U-F9028UZ 사용자

웹 운용 설명서

목차

1. 소개

1.1 제품 소개

U-F9028UZ 는 8 개의 × 10/100/1000Mbps RJ-45 콤보포트와 4 개의 SFP+포트, 24 개의 SFP 포트를 갖춘 고성능 레이어 2 관리형 기가비트 스위치입니다. IP 카메라, 무선 액세스 포인트 및 기타 원격 네트워크 장치와 통신에 적합합니다. 광섬유 업링크의 추가는 유연한 네트워크 확장과 안정적인 백본 연결을 보장합니다.

스위치는 802.1Q VLAN, QinQ, STP/RSTP/MSTP, 링크 집계, IGMP/MLD 스누핑, 고급 트래픽 제어 정책 등 풍부한 레이어 2 기능을 지원합니다. DHCP 스누핑, 포트 보안, ARP 검사, ACL, 폭풍 제어와 같은 통합 네트워크 보안 기능은 무단 접근, ARP 공격, 방송 플러딩으로부터 네트워크를 보호하며, QoS 는 음성 및 영상 등 주요 서비스의 안정성과 성능을 향상시킵니다.

U-F9028UZ 는 웹 GUI, 텔넷, CLI, SNMP v1/v2/v3 을 통한 유연한 관리를 제공하며, 포트 미러링, 시스템 로그, 케이블 진단을 통한 효율적인 유지보수를 지원합니다. 팬리스 금속 인클로저, 장수명 부품, -10°C 에서 45°C 까지의 작동 온도 능력으로 설계되어 기업 사무실, 지능형 건물, 보안 감시 네트워크에서의 높은 신뢰성을 보장합니다.

1.2 특징

- 지원 IEEE802.3, IEEE802.3u, IEEE802.3ab, IEEE802.3z
- 4 개의 × 10/100/1000Base-T(X) 콤보포트 + 4 개의 SFP+포트 + 24 개의 SFP 포트
- 지원 VLAN, IEEE802.1Q, QinQ
- 멀티캐스트 최적화를 위한 IGMP 스누핑 / MLD 스누핑 지원
- 무단 DHCP 서버를 방지하기 위해 DHCP 스누핑을 지원하세요
- IPv4 정적 라우팅 지원
- SNMP v1/v2/v3, 웹 기반 GUI, 텔넷, CLI 관리 지원
- 온라인 디버깅 및 트래픽 분석을 위한 포트 미러링 지원
- 루프 탐지 및 루프 보호, 폭풍 제어
- 서비스 우선순위 보장을 위한 지원 QoS
- 네트워크 보안을 강화하기 위한 ACL 지원
- 링크 견고성을 향상시키기 위한 LACP 링크 집계 지원
- 정확한 네트워크 시간 동기화를 위해 NTP 지원
- 포트 보안 및 MAC 바인딩 지원

- 작동 온도: -10°C ~ 45°C
- 보관 온도: -40°C ~ 70°C
- 팬리스 무소음 설계, 벽걸이 및 데스크탑 설치 지원
- FCC / CE 안전 및 EMC 기준을 준수합니다

1.3 요약

U-F9028UZ 관리형 이더넷 스위치를 선택해 주셔서 감사합니다. 이 시리즈 스위치는 HTML 기반 내장 웹 관리 인터페이스를 갖추고 있습니다. 사용자는 브라우저를 통해 장치의 다양한 소프트웨어 기능을 구성, 관리 및 모니터링할 수 있습니다.

스위치와 같은 네트워크에 속한 컴퓨터에서는 표준 웹 브라우저(예: 크롬, 엣지, 파이어폭스 등)를 사용해 스위치의 관리 IP 주소를 주소 표시줄에 입력하세요. 추가 관리 소프트웨어를 설치하지 않고도 기기의 웹 관리 페이지에 원격으로 접속할 수 있습니다.

1.4 로그인

PC 에서 설치된 웹 브라우저를 열고 스위치의 관리 IP 주소를 입력하세요.
참고: 스위치의 기본 관리 IP 주소는 192.168.2.1 입니다. 브라우저 주소창에 http://192.168.2.1 입력해 주세요.
본 제품의 웹 인터페이스는 보안이 강화된 HTTPS 를 기본으로 사용합니다.

따라서, 처음 접속시 위와 같이 경고 메시지가 발생할 수도 있습니다. 고급 버튼을 클릭하고 해당 IP 의 안전한지 않음으로 이동을 클릭해 주어야 정상적인 웹 접속이 이루어질 수 있습니다.
또한, 브라우저마다 표시하는 내용이 조금씩 다를 수 있으며, 위 그림의 예는 크롬 브라우저를 사용하여 접속할 때의 표시 내용입니다.

로그인 페이지가 나타나면 기본 사용자 이름과 비밀번호를 입력한 후 "로그인"을 클릭해 주세요.

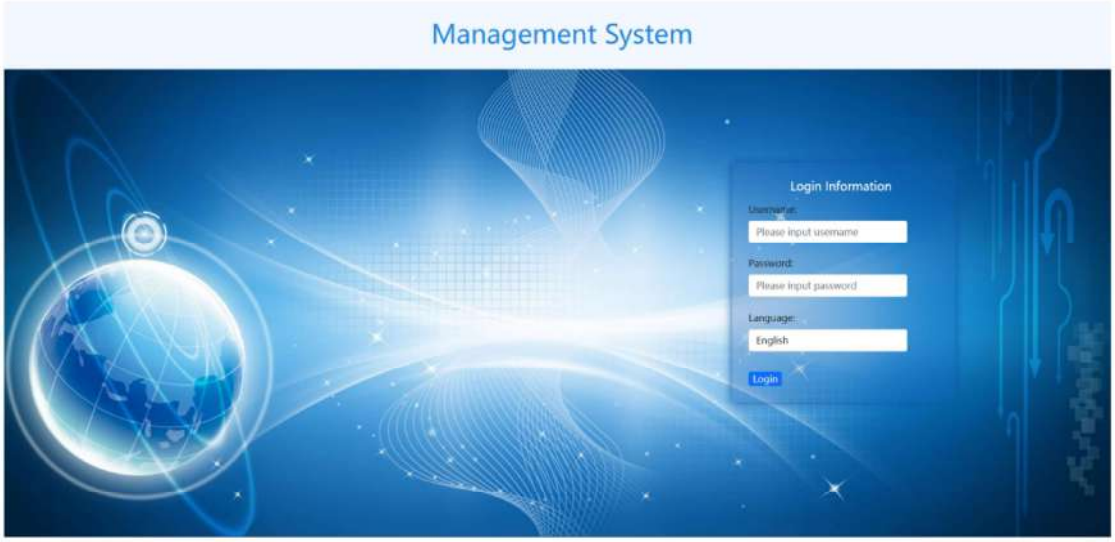

그림 1-4-1 로그인 창

로그인 ID:admin

로그인 비밀번호:system

첫 번째 로그인 시 비밀번호를 변경해야 합니다.

그림 1-4-2 웹페이지 홈 화면

1.5 웹 사용자 인터페이스

사용자 이름과 비밀번호를 입력하면 그림 1-3 에 나타난 메인 화면이 나타납니다.

그림 1-5 웹페이지 홈 화면

주요 인터페이스는 세 가지 기능 영역으로 구성됩니다:

지역	묘사
탑 바	모니터 / 설정/유지, **내비게이션 카테고리, 언어 선택, 저장, 로그아웃 버튼** 포함
왼쪽 메뉴 패널	다양한 구성 및 모니터링 모듈에 접근할 수 있는 기능 내비게이션 메뉴
메인 디스플레이 패널	현재 선택된 함수의 상세 정보와 매개변수 구성을 보여줍니다

이 페이지에는 장치 설명, 하드웨어 버전, 소프트웨어 버전, MAC 주소 등의 정보가 표시됩니다.

1.6 구성

Path:

시스템 관리 → 구성

그림 1-6 웹페이지 홈 화면

구성 그룹	기능 설명
시스템 관리	시스템 정보, 호스트 이름, 위치, 연락처 및 기본 시스템 관리
사용자 관리	로그인 비밀번호 변경, 사용자 접근 수준, 인증 방법
포트 관리	포트 링크 모드, 속도/이중, 흐름 제어, 폭풍 제어, 포트 보안, 포트 통계
기본 복무	VLAN, QoS, 멀티캐스트(IGMP 스누핑), DHCP 스누핑, LLDP
Advanced Service	802.1X 인증, MAC 필터링, ACL 규칙, QinQ, 보안 제어

이 섹션에서는 웹 인터페이스를 통해 스위치 설정을 설정하는 방법을 설명합니다. 상단 내비게이션 바에서 설정 메뉴를 선택하여 그림 1-4 에 표시된 대로 설정 페이지로 들어가세요.

1.7 항구 정보

1.7.1 기본 정보

Path:

기본 정보 →→ 포트 정보 모니터링

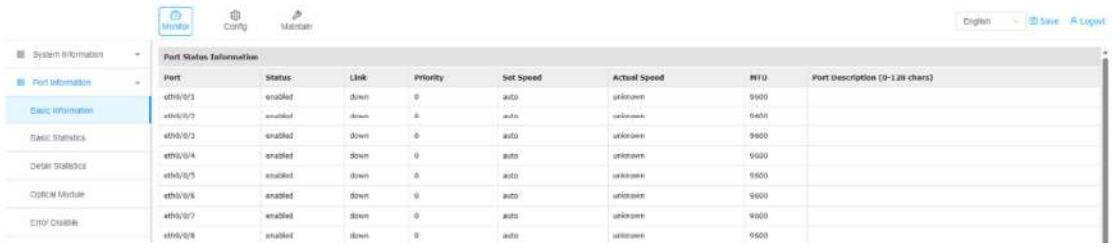

그림 1-7-1 기본 정보

이 페이지는 포트 상태, 우선순위, 속도, MTU, 설명 및 기타 정보를 표시합니다.

1.7.2 기본 통계

Path:

→ 포트 정보→ 기본 통계를 모니터링하세요

그림 1-7-2 기본 통계

이 페이지는 포트가 송수신하는 패킷에 관한 간단한 통계를 보여줍니다.

1.7.3 상세 통계

Path:

항→ 정보→ 세부 통계 모니터링

그림 1-7-3 상세 통계량

이 페이지는 포트에서 수신 및 송신 패킷에 대한 상세한 통계를 보여줍니다.

2. 시스템 설정

2.1 관리자 설정

참고: 기본 관리자 사용자 이름과 비밀번호는 admin / Admin@123 입니다.

초기 로그인 후에는 기본 비밀번호를 변경하는 것이 강력히 권장됩니다.

Path:

설정 → 사용자 관리 → 사용자 수정

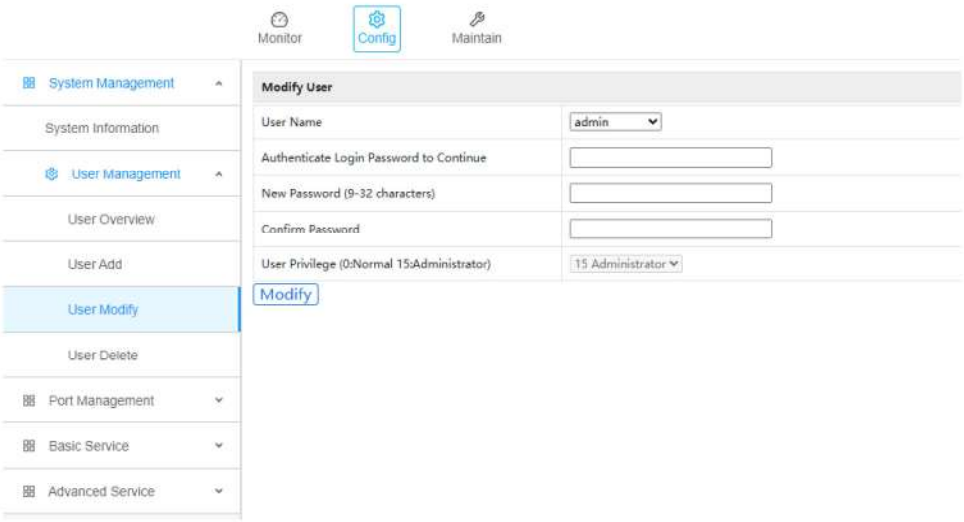

그림 2-1 관리자 페이지 수정

항목	묘사
사용자 이름	수정할 사용자 계정을 선택하세요 (기본적으로 관리자)
로그인 비밀번호를 인증하여 계속하세요	접근 권한을 확인하려면 현재 비밀번호를 입력하세요
새로운 비밀번호 (9–32 자)	선택한 계정의 새 비밀번호를 입력하세요
비밀번호 확인	인증을 위해 비밀번호를 다시 입력하세요
사용자 특권	계정 접근 수준 선택: 0 = 일반 사용자 15 = 관리자

변경 사항을 적용하려면 수정(Modify)을 클릭하세요:

비밀번호 규칙은 비밀번호 복잡성 정책을 준수해야 합니다.

보안 권고사항:

대문자/소문자, 숫자, 특수 문자가 포함된 강력한 비밀번호를 사용하세요

무단 접근을 방지하기 위해 주기적으로 비밀번호를 변경하세요

2.2 사용자 설정

2.2.1 사용자 개요

Path:

구성 → 시스템 관리 → 사용자 관리 → 사용자 개요

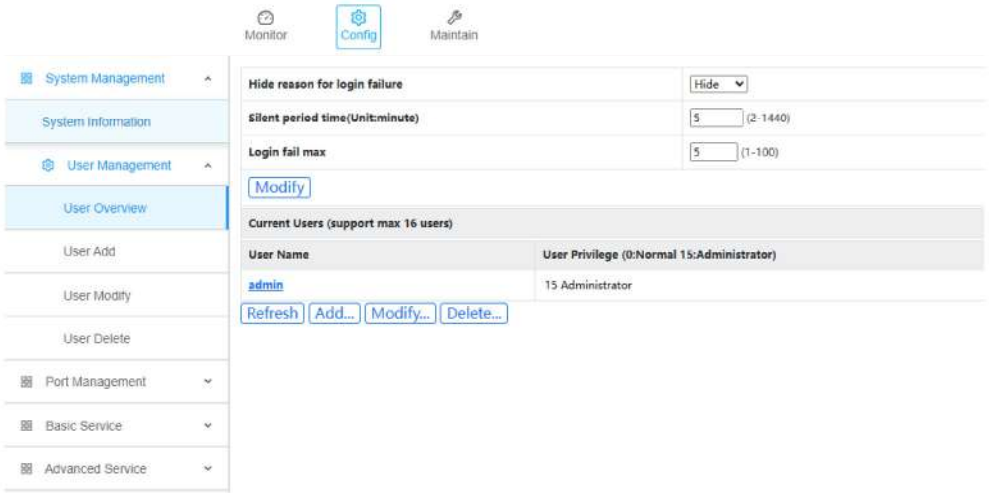

그림 2-2-1 사용자 개요 페이지

이 페이지는 기기의 모든 계정과 권한을 보여줍니다.

