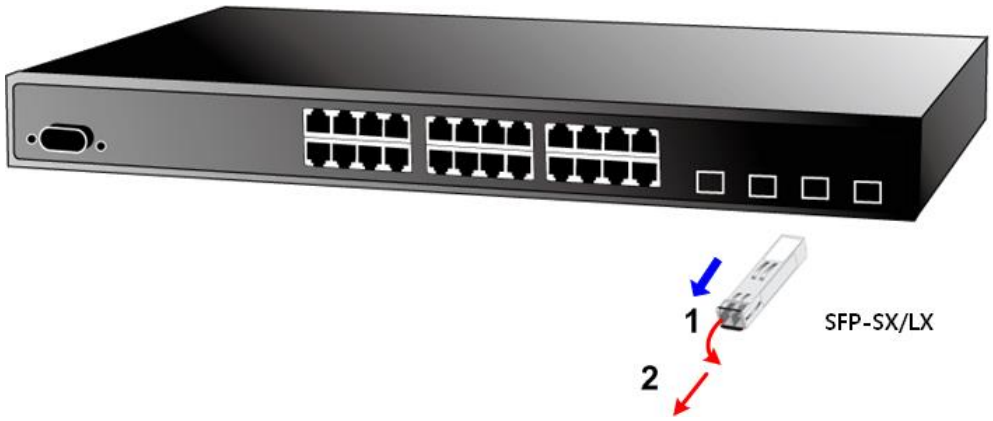


그림 2-11 Pull out the SFP transceiver

Note

모듈의 손잡이 나 누름 볼트를 당기지 말고 모듈을 잡아 당기지 마십시오. 폭력적인 모듈을 직접 당겨 내면 관리 스위치의 모듈 및 SFP 모듈 슬롯이 손상 될 수 있습니다.

1.2.4 DC 전원 공급 장치 연결 - SFC4000T-DC

1. SFC4000T-DC는 -48VDC 전원 입력을 지원하며 전원 케이블을 입력 단자 블록의 스위치에 연결합니다.
2. 1. 단자대에있는 3 개의 나사의 크기는 M3.5입니다.
3. 2. 터미널은 "V +", "V-"& "FG"로 표시됩니다.
4. 3. 3 개의 나사를 풀고 DC 케이블을 그 아래로 밀어 넣으십시오. 먼저 커넥터에 DC 케이블을 삽입하고 단단히 조입니다.

5. 전원 케이블을 DC 전원 공급 장치에 연결하십시오. 전원을 켜거나 재설정 한 후 관리 스위치는 콜드 스타트 절차를 수행합니다.

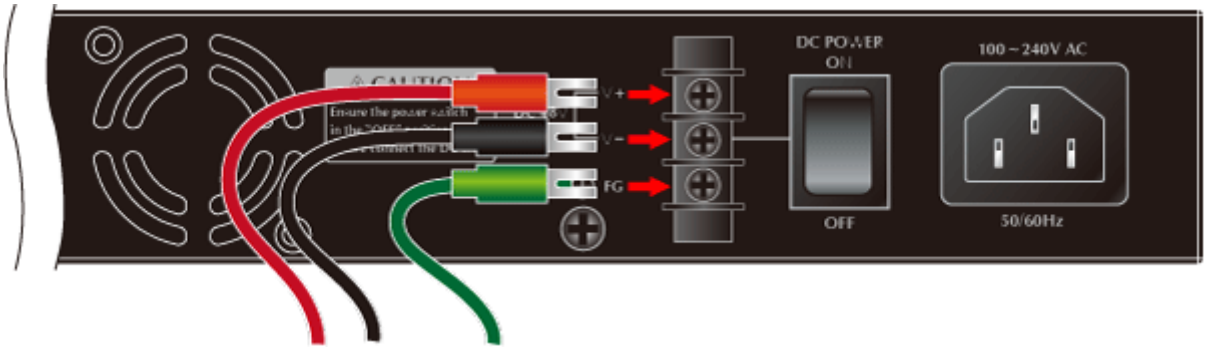


그림 2-20 -48VDC connector

경고	DC 전원 케이블을 Managed 스위치의 입력 단자 블록에 연결하기 전에 전원 스위치가 "OFF"위치에 있고 DC 전원이 꺼져 있는지 확인하십시오

2. 스위치 관리

이 장에서는 관리형 스위치 접근을 구성 하는 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. 또한 Port 연결 옵션에 대한 정보도 들어 있습니다.

이 장에서는 다음 주제를 다룹니다.

- 요구 사항
- 관리 접근 개요
- 관리 컨솔 개요
- Web 관리 접근
- SNMP 접근
- 표준,프로토콜, 딜레이 읽

2.1 요구조건

- 네트워크 cables - Use standard 네트워크 (UTP) cables with RJ45 connectors.
- Windows 2000 / XP, 2003, Vista / 7, 2008, MAC OS9 이상, TCP / IP 프로토콜과 호환되는 Linux, UNIX 또는 기타 플랫폼을 실행하는 가입자의 워크 스테이션.
- Ethernet NIC (네트워크 인터페이스 카드)가 설치된 워크 스테이션
- 시리얼 Port 연결 (터미널)
- • COM Port (DB9 / RS-232) 또는 USB-RS-232 변환기가있는 PC 이상
- 이더넷 Port 연결
- • 네트워크 케이블 - RJ45 커넥터가있는 표준 네트워크 (UTP) 케이블을 사용하십시오.
- WEB Browser 및 JAVA Runtime Environment 플러그인이 설치된 워크 스테이션 위

Internet Explore 7.0 이상의 버전을 사용하기를 권고한다.

2.2 관리 접근 개요

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

- 관리 콘솔
- 웹 브라우저 인터페이스
- 외부 SNMP 기반 인터페이스

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

Method	Advantages	Disadvantages
Console	• IP 없는 주소 or 서브넷이 필요한경우 • Text 기반 일경우 • 윈도우 95/98/NT/2000/ME/XP 운영체제에 내장 된 텔넷 기능 및 하이퍼 터미널 • 보안성	• 스위치 근처에 있거나 전화 접속 연결을 사용 • 원격 user 에게는 불편하다 • 모뎀연결이 불안정 할 수 있다.
Web Browser	• 원격으로 스위치를 구성 하는데 이상적 • 모든 유명한 브라우저와 호환가능 • 어느 위치에서나 접근가능 • 시각적으로 가장 매력적	• 보안이 손상될 수 있다 • 열악한 연결에서 지연시간이 발생 가능하다
SNMP Agent	• MIB 단계에서 스위치 기능과 통신 • 개방형 표준 기반	• SNMP 관리자 소프트웨어 필요 • 세 가지 방법 모두가 시각적으로 매력적 • 일부 설정은 계산이 필요 • 보안이 손상될 수 있다.

테이블 3-1 관리 방법 비교

2.3 관리 콘솔

관리 콘솔은 통계 표시 또는 옵션 설정 변경과 같은 시스템 관리를 수행하기위한 내부, 문자 지향 및 명령 행 user 인터페이스입니다. 이 방법을 사용하면 스위치의 콘솔 (직렬) Port 에 연결된 터미널, 개인용 컴퓨터, Apple Macintosh 또는 워크 스테이션에서 관리 콘솔을 볼 수 있습니다.
이 관리 방법을 사용하는 방법에는 직접 액세스 또는 모뎀 Port 액세스를 사용하는 두 가지가 있습니다. 다음 섹션에서는 이러한 방법에 대해 설명합니다. 콘솔 사용에 대한 자세한 내용은 5 장 명령 줄 인터페이스 콘솔 관리를 참조하십시오.

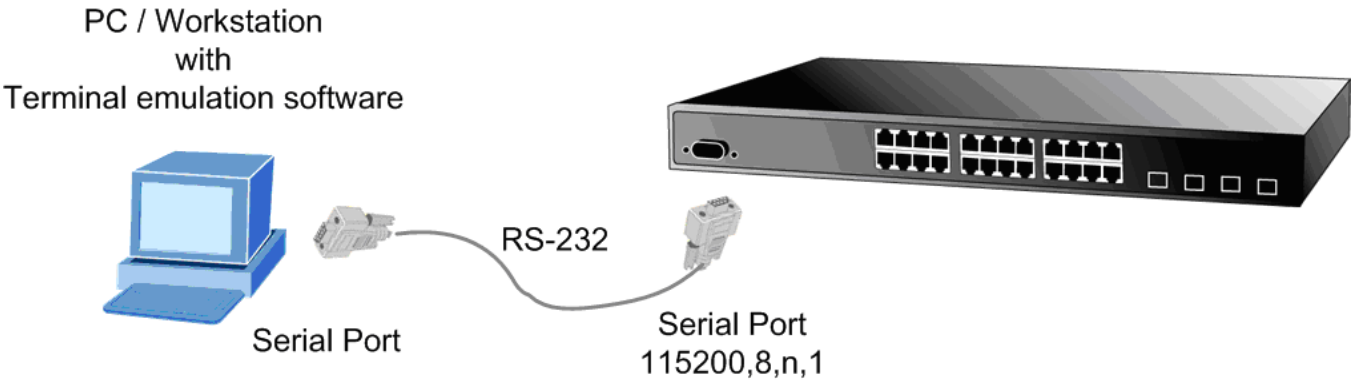


그림 3-1 Console 관리

직접 접근

터미널 또는 터미널 에뮬레이션 프로그램 (예 : 하이퍼 터미널)이 장착 된 PC 를 관리형 스위치 콘솔 (직렬) Port 에 직접 연결하여 관리 콘솔에 직접 액세스 할 수 있습니다.

이 관리 방법을 사용할 때는 스위치를 PC 에 연결하기 위해 직선형 DB9 RS-232 케이블이 필요합니다. 이 연결을 한 후에 터미널 에뮬레이션 프로그램이 다음 매개 변수를 사용하도록 구성 하십시오.

기본 매개 변수는 다음과 같습니다.

- 115200 bps
- 8 data bits
- No parity
- 1 stop bit

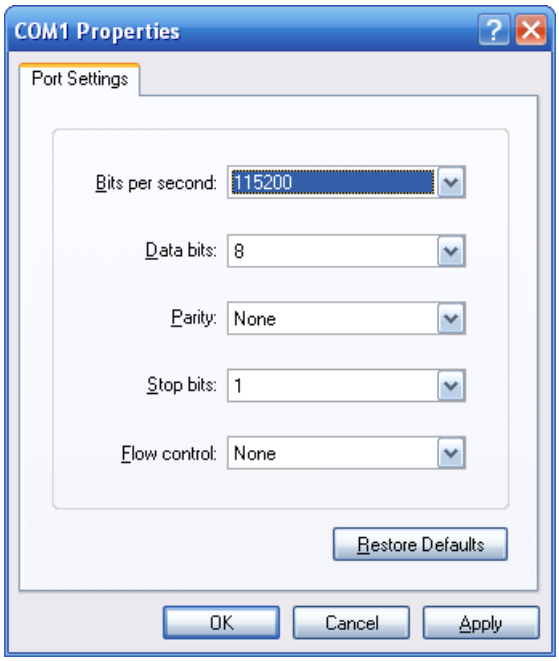


그림 3-2 종단 파라미터값 셋

로그온 한 후에 원하는 경우 이러한 설정을 변경할 수 있습니다. 이 관리 방법은 시스템을 다시 부팅하는 동안 연결되어 있고 시스템을 모니터링 할 수 있기 때문에 선호되는 경우가 많습니다. 또한 관련 작업이 시작된 인터페이스에 관계없이 특정 오류 메시지가 직렬 Port 로 전송됩니다. Macintosh 또는 PC 연결은 터미널 직렬 Port 에 연결하기 위해 터미널

에뮬레이션 프로그램을 사용할 수 있습니다. UNIX 에서 워크 스테이션 첨부는 TIP 와 같은 에뮬레이터를 사용할 수 있습니다.

2.4 Web 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 설정 한 후에는 관리되는 스위치의 IP 주소를 입력하여 웹 브라우저에서 직접 관리되는 스위치의 웹 인터페이스 응용 프로그램에 액세스 할 수 있습니다

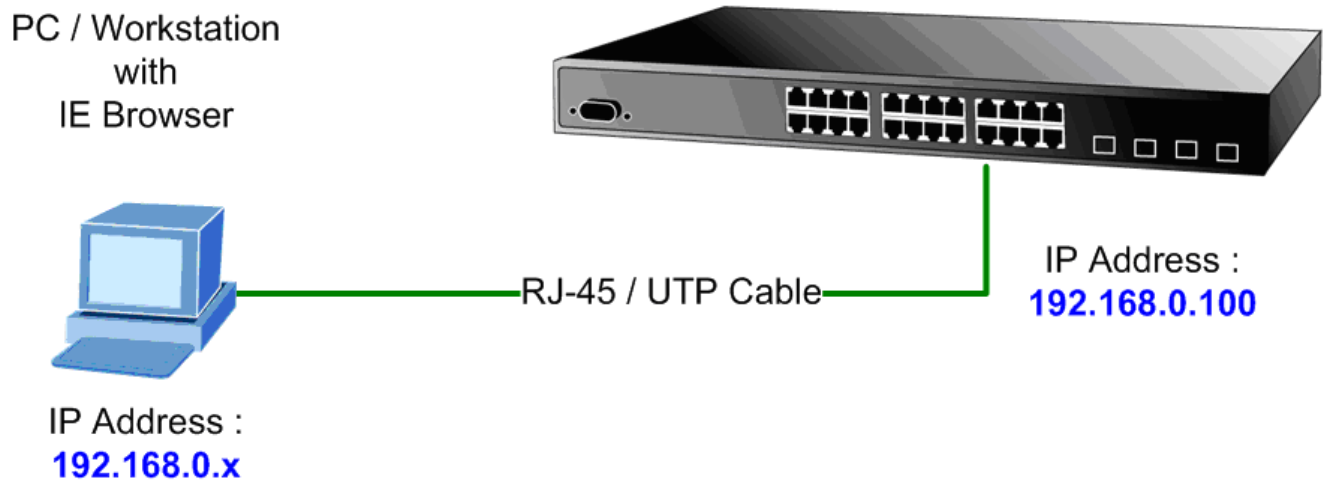


그림 3-3 Web 관리

그런 다음 웹 브라우저를 사용하여 관리 대상 스위치의 콘솔 Port 에 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 3-4 Web main screen of Managed 스위치

2.5 SNMP 기반 네트워크 관리

외부 SNMP 기반 응용 프로그램을 사용하여 SNMPc Network Manager, HP Openview 네트워크 노드 관리 (NNM) 또는 What 's Up Gold 와 같은 관리 대상 스위치를 구성 하고 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 커뮤니티 문자열 만 알면 MIB 만 읽을 수 있습니다. 관리 스위치의 커뮤니티 문자열은 기본 gets 및 set public 입니다..

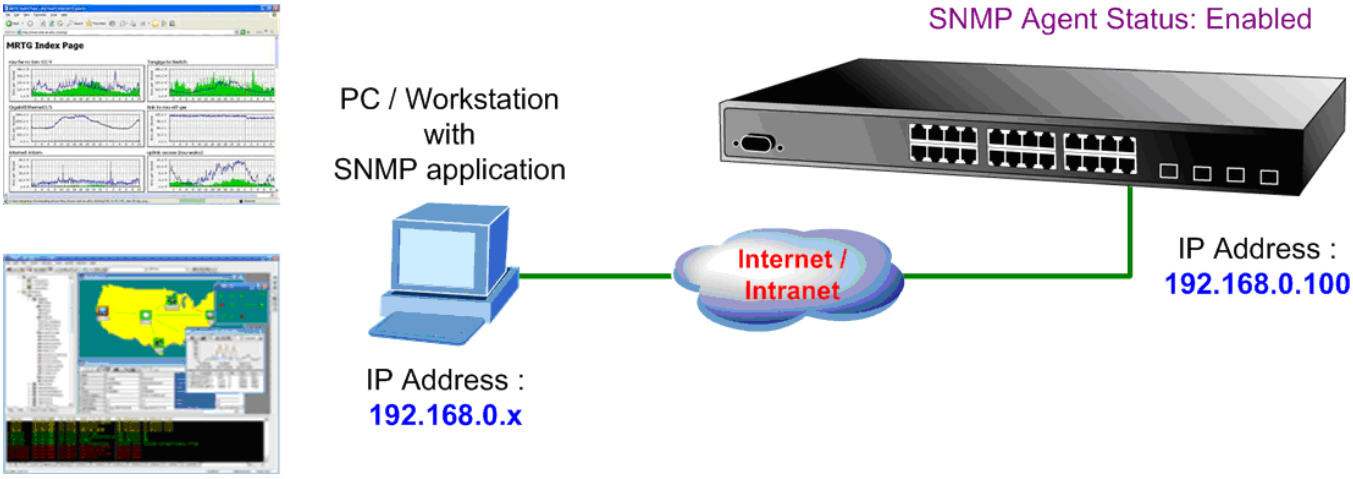


그림 3-5 SNMP 관리

3. WEB 구성

이 단계에서는 웹 기반 관리의 구성 과 기능을 소개합니다 .

웹 기반 관리에 관하여..
관리형 스위치는 Internet Explorer 와 같은 표준 브라우저를 통해 네트워크의 어느 곳에서나 관리형 스위치를 관리 할 수있는 관리 기능을 제공합니다.

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

Note

기본적으로 IE7.0 이상 버전에서는 Java 애플릿이 소켓을 열 수 없습니다. user 는 Java 애플릿이 네트워크 Port 를 사용할 수 있도록 브라우저 설정을 명시적으로 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 SFC4000 관리 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) 및 기본 서브넷 마스크 255.255.255.0 입니다.

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 구성 을 수행하십시오.

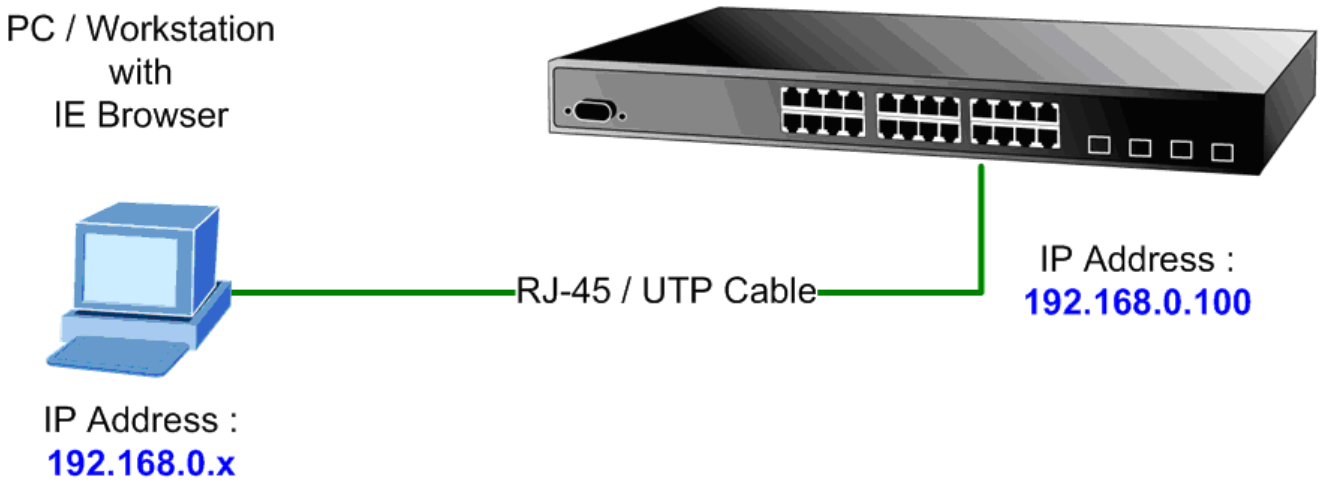


그림 4-1-1 Web 관리

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

그림 4-1-2 Login screen

Default user : admin

Default 비밀번호 admin

그림 4-1-3 을보면 아이디와 비밀번호를 입력하면 다음과 같이 들어가진다.

그림 4-1-3 기본설정 페이지

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

Note

1. Internet Explorer 7.0 이상을 사용하여 관리형 스위치에 액세스하는 것이 좋습니다.

2. 변경된 IP 주소는 저장 단추를 누른 후 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 명령 만 수락하십시오.

3.1 주요 웹 페이지

SFC4000 관리 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.

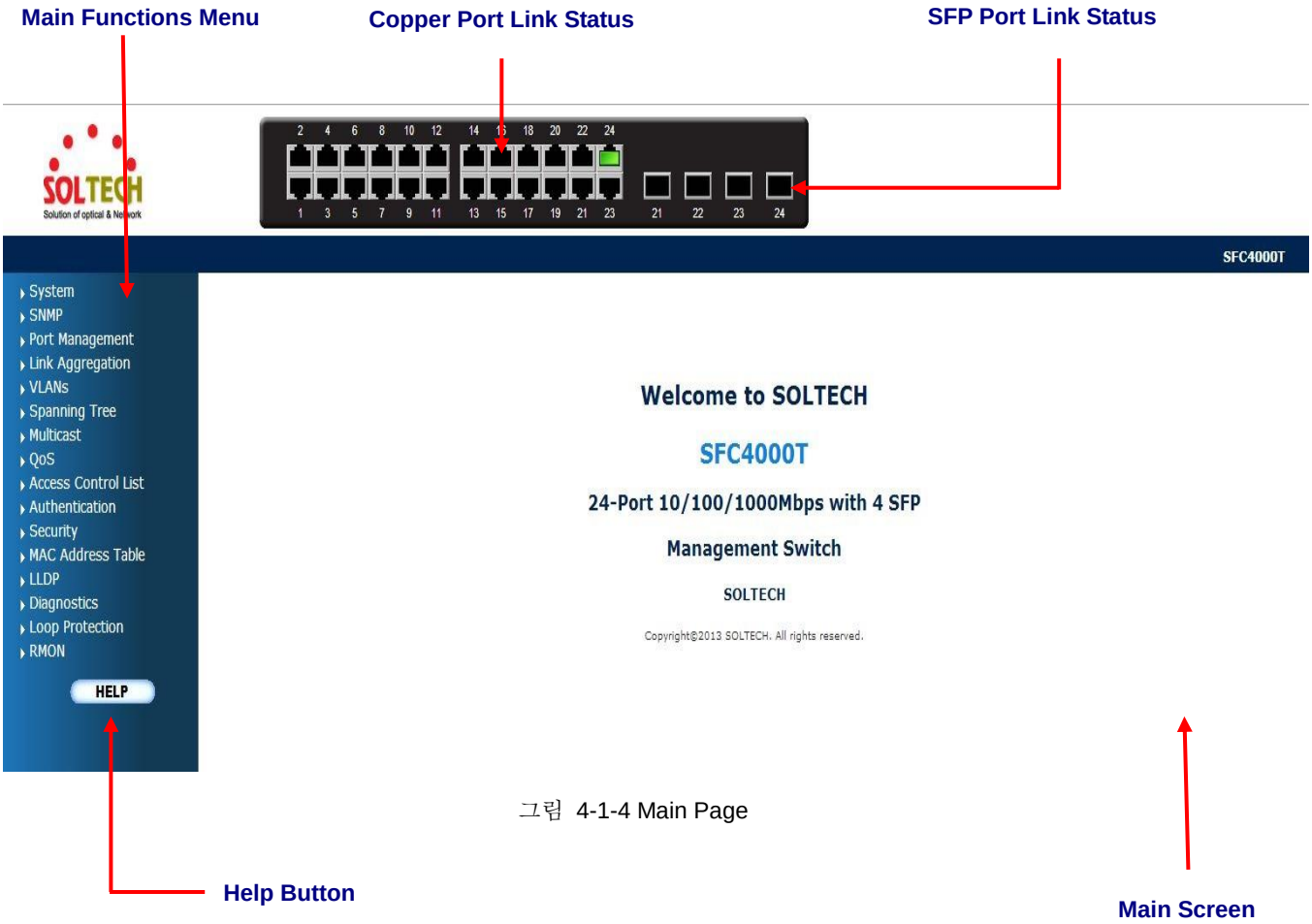


그림 4-1-4 Main Page

표시판

패널 디스플레이웹 에이전트는 관리형 스위치의 Port 이미지를 표시합니다. 방식은는 링크 업 또는 링크 다운을 포함하여 Port 에 대한 다른 정보를 표시하도록 설정할 수 있습니다. Port 의 이미지를 클릭하면 Port 통계 페이지가 열립니다.Port 상태는 다음과 같이 설명됩니다.

State	Disabled	Down	Link
RJ-45 Port			
SFP / SFP+ Port			

주요메뉴

온보드 웹 에이전트를 사용하여 시스템 매개 변수를 정의하고 관리형 스위치 관리 및 제어하며 모든 Port 또는 모니터 네트워크 조건을 정의 할 수 있습니다. Web- 관리를 통해 관리자는 Main Function 에 나열된 기능을 선택하여 관리형 스위치를설치할 수 있습니다. 그림 4-1-5 의 화면이 나타납니다.

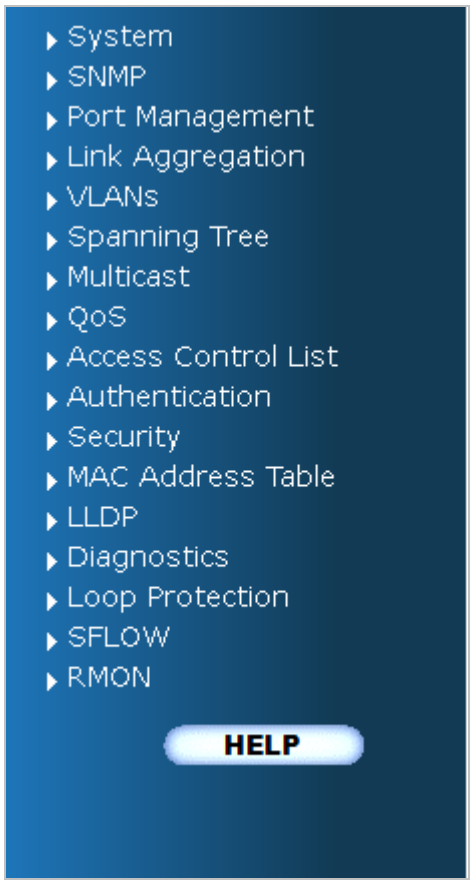


그림 4-1-5 관리형 스위치 주요 기능 메뉴

3.2 시스템

시스템 메뉴 항목을 사용하여 관리형 스위치의 기본 관리 정보를 표시하고 구성 하십시오. 시스템 아래에 다음과 같은 주제가 제공되어 시스템 안내를 구성 하고 볼 수 있습니다 :이 절에는 다음 항목이 있습니다

:

■ 시스템 정보	스위치 시스템 정보는 여기에 나와 있습니다.
■ IP 구성	이 페이지에서 스위치 관리 IP 정보를 구성 하십시오.
■ IPv6 구성	이 페이지에서 스위치 관리 IPv6 정보를 구성 하십시오.
■ user 구성	이 페이지는 현재 user 의 개요를 제공합니다. 현재 웹 서버에서 다른 user 로 로그인하는 유일한 방법은 브라우저를 닫았다가 다시 열 수 있습니다.
■ 권한 수준	이 페이지에서는 권한 수준에 대한 개요를 제공합니다.
■ NTP 구성	이 페이지에서 NTP 를 구성 하십시오.
■ UPnP	이 페이지에서 UPnP 를 구성 하십시오.
■ DHCP 릴레이	이 페이지에서 DHCP 릴레이를 구성 하십시오.
■ DHCP 릴레이 통계	이 페이지는 DHCP 릴레이에 대한 통계를 제공합니다.
■ CPU 로드	
■ 시스템 로그	이 페이지는 SVG 그래프를 사용하여 CPU 로드를 표시합니다.
■ 상세 로그	스위치 시스템 로그 정보는 여기에 나와 있습니다.
■ 원격 시스템 로그	스위치 시스템의 자세한 로그 정보는 여기에 나와 있습니다.
■ SMTP 구성	이 페이지에서 원격 syslog 를 구성 하십시오.
■ 웹 펌웨어 업그레이드	이 페이지에서 SMTP 매개 변수를 구성 하십시오.
■ TFTP 펌웨어 업그레이드	이 페이지는 스위치를 제어하는 펌웨어의 업데이트를 용이하게합니다.
■ 구성 백업	TFTP 서버를 통해 펌웨어 업그레이드
■ 구성 업로드	스위치 구성 을 저장할 수 있습니다. 구성 파일은 태그 계층이있는 XML 형식입니다.
■ 이미지 선택	스위치 구성 을 로드 할 수 있습니다. 구성 파일은 태그 계층이있는 XML 형식입니다.
■ 제조시 기본값	이 페이지에서 스택 스위치의 구성 을 리셋할 수 있습니다. IP 구성 은 유지 됩니다.
■ 시스템 재부팅	이 페이지에서 스택 스위치를 리셋할수 있고 리셋후에는 스위치가 정상적으로 부팅됩니다.

3.2.1 시스템 안내

시스템 정보페이지는 현재 장치 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.

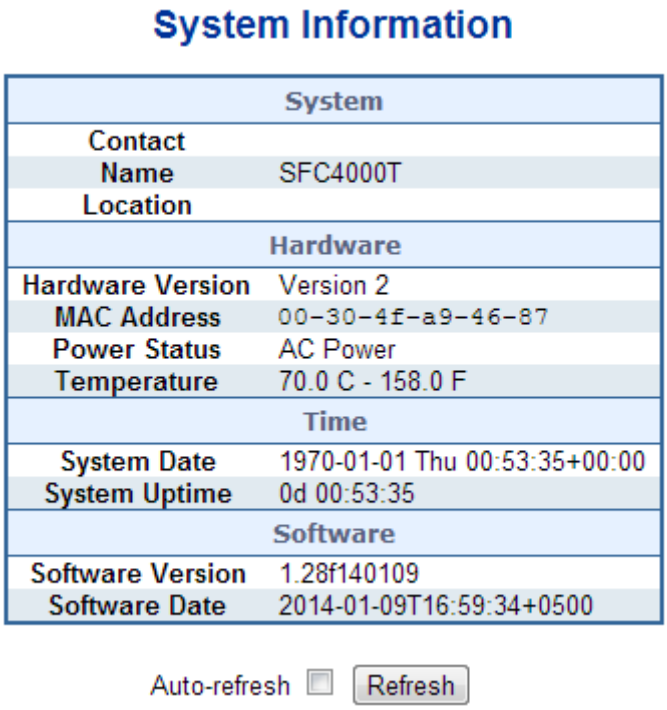


그림 4-2-1 시스템 안내화면

이 페이지는 다음과 같은 정보를 포함한다.

대상	내용
• Contact	시스템구성 에 설정|정보|시스템구성 으로 구성 되어있음
• Name	시스템이름에 설정|정보|시스템이름으로 구성 되어있음
• Location	시스템로컬에 설정|정보|시스템로컬로 구성 되어있음
• MAC Address	스위치의 MAC 주소입니다.
• Power Status	스위치의 AC/DC 전원 공급 장치 입력을 나타낸다.
• Temperature	주요 칩셋의 온도를 나타낸다.
• System Date	현 (GMT) 시스템 시간과 날짜를 말한다. 시스템시간은 SNTP 서버가 있는경우 얻습니다.
• System Uptime	장치가 작동된 기간입니다.
• Software Version	스위치 소프트웨어 버전입니다.
• Software Date	스위치 소프트웨어 생산 날짜를 의미합니다 .

버튼

Auto-refresh ☐ :3 초단위로 자동적으로 새로고침을 해주는 기능입니다.

Refresh: 페이지를 새로 고침하려면 클릭하십시오. 로컬에서 변경 한 사항은 실행 취소됩니다.

3.2.2 IP 구성

IP 구성 . 장치의 IP 주소, 서브넷 마스크 및 게이트웨이를 채 웁니다. 그림 4-2-2 의 화면이 나타납니다..

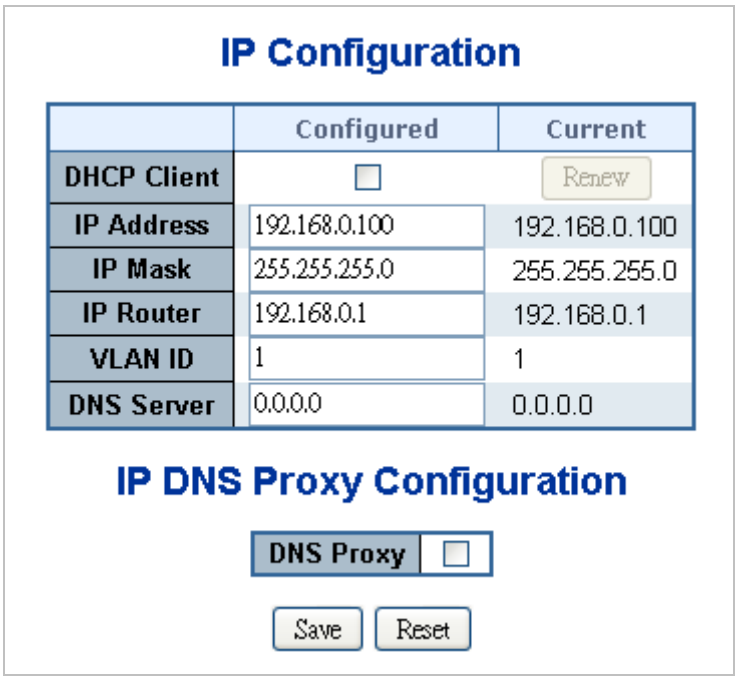


그림 4-2-2 IP 구성 페이지 화면

현재 컬럼은 활성화된 IP 구성 을 표시하는데 사용됩니다 .

Object	Description
• DHCP Client	DHCP 클라이언트를 활성화하고 DHCP 가 실패하고 구성 IP 주소가 0 이면 DHCP 가 다시 시도합니다. DHCP 가 실패하고 구성 IP 주소가 0 이 아니면 DHCP 가 중지되고 구성 된 IP 설정이 사용됩니다. DHCP 클라이언트는 DNS 조회를 제공하기 위해 구성 된 시스템 이름을 호스트 이름으로 알립니다.
• IP Address	이 스위치의 IP 주소를 점으로 구분 된 10 진수 표기법으로 제공합니다.
• IP Mask	이 스위치 점으로 구분된 십진수 표기법의 IP 마스크를 제공합니다.
• IP Router	점으로 구분 된 십진수 표기법으로 라우터의 IP 주소를 제공합니다.
• VLAN ID	관리 VLAN ID 를 제공하십시오. 허용되는 범위는 1 에서 4095 사이입니다.
• DNS 서버	점으로 구분 된 십진수 표기법으로 DNS 서버의 IP 주소를 제공합니다.

• DNS Proxy	DNS 프록시가 활성화되면 DUT 는 DNS 요청을 DUT 의 현재 구성 된 DNS 서버로 전달하고 DNS 확인자로 네트워크의 클라이언트 장치에 응답합니다.

버튼

Save 클릭하여 저장하고 변경한다. .

Reset: 로컬에서 변경한 값에 대하여 취소하고 이전에 저장상태로 돌리려면 클릭하세요

Renew: DHCP 를 갱신하기위해 클릭, 이버튼은 DHCP 가 활성화 된 후에 사용이 가능하다.

3.2.3 IPv6 구성

이 페이지에서 스위치 관리 IPv6 정보를 구성 한다, 구성 된 열은 IPv6 구성 을 변경하거나 볼 수 있습니다. 현재 열은 활성 Ipv6 구성 을 표시하는 데 사용됩니다. 그림 4-2-3 의 화면이나타납니다.

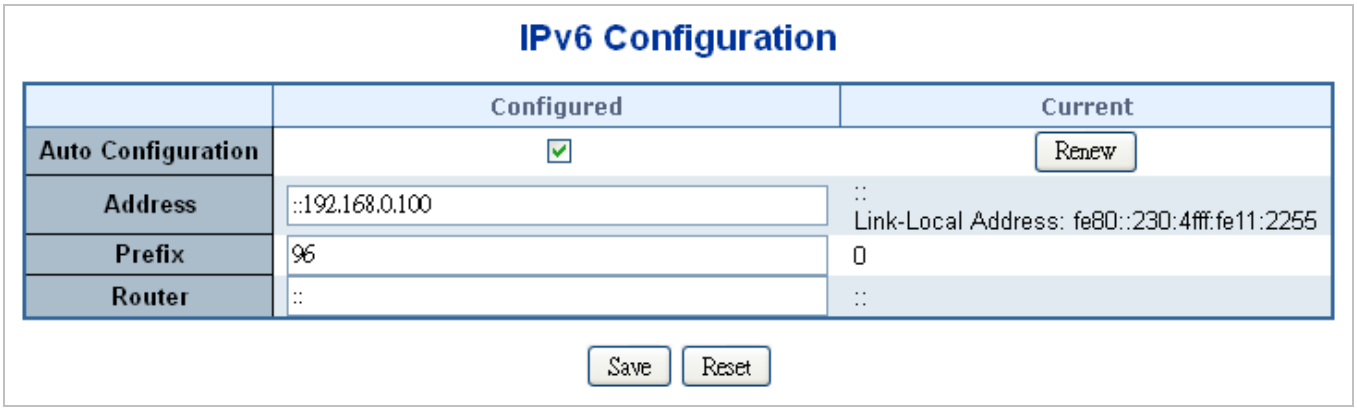


그림 4-2-3 IPv6 구성 페이지 화면

위의 내용은 다음과 같다.

설정	세부사항
• Auto matically	이 상자를 선택하여 IPv6 자동 구성 을 활성화하십시오. 실패 할 경우 구성 된 IPv6 주소는 0 입니다. 라우터가 라우터 요청에 대한 응답을 몇 초 동안 지연시킬 수 있으므로 자동 구성 을 완료하는 데 필요한 총 시간이 상당히 길어질 수 있습니다.
• address	이 스위치의 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 IPv4 주소를 사용했습니다. 예 : ':: 192.1.2.34'.
• Prefix	이 스위치의 IPv6 접두사를 제공하십시오. 허용되는 범위는 1 에서

	128 까지입니다..
Router	이 스위치의 IPv6 게이트웨이 주소를 제공한다. 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 IPv4 주소를 사용한다. 예 : ':: 192.1.2.34'. 이 스위치의 IPv6 SNTP 서버 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

Save: 변경사항을 저장할경우 클릭

Reset: 로컬 변경 사항을 취소하고 이전 저장된 값으로 되돌립니다.

Renew: IPv6 AUTOCONF 를 갱신시 클릭, 이 버튼은 IPv6 AUTOCONF 가 활성화 된 경우에만 사용합니다.

3.2.4 사용자의 구성

이 페이지는 현재 사용자의 개요를 제공합니다. 현재 웹 서버에 다른 user 로 로그인하는 유일한 방법은 브라우저를 닫았다가 다시 열 수 있습니다. 설정이 완료되면 "저장"버튼을 눌러 적용하십시오. 새 user 이름과 암호로 웹 인터페이스에 로그인하십시오. 그림 4-2-4 의 화면이 나타납니다.

그림 4-2-4 users 구성 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description

Username	사용자를 식별하는 이름입니다. 이것은 또한 사용자 추가 / 편집에 대한 링크입니다.
• Privilege Level	사용자의 권한 수준입니다. 허용 된 범위는 1 에서 15 까지입니다. 권한 수준 값이 15 이면 모든 그룹을 액세스 할 수 있습니다. 즉, 장치의 완전한 권한이 부여됩니다. 그러나 다른 사람들은 각 그룹 권한 수준을 참조 할 필요가 있습니다. 사용자의 권한은 그 그룹의 접근 권한을 가진 그룹 특권 레벨과 같거나 커야합니다. 기본적으로 대부분의 그룹 권한 수준 5 는 읽기 전용 접근 및 권한 수준 10 에 읽기 - 쓰기 접근 권한이 있습니다. 또한 시스템 유지 관리 (소프트웨어 업로드, 공장 기본값 등)에는 사용자 권한 수준 15 이 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 유저 추가버튼

사용자 추가 / 편집 유저

이 페이지는 사용자의 추가하거나 편집할경우 사용합니다 .

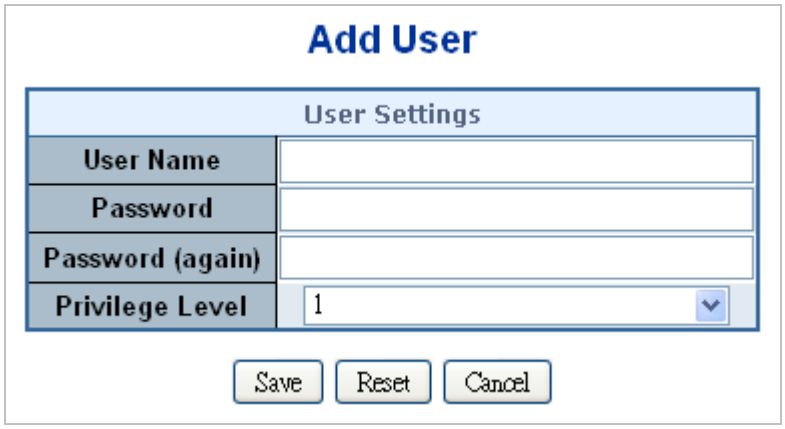


그림 4-2-5 사용자의 추가 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• User name	이 항목이 속해야하는 사용자 이름을 식별하는 문자열. 허용되는 문자열 길이는 1 - 32 입니다. 올바른 사용자 이름은 문자, 숫자 및 밑줄 문자 조합입니다.
• Password	사용자가 Username 과 같이 사용할 비밀번호의 길이는 0 ~ 32. 입니다.
• 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. 시스템 유지 관리 (소프트웨어 업로드, 공장 기본값 등)에는 사용자 권한 수준 15 이 필요합니다. 일반적으로 권한 수준 15 는 관리자 계정, 표준 사용자 계정의 권한 수준 10, 게스트 계정의 권한 수준 5 에 사용할 수 있습니다 .

버튼

Save: 변경사항 저장한다

Reset: 이전의 설정값으로 되돌린다.

Cancel:. 설정변경 취소

Delete User: 유저 제거

새 사용자가 추가되면 사용자 구성 페이지에 새 사용자 항목이 표시됩니다.

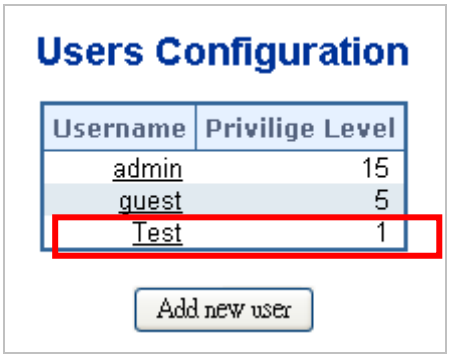


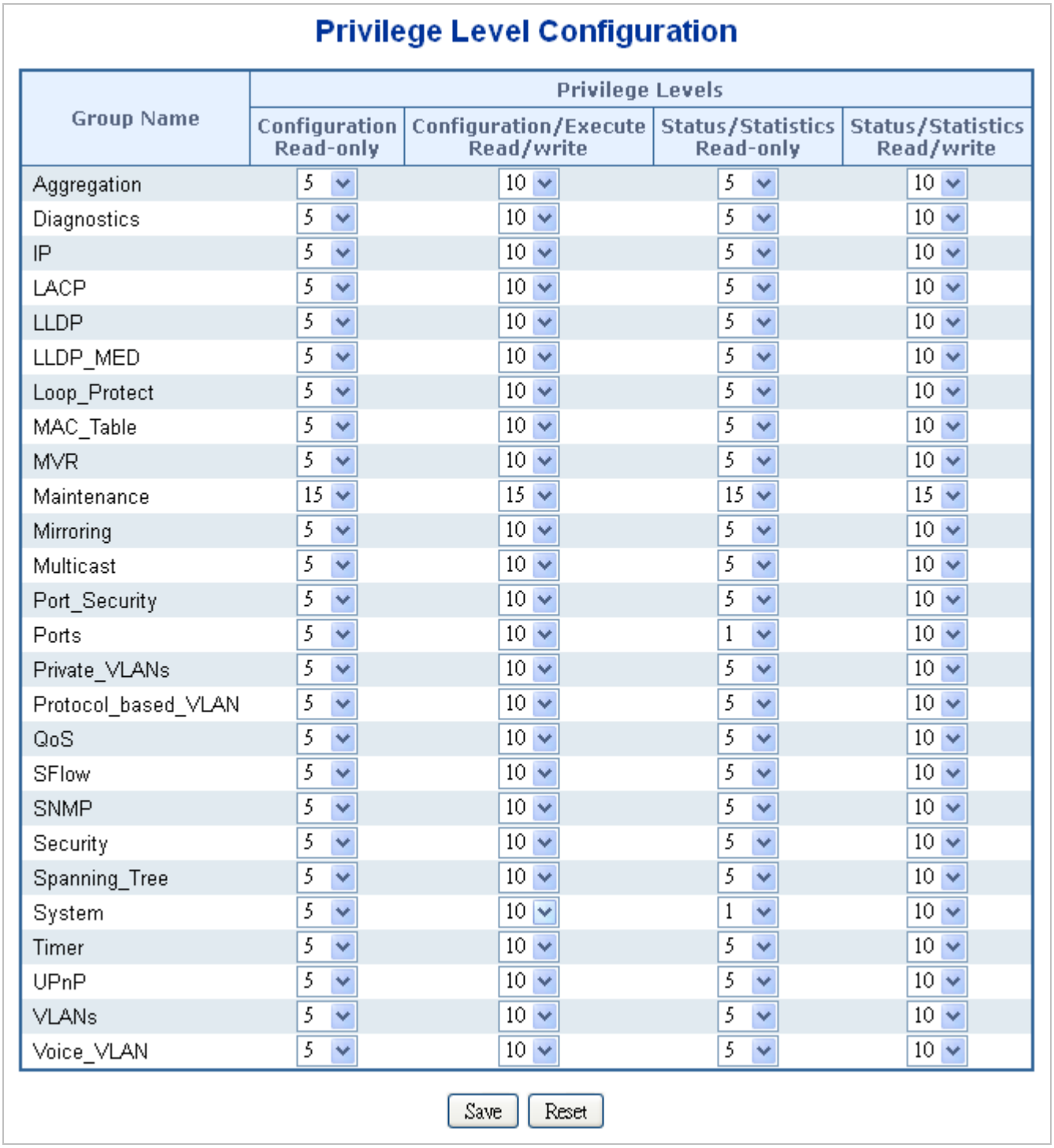
그림 4-2-6 사용자 구성 페이지 화면

Note

암호를 잊어 버린 경우 기본 암호를 변경하십시오. 10 초 이상 관리형 스위치의 전면 패널에있는 "Reset" 버튼을 누른 다음 손을 떼면 현재 설정에 VLAN 이 포함되어 손실되고 Managed Switch 가 기본 방식으로로 복원됩니다.

3.2.5 권한 단계

이 페이지에서는 권한 수준에 대한 개요를 제공합니다. 설정이 완료되면 "저장"버튼을 눌러 적용하십시오. 새 사용자 이름과 암호로 웹 인터페이스에 로그인하십시오. 그림 4-2-7 의 화면이 나타납니다.



Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Diagnostics	5	10	5	10
IP	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
LLDP_MED	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
MVR	5	10	5	10
Maintenance	15	15	15	15
Mirroring	5	10	5	10
Multicast	5	10	5	10
Port_Security	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
Protocol_based_VLAN	5	10	5	10
QoS	5	10	5	10
SFlow	5	10	5	10
SNMP	5	10	5	10
Security	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
Timer	5	10	5	10
UPnP	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10

Save Reset

그림 4-2-7 권한 수정 구성 페이지 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Group Name	권한 그룹을 식별하는 이름. 대부분의 경우 권한 수준 그룹은 단일 모듈 (예 : LACP, RSTP 또는 QoS)로 구성 되지만 그 중 일부는 둘 이상을 포함합니다. 다음 설명에서는 이러한 권한 수준 그룹을 세부적으로 정의합니다. 시스템 : 연락처, 이름, 위치, 시간대, 로그. 보안 : 인증, 시스템 액세스 관리, Port (Dot1x Port, MAC 기반 및 MAC 주소 제한 포함), ACL, HTTPS, SSH, ARP 검사 및 IP 소스 가드. IP : '핑 (ping)'을 제외한 모든 것. Port : 'VeriPHY'를 제외한 모든 항목 진단 : 'ping'및 'VeriPHY'. 유지 관리 : CLI- 시스템 재부팅, 시스템 복원 기본값, 시스템 암호, 구성 저장, 구성 로드 및 펌웨어로드. 웹 - 사용자, 권한 수준 및 유지 관리의 모든 것. 디버그 : CLI 에만 표시됩니다.
• Privilege Level	모든 권한 수준 그룹에는 구성 읽기 전용, 구성 / 실행 읽기 / 쓰기, 상태 / 통계 읽기 전용, 상태 / 통계 읽기 / 쓰기 (예 : 통계 지우기) 하위 수준의 권한 수준이 있습니다.

버튼

Save: 변경 사항을 저장하려면 클릭하십시오..

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

3.2.6 NTP 구성

NTP 구성 은 이 페이지에서 합니다

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 지정하고 GMT 시간대를 설정할 수 있습니다. 그림 4-2-8 의 NTP Configuration (NTP 구성) 화면이 나타납니다.

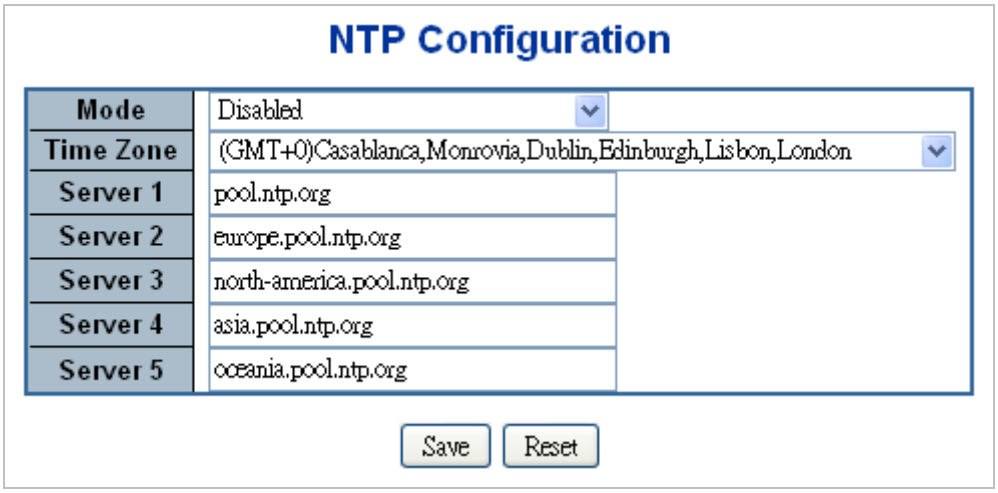


그림 4-2-8 NTP 구성 페이지화면

이 페이지는 다음의 사항과 같습니다.

설정	설명
• Mode	NTP 방식 작동을 나타냅니다. 가능한 방식은는 다음과 같습니다. 활성화 : NTP 방식 작동을 활성화합니다. NTP 방식 작동을 활성화하면 에이전트는 동일한 서브넷 도메인에 있지 않을 때 클라이언트와 서버간에 전달하고 NTP 메시지를 전송합니다. 비활성화 됨 : NTP 방식 작동을 비활성화합니다.
• Time Zone	스위치의 현재 위치에 따라 시간대를 선택하십시오.
• 서버	이 스위치의 NTP IPv4 또는 IPv6 주소를 제공하십시오. IPv6 주소는 콜론이 각 필드 (:)를 구분하는 최대 네 개의 16 진수로 된 8 개의 필드로 표현되는 128 비트 레코드에 있습니다. 예 : 'fe80 :: 215 : c5ff : fe03 : 4dc7'. '::'기호는 인접한 0 의 여러 16 비트 그룹을 표현하는 약자로 사용할 수있는 특수 구문입니다. 그러나 그것은 한 번 나타날 수 있습니다. 또한 다음과 같은 법적 IPv4 주소를 사용합니다. 예 : '::192.1.2.34'.

버튼

Save: 변경사항 저장\ㅇ: 이전에 저장된 값으로 되돌리면 클릭해야한다

3.2.7 UPnP

UPnP 구성 방안

이 스위치의 NTP IPv4 또는 IPv6 주소를 제공하십시오. IPv6 주소는 콜론이 각 필드 (:)를 구분하는 최대 네 개의 16 진수로 된 8 개의 필드로 표현되는 128 비트 레코드에 있습니다. 예 : 'fe80 :: 215 : c5ff : fe03 : 4dc7'. '::'기호는 인접한

0 의 여러 16 비트 그룹을 표현하는 약자로 사용할 수있는 특수 구문입니다. 그러나 그것은 한 번 나타날 수 있습니다. 또한 다음과 같은 법적 IPv4 주소를 사용합니다. 예 : ':: 192.1.2.34'.

그림 4-2-9 UPnP 구성 페이지 스크린캡처

이 페이지는 다음을 나타냅니다.

Object	Description
Mode	UPnP 작동 방식을를 나타냅니다. 가능한 방식은는 다음과 같습니다. 활성화 됨 : UPnP 방식 작동을 활성화합니다. 비활성화 됨 : UPnP 방식 작동을 비활성화합니다. 방식이가 활성화되면 두 개의 ACE 가 자동으로 추가되어 UPNP 관련 패킷을 CPU 에 트래핑합니다. ACE 는 방식이가 비활성화되면 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 지점에이 스위치에서 SSDP 광고 메시지를받는 빈도를 알리는 데 사용됩니다. 컨트롤 포인트가 지속 시간 내에 아무런 메시지도받지 못하면 스위치가 더 이상 존재하지 않는다고 생각할 것입니다. UDP 의 신뢰할 수없는 특성 때문에 표준에서 광고 지속 시간의 절반 이하로 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

Save : 저장버튼 클릭해야한다.

Reset : 이전에 저장된 값으로 되돌리면 클릭해야한다

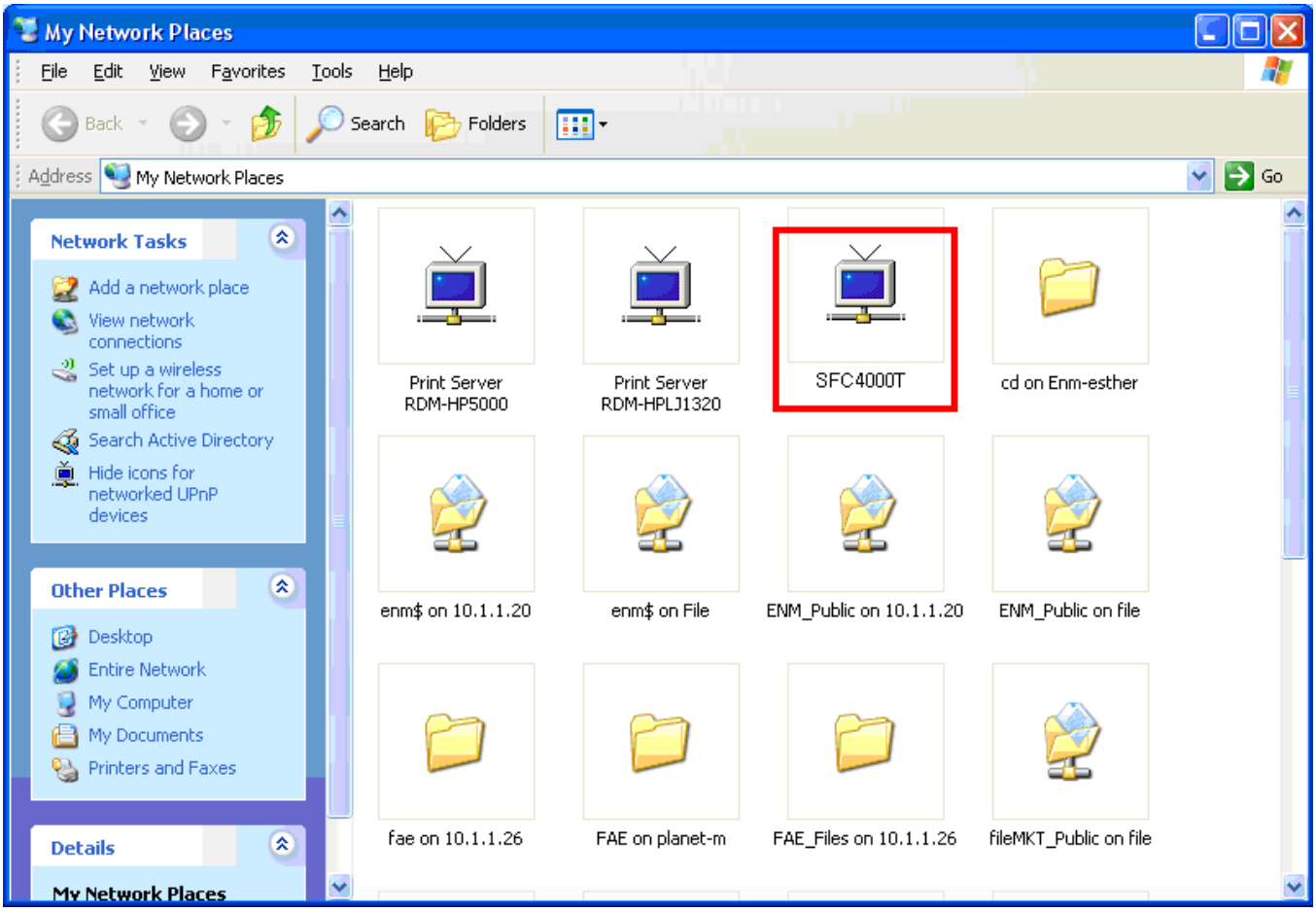


그림 4-2-10 UPnP 장치가 보여진다. 위치는 Windows My Network Places

3.2.8 DHCP Relay

이 페이지에서 DHCP 릴레이를 구성 하십시오. DHCP 릴레이는 동일한 서브넷 도메인에 있지 않을 때 클라이언트와 서버간에 DHCP 메시지를 전달하고 전송하는 데 사용됩니다.

DHCP -82 옵션은 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 제거할 수있게합니다. DHCP 서버는이 정보를 사용하여 IP 주소 또는 기타 할당 정책을 구현할 수 있습니다. 특히이 옵션은 두 가지 하위 옵션을 설정하여 작동합니다.

- 순환 ID (옵션 1)
- 원격 ID (옵션 2).

.순환 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"의 매개 변수는 VLAN ID 를 나타내는 처음 두 바이트입니다. "module_id"매개 변수는 모듈 ID 의 세 번째 바이트입니다 (독립 실행 형 스위치에서는 항상 0, 스택 가능 스위치에서는 스위치 ID 를 의미 함). "port_no"의 매개 변수는 네 번째 바이트이며 Port 번호를 의미합니다.

원격 ID 의 길이는 6 바이트이며 값은 DHCP 릴레이 에이전트의 MAC 주소와 동일합니다. 그림 4-2-11 의 DHCP Relay Configuration (DHCP 릴레이 구성) 화면이 나타납니다.

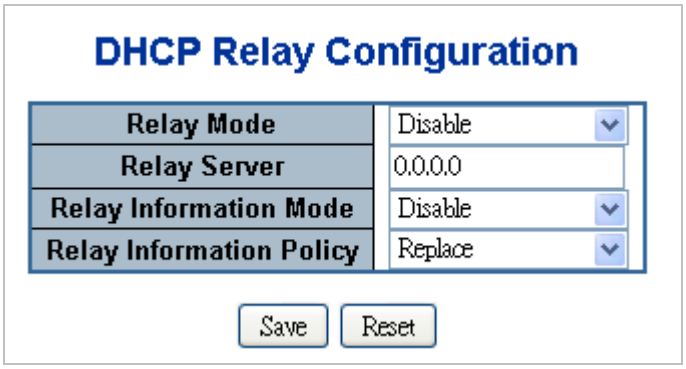


그림 4-2-11 DHCP Relay 구성 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Relay mode	DHCP 릴레이 방식 작업을 나타냅니다. 가능한 방식은는 다음과 같습니다. 활성화 : DHCP 릴레이 방식 작동을 활성화합니다. DHCP 릴레이 방식 작업을 활성화하면 에이전트는 동일한 서브넷 도메인에 있지 않을 때 클라이언트와 서버간에 DHCP 메시지를 전달하고 전달합니다. 그리고 DHCP 브로드 캐스트 메시지는 고려 된 보안을 위해 범람하지 않을 것입니다. 비활성화 됨 : DHCP 릴레이 방식 작동을 비활성화합니다.
• Relay 서버	DHCP 릴레이 서버 IP 주소를 나타냅니다. DHCP 릴레이 에이전트는 클라이언트와 서버가 동일한 서브넷 도메인에 있지 않을 때 DHCP 메시지를 전달하고 전달하는 데 사용됩니다.
• Relay Information policy	DHCP 릴레이 정보 방식 옵션 작업을 나타냅니다. 가능한 방식은는 다음과 같습니다. 활성화 : DHCP 릴레이 정보 방식 작동을 활성화합니다. DHCP 릴레이 정보 방식 작동을 활성화하면 에이전트는 DHCP 서버로 전달할 때 DHCP 메시지에 특정 정보 (option82)를 삽입하고 DHCP 클라이언트로 전송할 때 DHCP 메시지에서 해당 정보를 제거합니다. DHCP 릴레이 작동 방식에서만 작동합니다. 비활성화 됨 : DHCP 릴레이 정보 방식 작동을 비활성화합니다.
• Relay information Policy	DHCP 릴레이 정보 옵션 정책을 나타냅니다. DHCP 릴레이 정보 방식

	작동을 활성화하면 에이전트가 이미 릴레이 에이전트 정보가 들어있는 DHCP 메시지를 수신합니다. 정책을 집행 할 것입니다. DHCP 릴레이 정보 작동 방식에서만 작동합니다. 가능한 정책은 다음과 같습니다. 교체 : 이미 포함되어있는 DHCP 메시지를 받으면 원본 릴레이 정보를 교체하십시오. 유지 : 이미 포함되어있는 DHCP 메시지를 받으면 원본 릴레이 정보를 유지하십시오

버튼

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

3.2.9 DHCP Relay 통계

이 페이지는 DHCP 릴레이에 대한 통계를 제공합니다. 그림 4-2-12 의 DHCP Relay 통계화면이 나타납니다.

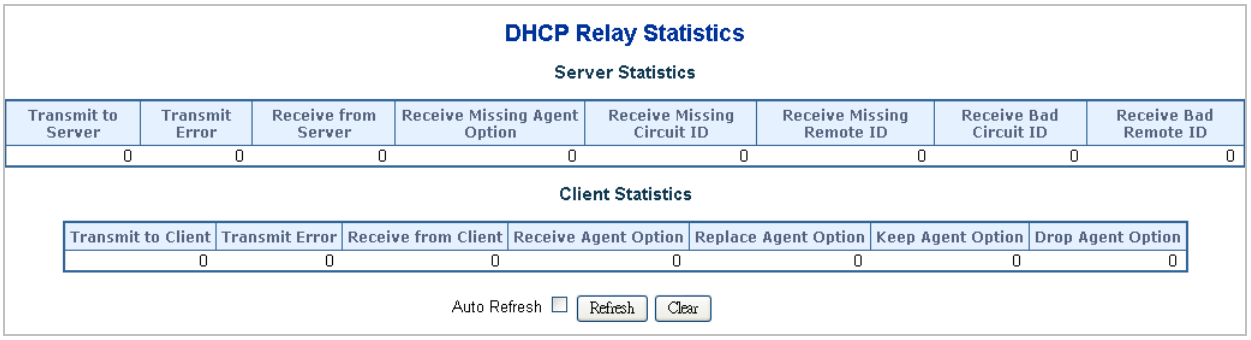


그림 4-2-12 DHCP Relay 통계 페이지 스크린샷

이 페이지는 다음을 포함해 나타냅니다.

서버 통계

Object	Description
• Transmit to 서버	클라이언트에서 서버로 중계 된 패킷 번호
• Transmit Error	클라이언트에 패킷을 보내는 동안 발생하는 오류의 패킷 번호
• Receive from 서버	서버로부터 패킷을 수신 한 패킷 수
• Receive Missing Agent Option	에이전트 정보 옵션없이 패킷을 수신 한 패킷 번호입니다.
• Receive Missing Circuit ID	회선 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.

Client 통계

Object	Description
• Transmit to Client	서버에서 클라이언트로 패킷을 전달한 패킷 번호입니다.
• Transmit Error	서버로 패킷을 보내는 중 오류가 발생한 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 Optin	릴레이 에이전트 정보 옵션을 사용하여 수신 된 패킷을 보관 한 패킷 번호입니다.
• Drop Agent Option	릴레이 에이전트 정보 옵션을 사용하여 수신 패킷을 삭제 한 패킷 번호입니다.

버튼

Auto-refresh : 선택한경우 페이지를 3 초마다 자동으로 새로 고칩니다...

Refresh: 즉시 페이지를 새로 고칩니다.

Clear: 통계 자료를 초기화합니다.

3.2.10 CPU Load

이 페이지는 SVG 그래프를 사용하여 CPU 로드를 표시합니다.하중은 마지막 100ms, 1sec 및 10 초 간격으로 평균 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 4-2-13 의 CPU Load 화면이 나타납니다.

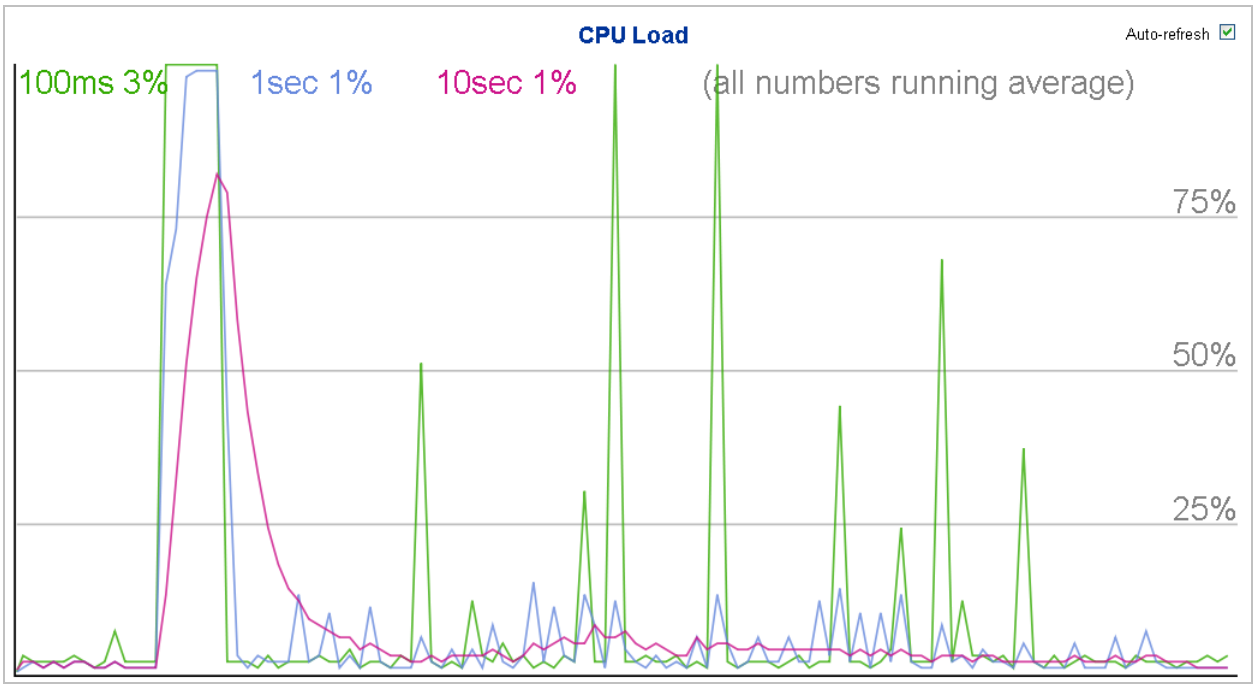


그림 4-2-13 CPU Load 설정 화면

버튼

Auto-refresh : 선택한경우 페이지를 3 초마다 자동으로 새로 고칩니다...

Note

브라우저가이 페이지의 내용을 변경할 수 없으면 Adobe SVG 도구를 다운로드하여 컴퓨터에 설치하십시오.

3.2.11 시스템 Log

스위치 시스템 로그 정보는 여기에 나와 있습니다. 그림 4-2-14 의 시스템 로그 화면이 나타납니다.

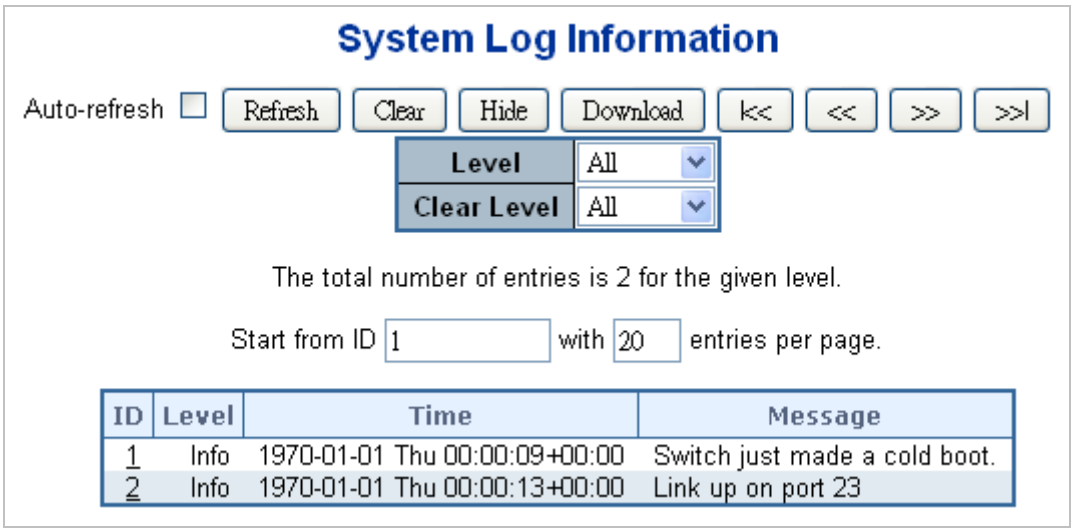


그림 4-2-14 시스템 로그화면 안내

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• ID	시스템 로그 항목 ID(>=1)
• Level	시스템 로그 항목 레벨 설정. 지원레벨 유형 Info : 시스템 로그의 정보 레벨. 경고 : 시스템 로그의 경고 수준입니다. 오류 : 시스템 로그의 오류 수준입니다. 전체 : 모든 레벨.
• Clear Level	시스템 로그 항목 레벨을 지우는 것. 지원레벨 유형 Info : 시스템 로그의 정보 레벨. 경고 : 시스템 로그의 경고 수준입니다. 오류 : 시스템 로그의 오류 수준입니다. 전체 : 모든 레벨.
• Time	시스템 로그 항목의 시간
• Message	시스템 로그 항목의 메시지

버튼

Auto-refresh : 선택한경우 페이지를 3 초마다 자동으로 새로 고칩니다...

Refresh: 현재 항목 ID 부터 시스템 로그 항목을 업데이트합니다.

Clear: 선택한로그 항목을 플러시합니다.

Hide: 선택한 로그 항목음 숨깁니다.

Download: 선택한 로그 항복을 다운로드 합니다

k<: 업데이트한 시스템로그항목에 제일처음 ID 로 돌아갑니다

<< : 업데이트한 시스템로그항목에 현재 보이는곳에서 마지막으로 이동합니다.

>> : 업데이트한 시스템로그항목에 현재 보이는곳에서 마지막으로 시작한곳으로 이동합니다.

>>| : 업데이트한 시스템로그항목에 제일 마지막 ID 로 이동합니다

3.2.12 세부 사항 ed Log

스위치 시스템의 자세한 로그 정보는 여기에 나와 있습니다. 그림 4-2-15 의 상세 로그 화면이 나타납니다.

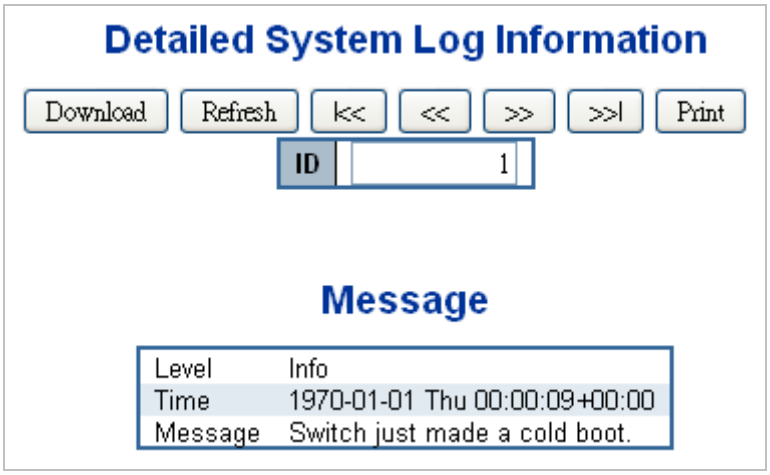


그림 4-2-15 세부 사항 ed Log 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• ID	시스템 로그 항목의 ID (> = 1).
• Message	시스템 로그 항목의 메시지.

버튼

Download : 시스템 로그 항목을 현재 항목 ID 로 다운로드하십시오.

Refresh : 시스템 로그 항목을 현재 항목 ID 로 업데이트합니다.

|<< : 시스템 로그 항목을 사용가능 한 첫번째 ID 항목으로 업데이트합니다.

<< : 시스템 로그 항목을 이전에 사용가능한 ID 항목으로 업데이트합니다.

>> : 시스템 로그 항목을 다음에 사용가능한 ID 항목으로 업데이트합니다.

>>| : 시스템 로그 항목을 마지막으로 사용 가능한 ID 항목으로 업데이트합니다

Print: 시스템 로그 항목을 현재 항복 ID 로 인쇄하십시오

3.2.13 Remote Syslog

페이지에서 원격 syslog 를 구성 하십시오. 그림 4-2-16 의 Remote Syslog 화면이 나타납니다.

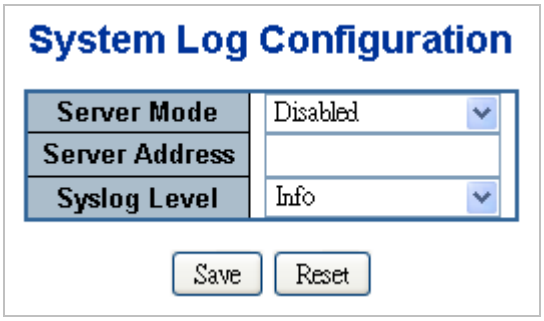


그림 4-2-16 원격 시스로그 캡처화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Mode	서버 방식 조작을 수행합니다. 방식 작업이 활성화되면 syslog 메시지가 syslog 서버로 전송됩니다. syslog 프로토콜은 UDP 통신을 기반으로하며 UDP Port 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 방식은는 다음과 같습니다. 활성화 : 원격 syslog 방식 작동을 활성화합니다. 비활성화 됨 : 원격 syslog 방식 작업을 비활성화합니다.
• Syslog Seruer 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 방식은는 다음과 같습니다. 정보 : 정보, 경고 및 오류를 보냅니다. 경고 : 경고 및 오류를 보냅니다. 오류 : 오류를 보냅니다.

버튼

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

3.2.14 SMTP 구성

이 페이지는 SMTP 를 쉽게 접하도록합니다 스위치를 구성 하고 4-2-17 의 SMTP 구성 화면이 나타납니다.

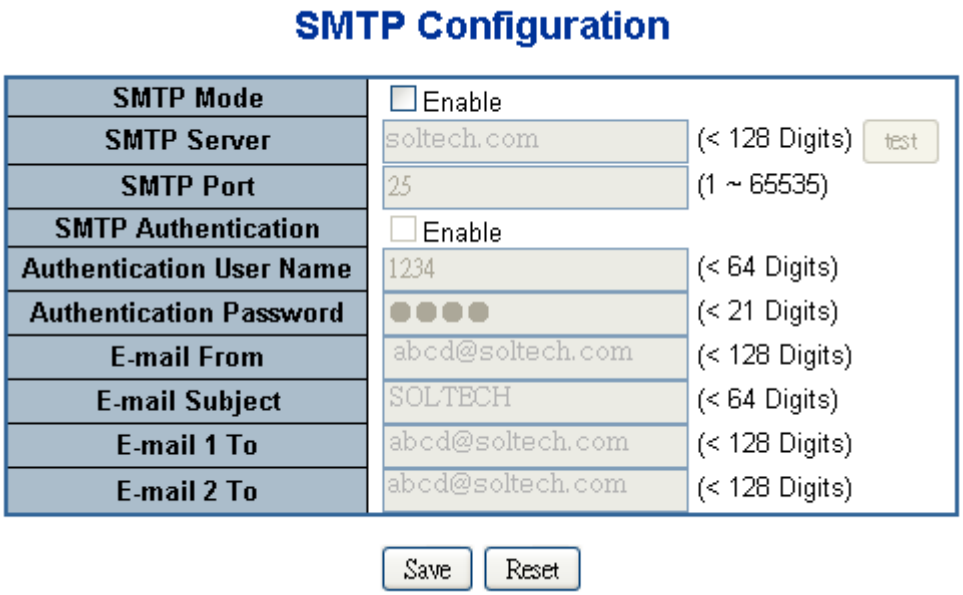


그림 4-2-17 SMTP 구성 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• SMTP Mode	이 스위치에서 SMTP 를 사용할지 여부를 제어합니다.
• SMTP 서버	SMTP 서버의 SMTP 서버 이름 또는 IP 주소를 입력하십시오.
• SMTP Port	SMTP 서비스의 Port 번호를 설정합니다.
• SMTP Authentication	SMTP 인증 사용 여부 제어 전자 메일을 보낼 때 인증이 필요한 경우.
• Authentication User Name	인증이 사용 가능한 경우 SMTP 서버의 사용자 이름을 입력하십시오.
• Authentication Password	인증이 사용 가능한 경우 SMTP 서버의 암호를 입력하십시오.
• E-mail From	보낸 사람의 전자 메일 주소를 입력하십시오. 이 주소는 답장 전자 메일에 사용됩니다.
• E-mail Subject	전자 메일의 제목을 입력하십시오.

• E-mail 1 To • E-mail 2 To	수신자의 이메일 주소를 입력하십시오.

버튼

test: 테스트 메일을 메일 서버로 보내이 계정을 사용할 수 있는지 확인하십시오.

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

3.2.15 Web 펌웨어 업그레이드

스위치를 제어하는 펌웨어의 업데이트를 용이하게 합니다.

그림 4-2-18 웹페이지 펌웨어 업그레이드 화면

펌웨어 업그레이드 화면을 열려면 실행하십시오 :

1. 시스템 -> 웹 펌웨어 업그레이드를 클릭하십시오.
2. 펌웨어 업그레이드 화면이 그림 4-2-18 과 같이 표시됩니다.
3. 메인 페이지의 "Browse"버튼을 클릭하면, 시스템이 펌웨어를 선택하기 위해 파일 선택 메뉴를 팝업합니다.
4. 펌웨어를 선택한 다음 "Upload"을 클릭하면 소프트웨어 업로드 진행 상태가 파일 업로드 상태를 표시합니다.
5. 일단 소프트웨어가 시스템에 성공적으로 로드됩니다. 다음 화면이 나타납니다. 시스템은 재부팅 후 새 소프트웨어를로드합니다.

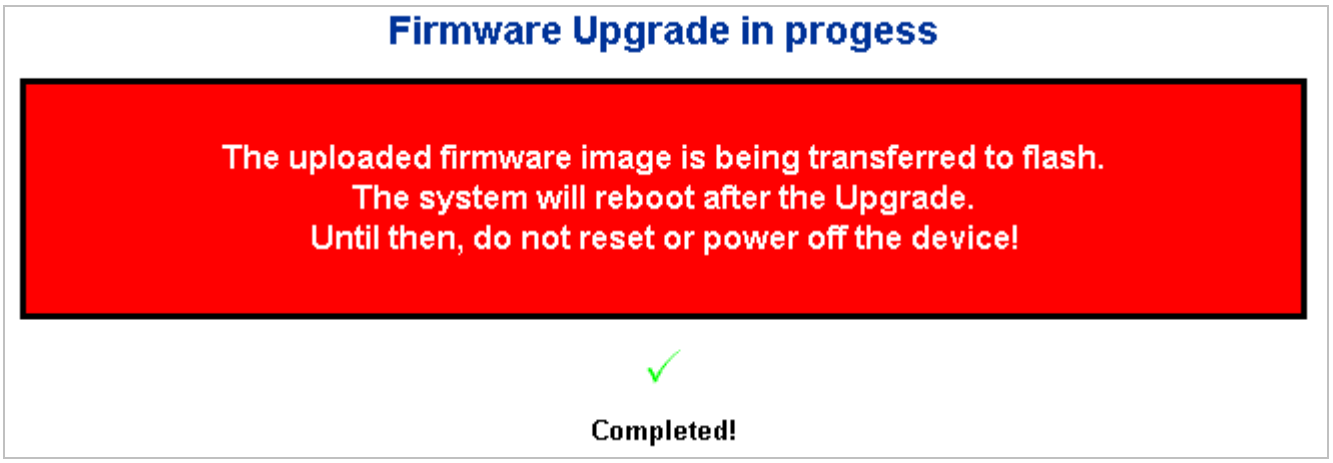


그림 4-2-19 소프트웨어를 성공적으로 업데이트 한 모습

Note

업데이트 진행이 완료 될 때까지 관리되는 스위치의 전원을 끄지 마십시오.

Note

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

3.2.16 TFTP 펌웨어 업그레이드

펌웨어 업그레이드 (펌웨어 업그레이드) 페이지는 사용자가 네트워크의 TFTP 서버에서 Managed 스위치 펌웨어를 업데이트 할 수있는 기능을 제공합니다. 업데이트하기 전에 TFTP 서버를 준비하고 펌웨어 이미지가 TFTP 서버에 있는지 확인하십시오. 그림 4-2-20 의 TFTP 펌웨어 업그레이드 화면이 나타납니다.

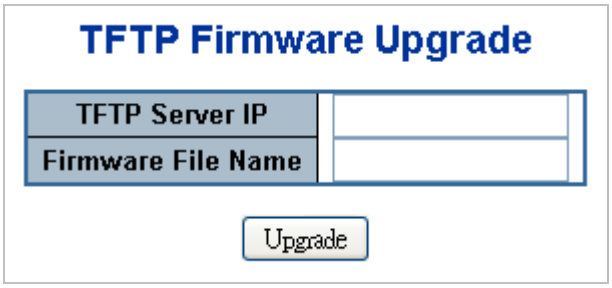


그림 4-2-20 TFTP Firmware Update 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• TFTP 서버 IP	TFTP 서버 IP 주소.
• Firmware File Name	펌웨어 이미지의 이름. (최대 길이 : 24 자)

버튼

Upload : 펌웨어 업그레이드를 하시려면 클릭하세요 .

Note

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

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

3.2.17 구성 복원

이 기능을 사용하면 관리 대상 스위치의 현재 구성 을 로컬 관리 스테이션에 백업하고 다시로드 할 수 있습니다. 그림 4-2-21 의 구성 백업 화면이 나타납니다.

그림 4-2-21 구성 Save 설정 화면

스위치 구성 을 저장 /보기 또는로드 할 수 있습니다. 구성 파일은 태그 계층이있는 XML 형식입니다.

Header tags:	<?xml version="1.0"?> and <구성 >. 이 태그는 필수이며 파일의 시작 부분에 있어야합니다.
Section tags:	<platform>, <global> and <스위치>. 플랫폼 섹션은 첫 번째 섹션 태그 여야하며이 섹션에는 올바른 플랫폼 ID 및 버전이 포함되어야합니다. 전역 섹션은 선택적이며 특정 스위치 Port 와 관련이없는 구성 을 포함합니다. 스위치 섹션은 선택 사항이며 특정 스위치 Port 와 관련된 구성 을 포함합니다
Module tags:	<ip>, <mac>, <Port> etc. 이 태그는 구성 의 특정 부분을 포함하는 모듈을 식별합니다.
Group tags:	<Port_table>, <vlan_table > etc. 이 태그는 일반적으로 테이블 인 매개 변수 그룹을 식별합니다.
Parameter tags:	<mode>, <entry> etc. 이 태그는 특정 섹션, 모듈 및 그룹에 대한 매개 변수를 식별합니다. <entry> 태그는 테이블 항목에 사용됩니다.

구성 매개 변수는 속성 값으로 표시됩니다. 스위치에서 구성 을 저장할 때 구문 설명을 포함한 전체 구성 이 파일에 포함됩니다. 그런 다음 파일을 편집기를 사용하여 수정하고 스위치에로드 할 수 있습니다.

아래의 예는 MAC 주소 에이징 시간 및 Port 당 학습 방식의 구성 만 포함하는 작은 구성 파일을 보여줍니다. 이 파일을로드 할 때 포함 된 매개 변수 만 변경됩니다. 즉, 연령대가 200 으로 설정되고 학습 방식이가 자동으로 설정됩니다

설정 저장 1. "Save Configuration"버튼을 눌러 관리자 워크 스테이션에 현재 구성 을 저장하십시오. 그림 4-2-22 및 4-2-23의 다음 화면이 나타납니다

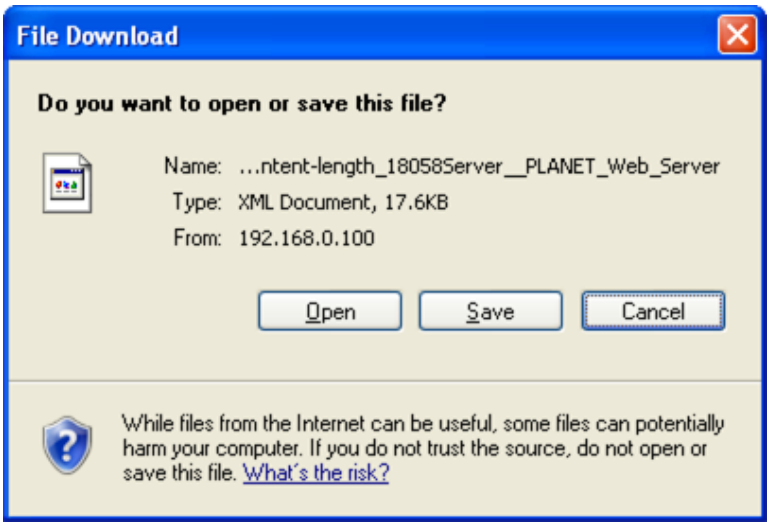


그림 4-2-22 File Download screen

관리 워크 스테이션에서 파일 저장 경로를 선택하십시오.

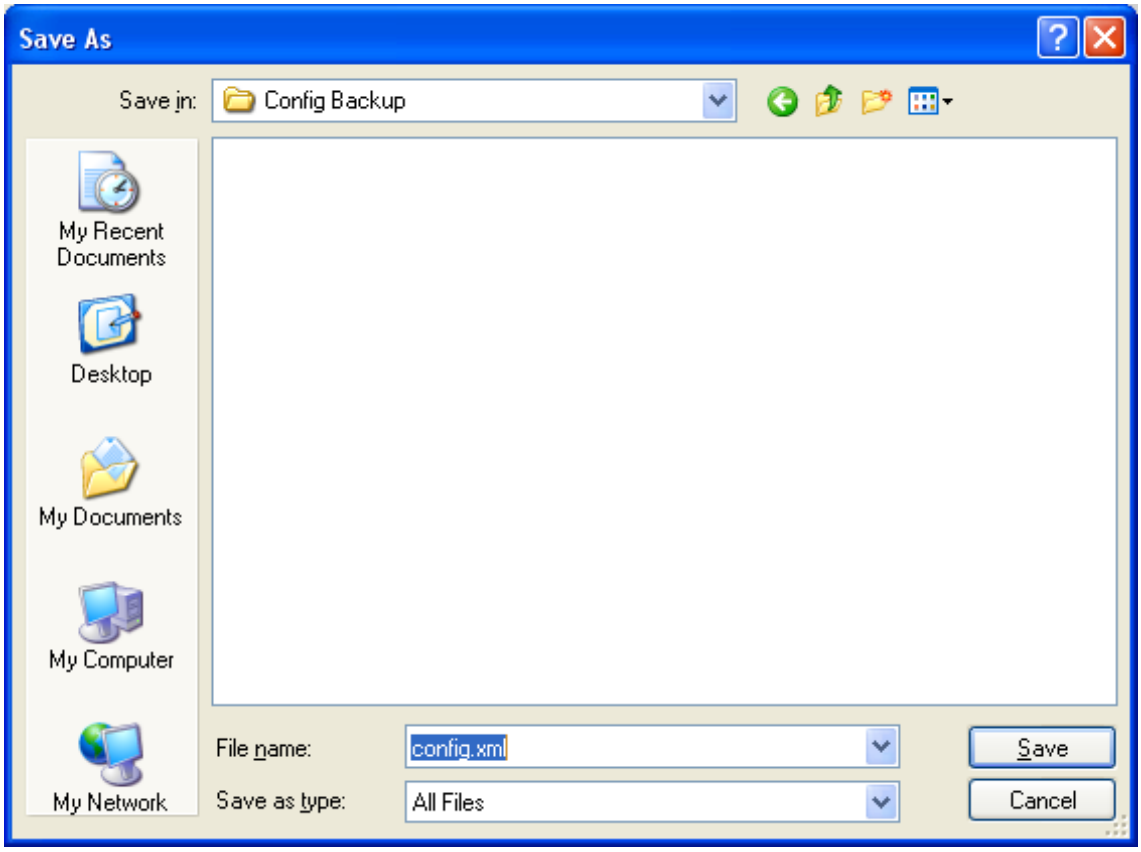


그림 4-2-23 File save screen

3.2.18 구성파일 업로드

이 기능을 사용하면 관리 대상 스위치의 현재 구성 을 로컬 관리 스테이션에 백업하고 다시로드 할 수 있습니다. 그림 4-2-24 의 구성 Upload 화면이 나타납니다.

그림 4-2-24 구성 Upload 설정 화면

■ 구성 Upload

1. 메인 페이지의 "Browse"버튼을 클릭하면 파일 선택 메뉴가 팝업되어 저장된 구성 을 선택할 수 있습니다

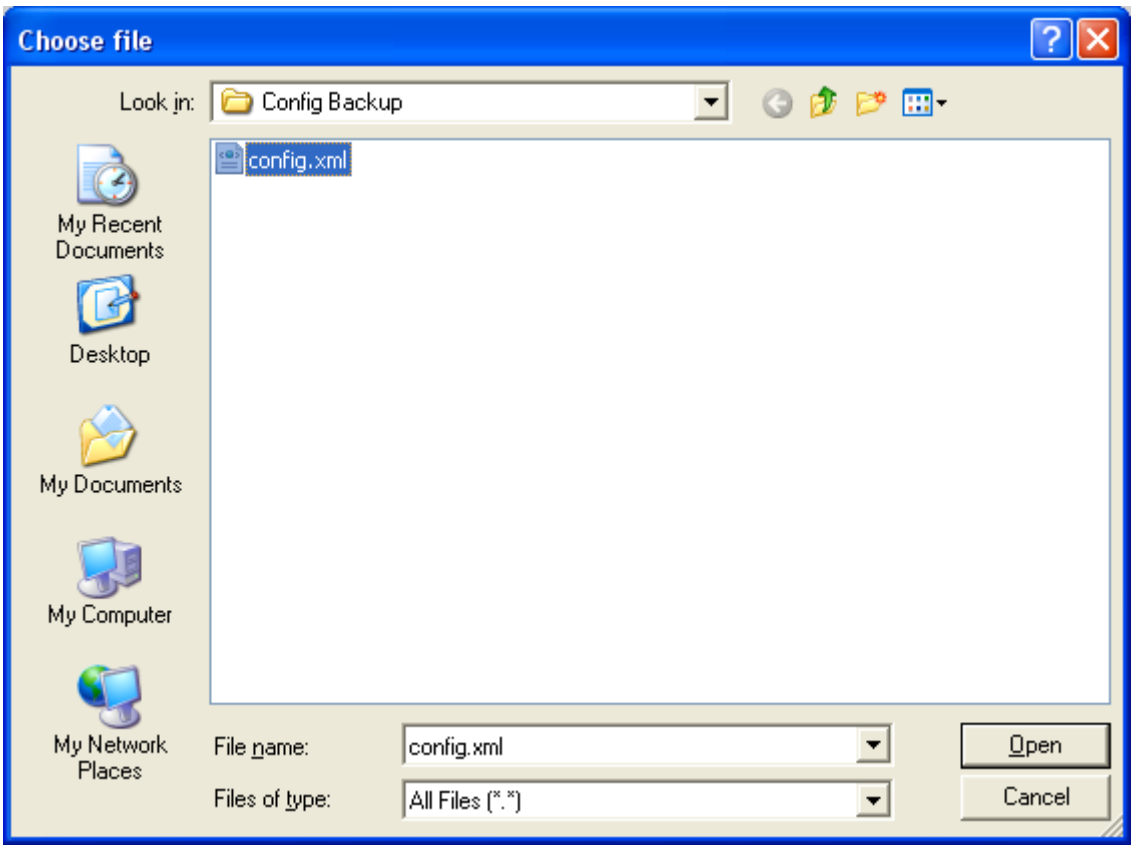


그림 4-2-25 팝업메뉴가 나오면 윈도우 파일을 선택한다

2. 구성 파일을 선택한 다음 "Upload"을 클릭하면 브라우저 하단에 업로드 상태가 표시됩니다.

3. 아래로 이동하면 기본 화면에 "전송 완료"가 나타납니다.

3.2.19 Image Select

이 페이지는 장치의 활성 및 대체 (백업) 펌웨어 이미지에 대한 정보를 제공하며 대체 이미지로 되돌릴 수 있습니다. 웹 페이지에는 활성 및 대체 펌웨어 이미지에 대한 정보가있는 두 개의 표가 표시됩니다. 그림 4-2-26 의 이미지 선택 화면이 나타납니다.

1. 활성 펌웨어 이미지가 대체 이미지 인 경우 "활성 이미지"테이블 만 표시됩니다. 이 경우 대체 이미지 활성화 버튼도 비활성화됩니다.
2. 대체 이미지가 활성화 된 경우 (기본 이미지 손상 또는 수동 개입으로 인해) 장치에 새 펌웨어 이미지를 업로드하면 기본 이미지 슬롯이 자동으로 사용되어 활성화됩니다. 3. 펌웨어 버전 및 날짜 정보는 이전 펌웨어 릴리스의 경우 비어있을 수 있습니다. 이것은 오류를 구성하지 않습니다.

그림 4-2-26 소프트웨어 이미지 선택 페이지 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Image	펌웨어 이미지의 플래시 색인 이름입니다. 주 (선호) 이미지의 이름은 image 이며, 대체 이미지의 이름은 image.bk 입니다.
• Version	펌웨어 이미지 버전입니다.
• Date	펌웨어 생성된 날짜입니다

버튼

Activate Alternate Image 이 버튼은 시스템에 따라 비활성화 될 수 있습니다.

Cancel :백업 이미지 활성화를 취소하십시오. 이 페이지에서 다른 곳으로 이동합니다.

3.2.20 공장 초기화

이 페이지에서 스택 스위치의 구성을 재설정 할 수 있습니다. IP 구성 만 유지됩니다. 새로운 구성을 즉시 사용할 수 있으므로 다시 시작할 필요가 없습니다. 그림 4-2-27 의 Factory Default 화면이 나타납니다.

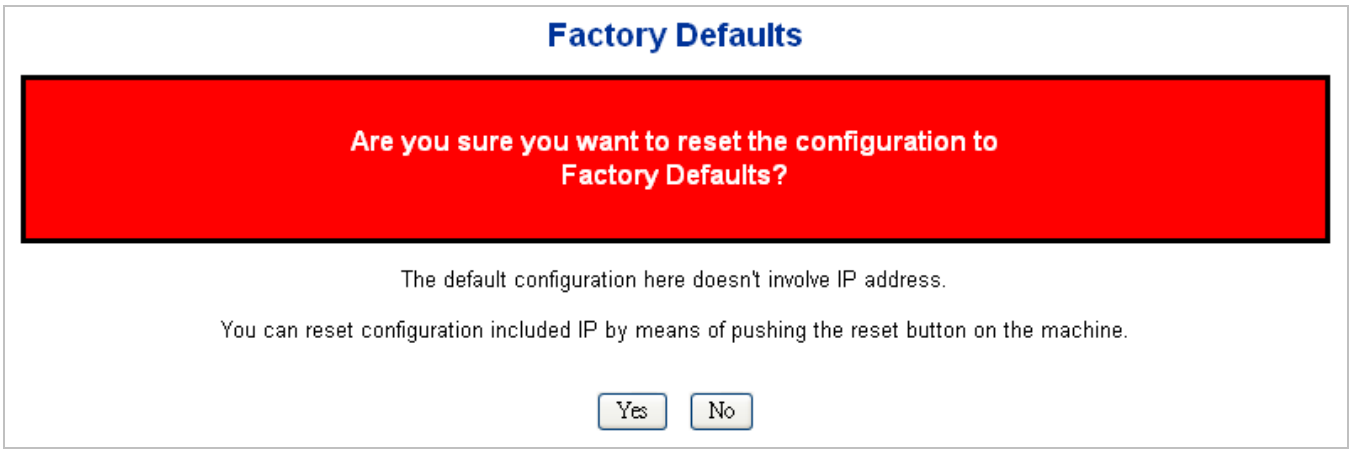


그림 4-2-27 Factory Default 설정 화면

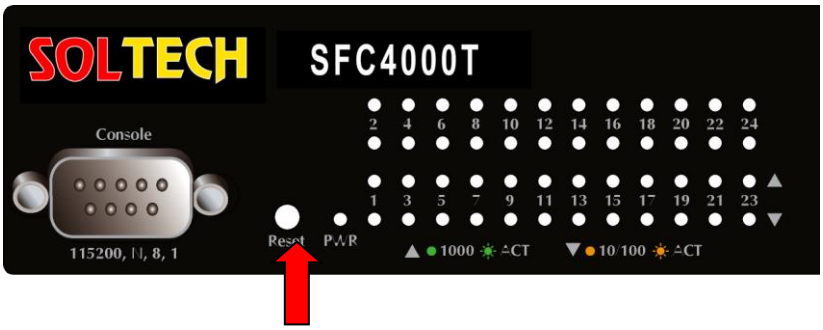
버튼

Yes : 구성을 공장 기본값으로 재설정하려면 클릭하십시오.

No : 구성을 재설정하지 않고 Port State (Port 상태) 페이지로 돌아가려면 누릅니다.

관리 대상 스위치를 공장 초기화시 기본 설정으로 재설정하려면 전면 패널에서 하드웨어 재설정 버튼을 약 10 초 정도 누릅니다. 장치가 재부팅 된 후 관리 웹 인터페이스를 192.168.0.xx 의 동일한 서브넷에 로그인 할 수 있습니다

Note



Hardware Reset button

3.2.21 시스템 Reboot

Reboot (재부팅) 사용하면 원격 위치에서 장치를 재부팅 할 수 있습니다. Reboot 버튼을 누르면 약 60 초 후에 WEB 인터페이스에 로그인, 그림 4-2-28 의 System Reboot 화면이 나타납니다.

그림 4-2-28 시스템 Reboot 설정 화면

버튼

Yes: 시스템을 재부팅하려면 클릭하시오

No: 시스템을 재부팅하지 않고 Port 상태 페이지로 돌아가려면 클릭하십시오

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

3.3 Simple Network Management Protocol(SNMP)

3.3.1 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.

◦ 네트워크 관리 스테이션 (Network Management Station, NMS) : 때로는 콘솔이라고 하는 이 장치는 네트워크 요소를 모니터링하고 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.

◦ 에이전트 : 에이전트는 네트워크 요소에 상주하는 소프트웨어 모듈입니다. 네트워크 요소가 수신 한 오류 패킷 수와 같은 관리 정보를 수집하고 저장합니다.

◦ 관리 정보베이스 (MIB) : MIB 는 가상 정보 저장소에있는 관리되는 개체의 모음입니다. 관련 관리 객체의 컬렉션은 특정 MIB 모듈에서 정의됩니다.

◦ 네트워크 관리 프로토콜 : 관리 프로토콜은 에이전트와 NMS 간에 관리 정보를 전달하는 데 사용됩니다. SNMP 는 인터넷 커뮤니티의 사실상 표준 관리 프로토콜입니다.

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

◦ Get - NMS 가 에이전트에서 객체 인스턴스를 검색 할 수 있습니다.

◦ Set - NMS 가 상담원 내의 개체 인스턴스 값을 설정할 수 있게합니다.

◦ 트랩 (Trap) - NMS 에 비동기 적으로 이벤트를 알리기 위해 에이전트에서 사용합니다. SNMPv2 트랩 메시지는 SNMPv1 트랩 메시지를 대체하도록 설계되었습니다.

◦ SNMP 커뮤니티 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. 쓰기 = 개인 읽음 = 공개

SNMP메뉴를 사용하여 중앙 관리 EVC(ManagedEquipment)의 SNMP기능을 표시하거나 구성합니다. 이 섹션에는 다음 항목이 포함되어 있습니다.

시스템 구성이 페이지에서 SNMP 구성.

이 페이지에서 트랩 구성 SNMP 트랩을 구성하십시오.

시스템 안내 시스템 안내는 여기에서 제공됩니다.

SNMPv3 커뮤니티는 이 페이지에서 SNMPv3 커뮤니티 테이블을 구성합니다.

SNMPv3 사용자는 이 페이지에서 SNMPv3 사용자 테이블을 구성합니다.

SNMPv3 그룹은 이 페이지에서 SNMPv3 그룹 테이블을 구성합니다.

SNMPv3 보기는 이 페이지에서 SNMPv3 보기 테이블을 구성합니다.

SNMPv3 은 이 페이지에서 SNMPv3 접근 테이블을 구성합니다

3.3.2 SNMP System 구성

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

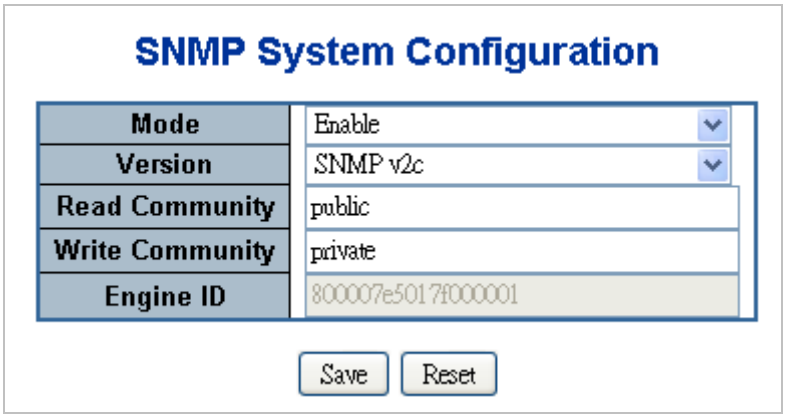


그림 4-3-1 SNMP 시스템 구성 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Mode	SNMP 방식 작업을 나타냅니다. 가능한 방식은는 다음과 같습니다. 활성화 : SNMP 방식 작동을 활성화합니다. 비활성화 됨 : SNMP 방식 작동을 비활성화합니다.
• Version	SNMP 지원 버전을 나타냅니다. 가능한 버전은 다음과 같습니다. SNMP v1 : SNMP 지원 버전 1 을 설정합니다. SNMP v2c : SNMP 지원 버전 2c 를 설정합니다. SNMP v3 : SNMP 지원 버전 3 을 설정합니다.
• Read Community	ISNMP 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 원본 주소를 사용하여 원본 서브넷을 제한 할 수 있습니다.
• Write Community	SNMP 에이전트에 접근을 허용하는 커뮤니티 쓰기 접근 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 문자열에 추가로 소스 주소의 특정 범위를 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.

3.3.3 SNMP Trap 구성

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

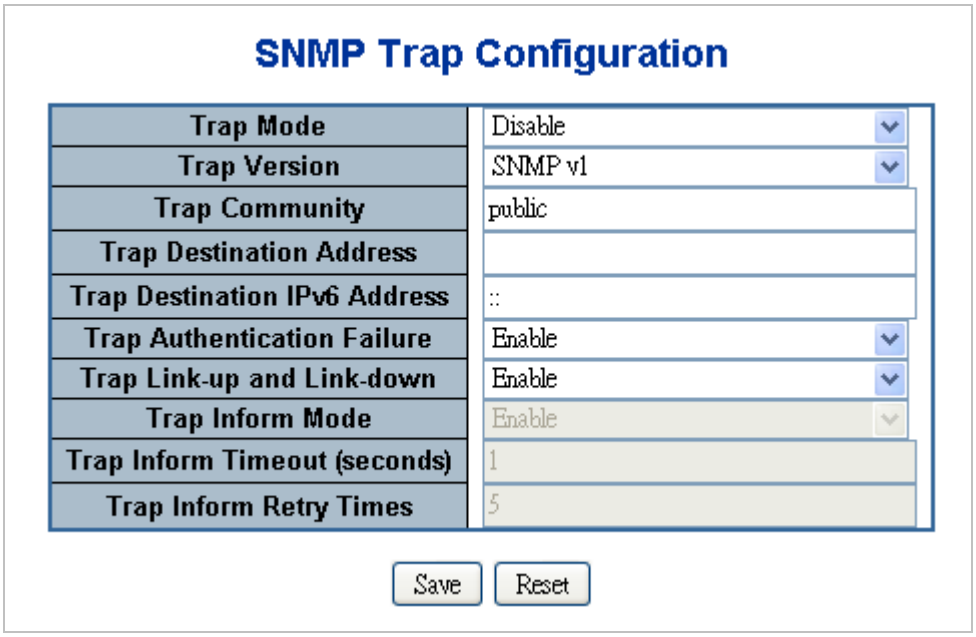


그림 4-3-2 SNMP 트랩 구성 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Trap Mode	SNMP 트랩 방식 작동을 나타냅니다. 가능한 방식은는 다음과 같습니다. 활성화 : SNMP 트랩 방식 작동을 활성화합니다. 비활성화 됨 : SNMP 트랩 방식 작동을 비활성화합니다.
• Trap Version	SNMP 트랩 지원 버전을 나타냅니다. 가능한 버전은 다음과 같습니다. SNMP v1 : SNMP 트랩 지원 버전 1 을 설정합니다. SNMP v2c : SNMP 트랩 지원 버전 2c 를 설정합니다. SNMP v3 : SNMP 트랩 지원 버전 3 을 설정합니다.
• Trap Community	SNMP 트랩 패킷을 보낼 때 커뮤니티 접근 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. 점으로 구분 된 십진수 표기법 ('x.y.z.w')으로 유효한 IP 주소를 허용합니다. 또한 유효한 호스트 이름을 허용합니다. 유효한 호스트 이름은 알파벳 (A-Za-z), 숫자 (0-9), 점 (.), 대시 (-)로 그려지는 문자열입니다. 공백은 허용되지 않으며 첫 번째 문자는 알파 문자 여야하며 첫 번째 문자와 마지막 문자는 점이나 대시가 아니어야합니다.
• Trap Destination IPv6 Address	SNMP 트랩 대상 IPv6 주소를 나타냅니다. IPv6 주소는 각 필드 (:)를 구분하는 콜론 (:)을 사용하여 최대 네 개의 16 진수로 이루어진 8 개의 필드로 표시된 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. 하지만 한 번만 나타날 수 있습니다. 또한 합법적으로 유효한 IPv4 주소를 나타낼 수도 있습니다. 예 : ':: 192.1.2.34'.
• Trap Authentication Failure	SNMP 엔티티가 인증 실패 트랩을 생성하도록 허용되었음을 나타냅니다. 가능한 방식은는 다음과 같습니다. 활성화 Enabled : SNMP 트랩 인증 실패를 사용합니다. 비활성화 됨 : SNMP 트랩 인증 실패를 비활성화합니다.
• Trap Link-up and Link-down	SNMP 트랩 링크 업 및 링크 다운 방식 작업을 나타냅니다. 가능한 방식은는 다음과 같습니다. Enabled (사용) : SNMP 트랩 링크 업 및 링크 다운 방식 작동을 활성화합니다. 비활성화 됨 : SNMP 트랩 링크 업 및 링크 다운 방식 작동을 비활성화합니다.
• Trap Inform Mode	SNMP 트랩 정보 방식 작업을 나타냅니다. 활성화 : SNMP 트랩 알림 방식 작동을 활성화합니다. 비활성화 됨 : SNMP 트랩 알림 방식 작동을 비활성화합니다.

• Trap Inform Timeout (seconds)	SNMP 트랩 정보 시간 초과를 나타냅니다. 허용되는 범위는 0 ~ 2147 입니다.
• Trap Inform Retry Times	재시도 시간을 알리는 SNMP 트랩을 나타냅니다. 허용되는 범위는 0 에서 255 까지입니다.
• Trap Probe Security Engine ID	SNMP 트랩 프로브 보안 엔진 ID 작동 방식을를 나타냅니다. 가능한 값은 다음과 같습니다. 사용 : SNMP 트랩 프로브 보안 엔진 ID 작동 방식을를 활성화합니다. 사용 안 함 : SNMP 트랩 프로브 보안 엔진 ID 작동 방식을를 사용하지 않습니다.
• 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.

버튼

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

3.3.4 SNMP 시스템안내

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

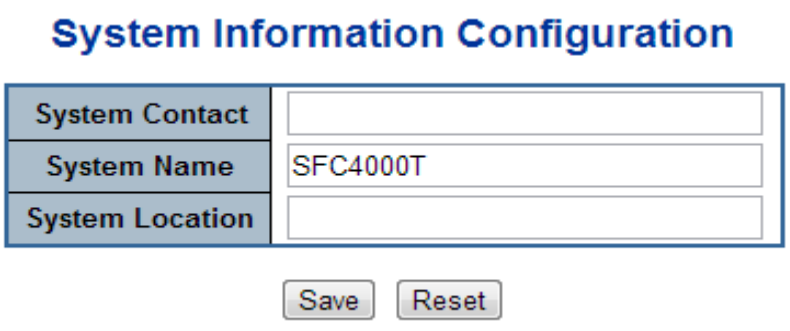


그림 4-3-3 시스템안내 설정화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• 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.

버튼

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

3.3.5 SNMPv3 구성

3.3.5.1 SNMPv3 Communities

이 페이지에서 SNMPv3 커뮤니티 표를 구성하십시오. 항목 색인 키는 커뮤니티입니다. 그림 4-3-4 의 SNMPv3 Communities 화면이 나타납니다.

그림 4-3-4 SNMPv3 Communities 구성 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• delete	항목을 삭제하려면 선택하세요, 다음엔 저장되어 삭제된다.
• 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 액세스 소스 주소 마스크를 나타냅니다.

버튼

Add New Entry: 새로운 커뮤니티엔트리를 추가하려면 클릭한다.