정보에는 다음이 포함됩니다:

항목	묘사
사용자 이름	장치에 설정된 사용자 계정 이름입니다
사용자 특권	사용자의 접근 수준:0 = 일반 사용자 15 = 관리자

추가적인 로그인 보호 설정도 구성할 수 있습니다:

설정	묘사
로그인 실패 원인 숨기기	로그인 실패 시 이유를 표시할지 선택하세요
무음 시간 (분)	여러 번 로그인 실패 후 강제로 무음 시간이 유지됩니다
로그인 실패 최대 횟수	최대 실패 횟수 허용

2.2.2 사용자 추가

Path:

구성 → 시스템 관리 → 사용자 관리 → 사용자 추가

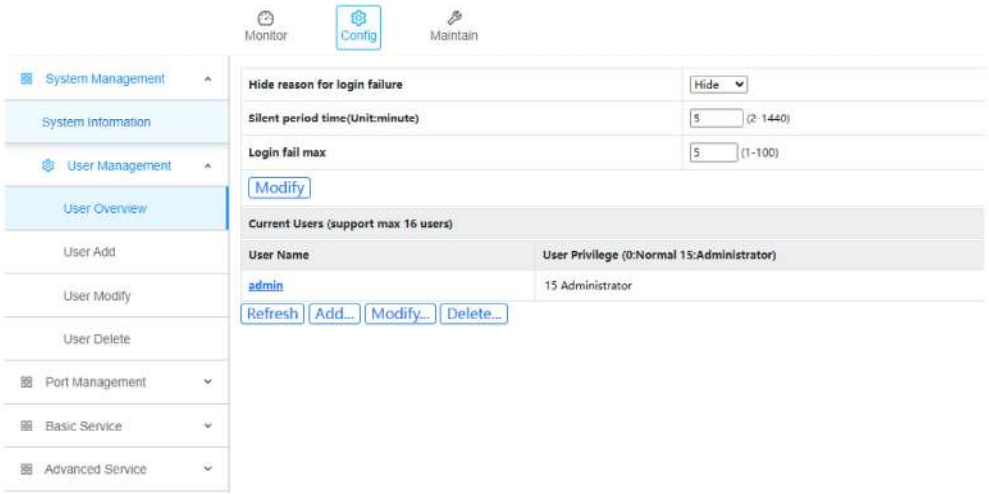

그림 2-2-2 사용자 추가 페이지

이 페이지는 사용자 계정과 비밀번호를 추가하는 데 사용됩니다.

2.2.3 사용자 수정

Path:

구성 → 시스템 관리 → 사용자 관리 → 사용자 수정

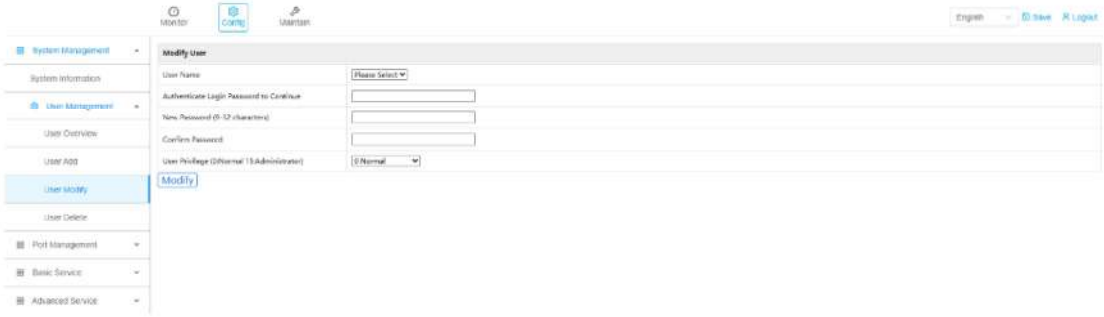

그림 2-2-3 사용자 수정 페이지

이 페이지는 사용자 비밀번호와 사용자 권한을 변경하는 데 사용됩니다. 관리자 계정 권한은 변경할 수 없습니다. 다른 사용자의 권한을 변경할 수 있는 권한은 오직 관리자 계정뿐입니다.

2.2.4 사용자 삭제

Path:

구성 → 시스템 관리 → 사용자 관리 → 사용자 삭제

그림 2-2-4 사용자 삭제 페이지

이 페이지는 사용자 계정을 삭제하는 데 사용됩니다. 이 작업은 관리자 사용자만 수행할 수 있습니다.

2.3 서비스 접근 시간 관리 설정

이 페이지는 관리자가 Telnet/SSH/HTTP/HTTPS 와 같은 관리 서비스를 활성화하거나 비활성화하고, 접근 포트를 설정하며, 세션 타임아웃 값을 설정할 수 있게 합니다.

Path:

Config → Advanced Service → Service Access Control

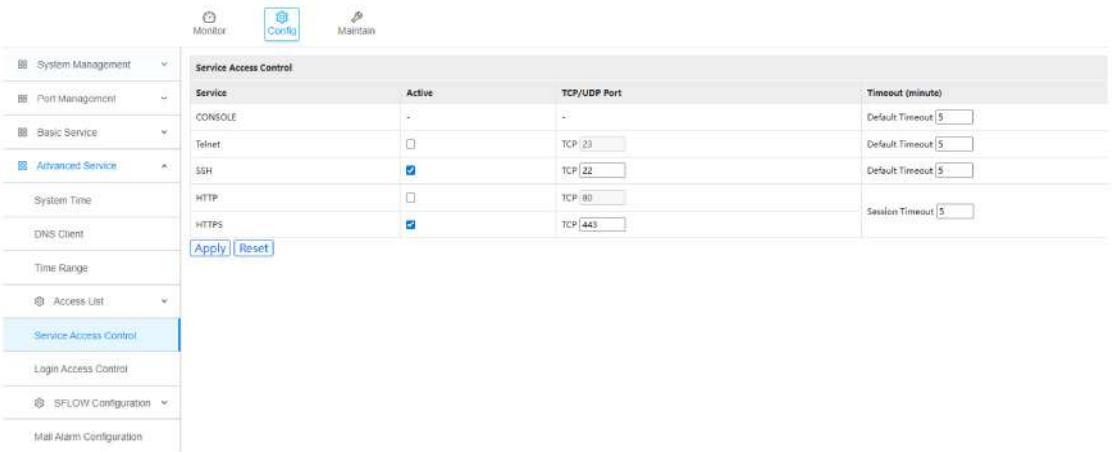

그림 2-3 서비스 접근 제어 페이지

매개변수 설명

항목	묘사
서비스	원하는 관리 프로토콜을 활성화하거나 비활성화할 것을 선택하세요
활동적인	서비스 활성화/비활성화
TCP/UDP 포트	원격 접속 통신에 사용되는 네트워크 포트

항목	묘사
타임아웃 (1 분)	선택한 서비스의 자동 로그아웃 타임아웃 현상은 유휴 상태입니다

이용 가능한 서비스

서비스	묘사
콘솔	로컬 콘솔 접근 (여기서 편집 불가)
텔넷	텔넷 원격 로그인 활성화 (보안이 취약한 프로토콜, 권장하지 않음)
SSH	암호화된 채널을 이용한 안전한 원격 로그인
HTTP	HTTP 프로토콜을 이용한 웹 접근
HTTPS	안전한 암호화된 웹 접근

추가 조치가 없으면 현재 연결된 사용자가 자동으로 로그아웃하는 시간을 설정할 수 있습니다. 콘솔, 텔넷, 웹 연결 등 각 세션마다 자동으로 로그아웃 시간을 지정할 수 있습니다. 기본 시간은 5 분입니다.

2.4 라우터 테이블 설정

2.4.1 정적 라우팅 테이블 설정

Path:

기본 서비스 →→ IP 및 경로 구성 → 정적 경로 구성

그림 2-4-1 정적 경로 구성 페이지

매개변수 설명

항목	묘사
목적지 IP	대상 네트워크 주소를 IPv4 형식으로 지정하세요
서브넷 마스크	목적지 네트워크의 네트워크 마스크를 정의합니다
넥스트홉	목적지 네트워크에 도달하는 데 사용되는 게이트웨이 IP 주소를 입력합니다

정적 경로는 특정 네트워크로 패킷을 전달하기 위한 고정 라우팅 경로를 정의하는 데 사용됩니다.

2.4.2 정적 경로 테이블 상태

이 페이지는 스위치에 현재 설정된 정적 라우팅 항목을 보여줍니다.

Path:

기본 서비스 → IP 및 경로 구성 →정적 경로 구성 → 기본 서비스

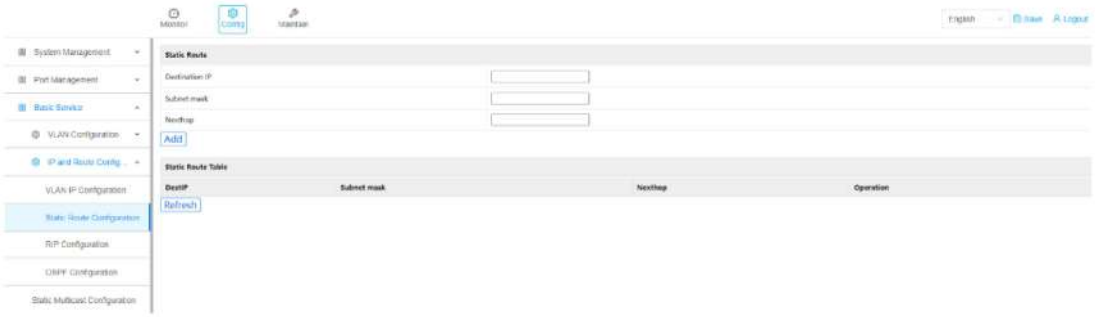

그림 2-4-2 정적 경로 테이블 상태 페이지

표시 정보

항목	묘사
DestIP	정적 경로의 목적지 네트워크 주소
서브넷 마스크	목적지 네트워크용 서브넷 마스크
넥스트홉	목적지에 도달하는 데 사용되는 게이트웨이 주소

현재 스위치에 연결된 장치의 라우팅 테이블 정보를 표시합니다.

2.4.3 ARP 테이블 현황

이 페이지는 스위치가 학습한 ARP 항목, IP 에서 MAC 으로의 주소 매핑 및 관련 포트/VLAN 을 보여줍니다.

Path:

ARP 테이블→ 서비스 정보 모니터링 →

그림 2-4-3 ARP 테이블 상태 페이지

현재 스위치의 ARP 테이블 정보를 표시합니다.

2.5 시스템 로그 설정 및 상태

이 페이지는 스위치가 생성한 시스템 로그 항목을 표시합니다. 로그에는 사용자 로그인 기록, 장치 운영 상태, 인터페이스 관련 알림이 포함됩니다.

Path:

Syslog 정보 → 모니터

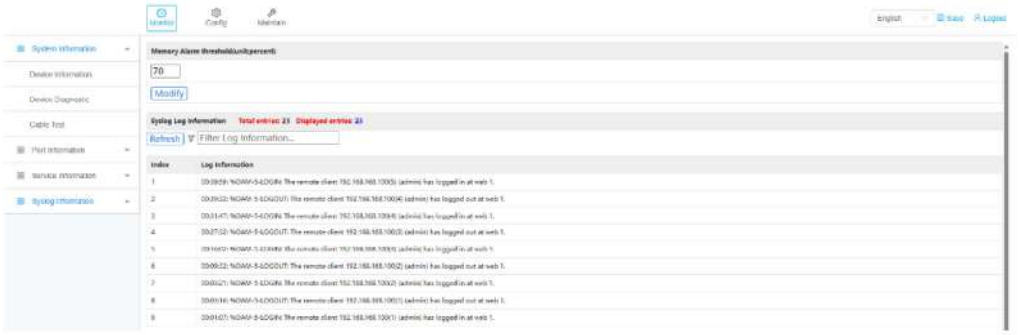

그림 2-5 시스템 로그 상태 페이지

메모리 알람 설정

설정	묘사
메모리 알람 임계치 (%)	메모리 알람 알림 트리거 임계값을 설정하세요

스위치가 생성한 모든 메시지를 지정된 수준에 따라 필터링하여 발생 순서대로 볼 수 있습니다.

2.6 환경 설정

2.6.1 펌웨어 업그레이드

Path:

소프트웨어 업그레이드 → 유지하세요 → 호스트 파일을 선택하세요

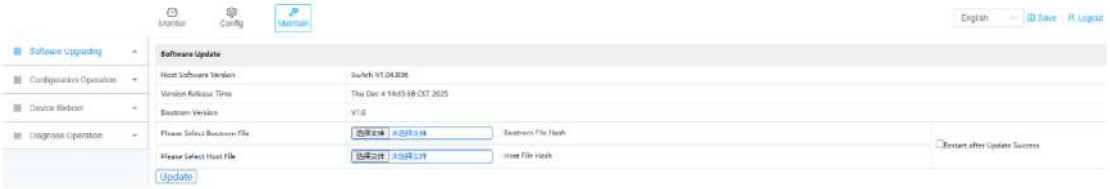

그림 2-6-1 펌웨어 업그레이드 페이지

이 기능을 통해 사용자는 로컬 컴퓨터에 저장된 펌웨어 버전을 불러와 스위치에 적용할 수 있습니다. 스위치 버전을 업데이트할 수 있습니다.

2.6.2 저장 구성 파일 및 업데이트 구성 파일

이 기능을 통해 시스템의 현재 설정 파일을 가져오고 내보낼 수 있습니다.

Path:

구성 → 유지→ 구성 저장

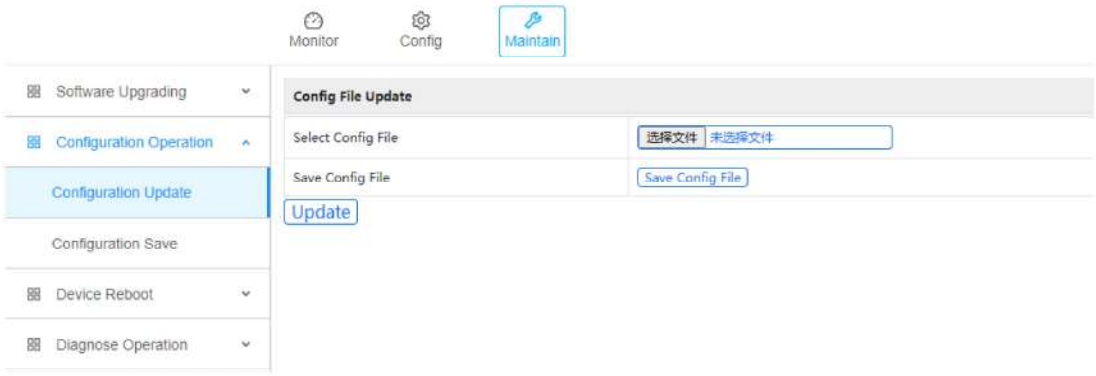

그림 2-6-2-1 현재 구성 파일 내보내기 페이지

스위치에 적용된 현재 환경 설정을 로컬 PC 에 저장할 수 있습니다.