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

3.3.5.2 SNMPv3 users

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

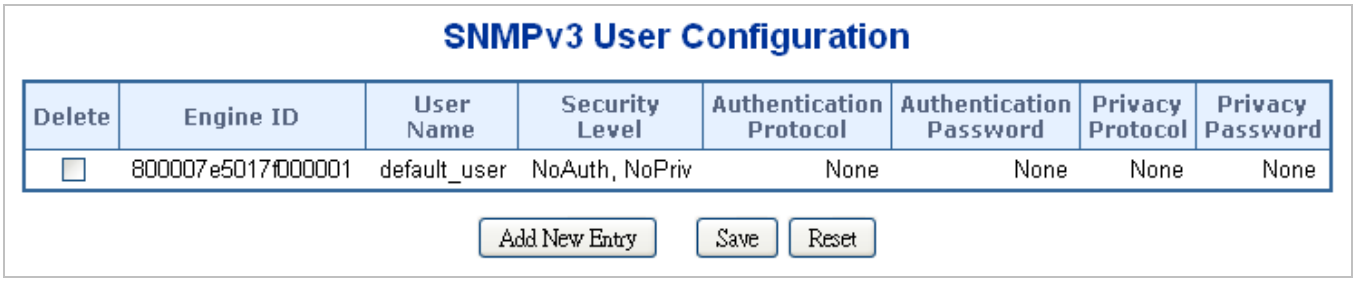


그림 4-3-5 SNMPv3 users 구성 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Delete	항목을 제거하려면 선택하고 저장하는동안 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.
• User Name	이 항목이 속해야하는 사용자 이름을 식별하는 문자열. 허용되는 문자열 길이는 1 에서 32 이며 허용되는 내용은 33 에서 126 사이의 ASCII 문자입니다.
• Security Level	이 엔트리가 속해야하는 보안 방식을를 나타낸다. 가능한 보안 방식은는 다음과 같습니다. NoAuth, NoPriv : 없음 인증 및 없음 개인 정보. Auth, NoPriv : 인증 및 없음 개인 정보. Auth, Priv : 인증 및 개인 정보 보호. 항목이 이미있는 경우 보안 수준 값을 수정할 수 없습니다. 즉, 먼저 값이 올바르게 설정되어 있는지 확인해야합니다.
• Authentication Protocol	이 항목이 속해야하는 인증 프로토콜을 나타냅니다. none : none 프로토콜을 인증합니다. MD5 :이 사용자가 MD5 인증 프로토콜을 사용하고 있음을 나타내는 선택적 플래그. SHA : SHA 인증 프로토콜을 사용하는이 사용자를 나타내는 선택적 플래그. 항목이 이미있는 경우 보안 수준 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 프라이버시 프로토콜은 다음과 같습니다. none : none 개인 정보 보호 프로토콜. DES : DES 인증 프로토콜을 사용하는 사용자를 나타내는 선택적 플래그.
• 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 유저 엔트리 추가한다.

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

3.3.5.3 SNMPv3 그룹

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

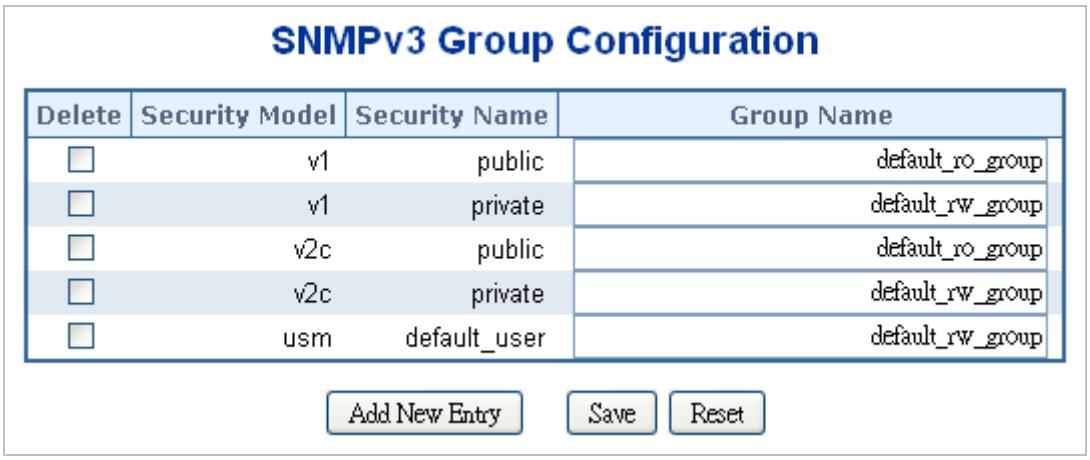


그림 4-3-6 SNMPv3 그룹구성 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Delete	항목을 제거하려면 선택하고 저장하는동안 삭제됩니다.
• Security Model	이 항목이 속해야하는 보안 모델을 나타냅니다. 가능한 보안 모델은 다음과 같습니다. v1 : SNMPv1 용으로 예약되었습니다. v2c : SNMPv2c 용으로 예약되어 있습니다. usm : 사용자 기반 보안 모델 (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: 그룹엔트리를 추가합니다 .

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

3.3.5.4 SNMPv3 Views

그림 4-3-7 의 SNMPv3 보기 화면이 나타납니다.

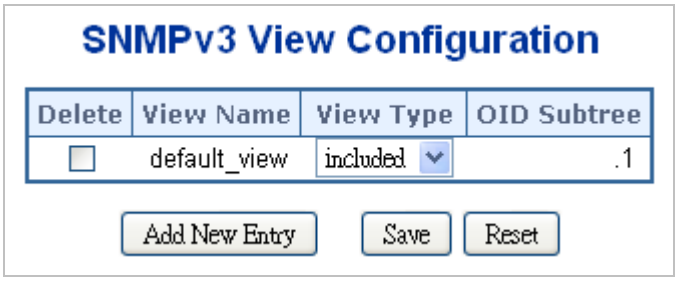


그림 4-3-7 SNMPv3 Views 구성 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• delete	항목을 삭제하려면 선택하십시오.다음 저장 중에 삭제됩니다.
• 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. 가능한보기 유형은 다음과 같습니다. included :이 뷰 하위 트리가 포함되어야 함을 나타내는 선택적 플래그. excluded :이 뷰 하위 트리를 제외해야 함을 나타내는 선택적 플래그입니다. 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 엔트리를 추가한다.

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

3.3.5.5 SNMPv3 접근

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

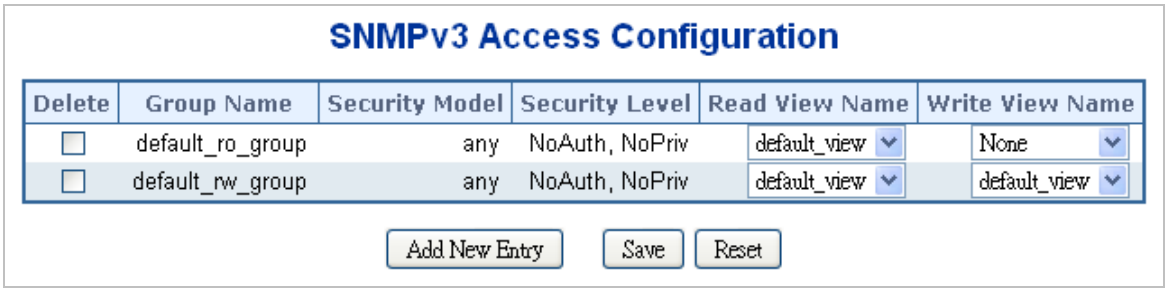


그림 4-3-8 SNMPv3 Access Configuration 구성화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Delete	항목을 제거하려면 선택하고 저장하는동안 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 모델 (v1 | v2c | usm)을 수락했습니다. v1 : SNMPv1 용으로 예약되었습니다. 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 없음 및 개인 정보 없음. Auth, NoPriv : 인증 및 없음 개인 정보. 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: 엔트리 추가 한다..

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

3.4 Port 관리

Port 메뉴를 사용하여 관리 대상 스위치의 Port 를 표시하거나 구성하십시오. 이 섹션에는 다음 항목이 있습니다.

- Port Configuration
- Port Statistics Overview
- Port Statistics Detail
- SFP Module Information
- Port Mirror

3.4.1 Port 구성

이 페이지는 현재 Port 구성을 표시합니다. 여기서도 Port 를 구성 할 수 있습니다. 그림 4-4-1 의 Port 구성 화면이 나타납니다.

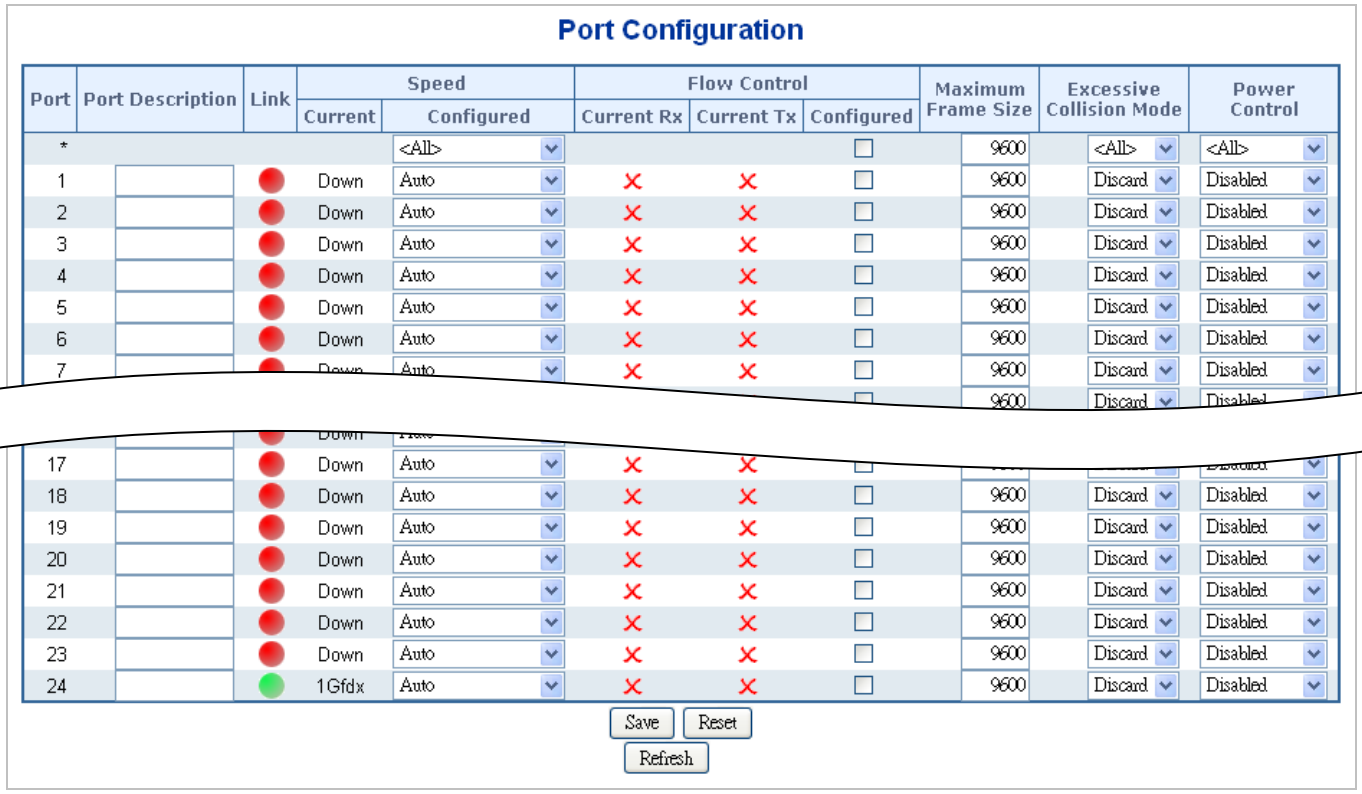


그림 4-4-1 Port 상태 확인 화면

이 페이지는 다음을 포함해 나타냅니다.

정의	설명
• Port	이것은이 행의 논리적인 논리 Port 번호입니다..
• Port Description	Port 별 설명

• Link	현재 링크 상태가 그래픽으로 표시됩니다. 녹색은 링크가 작동 중임을 나타내고 빨간색은 작동 중임을 나타냅니다.
• Current Link Speed	Port 의 링크속도를 제공한다.
• Configured Link Speed	주어진 스위치 Port에 대해 사용 가능한 링크 속도를 선택하십시오. 메뉴 막대를 그려서 방식을를 선택하십시오. 자동 - 구리 인터페이스의 자동 협상을 설정합니다. 10Mbps HDX - 강제로 10Mbps / 반이중 방식을를 설정합니다. 10Mbps FDX - 강제로 10Mbps / 전이중 방식을를 설정합니다. 100Mbps HDX - 강제로 100Mbps / 반이중 방식을를 설정합니다. 100Mbps FDX - 강제로 100Mbps / 전이중 방식을를 설정합니다. 1Gbps FDX - 강제로 10000Mbps / 전이중 방식을를 설정합니다. 사용 안함 - Port를 수동으로 종료합니다.
• Flow Control	Port 에서 자동 속도를 선택하면이 섹션은 링크 파트너에게 알리는 흐름 제어 기능을 나타냅니다. 고정 속도 설정이 선택되면 이것이 사용됩니다. 현재 Rx 열은 Port 의 일시 중지 프레임을 따르는 지 여부를 나타내며 현재 Tx 열은 Port 의 일시 중지 프레임이 전송되는지 여부를 나타냅니다. Rx 및 Tx 설정은 마지막 자동 협상의 결과에 따라 결정됩니다. 흐름 제어를 사용하도록 구성된 열(row)을 확인하십시오. 이 설정은 구성된 링크 속도 설정과 관련이 있습니다.
• Maximum Frame Size	FCS 를 포함하여 스위치 Port 에 허용되는 최대 프레임 크기를 입력하십시오. 허용되는 범위는 1518 바이트에서 9600 바이트입니다.
• Excessive Collision Mode	Port 전송 충돌 동작을 구성합니다. 폐기 : 16 회의 충돌 후 프레임 폐기 (기본값). 다시 시작 : 16 번의 충돌 후에 백 오프 알고리즘을 다시 시작합니다.
• Power Control	Usage 열은 Port 당 현재 전력 소비 비율을 나타냅니다. Configured 열을 사용하면 Port 당 절전 방식 매개 변수를 변경할 수 있습니다. 사용 안 함 : 모든 절전 메커니즘이 비활성화됩니다. ActiPHY : 절전 기능을 링크 다운합니다. 동적 : Link up power savings 가 가능합니다. Enabled (사용) : Link Up 및 Link Down 으로 절전을 활성화합니다.

각 Port 가 100M Full, 100M Half, 10M Full 및 10M Half-speed 방식으로로 실행되도록 설정할 때. Auto-MDIX 기능이 비활성화됩니다.

버튼

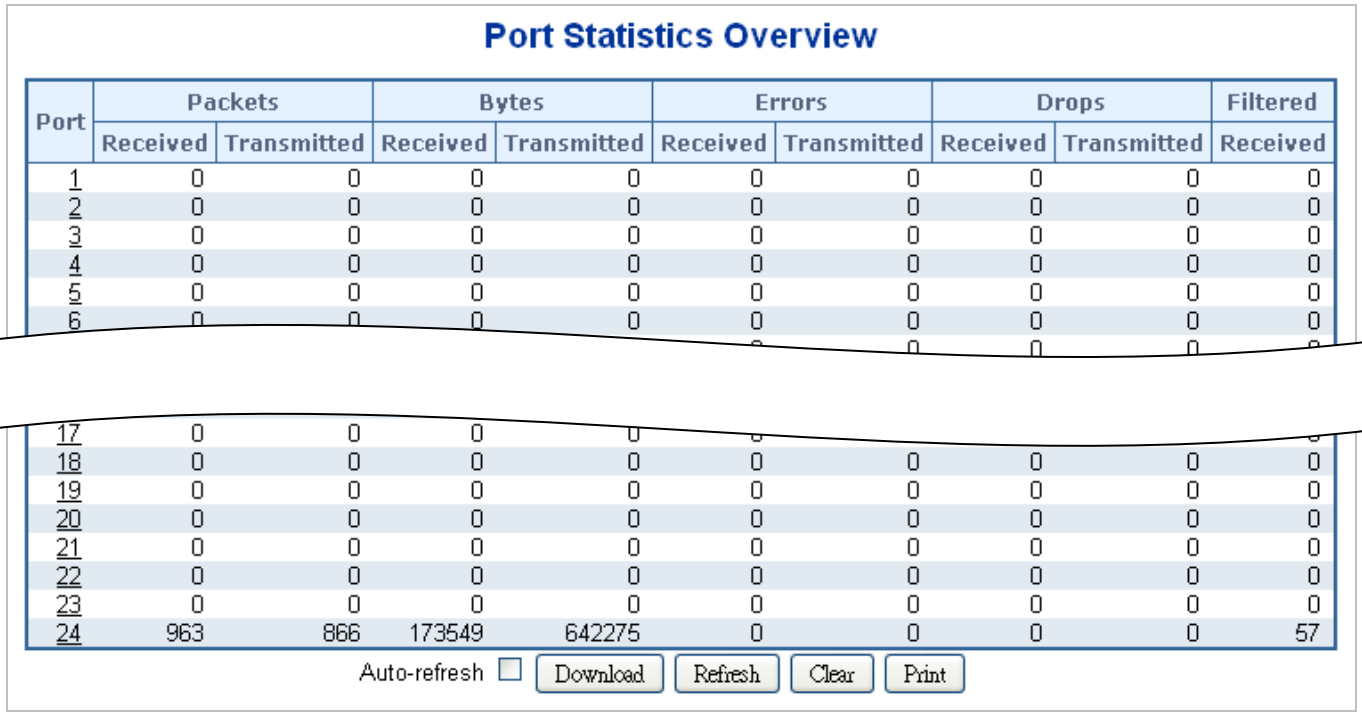
Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

Refresh: 페이지를 새로 고치려면 클릭하십시오. 로컬에서 변경 한 내용은 실행 취소됩니다.

3.4.2 Port 통계 개요

이 페이지는 모든 스위치 Port 에 대한 일반 트래픽 통계에 대한 개요를 제공합니다. 그림 4-4-2 의 Port 통계 개요 화면이 나타납니다.



Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
17	0	0	0	0					
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0
24	963	866	173549	642275	0	0	0	0	57

그림 4-4-2 Port 통계 개요 화면

The displayed counters are:

Object	Description
• Port	같은 열에 대한 설정값을 논리적인 Port 를 포함합니다.
• Packets	Port 당 수신 및 전송 된 패킷 수
• Bytes	Port 당 수신 및 전송된 바이트 수
• Errors	불완전한 전송 Port 및 수신 프레임 및 전송된 에러수
• Drops	프레임이 입출력시에 혼잡으로 인해 버려진 프레임 수
• Filtered	포워딩과정에 의해 필터링 된 수신 프레임 수

버튼

Refresh: 즉시 페이지를 새로 고칩니다.

Clear: 모든 Port 의 카운터를 지웁니다.

Auto-refresh : 페이지 자동 새로 고침을 사용한다

3.4.3 Port 통계 세부 사항

이 페이지는 특정 스위치 Port 에 대한 자세한 트래픽 통계를 제공합니다. Port 선택 상자를 사용하여 표시 할 스위치 Port 세부 정보를 선택하십시오. 선택된 Port 는 페이지 헤더에 반영된대로 현재 선택된 스택 단위에 속합니다. 표시된 카운터는 수신 및 전송의 합계, 수신 및 전송의 크기 카운터, 수신 및 전송의 오류 카운터입니다. 그림 4-4-3 의 Port 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 세부 사항 Port 통계 Port 1 페이지 화면

이 페이지는 다음을 포함해 나타냅니다.

Receive Total and Transmit Total

Object	Description
• Rx and Tx Packets	송신 수신이 된 패킷 수
• Rx and Tx Octets	송신 수신이 된 바이트수이며, FCS 를 포함하지만 프레이밍비트는 제외
• Rx and Tx Unicast	송신 수신이 된 유니케스트 패킷 수
• Rx and Tx Multicast	송신 수신이 된 멀티케스트 패킷 수
• Rx and Tx Broadcast	송신 수신이 된 브로드케스트 패킷 수
• Rx and Tx Pause	Pause 동작을 나타내는 Opcode 를 가진 Port 에서 송수신된 MAC 프레임

수신 및 전송 사이즈 카운터

송수신된 패킷의 수는 각각의 프레임에 따라 범주가 분리

송수신 큐 카운터

입출력 큐당 송수신 된 패킷의 수

오류카운터 수신.

Object	Description
• Rx Drops	수신 버퍼 부족 또는 송신혼잡으로 인해 드롭 된 프레임 수입니다.
• Rx CRC/Alignment	CRC 또는 정렬 오류로 수신 된 프레임 수입니다.
• Rx Undersize	유효한 CRC 로 수신 된 짧은 1 프레임의 수.
• Rx Oversize	유효한 CRC 로 수신 된 긴 2 프레임의 수.
• Rx Fragments	유효하지 않은 CRC 로 수신 된 짧은 1 프레임의 수.
• Rx Jabber	유효하지 않은 CRC 로 수신 된 긴 2 프레임의 수.
• Rx Filtered	포워딩과정에 필터링 된 수신프레임의 수입니다. 짧은 프레임은 64 바이트보다 작은 프레임입니다. 긴 프레임은 Port 에 구성된 최대 프레임 길이보다 긴프레임입니다.

1. 짧은 프레임은 64 바이트보다 짧은 프레임이다
2. 긴 프레임은 Port 의 구성된 최대프레임 길이보다 긴프레임입니다.

Transmit Error Counters

Object	Description
• Tx Drops	출력 버퍼 정체로 인해 삭제된 프레임 수
• Tx Late/Exc. Coll.	출력버퍼가 과도하거나 늦은 충돌로 인해 떨어지는 프레임수

버튼

Refresh: 즉시 페이지를 새로 고칩니다.

Clear: 모든 Port 의 카운터를 지운다.

Auto-refresh : 페이지 자동 새로 고침을 사용한다

3.4.4 SFP 안내

SFP 모듈 정보 페이지를 통해 SFP 모듈의 실제 또는 작동 상태를 점검 할 수 있습니다. 이 페이지는 트랜시버 유형, 속도 및 파장과 같은 작동 상태를 표시하고 특정 인터페이스에서 SFP 모듈의 거리를 지원합니다. Port 번호의 하이퍼 링크를 사용할 수도 있습니다. 특정 인터페이스에서 통계를 확인합니다. 그림 4-4-4 의 SFP 모듈 정보 화면이 나타납니다.

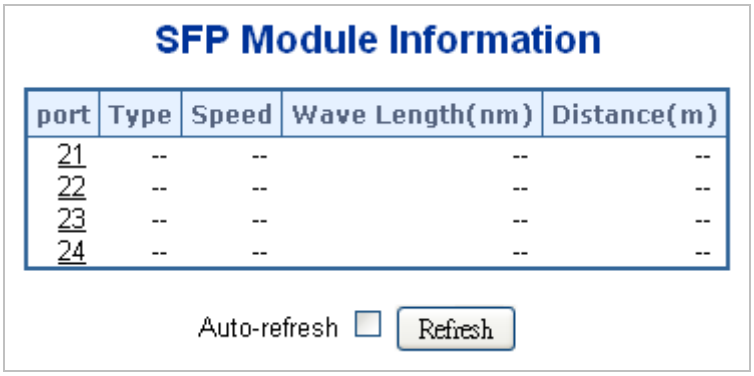


그림 4-4-4 SFP Module Information 안내화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Type	현재의 SFP 모듈중에 적용가능한 형태이다. ■ 1000Base-SX ■ 1000Base-LX ■ 100Base-FX
• Speed	현재의 SFP 모듈의 속도를 나타내는데 SFP 모듈로 속도값이나 묘사값을 얻는다, 다른 SFP 모듈의 밴더는 다른속도정보를 보여줄것이다.

• 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 모듈의지지 거리를 표시하십시오. 거리 값은 SFP 모듈에서 가져옵니다.

버튼

Auto-refresh : 페이지 자동 새로 고침을 사용한다

Refresh: 즉시 페이지를 새로 고칩니다.

3.4.5 Port Mirror

이 페이지에서 Port 미러링을 구성하십시오. 이 기능은 패킷을 연구 할 수있는 다른 Port 로 네트워크 스위치의 한 Port 에서 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 Port 로 복사하거나 미러링 할 수 있습니다.
- 관리 형 스위치는 모든 Port 에서 모니터 Port 로가는 트래픽을 눈에 띄지 않게 미러링 할 수 있습니다. 그런 다음이 Port 에 프로토콜 분석기 또는 RMON 프로브를 연결하여 트래픽 분석을 수행하고 연결 무결성을 확인할 수 있습니다.

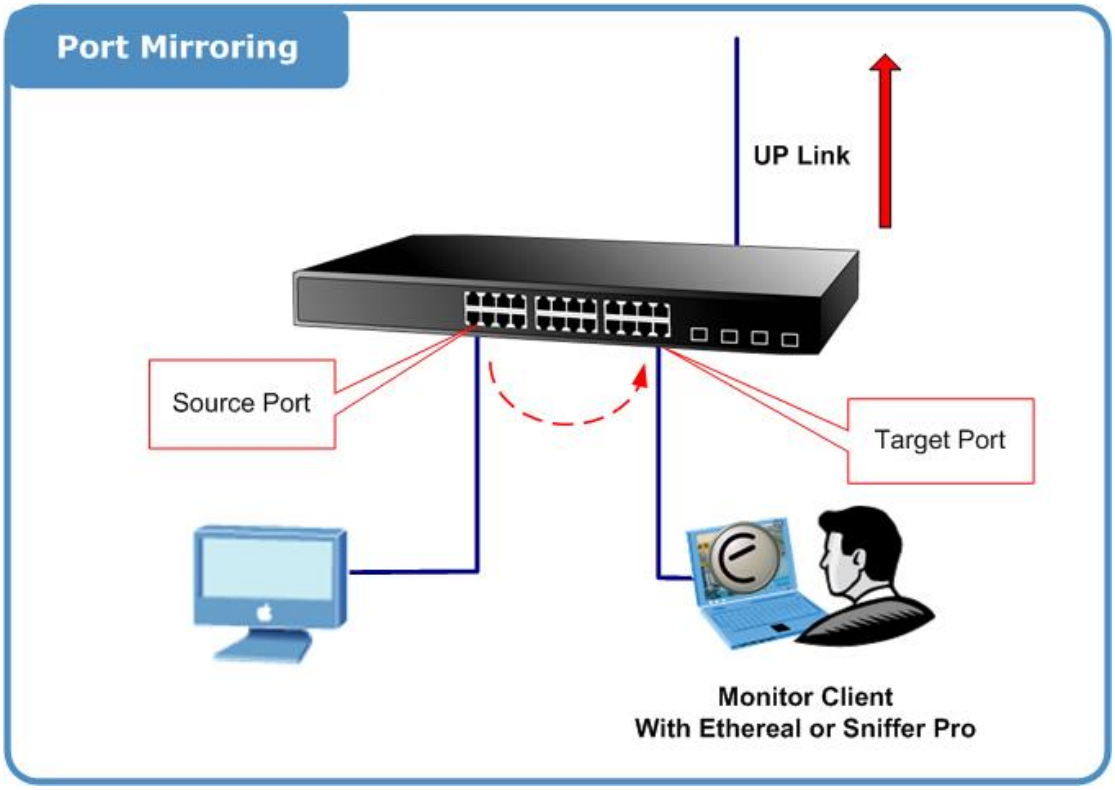


그림 4-4-5 Port Mirror application

미러 Port 에 복사 할 트래픽은 다음과 같이 선택됩니다.

- 할당 Port 에서 수신된 모든 프레임 (또는 소스미려링이나 입력이라고 한다)
- 할당 Port 에서 전송되는 모든 프레임 (또는 대상미러링이나 송신이라고 한다.)
- Mirror Port 구성

미러 Port 화면이 4-4-6 에 나와있다.

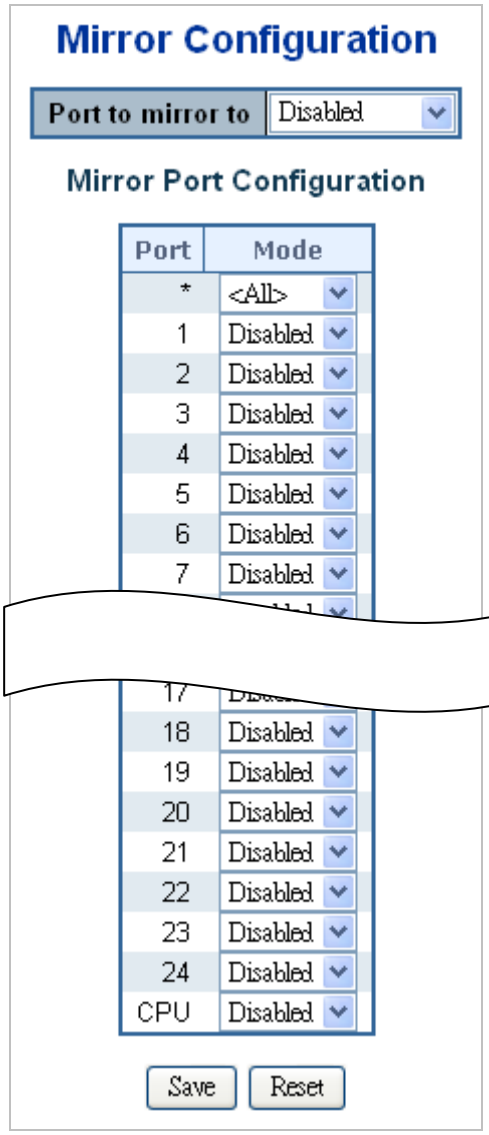


그림 4-4-6 미러구성 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Port to mirror on	소스 (rx) 또는 대상 (tx) 미러링이 활성화 된 Port 의 프레임은이 Port 에 미러링됩니다.
• Port	같은 열에 포함하는 설정값에 논리 Port 입니다.
• Mode	미러방식을를 선택합니다. Rx 만 해당사항: Port 에서 수신된 프레임은 미러링 Port 로 미러링된다. Tx 만 해당사항: Port 에서 전송된 프레임은 미러링 Port 로 미러링된다.
	비활성화(Disable) : 전송된 프레임이나 수신프레임이 미러링되지 않는다. 활성화(Enabled) : 수신된 프레임과 발신된 프레임은 미러링이 된다.

주어진 Port 의 경우 프레임은 한 번만 전송됩니다. 따라서 미러 Port 에서 Tx 프레임을 미러링 할 수 없습니다. 이 때문에 선택한 미러 Port 의 방식은는 Disabled 또는 Rx 로만 제한됩니다

버튼

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

3.5 링크 집계

Port 집합은 Port 그룹을 연결하여 단일 LAG (Link Aggregated Groups)를 형성함으로써 Port 사용을 최적화합니다. Port 집합은 장치 간 대역폭을 늘리고 Port 유연성을 높이며 링크 중복성을 제공합니다.
각 LAG 는 전이중 작업으로 설정된 동일한 속도의 Port 로 구성됩니다. LAG 의 Port 는 동일한 속도로 작동하는 경우 서로 다른 미디어 유형 (UTP / 파이버 또는 다른 파이버 유형) 일 수 있습니다.
집계 링크는 수동으로 (Port 트렁크) 또는 관련 링크에서 링크 집계 제어 프로토콜 (LACP)을 활성화하여 자동으로 할당 할 수 있습니다.
집계 링크는 시스템에서 단일 논리 Port 로 처리됩니다. 특히, 집계 링크는 자동 협상, 속도, 이중 설정 등을 포함하여 비 집합 Port 와 유사한 Port 속성을 가집니다.

이 링크 집합에 따라 장치를 지원한다.

- Static LAGs (Port Trunk) – 선택한 Port를 정리하여 트렁크 그룹으로 강제 설정..
- Link Aggregation Control Protocol (LACP) LAGs -
  LACP LAG는 다른 장치에있는 다른 LACP Port와 집계 된 Port 링크를 협상합니다. 다른 장치 Port가 LACP Port 인 경우 장치는 이들 장치간에 LAG를 설정합니다.

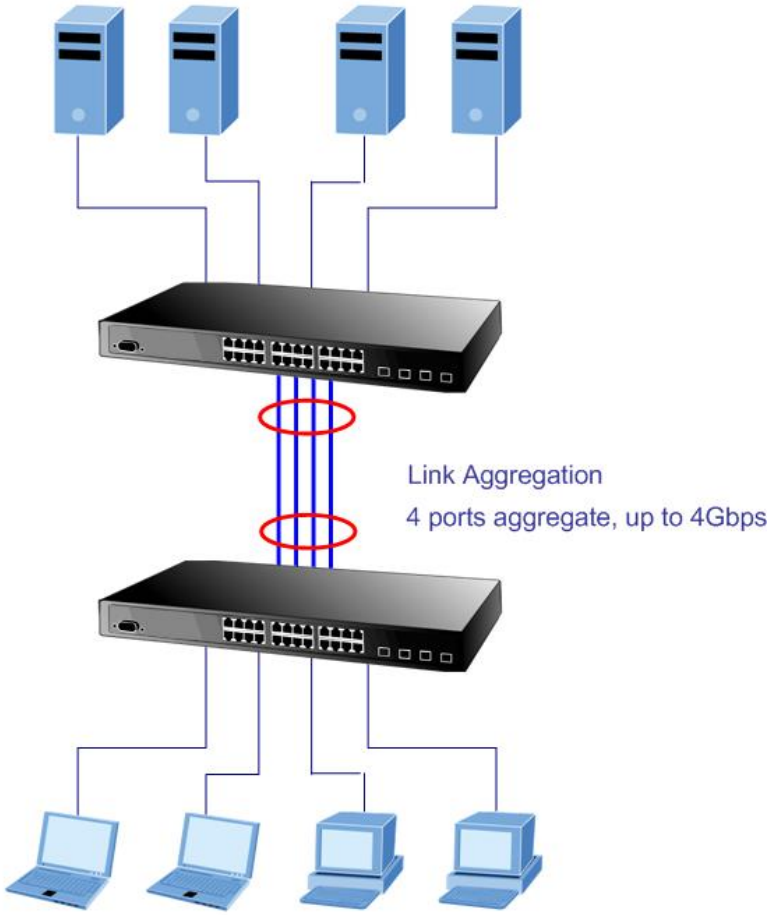


그림 4-5-1 Link Aggregation

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 Port 를 하나의 전용 연결로 그룹화 할 수 있습니다. 이 기능을 사용하면 네트워크의 장치로 대역폭을 확장 할 수 있습니다. LACP 작동에는 전이중 방식이가 필요하며 자세한 정보는 IEEE 802.3ad 표준을 참조하십시오.

Port 링크 집계를 사용하여 네트워크 연결의 대역폭을 높이거나 오류 복구를 보장 할 수 있습니다. Link Aggregation 을 사용하면 최대 4 개의 연속 Port 를 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. Port 링크 집계를 사용할 때 다음을 참고하십시오.

- 링크 집합에 사용되는 Port 는 모두 동일한 미디어 유형 (RJ-45, 100Mbps 광섬유)이어야합니다.
- 동일한 링크 집합에 할당 할 수있는 Port 에는 다른 제한 사항이 있습니다 (아래 참조).
- Port 는 하나의 링크 집합에만 할당 할 수 있습니다.
- 연결의 양쪽 끝에있는 Port 는 링크 집계 Port 로 구성되어야합니다.
- 링크 집계의 어느 Port 도 미러 소스 Port 또는 미러 대상 Port 로 구성 할 수 없습니다.

• 링크 집계의 모든 Port 는 VLAN 에서 이동, 추가 또는 삭제 될 때 전체적으로 처리되어야합니다.

• 스패닝 트리 프로토콜은 링크 집계의 모든 Port 를 전체적으로 처리합니다.

• 데이터 루프가 생성되지 않도록 스위치 사이에 케이블을 연결하기 전에 링크 집계를 활성화하십시오.

• 데이터 링크가 생성되지 않도록 Port 링크 집계를 제거하기 전에 모든 링크 집계 Port 케이블을 분리하거나 링크 집계 Port 를 비활성화하십시오. 동시에 최대 10 개의 Port 를 집계 할 수 있습니다. 관리 형 스위치는 기가비트 이더넷 Port (최대 5 개 그룹)를 지원합니다. 그룹이 LACP 정적 링크 집계 그룹으로 정의 된 경우 다른 Port 중 하나에 장애가 발생하면 여분의 Port 가 대기 방식으로로 전환되어 중복됩니다. 그룹이 로컬 정적 링크 집계 그룹으로 정의 된 경우 Port 수는 그룹 구성원 Port 와 같아야합니다. 집계 코드는 동일한 프레임 흐름 (예 : TCP 연결)에 속한 프레임이 항상 동일한 링크 집계 구성원 Port 에서 전달되도록합니다. 따라서 흐름 내의 프레임을 표현하는 것은 불가능합니다. 집계 코드는 다음 정보를 기반으로합니다.

1. 출발지 MAC
2. 목적지 MAC
3. 소스 및 대상 IPv4 주소.
4. IP v4 패킷의 원본 및 대상 TCP/ UDP Port

일반적으로 링크 집계 구성원 Port 간에 최상의 트래픽 분산을 얻으려면 집계 코드에 대한 5 가지 컨트 리뷰션을 모두 활성화해야합니다. 각 링크 집합은 최대 10 개의 구성원 Port 로 구성 될 수 있습니다. 임의의 수량의 링크 집합이 장치에 구성 될 수 있습니다 (장치의 Port 수량에 의해서만 제한됩니다.) 적절한 트래픽 분산을 구성하려면 링크 집계 내의 Port 가 동일한 링크 속도를 사용해야합니다.

3.5.1 Static Aggregation

이 페이지는 집계 해시 방식 및 집계 그룹을 구성하는 데 사용됩니다. 집계 해시 방식 설정은 전역이며 집계 그룹은 페이지 머리글에 반영된대로 현재 선택된 스택 단위와 관련됩니다.

Hash Code Contributors

The Static Aggeration screen 은 다음 4-5-2 의 자료화면에 나타난다..

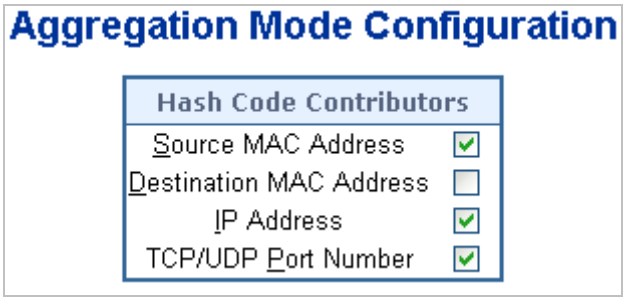


그림 4-5-2 Aggregation mode 구성 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Source MAC Address	소스 MAC 주소는 프레임의 대상 Port 를 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 Port 를 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 Port 를 계산하는 데 사용할 수 있습니다. IP 주소 사용을 활성화하려면 선택하고 비활성화하려면 선택을 취소하십시오. 기본적으로 IP 주소가 사용됩니다.
• TCP/UDP Port Number	TCP / UDP Port 번호는 프레임의 대상 Port 를 계산하는 데 사용할 수 있습니다. TCP / UDP Port 번호를 사용하려면 선택하고, 선택하지 않으려면 선택을 취소하십시오. 기본적으로 TCP / UDP Port 번호가 사용됩니다.

Static Aggregation Group 구성

그림 4-5-3 의 다음과 같은 화면이 나타납니다.

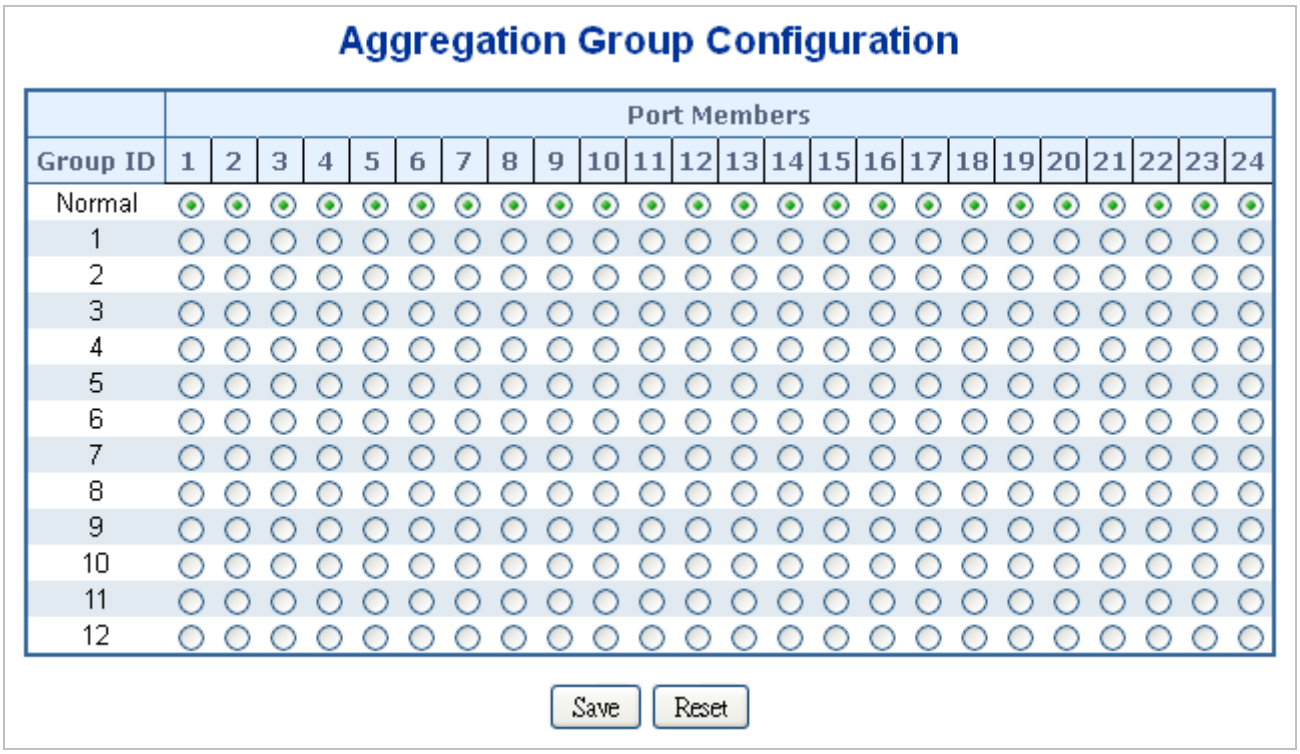


그림 4-5-3 Aggregation Group 구성 설정화면

이 페이지는 다음을 포함해 나타냅니다.

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

버튼

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

3.5.2 LACP 구성

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

이 페이지를 통해 사용자는 현재 LACP Port 구성을 검사 할 수 있으며 변경 가능할 수도 있습니다. LACP Port 설정은 페이지 머리글에 반영된대로 현재 선택된 스택 장치와 관련이 있습니다. 그림 4-5-4 의 LACP Configuration (LACP 구성) 화면이 나타납니다.

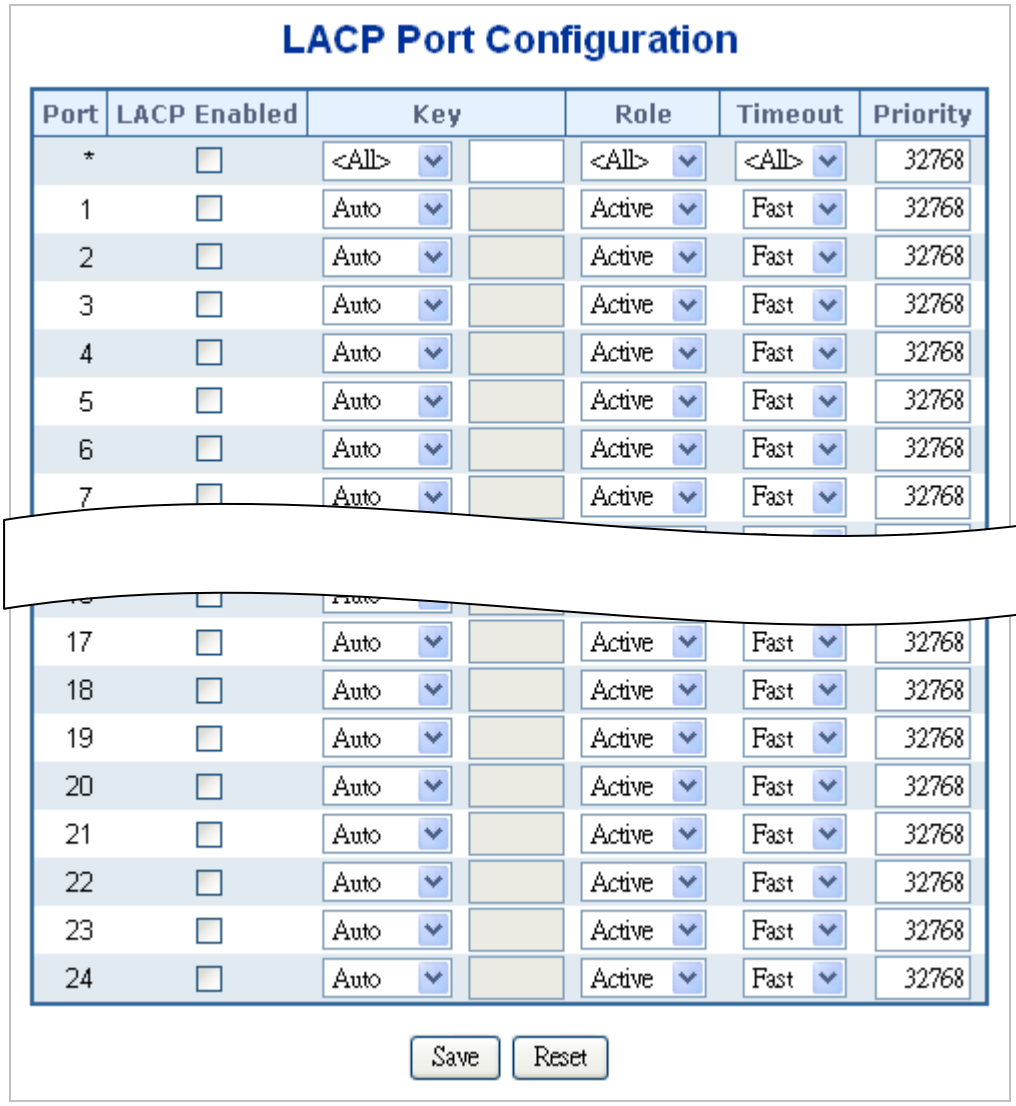


그림 4-5-4 LACP Port 구성 구성화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Port	스위치 Port 숫자
• LACP Enabled	이 스위치 Port 에서 LACP 를 활성화할지 여부를 제어합니다. LACP 는 2 개 이상의 Port 가 동일한 파트너에 연결된 경우 집계를 형성합니다. LACP 는 스택 당 최대 12 개의 LLAG 및 스택 당 2G LAG 를 형성 할 수 있습니다.
• Key	Port 에서 발생하는 키 값 (범위 : 1-65535) 자동 설정은 물리적 링크

	속도 인 10Mb = 1, 100Mb = 2, 1Gb = 3 으로 키를 적절히 설정합니다. 특정 설정을 사용하여 사용자 정의 값을 입력 할 수 있습니다. 동일한 키 값을 가진 Port 는 동일한 집계 그룹에 참여할 수 있지만 다른 키를 가진 Port 는 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 말하십시오).
• 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	Port 의 우선 순위를 제어합니다. LACP 파트너가이 장치에서 지원하는 것보다 큰 그룹을 구성하려는 경우이 매개 변수는 어떤 Port 가 활성 상태이고 어느 Port 가 백업 역할을 담당 할 것인지를 제어합니다. 숫자가 낮을수록 우선 순위가 높아집니다.

버튼

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

3.5.3 LACP 시스템 상태

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

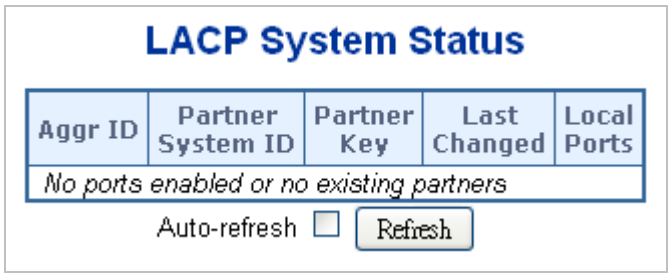


그림 4-5-5 LACP 시스템 상태 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Aggr ID	Aggr ID 와 연결된 인스턴스입니다.

• Partner System ID	집계 파트너의시스템 ID (MAC 주소) 입니다.
• Partner Key	집합아이디에게 파트너를 등록하는 키입니다 .
• Last changed	집계가 변화되는 때
• Local Ports	이 스위치의 스택이나 형식은 스위치 ID : Port 입니다.

버튼

Refresh: 즉시 페이지를 새로 고칩니다.

Auto-refresh ☐: 자동적으로 리프

3.5.4 LACP Port 상태

This page provides a 상태 개요 for LACP 상태 for all Port. The LACP Port 상태 screen in 그림 4-5-6 appears.

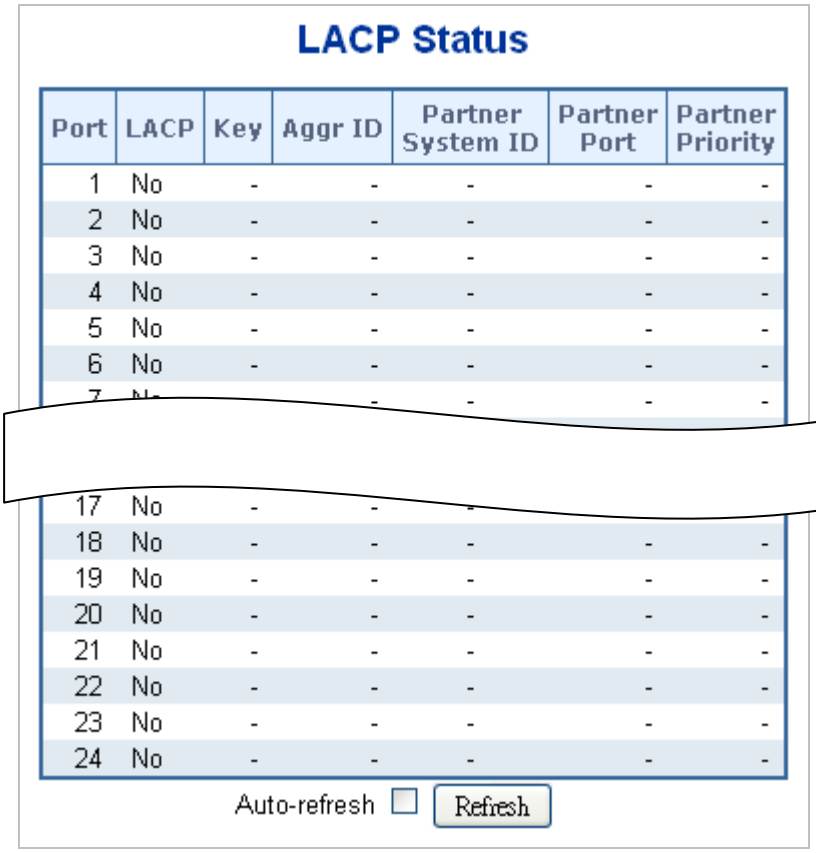


그림 4-5-6 LACP 상태 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description

• Port	스위치 Port 숫자
• LACP	'예시'는 LACP 가 활성화되어 있고 Port 링크가 작동 중임을 의미합니다. '아니요'는 LACP 가 활성화되어 있지 않거나 Port 링크가 다운되어 있음을 의미합니다. '백업'은 Port 가 집계 그룹에 참여할 수 없지만 다른 Port 가 나가면 참여할 수 있음을 의미합니다. LACP 상태는 사용할 수 없습니다.
• Key	이 Port 에서 지정된 키입니다. 동일한 키가 있ㅎ는 Port 만 함께그
• Aggr ID	집계 그룹에서 승인한 집계 ID
• Partner System ID	파트너 시스템 아이디 (MAC address_
• Partner Port	파트너 Port 숫자와 연결된 파트너 Port
• Partner Priority	파트너 Port 의 우선순위 .

버튼

Refresh: 즉시 페이지를 새로 고칩니다.

Auto-refresh : 새로운 엔트리를 추가한다.새로고침이 3 초마다 발생합니다.

3.5.5 LACP Port 통계

모돈 Port 의 LACP 통계에 대한 개요를 제공합니다. 그림 4-5-7 의 LACP Port 통계화면이 나타납니다.

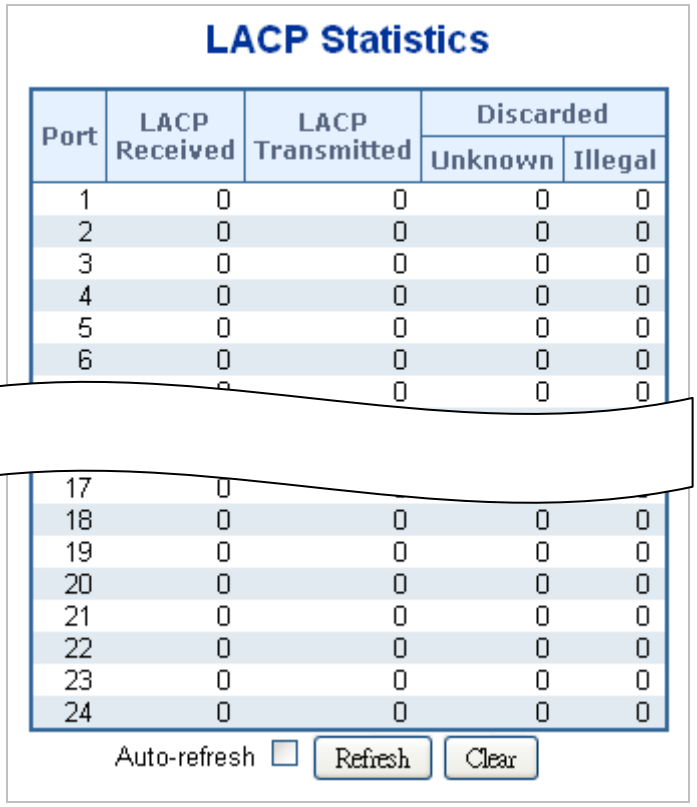


그림 4-5-7 LACP 통계 출력화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
Port	스위치 Port .
• LACP Received	각 Port 에서 보낸 LACP 프레임 수를 표시합니다.
• LACP Transmitted	각 Port 에서 수신 된 LACP 프레임 수를 표시합니다. 트.
• Discarded	각 Port 에서 알 수 없거나 불법 인 LACP 프레임이 몇 개 있는지를 보여줍니다.

버튼

Auto-refresh : 새로운 엔트리를 추가한다.새로고침이 3 초마다 발생합니다.

Refresh : 즉시 페이지를 새로 고칩니다.

Clear : 모든 Port 의 카운터를 지운다.

3.6 VLAN

3.6.1 VLAN 개요

A Virtual Local Area Network (VLAN) 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 Port 간에 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 VLAN간에 라우팅 기능을 수행하지 않으면 패킷이 VLAN을 통과 할 수 없습니다.

2. 관리 형 스위치는 IEEE 802.1Q VLAN을 지원합니다. Port 태그 해제 기능을 사용하면 태그를 인식하지 않는 장치와의 호환성을 유지하기 위해 패킷 헤더에서 802.1 태그를 제거 할 수 있습니다.

3. 스위치의 기본값은 모든 Port를 DEFAULT_VLAN이라는 단일 802.1Q VLAN에 할당하는 것입니다. 새 VLAN이 만들어지면 새 VLAN에 할당 된 구성원 Port가 DEFAULT_ VLAN Port 구성원 목록에서 제거됩니다. DEFAULT_VLAN의 VID는 1입니다

- VLAN Basic Information — Vlan 정보 표시
- VLAN Port Configuration — Vlan 그룹 사용
- VLAN Memberships — Vlan 멤버쉽을 구성합니다.
- VLAN Membership Status — Vlan 멤버쉽 상태 표시
- VLAN Port Status — Vlan Port 상태 표시
- Private VLAN — 기본 또는 커뮤니티 Vlan 생성/제거
- Port Isolation — Port 에서 Isolation 사용/사용안함
- MAC-based VLAN — MAC 기반 Vlan 항목을 구성
- MAC-based VLAN Status — MAC 기반 Vlan 항목 표시 안함
- IP-based VLAN — IP 기반 Vlan 항목을 구성합니다.

■ Protocol-based VLAN	프로토콜 기반 Vlan 항목을 구성합니다.
■ Protocol-based VLAN Membership	프로토콜 기반 Vlan 항목을 표시하지 않습니다.

3.6.2 IEEE 802.1Q VLAN

대규모 네트워크에서 라우터는 각 서브넷의 브로드 캐스트 트래픽을 별도의 도메인으로 Isolation 하는 데 사용됩니다. 이 관리 형 스위치는 VLAN 을 사용하여 네트워크 노드 그룹을 별도의 브로드 캐스트 도메인으로 구성하여 2 계층에서 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 위치에 나있을 수 있지만 동일한 물리적 세그먼트에 속한 것처럼 통신하는 Port 그룹입니다.

VLAN 을 사용하면 물리적 연결을 변경하지 않고도 장치를 새로운 VLAN 으로 이동할 수 있으므로 네트워크 관리가 단순 해집니다. 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.

관리형 스위치에 다음과 같은 Vlan 특징을 나타낸다.

- IEEE 802.1Q 표준에 기반한 최대 255 개의 VLAN
- Port 겹침, Port 가 여러 VLAN 에 참여할수 있음,
- 마지막위치에서는 여러 VLAN 에 속할 수 있습니다.

■ IEEE 802.1Q Standard

IEEE 802.1Q (태그) VLAN 은 스위치에 구현됩니다. 802.1Q VLAN 에는 태그 지정이 필요하므로 전체 네트워크를 스팬 할 수 있습니다 (네트워크상의 모든 스위치가 IEEE 802.1Q 를 준수한다고 가정). VLAN 을 사용하면 브로드 캐스트 도메인의 크기를 줄이기 위해 네트워크를 세그먼트 간소화할 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 Port 는 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 개의 802.1Q 호환 스위치로 확장 할 수 있으며 모든 Port 에서 스패닝 트리를 활성화하고 정상적으로 작동 할 수 있습니다.

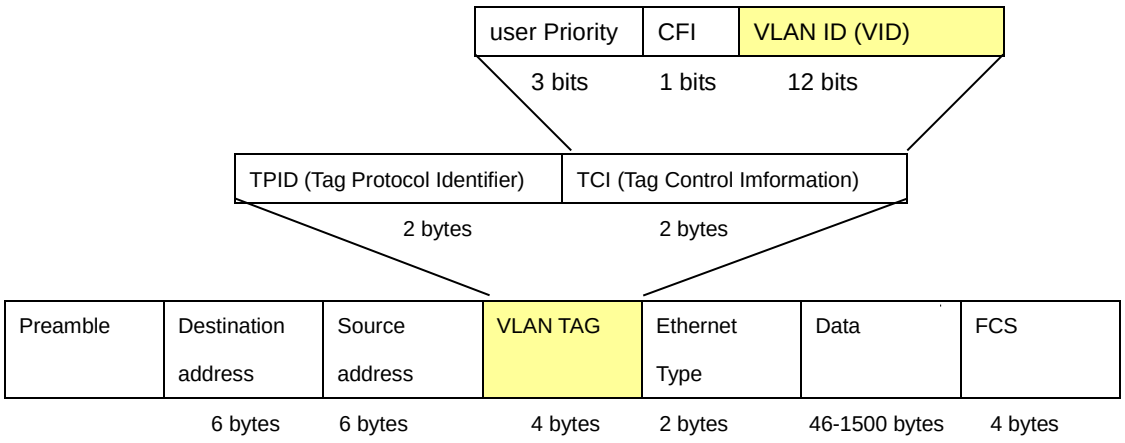
관련된 몇 가지의 용어:

- 태그 지정 - 패킷의 헤더에 802.1Q VLAN 정보를 넣는 행동
- 태그 해제 - 패킷의 해더에서 802.1Q VLAN 정보를 제거하는 행위

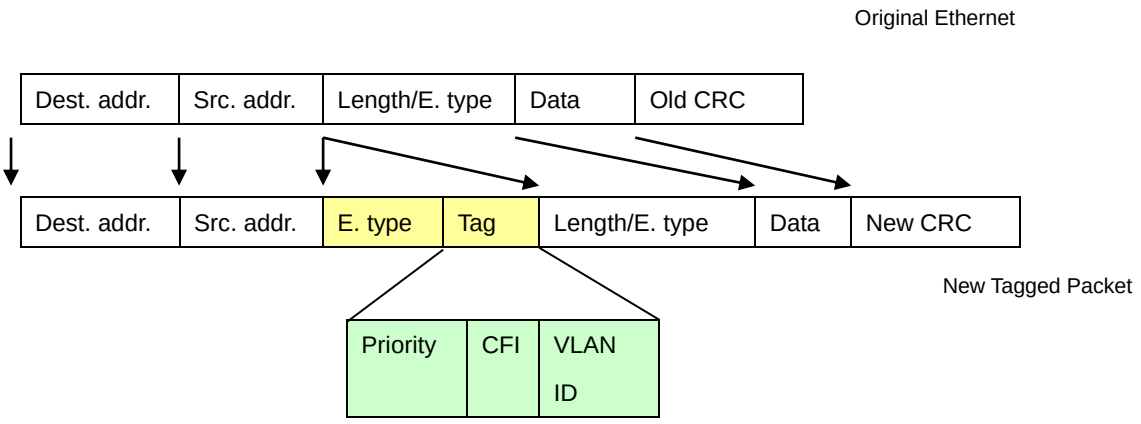
■ 802.1Q VLAN Tags

아래 그림은 802.1Q VLAN 태그를 보여줍니다. 소스 MAC 주소 뒤에 네 개의 추가 8 진수가 삽입됩니다. 그들의 존재 여부는 Ethernet Type 필드에 0x8100 값으로 표시됩니다. 패킷의 Ethernet Type 필드가 0x8100 인 경우, 패킷은 IEEE 802.1Q / 802.1p 태그를 전달합니다. 이 태그는 다음 두 옥텟에 포함되며 3 비트의 사용자 우선 순위, 1 비트의 Canonical Format Identifier (CFI - 토큰 링 패킷을 이더넷 백본을 통해 전송할 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



IEEE802.1Q Tag 추가하는 과정



■ 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 Port 에는 PVID 가 있습니다. 802.1Q Port 에는 스위치 내에서 사용하기 위해 PVID 가 할당됩니다. 스위치에 VLAN 이 정의되지 않은 경우 모든 Port 는 PVID 가 1 인 기본 VLAN 에 할당됩니다. 태그가없는 패킷에는 수신 된 Port 의 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 Port 의 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 Port 는 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 Port 에서 결정해야합니다 (전송할 패킷에 태그가 있어야하는지 여부). 전송 Port 가 태그 비 인식 장치에 연결되어 있으면 패킷에 태그가 없어야합니다. 전송 Port 가 태그 인식 장치에 연결되어 있으면 패킷에 태그가 지정되어야합니다.

■ Default VLANs

스위치는 초기에 "default"라는 하나의 VLAN 인 VID = 1 을 구성합니다. 공장 출하시의 기본 설정은 스위치의 모든 Port 를 "기본값"으로 지정합니다. 새 VLAN 이 Port 기반 방식으로로 구성되면 해당 구성원 Port 가 "기본값"에서 제거됩니다.

■ Assigning port to VLANs

스위치에 VLAN 을 활성화하기 전에 먼저 각 Port 를 참여시킬 VLAN 그룹에 할당해야합니다. 기본적으로 모든 Port 는 태그가없는 Port 로 VLAN 1 에 할당됩니다. 하나 이상의 VLAN 에 트래픽을 전달하고 연결의 다른 끝에있는 중간 네트워크 장치 또는 호스트가 VLAN 을 지원하려면 Port 를 태그있는 Port 로 추가하십시오. 그런 다음 GVRP 를 사용하여 수동 또는 동적으로이 트래픽을 전달할 경로를 따라 다른 VLAN 인식 네트워크 장치의 Port 를 동일한 VLAN 에 할당합니다. 그러나 이 스위치의 Port 를 하나 이상의 VLAN 에 참여 시키되 중간 네트워크 장치 나 연결의 다른 쪽 호스트가 VLAN 을 지원하지 않도록하려면이 Port 를 VLAN 에 태그 Port 가없는 Port 로 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 Port 의 기본 VLAN ID 를 기반으로 함). 그러나 프레임에 태그가 지정되면 스위치는 태그가 지정된 VLAN ID 를 사용하여 프레임의 Port 브로드 캐스트 도메인을 식별합니다.

■ Port Overlapping

Port 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 Port 사이에서만 전달됩니다. Untagged VLAN 은 사용자 그룹이나 서브넷을 수동으로 Isolation 하는 데 사용할 수 있습니다.

3.6.3 VLAN Basic Information

VLAN 기본 정보 페이지는 관리 대상 스위치에서 지원하는 VLAN 유형에 대한 기본 정보를 표시합니다.
그림 4-6-1 의 VLAN Basic Information 화면이 나타납니다.

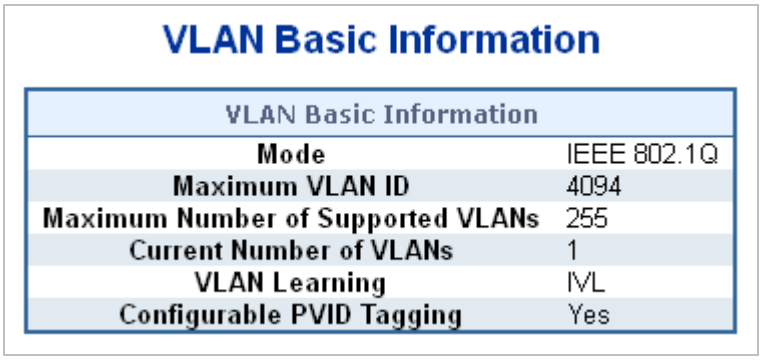


그림 4-6-1 LAN 기본 정보 페이지화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Mode	이 관리형 스위치에 Vlan 방식이가 나타난다. ■ Port-Based ■ IEEE 802.1Q VLAN
• Maximum VLAN ID	관리형 스위치가 알수있는 최대치 Vlan ID 입니다.
• Maximum Number of	관리형 스위치에 구성된 피무의 최대갯수입니다.

Supported VLANs	
• Current number of VLANs	현재의 Vlan 수 표시
• VLAN Learning	Vlan 학습방식을를 표시한다. 관리형 스위치ㅏ는 IVL(IVL 독립형 VLAN 학습)을 지원합니다.
• Configurable PVID Tagging	구성 가능한 PVID 태깅이 구현되는지 여부를 나타냅니다.

3.6.4 VLAN port 구성

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

스위치 명칭의 이해

■ IEEE 802.1Q Tagged and Untagged

802.1Q 호환 스위치의 모든 Port 는 태그로 지정되거나 태그가 지정되지 않은 Port 로 구성 될 수 있다.

- Tagged: 태깅이 활성화 된 Port 는 VID 번호, 우선 순위 및 기타 VLAN 정보를 해당 Port 로 유입되는 모든 패킷의 헤더에 넣습니다. 패킷에 이전에 태그가 지정되어 있으면 Port 가 패킷을 변경하지 않으므로 VLAN 정보가 손상되지 않습니다. 그런 다음 태그의 VLAN 정보를 네트워크의 다른 802.1Q 준수 장치가 사용하여 패킷 전달 결정을 내릴 수 있습니다.
- Untagged: 태그없는 태그가 설정된 Port 는 해당 Port 로 유입되는 모든 패킷에서 802.1Q 태그를 제거합니다. 패킷에 802.1Q VLAN 태그가 없으면 Port 가 패킷을 변경하지 않습니다. 따라서 태그없는 Port 가 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.

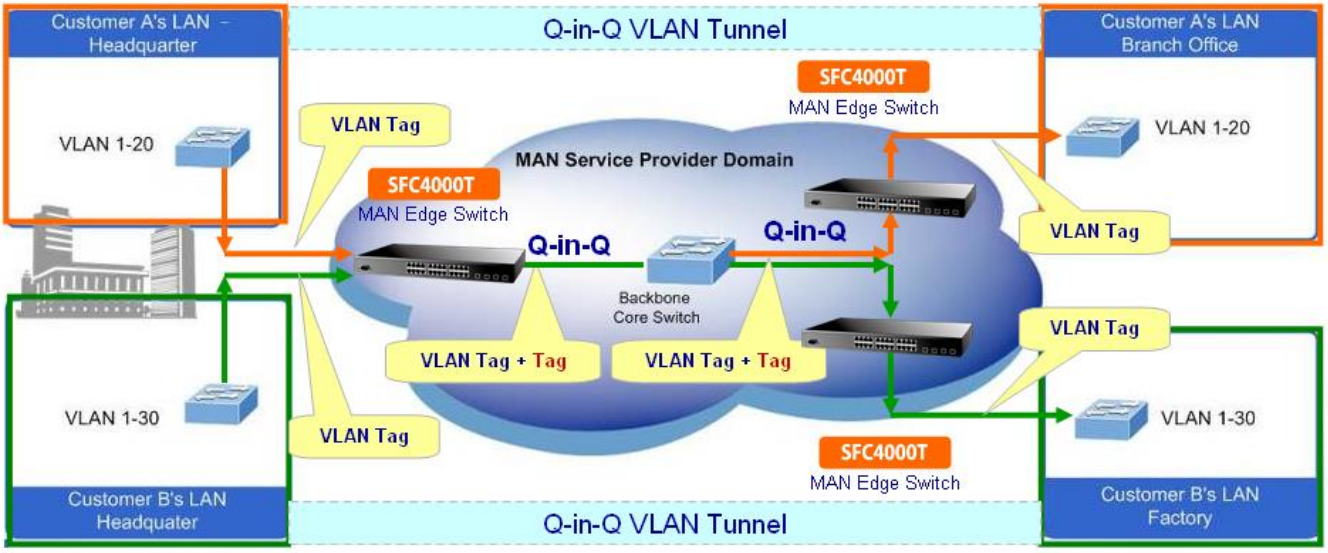
출입 프레임 / 방출 프레임	태그된 출입프레임	태그되지 않은 프레임
태그된 방출 Port	프레임이 태그되어있습니다.	태그가 삽입되었습니다.
태그되지 않은 방출 Port	태그가 제거되었습니다.	프레임이 태그되지 않은채로 남았습니다.

테이블 4-6-1 Ingress/Egress port with VLAN VID Tag/Untag 테이블

■ 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 2 계층 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 구성을 제한하고 VLAN 매핑 테이블을 집중적으로 처리해야하며 최대 VLAN 한계 인 4096 을 쉽게 초과 할 수 있습니다.



Managed Switch 는 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 Port 만있는 경우 특정 VLAN 에 대해 학습을 비활성화 할 수 있으므로 두 Port 간의 포워딩 메커니즘으로 플러딩을 사용할 수 있습니다. 이렇게하면 MAC 테이블 요구 사항이 줄어 듭니다.

VLAN Port 구성

The VLAN Port 구성은 다음과같이 4-6-2 처럼 나타난다.

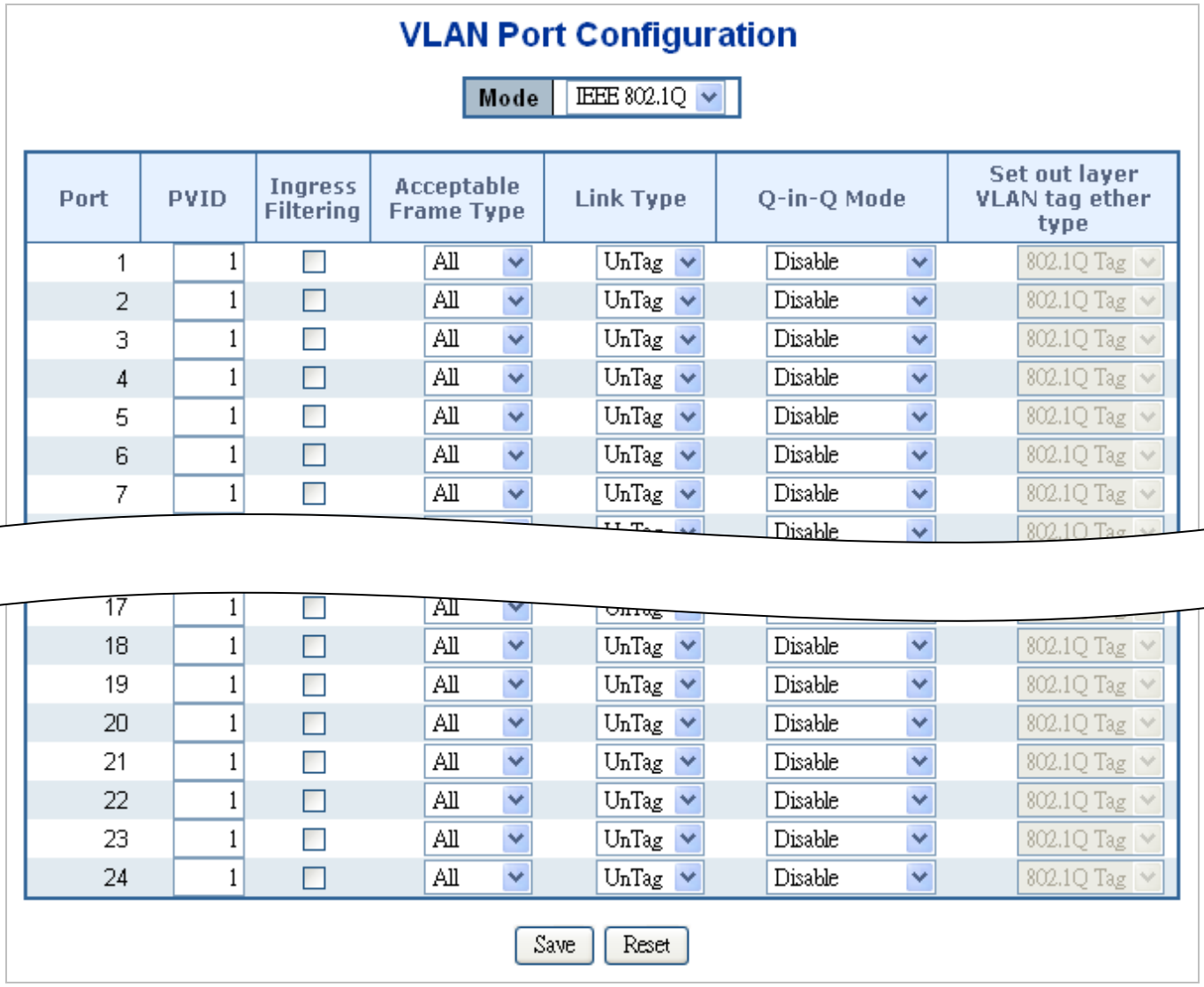


그림 4-6-2 VLAN Port 구성 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• **Port**	논리적인 Port 번호의 행입니다.
• **PVID**	선택한 Port 에 PVID 할당을 허용합니다. PVID 의 범위는 1-4094 입니다. PVID 는 수신 Port 에 들어가는 모든 태그되지 않은 프레임에 삽입됩니다. PVID 는 Port 가 VLAN 그룹에 속한 VLAN ID 와 같아야합니다. 그렇지 않으면 태그없는 트래픽이 삭제됩니다.
Ingress Filtering	상자에 체크하여 Port 에 대한 수신 필터링을 활성화하십시오. 이 매개 변수는 VLAN 수신 처리에 영향을줍니다. 수신 필터링이 활성화되고 수신 Port 가 프레임의 분류 된 VLAN 의 구성원이 아닌 경우 프레임이

	삭제됩니다. 기본적으로 수신 필터링은 비활성화되어 있습니다 (체크 표시 없음)..
• **Accept Frame Type**	Port 가 모든 프레임을 수신할지 태그가 지정된 프레임 만 수신할지 결정합니다. 이 매개 변수는 VLAN 수신 처리에 영향을줍니다. Port 가 태그가 지정된 프레임 만 허용하는 경우 Port 에서 수신 된 태그가없는 프레임은 삭제됩니다. 기본적으로이 필드는 모두로 설정됩니다.
• **Link Type**	선택한 Port 에 대해 802.1Q 태그없는 VLAN 또는 태그 VLAN 허용 선택한 Port 에 VLAN 을 추가하면 스위치가 이탈시 프레임에서 태그를 유지할지 또는 제거할지 여부를 스위치에 알려줍니다. - Untag: VLAN 태그가없는 발신 프레임. - Tagged: VLAN 태그가있는 발신 프레임.
• **Q-in-Q Mode**	관리 스위치를 QinQ 방식으로로 설정하고 QinQ 터널 Port 를 구성 할 수 있습니다. 기본값은 관리 대상 스위치가 비활성화 방식으로로 작동하는 것입니다. - Disable: Port 가 정상적인 Vlan 방식에서 작동합니다(기본값) - MAN port: 서비스 공급자 네트워크 내의 다른 장치에 대한 업 링크 Port 에 대한 IEEE 802.1Q 터널링 (QinQ)을 구성합니다. - Customer port: 클라이언트 액세스 Port 에 대한 IEEE 802.1Q 터널링 (QinQ)을 구성하여 서비스 공급자 네트워크를 통과하는 트래픽의 고객 VLAN ID 를 분리하고 보존합니다.
Set Out layer VLAN tag ether type	TPID (Tag Protocol Identifier)는 터널 액세스 Port 에서 들어오는 패킷의 이더넷 유형을 지정합니다. - 802.1Q Tag: 8100 - vMAN Tag: 88A8 Default : 802.1Q Tag

Port 는 Port VLAN ID 와 동일한 VLAN 의 구성원이어야합니다..

버튼

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

3.6.5 VLAN Membership

■ VLAN 정적 정적멤버 추가 (Vlan 인덱스)

VLAN 정적 테이블을 사용하여 선택한 VLAN 인덱스에 대한 Port 구성원을 구성합니다. 선택한 스택 스위치 / 유닛 스위치에 대한 VLAN 멤버십 구성을 여기에서 모니터링하고 수정할 수 있습니다. 최대 255 개의 VLAN 이 지원됩니다. 이 페이지에서는 VLAN 추가 및 삭제는 물론 각 VLAN 의 Port 구성원을 추가 및 삭제할 수 있습니다. 그림 4-6-3 의 VLAN Membership 화면이 나타납니다.

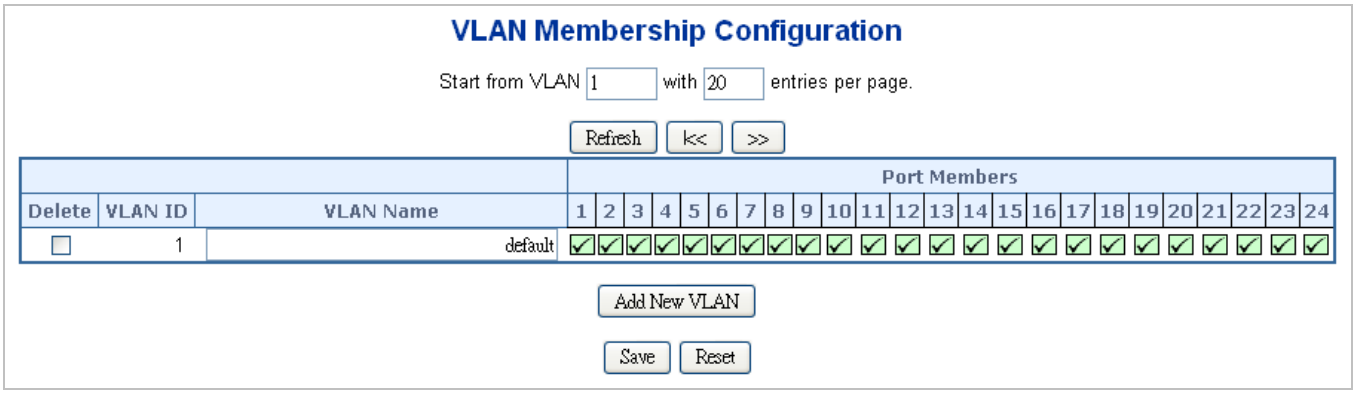


그림 4-6-3 VLAN Membership 구성 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• **Delete**	VLAN 항목을 삭제하려면이 상자를 선택하십시오. 다음 저장 중에 모든 스택 스위치 장치에서 항목이 삭제됩니다.
• **VLAN ID**	특정 VLAN 의 ID 를 나타냅니다.
• **VLAN Name**	VLAN 의 이름을 나타냅니다. 길이는 최대 32 이며 이름은 알파벳과 숫자를 포함해야 하며 최소한 하나의 알파벳을 포함해야합니다. Vlan 이름은 기존 Vlan 항목에 대해 편집하거나 새항목에 추가 할 수 있습니다.
• **Port Members**	각 VLAN ID 에 행의 체크박스가 각 포트마다 나타납니다. ☑ Vlan 포트에 포함시키려면 체크박스를 선택하세요 ☒ 금지된 포트 목록에 포함시키려면 체크박스를 선택하세요 ☐ . VLAN 에 포트를 제거 및 제외하려면 선택상자처럼 비활성화 합니다.. 기본적으로 포트는 구성원이아니며 새로운 모든 업무에 선택되지 않습니다
• **Adding a New VLAN**	"Add New VLAN (새 VLAN 추가)"을 클릭하여 새 VLAN ID 를 낮은 순위로추가합니다. 빈 행이 테이블에 추가되고 필요에 따라 VLAN 을 구성 할 수 있습니다. VLAN ID 의 유효한 값은 1 ~ 4095 입니다.

	VLAN 은 "저장"을 클릭하면 활성화됩니다. "삭제"버튼을 사용하여 새 VLAN 추가를 취소 할 수 있습니다.

버튼

Add New Entry: 새로운 Vlan 을 추가합니다..

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

Refresh: Vlan ID 입력 필드에서 표시된 테이블을 새로 고침한다.

<<: VLAN 테이블의 첫 번째 항목, 즉 VLAN ID 가 가장 낮은 항목부터 테이블을 업데이트합니다,

4.4 Vlan 맴버쉽 상태

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

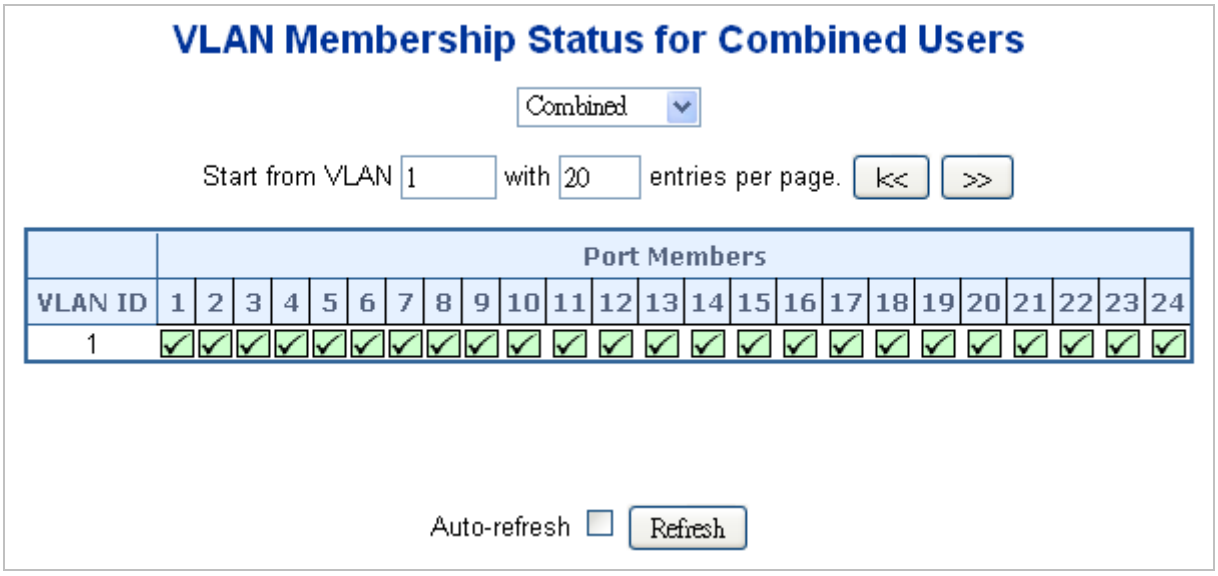


그림 4-6-4 VLAN Membership 상태 정적 사용자 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• VLAN user	VLAN 사용자는 VLAN 관리 기능의 서비스를 사용하여 PVID, UVID 와 같은 VLAN 구성원 및 VLAN Port 구성을 구성하는 모듈입니다. 현재 우리는 다음과 같은 VLAN 을 지원합니다 - CLI/Web/SNMP : 이것은 정적으로 간주된다 - NAS : NAS 는 요청자 , 입안자 및 인증 서버 간의 통신을 포함하는 Port 기반 인증을 제공합니다.

	- Voice VLAN: Voice VLAN 은 일반적으로 IP 전화에서 발생하는 음성 트래픽을 위해 특별히 구성된 VLAN 입니다 - MVR : MVR 은 각 VLAN 의 가입자에 대한 멀티캐스트 트래픽을 복제 할 필요를 없애기 위해 사용됩니다. 모든 채널의 멀티 캐스트 트래픽은 단일 (멀티 캐스트) VLAN 에서만 전송됩니다.. - MSTP : 802.1s MSTP (Multiple Spanning Tree Protocol)는 VLAN 을 사용하여 네트워크에서 여러 스패닝 트리를 생성하므로 네트워크 환경을 유지하면서 네트워크 자원 활용도를 크게 향상시킵니다.
• Port Members	각 VLAN ID 마다 각 포트의 확인란 행이 표시됩니다. 포트가 Vlan 에 포함되어있으면 표시됩니다. 포트가 금지 된 포트 목록에 포함되면 이미지가 표시됩니다. 포트가 동일한 금단 포트 금지 포트 목록 및 동적 VLAN 사용자 레지스터 VLAN 에 포함되면, 충돌은 충돌 포트 포트로 표시한다.
• 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 표시되며 이는 기본적으로 나타납니다. VLAN 멤버십을 사용하면 VLAN ID 로 분류 된 프레임을 각 VLAN 멤버 포트에서 전달할 수 있습니다.

버튼

Static :Vlan 사용자에 드롭다운리스트를 선택하세요..

Auto-refresh : 선택한경우 페이지를 3 초마다 자동으로 새로 고칩니다...

Refresh : 즉시 페이지를 새로 고칩니다.

<< : Vlan 의 테이블 첫 번째 항목, 즉 Vlan ID 가 가장 낮은 항목부터 테이블을 업데이트합니다.

>> : 현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 업데이트 합니다.

3.6.7 VLAN Port status

Vlan 상태포트는 그림 4-6-5 와 같이 나타납니다 .

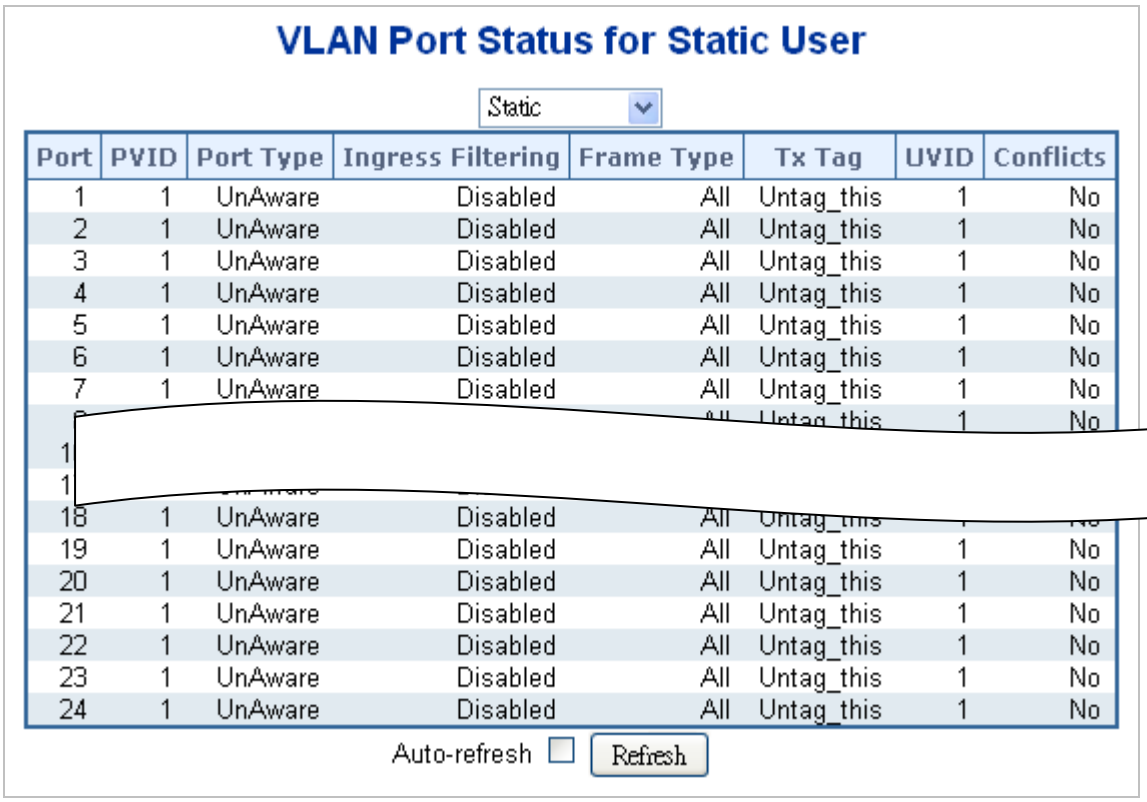


그림 4-6-5 VLAN Port status 수동 사용자설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Port	같은 행의 포함된 논리포트의 설정입니다.
• PVID	기본값이 1 인 Vlan 의 식별자를 보여주고 허용값은 1~4095 입니다.
• Port Type	포트에 Vlan 에 알고있는 것을 보여줍니다 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 변수는 VLAN 수신 처리에 영향을줍니다. 수신 필터링이 활성화되고 수신 포트가 프레임의 분류 된 VLAN 의 구성원이 아닌 경우 프레임은 폐기됩니다.
• Frame Type	포트가 모든 프레임을 허용하는지 태그가 지정된 프레임 만 허용하는지 표시합니다. 이 변수는 VLAN 수신 처리에 영향을줍니다. 포트가 태그가있는 프레임 만 수신하는 경우 해당 포트에서 수신 된 태그가없는 프레임은 무시됩니다.
• Tx Tag	지정 태그인지 아닌지에 따라 출력 필터링 프레임 상태를 표시합니다.

• UVID	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 인해 충돌이 발생합니다. 사용자 모듈 간의 직접 충돌.

버튼

: 사용자 Vlan 의 내림목록에서 선택합니다..

Auto-refresh  : 선택한경우 페이지를 3 초마다 자동으로 새로 고칩니다...

: 즉시 페이지를 새로 고칩니다.

3.6.8 Private VLAN

스위치의 개인 VLAN 멤버쉽 구성은 여기에서 모니터링하고 수정할 수 있습니다. 여기에 Private VLAN 을 추가하거나 삭제할 수 있습니다. 각 Private VLAN 의 포트 구성원을 여기에 추가하거나 제거 할 수 있습니다.
Private VLAN 은 소스 포트 마스크를 기반으로하며 VLAN 에 연결되지 않습니다. 이는 VLAN ID 와 Private VLAN ID 가 동일 할 수 있음을 의미합니다.
패킷을 전달할 수 있으려면 포트가 VLAN 및 Private VLAN 의 구성원이어야합니다. 기본적으로 모든 포트는 VLAN 을 인식하지 않으며 VLAN 1 및 개인 VLAN 1 의 구성원입니다.
VLAN 비 인식 포트는 하나의 VLAN 의 멤버 일 수 있지만 여러 개인 VLAN 의 멤버 일 수 있습니다.
그림 4-6-6 의 Private VLAN 화면이 나타납니다.

그림 4-6-6 Private VLAN Membership 구성 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• **Delete**	Private VLAN 항목을 삭제하려면이 상자를 선택하십시오. 항목은 다음 저장 중에 삭제됩니다.
• **Private VLAN ID**	이 특정 개인 VLAN 의 ID 를 나타냅니다.
• **Port Members**	각 포트의 확인란 행은 각 Private VLAN ID 에 대해 표시됩니다. Private VLAN 에 포트를 포함 시키려면 상자를 선택하십시오. Private VLAN 에서

	포트를 제거하거나 제외하려면 상자가 선택 해제되어 있는지 확인하십시오. 기본적으로 포트는 구성원이 아니며 모든 상자는 선택되지 않습니다.
• **Adding a New Private VLAN**	"새 개인 VLAN 추가"를 클릭하여 새 개인 VLAN ID 를 추가하십시오. 빈 행이 테이블에 추가되고 필요에 따라 Private VLAN 을 구성 할 수 있습니다. Private VLAN ID 의 허용 범위는 스위치 포트 번호 범위와 동일합니다. 이 범위를 벗어난 값은 허용되지 않으며 경고 메시지가 나타납니다. "OK"를 클릭하여 잘못된 항목을 버리거나 "취소"를 클릭하여 편집으로 돌아가서 수정하십시오. "저장"을 클릭하면 Private VLAN 이 활성화됩니다. "Delete (삭제)"버튼을 사용하여 새 개인 VLAN 추가를 취소 할 수 있습니다.

버튼

Add new Private VLAN: Vlan 을 새로 추가합니다..

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

Auto-refresh : 선택한경우 페이지를 3 초마다 자동으로 새로 고칩니다...

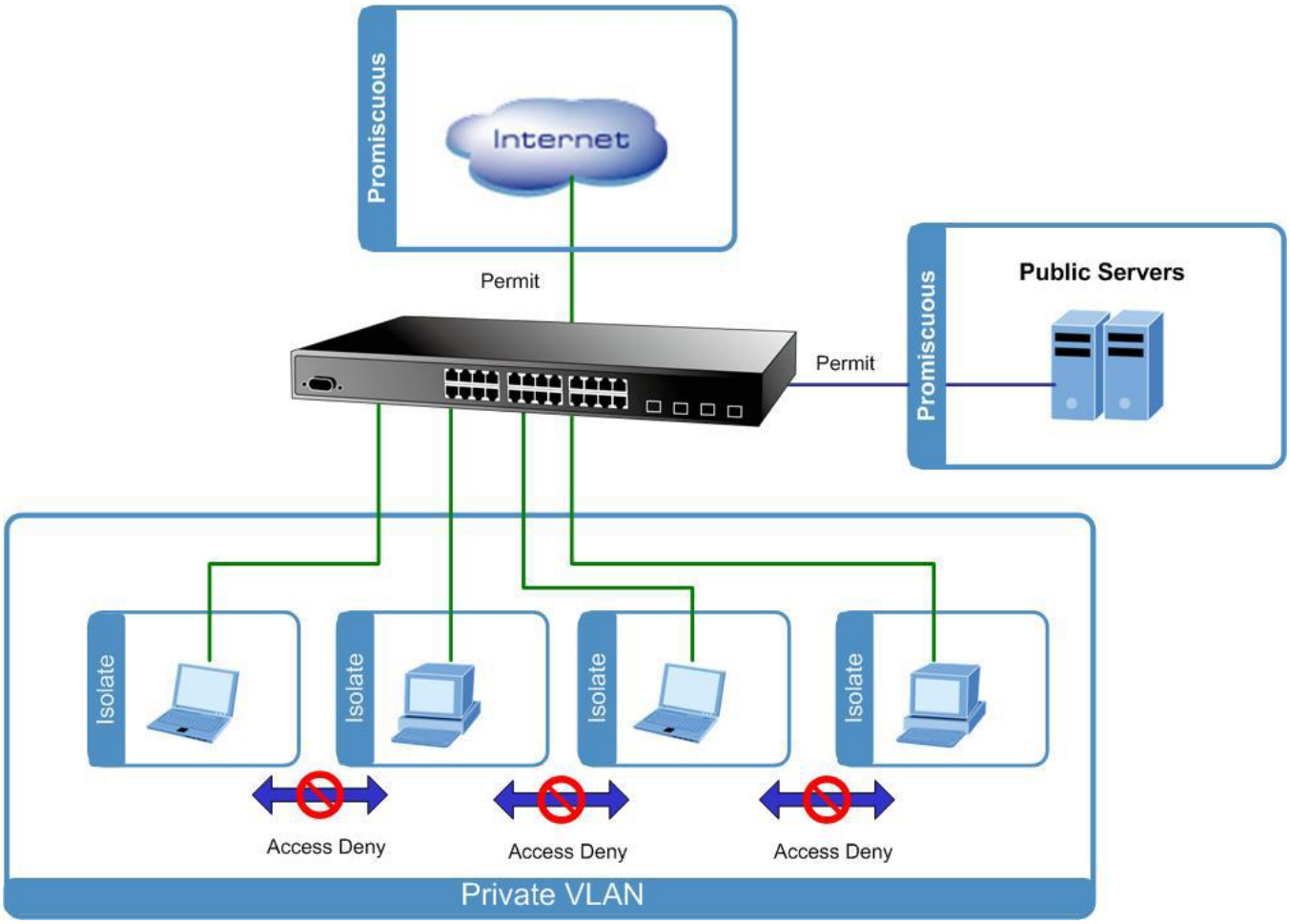
Refresh: 즉시 페이지를 새로 고칩니다.

3.6.9 Port isolation

개요

Vlan이 PrivateVlan으로 구성되면 해당 Vlan 내의 포트 간 통신이 차단 될 수있어 두가지 응용 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



Private VLAN을 적용하려면 스위치를 먼저 표준 VLAN 작동을 위해 구성해야합니다. 이 스위치를 배치하면 하나 이상의 구성 VLAN을 Private VLAN으로 구성 할 수 있습니다. Private VLAN의 포트는 다음 두 그룹 중 하나에 속합니다.

- 무분별한 포트
  - 트래픽을 개인 Vlan의 모든 포트로 전달 할 수 있는 포트
  - 개인 VLAN의 모든 포트로부터 트래픽을 수신 할 수 있는 포트
- 독립 포트
  - 트래픽을 개인 Vlan의 무분별 포트로만 전달 할 수 잇는 포트
  - 개인 VLAN의 무분별 포트에서만 트래픽을 수신 할 수 있는 포트

무분별 및 독립 포트의 구성은 모든 Private VLAN에 적용됩니다. 트래픽이 Private VLAN의 무분별 포트로 들어 오면 VLAN 테이블의 VLAN 마스크가 적용됩니다. 독립 된 포트에서 트래픽이 들어 오면 Private VLAN 마스크가 VLAN 테이블의 VLAN 마스크에 추가로 적용됩니다. 이렇게하면 포워딩을 수행 할 수있는 포트가 Private VLAN 내의 무차별 포트로만 줄어 듭니다.

이 페이지는 Private VLAN의 포트에서 포트 독립성을 활성화 또는 비활성화하는 데 사용됩니다. VLAN의 포트 구성원은 동일한 VLAN 및 Private VLAN의 다른 독립 된 포트로 Isolation 될 수 있습니다. 그림 4-6-7의 포트 독립 화면이 나타납니다.

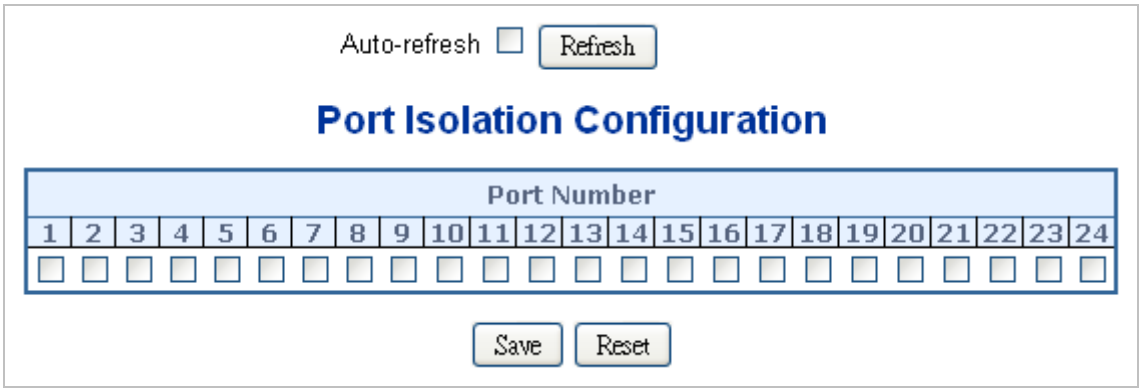


그림 4-6-7 Port Isolation 구성 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Port Members	Private Vlan 의 각 포트가 체크박스로 제공됩니다. 체크했을 경우 포트의 독립성이 활성화 되고 체크하지 않을경우(기본값) 비활성화합니다.

버튼

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

Auto-refresh : 선택한경우 페이지를 3 초마다 자동으로 새로 고칩니다...

Refresh: 즉시 페이지를 새로 고칩니다.

3.6.10 VLAN 셋팅 예제

- Separate VLAN
- 802.1Q VLAN Trunk
- Port Isolate

3.6.10.1 두 부류의 802.1Q VLAN

이 다이어그램이 관리형 스위치가 두 Vlan 태그 및 언태그 트래픽 흐름을 처리하는 방법을 보여줍니다. VLAN 그룹 2 와 3 은 분류되는데 각 네트워크 트래픽을 Vlan 멤버만 동일한 맴버의 트래픽을 수신합니다. 그림 4-6-8 의 화면이 나타나고 표 4-6-9 는 관리형 스위치의 포트 구성을 설명합니다.

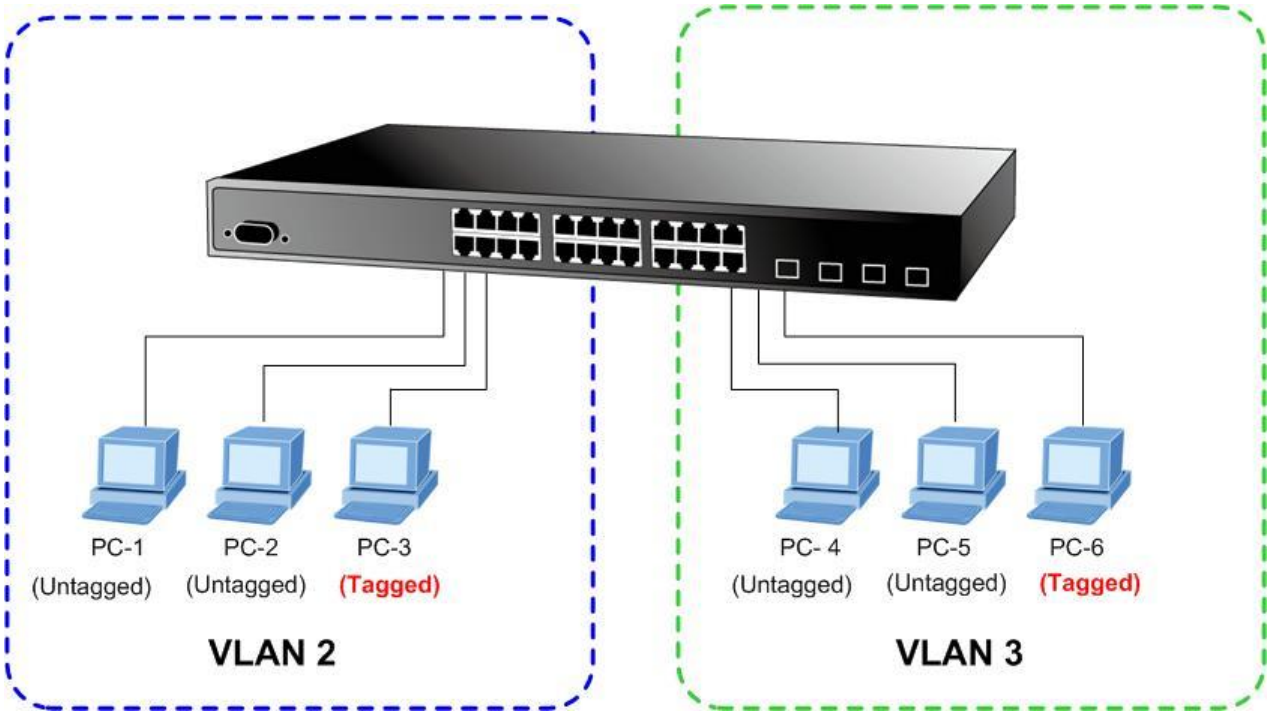


그림 4-6-8 두 부류의 VLAN 다이아그램

VLAN 그룹	VID	태그되지 않은 포트	태그된 포트
VLAN 그룹 1	1	Port-7 ~ Port-10	N/A
VLAN 그룹 2	2	Port-1,Port-2	Port-3
VLAN 그룹 3	3	Port-4,Port-5	Port-6

Table 4-1 VLAN and Port 구성

시나리오는 다음과 같이 설명됩니다.

VLAN 2에 들어가는 태그 없는 패킷

1. [PC-1]이 untagged 패킷을 Port-1로 전송하는 동안, Managed Switch는 VLAN Tag = 2로 태그를 붙입니다. [PC-2] 및 [PC-3]은 Port-2 및 Port-3을 통해 패킷을 수신합니다.
2. [PC-4], [PC-5] 및 [PC-6]에는 패킷이 수신되지 않았습니다.
3. 패킷이 Port-2를 떠나는 동안 태그가 제거되어 태그가 태그없는 패킷이됩니다.
4. 패킷이 Port-3을 떠나는 동안 VLAN Tag = 2 인 태그가 지정된 패킷으로 유지됩니다.

■ VLAN 2에 들어가는 태그가있는 패킷

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.

■ VLAN 3에 들어가는 태그없는 패킷

1. [PC-4]가 태그가없는 패킷을 포트 -4로 전송하는 동안 스위치는 VLAN 태그 = 3으로 태그를 붙입니다. [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

이 예제로 Vlan 의 1 번 그룹은 기본이고 vlan2 와 3 은 트래픽의 흐름을 목표로 한다.

설치 단계

1. Vlan 그룹을 생성

Vlan 그룹 1 번 = 기본 Vlan 과 VID (vlan ID)=1

두개의 Vlan 을 추가 -Vlan2 와 Vlan 3

VLAN 그룹 2 와 VID=*2*

VLAN 그룹 3 와 VID=*3*

2. Vlan 멤버 등록:

VLAN 2 : Port-1,Port-2 and Port-3

VLAN 3 : Port-4, Port-5 and Port-6

VLAN 1 : All other Port – Port-7~Port-10

3. VLAN 1에서 Vlan 멤버를 제거 :

Vlan1 멤버십에서 포트 1 번-6 번 을 제거해야한다 vlan2 과 3 에 할당하였으므로

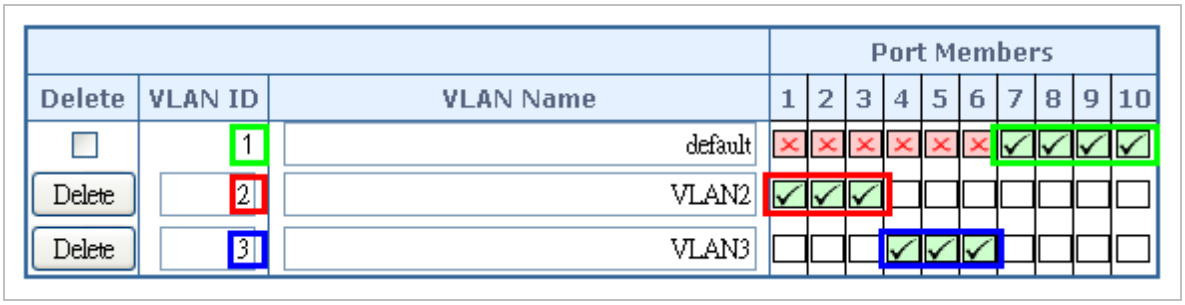


그림 4-6-9 새로운 Vlan 그룹을 추가하고 Vlan 의 2 번과 3 번의 특정포트를 1 번에서 제외할수 있다.

Note

Vlan 1 구성에서 Vlan 멤버를 제거하는 것은 중요하고 중복 설정되는것입니다. 중복 Vlan 구성에 eoo 선 다음 Vlan 예제 구성안을 볼수있다.

4. 각 포트에 PVID를 등록한다.:

   Port-1,Port-2 and Port-3 : PVID=*2*

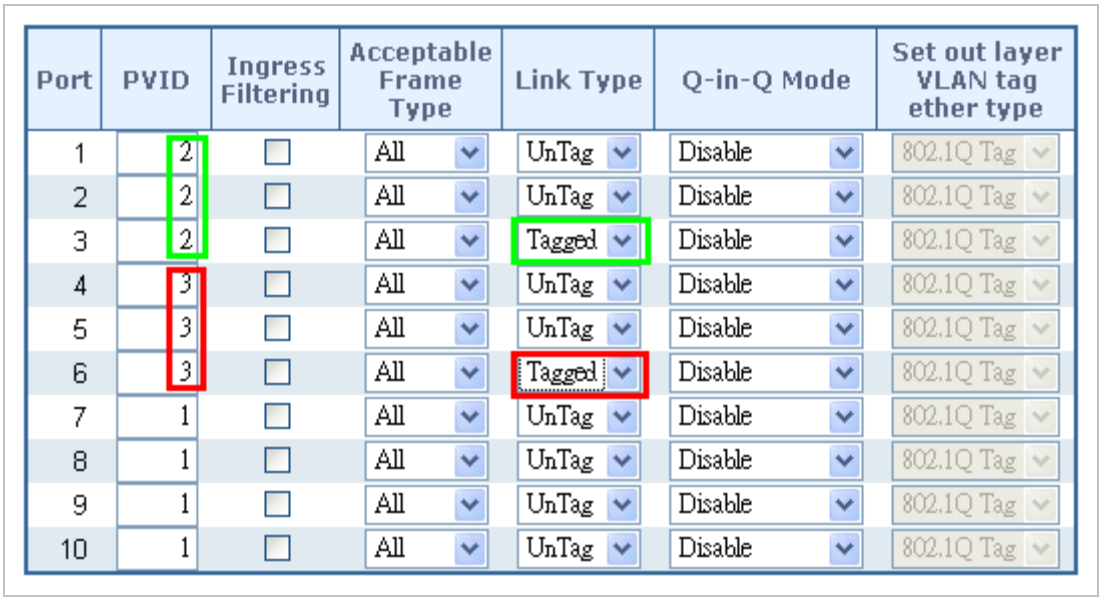
   Port-4,Port-5 and Port-6 : PVID=*3*

   Port-7~Port-10 : PVID=*1*

5. 특정포트에 Vlan 태그를 넣을수 있다.

   링크 타입: *Port-3* (VLAN-2) 과 *Port-6* (VLAN-3)

그림 4-6-10 각 포트 Vlan 을 나타낸다.

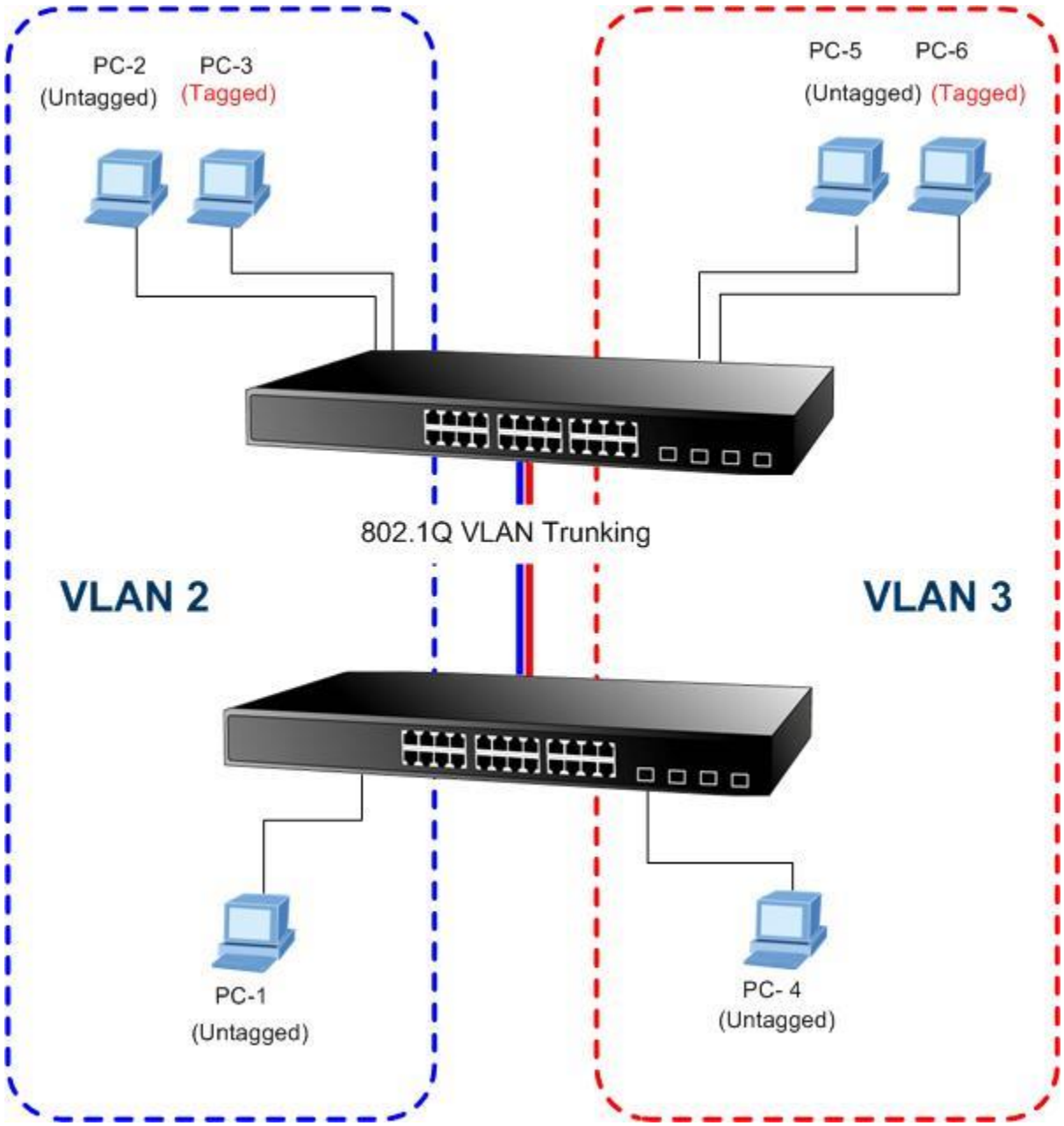


Port	PVID	Ingress Filtering	Acceptable Frame Type	Link Type	Q-in-Q Mode	Set out layer VLAN tag ether type
1	2	☐	All	UnTag	Disable	802.1Q Tag
2	2	☐	All	UnTag	Disable	802.1Q Tag
3	2	☐	All	Tagged	Disable	802.1Q Tag
4	3	☐	All	UnTag	Disable	802.1Q Tag
5	3	☐	All	UnTag	Disable	802.1Q Tag
6	3	☐	All	Tagged	Disable	802.1Q Tag
7	1	☐	All	UnTag	Disable	802.1Q Tag
8	1	☐	All	UnTag	Disable	802.1Q Tag
9	1	☐	All	UnTag	Disable	802.1Q Tag
10	1	☐	All	UnTag	Disable	802.1Q Tag

그림 4-6-10 Port 1-Port 6 VLAN 구성

3.6.10.2 Vlan 트렁킹과 802.1Q 의 두 인식스위치

대부분의 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.