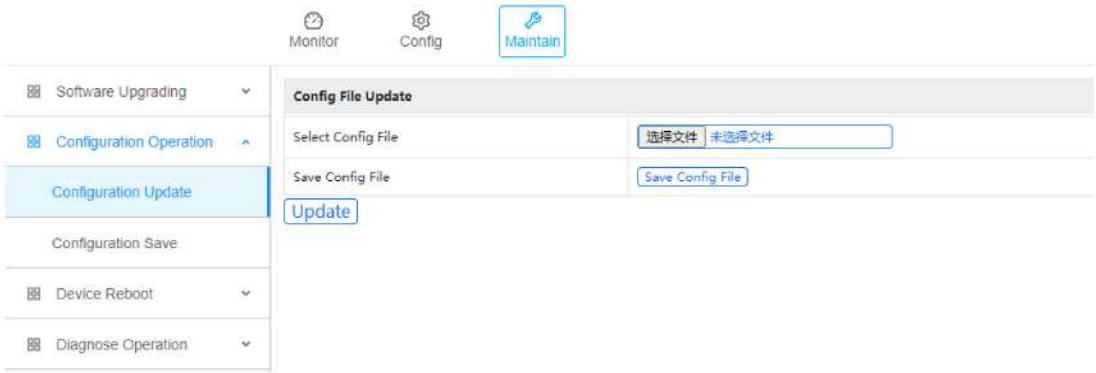

그림 2-6-2-2 현재 설정 파일 페이지 포팅

스위치에 적용된 현재 환경 설정을 로컬 PC 에 저장된 것으로 업데이트할 수 있습니다.

2.6.3 공장 데이터 초기화

Path:

장치 재부팅→ → 구성 작업을 유지하세요

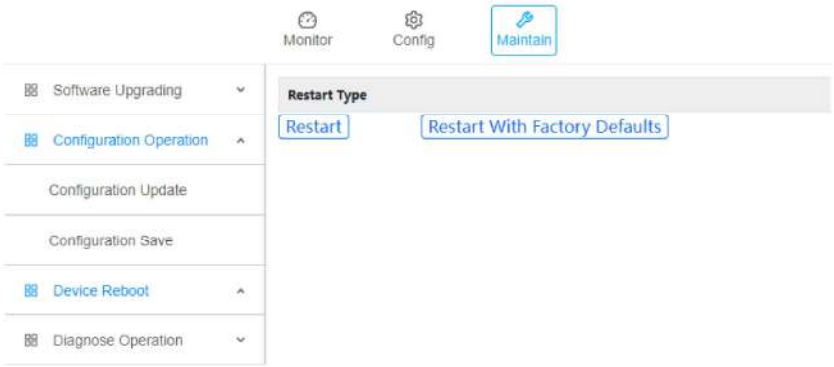

그림 2-6-3 공장 기본 복원 페이지

이 기능은 스위치를 원래 공장 기본 설정으로 복원하고 자동으로 장치를 재부팅합니다.

2.7 타임셋

2.7.1 수동 시간 설정

Path:

Config > Advanced Service > System Time

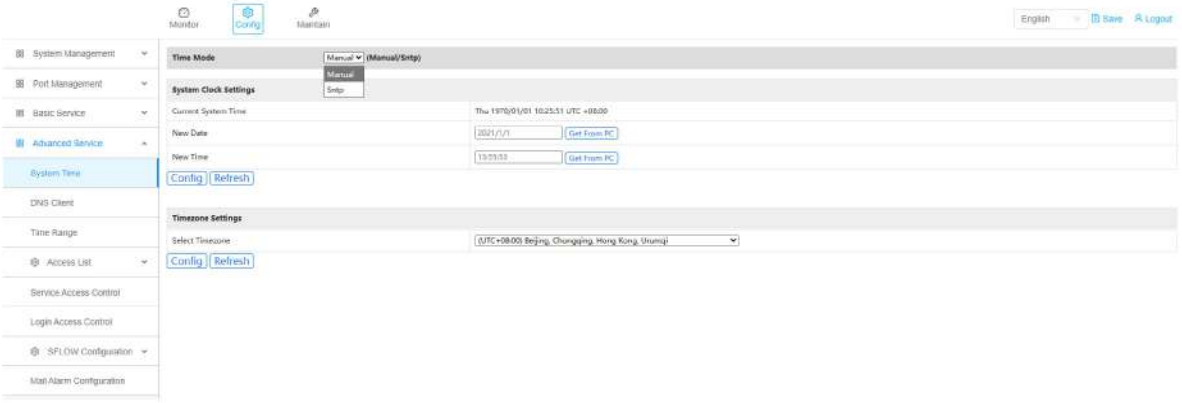

그림 2-7-1 수동 시간 설정 페이지

항목	묘사
현재 시스템 시간	실시간 시스템 시계를 표시합니다.
새로운 날짜	시스템 캘린더 날짜를 수동으로 설정하세요.
뉴 타임	시스템 클럭 시간을 수동으로 설정하세요.
PC 에서 벗어나세요	빠른 동기화를 위해 현재 로컬 PC 시간을 가져오는 기능입니다.
구성	새로운 구성을 시스템에 적용합니다.
리프레쉬	표시되는 시스템 시간이 새로고침됩니다.
시간대 설정	설치된 지역에 맞는 시간대를 선택하세요.

수동 모드에서는 관리자가 시스템의 날짜와 시간을 직접 설정하거나 로컬 PC 에서 동기화할 수 있습니다.

2.7.2 SNTP 시간 설정

Path:

Config > Advanced Service > System Time

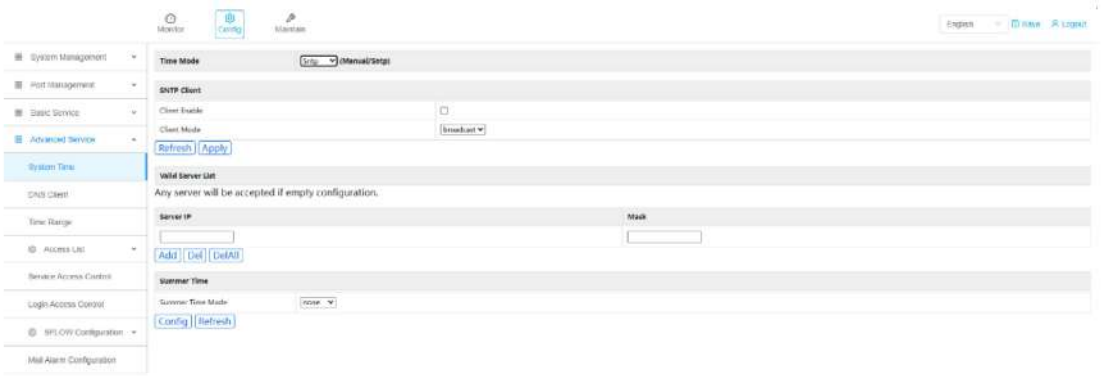

그림 2-7-2 SNTP 시간 설정 페이지

항목	묘사
SNTP 클라이언트	SNTP 시간 동기화 사용을 가능하게 합니다.
클라이언트 모드	통신 모드(Broadcast / Unicast)를 선택하세요.
서버 IP	SNTP 서버 IP 주소를 지정합니다. 여러 서버를 추가할 수도 있습니다.
마스크	필요 시 SNTP 서버 도달성을 위해 네트워크 마스크를 구성합니다.
Add / Del / DelAll	SNTP 서버 리스트 항목을 관리하세요.
서머타임 (일광절약시간제)	적용 시 자동 DST 조정이 활성화됩니다.
지원 / 새로고침	구성 저장이나 디스플레이 상태를 새로고침합니다.

SNTP 모드는 스위치가 네트워크 시간 서버와 시간을 자동으로 동기화할 수 있게 합니다.

2.8 현재 환경 상태 확인

Path:

시스템 정보> 장치 정보 > 모니터링하세요

그림 2-8 현재 환경 상태 페이지

장치 상태 페이지는 현재 시스템 실행 중인 정보의 요약을 보여줍니다.

2.9 스위치 재시작

Path:

기기 재부팅 유지 >

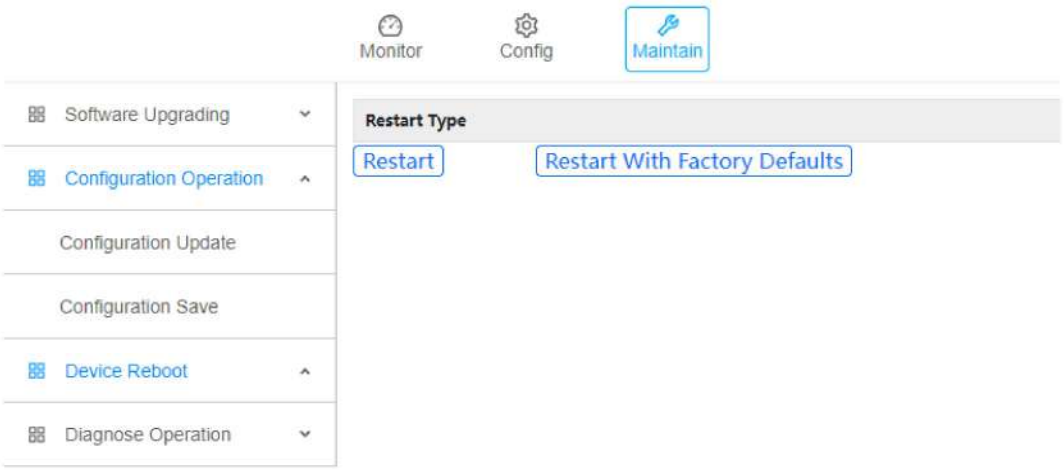

그림 2-9 스위치 페이지 재시작

공장 기본 복원 기능은 관리자가 모든 구성 설정을 공장 설정 상태로 초기화할 수 있게 해줍니다. 작업이 실행되면 장치는 자동으로 재부팅하고 기본 구성을 불러옵니다.

3. 포트 관리

3.1 기본 구성

Path:

구성 > 포트 관리 > 기본 구성

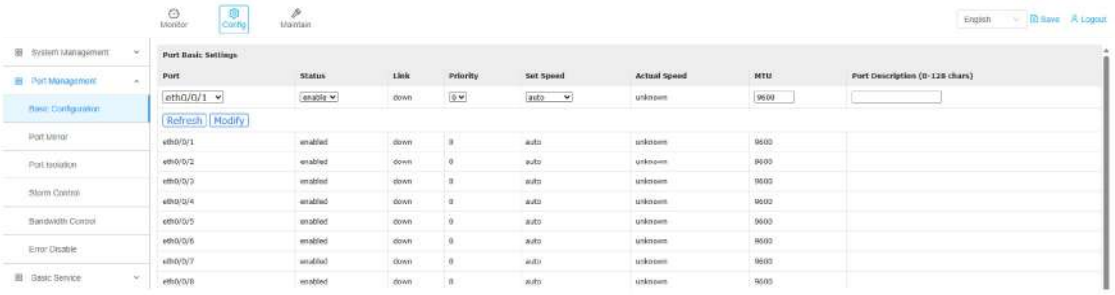

그림 3-1 기본 구성 페이지

이 페이지는 스위치 포트 상태, 우선순위, 속도, MTU, 포트 설명 정보를 구성합니다.

3.2 포트 미러

Path:

포트 미러> 포트 관리 > 구성

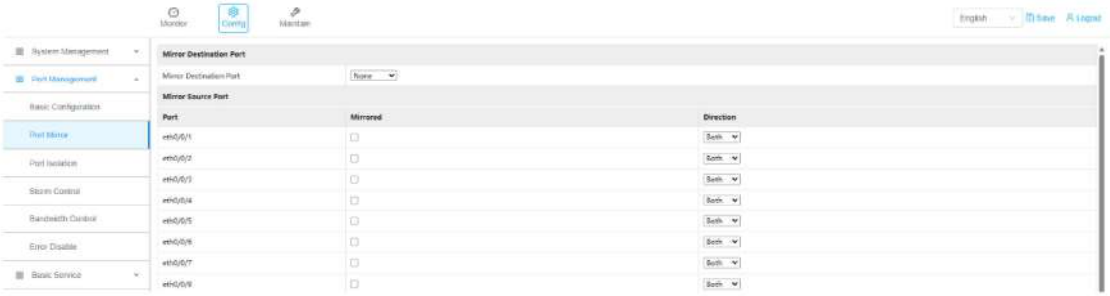

그림 3-2 포트 미러 페이지

이 페이지는 스위치 포트 상태, 우선순위, 속도, MTU, 포트 설명 정보를 구성합니다.

3.3 항구 격리

Path:

포트 격리> 포트 관리 > 구성

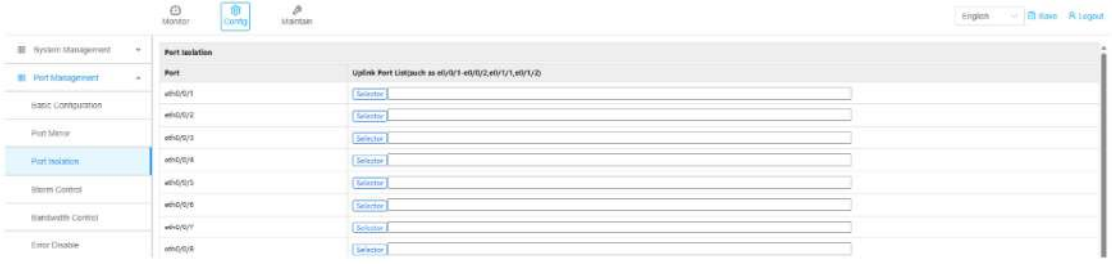

그림 3-3 포트 격리 페이지

이 페이지는 포트 격리 함수를 구성합니다. 격리 그룹의 포트들은 서로 격리되어 있으며, 업링크 포트와만 통신할 수 있고 다른 포트와는 통신할 수 없습니다.

3.4 폭풍 통제

Path:

Storm Control> 포트 관리 > 구성

그림 3-4 폭풍 통제 페이지

이 페이지는 스톰 제어 기능을 구성하며, 설정된 속도를 초과하는 패킷은 버려집니다.

3.5 대역폭 제어

Path:

구성 > 포트 관리 > 대역폭 제어

그림 3-5 대역폭 제어 페이지

이 페이지는 스위치 포트의 입출력 속도를 구성하며, 대역폭은 64 의 정수 배수로 제한됩니다.

3.6 오류 비활성화

Path:

설정 > 포트 관리 > 오류 비활성화

그림 3-6 오류 비활성화 페이지

이 페이지는 보안 또는 네트워크 보호 메커니즘이 비정상적인 상황을 감지할 때 자동으로 포트 종료 및 복구 동작을 설정할 수 있도록 합니다.

4 기본 복무

4.1 VLAN 구성

4.1.1 정적 VLAN

Path:

기본 서비스 > VLAN 설정 > 정적 VLAN >

그림 4-1-1 정적 VLAN 페이지

이 페이지는 VLAN 에 대한 설명 정보를 추가, 수정, 삭제 및 추가할 수 있습니다.

4.1.2 VLAN 포트

Path:

기본 서비스 > VLAN 포트 > 설정 >

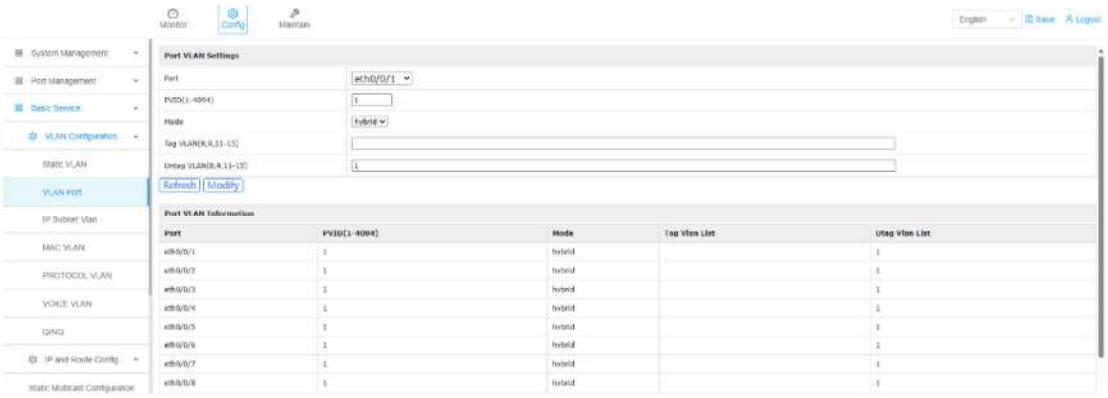

그림 4-1-2 VLAN 포트 페이지

이 페이지는 포트 기본 VLAN 과 모드를 구성합니다.

4.1.3 IP 서브넷 VLAN

Path:

기본 서비스 > VLAN 구성 > IP 서브넷 VLAN > 구성

그림 4-1-3 IP 서브넷 VLAN 페이지

이 페이지를 통해 관리자는 IP 서브넷 기반 VLAN 매핑을 구성할 수 있어, 스위치가 연결된 장치의 소스 IP 주소 또는 서브넷에 따라 자동으로 VLAN 을 할당할 수 있습니다.

4.1.4 MAC VLAN

Path:

기본 서비스 > VLAN 구성 > MAC VLAN > 구성

그림 4-1-4 MAC VLAN 페이지

이 페이지는 관리자가 MAC 기반 VLAN 매핑을 구성할 수 있게 하여, 스위치가 연결된 장치의 출처 MAC 주소에 따라 자동으로 VLAN 을 할당할 수 있게 합니다.

4.1.5 프로토콜 VLAN

Path:

기본 서비스 > VLAN 구성 >프로토콜 VLAN >

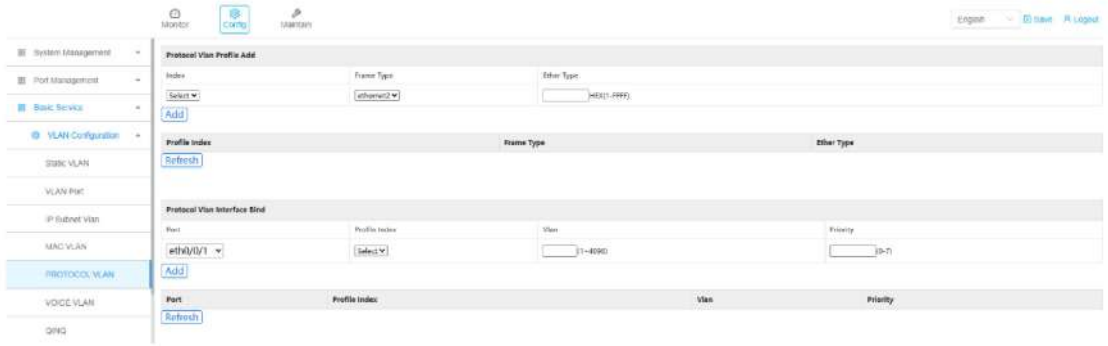

그림 4-1-5 프로토콜 VLAN 페이지

이 페이지는 관리자가 프로토콜 기반 VLAN 을 구성할 수 있게 하여, 스위치가 IPv4, IPv6, ARP, PPPoE 와 같은 상위 계층 프로토콜 유형에 따라 트래픽을 서로 다른 VLAN 으로 분류할 수 있게 합니다.

4.1.6 음성 VLAN

Path:

기본 서비스 > VLAN 구성 >음성 VLAN >

그림 4-1-6 음성 VLAN 페이지

이 페이지에서는 관리자가 음성 VLAN 을 설정할 수 있어, MAC 주소/OUI 를 기반으로 VoIP 전화기를 자동으로 식별하고, 최적의 음성 품질을 보장하기 위해 고우선순위의 전용 VLAN 에 할당할 수 있습니다.

4.1.7 QINQ

Path:

기본 서비스 > VLAN 구성 >QINQ >

그림 4-1-7 QINQ 페이지

이 페이지는 관리자가 QinQ 매핑 규칙을 구성할 수 있게 하여 고객 VLAN 범위를 하나의 서비스 VLAN(S-VLAN)으로 캡슐화하여 통신사 네트워크 전송을 가능하게 합니다.

4.2 IP 및 경로 구성

4.2.1 VLAN IP 구성

Path:

기본 서비스 > IP 및 라우팅 구성> VLAN IP 구성 > 설정

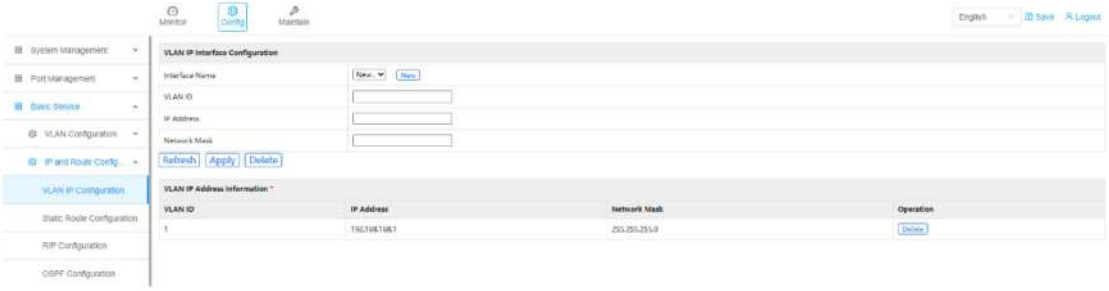

그림 4-2-1 VLAN IP 구성 페이지

이 페이지는 VLAN 인터페이스를 추가, 수정 및 삭제할 수 있습니다.

4.2.2 정적 경로 구성

Path:

기본 서비스 > IP >및 경로 구성 > 정적 경로 구성

그림 4-2-2 정적 경로 구성 페이지

이 페이지는 정적 경로를 표시, 추가, 삭제합니다.

4.2.3 RIP 구성

4.2.3.1 일반 구성 RIP

Path:

기본 서비스 > IP 및 경로 구성 >> RIP 구성 > RIP 일반 구성

그림 4-2-3-1 RIP 일반 구성 페이지

이 페이지에서는 관리자가 글로벌 RIP 라우팅을 활성화하고, RIP 프로토콜 버전을 설정하며, 라우팅 업데이트 타이머, 지표, 관리 거리를 조정할 수 있습니다. RIP 라우팅에 참여하는 네트워크나 인터페이스도 이 페이지에서 추가할 수 있습니다.

4.2.3.2 RIP 인터페이스 구성

Path:

기본 서비스 > IP 및 경로 구성 >> RIP 구성 > RIP 인터페이스 구성

그림 4-2-3-2 RIP 인터페이스 구성 페이지

이 페이지는 관리자가 RIP 라우팅에 참여하는 개별 3 계층 인터페이스를 구성할 수 있게 해줍니다. 각 인터페이스는 업데이트 송수신을 위한 특정 RIP 버전을 할당할 수 있으며, 선택적 인증을 활성화하여 RIP 메시지를 안전하게 할 수 있습니다.

4.2.4 OSPF 구성

Path:

기본 서비스 >> IP 및 경로 구성 > OSPF 구성

그림 4-2-4 OSPF 구성 페이지

이 페이지에서는 관리자가 OSPF(Open Shortest Path First)를 구성할 수 있는데, 이는 빠른 수렴과 대규모 네트워크 배포를 위해 설계된 링크 상태 라우팅 프로토콜입니다.

4.3 정적 멀티캐스트 구성

Path:

기본 서비스 > 정적 멀티캐스트 구성 > 구성

그림 4-3 정적 멀티캐스트 구성 페이지

이 페이지는 관리자가 수동으로 멀티캐스트 포워딩 항목을 추가할 수 있게 해줍니다. 정적 멀티캐스트는 특정 멀티캐스트 트래픽이 IGMP 스누핑이나 동적 멀티캐스트 메커니즘에 의존하지 않고 지정된 포트로 전달되도록 보장합니다.

4.4 IGMP 구성

4.4.1 글로벌 구성

Path:

구성 > 기본 서비스 > IGMP 스누핑 구성 > 글로벌 구성

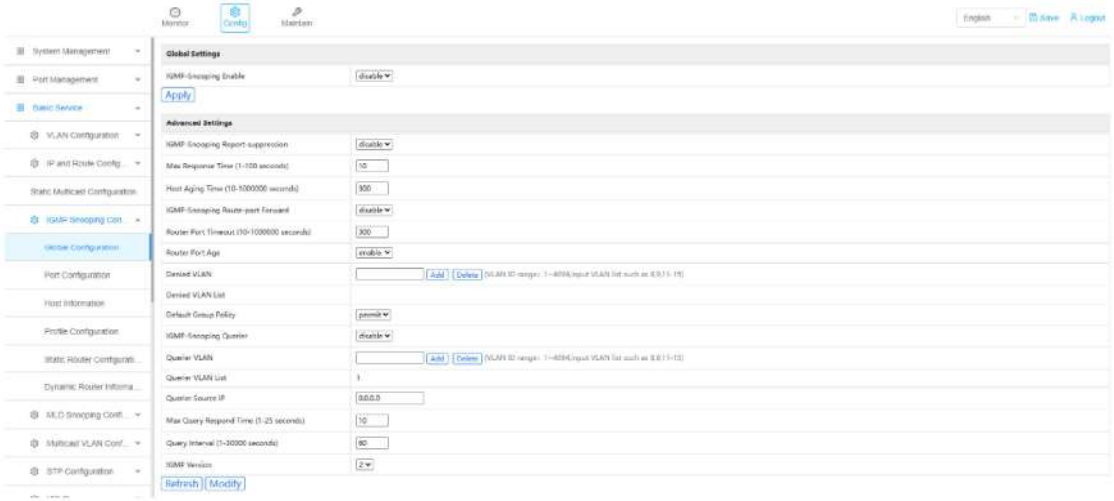

그림 4-4-1 정적 멀티캐스트 구성 페이지

이 페이지는 관리자가 전역 IGMP 스누핑 매개변수를 설정할 수 있게 합니다. IGMP 스누핑은 그룹 구성원 정보를 학습하고 네트워크 전반에 걸친 멀티캐스트 플러딩을 방지하여 멀티캐스트 트래픽 전달을 최적화합니다.

매개변수 설명

항목	묘사
IGMP 감시 활성화	전 세계적으로 IGMP 스누핑을 활성화하거나 비활성화합니다. 활성화되면 스위치는 IGMP 보고서를 기반으로 멀티캐스트 멤버 포트를 학습합니다.
보고서 억제	불필요하거나 중복된 IGMP 보고 메시지를 억제하여 멀티캐스트 트래픽을 줄입니다.
최대 응답 시간	호스트가 IGMP 쿼리에 응답하는 데 걸릴 수 있는 최대 시간은 1–100 초입니다.
숙주 노화 시간	그 후 비활성 멀티캐스트 호스트는 스누핑 테이블에서 제거됩니다.
보고서 전달	IGMP 보고 메시지를 다른 포트로 전달할지 여부를 결정합니다.
라우터 포트 타임아웃	멀티캐스트 라우터 메시지가 감지되지 않을 때 라우터 포트 제거에 대한 타임아웃 값.
라우터 포트 에이징	멀티캐스트 라우터 포트의 노화 메커니즘을 활성화합니다.
거부된 VLAN 목록	IGMP 스누핑이 비활성화된 VLAN 을 지정합니다.
기본 그룹 정책	멀티캐스트 그룹 멤버십의 기본 동작: *허용* 또는 *거부*.
IGMP 스누핑 쿼리어	멀티캐스트 라우터가 없을 때 스위치가 IGMP 쿼리어 역할을 할 수 있게 해줍니다.

항목	묘사
VLAN 쿼리	IGMP 쿼리 메시지 전송에 사용되는 VLAN ID.
쿼리어 소스 IP	스위치가 IGMP 쿼리어로 동작할 때 사용하는 소스 IP 주소입니다.
최대 쿼리 응답 시간	호스트가 IGMP 쿼리에 응답할 수 있는 최대 응답 시간을 허용했습니다.
쿼리 간격	IGMP 일반 쿼리 메시지 사이의 간격(초 단위).
IGMP 버전	IGMP 프로토콜 버전을 선택: IGMPv1, IGMPv2, 또는 IGMPv3.
새로고침 / 수정	페이지를 새로고침하거나 수정된 매개변수를 적용합니다.

4.4.3 포트 구성

Path:

구성 > 기본 서비스 > IGMP 스누핑 구성 > 포트 구성

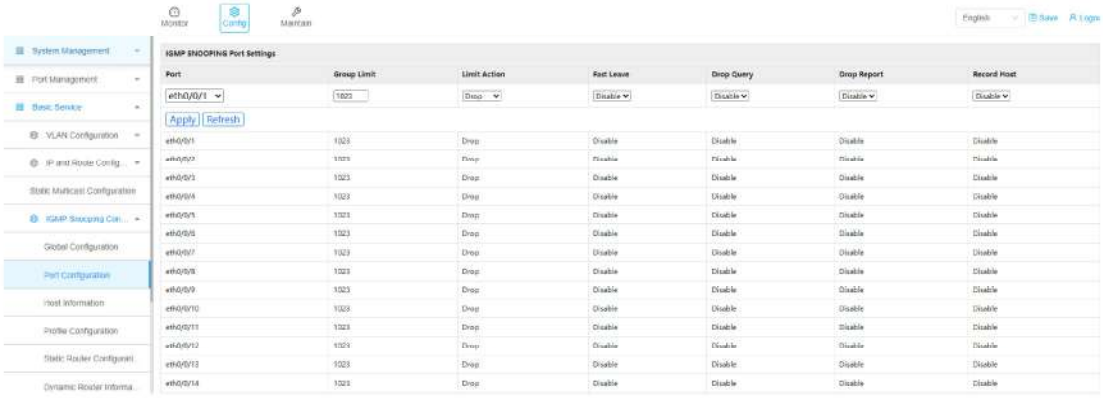

그림 4-4-2 포트 구성 페이지

이 페이지는 관리자가 각 스위치 포트별로 그룹 제한, 빠른 리브 처리, 패킷 필터링 옵션 등 IGMP 스누핑 동작을 설정할 수 있게 합니다.

4.4.4 호스트 구성

Path:

구성 > 기본 서비스 > IGMP 스누핑 구성 > 호스트 구성

그림 4-4-3 호스트 구성 페이지

이 페이지는 관리자가 IGMP 스누핑을 기반으로 학습된 멀티캐스트 호스트 정보를 볼 수 있게 합니다. 어떤 호스트가 멀티캐스트 그룹에 가입했는지, 어떤 포트를 통해 어떤 VLAN 을 거쳤는지 가시성을 제공합니다.