설치 단계

1. Vlan 그룹 생성

VLAN Group 1 설치 = 기본 Vlan 과 VID(vlan ID) =1

2 개 Vlan – VLAN 2 and VLAN 3

VLAN Group 2 과 VID=*2*

VLAN Group 3 과 VID=*3*

2. Vlan 맴버 등록:

VLAN 2 : Port-1,Port-2 and Port-3

VLAN 3 : Port-4, Port-5 and Port-6

VLAN 1 : All other Port – Port-7~Port-10

VLAN 포트 정보는 호스트에 연결됩니다 (3.6.10.1 예 참조). 다음 단계는 VLAN 트렁크 포트 구성에 초점을 맞춥니다.

1. 포트 8을 802.1Q VLAN 트렁크 포트로 지정하십시오.
2. VLAN 멤버 구성 페이지에서 Port-8을 VLAN 2와 VLAN 3에 모두 할당합니다.
3. VLAN 1을 VLAN 2 구성원과 VLAN 3 구성원과 겹치는 "공용 영역"으로 정의하십시오.
4. VLAN 트렁크 포트를 각 VLAN의 구성원으로 할당합니다. - 집계 할 VLAN입니다. 이 샘플에서는 Port-8을 VLAN 2 및 VLAN 3 구성원 포트로 추가하십시오. 그림 4-6-12의 화면이 나타납니다.

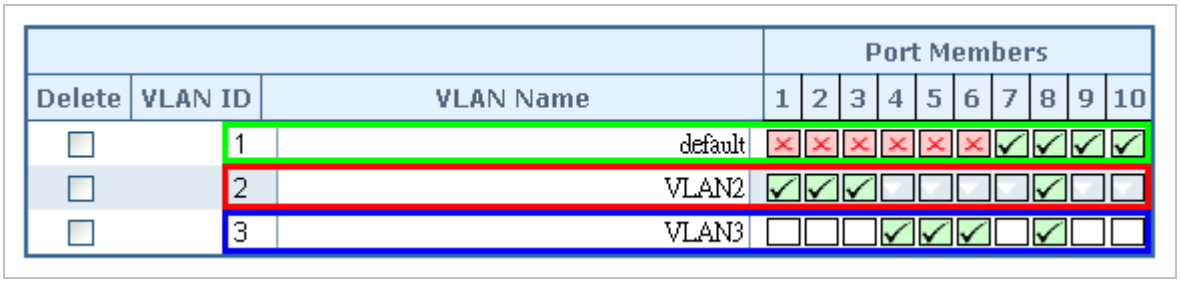


그림 4-6-12 VLAN 의 중복 포트 셋팅과 Vlan1 - 공공 지역에 등록되는 맴버

5. 포트 8을 802.1Q VLAN 트렁크 포트로 지정하고 트렁킹 포트는 송신 중에 태그 지정 포트 여야합니다. Port-8은 그림 4-6-13의 다음 화면과 같이 구성됩니다

그림 4-6-13 Vlan 트렁크 포트 구성

6. 1 ~ 5 단계를 반복하고 파트너 스위치에서 VLAN 트렁크 포트를 설치하고 VLAN 트렁크에 참가할 다른 VLAN 을 추가 한 후 1 ~ 3 단계를 반복하여 트렁크 포트를 VLAN 에 할당합니다.

즉, VLAN 2 구성원 인 Port1 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 접근합니다.

3.6.10.3 독립 포트

이 다이어그램은 관리스위치 가 Isolation 포트와 무차별 포트를 처리하는 방법을 보여 주며 각 PC 는 각 Isolation 포트의 서로 다른 PC 에 접근 할 수 없습니다. 하지만 그들은 모두 동일한 서버 / AP / 프린터로 접근해야합니다. 그림 4-6-14 의 화면이 나타납니다. 이 섹션에서는 각 분리 포트에 접근 할 수있는 서버 포트를 구성하는 방법을 보여줍니다.

설치 단계

1. 지정 포트 방식

독립 포트에 Port-1 ~ Port-4 를 설정합니다.

무차별 포트에 Port5 및 Port-6 을 설정하십시오. 그림 4-6-15 의 화면이 나타납니다.

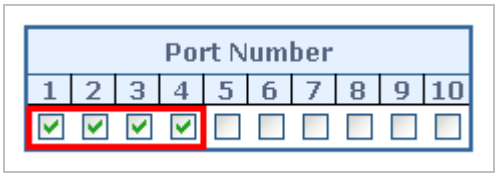


그림 4-6-15 무작위 포트의 구성과 독립

2. Vlan포트 멤버스에 구성:

VLAN 1 : Port-1,Port-2 ,Port-5 과 Port-6

VLAN 2 : Port-3~Port-6.그림 4-6-16 에 나타난다.

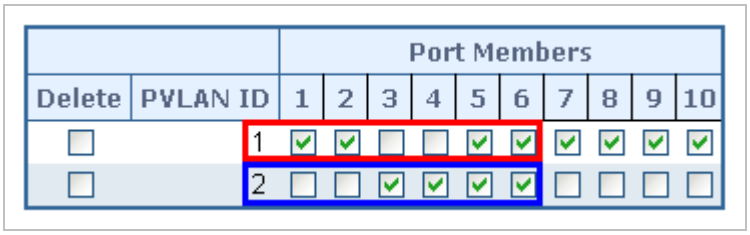


그림 4-6-16 Pvlan 포트 생성

3.6.11 MAC 기반 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 4-6-17 의 MAC 기반 VLAN 화면이 나타납니다.

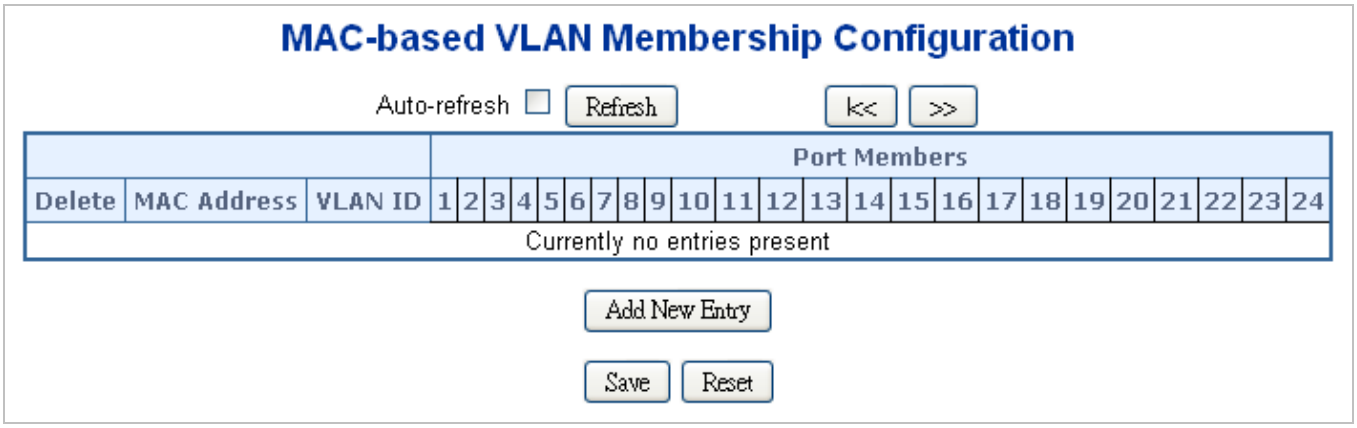


그림 4-6-17 MAC 기반 VLAN Membership 구성 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description

• Delete	MAC 기반 VLAN 항목을 삭제하려면이 상자를 선택하고 저장을누릅니다. 항목이 스택에서 삭제됩니다.
• MAC Address	MAC 주소를 나타냅니다.
• VLAN ID	Vlan ID 를 나타냅니다.
• Port Members	MACbased VLAN 항목마다 각 포트의 확인란 행에 표시됩니다. MAC 기반 VLAN 에 포트를 포함하려면 해당 상자를 선택하십시오. MAC 기반 VLAN 에서 포트를 제거하거나 제외하려면 상자가 선택 해제되어 있는지 확인하십시오. 기본적으로 포트는 구성원이 아니며 모든 상자는 선택되어 있지 않습니다.
• Adding a New MACbased VLAN	"Add New Entry"를 클릭하여 새로운 MAC 기반 VLAN 항목을 추가하십시오. 테이블에 빈 행이 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. "저장"을 클릭하면 MAC 기반 VLAN 항목이 활성화됩니다. "저장"을 클릭하면 포트 구성원이없는 MAC 기반 VLAN 이 삭제됩니다. "삭제"버튼은 새로운 MAC 기반 VLAN 의 추가를 취소하는 데 사용할 수 있습니다.

버튼

Add New Entry: 새로운 맥기반 Vlan 의 99

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

Auto-refresh : 선택한경우 페이지를 3 초마다 자동으로 새로 고칩니다...

Refresh: 즉시 페이지를 새로 고칩니다.

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

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

3.6.12 MAC 기반으로한 Vlan 의 상태

이 페이지는 다양한 MAC 기반 VLAN 사용자가 구성한 MAC 기반 VLAN 항목을 표시합니다. 그림 4-6-18 의 MAC 기반 VLAN 상태 화면이 나타납니다.

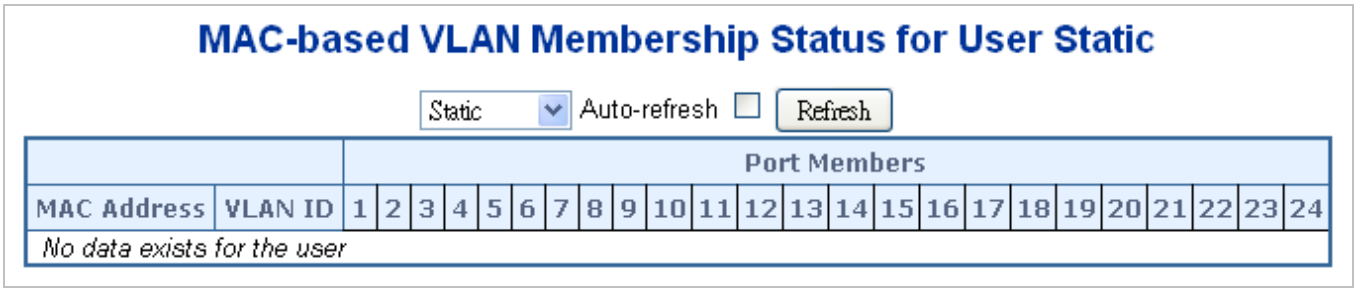


그림 4-6-18 MAC 기반 Vlan Membership 사용자 수동 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• MAC Address	MAC 주소를 나타낸다
• VLAN ID	Vlan ID 를 나타낸다
• Port Members	Vlan 엔트리의 MAC 기반 포트 맴버를 나타낸다.

버튼

Auto-refresh : 선택한경우 페이지를 3 초마다 자동으로 새로 고칩니다...

Refresh: 즉시 페이지를 새로 고칩니다.

3.6.13 IP 서브넷 기반 VLAN

IP 서브넷 기반 VLAN 엔티티는 여기에서 구성 할 수 있습니다. 이 페이지에서는 IP 서브넷 기반 VLAN 항목을 추가, 업데이트 및 삭제하고 다른 포트에 항목을 할당 할 수 있습니다. 이 페이지에는 정적 항목 만 표시됩니다. 그림 4-6-19 의 IP 기반 VLAN 화면이 나타납니다.

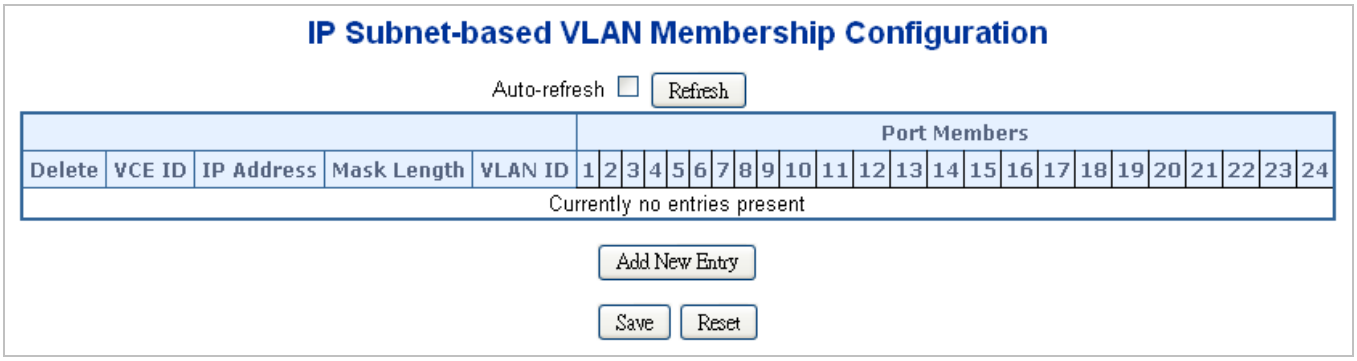


그림 4-6-19 Protocol to Group Mapping Table 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Delete	그룹 이름에 대한 프로토콜을 삭제하려면이 상자를 선택하십시오. 항목은 다음 저장 중에 스위치에서 삭제됩니다
• VCE ID	항목의 색인을 나타냅니다. 그것은 사용자가 구성 할 수 있습니다. 값 범위는 0-256 입니다. VCE ID 가 0 이면 응용 프로그램은 해당 항목의 VCE ID 를 자동으로 생성합니다. IP 서브넷 기반 VLAN 의 삭제 및 조회는 VCE ID 를 기반으로합니다.
• IP Address	IP 주소를 나타냅니다.
• Mask Length	네트워크 마스크 길이를 나타냅니다.
• VLAN ID	VLAN ID 를 나타냅니다. VLAN ID 는 기존 항목에 대해 변경할 수 있습니다.
• Port Members	각 IP 서브넷 기반 VLAN 항목에 대해 각 포트의 확인란 행이 표시됩니다. IP 서브넷 기반 VLAN 에 포트를 포함하려면 해당 상자를 선택하십시오. IP 서브넷 기반 VLAN 에서 포트를 제거하거나 제외하려면 상자가 선택 해제되어 있는지 확인하십시오. 기본적으로 포트는 구성원이 아니며 모든 상자는 선택되어 있지 않습니다
• Adding a New IP subnetbased VLAN	새 IP 서브넷 기반 VLAN 항목을 추가하려면 "새 항목 추가"를 클릭하십시오. 테이블에 빈 행이 추가되고 필요에 따라 IP 서브넷 기반 VLAN 항목을 구성 할 수 있습니다. 모든 IP 주소 / 마스크는 IP 서브넷 기반 VLAN 항목에 대해 구성 할 수 있습니다. VLAN ID 의 유효한 값은 1 ~ 4095 입니다. IP 서브넷 기반 VLAN 항목은 "저장"을 클릭하면 활성화됩니다. "삭제 :"버튼을 사용하여 새 IP 서브넷 기반 VLAN 추가를 취소 할 수 있습니다.

버튼

Add New Entry: 메핑테이블을 새로 추가합니다.

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

Auto-refresh : 선택한경우 페이지를 3 초마다 자동으로 새로 고칩니다...

Refresh: 즉시 페이지를 새로 고칩니다.

3.6.14 프로토콜 기반 Vlan

이 페이지에서는 그룹이름(고유 이름) 메핑 항목에 새 프로토콜을 추가하고 스위치에 이미 매핑 된 항목을 보고 삭제 할 수 있습니다. 그림 4-6-20 의 프로토콜기반 Vlan 화면 입니다.

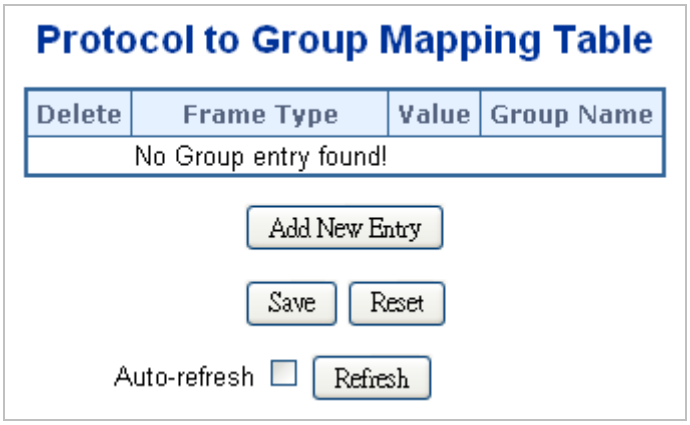


그림 4-6-20 Protocol to Group Mapping Table 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Delete	그룹 이름에 대한 프로토콜을 삭제하려면 상자를 선택하십시오, 항목은 다음 중 저장 스위치에서 삭제된다 .
• Frame Type	프레임 유형은 다음 중 하나를 갖는다. 1. Ethernet 2. LLC 3. SNAP 참고 : 프레임 유형 필드를 변경하면 다음 문자항목에 유효값이 선택한 새 프레임 유형에 따라 달라진다.
• Value	이 텍스트 필드에 입력 할 수있는 유효한 값은 이전 프레임 유형 선택 메뉴에서 선택한 옵션에 따라 다릅니다. 다음은 세 가지 프레임 유형에 대한 기준입니다. 1. For Ethernet: 프레임 유형으로 이더넷을 선택한 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 길이의 문자열 (0x00-0xff) b. SSAP: 1 바이트 길이의 문자열 (0x00-0xff) 3. For SNAP: 이 경우 유효한값은 두개의 다른 하위 값으로 구성된다. a.OUI: OUI (Organizationally Unique Identifier) 는 xx-xx-xx 형식의

	값으로 문자열의 각 쌍 (xx)은 0x00-0xff 의 16 진수 값 범위입니다. b. PID: OUI 가 16 진수 000000 이면 프로토콜 ID 는 SNAP 상단에서 실행되는 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. 즉, 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 표에 추가됩니다. 프레임 유형, 값 및 그룹 이름은 필요에 따라 구성 할 수 있습니다. "삭제"버튼을 사용하여 새 항목의 추가를 취소 할 수 있습니다.

버튼

Add New Entry: 메핑테이블안에 새로운 엔트리추가한다.

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

Auto-refresh : 선택한경우 페이지를 3 초마다 자동으로 새로 고칩니다...

Refresh: 즉시 페이지를 새로 고칩니다.

3.6.15 프로토콜 기반의 Vlan 멤버쉽

이 페이지에서 이미 구성한 그룹 이름을 스위치용 VLAN 에 매핑 할 수 있습니다. 그림 4-6-21 의 Group Name to VLAN Mapping Table 화면이 나타납니다.

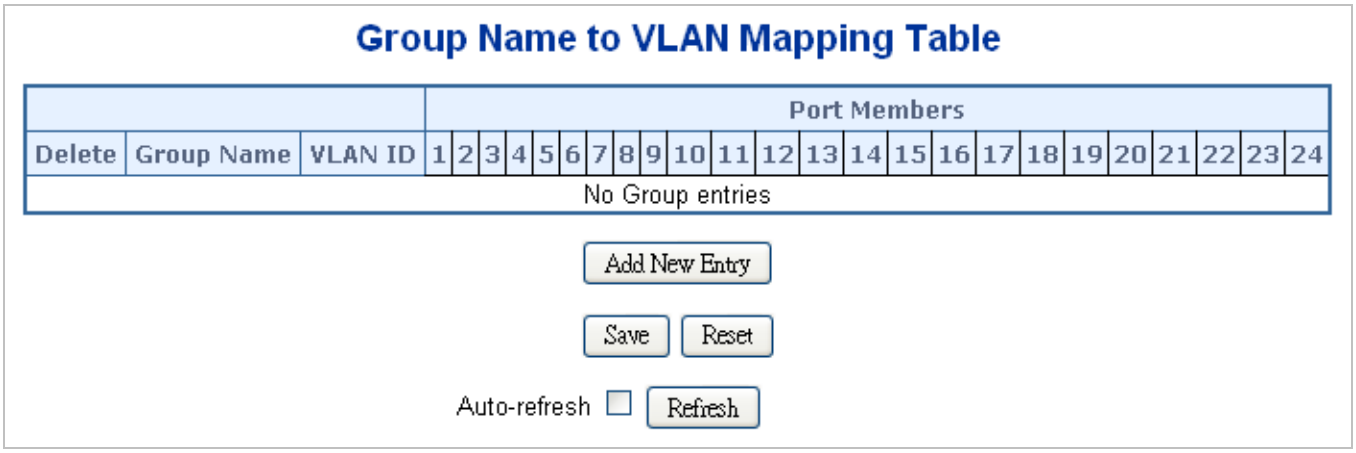


그림 4-6-21 Group Name to VLAN Mapping Table 설정 화면

이 페이지는 다음을 포함해 나타냅니다.

Object	Description
• Delete	그룹 이름 - VLAN 맵 항목을 삭제하려면이 상자를 선택하십시오. 항목은 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 포함 시키려면 상자를 선택하십시오. 매핑에서 포트를 제거하거나 제외하려면 상자가 선택 취소되어 있는지 확인하십시오. 기본적으로 포트는 구성원이 아니며 모든 상자는 선택되어 있지 않습니다.
• Adding a New Group to VLAN mapping entry	"새 항목 추가"를 클릭하여 매핑 테이블에 새 항목을 추가하십시오. 빈 행이 테이블에 추가되고 그룹 이름, VLAN ID 및 포트 구성원을 필요에 따라 구성 할 수 있습니다. VLAN ID 의 유효한 값은 1 ~ 4095 입니다. "삭제"버튼을 사용하여 새 항목의 추가를 취소 할 수 있습니다.

버튼

Save: 변경된 내용을 저장한다.

Reset: 이전에 저장된 값으로 되돌리면 클릭해야한다

Auto-refresh : 선택한경우 페이지를 3 초마다 자동으로 새로 고칩니다...

Refresh: 즉시 페이지를 새로 고칩니다.

3.7 Spanning Tree Protocol(STP)

3.7.1 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 네트워크상의 두 스테이션간에 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)

EEE 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 구성되어 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

d. 기본값을 변경하기 전에 다음을 읽으십시오.

스위치 STP 는 다음 기능을 수행합니다.

- 스위칭 또는 브리징 요소의 모든 조합에서 단일 스패닝 트리를 생성합니다.
- 다중 스패닝 트리를 만든다.- 단일 스위치에 포함 된 포트 조합 (사용자 지정 그룹).
- 트리의 모든 요소의 오류, 추가 또는 제거를 보완하기 위해 스패닝 트리를 자동으로 재구성합니다..
- 운영자 개입없이 스패닝 트리를 재구성합니다.

Bridge Protocol Data Units(BPDU)

STP 가 안정적인 네트워크 토폴로지에 도달하려면 다음 정보가 사용됩니다

- 지정된 스위치 식별자
- 각 스위치 포트와 관련된 루트에 대한 경로 비용
- 포트 구별자

STP 는 BPDU (Bridge Protocol Data Units)를 사용하여 네트워크의 스위치간에 통신합니다. 각 BPDU 에는 다음 정보가 들어 있습니다

- 송신 스위치가 현재 신뢰하는 스위치의 고유 식별자는 루트 스위치입니다
- 전송 포트에서 루트에 대한 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 간의 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 패킷이 루트로 전달됩니다.
- 각 스위치의 포트가 선택됩니다. 이 스위치는 스위치에서 루트 스위치로가는 최상의 경로를 제공합니다.
- STP 에 포함 된 포트가 선택됩니다..

안정적인 STP 토폴로지 만들기

루트 포트를 가장 빠른 링크로 만드는 것입니다. 모든 스위치의 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 가장 적합한 스위치를 선택해야합니다.

기본 매개 변수를 사용하여 STP 를 활성화하면 전환 된 네트워크에서 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 새로운 네트워크 토폴로지 정보가 네트워크 전체에 전파 될 때까지 기다려야합니다. 또한 이전 토폴로지를 기반으로 전달 된 BPDU 패킷의 패킷 aging 이 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 일련의 상태를 지정합니다.

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

- Blocking 포트가 패킷을 전달하거나 수신하지 못하도록 차단됨
- listening 포트가 BPDU 패킷을 수신하기 위해 대기하고 있으며 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 먼저 차단 상태로 돌아와야합니다

포트는 다음과 한 가지경우의 상태에서 다른상태로 전환됩니다.

- 차단에서 초기화(스위치 부팅)
- 차단되어 전달받거나 사용불능하도록
- 전달받아 학습하거나 사용불능하도록
- 학습하여 전달하거나 사용불능하도록
- 전달되어 사용불능한곳까지

■ 차단되어 사용불능한곳까지

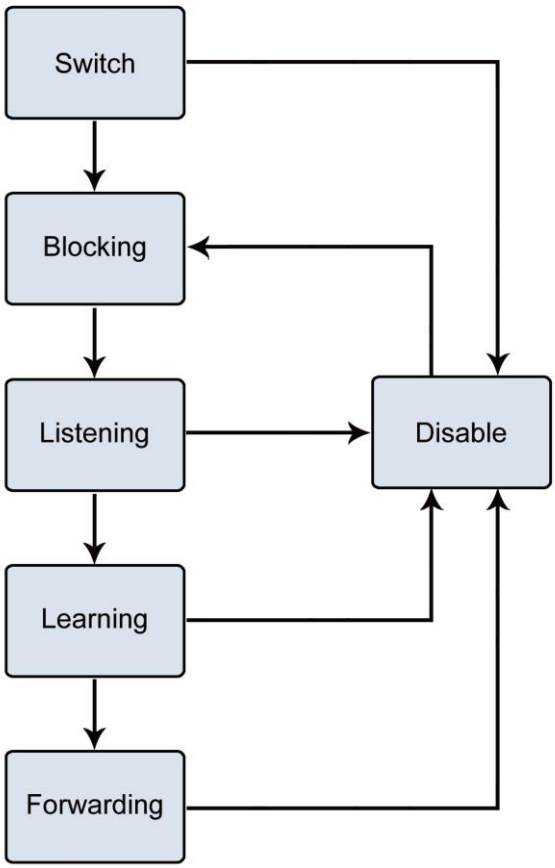


그림 4-7-1 STP 포트 구성 전송과정

관리 소프트웨어를 사용하여 각 포트 상태를 수정할 수 있습니다. TP 를 활성화하면 네트워크의 모든 스위치에있는 모든 포트가 차단 상태를 통과한 다음 전원을 켰을 때 전달 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 파라미터

STP 운영단계

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 **(아래 우선 순위 설정을 제외하고는 사용자가 설정할 수 없음)**	사용자 설정 우선 순위와 스위치의 MAC 주소의 조합. Bridge Identifier 는 두 부분으로 구성됩니다. 16 비트 우선 순위 및 48 비트 이더넷 MAC 주소 32768 + MAC	32768 + MAC
Priority	각 스위치의 상대적 우선 순위 - 낮은 숫자는 우선 순위를 높이고 주어진 스위치가 루트 브리지로 선택 될 가능성을 높입니다.	32768
Hello Time	스위치에 의한 hello 메시지 브로드 캐스트 간 시간.	2 seconds
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 seconds
Forward Delay Timer	포트가 차단 상태가 될 수있는 BPDU 를 기다리는 동안 학습 및 수신 대기 상태에서 포트가 소비 한 시간.	15 seconds

다음은 포트 또는 포트 그룹 수준에 대해 사용자가 구성 할 수있는 STP 매개 변수입니다.

종류	설명	기본값
Port Priority	각각에 대한 상대적 우선 순위 포트 번호가 낮을수록 주어진 포트가 루트 포트로 선택 될 확률이 높아집니다.	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 - Auto

기본 스패닝트리 구성

특징	기본값
Enable state	STP 모두 비활성화시킨다
Port priority	128

Port cost	0
Bridge Priority	32,768

사용자 변환 STA 파라메타

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.

헬로우 타임 - 헬로우 타임은 1 ~ 10 초가 될 수 있습니다. 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 시간은 최대 값보다 길 수 없습니다. 나이. 그렇지 않으면 구성 오류가 발생합니다.

맥스.치 – 최대친는 6 ~ 40 초입니다. 최대 aging 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.

전달 지연 타이머 - 전달 지연은 4 ~ 30 초가 될 수 있습니다. 이것은 포트가있는 시간입니다.

스위치는 차단 상태에서 전달 상태로 이동하는 동안 수신 상태로 유지됩니다.

위의 매개 변수를 설정할 때 다음 공식을 준수하십시오.

Max. Age _ 2 x (전송지연- 1 초)

Max. Age _ 2 x (Hello 시간 + 1 초)

우선순위포트 – 포트 우선 순위는 0 ~ 240 이 될 수 있습니다. 숫자가 낮을수록 포트가 루트 포트로 선택 될 확률이 높아집니다.

포트 비용 - 포트 비용은 0 에서 200000000 까지 설정할 수 있습니다. 숫자가 낮을수록 포트가 패킷을 전달할 확률이 높아집니다.

3 3. STP 의 일러스트레이션

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.

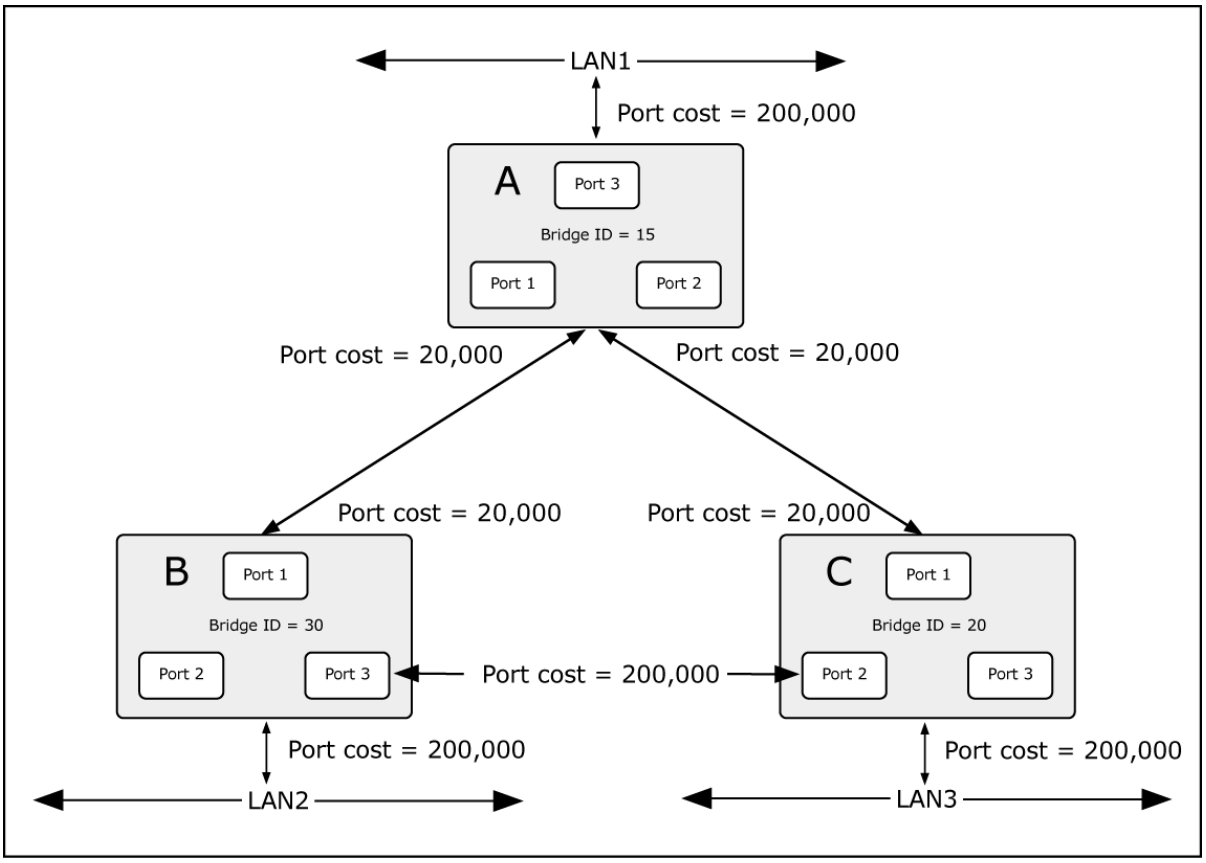


그림 4-7-5 STA 규칙을 적용하기 전에

이 예제에서는 기본 STP 값만 사용됩니다.

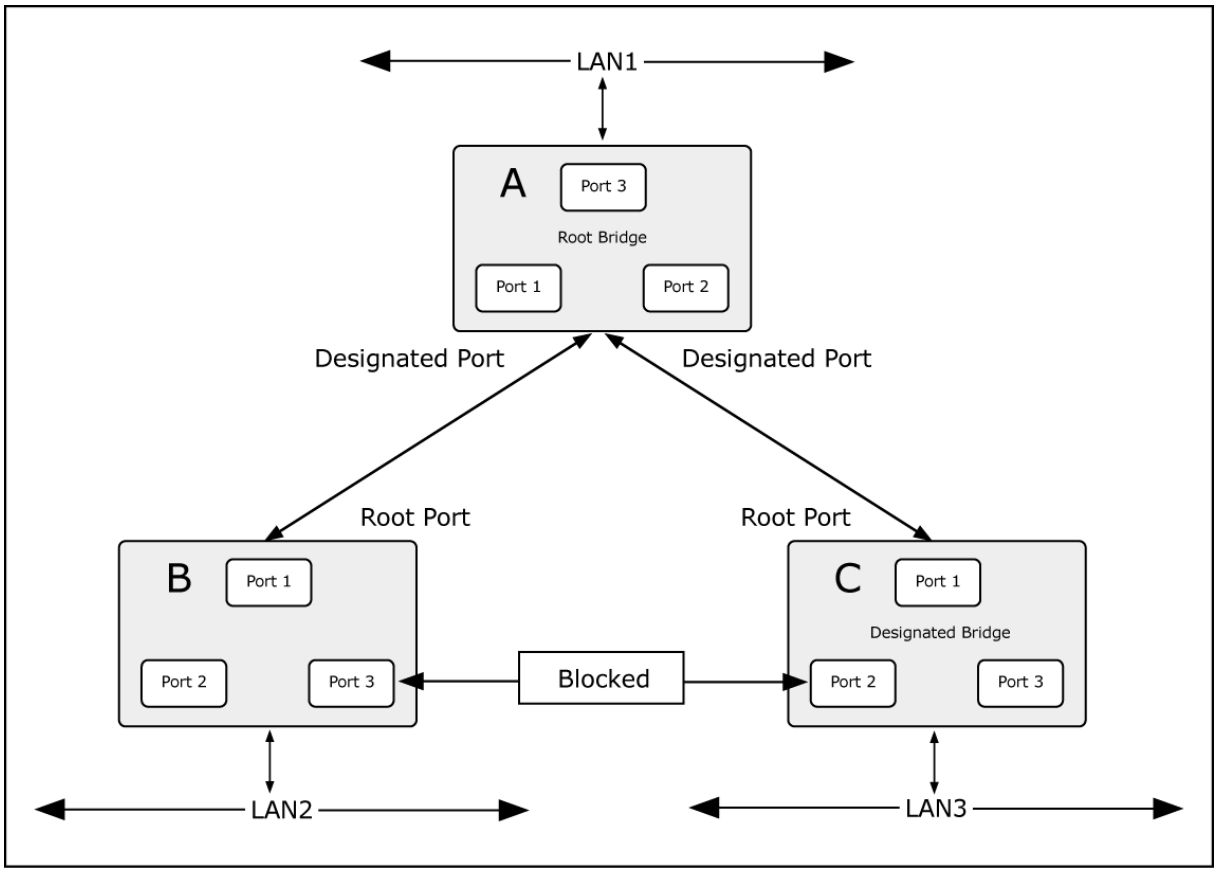


Figure 4-7-6 STA 규칙을 적용 한후

가장 낮은 브리지 ID (스위치 C)를 가진 스위치가 루트 브리지로 선택되었으며 스위치 B 와 C 사이의 포트 비용이 높도록 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.

3.7.2 STP 시스템 구성

이 페이지에서는 STP 시스템 설정을 구성 할 수 있습니다. 이 설정은 스위치 또는 스위치 스택의 모든 STP 브리지 인스턴스에서 사용됩니다. 관리 형 스위치는 다음과 같은 스패닝 트리 프로토콜을 지원합니다.

- **Compatiable -- Spanning Tree Protocol (STP): 루프를 피하고 제거함으로써 엔드 스테이션 사이에 단일 경로를 제공합니다.**
- **Normal -- Rapid Spanning Tree Protocol (RSTP) : 포워딩 루프를 만들지 않고 빠른 스패닝 트리 수렴을 제공하는 네트워크 토폴로지 감지 및 사용.**
- **Extension – 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 구성 시스템은 4-7-7 에 다음과 같이 나타난다.

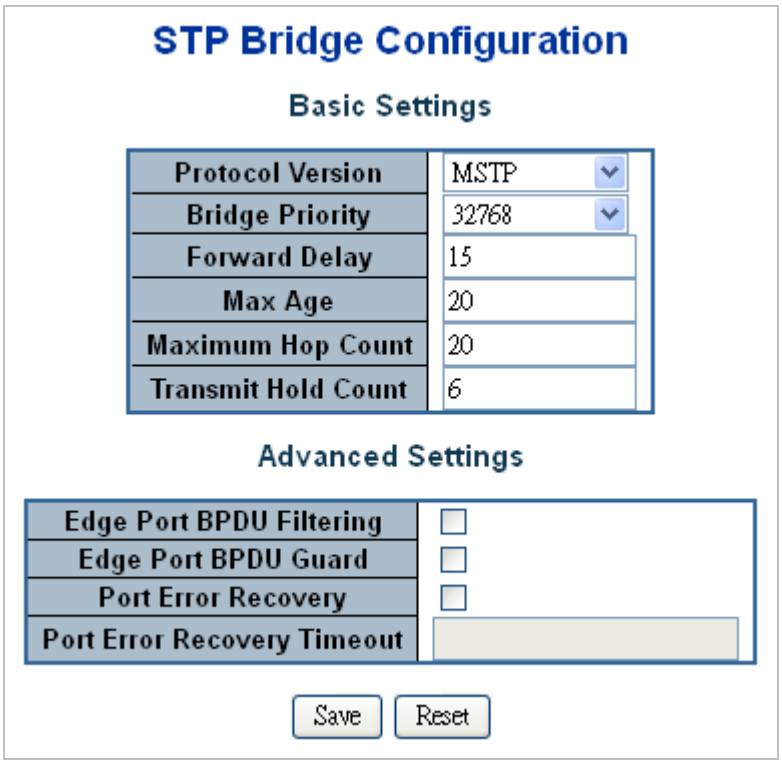


Figure 4-7-7 STP 브릿지 구성화면

위 그림은 다음과 같은 기능을 포함한다.

기본설정

기능	설명
• **Protocol Version**	STP 프로토콜 버전 설정입니다. 유효한 값은 STP, RSTP 및 MSTP 입니다.
• **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 구성합니다. MSTP 작동의 경우 CIST 의 우선 순위입니다. 그렇지 않으면 STP / RSTP 브리지의 우선 순위입니다
• **Forward Delay**	STP 브리지가 루트 및 지정된 포트를 전달로 전환하는 데 사용하는 지연 (STP 호환 방식에서 사용됨). 유효한 값의 범위는 4 ~ 30 초입니다. - 기본 : 15 - 최소 : 4 또는 [(최대 메시지 aging / 2) + 1] - 최대 : 30
• **Max Age**	브리지가 루트 브리지 일 때 브리지가 전송하는 정보의 최대 aging 입니다. 유효한 값은 6 - 40 초입니다. - 기본 : 20 -Minimum : 6 또는 [2 x (Hello Time + 1)] 중 높은 값입니다.

	- 최대 : 40 또는 [2 x (전달 지연 -1)] 중 낮은 값
• **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 설정

기능	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.
• **Port Error Recovery**	포트는 오류 비활성화 상태가되고 활성 토폴로지에서 제거됩니다. 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 재부팅으로도 지워집니다
• **Port Error Recovery Timeout**	오류 비활성화 상태의 포트가 통과해야하는 시간을 활성화 할 수 있습니다. 유효한 값은 30 에서 86400 초 (24 시간)입니다

기가비트 이더넷 스위치는 Rapid Spanning Protocol 을 기본 스패닝 트리 프로토콜로 구현합니다. "호환"방식을를 선택하는 동안 시스템은 다른 STP (802.1d)의 BPDU 제어 패킷과 호환 및 작동하도록 RSTP (802.1w)를 사용합니다.

Buttons

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.7.3 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 4-7-8 의 Bridge Status (브리지 상태) 화면이 나타납니다..

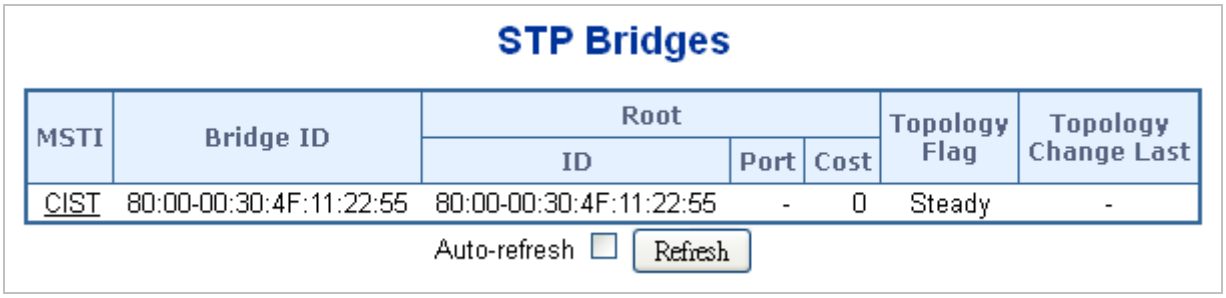


그림 4-7-8 STP Bridge 상태 화면 페이지

다음과 같은 기능을 소개합니다.

기능	설명
• **MSTI**	브리지 인스턴스. 이것은 STP Detailed Bridge Status 에 대한 링크이기도합니다.
• **Bridge ID**	이 Bridge 인스턴스의 Bridge ID 입니다.
• **Root ID**	현재 선출 된 루트 브리지의 브리지 ID 입니다.
• **Root Port**	스위치 포트에 현재 루트 포트 역할이 할당되었습니다.
• **Root Cost**	루트 경로 비용. 루트 브리지의 경우 이것은 0 입니다. 다른 모든 브리지의 경우 루트 브리지에 대한 최소 비용 경로의 포트 경로 비용 합계입니다.
• **Topology Flag**	이 Bridge 인스턴스의 토폴로지 변경 플래그의 현재 상태입니다.
• **Topology Change Last**	마지막 토폴로지 변경이 발생한 이후의 시간입니다.

Buttons

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

Refresh : 페이지를 새로고칩니다.

3.7.4 CIST 포트 구성

이 페이지에서 사용자는 현재 STP CIST 포트 구성을 검사 할 수 있으며 가능하면이를 변경할 수도 있습니다. 그림 4-7-9 의 CIST 포트 구성 화면이 나타납니다.

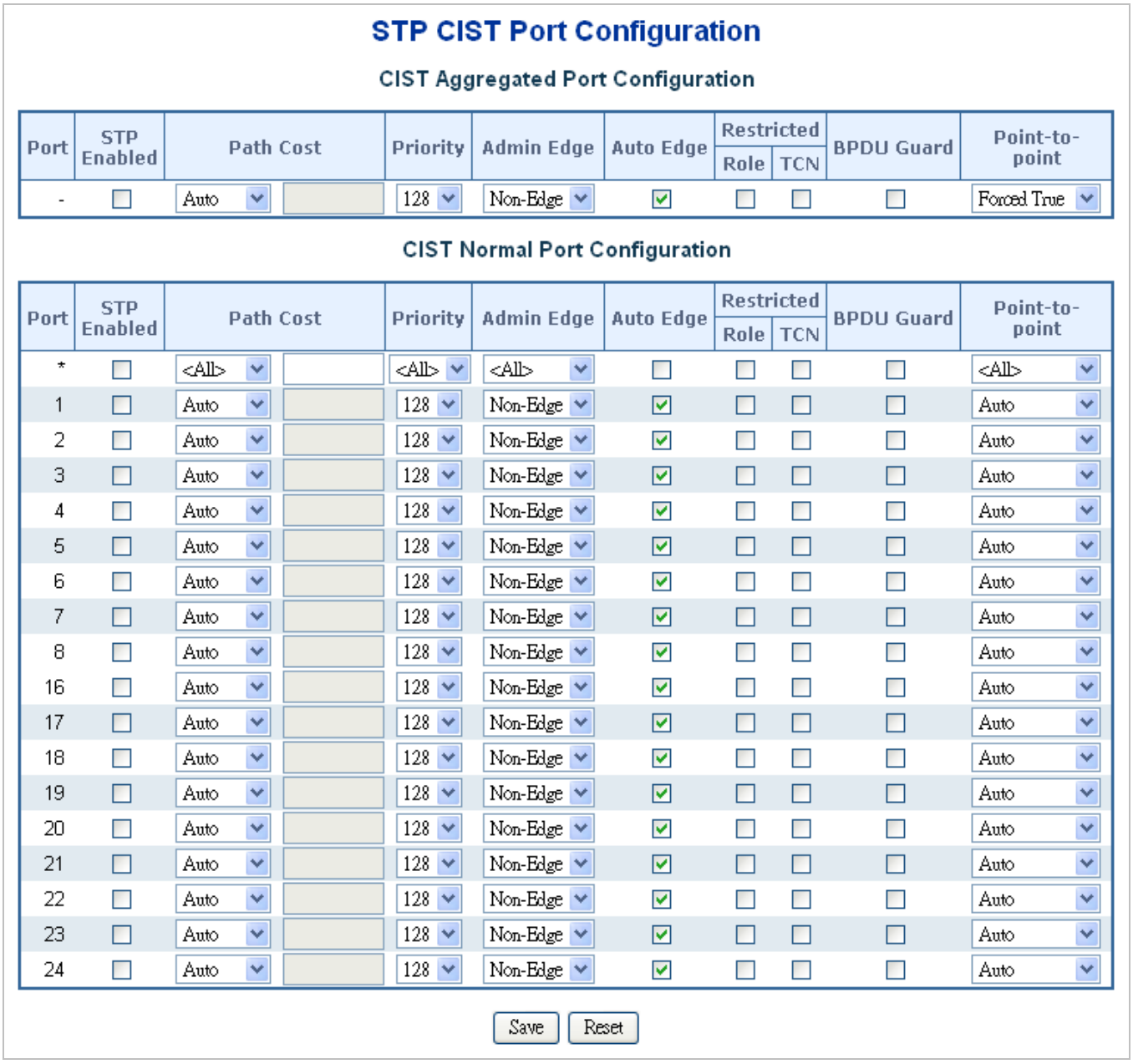


그림 4-7-9 STP CIST 포트구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Port**	논리적 STP 포트의 스위치 포트 번호입니다.
• **STP Enabled**	이 스위치 포트에서 RSTP 를 활성화할지 여부를 제어합니다.
• **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 사용될 수 있습니다. (위 참조). 기본값 : 128 범위 : 0-240, 16 단계
• **AdminEdge**	operEdge 플래그를 집합 할지 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. 이 설정으로 인해 포트가 오류 비활성화 상태로 들어가면 브리지 포트 오류 복구 설정이 적용됩니다.
• **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 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

기본적으로 시스템은 각 포트에서 사용되는 속도 및 이중 방식을를 자동으로 감지하고 아래 표시된 값에 따라 경로 비용을 구성합니다. 경로 비용 "0"은 자동 구성 방식을를 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 STP 경로 비용 추천 값

포트타입	링크타입	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	반이중	100	2,000,000
	전이중	95	1,999,999
	트렁크	90	1,000,000
Fast Ethernet	반이중	19	200,000
	전이중	18	100,000
	트렁크	15	50,000
Gigabit Ethernet	전이중	4	10,000
	트렁크	3	5,000

표 4-7-2 STP 경로비용 추천값

포트 타입	링크 타입	IEEE 802.1w-2001
Ethernet	반이중	2,000,000
	전이중	1,000,000
	트렁크	500,000
Fast Ethernet	반이중	200,000
	전이중	100,000
	트렁크	50,000
Gigabit Ethernet	전이중	10,000
	트렁크	5,000

표 4-7-3 기본 STP 비용

3.7.5 MSTI 우선순위

이 페이지를 통해 사용자는 현재 STP MSTI 브리지 인스턴스 우선 순위 구성을 검사하고 가능하면이를 변경할 수 있습니다. 그림 4-7-10 의 MSTI Priority 화면이 나타납니다.

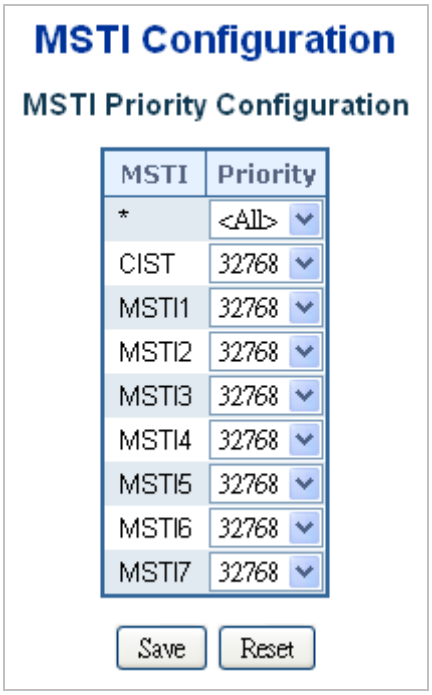


그림 4-7-10 MSTI Priority 설정 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **MSTI**	브리지 인스턴스입니다. CIST 는 항상 활성 상태 인 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 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.7.6 MSTI 구성

이 페이지를 통해 사용자는 현재 STP MSTI 브리지 인스턴스 우선 순위 구성을 검사하고 가능하면이를 변경할 수 있습니다. 그림 4-7-11 의 MSTI 구성 화면이 나타납니다.

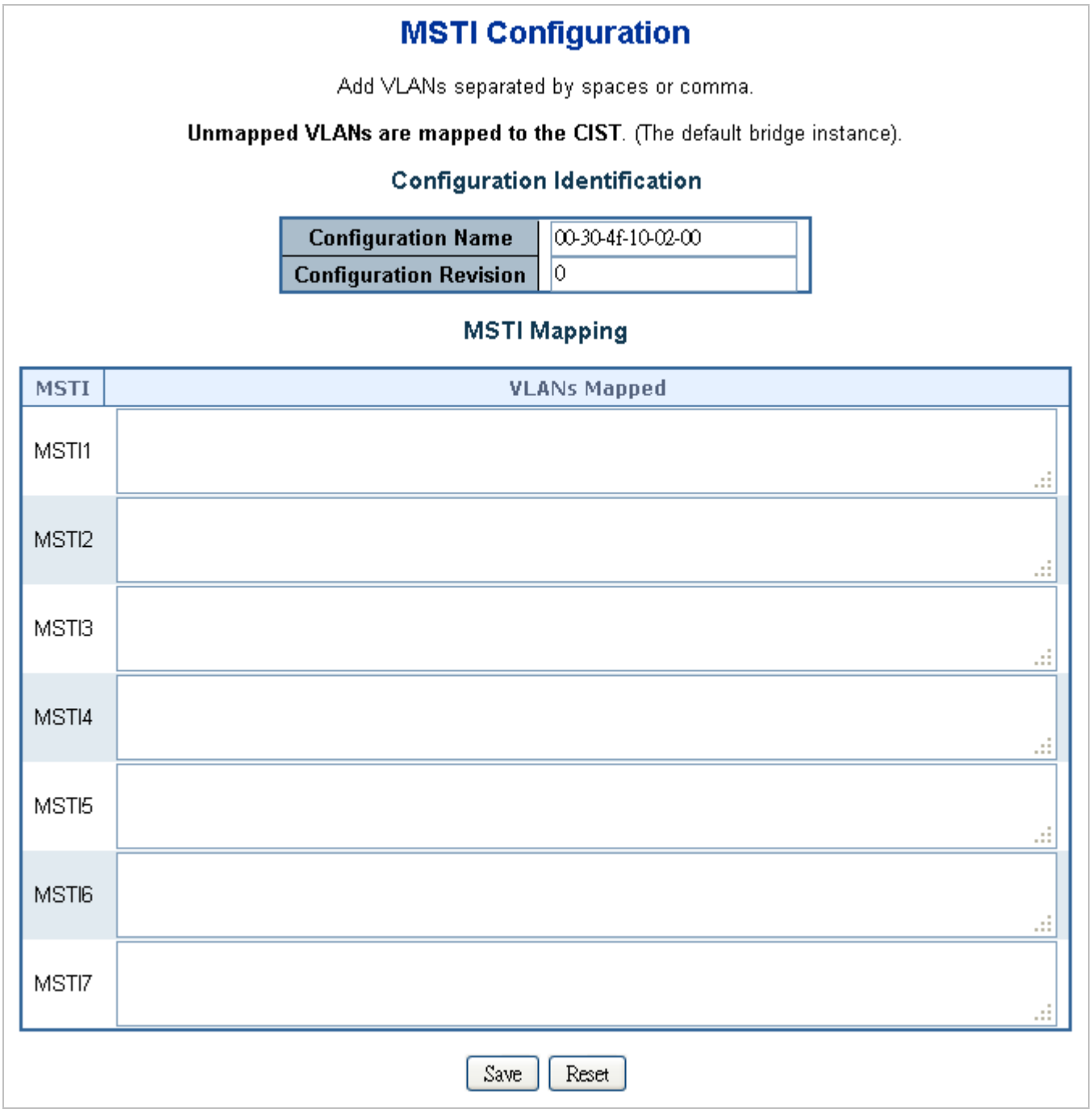


그림 4-7-11 MSTI 구성화면

다음과 같은 기능을 소개합니다.

구성과 확인

기능	설명
• **Configuration Name**	LAN 을 MSTI 로 매핑하는 이름입니다. 브리지는 MSTI 의 스패닝 트리를 공유하기 위해 VLAN-MSTI 매핑 구성뿐 아니라 이름과 버전 (아래 참조)을 공유해야합니다. (지역 내). 이름은 최대 32 자입니다.

• **Configuration Revision**	위에 명명 된 MSTI 구성의 개정판. 0 에서 65535 사이의 정수 여야합니다.

MSTI Mapping

기능	설명
• **MSTI**	브리지 인스턴스입니다. 명시 적으로 매핑되지 않은 VLAN 을 수신하므로 CIST 는 명시 적 매핑에 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 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.7.7 MSTI 포트 구성

이 페이지를 통해 사용자는 현재 STP MSTI 포트 구성을 검사하고 가능하면이를 변경할 수 있습니다.
MSTI 포트는 각각의 MSTI 인스턴스에 대한 활성 CIST (물리적) 포트에 대해 개별적으로 인스턴스화되고 포트에 적용 가능한 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 스택 전역입니다.
그림 4-7-12 및 그림 4-7-13 의 MSTI 포트 구성 화면이 나타납니다.

그림 4-7-12 MSTI Port 구성화면

다음과 같은 기능을 소개합니다.

MSTI 포트 구성

기능	설명
• **Select MSTI**	브리지 인스턴스를 선택하고 자세한 구성을 설정하십시오.

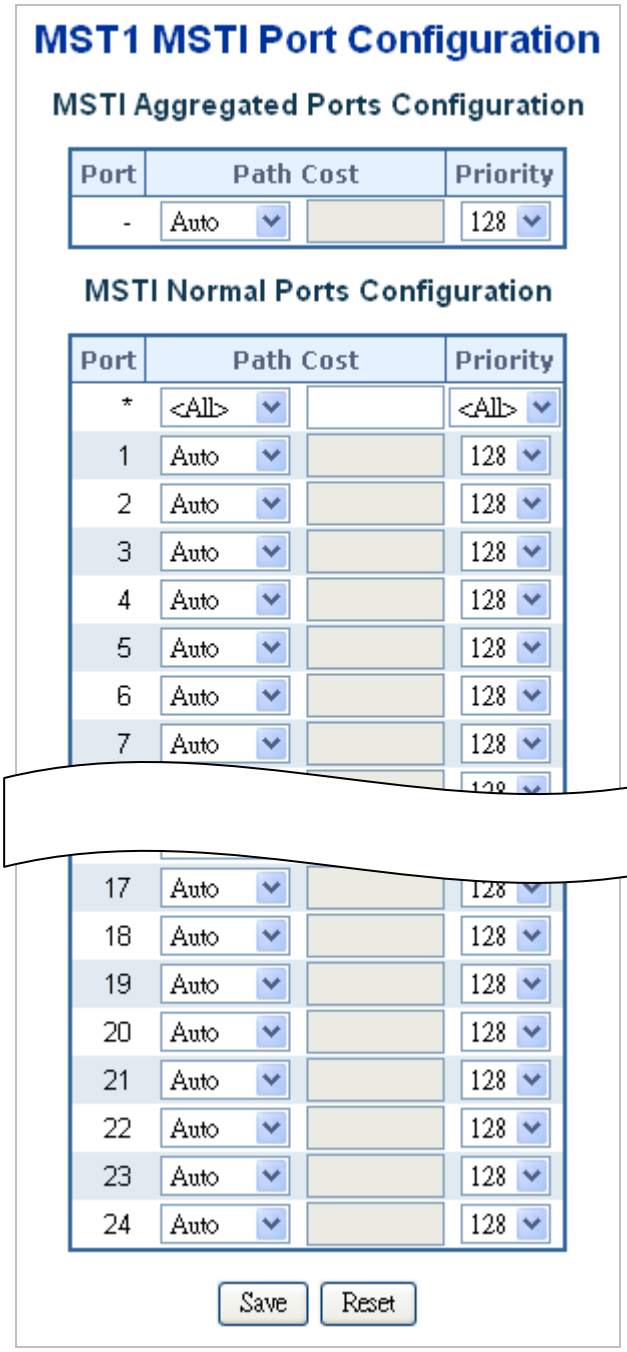


그림 4-7-13 MST1 MSTI Port 구성화면

다음과 같은 기능을 소개합니다.

MSTx MSTI 포트 구성

기능	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 적절한 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.

버튼 안내

Get: MSTx 구성으로 설정합니다.

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.7.8 포트 상태

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

그림 4-7-14 의 STP 포트 상태 화면이 나타납니다.

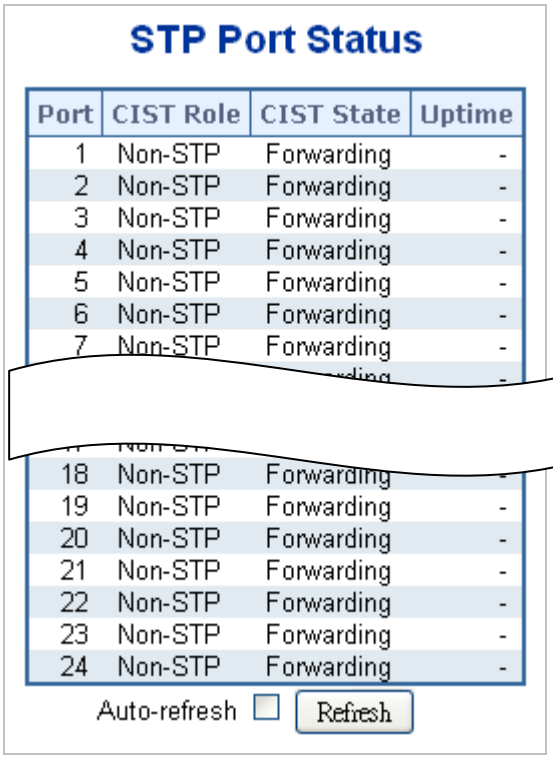


그림 4-7-14 STP Port 상태 화면 페이지

다음과 같은 기능을 소개합니다.

기능	설명
• **Port**	논리적인 STP 의 포트를 나타낸다
• **CIST Role**	**ICST 포트의 현재 STP 포트 역할. 포트 역할은 다음 값 중 하나 일 수 있습니다.** **AlternatePort** **BackupPort** **RootPort** **DesignatedPort** **Disable**
• **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 안내

Refresh: 페이지를 새로고칩니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

3.7.9 포트이용 통계

이 페이지는 현재 선택된 스위치의 포트 물리적 포트에 대한 STP 포트 통계 카운터를 표시합니다.

그림 4-7-15 의 STP 포트 통계 화면이 나타납니다.

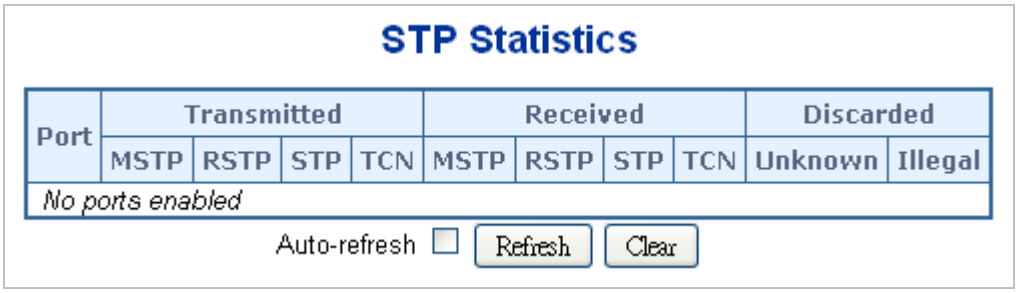


그림 4-7-15 STP Statistics 페이지 화면

다음과 같은 기능을 소개합니다.

기능	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 안내

Refresh: 페이지를 새로고칩니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

Clear: 정보를 즉시 제거한다

3.8 멀티케스트(Multicast)

3.8.1 IGMP 스누핑

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.

IGMP (Internet Group Management Protocol) 스누핑 정보
멀티 캐스트 전송을 수신하려는 컴퓨터 및 네트워크 장치는 주변 라우터에 멀티 캐스트 그룹의 구성원이 될 것임을 알릴 필요가 있습니다. IGMP (Internet Group Management Protocol)는이 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.

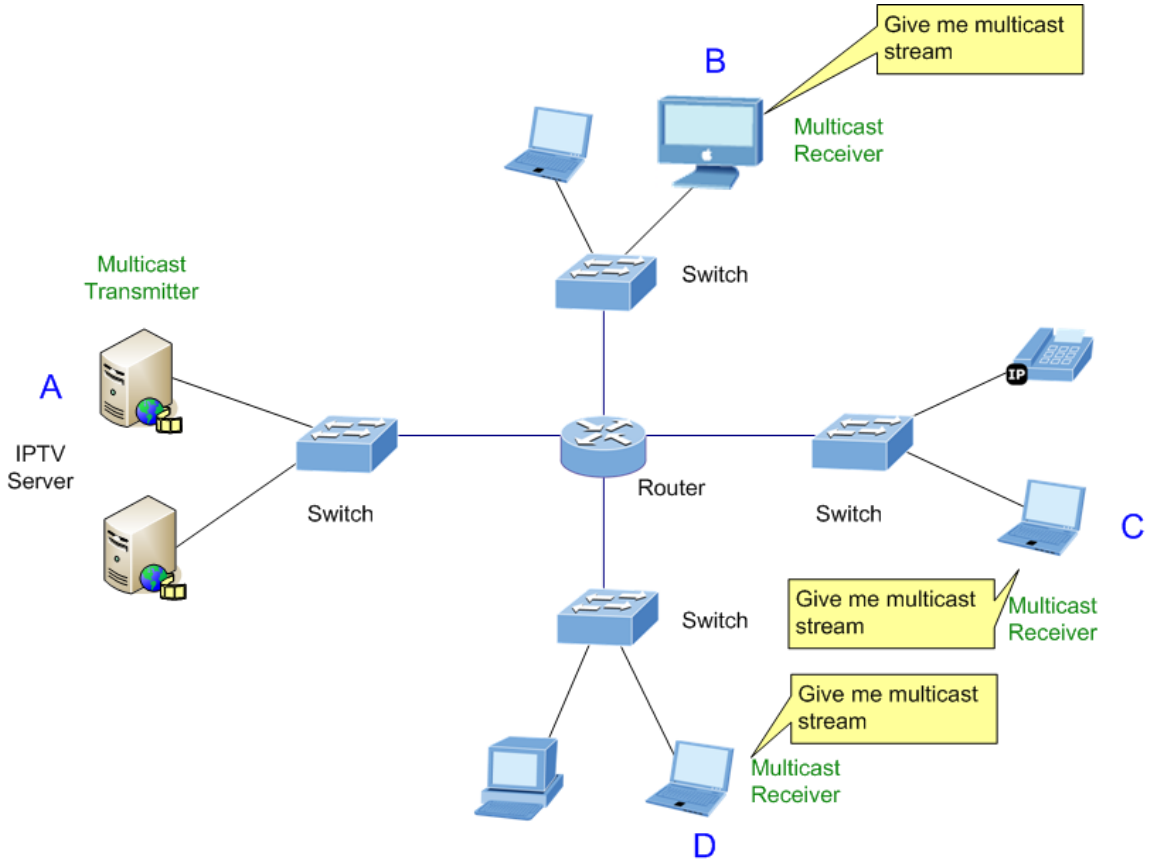


그림 4-8-1 멀티케스트 서비스

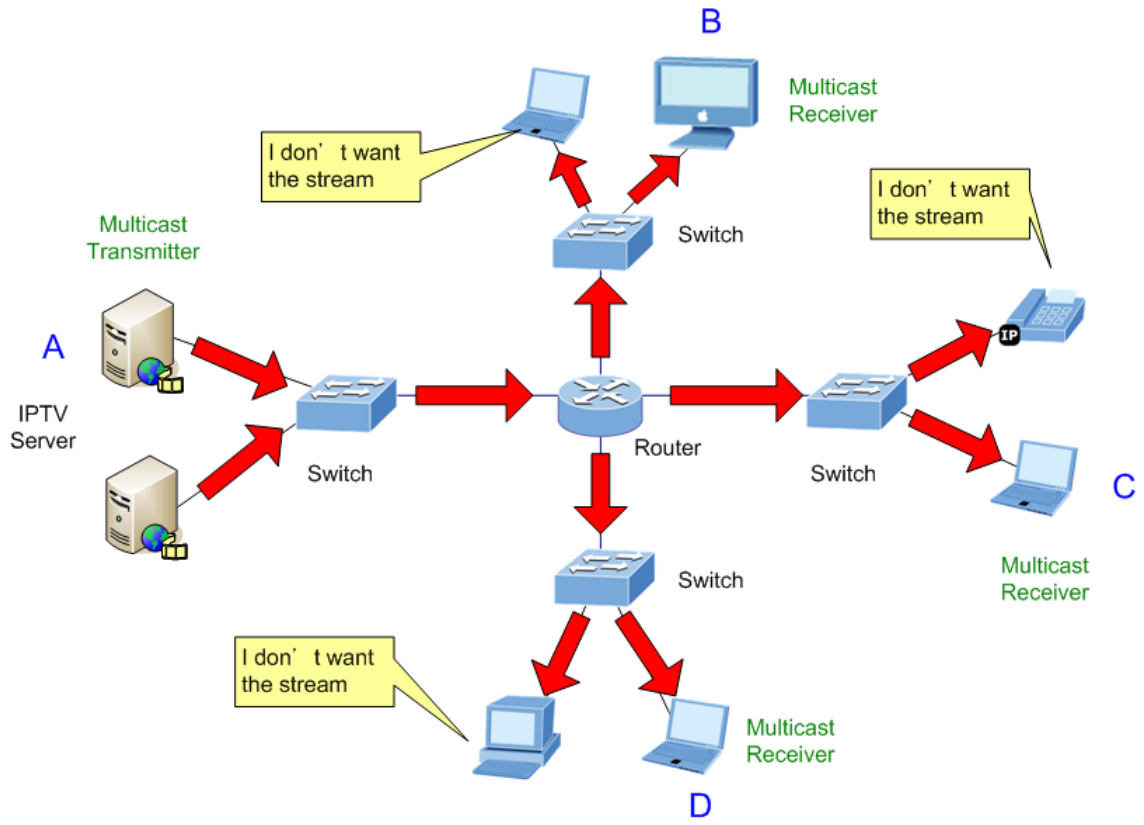


그림 4-8-2 멀티캐스트 플러딩

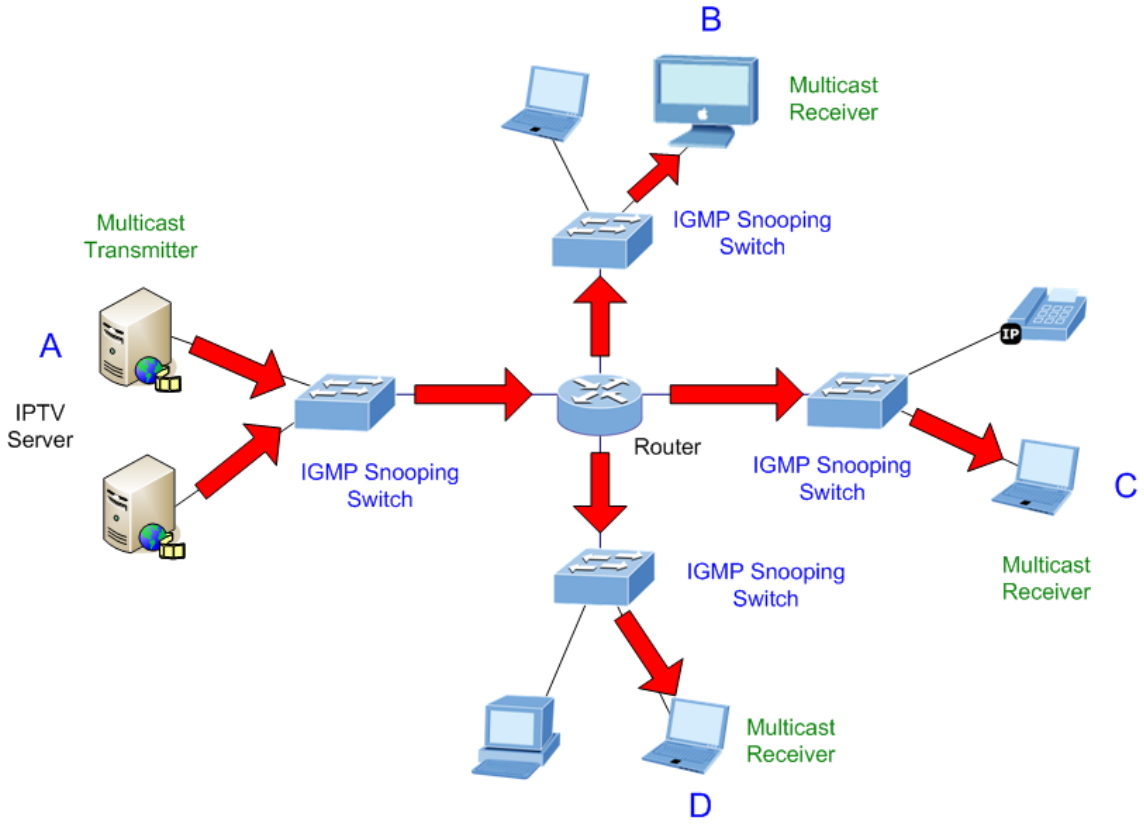


그림 4-8-3 IGMP 스누핑 멀티케스트 컨트롤

IGMP 버전 1 과 2

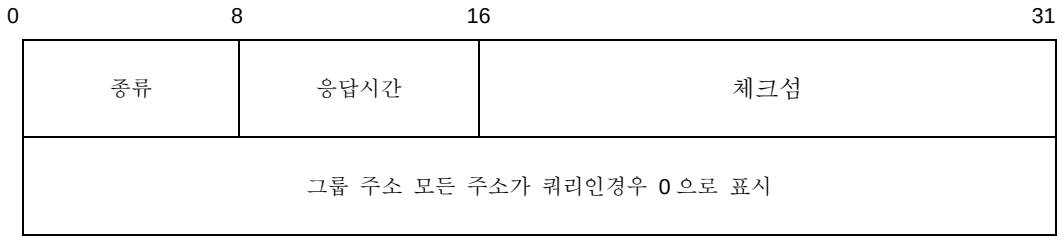
멀티 캐스트 그룹을 사용하면 언제든지 멤버을 가입하거나 탈퇴 할 수 있습니다. IGMP 는 멀티 캐스트 그룹에 가입하거나 탈퇴 할 때 구성원 및 멀티 캐스트 라우터가 통신 할 수있는 방법을 제공합니다.

IGMP 버전 1 은 RFC 1112 에 정의되어 있습니다. 패킷 크기는 고정되어 있으며 선택적 데이터는 없습니다.

IGMP 패킷의 형식은 다음과 같습니다.

IGMP 메시지 형태

옥텟(단위)



IGMP 유형 코드는 다음과 같습니다.

종류	의미
0x11	멤버쉽 쿼리 (그룹 주소가 0.0.0.0 인 경우)
0x11	특정 그룹 멤버쉽 쿼리 (그룹 주소가있는 경우)
0x16	멤버쉽 보고서 (버전 2)
0x17	그룹 탈퇴 (버전 2)
0x12	멤버쉽 보고서 (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) "휴가"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.

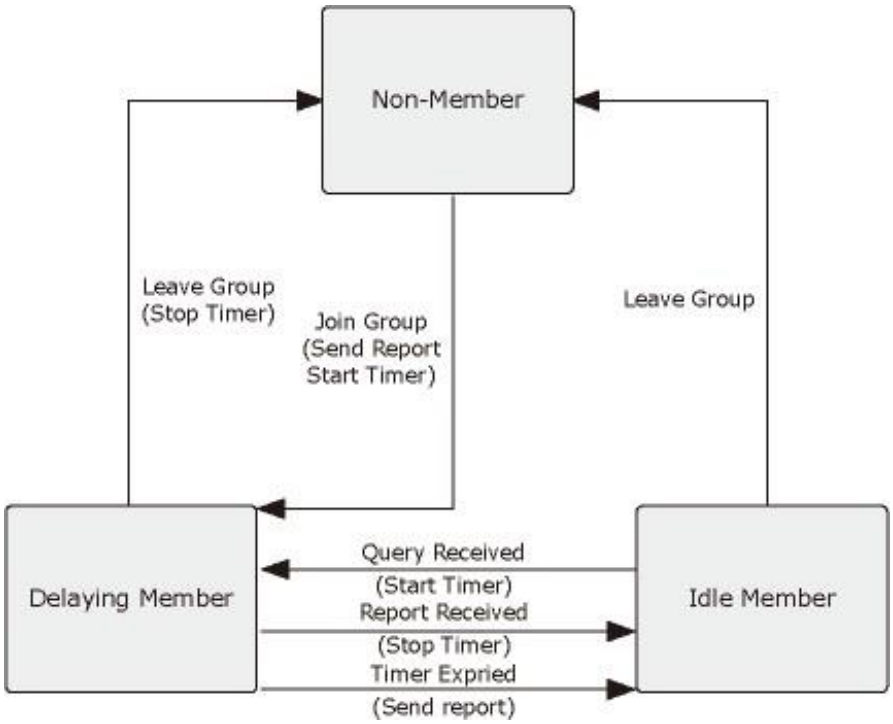


그림 4-8-4 IGMP 전송상태

■ **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.

3.8.2 IGMP 스누핑 구성

이 페이지는 IGMP Snooping 관련 구성을 제공합니다.그림 4-8-5 참조

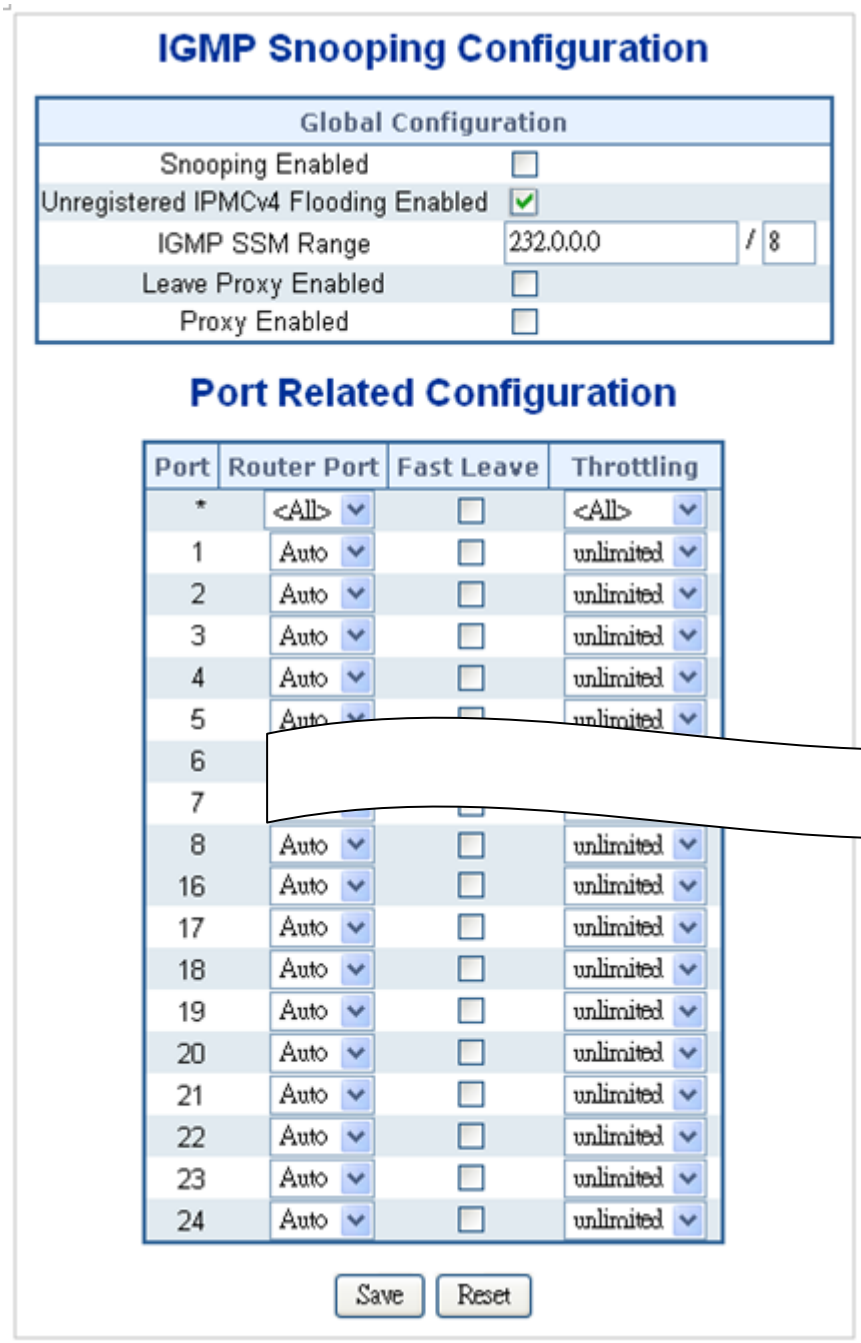


그림 4-8-5 IGMP Snooping 구성화면

다음과 같은 기능을 소개합니다.

기능	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. ■ **Auto:** 포트가 IGMP 쿼리 패킷을 수신하는 경우 관리되는 스위치가 자동으로 포트를 IGMP 라우터 포트로 사용하려면 "자동"을 선택합니다. ■ **Static**: Managed Switch 는 항상 지정된 포트를 IGMP 라우터 포트로 사용합니다. 포트에 멀티 캐스트 프로토콜을 적용한 IGMP 멀티 캐스트 서버 또는 IP 카메라를 연결할 때이 방식을를 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 방식을를 사용하십시오.
• **Fast Leave**	포트를 빠르게 빠져 나가십시오
• **Throtting**	스위치 포트가 속할수 있는 멀티캐스트그룹수를제한합니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.8.3 IGMP 스누핑 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 테이블의 처음부터 처음 20 개의 항목을 보여줍니다. 가장 먼저 표시되는 VLAN ID 는 VLAN 테이블에 있습니다.

"VLAN"입력 필드는 사용자가 VLAN 테이블에서 시작점을 선택할 수 있도록합니다. 그림 4-8-6 의 IGMP Snooping VLAN Configuration 화면이 나타납니다.

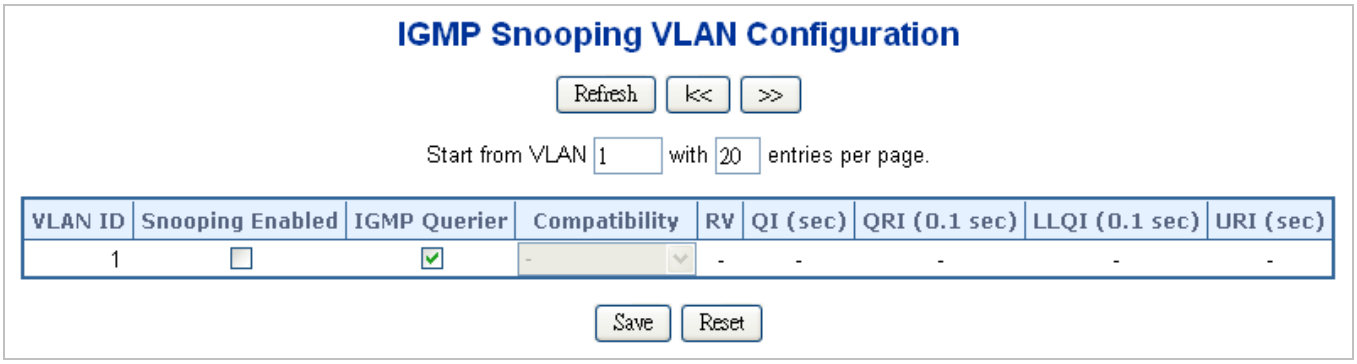


그림 4-8-6 IGMP Snooping VLAN 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **VLAN ID**	항목의 VLAN ID 입니다.
• **IGMP Snooping Enable**	VLAN 별 IGMP 스누핑을 활성화합니다. 최대 64 개의 VLAN 만 선택할 수 있습니다.
• **IGMP Querier**	VLAN 에서 IGMP Querier 를 활성화합니다.
• **Compatibility**	호환성은 호스트 및 라우터가 네트워크 내의 호스트 및 라우터에서 작동하는 IGMP 버전에 따라 적절한 조치를 취함으로써 유지됩니다. 허용되는 항목은 **IGMP-Auto**, **Forced IGMPv1**, **Forced IGMPv2**, **Forced IGMPv3**, 기본 호환성 값은 IGMP-Auto 입니다.
• **RV**	견고성. Robustness Variable 을 사용하면 네트워크에서 예상되는 패킷 손실을 조정할 수 있습니다. 허용 범위는 1 ~ 255 이며 기본 견고성 변수 값은 2 입니다.
• **QI**	쿼리 간격. Query Interval 은 Querier 가 보낸 General Queries 간의 간격입니다. 허용되는 범위는 1 - 31744 초이며, 기본 쿼리 간격은 125 초입니다.
• **QRI**	질의 응답 간격. 정기적 인 일반 쿼리에 삽입 된 최대 응답 코드 를 계산하는 데 사용 된 최대응답시간 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 간격. 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**	원치 않는 보고서 간격(Unsolicited Report Interva)은 호스트의 그룹 구성원 초기 보고서 반복 간격입니다. 허용되는 범위는 0 ~ 31744 초이며, 기본 원치 않는 보고서 간격은 1 초입니다.

버튼 안내

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

<<: VLAN 테이블의 첫 번째 항목, 즉 VLAN ID 가 가장 낮은 항목부터 테이블을 업데이트합니다..

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

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.8.4 IGMP 스누핑 포트그룹 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. 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 4-8-7 의 IGMP 스누핑 포트 그룹 필터링 구성 화면이 나타납니다..

그림 4-8-7 IGMP Snooping Port Group Filtering 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제됩니다.
• **Port**	설정에 대한 논리 포트입니다.
• **Filtering Group**	필터링 할 IP 멀티 캐스트 그룹입니다.
• **Add New Filtering Group**	새 필터링 그룹 추가를 클릭하여 그룹 필터링 테이블에 새 항목을 추가합니다. 새 항목의 포트 및 필터링 그룹을 지정하십시오. "저장"을 클릭하십시오.

버튼 안내

Add new Filtering Group: 필터링 그룹을 새로 추가합니다.

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.8.5 IGMP Snooping Status

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

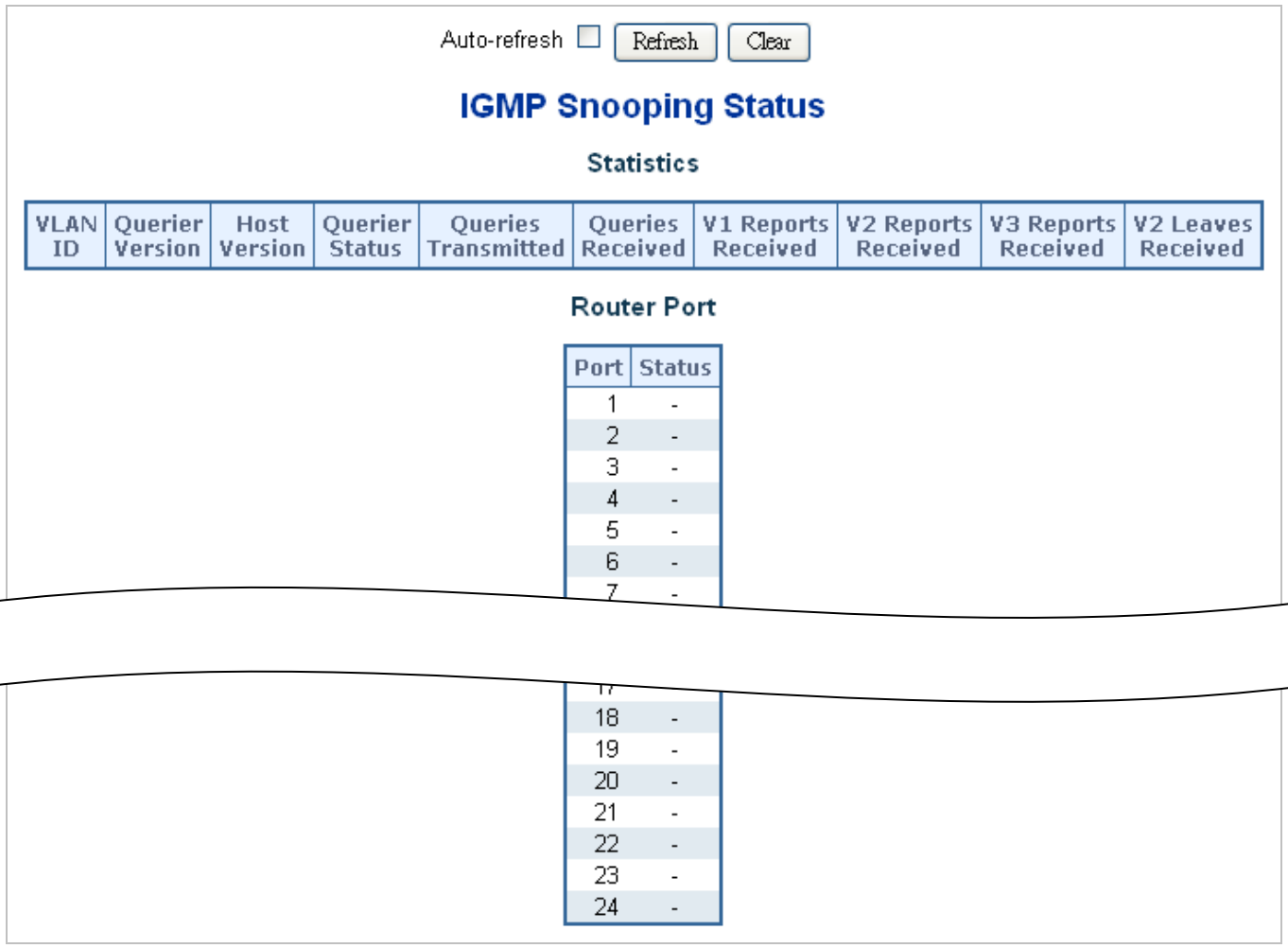


그림 4-8-8 IGMP Snooping 상태 화면 페이지

다음과 같은 기능을 소개합니다.

기능	설명
• **VLAN ID**	항목의 VLAN ID 입니다.
• **Querier Version**	근무 Querier 버전은 현재.
• **Host Version**	현재 작업 호스트 버전.
• **Querier Status**	신임 상태가 "활성"또는 "유휴"임을 표시하십시오.
• **Querier Transmitted**	Transmitted Querier 의 수.
• **Querier Received**	Received Querier 의 수.
• **V1 Reports Received**	받은 V1 보고서의 수입니다.
• **V2 Reports Received**	받은 V2 보고서의 수입니다.
• **V3 Reports Received**	받은 V3 보고서 수.
• **V2 Leave Received**	Received V2 Leave 의 수입니다.

• **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 안내

Refresh: 페이지를 새로고칩니다.

Clear: 모든 통계를 지웁니다.

Auto-refresh : 자동으로 3 초 마다 새로고침을 합니다.

3.8.6 IGMP 그룹 정보

이 페이지에는 IGMP 그룹 테이블의 항목이 표시됩니다. IGMP 그룹 테이블은 먼저 VLAN ID 별로 정렬 된 다음 그룹별로 정렬됩니다.

각 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 테이블의 처음부터 처음 20 개의 항목을 보여줍니다.

"Start from VLAN (VLAN 에서 시작)"및 "group (그룹)"입력 필드를 통해 사용자는 IGMP Group Table (IGMP 그룹 테이블)에서 시작점을 선택할 수 있습니다.

그림 4-8-9 의 IGMP Groups Informatino 화면이 나타납니다.

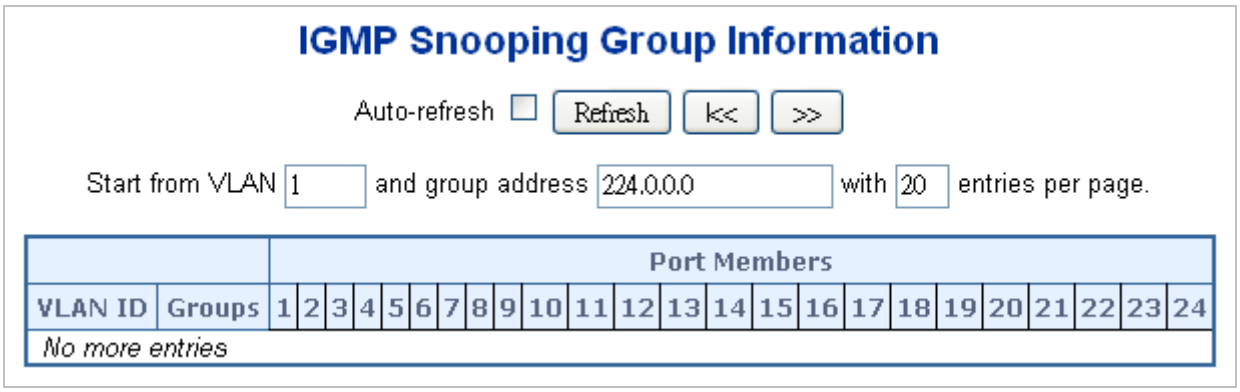


그림 4-8-9 IGMP Snooping Groups Information 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **VLAN ID**	VLAN ID of the group.
• **Groups**	Group address of the group displayed.
• **Port Members**	Ports under this group.

버튼 안내

Auto-refresh : 자동으로 3 초 마다 새로고침을 합니다.

Refresh: 테이블에 삽입된 값을 초기화 합니다.

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

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

3.8.7 IGMPv3 정보

이 페이지에는 IGMP SSM 정보 표의 항목이 표시됩니다. IGMP SSM 정보 테이블은 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 개 항목을 표시하며, 기본값은 20 개이며 "페이지 당 항목 수"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 4-8-10 의 IGMPv3 Information 화면이 나타납니다.

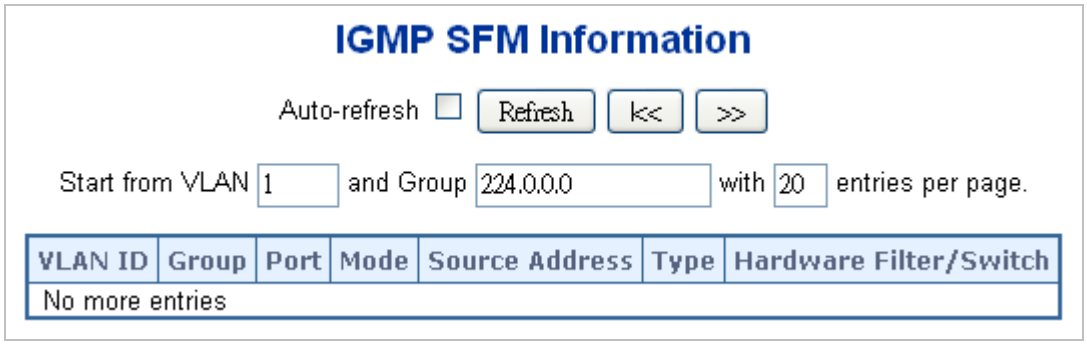


그림 4-8-10 IGMP SSM Information 페이지 화면

다음과 같은 기능을 소개합니다.

기능	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 방식을를 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 안내

Auto-refresh : 페이지에 대한 주기적인 새로고침을 자동으로 이행합니다.

Refresh: 페이지를 새로고칩니다.

<<: GMP 그룹 테이블의 첫 번째 항목부터 테이블을 업데이트합니다.

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

3.8.8 MLD(Multicast listener discovery) 스누핑 구성

이 페이지는 MLD 스누핑 관련 구성을 제공합니다. 그림 4-8-11 의 MLD Snooping Configuration 화면이 나타납니다.

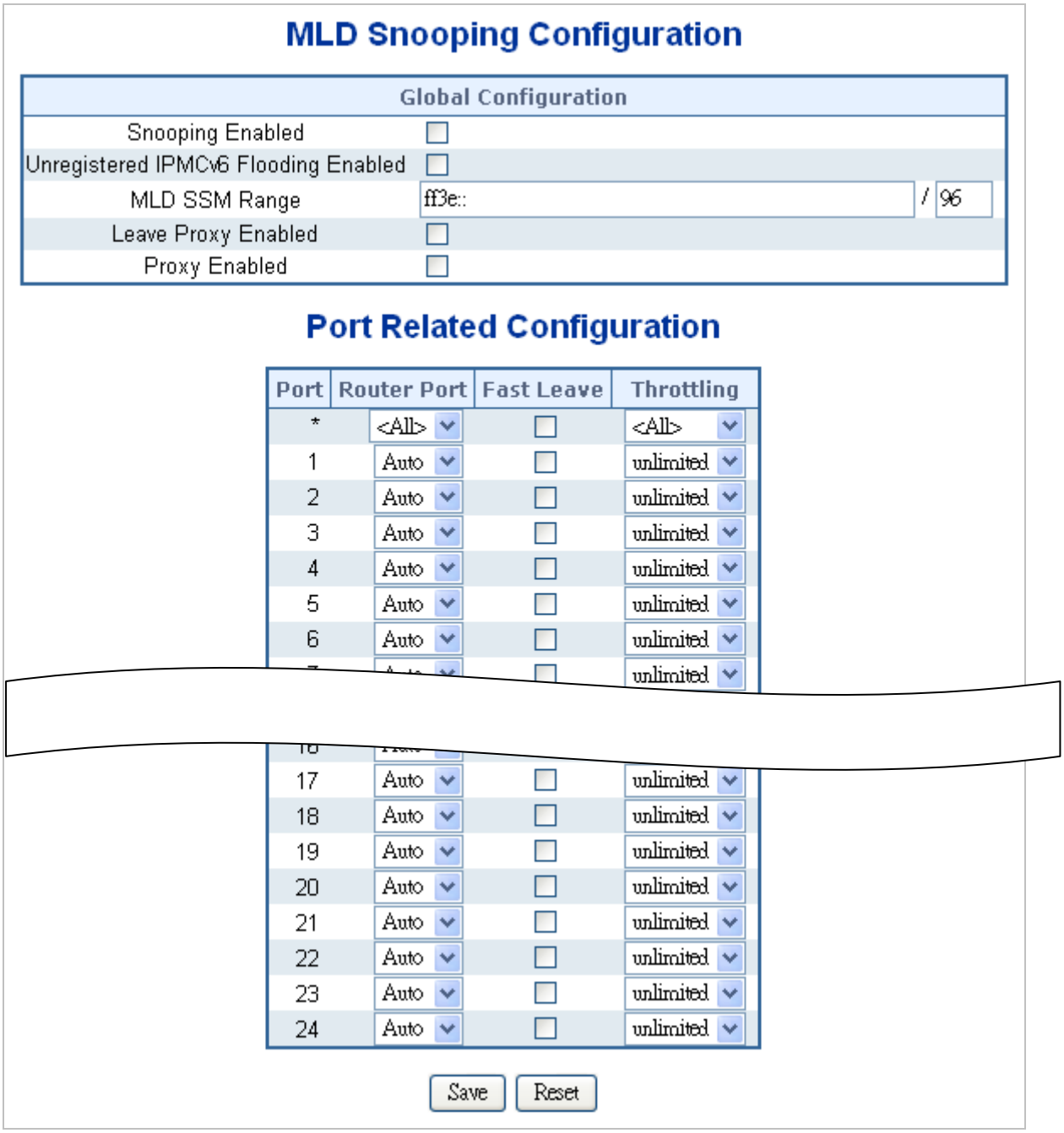


그림 4-8-11 MLD Snooping 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Snooping Enabled**	전체적인 MLD 스누핑을 활성화한다.
• **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 이러한 플러딩은 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**	MLD 프록시를 활성화하십시오. 이 기능은 라우터 측에 불필요한 가입 및 탈퇴 메시지 전달을 방지하는 데 사용할 수 있습니다
• **Router Port**	라우터 포트로 사용할 포트를 지정하십시오. 라우터 포트는 이더넷 스위치의 레이어 3 멀티 캐스트 장치 또는 MLD 쿼리 러쪽으로 연결되는 포트입니다. 집계 구성원 포트가 라우터 포트로 선택된 경우 전체 집계가 라우터 포트로 작동합니다. 허용되는 선택 항목은 Auto, Fix, Fone 입니다. 기본 호환성 값은 Auto 입니다.
• **Fast Leave**	포트를 빠르게 빠져 나가십시오.
• **Throtting**	스위치 포트가 속할 수있는 멀티 캐스트 그룹 수를 제한합니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.8.9 MLD 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 테이블의 처음부터 처음 20 개의 항목을 보여줍니다. 가장 먼저 표시되는 VLAN ID 는 VLAN 테이블에 있습니다.

"VLAN"입력 필드는 사용자가 VLAN 테이블에서 시작점을 선택할 수 있도록합니다. 그림 4-8-12 의 MLD Snooping VLAN 구성화면이 나타납니다.

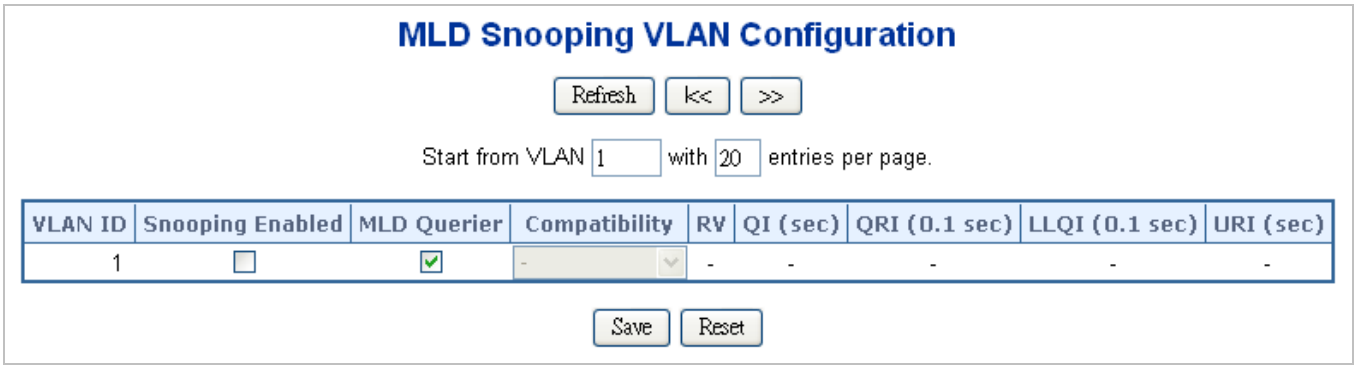


그림 4-8-12 IGMP Snooping VLAN 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **VLAN ID**	Vlan 항목의 ID 입니다.
• **MLD Snooping Enable**	VLAN 별 MLD 스누핑을 활성화합니다. 최대 32 개의 VLAN 만 선택할 수 있습니다.
• **MLD Querier**	VLAN 에서 MLD Querier 를 활성화하십시오.
• **Compatibility(호환성)**	호환성은 호스트 및 라우터가 네트워크 내의 호스트 및 라우터에서 작동하는 MLD 버전에 따라 적절한 조치를 취함으로써 유지됩니다. 허용 된 선택은 MLD-Auto, **Forced** MLD **v2,v1** 입니다. 기본 호환성 값은 MLD-Auto 입니다.
• **RV**	Robustness Variable 은 링크에 예상되는 패킷 손실을 조정할 수 있습니다. 허용 범위는 1 ~ 255 이며 기본 견고성 변수 값은 2 입니다.
• **QI**	쿼리 간격. Query Interval 변수는 Querier 가 보낸 일반 Queries 간의 간격을 나타냅니다. 허용되는 범위는 1 - 31744 초이며, 기본 쿼리 간격은 125 초입니다.
• **QRI**	질의 응답 간격. 주기적 일반 쿼리에 삽입 된 최대 응답 코드를 계산하는 데 사용되는 최대 응답 지연입니다. 허용되는 범위는 0 에서 31744 초까지이며 기본 쿼리 응답 간격은 10 분의 1 초 (10 초) 단위로 100 입니다.
• **LLQI**	마지막 리스너 쿼리 간격. 마지막 리스너 쿼리 간격은 버전 1 멀티 캐스트 리스너 완료 메시지에 대한 응답으로 전송 된 멀티캐스트 주소 특정 쿼리에 삽입 된 최대 응답 코드를 계산하는 데 사용 된 최대 응답 지연입니다. 멀티 캐스트 주소 및 소스 특정 쿼리 메시지에 삽입 된 최대 응답 코드를 계산하는 데 사용되는 최대 응답 지연이기도합니다. 허용되는 범위는 0 ~ 31744 초이며, 기본 리스너 질의 간격은 10 분의 1 초 (10 초)입니다.
• **URI**	원치 않는 보고서 간격. Unsolicited Report Interval 은 멀티 캐스트 주소에서 노드의 초기 관심 보고서가 반복되는 간격입니다. 허용되는 범위는 0 ~ 31744 초이며, 기본 원치 않는 보고서 간격은 1 초입니다.

버튼 안내

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

k<<: VLAN 테이블의 첫 항목부터 테이블을 업데이트하며. 가장 낮은 VLAN ID 항목을 업데이트합니다.

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

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.8.10 MLD Snooping 포트 그룹 필터링

특정 스위치 응용 프로그램에서 관리자는 최종 사용자가 사용할 수 있는 멀티캐스트 서비스를 제어하려고 할 수 있습니다. 예를 들어, 특정 가입 계획에 기반한 IP / TV 서비스. MLD 필터링 기능은 스위치 포트에서 지정된 멀티캐스트 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 프로파일에는 하나 이상의 멀티 캐스트 주소 또는 범위가 포함될 수 있습니다. 하나의 프로파일에만 포트에 할당 할 수 있습니다. 활성화되면 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.

MLD 제한은 한 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 MLD 참가 보고서가 삭제됩니다. 동작이 바꾸기로 설정되면 스위치는 기존 그룹을 임의로 제거하고이를 새 멀티 캐스트 그룹으로 바꿉니다. 그림 4-8-13 의 MLD 스누핑 포트 그룹 필터링 구성 화면이 나타납니다.

그림 4-8-13 MLD Snooping Port Group Filtering 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제 됩니다.
• **Port**	설정에 대한 논리 포트입니다.
• **Filtering Group**	필터링 할 IP 멀티 캐스트 그룹입니다.
• **Add New Filtering Group**	새 필터링 그룹 추가를 클릭하여 그룹 필터링 테이블에 새 항목을 추가합니다. 새 항목의 포트 및 필터링 그룹을 지정하십시오. "저장"을 클릭하십시오.

버튼 안내

Add new Filtering Group: 새로운 그룹필터링을 추가합니다.

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.8.11 MLD Snooping 상태

이 페이지는 MLD 스누핑 상태를 제공합니다. 그림 4-8-14 의 IGMP Snooping Status 화면이 나타납니다..

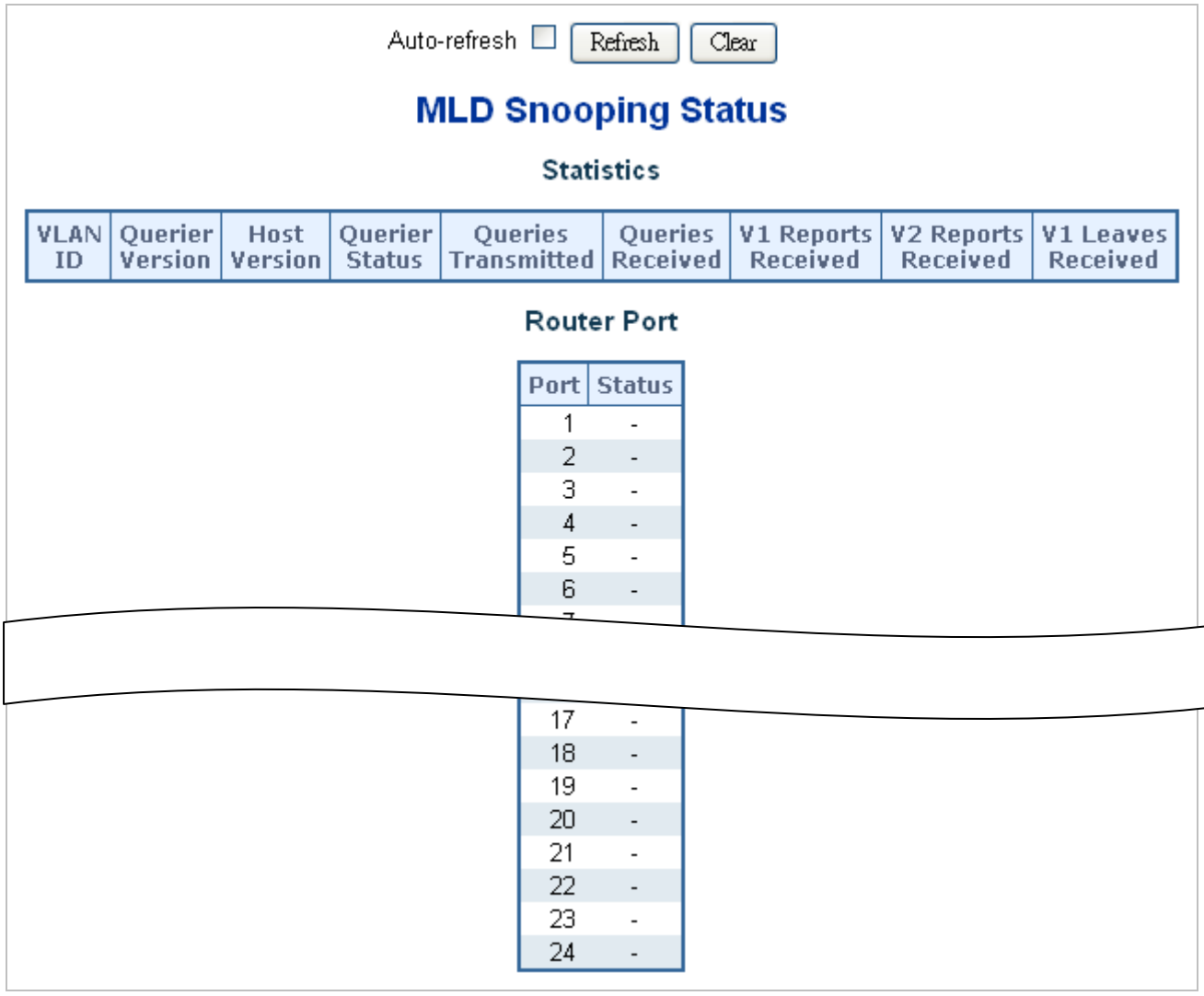


그림 4-8-14 MLD Snooping status 화면 페이지

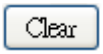
다음과 같은 기능을 소개합니다.

기능	설명
• **VLAN ID**	엔트리의 Vlan ID
• **Querier Version**	현재의 쿼리어 버전
• **Host Version**	현재의 호스트 버전

• **Querier Status**	상태가 “활성” 또는 “유후”상태임을 보여줍니다. "DISABLE"은 특정 인터페이스가 관리 상 사용 불가능 함을 나타냅니다.
• **Querier Transmitted**	송신 쿼리어의 수.
• **Querier Received**	수신 쿼리어의 수.
• **V1 Reports Received**	받은 V1 보고서의 수
• **V2 Reports Received**	받은 V2 보고서의 수
• **V1 Leave Received**	받은 V1 의 남은 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 안내

: 페이지를 새로고칩니다.



: 모든 통계 카운터를 지웁니다 .

Auto-refresh  : 자동으로 3 초 마다 새로고침을 합니다.

3.8.12 MLD 그룹 안내

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

각 페이지는 MLD 그룹 테이블에서 최대 99 개의 항목을 표시하며 기본값은 20 이고 "페이지 당 항목 수"입력 필드를 통해 선택됩니다. 처음 방문했을 때, 웹 페이지는 MLD 그룹 테이블의 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 4-8-15 의 MLD Groups Informatino 화면이 나타납니다.

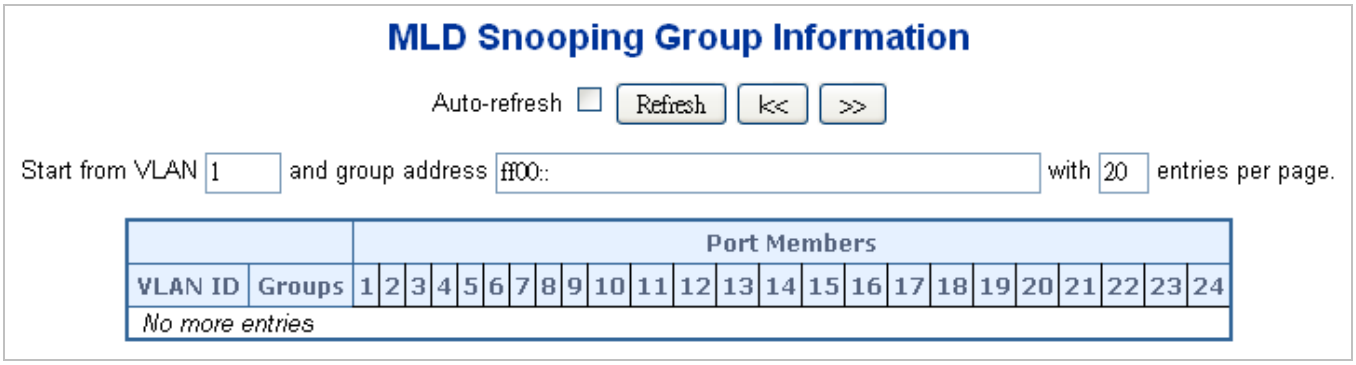


그림 4-8-15 MLD Snooping Groups Information 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **VLAN ID**	그룹의 Vlan ID
• **Groups**	비치된 그룹의 주소
• **Port Members**	그룹화 된 포트들

버튼 안내

Auto-refresh : 자동으로 3 초 마다 새로고침을 합니다.

Refresh: 페이지를 새로고칩니다.

<<: IGMP 그룹 테이블의 첫번째 항목부터 테이블을 업데이트합니다

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

3.8.13 MLDv2 안내

이 페이지에는 MLD SFM 정보 표의 항목이 표시됩니다. MLD SFM (Source-Filtered Multicast) 정보 표에는 SSM (Source-Specific Multicast) 정보도 들어 있습니다. 이 테이블은 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 수"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 4-8-16 의 MLDv2 Information 화면이 나타납니다.

그림 4-8-16 MLD SSM Information 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **VLAN ID**	그룹의 Vlan ID
• **Group**	그룹의 비치된 그룹주소
• **Port**	스위치 포트 수
• **Mode**	(VLAN ID, 포트 번호, 그룹 주소) 단위로 유지 관리되는 필터링 방식을를 나타냅니다. Include 또는 Exclude 중 하나 일 수 있습니다.
• **Source Address**	LAN ID, 포트 번호, 그룹 주소) 단위로 유지 관리되는 필터링 방식을를 나타냅니다. Include 또는 Exclude 중 하나 일 수 있습니다. 소스의 IP 주소. 현재 시스템은 필터링 할 IP 원본 주소의 총 수를 128 개로 제한합니다. 유형을 나타냅니다. 허용 또는 거부 중 하나 일 수 있습니다. 소스 IPv6 주소의 특정 그룹 주소를 대상으로하는 데이터 플레인이 칩별로 처리 될 수 있는지 여부를 나타냅니다.
• **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 안내

Auto-refresh : 3 초마다 주기적으로 새로고침

Refresh: 표시된 필드를 입력 필드에서 새로 고칩니다.

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


: 현재 표시된 마지막 항목 이후의 항목으로 시작하여 표를 갱신합니다.

3.8.14 MVR

MVR 기능을 사용하면 멀티 캐스트 VLAN 에서 멀티 캐스트 트래픽을 전달할 수 있습니다. 멀티 캐스트 텔레비전 애플리케이션에서, PC 또는 네트워크 텔레비전 또는 셋톱 박스는 멀티 캐스트 스트림을 수신 할 수있다. 여러 셋톱 박스 또는 PC 를 MVR 수신기 포트로 구성된 스위치 포트 인 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 VLAN 과주고받는 멀티 캐스트 데이터를 송수신하는 업 링크 포트를 MVR 소스 포트라고합니다. 최대 8 개의 MVR VLAN 을 각 멀티 캐스트 VLAN 에 해당하는 채널 설정으로 생성 할 수 있습니다. 채널 설정을위한 그룹 주소는 최대 256 개입니다.
이 페이지에는 다음과 같이 설명합니다.

기능	설명
• **MVR Mode**	모든 MVR 을 활성화 또는 비활성화 합니다. 등록되지 않은 플러딩제어는 IGMP /MLD 스누핑의 현재 구성에 이행하고 현재는 그룹이 가득찼습니다.
• **Delete**	삭제하려면 선택하십시오. 지정된 항목은 저장이 되지 않습니다..
• **MVR VID**	멀티 캐스트 VLAN ID 를 지정하십시오. 주의 : MVR 원본 포트는 관리 VLAN 포트와 겹치지 않는 것이 좋습니다.
• **MVR Name**	MVR Name 은 특정 MVR VLAN 의 이름을 나타내는 선택적 속성입니다. MVR VLAN 이름 문자열의 최대 길이는 32 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.
• **Mode**	MVR 작동 방식을를 지정하십시오. 동적 방식에서 MVR 은 소스 포트에 대한 동적 MVR 멤버십 보고서를 허용합니다. 호환 방식에서는 MVR 멤버쉽 보고서가 소스 포트에서 금지됩니다. 기본값은 동적 방식입니다.
• **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 이 만들어지면 편집 기호를 클릭하여 특정 MVR VLAN 에 해당하는 멀티 캐스트 채널 설정을 확장합니다. 편집 채널 외에도 MVR VLAN 의 인터페이스 채널 설정에 대한 요약이 표시됩니다.
• **Port**	설정에 대한 논리 포트입니다.
• **Port Role**	지정된 MVR VLAN 의 MVR 포트를 다음 역할 중 하나로 구성합니다. 비활성 : 지정된 포트가 MVR 작업에 참여하지 않습니다. 소스 : 멀티 캐스트 데이터를 수신하고 소스 포트로 보내는 업 링크 포트를 구성합니다. 구독자는 소스 포트에 직접 연결할 수 없습니다. 수신자 : 수신자 포트 인 경우 수신 포트로 구성하고 멀티 캐스트 데이터 만 수신해야합니다. IGMP / MLD 메시지를 발행하여 멀티 캐스트 그룹의 구성원이 아닌 경우 데이터를 수신하지 않습니다. 주의 : MVR 원본 포트는 관리 VLAN 포트와 겹치지 않는 것이 좋습니다. 역할 기호를 눌러 포트 역할을 선택하여 설정을 전환하십시오. 나는 비활성을 나타냅니다. S 는 소스를 나타냅니다. R 은 수신기를 나타냅니다. 기본 역할은 비활성입니다.
• **Immediate Leave**	포트를 빠르게 빠져 나가십시오.

버튼 안내

Add New MVR VLAN: 새 MVR VLAN 을 추가하려면 클릭하십시오.

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.8.15 MVR Status

이 페이지는 MVR 상태를 제공합니다. 그림 4-8-18 의 MVR 상태 화면이 나타납니다.

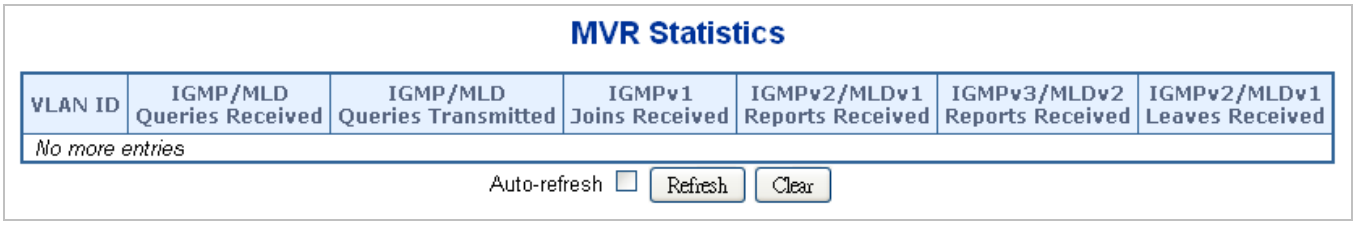


그림 4-8-18 MVR 상태 화면 페이지

다음과 같은 기능을 소개합니다.

기능	설명
• **VLAN ID**	멀티케스트 Vlan ID.
• **IGMP/MLD Queries Received**	IGMP 및 MLD 에 대한 각각의 수신 쿼리 수입니다.
• **IGMP/MLD Queries Transmitted**	IGMP 및 MLD 에 대한 각각의 송신 쿼리 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 안내

Refresh: 페이지를 새로고칩니다.

Clear:모든 통계 카운터를 초기화 합니다..

Auto-refresh : 자동으로 3 초 마다 새로고침을 합니다.

3.8.16 MVR Groups Information

이 페이지에는 MVR 그룹 테이블의 항목이 표시됩니다. MVR 그룹 테이블은 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 4-8-19 의 MVR 그룹 정보 화면이 나타납니다.

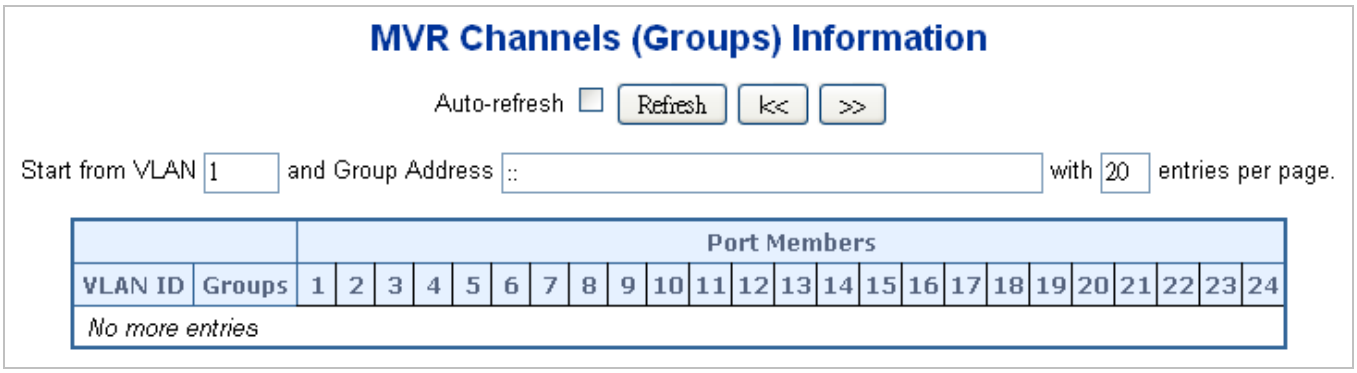


그림 4-8-19 MVR Groups Information 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **VLAN**	그룹의 Vlan ID
• **Groups**	표시된 그룹의 ID
• **Port Members**	지정 그룹하에 포트

버튼 안내

Auto-refresh : 자동으로 3 초 마다 새로고침을 합니다.

Refresh: 표시된 필드를 입력 필드에서 새로 고칩니다.

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

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

3.8.17 MVR SFM 정보

이 페이지에는 MVR SFM 정보 테이블의 항목이 표시됩니다. MVR SFM (Source-Filtered Multicast) 정보 표에는 SSM (Source-Specific Multicast) 정보도 들어 있습니다. 이 테이블은 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 4-8-20 의 MVR SFM 정보 화면이 나타납니다.

그림 4-8-20 MVR SFM Information 페이지 화면

다음과 같은 기능을 소개합니다.

기능	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 방식을를 나타냅니다. 포함 또는 불포함 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.

버튼 안내

Auto-refresh : 자동으로 3 초 마다 새로고침을 합니다.

Refresh :입력한 필드로부터 새로고침을 합니다..

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

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

3.9 Quality of Service

3.9.1 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 정체 관리.

QoS 기술력

- **분류기**– 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.
- **차별화 코드 포인트 (DSCP)** – 특정 응용 프로그램 및 / 또는 장치에 의해 인코딩 된 IP 헤더 내의 트래픽 우선 순위 지정 비트로서 네트워크에서 패킷에 필요한 서비스 수준을 나타냅니다.
- **서비스 단계**– 분류 된 트래픽 집합에 부여 할 우선 순위를 정의합니다. 서비스 레벨을 작성하고 수정할 수 있습니다.
- **정책** –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 프로파일**– 여러 세트의 규칙 (분류 자와 서비스 수준 조합)으로 구성됩니다. QoS 프로파일은 포트에 할당됩니다.
- **규칙**–스위치가 특정 유형의 트래픽을 처리하는 방법을 정의하는 서비스 수준과 분류 자로 구성됩니다. 규칙은 QoS 프로파일과 관련됩니다 (위 참조).

QoS 를 구현하려면 다음과 가은 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.

3.9.2 포트 정책

이 페이지에서는 모든 스위치 포트 정책에 대한 설정을 구성 할 수 있습니다. 그림 4-9-1 의 포트 폴리싱 화면이 나타납니다.

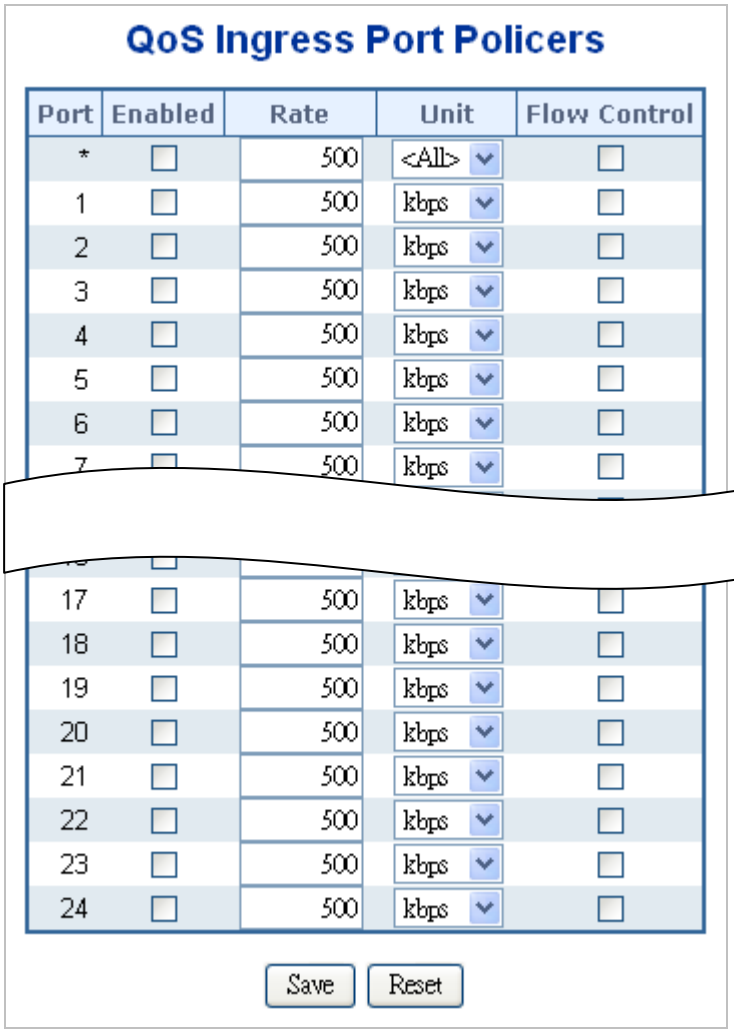


그림 4-9-1 QoS Ingress Port Policers 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Port**	아래에 적용 되는 포트 번호입니다.
• **Enable**	정책이 적용되는지 여부를 제어합니다.
• **Rate**	기본 속도 조정합니다. 기본값은 500 입니다.이 값은 "Unit"이 "kbps"또는 "fps"일 때 100-1000000 으로 제한되며 "Unit"가 "Mbps"또는 "kfps"일 때 1-3300 으로 제한됩니다

• **Unit**	정책 속도의 측정 단위를 kbps, Mbps, fps 또는 kfps 로 제어합니다. 기본값은 "kbps"입니다.
• **Flow Control**	흐름 제어가 활성화되고 포트가 흐름 제어 방식 인 경우 프레임을 삭제하는 대신 일시 중지 프레임이 전송됩니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.9.3 포트 분류

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

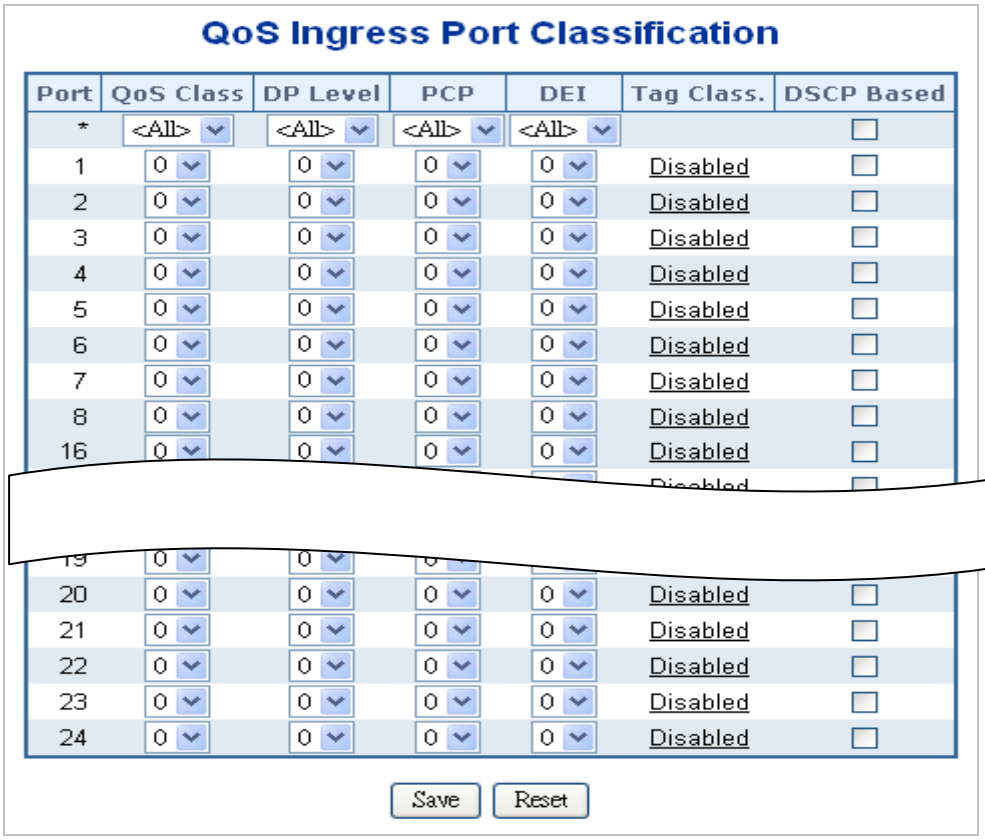


그림 4-9-2 QoS Ingress Port Classification 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Port**	아래 구성이 적용되는 포트 번호입니다.

• **QoS Class**	기본 QoS 클래스, 즉 다른 방식으로 분류되지 않은 프레임의 QoS 클래스를 제어합니다. QoS 클래스, 대기열 및 우선 순위 사이에는 일대일 매핑이 있습니다. QoS 클래스 0 (영)이 가장 낮은 우선 순위를 갖습니다. 참고 : QoS 클래스가 동적으로 변경된 경우 실제 QoS 클래스는 구성된 QoS 클래스 다음에 괄호 안에 표시됩니다.
• **DP Level**	기본 놓기 우선 순위, 즉 다른 방식으로 분류되지 않은 프레임의 DP 수준을 제어합니다.
• **PCP**	태그없는 프레임의 기본 PCP 를 제어합니다.
• **DEI**	태그없는 프레임의 기본 DEI 를 제어합니다.
• **Tag Class.**	이 포트의 태그가 지정된 프레임의 분류 방식을를 표시합니다. 비활성화 됨 : 태그가 지정된 프레임에 대해 기본 QoS 클래스 및 DP 수준을 사용합니다. 사용 가능 : 태그가있는 프레임에 대해 맵핑 된 버전의 PCP 및 DEI 를 사용하십시오. 방식 및 / 또는 매핑을 구성하려면 방식을를 클릭하십시오.
• **DSCP Based**	DSCP 기반 QoS 수신 포트 분류를 활성화하려면 클릭하십시오

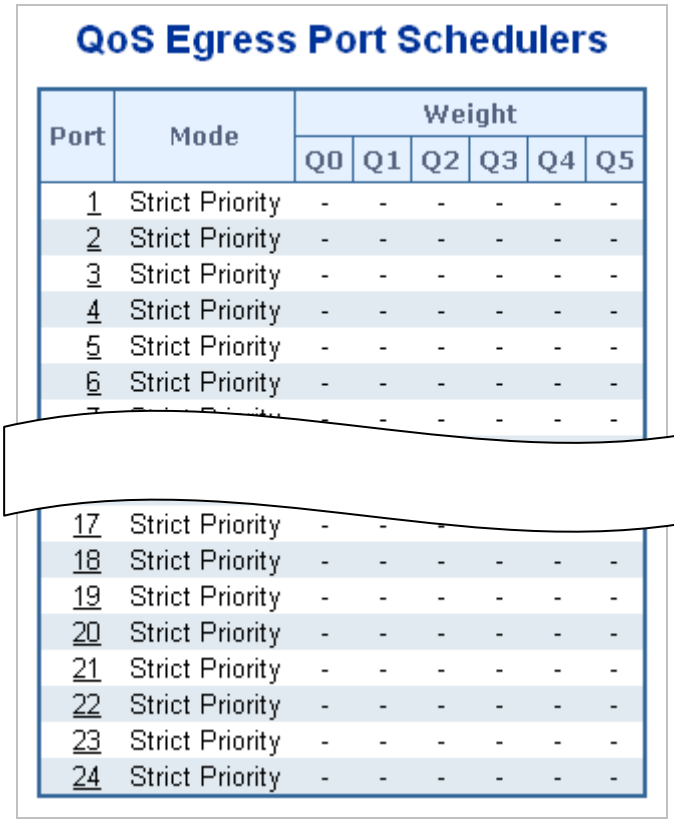
버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.9.4 Port Scheduler

이 페이지는 모든 스위치 포트에 대한 QoS 출력 포트 스케줄러의 개요를 제공합니다. 그림 4-9-4 의 포트 스케줄러 화면이 나타납니다.



QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
17	Strict Priority	-	-	-			
18	Strict Priority	-	-	-	-	-	-
19	Strict Priority	-	-	-	-	-	-
20	Strict Priority	-	-	-	-	-	-
21	Strict Priority	-	-	-	-	-	-
22	Strict Priority	-	-	-	-	-	-
23	Strict Priority	-	-	-	-	-	-
24	Strict Priority	-	-	-	-	-	-

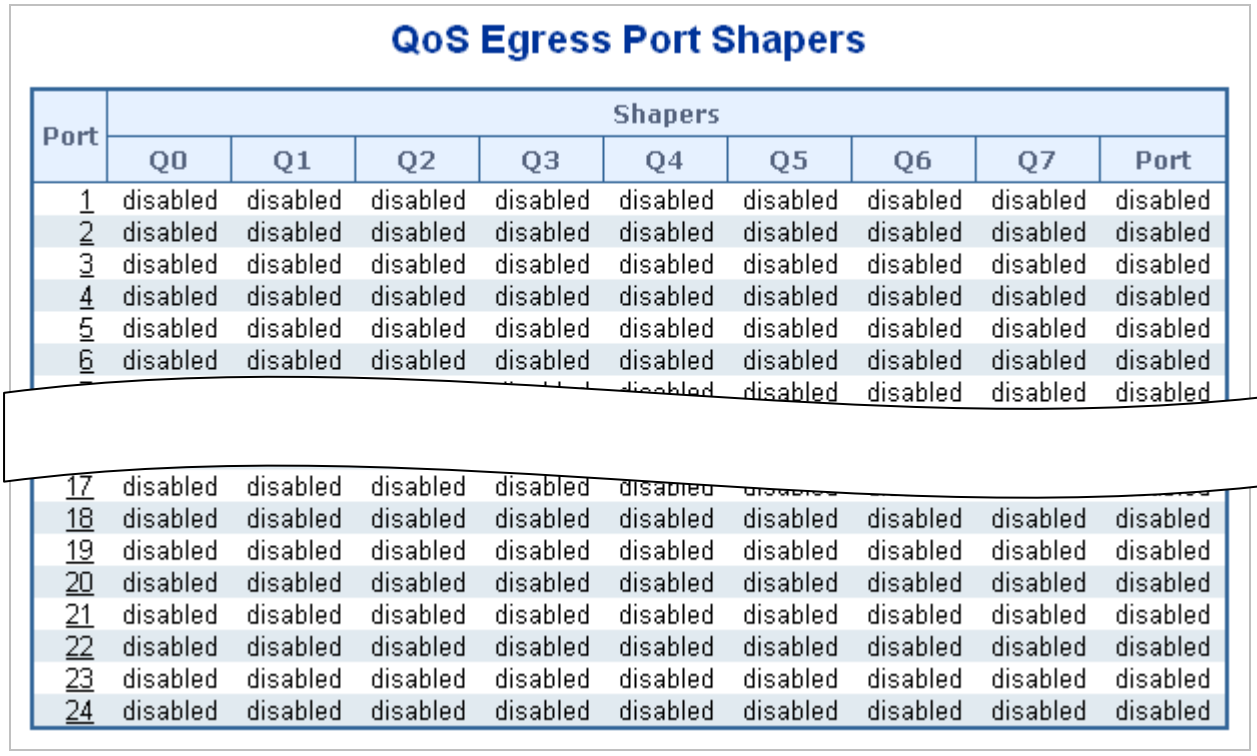
그림 4-9-4 QoS Egress Port Schedule 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Port**	동일한 행에 포함 된 설정의 논리 포트입니다. 스케줄러를 구성하려면 포트 번호를 클릭하십시오. 자세한 내용은 3.9.5.1 장을 참조하십시오.
• **Mode**	이 포트의 스케줄링 방식을를 표시합니다.
• **Q0 ~ Q5**	이 대기열 및 포트의 가중치를 표시합니다.

3.9.5 Port Shaping

이 페이지는 모든 스위치 포트에 대한 QoS 송신 포트 셰이퍼의 개요를 제공합니다. 그림 4-9-5 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
17	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
18	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
19	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
20	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
21	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
22	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
23	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
24	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

그림 4-9-5 QoS Egress Port Shapers 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Port**	동일한 행에 포함 된 설정의 논리 포트입니다. 셰이퍼를 구성하려면 포트 번호를 클릭하십시오. 자세한 내용은 3.9.5.1 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".

3.9.5.1 QoS 출력 포트 스케줄 및 셰이퍼

특정 포트에 대한 Port Scheduler 및 Shapers 가 이 페이지에서 구성됩니다. 그림 4-9-6 의 QoS 출력 포트 스케줄과 셰이퍼 화면이 나타납니다.

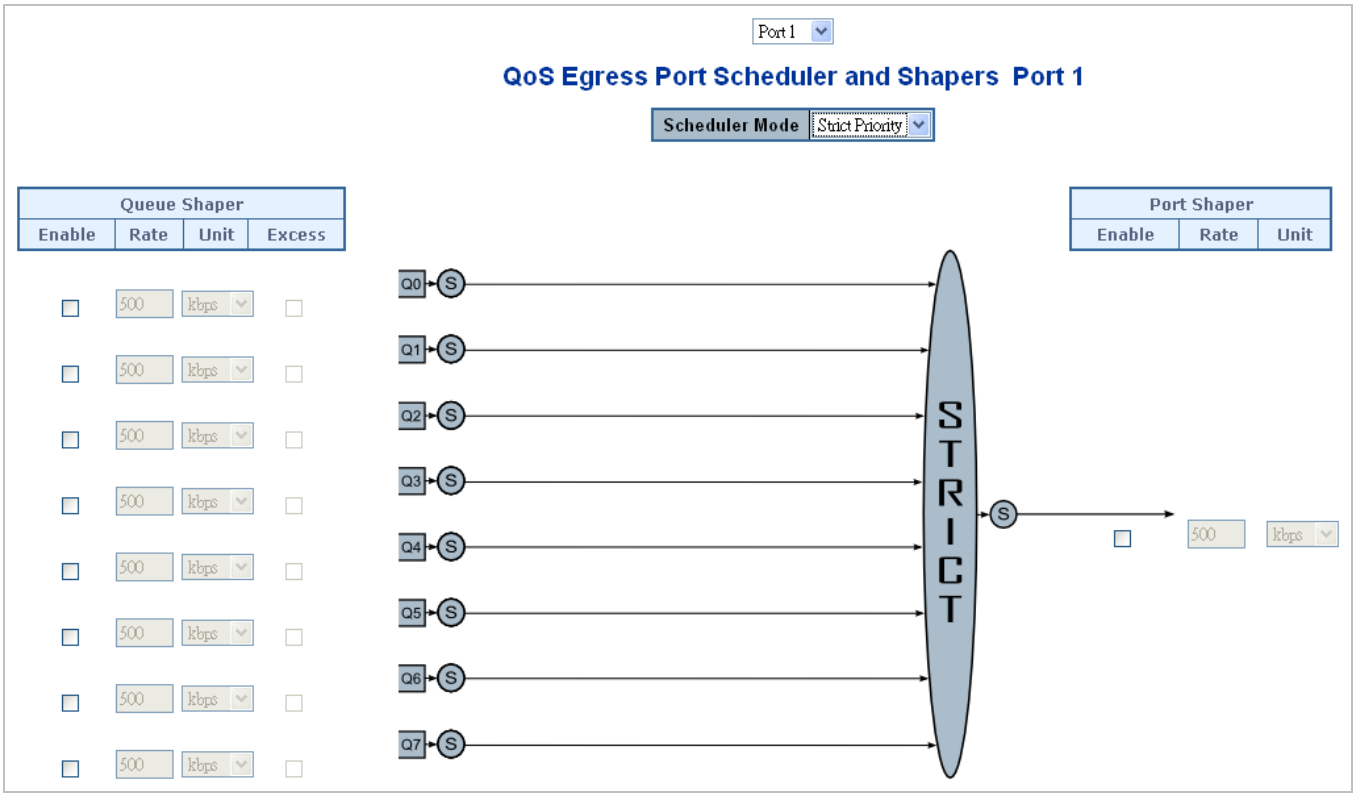


그림 4-9-6 QoS Egress Port Schedule 과 Shapers 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Schedule Mode**	이 스위치 포트에서 스케줄러 방식이가 "제어 우선 순위"인지 "가중치"인지 여부를 제어합니다.
• **Queue Shaper Enable**	이 스위치 포트에서이 큐에 대해 큐 셰이 퍼를 사용할 수 있는지 여부를 제어합니다.
• **Queue Shaper Rate**	큐 셰이퍼의 속도를 제어합니다. 기본값은 500 입니다.이 값은 "Unit"이 "kbps"일 때 100-1000000 으로 제한되고 "Unit"가 "Mbps"일 때 1-3300 으로 제한됩니다.
• **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 Weight**	이 대기열의 가중치를 제어합니다. 기본값은 "17"입니다. 이 값은 1-100 으로 제한됩니다. 이 매개 변수는 "스케줄러 방식"가 "가중치"로 설정된 경우에만 표시됩니다.
• **Queue Scheduler Percent**	이 대기열에 대한 가중치 (%)를 표시합니다. 이 매개 변수는 "스케줄러 방식"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. 기본값은 500 입니다.이 값은 "Unit"이 "kbps"일 때 100-1000000 으로 제한되고 "Unit"가 "Mbps"일 때 1-13200 으로 제한됩니다.
• **Port Shaper Unit**	포트 셰이퍼 속도의 측정 단위를 "kbps"또는 "Mbps"로 제어합니다. 기본값은 "kbps"입니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

Cancel: 로컬로 변경한 내용을 취소하고 이전 페이지로 돌아갑니다.

3.9.6 포트 태그

이 페이지는 모든 스위치 포트에 대한 QoS 출력 포트 태그 리마킹의 개요를 제공합니다. 그림 4-9-7 의 Port Tag Remarking 화면이 나타납니다.

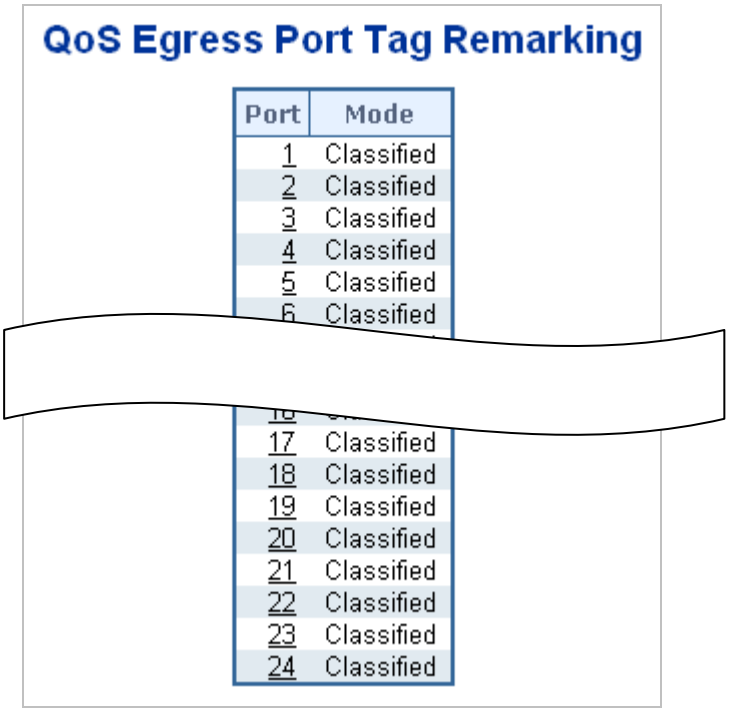


그림 4-9-7 QoS Egress Port Tag Remarking 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명

• **Port**	동일한 행에 포함 된 설정의 논리 포트입니다. 태그 설명을 구성하려면 포트 번호를 클릭하십시오. 자세한 내용은 3.9.6.1 장을 참조하십시오.
• **Mode**	이 포트에 대한 태그 remarking 방식을를 표시합니다. **Classified**: 분류된 PCP / DEI 값을 사용합니다. **Default**: 기본값: 기본 PCP / DEI 값을 사용합니다 **Mapped**: 매핑 된 버전의 Qos 클래스 및 DP 수준을 사용합니다.

3.9.6.1 송신 포트 태그 입력

특정 포트에 대한 QoS 출력 포트 태그 리마킹이 페이지에서 구성됩니다. 그림 4-9-8 의 QoS Egress Port Tag Remarking sscreen 이 나타납니다.

그림 4-9-8 QoS Egress Port Tag Remarking 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Mode**	이 포트에 대한 태그 remarking 방식을를 제어합니다. **Classified**: 분류 된 PCP / DEI 값을 사용 **Default**: 기본 PCP / DEI 값을 사용 **Mapped**: 핑 된 버전의 QoS 클래스 및 DP 수준을 사용
• **PCP/DEI Configuration**	방식이가 Default 로 설정된 경우 사용되는 기본 PCP 및 DEI 값을 조정합니다.
• **DP level Configuration**	방식이가 맵핑으로 설정된 경우 놓기 우선 순위 레벨 변환 테이블을 제어합니다. 이 표의 목적은 2 비트 분류 된 DP 레벨을 (QoS 클래스, DP 레벨)에서 (PCP, DEI) 맵핑 프로세스에서 사용되는 1 비트 DP 레벨로 줄이는 것입니다.
• **(QoS class, DP level) to (PCP, DEI) Mapping**	방식이가 맵핑으로 설정된 경우 분류 (QoS 클래스, DP 레벨)에서 (PCP, DEI) 값으로의 매핑을 제어합니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

Cancel: 취소하고 이전페이지의 모습으로 돌아갑니다.

3.9.7 Port DSCP

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

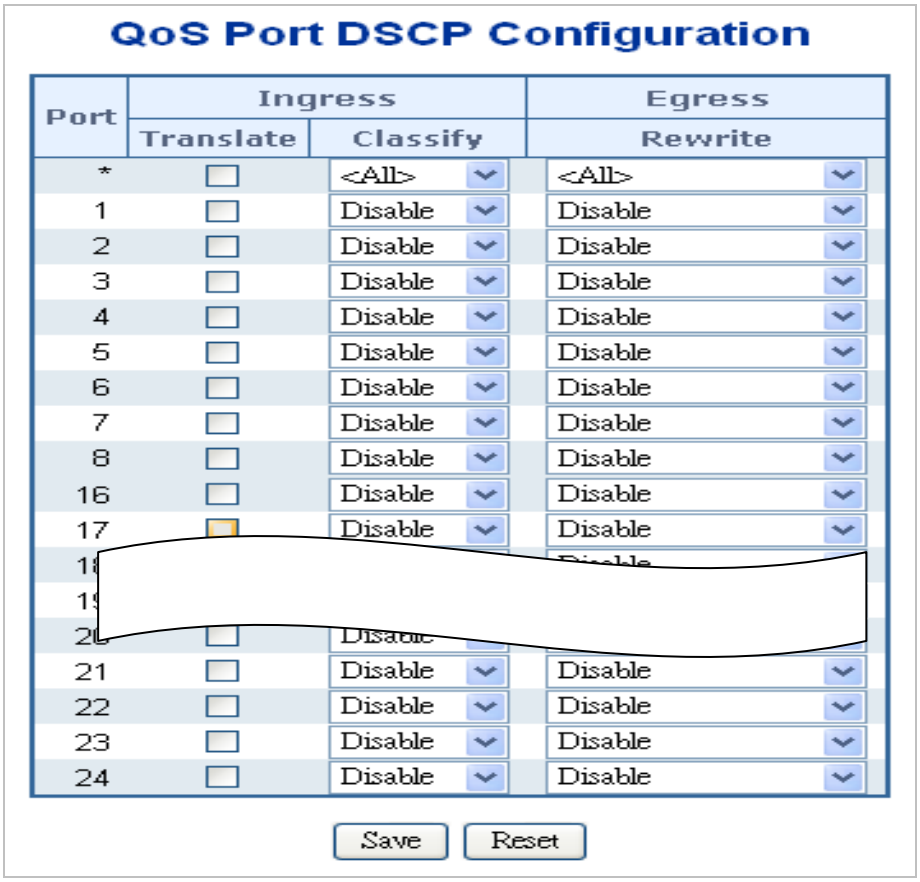


그림 4-9-9 QoS Port DSCP 구성화면

다음과 같은 기능을 소개합니다.

기능	
• **Port**	포트의 열은 dscp 입구 및 출구 설정을 구성 할 수있는 포트 목록을 표시합니다.
• **Ingress**	Ingress 설정에서 개별 포트의 진입 변환 및 분류 설정을 변경할 수

	있습니다. Ingress 에는 두 가지 구성 매개 변수가 있습니다. ■ **분류** ■ **번역**
• **Translate**	입력 변환을 사용하려면 확인란을 클릭합니다.
• **Classify**	포트의 분류에는 4 가지 값이 있습니다. ■ **Disable**: 진입 DSCP 분류 없음. ■ **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 분류합니다.
• **Egress**	포트 출력 재기록은 다음 중 하나 일 수 있습니다. ■ **Disable**: 출력 재 작성 없음. ■ **Enable**: 다시 매핑하지 않고 다시 쓰기 활성화. ■ **Remap DP Unaware**: 분석기의 DSCP 가 재 매핑되고 재 매핑 된 DSCP 값으로 프레임이 주목됩니다. 다시 매핑 된 DSCP 값은 항상 'DSCP Translation-> Egress Remap DP0'테이블에서 가져옵니다. ■ **Remap DP Aware**: 분석기의 DSCP 가 다시 매핑되고 다시 매핑 된 DSCP 값으로 프레임이 다시 표시됩니다. 프레임의 DP 수준에 따라 다시 매핑 된 DSCP 값은 'DSCP Translation-> Egress Remap DP0'테이블 또는 'DSCP Translation-> Egress Remap DP1'테이블에서 가져옵니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.9.8 DSCP 기반 QoS

이 페이지에서는 모든 스위치에 대한 기본 QoS DSCP 기반 QoS 입력 분류 설정을 구성 할 수 있습니다. 그림 4-9-10 의 DSCP 기반 QoS 화면이 나타납니다.

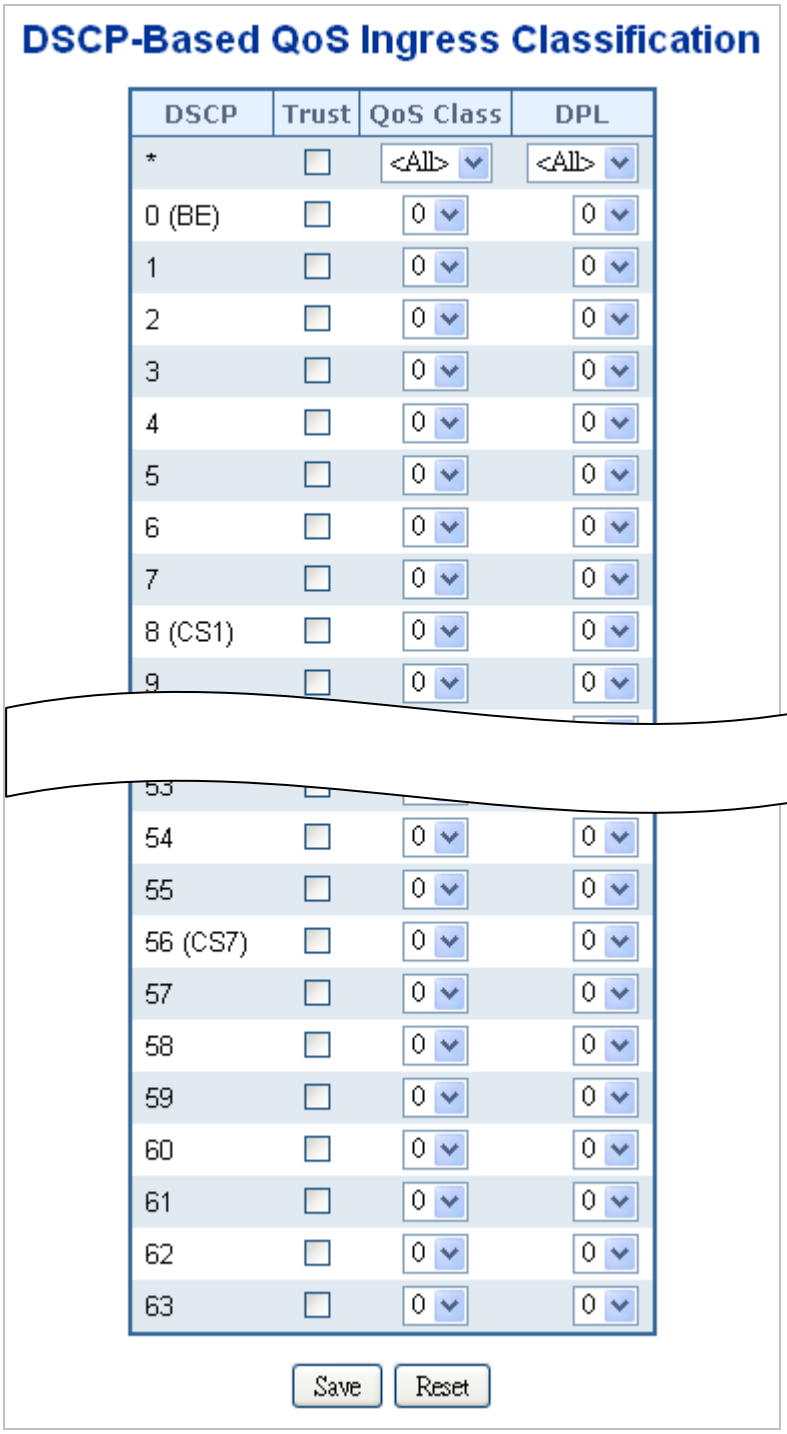


그림 4-9-10 DSCP-Based QoS Ingress Classification 페이지 화면

다음과 같은 기능을 소개합니다.

기능	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**	제거 우선 순위 (0-1)

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.9.9 DSCP 변환

이 페이지에서는 모든 스위치에 대한 기본 QoS DSCP 변환 설정을 구성 할 수 있습니다. 송수신에서 DSCP 변환을 수행 할 수 있습니다. 그림 4-9-11 의 DSCP 변환 화면이 나타납니다

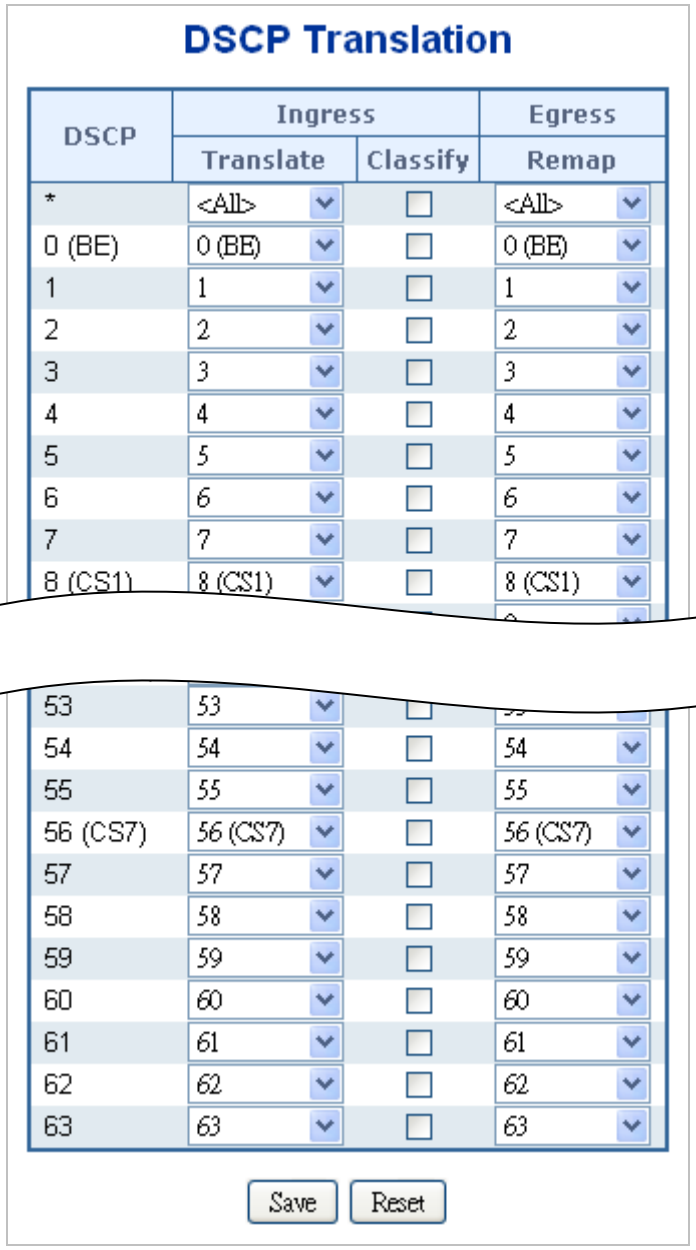


그림 4-9-11 DSCP Translation 페이지 화면

다음과 같은 기능을 소개합니다.

기능	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**	수신 측 DSCP 는 (0-63) DSCP 값 중 하나로 변환 할 수 있습니다.

• **Classify**	수신 측에서 분류법을 사용할수 있습니다.
• **Egress**	출력면에는 다음과 같은 구성 가능한 매개 변수가 있습니다. **Remap**
• **Remap**	선택 메뉴에서 재 매핑하려는 DSCP 값을 선택하십시오. DSCP 값 범위는 0 에서 63 사이입니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.9.10 DSCP 분류

이 페이지에서 DSCP 값을 QoS 클래스 및 DPL 값에 매핑 할 수 있습니다. 그림 4-9-12 의 DSCP 분류 화면이 나타납니다.

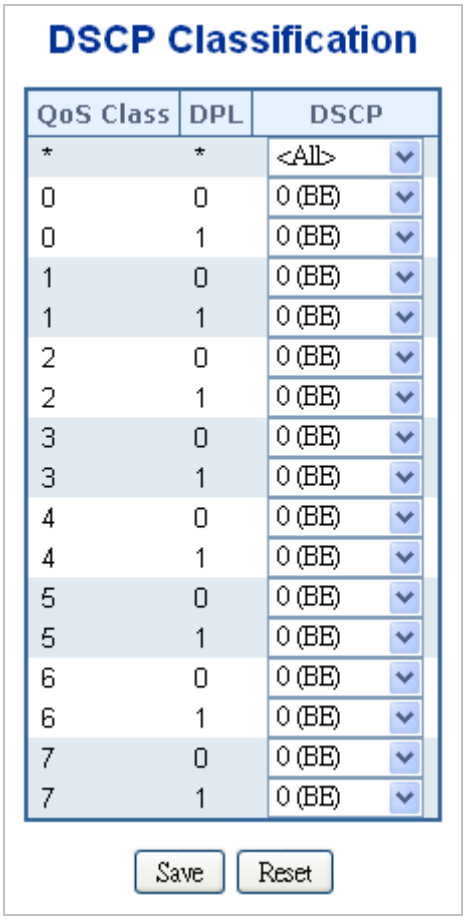


그림 4-9-12 DSCP Classification 페이지 화면

다음과 같은 기능을 소개합니다.

기능	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.
• **DSCP**	DSCP 메뉴에서 DSCP 값 (0-63)을 선택하여 DSCP 를 해당 QoS 클래스 및 DPL 값에 매핑합니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.9.11 QoS 제어 리스트

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 가장 낮은 더하기 기호를 클릭하십시오.

그림 4-9-13 의 QoS Control List 화면이 나타납니다.

그림 4-9-13 QoS Control List 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **QCE#**	QCE 의 색인을 나타냅니다.
• **Port**	QCE 로 구성 된 포트 목록을 나타냅니다.
• **Frame Type**	신규프레임에 프레임 타입을 나타냅니다. 가능한 프레임 형태는: **Any**: QCE 는 모든 타입에들어간다. **Ethernet**: 이더넷 프레임 (이더넷 유형 0x600-0xFFFF) 만 허용됩니다 LLC : 전용 (LLC) 프레임이 허용됩니다. SNAP : (SNAP) 프레임 만 허용됩니다. IPv4 : QCE 는 IPV4 프레임 만 일치시킵니다. IPv6 : QCE 는 IPV6 프레임 만 일치시킵니다.

• **SMAC**	발신지 MAC 주소의 OUI 필드, 즉 MAC 주소의 처음 3 옥텟 (바이트)을 표시합니다.
• **DMAC**	수신 프레임의 대상 MAC 주소 유형을 지정하십시오. 가능한 값은 다음과 같습니다. **Any**: 모든 유형의 대상 MAC 주소가 허용됩니다. **Unicast**: 유니 캐스트 MAC 주소 만 허용됩니다. **Multicast**: 멀티 캐스트 MAC 주소 만 허용됩니다. **Broadcast**: 브로드 캐스트 MAC 주소 만 허용됩니다. 기본값은 'Any'로 표시 됩니다.
• **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**	감소표시등 : DEI 의 유효 값은 0, 1 또는 'Any'사이의 값 중 하나 일 수 있습니다.
• **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 **DPL**: 분류 된 우선 순위 수준 **DSCP**: 분류 된 DSCP 값.
• **Modification Buttons**	다음을 사용하여 테이블의 각 QCE 를 수정할 수 있습니다. : 현재 행 앞에 새로운 QCE 를 삽입합니다. : QCE 를 편집합니다. : QCE 를 목록 위로 이동합니다. : QCE 를 목록 아래로 이동합니다. : QCE 를 삭제합니다. :가장 낮은 plus 신호는 QCL 목록 맨 아래에 새 항목을 추가합니다..

3.9.11.1 QoS Control 전체 구성

그림 4-9-14 의 QCE Configuration 화면이 나타납니다..

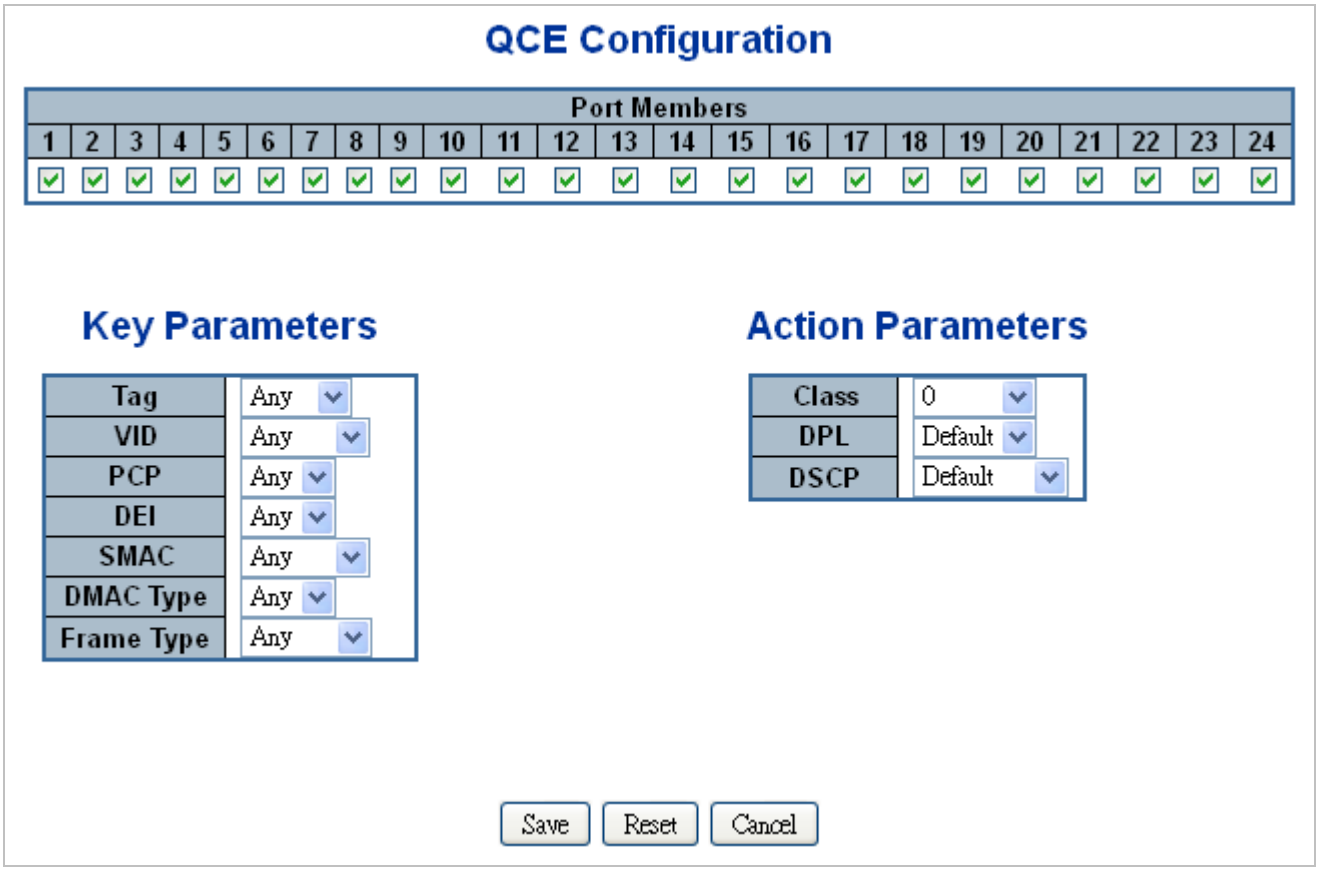


그림 4-9-14 QCE 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Port Members**	QCL 항목의 포트 구성원을 만들 경우 확인란을 선택하십시오. 기본적으로 모든 포트가 검사됩니다.
• **Key Parameters**	키 구성 파라미터는 다음과 같이 나타납니다. **Tag** 태그 필드 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** 드롭 다운 표시등: DEI 의 유효한 값은 0,1 또는'임의'값 사이의 값일 수 있습니다. **SMAC** 소스 MAC 주소:24MS 비트(OUI)또는 'Any' **DMAC Type** 대상 MAC 유형:가능한 값은 유니캐스트(UC), 멀티 캐스트(MC), 브로드캐스트(BC)또는 'Any '입니다. **Frame Type** 프레임 형식은 다음에 따라 변형이 가능하다. 1. **Any**

	2. **Ethernet** 3. **LLC** 4. **SNAP** 5. **IPv4** 6. **IPv6** 모든 프레임의 형식은 위와같이 설명된다.
• **Any**	모든 유형의 프레임을 허용합니다.
• **Ethernet**	**Ethernet Type** 유효한 이더넷 유형은 0x600 또는 'Any'이지만 0x800(IPv4)및 0x86HDD(IPv6)를 제외하고 기본 값은 '임의'입니다.
• **LLC**	**SSAP Address** 유효한 SSAP(소스 서비스 액세스 지점)는 0x00 부터 0xFF 또는'Any'로 다를 수 있습니다. 기본 값은 'Any '입니다. **DSAP Address** 유효한 DSAP(목적 서비스 액세스 지점)는 0x00 부터 0xFF 또는'Any'로 다를 수 있습니다. 기본 값은 '**Any** '입니다. **Control Address** 유효한 제어 주소는 0x00~0xFF 또는'Any'로 달라질 수 있으며, 기본 값은 'Any'입니다.
• **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 : (0-255, TCP or UDP) or '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 Code Point value(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 조각 옵션 : 예|아니오|모두 **Sport** 출발지 TCP / UDP 포트 : (0-65535) 또는 '모두', 특정 또는 IP 프로토콜에 해당하는 포트 범위 UDP / TCP **Dport** 목적지 TCP / UDP 포트 : (0-65535) 또는 '모두', 특정 또는 IP 프로토콜에 해당하는 포트 범위 UDP / TCP
• **IPv6**	**Protocol** IP 프로토콜 수: (0-255, TCP or UDP) or 'Any' **Source IP** IPv6 시작 주소: (a.b.c.d) or 'Any', 32 LS bits **DSCP** Diffserv Code Point value(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** 출발 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) or '기본값'. **DP** 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. '기본값'은 기본 분류 된 값이 이 QCE 에 의해 수정되지 않는다는 것을 의미합니다.

버튼 안내

Save: 구성을 저장하고 기본 QCL 페이지로 이동합니다.

Reset: 이전 저장값으로 되돌립니다.

Cancel: 모든 변환값에 저장없이 이전 상태로 되돌립니다.

3.9.12 QoS Status

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 4-9-15 의 QoS Control List Status 화면이 나타납니다.

그림 4-9-15 QoS Control List 상태 화면 페이지

다음과 같은 기능을 소개합니다.

기능	설명
• **User**	QCL 관리자
• **QCE#**	QCE 의 색인을 나타냅니다.

• **Frame Type**	송신프레임을 찾는 프레임 유형을 나타냅니다. 가능한 프레임은 다음과 같다: Any : QCE 가 모든 프레임 유형과 일치합니다. Ethernet: 이더넷 프레임 (이더넷 유형 0x600-0xFFFF) 만 허용됩니다. LLC : 전용 (LLC) 프레임이 허용됩니다. SNAP : (SNAP) 프레임 만 허용됩니다. IPv4 : QCE 는 IPV4 프레임 만 일치시킵니다. IPv6 : QCE 는 IPV6 프레임 만 일치시킵니다.
• **Port**	QCE 로 구성된 포트 목록을 나타냅니다.
• **Action**	구성된 매개 변수가 프레임의 내용과 일치하는 경우 수신 프레임에서 수행되는 분류 작업을 나타냅니다. 세가지의 종류로 구성이됩니다. **Class**:분류 된 Qos 클래스, 프레임이 QCE 와 일치하면 큐에 놓입니다. **DPL**: 우선순위 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 안내

Combined : 메뉴선택 칸에서 QCL 상태를 선택합니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

Resolve Conflict : QCL 항목의 충돌상태인 경우 항목을 추가하는 데 필요한 자원을 클릭하여 해제하십시오

Refresh : 새로고침을 합니다.

3.9.13 Storm Control 구성

스위치에 대한 Storm Contro 이 이 페이지에서 구성됩니다.

유니캐스트 스톰율 제어, 멀티캐스트스톰율 제어 및 브로드캐스트 스톰율 제어가 있습니다. 플러딩 된 프레임, 즉 MAC 주소 테이블에 존재하지 않는 (VLAN ID, DMAC) 쌍이있는 프레임에만 영향을 줍니다. 구성은 스위치에서 유니캐스트, 멀티 캐스트 또는 브로드캐스트 트래픽에 대해 허용된 패킷 속도를 나타냅니다. 그림 4-9-16 의 Storm Control Configuration 화면이 나타납니다.

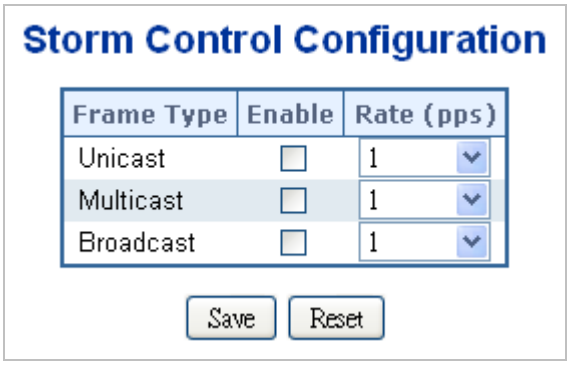


그림 4-9-16 Storm Control 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Frame Type**	특정 행의 설정은 여기에 나열된 프레임 유형 (유니 캐스트, 멀티 캐스트 또는 브로드 캐스트)에 적용됩니다.
• **Enable**	주어진 프레임 유형에 대한 스톰 제어 상태를 활성화 또는 비활성화합니다.
• **Rate**	비율단계는 초당패킷단위로 유효한 값으로는 **1**, **2**, **4**, **8**, **16**, **32**, **64**, **128**, **256**, **512**, **1K**, **2K**, **4K**, **8K**, **16K**, **32K**, **64K**, **128K**, **256K**, **512K**, **1024K**, **2048K**, **4096K**, **8192K**, **16384K** **32768K**

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.9.14 QoS Statistics

이 페이지는 모든 스위치 포트의 다른 대기열에 대한 통계를 제공합니다. 그림 4-9-18 의 QoS Statistics 화면이 나타납니다.

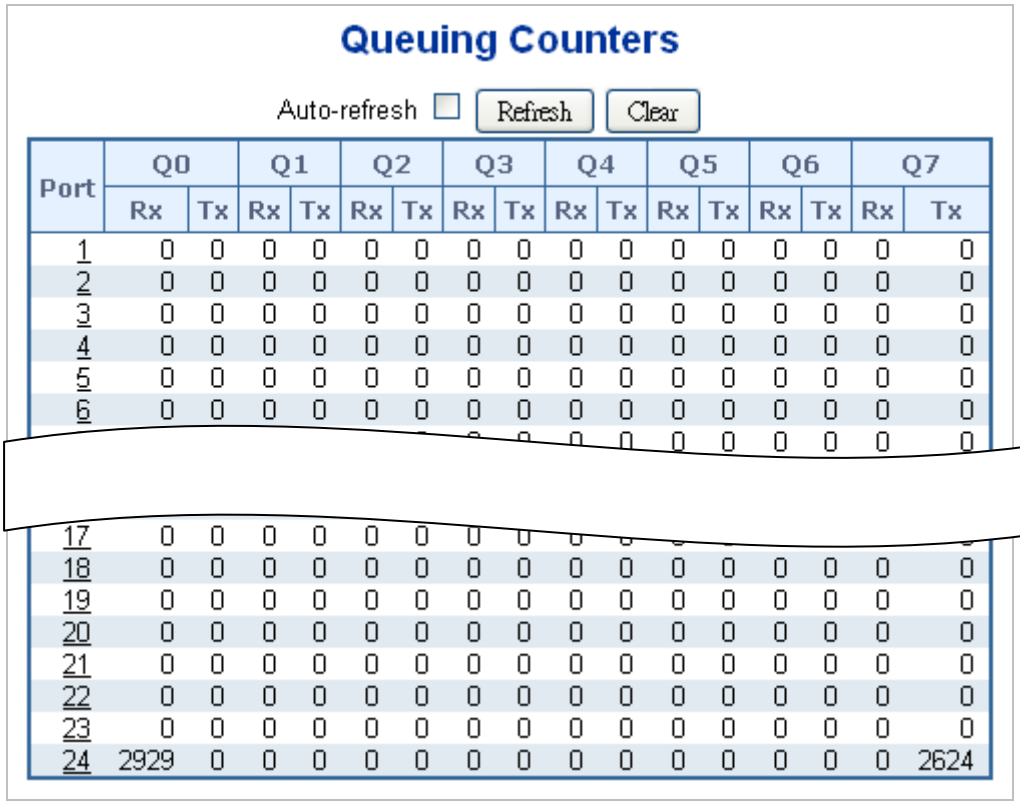


그림 4-9-18 Queuing Counters 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Port**	설정값은 포함한 동일한 행들의 논리포트
• **Q0 ~ Q7**	Q0 부터 8 개의 QoS 가 있는데 Q0 이 가장 낮은 우선순위 큐이다.
• **Rx/Tx**	큐에 대한 송수신 패킷을 주고 받는다.

버튼 안내

Refresh: 페이지를 새로고칩니다.

Clear: 모든 카운터의 기록을 청소합니다.

Auto-refresh : 페이지에 대한 주기적인 새로고침을 자동으로 이행합니다.

3.9.15 보이스 VLAN 구성

보이스 Vlan 은 트래픽전달이 가능하고 스위치는 네트워크트래픽을 스케줄화하고 분류 할수있다. 데이터 하나에 보이스하나를 포트 하나에 두개의 Vlan 사용을 권장합니다. 스위치 IP 장치에 연결하기전에 전화기 IP 에 보이스 ID 를 설정하고 고유의 GUI 틀 통해 구성해야합니다. 그림 4-9-19 참조.

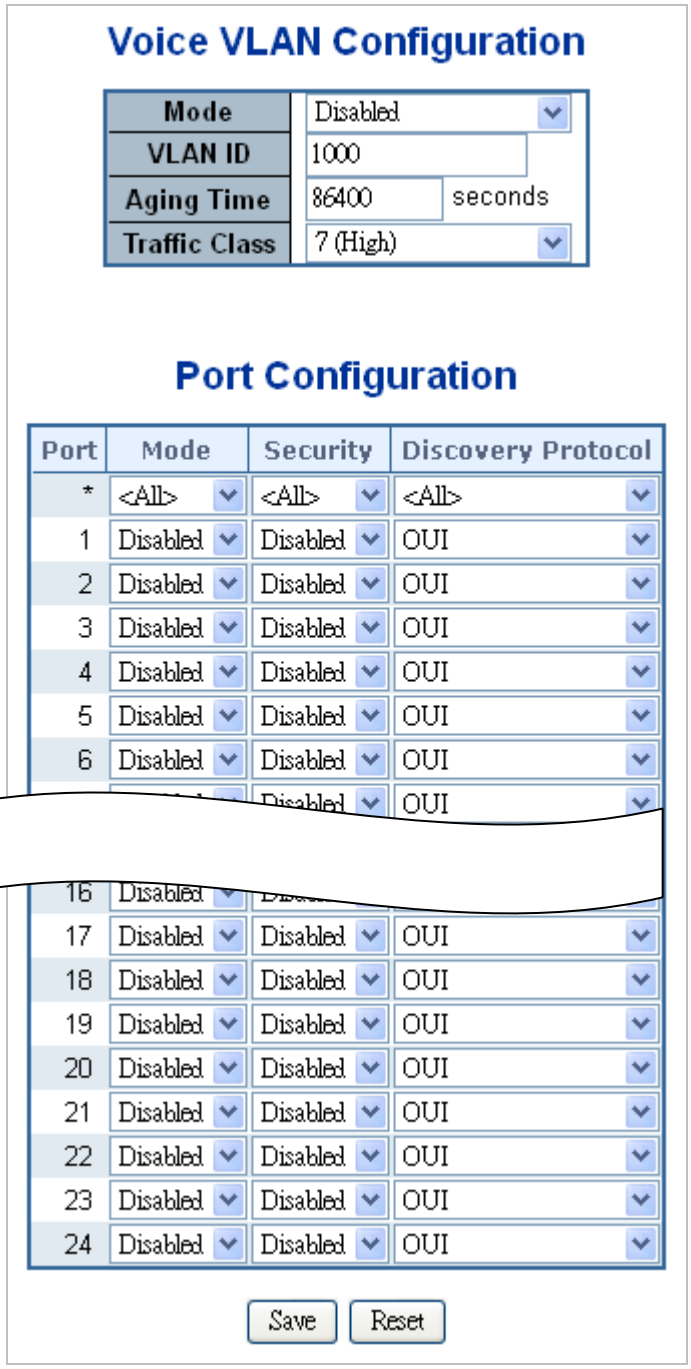


그림 4-9-19 Voice VLAN 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Mode**	보이스 Vlan 방식 작동을 나타냅니다. 음성 Vlan 을 활성화하기전에 MSTP 기능을 비활성화 해야합니다. **Enabled**: 보이스 Vlan 방식 작동을 활성화합니다. **Disabled**: 보이스 Vlan 방식 작동을 비활성화합니다.
• **VLAN ID**	보이스 Vlan ID 를 나타내고 시스템의 고유한 ID 이며 PVID 등등과 같으면

	충돌이며 허용 값의 범위는 1 ~ 4095 입니다.
• **Age Time**	보이스 VLAN 보안 학습 기간 시간을 나타냅니다. 허용 범위는 10 ~ 10000000 초입니다. 보안방식 또는 자동 감지방식이가 활성화되었을 때 사용됩니다. 다른 경우에는 하드웨어 aging 시간을 기반으로합니다. 실제 기간은 [age_time; 2 * age_time] 간격을 의미한다.
• **Traffic Class**	보이스 Vlan 의 트래픽 단계를 나타낸다. 모든 트래픽은 이곳에 적용된다.
• **Port Security**	보이스 Vlan 의 보호방식을를 설정하는것으로 이기능은 보이스 Vlan 의 전화기 Mac 주소가 10 초동안 차단됩니다. 선택박스는 다음과 같습니다. **Enabled**: 보이스 Vlan 의 보호방식을를 활성화합니다. **Disabled**: 보이스 Vlan 의 보호방식을를 비활성화합니다..
• **Port Discovery Protocol**	보이스 VLAN 포트 검색 프로토콜을 나타냅니다. 자동 감지 방식이가 활성화된 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**: OUI 주소로 전화통신 장치를 검색합니다. **LLDP**: LLDP 로 전화통신 장치를 감지합니다. **Both**: OUI 와 LLDP 를 둘다 사용합니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.9.16 Voice VLAN OUI Table

이 페이지에서 VOICE VLAN OUI 테이블을 구성하십시오. 최대 항목 수는 16 입니다. OUI 테이블을 수정하면 OUI 프로세스의 자동 검색이 다시 시작됩니다. 그림 4-9-20 의 Voice VLAN OUI 테이블 화면이 나타납니다.

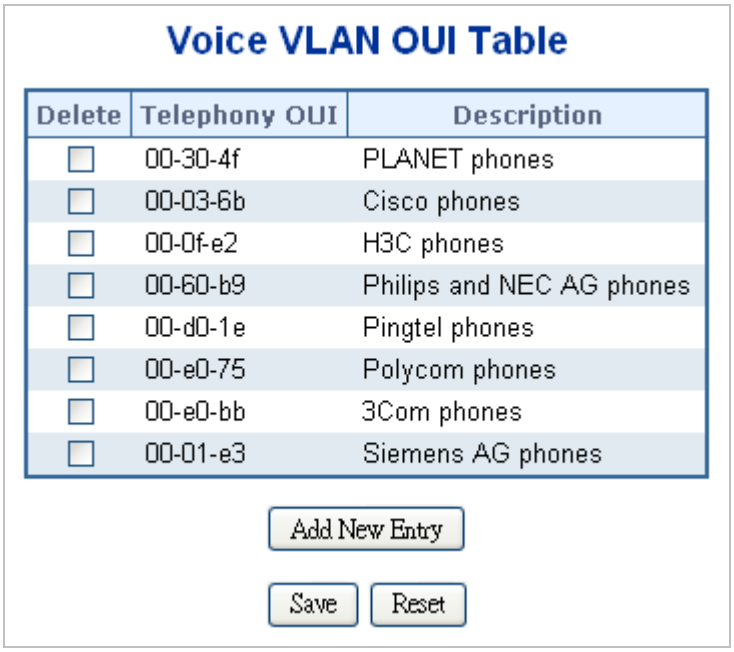


그림 4-9-20 Voice VLAN OUI Table 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Delete**	항목중에 삭제하려면 선택하십시오. 다음 저장 항목중에 삭제 됩니다.
• **Telephony OUI**	전화 통신 OUI 주소는 IEEE 에서 공급 업체에 할당 한 전체적으로 고유한 6 자 “xx-xx-xx” 이며 16 진수로 표현합니다.
• **Description**	OUI 주소에 대한 설명하며 길이는 0-32 사이 입니다.

버튼 안내

Add New Entry: 새로운 전체체 관리항목에 대하여 추가합니다.

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.10 접근 통제 목록(Access Control Lists)

ACL 은 Access Control List 의 약자입니다. 프로세스 또는 프로그램과 같은 특정 트래픽 개체에 대해 허용되거나 거부되는 개별 사용자 또는 그룹을 지정하는 액세스 제어 항목이 포함 된 ACE 목록 표입니다. 액세스 가능한 각 트래픽 객체에는 해당 ACL 에 대한 식별자가 포함됩니다. 권한은 특정 트래픽 개체 액세스 권한 여부를 결정합니다.

ACL 구현은 ACE 가 다양한 상황에 우선 순위가 매겨지는 경우와 같이 복잡 할 수 있습니다. 네트워킹에서 ACL 은 호스트나 서버에서 사용할 수 있는 서비스 포트와 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 있으며 이 컨텍스트에서는 방화벽과 유사합니다.

ACE 는 Access Control Entry 의 약자입니다. 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 다양한 매개 변수 옵션이 포함되어 있습니다.

3.10.1 Access Control List Status

이 페이지는 여러 ACL 사용자의 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 Voice VLAN OUI Table 화면이 나타납니다.

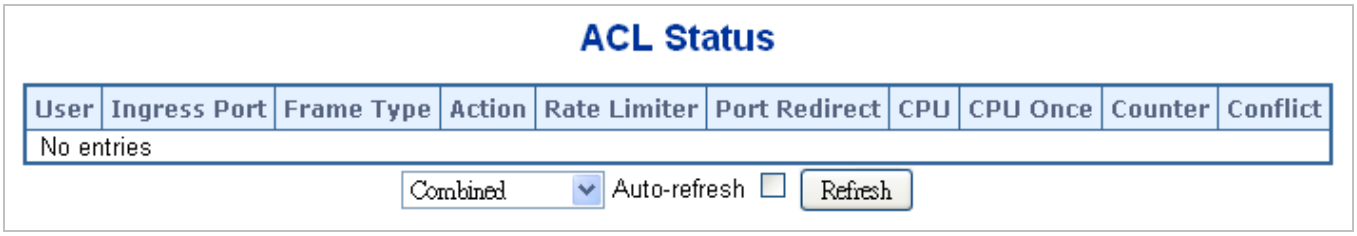


그림 4-10-1 ACL 상태 화면 페이지

다음과 같은 기능을 소개합니다.

기능	설명
• **User**	ACL 사용자를 나타낸다.
• **Ingress Port**	ACE 의 수신포트를 나타낸다. 가능한 값은 다음과 같습니다. **Any**: ACE 는 수신포트와 일치한다. **Policy**:ACE 는 진입 포트를 특정 정책과 일치시킵니다.. **Port**: ACE 는 특정 수신 포트와 일치시킵니다.
• **Frame Type**	ACE 의 프레임 타입을 나타냅니다.가능한 값은 다음과 같습니다: **Any**:ACE 는 모든 프레임값과 일치합니다.. **EType**:ACE 는 이더넷 유형 프레임과 일치합니다. ARP 와 IP 프레임은 이더넷유형과 일치하지 않는다.

	ARP: ARP/RARP 프레임은 ACE 와 일치합니다 **IPv4**: 모든 IPv4 프레임은 ACE 와 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 기능의 전달작업을 나타낸다. **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 제한기 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.
• **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 안내

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

Refresh: 새로고침을 합니다.

3.10.2 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 256 입니다.

새 ACE 를 목록에 추가하려면 가장 낮은 더하기 기호를 클릭하십시오. 내부 프로토콜에 사용되는 예약 된 ACE 는 편집하거나 삭제할 수 없으며 주문 순서를 변경할 수 없으며 우선 순위가 가장 높습니다.

그림 4-10-2 의 액세스 제어 목록 구성 화면이 나타납니다.

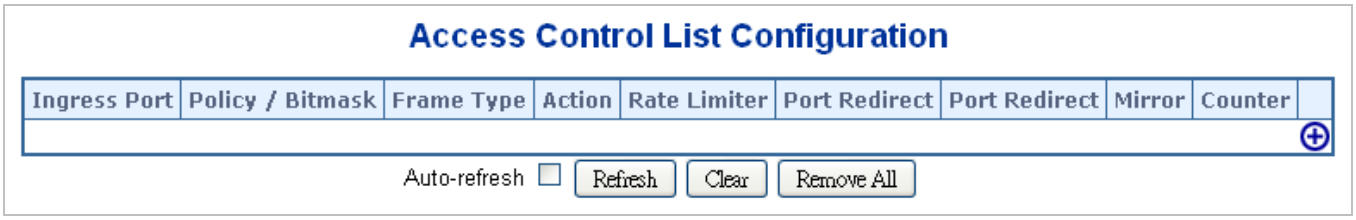


그림 4-10-2 Access Control List 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Ingress Port**	ACE 의 수신 포트를 나타냅니다. 가능한 값은 다음과 같습니다. All : ACE 는 모든 진입 포트와 일치합니다. Port : ACE 는 특정 수신 포트와 일치합니다
• **Policy / Bitmask**	ACE 의 정책 번호와 비트 마스크를 나타냅니다.
• **Frame Type**	ACE 의 프레임 유형을 나타냅니다. 가능한 값은 다음과 같습니다. **Any**: ACE 에 어떤프레임과도 유형이 일치한다. **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**: 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 프레임을 전달하고 학습을 할 수 있다. **Deny**: ACE 와 일치하는 프레임이 삭제됩니다.
• **Rate Limiter**	ACE 의 속도 제한기 번호를 나타냅니다. 허용 범위는 1- 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.
• **Mirror**	이 포트의 미러 작동을 지정하십시오. ACE 와 일치하는 프레임은 대상 미러포트에 미러링됩니다 . 선택값은 다음과 같습니다. **Enabled**: 포트에서 수신된 것은 미러링된다. **Disabled**: 포트에서 수신된 프레임은 미러링 되지 않는다. 기본값은 'Disable'값 입니다.

• **Counter**	카운터는 ACE 에 프레임이 도달 한 횟수를 나타냅니다.
• **Modification Buttons Information.**	다음의 버튼 설명을 사용하여 테이블의 각 ACE (Access Control Entry)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. : 가장 작은 더하기 기호는 ACE 목록 맨 아래에 새 항목을 추가합니다.

버튼 안내

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

Refresh: 새로고침을 합니다.;모든 변경사항을 초기화합니다.

Clear: 카운터를 모두 초기화 한다.

Remove All:모든 ACE 목록을 지웁니다..

3.10.3 ACE 구성

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.

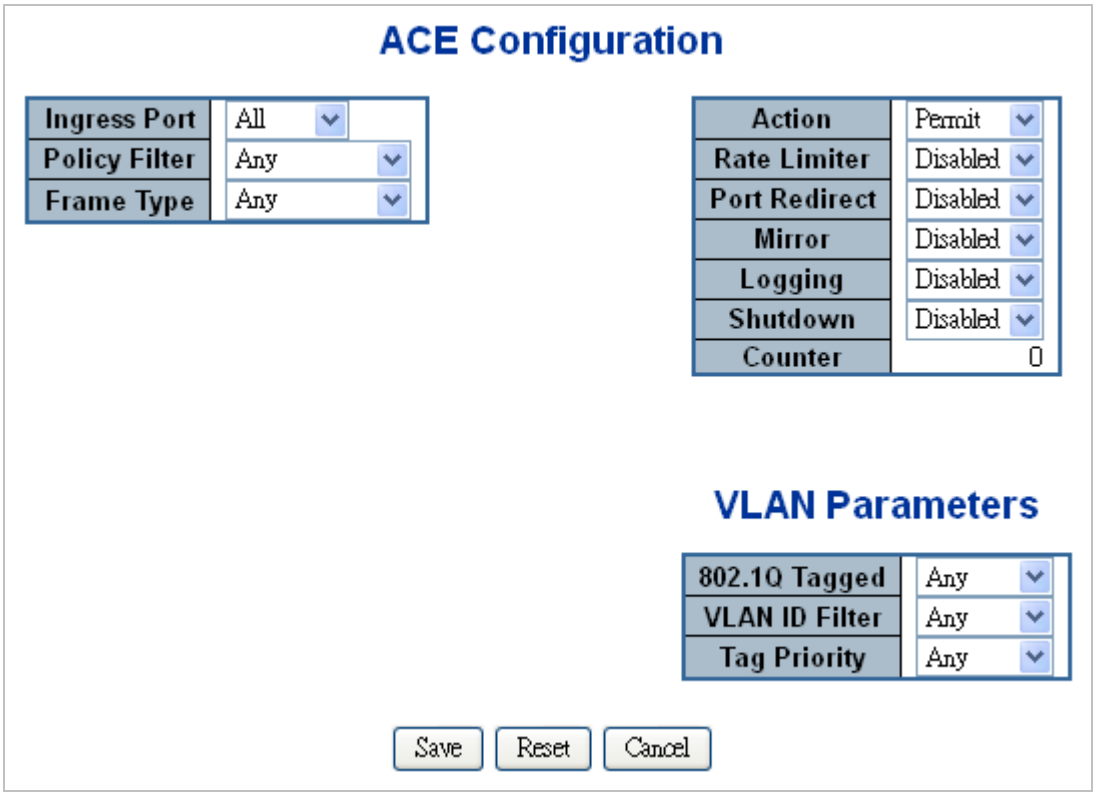


그림 4-10-3 ACE 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Ingress Port**	ACE 가 적용되는 수신포트를 선택하시오 **Any**: 모든포트 선택 **Port n**: 적용할 특정 포트 선택
• **Policy Filter**	ACE 필터에 대한 정책 번호를 지정하세요. **Any**: 정책필터가 지정되지 않는다. (정책필터는 신경쓰지 않는다) **Specific**: 이 ACE 로 특정 정책을 필터링하려면이 값을 선택하십시오. 정책 값을 입력하기위한 두 개의 필드와 비트 마스크가 나타납니다.
• **Policy Value**	정책 필터에 대해 "특정"을 선택한 경우 특정 정책 값을 입력 할 수 있습니다. 허용되는 범위는 0 에서 255 까지입니다.
• **Policy Bitmask**	정책 필터에 대해 "특정"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 프레임이 ACE 와 일치한다. **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**: 이 ACE 에 도달하는 프레임에 ACE 작업에 대한 권한이 부여됩니다. **Deny**: 이 ACE 에 도달하는 프레임이 삭제됩니
• **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.
• **Mirror**	이 포트의 미러 작동을 지정하십시오. ACE 와 일치하는 프레임은 대상 미러 포트에 미러링됩니다. 허용되는 값은 다음과 같습니다. **Enabled**: 미러링한 포트를 프레임이 받는다 **Disabled**: 포트에서 수신 된 프레임은 미러링되지 않습니다.. 기본값은 Disabled 입니다.
• **Logging**	ACE 의 로깅 작업을 지정하십시오. 허용되는 값은 다음과 같습니다. **Enabled**: ACE 와 일치하는 프레임은 시스템로그에 저장된다. **Disabled**: 프레임과 일치하는 것은 로그에 저장되지 않는다. 시스템 로그 메모리 크기와 로깅속도는 제한적입니다.
• **Shutdown**	ACE 의 포트 종료 작동을 지정하십시오. 허용되는 값은 다음과 같습니다 **Enabled**: 프레임이 ACE 와 일치하면 수신 포트가 비활성화됩니다. **Disabled**: ACE 의 셧다운이 비활성화됩니다.
• **Counter**	카운터는 ACE 에 프레임이 도달한 횟수를 나타낸다.

■ MAC Parameters

기능	설명
• **SMAC Filter**	(프레임 유형이 이더넷 또는 ARP 인 경우에만 표시됨) 이 ACE 에 대한 소스 MAC 필터를 지정하십시오. **Any**: SMAC 필터가 지정되지 않습니다. 필터상태는 “무시”상태입니다. **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"입니다. 이 ACE 를 통한 프레임이 이 SMAC 값과 일치합니다.
• **DMAC Filter**	이 ACE 에 대한 대상 MAC 필터를 지정하십시오. **Any**: DMAC 필터가 지정되지 않는다. **MC**: 프레임은 반드시 멀티케스트 **BC**: 프레임은 반드시 브로드케스트 **UC**: 프레임은 반드시 유니케스트 **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"입니다. 이 ACE 를 치는 프레임이이 DMAC 값과 일치합니다.

■ VLAN Parameters

기능	설명
• **802.1Q Tagged**	태그가 지정 된 802.1Q 에 따라 프레임이 동작을 수행 할 수 있는지 여부를 지정합니다 . 허용되는 값은 다음과 같습니다. **Any**: 모든값을 허용 이외는 '무시' 상태. **Enabled**: 프레임 태그 활성화 전용. **Disabled**: 프레임 태그 비활성화 전용. 기본값은 'Any' 형태로 설정되어있음
• **VLAN ID Filter**	ACE 에 Vlan ID 필터를 지정합니다. **Any**: Vlan ID 필터가 지정되지 않았다. 이외는 '무시'상태 **Specific**: ACE 로 특정 ID 를 필터링할경우 선택합니다.
• **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 ACE의 태그 우선 순위를 지정하십시오. 이 ACE를 치는 프레임이이 태그 우선 순위와 일치합니다. 허용되는 숫자 범위는 0 에서 7 까지입니다. 값은 태그 우선 순위가 지정되지 않음을 의미합니다 (태그 우선 순위는 "무시"입니다).

■ ARP Parameters

프라임 형태인 ARP 가 선택될 때 ARP 매개체로 구성되어있습니다.

기능	설명

• **ARP/RARP**	이 ACE 에 대해 사용 가능한 ARP / RARP opcode (OP) 플래그를 지정하십시오. **Any**: ARP/RARP OP flag 비활성화 상태입니다. (OP 는 유후상태입니다) **ARP**: 프레임에 ARP/RARP 가 opcode 가 ARP 로 설정해야한다. **RARP**: 프레임에 ARP/RARP 가 Opcode 가 RARP 로 설정해야한다. **Other**: 프레임에 알수없는 ARP/RARP Opcode 플래그가 있습니다.
• **Request/Reply**	ACE 에 대한 사용가능한 ARP /RARP (OP)플래그를 지정합니다.. **Any**: ARP 나 RARP OP flag 가 비활성화 상태입니다. **Request**:프레임에 요청 ARP 나 요청 RARP OP 플래그가 있어야합니다. **Reply**:프레임에 응답 ARP 나 응답 RARP OP 플래그가 있어야합니다..
• **Sender IP Filter**	ACE 에 송신자 IP 필터를 지정합니다. **Any**: 송신자의 IP 필터를 지정하지 않습니다. **Host**: 송신자 IP 필터를 호스트로 설정합니다. SIP 주소필드에 + **Network**: 송신자 IP 필터가 네트워크로 설정하고 SIP 주소 및 마스크필드에 송신자 IP 주소와 마스크를 지정하십시오.
• **Sender IP Address**	송신 IP 필터에 호스트나 네트워크를 선택한경우, 십진수 표기법으로 특정 송신 IP 주소를 입력 할 수 있습니다.
• **Sender IP Mask**	송신 IP 필터에 네트워크를 선택한 경우 특정 송신자 IP 마스크를 십진수 표기법으로 입력할 수 있습니다.
• **Target IP Filter**	특정 ACE 에 지정 IP 필터를 설정합니다. **Any**: 모든 IP 필터링에 대해 를 허용합니다. **Host**:호스트로 IP 필터가 설정된 경우 목표 IP 주소 필드에 IP 주소를 지정하십시오. **Network**:네트워크로 IP 필터가 설정된 경우 목표 IP 주소 및 목표 IP 마스크 필드에 지정하십시오.
• **Target IP Address**	목표 IP 주소에 호스트나 아이피주소가 선택된 경우 십진수로 표기 할 수 있습니다.
• **Target IP Mask**	지정 IP 필터에 네트워크로 선택한경우 IP 마스크를 십진수로 표기 할 수 있습니다.
• **ARP Sender MAC Match**	프레임이 송신자 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 값이 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: 모든값을 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 값이 허용됩니다
• **IP**	프레임이 ARP / RARP 하드웨어 주소 공간 (HRD) 설정에 따라 동작을 수행 할 수 있는지 여부를 지정합니다. **0**: HLD 가 이더넷 (1)인 ARP/RARP 프레임 **1**: HLD 가 이더넷 (1)인 ARP/RARP 프레임 **Any**: 모든 값이 허용됩니다.
• **Ethernet**	프레임이 ARP/ RARP 프로토콜 주소공간 **(PAD)** 설정에 따라 동작을 수행 할 수 있는지 여부를 지정합니다. **0**: PRO 가 IP (0x800)와 동일한 ARP / RARP 프레임 **1**: PRO 가 IP (0x800)와 동일한 ARP / RARP 프레임 **Any**: 모든 값이 허용됩니다.

■ IP Parameters

IP 파라미터는 IPv4 를 선택할 경우에만 작동하는 기능이다.

기능	설명
• **IP Protocol Filter**	ACE 에 대한 IP 프로토콜 필터를 지정합니다. **Any**: 모든값을 허용합니다, **Specific**: ACE 로 특정 IP 프로토콜 필터를 입력합니다,—(아닐경우 전부사망) **ICMP**: Ipv4 ICMP 포르토콜 프레임을 필터링 하려면 ICMP 를 선택하고 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 프로토콜값이 “지정”일 때 특정값을 입력이 가능하고 허용범위 0~255 까지이다. 이 IP 프로토콜 값은 ACE 의 프레임과 일치한다.
• **IP TTL**	실시간으로 지정설정이 ACE 에서 가능합니다. **zero**: 0 보다 큰 TTL(Time-To-Live)필드가 있는 IPv4 프레임은 일치하지 않는다.

	non-zero: 0 보다 큰 TTL(Time-To-Live)필드가 있는 IPv4 프레임은 일치한다. **Any**: 모든 값이 허용됩니다.
• **IP Fragment**	ACE 에 대한 조각 오프셋 설정을 지정합니다. 여기에 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 불일치합니다. **Yes**: MF 비트가 설정되거나 FRAG OFFSET 필드가 0 보다 큰 IPv4 프레임은이 항목과 일치해야 합니다. **Any**: 모든 값이 허용됩니다.
• **IP Option**	ACE 에 대한 플레이그 옵션을 지정하여 설정합니다. **No**: 옵션 플래그가 설정 된 IPv4 프레임은 항목과 불일치합니다. **Yes**: 옵션 플래그가 설정 된 IPv4 프레임은 항목과 일치합니다 **Any**: 모든 값이 허용됩니다.
• **SIP Filter**	ACE 에 대한 원본 IP 필터를 설정합니다. **Any**: 지정 IP 필터를 설정하지 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 마스크 필드에 IP 주소와 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 지정합니다. **Any:** 목적지 IP 필터가 설정되지 않습니다. **Host**: 목적지 IP 필터가 호스트로 설정되고 DIP 주소 필드에 목적지 IP 주소를 설정하도록 나타냅니다. **Network**: 목적지 IP 필터가 네트워크로 설정되고 DIP 주소 및 마스크 필드에 목적지 IP 주소 및 마스크를 설정하도록 나타냅니다.
• **DIP Address**	목적지 IP 필터에 네트워크나 호스트를 선택할 때 지정 DIP 주소를 10 진수 표기법으로 입력합니다.
• **DIP Mask**	목적지 IP 필터에 네트워크를 선택한경우 10 진수표기법, 지정 DIP 마스크 입력이 가능합니다 .

■ **ICMP Parameters**

기능	설명

• **ICMP Type Filter**	ACE 에서 ICMP 필터를 설정합니다. **Any**: 특정 ICMP 필터를 사용하지 않습니다. **Specific**: 지정 ICMP 값을 사용하여 필드에 나타냅니다.
• **ICMP Type Value**	ICMP 필터에 "지정"을 선택하면 지정 ICMP 값을 입력 할수 있습니다.
• **ICMP Code Filter**	ACE 에서 ICMP 코드필터를 설정합니다. **Any**: 지정 ICMP 코드필터를 설정하지 않습니다. **Specific**: 지정 ICMP 코드필터를 설정하여 필드에 나타냅니다.
• **ICMP Code Value**	코드필터를 지정하여 선택하면 코드값을 입력 할 수 있습니다. 허용범위는 0~255 까지이며 ACE 프레임이 코드값과 일치해야합니다.

■ **TCP/UDP Parameters**

기능	설명
• **TCP/UDP Source Filter**	ACE 에 대하여 TCP /UDP 전송 필터를 지정합니다. **Any**: 특정한 TCP/UDP 전송 필터를 지정하지 않습니다 **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 관하여 TCP/UDP 특정 필터를 지정합니다.. . **Any**: TCP/UDP 목적지 필터가 설정되지 않았습니다. **Specific**: TCP/UDP 목적지로 필 특정필터로 설정합니다 **Range**: ACE 를 사용하여 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 "지정"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 TCP / UDP 특정 값을 입력 할 수 있습니다. 허용되는 범위는 0 ~ 65535 입니다.이 ACE 에 도달하는

	프레임이이 TCP / UDP 특정 값과 일치합니다.
• **TCP FIN**	ACE 에 대하여 TCP “발신자의 데이터가 없습니다”(FIN)를 설정합니다. **0**: FIN 필드와 설정된 TCP 프레임은 불일치합니다. **1**: FIN 필드와 설정된 TCP 프레임은 일치합니다.. **Any**: 모든 값이 허용됩니다.
• **TCP SYN**	ACE 의 TCP "Synchronize sequence numbers"(SYN) 값을 지정합니다. **0**: SYN 필드가 설정된 TCP 프레임은이 불일치합니다. **1**: SYN 필드가 설정된 TCP 프레임은이 일치합니다. **Any**: 모든 값이 허용됩니다.
• **TCP RST**	ACE 에 대한 TCP "Reset the connection" (RST) 값을 지정하십시오. **0**: RST 필드가 설정된 TCP 프레임은 불일치합니다. **1**: RST 필드가 설정된 TCP 프레임은 일치합니다. **Any**: 모든 값이 허용됩니다.
• **TCP PSH**	ACE 에 대한 TCP "Push Function"(PSH) 값을 지정합니다. **0**: PSH 필드가 설정된 TCP 프레임은 불일치합니다. **1**: PSH 필드가 설정된 TCP 프레임은 일치합니다. **Any**: 모든 값이 허용됩니다.
• **TCP ACK**	ACE 의 TCP "Acknowledgement field significant"(ACK) 값을 지정합니다 **0**: ACK 필드가 설정된 TCP 프레임은 불일치 합니다. **1**: ACK 필드가 설정된 TCP 프레임은 일치합니다. **Any**: 모든 값이 허용됩니다.
• **TCP URG**	ACE 에 대한 TCP "Urgent Pointer field significant"(URG) 값을 지정합니다 **0**: URG 필드가 설정된 TCP 프레임은 불일치합니다. **1**: URG 필드가 설정된 TCP 프레임은 일치합니다. **Any**: 모든 값이 허용됩니다.

■ Ethernet Type Parameters

이더넷 형태의 파라미터는 “이더넷 유형”으로 선택 될 경우 구성 될 수 있습니다.

기능	설명
• **EtherType Filter**	ACE 에 이더넷 유형 필터를 지정하십시오. **Any**: 이더넷 형식의 피럳가 지정되지 않습니다. **Specific**: ACE 로 특정 이더넷 필터 적용을 원하면 값을 입력 할 수 있습니다. 이더넷형식의 값을 입력하는 필드를 나타냅니다.
• **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. ACE 를 다루는 프레임이이 EtherType 값과 일치합니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

Cancel: 이전 페이지로 돌아갑니다

3.10.4 ACL Ports Configuration

각 스위치 포트의 ACL 파라메타(ACE)를 구성하십시오. 이 매개 변수는 프레임이 특징 ACE 와 일치하지 않으면 포트에서 수신된 프레임의 영향을 주는데 그림 4-10-4 의 ACL 설정화면이 나타납니다.

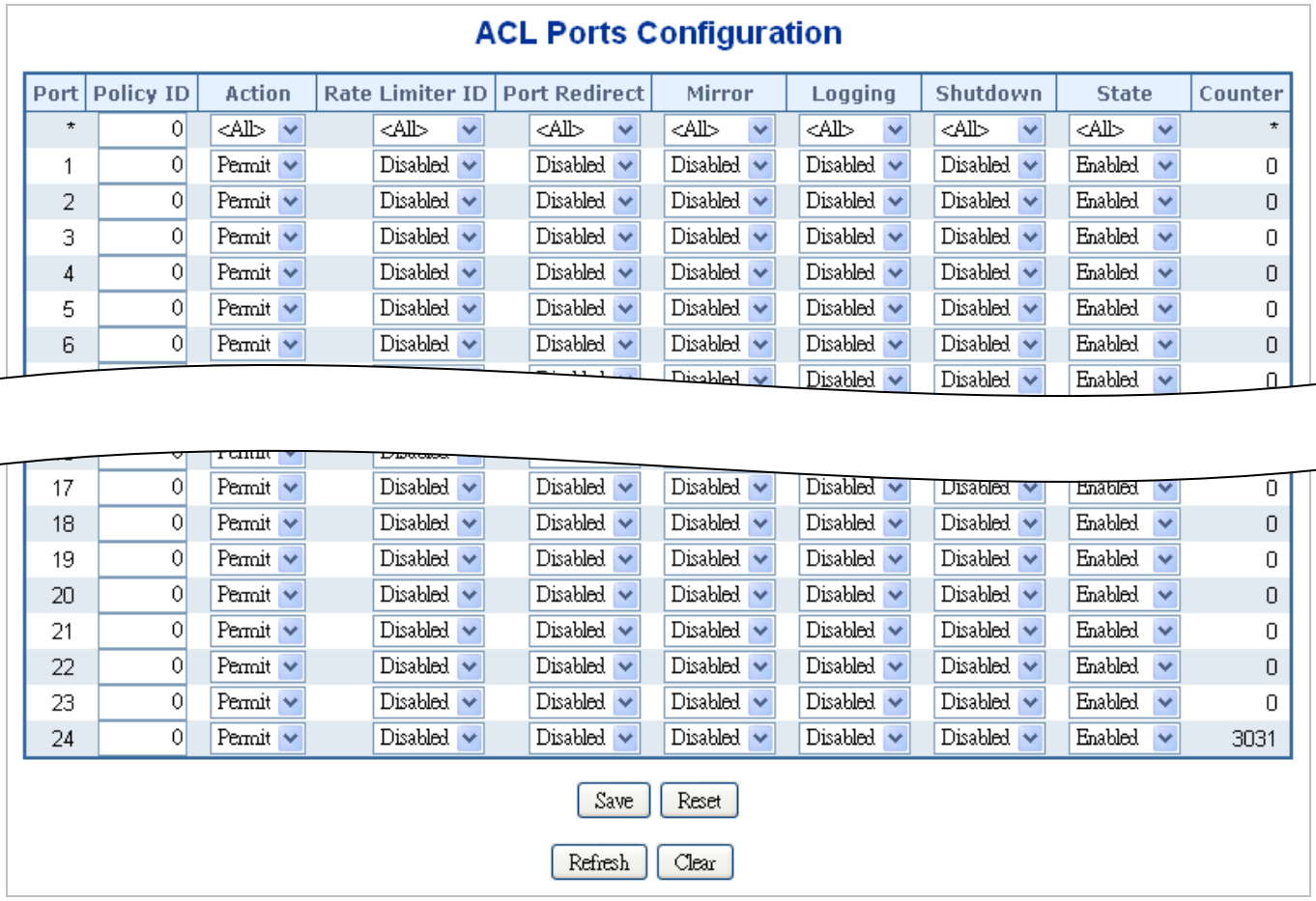


그림 4-10-4 ACL Ports 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Port**	각 행마다 포트 셋팅값을 설정 할 수 있습니다.
• **Policy ID**	포트에 적용할 정책을 선택하십시오 기본값은 0 이며 0 부터 255 까지

	허용됩니다.
• **Action**	전달내용의 허가 또는 거부를 선택하십시오. 기본설정은 허가입니다.
• **Rate Limiter ID**	이 포트에 적용 할 속도 제한 ID 를 선택하십시오 Disable 과 1-16 까지입니다. 기본값은 Disable 입니다.
• **Port Redirect**	변형할 포트 프레임을 선ㄴ택하세요 허용값은 Disable 과 특정 포트 번호이며 작업이 허용될 경우 설정할 수 없습니다. 기본값은 “사용 안함”입니다..
• **Mirror**	포트의 미러링 작동을 설정하십시오 허용값은 다음과 같습니다. **Enabled**: 포트에서 수신 된 프레임이 미러링됩니다. **Disabled**: 포트에서 수신 된 프레임이 미러링되지 않습니다. 기본값은 Disable 입니다.
• **Logging**	이 포트의 로그 작업을 지정하십시오. 허용값은 다음과 같습니다 . **Enabled**: 포트에서 수신 된 프레임이 시스템 로그에 저장됩니다. **Disabled**: 포트에서 수신 된 프레임이 시스템 로그에 저장되지 않습니다. 기본값은 Disable 입니다. 시스템 로그 메모리 크기와 로깅 속도는 제한되어 있습니다.
• **Shutdown**	특정포트를 셧다운 합니다. 설정값은 다음과 같습니다. **Enabled**:포트에서 프레임을 받는 포트가 셧다운이 되어집니다. . **Disabled**: 포트셧다운이 해제됩니다. 기본값은 Disable 입니다.
• **State**	포트의 특정 상태를 나타냅니다. 설정값은 다음과 같습니다. **Enabled**: ACL 사용자 모듈의 불완전 포트 구성을 변경하여 다시 엽니다. **Disabled**: ACL 사용자 모듈의 불완전포트 구성을 변경하여 포트를 닫습니다.기본값은 Enable 입니다
• **Counter**	ACE 와 일치하는 프레임수를 카운터를 표시합니다 .

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

Refresh: 새로고침을 실행합니다.

Clear: 카운터값을 클리어합니다.

3.10.5 ACL Rate Limiter Configuration

스위치의 ACL 기능에서 속도제한을 설정합니다.

그림 4-10-5 에 ACL 속도 제한 설정을 나타냅니다.

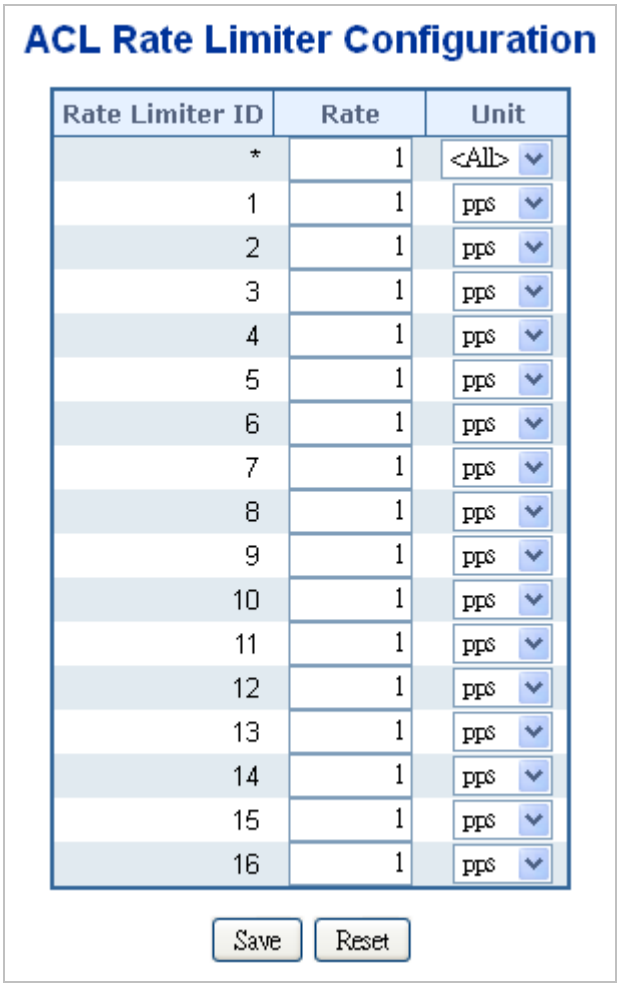


그림 4-10-5 ACL Rate Limiter 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Rate Limiter ID**	각 행의 포함된 설정을 속도 제한 ID 에 설정합니다.
• **Rate**	사용값은 다음과 같습니다: **0-3276700** (pps) 와 **0, 100, 200, 300, ..., 1000000** kbps.
• **Unit**	특정 속도 구성값은 다음과 같습니다. **pps**: packets per second. **kbps**: Kbits per second.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.11 Authentication

사용자의 접근과 관리 통제를 포함한 관리형 스위치의 접근을 제어합니다.

- **IEEE 802.1X Port-Based Network Access Control**
- **MAC-Based Authentication**
- **User Authentication**

802.1X (Port-Based) Authentication 의 예시

802.1X 환경에서 사용하는 요청자이고 스위치는 인증하고 RADIUS 서버는 인증서버입니다. 스위치는 중간단계의 역할을 하면서 요청 및 응답을 요청자와 인증서버간에 제어를 합니다. 전송되는 프레임은 EAPOL(EAP over LANs) 프레임으로 알려진 특수한 802.1X 프레임 입니다. 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 유용합니다. 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 스위치는 이를 사용하여 요청자와 연결된 스위치 포트에서 트래픽을 허용하거나 차단합니다.

MAC 주소 기반 인증의 예

802.1X 와는 달리 MAC 기반 인증은 표준이 아니며 업계에서 채택한 최고의 방법입니다. MAC 기반 인증에서 사용자는 클라이언트라고하며 스위치는 클라이언트를 대신하여 요청자 역할을합니다. 클라이언트가 보낸 초기 프레임 (모든 종류의 프레임)은 스위치에 의해 Snooping 되며, 스위치는 RADIUS 서버와의 후속 EAP 교환에서 클라이언트의 MAC 주소를 사용자 이름과 암호로 사용합니다. 6 바이트 MAC 주소는 "xx-xx-xx-xx-xx-xx"형식의 문자열로 변환됩니다. 즉, 대시표시 (-)가 하위 케이스의 16 진수 사이의 구분 기호로 사용됩니다. 스위치는 MD5-Challenge 인증 방법 만 지원하므로 RADIUS 서버를 적절히 구성해야합니다.

인증이 완료되면 RADIUS 서버는 MAC 테이블에 정적 항목을 사용하여 성공 또는 실패 표시를 보내 스위치가 특정 클라이언트에 대한 트래픽을 허용하거나 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 클라이언트가 동일한 포트 (예 : 타사 스위치 또는 허브를 통해)에 연결될 수 있고 개별 인증이 필요하며 클라이언트가 특정 인증 자 소프트웨어를 필요로하지 않는다는 것입니다. 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.

사용자 인증 예시

웹브라우저와 텔넷과 같은 원격 인증 방법이나 로컬로 접근하여 관리하는 시스템으로 사용자의 인증로그가 관리형스위치에 구성하는 것을 허용합니다. 관리형 스위치는 다음과 같은 옵션을 사용하여 안전한 네트워크 관리 액세스를 제공합니다.

- **원격 인증 다이얼 인 사용자 서비스 (RADIUS)**
- **터미널 액세스 컨트롤러 액세스 제어 시스템 플러스 (TACACS +)**
- **로컬 사용자 이름 및 권한 수준 제어**
- **주소**

RADIUS and TACACS+ 네트워크상의 RADIUS 인식 또는 TACACS 인식 장치에 대한 액세스를 제어하기 위해 중앙 서버에서 실행되는 소프트웨어를 사용하는 로그온 인증 프로토콜입니다. 인증 서버에는 관리 대상 스위치에 대한 관리 액세스가 필요한 각 사용자에 대한 관련 권한 수준이있는 여러 사용자 이름 / 암호 쌍방의 데이터베이스가 있습니다.

3.11.1 Understanding IEEE 802.1X Port-Based Authentication

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.

- 장치 역할
- 인증 시작 및 메시지 교환
- 허가 및 비허가 상태에 있는 포트

■ 장치 역할

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

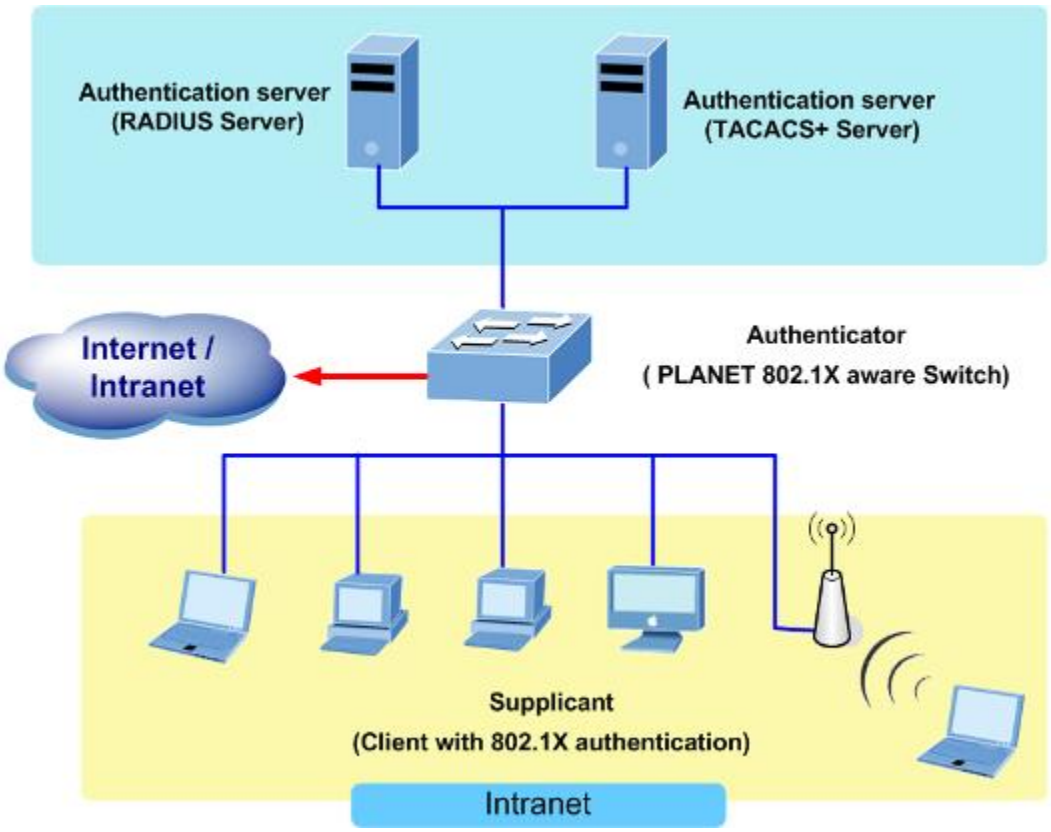


그림 4-11-1

- ***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 부팅하는 동안 클라이언트가 스위치에서 EAP 요청 / 아이디 프레임을받지 못하면 클라이언트는 EAPOL 시작 프레임을 보내 인증을 시작하여 클라이언트의 ID 를 요청하도록 스위치에 지시합니다.

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.