4.4.5 프로필 구성

Path:

구성 > 기본 서비스 > IGMP 스누핑 구성 > 프로파일 구성

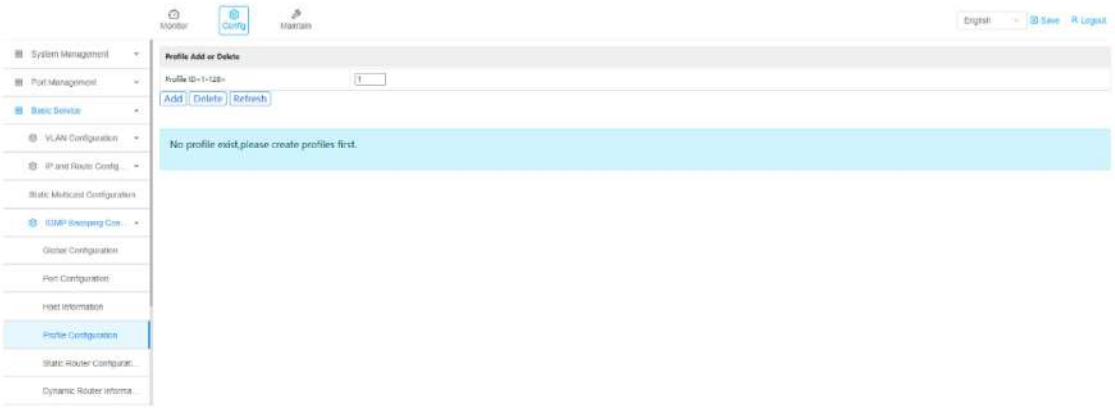

그림 4-4-4 프로필 구성 페이지

이 페이지는 관리자가 IGMP 스누핑 프로필을 생성하고 삭제할 수 있게 해줍니다. 프로파일은 포트나 VLAN 에 적용할 수 있는 미리 정의된 템플릿을 나타냅니다. 프로필이 생성되지 않으면 시스템이 알림 메시지를 표시합니다.

4.4.6 정적 라우터 구성

Path:

기본 서비스 >> IGMP 감시 설정 > 정적 라우터 구성

그림 4-4-5 정적 라우터 구성 페이지

이 페이지는 관리자가 IGMP 스누핑을 위해 정적 라우터 포트를 수동으로 설정할 수 있게 해줍니다. 정적 라우터 포트는 스위치가 멀티캐스트 라우터 인터페이스를 자동으로 감지하지 못하더라도 멀티캐스트 트래픽이 올바르게 상류로 전달되도록 보장합니다.

4.4.7 동적 라우터 구성

Path:

기본 서비스 >> IGMP 스누핑 구성 > 동적 라우터 구성

그림 4-4-6 동적 라우터 구성 페이지

이 페이지는 스위치가 IGMP 스누핑 또는 MLD 스누핑을 통해 자동으로 학습한 라우터 포트를 보여줍니다. 멀티캐스트 라우터가 IGMP/MLD 쿼리 메시지를 보낼 때, 스위치는 해당 포트를 동적 라우터 포트로 식별합니다.

이 페이지는 모니터링 전용이며 수동 설정은 허용되지 않습니다.

4.5 MLD 스누핑 구성

4.5.1 기본 구성

Path:

기본 서비스 > 구성 > MLD 스누핑 구성 > 기본 구성

그림 4-5-1 기본 구성 페이지

이 페이지는 관리자가 MLD 스누핑 기능의 기본 운영 매개변수를 설정할 수 있게 해주며, 이 기능은 멀티캐스트 멤버십을 학습하고 멀티캐스트 패킷을 필요한 포트로만 전달하여 IPv6 멀티캐스트 트래픽을 관리합니다.

매개변수 설명

항목	묘사
글로벌 이네이블	MLD 스누핑 기능을 전반적으로 활성화하거나 비활성화합니다.
최대 응답 시간	호스트가 멀티캐스트 쿼리 메시지에 응답할 수 있는 최대 시간(초 단위).
숙주 노화 시간	숙주 회원 등록의 나이 드는 시간. 이 기간 내에 신고가 접수되지 않으면 항목이 삭제됩니다.
라우터 포트 포워드	라우터 포트를 통한 멀티캐스트 패킷 전달을 가능하게 합니다.
라우터 포트 노화 시간	동적 학습 라우터 포트의 노후 타임아웃.
라우터 포트 사용 연령	라우터 포트가 동적으로 학습되는지 여부를 설정합니다.
MLD 쿼리어	활성화되면 스위치는 MLD 쿼리어로 동작하며 주기적으로 쿼리 메시지를 전송합니다.
쿼리에 최대 응답 시간	스위치가 쿼리어 역할을 할 때 호스트가 허용하는 최대 응답 시간.
쿼리어 쿼리 간격	쿼리어가 Query 메시지를 보내는 간격(초 단위).
적용하다	구성에 적용합니다.
리프레쉬	현재 설정 값을 다시 불러옵니다.

4.5.2 포트 구성

Path:

Config > Basic Service > MLD Snooping Configuration > Port Configuration

그림 4-5-2 포트 구성 페이지

이 페이지는 관리자가 각 개별 포트에 대해 MLD 스누핑 동작을 설정할 수 있게 해줍니다.

IPv6 멀티캐스트 멤버십과 포워딩을 제어할 때는 포트 수준 설정이 우선시됩니다.

4.5.3 정적 라우터 구성

Path:

기본 서비스 >> MLD 스누핑 구성 > 정적 라우터 구성 구성

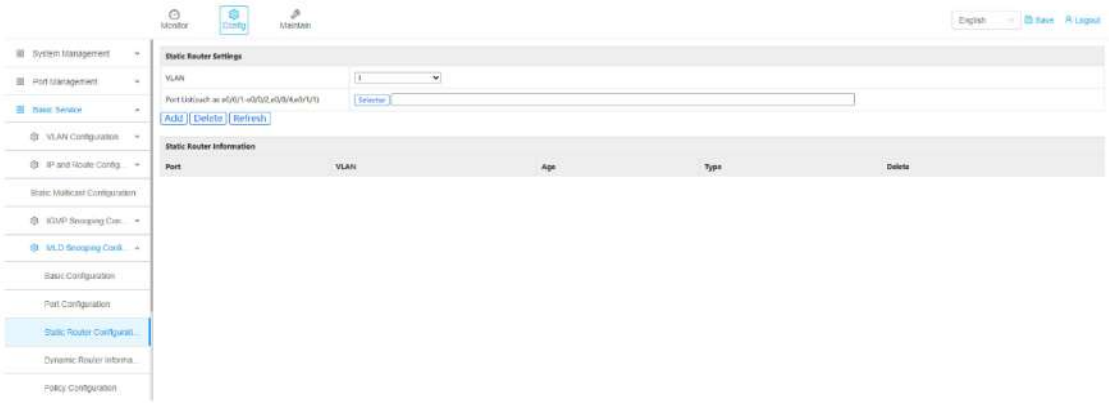

그림 4-5-3 정적 라우터 구성 페이지

이 페이지는 관리자가 VLAN 내에서 멀티캐스트 라우터 포트를 수동으로 지정할 수 있게 해줍니다.

정적 라우터 포트는 라우터가 자동으로 학습되지 않을 때 IGMP/MLD 제어 메시지와 멀티캐스트 스트림이 올바르게 전달되도록 보장합니다.

4.5.4 동적 라우터 정보

Path:

기본 서비스 >> MLD 스누핑 구성 > 동적 라우터 정보

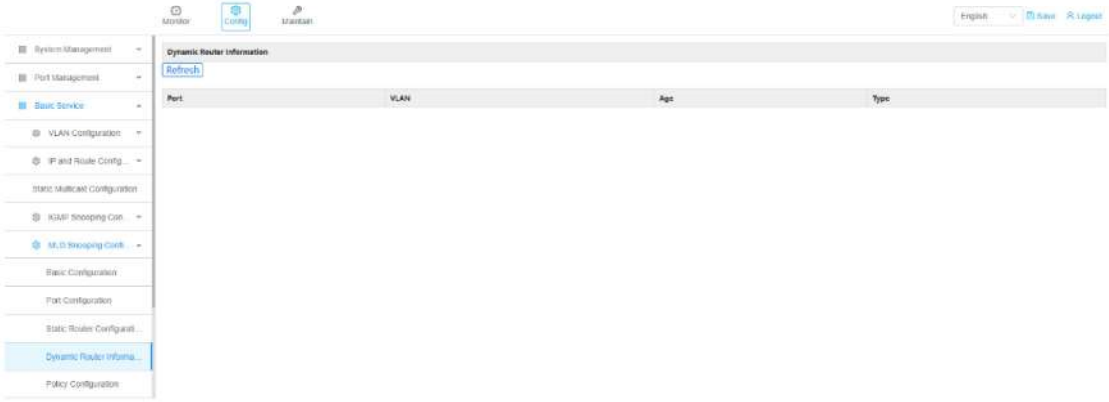

그림 4-5-4 동적 라우터 정보 페이지

이 페이지는 관리자가 VLAN 내에서 멀티캐스트 라우터 포트를 수동으로 지정할 수 있게 해줍니다.

정적 라우터 포트는 라우터가 자동으로 학습되지 않을 때 IGMP/MLD 제어 메시지와 멀티캐스트 스트림이 올바르게 전달되도록 보장합니다.

4.5.5 정책 구성

Path:

Config > Basic Service > MLD Snooping Configuration > Policy Configuration

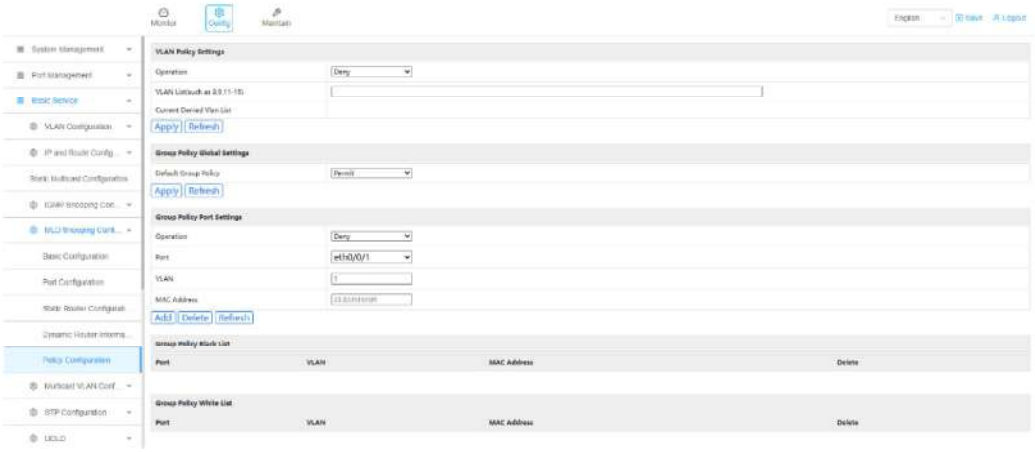

그림 4-5-5 정책 구성 페이지

정책 구성 페이지는 관리자가 VLAN, 포트, 호스트 MAC 주소를 기반으로 멀티캐스트 접근 동작을 제어할 수 있게 해줍니다. 이러한 설정은 IPTV, 엔터프라이즈 멀티캐스트 제어, 네트워크 보안 환경에서 흔히 사용됩니다.

4.6 멀티캐스트 VLAN 구성

4.6.1 IS MVR 구성

Path:

기본 서비스 >> 멀티캐스트 VLAN 구성 > IS MVR 구성

그림 4-6-1 IS MVR 구성 페이지

이 페이지는 관리자가 IGMP 스누핑 MVR(멀티캐스트 VLAN 등록)을 구성할 수 있게 해주며, 이를

통해 제공자 VLAN 에서 발생하는 멀티캐스트 트래픽을 여러 고객 VLAN 에 효율적으로 전달할 수 있습니다.

MVR 은 일반적으로 IPTV 및 멀티캐스트 서비스 배포에서 멀티캐스트 중복을 줄이고 네트워크 설계를 단순화하기 위해 사용됩니다.

4.6.2 IS 멀티캐스트 VLAN 구성

Path:

구성 > 기본 서비스 > 멀티캐스트 VLAN 구성 > IS 멀티캐스트 VLAN 구성

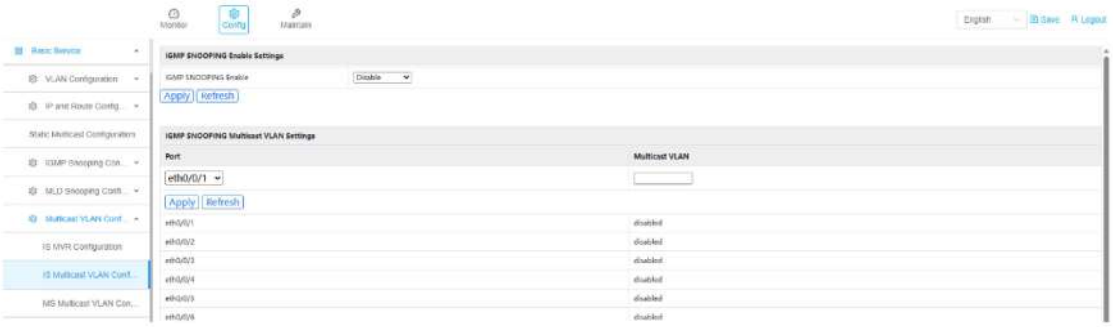

그림 4-6-2 IS 멀티캐스트 VLAN 구성 페이지

이 페이지는 IGMP 스누핑이 활성화된 경우 관리자가 포트별로 멀티캐스트 VLAN 할당을 설정할 수 있게 해줍니다.

특정 포트에서 허용되는 멀티캐스트 VLAN 트래픽을 제어하여 불필요한 멀티캐스트 플러딩을 방지하는 데 사용됩니다.

4.6.3 MS 멀티캐스트 VLAN 구성

Path:

구성 > 기본 서비스 > 멀티캐스트 VLAN 구성 > MS 멀티캐스트 VLAN 구성

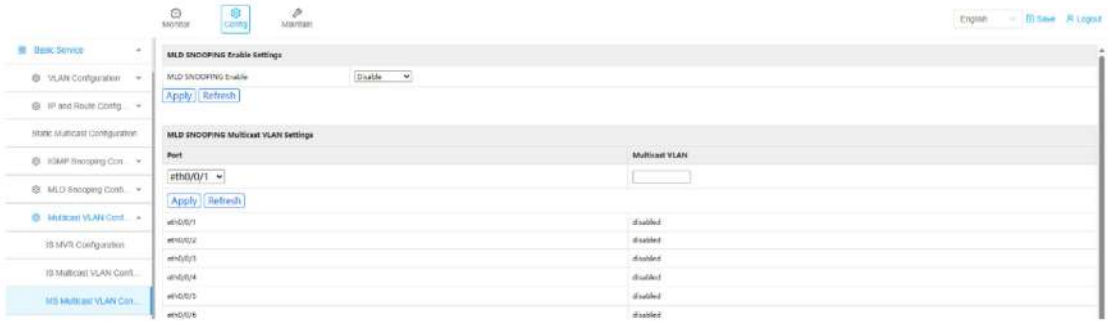

그림 4-6-3 MS 멀티캐스트 VLAN 구성 페이지

이 페이지는 MLD 스누핑이 활성화된 경우 IPv6 멀티캐스트 트래픽에 대해 관리자가 포트별로 멀티캐스트 VLAN 할당을 설정할 수 있게 해줍니다. IPv6 멀티캐스트 포워딩에 대한 세밀한 제어를

제공하고 불필요한 멀티캐스트 플러딩을 방지합니다.