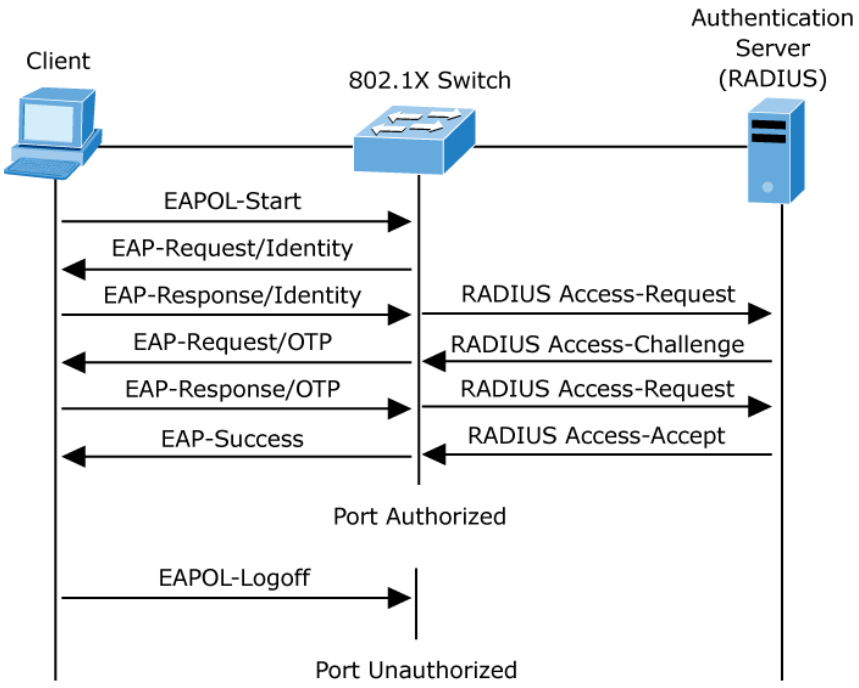


그림 4-11-2 EAP message exchange

■ **허가 또는 비허가 상태에 있는 포트**

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.

3.11.2 인증 설정

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

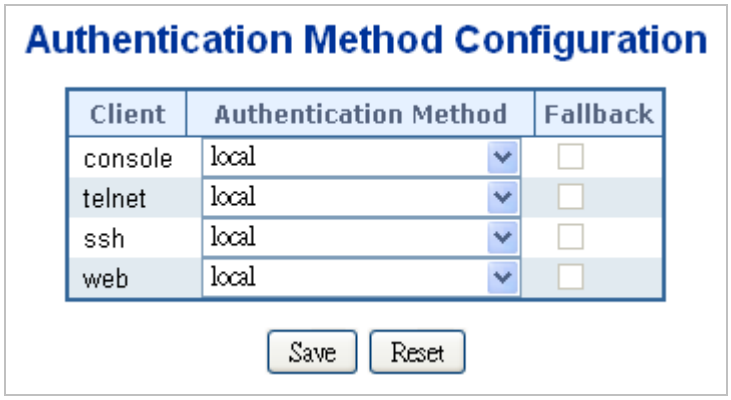


그림 4-11-3 Authentication Method 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Client**	아래 구성이 적용되는 관리 클라이언트.
• **Authentication Method**	인증 방법은 다음 값 중 하나로 설정할 수 있습니다. 없음 : 인증이 사용 불가능하며 로그인 할 수 없습니다. local : 인증을 위해 스위치 스택에서 로컬 사용자 데이터베이스를 사용합니다. radius : 인증을 위해 원격 RADIUS 서버를 사용합니다. tacacs + : 인증에 원격 TACACS + 서버를 사용합니다.
• **Fallback**	이 상자를 선택하여 로컬 인증으로 폴백을 활성화합니다. 구성된 인증 서버가 생존하지 않으면 로컬 사용자 데이터베이스가 인증에 사용됩니다. 이는 인증 메소드가 'none'또는 'local'이 아닌 다른 값으로 설정된 경우에만 가능합니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.11.3 네트워크 액세스 서버 구성

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. 이러한 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.

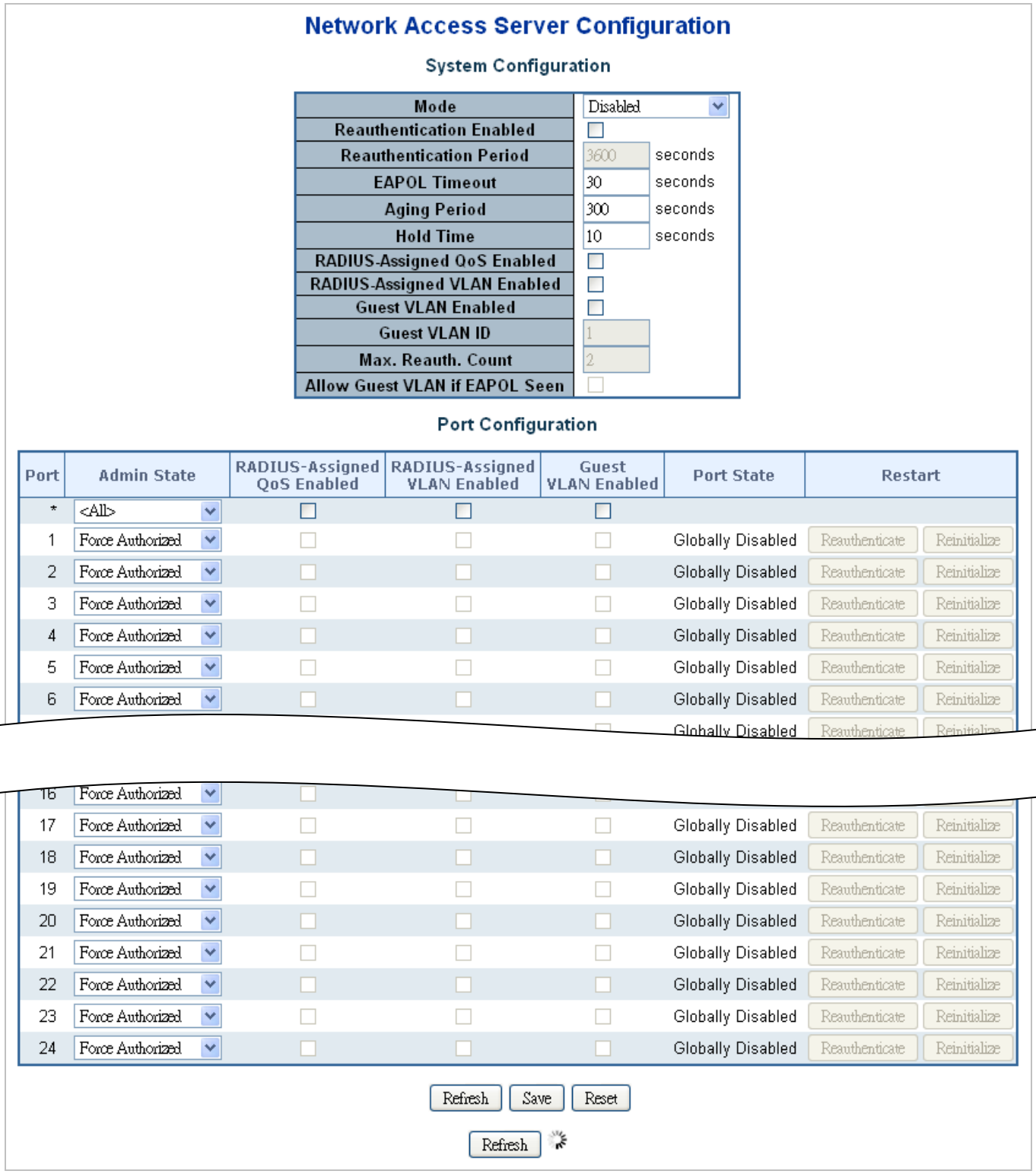


그림 4-11-4 Network Access Server 구성화면

다음과 같은 기능을 소개합니다.

시스템 설정

기능	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 지정된 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. MAC 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 포트에는 영향을 미치지 않습니다.
• **Aging Period**	이 설정은 포트 보안 기능을 사용하여 MAC 주소를 보호하는 방식과와 같은 다음 방식에 적용됩니다. 단일 802.1X 다중 802.1X MAC 기반 인증. NAS 모듈이 포트 보안 모듈을 사용하여 MAC 주소를 보호 할 때 포트 보안 모듈은 일정한 간격으로 문제의 MAC 주소에서 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 방식 인 경우 포트에 더 이상 연결되지 않은 요청자가 다음 재 인증시 제거되어 실패 할 것이므로 이는 그리 중요하지 않습니다. 그러나 재 인증을 사용할 수없는 경우 자원을 비울 수있는 유일한 방법은 항목을 에이징하는 것입니다. MAC 기반 인증의 포트 방식에서 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 방식과와 같은 다음 방식에 적용됩니다. 단일 802.1X 다중 802.1X MAC 기반 인증. RADIUS 서버가 클라이언트 액세스를 거부했거나 RADIUS 서버 요청이 ("구성 → 보안 → AAA"페이지에 지정된 시간 초과에 따라) 시간 초과되어 클라이언트가 액세스를 거부 할 경우 - 클라이언트는 승인되지 않은 상태. hold 타이머는 진행중인 인증 중에 계산되지 않습니다. MAC 기반 인증에서 방식에서 스위치는 hold 시간 동안 클라이언트에서 오는 새 프레임을 무시합니다. Hold Time 은 10 ~ 1000000 초 사이의 숫자로 설정할 수 있습니다.
• **RADIUS-Assigned QoS 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. "R ADIUS-Assigned QoS Enabled"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 VLAN 은 성공적으로 인증 된 요청자가 스위치에 배치 된 VLAN 을 중앙에서 제어 할 수있는 방법을 제공합니다. 들어오는 트래픽은 RADIUS 로 할당 된 VLAN 으로 분류되어 스위치됩니다. 이 기능을 사용하려면 RADIUS 서버가 특수 RADIUS 특성을 전송하도록 구성되어야합니다. "RADIUS 할당 VLAN 사용"확인란을 사용하면 RADIUS 서버에 할당 된 VLAN 기능을 전체적으로 활성화 / 비활성화 할 수 있습니다. 이 옵션을 선택하면 개별 포트의 Ditto 설정에 따라 해당 포트에 RADIUS 할당 VLAN 이

	활성화되었는지 여부가 결정됩니다. 이 옵션을 선택하지 않으면 RADIUS 서버 할당 VLAN 이 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 aging 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 aging 동안 포트에서 EAPOL 프레임을 수신하지 않은 경우에만 게스트 VLAN 으로 들어갑니다. 활성화 (선택)되어있는 경우 스위치는 포트의 aging 동안 포트에서 EAPOL 프레임을 수신하더라도 게스트 VLAN 입력을 고려합니다. Guest VLAN 옵션이 전역 적으로 활성화 된 경우에만 값을 변경할 수 있습니다.

포트 설정

테이블에는 스택의 선택된 스위치에있는 각 포트에 대해 하나의 행과 여러 열이 있습니다.

기능	설명
• **Port**	아래 구성이 적용되는 포트 번호입니다.
• **Admin State**	NAS 가 전역 적으로 활성화 된 경우이 선택은 포트의 인증 방식을를 제어합니다. 다음 방식을를 사용할 수 있습니다. 강제 승인 이 방식에서 스위치는 포트 링크가 올라 오면 하나의 EAPOL 성공 프레임을 보내고 포트의 클라이언트는 인증없이 네트워크 액세스를 허용합니다. 무단으로 강제 이 방식에서 스위치는 포트 링크가 올라 오면 하나의 EAPOL 실패 프레임을 보내고 포트의 클라이언트는 네트워크 액세스를 허용하지 않습니다. 포트 기반 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. 참고 : 두 개의 백엔드 서버가 활성화되어 있고 서버 시간 초과가 X 초 (AAA 구성 페이지 사용)로 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 방식 중에서 가장 안전합니다. 이 방식에서는 포트 보안 모듈을 사용하여 인증이 완료되면 요청자의 MAC 주소를 보호합니다. **Multi 802.1X** Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module. In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any

	supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality. **MAC-based Auth.** 포트 기반 802.1X 와 달리 MAC 기반 인증은 표준이 아니며 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 적절히 구성해야합니다. 인증이 완료되면 RADIUS 서버는 성공 또는 실패 표시를 보내고 포트 보안 모듈을 사용하여 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. 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 클라이언트에 특수 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 전역 적으로 활성화되고 활성화 (확인)되면 스위치는 요청자가 성공적으로 인증 될 때 RADIUS 서버가 전송 한 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 방식에서만 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; 7]의 원하는 QoS 클래스로 변환됩니다.
• **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 방식으로로 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 방식에서만 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. 다음 기준이 사용됩니다. - Tunnel-Medium-Type, Tunnel-Type 및 Tunnel-Private-Group-ID 속성은 모두 Access-Accept 패킷에 적어도 한 번 있어야합니다.

	- 스위치는 동일한 태그 값을 가지며 다음 요구 사항을 충족하는 첫 번째 속성 집합을 찾습니다 (Tag == 0 을 사용하면 Tunnel-Private-Group-ID 에 태그를 포함 할 필요가 없음). - Tunnel-Medium-Type 의 값은 "IEEE-802"(서수 6)로 설정되어야합니다. - Tunnel-Type 의 값은 "VLAN"(서수 13)으로 설정되어야합니다. - - Tunnel-Private-Group-ID 의 값은 '0'- '9'범위의 ASCII 문자로 된 문자열이어야하며 VLAN ID 를 나타내는 십진 문자열로 해석됩니다. 선행 0 은 무시됩니다. 최종 값은 [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 방식에서만 사용할 수 있습니다. 즉, **• Port-based 802.1X** **• Single 802.1X** **• Multi 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. **게스트 VLAN 작동 :** 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 아이디 프레임 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 방식에 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. 전체적으로 비활성화 됨 : NAS 가 전역 적으로 비활성화되었습니다. 링크 다운 : NAS 는 전체적으로 활성화되어 있지만 포트에는 링크가 없습니다. Authorized : 포트가 Force Authorized 또는 단일 요청자 방식이며 요청자가 인증됩니다. Unauthorized : 포트가 Force Unauthorized 또는 단일 요청자 방식이고 RADIUS 서버에 의해 인증자가 성공적으로 승인되지 않았습니다. X Auth / Y Unauth : 포트가 다중 요청자 방식입니다. 현재 X 클라이언트는 권한이 부여되며 Y 는 권한이 없습니다.
• **Restart**	각 행에 대해 두 개의 단추를 사용할 수 있습니다. 이 단추는 인증이 전역적으로 사용되고 포트의 Admin State 가 EAPOL 기반 또는 MAC 기반 방식인 경우에만 활성화됩니다. 이 버튼을 클릭해도 페이지에서 변경된 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 버튼은 포트에서 성공적으로 인증 된 클라이언트에 대해서만 영향을 미치며 클라이언트가 일시적으로 무단으로되지 않게합니다. 다시 초기화 : 포트에서 클라이언트의 재 초기화를 강제하므로 재 인증이 즉시 이루어집니다. 클라이언트는 재 인증이 진행되는 동안 허가되지 않은 상태로 전환합니다.

버튼 안내

Refresh: 새로고침을 합니다.

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.11.4 네트워크 액세스 개요

이 페이지는 선택된 스위치의 현재 NAS 포트 상태에 대한 개요를 제공합니다. 그림 4-11-5 의 Network Access Overview 화면이 나타납니다.

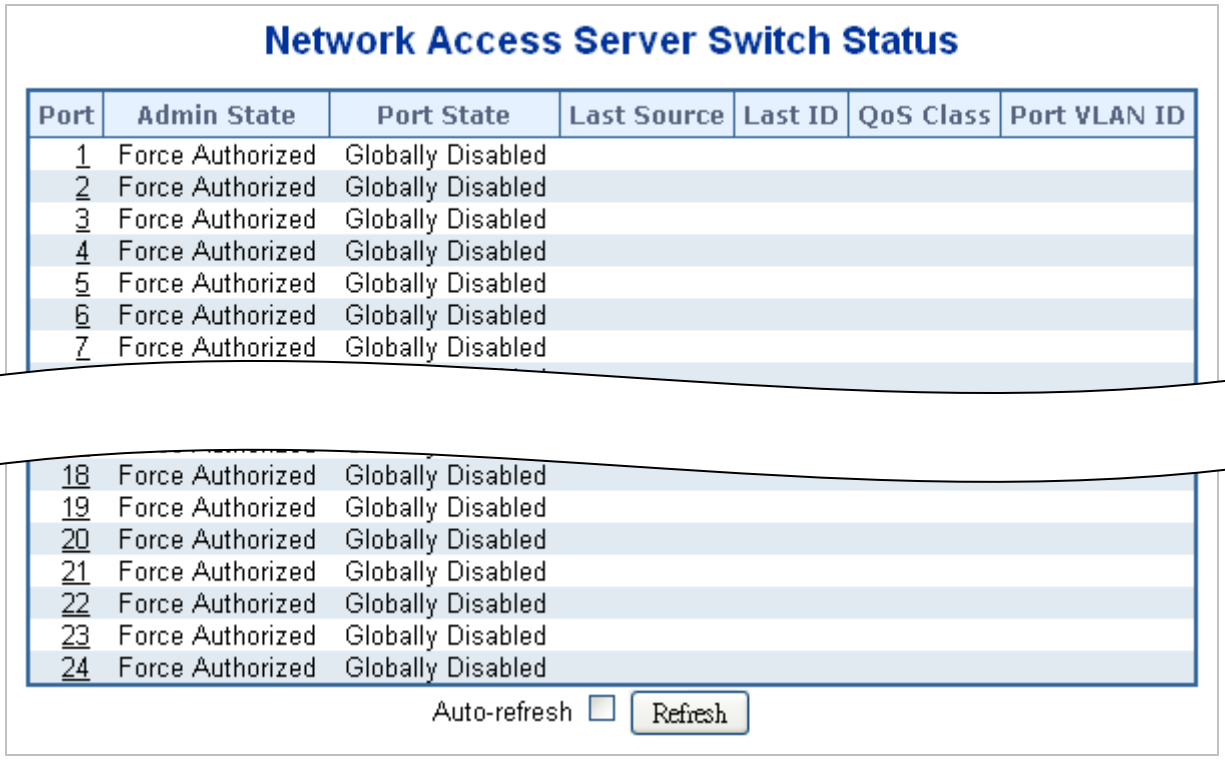


그림 4-11-5 Network Access Server Switch 상태 화면 페이지

다음과 같은 기능을 소개합니다.

기능	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 된 응답 ID 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 Class assigned to the port by the RADIUS server if enabled.
• **Port VLAN ID**	NAS가 포트를 넣은 VLAN ID입니다. 포트 VLAN ID가 NAS에 의해 무시되지 않으면이 필드는 비어 있습니다. VLAN ID가 RADIUS 서버에 의해 할당되면 "(RADIUS가 할당 됨)"이 VLAN ID에 추가됩니다. RADIUS 할당 VLAN에 대한 자세한 내용은 여기를 참조하십시오. 포트가 게스트 VLAN으로 이동되면 "(게스트)"가 VLAN ID에 추가됩니다. 여기에 게스트 VLAN에 대해 자세히 읽어보십시오.

버튼 안내

Refresh: 페이지를 새로고침니다.

Auto-refresh : 페이지를 자동으로 새로 고치려면이 상자를 선택하십시오. 3 초주기로 페이지를 자동으로 새로고침합니다. .

3.11.5 네트워크 액세스 통계

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.

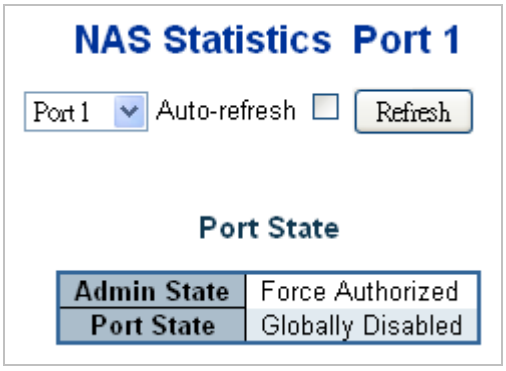


그림 4-11-6 Network Access Statistics 페이지 화면

다음과 같은 기능을 소개합니다.

포트 상태

기능	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**	NAS가 포트를 넣은 VLAN ID입니다. 포트 VLAN ID가 NAS에 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.

포트 카운터

기능	설명			
• **EAPOL Counters**	이러한 요청자 프레임 카운터는 다음 관리 상태에서 사용할 수 있습니다. 강제 승인 무단으로 강제 포트 기반 802.1X 단일 802.1X 다중 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 수입니다.
	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.

Direction	이름	IEEE 이름	설명
Rx	**Access Challenges**	dot1xAuthBackendAccessChallenges	**802.1X-based**: 스위치가 요청자의 첫 번째 응답 다음에 백엔드 서버로부터 첫 번째 요청을 수신 한 횟수를 계산합니다. 백엔드 서버가 스위치와

				통신하고 있음을 나타냅니다. **MAC-based**: 이 포트 (맨 왼쪽 테이블) 또는 클라이언트 (맨 오른쪽 테이블)에 대해 백엔드 서버에서받은 모든 액세스 챌린지를 계산합니다.
	Rx	**Other Requests**	dot1xAuthBackendOtherRequestsToSupplicant	**802.1X-based**: 스위치가 첫 번째 요청자 다음에 요청자에게 EAP 요청 패킷을 보내는 횟수를 계산합니다. 백엔드 서버가 EAP 방법을 선택했음을 나타냅니다. **MAC-based**: 해당 사항 없음.
	Rx	**Auth. Successes**	dot1xAuthBackendAuthSuccesses	**802.1X- and MAC-based**: 스위치가 성공 표시를 수신한 횟수를 계산합니다. 요청자 / 클라이언트가 백엔드 서버에 성공적으로 인증되었음을 나타냅니다.
	Rx	**Auth. Failures**	dot1xAuthBackendAuthFails	**802.1X- and MAC-based**: 스위치가 오류 메시지를 수신한 횟수를 계산합니다. 이는 요청자 / 클라이언트가 백엔드 서버에 대해 인증하지 않았 음을 나타냅니다.
	Tx	**Responses**	dot1xAuthBackendResponses	**802.1X-based:** 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	마지막 요청자 / 클라이언트의 MAC 주소입니다.
VLAN ID	-	마지막 요청자 / 클라이언트의 마지막 프레임이 수신 된 VLAN ID 입니다.
Version	dot1xAuthLastEapolFrameVersion	**802.1X-based**: 가장 최근에 수신 한 EAPOL 프레임에서 수행 된 프로토콜 버전 번호입니다. **MAC-based**: 해당 사항 없음.
Identity	-	**802.1X-based**: 가장 최근에받은 Response Identity EAPOL 프레임에서 전달 된 사용자 이름 (요청자 신원). **MAC-based**: 해당 사항 없음.

선택된 카운터

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

첨부 된 MAC 주소

기능	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 hold 시간 (초) 동안 인증되지 않은 상태를 유지합니다.
• **Last Authentication**	클라이언트의 마지막 인증 날짜 및 시간을 표시합니다 (성공적 일뿐만 아니라 성공하지 못했습니다).

버튼 안내

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

Refresh : 페이지를 새로고침니다.

Clear : 이 버튼은 다음 방식에서 사용할 수 있습니다.

• Force Authorized

• Force Unauthorized

• Port-based 802.1X

• Single 802.1X

선택한 포트에 대한 카운터를 지우려면 클릭하십시오.

Clear All: 이 버튼은 다음 방식에서 사용할 수 있습니다.:

• Multi 802.1X

• MAC-based Auth.X

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

Clear This: 이 버튼은 다음 방식에서 사용할 수 있습니다.:

• Multi 802.1X

• MAC-based Auth.X

현재 선택된 클라이언트의 카운터 만 지우려면 클릭하십시오.

3.11.6 인증 서버 구성

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

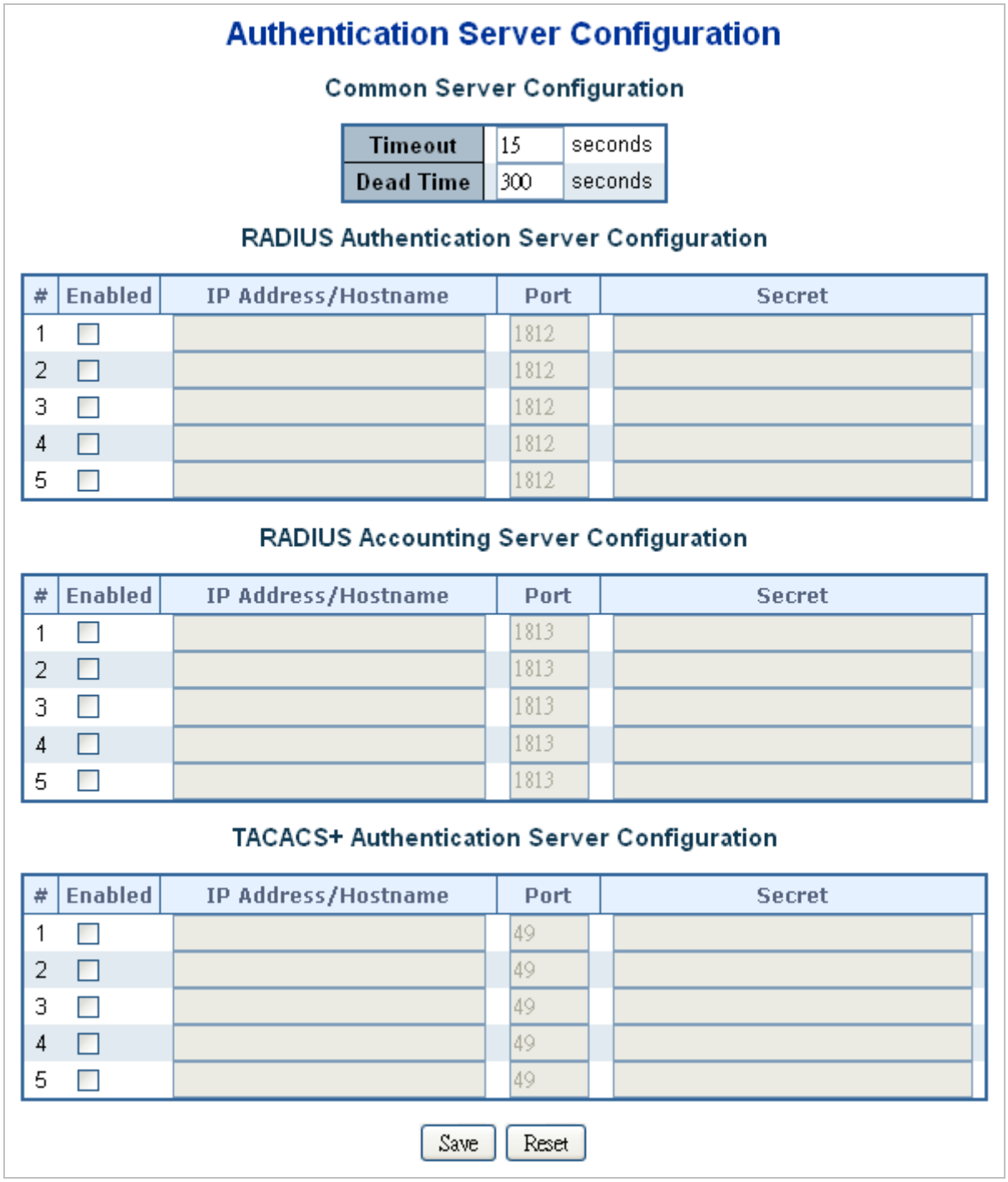


그림 4-11-7 Authentication Server 구성화면

다음과 같은 기능을 소개합니다.

포트 상태

이 설정은 모든 인증 서버에 공통입니다.

기능	설명

• **Timeout**	Timeout (3 - 3600 초 사이의 숫자로 설정할 수 있음)은 서버로부터의 응답을 기다리는 최대 시간입니다. 서버가이 시간 내에 응답하지 않으면 서버가 작동하지 않는 것으로 간주하여 사용 가능한 다음 서버 (있는 경우)로 계속 진행합니다. RADIUS 서버는 디자인 상 신뢰할 수없는 UDP 프로토콜을 사용하고 있습니다. 손실 된 프레임에 대처하기 위해 타임 아웃 간격은 동일한 길이의 3 개의 하위 간격으로 나누어집니다. 서브 구간 내에 응답이 수신되지 않으면 요청이 다시 전송됩니다. 이 알고리즘을 사용하면 RADIUS 서버가 죽은 것으로 간주되기 전에 최대 3 번 쿼리됩니다.
• **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.

RADIUS 인증 서버 구성

이 테이블에는 각 RADIUS 인증 서버 및 다음과 같은 여러 열에 대해 하나의 행이 있습니다.

기능	설명
• **#**	아래 구성이 적용되는 RADIUS 인증 서버 번호입니다.
• **Enabled**	이 상자를 선택하여 RADIUS 인증 서버를 활성화하십시오.
• **IP Address/Hostname**	RADIUS 인증 서버의 IP 주소 또는 호스트 이름. IP 주소는 점으로 구분 된 십진수 표기법으로 표시됩니다.
• **Port**	RADIUS 인증 서버에서 사용할 UDP 포트입니다. 포트가 0 (영)으로 설정된 경우 RADIUS 인증 서버에서 기본 포트 (1812)가 사용됩니다.
• **Secret**	비밀 번호는 최대 29 자이며 RADIUS 인증 서버와 스위치간에 공유됩니다.

RADIUS 계정 서버 구성

이 테이블에는 각 RADIUS 계정 서버에 대한 행과 여러 열이 있습니다.

기능	설명
• #	아래 구성이 적용되는 RADIUS 계정 서버 번호입니다.
• Enabled	이 상자를 선택하여 RADIUS 계정 서버를 활성화하십시오.
• IP Address/Hostname	RADIUS 계정 서버의 IP 주소 또는 호스트 이름입니다. IP 주소는 점으로 구분 된 십진수 표기법으로 표시됩니다.
• Port	RADIUS 계정 서버에서 사용할 UDP 포트입니다. 포트가 0 (영)으로 설정된 경우 RADIUS 계정 서버에서 기본 포트 (1813)가 사용됩니다.
• Secret	RADIUS 계정 서버와 스위치간에 공유되는 비밀 - 최대 29 자.

TACACS + 인증 서버 구성

이 테이블에는 각 TACACS + 인증 서버 및 다음과 같은 여러 열에 대해 하나의 행이 있습니다.

기능	설명
• #	아래 구성이 적용되는 TACACS + 인증 서버 번호입니다.
• Enabled	이 상자를 선택하여 TACACS + 인증 서버를 활성화하십시오.
• IP Address/Hostname	TACACS + 인증 서버의 IP 주소 또는 호스트 이름. IP 주소는 점으로 구분 된 십진수 표기법으로 표시됩니다.
• Port	TACACS + 인증 서버에서 사용할 TCP 포트입니다. 포트가 0 (영)으로 설정된 경우 기본 포트 (49)가 TACACS + 인증 서버에서 사용됩니다.
• Secret	비밀 번호는 최대 29 자이며 TACACS + 인증 서버와 스위치간에 공유됩니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.11.7 RADIUS 개요

이 페이지에서는 인증 구성 페이지에서 구성 가능한 RADIUS 서버의 상태에 대한 개요를 제공합니다. 그림 4-11-8 의 RADIUS 인증 / 계정 서버 개요 화면이 나타납니다.

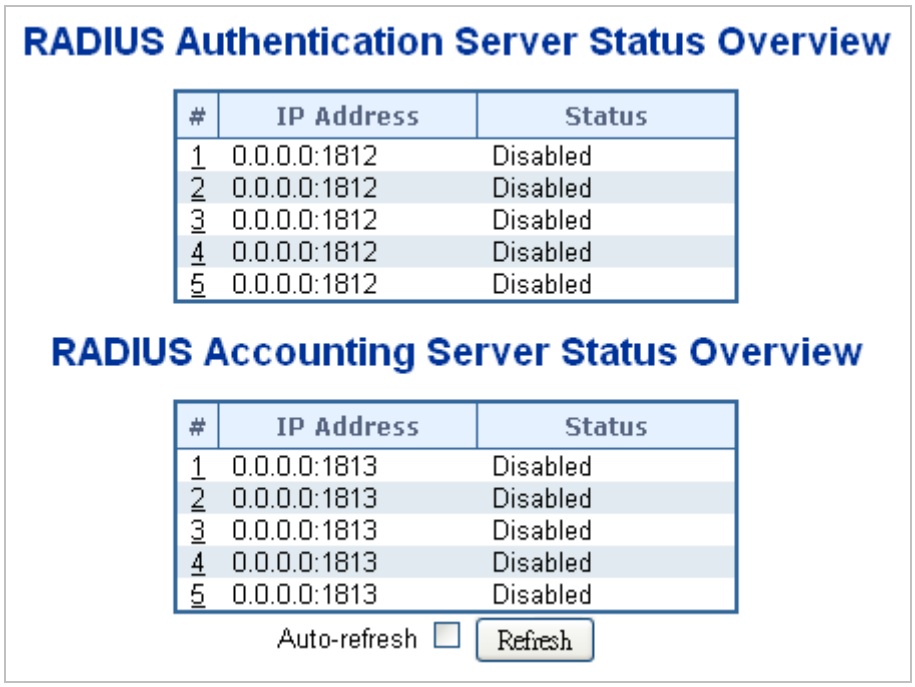


그림 4-11-8 RADIUS Authentication/Accounting Server Overview 페이지 화면

다음과 같은 기능을 소개합니다.

RADIUS 인증 서버

기능	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)
• **State**	서버의 현재 상태. 이 필드에는 다음 값 중 하나가 사용됩니다. ■ **Disabled**: 서버가 사용 불가능합니다. ■ **Not Ready**: 서버가 사용 가능하지만 IP 통신이 아직 실행되지 않고 실행 중입니다. ■ **Ready**: 서버가 활성화되고 IP 통신이 실행되고 RADIUS 모듈이 액세스 시도를 수락 할 준비가되었습니다. ■ **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 계정 서버

기능	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)
• **State**	서버의 현재 상태. 이 필드에는 다음 값 중 하나가 사용됩니다. ■ **Disabled**: 서버가 사용 불가능합니다. ■ **Not Ready**: 서버가 사용 가능하지만 IP 통신이 아직 실행 및 실행되지 않습니다. ■ **Ready**: 서버가 활성화되고 IP 통신이 실행되고 RADIUS 모듈이 계정 시도를 받아 들일 준비가되었습니다. Dead (X 초 남음) :이 서버에 대한 계정을 시도했지만 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.

버튼 안내

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

Refresh: 페이지를 새로고침니다.

3.11.8 RADIUS 세부 정보

이 페이지는 특정 RADIUS 서버에 대한 자세한 통계를 제공합니다. 그림 4-11-9 의 서버 개요 RADIUS 인증 / 계정 화면이 나타납니다.

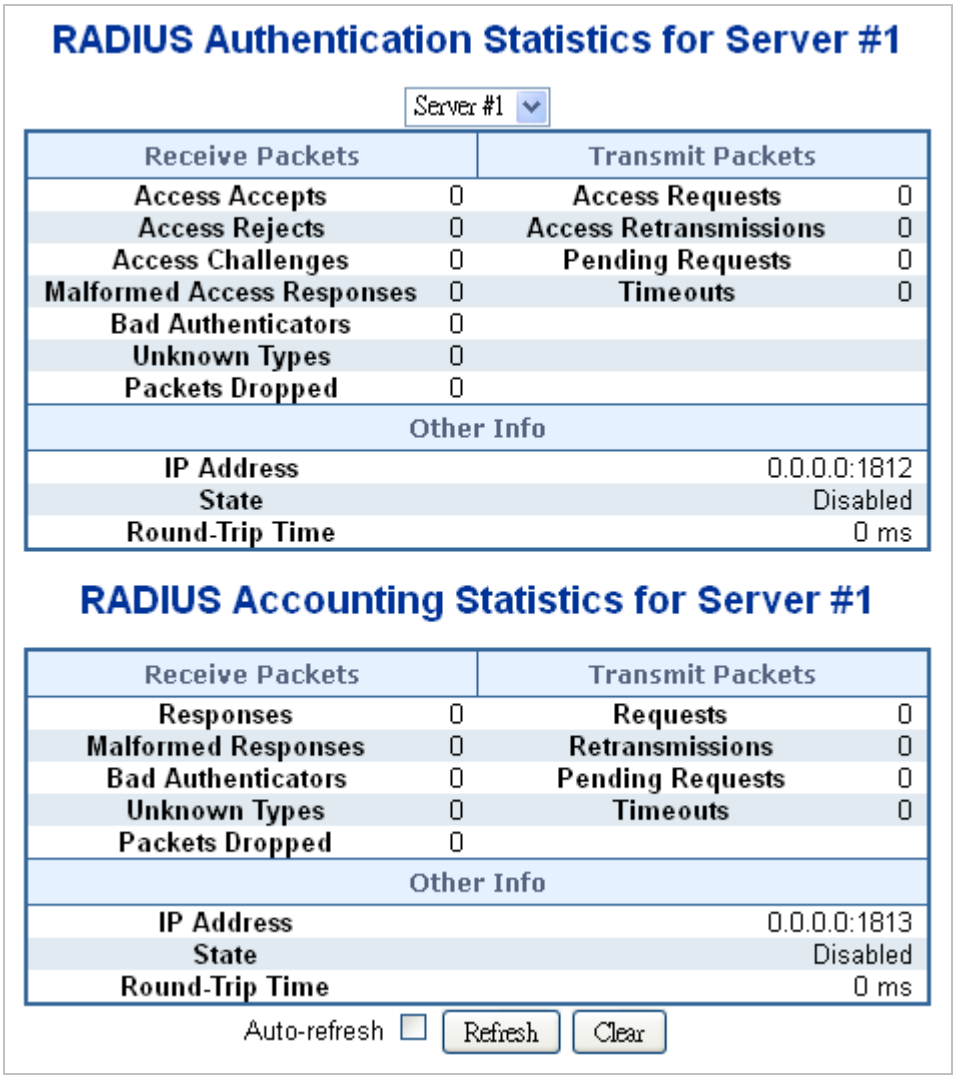


그림 4-11-9 RADIUS Authentication/Accounting for Server Overview 페이지 화면

다음과 같은 기능을 소개합니다.

RADIUS 인증 서버

통계는 RFC4668 - RADIUS 인증 클라이언트 MIB 에 지정된 것과 밀접하게 매핑됩니다.

세부 사항을 표시 할 백엔드 서버 사이를 전환하려면 서버 선택 상자를 사용하십시오.

기능	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**	radiusAuthClientExtAccessAccepts	서버로부터 수신 한 RADIUS 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 수신되어 다른 이유로 인해 삭제 된 RADIUS 패킷 수입니다.
	Rx	**Packets Dropped**	radiusAuthClientExtPacketsDropped	인증 포트에서 서버로부터 수신되어 다른 이유로 인해 삭제 된 RADIUS 패킷 수입니다.
	Tx	**Access Requests**	radiusAuthClientExtAccessRequests	서버에 보낸 RADIUS 액세스 요청 패킷 수입니다. 여기에는 재전송이 포함되지 않습니다.
	Tx	**Access**	radiusAuthClientExtA	RADIUS 인증 서버에 재전송

		Retransmissions	ccessRetransmissions	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.

이름	RFC4668 이름	설명
IP Address	-	해당 인증 서버의 IP 주소 및 UDP 포트
State	-	서버의 상태를 표시합니다. 다음 값 중 하나를 취합니다. **Disabled**: 선택한 서버가 비활성화됩니다. **Not Ready**: 서버가 활성화되어 있지만 IP 통신이 아직 시작 및 실행되지 않습니다. **Ready**: 서버가 활성화되고 IP 통신이 실행되고 RADIUS 모듈이 액세스 시도를 수락 할 준비가되었습니다. **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.
	Round-Trip Time	radiusAuthClientExtRoundTripTime	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 계정 서버

통계는 RFC4670 - RADIUS Accounting Client MIB 에 지정된 것과 밀접하게 매핑됩니다.

세부 사항을 표시 할 백엔드 서버 사이를 전환하려면 서버 선택 상자를 사용하십시오.

기능	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 계정 서버의 IP 주소 및 UDP 포트

	State	-	서버의 상태를 표시합니다. 다음 값 중 하나를 취합니다. **Disabled**: 선택한 서버가 비활성화됩니다. **Not Ready**: 서버가 활성화되어 있지만 IP 통신이 아직 시작 및 실행되지 않습니다. **Ready**: 서버가 활성화되고 IP 통신이 실행되고 RADIUS 모듈이 계정 시도를 받아들일 준비가되었습니다. **Dead (X seconds left)**: 이 서버에 대한 계정을 시도했지만 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 안내

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

Refresh: 페이지를 새로고칩니다.

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

3.11.9 Windows 플랫폼 RADIUS 서버 구성

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

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

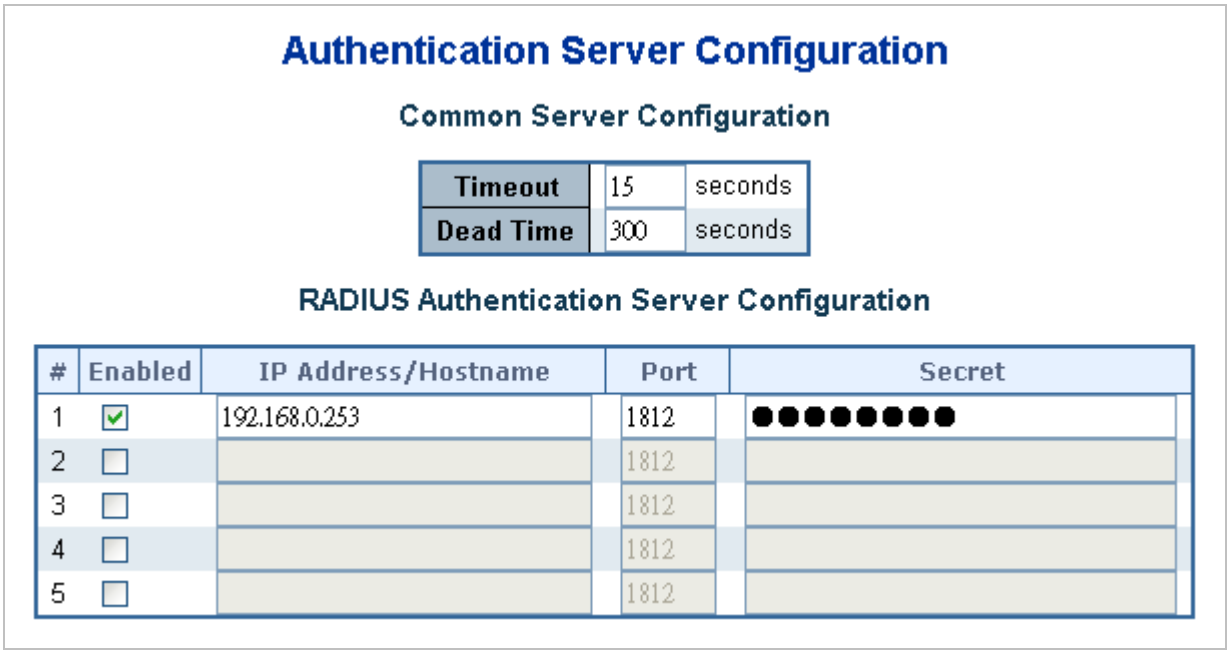


그림 4-11-10 RADIUS 서버 설정 화면

2. Windows 2003 서버에 새 RADIUS 클라이언트 추가

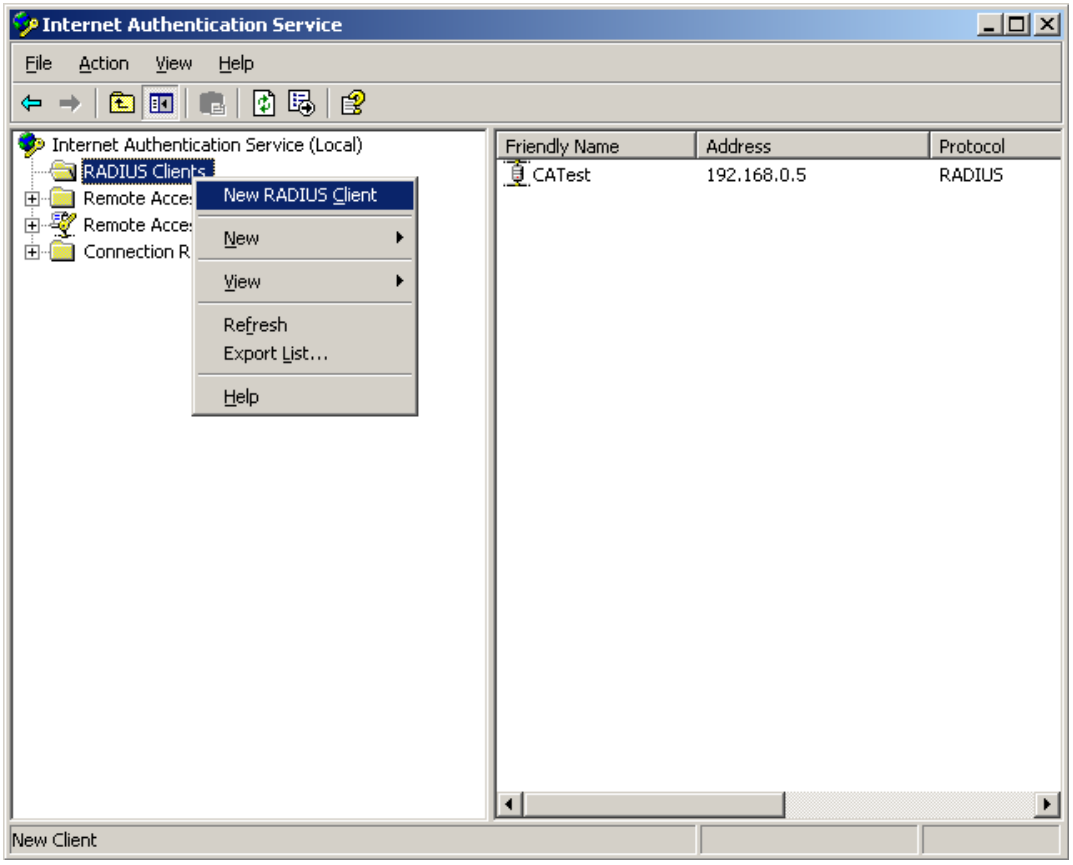


그림 4-11-11 Windows Server – add new RADIUS client setting

3. 클라이언트 IP 주소를 Managed 스위치에 할당합니다.

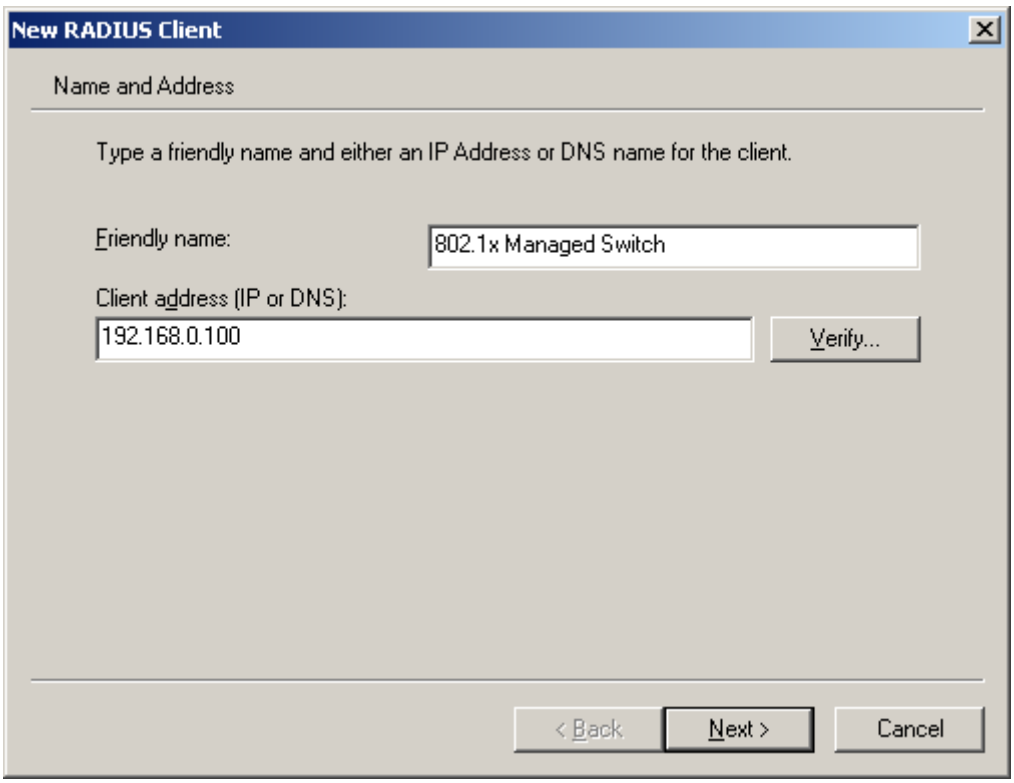


그림 4-11-12 Windows Server RADIUS 서버 설정

4. 공유 비밀 키는 Managed Switch 에 구성된 키와 같아야합니다.

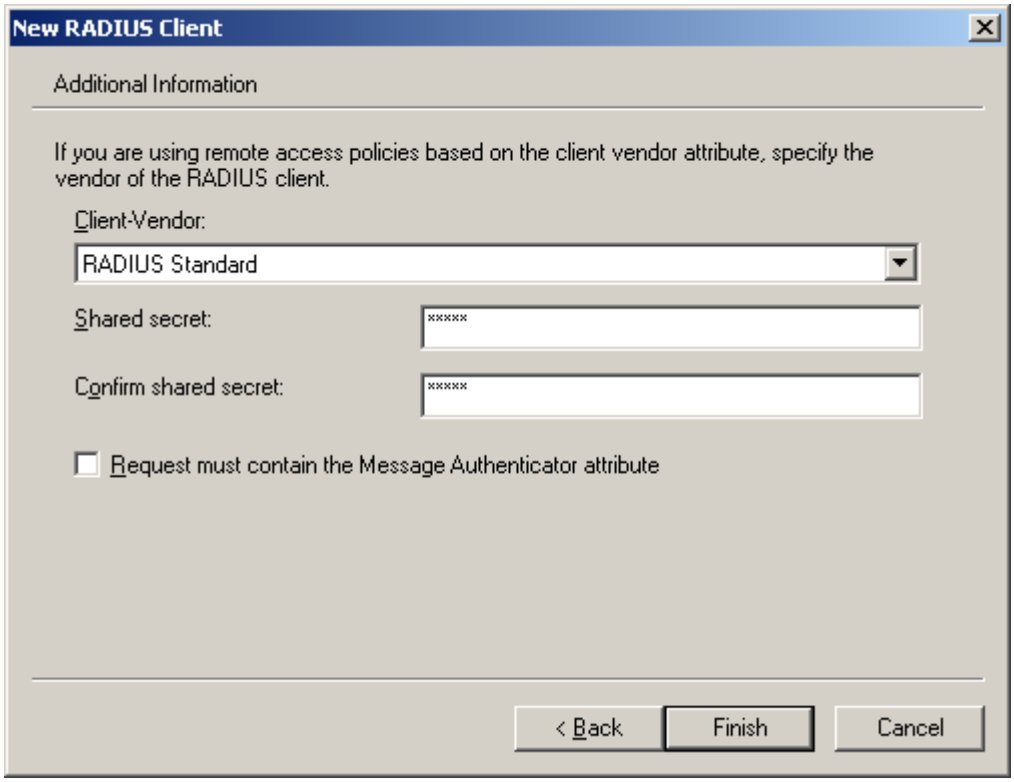


그림 4-11-13 Windows Server RADIUS 서버 설정

5. "802.1X 포트 구성"과 동일한 802.1X 의 포트 속성을 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 4-11-14 802.1x 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.

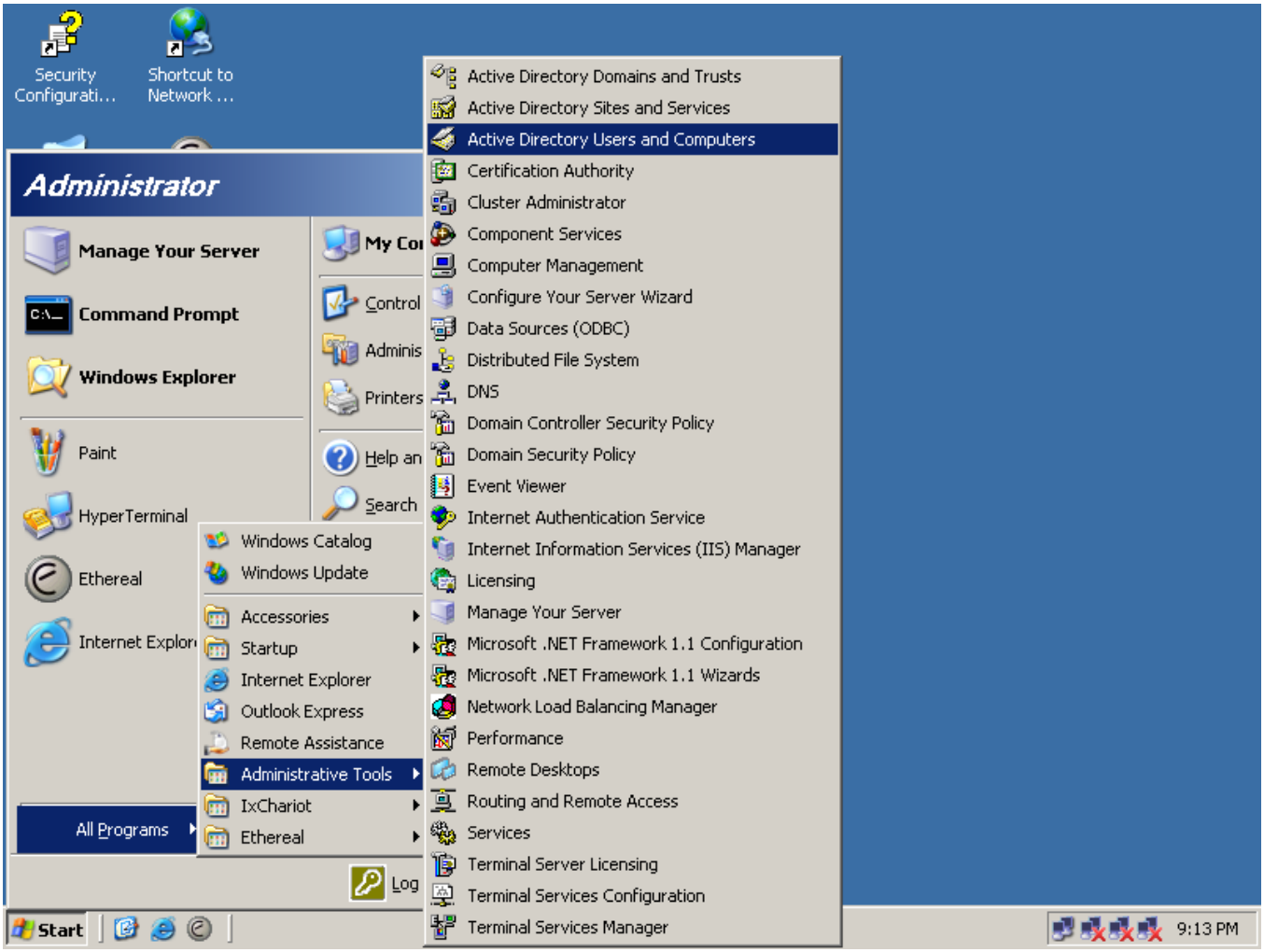


그림 4-11-15 Windows 2003 AD 서버 설정 경로

7. "Active Directory 사용자 및 컴퓨터"를 입력하고 합법적 인 사용자 데이터를 작성한 다음 다음 사용자로 등록한 사용자를 마우스 오른쪽 단추로 클릭하여 등록 정보를 입력하고 알아 두어야 할 사항을 입력하십시오.

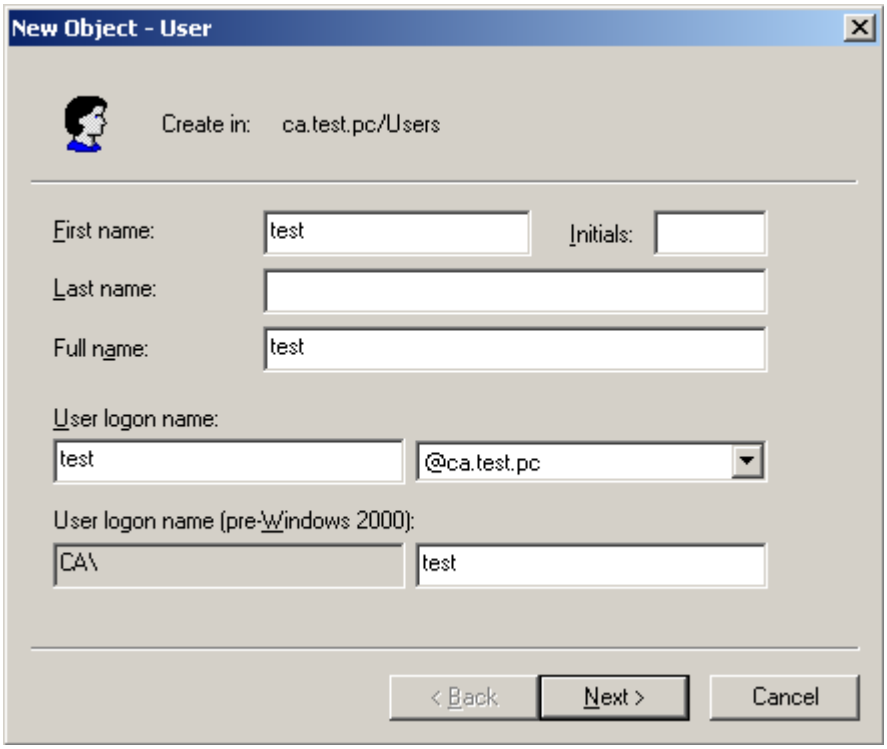


그림 4-11-16 사용자 속성 추가 화면

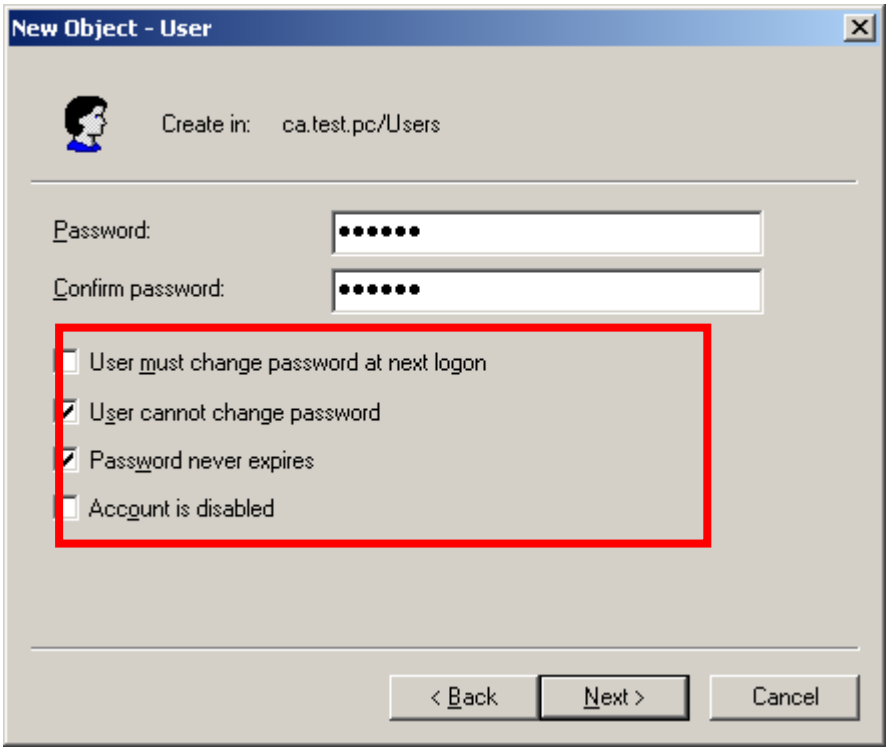


그림 4-11-17 사용자 속성 추가 화면

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 통계가 작동하면 스위치가 RADIUS 서버에 액세스하지 못할 수 있습니다.

3.11.10 802.1X 클라이언트 구성

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.

■ 샘플 구성 : EAP-MD5 인증

1. 시작> 제어판으로 이동하여 "네트워크 연결"을 두 번 클릭하십시오.
2. 로컬 네트워크 연결을 마우스 오른쪽 단추로 누릅니다.
3. "속성"을 클릭하여 속성 설정 창을 엽니 다.

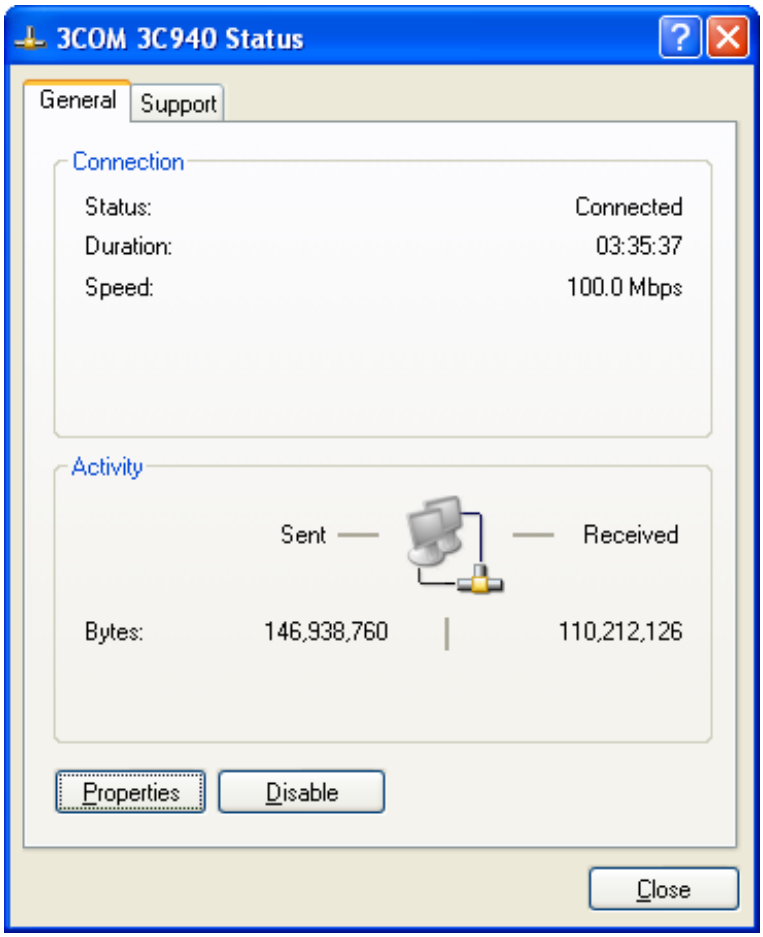


그림 4-11-18

4. "인증"탭을 선택하십시오.
5. "IEEE 802.1X를 사용하여 네트워크 액세스 제어 활성화"를 선택하여 802.1x 인증을 활성화합니다.
6. EAP 유형의 드롭 다운 목록 상자에서 "MD-5 Challenge"를 선택하십시오.

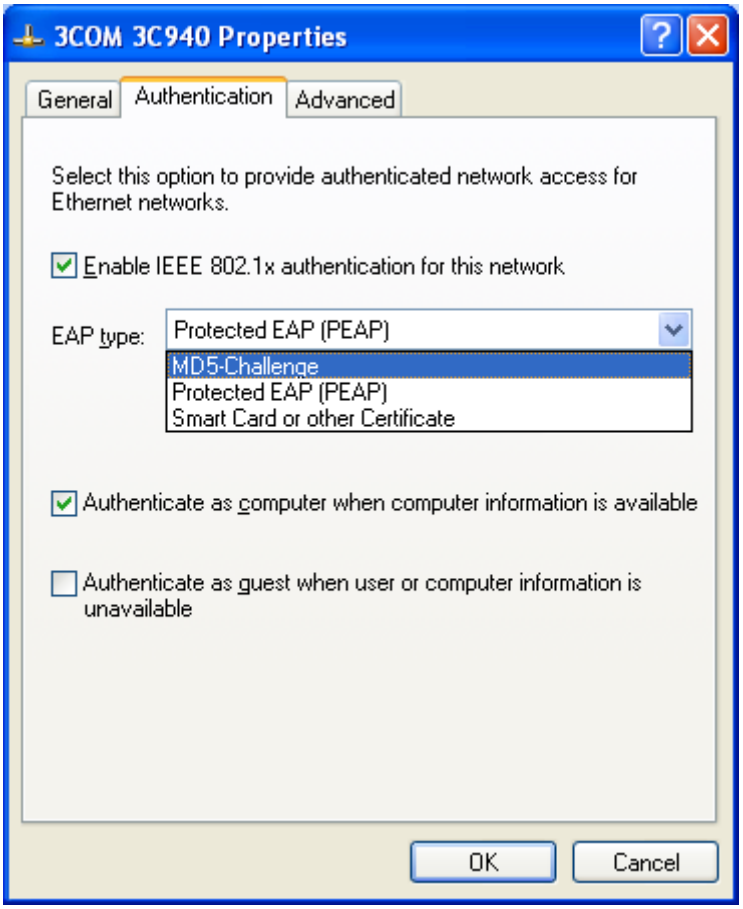


그림 4-11-19

7. "확인"을 클릭하십시오.
8. 클라이언트가 Managed Switch와 연결되면 사용자 인증 고지가 시스템 트레이에 나타납니다. 계속하려면 알림을 클릭하십시오.

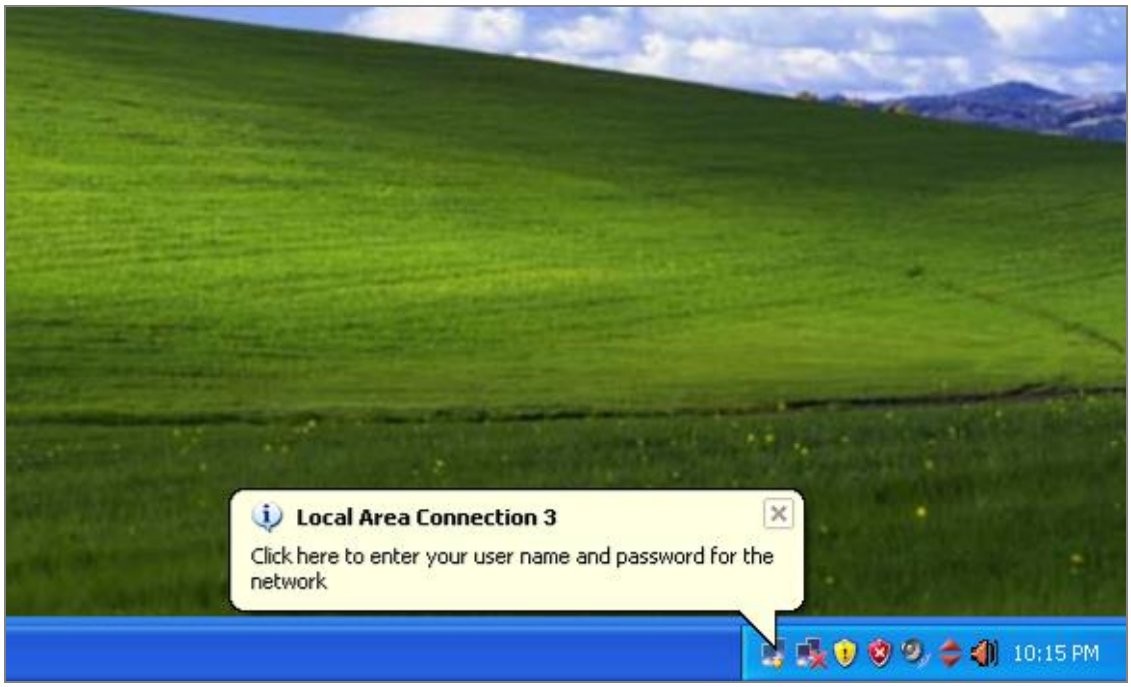


그림 4-11-20 Windows 클라이언트 팝업 로그인 요청 메시지

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

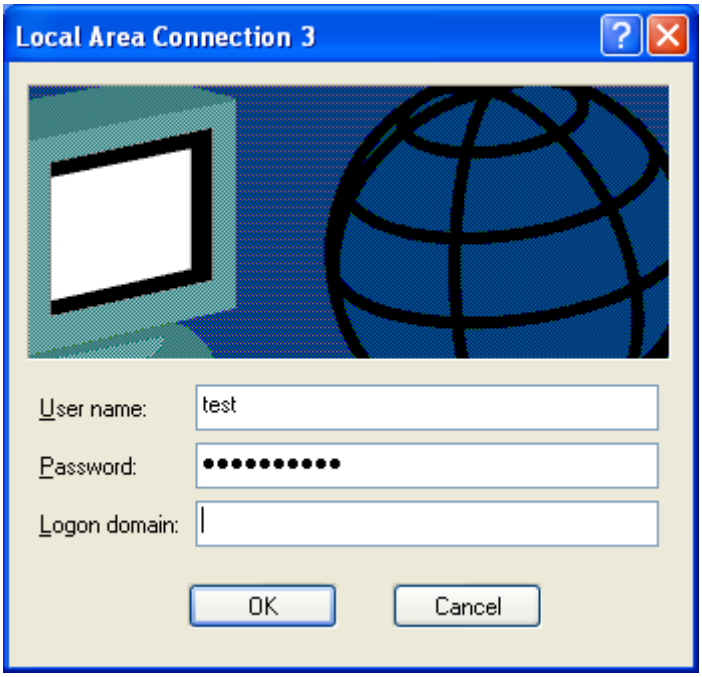


그림 4-11-21

3.12 Security

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

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

3.12.1 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.

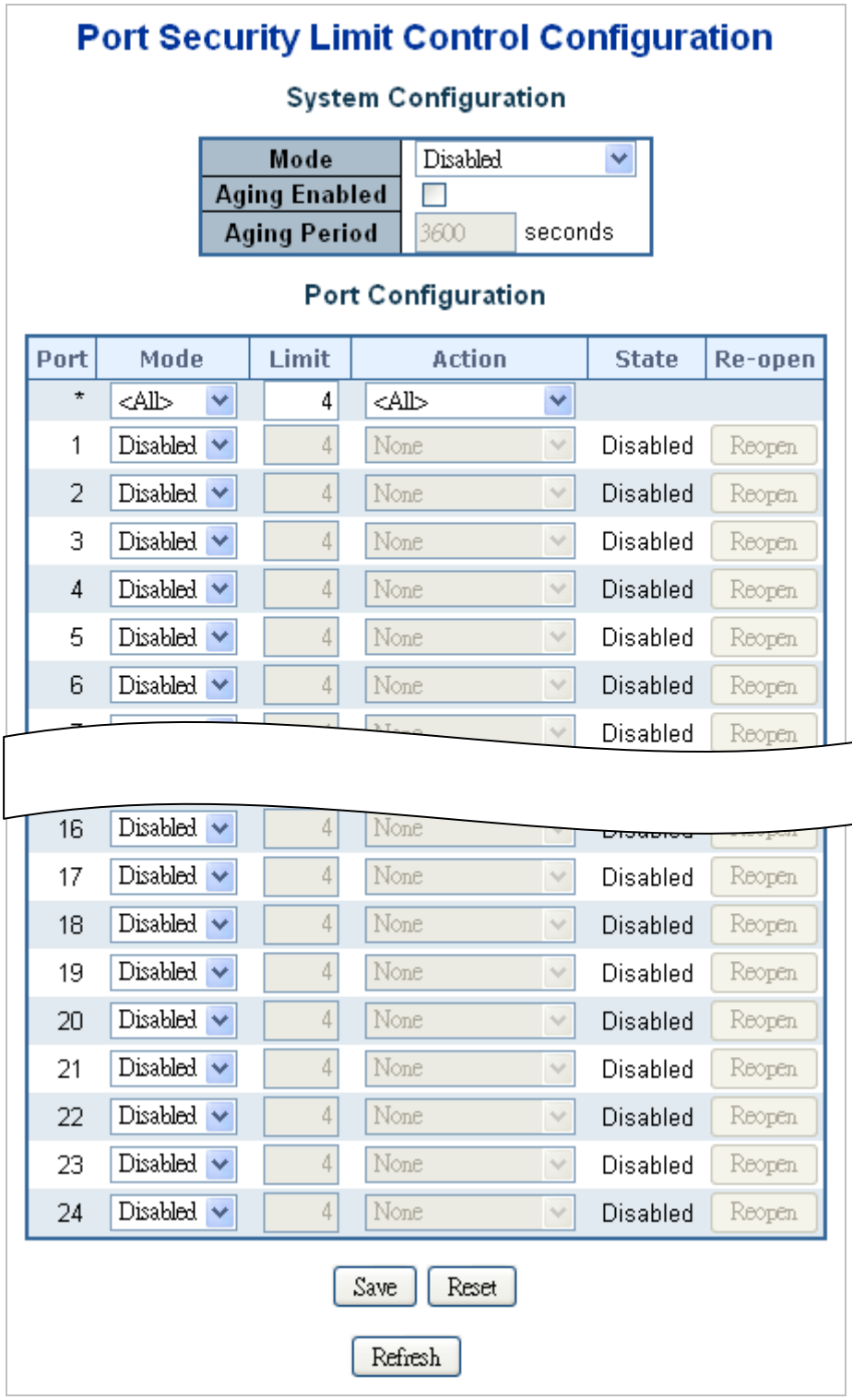


그림 4-12-1 포트 제한 제어 구성 개요 페이지 화면

다음과 같은 기능을 소개합니다.

시스템 설정

기능	설명

• **Mode**	제한 제어가 스위치 스택에서 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**	이 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 시작합니다. 이러한 프레임이 다음 에이징 기간 내에 표시되지 않으면 최종 호스트는 연결이 해제 된 것으로 간주되고 해당 리소스는 스위치에서 해제됩니다.

포트 구성

테이블에는 스택의 선택된 스위치에있는 각 포트에 대해 하나의 행과 여러 열이 있습니다.

기능	설명
• **Port**	아래 구성이 적용되는 포트 번호입니다.
• **Mode**	제한 제어가이 포트에서 활성화되었는지 여부를 제어합니다. Limit Control 을 적용하려면이 방식과와 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.

	스택 스위치는 포트 보안이 활성화 된 포트에 새 MAC 주소가 표시 될 때마다 모든 포트가 그려지는 총 MAC 주소 수와 함께 "출생"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 제한하는 것 이상을 허용하지 않지만 더 이상 조치하지 않습니다. **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 연결되더라도 (케이블을 분리하여) 포트는 계속 종료됩니다. 포트를 다시 열려면 세 가지 방법이 있습니다. 1) 스택을 부팅하거나 새 masterthe 스위치를 선택하십시오. 2) 포트 또는 스택 스위치의 제한 제어를 비활성화 한 다음 다시 활성화합니다. 3) Reopen 버튼을 클릭하십시오. **Trap & Shutdown**: 포트에 Limit + 1 MAC 주소가 표시되면 위에서 설명한 "트랩"및 "셧다운"동작이 수행됩니다.
• **State**	이 열은 제한 컨트롤의 관점에서 본 포트의 현재 상태를 보여줍니다. 상태는 다음 네 가지 값 중 하나를 취합니다. **Disabled**: 제한 제어가 포트에서 전체적으로 비활성화되거나 비활성화됩니다. **Ready**: 한도에 아직 도달하지 못했습니다. 이것은 모든 작업에 대해 표시 될 수 있습니다. **Limit Reached**: 이 포트에서 한계에 도달했음을 나타냅니다. 이 상태는 동작이 없음 또는 트랩으로 설정된 경우에만 표시 될 수 있습니다. **Shutdown**: Limit Control 모듈에 의해 포트가 차단되었음을 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 안내

Refresh: 새로고침을 합니다. 저장되지 않은 변경사항은 소실됩니다.

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.12.2 접근 관리

이 페이지에서 액세스 관리 테이블을 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 (액세스 관리 구성) 화면이 나타납니다.

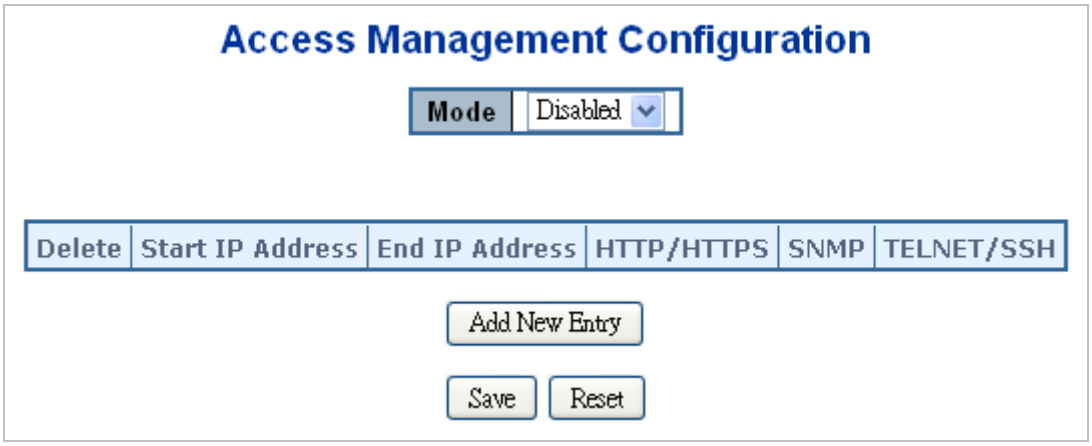


그림 4-12-2 Access Management Configuration Overview 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Mode**	액세스 관리 방식 조작을 나타냅니다. 가능한 방식은는 다음과 같습니다. **Enabled**: 액세스 관리 방식 조작을 사용 가능하게하십시오. **Disabled**: 액세스 관리 방식 작업을 비활성화합니다.
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제됩니다.
• **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 안내

Add New Entry: 새 액세스 관리 항목을 추가하려면 클릭하십시오.

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.12.3 접근 관리 통계

이 페이지는 액세스 관리에 대한 통계를 제공합니다. 그림 4-12-3 의 액세스 관리 통계 화면이 나타납니다.

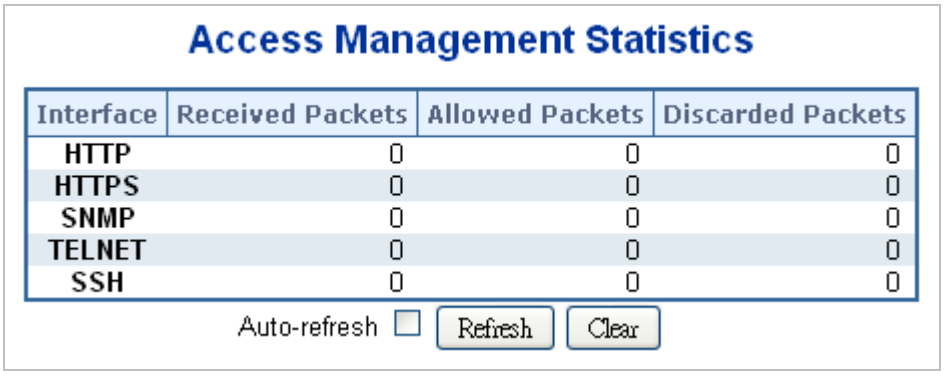


그림 4-12-3 Access Management Statistics Overview 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Interface**	원격 호스트를 허용 한 인터페이스가 스위치에 액세스 할 수 있습니다.
• **Receive Packets**	액세스 관리 방식에서 인터페이스로부터 수신 된 패킷 번호가 사용 가능합니다.
• **Allow Packets**	액세스 관리 방식에서 인터페이스로부터 허용 된 패킷 수를 사용할 수 있습니다.
• **Discard Packets**	액세스 관리 방식에서 인터페이스에서 버려진 패킷 번호가 사용 가능합니다.

버튼 안내

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

Refresh: 페이지를 새로고칩니다.

Clear: 모든 통계를 지 웁니다.

3.12.4 HTTPs

이 페이지에서 HTTPS 를 구성하십시오. 그림 4-12-4 의 HTTPS Configuration 화면이 나타납니다.

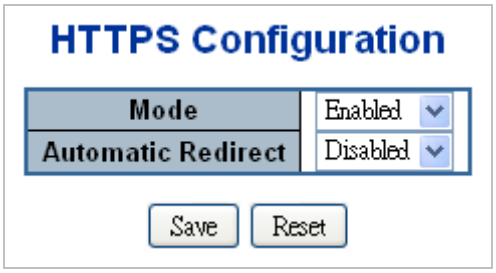


그림 4-12-4 HTTPS Configuration screen 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Mode**	HTTPS 방식 작업을 나타냅니다. 현재 연결이 HTTPS 인 경우 HTTPS 사용 안 함 방식을를 적용하면 웹 브라우저가 자동으로 HTTP 연결로 리디렉션됩니다. 가능한 방식은는 다음과 같습니다. ■ **Enabled**: HTTPS 방식 작동을 활성화합니다. ■ **Disabled**: HTTPS 방식 작동을 비활성화합니다.
• **Automatic Redirect**	HTTPS 리디렉션 방식 작업을 나타냅니다. HTTPS 방식 "Enabled"가 선택된 경우에만 중요합니다. HTTPS 방식과와 자동 리디렉션이 모두 활성화 된 경우 자동으로 웹 브라우저를 HTTPS 연결로 리디렉션하거나 둘 다 사용할 수없는 경우 웹 브라우저를 HTTP 연결로 리디렉션합니다. 가능한 방식은는 다음과 같습니다. ■ **Enabled**: HTTPS 리디렉션 방식 작동을 활성화합니다. ■ **Disabled**: HTTPS 리디렉션 방식 작동을 비활성화합니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.12.5 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 방식에서는 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.

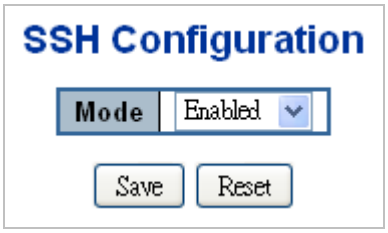


그림 4-12-5 SSH Configuration screen 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Mode**	SSH 방식 작동을 나타냅니다. 가능한 방식은는 다음과 같습니다. ■ **Enabled**: SSH 방식 작동을 활성화합니다. ■ **Disabled**: SSH 방식 작동을 비활성화합니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.12.6 포트 보안 상태

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 방식에서는 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 화면이 나타납니다.

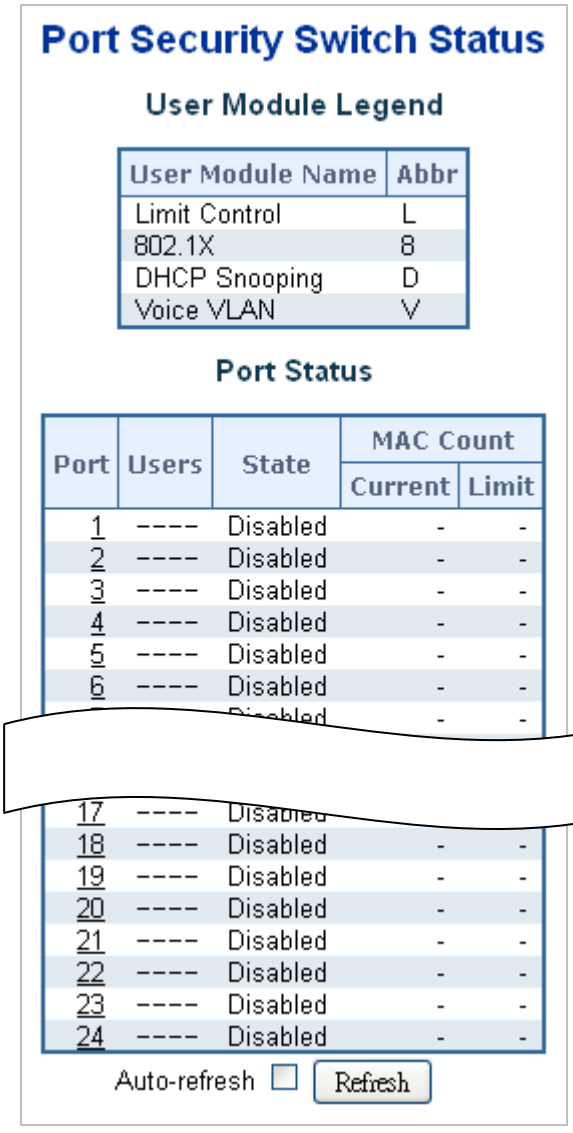


그림 4-12-6 Port Security Status screen 페이지 화면

다음과 같은 기능을 소개합니다.

사용자 모듈 범례

범례에는 포트 보안 서비스를 요청할 수있는 모든 사용자 모듈이 표시됩니다.

기능	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.

포트 상태

이 테이블에는 스위치의 선택된 스위치에있는 각 포트에 대해 하나의 행과 여러 열이 있습니다.

기능	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 않았 음을 의미하는 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 활성화되어 있으며 해당 모듈은 한계에 도달했으며 더 이상 MAC 주소를 가져 오지 않아야 함을 나타냅니다. **Shutdown**: Port Security 서비스가 적어도 Limit Control 사용자 모듈에 의해 활성화되고, 그 모듈은 한계가 초과되었음을 나타냅니다. 제한 제어 구성 웹 페이지에서 관리 상 다시 열 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 안내

Refresh: 페이지를 새로고칩니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

3.12.7 포트 보안 세부 사항

이 페이지는 포트 보안 모듈에 의해 보안 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 방식에서는 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 Port Security Detail 화면이 나타납니다.

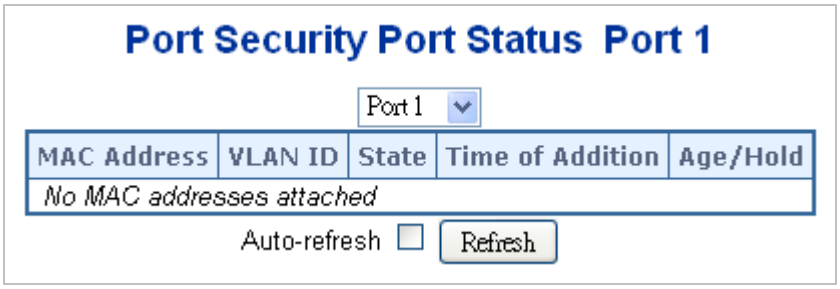


그림 4-12-7 Port Security Detail screen 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **MAC Address & VLAN ID**	이 포트에 표시되는 MAC 주소 및 VLAN ID 입니다. 학습 된 MAC 주소가 없으면 "No MAC addresses attached"라는 단일 행이 표시됩니다.
• **State**	해당 MAC 주소가 차단되었는지 또는 전달 중인지 여부를 나타냅니다. 차단 된 상태에서는 트래픽을 전송하거나 수신 할 수 없습니다.
• **Time of Adding**	이 MAC 주소가 포트에서 처음으로 표시 된 날짜와 시간을 표시합니다.
• **Age/Hold**	하나 이상의 사용자 모듈이이 MAC 주소를 차단하기로 결정한 경우 hold 시간 (초 단위)이 만료 될 때까지 차단 된 상태로 유지됩니다. 모든 사용자 모듈이이 MAC 주소의 전달을 허용하고 에이징을 사용하도록 설정 한 경우 포트 보안 모듈은 주기적으로이 MAC 주소가 트래픽을 전달하는지 확인합니다. 경과 시간 (초 단위로 측정)이 만료되고 프레임이 표시되지 않으면 MAC 주소가 MAC 테이블에서 제거됩니다. 그렇지 않으면 새로운 연령대가 시작됩니다. 에이징이 비활성화되거나 사용자 모듈이 MAC 주소를 무기한 보유하기로 결정하면 대시 (-)가 표시됩니다.

버튼 안내

Refresh: 페이지를 새로고칩니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

3.12.8 DHCP Snooping

DHCP 스누핑은 DHCP 클라이언트와 서버 간의 합법적 인 대화에 가짜 DHCP 응답 패킷을 주입하여 간섭을 시도할 때 DUT 의 신뢰할 수없는 포트에서 침입자를 차단하는 데 사용됩니다. 이 페이지에서 DHCP 스누핑을 구성하십시오. 그림 4-12-8 의 DHCP Snooping Configuration (DHCP 스누핑 구성) 화면이 나타납니다.

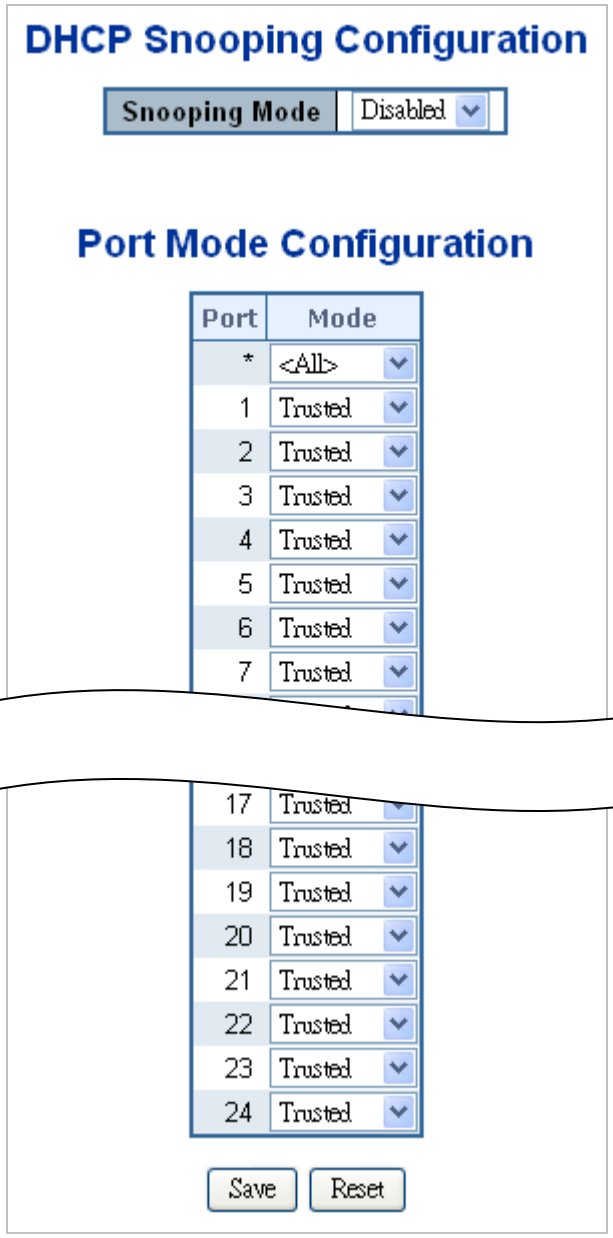


그림 4-12-8 DHCP Snooping Configuration screen 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Snooping Mode**	DHCP 스누핑 모드 작업을 나타냅니다. 가능한 모드는 다음과 같습니다.: **Enabled**: DHCP 스누핑 모드 작업을 활성화합니다. DHCP 스누핑 모드 작동을 활성화하면 요청 DHCP 메시지가 트러스트 된 포트로 전달되고 트러스트 된 포트의 응답 패킷 만 허용됩니다. **Disabled**: DHCP 스누핑 모드 작업을 비활성화합니다.
• **Port Mode Configuration**	DHCP 스누핑 포트 모드를 나타냅니다. 가능한 포트 모드는 다음과 같습니다. **Trusted**: 포트를 DHCP 메시지의 신뢰할 수있는 원본으로 구성합니다. **Untrusted**: 포트를 DHCP 메시지의 신뢰할 수없는 소스로 구성합니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.12.9 DHCP Snooping Statistics

페이지는 DHCP 스누핑에 대한 통계를 제공합니다. DHCP 스누핑 모드의 통계 만 카운터 패킷이 활성화되고 릴레이 모드가 비활성화됩니다. 그리고 그것은 시스템 DHCP 클라이언트에 대한 DHCP 패킷을 계산하지 않습니다. 그림 4-12-9 의 DHCP Snooping Port Statistics 화면이 나타납니다.

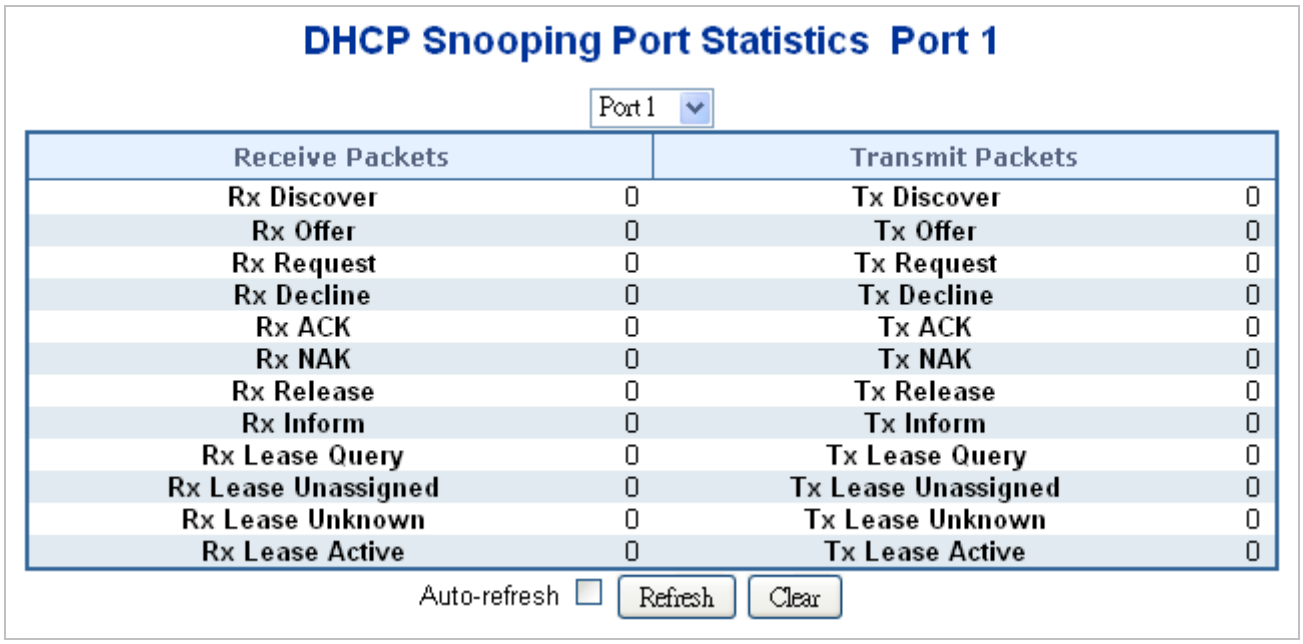


그림 4-12-9 DHCP Snooping Port Statistics screen 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Rx and Tx Discover**	송수신 된 패킷 수 (수신 된 옵션 1, 값 1).
• **Rx and Tx Offer**	송수신 된 (옵션 53 값 2) 패킷 수 및 전송.
• **Rx and Tx Request**	수신 및 전송 된 요청 수 (옵션 53 값 3).
• **Rx and Tx Decline**	송수신 된 패킷 수 (옵션 53, 값 4).
• **Rx and Tx ACK**	수신 및 전송 된 ACK (옵션 53 값 5)의 수.
• **Rx and Tx NAK**	송수신되는 NAK (옵션 53 값 6) 패킷의 수.
• **Rx and Tx Release**	송수신 된 패킷 수 (옵션 53, 값 7).
• **Rx and Tx Inform**	수신 및 전송 된 정보의 수 (옵션 53 값 8).
• **Rx and Tx Lease Query**	수신 및 전송 된 임대 쿼리 (옵션 53 값 10)의 수.
• **Rx and Tx Lease Unassigned**	수신되고 전송 된 임대되지 않은 임대 (옵션 53 값 11)의 수.
• **Rx and Tx Lease Unknown**	수신 및 전송 된 임대 알 수없는 (옵션 53 값 12) 패킷 수.
• **Rx and Tx Lease Active**	송수신 된 임대 활성 (옵션 53 값 13) 패킷 수.

버튼 안내

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

Refresh: 페이지를 새로고칩니다.

Clear: 선택한 포트에 대한 카운터를 지 웁니다.

3.12.10 IP Source Guard 설정

IP 소스 가드는 DHCP 스누핑 테이블 또는 수동으로 구성된 IP 소스 바인딩을 기반으로 트래픽을 필터링하여 DHCP 스누핑 트러스트되지 않은 포트의 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 설정을 제공합니다. 그림 4-12-10 의 IP Source Guard Configuration 화면이 나타납니다.

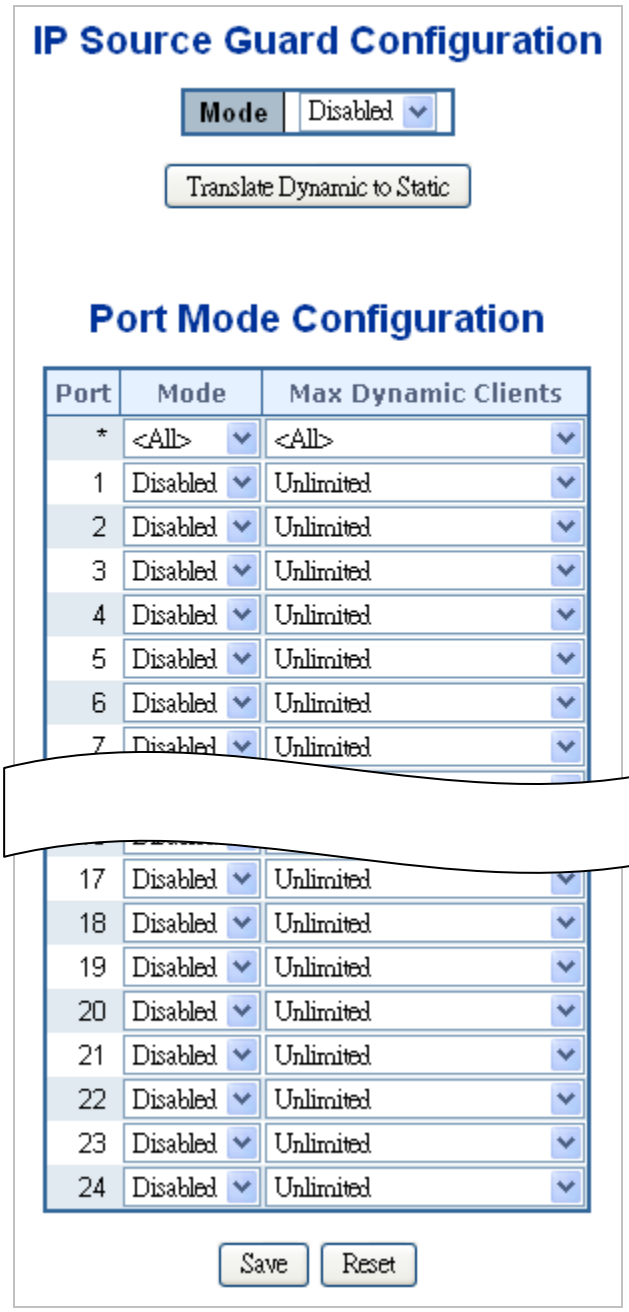


그림 4-12-10 IP Source Guard Configuration screen 페이지 화면

다음과 같은 기능을 소개합니다.

기능	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 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

Translate Dynamic to Static: 모든 동적 항목을 정적 항목으로 변환하려면 클릭하십시오.

3.12.11 IP Source Guard Static Table

이 페이지는 정적 IP 소스 가드 테이블을 제공합니다. 그림 4-12-11 의 정적 IP 소스 가드 테이블 화면이 나타납니다.

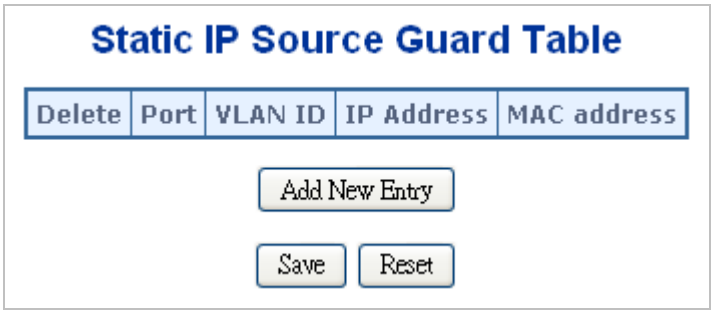


그림 4-12-11 Static IP Source Guard Table screen 페이지 화면

다음과 같은 기능을 소개합니다.

기능	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 안내

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

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.12.12 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 응답 만 DUT 를 통과 할 수 있습니다. 이 페이지는 ARP 검사와 관련된 구성을 제공합니다. 그림 4-12-12 의 ARP Inspection Configuration 화면이 나타납니다.

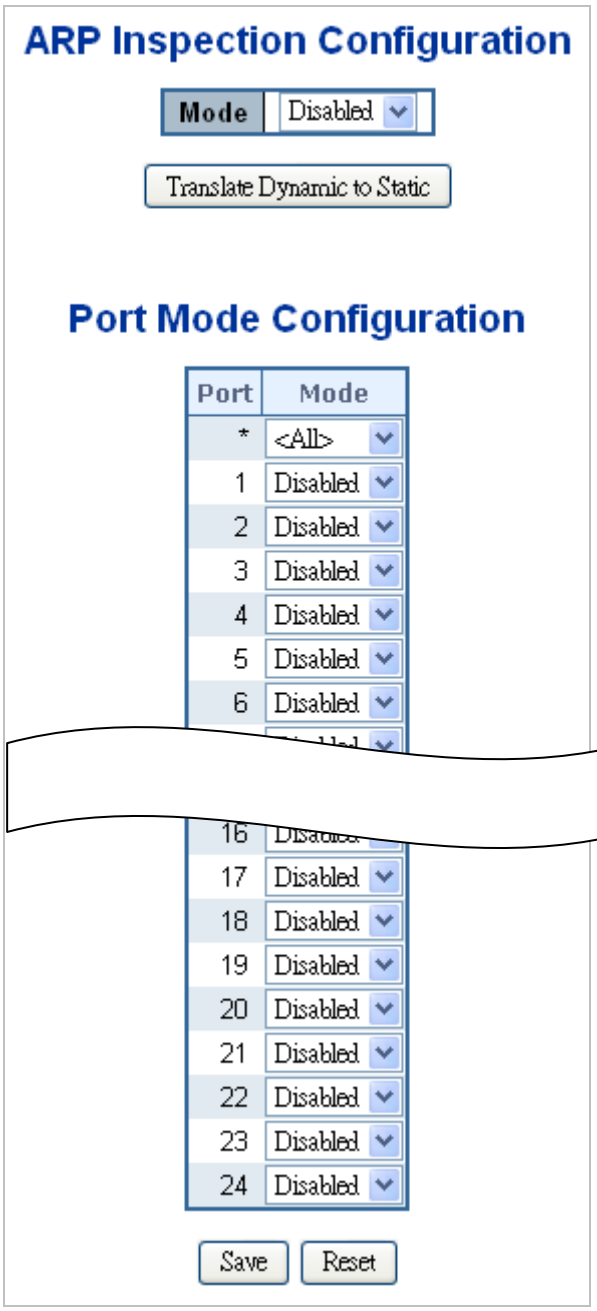


그림 4-12-12 ARP Inspection Configuration screen 페이지 화면

다음과 같은 기능을 소개합니다.

기능	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.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

Translate Dynamic to Static: 모든 동적 항목을 정적 항목으로 변환하려면 클릭하십시오..

3.12.13 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 Table screen 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제됩니다.
• **Port**	설정에 대한 논리 포트입니다.
• **VLAN ID**	설정에 대한 VLAN ID 입니다.
• **MAC Address**	ARP 요청 패킷의 소스 MAC 주소 허용.

• **IP Address**	허용 된 소스 IP 주소는 ARP 요청 패킷입니다.

버튼 안내

Add New Entry: 정적 ARP 검사 표를 만듭니다.

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.13 Address Table

. 프레임 전환은 프레임에 포함 된 DMAC 주소를 기반으로합니다. 관리 형 스위치는 MAC 주소를 스위치 포트에 매핑하는 테이블을 구성하여 프레임이 어느 포트로 이동해야하는지 (프레임의 DMAC 주소를 기준으로)를 파악합니다. 이 테이블에는 정적 항목과 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 테이블을 이러한 동적 MAC 주소로 업데이트하는 데 사용됩니다. 구성 가능한 에이징 시간 후에 해당 SMAC 주소가있는 프레임이 표시되지 않으면 동적 항목이 MAC 테이블에서 제거됩니다.

3.13.1 MAC 주소 표

MAC 주소 표가이 페이지에서 구성됩니다. 동적 MAC 테이블의 항목에 대한 시간 초과를 설정하고 여기에 정적 MAC 테이블을 구성하십시오. 그림 4-13-1 의 MAC 주소 표 (MAC 주소 표 구성) 화면이 나타납니다.

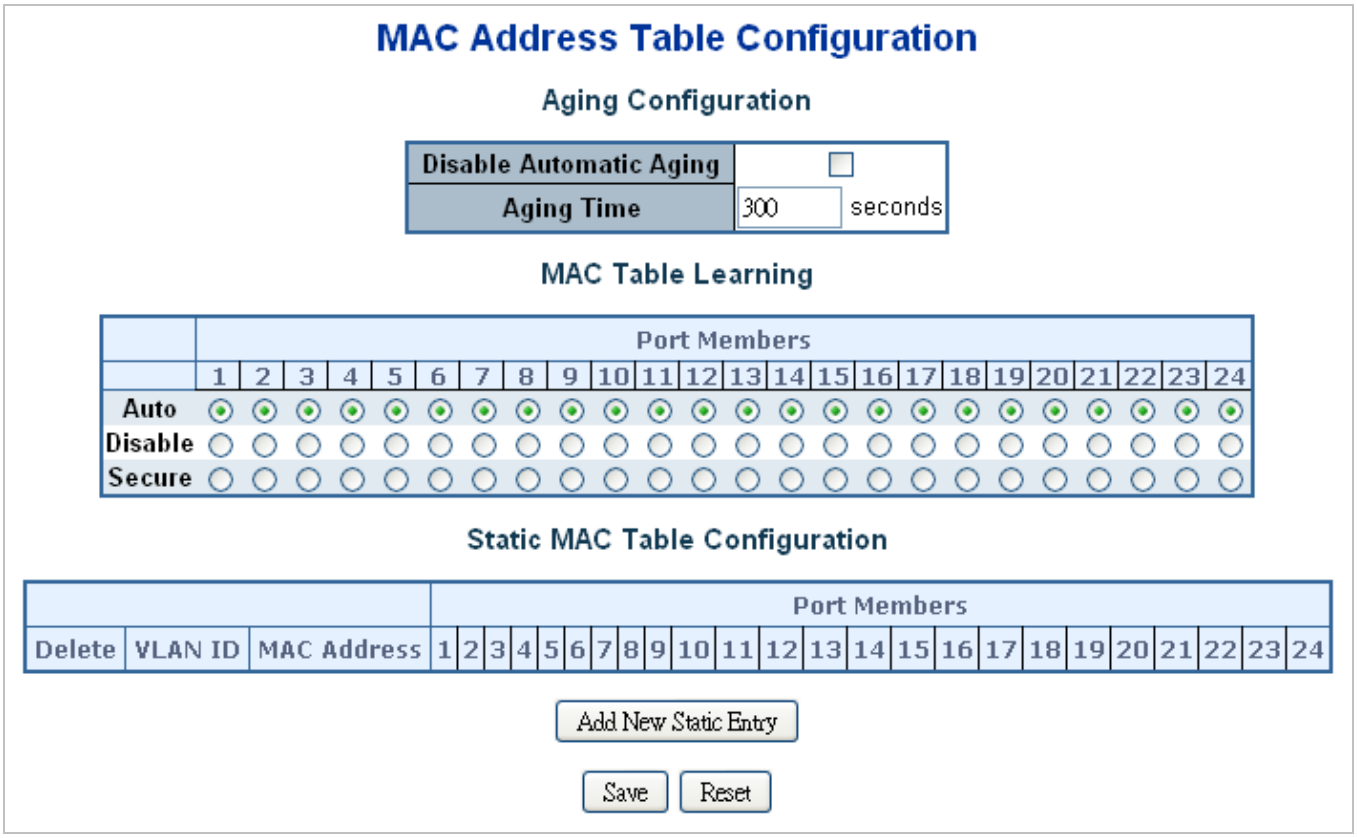


그림 4-13-1 MAC Address Table 구성화면

다음과 같은 기능을 소개합니다.

Aging 설정

기본적으로 300 초 후에 동적 항목이 MAC 테이블에서 제거됩니다. 이 제거는 aging 이라고 합니다..

기능	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 Table 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.

기능	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 Table 에 추가되었는지 확인하십시오. 그렇지 않으면 관리 링크가 손실되고 다른 비보안 포트를 사용하거나 스위치에 연결해야만 직렬인터페이스를 통해 복원을 할 수 있습니다.

고정 Mac 테이블 설정

테이블에는 MAC 테이블의 정적 항목이 표시됩니다. 정적 MAC 테이블은 64 개의 엔트리를 포함 할 수 있습니다. MAC 테이블은 먼저 VLAN ID 와 MAC 주소 순으로 정렬됩니다.

기능	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**	정적 MAC 테이블에 새 항목을 추가하려면 "새 정적 항목 추가"를 클릭하십시오. 새 항목에 대한 VLAN ID, MAC 주소 및 포트 구성원을 지정하십시오. "저장"을 클릭하십시오.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.13.2 MAC Address Table Status

Dynamic MAC Table

이 페이지에는 MAC 테이블의 항목이 표시됩니다. MAC 테이블은 최대 8192 개의 항목을 포함하며 VLAN ID, MAC 주소 순서로 먼저 정렬됩니다. 그림 4-13-2 의 MAC Address Table 화면이 나타납니다.

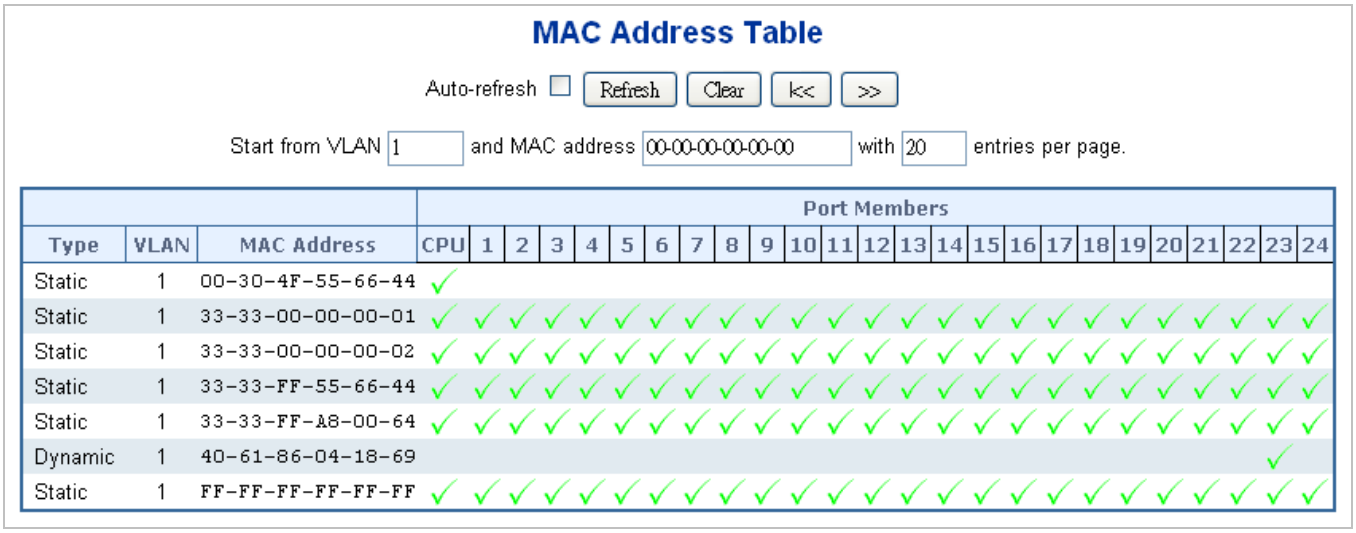


그림 4-13-2 MAC Address Table Status

MAC 표 탐색

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 테이블의 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 표시된 테이블이 가장 가까운 다음 MAC 테이블과 일치하는 것으로 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. "| <<"버튼을 사용하여 다시 시작하십시오.

다음과 같은 기능을 소개합니다.

기능	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 안내

Auto-refresh : 자동으로 3 초 마다 새로고침을 합니다.

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 테이블을 업데이트합니다.

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

3.13.3 동적 ARP 검사 표

이 페이지에는 동적 ARP 검사 표의 항목이 표시됩니다. Dynamic ARP Inspection Table (동적 ARP 검사 표)은 최대 1024 개의 항목을 포함하며 포트별로 먼저 정렬 된 다음 VLAN ID, MAC 주소 및 IP 주소 순으로 정렬됩니다. 그림 4-13-3 의 동적 ARP 검사 표 화면이 나타납니다.

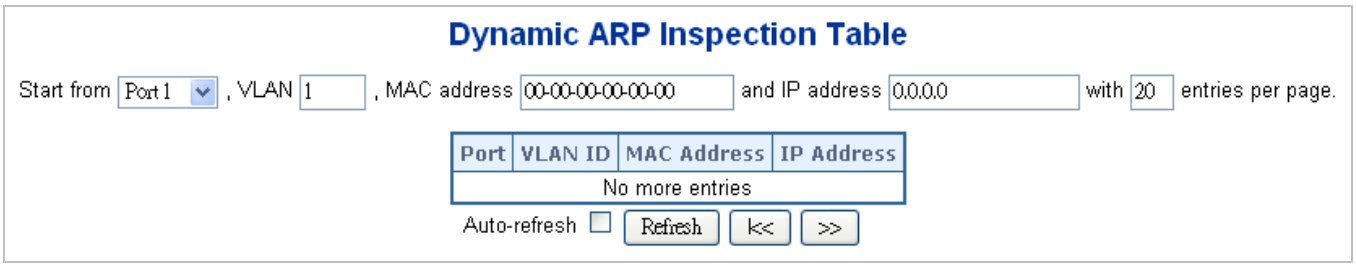


그림 4-13-3 Dynamic ARP Inspection Table 화면

ARP 검사 표 탐색

각 페이지에는 Dynamic ARP Inspection (동적 ARP 검사) 테이블에서 최대 99 개의 항목 (기본값은 20 페이지)이 "페이지 당 항목 수"입력 필드를 통해 선택되어 표시됩니다. 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 테이블이 업데이트되거나 가장 가까운 다음 동적 ARP 검사 테이블 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. "| <<"버튼을 사용하여 다시 시작하십시오.

다음과 같은 기능을 소개합니다.

기능	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**	항목의 IP 주소.

버튼 안내

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

Refresh: "MAC 주소에서 시작"및 "VLAN"입력 필드에서 표시된 테이블을 새로 고칩니다.

Clear: 모든 동적 항목을 플러시합니다.

<<: 가장 낮은 VLAN ID 및 MAC 주소를 갖는 항목 인 MAC 테이블의 첫 번째 항목부터 시작하여 테이블을 업데이트합니다.

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

3.13.4 Dynamic IP Source Guard Table

동적 IP 소스 가드 테이블의 항목이이 페이지에 표시됩니다. 동적 IP 소스 가드 테이블은 먼저 포트별로 분류 된 다음 VLAN ID, IP 주소 및 IP 마스크 순으로 정렬됩니다. 그림 4-13-4 의 동적 IP 소스 가드 테이블 화면이 나타납니다.

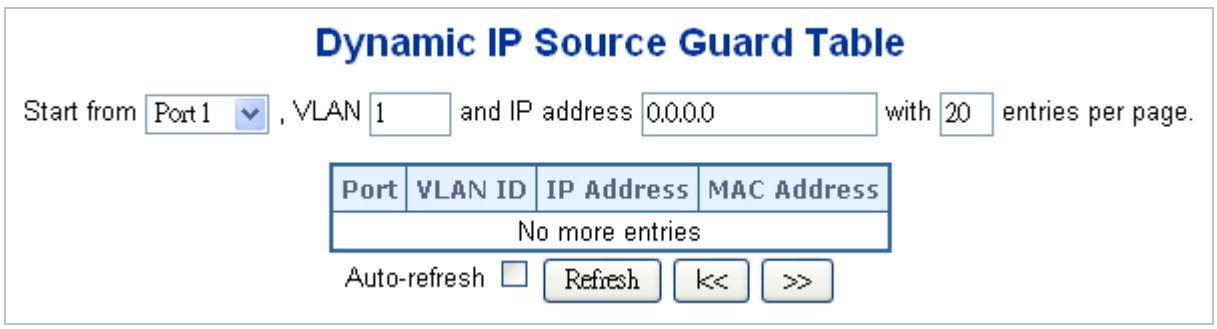


그림 **4-13-4** Dynamic IP Source Guard Table 화면

ARP 검사표 탐색

각 페이지는 동적 IP 소스 가드 테이블에서 최대 99 개의 항목을 표시하며, 기본값은 20 이고 "페이지 당 항목 수"입력 필드를 통해 선택됩니다. 처음 방문했을 때, 웹 페이지는 동적 IP 소스 가드 테이블의 처음부터 처음 20 개의 항목을 보여줍니다.

"포트 주소에서 시작", "VLAN", "IP 주소"및 "IP 마스크"입력 필드를 사용하여 동적 IP 소스 가드 테이블에서 시작 지점을 선택할 수 있습니다. "Refresh (새로 고침)"버튼을 클릭하면 표시된 테이블 또는 가장 가까운 다음 동적 IP 소스 가드 테이블 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. "| <<"버튼을 사용하여 다시 시작하십시오.

다음과 같은 기능을 소개합니다.

기능	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**	항목의 IP 주소.

버튼 안내

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

Refresh: "MAC 주소에서 시작"및 "VLAN"입력 필드에서 표시된 테이블을 새로 고칩니다..

Clear: 모든 동적 항목을 플러시합니다.

<<: MAC 테이블의 첫 번째 항목, 즉 VLAN ID 와 MAC 주소가 가장 낮은 항목부터 테이블을 업데이트합니다.

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

3.14 LLDP

3.14.1 Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) 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.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) 는 IP 폰 및 네트워크 스위치와 같은 종단점 장치를 관리하기위한 LLDP 의 확장입니다. LLDP-MED TLV 는 네트워크 정책, 전원, 인벤토리 및 장치 위치 세부 정보와 같은 정보를 알립니다. LLDP 및 LLDP-MED 정보는 SNMP 응용 프로그램에서 사용하여 문제 해결을 단순화하고 네트워크 관리를 향상 시키며 정확한 네트워크 토폴로지를 유지 관리 할 수 있습니다.

3.14.2 LLDP Configuration

이 페이지에서 사용자는 현재 LLDP 포트 설정을 검사하고 구성 할 수 있습니다. 그림 4-14-1 의 LLDP Configuration (LLDP 구성) 화면이 나타납니다..

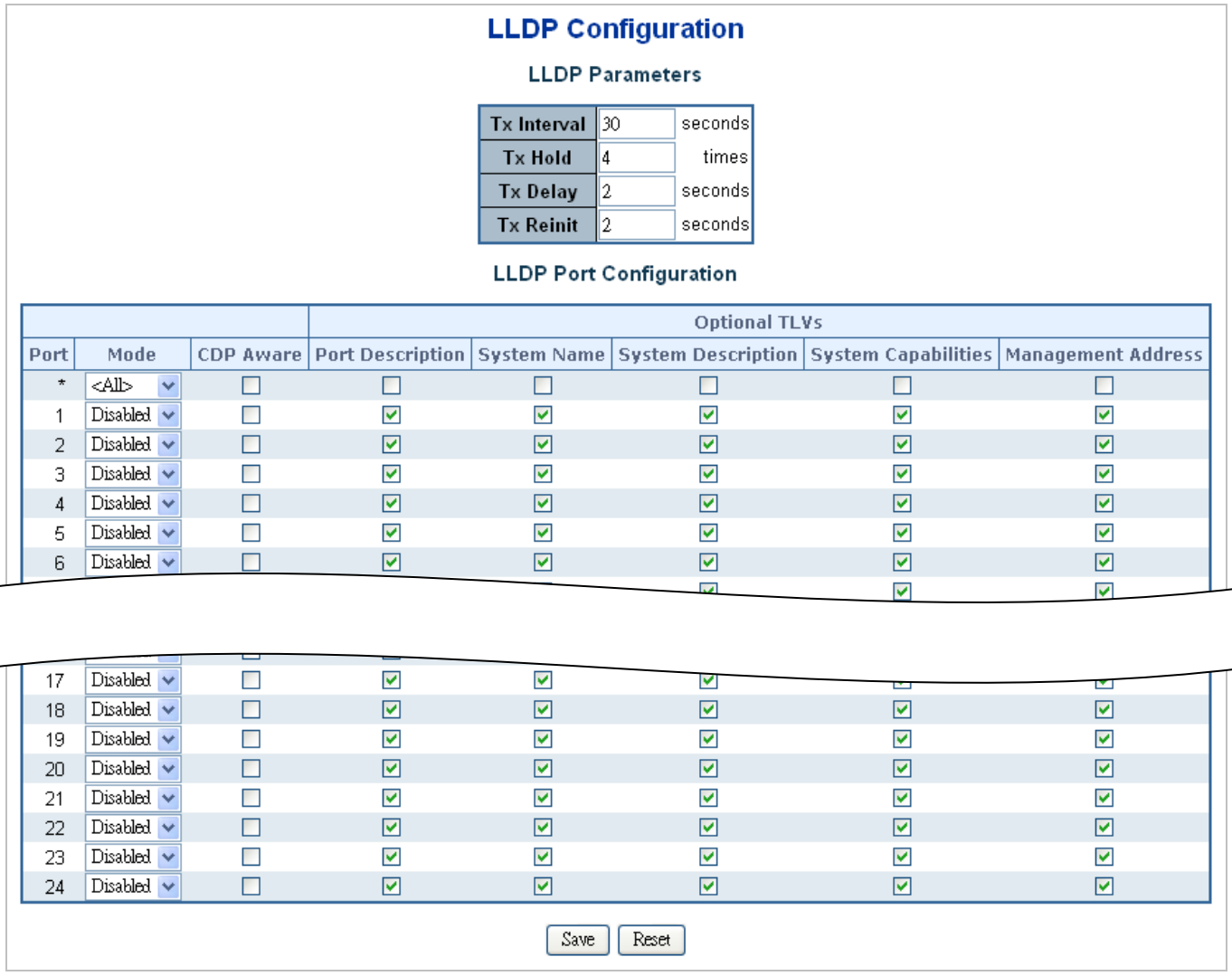


그림 4-14-1 LLDP 구성화면

다음과 같은 기능을 소개합니다.

LLDP Parameters

기능	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 시간 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 * 홀드 타임 멀티 플라이어) ≤ 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 * 지연 간격) ≤ 전송 간격
• **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 포트 설정

LLDP 포트 설정은 페이지 머리글에 반영된대로 현재 선택된 스택 장치와 관련됩니다.

기능	설명
• **Port**	논리적 LLDP 포트의 스위치 포트 번호입니다.
• **Mode**	LLDP 모드를 선택하십시오. **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** 스위치는 LLDP 정보를 전송하지 않으며 이웃 라우터로부터 수신 한 LLDP 정보를 삭제합니다. **Enabled** 스위치는 LLDP 정보를 보내고 이웃 라우터로부터 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 테이블의 해당 필드에 매핑 할 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 아래 그림과 같이 LLDP 인접 테이블에 매핑됩니다. CDP TLV "장치 ID"는 LLDP "섀시 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 Descr**	Optional TLV: "포트 설명"이 선택되면 전송 된 LLDP 정보에 포함됩니다.
• **Sys Name**	Optional TLV:이 옵션을 선택하면 "시스템 이름"이 전송 된 LLDP 정보에 포함됩니다.
• **Sys Descr**	Optional TLV (선택 TLV) : 선택하면 "시스템 설명"이 전송 된 LLDP 정보에 포함됩니다.
• **Sys Capa**	Optional TLV (선택 TLV) : 선택하면 "시스템 기능"이 전송 된 LLDP 정보에 포함됩니다.
• **Mgmt Addr**	Optional TLV : 선택하면 "관리 주소"가 전송 된 LLDP 정보에 포함됩니다.

버튼 안내

Save : 변경내용을 저장합니다.

Reset : 이전의 저장값으로 되돌립니다.

3.14.3 LLDP MED Configuration

이 페이지에서 LLDP-MED 를 구성 할 수 있습니다. 그림 4-14-2 의 LLDPMED Configuration 화면이 나타납니다.

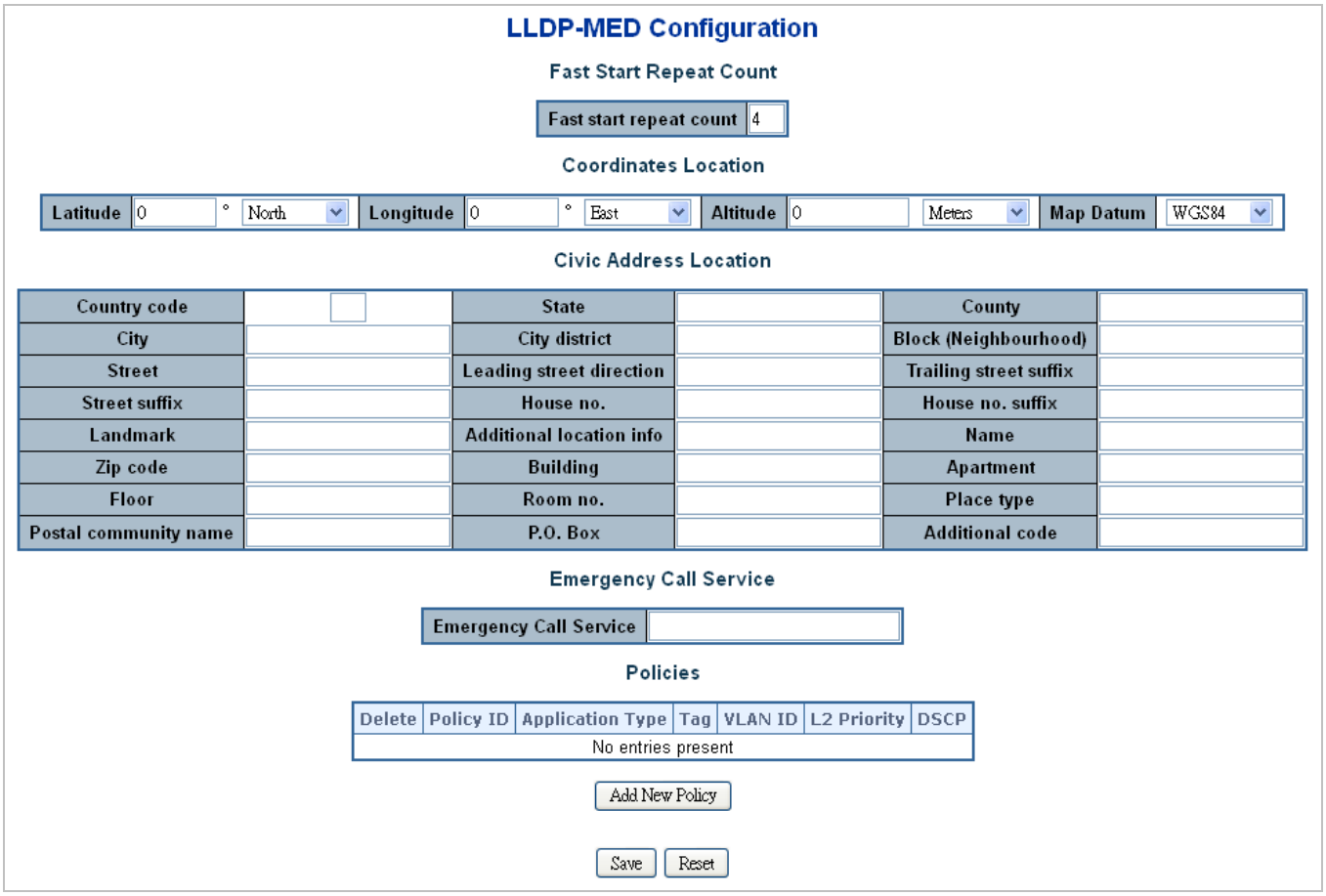


그림 4-14-2 LLDPMED 구성화면

다음과 같은 기능을 소개합니다.

Fast start repeat count

기능	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 공유 할 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

기능	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 (SHOULD). 본초 자오선의 동쪽 또는 본 자오선의 서쪽 방향을 지정할 수 있습니다.
• **Altitude**	**Altitude** -32767 ~ 32767 범위 내에서 최대 4 자리까지 정규화되어야합니다. 두 고도 유형 (층 또는 미터) 중에서 선택할 수 있습니다. **Meters**: 지정된 수직 데이터로 정의 된 고도 미터를 나타냅니다.. **Floors**: 바닥에서 바닥까지의 치수가 다른 건물에서보다 관련성이 높은 형태로 고도 표현. 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**: 북미 표준시 1983, CRS 코드 4269, 본초 자오선 이름 : 그리니치; 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**: 북미 표준시 1983, CRS 코드 4269, 본초 자오선 이름 :

	그리니치; 관련 수직 자료는 평균 저수위 (MLLW)입니다. 이 데이텀 쌍은 물 / 바다 / 바다에서 위치를 참조 할 때 사용됩니다.

Civic Address Location

IETF Geopriv Civic Address 기반의 위치 구성 정보 (Civic Address LCI)..

기능	설명
• **Country code**	두 자로 된 ISO 3166 국가 코드 (대문자 ASCII 문자) - 예 : DK, DE 또는 US.
• **State**	국가 세분 (주, 주, 지방, 지방, 현).
• **County**	카운티, 교구, 총 (일본), 지구.
• **City**	시, 군구,시 (일본) - 예 : 코펜하겐
• **City district**	시구 정촌, 구청, 구청, 구, 주오 (일본)
• **Block (Neighborhood)**	이웃, 블록
• **Street**	거리 - 예 : Poppelvej
• **Leading street direction**	선도 방향 - 예 : N
• **Trailing street suffix**	후행 거리 접미사 - 예 : SW
• **Street suffix**	거리 접미사 - 예 : Ave, Platz
• **House no.**	집 번호 - 예 : 21
• **House no. suffix**	집 번호 접미사 - 예 : A, 1/2
• **Landmark**	랜드 마크 또는 허영심 주소 - 예 : Columbia University
• **Additional location info**	추가 위치 정보 - 예 : South Wing
• **Name**	이름 (거주지 및 사무실 거주자) - 예 : Flemming Jahn
• **Zip code**	우편 / 우편 번호 - 예 : 2791
• **Building**	건물 (구조) - 예 : 낮은 도서관
• **Apartment**	단위 (아파트, 스위트) - 예 : Apt 42
• **Floor**	층 - 예 : 4
• **Room no.**	방 번호 - 예 : 450F
• **Place type**	장소 유형 - 예 : 사무실
• **Postal community**	우편 커뮤니티 이름 - 예 : Leonia

name	
• **P.O. Box**	우체국 상자 (사서함) - 예 : 12345
• **Additional code**	추가 코드 - 예 : 1320300003

Emergency Call Service

TIA 또는 NENA 에서 정의한 비상 전화 서비스 (예 : E911 및 기타).

기능	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.

정책

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 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

이 네트워크 정책은 잠재적으로 알려지며 주어진 포트에서 지원되는 여러 유형의 응용 프로그램과 연관됩니다.
특별히 처리 된 응용 프로그램 유형은 다음과 같습니다.:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signaling (conditionally support a separate network policy for the media types above)

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 종점 간 링크 이외의 링크에서 실행되지 않으므로 LAN 내부의 집계 링크에서 자주 실행되는 수많은 네트워크 정책을 광고 할 필요가 없습니다.

기능	설명
• **Delete**	정책을 삭제하려면 선택하십시오. 다음 저장 중에 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 (conditional)** - 음성 신호보다 음성 신호에 대해 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** - 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 (conditional)** - 게스트 음성 신호 대신 게스트 음성 신호에 대해 다른 정책을 요구하는 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 장치에서 소프트 폰 응용 프로그램에 사용됩니다. 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** - 실시간 대화 형 비디오 / 오디오 서비스를 지원하는 전용 화상 회의 장비 및 기타 유사한 어플라이언스에서 사용합니다 **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 (conditional)** - 비디오 신호보다 비디오 신호에 대한 별도의 정책이 필요한 네트워크 토폴로지에서 사용하기위한 것입니다. 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 는 장치가 태그없는 프레임 형식을 사용하고 있으며 IEEE 802.1Q-2003 에 정의 된대로 태그 머리글을 포함하지 않음을 나타냅니다. 이 경우 VLAN ID 및 레이어 2 우선 순위 필드는 모두 무시되며 DSCP 값만 관련성을 갖습니다. Tagged 는 장치가 IEEE 802.1Q 태그가 지정된 프레임 형식을 사용하고 있고 VLAN ID 와 계층 2 우선 순위 값이 모두 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 정책 추가"를 클릭하여 새 정책을 추가하십시오. 새 정책에 대해 응용 프로그램 유형, 태그, VLAN ID, L2 우선 순위 및 DSCP 를 지정하십시오. "저장"을 클릭하십시오. 지원되는 정책 수는 32 개입니다.

포트 정책 설정

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.

기능	설명
• **Port**	구성이 적용되는 포트 번호입니다.

• **Policy ID**	특정 포트에 적용되는 정책 집합입니다. 정책 집합은 정책에 해당하는 확인란을 선택하여 선택합니다.

버튼 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.14.4 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 들어 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 페이지 화면

다음과 같은 기능을 소개합니다.

Fast start repeat count

기능	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 Network Connectivity Device Definition** 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 브리지

3. IEEE 802.3 중계기 (역사적 이유로 포함)

4. IEEE 802.11 무선 액세스 포인트

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 Endpoint Device Definition

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 Generic Endpoint (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 Media Endpoint (Class II)

LLDP-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 Communication Endpoint (Class III)

LLDP-MED 통신 종점 (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 확장 전원 5. MDI-PD 를 통한 연장 된 전력 6. 재고 7. 예약 됨
• **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** - 전용 IP 텔레포니 핸드셋 및 대화 형 음성 서비스를 지원하는 기타 유사한 어플라이언스에서 사용합니다. 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 사용합니다. **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 - 게스트 음성 미디어보다 게스트 음성 시그널링에 대해 다른 정책이 필요한 네트워크 토폴로지에서 사용합니다 **Softphone Voice** - PC 또는 랩톱과 같은 일반적인 데이터 중심 장치의 소프트 폰 응용 프로그램에서 사용합니다. **Video Conferencing** - 전용 화상 회의 장비 및 실시간 대화식 비디오 / 오디오 서비스를 지원하는 기타 유사한 장비에서 사용합니다. **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** - 비디오 신호보다는 비디오 신호에 대해 별도의 정책이 필요한 네트워크 토폴로지에서 사용합니다
• **Policy**	정책은 엔드 포인트 장치가 정책이 장치에 필요하다는 것을 명시 적으로 알리고 싶어 함을 나타냅니다. 정의 또는 알 수 없음 알 수 없음 : 지정된 응용 프로그램 유형에 대한 네트워크 정책은 현재 알 수 없습니다. 정의 : 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 계층 2 우선 순위입니다. 우선 순위 8 개 중 하나 (0-7)
• **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**	자동 협상은 링크 파트너가 MAC / PHY 자동 협상을 지원하는지 식별합니다.
• **Auto-negotiation status**	자동 협상 상태는 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 안내

Refresh: 페이지를 새로고칩니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

3.14.5 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 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Local Port**	LLDP 프레임을 수신 한 포트입니다.
• **Chassis ID**	Chassis ID 는 이웃의 LLDP 프레임을 식별합니다.
• **Remote Port ID**	원격 포트 ID 는 인접 포트의 ID 입니다.
• **System Name**	시스템 이름은 이웃 장치가 알리는 이름입니다.
• **Port Description**	Port Description (포트 설명)은 인접 장치가 알린 포트 설명입니다.
• **System Capabilities**	시스템 기능은 이웃 장치의 기능을 설명합니다. 가능한 기능은 다음과 같습니다: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved 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.

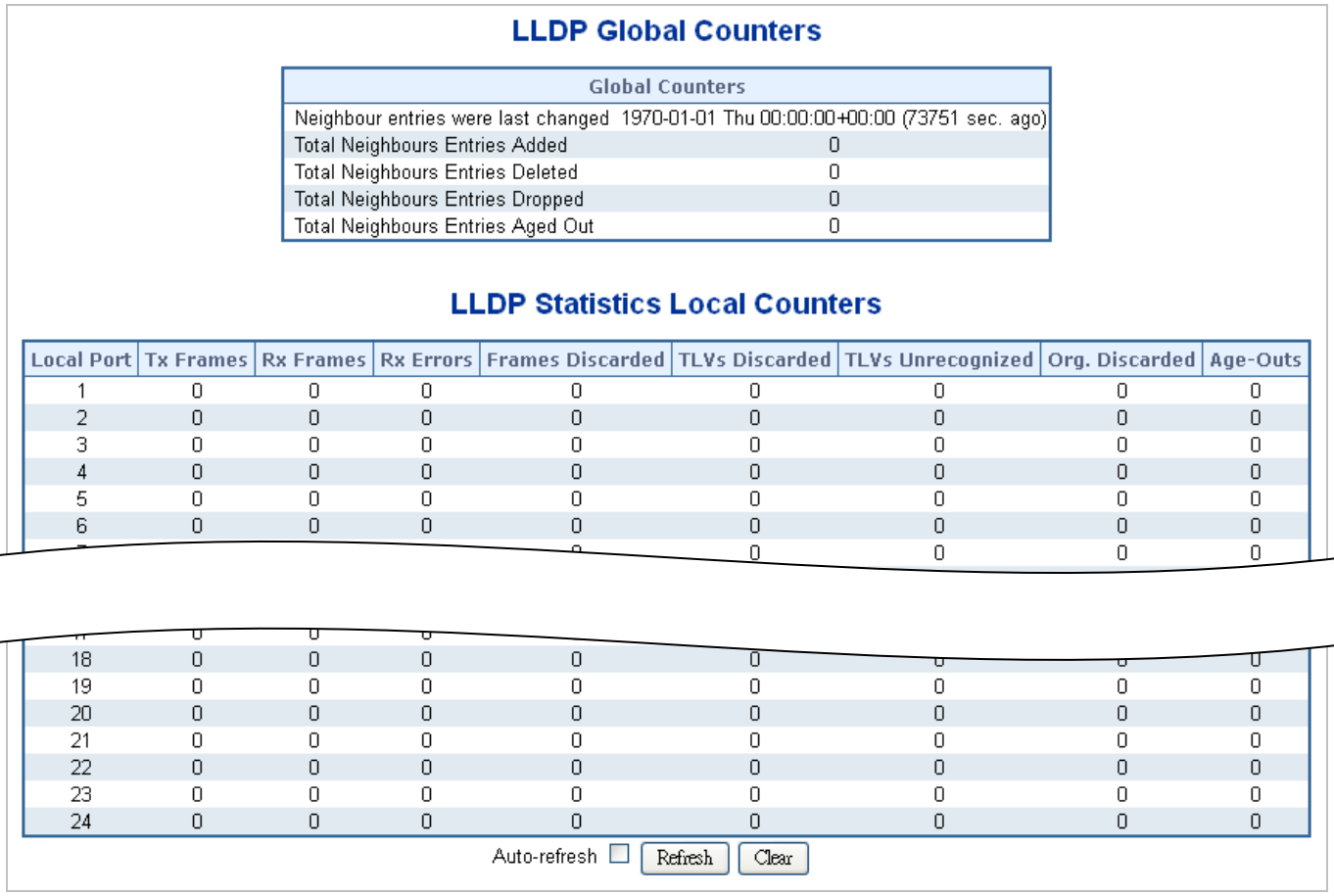
버튼 안내

Refresh: 페이지를 새로고칩니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

3.14.6 Port Statistics

페이지는 모든 LLDP 트래픽의 개요를 제공합니다. 두 종류의 카운터가 표시됩니다. 글로벌 카운터는 전체 스택을 나타내는 카운터이며, 로컬 카운터는 현재 선택된 스위치의 카운터를 나타냅니다. 그림 4-14-5 의 LLDP Statistics (LLDP 통계) 화면이 나타납니다..



LLDP Global Counters

Global Counters	
Neighbour entries were last changed	1970-01-01 Thu 00:00:00+00:00 (73751 sec. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours 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
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0

Auto-refresh Refresh Clear

그림 4-14-5 LLDP Statistics 페이지 화면

다음과 같은 기능을 소개합니다.

Global Counters

기능	설명
• **Neighbor entries were last changed**	마지막 항목이 마지막으로 삭제되거나 추가 된 시간도 표시됩니다. 또한 마지막 변경이 감지 된 이후 경과 된 시간을 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**	항목 테이블이 가득 차서 삭제 된 LLDP 프레임 수를 나타냅니다.

• **Total Neighbors Entries Aged Out**	TTL (Time-To-Live) 만료로 인해 삭제 된 항목 수를 표시합니다.

로컬 카운터

표시된 표에는 각 포트에 대한 행이 들어 있습니다. 열에는 다음 정보가 들어 있습니다.:

기능	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 테이블이 가득차면 LLDP 프레임은 카운트되고 폐기됩니다. 이 상황을 LLDP 표준에서 "너무 많은 이웃"이라고합니다. 섀시 ID 또는 원격 포트 ID 가 테이블에 아직 포함되어 있지 않으면 LLDP 프레임에 테이블에 새 항목이 필요합니다. 주어진 포트가 연결될 때, LLDP 종료 프레임을 수신 할 때 또는 항목이 오래 될 때 테이블에서 항목이 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**	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 안내

Refresh: 페이지를 새로고칩니다.

Clear: 로컬 카운터를 지웁니다. 모든 카운터 (글로벌 카운터 포함)는 재부팅시 지워집니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

3.15 네트워크 진단

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 사항을 표시하고 구성하십시오. 시스템 아래에서 시스템 정보를 구성하고 볼 수있는 다음 항목이 제공됩니다.
이 섹션에는 다음 항목이 있습니다.

핑
IPv6 Ping
원격 IP 핑
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.

케이블 진단

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 모드의 트위스티드 페어 인터페이스에 링크가 설정된 경우 링크 또는 데이터 전송을 중단하지 않고도 케이블 진단을 실행할 수 있습니다.

링크가 100Base-TX 또는 10Base-T 에 설정된 경우, 케이블 진단은 진단이 실행되는 동안 링크가 끊어지도록합니다.
진단이 끝나면 링크가 다시 설정됩니다. 그리고 다음과 같은 기능을 사용할 수 있습니다.

케이블 쌍 사이의 커플 링.
케이블 쌍 종단
케이블 길이

3.15.1 Ping

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. 페이지는 모든 패킷에 대한 응답이 수신되거나 시간이 초과 될 때까지 자동 새로고침됩니다. 그림 4-15-1 의 ICMP Ping 화면이 나타납니다.

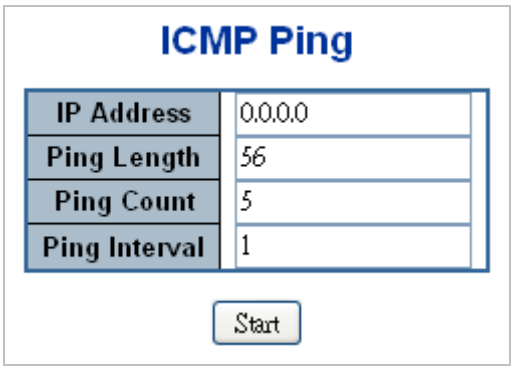


그림 4-15-1 ICMP Ping 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **IP Address**	목적지 IP 주소.
• **Ping Length**	ICMP 패킷의 페이로드 크기입니다. 값의 범위는 2 바이트에서 1452 바이트입니다.
• **Ping Count**	ICMP 패킷의 수. 값의 범위는 1 에서 60 까지입니다.
• **Ping Interval**	ICMP 패킷의 간격. 값의 범위는 0 초에서 30 초 사이입니다

Note

대상 IP 주소가 스위치의 동일한 네트워크 서브넷 내에 있거나 올바른 게이트웨이 IP 주소를 설정했는지 확인하십시오.

버튼 안내

Start: ICMP 패킷을 전송하려면 클릭하십시오.

New Ping: 핑 테스트를 다시시작합니다.

3.15.2 IPv6 Ping

이 페이지에서 ICMPv6 PING 패킷을 발행하여 IPv6 연결 문제를 해결할 수 있습니다.

"시작"을 누르면 5 개의 ICMPv6 패킷이 전송되고 응답을 받으면 순번과 왕복 시간이 표시됩니다. 페이지는 모든 패킷에 대한 응답이 수신되거나 시간이 초과 될 때까지 자동으로 새로 고침됩니다. 그림 4-15-2 의 ICMPv6 Ping 화면이 나타납니다..

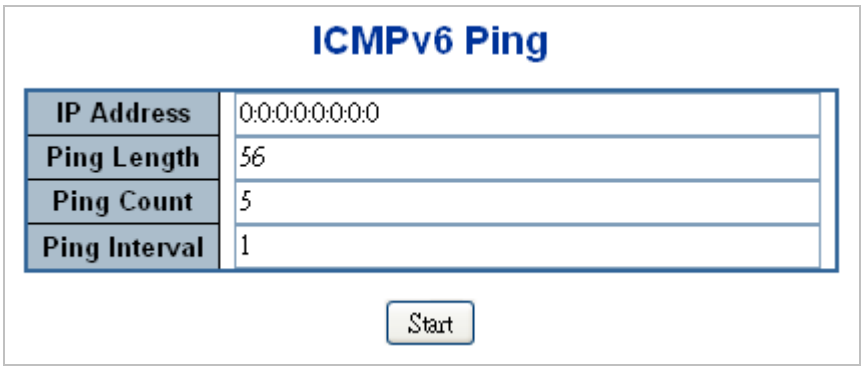


그림 4-15-2 ICMPv6 Ping 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **IP Address**	목적지 IP 주소.
• **Ping Length**	ICMP 패킷의 페이로드 크기입니다. 값의 범위는 2 바이트에서 1452 바이트입니다.
• **Ping Count**	ICMP 패킷의 수. 값의 범위는 1 에서 60 까지입니다.
• **Ping Interval**	ICMP 패킷의 간격. 값의 범위는 0 초에서 30 초 사이입니다.

버튼 안내

Start: ICMP 패킷을 전송하려면 클릭하십시오.

New Ping: PING 으로 진단을 다시 시작하려면 클릭하십시오.

3.15.3 원격 Ping 테스트

이 페이지에서는 ICMP PING 패킷을 실행하여 특수 포트에서 IP 연결 문제를 해결할 수 있습니다.

"Test"를 누르면 5 개의 ICMP 패킷이 전송되고 응답을 받으면 순번과 왕복 시간이 표시됩니다. 페이지는 모든 패킷에 대한 응답이 수신되거나 시간이 초과 될 때까지 자동으로 새로 고침됩니다. 그림 4-15-3 의 ICMP Ping 화면이 나타납니다.

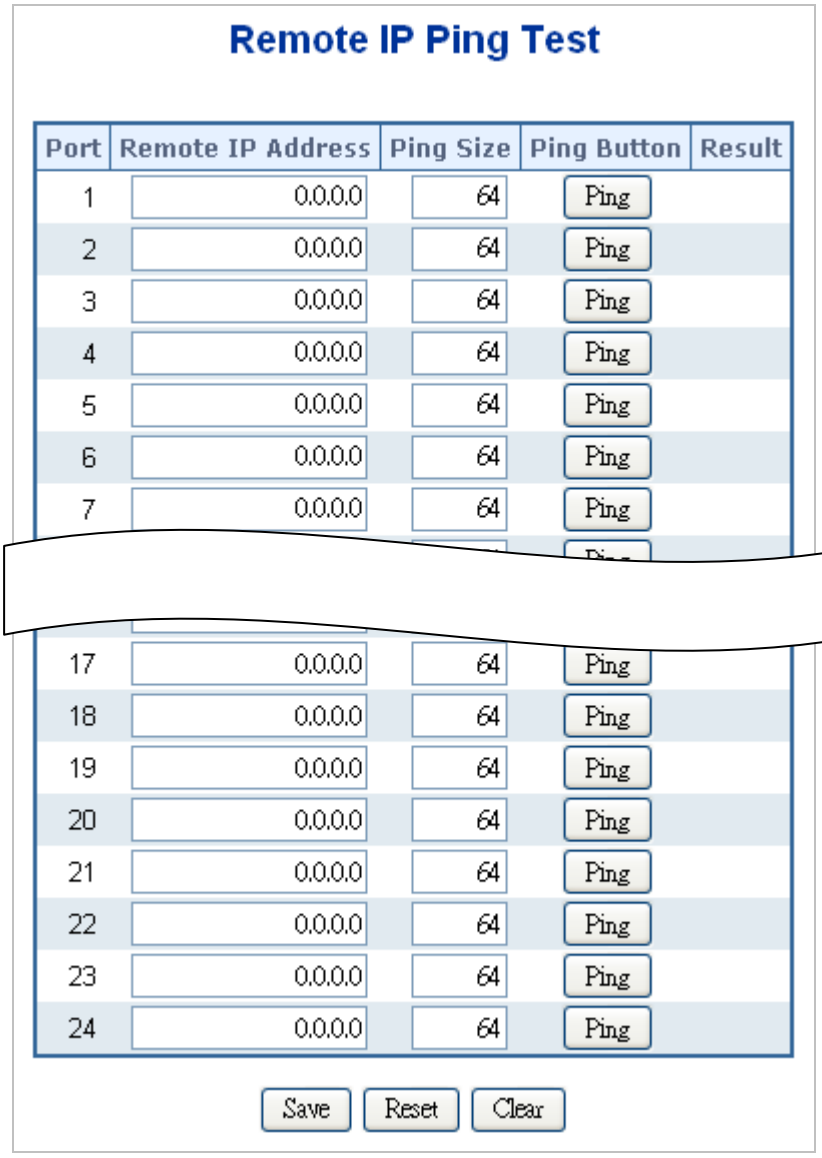


그림 4-15-3 Remote IP Ping Test 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Port**	설정에 대한 논리 포트입니다.
• **Remote IP Address**	목적지 IP 주소.
• **Ping Size**	ICMP 패킷의 페이로드 크기입니다. 값의 범위는 8 바이트에서 1400 바이트입니다.
• **Result**	ping 결과를 표시합니다.

3.15.4 케이블 진단

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. 포트는 페이지 헤더에 반영된대로 현재 선택된 스택 단위에 속합니다. 그림 4-15-4 의 VeriPHY 케이블 진단 화면이 나타납니다.

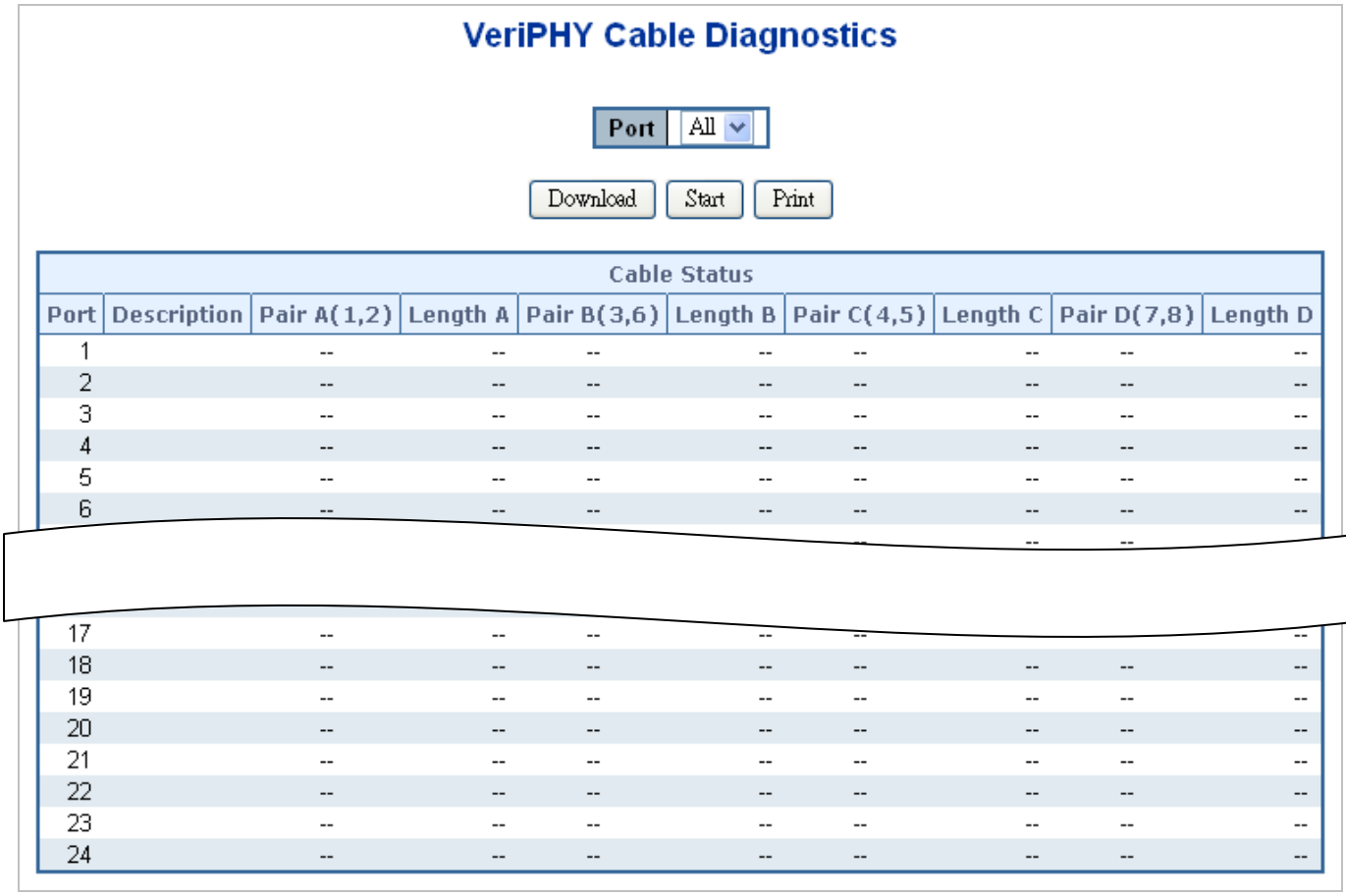


그림 4-15-4 VeriPHY Cable Diagnostics 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Port**	케이블 진단을 요청하는 포트.
• **Cable Status**	**Port**: 포트번호

	Pair: 케이블 쌍의 상태. OK - 올바르게 종료 된 쌍 Open - 열기 쌍 Short - 쇼트 페어 Short A - A 와 교차 하는 짧은 페어 Short B - B 와 교차 하는 짧은 페어 Short C - C 와 교차 하는 짧은 페어 Short D - D 와 교차 하는 짧은 페어 Cross A - 비정상교차 하는 페어 A Cross B - 비정상교차 하는 페어 B Cross C - 비정상교차 하는 페어 C Cross D - 비정상교차 하는 페어 D **Length**: 케이블 쌍의 길이 (미터). 최상도는 3 미터입니다.

버튼 안내

Start: 진단을 시작합니다.

3.16 Loop Protection

이 장에서는 루프 보호를 제공하는 루프 보호 기능을 사용하여 SFC4000T 의 브로드 캐스트 루프를 방지하는 방법에 대해 설명합니다.

3.16.1 설정

이 페이지에서는 사용자가 현재 Loop Protection 구성을 검사 할 수 있으며, 가능하면이를 변경할 수도 있습니다.
그림 4-16-1 의 화면이 나타납니다.

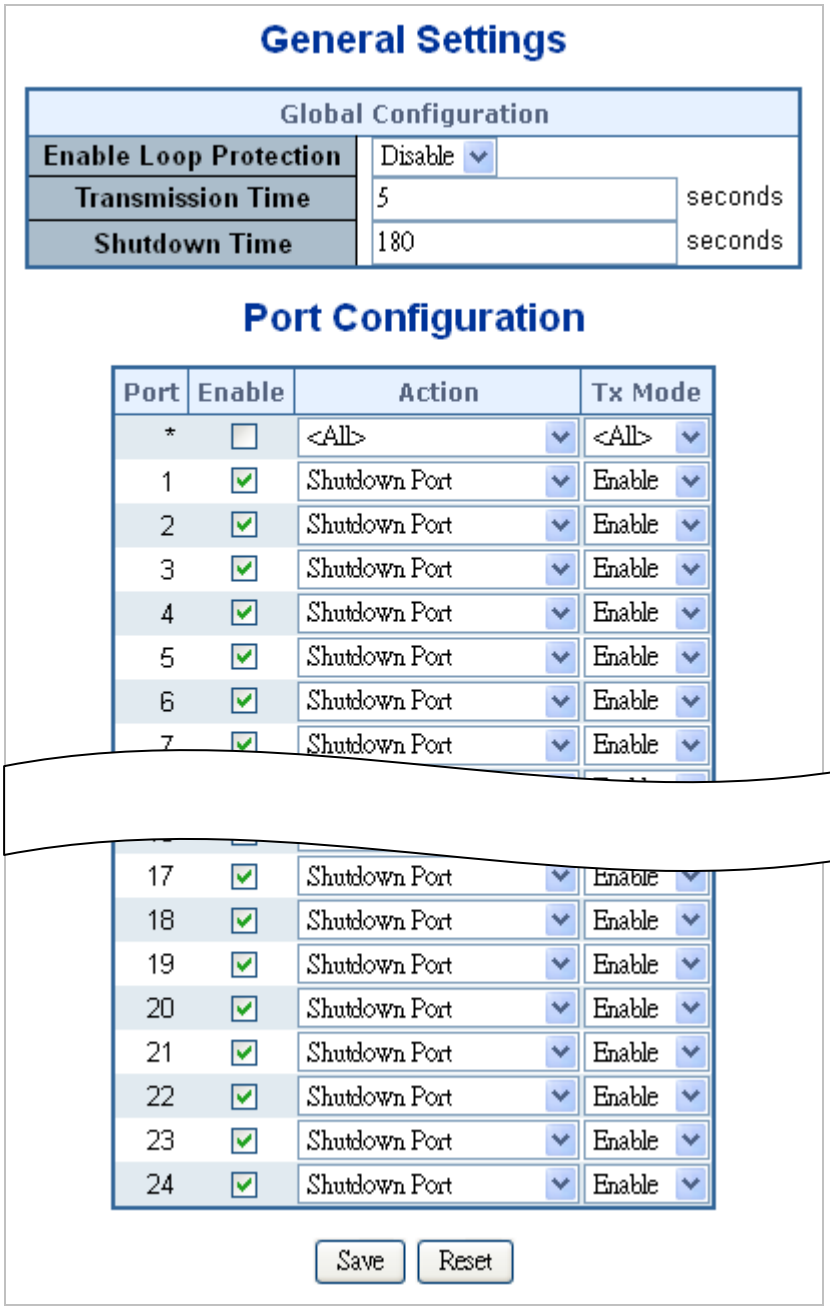


그림 4-16-1 Loop protection 구성화면

다음과 같은 기능을 소개합니다.

일반 설정

기능	설명
• **Enable Loop Protection**	루프 보호를 활성화할지 여부를 제어합니다 (전체적으로).
• **Transmission Time**	각 포트에서 전송 된 각 루프 보호 PDU 사이의 간격입니다. 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 (다음 장치를 다시 시작할 때까지).

포트 설정

기능	설명
• **Port**	포트의 스위치 포트 번호입니다.
• **Enable**	스위치 포트에서 루프 보호를 활성화할지 여부를 제어합니다.
• **Action**	루프가 포트에서 감지 될 때 수행되는 작업을 구성합니다. 유효한 값은 Shutdown Port (종료 포트), 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 안내

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.16.2 Loop Protection Status

이 페이지는 그림 4-16-2 의 스위치의 포트, 루프 보호 포트 상태를 표시합니다.

그림 4-16-2 Loop protection status 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Port**	논리 포트의 스위치 포트 번호입니다.
• **Action**	현재 구성된 포트 동작입니다.
• **Transmit**	현재 구성된 포트 전송 모드입니다.
• **Loops**	이 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 안내

Refresh: 페이지를 새로고칩니다.

Auto-refresh : 페이지에 대한 주기적인 새로고침을 자동으로 이행합니다.

3.17 sFlow

sFlow (RFC 3176)는 표준 네트워크 내보내기를 기반으로하는 프로토콜로 InMon Company 에서 개발 한 네트워크 트래픽 정보를 모니터링하는 데 사용됩니다. 모니터링 된 스위치 또는 라우터는 샘플링 및 통계와 같은 주요 작업을 통해 클라이언트 분석기로 날짜를 전송 한 다음 분석기는 사용자 요구 사항에 따라 네트워크를 모니터링합니다.

sFlow 모니터 시스템에는 sFlow 프록시, 중앙 데이터 수집기 및 sFlow 분석기가 포함됩니다. sFlow 프록시는 샘플링 기술을 사용하여 스위치에서 데이터를 수집합니다. sFlow 수집기는 sFlow 분석기로 전달 될 샘플 데이터 통계를 형식화하여 샘플 데이터를 분석하고 결과에 따라 해당 측정을 수행합니다. 여기서 스위치는 sFlow 시스템의 프록시 및 중앙 데이터 수집기 역할을합니다. 우리는 데이터 샘플링과 통계 포트 물리적 포트를 달성했습니다.

우리의 데이터 샘플은 IPv4 및 IPv6 패킷을 포함합니다. 지금까지 다른 유형의 확장은 지원되지 않습니다. 비 IPv4 및 IPv6 패킷의 경우, RFC 3176 의 요구 사항에 따라 통합 헤더 모드가 채택되어 프로토콜의 유형을 분석하여 패킷의 헤드 정보를 복사합니다.

InMon Company 가 발표 한 최신 sFlow 프로토콜은 버전 5 입니다. RFC3176 에서 구현 된 버전 4 이므로 구조 및 패킷 형식과 같은 버전 충돌이있을 수 있습니다. 이것은 버전 5 가 공식 프로토콜이 아니기 때문에 현재 응용 프로그램과 호환되도록 RFC3176 을 계속 따라 가게됩니다..

3.17.1 sFlow Configuration

이 페이지에서는 sFlow 를 구성 할 수 있습니다. 구성은 두 부분으로 나뉩니다. sFlow 수신기 (a.k.a. sFlow 수집기) 구성 및 포트 별 흐름 및 카운터 샘플러 구성.
sFlow 구성은 비 휘발성 메모리에 유지되지 않습니다. 다시 부팅하면 sFlow 샘플링이 비활성화됩니다. 그림 4-17-1 의 화면이 나타납니다.

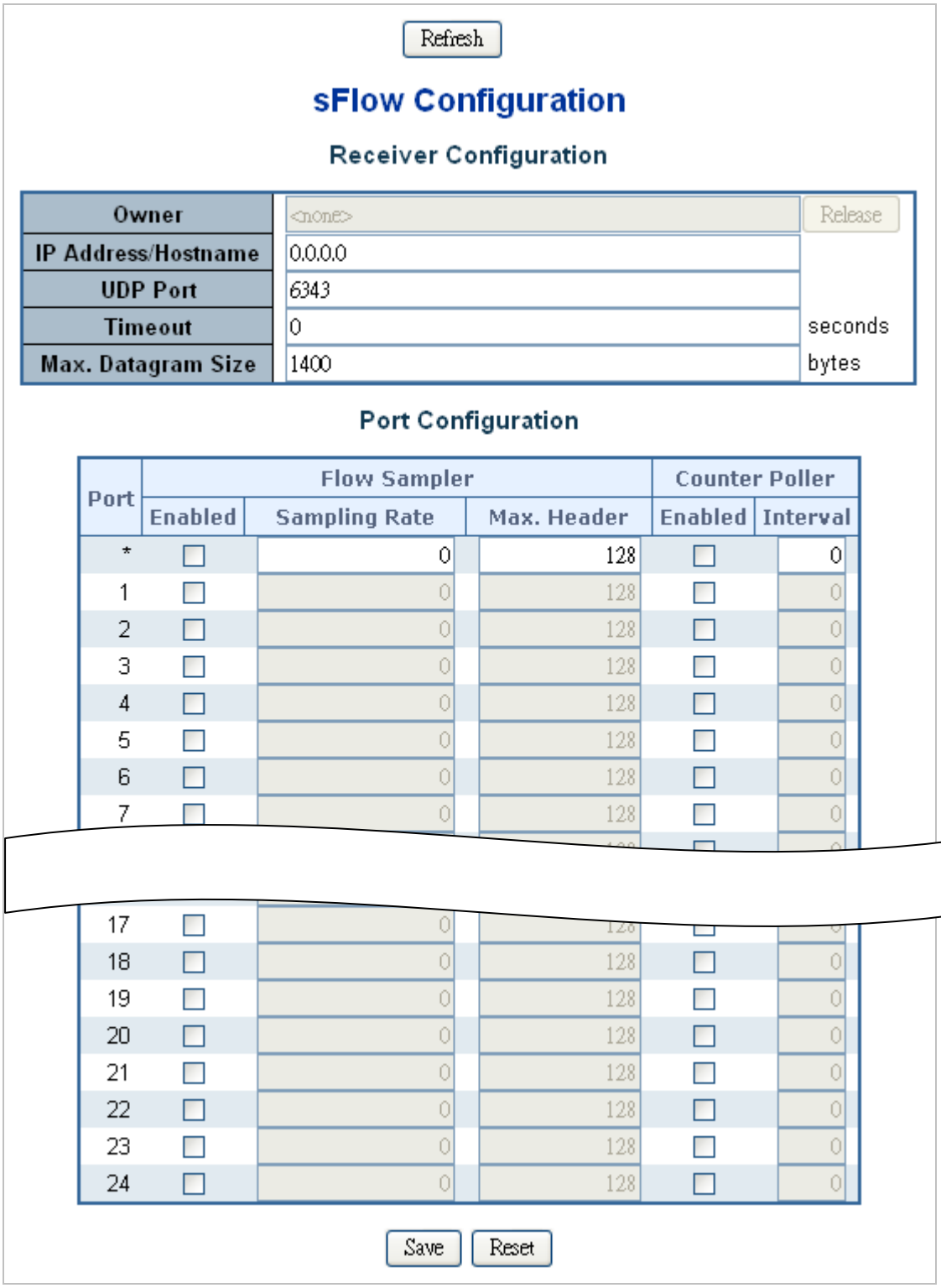


그림 4-17-1 sFlow 구성화면

다음과 같은 기능을 소개합니다.

Receiver Configuration

기능	설명

• **Owner**	기본적으로 sFlow 는 웹 또는 CLI 인터페이스 또는 SNMP 를 통한 로컬 관리를 통해 두 가지 방식으로 구성 할 수 있습니다. 이 읽기 전용 필드는 현재 sFlow 구성의 소유자를 표시하며 값은 다음과 같이 가정합니다. • sFlow 가 현재 구성 해제 / 청구되지 않은 경우 소유자는 <없음>을 포함합니다. • sFlow 가 현재 웹 또는 CLI 를 통해 구성되어있는 경우 소유자는 <로컬 관리를 통해 구성 됨>을 포함합니다. • sFlow 가 현재 SNMP 를 통해 구성된 경우 소유자는 sFlow 수신기를 식별하는 문자열을 포함합니다. SNMP 를 통해 sFlow 를 구성하면 실수로 재구성되는 것을 방지하기 위해 릴리스 버튼을 제외한 모든 컨트롤이 비활성화됩니다.. Refresh 버튼을 허용하여 현재 소유자를 해제하고 sFlow 샘플링을 비활성화 할 수 있습니다. sFlow 가 현재 청구되지 않은 경우 버튼이 비활성화됩니다. SNMP 를 통해 구성된 경우 릴리스를 확인해야합니다 (확인 요청이 표시됨).
• **IP Address/Hostname**	sFlow 수신기의 IP 주소 또는 호스트 이름. IPv4 및 IPv6 주소가 모두 지원됩니다.
• **UDP Port**	sFlow 수신기가 sFlow 데이터 그램을 수신하는 UDP 포트입니다. 0 으로 설정하면 기본 포트 (6343)가 사용됩니다.
• **Timeout**	샘플링이 중지되고 현재 sFlow 소유자가 해제되기까지 남은 시간 (초). 활성화 된 상태에서 새로 고침 버튼을 클릭하면 남아있는 현재 시간을 업데이트 할 수 있습니다. 로컬로 관리되는 경우 다른 설정에는 영향을 미치지 않고 즉시 타임 아웃을 변경할 수 있습니다.
• **Max. Datagram Size**	단일 샘플 데이터 그램에서 전송할 수있는 최대 데이터 바이트 수입니다. 이 값은 sFlow 데이터 그램의 단편화를 방지하는 값으로 설정되어야합니다. 유효한 범위는 200 ~ 1468 바이트이며 기본값은 1400 바이트입니다.

Port Configuration

기능	설명
• Port	아래 구성이 적용되는 포트 번호입니다.
• **Flow Sampler Enabled**	포트에서 플로우 샘플링을 활성화 / 비활성화합니다.
• **Flow Sampler Sampling Rate**	패킷 샘플링의 통계 샘플링 속도. 포트에서 전송 / 수신 된 패킷의 평균 1 / Nth 에서 샘플링하려면 N 으로 설정하십시오. 모든 샘플링 속도를 달성 할 수있는 것은 아닙니다. 지원되지 않는 샘플링 속도가 요청되면 스위치는 자동으로 가장 가까운 샘플링 속도로 조정합니다.

	이 필드에 다시보고됩니다.
• **Flow Sampler Max. Header**	샘플링 된 패킷에서 sFlow 데이터 그램으로 복사해야하는 최대 바이트 수입니다. 유효한 범위는 14 ~ 200 바이트이며 기본값은 128 바이트입니다. 최대 데이터 그램 크기가 최대 헤더 크기를 고려하지 않으면 샘플이 삭제 될 수 있습니다.
• **Counter Poller Enabled**	포트에서 카운터 폴링을 활성화 / 비활성화합니다.
• **Counter Poller Interval**	카운터 폴링이 활성화되면 카운터 폴러 샘플 간의 간격 (초)을 지정합니다.

버튼 안내

Release: 자신의 아래 설명을 확인합니다.

Refresh: 새로고침을 합니다. 저장하지 않은 변경 사항은 손실됩니다.

Save: 변경내용을 저장합니다 sFlow 구성은 비 휘발성 메모리에 유지되지 않습니다.Reset: 이전의 저장값으로 되돌립니다.

3.17.2 sFlow Status

페이지는 수신기 및 포트 별 sFlow 통계를 보여 주며 그림 4-17-2 의 화면이 나타납니다.

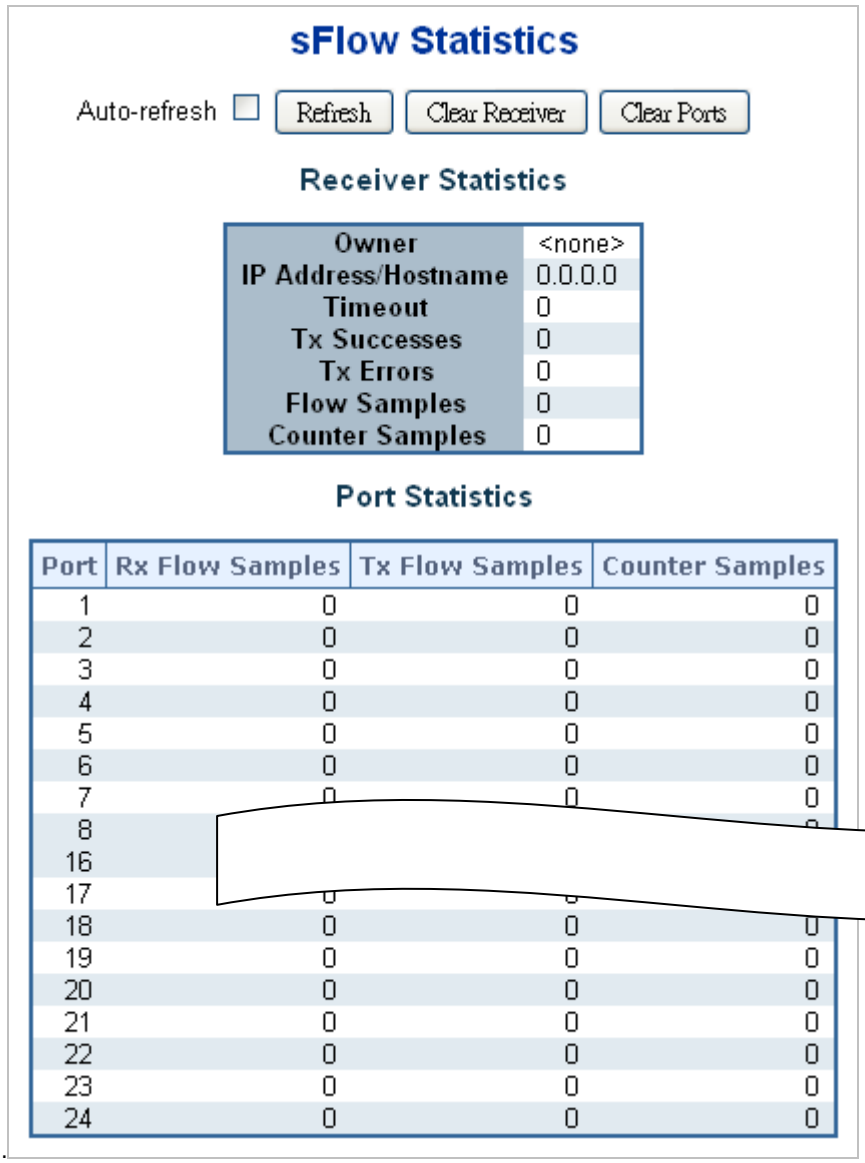


그림 4-17-2 sFlow Statistics 페이지 화면

다음과 같은 기능을 소개합니다.

Receiver Statistics

기능	설명
• **Owner**	이 필드는 sFlow 구성의 현재 소유자를 표시합니다. 다음 세 가지 값 중 하나를 가정합니다.: • sFlow 가 현재 구성 해제 / 청구되지 않은 경우 소유자는 <없음>을 포함합니다. • sFlow 가 현재 웹 또는 CLI 를 통해 구성되어있는 경우 소유

	<지역 관리를 통한 구성 >. •sFlow 가 현재 SNMP 를 통해 구성된 경우 소유자는 sFlow 수신기를 식별하는 문자열을 포함합니다.
• **IP Address/Hostname**	sFlow 수신기의 IP 주소 또는 호스트 이름.
• **Timeout**	샘플링이 중지되고 현재 sFlow 소유자가 해제되기까지 남은 시간 (초).
• **Tx Successes**	sFlow 수신기에 성공적으로 전송 된 UDP 데이터 그램의 수
• **Tx Errors**	가장 일반적인 오류 소스는 잘못된 sFlow 수신기 IP / 호스트 이름 구성입니다. 진단하려면 수신자의 IP 주소 / 호스트 이름을 Ping 웹 페이지 (진단 → Ping / Ping6)에 붙여 넣으십시오
• **Flow Samples**	sFlow 수신기로 전송 된 총 유량 샘플 수입니다.
• **Counter Samples**	sFlow 수신기로 보낸 카운터 샘플의 총 수.

Port Statistics

기능	설명
• **Port**	다음 통계가 적용되는 포트 번호입니다.
• **Rx and Tx Flow Samples**	이 포트에서 시작된 sFlow 수신기로 전송 된 플로우 샘플의 수. 여기에서 플로우 샘플은 Rx 및 Tx 플로우 샘플로 나뉩니다. 여기서 Rx 플로우 샘플은 포트에서 수신 (수신) 할 때 샘플링 된 패킷 수를 포함하고 Tx 플로우 샘플은 송신시 샘플링 된 패킷 수를 포함합니다
• **Counter Samples**	포트에서 발생한 sFlow 수신기로 보내진 카운터 샘플의 총 수.

버튼 안내

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

Refresh: 새로고침을 합니다.

Clear Receiver: sFlow 수신기 카운터를 지웁니다.

Clear Ports: 포트 별 카운터를 지웁니다.

3.18 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.

3.18.1 RMON 알람 설정

이 페이지에서 RMON 경보 표를 구성하십시오. 엔트리 인덱스 키는 ID 입니다.; 그림 4-18-1 의 화면이 나타납니다..

그림 4-18-1 RMON Alarm 구성화면

다음과 같은 기능을 소개합니다.

기능	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**: 프레이밍 문자를 포함하여 인터페이스에서 수신 한 총 8 진수. **InUcastPkts**: 상위 계층 프로토콜에 전달되는 유니 캐스트 패킷의 수. **InNUcastPkts**: 상위 계층 프로토콜로 전달되는 브로드 캐스트 및 멀티 캐스트 패킷 수입니다 **InDiscards**: 패킷이 정상적 일 때라도 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**: 프레이밍 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 삭제되는 아웃 바운드 패킷 수입니다. **OutErrors**: 오류로 인해 전송할 수없는 아웃 바운드 패킷 수입니다. **OutQLen**: 출력 패킷 대기열의 길이 (패킷 단위).
• **Sample Type**	선택한 변수를 샘플링하고 임계 값과 비교할 값을 계산하는 방법, 가능한 샘플 유형은 다음과 같습니다.: **Absolute**: 샘플을 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: **Rising** 첫 번째 값이 상승 임계 값보다 클 때 경보를 트리거합니다. **Falling** 첫 번째 값이 하한 임계 값보다 작 으면 알람을 트리거합니다. **RisingOrFalling** 첫 번째 값이 상승 임계 값보다 크거나 하강 임계 값보다 작 으면 (기본값) 알람을 트리거합니다.
• **Rising Threshold**	상승 임계 값 (-2147483648-2147483647).
• **Rising Index**	상승 이벤트 색인 (1-65535).
• **Falling Threshold**	하강 임계 값 (-2147483648-2147483647)
• **Falling Index**	이벤트 지수 하락 (1-65535).

버튼 안내

Add New Entry: 새 커뮤니티 항목을 추가하려면 클릭하십시오.

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.18.2 RMON Alarm Detail

페이지는 특정 RMON 통계 항목의 세부 정보를 제공합니다. 그림 4-18-2 의 화면이 나타납니다.

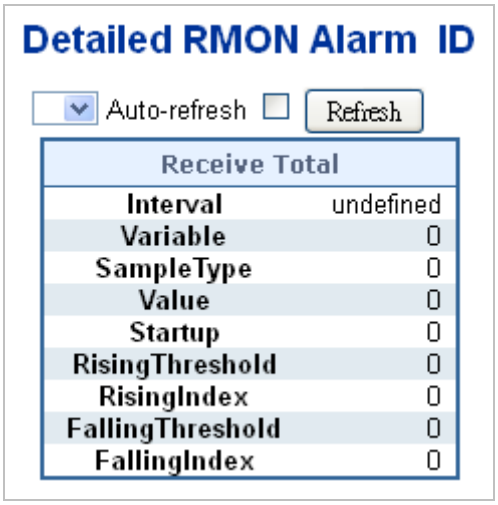


그림 4-18-2 Detailed RMON Alarm ID 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **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**	항목이 처음 유효한 것으로 설정된 경우 보낼 수있는 알람입니다.
• **Rising Threshold**	상승 임계 값.
• **Rising Index**	상승 이벤트 인덱스.
• **Falling Threshold**	떨어지는 임계 값.
• **Falling Index**	떨어지는 이벤트 색인.

버튼 안내

Refresh: 페이지를 새로고칩니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

<<:. 가장 낮은 ID 를 가진 항목 인 Alarm Table 의 첫 번째 항목부터 시작하여 테이블을 업데이트합니다.

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

3.18.3 RMON Alarm Status

페이지는 RMON 알람 항목의 개요를 제공합니다. 각 페이지는 "페이지 당 입력"입력 필드를 통해 선택된 알람 테이블에서 최대 99 개의 항목 (기본값은 20)을 표시합니다. 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 4-18-3 의 화면이 나타납니다..

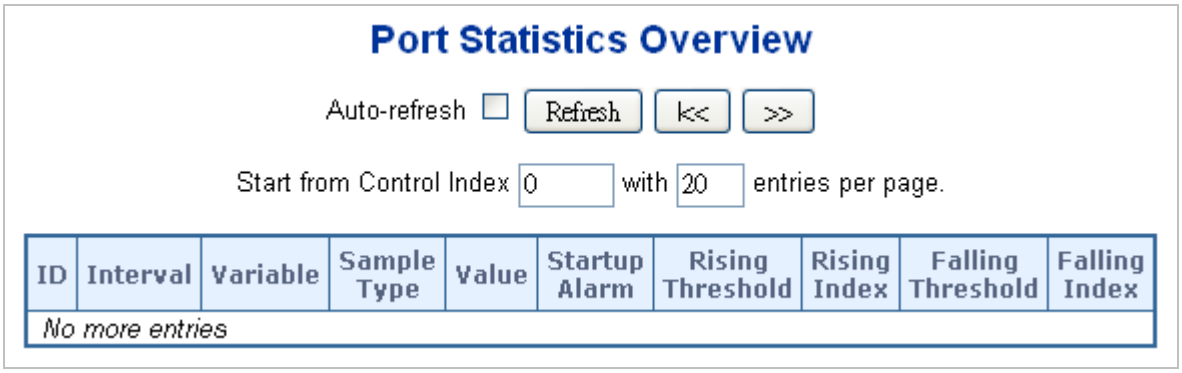


그림 4-18-3 Port Statistics Overview 페이지 화면

다음과 같은 기능을 소개합니다.

기능	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**	상승 임계 값.
• **Rising Index**	상승 이벤트 인덱스.

• **Falling Threshold**	떨어지는 임계 값.
• **Falling Index**	떨어지는 이벤트 색인.

버튼 안내

Refresh: 페이지를 새로고칩니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

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

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

3.18.4 RMON Event Configuration

페이지에서 RMON 이벤트 테이블을 구성하십시오. 엔트리 인덱스 키는 ID 입니다. 그림 4-18-4 의 화면이 나타납니다.

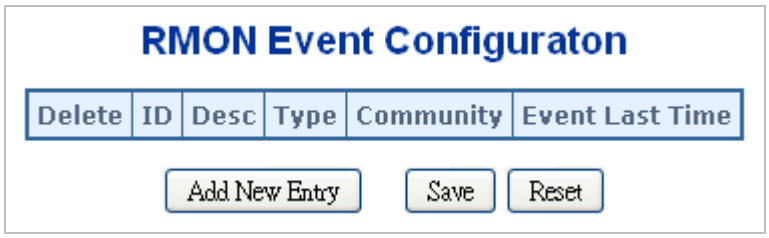


그림 4-18-4 RMON event 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Delete**	항목을 삭제하려면 선택하십시오. 다음 저장 중에 삭제됩니다.
• **ID**	항목의 색인을 나타냅니다. 범위는 1 에서 65535 사이입니다.
• **Desc**	이벤트를 나타냅니다. 캐릭터 라인의 길이는 0 ~ 127 이며, 디폴트는 null 입니다.
• **Type**	이벤트의 통지를 나타냅니다. 가능한 타입은 다음과 같습니다. **none**: 프레이밍 문자를 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 일 때라도 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 안내

Add New Entry: 새 커뮤니티 항목을 추가하려면 클릭하십시오.

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.18.5 RMON Event Detail

페이지는 RMON 이벤트 항목의 개요를 제공합니다. 그림 4-18-5 의 화면이 나타납니다.

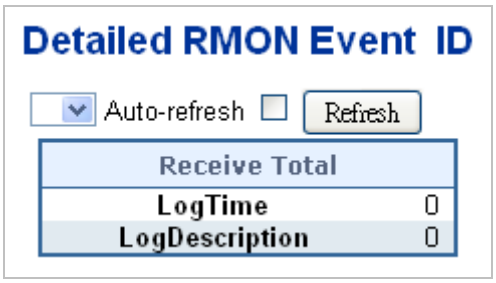


그림 4-18-5 Detailed RMON Event ID 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Event Index**	이벤트 항목의 색인을 나타냅니다.
• **Log Index**	로그 항목의 색인을 나타냅니다.
• **LogTime**	이벤트 로그 시간을 나타냅니다.
• **Logdescription**	이벤트 설명을 나타냅니다.

버튼 안내

Refresh: 페이지를 새로고칩니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

3.18.6 RMON Event Status

이 페이지는 RMON 이벤트 테이블 항목의 개요를 제공합니다. 각 페이지는 "페이지 당 항목 수"입력 필드를 통해 선택된 이벤트 표의 최대 99 개 항목 (기본값은 20)을 표시합니다. 처음 방문했을 때, 웹 페이지는 이벤트 표의 처음부터 처음 20 개의 항목을 보여줍니다. 가장 먼저 표시되는 이벤트 색인 및 로그 색인은 이벤트 테이블에 있습니다. 그림 4-18-6 의 화면이 나타납니다.

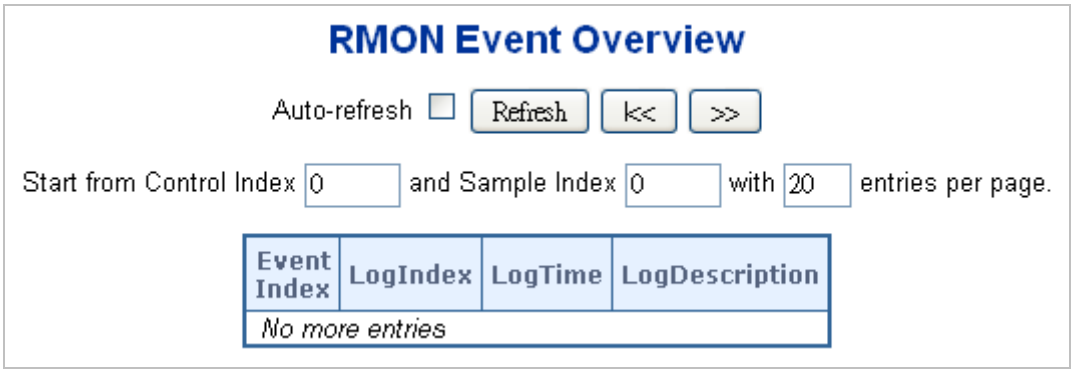


그림 4-18-6 RMON Event Overview 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Event Index**	이벤트 항목의 색인을 나타냅니다.
• **Log Index**	로그 항목의 색인을 나타냅니다.
• **LogTime**	이벤트 로그 시간을 나타냅니다.
• **Logdescription**	이벤트 설명을 나타냅니다.

버튼 안내

Refresh: 페이지를 새로고칩니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

<<: 가장 낮은 ID 를 가진 항목 인 Alarm Table 의 첫 번째 항목부터 시작하여 테이블을 업데이트합니다.

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

3.18.7 RMON History Configuration

이 페이지에서 RMON History 표를 구성하십시오. 엔트리 인덱스 키는 ID 입니다. 그림 4-18-7 의 화면이 나타납니다.

그림 4-18-7 RMON history 구성화면

다음과 같은 기능을 소개합니다.

기능	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. 스태킹 스위치를 사용하는 경우 값이 1000 * (스위치 ID-1)을 추가해야합니다. 예를 들어 포트가 3 번 포트 5 번 스위치 인 경우 값은 2005 입니다.
• **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 안내

Add New Entry: 새 커뮤니티 항목을 추가하려면 클릭하십시오.

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.18.8 RMON History Detail

이 페이지는 RMON 기록 항목에 대한 세부 정보를 제공합니다. 그림 4-18-8 의 화면이 나타납니다.

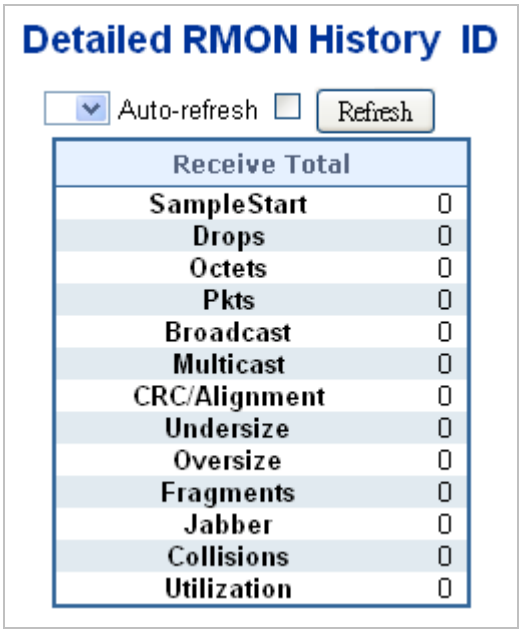


그림 4-18-8 RMON history Detail 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **History Index**	기록 제어 항목의 색인을 나타냅니다.
• **Sample Index**	컨트롤 항목과 연결된 데이터 항목의 인덱스를 나타냅니다.
• **Sample Start**	자원 부족으로 인해 프로브가 패킷을 삭제 한 총 이벤트 수입니다.
• **Drops**	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 , 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.
• **CRCErrors**	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.
• **Fragments**	크기가 유효하지 않은 CRC 로 수신 된 64 옥텟보다 작은 프레임 수입니다.
• **Jabber**	크기가 유효하지 않은 CRC 로 수신 된 64 옥텟보다 큰 프레임 수입니다.

• **Collisions**	이 이더넷 세그먼트의 총 충돌 수를 가장 잘 예측 한 것입니다.
• **Utilization**	샘플링 간격 동안이 인터페이스에서 평균 물리 계층 네트워크 사용률을 가장 잘 예측 한 값입니다 (단위 : 백분율).

버튼 안내

Refresh: 페이지를 새로고칩니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

3.18.9 RMON History Status

이 페이지는 RMON History 항목의 개요를 제공합니다. 각 페이지에는 기록 테이블의 항목이 최대 99 개까지 표시되며 기본값은 20 이고 "페이지 당 항목 수"입력 필드를 통해 선택됩니다. 처음 방문했을 때 웹 페이지는 History 테이블의 처음부터 처음 20 개의 항목을 표시합니다. 처음 표시되는 것은 가장 낮은 히스토리 인덱스 및 샘플 인덱스가 히스토리 테이블에있는 것입니다. 그림 4-18-9 의 화면이 나타납니다.

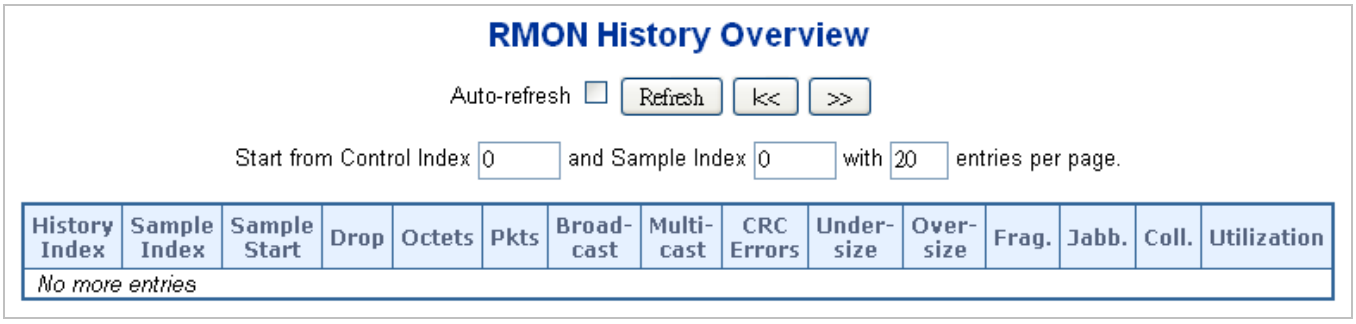


그림 4-18-9 RMON history overview 페이지 화면

다음과 같은 기능을 소개합니다.

기능	설명
• **History Index**	기록 제어 항목의 색인을 나타냅니다.
• **Sample Index**	컨트롤 항목과 연결된 데이터 항목의 인덱스를 나타냅니다.
• **Sample Start**	자원 부족으로 인해 프로브가 패킷을 삭제 한 총 이벤트 수입니다.
• **Drops**	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.
• **CRCErrors**	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.
• **Utilization**	샘플링 간격 동안이 인터페이스에서 평균 물리 계층 네트워크 사용률을 가장 잘 예측 한 값입니다 (단위 : 백분율).

버튼 안내

Refresh: 페이지를 새로고칩니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

<<: 경보 테이블의 첫 항목부터 테이블을 업데이트합니다. 즉 가장 낮은 ID 를 가진 항목을 업데이트합니다.

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

3.18.10 RMON Statistics Configuration

이 페이지에서 RMON Statistics (RMON 통계) 테이블을 구성하십시오. 엔트리 인덱스 키는 ID 입니다

그림 4-18-10 RMON Statistics 구성화면

다음과 같은 기능을 소개합니다.

기능	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. 스태킹 스위치를 사용하는 경우 값이 1000 * (스위치 ID-1)을 추가해야합니다 (예 : 포트가 스위치 3 포트 5 이고 값이 2005 인 경우)

버튼 안내

Add New Entry: 새로운 커뮤니티 엔트리를 추가합니다.

Save: 변경내용을 저장합니다.

Reset: 이전의 저장값으로 되돌립니다.

3.18.11 RMON 상세 통계

이 페이지는 특정 RMON 통계 항목의 세부 정보를 제공합니다. 그림 4-18-11 의 화면이 나타납니다..

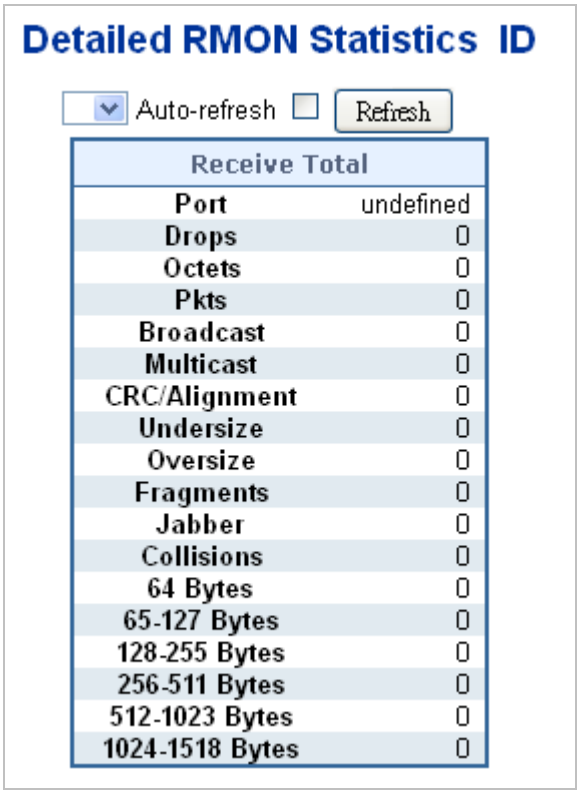


그림 4-18-11 Loop protection 구성화면

다음과 같은 기능을 소개합니다.

기능	설명
• **Data Source**	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, 브로드 캐스트 패킷 및 멀티 캐스트 패킷 포함).
• **Broad-cast**	브로드 캐스트 주소로 향하는 수신 된 양호한 패킷의 총 수.
• **Multi-cast**	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.
• **Under-size**	64 옥텟보다 적게 수신 된 총 패킷 수입니다.
• **Over-size**	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**	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.
• **1024~1588**	길이가 1024 에서 1588 옥텟 사이 인 총 패킷 수 (불량 패킷 포함).

버튼 안내

Refresh: 페이지를 새로고칩니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

3.18.12 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 4-18-12 의 화면이 나타납니다.

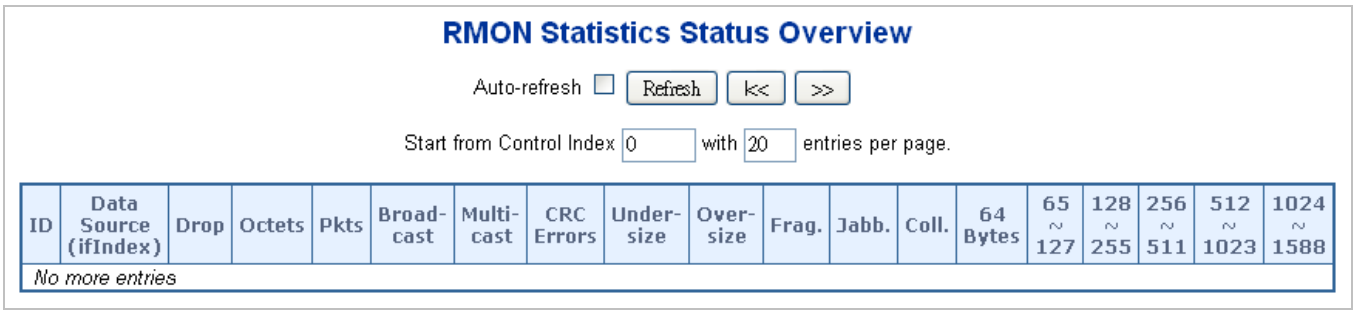


그림 4-18-12 RMON Statistics Status Overview 페이지 화면

다음과 같은 기능을 소개합니다.

기능	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, 브로드 캐스트 패킷 및 멀티 캐스트 패킷 포함).
• **Broad-cast**	브로드 캐스트 주소로 향하는 수신 된 양호한 패킷의 총 수.
• **Multi-cast**	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.
• **Under-size**	64 옥텟보다 적게 수신 된 총 패킷 수입니다. 수신 된 총 패킷 수는 1518 옥텟보다 길었습니다.
• **Over-size**	크기가 유효하지 않은 CRC 로 수신 된 64 옥텟보다 작은 프레임 수입니다.
• **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**	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.
• **1024~1588**	길이가 1024 에서 1588 옥텟 사이 인 총 패킷 수 (불량 패킷 포함).

버튼 안내

Refresh: 페이지를 새로고칩니다.

Auto-refresh : 3 초주기로 페이지를 자동으로 새로고침합니다. .

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

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

4. 인터페이스 명령어 줄

4.1 CLI 접근방법

서버의 콘솔 포트에 직접 연결하거나 텔넷 연결을 통해 스위치의 관리 인터페이스에 액세스 할 때 프롬프트에서 명령 키워드와 매개 변수를 입력하여 스위치를 관리 할 수 있습니다. 스위치의 CLI (명령어-Line Interface) 사용은 UNIX 시스템에 명령을 입력하는 것과 매우 유사합니다.

이 장에서는 CLI (명령 줄 인터페이스)를 사용하는 방법에 대해 설명합니다.

4.1.1 콘솔을 통한 로그온

터미널이 장치에 연결되면 관리 대상 스위치의 전원을 켜고 터미널에 테스트 절차가 실행 중임을 표시합니다.

그런 다음, 다음 메시지는 로그인 사용자 이름 및 암호를 묻습니다. 다음과 같은 공장 기본 암호와 그림 5-1 의 로그인 화면이 나타납니다.

Username: **admin**
Password: **admin**

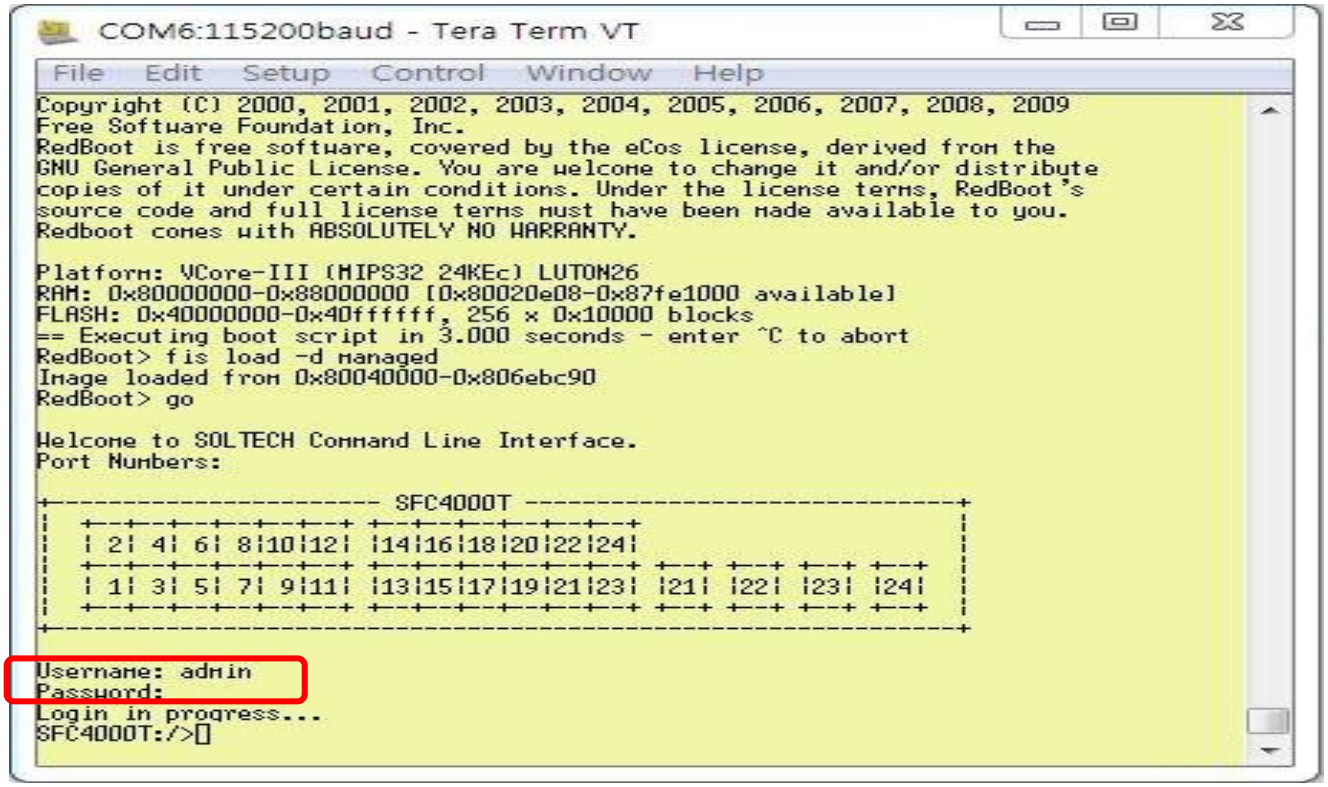


그림 5-1 관리 형 스위치 콘솔 로그인 화면

Note

1. 보안상의 이유로이 첫 번째 설정 후에 새 암호를 변경하고 기억하십시오.
2. 콘솔 인터페이스에서 소문자로 된 명령만 수락하십시오.

4.1.2 IP 주소 구성

SFC4000 관리 스위치는 다음과 같이 기본 IP 주소와 함께 제공됩니다.

IP Address: **192.168.0.100**

Subnet Mask: **255.255.255.0**

스위치의 현재 IP 주소를 확인하거나 새 IP 주소를 수정하려면 다음 절차를 따르십시오.

현재 IP 주소를 표시합니다.

1. "SFC4000T />"프롬프트에서 "ip configuration"을 입력하십시오.

2. 화면에 현재 IP 주소, 서브넷 마스크 및 게이트웨이가 표시됩니다. 그림 5-2 와 같이.

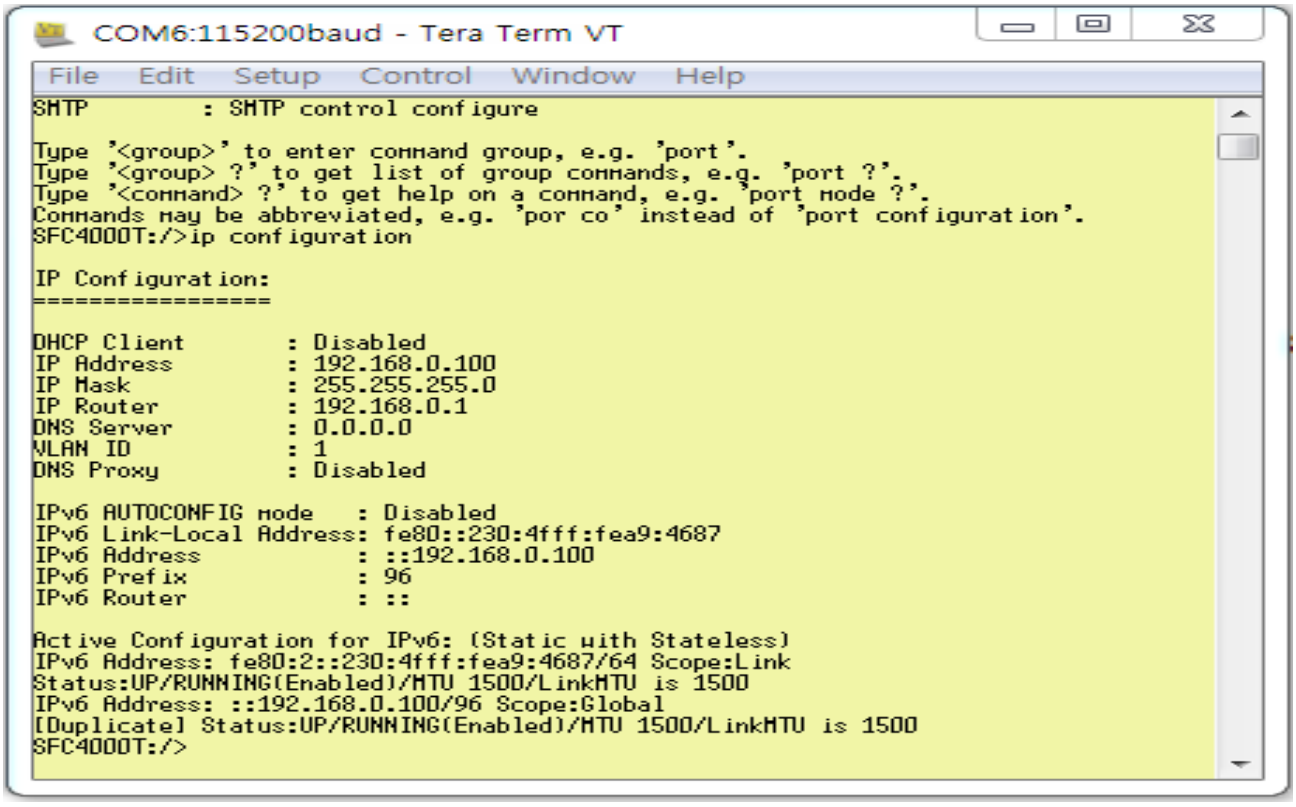


그림 5-2 IP 정보 화면

■ **구성 IP address**

1. "SFC4000T />"프롬프트에서 다음 명령을 입력하고 <Enter> 키를 누릅니다. 그림 5-3 과 같습니다.

SFC4000T/> ip setup 192.168.0.101 255.255.255.0 192.168.0.253 1

이전 명령은 스위치에 대한 다음 설정을 적용합니다.

IP: 192.168.0.101
Subnet Mask: 255.255.255.0
Gateway: 192.168.0.253
VLAN ID: 1

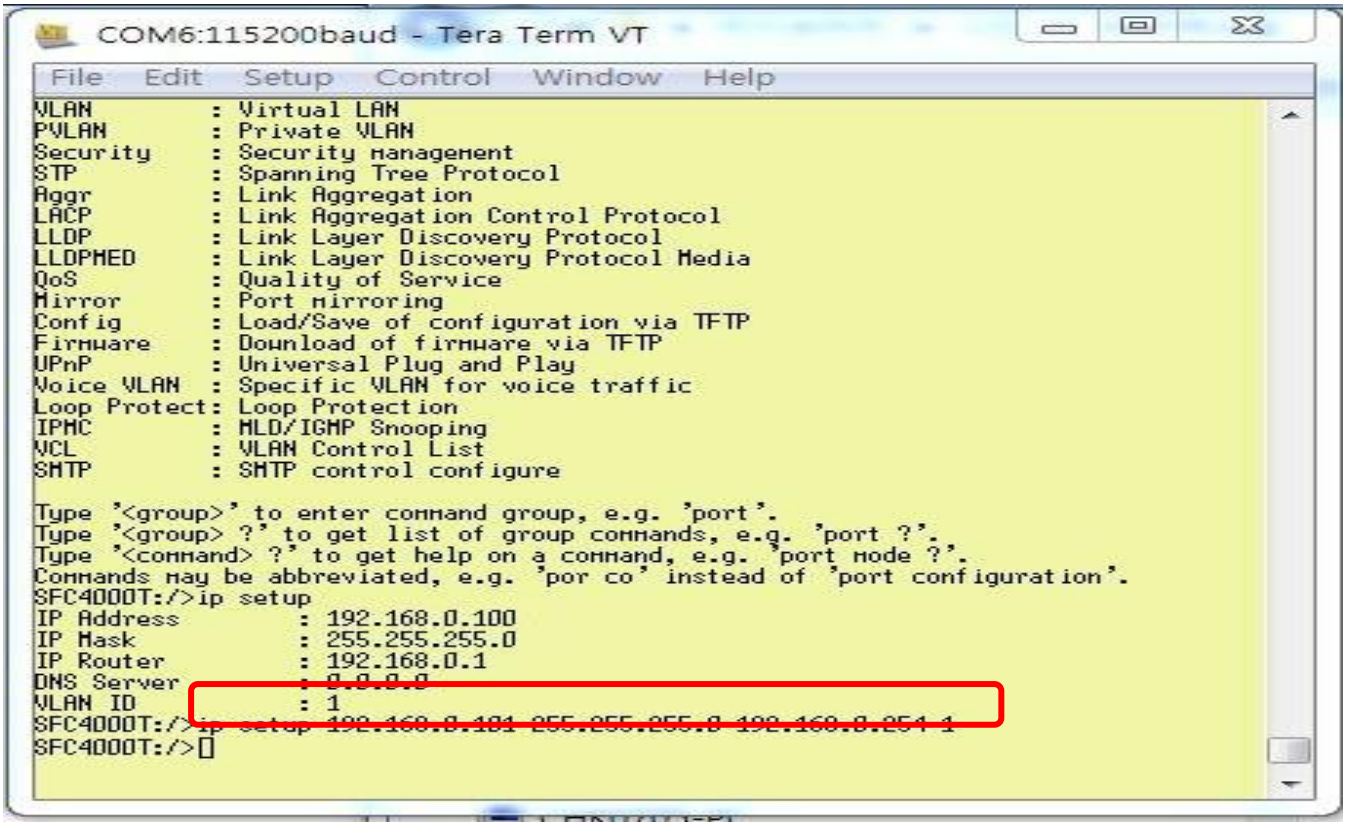


그림 5-3 IP 주소 설정 화면

2. 1 단계를 반복하여 IP 주소가 변경되었는지 확인하십시오. IP 주소가 성공적으로 구성되면 관리 대상 스위치는 새 IP 주소 설정을 즉시 적용합니다. 새 IP 주소를 통해 Managed Switch 의 웹 인터페이스에 액세스 할 수 있습니다.

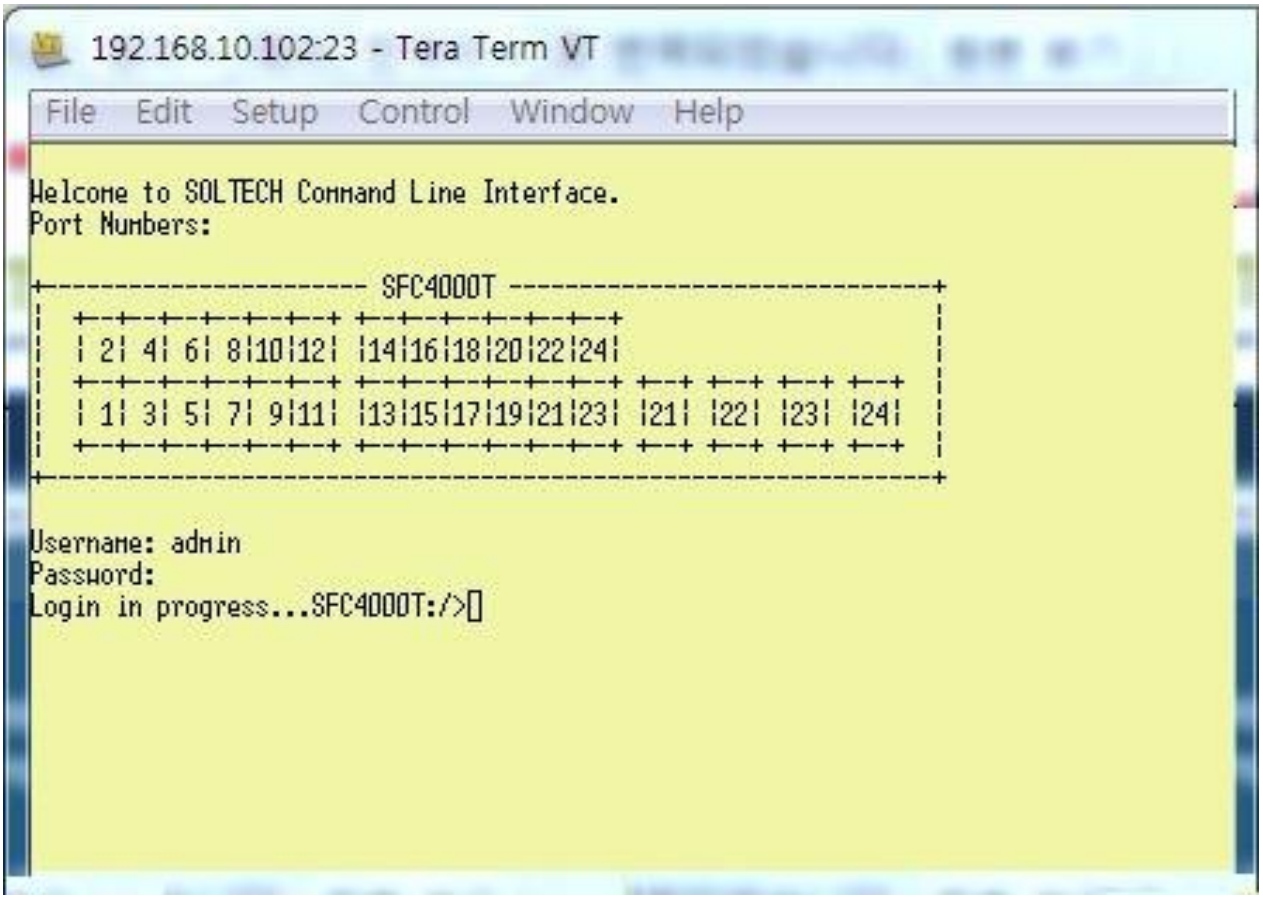
Note

콘솔 명령 또는 관련 매개 변수에 익숙하지 않은 경우, 콘솔에 "help"를 입력하여 도움말을 얻으십시오.

로그온 한 후에 원하는 경우 이러한 설정을 변경할 수 있습니다. 이 관리 방법은 시스템을 다시 부팅하는 동안 연결되어 있고 시스템을 모니터링 할 수 있기 때문에 선호되는 경우가 많습니다. 또한 관련 작업이 시작된 인터페이스에 관계없이 특정 오류 메시지가 직렬 포트로 전송됩니다. Macintosh 또는 PC 연결은 터미널 직렬 포트에 연결하기 위해 터미널 에뮬레이션 프로그램을 사용할 수 있습니다. UNIX 에서 워크 스테이션 첨부는 TIP 와 같은 에뮬레이터를 사용할 수 있습니다.

4.2 Telnet Login

또한 Managed Switch 는 원격 관리를 위해 텔넷을 지원합니다. 텔넷을 사용할 때 스위치는 원격 로그인을 위해 사용자 이름과 암호를 묻습니다. 사용자 이름과 암호는 "admin"을 사용하십시오.



5. 명령어 줄 방식

CLI 는 명령의 특성에 따라 모든 모드를 적절한 모드로 그룹화합니다. CLI 명령 모드의 샘플은 아래에 설명되어 있습니다. 각 명령 모드는 특정 소프트웨어 명령을 지원합니다.

명령어 그룹:

System	System settings and reset options
IP	IP configuration and Ping
Port	Port management
MAC	MAC address table
VLAN	Virtual LAN
PVLAN	Private VLAN
Security	Security management
STP	Spanning Tree Protocol
Aggr	Link Aggregation
LACP	Link Aggregation Control Protocol
LLDP	Link Layer Discovery Protocol
LLDPMED	Link Layer Discovery Protocol Media
QoS	Quality of Service
Mirror	Port mirroring
Config	Load/Save of configuration via TFTP
Firmware	Download of firmware via TFTP
UPnP	Universal Plug and Play
MVR	Multicast VLAN Registration
Voice VLAN	Specific VLAN for voice traffic
Loop Protection	Loop Protection
IPMC	MLD/IGMP Snooping
VLC	VLAN Control List
SMTP	SMTP Control 구성

5.1 시스템 명령어

시스템 설정

설명 :

시스템 구성을 표시하십시오.

통사:

시스템 구성 [all | (포트 <port_list>)]

매개 변수 :

all : 모든 스위치 구성 표시, default : 시스템 구성 표시

port : 스위치 포트 구성 표시

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

시스템 정보를 표시하려면,

```
SFC4000T:/>System configuration
System Contact    :
System Name       : SFC4000T
System Location :
Timezone Offset : 0
MAC Address       : 00-30-4f-11-22-33
System Time       : 1970-01-01 Thu 00:24:39+00:00
System Uptime     : 00:24:39
Software Version: Beta1205281742
Software Date     : 2012-05-28T17:42:57+0800
Previous Restart: Cold
SFC4000T:/>
```

시스템 로그 구성

설명 :

시스템 로그 구성을 표시합니다.

통사:

시스템 로그 구성

예:

시스템 로그 정보를 표시하려면,

```
SFC4000T:/>System log configuration
System Log Configuration:
========================
```

```
System Log Server Mode       : Disabled
System Log Server Address    :
System Log Level             : Info
SFC4000T:/>
```

시스템 버전

설명 :

시스템 버전 정보를 표시합니다.

통사:

시스템 버전

예:

시스템 버전을 표시하려면,

```
SFC4000T:/>System version
Version         : Beta1205281742
Build Date      : 2012-05-28T17:42:57+0800
SFC4000T:/>
```

시스템 로그 서버 모드

설명 :

시스템 로그 서버 모드를 표시하거나 설정하십시오.

통사:

시스템 로그 서버 모드 [enable | disable]

매개 변수 :

enable : 시스템 로그 서버 모드 사용

disable : 시스템 로그 서버 모드 사용 불가

(기본값 : 시스템 로그 서버 모드 표시)

기본 설정:

disable

예:

로그 서버 모드를 표시하려면 다음과 같이하십시오.

```
SFC4000T:/>System log server mode
System Log Server Mode        : Disabled
```

시스템 이름

설명 :

시스템 이름을 설정하거나 표시하십시오.

통사:

시스템 이름 [<이름>]

매개 변수 :

<name> : 시스템 이름 문자열. (1-255)

문자열을 지우려면 ""을 사용하십시오.

시스템 이름은 알파벳 (A-Za-z), 숫자 (0-9), 빼기 기호 (-)로 그려지는 텍스트 문자열입니다.

공백이나 공백 문자는 이름의 일부로 사용할 수 없습니다.

첫 번째 문자는 알파 문자 여야하며 첫 번째 문자 또는 마지막 문자는 빼기 기호가 아니어야합니다.

예:

기기 제목을 설정하려면 다음 단계를 따르세요.

```
SFC4000T:/>System name SFC4000T-LAB
```

시스템 내용

설명 :

시스템 담당자를 설정하거나 표시하십시오.

통사:

System contact [<contact>]

매개 변수 :

<연락처> : 시스템 내용 문자열입니다. (1-255)

문자열을 지우려면 ""을 사용하십시오.

CLI 에서는 연락처의 일부로 공백이나 공백 문자를 사용할 수 없습니다.

기본 설정:

빈

예:

기기 내용 설정하려면 다음 단계를 따르세요.

```
SFC4000T:/>System contact SFC4000T-Test
```

시스템 로그 서버 주소

설명 :

시스템 로그 서버 주소를 표시하거나 설정하십시오.

통사:

System Log server address [<ip_addr_string>]

매개 변수 :

<ip_addr_string> : IP 호스트 주소 (a.b.c.d) 또는 호스트 이름 문자열

기본 설정:

Empty

예:

로그 서버 주소를 설정하려면 다음과 같이하십시오.

```
SFC4000T:/> log server address 192.168.0.21
```

시스템 위치

설명 :

시스템 위치를 설정하거나 표시하십시오.

통사:

System Location [<location>]

매개 변수 :

<location> : 시스템 위치 문자열. (1-255)

문자열을 지우려면 ""을 사용하십시오.

CLI 에서는 위치의 일부로 공백이나 공백 문자를 사용할 수 없습니다.

기본 설정:

빈

예:

기기 위치를 설정하려면 다음 단계를 따르세요.

```
SFC4000T:/>System location 9F-LAB
```

시스템 로그 수준

설명 :

시스템 로그 수준을 표시하거나 설정하십시오.

그것은 어떤 종류의 메시지가 syslog 서버에 보낼지 결정하는 데 사용됩니다.

통사:

시스템 로그 수준 [정보 | 경고 | 오류]

매개 변수 :

정보 : 정보, 경고 및 오류 보내기

경고 : 경고 및 오류 보내기

오류 : 오류 보내기

기본 설정:

정보

예:

로그 수준을 설정하려면 다음과 같이하십시오.

```
SFC4000T:/> log level warning
```

시스템 시간대

설명 :

시스템 시간대 오프셋을 설정하거나 표시하십시오.

통사:

System Timezone [<offset>]

매개 변수 :

<offset> : UTC 를 기준으로 표준 시간대 오프셋 (분) (-720-720)

기본 설정:

0

예:

시간대를 설정하려면 다음을 수행하십시오.

```
SFC4000T:/>system timezone 120
```

시스템 로그 조회

설명 :

시스템 로그를 표시하거나 지우십시오.

통사:

System Log Lookup [<log_id>] [all | info | warning | error]

매개 변수 :

<log_id> : 시스템 로그 ID 또는 범위 (기본값 : 모든 항목)

all : 모든 레벨 표시 (기본값)

정보 : 정보 표시

경고 : 경고 표시

오류 : 오류 표시

예:

시스템 로그를 표시하려면,

```
SFC4000T:/>system log lookup
Number of entries:
Info     : 2
Warning: 0
Error    : 0
All      : 2

ID      Level     Time                            Message
----    ------    -------------------------    -------
    1   Info      1970-01-01 Thu 00:00:02+00:00   Switch just made a cold boot.
    2   Info      1970-01-01 Thu 00:00:06+00:00   Link up on port 23
SFC4000T:/>
```

시스템 로그 지우기

설명 :

시스템 로그를 지우십시오.

통사:

시스템 로그 지우기 [all | info | warning | error]

매개 변수 :

all : 모든 레벨 표시 (기본값)

정보 : 정보 표시

경고 : 경고 표시

오류 : 오류 표시

예:

시스템 로그를 지우려면 다음을 수행하십시오.

```
SFC4000T:/>system log clear
SFC4000T:/>
```

시스템 재부팅

설명 :

시스템을 재부팅하십시오.

통사:

시스템 재부팅

예:

설정을 변경하지 않고 장치를 재부팅하려면 다음을 수행하십시오.

```
SFC4000T:/>system reboot
```

시스템 복원 기본값

설명 :

공장 기본 구성 복원.

통사:

시스템 복원 기본값 [keep_ip]

매개 변수 :

keep_ip : IP 구성 유지, 기본값 : 전체 구성 복원

예:

기본값을 복원하고 IP 주소를 재설정하지 않으려면 다음을 수행하십시오.

```
SFC4000T:/>system restore default keep_ip
```

시스템로드

설명 :

현재 CPU 로드 표시 : 100ms, 1 초 및 10 초의 실행 평균 (백분율, 0 은 유휴).

통사:

System Load

예:

현재 CPU 로드를 표시하려면,

```
SFC4000T:/>system load
Load average(100ms, 1s, 10s):    1%,    1%,    1%
```

5.2 IP 명령어

IP 구성

설명 :

Show IP configuration (IP 구성 표시).