4.7 STP 구성

4.7.1 글로벌 구성

Path:

기본 서비스 > STP 구성 > 전역 구성 > 구성

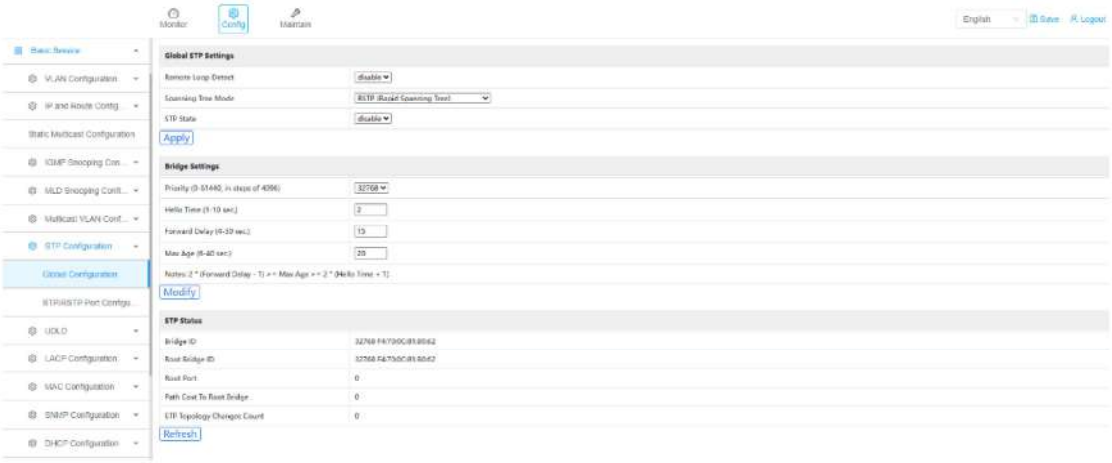

그림 4-7-1 전역 구성 페이지

이 페이지는 관리자가 전역 스패닝 트리 프로토콜(STP) 설정을 구성할 수 있게 해줍니다.

STP 는 레이어 2 네트워크 루프를 방지하고, 방송 폭풍을 제거하며, 네트워크의 안정성과 신뢰성을 보장하는 데 사용됩니다.

스패닝 트리 모드 설명

STP (IEEE 호환 스패닝 트리)

전통적인 IEEE 802.1D 스패닝 트리 프로토콜.

기본적인 루프 방지를 제공하며 호환성은 높지만 수렴 속도는 느립니다.

RSTP (Rapid Spanning Tree)

IEEE 802.1w 신속 스패닝 트리 프로토콜.

수렴 속도를 크게 향상시키고 STP 장치와의 하위 호환성을 제공합니다.

MSTP (다중 스패닝 트리)

IEEE 802.1s 다중 스패닝 트리 프로토콜.

여러 VLAN 을 서로 다른 스패닝 트리 인스턴스에 매핑할 수 있어 링크 활용도와 확장성을 향상시킵니다.

4.7.2 STP/RSTP 포트 구성

Path:

기본 서비스 > STP 구성 >> STP/RSTP 포트 구성

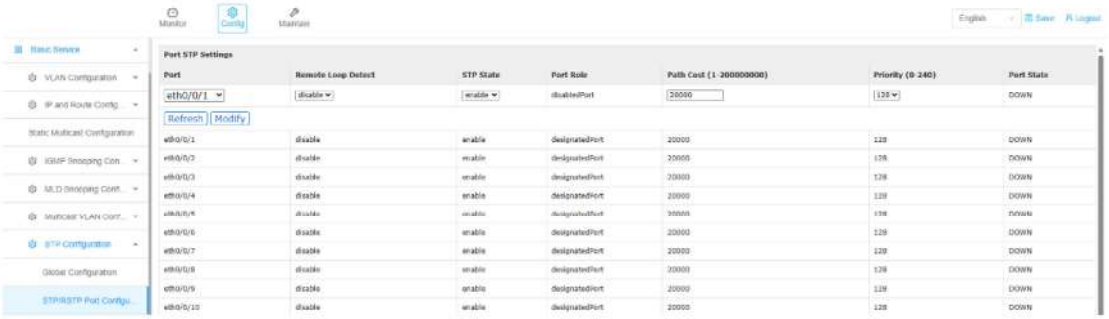

그림 4-7-2 STP/RSTP 포트 구성 페이지

이 페이지는 관리자가 포트별로 스패닝 트리 프로토콜(STP) 매개변수를 구성할 수 있게 합니다. 각 물리적 포트가 스패닝 트리 토폴로지에 어떻게 참여하는지 상세히 제어할 수 있습니다.

4.8 UDLD

4.8.1 UDLD 구성

Path:

Config > Basic Service > UDLD > UDLD Configuration

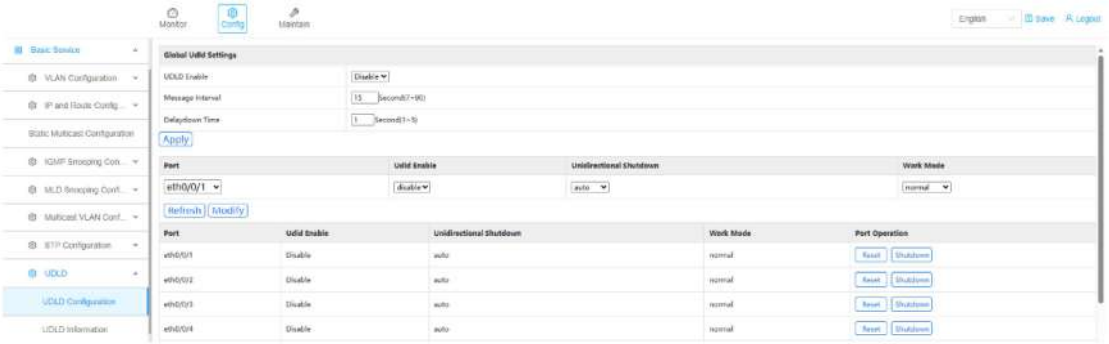

그림 4-8-1 UDLD 구성 페이지

이 페이지는 관리자가 단방향 링크 감지(UDLD)를 설정하여 단방향 링크 장애를 감지하고 보호할 수

있도록 합니다.

UDLD 는 작동하는 것처럼 보이지만 트래픽을 한 방향으로만 전송하는 링크로 인한 네트워크 루프와 전달 이상 현상을 방지하는 데 도움을 줍니다.

4.8.2 UDLD 정보

Path:

UDLD > 기본 서비스 > UDLD > UDLD 정보

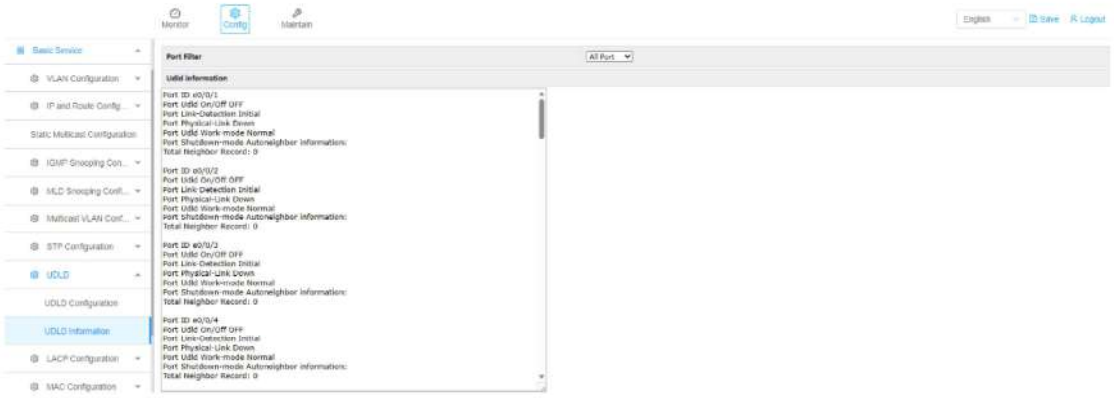

그림 4-8-2 UDLD 정보 페이지

이 페이지는 각 스위치 포트에 대한 단방향 링크 감지(UDLD)의 작동 상태와 감지 결과를 보여줍니다. 관리자가 단방향 링크 장애를 식별하고 UDLD 작동을 검증하는 데 도움을 주는 실시간 모니터링 정보를 제공합니다.

4.9 LACP 구성

4.9.1 상태 표시

Path:

기본 서비스 > 구성 > LACP 구성 > 상태 표시

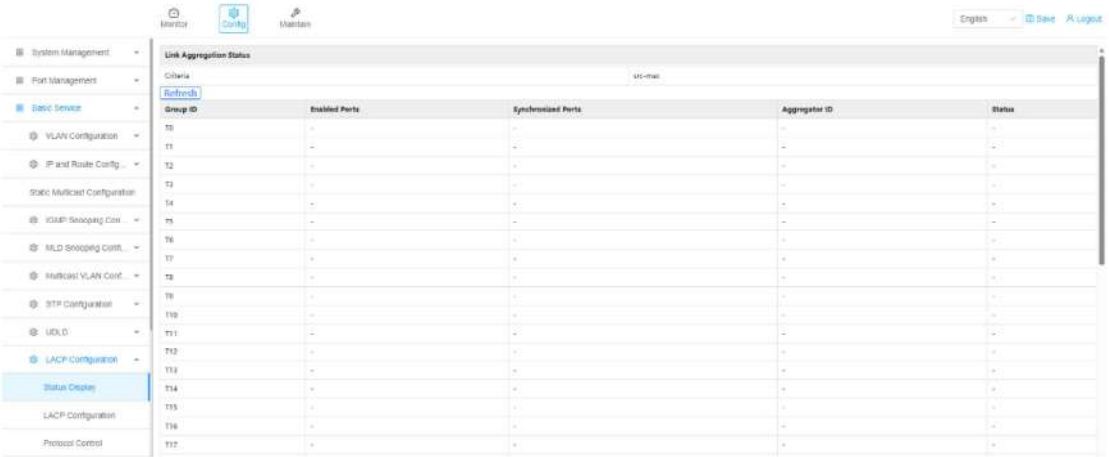

그림 4-9-1 상태 표시 페이지

이 페이지는 스위치 내 링크 집계(LACP) 그룹의 현재 운영 상태를 보여줍니다.

이 도구는 구성된 집계 그룹, 참여 포트, 동기화 상태, 부하 분산 기준에 관한 정보를 제공합니다.

4.9.2 LACP 구성

Path:

기본 서비스 > LACP 구성 >> LACP 구성

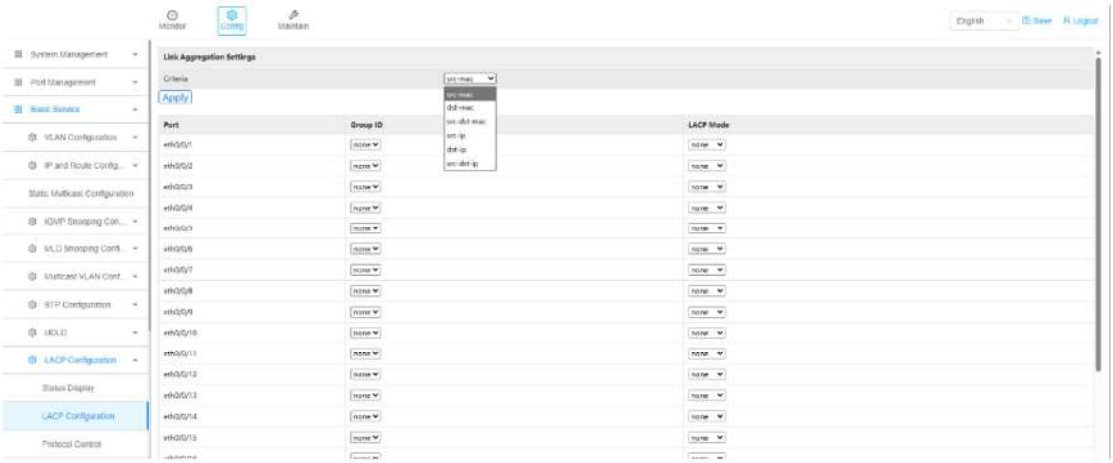

그림 4-9-2 LACP 구성 페이지

이 페이지는 관리자가 스위치에서 링크 집계(LACP)를 구성할 수 있게 해줍니다.

여러 개의 물리 포트를 하나의 논리 링크로 결합하여 대역폭을 늘리고 링크 중복성을 제공할 수 있습니다.

4.9.3 프로토콜 제어

Path:

기본 서비스 > 구성 > LACP 구성 > 프로토콜 제어

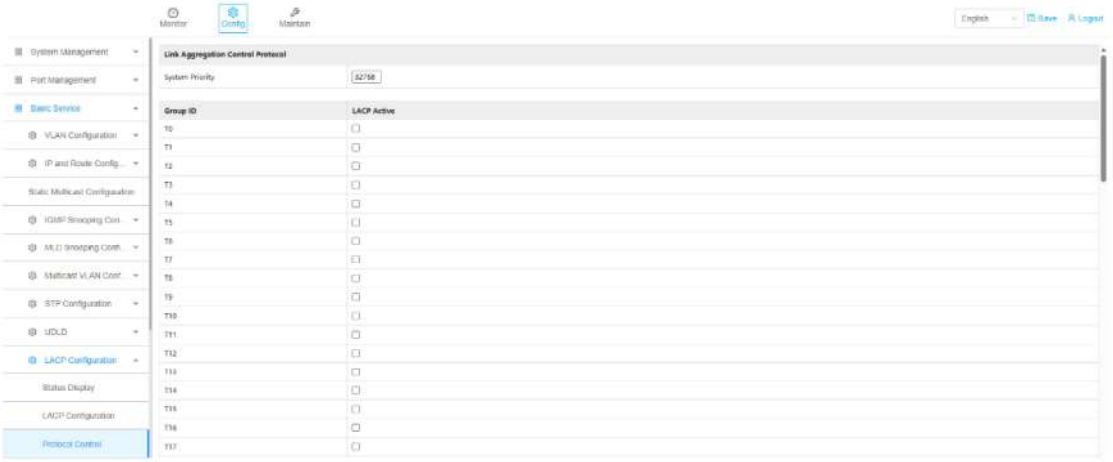

그림 4-9-3 프로토콜 제어 페이지

이 페이지는 관리자가 전역 LACP 프로토콜 매개변수를 설정하고 각 링크 집계 그룹에 대해 LACP

협상을 활성화하거나 비활성화할 수 있게 합니다.

4.10 MAC 구성

4.10.1 포트 바인딩 디스플레이

Path:

기본 서비스 > 구성 > MAC 구성 > 포트 바인딩 디스플레이

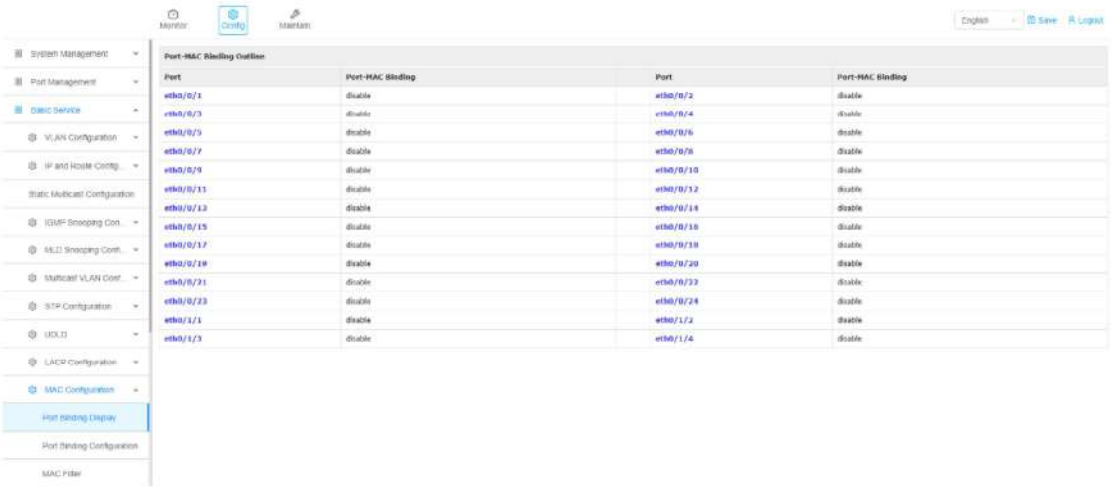

그림 4-10-1 포트 바인딩 디스플레이 페이지

이 페이지는 스위치의 각 물리적 포트에 대한 MAC 바인딩 상태에 대한 개요를 제공합니다.