통사:

IP 구성

예:

IP 구성 표시 :

```
SFC4000T:/>ip configuration

IP Configuration:
=================

DHCP Client          : Disabled
IP Address           : 192.168.0.101
IP Mask              : 255.255.255.0
IP Router            : 192.168.0.254
DNS Server           : 0.0.0.0
VLAN ID              : 1
DNS Proxy            : Disabled

IPv6 AUTOCONFIG mode    : Disabled
IPv6 Link-Local Address: fe80::230:4fff:fe11:2233
```

```
IPv6 Address                : ::192.168.0.100
IPv6 Prefix                 : 96
IPv6 Router                 : ::

Active Configuration for IPv6: (Static with Stateless)
IPv6 Address: fe80:2::230:4fff:fe11:2233/64 Scope:Link
Status:UP/RUNNING(Enabled)/MTU 1500/LinkMTU is 1500
IPv6 Address: ::192.168.0.100/96 Scope:Global
Status:UP/RUNNING(Enabled)/MTU 1500/LinkMTU is 1500
SFC4000T:/>
```

IP DHCP

설명 :

DHCP 클라이언트 모드를 설정하거나 표시합니다.

통사:

IP DHCP [enable | disable]

매개 변수 :

enable : DHCP 클라이언트 활성화 또는 갱신

disable : DHCP 클라이언트 비활성화

기본 설정:

사용 안함

예:

DHCP 서버 비활성화 :

```
SFC4000T:/>ip dhcp disable
```

IP 설정

설명 :

IP 설정을 지정하거나 표시하십시오.

통사:

IP 설정 [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]

매개 변수 :

<ip_addr> : IP 주소 (a.b.c.d), 기본값 : IP 주소 표시

<ip_mask> : IP 서브넷 마스크 (a.b.c.d), 기본값 : IP 마스크 표시

<ip_router> : IP 라우터 (a.b.c.d), 기본값 : IP 라우터 표시

<vid> : VLAN ID (1-4095), 기본값 : VLAN ID 표시

기본 설정:

IP 주소 : 192.168.0.100

IP 마스크 : 255.255.255.0

IP 공유기 : 192.168.0.1

DNS 서버 : 0.0.0.0

VLAN ID : 1

예:

IP 주소 설정 :

```
SFC4000T:/>ip setup 192.168.0.100 255.255.255.0
```

IP Ping

설명 :

Ping IP 주소 (ICMP 에코).

통사:

IP Ping <ip_addr_string> [(길이 <ping_length>)] ((카운트 <ping_count>)) [(간격 <ping_interval>)]

매개 변수 :

<ip_addr_string> : IPv4 호스트 주소 (a.b.c.d) 또는 호스트 이름 문자열

길이 : PING 길이 키워드

<ping_length> : MAC, IP 및 ICMP 헤더를 제외하고 Ping ICMP 데이터 길이 (2-1452, 기본값은 56)

count : PING Count 키워드

<ping_count> : ECHO_REQUEST 패킷 수를 전송합니다 (1-60, 기본값은 5 입니다).

간격 : PING 간격 키워드

<ping_interval> : 핑 간격 (0-30, 기본값은 0)

예:

```
SFC4000T:/>ip ping 192.168.0.21
PING server 192.168.0.21
60 bytes from 192.168.0.21: icmp_seq=0, time=0ms
60 bytes from 192.168.0.21: icmp_seq=1, time=0ms
```

```
60 bytes from 192.168.0.21: icmp_seq=2, time=0ms
60 bytes from 192.168.0.21: icmp_seq=3, time=10ms
60 bytes from 192.168.0.21: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

IP DNS

설명 :

DNS 서버 주소를 설정하거나 표시하십시오.

통사:

IP DNS [<ip_addr>]

매개 변수 :

<ip_addr> : IP 주소 (a.b.c.d), 기본값 : Showdne IP 주소

기본 설정:

0.0.0.0

예:

DNS IP 주소 설정 :

```
SFC4000T:/>ip dns 168.95.1.1
```

IP DNS 프록시

설명 :

IP DNS 프록시 모드를 설정하거나 표시합니다.

통사:

IP DNS_Proxy [enable | disable]

매개 변수 :

enable : DNS 프록시 사용

disable : DNS 프록시 비활성화

기본 설정:

disable

예:

DNS 프록시 기능 사용 :

```
SFC4000T:/>ip dns_proxy enable
```

IPv6 AUTOCONFIG

설명 :

IPv6 AUTOCONFIG 모드를 설정하거나 표시하십시오.

통사:

IP IPv6 AUTOCONFIG [enable | disable]

매개 변수 :

enable : IPv6 AUTOCONFIG 모드 활성화

disable : IPv6 AUTOCONFIG 모드를 비활성화합니다.

기본 설정:

disable

예:

IPv6 자동 구성 기능 사용 :

```
SFC4000T:/>ip ipv6 autoconfig enable
```

IPv6 설정

설명 :

IPv6 설정을 지정하거나 표시하십시오.

통사:

IP IPv6 설정 [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>]

매개 변수 :

<ipv6_addr> : IPv6 주소는 콜론이 각 필드 (:)를 구분하는 최대 네 개의 16 진수로 구성된 8 개의 필드로 표현 된 128 비트 레코드에 있습니다. 예를 들어, 콜론이있는 4 개의 16 진수는 각 필드 (:)를 구분합니다. 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'.

<ipv6_prefix> : IPv6 서브넷 마스크, 기본값 : IPv6 접두어 표시

<ipv6_router> : IPv6 라우터, 기본값 : IPv6 라우터 표시. 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'.

기본 설정:

IPv6 AUTOCONFIG 모드 : 사용 안 함

IPv6 링크 - 로컬 주소 : fe80 :: 6082 : cdb9 : 19ab : c0e2

IPv6 주소 :: 192.168.0.100

IPv6 접두사 : 96

IPv6 라우터 ::

예:

IPv6 주소 설정 :

```
SFC4000T:/>ip ipv6 setup 2001::0002 64 2100::0001
```

IPv6 Ping

설명 :

Ping IPv6 주소 (ICMPv6 에코).

통사:

IP IPv6 Ping6 <ipv6_addr> [(길이 <ping_length>)] ((카운트 <ping_count>)) [(간격 <ping_interval>)]

매개 변수 :

<ipv6_addr> : IPv6 호스트 주소. IPv6 주소는 콜론 (:)이 각 필드 (:)를 구분하여 최대 네 개의 16 진수로 된 8 개의 필드로 표현되는 128 비트 레코드에 있습니다. 예를 들어, 콜론이있는 4 개의 16 진수는 각 필드 (:)를 구분합니다. 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'.

길이 : PING 길이 키워드

<ping_length> : MAC, IP 및 ICMP 헤더를 제외하고 Ping ICMP 데이터 길이 (2-1452, 기본값은 56)

count : PING Count 키워드

<ping_count> : ECHO_REQUEST 패킷 수를 전송합니다 (1-60, 기본값은 5 입니다).

간격 : PING 간격 키워드

<ping_interval> : 핑 간격 (0-30, 기본값은 0)

```
SFC4000T:/>ip ipv6 ping 2001::0002
PING6 server 2001::2
68 bytes from 2001::2: icmp_seq=0, time=0ms
```

```
68 bytes from 2001::2: icmp_seq=1, time=0ms
68 bytes from 2001::2: icmp_seq=2, time=0ms
68 bytes from 2001::2: icmp_seq=3, time=0ms
68 bytes from 2001::2: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

IP NTP 구성

설명 :

NTP 구성을 표시합니다.

통사:

IP NTP 구성

기본 설정:

IP NTP 구성 :

==========

NTP 모드 : 사용 안 함

Idx 서버 IP 호스트 주소 (a.b.c.d) 또는 호스트 이름 문자열

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

1 pool.ntp.org

2 europe.pool.ntp.org

3 north-america.pool.ntp.org

4 asia.pool.ntp.org

5 oceania.pool.ntp.org

IP NTP 모드

설명 :

NTP 모드를 설정하거나 표시합니다.

통사:

IP NTP 모드 [enable | disable]

매개 변수 :

enable : NTP 모드 사용

disable : NTP 모드 사용 안 함

(기본값 : NTP 모드 표시)

기본 설정:

disable

예:

NTP 모드 사용 :

```
SFC4000T:/>ip ntp mode enable
```

NTP 서버 추가

설명 :

NTP 서버 항목을 추가하십시오.

통사:

IP NTP 서버 <server_index> <ip_addr_string>

매개 변수 :

<server_index> : 서버 색인 (1-5)

<ip_addr_string> : IP 호스트 주소 (a.b.c.d) 또는 호스트 이름 문자열

예:

NTP 서버를 추가하려면

```
SFC4000T:/>ip ntp server add 1 60.249.136.151
```

IP NTP 서버 IPv6 추가

설명 :

NTP 서버 IPv6 항목을 추가하십시오.

통사:

IP NTP 서버 IPv6 추가 <server_index> <server_ipv6>

매개 변수 :

<server_index> : 서버 색인 (1-5)

<server_ipv6> : IPv6 서버 주소. 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'.

예:

IPv6 NTP 서버를 추가하려면 다음을 수행하십시오.

```
SFC4000T:/>ip ntp server ipv6 add 1 2001:7b8:3:2c::123
```

IP NTP 서버 삭제

설명 :

NTP 서버 항목을 삭제하십시오.

통사:

IP NTP 서버 삭제 <server_index>

매개 변수 :

<server_index> : 서버 색인 (1-5)

예:

NTP 서버를 삭제하려면 다음과 같이하십시오.

```
SFC4000T:/>ip ntp server delete 1
```

5.3 Port Management 명령어

포트 구성

설명 :

포트 구성 표시.

통사:

포트 구성 [<port_list>] [up | down]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

up : 위로있는 포트 표시

down : 다운 된 포트 표시

(기본값 : 모든 포트 표시)

예:

포트 1 ~ 4 상태 표시

```
SFC4000T:/>port configuration 1-4

Port Configuration:
====================


Port   State       Mode            Flow Control   MaxFrame   Power       Excessive   Link
설명
----   --------   -----------   ------------   --------   --------   ---------   ----   -----------
1      Enabled    Auto            Disabled       9600       Disabled   Discard     Down
2      Enabled    Auto            Disabled       9600       Disabled   Discard     Down
3      Enabled    Auto            Disabled       9600       Disabled   Discard     Down
4      Enabled    Auto            Disabled       9600       Disabled   Discard     Down
```

포트 모드

설명 :

포트 속도 및 이중 모드를 설정하거나 표시합니다.

통사:

포트 모드 [<port_list>] [auto | 10hdx | 10fdx | 100hdx | 100fdx | 1000fdx | 1000x_ams | 1000x]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

자동 : 속도 및 이중의 자동 협상

10hdx : 10Mbps, 반이중

10fdx : 10Mbps, 전이중

100hdx : 100Mbps, 반이중

100fdx : 100Mbps, 전이중

1000fdx : 1Gbps, 전이중

1000x_ams : 자동 미디어 감지 기능이있는 1000BASE-X

1000x : 1000BASE-X

(기본값 : 구성된 모드 및 현재 모드 표시)

기본 설정:

자동

예:

포트 1 에 대해 10Mbps (반이중) 속도 설정

```
SFC4000T:/>port mode 1 10hdx
```

포트 흐름 제어

설명 :

포트 흐름 제어 모드를 설정하거나 표시하십시오.

통사:

포트 흐름 제어 [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable : 흐름 제어 사용

disable : 흐름 제어 사용 안 함

(기본값 : 흐름 제어 모드 표시)

기본 설정:

사용 안함

예:

port1 에 대한 흐름 제어 기능 사용

```
SFC4000T:/>port flow control 1 enable
```

포트 상태

설명 :

포트 관리 상태를 설정하거나 표시합니다.

통사:

포트 상태 [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable : 포트 사용

disable : 포트 비활성화

(기본값 : 관리 모드 표시)

기본 설정:

사용

예:

포트 1 사용 중지

```
SFC4000T:/>port state 1 disable
```

포트 최대 프레임

설명 :

포트 최대 프레임 크기를 설정하거나 표시하십시오.

통사:

Port MaxFrame [<port_list>] [<max_frame>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<max_frame> : 포트 최대 프레임 크기 (1518-9600), 기본값 : 최대 프레임 크기 표시

기본 설정:

9600

예:

포트 1 에 2048 프레임 크기 설정

```
SFC4000T:/>port maxframe 1 2048
```

포트 전원

설명 :

포트 PHY 전원 모드를 설정하거나 표시하십시오.

통사:

포트 전원 [<port_list>] [enable | disable | actiphy | dynamic]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable : 모든 전원 제어 활성화

disable : 모든 전원 제어 비활성화

actiphy : ActiPHY 전원 제어 활성화

동적 : 동적 전원 제어 사용

기본 설정:

disable

예:

포트 1-4 의 포트 전원 기능 비활성화

```
SFC4000T:/>port power 1-4 enable
```

Port **Excessive**

설명 :

과도한 충돌 모드를 설정하거나 표시합니다.

통사:

port **Excessive** [<port_list>] [discard | restart]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

discard : 16 개의 충돌 후 프레임 폐기

다시 시작 : 16 번 충돌 후 백 오프 알고리즘 다시 시작

(기본값 : 표시 모드)

기본 설정:

포기

예:

```
SFC4000T:/>port excessive 1 restart
```

포트 통계

설명 :

포트 통계를 표시합니다.

통사:

포트 통계 [<port_list>] [<명령어>] [up | down]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<명령어> : 명령어 매개 변수는 다음 값을 사용합니다.

clear : 포트 통계 지우기

패킷 : 패킷 통계 표시

바이트 : 바이트 통계 표시

errors : 오류 통계 표시

폐기 : 통계 삭제 표시

filtered : 필터링 된 통계 표시

0..7 : 우선 순위 통계 표시

(기본값 : 모든 포트 통계 표시)

up : 위로있는 포트 표시

down : 다운 된 포트 표시

포트 VeriPHY

설명 :

케이블 진단을 실행하십시오.

통사:

포트 VeriPHY [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

포트 SFP

설명 :

SFP 포트 정보를 표시합니다.

통사:

포트 SFP [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

포트 21-22 에 대한 SFP 정보 표시

```
SFC4000T:/>port sfp

Port   Type              Speed        Wave Length(nm)   Distance(m)
----   --------------    --------     ---------------   -----------
21     1000Base-LX       1000-Base    1310              10000
22     1000Base-LX       1000-Base    1310              10000
```

포트 설명

설명 :

포트 설명을 설정하거나 표시합니다.

통사:

포트 설명 [<port_list>] [<descr_text>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<descr_text> : 포트 설명 텍스트

기본 설정:

Empty

5.4 MAC Address Table 명령어

MAC 구성

설명 :

MAC 주소 테이블 구성을 표시합니다.

통사:

MAC 구성 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

Mac 주소 상태 표시

```
SFC4000T:/>mac configuration 1

MAC Configuration:
==================

MAC Address       : 00-30-4f-24-04-d1
MAC Age Time: 300

Port   Learning
----   --------
1       Auto
```

MAC 주소 추가

설명 :

MAC 주소 테이블 항목을 추가하십시오.

통사:

MAC add <mac_addr> <port_list> [<vid>]

매개 변수 :

<mac_addr> : MAC 주소 ('xx-xx-xx-xx-xx-xx'또는 'xx.xx.xx.xx.xx.xx'또는 'xxxxxxxxxxxx', x 는 16 진수)

<port_list> : 포트 목록 또는 'all'또는 'none'

<vid> : VLAN ID (1-4095), 기본값 : 1

예:

port1 및 vid1 에 Mac 주소 00-30-4F-01-01-02 추가

```
SFC4000T:/>mac add 00-30-4f-01-01-02 1 1
```

MAC 삭제

설명 :

MAC 주소 항목을 삭제하십시오.

통사:

MAC delete <mac_addr> [<vid>]

매개 변수 :

<mac_addr> : MAC 주소 ('xx-xx-xx-xx-xx-xx'또는 'xx.xx.xx.xx.xx.xx'또는 'xxxxxxxxxxxx', x 는 16 진수)

<vid> : VLAN ID (1-4095), 기본값 : 1

예:

vid1 에서 Mac 주소 00-30-4F-01-01-02 삭제

```
SFC4000T:/>mac delete 00-30-4f-01-01-02 1
```

MAC 조회

설명 :

Lookup MAC 주소 항목.

통사:

MAC 조회 <mac_addr> [<vid>]

매개 변수 :

<mac_addr> : MAC 주소 ('xx-xx-xx-xx-xx-xx'또는 'xx.xx.xx.xx.xx.xx'또는 'xxxxxxxxxxxx', x 는 16 진수)

<vid> : VLAN ID (1-4095), 기본값 : 1

예:

Mac 주소 조회 상태 00-30-4F-01-01-02

```
SFC4000T:/>mac lookup 00-30-4f-01-01-02
```

MAC aging 시간

설명 :

MAC 주소 aging 타이머를 설정하거나 표시하십시오.

통사:

MAC Agetime [<연령 _ 시간>]

매개 변수 :

<age_time> : MAC 주소 보존 기간 (0,10-1000000) 0 = 해제,

(기본값 : 연령대 표시)

기본 설정:

300 자

예:

연령대 값을 30 으로 설정하십시오.

```
SFC4000T:/>mac agetime 30
```

MAC 학습

설명 :

포트 학습 모드를 설정하거나 표시합니다.

통사:

MAC 학습 [<port_list>] [auto | disable | secure]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

자동 : 자동 학습

사용 중지 : 학습 사용 중지

보안 : 안전한 학습

(기본값 : 학습 모드 표시)

기본 설정:

자동

예:

포트 1 에서 보안 학습 모드 설정

```
SFC4000T:/>mac learning 1 secure
```

MAC 덤프

설명 :

정렬 된 MAC 주소 항목 목록을 표시합니다.

통사:

MAC 덤프 [<mac_max>] [<mac_addr>] [<vid>]

매개 변수 :

<mac_max> : 최대 MAC 주소 수 1-8192, 기본값 : 모든 주소 표시

<mac_addr> : 첫 번째 MAC 주소 ('xx-xx-xx-xx-xx-xx'또는 'xx.xx.xx.xx.xx.xx'또는 'xxxxxxxxxxxx', x 는 16 진수)

기본값 : MAC 주소 제로

<vid> : 첫 번째 VLAN ID (1-4095), 기본값 : 1

예:

모든 MAC 테이블 표시

```
SFC4000T:/>mac dump
Type      VID   MAC Address           Ports
------    ---   -----------------     -----
Static    1     00-30-4f-11-22-33     None,CPU
Static    1     33-33-00-00-00-01     1-28,CPU
Static    1     33-33-00-00-00-02     1-28,CPU
Static    1     33-33-ff-11-22-33     1-28,CPU
Static    1     33-33-ff-a8-00-64     1-28,CPU
Dynamic 1       40-61-86-04-18-69     23
Static    1     ff-ff-ff-ff-ff-ff     1-28,CPU
```

MAC 통계

설명 :

MAC 주소 테이블 통계를 표시합니다.

통사:

MAC statistics [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

모든 MAC 통계 설정

```
SFC4000T:/>mac statistics
Port   Dynamic Addresses
----   -----------------
1      0

Total Dynamic Addresses: 1
Total Static Addresses : 6
```

MAC 플러시

설명 :

모든 학습 된 항목을 플러시합니다.

통사:

MAC 플러시

5.5 VLAN Configuration 명령어

VLAN 구성

설명 :

VLAN 구성을 표시합니다.

통사:

VLAN 구성 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

port1 의 VLAN 상태 표시

```
SFC4000T:/>vlan configuration 1

VLAN Configuration:
====================



Mode : IEEE 802.1Q
Port   PVID   IngrFilter   FrameType    LinkType   Q-in-Q Mode   Eth type
----   ----   ----------   ----------   --------   -----------   --------
1      1      Disabled     All          UnTag      Disable       N/A

VID    VLAN Name                              Ports
----   --------------------------------   -----
1      default                                1-24

VID    VLAN Name                              Ports
----   --------------------------------   -----
VLAN forbidden table is empty
```

VLAN PVID

설명 :

포트 VLAN ID 를 설정하거나 표시하십시오.

통사:

VLAN PVID [<port_list>] [<vid> | none]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<vid> | none : 포트 VLAN ID (1-4095) 또는 'none', 기본값 : 포트 VLAN ID 표시

기본 설정:

1

예:

port10 에 대해 PVID2 설정

```
SFC4000T:/>vlan pvid 10 2
```

VLAN 프레임 유형

설명 :

포트 VLAN 프레임 유형을 설정하거나 표시합니다.

통사:

VLAN 프레임 유형 [<port_list>] [all | tagged]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

all : 태그가있는 프레임과 태그가없는 프레임을 허용합니다.

tagged : 태그가 달린 프레임 만 허용

(기본값 : 허용 된 프레임 유형 표시)

기본 설정:

모든

예:

태그가 지정된 프레임 만 허용하는 포트 10 설정

```
SFC4000T:/>vlan frametype 10 tagged
```

VLAN 수신 필터

설명 :

포트 VLAN 입구 필터를 설정하거나 표시하십시오.

통사:

VLAN IngressFilter [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable : VLAN 수신 필터링 사용

disable : VLAN 수신 필터링을 비활성화합니다.

(기본값 : VLAN 수신 필터링 표시)

기본 설정:

사용 안함

예:

port10 에 대해 VLAN 수신 필터링 사용

```
SFC4000T:/>vlan ingressfilter 10 enable
```

VLAN 모드

설명 :

VLAN 모드를 설정하거나 표시합니다.

통사:

VLAN 모드 [포트 기반 | dot1q]

매개 변수 :

portbased : 포트 기반 VLAN 모드

dot1q : 802.1Q VLAN 모드

(기본값 : VLAN 모드 표시)

기본 설정:

IEEE 802.1Q

예:

포트베이스에 VLAN 모드 설정

```
SFC4000T:/>vlan mode portbased
```

VLAN 링크 유형

설명 :

포트 VLAN 링크 유형을 설정하거나 표시합니다.

통사:

VLAN 링크 유형 [<port_list>] [untagged | tagged]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

태그없는 태그 : VLAN Link Type Tagged

tagged : VLAN 링크 유형 태그가 지정되지 않음

(기본값 : VLAN 링크 유형 표시)

기본 설정:

태그가 지정되지 않음

예:

port2 에 대해 태그가 지정된 프레임 사용

```
SFC4000T:/>vlan linktype 2 tagged
```

VLAN Q-in-Q 모드

설명 :

포트 Q-in-Q 모드를 설정하거나 표시하십시오.

통사:

VLAN QinQ [<port_list>] [disable | man | 고객]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

disable : Q-in-Q VLAN 모드 비활성화

man : Q-in-Q MAN 포트 모드

고객 : Q-in-Q 고객 포트 모드

(기본값 : Show VLAN QinQ Mode)

예:

man 포트에 port2 설정

```
SFC4000T:/>vlan qinq 2 man
```

VLAN 이더넷 유형

설명 :

Q-in-Q VLAN 모드에서 계층 VLAN 태그 이더넷 유형을 설정하거나 표시합니다.

통사:

VLAN Ethtype [<port_list>] [man | dot1q]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

man : 레이어 VLAN 태그 에테르 유형 설정 : MAN

dot1q : 레이어 VLAN 태그 에테르 유형 설정 : 802.1Q

(기본값 : VLAN 외부 레이어 VLAN 태그 이더넷 유형 표시)

기본 설정:

N / A

예:

이더넷 포트 유형에 포트 10 에 대한 레이어 VLAN 태그 이더넷 유형 설정

```
SFC4000T:/>vlan ethtype 10 man
```

VLAN 추가

설명 :

VLAN 항목을 추가 또는 수정하십시오.

통사:

VLAN 추가 <vid> | <name> [<port_list>]

매개 변수 :

<vid> | <name> : VLAN ID (1-4095) 또는 VLAN 이름

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

기본 설정:

1

예:

VLAN10 의 port4 에 port1 추가

```
SFC4000T:/>vlan add 10 1-4
```

VLAN 금지 추가

설명 :

금지 된 테이블에 VLAN 항목을 추가하거나 수정하십시오.

통사:

금지 된 VLAN <vid> | <name> [<port_list>]

매개 변수 :

<vid> | <name> : VLAN ID (1-4095) 또는 VLAN 이름

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

Frobidden 은 VLAN10 의 포트 1 에서 포트 4 까지 추가합니다.

```
SFC4000T:/>vlan forbidden add 10 1-4
```

VLAN 삭제

설명 :

VLAN 항목을 삭제하십시오.

통사:

VLAN 삭제 <vid> | <name>

매개 변수 :

<vid> | <name> : VLAN ID (1-4095) 또는 VLAN 이름

예:

VLAN10 삭제

```
SFC4000T:/>vlan delete 10
```

VLAN 금지 삭제

설명 :

VLAN 항목을 삭제하십시오.

통사:

LAN 금지됨 <vid> | <name>

매개 변수 :

<vid> | <name> : VLAN ID (1-4095) 또는 VLAN 이름

예:

금지 된 VLAN10 삭제

```
SFC4000T:/>vlan forbidden delete 10
```

VLAN 금지 검색

설명 :

조회 VLAN 금지 된 포트 항목입니다.

통사:

VLAN 금지 검색 [<vid>] [(name <name>)]

매개 변수 :

<vid> : VLAN ID (1-4095), 기본값 : 모든 VLAN 표시

이름 : VLAN 이름 문자열

<이름> : VLAN 이름 - 최대 32 자입니다. VLAN 이름에는 영문자 또는 숫자 만 사용할 수 있습니다.

VLAN 이름은 최소한 하나의 알파벳을 포함해야합니다.

VLAN 조회

설명 :

조회 VLAN 항목.

통사:

VLAN 조회 [<vid>] [(name <name>)] [combined | static | nas | mvr | voice_vlan | all]

매개 변수 :

<vid> : VLAN ID (1-4095), 기본값 : 모든 VLAN 표시

이름 : VLAN 이름 문자열

<이름> : VLAN 이름 - 최대 32 자입니다. VLAN 이름에는 영문자 또는 숫자 만 사용할 수 있습니다.

VLAN 이름은 최소한 하나의 알파벳을 포함해야합니다.

combined : 모든 결합 VLAN 데이터베이스를 표시합니다.

static : 관리자가 구성한 VLAN 항목을 표시합니다.

nas : NAS 가 구성한 VLAN 을 표시합니다.

mvr : MVR 로 구성된 VLAN 을 표시합니다.

voice_vlan : 음성 VLAN 으로 구성된 VLAN 을 표시합니다.

all : 모든 VLAN 구성을 표시합니다.

(기본값 : 결합 된 VLAN 사용자 구성)

예:

VLAN 상태 표시

```
SFC4000T:/>vlan lookup

VID    VLAN Name                        Ports
----   --------------------------------  -----
1      default                          1-10
```

VLAN 이름 추가

설명 :

VLAN ID 매핑에 VLAN 이름을 추가하십시오.

통사:

VLAN 이름 <name> <vid>

매개 변수 :

<이름> : VLAN 이름 - 최대 32 자입니다. VLAN 이름에는 영문자 또는 숫자 만 사용할 수 있습니다.

VLAN 이름은 최소한 하나의 알파벳을 포함해야합니다.

<vid> : VLAN ID (1-4095)

예:

VLAN 1 에 VLAN 이름 추가

```
SFC4000T:/>vlan name add test 1
```

VLAN 이름 삭제

설명 :

VLAN 이름을 VLAN ID 매핑으로 삭제하십시오.

통사:

VLAN name delete <이름>

매개 변수 :

<이름> : VLAN 이름 - 최대 32 자입니다. VLAN 이름에는 영문자 또는 숫자 만 사용할 수 있습니다.

VLAN 이름은 최소한 하나의 알파벳을 포함해야합니다.

예:

VLAN 이름 삭제

```
SFC4000T:/>vlan name delete test
```

VLAN 이름 조회

설명 :

VLAN 이름 표 표시.

통사:

VLAN 이름 조회 [<이름>]

매개 변수 :

<이름> : VLAN 이름 - 최대 32 자입니다. VLAN 이름에는 영문자 또는 숫자 만 사용할 수 있습니다.

VLAN 이름은 최소한 하나의 알파벳을 포함해야합니다.

예:

VLAN 이름 테이블을 표시하려면

```
SFC4000T:/>vlan name lookup
VLAN NAME                       vid
------------------------------  ---
test                            1
```

VLAN 상태

설명 :

VLAN 포트 구성 상태.

통사:

VLAN 상태 [<port_list>] [combined | static | nas | mvr | voice_vlan | mstp | all | conflicts]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

조합 : VLAN 사용자 조합 구성

static : 정적 포트 구성

nas : NAS 포트 구성

mvr : MVR 포트 구성

voice_vlan : 음성 VLAN 포트 구성

mstp : MSTP 포트 구성

vcl : VCL 포트 구성

all : 모든 VLAN 사용자 구성

(기본값 : 모든 VLAN 사용자 구성)

예:

port1 의 VLAN 구성 표시

```
SFC4000T:/>status 1

Port  VLAN User      PortType         PVID   Frame Type   Ing Filter    Tx Tag         UVID
Conflicts
----  ------------  -------------    ----   ----------   ------------  ------------  -----  ---------
1     Static        Unaware          1      All          Disabled      Untag This    1
      NAS
No
      MVR
No
      Voice VLAN
No
      MSTP
No
      VCL
No
      Combined      Unaware          1      All          Disabled      Untag This    1
No
```

5.6 Private VLAN Configuration 명령어

PVLAN 구성

설명 :

개인 VLAN 구성을 표시합니다.

통사:

PVLAN 구성 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

사설 VLAN 구성 표시

```
SFC4000T:/> pvlan configuration

Private VLAN Configuration:
===========================



Port    Isolation
----    ---------
1       Disabled

PVLAN ID    Ports
--------    -----
1             1-28
```

PVLAN 추가

설명 :

사설 VLAN 항목을 추가 또는 수정하십시오.

통사:

PVLAN 추가 <pvlan_id> [<port_list>]

매개 변수 :

<pvlan_id> : 사설 VLAN ID. 사설 VLAN ID 의 허용 범위는 스위치 포트 번호 범위와 동일합니다.

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

PVLAN10 의 port4 에 port1 추가

```
SFC4000T:/>pvlan add 10 1-4
```

PVLAN 삭제

설명 :

사설 VLAN 항목을 삭제하십시오.

통사:

PVLAN 삭제 <pvlan_id>

매개 변수 :

<pvlan_id> : 사설 VLAN ID. 사설 VLAN ID 의 허용 범위는 스위치 포트 번호 범위와 동일합니다.

예:

PVLAN10 삭제

```
SFC4000T:/>pvlan delete 10
```

PVLAN 조회

설명 :

Lookup Private VLAN 항목.

통사:

PVLAN 조회 [<pvlan_id>]

매개 변수 :

<pvlan_id> : 사설 VLAN ID, 기본값 : 모든 PVLAN 을 표시합니다. 사설 VLAN ID 의 허용 범위는 스위치 포트 번호 범위와 동일합니다.

예:

조회 PVLAN

```
SFC4000T:/>pvlan lookup
```

```
PVLAN ID    Ports
--------    -----
1               1-10
```

PVLAN 격리

설명 :

포트 격리 모드를 설정하거나 표시합니다.

통사:

PVLAN 격리 [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable : 포트 격리 사용

disable : 포트 격리 비활성화

(기본값 : 포트 격리 포트 목록 표시)

기본 설정:

disable

예:

포트 10 에 격리 가능

```
SFC4000T:/>pvlan isolate 10 enable
```

5.7 Security 명령어

보안 스위치 사용자 구성

설명 :

사용자 구성을 표시합니다.

통사:

보안 스위치 사용자 구성

기본 설정:

사용자이름	권한
admin	15

예제:

사용자 설정을 나타냅니다.

```
SFC4000T:/>security switch user configuration

Users Configuration:
====================

User Name                       Privilege Level
------------------------------  ---------------
admin                                       15
```

보안 스위치 사용자 추가

설명 :

사용자 항목을 추가 또는 수정하십시오.

통사:

보안 스위치 사용자 <user_name> <password> <privilege_level>

매개 변수 :

<user_name> :이 항목이 속해야하는 사용자 이름을 식별하는 문자열. 허용되는 문자열 길이는 (1-32)입니다. 유효한 사용자 이름은 문자, 숫자 및 밑줄의 조합입니다.

<password> :이 사용자 이름의 암호. 허용되는 문자열 길이는 (0-32)입니다. 'clear'또는 "을 null 문자열로 사용하십시오.

<privilege_level> : 사용자 권한 수준 (1-15)

예:

새 사용자 추가 : 사용자 이름 : 테스트, 비밀번호 : 테스트 및 권한 : 10

```
SFC4000T:/>security switch users add test test 10
```

보안 스위치 사용자 삭제

설명 :

사용자 항목을 삭제하십시오.

통사:

보안 스위치 사용자 <user_name>

매개 변수 :

<user_name> :이 항목이 속해야하는 사용자 이름을 식별하는 문자열. 허용되는 문자열 길이는 (1-32)입니다. 유효한 사용자 이름은 문자, 숫자 및 밑줄의 조합입니다.

예:

테스트 계정을 삭제하십시오.

```
SFC4000T:/>security switch users delete user
```

보안 스위치 권한 수준 구성

설명 :

권한 구성 표시.

통사:

보안 스위치 권한 수준 구성

예:

권한 수준 표시

```
SFC4000T:/>security switch privilege level configuration

Privilege Level Configuration:
==============================

Privilege Current Level: 15
Group Name                          Priviliege Level
                                    CRO CRW SRO SRW
------------------------------- --- --- --- ---
Aggregation                          5   10    5   10
Diagnostics                          5   10    5   10
IP                                   5   10    5   10
LACP                                 5   10    5   10
LLDP                                 5   10    5   10
LLDP_MED                             5   10    5   10
Loop_Protect                         5   10    5   10
MAC_Table                            5   10    5   10
MVR                                  5   10    5   10
Maintenance                         15   15   15   15
```

Mirroring	**5**	**10**	**5**	**10**
Multicast	**5**	**10**	**5**	**10**
Port_Security	**5**	**10**	**5**	**10**
Ports	**5**	**10**	**1**	**10**
Private_VLANs	**5**	**10**	**5**	**10**
Protocol_based_VLAN	**5**	**10**	**5**	**10**
QoS	**5**	**10**	**5**	**10**
SFlow	**5**	**10**	**5**	**10**
SNMP	**5**	**10**	**5**	**10**
Security	**5**	**10**	**5**	**10**
Spanning_Tree	**5**	**10**	**5**	**10**
System	**5**	**10**	**1**	**10**
Timer	**5**	**10**	**5**	**10**
UPnP	**5**	**10**	**5**	**10**
VLANs	**5**	**10**	**5**	**10**
Voice_VLAN	**5**	**10**	**5**	**10**

보안 스위치 권한 수준 그룹

설명 :

권한 수준 그룹을 구성합니다.

통사:

보안 스위치 권한 수준 그룹 <group_name> [<cro>] [<crw>] [<sro>] [<srw>]

매개 변수 :

<group_name> : 권한 그룹 이름

<cro> : 구성 읽기 전용 권한 수준 (1-15)

<crw> : 읽기 / 쓰기 권한 수준 구성 / 실행 (1-15)

<sro> : 상태 / 통계 읽기 전용 권한 수준 (1-15)

<srw> : 상태 / 통계 읽기 - 쓰기 권한 수준 (1-15)

예:

MVR 그룹의 권한 수준을 변경합니다.

```
SFC4000T:/>security switch privilege level group mvr 15 15 15 15
```

보안 스위치 권한 수준 단계 흐름

설명 :

현재 권한 수준을 표시합니다.

통사:

보안 스위치 권한 수준 전류

기본 설정:

15 명

보안 스위치 인증 구성

설명 :

인증 구성 표시.

통사:

보안 스위치 인증 구성

예:

인증 구성 표시.

```
SFC4000T:/>security switch auth configuration

Auth Configuration:
===================

Client     Authentication Method     Local Authentication Fallback
-------    ----------------------    -----------------------------
console    local                     Disabled
telnet     local                     Disabled
ssh        local                     Disabled
web        local                     Disabled
```

보안 스위치 인증 방법

설명 :

인증 방법 설정 또는 표시. (기본값 : Auth 메소드 표시).

통사:

보안 스위치 인증 방법 [console | telnet | ssh | web] [none | local | tacacs +] [enable | disable]

매개 변수 :

console : 콘솔 설정

telnet : 텔넷 설정

ssh : ssh 설정

web : 웹 설정

(기본값 : 특정 클라이언트 인증 방법 설정 또는 표시)

없음 : 인증이 사용 중지되었습니다.

local : 로컬 인증 사용

radius : 원격 RADIUS 인증 사용

tacacs + : 원격 TACACS + 인증 사용

(기본값 : 클라이언트 인증 방법 표시)

enable : 원격 인증에 실패 할 경우 로컬 인증 사용

disable : 원격 인증에 실패 할 경우 로컬 인증 사용 안 함

(매개 변수는 입력 할 때 유효합니다)

기본 설정:

disable

예:

텔넷에 RADIUS 인증 방법을 사용하십시오.

```
SFC4000T:/>security switch auth method telnet radius enable
```

보안 스위치 SSH 구성

설명 :

SSH 구성을 표시합니다.

통사:

보안 스위치 SSH 구성

예:

SSH 구성을 표시합니다.

```
SFC4000T:/>security switch ssh configuration

SSH Configuration:
```

```
==================

SSH Mode : Enable
```

보안 스위치 SSH 모드

설명 :

SSH 모드를 설정하거나 표시하십시오.

통사:

보안 스위치 SSH 모드 [enable | disable]

매개 변수 :

enable : SSH 사용

disable : SSH 비활성화

(기본값 : Show SSH mode)

기본 설정:

가능하게하다

예:

SSH 기능을 사용하십시오.

```
SFC4000T:/>security switch ssh mode enable
```

보안 스위치 HTTPs 구성

설명 :

HTTPS 구성 표시.

통사:

보안 스위치 HTTPS 구성

예:

HTTPS 구성 표시.

```
SFC4000T:/>security switch https configuration
```

```
HTTPS Configuration:
====================

HTTPS Mode              : Enable
HTTPS Redirect Mode : Disabled
```

보안 스위치 HTTPs 모드

설명 :

HTTPS 모드를 설정하거나 표시합니다.

통사:

보안 스위치 HTTPS 모드 [enable | disable]

매개 변수 :

enable : HTTPs 사용

disable : HTTPs 사용 안함

(기본값 : HTTP 모드 표시)

기본 설정:

가능하게하다

예:

HTTPs 기능을 사용합니다.

```
SFC4000T:/>security switch https mode enable
```

보안 스위치 HTTPs 리디렉션

설명 :

HTTPS 리디렉션 모드를 설정하거나 표시합니다.

HTTPS 모드가 활성화되는 동안 자동으로 웹 브라우저를 HTTPS 로 리디렉션합니다.

통사:

보안 스위치 HTTPS Redirect [enable | disable]

매개 변수 :

enable : HTTPs 리디렉션 사용

disable : HTTPs 리디렉션 사용 안 함

(기본값 : HTTPs 리디렉션 모드 표시)

기본 설정:

disable

예:

HTTPs 리디렉션 기능을 사용합니다.

```
SFC4000T:/>security switch https redirect enable
```

보안 스위치 액세스 구성

설명 :

액세스 관리 구성 표시.

통사:

보안 스위치 액세스 구성

예:

액세스 관리 구성 표시.

```
SFC4000T:/>security switch access configuration

Access Mgmt Configuration:
==========================

System Access Mode : Disabled
W: WEB/HTTPS
S: SNMP
T: TELNET/SSH

Idx Start IP Address                End IP Address                  W S T
--- ------------------------------- ------------------------------- - - -
```

보안 스위치 액세스 모드

설명 :

액세스 관리 모드를 설정하거나 표시하십시오.

통사:

보안 스위치 액세스 모드 [enable | disable]

매개 변수 :

enable : 액세스 관리 사용

disable : 액세스 관리 사용 중지

(기본값 : 액세스 관리 모드 표시)

기본 설정:

disable

예:

액세스 관리 기능을 사용합니다.

```
SFC4000T:/>security switch access mode enable
```

보안 스위치 액세스 추가

설명 :

액세스 관리 항목 추가, 기본값 : 지원되는 모든 프로토콜을 추가하십시오.

통사:

보안 스위치 액세스 <access_id> <start_ip_addr> <end_ip_addr> [web] [snmp] [telnet]

매개 변수 :

<access_id> : 항목 색인 (1-16)

<start_ip_addr> : 시작 IP 주소 (a.b.c.d)

<end_ip_addr> : 최종 IP 주소 (a.b.c.d)

web : 호스트가 HTTP / HTTPS 에서 스위치에 액세스 할 수 있음을 나타냅니다.

snmp : 호스트가 SNMP 에서 스위치에 액세스 할 수 있음을 나타냅니다.

telnet : 호스트가 TELNET / SSH 에서 스위치에 액세스 할 수 있음을 나타냅니다.

예:

웹 인터페이스를 통해 192.168.0.1 에서 192.168.0.200 까지 액세스 관리 목록을 추가하십시오.

```
SFC4000T:/>security switch access add 1 192.168.0.1 192.168.0.200 web
```

보안 스위치 액세스 IPv6 추가

설명 :

액세스 관리 IPv6 항목 추가, 기본값 : 지원되는 모든 프로토콜을 추가하십시오.

통사:

보안 스위치 액세스 Ipv6 추가 <access_id> <start_ipv6_addr> <end_ipv6_addr> [web] [snmp] [telnet]

매개 변수 :

<access_id> : 항목 색인 (1-16)

<start_ipv6_addr> : IPv6 주소를 시작하십시오.

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'.

<end_ipv6_addr> : 끝 IPv6 주소.

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'.

web : 호스트가 HTTP / HTTPS 에서 스위치에 액세스 할 수 있음을 나타냅니다.

snmp : 호스트가 SNMP 에서 스위치에 액세스 할 수 있음을 나타냅니다.

telnet : 호스트가 TELNET / SSH 에서 스위치에 액세스 할 수 있음을 나타냅니다.

예:

2001 :: 0001 에서 2001 :: 0100 웹 인터페이스를 통해 액세스 관리 목록을 추가하십시오.

```
SFC4000T:/> security switch access add 2001::0001 2001::0100 web
```

보안 스위치 액세스 삭제

설명 :

액세스 관리 항목을 삭제하십시오.

통사:

보안 스위치 액세스 삭제 <access_id>

매개 변수 :

<access_id> : 항목 색인 (1-16)

예:

액세스 관리 ID 1 삭제

```
SFC4000T:/>security switch access delete 1
```

보안 스위치 액세스 조회

설명 :

조회 액세스 관리 항목.

통사:

보안 스위치 액세스 조회 [<access_id>]

매개 변수 :

<access_id> : 항목 색인 (1-16)

예:

조회 액세스 관리 항목.

```
SFC4000T:/>security switch access lookup 1
```

보안 스위치 액세스 지우기

설명 :

액세스 관리 항목을 지우십시오.

통사:

보안 스위치 액세스 지우기

예:

액세스 관리 항목을 지우십시오.

```
SFC4000T:/>security switch access clear
```

보안 스위치 액세스 통계

설명 :

액세스 관리 통계를 표시하거나 지우십시오.

통사:

보안 스위치 액세스 통계 [지우기]

매개 변수 :

clear : 액세스 관리 통계 지우기

예:

액세스 관리 통계를 표시합니다.

```
SFC4000T:/>security switch access statistics

Access Management Statistics:
-----------------------------
HTTP      Receive:      0     Allow:      0     Discard:      0
HTTPS     Receive:      0     Allow:      0     Discard:      0
SNMP      Receive:      0     Allow:      0     Discard:      0
TELNET    Receive:      0     Allow:      0     Discard:      0
SSH       Receive:      0     Allow:      0     Discard:      0
```

보안 스위치 SNMP 구성

설명 :

SNMP 구성 표시.

통사:

보안 스위치 SNMP 구성

보안 스위치 SNMP 모드

설명 :

SNMP 모드를 설정하거나 표시합니다.

통사:

보안 스위치 SNMP 모드 [enable | disable]

매개 변수 :

enable : SNMP 사용

disable : SNMP 비활성화

(기본값 : SNMP 모드 표시)

기본 설정:

가능하게하다

예:

SNMP 모드를 비활성화하십시오.

```
SFC4000T:/>security switch snmp mode disable
```

보안 스위치 SNMP 버전

설명 :

SNMP 프로토콜 버전을 설정하거나 표시하십시오.

통사:

보안 스위치 SNMP 버전 [1 | 2c | 3]

매개 변수 :

1 : SNMP 버전 1

2c : SNMP 버전 2c

3 : SNMP 버전 3

(기본값 : SNMP 버전 표시)

기본 설정:

2c

예:

버전 3 에서 SNMP 를 설정하십시오.

```
SFC4000T:/>security switch snmp version 3
```

보안 스위치 SNMP 읽기 커뮤니티

설명 :

SNMP 읽기 액세스를위한 커뮤니티 문자열을 설정하거나 표시하십시오.

통사:

보안 스위치 SNMP 읽기 커뮤니티 [<community>]

매개 변수 :

<community> : 커뮤니티 문자열. 'clear'또는 ''을 사용하여 문자열 지우기

허용되는 최대 길이는 최대 256 자입니다.

(기본값 : SNMP 읽기 커뮤니티 표시)

기본 설정:

공공의

예:

SNMP 읽기 커뮤니티를 비공개로 설정합니다.

```
SFC4000T:/>security switch snmp read community private
```

보안 스위치 SNMP 쓰기 커뮤니티

설명 :

SNMP 쓰기 액세스를위한 커뮤니티 문자열을 설정하거나 표시하십시오.

통사:

보안 스위치 SNMP 쓰기 커뮤니티 [<community>]

매개 변수 :

<community> : 커뮤니티 문자열. 'clear'또는 ''을 사용하여 문자열 지우기

허용되는 최대 길이는 최대 256 자입니다.

(기본값 : SNMP 쓰기 커뮤니티 표시)

기본 설정:

은밀한

예:

SNMP 쓰기 커뮤니티에서 공개 가치를 설정하십시오.

```
SFC4000T:/>security switch snmp write community public
```

보안 스위치 SNMP 트랩 모드

설명 :

SNMP 트랩 모드를 설정하거나 표시하십시오.

통사:

보안 스위치 SNMP 트랩 모드 [enable | disable]

매개 변수 :

enable : SNMP 트랩 사용

disable : SNMP 트랩을 비활성화합니다.

(기본값 : SNMP 트랩 모드 표시)

기본 설정:

disable

예:

SNMP 트랩 모드를 활성화합니다.

```
SFC4000T:/>security switch snmp trap mode enable
```

보안 스위치 SNMP 트랩 버전

설명 :

SNMP 트랩 프로토콜 버전을 설정하거나 표시하십시오.

통사:

보안 스위치 SNMP 트랩 버전 [1 | 2c | 3]

매개 변수 :

1 : SNMP 버전 1

2c : SNMP 버전 2c

3 : SNMP 버전 3

(기본값 : SNMP 트랩 버전 표시)

기본 설정:

1

예:

버전 2c 에서 SNMP 트랩 버전을 설정하십시오.

```
SFC4000T:/>security switch snmp trap version 2c
```

보안 스위치 SNMP 트랩 커뮤니티

설명 :

SNMP 트랩에 대한 커뮤니티 문자열을 설정하거나 표시하십시오.

통사:

보안 스위치 SNMP 트랩 커뮤니티 [<community>]

매개 변수 :

<community> : 커뮤니티 문자열. 'clear'또는 ''을 사용하여 문자열 지우기

허용되는 최대 길이는 최대 256 자입니다.

(기본값 : SNMP 트랩 커뮤니티 표시)

기본 설정:

공공의

예:

SNMP 트랩 커뮤니티의 개인적인 가치를 설정하십시오.

```
SFC4000T:/>security switch snmp trap community private
```

보안 스위치 SNMP 트랩 대상

설명 :

SNMP 트랩 대상 주소 설정 또는 표시.

통사:

보안 스위치 SNMP 트랩 대상 [<ip_addr_string>]

매개 변수 :

<ip_addr_string> : IP 호스트 주소 (a.b.c.d) 또는 호스트 이름 문자열

예:

192.168.0.20 에 대한 SNMP 트랩 대상 주소 설정

```
SFC4000T:/>security switch snmp trap destination 192.168.0.20
```

보안 스위치 SNMP 트랩 IPv6 대상

설명 :

SNMP 트랩 대상 IPv6 주소 설정 또는 표시.

통사:

보안 스위치 SNMP 트랩 IPv6 대상 [<ipv6_addr>]

매개 변수 :

<ipv6_addr> : IPv6 주소는 콜론이 각 필드 (:)를 구분하는 최대 네 개의 16 진수로 구성된 8 개의 필드로 표현 된 128 비트 레코드에 있습니다. 예를 들어, 콜론이있는 4 개의 16 진수는 각 필드 (:)를 구분합니다. 예를 들어, fe80 :: 215 : c5ff : fe03 : 4dc7 '입니다. '::'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'.

예:

2001 에 대한 SNMP 트랩 IPv6 대상 주소 설정 :: 0001

```
SFC4000T:/>security switch snmp trap ipv6 destination 2001::0001
```

보안 스위치 SNMP 트랩 인증 실패

설명 :

SNMP 인증 실패 트랩 모드를 설정하거나 표시하십시오.

통사:

보안 스위치 SNMP 트랩 인증 실패 [enable | disable]

매개 변수 :

enable : SNMP 트랩 인증 실패 사용

disable : SNMP 트랩 인증 실패 사용 안 함

(기본값 : SNMP 트랩 인증 실패 모드 표시)

기본 설정:

가능하게하다

예:

SNMP 트랩 인증 실패 사용 안 함

```
SFC4000T:/>security switch snmp trap authentication failure disable
```

보안 스위치 SNMP 트랩 연결

설명 :

포트 링크 업 및 링크 다운 트랩 모드를 설정하거나 표시합니다.

통사:

보안 스위치 SNMP 트랩 연결 [사용 | 사용 안 함]

매개 변수 :

enable : SNMP 트랩 링크 업 및 링크 다운 사용

disable : SNMP 트랩 링크 업 및 링크 다운 비활성화

(기본값 : SNMP 트랩 링크 업 및 링크 다운 모드 표시)

기본 설정:

가능하게하다

예:

SNMP 트랩 연결 해제

```
SFC4000T:/>security switch snmp trap link-up disable
```

보안 스위치 SNMP 트랩 정보 모드

설명 :

SNMP 트랩 정보 모드를 설정하거나 표시하십시오.

통사:

보안 스위치 SNMP 트랩 정보 모드 [enable | disable]

매개 변수 :

enable : SNMP 트랩 알림 활성화

disable : SNMP 트랩 알림 사용 안 함

(기본값 : SNMP 알림 모드 표시)

기본 설정:

가능하게하다

예:

SNMP 트랩 정보 모드를 비활성화합니다.

```
SFC4000T:/>security switch snmp trap inform mode disable
```

보안 스위치 SNMP 트랩 알림 시간 제한

설명 :

SNMP 트랩 정보 시간 초과 (usecs)를 설정하거나 표시하십시오.

통사:

보안 스위치 SNMP 트랩 알림 시간 초과 [<timeout>]

매개 변수 :

<timeout> : SNMP 트랩이 시간 초과 알림 (0-2147 초)

기본 설정:

1

예:

20 초 안에 SNMP 트랩 정보 시간 초과를 설정하십시오.

```
SFC4000T:/>security switch snmp trap inform timeout 20
```

보안 스위치 SNMP 트랩 알림 재시도 횟수

설명 :

재 시도 시간을 알려주는 SNMP 트랩을 설정하거나 표시하십시오.

통사:

보안 스위치 SNMP 트랩 알림 재시도 횟수 [<retries>]

매개 변수 :

<retries> : SNMP 트랩이 재전송 시간을 알려줍니다 (0-255).

(기본값 : 재시도 시간을 알려주는 SNMP 트랩 표시)

기본 설정:

5

예:

재시도 횟수를 10 으로 설정합니다.

```
SFC4000T:/>security switch snmp trap inform retry times 10
```

보안 스위치 SNMP 트랩 프로브 보안 엔진 ID

설명 :

SNMP 트랩 보안 엔진 ID 프로브 모드를 표시합니다.

통사:

보안 스위치 SNMP 트랩 프로브 보안 엔진 ID [enable | disable]

매개 변수 :

enable : SNMP 트랩 보안 엔진 ID 프로브 활성화

disable : SNMP 트랩 보안 엔진 ID 프로브 비활성화

(기본값 : SNMP 트랩 보안 엔진 ID 프로브 모드 표시)

기본 설정:

가능하게하다

예:

SNMP 트랩 프로브 보안 엔진 ID 사용 안 함

```
SFC4000T:/>security switch snmp trap probe security engine id disable
```

보안 스위치 SNMP 트랩 보안 엔진 ID

설명 :

SNMP 트랩 보안 엔진 ID 를 설정하거나 표시합니다.

통사:

보안 스위치 SNMP 트랩 보안 엔진 ID [<engineid>]

매개 변수 :

<engineid> : 엔진 ID 입니다. 형식이 모두 0 또는 모두 'ff'H 가 아니며 5 - 32 옥텟 문자열로 제한됩니다

예:

SNMP 트랩 보안 엔진 ID 설정

```
SFC4000T:/>security switch snmp trap security engine id 800007e5017f000011
```

보안 스위치 SNMP 트랩 보안 이름

설명 :

SNMP 트랩 보안 이름을 설정하거나 표시하십시오.

통사:

보안 스위치 SNMP 트랩 보안 이름 [<security_name>]

매개 변수 :

<security_name> : 보안 주체의 보안 이름을 나타내는 문자열입니다 (기본값 : SNMP 트랩 보안 이름 표시). 허용되는 문자열 길이는 (1-32)이며 허용되는 내용은 33 에서 126 사이의 ASCII 문자입니다

예:

SNMP 트랩 보안 이름 설정

```
SFC4000T:/>security switch snmp trap security name 12345678
```

보안 스위치 SNMP 엔진 ID

설명 :

SNMPv3 로컬 엔진 ID 를 설정하거나 표시합니다.

통사:

보안 스위치 SNMP 엔진 ID [<engineid>]

매개 변수 :

<engineid> : 엔진 ID 입니다. 형식이 모두 0 또는 모두 'ff'H 가 아니며 5 - 32 옥텟 문자열로 제한됩니다

기본 설정:

800007e5017f000001

예:

SNMPv3 로컬 엔진 ID 에 대해 800007e5017f000002 설정

```
SFC4000T:/>security switch snmp engine id 800007e5017f000002
```

보안 스위치 SNMP 커뮤니티 추가

설명 :

SNMPv3 커뮤니티 항목을 추가 또는 수정하십시오.

항목 색인 키는 <community>입니다.

통사:

보안 스위치 SNMP 커뮤니티 <community> [<ip_addr>] [<ip_mask>]

매개 변수 :

<community> : 커뮤니티 문자열

<ip_addr> : IP 주소 (a.b.c.d), 기본값 : IP 주소 표시

<ip_mask> : IPv4 서브넷 마스크 (a.b.c.d), 기본값 : IP 마스크 표시

예:

SNMPv3 커뮤니티 항목을 추가하십시오.

```
SFC4000T:/>security switch snmp community add public 192.168.0.20 255.255.255.0
```

보안 스위치 SNMP 커뮤니티 삭제

설명 :

SNMPv3 커뮤니티 항목을 삭제하십시오.

통사:

보안 스위치 SNMP 커뮤니티 <index>

매개 변수 :

<index> : 항목 색인 (1-64)

예:

SNMPv3 커뮤니티 항목 삭제

```
SFC4000T:/>security switch snmp community delete 3
```

보안 스위치 SNMP 커뮤니티 조회

설명 :

SNMPv3 커뮤니티 항목을 조회합니다.

통사:

보안 스위치 SNMP 커뮤니티 조회 [<index>]

매개 변수 :

<index> : 항목 색인 (1-64)

예:

SNMPv3 커뮤니티 항목 조회

```
SFC4000T:/>security switch snmp community lookup
Idx Community                        Source IP         Source Mask
--- -------------------------------- ----------------- ---------------
1   public                           192.168.0.20      255.255.255.0
2   private                          0.0.0.0           0.0.0.0

Number of entries: 2
```

보안 스위치 SNMP 사용자 추가

설명 :

SNMPv3 사용자 항목을 추가하십시오.

항목 색인 키는 <engineid> 및 <user_name>이며 수정을 허용하지 않습니다.

통사:

보안 스위치 SNMP 사용자 <engineid> <user_name> [MD5 | SHA] [<auth_password>] [DES] [<priv_password>]

매개 변수 :

<engineid> : 엔진 ID 입니다. 형식이 모두 0 또는 모두 'ff'H 가 아니며 5 - 32 옥텟 문자열로 제한됩니다

<user_name> :이 항목이 속해야하는 사용자 이름을 식별하는 문자열. "없음"의 이름은 예약되어 있습니다.

허용되는 문자열 길이는 (1-32)이며 허용되는 내용은 33 에서 126 사이의 ASCII 문자입니다

md5 :이 사용자가 MD5 인증 프로토콜을 사용하고 있음을 나타내는 선택적 플래그. 허용되는 길이는 (8-32)이며 허용되는 내용은 33 에서 126 까지의 ASCII 문자입니다

sha : SHA 인증 프로토콜을 사용하는이 사용자를 나타내는 선택적 플래그. 허용되는 길이는 (8-40)이고 허용되는 내용은 33 에서 126 사이의 ASCII 문자입니다

<auth_password> : 인증 통과 구문을 식별하는 문자열

des : DES 개인 정보 보호 프로토콜을 사용하는이 사용자가에 속해야 함을 나타내는 선택적 플래그.

허용되는 문자열 길이는 (8-32)이고 허용되는 내용은 33 에서 126 사이의 ASCII 문자입니다

<priv_password> : 개인 정보 보호 암호 구문을 식별하는 문자열입니다.

허용되는 문자열 길이는 (8-40)이고 허용되는 내용은 33 에서 126 사이의 ASCII 문자입니다

예:

SNMPv3 사용자 항목 추가

```
SFC4000T:/>security switch snmp user add 800007e5017f000003 admin_snmpv3 md5
12345678 des abcdefgh
```

보안 스위치 SNMP 사용자 삭제

설명 :

SNMPv3 사용자 항목을 삭제하십시오.

통사:

보안 스위치 SNMP 사용자 <index>

매개 변수 :

<index> : 항목 색인 (1-64)

예:

SNMPv3 사용자 항목 삭제

```
SFC4000T:/>security switch snmp user delete 1
```

보안 스위치 SNMP 사용자 Changekey

설명 :

SNMPv3 사용자 암호를 변경하십시오.

통사:

보안 스위치 SNMP 사용자 Changekey <engineid> <user_name> <auth_password> [<priv_password>]

매개 변수 :

<engineid> : 엔진 ID 입니다. 형식이 모두 0 또는 모두 'ff'H 가 아니며 5 - 32 옥텟 문자열로 제한됩니다

<user_name> :이 항목이 속해야하는 사용자 이름을 식별하는 문자열. "없음"의 이름은 예약되어 있습니다. 허용되는 문자열 길이는 (1-32)이며 허용되는 내용은 33 에서 126 사이의 ASCII 문자입니다

<auth_password> : 인증 통과 구문을 식별하는 문자열

<priv_password> : 개인 정보 보호 암호 구문을 식별하는 문자열입니다.

허용되는 문자열 길이는 (8-40)이고 허용되는 내용은 33 에서 126 사이의 ASCII 문자입니다

예:

SNMPv3 사용자 항목 삭제

```
SFC4000T:/>security switch snmp user changekey 800007e5017f000003 admin_snmpv3
87654321 12345678
```

보안 스위치 SNMP 사용자 조회

설명 :

SNMPv3 사용자 항목을 조회합니다.

통사:

보안 스위치 SNMP 사용자 조회 [<index>]

매개 변수 :

<index> : 항목 색인 (1-64)

예:

SNMPv3 사용자 항목 조회

```
SFC4000T:/>security switch snmp user lookup
Idx Engine ID     User Name                       Level          Auth    Priv
```

```
---  ---------  -------------------------------  --------------  ----  ----
1    Remote     admin_snmpv3                     Auth, Priv      MD5   DES

Number of entries: 1
```

보안 스위치 SNMP 그룹 추가

설명 :

SNMPv3 그룹 항목을 추가 또는 수정합니다.

항목 색인 키는 <security_model> W <security_name>입니다.

통사:

보안 스위치 SNMP 그룹 추가 <security_model> <security_name> <group_name>

매개 변수 :

<security_model> : v1 - SNMPv1 용으로 예약 됨

v2c - SNMPv2c 를 위해 예약 됨

usm - 사용자 기반 보안 모델 (USM)

<security_name> :이 항목이 속해야하는 보안 이름을 식별하는 문자열. 허용되는 문자열 길이는 (1-32)이며 허용되는 내용은 33 에서 126 사이의 ASCII 문자입니다

<group_name> :이 항목이 속해야하는 그룹 이름을 식별하는 문자열. 허용되는 문자열 길이는 (1-32)이며 허용되는 내용은 33 에서 126 사이의 ASCII 문자입니다

예:

SNMPv3 그룹 항목 추가

```
SFC4000T:/>security switch snmp group add usm admin_snmpv3 group_snmpv3
```

보안 스위치 SNMP 그룹 삭제

설명 :

SNMPv3 그룹 항목을 삭제하십시오.

통사:

보안 스위치 SNMP 그룹 <index>

매개 변수 :

<index> : 항목 색인 (1-64)

예:

SNMPv3 그룹 항목 삭제

```
SFC4000T:/>security switch snmp group delete 1
```

보안 스위치 SNMP 그룹 조회

설명 :

SNMPv3 그룹 항목을 조회합니다.

통사:

보안 스위치 SNMP 그룹 조회 [<index>]

매개 변수 :

<index> : 항목 색인 (1-64)

예:

SNMPv3 그룹 항목 조회

```
SFC4000T:/>security switch snmp group lookup
Idx Model Security Name                    Group Name
--- ----- -------------------------------- --------------------------------
1   v1    public                           default_ro_group
2   v1    private                          default_rw_group
3   v2c   public                           default_ro_group
4   v2c   private                          default_rw_group
5   usm   default_user                     default_rw_group

Number of entries: 5
```

보안 스위치 SNMP 보기 추가

설명 :

SNMPv3 보기 항목을 추가 또는 수정하십시오.

입력 인덱스 키는 <view_name> 및 <oid_subtree>입니다.

통사:

보안 스위치 SNMP 보기 추가 <view_name> [included | excluded] <oid_subtree>

매개 변수 :

<view_name> :이 항목이 속해야하는보기 이름을 식별하는 문자열. 허용되는 문자열 길이는 (1-32)이며 허용되는 내용은 33 에서 126 사이의 ASCII 문자입니다

included :이 뷰 하위 트리가 포함되어야 함을 나타내는 선택적 플래그

excluded :이 뷰 하위 트리를 제외해야 함을 나타내는 선택적 플래그

<oid_subtree> : 명명 된 뷰에 추가 할 하위 트리의 루트를 정의하는 OID

예:

SNMPv3 보기 항목 추가

```
SFC4000T:/>security switch snmp view add snmpv3_view include .1
```

보안 스위치 SNMP 보기 삭제

설명 :

SNMPv3 보기 항목을 삭제하십시오.

통사:

보안 스위치 SNMP 보기 <index>

매개 변수 :

<index> : 항목 색인 (1-64)

예:

SNMPv3 보기 항목 삭제

```
SFC4000T:/>security switch snmp view delete 3
```

보안 스위치 SNMP 보기 조회

설명 :

SNMPv3 보기 항목을 조회합니다.

통사:

Security Switch SNMP View Lookup [<index>]

매개 변수 :

<index> : 항목 색인 (1-64)

예:

SNMPv3 보기 항목 조회

```
SFC4000T:/>security switch snmp view lookup
Idx   View Name                       View Type   OID Subtree
---   -------------------------------  ---------   -------------------------------
```

```
1    default_view                    included    .1
2    snmpv3_viwe                     included    .1

Number of entries: 2
```

보안 스위치 SNMP 액세스 추가

설명 :

SNMPv3 액세스 항목을 추가 또는 수정하십시오.

항목 색인 키는 <group_name>, <security_model> 및 <security_level>입니다.

통사:

보안 스위치 SNMP access <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>]

매개 변수 :

<group_name> :이 항목이 속해야하는 그룹 이름을 식별하는 문자열. 허용되는 문자열 길이는 (1-32)이며 허용되는 내용은 33 에서 126 사이의 ASCII 문자입니다

<security_model> : any - 허용되는 모든 보안 모델 (v1 | v2c | usm)

v1 - SNMPv1 용으로 예약 됨

v2c - SNMPv2c 를 위해 예약 됨

usm - 사용자 기반 보안 모델 (USM)

<security_level> : noAuthNoPriv - 인증 및 개인 정보 없음

AuthNoPriv - 인증 및 없음 개인 정보

AuthPriv - 인증 및 개인 정보

<read_view_name> :이 요청이 현재 값을 요청할 수있는 MIB 기능을 정의하는 MIB 보기의 이름입니다.

"없음"의 이름은 예약되어 있습니다.

허용되는 문자열 길이는 (1-32)이며 허용되는 내용은 33 에서 126 사이의 ASCII 문자입니다

예:

SNMPv3 액세스 항목 추가

```
SFC4000T:/>security switch snmp access add group_snmpv3 usm authpriv snmpv3_view
snmpv3_view
```

보안 스위치 SNMP 액세스 삭제

설명 :

SNMPv3 액세스 항목을 삭제하십시오.

통사:

보안 스위치 SNMP 액세스 삭제 <index>

매개 변수 :

<index> : 항목 색인 (1-64)

예:

SNMPv3 액세스 항목 삭제

```
SFC4000T:/>security switch snmp access delete 3
```

보안 스위치 SNMP 액세스 조회

설명:

SNMPv3 액세스 항목을 조회합니다.

통사:

보안 스위치 SNMP 액세스 조회 [<index>]

매개 변수 :

<index> : 항목 색인 (1-64)

예:

SNMPv3 액세스 항목 조회

```
SFC4000T:/>security switch snmp access lookup
Idx Group Name                          Model Level
--- ------------------------------- ----- --------------
1    default_ro_group                   any    NoAuth, NoPriv
2    default_rw_group                   any    NoAuth, NoPriv

Number of entries: 2
```

보안 스위치 RMON 통계 추가

설명 :

RMON 통계 항목을 추가 또는 수정하십시오. 항목 색인 키는 <stats_id>입니다.

통사:

보안 스위치 RMON 통계 <stats_id> <data_source>

매개 변수 :

<stats_id> : 통계 ID (1-65535).

<data_source> : ifEntry 의 ifIndex 를 나타내는 OID.

값은 .1.3.6.1.2.1.2.2.1.1.xxx 와 같아야합니다.

보안 스위치 RMON 통계 삭제

설명 :

RMON Statistics 항목을 삭제하십시오. 항목 색인 키는 <stats_id>입니다.

통사:

보안 스위치 RMON 통계 <stats_id>

매개 변수 :

<stats_id> : 통계 ID (1-65535).

보안 스위치 RMON 통계 조회

설명 :

RMON 통계 항목 표시.

통사:

보안 스위치 RMON 통계 조회 [<stats_id>]

매개 변수 :

<stats_id> : 통계 ID (1-65535).

보안 스위치 RMON 기록 추가

설명 :

RMON Hisotry 항목을 추가하거나 수정하십시오. 항목 색인 키는 <history_id>입니다.

통사:

보안 스위치 RMON 기록 <history_id> <data_source> [<interval>] [<buckets>]

매개 변수 :

<history_id> : 기록 ID (1-65535).

<data_source> : ifEntry 의 ifIndex 를 나타내는 OID.

값은 .1.3.6.1.2.1.2.2.1.1.xxx 와 같아야합니다.

<간격> : 샘플링 간격 (1 ~ 3600) (기본값 : 1800).

<버킷> : RMON (1-65535) (기본값 : 50)에 저장된이 기록 제어 항목과 관련된 최대 데이터 항목입니다.

보안 스위치 RMON 기록 삭제

설명 :

RMON Hisotry 항목을 삭제하십시오. 항목 색인 키는 <history_id>입니다.

통사:

보안 스위치 RMON 기록 삭제 <history_id>

매개 변수 :

<history_id> : 기록 ID (1-65535).

보안 스위치 RMON 히스토리 조회

설명 :

RMON 기록 항목을 표시합니다.

통사:

보안 스위치 RMON 내역 조회 [<history_id>]

매개 변수 :

<history_id> : 기록 ID (1-65535).

보안 스위치 RMON Alarm Add

설명 :

RMON Alarm 항목을 추가 또는 수정하십시오. 항목 색인 키는 <alarm_id>입니다.

통사:

보안 스위치 RMON 알람 <alarm_id> <interval> <alarm_vairable> [absolute | delta] <rising_threshold> <rising_event_index> <falling_threshold> <falling_event_index> [rising | falling | both]

매개 변수 :

<alarm_id> : 알람 ID (1-65535).

<간격> : 샘플링 간격 (1-2147483647) (기본값 : 30).

<alarm_vairable> : 참조해야하는 MIB OID 입니다.

.1.3.6.1.2.1.2.2.1.10.xxx - ifInOctets

.1.3.6.1.2.1.2.2.1.11.xxx - ifInUcastPkts

.1.3.6.1.2.1.2.2.1.12.xxx - ifInNUcastPkts

.1.3.6.1.2.1.2.2.1.13.xxx - ifInDiscards

.1.3.6.1.2.1.2.2.1.14.xxx - ifInErrors

.1.3.6.1.2.1.2.2.1.15.xxx - ifInUnkownProtos

.1.3.6.1.2.1.2.2.1.16.xxx - ifOutOctets

.1.3.6.1.2.1.2.2.1.17.xxx - ifOutUcastPkts

.1.3.6.1.2.1.2.2.1.18.xxx - ifOutNUcastPkts

.1.3.6.1.2.1.2.2.1.19.xxx - ifOutDiscards

.1.3.6.1.2.1.2.2.1.20.xxx - ifOutErrors

.1.3.6.1.2.1.2.2.1.21.xxx - ifOutQLen

"xxx"는이 색인의 특정 값으로 식별되는 인터페이스가 OID 'ifIndex'와 동일한 값으로 식별되는 동일한 인터페이스임을 의미합니다.

absolute : 샘플을 직접 가져옵니다.

델타 : 샘플 간의 차이를 계산합니다 (기본값).

<rising_threshold> : 상승 임계 값 (-2147483648-2147483647).

<rising_event_index> : 상승 이벤트 색인 (1-65535).

<falling_threshold> : 하강 임계 값 (-2147483648-2147483647).

<falling_event_index> : 하강 이벤트 인덱스 (1-65535).

rising : 첫 번째 값이 상승 임계 값보다 클 때 경보를 트리거합니다.

falling : 첫 번째 값이 하한 임계 값보다 작 으면 경보를 트리거합니다.

both : 첫 번째 값이 상승 임계 값보다 크거나 하강 임계 값보다 작 으면 경보를 트리거합니다 (기본값)

보안 스위치 RMON 알람 삭제

설명 :

RMON 알람 항목을 삭제하십시오. 항목 색인 키는 <alarm_id>입니다.

통사:

보안 스위치 RMON 알람 삭제 <alarm_id>

매개 변수 :

<alarm_id> : 알람 ID (1-65535).

보안 스위치 RMON 경보 조회

설명 :

RMON 알람 항목 표시.

통사:

보안 스위치 RMON 알람 조회 [<alarm_id>]

매개 변수 :

<alarm_id> : 알람 ID (1-65535).

보안 스위치 RMON 이벤트 추가

설명 :

RMON 이벤트 항목을 추가 또는 수정하십시오. 항목 색인 키는 <event_id>입니다.

통사:

보안 스위치 RMON 이벤트 <event_id> [없음 | 로그 | 트랩 | log_trap] [<커뮤니티>] [<설명>]

매개 변수 :

<event_id> : 이벤트 ID (1-65535).

none : 샘플을 직접 가져옵니다.

로그 : 샘플을 직접 가져옵니다.

함정 : 샘플을 직접 가져옵니다.

log_trap : 샘플 간의 차이를 계산합니다 (기본값).

<community> : 트랩을 보낼 때 커뮤니티를 지정합니다 (문자열 길이는 0 ~ 127) (기본값 : public).

<설명> :이 이벤트를 설명하는 문자열입니다 (길이는 0 ~ 127) (기본값 : null 문자열).

보안 스위치 RMON 이벤트 삭제

설명 :

RMON 이벤트 항목을 삭제하십시오. 항목 색인 키는 <event_id>입니다.

통사:

보안 스위치 RMON 이벤트 삭제 <event_id>

매개 변수 :

<event_id> : 이벤트 ID (1-65535).

보안 스위치 RMON 이벤트 조회

설명 :

RMON 이벤트 항목을 표시하십시오.

통사:

보안 스위치 RMON 이벤트 조회 [<event_id>]

매개 변수 :

<event_id> : 이벤트 ID (1-65535).

보안 네트워크 Psec 스위치

설명 :

포트 보안 상태 표시.

통사:

보안 네트워크 Psec 스위치 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

포트 보안 상태를 표시합니다.

```
SFC4000T:/>security network psec switch
Users:
L = Limit Control
8 = 802.1X
D = DHCP Snooping
V = Voice VLAN

Port   Users   State                MAC Cnt
----   -----   -------------        -------
1      ----    No users                 0
```

보안 네트워크 Psec 포트

설명 :

포트 보안에서 얻은 MAC 주소를 표시합니다.

통사:

보안 네트워크 Psec 포트 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

포트 1 에서 학습 한 MAC 주소 표시

```
SFC4000T:/>security network psec port 1

Port 1:
-------

MAC Address        VID    State       Added                      Age/Hold Time
-----------------  ----   ----------  -------------------------  -------------
<none>
```

보안 네트워크 제한 구성

설명 :

제한 제어 표시 제한.

통사:

보안 네트워크 한도 구성 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

제한 제어 표시 제한.

```
SFC4000T:/>security network limit configuration

Port Security Limit Control Configuration:
```

```
=======================================

Mode         : Disabled
Aging        : Disabled
Age Period: 3600

Port   Mode          Limit   Action
----    --------          -----   ---------------
1       Disabled        4     None
```

보안 네트워크 제한 모드

설명 :

전역 상태를 설정하거나 표시합니다.

통사:

보안 네트워크 제한 모드 [enable | disable]

매개 변수 :

enable : 전역 적으로 포트 보안 활성화

disable : 포트 보안을 전역 적으로 비활성화합니다.

(기본값 : 포트 보안 제한 제어의 현재 전역 활성화 표시)

기본 설정:

disable

예:

제한 모드 사용

```
SFC4000T:/>security network limit mode enable
```

보안 네트워크 한도 연장

설명 :

aging 상태를 설정하거나 표시합니다.

통사:

보안 네트워크 제한 에이징 [enable | disable]

매개 변수 :

활성화 : aging 활성화

사용 중지 : aging 해제

(기본값 : 현재 사용 가능한 aging 표시)

기본 설정:

disable

예:

한도 aging 활성화

```
SFC4000T:/>security network limit aging enable
```

보안 네트워크 제한 Agetime

설명 :

학습 된 MAC 주소의 활동을 확인하는 시간 (초).

통사:

보안 네트워크 제한 Agetime [<age_time>]

매개 변수 :

<age_time> : MAC 주소의 활동 확인 간격 (초) (10-10000000 초)

(기본값 : 현재 연령대 시간 표시)

기본 설정:

3600

예:

agetime 를 100 초로 설정하십시오.

```
SFC4000T:/>security network limit agetime 100
```

보안 네트워크 제한 포트

설명 :

포트 별 사용 가능 여부 설정 또는 표시.

통사:

보안 네트워크 제한 포트 [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable :이 포트에서 포트 보안 사용

disable :이 포트의 포트 보안을 비활성화합니다.

(기본값 : 포트 보안 제한 제어의 현재 포트 활성화 표시)

기본 설정:

disable

예:

포트 1 의 포트 제한 사용

```
SFC4000T:/>security network limit port 1 enable
```

보안 네트워크 한도

설명 :

최대 값을 설정하거나 표시하십시오. 이 포트 세트에서 학습 할 수있는 MAC 주소 수.

통사:

보안 네트워크 제한 한도 [<port_list>] [<limit>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<limit> : 최대 이 포트의 MAC 주소 수

(기본값 : 전류 제한 표시)

기본 설정:

4

예:

5 로 한도 설정

```
SFC4000T:/>security network limit limit 1-10 5
```

보안 네트워크 제한 조치

설명 :

한계를 초과하는 작업을 설정하거나 표시합니다.

통사:

보안 네트워크 제한 동작 [<port_list>] [none | trap | shut | trap_shut]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

none | trap | shut | trap_shut : MAC 주소의 수가 한계를 초과하는 경우 취해야 할 조치

none : 아무 것도하지 마라.

트랩 : SNMP 트랩 보내기

shut : 포트를 종료합니다.

trap_shut : SNMP 트랩을 보내고 포트를 종료합니다.

(기본값 : 현재 작업 표시)

기본 설정:

없음

예:

포트 1 의 제한 동작을위한 트랩 모드 설정

```
SFC4000T:/>security network limit action 1 trap
```

보안 네트워크 한도가 다시 열림

설명 :

한도를 초과 한 하나 이상의 포트를 다시 열고 종료하십시오.

통사:

보안 네트워크 제한 다시 열기 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

포트 1 다시 엽니 다.

```
SFC4000T:/>security network limit reopen 1
```

보안 네트워크 NAS 구성

설명 :

802.1X 구성을 표시합니다.

통사:

보안 네트워크 NAS 구성 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

포트 1 의 802.1X 구성 표시

```
SFC4000T:/>security network nas configuration 1

802.1X Configuration:
=====================

Mode                  : Disabled
Reauth.               : Disabled
Reauth. Period        : 3600
EAPOL Timeout         : 30
Age Period            : 300
Hold Time             : 10
RADIUS QoS            : Disabled
RADIUS VLAN           : Disabled
Guest VLAN            : Disabled
Guest VLAN ID         : 1
Max. Reauth Count: 2
Allow Guest VLAN if EAPOL Frame Seen: Disabled

Port   Admin State          Port State              Last Source          Last ID
----   ------------------   ---------------------   ------------------   ------------------
1      Force Authorized     Globally Disabled       -                    -
```

보안 네트워크 NAS 모드

설명 :

전역 NAS 상태를 설정하거나 표시합니다.

통사:

보안 네트워크 NAS 모드 [enable | disable]

매개 변수 :

enable : 802.1X 를 전역 적으로 활성화

disable : 802.1X 를 전역 적으로 비활성화합니다.

(기본값 : 현재 802.1X 전역 활성화 표시)

기본 설정:

disable

예:

IEEE802.1X 기능 활성화

```
SFC4000T:/>security network nas mode enable
```

보안 네트워크 NAS 상태

설명 :

포트 보안 상태를 설정하거나 표시합니다.

통사:

보안 네트워크 NAS 상태 [<port_list>] [auto | authorized | unauthorized | single | multi | macbased]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

auto : 포트 기반 802.1X 인증

승인 됨 : 포트 액세스가 허용됨

허가되지 않음 : 포트 액세스가 허용되지 않습니다.

단일 : 단일 호스트 802.1X 인증

multi : 다중 호스트 802.1X 인증

macbased : 클라이언트를 대신하여 스위치를 인증합니다.

(기본값 : 802.1X 상태 표시)

기본 설정:

없음

예:

포트 1 보안 상태를 표시합니다.

```
SFC4000T:/>security network nas state 1

Port   Admin State          Port State              Last Source          Last ID
----   -----------------    ---------------------   -----------------    -----------------
1      Force Authorized     Globally Disabled       -                    -
```

보안 네트워크 NAS 재 인증

설명 :

재 인증 상태를 설정하거나 표시합니다.

통사:

보안 네트워크 NAS 재 인증 [enable | disable]

매개 변수 :

enable : 재 인증 활성화

disable : 재 인증 비활성화

(기본값 : 현재 재 인증 모드 표시)

기본 설정:

disable

예:

재 인증 기능을 사용하십시오.

```
SFC4000T:/>security network nas reauthentication enable
```

보안 네트워크 NAS 재인증 간격

설명 :

재 인증 시도 간격을 설정하거나 표시하십시오.

통사:

보안 네트워크 NAS ReauthPeriod [<reauth_period>]

매개 변수 :

<reauth_period> : 재 인증 시도 간격 (1-3600 초)

(기본값 : 현재 재 인증 기간 표시)

기본 설정:

3600

예:

재 인증 시도 간격을 표시합니다.

```
SFC4000T:/>security network nas reauthperiod
```

보안 네트워크 NAS EapolTimeout

설명 :

EAPOL 재전송 사이의 시간을 설정하거나 표시합니다.

통사:

보안 네트워크 NAS EapolTimeout [<eapol_timeout>]

매개 변수 :

<eapol_timeout> : EAPOL 재전송 사이의 시간 (1-65535 초)

(기본값 : 현재 EAPOL 재전송 시간 초과 표시)

기본 설정:

30

예:

EAPOL 재전송 사이의 시간을 100 초로 설정하십시오.

```
SFC4000T:/>security network nas eapoltimeout 100
```

보안 네트워크 NAS Agetime

설명 :

성공적으로 인증 된 MAC 주소의 활동을 확인하는 시간 (초).

통사:

보안 네트워크 NAS Agetime [<age_time>]

매개 변수 :

<age_time> : 수표 사이의 시간 (10-1000000 초)

(기본값 : 현재 연령대 시간 표시)

기본 설정:

300 자

예:

NAS aging 시간을 1000 초 단위로 설정합니다.

```
SFC4000T:/>security network nas agetime 1000
```

보안 네트워크 NAS 대기 시간

설명 :

인증에 실패한 MAC 주소가 새로운 인증 기회를 얻는 데 걸리는 시간 (초).

통사:

보안 네트워크 NAS 대기 시간 [<hold_time>]

매개 변수 :

<hold_time> : 대기 시간 (10-1000000 초)

(기본값 : 현재 hold 시간 표시)

기본 설정:

10

예:

NAS 대기 시간을 100 초로 설정합니다.

```
SFC4000T:/>security network nas holdtime 100
```

보안 네트워크 NAS RADIUS_QoS

설명 :

전역 상태 (global 키워드 사용) 또는 RADIUS 할당 QoS 의 포트 별 상태를 설정하거나 표시합니다.

통사:

보안 네트워크 NAS RADIUS_QoS [global | <port_list>] [enable | disable]

매개 변수 :

global : 글로벌 RADIUS 할당 QoS 설정 선택

<port_list> : 포트 별 RADIUS 할당 QoS 설정 선택

(기본값 : 현재 포트 별 RADIUS 할당 QoS 상태 표시)

enable : RADIUS 로 할당 된 QoS 를 전역 또는 하나 이상의 포트에서 활성화합니다.

disable : RADIUS 할당 QoS 를 전역 또는 하나 이상의 포트에서 비활성화합니다.

(기본값 : 현재 RADIUS 할당 QoS 상태 표시)

기본 설정:

disable

예:

NAS RADIUS QoS 활성화

```
SFC4000T:/>security network nas radius_qos enable
```

보안 네트워크 NAS RADIUS_VLAN

설명 :

전역 상태 (global 키워드 사용) 또는 RADIUS 할당 VLAN 의 포트 별 상태를 설정하거나 표시합니다.

통사:

보안 네트워크 NAS RADIUS_VLAN [global | <port_list>] [enable | disable]

매개 변수 :

global : 글로벌 RADIUS 할당 VLAN 설정 선택

<port_list> : 포트 별 RADIUS 할당 VLAN 설정 선택

(기본값 : 현재 포트 별 RADIUS 할당 VLAN 상태 표시)

enable : RADIUS 로 할당 된 VLAN 을 전역 또는 하나 이상의 포트에서 활성화합니다.

disable : RADIUS 로 할당 된 VLAN 을 전역 또는 하나 이상의 포트에서 비활성화합니다.

(기본값 : 현재 RADIUS 로 할당 된 VLAN 상태 표시)

기본 설정:

disable

예:

NAS RADIUS VLAN 활성화

```
SFC4000T:/>security network nas radius_vlan enable
```

보안 네트워크 NAS Guest_VLAN

설명 :

전역 상태와 매개 변수 (global 키워드 사용) 또는 게스트 VLAN 의 포트 별 상태를 설정하거나 표시합니다.

'global'키워드가 사용되지 않으면 <reauth_max> 및 <allow_if_eapol_seen> 매개 변수가 사용되지 않습니다.

통사:

보안 네트워크 NAS Guest_VLAN [global | <port_list>] [enable | disable] [<vid>] [<reauth_max>] [<allow_if_eapol_seen>]

매개 변수 :

global : 전역 게스트 VLAN 설정을 선택하십시오.

<port_list> : 포트 별 게스트 VLAN 설정 선택

(기본값 : 현재 포트 별 게스트 VLAN 상태 표시)

enable | disable : enable : 게스트 VLAN 을 전역 또는 하나 이상의 포트에서 사용 가능하게합니다.

disable : 게스트 VLAN 을 전역 또는 하나 이상의 포트에서 비활성화합니다.

(기본값 : 현재 게스트 VLAN 상태 표시)

<vid> : 게스트 VLAN 을 입력 할 때 사용되는 게스트 VLAN ID 입니다. '글로벌'키워드를 사용하여 변경하십시오.

(기본값 : 현재 게스트 VLAN ID 표시)

<reauth_max> : 명령의 시작 부분에 'global'키워드를 사용하는 경우에만 값을 설정할 수 있습니다.

게스트 VLAN 을 입력하기 전에 요청 Identity EAPOL 프레임이 응답없이 전송 된 횟수

(기본값 : 현재 최대 재실행 횟수 표시

<allow_if_eapol_seen> : 명령의 시작 부분에 'global'키워드를 사용하는 경우에만 값을 설정할 수 있습니다.

disable : 포트 aging 동안 포트에서 수신 된 EAPOL 프레임이없는 경우에만 게스트 VLAN 을 입력 할 수 있습니다

enable : EAPOL 프레임이 포트 aging 동안 수신 된 경우에도 게스트 VLAN 을 입력 할 수 있습니다

(기본값 : 현재 설정 표시)

기본 설정:

disable

예:

NAS 게스트 VLAN 사용

```
SFC4000T:/>security network nas guest_vlan enable
```

보안 네트워크 NAS 인증

설명 :

802.1X 인증 프로세스를 새로 고칩니다 (다시 시작).

통사:

보안 네트워크 NAS 인증 [<port_list>] [now]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

지금 : 재 인증 즉시 적용

(기본값 : 재 인증 예약)

예:

포트 1 에 대한 NAS 인증을 지금 시작하십시오.

```
SFC4000T:/>security network nas authenticate 1 now
```

보안 네트워크 NAS 통계

설명 :

802.1X 통계를 보거나 지 웁니다.

통사:

보안 네트워크 NAS 통계 [<port_list>] [clear | eapol | radius]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

clear : 통계 지우기

eapol : EAPOL 통계보기

radius : 백엔드 서버 통계 표시

(기본값 : 모든 통계 표시)

예:

포트 1 에 802.1X 통계 표시

```
SFC4000T:/>security network nas statistics 1
Rx Total:                    0    Tx Total:                    0
Rx Response/Id:              0    Tx Request/Id:               0
Rx Response:                 0    Tx Request:                  0
Rx Start:                    0
Rx Logoff:                   0
Rx Invalid Type:             0
Rx Invalid Length:           0

Port 1 Backend Server Statistics:

Rx Access Challenges:        0    Tx Responses:                0
Rx Other Requests:           0
```

Rx Auth. Successes: 0
Rx Auth. Failures: 0

보안 네트워크 ACL 구성

설명 :

ACL 구성 표시.

통사:

보안 네트워크 ACL 구성 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

보안 네트워크 ACL 작업

설명 :

ACL 포트 기본 조치를 설정하거나 표시하십시오.

통사:

보안 네트워크 ACL 작업 [<port_list>] [허용 | 거부] [<rate_limiter>] [<port_redirect>] [<logging>] [<shutdown>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

허용 : 전달 허용 (기본값)

거부 : 전달 거부

<rate_limiter> : 속도 제한 기 번호 (1 ~ 15) 또는 '사용 안함'

<port_copy> : 프레임 복사를위한 포트 번호 또는 '비활성화'

<logging> : 프레임의 시스템 로깅 : log | log_disable

<shutdown> : 입구 포트 종료 : shut | shut_disable

예:

포트 1 에 ACL 작업 표시

SFC4000T:/>**security network acl action 1**

```
Port   Action   Rate Limiter   Port Copy   Mirror     Logging    Shutdown   Counter
----   ------   ------------   ---------   --------   --------   --------   -------
1      Permit   Disabled       Disabled    Disabled   Disabled   Disabled   0
```

보안 네트워크 ACL 정책

설명 :

ACL 포트 정책을 설정하거나 표시하십시오.

통사:

보안 네트워크 ACL 정책 [<port_list>] [<policy>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<policy> : 정책 번호 (0-255)

기본 설정:

0

예:

포트 1 에 대한 ACL policy 2 설정

```
SFC4000T:/>security network acl policy 1 2
```

보안 네트워크 ACL 비율

설명 :

ACL 속도 제한기를 설정하거나 표시하십시오.

통사:

보안 네트워크 ACL 비율 [<rate_limiter_list>] [<rate>]

매개 변수 :

<rate_limiter_list> : 속도 제한 기 목록 (1-16), 기본값 : 모든 속도 제한 기

<rate> : 요율 (PPS) (0-131071)

기본 설정:

1

예:

포트 1 의 속도 제한 값을 100 으로 설정하십시오.

```
SFC4000T:/>security network acl rate 1 100
```

Security Network ACL Add

설명:

ACE (액세스 제어 항목)를 추가하거나 수정합니다.

ACE ID 매개 변수 <ace_id>가 지정되고이 ACE ID 가있는 항목이 이미 있으면 ACE 가 수정됩니다. 그렇지 않으면 새 ACE 가 추가됩니다. ACE ID 를 지정하지 않으면 사용 가능한 다음 ACE ID 가 사용됩니다.

다음 ACE ID 매개 변수 <ace_id_next>가 지정되면 ACE 는이 ACE 앞에 나열됩니다. 다음 ACE ID 가 지정되지 않으면 ACE 가 목록의 마지막에 배치됩니다.

Switch 키워드를 사용하면 규칙이 모든 포트에 적용됩니다. Port 키워드를 사용하면 규칙은 지정된 포트에만 적용됩니다. Policy 키워드가 사용되면 규칙은 지정된 정책으로 구성된 모든 포트에 적용됩니다. 기본값은 규칙이 모든 포트에 적용된다는 것입니다..

Syntax:

Security Network ACL Add [<ace_id>] [<ace_id_next>] [(port <port>)] [(policy <policy> <policy_bitmask>)] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit|deny] [<rate_limiter>] [<port_redirect>] [<logging>] [<shutdown>]

매개 변수 :

<ace_id> : ACE ID (1-512), 기본값 : 다음 사용 가능한 ID

<ace_id_next> : 다음 ACE ID (1-512), 기본값 : ACE 를 마지막으로 추가

port : 포트 ACE 키워드

<port> : 포트 번호 또는 'all'

정책 : 정책 ACE 키워드

<policy> : 정책 번호 (0-255)

<policy_bitmask> : 정책 번호 비트 마스크 (0x0-0xFF)

<vid> : VLAN ID (1-4095) 또는 'any'

<tag_prio> : VLAN 태그 우선 순위 (0-7) 또는 'any'

<dmac_type> : DMAC 유형 : any | unicast | multicast | 브로드 캐스트

etype : 이더넷 유형 키워드

<etype> : 이더넷 유형 : 0x600 - 0xFFFF 또는 'any'(0x800 (IPv4) 0x806 (ARP) 및 0x86DD (IPv6) 제외)

<smac> : 원본 MAC 주소 ('xx-xx-xx-xx-xx-xx'또는 'xx.xx.xx.xx.xx.xx'또는 'xxxxxxxxxxxx', x 는 16 진수) 또는 'any'

<dmac> : 대상 MAC 주소 ('xx-xx-xx-xx-xx-xx'또는 'xx.xx.xx.xx.xx.xx'또는 'xxxxxxxxxxxx', x 는 16 진수) 또는 'any'

arp : ARP 키워드

<sip> : 소스 IP 주소 (a.b.c.d / n) 또는 'any'

<dip> : 대상 IP 주소 (a.b.c.d / n) 또는 'any'

<arp_opcode> : ARP 작업 코드 : any | arp | rarp | 기타

<arp_flags> : ARP 플래그 : 요청 | smac | tmac | len | ip | ether [0 | 1 | any]

ip : IP 키워드

<protocol> : IP 프로토콜 번호 (0-255) 또는 'any'

<ip_flags> : IP 플래그 : ttl | options | fragment [0 | 1 | any]

icmp : ICMP 키워드

<icmp_type> : ICMP 유형 번호 (0-255) 또는 'any'

<icmp_code> : ICMP 코드 번호 (0-255) 또는 'any'

udp : UDP 키워드

<sport> : 소스 UDP / TCP 포트 범위 (0-65535) 또는 'any'

<dport> : 대상 UDP / TCP 포트 범위 (0-65535) 또는 'any'

tcp : TCP 키워드

<tcp_flags> : TCP 플래그 : fin | syn | rst | psh | ack | urg [0 | 1 | any]

허용 : 전달 허용 (기본값)

거부 : 전달 거부

<rate_limiter> : 속도 제한 기 번호 (1 ~ 15) 또는 '사용 안함'

<port_redirect> : 프레임 복사를위한 포트 번호 또는 '비활성화'

<logging> : 프레임의 시스템 로깅 : log | log_disable

<shutdown> : 입구 포트 종료 : shut | shut_disable

보안 네트워크 ACL 삭제

설명 :

ACE 를 삭제하십시오.

통사:

보안 네트워크 ACL 삭제 <ace_id>

매개 변수 :

<ace_id> : ACE ID (1-512)

예:

ACE 1 삭제

```
SFC4000T:/>security network acl delete 1
```

보안 네트워크 ACL 조회

설명 :

ACE 표시, 기본값 : 모든 ACE.

통사:

보안 네트워크 ACL 조회 [<ace_id>]

매개 변수 :

<ace_id> : ACE ID (1-512)

예:

ACE 1 조회

```
SFC4000T:/>security network acl lookup 1
```

보안 네트워크 ACL 클리어

설명 :

모든 ACL 카운터를 지 웁니다.

통사:

보안 네트워크 ACL 클리어

예:

모든 ACL 카운터를 지 웁니다.

```
SFC4000T:/>security network acl clear
```

보안 네트워크 ACL 상태

설명 :

ACL 상태를 표시합니다.

통사:

보안 네트워크 ACL 상태 [combined | static | loop_protect | dhcp | upnp | arp_inspection | ipmc | ip_source_guard | conflicts]

매개 변수 :

결합 : 결합 상태 표시

static : 정적 사용자 구성 상태 표시

loop_protect : 루프 보호로 상태를 표시합니다.

dhcp : DHCP 상태 표시

upnp : UPnP 상태 표시

arp_inspection : ARP 검사 상태 표시

ipmc : IPMC 상태 표시

ip_source_guard : IP 소스 가드 상태 표시

충돌 : 충돌 상태 표시

(기본값 : 결합 상태 표시)

예:

ACL 상태를 표시합니다.

```
SFC4000T:/>security network acl status
```

보안 네트워크 ACL 포트 상태

설명 :

ACL 포트 상태를 설정하거나 표시합니다.

통사:

보안 네트워크 ACL 포트 상태 [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable | disable : ACL 포트 상태

기본 설정:

사용

보안 네트워크 DHCP 릴레이 구성

설명 :

DHCP 릴레이 구성 표시.

통사:

보안 네트워크 DHCP 릴레이 구성

예:

DHCP 릴레이 구성 표시.

```
SFC4000T:/>security network dhcp relay configuration

DHCP Relay Configuration:
=========================

DHCP Relay Mode                    : Disabled
DHCP Relay Server                  : NULL
DHCP Relay Information Mode        : Disabled
DHCP Relay Information Policy : replace
```

보안 네트워크 DHCP 릴레이 모드

설명 :

DHCP 릴레이 모드를 설정하거나 표시합니다.

통사:

보안 네트워크 DHCP 릴레이 모드 [enable | disable]

매개 변수 :

enable : DHCP 관련 모드를 사용합니다. DHCP 릴레이 모드 작업을 활성화하면 에이전트는 동일한 서브넷 도메인에 있지 않을 때 클라이언트와 서버간에 DHCP 메시지를 전달하고 전달합니다. 그리고 DHCP 브로드 캐스트 메시지는 고려 된 보안을 위해 범람하지 않을 것입니다.

disable : DHCP relaly 모드를 비활성화합니다.

(기본값 : Show flow DHCP relaly mode)

기본 설정:

disable

예:

DHCP 릴레이 모드 사용

```
SFC4000T:/>security network dhcp relay mode enable
```

보안 네트워크 DHCP 릴레이 서버

설명 :

DHCP 릴레이 서버를 보거나 설정하십시오.

통사:

보안 네트워크 DHCP 릴레이 서버 [<ip_addr>]

매개 변수 :

<ip_addr> : IP 주소 (a.b.c.d), 기본값 : IP 주소 표시

기본 설정:

없는

예:

192.168.0.20 에 DHCP 릴레이 서버 설정

```
SFC4000T:/>security network dhcp relay server 192.168.0.20
```

보안 네트워크 DHCP 릴레이 정보 모드

설명 :

DHCP 릴레이 에이전트 정보 옵션 모드를 설정하거나 표시합니다.

DHCP 릴레이 정보 모드 작동을 활성화하면 에이전트는 DHCP 서버로 전달할 때 DHCP 메시지에 특정 정보 (옵션 82)를 삽입하고 DHCP 클라이언트로 전송할 때 DHCP 메시지에서 원격 정보를 삽입합니다 (옵션 82). DHCP 릴레이 작동 모드에서만 작동합니다.

통사:

보안 네트워크 DHCP 릴레이 정보 모드 [enable | disable]

매개 변수 :

enable : DHCP 릴레이 에이전트 정보 옵션 모드 사용

disable : DHCP 릴레이 에이전트 정보 옵션 모드 비활성화

(기본값 : DHCP 릴레이 에이전트 정보 표시 옵션 모드)

기본 설정:

disable

예: DHCP 릴레이 에이전트 정보 옵션 모드를 사용합니다.

```
SFC4000T:/>security network dhcp relay information mode enable
```

보안 네트워크 DHCP 릴레이 정보 정책

설명 :

DHCP 릴레이 모드를 설정하거나 표시합니다.

DHCP 릴레이 정보 모드 작동을 활성화하면 에이전트가 이미 릴레이 에이전트 정보가 포함 된 DHCP 메시지를 수신합니다. 정책을 집행 할 것입니다.

통사:

보안 네트워크 DHCP 릴레이 정보 정책 [replace | keep | drop]

매개 변수 :

replace : 이미 포함하고있는 DHCP 메시지를 수신하면 원래의 중계 정보를 교체합니다.

유지 : 원래의 릴레이 정보를 이미 포함하고있는 DHCP 메시지를 받으면 원래의 릴레이 정보를 유지하십시오.

drop : 이미 중계 정보가 들어있는 DHCP 메시지를 받으면 패키지를 버립니다.

(기본값 : DHCP 릴레이 정보 정책 표시)

기본 설정:

바꾸다

예:

이미 포함되어있는 DHCP 메시지를 수신하면 원래의 릴레이 정보를 유지하십시오.

```
SFC4000T:/>security network dhcp relay information policy keep
```

보안 네트워크 DHCP 릴레이 통계

설명 :

DHCP 릴레이 통계를 표시하거나 지우십시오.

통사:

보안 네트워크 DHCP 릴레이 통계 [지우기]

매개 변수 :

clear : DHCP 릴레이 통계 지우기

예:

DHCP 릴레이 통계를 표시합니다.

```
SFC4000T:/>security network dhcp relay statistics
```

보안 네트워크 DHCP 스누핑 구성

설명 :

DHCP 스누핑 구성 표시.

통사:

보안 네트워크 DHCP 스누핑 구성

보안 네트워크 DHCP 스누핑 모드

설명 :

DHCP 스누핑 모드를 설정하거나 표시하십시오.

통사:

보안 네트워크 DHCP 스누핑 모드 [enable | disable]

매개 변수 :

활성화 : DHCP 스누핑 모드를 활성화합니다.

DHCP 스누핑 모드 작동을 활성화하면 요청 DHCP 메시지가 trust 된 포트로 전달되고 trust 된 포트의 응답 패킷 만 허용됩니다.

disable : DHCP 스누핑 모드를 비활성화합니다.

(기본값 : 흐름 표시 DHCP 스누핑 모드)

기본 설정:

disable

예:

DHCP 스누핑 모드 사용

```
SFC4000T:/>security network dhcp snooping mode enable
```

보안 네트워크 DHCP 스누핑 포트 모드

설명 :

DHCP 스누핑 포트 모드를 설정하거나 표시하십시오.

통사:

보안 네트워크 DHCP 스누핑 포트 모드 [<port_list>] [trusted | untrusted]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

trusted : 포트를 DHCP 메시지의 신뢰할 수있는 원본으로 구성합니다.

untrusted : 포트를 DHCP 메시지의 신뢰할 수없는 소스로 구성합니다.

(기본값 : Show flow DHCP 스누핑 포트 모드)

기본 설정:

신뢰할 수있는

예:

포트 1 에서 신뢰할 수없는 DHCP 스누핑 포트 모드 설정

```
SFC4000T:/>security network dhcp snooping port mode 1 untrusted
```

보안 네트워크 DHCP 스누핑 통계

설명 :

DHCP 스누핑 통계를 표시하거나 지우십시오.

통사:

보안 네트워크 DHCP 스누핑 통계 [<port_list>] [clear]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

clear : DHCP 스누핑 통계 지우기

예:

포트 1 의 DHCP 스누핑 통계를 표시합니다.

```
SFC4000T:/>security network dhcp snooping statistics 1
Port 1 Statistics:
--------------------
Rx Discover:                    0    Tx Discover:                    0
```

Rx Offer:	**0**	**Tx Offer:**	**0**
Rx Request:	**0**	**Tx Request:**	**0**
Rx Decline:	**0**	**Tx Decline:**	**0**
Rx ACK:	**0**	**Tx ACK:**	**0**
Rx NAK:	**0**	**Tx NAK:**	**0**
Rx Release:	**0**	**Tx Release:**	**0**
Rx Inform:	**0**	**Tx Inform:**	**0**
Rx Lease Query:	**0**	**Tx Lease Query:**	**0**
Rx Lease Unassigned:	**0**	**Tx Lease Unassigned:**	**0**
Rx Lease Unknown:	**0**	**Tx Lease Unknown:**	**0**
Rx Lease Active:	**0**	**Tx Lease Active:**	**0**

보안 네트워크 IP 소스 가드 구성

설명 :

IP 소스 가드 구성을 표시합니다.

통사:

보안 네트워크 IP 소스 가드 구성

보안 네트워크 IP 소스 가드 모드

설명 :

IP 소스 보호 모드를 설정하거나 표시합니다.

통사:

보안 네트워크 IP 소스 가드 모드 [enable | disable]

매개 변수 :

enable : IP 소스 가드 활성화

disable : IP Source Guard 를 비활성화합니다.

기본 설정:

disable

예:

IP 소스 보호 모드 사용

```
SFC4000T:/>security network ip source guard mode enable
```

보안 네트워크 IP 소스 가드 포트 모드

설명 :

IP 소스 가드 포트 모드를 설정하거나 표시하십시오.

통사:

보안 네트워크 IP 소스 가드 모드 [enable | disable]

매개 변수 :

enable : IP 소스 가드 활성화

disable : IP Source Guard 를 비활성화합니다.

기본 설정:

disable

예:

IP 소스 가드 포트 모드 사용

```
SFC4000T:/>security network ip source guard port mode enable
```

보안 네트워크 IP 소스 가드 제한

설명 :

동적 항목에 대한 IP 소스 가드 포트 제한을 설정하거나 표시하십시오.

통사:

보안 네트워크 IP 소스 가드 제한 [<port_list>] [<dynamic_entry_limit> | 무제한]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<dynamic_entry_limit> | 무제한 : 동적 항목 제한 (0-2) 또는 무제한

기본 설정:

제한 없는

예:

IP 소스 가드 한계 설정

```
SFC4000T:/>security network ip source guard 1 1
```

보안 네트워크 IP 소스 가드 항목

설명 :

IP 소스 가드 정적 항목을 추가 또는 삭제하십시오.

통사:

보안 네트워크 IP 소스 가드 항목 [<port_list>] add | delete <vid> <allowed_ip> <ip_mask>

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

add : 새 포트 IP 소스 가드 정적 항목 추가

삭제 : 기존 포트 IP 소스 가드 정적 항목 삭제

<vid> : VLAN ID (1-4095)

<allowed_ip> : IPv4 주소 (a.b.c.d), IP 소스 보호를 허용하는 IP 주소

<ip_mask> : IPv4 마스크 (a.b.c.d), 허용 된 IP 주소의 IP 마스크

예:

IP 소스 가드 정적 항목을 추가하십시오

```
SFC4000T:/>security network ip source guard entry 1 add 1 192.168.0.20
```

보안 네트워크 IP 소스 가드 상태

설명 :

IP 소스 가드 정적 및 동적 항목을 표시합니다.

통사:

보안 네트워크 IP 소스 가드 상태 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

IP 소스 가드 정적 및 동적 항목을 표시합니다.

```
SFC4000T:/>security network ip source guard status
```

보안 네트워크 IP 소스 가드 변환

설명 :

IP 소스 가드 동적 항목을 정적 항목으로 변환합니다.

통사:

보안 네트워크 IP 소스 가드 번역

보안 네트워크 ARP 검사 구성

설명 :

ARP 검사 구성을 표시합니다.

통사:

보안 네트워크 ARP 검사 구성

예:

ARP 검사 구성을 표시합니다.

```
SFC4000T:/>security network arp inspection configuration
```

보안 네트워크 ARP 검사 모드

설명 :

ARP 검사 모드를 설정하거나 표시합니다.

통사:

보안 네트워크 ARP 검사 모드 [enable | disable]

매개 변수 :

enable : ARP 검사 활성화

disable : ARP 검사 비활성화

기본 설정:

disable

예:

ARP 검사 모드 사용

```
SFC4000T:/>security network arp inspection mode enable
```

보안 네트워크 ARP 검사 포트 모드

설명 :

ARP 검사 포트 모드를 설정하거나 표시합니다.

통사:

보안 네트워크 ARP 검사 포트 모드 [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable : ARP 검사 포트 사용

disable : ARP 검사 포트 비활성화

(기본값 : ARP 검사 포트 모드 표시)

기본 설정:

사용 안함

예:

포트 1 의 ARP 검사 모드 활성화

```
SFC4000T:/>security network arp inspection port mode 1
```

보안 네트워크 ARP 검사 항목

설명 :

ARP 검사 정적 항목을 추가 또는 삭제합니다.

통사:

보안 네트워크 ARP 검사 항목 [<port_list>] add | delete <vid> <allowed_mac> <allowed_ip>

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

add : 새 포트 ARP 검사 정적 항목 추가

삭제 : 기존 포트 ARP 검사 정적 항목 삭제

<vid> : VLAN ID (1-4095)

<allowed_mac> : MAC 주소 ('xx-xx-xx-xx-xx-xx'또는 'xx.xx.xx.xx.xx.xx'또는 'xxxxxxxxxxxx', x 는 16 진수), 허용 된 MAC 주소 ARP 요청 수행 중

<allowed_ip> : IPv4 주소 (a.b.c.d), ARP 요청을 허용하는 IP 주소

예:

ARP 검사 정적 항목을 추가하십시오.

```
SFC4000T:/>security network arp inspection entry 1 add 1 00-30-4f-00-00-11 192.168.0.11
```

보안 네트워크 ARP 검사 상태

설명 :

ARP 검사 정적 및 동적 항목 표시.

통사:

보안 네트워크 ARP 검사 상태 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

ARP 검사 정적 및 동적 항목 표시.

```
SFC4000T:/>security network arp inspection status
```

보안 네트워크 ARP 검사 번역

설명 :

ARP 검사 동적 항목을 정적 항목으로 변환합니다.

통사:

보안 네트워크 ARP 검사 번역

보안 AAA 구성

설명 :

인증 구성 표시.

통사:

보안 AAA 구성

예:

인증 구성 표시.

```
SFC4000T:/>security aaa configuration
```

```
AAA Configuration:
==================



Server Timeout     : 15 seconds


Server Dead Time : 300 seconds


RADIUS Authentication Server Configuration:
=========================================
Server   Mode        IP Address          Secret                          Port
------    --------     ---------------     ------------------------------    -----
1         Disabled                                                       1812
2         Disabled                                                       1812
3         Disabled                                                       1812
4         Disabled                                                       1812
5         Disabled                                                       1812


RADIUS Accounting Server Configuration:
=====================================
Server   Mode        IP Address          Secret                          Port
------    --------     ---------------     ------------------------------    -----
1         Disabled                                                       1813
2         Disabled                                                       1813
3         Disabled                                                       1813
4         Disabled                                                       1813
5         Disabled                                                       1813


TACACS+ Authentication Server Configuration:
==========================================
Server   Mode        IP Address          Secret                          Port
------    --------     ---------------     ------------------------------    -----
1         Disabled                                                         49
2         Disabled                                                         49
3         Disabled                                                         49
4         Disabled                                                         49
5         Disabled                                                         49
```

보안 AAA 시간 초과

설명 :

서버 시간 초과를 설정하거나 표시하십시오.

통사:

보안 AAA 시간 초과 [<timeout>]

매개 변수 :

<timeout> : 서버 응답 시간 초과 (3-3600 초)

(기본값 : 서버 시간 초과 구성 표시)

기본 설정:

15 명

예:

서버 시간 초과를 위해 30 초 설정

```
SFC4000T:/>security aaa timeout 30
```

보안 AAA 데드 타임

설명 :

서버 데드 타임을 설정하거나 표시합니다.

통사:

보안 AAA 데드 타임 [<dead_time>]

매개 변수 :

<dead_time> : 요청에 응답하지 않으면 서버가 작동하지 않는 것으로 간주되는 시간 (0-3600 초)

(기본값 : 서버 데드 타임 구성 표시)

기본 설정:

300 자

예:

서버 불감 시간 1000sec 설정

```
SFC4000T:/>security aaa deadtime 1000
```

보안 AAA RADIUS

설명 :

RADIUS 인증 서버 설정을 지정하거나 표시합니다.

통사:

보안 AAA RADIUS [<server_index>] [enable | disable] [<ip_addr_string>] [<secret>] [<server_port>]

매개 변수 :

서버 색인 (1-5)

(기본값 : RADIUS 인증 서버 구성 표시)

enable : RADIUS 인증 서버 사용

disable : RADIUS 인증 서버를 비활성화합니다.

(기본값 : RADIUS 서버 모드 표시)

<ip_addr_string> : IP 호스트 주소 (a.b.c.d) 또는 호스트 이름 문자열

<secret> : 외부 인증 서버와 공유되는 비밀.

비어있는 비밀을 설정하려면 두 개의 따옴표 ("")를 사용하십시오.

비밀리에 공백을 사용하려면 그 비밀을 인용하십시오.

비밀에있는 따옴표는 허용되지 않습니다.

<server_port> : 서버 UDP 포트. 0 을 사용하여 기본 RADIUS 포트 사용 (1812)

예:

RADIUS 인증 서버 구성을 설정합니다.

```
SFC4000T:/>security aaa radius 1 enable 192.168.0.20 12345678 1812
```

보안 AAA ACCT_RADIUS

설명 :

RADIUS 계정 설정을 설정하거나 보여줍니다.

통사:

보안 AAA ACCT_RADIUS [<server_index>] [enable | disable] [<ip_addr_string>] [<secret>] [<server_port>]

매개 변수 :

서버 색인 (1-5)

(기본값 : RADIUS 계정 서버 구성 표시)

enable : RADIUS 계정 서버 사용

disable : RADIUS 계정 서버 사용 안 함

(기본값 : RADIUS 서버 모드 표시)

<ip_addr_string> : IP 호스트 주소 (a.b.c.d) 또는 호스트 이름 문자열

<secret> : 외부 회계 서버와 공유되는 비밀.

비어있는 비밀을 설정하려면 두 개의 따옴표 ("")를 사용하십시오.

비밀리에 공백을 사용하려면 그 비밀을 인용하십시오.