4.10.2 포트 바인딩 구성

Path:

구성 > 기본 서비스 > MAC 구성 > 포트 바인딩 구성

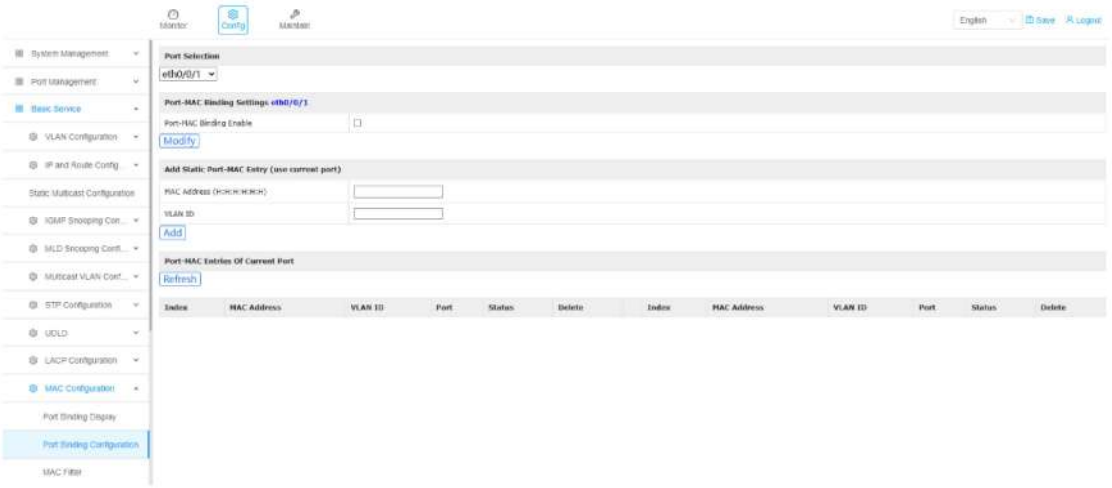

그림 4-10-2 포트 바인딩 구성 페이지

이 페이지는 관리자가 특정 포트에서 MAC 바인딩을 활성화하고 정적 MAC 주소 항목을 접근 제어를

구성할 수 있게 합니다.

4.10.3 MAC 필터

Path:

기본 서비스 > MAC 필터> MAC 구성 > 구성

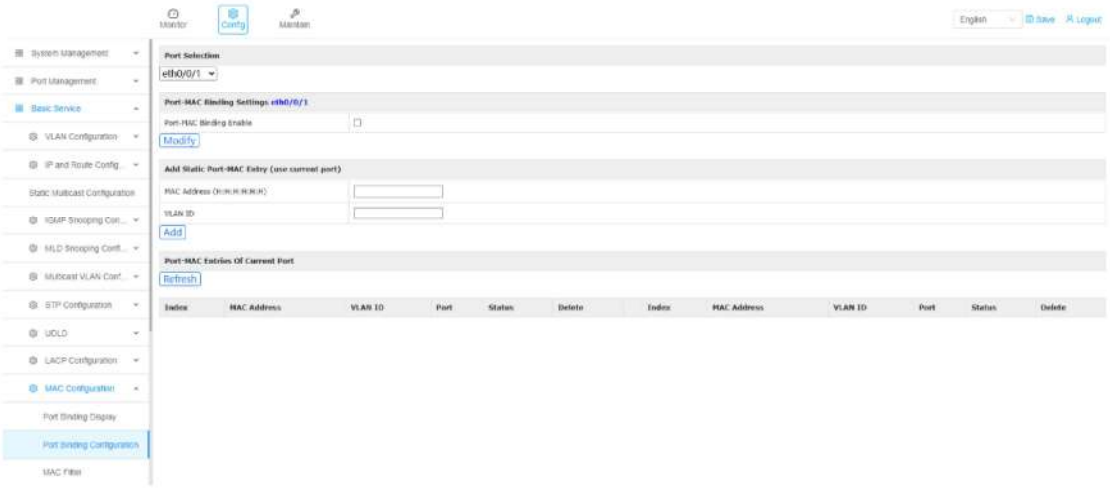

그림 4-10-3 MAC 필터 페이지

이 페이지는 관리자가 VLAN 을 기반으로 MAC 주소 필터링 규칙을 설정할 수 있게 해주며, 특정 장치가 네트워크에서 통신할 수 있는지 제어할 수 있습니다.

4.11 SNMP 구성

4.11.1 커뮤니티 구성

Path:

구성 > 기본 서비스 > SNMP 구성 > 커뮤니티 구성

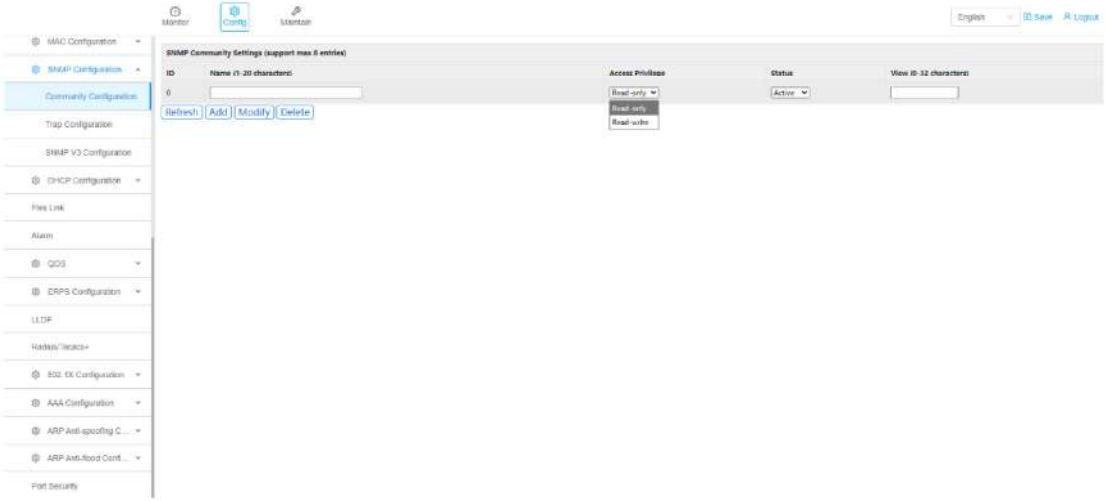

그림 4-11-1 커뮤니티 구성 페이지

이 페이지는 관리자가 스위치에 접근하는 네트워크 관리 시스템(NMS)의 접근 권한을 제어하는

SNMP v1/v2c 커뮤니티 문자열을 구성할 수 있게 합니다.

4.11.2 트랩 구성

Path:

기본 서비스 > 구성 > SNMP 구성 > 트랩 구성

그림 4-11-2 트랩 구성 페이지

이 페이지는 관리자가 SNMP Trap 목적지를 설정할 수 있게 하여 스위치가 네트워크 관리 시스템(NMS)에 이벤트 알림과 알람을 선제로 전송할 수 있게 합니다.

4.11.3 SNMP V3 구성

4.11.3.1 SNMP 엔진

Path:

기본 서비스 > SNMP V3 구성 >> SNMP 엔진

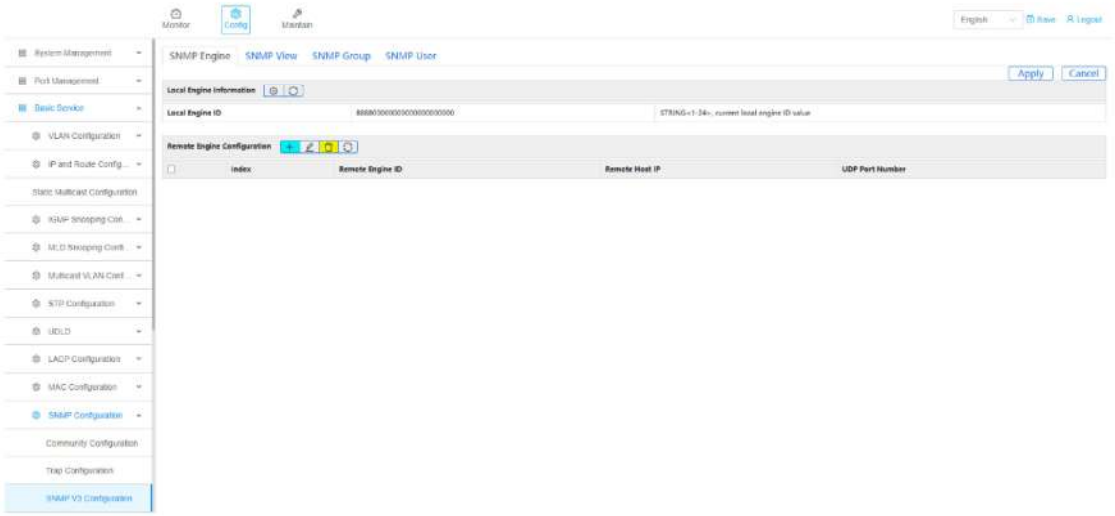

그림 4-11-3-1 SNMP 엔진 페이지

이 페이지는 관리자가 로컬 SNMP 엔진 ID 를 확인하거나 설정하고 원격 엔진 항목을 관리할 수 있게 합니다.

엔진 ID 는 SNMPv3 보안 메커니즘(인증, 프라이버시, 재생 방지)에서 사용하는 고유 식별자입니다. 엔진 ID 변경은 SNMP 관리 시스템에서 재구성이 필요할 수 있습니다.

4.11.3.2 SNMP 뷰

Path:

기본 서비스 >> SNMP V3 구성 > SNMP 뷰

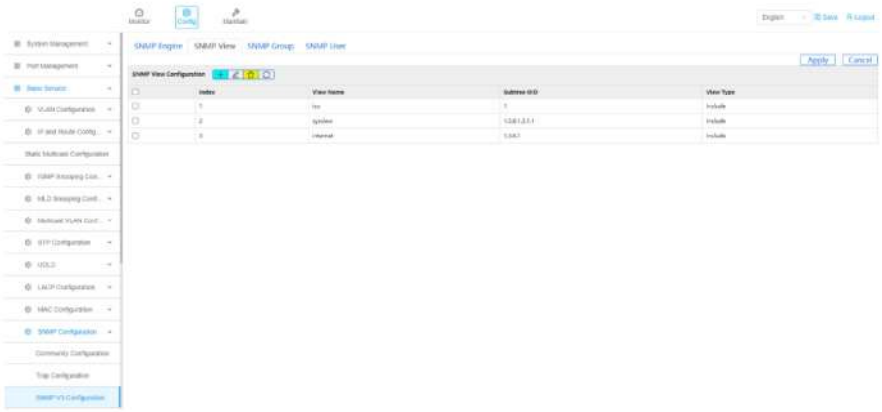

그림 4-11-3-2 SNMP 보기 페이지

이 페이지는 관리자가 SNMP 뷰를 구성할 수 있게 해주며, SNMPv3 사용자를 위한 접근 가능한 MIB 서브트리 범위를 정의합니다. SNMP 뷰는 어떤 OID 에 접근할 수 있고 SNMP 그룹이 참조하는지 제어하는 데 사용됩니다.

4.11.3.3 SNMP 그룹

Path:

기본 서비스 > SNMP V3 구성 >> SNMP 그룹

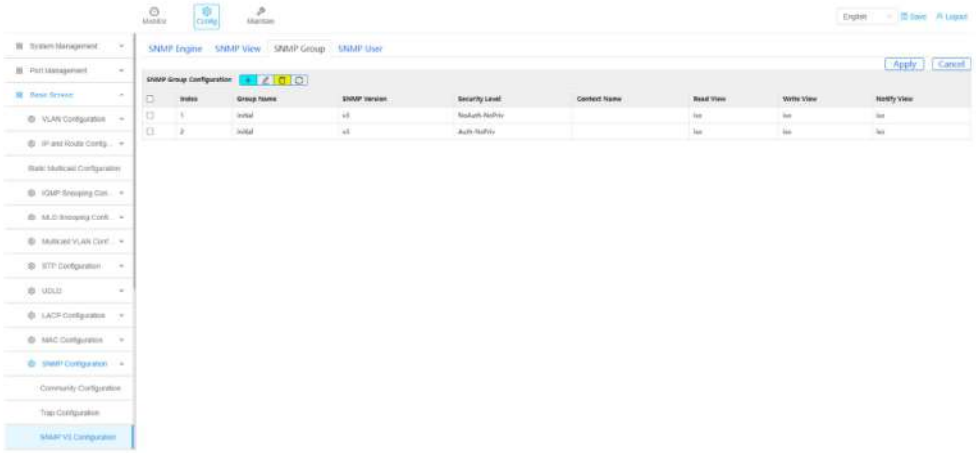

그림 4-11-3-3 SNMP 그룹 페이지

이 페이지는 관리자가 SNMP 사용자를 위한 접근 제어 정책을 정의하는 SNMP 그룹을 구성할 수 있게 합니다. SNMP 그룹은 보안 수준과 SNMP 뷰를 연동하여 읽기, 쓰기, 알림 권한을 제어합니다.

4.11.3.4 SNMP 사용자

Path:

기본 서비스 > SNMP V3 구성 >> SNMP 사용자 설정

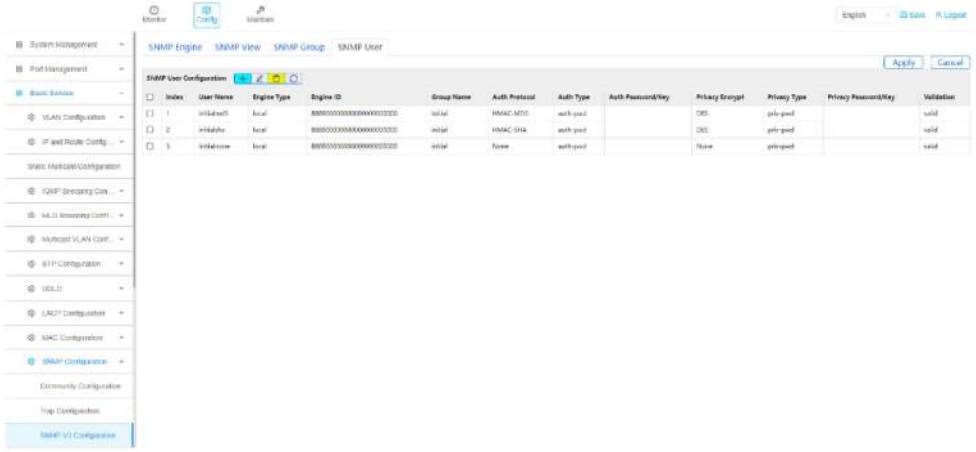

그림 4-11-3-4 SNMP 사용자 페이지

이 페이지는 관리자가 SNMPv3 사용자를 구성할 수 있게 해줍니다.