비밀에있는 따옴표는 허용되지 않습니다.

<server_port> : 서버 UDP 포트. 0 을 사용하여 기본 RADIUS 포트 사용 (1813)

예:

RADIUS 계정 서버 구성을 설정합니다.

```
SFC4000T:/>security acct_radius 1 enable 192.168.0.20 12345678 1813
```

보안 AAA TACACS +

설명 :

TACACS + 인증 서버 설정을 설정하거나 표시하십시오.

통사:

보안 AAA TACACS + [<server_index>] [enable | disable] [<ip_addr_string>] [<secret>] [<server_port>]

매개 변수 :

서버 색인 (1-5)

(기본값 : Show TACACS + 인증 서버 구성)

enable : TACACS + 인증 서버 사용

disable : TACACS + 인증 서버를 비활성화합니다.

(기본값 : TACACS + 서버 모드 표시)

<ip_addr_string> : IP 호스트 주소 (a.b.c.d) 또는 호스트 이름 문자열

<secret> : 외부 인증 서버와 공유되는 비밀.

비어있는 비밀을 설정하려면 두 개의 따옴표 ("")를 사용하십시오.

비밀리에 공백을 사용하려면 그 비밀을 인용하십시오.

비밀에있는 따옴표는 허용되지 않습니다.

<server_port> : 서버 TCP 포트. 0 을 사용하여 기본 TACACS + 포트 (49) 사용

예:

TACACS + 인증 서버 구성을 설정하십시오.

```
SFC4000T:/>security aaa tacacs+ 1 enable 192.168.0.20 12345678 49
```

보안 AAA 통계

설명 :

RADIUS 통계를 표시합니다.

통사:

보안 AAA 통계 [<server_index>]

매개 변수 :

서버 색인 (1-5)

(기본값 : 모든 서버에 대한 통계 표시)

예:

RADIUS 통계를 표시합니다.

```
SFC4000T:/>security aaa statistics
```

5.8 Spanning Tree Protocol 명령어

STP 구성

설명 :

STP 브리지 구성을 표시합니다.

구문 :

STP 구성

예 :

STP 구성을 표시합니다.

```
SFC4000T:/>stp cofiguration
```

```
STP Configuration:
==================

Protocol Version: MSTP
Max Age              : 20
Forward Delay    : 15
Tx Hold Count    : 6
Max Hop Count    : 20
BPDU Filtering   : Disabled
BPDU Guard         : Disabled
Error Recovery   : Disabled
```

STP 버전

설명 :

STP 브리지 프로토콜 버전을 설정하거나 표시합니다.

통사:

STP 버전 [<stp_version>]

매개 변수 :

<stp_version> : mstp | rstp | stp

기본 설정:

MSTP

예:

STP 브리지 프로토콜 버전을 설정합니다.

```
SFC4000T:/> stp version rstp
```

STP Tx Hold

설명 :

STP Bridge Transmit Hold Count 매개 변수를 설정하거나 표시합니다.

통사:

STP Txhold [<holdcount>]

매개 변수 :

<홀드 카운트> : STP 송신 홀드 카운트 (1-10)

기본 설정:

6

예:

STP Tx 10 을 설정합니다.

```
SFC4000T:/>stp txhold 10
```

STP MaxHops

설명 :

MSTP Bridge Max Hop Count 매개 변수를 설정하거나 표시하십시오.

통사:

STP MaxHops [<maxhops>]

매개 변수 :

<maxhops> : STP BPDU MaxHops (6-40)

기본 설정:

20

예:

STP 최대 홉을 25 로 설정하십시오.

```
SFC4000T:/>stp maxhops 25
```

STP MaxAge

설명 :

브리지 인스턴스 최대 aging 을 설정하거나 표시합니다.

통사:

STP MaxAge [<max_age>]

매개 변수 :

<max_age> : STP 최대 에이징 시간 (6-40 및 max_age <= (forward_delay-1) * 2)

기본 설정:

20

예:

STP 최대 aging 시간을 10 으로 설정

```
SFC4000T:/>stp maxage 10
```

STP FwdDelay

설명 :

브리지 인스턴스 전달 지연을 설정하거나 표시합니다.

통사:

STP FwdDelay [<지연>]

매개 변수 :

<지연> : MSTP 전달 지연 (4-30 및 max_age <= (forward_delay-1) * 2))

기본 설정:

15 명

예:

STP 전달 지연 값을 25 로 설정합니다.

```
SFC4000T:/>stp fwddelay 25
```

STP CName

설명 :

MSTP 구성 이름 및 개정을 설정 또는 표시하십시오.

통사:

STP CName [<구성 이름>] [<정수>]

매개 변수 :

<config-name> : MSTP 구성 이름입니다. 최대 32 자의 텍스트 문자열.

따옴표 (")를 사용하여 공백을 이름에 포함하십시오.

<integer> : 정수 값

기본 설정:

구성 이름 : MAC 주소

구성 rev .: 0

예:

MSTP 구성 이름과 개정을 설정하십시오.

```
SFC4000T:/>stp cname 9f_SFC4000T 1
```

STP BPDU 필터

설명 :

에지 포트 BPDU 필터링을 설정하거나 표시합니다.

통사:

STP bpduFilter [enable | disable]

매개 변수 :

enable | disable : 에지 포트에 대한 BPDU 필터링 활성화 또는 비활성화

기본 설정:

사용 안함

예:

에지 포트 BPDU 필터링 설정

```
SFC4000T:/>stp bpdufilter enable
```

STP BPDU 가드

설명 :

에지 포트 BPDU Guard 를 설정하거나 표시합니다.

통사:

STP bpduGuard [enable | disable]

매개 변수 :

enable | disable : BPDU Guard for Edge 포트를 활성화 또는 비활성화합니다.

기본 설정:

사용 안함

예:

에지 포트 BPDU 가드 설정

```
SFC4000T:/>stp bpduguard enable
```

STP 복구

설명 :

에지 포트 오류 복구 시간 초과를 설정하거나 표시하십시오.

통사:

STP 복구 [<timeout>]

매개 변수 :

<timeout> : 오류 비활성화 포트가 다시 활성화되기 전의 시간 (30-86400 초, 0 비활성화)

(기본값 : 복구 시간 초과 표시)

기본 설정:

사용 안함

예:

STP 복구 값을 30 초 내에 설정하십시오.

```
SFC4000T:/>stp recovery 30
```

STP 상태

설명 :

STP 브리지 상태를 표시합니다.

통사:

STP 상태 [<msti>] [<port_list>]

매개 변수 :

<msti> : STP 브리지 인스턴스 번호 (0-7, CIST = 0, MSTI1 = 1, ...)

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

STP 브리지 상태를 표시합니다.

```
SFC4000T:/>stp status
CIST Bridge STP Status
Bridge ID      : 80:00-00:30:4F:24:04:D1
Root ID        : 80:00-00:30:4F:24:04:D1
Root Port      : -
Root PathCost: 0
Regional Root: 80:00-00:30:4F:24:04:D1
Int. PathCost: 0
Max Hops       : 20
TC Flag        : Steady
TC Count       : 0
TC Last        : -
Port         Port Role         State         Pri   PathCost   Edge   P2P   Uptime
---------    --------------    ----------    ---   --------   ----   ---   -------------
10           DesignatedPort    Forwarding    128   20000       Yes    Yes   0d 00:10:32
```

STP MSTI 우선 순위

설명 :

브리지 인스턴스 우선 순위를 설정하거나 표시합니다.

통사:

STP Msti 우선 순위 [<msti>] [<priority>]

매개 변수 :

<msti> : STP 브리지 인스턴스 번호 (0-7, CIST = 0, MSTI1 = 1, ...)

<priority> : STP 브리지 우선 순위 (0/4096/8192/12288/.../ 53248/57344/61440)

기본설정값:

32768

예:

4096 에 MST1 우선 순위 값을 설정하십시오.

```
SFC4000T:/>stp msti priority 1 4096
```

STP MSTI 지도

설명 :

MSTP MSTI VLAN 매핑 구성을 보거나 지 웁니다.

통사:

STP Msti 지도 [<msti>] [clear]

매개 변수 :

<msti> : STP 브리지 인스턴스 번호 (0-7, CIST = 0, MSTI1 = 1, ...)

지우기 : VID 를 MSTI 매핑으로 지 웁니다.

STP MSTI 추가

설명 :

MSTI 에 VLAN (단일 또는 범위)을 추가합니다.

통사:

STP Msti <msti> <vid-range> 추가

매개 변수 :

<msti> : STP 브리지 인스턴스 번호 (0-7, CIST = 0, MSTI1 = 1, ...)

<vid-range> : 단일 VLAN ID (1-4095) 또는 'xx-yy'VLAN ID 범위

예:

vlan1 에 MST1 을 추가하십시오.

```
SFC4000T:/>stp msti add 1 1
```

STP 포트 구성

설명 :

STP 포트 구성을 표시합니다.

통사:

STP 포트 구성 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all'. 포트 제로는 집계를 의미합니다.

예:

Port1 의 STP 상태 표시

```
SFC4000T:/>stp port configuration 1

Port   Mode        AdminEdge AutoEdge   restrRole restrTcn   Point2point
----   --------   ----------------   ----------------   ----------
1      Disabled   Disabled   Enabled    Disabled   Disabled   Auto
```

STP 포트 모드

설명 :

포트에 대해 STP 를 활성화 또는 설정하십시오.

통사:

STP 포트 모드 [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all'. 포트 제로는 집계를 의미합니다.

활성화 : MSTP 프로토콜 사용

Disable : MSTP 프로토콜을 비활성화합니다.

기본설정:

disable

예:

포트 1 에서 STP 기능 사용

```
SFC4000T:/>stp port mode 1 enable
```

STP 포트 edge

설명 :

STP adminEdge 포트 매개 변수를 설정하거나 표시하십시오.

통사:

STP 포트 에지 [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

Enable : Edge 로 MSTP adminEdge 구성

Disable : MSTP adminEdge 를 Non-edge 로 구성합니다.

기본설정값:

disable

예:

포트 1 에서 STP 에지 기능 활성화

```
SFC4000T:/>stp port edge 1 enable
```

STP 포트 AutoEdge

설명 :

STP autoEdge 포트 매개 변수를 설정하거나 표시하십시오.

통사:

STP 포트 AutoEdge [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

Enable : MSTP autoEdge 를 활성화합니다.

Disable : MSTP autoEdge 를 비활성화합니다.

기본설정값:

enable

예:

포트 1 에서 STP 에지 기능을 비활성화하십시오.

```
SFC4000T:/>stp port autoedge 1 disable
```

STP 포트 P2P

설명 :

STP point2point 포트 매개 변수를 설정하거나 표시하십시오.

통사:

STP 포트 P2P [<port_list>] [enable | disable | auto]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

활성화 : MSTP point2point 활성화

disable : MSTP point2point 비활성화

자동 : 자동 MSTP 포인트 2 포인트 감지

기본설정값:

자동

예:

포트 1 에서 STP P2P 기능 비활성화

```
SFC4000T:/>stp port p2p 1 disable
```

STP 포트 제한된 롤

설명 :

MSTP restrictedRole 포트 매개 변수를 설정하거나 표시하십시오.

통사:

STP 포트 RestrictedRole [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

활성화 : MSTP 제한된 역할 사용

disable : MSTP 제한된 역할 비활성화

기본설정값:

disable

예:

Port1 에서 Eisable STP 제한 역할

```
SFC4000T:/>stp port restrictedrole 1 enable
```

STPPortrestrictedTcn

설명 :

MSTP restrictedTcn 포트 매개 변수를 설정하거나 표시하십시오.

통사:

STP 포트 RestrictedTcn [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable : MSTP 제한 TCN 사용

disable : MSTP 제한 TCN 사용 안 함

기본설정값:

disable

예:

포트 1 에서 EISABLE STP 제한 TCN

```
SFC4000T:/>stp port restrictedtcn 1 enable
```

STP 포트 bpduGuard

설명 :

bpduGuard 포트 매개 변수를 설정하거나 표시하십시오.

통사:

STP 포트 bpduGuard [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable : 포트 BPDU Guard 활성화

disable : 포트 BPDU Guard 비활성화

기본설정값:

disable

예:

Port1 의 Eisable BPDU 가드

```
SFC4000T:/>stp port bpduguard 1 enable
```

STP 포트 통계

설명 :

STP 포트 통계를 표시합니다.

통사:

STP 포트 통계 [<port_list>] [clear]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

clear : 선택한 포트 통계 지우기

예:

STP 포트 통계를 표시합니다.

```
SFC4000T:/>stp port statistics
Port          Rx MSTP     Tx MSTP     Rx RSTP     Tx RSTP     Rx STP     Tx STP     Rx TCN
Tx TCN     Rx Ill.   Rx Unk.
---------   --------   --------   --------   --------   -------   -------   -------   -------   -------   -------
```

STP 포트 맥 체크

설명 :

포트에 대한 STP mCheck (마이그레이션 검사) 변수를 설정합니다.

통사:

STP Port Mcheck [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

포트 1 에 대한 STP mCheck (마이그레이션 검사) 변수를 설정하십시오.

```
SFC4000T:/>stp port mcheck 1
```

STP MSTI 포트 구성

설명 :

STP 포트 인스턴스 구성을 표시합니다.

통사:

STP Msti 포트 구성 [<msti>] [<port_list>]

매개 변수 :

<msti> : STP 브리지 인스턴스 번호 (0-7, CIST = 0, MSTI1 = 1, ...)

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

기본설정값:

자동

STP MSTI 포트 비용

설명 :

STP 포트 인스턴스 경로 비용을 설정하거나 표시합니다.

통사:

STP Msti 포트 비용 [<msti>] [<port_list>] [<path_cost>]

매개 변수 :

<msti> : STP 브리지 인스턴스 번호 (0-7, CIST = 0, MSTI1 = 1, ...)

<port_list> : 포트 목록 또는 'all'. 포트 제로는 집계를 의미합니다.

<path_cost> : STP 포트 경로 비용 (1-200000000) 또는 'auto'

기본설정값:

자동

예:

port1 에 MSTI7 설정

```
SFC4000T:/>stp msti port cost 7 1

MSTI   Port   Path Cost
----   ----   ----------
MST7   1      Auto
```

STP MSTI 포트 우선 순위

설명 :

STP 포트 인스턴스 우선 순위를 설정하거나 표시합니다.

통사:

STP Msti 포트 우선 순위 [<msti>] [<port_list>] [<priority>]

매개 변수 :

<msti> : STP 브리지 인스턴스 번호 (0-7, CIST = 0, MSTI1 = 1, ...)

<port_list> : 포트 목록 또는 'all'. 포트 제로는 집계를 의미합니다.

<priority> : STP 포트 우선 순위 (0/16/32/48 /.../ 224/240)

기본값:

128 자

5.9 Link Aggregation 명령어

Aggr Configuration

설명 :

링크 집계 구성 표시

통사:

Aggr Configuration

집계 추가

설명 :

링크 집계를 추가하거나 수정하십시오.

통사:

Aggr <port_list> [<aggr_id>] 추가

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<aggr_id> : 집계 ID : 1-14

예:

Group1 에 포트 1 ~ 4 추가

```
SFC4000T:/>aggr add 1-4 1
```

집계 삭제

설명 :

링크 집계 삭제

통사:

Aggr 삭제 <aggr_id>

매개 변수 :

<aggr_id> : 집계 ID : 1-14

예:

그룹 2 삭제

```
SFC4000T:/>aggr delete 2
```

집계 조회

설명 :

링크 연결 집계를 조회합니다.

통사:

Aggr Lookup [<aggr_id>]

매개 변수 :

<aggr_id> : 집계 ID : 1-14

집계 모드

설명 :

링크 집계 트래픽 분배모드를 설정하거나 표시합니다.

통사:

Aggr 모드 [smac | dmac | ip | port] [enable | disable]

매개 변수 :

smac : 발신지 MAC 주소

dmac : 대상 MAC 주소

ip : 출발지 및 목적지 IP 주소

포트 : 원본 및 대상 UDP / TCP 포트

사용 : 트래픽 분산에서 필드 사용

사용 중지 : 트래픽 분산에서 필드 사용 중지

기본 설정:

SMAC : 사용 가능

DMAC : 사용 안 함

IP : 사용함

포트 : 사용

예:

SMAC 모드 사용 안 함

```
SFC4000T:/>Aggr mode smac disable
```

5.10 Link Aggregation Control Protocol 명령어

LACP 구성

설명 :

LACP 구성을 표시합니다.

통사:

LACP 구성 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

LACP 구성 표시

```
SFC4000T:/>lacp configuration

Port   Mode       Key    Role
----   --------   ----   ------
```

```
1      Disabled   Auto   Active
2      Disabled   Auto   Active
3      Disabled   Auto   Active
4      Disabled   Auto   Active
5      Disabled   Auto   Active
6      Disabled   Auto   Active
7      Disabled   Auto   Active
8      Disabled   Auto   Active
9      Disabled   Auto   Active
10     Disabled   Auto   Active
```

LACP 모드

설명 :

LACP 모드를 설정하거나 표시합니다.

통사:

LACP 모드 [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable : LACP 프로토콜 사용

disable : LACP 프로토콜을 비활성화합니다.

(기본값 : LACP 모드 표시)

기본 설정:

disable

예:

포트 1 ~ 4 에 LACP 사용

```
SFC4000T:/>lacp mode 1-4 enable
```

LACP 키

설명 :

LACP 키를 설정하거나 표시하십시오.

통사:

LACP key [<port_list>] [<key>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<key> : LACP 키 (1-65535) 또는 'auto'

기본 설정:

자동

예:

포트 1 ~ 4 에 대해 key1 설정

```
SFC4000T:/>lacp key 1-4 1
```

LACP 우선 순위

설명 :

LACP 프리오를 설정하거나 표시하십시오.

통사:

LACP Prio [<port_list>] [<prio>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<prio> : LACP Prio (0-65535)

기본 설정:

32768

LACP 시스템 우선 순위

설명 :

LACP 시스템 prio 를 설정하거나 표시하십시오.

통사:

LACP 시스템 Prio [<sysprio>]

매개 변수 :

<sysprio> : LACP 시스템 Prio (0-65535)

기본 설정:

32768

LACP 역할

설명 :

LACP 역할을 설정하거나 표시합니다.

통사론

LACP 역할 [<port_list>] [활성 | 수동]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

활성 : LACP 협상 시작

passive : LACP 패킷을 수신합니다.

(기본값 : LACP 역할 표시)

기본 설정:

유효한

예:

포트 1 ~ 4 에 수동 설정

```
SFC4000T:/>lacp role 1-4 passive
```

LACP 상태

설명 :

LACP 상태 표시.

통사:

LACP status [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

포트 1 ~ 4 의 LACP 상태 표시

```
SFC4000T:/>lacp status 1-4

Port   Mode        Key     Aggr ID   Partner System ID   Partner Port
----   --------    -----   -------   -----------------   ------------
1      Disabled    1       -         -                   -
2      Disabled    1       -         -                   -
3      Disabled    1       -         -                   -
4      Disabled    1       -         -                   -
```

LACP 통계

설명 :

LACP 통계 표시

통사론:

LACP 통계 [<port_list>] [clear]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

clear : LACP 통계 지우기

예:

포트 1 ~ 4 의 LACP 통계보기

```
SFC4000T:/>lacp statistics 1-4

Port   Rx Frames     Tx Frames     Rx Unknown    Rx Illegal
------ ------------- ------------- ------------- ----------
1       0             0            0             0
2       0             0            0             0
3       0             0            0             0
4       0             0            0             0
```

LACP Timeout

설명 :

LACP 시간 초과를 설정하거나 표시하십시오.

통사론:

LACP 시간 초과 [<port_list>] [fast | slow]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

고속 : 고속 PDU 전송 (빠른 시간 초과)

느린 : 느린 PDU 전송 (느린 시간 초과)

(기본값 : Show LACP timeout)

기본 설정:

빠른

5.11 LLDP

LLDP 구성

설명 :

LLDP 구성을 표시합니다.

통사:

LLDP 구성 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

포트 1 ~ 4 의 LLDP 구성 표시

```
SFC4000T:/>lldp configuration 1-4

LLDP Configuration:
```

```
==================

Interval      : 30
Hold          : 3
Tx Delay      : 2
Reinit Delay: 2

Port Mode       Port Descr System Name System Descr System Capa Mgmt Addr CDP awareness
---- --------   ---------- ----------- ------------ ----------- --------- -------------
1    Enabled    Enabled    Enabled     Enabled      Enabled     Enabled   Disabled
2    Enabled    Enabled    Enabled     Enabled      Enabled     Enabled   Disabled
3    Enabled    Enabled    Enabled     Enabled      Enabled     Enabled   Disabled
4    Enabled    Enabled    Enabled     Enabled      Enabled     Enabled   Disabled
```

LLDP 모드

설명 :

LLDP 모드를 설정하거나 표시합니다.

통사:

LLDP 모드 [<port_list>] [enable | disable | rx | tx]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

활성화 : LLDP 수신 및 전송 활성화

disable : LLDP 비활성화

rx : LLDP 수신 만 가능

tx : LLDP 전송 만 사용 가능

(기본값 : LLDP 모드 표시)

기본 설정:

disable

예:

포트 1 LLDP 기능을 활성화하십시오.

```
SFC4000T:/>lldp mode 1 enable
```

LLDP 선택적 TLV

설명 :

LLDP 선택적 TLV 표시 또는 설정

통사:

LLDP Optional_TLV [<port_list>] [port_descr | sys_name | sys_descr | sys_capa | mgmt_addr] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

port_descr : 포트 설명

sysm_name : 시스템 이름

sys_descr : 시스템 설명

sys_capa : 시스템 기능

mgmt_addr : 마스터의 IP 주소

(기본값 : 선택적 TLV 구성 표시)

enable : TLV 를 활성화합니다.

disable : TLV 사용 중지

(기본값 : 선택적 TLV 구성 표시)

기본 설정:

포트 설명 : 사용

시스템 이름 : 사용

시스템 설명 : 사용

시스템 기능 : 사용

마스터의 IP 주소 : 사용

예:

port1 에 대한 포트 설명 사용 안 함

```
SFC4000T:/>lldp optional_tlv 1 port_descr disable
```

LLDP 간격

설명 :

LLDP Tx 간격을 설정하거나 표시합니다.

통사:

LLDP 간격 [<interval>]

매개 변수 :

<간격> : LLDP 전송 간격 (5-32768)

기본 설정:

30

예:

송신 간격을 10 으로 설정합니다.

```
SFC4000T:/>lldp interval 10
```

LLDP hold

설명 :

LLDP Tx hold 값을 설정하거나 표시합니다.

통사:

LLDP hold [<hold>]

매개 변수 :

<hold> : LLDP 홀드 값 (2-10)

기본 설정:

삼

예:

10 에 LLDP hold 값 설정

```
SFC4000T:/>lldp hold 10
```

LLDP 지연

설명 :

LLDP Tx 지연을 설정하거나 표시합니다.

통사:

LLDP 지연 [<지연>]

매개 변수 :

<지연> : LLDP 전송 지연 (1-8192)

기본 설정:

2

예:

LLDP 지연 값을 1 로 설정합니다.

```
SFC4000T:/>lldp delay 1
```

LLDP 재부팅

설명 :

LLDP reinit delay 를 설정 또는 표시합니다.

통사:

LLDP Reinit [<reinit>]

매개 변수 :

<reinit> : LLDP 지연 지연 (1-10)

기본 설정:

2

예:

LLDP 는 지연 지연 값을 3 으로 설정합니다.

```
SFC4000T:/>lldp reinit 3
```

LLDP 통계

설명 :

LLDP 통계 표시

통사:

LLDP 통계 [<port_list>] [지우기]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

clear : LLDP 통계 지우기

예:

포트 1 의 LLDP 통계 표시

```
SFC4000T:/>lldp statistics 1

LLDP global counters
Neighbor entries was last changed at - (18819 sec. ago).
Total Neighbors Entries Added      0.
Total Neighbors Entries Deleted    0.
Total Neighbors Entries Dropped    0.
Total Neighbors Entries Aged Out 0.

LLDP local counters
        Rx         Tx         Rx         Rx         Rx TLV    Rx TLV    Rx TLV
Port    Frames     Frames     Errors     Discards Errors     Unknown   Organz.   Aged
----    ------     ------     ------     --------   ------    -------   -------   -----
1       0          0          0          0          0         0         0         0
```

LLDP 정보

설명 :

LLDP 인접 장치 정보를 표시합니다.

통사:

LLDP 정보 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

LLDP CDP 인식

설명 :

수신 된 CDP (Cisco Discovery Protocol) 프레임의 검색 정보가 LLDP 인접 테이블에 추가되면 설정 또는 표시합니다.

통사:

LLDP cdp_aware [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

활성화 : CDP 인식 활성화 (CDP 검색 정보가 LLDP 인접 테이블에 추가됨)

disable : CDP 인식 비활성화

(기본값 : CDP 인식 구성 표시)

5.12 LLDPMED 명령어

LLDPMED 구성

설명 :

LLDP-MED 구성을 표시합니다.

통사:

LLDPMED 구성 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

포트 1 ~ 4 의 LLDP-MED 구성 표시

```
SFC4000T:/>lldpmed configuration 1-4

LLDP-MED Configuration:
=======================

Fast Start Repeast Count : 4
Location Coordinates      : Latitude                  - 0.0000 North
                            Longitude                 - 0.0000 East
                            Altitude                  - 0.0000 meter(s)
                            Map datum                 - WGS84
Civic Address Location    :



Port          Policies
```

1	**none**
2	**none**
3	**none**
4	**none**

LLDPMED Civic

설명 :

LLDP-MED 시민 주소 위치를 설정하거나 표시하십시오.

통사:

LLDPMED 시민 [국가 | 군 | 도시 | 지구 | 구획 | 거리 | 선도하는 방향 | 후행하는 _street_suffix | str_sufix | str_sufix | 집 _no_suffix | 경계표 | additional_info | 이름 | zip_code | 건물 | 아파트 |지면 | room_number | place_type | postal_com_name | p_o_box | additional_code] [<civic_value>]

매개 변수 :

나라 : 국가

주 : 국가 세분 (주, 캐톤, 지역,도, 현)

카운티 : 카운티, 교구, 총 (JP), 지구 (IN)

시 : City, townchip, shi (JP)

지구 : 도시 구획, 보로,시, 구, 구, 주오 (JP)

블록 : 이웃, 블록

거리 : 거리

leading_street_direction : 선도 방향

trailing_street_suffix : 후행 거리 접미사

str_suf : 거리 접미어

house_no : 집 번호

house_no_suffix : 집 번호 접미사

랜드 마크 : 랜드 마크 또는 허영심 주소

additional_info : 추가 위치 정보

이름 : 바메 (거주 및 사무실 점유자)

zip_code : 우편 / 우편 번호

건물 : 건물 (구조)

아파트 : 유닛 (아파트, 스위트)

층 : 층

room_number : 방 번호

place_type : Placetype

postal_com_name : 우편 커뮤니티 이름

p_o_box : 우체국 상자 (사서함)

additional_code : 추가 코드

(기본값 : 도시 주소 표시 위치 구성 표시)

<civic_value> : lldpmed Civic Address Location 항목의 값입니다.

LLDPMED ECS

설명 :

LLDP-MED 응급 콜 서비스를 설정하거나 표시합니다.

통사:

LLDPMED ecs [<ecs_value>]

매개 변수 :

<ecs_value> : lldpmed 응급 호출 서비스의 값

LLDPMED 정책 삭제

설명 :

선택한 정책을 삭제하십시오.

통사:

LLDPMED 정책 삭제 [<정책 목록>]

매개 변수 :

<policy_list> : 삭제할 정책 목록

예:

정책 삭제 1

```
SFC4000T:/>lldpmed policy delete 1
```

LLDPMED 정책 추가

설명 :

정책 목록에 정책을 추가합니다.

통사:

LLDPMED 정책은 <policy_type> [태그가 추가됨 | 태그가 지정되지 않음] [<vlan_id>] [<l2_priority>] [<dscp>]를 추가합니다.

매개 변수 :

<policy_type> : policy_type 매개 변수는 다음 값을 사용합니다.

음성 : 전용 IP 텔레포니 핸드셋 및 대화 형 음성 서비스를 지원하는 기타 유사한 어플라이언스에서 사용하는 음성. 이러한 장치는 일반적으로 배포 용이성 및 데이터 응용 프로그램과의 격리로 향상된 보안을 위해 별도의 VLAN 에 배포됩니다

voice_signaling : 음성 신호 대신 음성 시그널에 대해 다른 정책이 필요한 네트워크 토폴로지에서 사용하기위한 음성 시그널링 (조건부).

guest_voice : 게스트 보이스는 자체 IP 텔레포니 핸드셋 및 대화 형 음성 서비스를 지원하는 기타 유사한 어플라이언스로 게스트 사용자 및 방문객을위한 별도의 제한된 기능 세트 음성 서비스를 지원합니다.

guest_voice_signaling : 게스트 음성 신호 대신 게스트 음성 신호에 대해 다른 정책이 필요한 네트워크 토폴로지에서 사용하기위한 게스트 음성 신호 (조건부).

softphone_voice : Softphone Voice 는 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.

video_conferencing : 화상 회의는 전용 화상 회의 장비 및 실시간 대화 형 비디오 / 오디오 서비스를 지원하는 기타 유사한 장비에서 사용하기위한 것입니다.

streaming_video : 브로드 캐스트 또는 멀티 캐스트 기반 비디오 컨텐츠 배포 및 특정 네트워크 정책 처리가 필요한 스트리밍 비디오 서비스를 지원하는 기타 유사한 응용 프로그램에서 사용하기위한 스트리밍 비디오입니다. 버퍼링을 사용하여 TCP 를 사용하는 비디오 응용 프로그램은이 응용 프로그램 유형을 의도 한 용도로 사용하지 않습니다.

video_signaling : 비디오 신호 대신 비디오 신호에 대한 별도의 정책이 필요한 네트워크 토폴로지에서 사용하기위한 비디오 신호 (조건부).

tagged : 장치가 태그가 지정된 프레임을 사용 중입니다.

unragged : 장치가 태그가없는 프레임을 사용 중입니다.

<vlan_id> : VLAN ID

<l2_priority> :이 필드는 IEEE 802.1D-2004 [3]에 정의 된대로 8 개의 우선 순위 레벨 (0 에서 7 까지) 중 하나를 지정할 수 있습니다.

<dscp> :이 필드는 IETF RFC 2474 [5]에 정의 된대로 지정된 응용 프로그램 유형에 대해 Diffserv 노드 동작을 제공하는 데 사용할 DSCP 값을 포함해야합니다. 이 6 비트 필드는 64 코드 포인트 값 (0 ~ 63) 중 하나를 포함 할 수 있습니다. 값 0 은 RFC 2475 에 정의 된 기본 DSCP 값의 사용을 나타냅니다.

LLDPMED 포트 정책

설명 :

LLDP-MED 포트 폴리시를 설정하거나 표시합니다.

통사:

LLDPMED 포트 정책 [<port_list>] [<policy_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<policy_list> : 삭제할 정책 목록

LLDPMED 좌표

설명 :

LLDP-MED 위치를 설정하거나 표시합니다.

통사:

LLDPMED 좌표 [<tude_type>] [<direction>] [coordinate_value]

매개 변수 :

<tude_type> : tude_type 매개 변수는 다음 값을 취합니다.

위도 : 위도, 최대 0 도 ~ 90 도 4 자리 (양수는 적도의 북쪽이고 음수는 적도의 남쪽입니다.)

경도 : 경도, 최대 0 ~ 180 도 4 자리 (양의 값은 자오선의 동쪽이고 음수는 자오선의 서쪽입니다.)

고도 : 고도, -32767 ~ 32767 미터 또는 플로어 최대. 4 자리.

<direction> : direction 매개 변수는 다음 값을 취합니다.

북쪽 : 북쪽 (위도 유효)

남쪽 : 남쪽 (위도 유효)

서쪽 : 서쪽 (경도에 유효)

동쪽 : 동쪽 (경도로 유효)

미터 : 미터 (고도 기준)

층 : 층 (고도에 유효)

coordinate_value : 좌표 값

LLDPMED datum

설명 :

LLDP-MED 좌표 맵 데이터를 설정하거나 표시합니다.

통사:

LLDPMED Datum [<datum_type>]

매개 변수 :

<datum_type> : datum_type 매개 변수는 다음 값을 사용합니다.

wgs84 : WGS84

nad83_navd88 : NAD83_NAVD88

nad83_mllw : NAD83_MLLW

LLDPMED Fast

설명 :

LLDP-MED 빠른 시작 반복 횟수를 설정하거나 표시합니다.

통사:

LLDPMED 빠름 [<count>]

매개 변수 :

<count> : LLDP-MED (1-10)에 정의 된 빠른 시작 메커니즘을 활성화하는 동안 고속 시작 LLDPDU 가 전송되는 횟수입니다.

LLDPMED 정보

설명 :

LLDP-MED 인접 장치 정보를 표시합니다.

통사:

LLDPMED 정보 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

5.13 Quality of Service 명령어

QoS 구성

설명 :

QoS 구성 표시.

통사:

QoS 구성 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

QoS 포트 분류 클래스

설명 :

기본 QoS 클래스를 설정하거나 표시합니다.

QoS 클래스가 동적으로 변경되면 구성된 QoS 클래스 다음에 괄호 안에 실제 QoS 클래스가 표시됩니다.

통사:

QoS 포트 분류 클래스 [<port_list>] [<class>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<class> : QoS 클래스 (0-7)

기본 설정:

0

예:

포트 1 의 기본 QoS 클래스를 1 로 설정

```
SFC4000T:/>qos Port Classification Class 1 1
```

QoS 포트 분류 DPL

설명 :

기본 놓기 우선 순위를 설정하거나 표시하십시오.

통사:

QoS 포트 분류 DPL [<port_list>] [<dpl>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<dpl> : 놓기 우선 순위 (0-3)

기본 설정:

0

예:

port1 에 대해 기본 놓기 우선 순위를 1 로 설정하십시오.

```
SFC4000T:/>qos Port Classification dpl 1 1
```

QoS 포트 분류 태그

설명 :

분류가 태그가있는 프레임의 PCP 및 DEI 값을 기반으로하는지 설정하거나 표시합니다.

통사:

QoS 포트 분류 태그 [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

사용 : 태그 분류 사용

disable : 태그 분류 사용 중지

(기본값 : 태그 분류 모드 표시)

기본 설정:

disable

예:

QoS 포트 분류 태그 사용.

```
SFC4000T:/>qos Port Classification tag 1-10 enable
```

QoS 포트 분류 맵

설명 :

포트 분류 맵을 설정하거나 표시하십시오.

이 맵은 포트 분류 태그가 사용 가능할 때 사용되며, 목적은 PCP (Priority Code Point) 및 DEI (Drop Eligible Indicator)를 태그가있는 프레임에서 QoS 클래스 및 DP 수준으로 변환하는 데 사용됩니다.

통사:

QoS 포트 분류 맵 [<port_list>] [<pci_list>] [<dei_list>] [<class>] [<dpl>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<pcp_list> : PCP 목록 또는 'all', 기본값 : 모든 PCP (0-7)

<dei_list> : DEI 목록 또는 'all', 기본값 : 모든 DEI (0-1)

<class> : QoS 클래스 (0-7)

<dpl> : 놓기 우선 순위 (0-3)

QoS 포트 분류 DSCP

설명 :

분류가 IP 프레임의 DSCP 값을 기반으로하는지 설정하거나 표시합니다.

통사:

QoS 포트 분류 DSCP [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable : DSCP 기반 분류 사용

disable : DSCP 기반 분류를 비활성화합니다.

(기본값 : DSCP 기반 분류 모드 표시)

기본 설정:

disable

예:

QoS 포트 분류 DSCP 를 사용합니다.

```
SFC4000T:/>qos Port Classification dscp 1-10 enable
```

QoS 포트 정책 모드

설명 :

포트 정책 모드 설정 또는 표시

통사:

QoS 포트 폴리 서 모드 [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable : 포트 폴리 서 사용

disable : 포트 폴리 서 비활성화

(기본값 : 포트 폴리 서 모드 표시)

기본 설정:

disable

예:

QoS 포트 폴리 서 사용

```
SFC4000T:/>qos Port Policer Mode 1-10 enable
```

QoS 포트 폴리시 비율

설명 :

포트 폴리 서 속도를 설정하거나 표시하십시오.

통사:

QoS 포트 폴리 서 속도 [<port_list>] [<rate>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<rate> : kbps 또는 fps 단위의 속도 (100-13200000)

기본 설정:

500

예:

포트 폴리 서 속도를 1000 으로 설정하십시오.

```
SFC4000T:/>qos Port Policer Rate 1-10 1000
```

QoS 포트 폴리시 장치

설명 :

포트 폴리 서 장치를 설정하거나 표시하십시오.

통사:

QoS 포트 폴리서 장치 [<port_list>] [kbps | fps]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

kbps : 단위는 킬로 비트 / 초입니다.

fps : 단위는 초당 프레임입니다.

(기본값 : 포트 폴리 서 장치 표시)

기본 설정:

kbps

예:

포트 폴리 서 유닛을 fps 로 설정하십시오.

```
SFC4000T:/>qos Port Policer unit 1-10 fps
```

QoS 포트 폴리 서 흐름 제어

설명 :

포트 폴리 서 흐름 제어를 설정하거나 표시하십시오.

폴리 서 흐름 제어가 활성화되어 있고 포트가 흐름 제어 모드에 있으면 프레임을 버리는 대신 일시 중지 프레임이 전송됩니다.

통사:

QoS 포트 폴리 서 흐름 제어 [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable : 포트 폴리 서 흐름 제어 활성화

disable : 포트 폴리 서 흐름 제어 비활성화

(기본값 : 포트 폴리 서 흐름 제어 모드 표시)

기본 설정:

disable

QoS 포트 스케줄러 모드

설명 :

포트 스케줄러 모드를 설정하거나 표시하십시오.

통사:

QoS 포트 스케줄러 모드 [<port_list>] [strict | weighted]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

엄격 : 엄격 모드

가중치 : 가중치 적용 모드

(기본값 : 포트 스케줄러 모드 표시)

기본 설정:

엄격한

예:

가중치 모드에서 포트 일정 모드 설정

```
SFC4000T:/>qos Port Scheduler Mode 1-10 weighted
```

QoS 포트 스케줄러 무게

설명 :

포트 스케줄러 가중치를 설정하거나 표시하십시오.

통사:

QoS 포트 스케줄러 무게 [<port_list>] [<queue_list>] [<weight>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<queue_list> : 가중치 대기열 목록 또는 'all', 기본값 : 가중치 대기열 (0-5)

<weight> : 스케줄러 가중치 (1-100)

QoS 포트 큐 셰이퍼 모드

설명 :

포트 큐 셰이퍼 모드를 설정하거나 표시하십시오.

통사:

QoS 포트 큐 모드 [<port_list>] [<queue_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<queue_list> : 대기열 목록 또는 'all', 기본값 : 모든 대기열 (0-7)

enable : 포트 대기열 셰이퍼 사용

disable : 포트 대기열 셰이퍼 사용 안 함

(기본값 : 포트 대기열 셰이퍼 모드 표시)

기본 설정:

disable

예:

모든 포트 및 대기열에 대해 포트 대기열 셰이 퍼 사용

```
SFC4000T:/>qos Port QueueShaper Mode 1-10 0-7 enable
```

QoS 포트 큐 쉐이퍼 비율

설명 :

포트 큐 셰이퍼 속도를 설정하거나 표시하십시오.

통사:

QoS 포트 QueueShaper 속도 [<port_list>] [<queue_list>] [<bit_rate>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<queue_list> : 대기열 목록 또는 'all', 기본값 : 모든 대기열 (0-7)

<bit_rate> : 초당 킬로 비트 수 (100-13200000)

기본 설정:

500kbps

예:

포트 대기열 셰이퍼 비율을 1000 으로 설정합니다.

```
SFC4000T:/>qos Port QueueShaper rate 1-10 0-7 1000
```

QoS 포트 QueueShaper 초과

설명 :

포트 대기열 초과 대역폭 모드를 설정하거나 표시합니다.

통사:

QoS 포트 QueueShaper 초과 [<port_list>] [<queue_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<queue_list> : 대기열 목록 또는 'all', 기본값 : 모든 대기열 (0-7)

enable : 초과 대역폭 사용을 활성화합니다.

disable : 초과 대역폭 사용 중지

(기본값 : 포트 대기열 초과 대역폭 모드 표시)

기본 설정:

disable

예:

포트 대기열 초과 대역폭 모드를 활성화합니다.

```
SFC4000T:/>qos Port QueueShaper Excess 1-10 0-7 enable
```

QoS 포트 태그 표시 모드

설명 :

포트 태그 remarking 모드를 설정하거나 표시하십시오.

통사:

QoS 포트 태그 표시 모드 [<port_list>] [분류 | 기본값 | 매핑 됨]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

분류 : 분류 된 PCP / DEI 값 사용

기본값 : 기본 PCP / DEI 값 사용

맵핑 : 맵핑 된 버전의 QoS 클래스 및 DP 레벨 사용

(기본값 : 포트 태그 remarking 모드 표시)

기본 설정:

분류 된

예:

매핑 된 포트 태그 remarking 모드를 설정하십시오.

```
SFC4000T:/>qos Port TagRemarking Mode 1-10 mapped
```

QoS 포트 태그 PCP 리마킹

설명 :

기본 PCP 를 설정하거나 표시하십시오. 이 값은 포트 태그 remarking 모드가 'default'로 설정된 경우 사용됩니다.

통사:

QoS 포트 태그 표시 PCP [<port_list>] [<pcp>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<pcp> : 우선 순위 코드 포인트 (0-7)

기본 설정:

0

예:

기본 PCP 를 1 로 설정하십시오.

```
SFC4000T:/>qos Port TagRemarking PCP 1-10 1
```

QoS 포트 태그 표시 DEI

설명 :

기본 DEI 를 설정하거나 표시하십시오. 이 값은 포트 태그 remarking 모드가 'default'로 설정된 경우 사용됩니다.

통사:

QoS 포트 태그 리 마크 DEI [<port_list>] [<dei>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<dei> : 하락 적격 지시자 (0-1)

기본 설정:

0

예:

기본 EDI 를 1 로 설정하십시오.

```
SFC4000T:/>qos Port TagRemarking EDI 1-10 1
```

QoS 포트 태그 리 맵핑

설명 :

포트 태그 remarking map 을 설정하거나 표시하십시오. 이 맵은 포트 태그 리 마킹 모드가 'mapped'로 설정되고 분류된 QoS 클래스 (0-7)와 DP 레벨 (0-1)을 PCP 와 DEI 로 변환하는 데 사용됩니다.

통사:

QoS 포트 태그 매핑 맵 [<port_list>] [<class_list>] [<dpl_list>] [<pcp>] [<dei>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<class_list> : QoS 클래스 목록 또는 'all', 기본값 : 모든 QoS 클래스 (0-7)

<dpl_list> : DP 레벨 목록 또는 'all', 기본값 : 모든 DP 레벨 (0-1)

<pcp> : 우선 순위 코드 포인트 (0-7)

<dei> : 하락 적격 지시자 (0-1)

QoS 포트 DSCP 변환

설명 :

DSCP 수신 변환 모드를 설정하거나 표시합니다.

포트에 대해 변환이 활성화되면 수신 프레임 DSCP 값이 변환되고 변환 된 값이 QoS 분류에 사용됩니다.

통사:

QoS 포트 DSCP 변환 [<port_list>] [enable | disable]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable : DSCP 수신 번역 활성화

disable : DSCP 입력 변환 사용 안 함

(기본값 : DSCP 입력 변환 모드 표시)

기본 설정:

disable

예:

모든 포트에서 DSCP 수신 변환을 활성화합니다.

```
SFC4000T:/>qos Port DSCP Translation 1-10 enable
```

QoS 포트 DSCP 분류

설명 :

QoS 클래스를 기반으로 DSCP 분류를 설정하거나 표시합니다.

이렇게하면 포트별로 QoS 클래스에 따라 새로운 DSCP 값을 매핑 할 수 있습니다.

통사:

QoS 포트 DSCP 분류 [<port_list>] [none | zero | selected | all]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

없음 : DSCP 입력 분류 없음

0 : DSCP = 0 인지 DSCP 를 분류합니다.

selected : DSCP 를 분류하여 분류합니다. 모드가 '사용'

all : 모든 DSCP 분류

(기본값 : 포트 DSCP 수신 분류 모드 표시)

기본 설정:

없음

예:

QoS 클래스 및 DP 레벨을 기준으로 DSCP 분류를 0 으로 설정합니다.

SFC4000T : /> QoS 포트 DSCP 분류 1-10 제로

QoS 포트 DSCP EgressRemark

설명 :

포트 DSCP remarking 모드를 설정하거나 표시하십시오.

통사:

QoS 포트 DSCP EgressRemark [<port_list>] [disable | enable | remap]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

disable : DSCP 이탈 재 작성 비활성화

enable : 분석기에서 수신 한 값으로 DSCP 출구 다시 쓰기를 활성화합니다.

재 매핑 : 재 매핑 된 DSCP 를 사용하여 송신 프레임의 DSCP 를 다시 작성합니다.

(기본값 : 포트 DSCP 이탈 표시 모드 표시)

기본 설정:

disable

예:

DSCP 송신 재 작성 활성화

```
SFC4000T:/> QoS Port DSCP EgressRemark 1-10 enable
```

QoS DSCP 맵

설명 :

DSCP 매핑 테이블을 설정하거나 표시합니다.

이 표는 DSCP 값을 기반으로 QoS 등급과 DP 수준을 매핑하는 데 사용됩니다.
QoS 클래스 매핑에 사용되는 DSCP 값이며 DPL 은 변환 된 DSCP 값 또는 수신 프레임 DSCP 값입니다.

통사:
QoS DSCP 맵 [<dscp_list>] [<class>] [<dpl>]

매개 변수 :
<dscp_list> : DSCP (0-63, BE, CS1-CS7, EF 또는 AF11-AF43) 목록 또는 'all'
(기본값 : DSCP 입력 맵 테이블 표시, 즉 DSCP -> (클래스, DPL))
<class> : QoS 클래스 (0-7)
<dpl> : 놓기 우선 순위 (0-3)

QoS DSCP 변환
설명 :
글로벌 진입 DSCP 변환 테이블을 설정하거나 표시합니다.
포트 DSCP 변환이 활성화 된 경우 변환 테이블은 들어오는 프레임을 변환하는 데 사용되며 DSCP 값과 변환 된 값은 QoS 클래스와 DP 수준을 매핑하는 데 사용됩니다.

통사:
QoS DSCP 번역 [<dscp_list>] [<trans_dscp>]

매개 변수 :
<dscp_list> : DSCP (0-63) 목록 또는 'all'
(기본값 : DSCP 변환 테이블 표시)
<trans_dscp> : 번역 된 DSCP : 0-63, BE, CS1-CS7, EF 또는 AF11-AF43

QoS DSCP trust
설명 :
QoS 분류에 사용되는 신뢰할 수있는 DSCP 값을 설정하거나 표시합니다.
trust 를 검사 할 DSCP 값은 들어오는 포트에 대해 DSCP 변환이 활성화 된 경우 변환 된 값이거나 포트에 대해 변환이 비활성화 된 경우 들어오는 프레임 DSCPvalue 입니다. 신뢰할 수있는 DSCP 값은 QoS 분류에만 사용됩니다.

통사:
QoS DSCP trust [<dscp_list>] [enable | disable]

매개 변수 :

<dscp_list> : DSCP (0-63) 목록 또는 'all'

enable : DSCP 를 신뢰할 수있는 DSCP 로 설정합니다.

disable : DSCP 를 신뢰할 수없는 DSCP 로 설정합니다.

(기본값 : DSCP 신뢰 상태 표시)

기본 설정:

disable

QoS DSCP 분류 모드

설명 :

DSCP 수신 분류 모드를 설정하거나 표시합니다.

포트 DSCP 분류가 '선택됨'인 경우 분류 모드가 '사용 가능'인 DSCP 값에 대해서만 DSCP 가 QoS 클래스 및 DP 레벨에 따라 분류됩니다. 포트에 대한 변환이 활성화 된 경우 DSCP 는 DSCP 로 변환 될 수 있습니다.

통사:

QoS DSCP 분류 모드 [<dscp_list>] [enable | disable]

매개 변수 :

<dscp_list> : DSCP (0-63) 목록 또는 'all'

enable : DSCP 수신 분류 사용

disable : DSCP 수신 분류 해제

(기본값 : DSCP 분류 모드 표시)

기본 설정:

disable

QoS DSCP 분류 MAP

설명 :

DSCP 수신 분류 테이블을 설정하거나 표시합니다.

이 테이블은 DSCP 를 QoS 클래스 및 DP 수준에서 매핑하는 데 사용됩니다. 분류가 필요한 DSCP 는 포트 DSCP 분류 및 DSCP 분류 모드에 따라 다릅니다. 수신 프레임 DSCP 는 분류 값을 사용하기 전에 변환 될 수 있습니다.

통사:

QoS DSCP 분류 맵 [<class_list>] [<dpl_list>] [<dscp>]

매개 변수 :

<class_list> : QoS 클래스 목록 또는 'all', 기본값 : 모든 QoS 클래스 (0-7)

<dpl_list> : DP 레벨 목록 또는 'all', 기본값 : 모든 DP 레벨 (0-1)

<dscp> : 매핑 된 DSCP : 0-63, BE, CS1-CS7, EF 또는 AF11-AF43

기본 설정:

disable

QoS DSCP EgressRemap

설명 :

DSCP 출구 재구성 테이블을 설정하거나 표시합니다. 이 표는 포트 이탈 remarking 모드가 'remap'이고 분류 된 DSCP 를 새로운 DSCP 값에 매핑하는 목적으로 사용됩니다.

통사:

QoS DSCP EgressRemap [<dscp_list>] [<dscp>]

매개 변수 :

<dscp_list> : DSCP (0-63) 목록 또는 'all'

<dscp> : 출력 재 매핑 된 DSCP : 0-63, BE, CS1-CS7, EF 또는 AF11-AF43

QoS 포트 스톰 유니 캐스트

설명 :

유니 캐스트 프레임에 포트 Storm 율 제한기를 설정하거나 표시하십시오.

통사:

QoS 포트 스톰 유니 캐스트 [<port_list>] [enable | disable] [<rate>] [kbps | fps]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable : 유니 캐스트 프레임의 스톰 정책 활성화

disable : 유니 캐스트 프레임의 스톰 정책 비활성화

<rate> : kbps 또는 fps 단위의 속도 (100-13200000)

kbps : 단위는 킬로 비트 / 초입니다.

fps : 단위는 초당 프레임입니다.

기본 설정:

disable

예:

유니 캐스트 Storm 제어를 2kbps 로 활성화

```
SFC4000T:/> QoS Port Storm Unicast enable 2
```

QoS 포트 스톰 멀티 캐스트

설명 :

브로드 캐스트 프레임의 포트 Storm 리미터를 설정하거나 표시합니다.

통사:

QoS 포트 Storm broadcast [<port_list>] [enable | disable] [<rate>] [kbps | fps]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

활성화 : 브로드 캐스트 프레임의 Storm 정책 활성화

disable : 브로드 캐스트 프레임의 스톰 정책 비활성화

<rate> : kbps 또는 fps 단위의 속도 (100-13200000)

kbps : 단위는 킬로 비트 / 초입니다.

fps : 단위는 초당 프레임입니다.

기본 설정:

disable

예:

2kbps 로 멀티 캐스트 스톰 제어 활성화

```
SFC4000T:/> QoS Port Storm multicast enable 2
```

QoS 포트 Broadcast Storm

설명 :

브로드 캐스트 스톰 율 제한기를 설정하거나 표시하십시오.
리미터는 플러딩 된 프레임, 즉 MAC 주소 테이블에없는 (VLAN ID, DMAC) 쌍이있는 프레임에만 영향을 미칩니다.

통사:
QoS 스톰 브로드 캐스트 [enable | disable] [<packet_rate>]

매개 변수 :
enable : 브로드 캐스트 스톰 제어 활성화
disable : 브로드 캐스트 스톰 제어 비활성화
<packet_rate> : fps 단위 (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 32768k)

기본 설정:
disable

QoS QCL 추가
설명 :
QCE (QoS Control Entry)를 추가 또는 수정합니다.

QCE ID 매개 변수 <qce_id>가 지정되고이 QCE ID 가있는 항목이 이미 존재하면 QCE 가 수정됩니다. 그렇지 않으면 새 QCE 가 추가됩니다. QCE ID 가 지정되지 않으면 다음 사용 가능한 QCE ID 가 사용됩니다. 다음 QCE ID 매개 변수 <qce_id_next>가 지정되면 QCE 는 목록의이 QCE 앞에 놓입니다. 다음 QCE ID 가 지정되지 않고 추가 된 새 항목인 경우 QCE 가 목록의 마지막에 배치됩니다. 그렇지 않으면 다음 QCE ID 가 지정되지 않고 기존 QCE 가 수정되면 QCE 는 목록의 동일한 위치에있게됩니다. 항목을 수정하고 목록에서 마지막으로 이동하려면 <qce_id_next>에 'last'라는 단어를 사용하십시오.

통사:
QoS QCL [<qce_id>] [<port_list>] [<tag>] [<vid>] [<dc>] [<smac>] [<dmac_type>] [(etype [<etype>]) | (LLC [<DSAP>] [<SSAP>] [<control>]) | (SNAP [<PID>]) | (ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) | ([ipv6] [<sip_v6>] [<dscp>] [<sport>] [<dport>])] [<class>] [<dp>] [<classified_dscp>]

매개 변수 :
<qce_id> : QCE ID (1-256), 기본값 : 다음 사용 가능한 ID
<qce_id_next> : 다음 QCE ID : "next_id (1-256) 또는 'last"'
<port_list> : 포트 목록 : "port <port_list> 또는 'all"', 기본값 : 모든 포트
<tag> : 프레임 태그 : untag | tag | any
<vid> : VID : 1-4095 또는 'Any', 특정 VID 또는 VID 범위

<pcp> : 우선 순위 코드 포인트 : 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> : 드롭 적격 지시자 : 0-1 또는 'any'

<smac> : 원본 MAC 주소 : (xx-xx-xx) 또는 'any', 24 MS 비트 (OUI)

<dmac_type> : 대상 MAC 유형 : 유니 캐스트 | 멀티 캐스트 | 브로드 캐스트 | 모든

etype : 이더넷 유형 키워드

<etype> : 이더넷 유형 : 0x600-0xFFFF 또는 'any'(0x800 (IPv4) 및 0x86DD (IPv6) 제외)

LLC : LLC 키워드

<dsap> : 대상 서비스 액세스 지점 : 0x00-0xFF 또는 'any'

<ssap> : 원본 서비스 액세스 지점 : 0x00-0xFF 또는 'any'

<control> : LLC 제어 : 0x00-0xFF 또는 'any'

snap : SNAP 키워드

<pid> : 프로토콜 ID (EtherType) 또는 'any'

ipv4 : IPv4 keyowrd

<protocol> : IP 프로토콜 번호 : (0-255, TCP 또는 UDP) 또는 'any'

<sip> : 소스 IP 주소 : (a.b.c.d / n) 또는 'any'

<dscp> : DSCP : (0-63, BE, CS1-CS7, EF 또는 AF11-AF43) 또는 'any', 특정 또는 범위

<fragment> : 조각화 된 IPv4 프레임 : yes | no | any

<sport> :TCP / UDP 포트 : (0-65535) 또는 'any', 특정 또는 포트 범위

<dport> : 목적지. TCP / UDP 포트 : (0-65535) 또는 'any', 특정 포트 또는 포트 범위

ipv6 : IPv6 keyword

<sip_v6> : IPv6 소스 주소 : (a.b.c.d / n) 또는 'any', 32 LS 비트

<class> : QoS 클래스 : "class (0-7)", 기본값 : 기본 분류

<dp> : DP 수준 : "dp (0-3)", 기본값 : 기본 분류

<classified_dscp> : DSCP : "dscp (0-63, BE, CS1-CS7, EF 또는 AF11-AF43)"

QoS QCL 삭제

설명 :

QoS 제어 목록에서 QCE 항목을 삭제하십시오.

통사:

QoS QCL 삭제 <qce_id>

매개 변수 :

<qce_id> : QCE ID (1-256), 기본값 : 다음 사용 가능한 ID

QoS QCL 조회

설명 :

조회 QoS 제어 목록.

통사:

QoS QCL 조회 [<qce_id>]

매개 변수 :

<qce_id> : QCE ID (1-256), 기본값 : 다음 사용 가능한 ID

QoS QCL 상태

설명 :

QCL 상태를 표시하십시오. differnet 사용자 유형에 대해 QCE 에 충돌이 있는지를 표시하는 데 사용할 수 있습니다.

통사:

QoS QCL 상태 [결합 된 | 정적 | voice_vlan | 충돌]

매개 변수 :

결합 된 | 정적 | voice_vlan | 충돌 : 결합 : 결합 된 상태를 표시합니다.

static : 정적 사용자 구성 상태를 표시합니다.

voice_vlan : 음성 VLAN 별 상태를 보여줍니다.

충돌 : 모든 충돌 상태를 표시합니다.

(기본값 : 결합 된 상태를 표시합니다)

QoS QCL 새로 고침

설명 :

QCE 충돌 상태를 해결합니다. 동일한 H / W 자원이 여러 응용 프로그램에 의해 공유되며 MAX QCE 입력 전에도 사용할 수 없습니다. 따라서 사용자는 다른 응용 프로그램에서 사용중인 자원을 해제하고이 명령을 사용하여 자원을 확보 할 수 있습니다.

통사:

QoS QCL 새로 고침

5.14 Mirror 명령어

미러 구성

설명 :

미러 구성을 표시합니다.

통사:

미러 구성 [<port_list>]

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

미러 구성을 표시합니다.

```
SFC4000T:/>mirror configuration
```

미러 포트

설명 :

미러 포트를 설정하거나 표시하십시오.

통사:

미러 포트 [<port> | disable]

매개 변수 :

<port> | disable : 미러 포트 또는 'disable', 기본값 : 포트 표시

기본 설정:

disable

예:

미러 포트에 대해 포트 2 를 설정하십시오.

```
SFC4000T:/>mirror port 2
```

미러 모드

설명 :

미러 모드를 설정하거나 표시합니다.

통사:

미러 모드 [<port_cpu_list>] [enable | disable | rx | tx]

매개 변수 :

<port_cpu_list> : 포트 목록 또는 CPU 또는 'all', 기본값 : 모든 포트 및 CPU

enable : Rx 및 Tx 미러링 사용

disable : 미러링 해제

rx : Rx 미러링 사용

tx : Tx 미러링 사용

(기본값 : 미러 모드 표시)

기본 설정:

disable

예:

포트 1-4 의 미러 모드를 활성화합니다.

```
SFC4000T:/>mirror mode 1-4 enable
```

5.15 Configuration 명령어

구성 저장

설명 :

구성을 TFTP 서버에 저장하십시오.

통사:

구성 저장 <ip_server> <file_name>

매개 변수 :

<ip_server> : TFTP 서버 IP 주소 (a.b.c.d)

<file_name> : 구성 파일 이름

구성로드

설명 :

TFTP 서버에서 구성을로드하십시오.

통사:

구성로드 <ip_server> <file_name> [확인]

매개 변수 :

<ip_server> : TFTP 서버 IP 주소 (a.b.c.d)

<file_name> : 구성 파일 이름

확인 : 구성 파일 만 확인, 기본값 : 파일 확인 및 적용

5.16 Firmware 명령어

펌웨어로드

설명 :

TFTP 서버에서 새 펌웨어를로드하십시오.

통사:

펌웨어로드 <ip_addr_string> <file_name>

매개 변수 :

<ip_addr_string> : IP 호스트 주소 (a.b.c.d) 또는 호스트 이름 문자열

<file_name> : 펌웨어 파일 이름

펌웨어 IPv6 로드

설명 :

IPv6 TFTP 서버에서 새 펌웨어를로드하십시오.

통사:

펌웨어 IPv6 로드 <ipv6_server> <file_name>

매개 변수 :

<ipv6_server> : TFTP 서버 IPv6 주소

<file_name> : 펌웨어 파일 이름

펌웨어 정보

설명 :

활성 및 대체 펌웨어 이미지에 대한 정보를 표시합니다.

통사:

펌웨어 정보

펌웨어 스왑

설명 :

대체 펌웨어 이미지를 활성화하십시오.

통사:

펌웨어 스왑

5.17 UPnP 명령어

UPnP 구성

설명 :

UPnP 구성을 표시합니다.

통사:

UPnP 구성

예:

UPnP 구성을 표시합니다.

```
SFC4000T:/>upnp configuration

UPnP Configuration:
==================

UPnP Mode                    : Disabled
UPnP TTL                     : 4
UPnP Advertising Duration : 100
```

UPnP 모드

설명 :

UPnP 모드를 설정하거나 표시합니다.

통사:

UPnP 모드 [enable | disable]

매개 변수 :

enable : UPnP 사용

disable : UPnP 비활성화

(기본값 : Show UPnP mode)

기본 설정:

disable

예:

UPnP 모드를 사용합니다.

```
SFC4000T:/>upnp mode enable
```

UPnP TTL

설명 :

SSDP 메시지에서 IP 헤더의 TTL 값을 설정하거나 표시합니다.

통사:

UPnP TTL [<ttl>]

매개 변수 :

<ttl> : ttl 범위 (1..255), 기본값 : UPnP TTL 표시

기본 설정:

4

예:

SSDP 메시지에서 IP 헤더의 TTL 값으로 10 을 설정하십시오.

```
SFC4000T:/>upnp ttl 10
```

UPnP 광고 기간

설명 :

UPnP 광고 기간 설정 또는 표시.

통사:

UPnP 광고 기간 [<기간>]

매개 변수 :

<duration> : 기간 범위 (100..86400), 기본값 : UPnP 지속 기간 표시

기본 설정:

100

예:

UPnP 광고 기간에 대해 1000 값을 설정하십시오.

```
SFC4000T:/>upnp advertising duration 1000
```

5.18 MVR 명령어

MVR 구성

설명 :

MVR 구성을 표시하십시오.

통사:

MVR 구성

예:

MVR 구성을 표시하십시오.

```
SFC4000T:/>mvr configuration

MVR Configuration:
==================

MVR Mode: Disabled
Muticast VLAN ID: 100

Port    Port Mode       Port Type       Immediate Leave
----    -----------     -----------     ---------------
1       Disabled        Receive         Disabled
2       Disabled        Receive         Disabled
3       Disabled        Receive         Disabled
4       Disabled        Receive         Disabled
5       Disabled        Receive         Disabled
6       Disabled        Receive         Disabled
7       Disabled        Receive         Disabled
8       Disabled        Receive         Disabled
9       Disabled        Receive         Disabled
10      Disabled        Receive         Disabled
```

MVR 모드

설명 :

MVR 모드를 설정하거나 표시합니다.

통사:

MVR 모드 [enable | disable]

매개 변수 :

enable : MVR 모드 사용

disable : MVR 모드 사용 불가

(기본값 : MVR 모드 표시)

기본 설정:

disable

예:

MVR 모드를 사용합니다.

```
SFC4000T:/>mvr mode enable
```

MVR VLAN 설정

설명 :

MVR VLAN 구성을 설정하거나 표시합니다.

통사:

MVR VLAN 설정 [<mvid>] [add | del | upd] [(Name <mvr_name>)]

매개 변수 :

<mvid> : MVR VLAN ID (1-4095)

추가 : 작업 추가

del : 작업 삭제

upd : 업데이트 작업

이름 : MVR 이름 키워드

<mvr_name> : MVR VLAN 이름 (최대 32 자)

MVR VLAN 모드

설명 :

MVR VLAN 모드 당 설정 또는 표시.

통사:

MVR VLAN 모드 [<vid> | <mvr_name>] [dynamic | compatible]

매개 변수 :

<vid> | <mvr_name> : MVR VLAN ID (1-4095) 또는 이름 (최대 32 자)

동적 : 동적 MVR 모드

호환 가능 : 호환 가능한 MVR 모드

(기본값 : MVR VLAN 모드 표시)

MVR VLAN 포트

설명 :

MVR VLAN 포트 역할을 설정하거나 표시합니다.

통사:

MVR VLAN 포트 [<vid> | <mvr_name>] [<port_list>] [source | receiver | inactive]

매개 변수 :

<vid> | <mvr_name> : MVR VLAN ID (1-4095) 또는 이름 (최대 32 자)

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

출처 : MVR 출처 포트

수신기 : MVR 수신기 포트

비활성 : MVR 사용 중지

(기본값 : MVR 포트 역할 표시)

MVR VLAN LLQI

설명 :

MVR VLAN 당 LLQI (Last Listener Query Interval)를 설정하거나 표시합니다.

통사:

MVR VLAN LLQI [<vid> | <mvr_name>] [mvr_param_llqi]

매개 변수 :

<vid> | <mvr_name> : MVR VLAN ID (1-4095) 또는 이름 (최대 32 자)

mvr_param_llqi :

-1 : 기본값 (5)

0 ~ 31744 : 마지막 청취자 쿼리 간격 (1/10 초)

(기본값 : MVR 인터페이스 마지막 수신기 쿼리 간격 표시

MVR VLAN 채널

설명 :

MVR VLAN 채널당 설정 또는 표시합니다.

통사:

MVR VLAN 채널 [<vid> | <mvr_name>] [add | del | upd] [채널] [channel_bound] [(Name <grp_name>)]

매개 변수 :

<vid> | <mvr_name> : MVR VLAN ID (1-4095) 또는 이름 (최대 32 자)

추가 : 작업 추가

del : 작업 삭제

upd : 업데이트 작업

채널 : IPv4 / IPv6 멀티 캐스트 그룹 주소

channel_bound : 채널의 경계 IPv4 / IPv6 멀티 캐스트 그룹 주소

이름 : MVR 이름 키워드

<grp_name> : MVR 채널 이름. (최대 32 자)

MVR VLAN 우선 순위

설명 :

MVR VLAN 우선 순위 및 VLAN 태그 당 설정 또는 표시.

통사:

MVR VLAN 우선 순위 [<vid> | <mvr_name>] [priority] [태그가 지정되지 않은 | 태그가 지정되지 않음]

매개 변수 :

<vid> | <mvr_name> : MVR VLAN ID (1-4095) 또는 이름 (최대 32 자)

priority : CoS 우선 순위 값의 범위는 0 ~ 7 입니다.

tagged : 태그 된 IGMP / MLD 프레임이 전송됩니다.

태그 없음 : 태그가 지정되지 않은 IGMP / MLD 프레임이 전송됩니다.

MVR Immediate Leave

설명 :

포트 당 MVR 즉시 설정 또는 표시.

통사:

MVR 즉시 종료 [<port_list>] [enable | disable]

매개 변수 :

<< port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

활성화 : 즉각 종료 가능

사용 안 함 : 즉시 사용 안 함

(기본값 : MVR 직접 종료 표시)

MVR 상태

설명 :

MVR 작동 상태 표시 / 지우기.

통사:

MVR 상태 [<vid>] [지우기]

매개 변수 :

<vid> : VLAN ID (1-4095)

clear : 로그 지우기

MVR 그룹

설명 :

MVR 그룹 주소를 표시합니다.

통사:

MVR 그룹 [<vid>]

매개 변수 :

<vid> : VLAN ID (1-4095)

MVR SFM

설명 :

MVR 에 대한 SFM (SSM 포함) 관련 정보 표시

통사:

MVR SFM [<vid>] [<port_list>]

매개 변수 :

<vid> : VLAN ID (1-4095)

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

5.19 Voice VLAN 명령어

음성 VLAN 구성

설명 :

음성 VLAN 구성을 표시합니다.

통사:

음성 VLAN 구성

예제:

음성 VLAN 구성을 표시합니다.

```
SFC4000T:/>voice vlan configuration

V oice VLAN Configuration:
==========================

Voice VLAN Mode                    : Disabled
Voice VLAN VLAN ID                 : 1000
Voice VLAN Age Time(seconds)   : 86400
Voice VLAN Traffic Class         : 7

Voice VLAN OUI Table:
=====================

Telephony OUI  설명
------------- -----------
00-30-4F         SOLTECH phones
00-03-6B         Cisco phones
00-0F-E2         H3C phones
00-60-B9         Philips and NEC AG phones
00-D0-1E         Pingtel phones
00-E0-75         Polycom phones
```

```
00-E0-BB          3Com phones
00-01-E3          Siemens AG phones

Voice VLAN Port Configuration:
==============================



Port    Mode         Security    Discovery Protocol
----    --------     --------    ------------------
1       Disabled     Disabled       OUI
2       Disabled     Disabled       OUI
3       Disabled     Disabled       OUI
4       Disabled     Disabled       OUI
5       Disabled     Disabled       OUI
6       Disabled     Disabled       OUI
7       Disabled     Disabled       OUI
8       Disabled     Disabled       OUI
9       Disabled     Disabled       OUI
10      Disabled     Disabled       OUI
```

음성 VLAN 모드

설명 :

음성 VLAN 모드를 설정하거나 표시합니다.

음성 VLAN 을 활성화하기 전에 MSTP 기능을 비활성화해야합니다.

수신 필터의 충돌을 피할 수 있습니다.

통사:

음성 VLAN 모드 [enable | disable]

매개 변수 :

enable : 음성 VLAN 모드를 활성화합니다.

disable : 음성 VLAN 모드 비활성화

(기본값 : Show flow Voice VLAN 모드)

기본 설정:

disable

예:

음성 VLAN 모드를 활성화하십시오.

```
SFC4000T:/>voice vlan mode enable
```

음성 VLAN ID

설명 :

음성 VLAN ID 를 설정하거나 표시합니다.

통사:

음성 VLAN ID [<vid>]

매개 변수 :

<vid> : VLAN ID (1-4095)

기본 설정:

1000

예:

음성 VLAN ID 에 대해 ID 2 를 설정하십시오.

```
SFC4000T:/>voice vlan id 2
```

음성 VLAN Agetime

설명 :

음성 VLAN aging 시간을 설정하거나 표시합니다.

통사:

음성 VLAN Agetime [<연령 _ 시간>]

매개 변수 :

<age_time> : MAC 주소 보존 기간 (10-10000000) 기본값 : 보존 기간 표시

기본 설정:

86400 초

예:

음성 VLAN aging 시간을 100 초로 설정하십시오.

```
SFC4000T:/>voice valn agetime 100
```

음성 VLAN 트래픽 클래스

설명 :

음성 VLAN ID 를 설정하거나 표시합니다.

통사:

음성 VLAN 트래픽 클래스 [<class>]

매개 변수 :

<class> : 트래픽 클래스 (0-7)

기본 설정:

7

예: 음성 VLAN 에 대해 4 개의 트래픽 클래스 설정

```
SFC4000T:/>voice vlan traffic class4
```

음성 VLAN OUI 추가

설명 :

음성 VLAN OUI 항목을 추가하십시오.

OUI 테이블을 수정하면 OUI 프로세스 자동 검색이 다시 시작됩니다. 최대 엔트리 수는 (16)입니다.

통사:

음성 VLAN OUI <oui_addr> 추가 [<설명>]

매개 변수 :

<oui_addr> : OUI 주소 (xx-xx-xx). null OUI 주소는 허용되지 않습니다.

<설명> : 항목 설명. 문자열을 지우려면 '지우기' 또는 " 사용하십시오. 연락처의 일부로 공백이나 공백 문자를 사용할 수 없습니다. (CLI 에서만)

예:

음성 VLAN OUI 항목을 추가하십시오.

SFC4000T : /> 음성 VLAN 을 oui 추가 00-11-22 테스트

음성 VLAN OUI 삭제
설명 :
음성 VLAN OUI 항목을 삭제하십시오.
OUI 테이블을 수정하면 OUI 프로세스 자동 검색이 다시 시작됩니다.

통사:
음성 VLAN OUI 삭제 <oui_addr>

매개 변수 :
<oui_addr> : OUI 주소 (xx-xx-xx). null OUI 주소는 허용되지 않습니다.

예:
음성 VLAN OUI 항목을 삭제하십시오.
SFC4000T : /> voice vlan oui delete 00-11-22

음성 VLAN OUI 지우기
설명 :
음성 VLAN OUI 항목 지우기.
OUI 테이블을 수정하면 OUI 프로세스 자동 검색이 다시 시작됩니다.

통사:
음성 VLAN OUI 지우기

예:
음성 VLAN OUI 항목 지우기.
SFC4000T : /> voice vlan oui clear

음성 VLAN OUI 조회
설명 :
조회 음성 VLAN OUI 항목.

통사:
음성 VLAN OUI 조회 [<oui_addr>]

매개 변수 :

<oui_addr> : OUI 주소 (xx-xx-xx), 기본값 : OUI 주소 표시

음성 VLAN 포트 모드
설명 :
음성 VLAN 포트 모드를 설정하거나 표시합니다.
포트 모드가 비활성화되어 있지 않으면 음성 VLAN 을 활성화하기 전에 MSTP 기능을
비활성화해야합니다. 수신 필터의 충돌을 피할 수 있습니다.

통사:
음성 VLAN 포트 모드 [<port_list>] [disable | auto | force]

매개 변수 :
<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트
disable : 음성 VLAN 에서 탈퇴하십시오.
auto : 자동 감지 모드를 활성화합니다. 특정 포트에 VoIP 전화가 연결되어 있는지 감지하고 음성 VLAN 멤버를 자동으로 구성합니다.
강제 : 음성 VLAN 에 강제 가입.
(기본값 : 음성 VLAN 포트 모드 표시)

기본 설정:
disable

예:
음성 VLAN 포트 모드의 포트 1-4 에 자동 모드를 설정하십시오.
SFC4000T : /> 음성 VLAN 포트 모드 1-4 자동

음성 VLAN 보안
설명 :
음성 VLAN 포트 보안 모드를 설정하거나 표시합니다. 이 기능을 사용하면 음성 VLAN 의 모든 비 전화 MAC 주소가 10 초 동안 차단됩니다.

통사:
음성 VLAN 보안 [<port_list>] [enable | disable]

매개 변수 :
<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

enable : 음성 VLAN 보안 모드를 활성화합니다.
disable : 음성 VLAN 보안 모드 비활성화
(기본값 : Show flow 음성 VLAN 보안 모드)

기본 설정:
disable

예:
포트 1-4 에 대해 음성 VLAN 포트 보안 모드를 활성화하십시오.
SFC4000T : /> 음성 VLAN 보안 1-4 활성화

음성 VLAN 발견 프로토콜
설명 :
음성 VLAN 포트 탐색 프로토콜 모드를 설정하거나 표시합니다. 자동 감지 모드에서만 작동합니다. 구성 검색 프로토콜을 'LLDP'또는 'Both'로 설정하기 전에 LLDP 기능을 활성화해야합니다. 검색 프로토콜을 'OUI'로 변경하거나 'LLDP'를 선택하면 자동 검색 프로세스가 다시 시작됩니다.

통사:
음성 VLAN 검색 프로토콜 [<port_list>] [oui | lldp | both]

매개 변수 :
<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트
OUI : OUI 주소로 전화 통신 장치를 검색합니다.
LLDP : LLDP 로 전화 통신 장치를 감지합니다.
둘 다 : OUI 와 LLDP 둘 다.
(기본값 : 음성 VLAN 검색 프로토콜 표시)

기본 설정:
OUI

5.20 Loop Protect 명령어

루프 보호 구성
설명 :
Show Loop Protection 구성.

통사:
루프 보호 구성

루프 보호 모드
설명 :
루프 보호 모드를 설정하거나 표시하십시오.

통사:
루프 보호 모드 [enable | disable]

매개 변수 :
enable : 루프 보호 사용
disable : 루프 보호 해제

기본 설정:
가능하게하다

루프 보호 전송
설명 :
루프 보호 전송 간격을 설정하거나 표시하십시오.

통사:
루프 보호 전송 [<전송 시간>]

매개 변수 :
전송 시간 간격 (1 ~ 10 초)

루프 보호 셧다운
설명 :
루프 보호 종료 시간을 설정하거나 표시하십시오.

통사:
루프 보호 종료 [<shutdown-time>]

매개 변수 :
종료 시간 간격 (0-604800 초)
0 값을 사용하면 포트를 다시 활성화 할 수 없습니다.

루프 보호 포트 구성
설명 :
Show Loop Protection 포트 구성.

통사:
루프 보호 포트 구성 [<port_list>]

매개 변수 :
<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

루프 보호 포트 모드
설명 :
루프 보호 포트 모드를 설정하거나 표시하십시오.

통사:
루프 보호 포트 모드 [<port_list>] [enable | disable]

매개 변수 :
<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트
enable : 루프 보호 사용
disable : 루프 보호 해제

루프 보호 포트 동작
설명 :
루프 보호 포트 동작을 설정하거나 표시합니다.

통사:
루프 보호 포트 작업 [<port_list>] [shutdown | shut_log | log]

매개 변수 :
<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트
shutdown : 포트를 종료합니다.
shut_log : 포트 및 로그 이벤트를 종료합니다.
log : (전용) 이벤트를 기록합니다.

5.21 IPMC 명령어

IPMC 구성

설명 :

IPMC 스누핑 구성을 표시합니다.

통사:

IPMC 구성 [mld | igmp]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

IPMC 모드

설명 :

IPMC 스누핑 모드를 설정하거나 표시합니다.

통사:

IPMC 모드 [mld | igmp] [enable | disable]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

enable : IPMC 스누핑을 활성화합니다.

disable : IPMC 스누핑을 비활성화합니다.

(기본값 : 글로벌 IPMC 스누핑 모드 표시)

기본 설정:

disable

예:

IGMP 스누핑 사용

SFC4000T : /> ipmc 모드 igmp enable

IPMC flooding

설명 :

IPMC 미등록 주소 플러딩 작업을 설정하거나 표시합니다.

통사:

IPMC 플러딩 [mld | igmp] [enable | disable]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

enable : IPMC 범람 활성화

disable : IPMC 홍수 비활성화

(기본값 : 글로벌 IPMC 플러딩 모드 표시)

기본 설정:

disable

예:

IGMP 플러딩 사용

SFC4000T : /> ipmc 범람 igmp enable

IPMC 에서 프록시 해제

설명 :

IPMC Leave Proxy 모드를 설정하거나 표시합니다.

통사:

IPMC 에서 프록시 나가기 [mld | igmp] [enable | disable]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

enable : IPMC Leave Proxy 사용

disable : IPMC Leave 프록시 비활성화

(기본값 : 글로벌 IPMC 프록시 모드 종료 표시)

기본 설정:

disable

예:

IGMP 나가기 프록시 사용

SFC4000T : /> ipmc 는 프록시 igmp 를 사용 가능으로 유지합니다.

IPMC 프록시

설명 :

IPMC 프록시의 모드를 설정하거나 표시합니다.

통사:

IPMC 프록시 [mld | igmp] [enable | disable]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

enable : IPMC 프록시 사용

disable : IPMC 프록시 비활성화

(기본값 : 글로벌 IPMC 프록시 모드 표시)

기본 설정:

disable

예:

IGMP 프록시 사용

SFC4000T : /> ipmc proxy igmp enable

IPMC SSM

설명 :

IPMC SSM 범위를 설정하거나 표시합니다.

통사:

IPMC SSM [mld | igmp] [(범위 <prefix> <mask_len>)]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

범위 : SSM 범위 키워드

<prefix> : IPv4 / IPv6 멀티 캐스트 그룹 주소

<mask_len> : IPv4 (4 ~ 32) / IPv6 (8 ~ 128) ssm 범위의 마스크 길이

IPMC VLAN 추가

설명 :

IPMC 스누핑 VLAN 인터페이스를 추가하십시오.

통사:

IPMC VLAN 추가 [mld | igmp] <vid>

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<vid> : VLAN ID (1-4095)

IPMC VLAN 삭제

설명 :

IPMC 스누핑 VLAN 인터페이스를 삭제하십시오.

통사:

IPMC VLAN 삭제 [mld | igmp] <vid>

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<vid> : VLAN ID (1-4095)

IPMC state

설명 :

VLAN 에 대한 IPMC 스누핑 상태를 설정하거나 표시합니다.

통사:

IPMC 상태 [mld | igmp] [<vid>] [enable | disable]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<vid> : VLAN ID (1-4095) 또는 'any', 기본값 : 모든 VLAN 표시

enable : MLD 스누핑 활성화

disable : MLD 스누핑을 비활성화합니다.

기본 설정:

disable

예:

VLAN 1 에 대해 IGMP 스누핑 상태 사용

SFC4000T : /> ipmc state igmp 1 enable

IPMC Querier

설명 :

VLAN 에 대한 IPMC snooping querier 모드를 설정하거나 표시합니다.

통사:

IPMC Querier [mld | igmp] [<vid>] [enable | disable]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<vid> : VLAN ID (1-4095) 또는 'any', 기본값 : 모든 VLAN 표시

활성화 : MLD 쿼리 러 사용

disable : MLD 쿼리를 비활성화합니다.

기본 설정:

가능하게하다

예:

VLAN 1 에 대해 IGMP 쿼리 작성 사용

SFC4000T : /> ipmc querier igmp 1 enable

IPMC 호환성

설명 :

IPMC 호환성을 설정하거나 표시하십시오.

통사:

IPMC 호환성 [mld | igmp] [<vid>] [auto | v1 | v2 | v3]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<vid> : VLAN ID (1-4095) 또는 'any', 기본값 : 모든 VLAN 표시

자동 | v1 | v2 | v3 :

자동 : 자동 호환성 (기본값)

v1 : IGMPv1 또는 MLDv1 의 강제 호환

v2 : IGMPv2 또는 MLDv2 의 강제 호환

v3 : IGMPv3 의 강제 호환

(기본값 : IPMC 인터페이스 호환성 표시)

IPMC Fastleave

설명 :

IPMC 스누핑 고속 포트 모드를 설정하거나 표시하십시오.

통사:

IPMC Fastleave [mld | igmp] [<port_list>] [enable | disable]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

활성화 : MLD 고속 탈퇴 활성화

disable : MLD fast leave 를 비활성화합니다.

(기본값 : IPMC 고속 대기 모드 표시)

기본 설정:

disable

예:

모든 포트에 대해 IGMP 고속 대기 사용

```
SFC4000T:/>ipmc fastleave igmp 1-10 enable
```

IPMC Throttling

설명 :

IPMC 포트 스로틀 상태를 설정하거나 표시합니다.

통사:

IPMC 스로틀 [mld | igmp] [<port_list>] [limit_group_number]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

0 : 제한 없음

1 ~ 10 : 그룹 학습 한도

(기본값 : Show IPMC Port Throttling)

기본 설정:

제한 없는

예:

최대 값을 설정하십시오. ICMP 포트 조절을위한 10 개 그룹 학습

```
SFC4000T:/>ipmc throttling igmp 1-10 10
```

IPMC 필터링

설명 :

IPMC 포트 그룹 필터링 목록을 설정하거나 표시합니다.

통사:

IPMC 필터링 [mld | igmp] [<port_list>] [add | del] [group_addr]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

add : 새 포트 그룹 필터링 항목을 추가합니다.

del : 기존 포트 그룹 필터링 항목을 삭제합니다.

(기본값 : IPMC 포트 그룹 필터링 목록 표시)

group_addr : IPv4 / IPv6 멀티 캐스트 그룹 주소

IPMC 라우터

설명 :

IPMC 스누핑 라우터 포트 모드를 설정하거나 표시합니다.

통사:

IPMC 라우터 [mld | igmp] [<port_list>] [auto | fix | none]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

auto : IGMP 라우터 모드 자동 활성화

수정 : IGMP 라우터 모드 수정 사용

none : IGMP 라우터 모드 사용 안 함

IPMC 상태

설명 :

그에 따라 IPMC 작동 상태를 표시하십시오.

통사:

IPMC 상태 [mld | igmp] [<vid>]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<vid> : VLAN ID (1-4095) 또는 'any', 기본값 : 모든 VLAN 표시

예:

VLAN 1 IPMC 작동 상태 표시

```
SFC4000T:/>ipmc status igmp 1
```

IPMC 그룹

설명 :

그룹에 따라 IPMC 그룹 주소를 표시하십시오.

통사:

IPMC 그룹 [mld | igmp] [<vid>]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<vid> : VLAN ID (1-4095) 또는 'any', 기본값 : 모든 VLAN 표시

예:

VLAN 1 IPMC 그룹 주소를 표시하십시오.

```
SFC4000T:/>ipmc groups igmp 1
```

IPMC 버전

설명 :

IPMC 버전 표시.

통사:

IPMC 버전 [mld | igmp] [<vid>]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<vid> : VLAN ID (1-4095) 또는 'any', 기본값 : 모든 VLAN 표시

예:

VLAN 1 IPMC 버전을 표시합니다.

```
SFC4000T:/>ipmc version igmp 1
```

IPMC SFM

설명 :

IPMC 에 SFM (SSM 포함) 관련 정보 표시

통사:

IPMC SFM [mld | igmp] [<vid>] [<port_list>]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<vid> : VLAN ID (1-4095) 또는 'any', 기본값 : 모든 VLAN 표시

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

IPMC 매개 변수 RV

설명 :

IPMC 견고성 변수를 설정하거나 보여줍니다.

통사:

IPMC 매개 변수 RV [mld | igmp] [<vid>] [ipmc_param_rv]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<vid> : VLAN ID (1-4095) 또는 'any', 기본값 : 모든 VLAN 표시

ipmc_param_rv :

-1 : 기본값 (2)

1 ~ 255 : 내구성 변수

(기본값 : Show IPMC Interface Robustness Variable

IPMC 매개 변수 QI

설명 :

IPMC 쿼리 간격을 설정하거나 표시합니다.

통사:

IPMC 매개 변수 QI [mld | igmp] [<vid>] [ipmc_param_qi]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<vid> : VLAN ID (1-4095) 또는 'any', 기본값 : 모든 VLAN 표시

ipmc_param_qi :

-1 : 기본값 (125)

1 ~ 31744 : 초 단위의 쿼리 간격

(기본값 : Show IPMC Interface Query Interval

IPMC 매개 변수 QRI

설명 :

IPMC 쿼리 응답 간격을 설정하거나 표시합니다.

통사:

IPMC 매개 변수 QRI [mld | igmp] [<vid>] [ipmc_param_qri]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<vid> : VLAN ID (1-4095) 또는 'any', 기본값 : 모든 VLAN 표시

ipmc_param_qri :

-1 : 기본값 (100)

0 ~ 31744 : 쿼리 응답 간격 (1/10 초)

(기본값 : IPMC 인터페이스 쿼리 응답 간격 표시

IPMC 매개 변수 LLQI

설명 :

IPMC 마지막 수신기 쿼리 간격을 설정하거나 표시합니다.

통사:

IPMC 매개 변수 LLQI [mld | igmp] [<vid>] [ipmc_param_llqi]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<vid> : VLAN ID (1-4095) 또는 'any', 기본값 : 모든 VLAN 표시

ipmc_param_llqi :

-1 : 기본값 (10)

0 ~ 31744 : 마지막 청취자 쿼리 간격 (1/10 초)

(기본값 : Show IPMC Interface 마지막 수신기 쿼리 간격

IPMC 매개 변수 URI

설명 :

IPMC Unsolicited Report Interval 을 설정하거나 표시합니다.

통사:

IPMC 매개 변수 URI [mld | igmp] [<vid>] [ipmc_param_uri]

매개 변수 :

mld | igmp :

mld : IPv6 MLD 용 IPMC

igmp : IPv4 용 IPMC IGMP

<vid> : VLAN ID (1-4095) 또는 'any', 기본값 : 모든 VLAN 표시

ipmc_param_uri :

-1 : 기본값 (1)

0 ~ 31744 : 원치 않는보고 간격 (초)

(기본값 : IPMC Interface Unsolicited Report Interval 표시

6.22 sFlow 명령

sFlow 구성

설명 :

전역 및 포트 별 sFlow 구성 표시.

통사:

sFlow 구성

sFlow 수신기

설명 :

sFlow 수신기 제한 시간, IP 주소 및 UDP 포트를 설정하거나 표시합니다.

통사:

sFlow 수신기 [해제] [<시간 초과>] [<ip_addr_host>] [<udp_port>] [<데이터 그램 크기>]

매개 변수 :

release : 수신자의 현재 소유자를 해제합니다.

소유주는 현재 누군가가 소유하지 않은 경우 "<없음>"일 수 있으며, CLI 또는 웹에 의해 현재 설정되어있는 경우 "<로컬 관리를 통해 구성 됨>"일 수 있습니다. 설정되어 있으면 소유자가 될 수 있습니다 SNMP 를 통해 리시버가 현재 소유 중이거나 CLI 또는 웹 소유인 경우에만 리시버를 구성 할 수 있습니다. 이 인수가 지정되면 나머지 인수는 무시됩니다.

<timeout> : 초 단위로 측정 한 수신기 시간 초과입니다. 스위치는 초 당 1 회 타임 아웃을 감소시키고, 0 이 아닌 한 수신기는 샘플을 수신합니다. 시간 초과가 0 에 도달하면 수신자와 모든 구성이 기본값으로 재설정됩니다. 유효한 범위는 0 - 2147483647 초입니다.

<ip_addr_host> : IPv4 / IPv6 주소 또는 수신자를 식별하는 호스트 이름.

<udp_port> : 수신자의 UDP 포트. 유효한 범위는 0 - 65535 입니다.

0 을 사용하여 기본 포트 (6343)를 가져옵니다.

<datagram_size> : 최대 데이터 그램 크기. 유효한 범위는 200-1,468 바이트입니다.

기본값은 1400 바이트입니다.

sFlow FlowSampler

설명 :

포트별로 플로우 샘플러 구성을 설정하거나 보여줍니다.

작동시 샘플링 속도 'N'은 지원되는 가장 가까운 값으로 반올림됩니다.

통사:

sFlow FlowSampler [<port_list>] [<sampling_rate>] [<max_hdr_size>]

매개 변수 :

<port_list> : 포트 목록 또는 'all'. 기본값 : 모든 포트.

<sampling_rate> : 통계적 샘플링 속도를 지정합니다.

샘플 속도는 모니터 된 플로우에서 패킷의 1 / N 번째를 샘플링하기 위해 N 으로 지정됩니다. 값에는 제한이 없지만 스위치는 가장 가까운 샘플링 속도로 조정합니다.

0 은 샘플링을 비활성화합니다.

<max_hdr_size> : 플로우 샘플 당 전송할 최대 바이트 수를 지정합니다.

유효한 범위는 14 - 200 바이트입니다. 기본값 : 128 바이트.

sFlow CounterPoller

설명 :

포트별로 카운터 폴링 간격 구성을 설정하거나 표시합니다.

통사:

sFlow 카운터 폴러 [<port_list>] [<interval>]

매개 변수 :

<port_list> : 포트 목록 또는 'all'. 기본값 : 모든 포트.

<interval> : 0 - 3600 범위의 폴링 간격.

이 포트의 자원을 해제하려면 0 으로 설정하십시오.

sFlow 통계 수신기

설명 :

수신기 통계를 가져 오거나 지우십시오.

통사:

sFlow 통계 수신기 [clear]

매개 변수 :

clear : 통계를 지 웁니다.

sFlow 통계 샘플러

설명 :

포트 별 통계를 가져 오거나 지 웁니다.

통사:

sFlow 통계 샘플러 [<port_list>] [clear]

매개 변수 :

<port_list> : 포트 목록 또는 'all'. 기본값 : 모든 포트.

clear : 통계를 지웁니다.

5.22 VLAN Control List 명령어

VCL MAC 기반 VLAN 구성

설명 :

VCL MAC 기반 VLAN 구성을 표시합니다.

통사:

VCL Macvlan 구성

VCL MAC 기반 VLAN 추가

설명 :

VCL MAC 기반 VLAN 항목을 추가 또는 수정하십시오.

통사:

VCL Macvlan Add <mac_addr> <vid> [<port_list>]

매개 변수 :

<mac_addr> : MAC 주소 (xx-xx-xx-xx-xx-xx)

<vid> : VLAN ID (1-4095)

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

예:

모든 포트에 대해 VLAN 20 에 00-11-22-33-44-55-66 을 추가하십시오.

SFC4000T : /> vcl macvlan add 00-11-22-33-44-55-66 20 1-10

VCL MAC 기반 VLAN 삭제

설명 :

VCL MAC 기반 VLAN 항목을 삭제하십시오.

통사:

VCL Macvlan Del <mac_addr>

매개 변수 :

<mac_addr> : MAC 주소 (xx-xx-xx-xx-xx-xx)

예제:

MAC 기반 VLAN 목록에서 00-11-22-33-44-55-66 삭제

SFC4000T:/> **vcl macvlan del 00-11-22-33-44-55-66**

VCL Status

설명 :

VCL MAC 기반 VLAN 사용자 구성을 표시합니다.

통사:

VCL 상태 [combined | static | nas | all]

매개 변수 :

결합 된 | static | nas | all : VCL 사용자

VCL 프로토콜 기반 VLAN 이더넷 II 추가

설명 :

VCL 프로토콜 기반 VLAN 이더넷 -II 프로토콜을 그룹 매핑에 추가합니다.

통사:

VCL ProtoVlan 프로토콜 Eth2 <ether_type> | arp | ip | ipx |를 <group_id>에 추가하십시오.

매개 변수 :

<ether_type> | arp | ip | ipx | at : Ether 유형 (0x0600 - 0xFFFF)

<group_id> : 프로토콜 그룹 ID

VCL 프로토콜 기반 VLAN SNAP 추가

설명 :

VCL 프로토콜 기반 VLAN SNAP 프로토콜을 그룹 매핑에 추가합니다.

통사:

VCL ProtoVlan 프로토콜 스냅 추가 <oui> | rfc_1042 | snap_8021h <pid> <group_id>

매개 변수 :

<oui> | rfc_1042 | snap_8021h : OUI 값 (16 진수 00-00-00 에서 FF-FF-FF).

<pid> : PID 값 (0x0-0xFFFF). OUI 가 00-00-00 이면 유효한 PID 범위는 0x0600-0xFFFF 입니다.

<group_id> : 프로토콜 그룹 ID

VCL 프로토콜 기반 VLAN 추가 LLC

설명 :

그룹 매핑에 VCL 프로토콜 기반 VLAN LLC 프로토콜을 추가합니다.

통사:

VCL ProtoVlan 프로토콜 Llc 추가 <dsap> <ssap> <group_id>

매개 변수 :

<dsap> : DSAP 값 (0x00-0xFF)

<ssap> : SSAP 값 (0x00-0xFF)

<group_id> : 프로토콜 그룹 ID

VCL 프로토콜 기반 VLAN 삭제 이더넷 II

설명 :

VCL 프로토콜 기반 VLAN Ethernet-II 프로토콜을 그룹 매핑으로 삭제합니다.

통사:

VCL ProtoVlan 프로토콜 삭제 Eth2 <ether_type> | arp | ip | ipx | at

매개 변수 :

<ether_type> | arp | ip | ipx | at : Ether 유형 (0x0600 - 0xFFFF)

VCL 프로토콜 기반 VLAN 삭제 SNAP

설명 :

VCL 프로토콜 기반 VLAN SNAP 프로토콜을 그룹 매핑으로 삭제합니다.

통사:

VCL ProtoVlan 프로토콜 삭제 스냅 <oui> | rfc_1042 | snap_8021h <pid>

매개 변수 :

<oui> | rfc_1042 | snap_8021h : OUI 값 (16 진수 00-00-00 에서 FF-FF-FF).

<pid> : PID 값 (0x0-0xFFFF). OUI 가 00-00-00 이면 유효한 PID 범위는 0x0600-0xFFFF 입니다.

VCL 프로토콜 기반 VLAN 삭제 LLC

설명 :

VCL 프로토콜 기반 VLAN LLC 프로토콜을 그룹 매핑으로 삭제합니다.

통사:

VCL ProtoVlan 프로토콜 삭제 Llc <dsap> <ssap>

매개 변수 :

<dsap> : DSAP 값 (0x00-0xFF)

<ssap> : SSAP 값 (0x00-0xFF)

VCL 프로토콜 기반 VLAN 추가

설명 :

VCL 프로토콜 기반 VLAN 그룹을 VLAN 매핑에 추가합니다.

통사:

VCL ProtoVlan Vlan 추가 [<port_list>] <group_id> <vid>

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<group_id> : 프로토콜 그룹 ID

<vid> : VLAN ID (1-4095)

VCL 프로토콜 기반 VLAN 삭제

설명 :

VCL 프로토콜 기반 VLAN 그룹을 VLAN 매핑으로 삭제합니다.

통사:

VCL ProtoVlan VLAN 삭제 [<port_list>] <group_id>

매개 변수 :

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

<group_id> : 프로토콜 그룹 ID

VCL 프로토콜 기반 VLAN 구성

설명 :

VCL 프로토콜 기반 VLAN 항목을 표시합니다.

통사:

VCL ProtoVlan Conf

VCL IP 기반 VLAN 구성

설명 :

VCL IP 서브넷 기반 VLAN 구성을 표시합니다.

통사:

VCL IPVlan 구성 [<vce_id>]

매개 변수 :

<vce_id> : 각 VCL 항목에 대한 고유 한 VCE ID

VCL IP 기반 VLAN 추가

설명 :

VCL IP 서브넷 기반 VLAN 항목을 추가 또는 수정하십시오.

통사:

VCL IPVlan [<vce_id>] <ip_addr_mask> <vid> [<port_list>] 추가

매개 변수 :

<vce_id> : 각 VCL 항목에 대한 고유 한 VCE ID

<ip_addr_mask> : 소스 IP 주소 및 마스크 (형식 : a.b.c.d / n).

<vid> : VLAN ID (1-4095)

<port_list> : 포트 목록 또는 'all', 기본값 : 모든 포트

VCL IP 기반 VLAN 삭제

설명 :

VCL IP 서브넷 기반 VLAN 항목을 삭제하십시오.

통사:

VCL IPVlan <vce_id> 삭제

매개 변수 :

<vce_id> : 각 VCL 항목에 대한 고유 한 VCE ID

5.23 SMTP 명령

SMTP 구성
설명 :
SMTP config remark.

SMTP mode
설명 :
SMTP 구성을 활성화 또는 비활성화합니다.

Syntax:
SMTP 모드 [enable | disable]

매개 변수 :
enable : SMTP 모드 사용
disable : SMTP 모드 사용 안 함
(기본값 : SMTP 모드 표시)

SMTP 서버
설명 :
SMTP 서버 구성을 설정 또는 표시하십시오.

Syntax:
SMTP 서버 [<server>] [<port>]

매개 변수 :
<server> : SMTP 서버 주소
<포트> : SMTP 서버 포트

SMTP 인증
설명 :
SMTP 인증 구성을 사용 또는 사용하지 않도록 설정합니다.

Syntax:
SMTP 인증 [사용 | 사용 안 함]

매개 변수 :
enable : SMTP 인증 사용
disable : SMTP 인증 사용 안 함
(기본값 : SMTP 인증 표시)

SMTP Auth_user
설명 :
SMTP 인증 사용자 이름 구성을 설정하거나 표시합니다.

Syntax:
SMTP Auth_user [<auth_user_text>]

매개 변수 :
<auth_user_text> : SMTP 인증 사용자 이름

SMTP Auth_pass
설명 :
SMTP 인증 암호 구성을 설정 또는 표시합니다.

Syntax:
SMTP Auth_pass [<auth_pass_text>]

매개 변수 :
<auth_pass_text> : SMTP 인증 암호

SMTP mailfrom
설명 :
SMTP 전자 메일을 구성에서 설정 또는 표시합니다.

Syntax:

SMTP Mailfrom [<mailfrom_text>]

매개 변수 :

<mailfrom_text> : 주소에서 보낸 SMTP 전자 메일

SMTP Mailsubject

설명 :

SMTP 전자 메일 주체 구성을 설정하거나 표시합니다.

Syntax:

SMTP Mailsubject [<mailsubject_text>]

매개 변수 :

<mailsubject_text> : SMTP 전자 메일 제목

SMTP Mailto1

설명 :

구성 할 SMTP 전자 메일 1 을 설정하거나 표시하십시오.

Syntax:

SMTP Mailto1 [<mailto1_text>]

매개 변수 :

<mailto1_text> : SMTP 전자 메일 주소 1

SMTP Mailto2

설명 :

구성 할 SMTP 전자 메일 2 를 설정하거나 표시하십시오.

Syntax:

SMTP Mailto2 [<mailto2_text>]

매개 변수 :

<mailto1_text> : SMTP 전자 메일 주소 2

6. SWITCH OPERATION

6.1 Address Table

스위치는 주소 테이블로 구현됩니다. 이 주소 테이블은 많은 항목으로 구성됩니다. 각 항목은 MAC 주소, 포트 번호 등을 포함하여 네트워크의 일부 노드의 주소 정보를 저장하는 데 사용됩니다.이 정보는 이더넷 스위치의 학습 과정에서 비롯됩니다..

6.2 Learning

어느 포트에서든 하나의 패킷이 들어 오면 스위치는 소스 주소 인 포트 번호를 기록합니다. 그리고 주소 테이블에있는 다른 관련 정보. 이 정보는 향후 패킷에 대한 전달 또는 필터링을 결정하는 데 사용됩니다.

6.3 Forwarding & Filtering

하나의 패킷이 이더넷 스위칭의 일부 포트에서 오는 경우 소스 주소 학습 외에도 목적지 주소도 확인합니다. 이더넷 스위칭은 대상 주소에 대한 주소 표를 조회합니다. 이 패킷이 없으면이 패킷은 패킷이 들어오는 포트를 제외한 다른 모든 포트로 전달됩니다.이 포트는이 패킷을 연결된 네트워크로 전송합니다. 발견되면 목적지 주소가이 패킷과 다른 포트에 위치하게되면 이더넷 스위치는이 패킷을 주소 테이블의 정보에 따라이 목적지 주소가있는 포트로 전달합니다. 그러나 목적지 주소가이 패킷과 같은 포트에 있으면이 패킷이 필터링됩니다. 따라서 네트워크 처리량과 가용성이 향상됩니다.

6.4 Store-and-Forward

Store-and-Forward 는 패킷 포워딩 기술의 한 유형입니다. 저장 - 전달 이더넷 스위칭은 들어오는 프레임을 내부 버퍼에 저장하고 전송 전에 완전한 오류 검사를 수행합니다. 따라서 오류 패킷이 발생하지 않아 네트워크가 효율성과 안정성을 필요로 할 때 최상의 선택입니다.
이더넷 스위치는 패킷 헤더에서 대상 주소를 검색하고, 필요한 경우에만 들어오는 포트에 대해 라우팅 테이블을 검색하고 패킷을 전달합니다. 고속 포워딩은 스위치를 서버를 네트워크에 직접 연결하여 처리량과 가용성을 향상시키는 데 유용합니다. 그러나 스위치는 존재하는 허브를 분류하는 데 가장 일반적으로 사용되며 거의 항상 전체 성능을 향상시킵니다. 모든 이더넷 네트워크 환경에서 이더넷 스위칭을 쉽게 구성하여 기존 케이블 및 어댑터를 사용하여 대역폭을 크게 높일 수 있습니다.
이더넷 스위칭의 학습 기능으로 인해, 각 수신 및 송신 패킷의 소스 주소 및 해당 포트 번호는 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.
스위치는 "저장 및 전달"을 수행하므로 오류 패킷이 발생하지 않습니다. 보다 신뢰성있게, 재전송 속도를 감소시킨다. 패킷 손실은 발생하지 않습니다.

6.5 자동 협상

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 모드와 속도를 감지하여 수행됩니다. 10Base-T 및 100Base-TX 장치 모두 Half 또는 Full-Duplex 모드로 포트에 연결할 수 있습니다.

If attached device is:	100Base-TX port will set to:
10Mbps, no auto-negotiation	10Mbps.
10Mbps, with auto-negotiation	10/20Mbps (10Base-T/Full-Duplex)
100Mbps, no auto-negotiation	100Mbps
100Mbps, with auto-negotiation	100/200Mbps (100Base-TX/Full-Duplex)

7. 문제 해결

이 장에는 문제점 해결에 도움이되는 정보가 들어 있습니다. 이더넷 스위치가 올바르게 작동하지 않는 경우이 설명서의 지침에 따라 이더넷 스위치가 설정되었는지 확인하십시오.

■ 링크 LED 가 켜지지 않음

해결책:

케이블 연결을 확인하고 이더넷 스위치의 이중 모드를 제거하십시오.

■ 일부 스테이션은 다른 포트에있는 다른 스테이션과 통신 할 수 없습니다

해결책:

VLAN 설정, 트렁크 설정 또는 포트 활성화 / 비활성화 상태를 확인하십시오.

■ 성능이 좋지 않습니다.

해결책:

이더넷 스위치의 전이중 상태를 확인하십시오. 이더넷 스위치가 전이중으로 설정되고 파트너가 반이중으로 설정된 경우 성능이 떨어집니다. port 의 입 / 퇴장율도 확인하십시오.

■ 스위치가 네트워크에 연결되지 않는 이유

해결책:

1. 스위치의 LNK / ACT LED 를 확인하십시오
2. 스위치에서 다른 포트를 사용해보십시오.
3. 케이블이 올바르게 설치되었는지 확인하십시오.
4. 케이블이 올바른 유형인지 확인하십시오
5. 전원을 끄십시오. 잠시 후 전원을 다시 켜십시오.

■ 100Base-TX 포트 링크 LED 가 켜져 있지만 트래픽이 불규칙합니다.

해결책:

연결된 장치가 전이중을 수행하도록 설정되어 있지 않은지 확인하십시오. 일부 장치는 물리적 또는 소프트웨어 스위치를 사용하여 이중 모드를 변경합니다. 자동 협상은이 유형의 전이중 설정을 인식하지 못할 수 있습니다.

■ 스위치가 켜지지 않을 경우

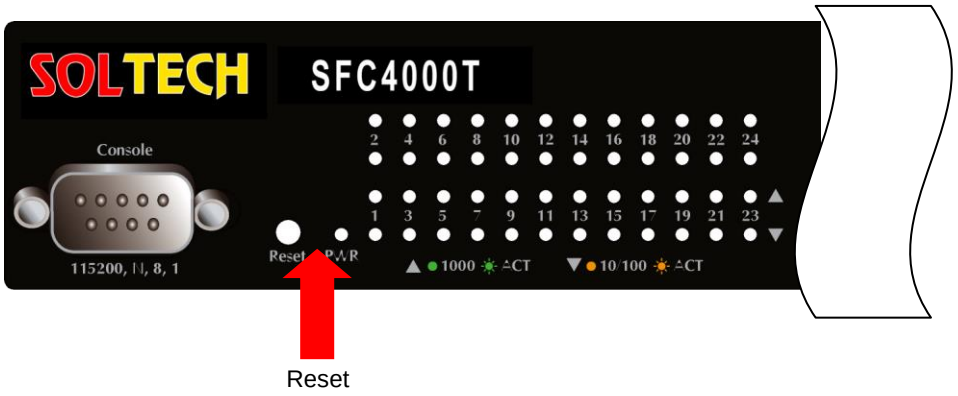
해결책:

1. AC 전원 코드가 삽입되지 않았거나 결함이 있습니다.
2. AC 전원 코드가 올바르게 꽂혀 있는지 확인하십시오

3. 전원 코드 교체 코드가 올바르게 삽입 된 경우 스위치 대신 다른 장치를 연결하여 AC 전원이 작동하는지 확인하십시오.
4. 해당 장치가 작동하면 다음 단계를 참조하십시오.
5. 장치가 작동하지 않으면 AC 전원을 확인하십시오

■ **IP 주소를 변경하거나 관리자 암호를 잊어 버린 경우–**

IP 주소를 기본 IP 주소 "192.168.0.100"으로 재설정하거나 암호를 기본값으로 재설정하십시오. 전면 패널에서 하드웨어 재설정 버튼을 약 10 초 동안 누릅니다. 장치가 재부팅 된 후 192.168.0.xx 의 동일한 서브넷에서 관리 웹 인터페이스에 로그인 할 수 있습니다.



부록 A

A.1 스위치의 RJ-45 지정 핀

1000Mbps, 1000Base T

Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

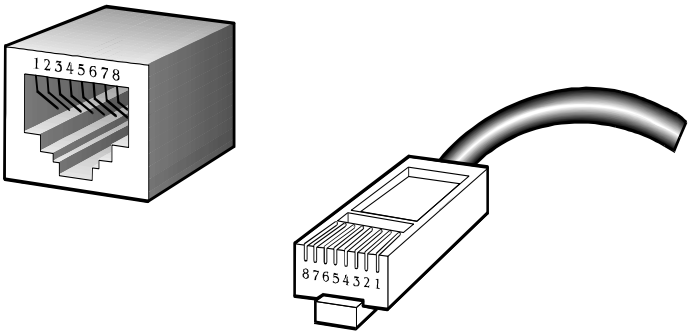
트위스트 페어 케이블 또는 와이어 링 패널 내에서 명시 적으로 금지되지 않은 크로스 오버 기능의 암시 적 구현은이 표준의 범위를 벗어납니다.

A.2 10/100Mbps, 10/100Base-TX

10 / 100Mbps 이더넷 스위치를 다른 스위치, 브리지 또는 허브에 연결할 때는 직선 또는 크로스 오버 케이블이 필요합니다. 스위치의 각 포트는 자동 MDI / MDI-X 감지를 지원합니다. 즉, 크로스 오버 케이블을 만들지 않고도 스위치를 모든 이더넷 장치에 직접 연결할 수 있습니다. 다음 표와 도표는 표준 RJ-45 콘센트 / 커넥터와 해당 핀 지정을 보여줍니다.

RJ-45 커넥터 할당 핀		
내용	MDI Media Dependant Interface	MDI-X Media Dependant Interface-Cross
1	Tx + 전송	Rx + 수신
2	Tx - 전송	Rx - 수신
3	Rx + 수신	Tx + 전송
4, 5	사용하지 않음	
6	Rx - 수신	Tx - 전송
7, 8	사용하지 않음	

표준케이블, RJ-45 허용 핀



표준 RJ-45 콘센트 / 커넥터

표준 UTP / STP 케이블에는 8 개의 전선이 있으며 각 전선은 색상으로 구분되어 있습니다. 다음은 직선 케이블과 크로스 오버 케이블 연결의 핀 할당과 색상을 보여줍니다.

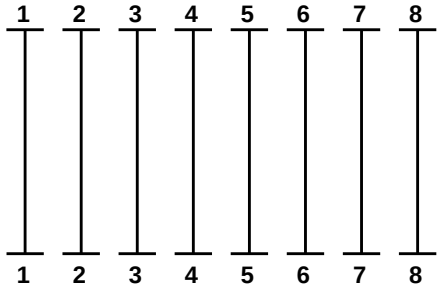
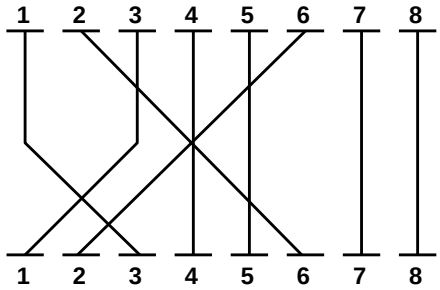
Straight Cable		SIDE 1	SIDE2
	SIDE 1	1 = White / Orange	1 = White / Orange
		2 = Orange	2 = Orange
		3 = White / Green	3 = White / Green
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Green
		7 = White / Brown	7 = White / Brown
	SIDE 2	8 = Brown	8 = Brown
Crossover Cable		**SIDE 1**	**SIDE2**
	SIDE 1	1 = White / Orange	1 = White / Green
		2 = Orange	2 = Green
		3 = White / Green	3 = White / Orange
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Orange
		7 = White / Brown	7 = White / Brown
	SIDE 2	8 = Brown	8 = Brown

그림 A-1: 직선 및 교차 케이블

네트워크에 설치하기 전에 연결된 케이블이 위의 그림과 동일한 핀 할당 및 색상을 가지는지 확인하십시오..

부록 B : 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 정보나 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

IP 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 시스템인 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.

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 t.

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 교환할 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 것이었습니다.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.

UDP 는 인터넷 프로토콜 (IP)을 사용하는 TCP (전송 제어 프로토콜) 대신 사용할 수 있습니다. TCP 와 달리 UDP 는 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 비인식 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 발견된 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 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 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.

WRES

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.