SNMP 사용자는 인증 및 암호화 매개변수를 포함한 네트워크 관리 시스템이 스위치에 접근하는 실제 엔터티를 나타냅니다.

4.12 DHCP 구성

4.12.1 DHCP 스누핑

Path:

기본 서비스 > DHCP 구성 >> DHCP 스누핑

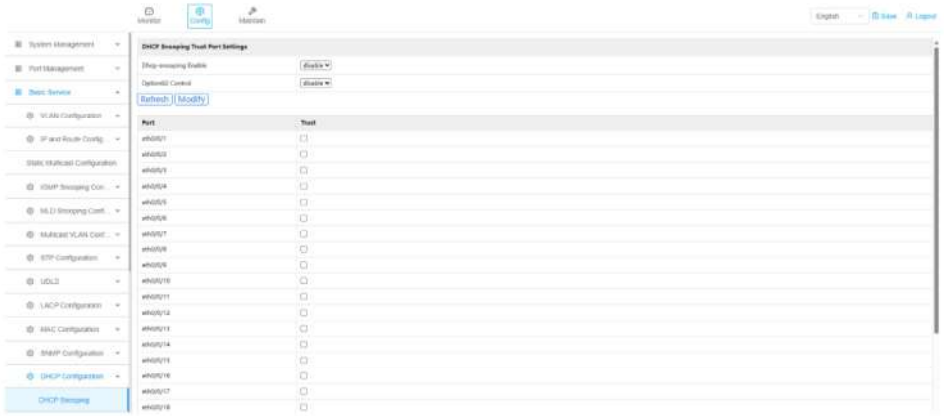

그림 4-12-1 DHCP 스누핑 페이지

이 페이지는 관리자가 DHCP 스누핑을 설정하고 스위치에서 신뢰할 수 있는 포트를 지정할 수 있게

해줍니다.

DHCP 스누핑은 무단 DHCP 서버가 네트워크 내 IP 주소를 배포하는 것을 방지하는 보안 기능입니다. 활성화되면 스위치는 DHCP 메시지를 검사하며 신뢰할 수 있는 포트에서만 DHCP 서버 응답을 허용합니다.

관리자는 DHCP 스누핑을 활성화하거나 비활성화하고, 옵션 82 삽입을 제어하며, 어떤 포트를 신뢰하는지 정의할 수 있습니다. 신뢰할 수 있는 포트는 일반적으로 허가된 DHCP 서버나 업링크 장치에 연결되며, 최종 호스트에 연결된 액세스 포트는 신뢰할 수 없는 상태로 유지되어야 합니다.

4.12.2 IP-MAC 바인딩

Path:

기본 서비스 > 기본 서비스 > IP MAC 바인딩 > DHCP 구성

그림 4-12-2 IP-MAC 바인딩 페이지

이 페이지는 관리자가 IP 주소, MAC 주소, 포트, VLAN 간 정적 바인딩을 구성할 수 있게 해줍니다. 바인딩 메커니즘은 IP 또는 MAC 주소 스푸핑을 방지하여 네트워크 보안을 강화합니다.

관리자는 언바인딩 장치가 네트워크에 접근할 수 있는지 통제하고, 수동으로 바인딩 항목을 추가하며, 바인딩 테이블을 관리할 수 있습니다. 바인딩 강제가 활성화되면 설정된 바인딩 항목과 일치하는 트래픽만 허용됩니다.

4.12.3 DHCP 서버 및 릴레이

Path:

기본 서비스 > DHCP 서버 및 릴레이> 구성 >

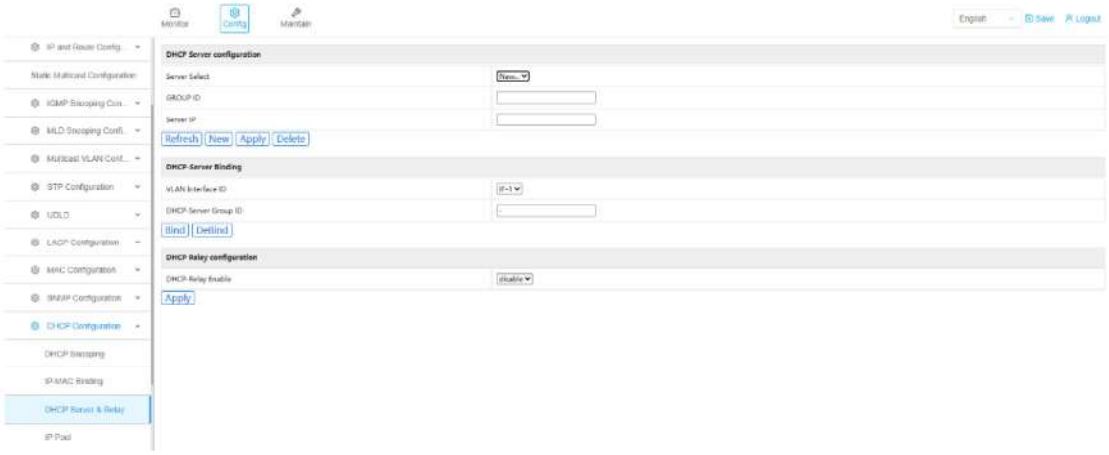

그림 4-12-3 DHCP 서버 및 릴레이 페이지

이 페이지는 관리자가 DHCP 서버 정보를 설정하고, DHCP 서버 그룹을 VLAN 인터페이스에 묶으며, DHCP 릴레이 기능을 활성화하거나 비활성화할 수 있게 합니다.

관리자는 DHCP 서버 그룹을 정의하고, 특정 VLAN 인터페이스와 연관시키며, DHCP 클라이언트 요청을 외부 DHCP 서버로 전달하는 DHCP 릴레이를 활성화할 수 있습니다. 이 구성은 중앙집중식 DHCP 배포 시나리오에서 일반적으로 사용됩니다.

4.12.4 IP 풀

Path:

기본 서비스 > IP 풀> 구성 > DHCP

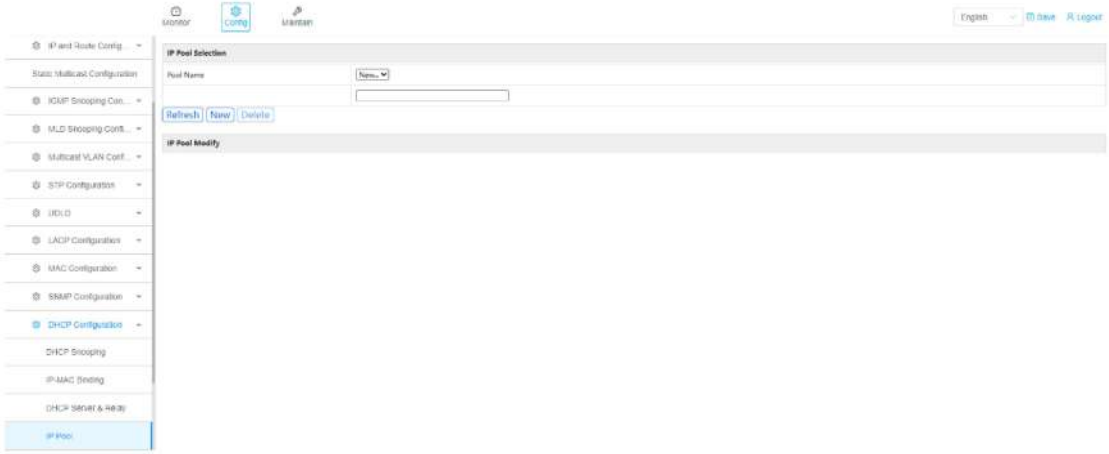

그림 4-12-4 IP 풀 페이지

이 페이지는 관리자가 DHCP IP 주소 풀을 생성, 선택 및 관리할 수 있게 해줍니다.

이 페이지는 관리자가 DHCP IP 주소 풀을 생성, 선택 및 관리할 수 있게 해줍니다.

IP 풀은 DHCP 서버가 특정 네트워크 세그먼트 또는 VLAN 내에서 클라이언트에게 할당할 수 있는 IP 주소 범위를 정의합니다.

관리자는 새로운 IP 풀을 생성하고, 기존 풀을 삭제하며, DHCP 주소 할당을 위한 상세한 풀 매개변수를 수정할 수 있습니다.

4.13 플렉스 링크

Path:

Flex Link > 기본 서비스 > 구성

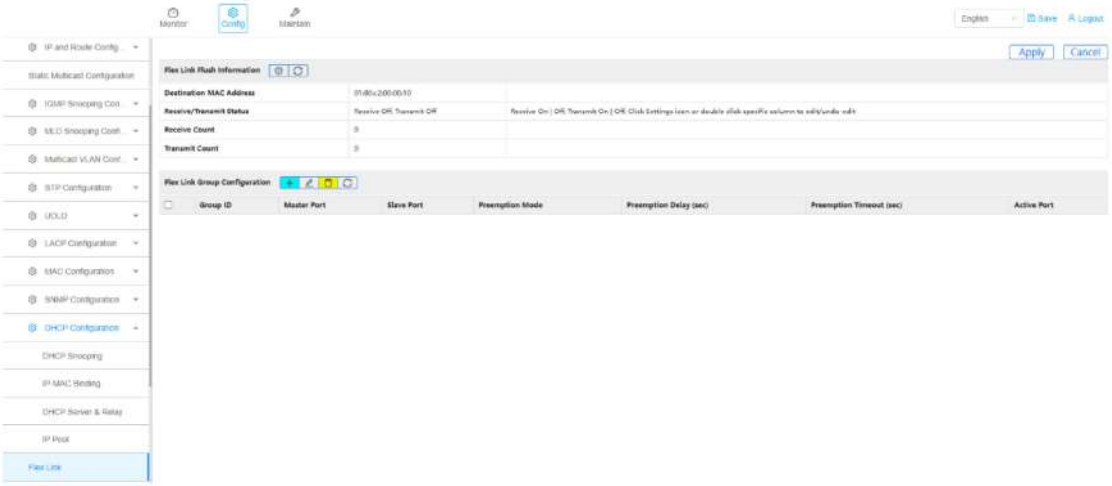

그림 4-13 플렉스 링크 페이지

이 페이지는 관리자가 STP 를 사용하지 않고도 빠른 링크 백업을 제공하는 2 계층 중복 메커니즘인 Flex Link 를 구성할 수 있게 합니다. Flex Link 는 마스터 포트와 슬레이브 포트를 정의하여 작동합니다. 마스터 포트가 실패하면 트래픽은 자동으로 슬레이브 포트로 전환됩니다.

이 페이지에는 링크 스위칭 중 MAC 테이블 업데이트를 가속화하는 플러시 제어 설정과, 선택적 선점 동작을 통해 마스터 및 슬레이브 포트 정의를 위한 Flex Link 그룹 구성도 포함되어 있습니다.

4.14 경보기

Path:

기본 서비스 > 알람 > 구성

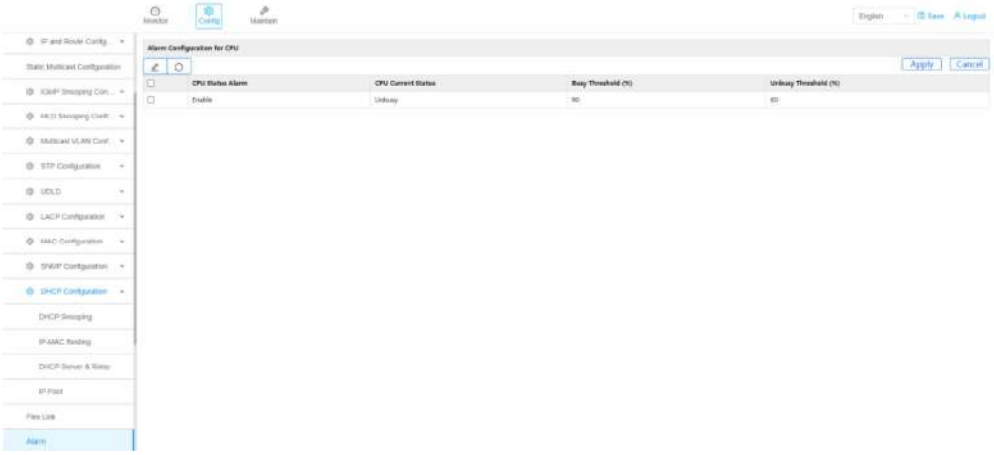

그림 4-14 경보 페이지

이 페이지는 관리자가 CPU 사용률 경보 임계값을 설정할 수 있게 해줍니다. CPU 사용률이 바쁜 임계값을 초과하거나 비통화 임계값 이하로 떨어지면, 시스템은 이에 따라 CPU 상태를 업데이트하고 알람을 트리거하거나 제거합니다.

CPU 경보 메커니즘은 관리자가 장치 성능을 모니터링하고 비정상적인 부하 상태를 제때 감지하는 데 도움을 줍니다.

4.15 QOS

4.15.1 큐 스케줄러

Path:

기본 서비스 > QOS > 큐 스케줄러 > 구성

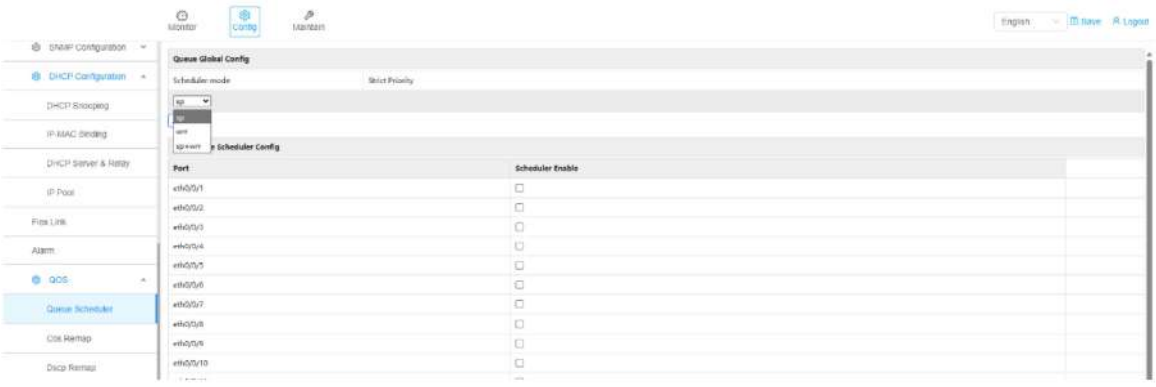

그림 4-15-1 큐 스케줄러 페이지

이 페이지는 관리자가 스위치에서 QoS 큐 스케줄링 동작을 설정할 수 있게 합니다. 큐 스케줄링은 혼잡 상황에서 서로 다른 우선순위 큐의 패킷이 어떻게 전달되는지 결정합니다.

스위치는 엄격한 우선순위 스케줄링 모드를 지원하여, 우선순위가 높은 트래픽이 항상 낮은 우선순위 트래픽보다 먼저 전송되도록 보장합니다. 관리자는 중요한 애플리케이션에 대한 서비스 품질을 보장하기 위해 포트별로 큐 스케줄링을 활성화할 수 있습니다.

4.15.2 코스 리맵

Path:

Config > Basic Service > QOS > Cos Remap

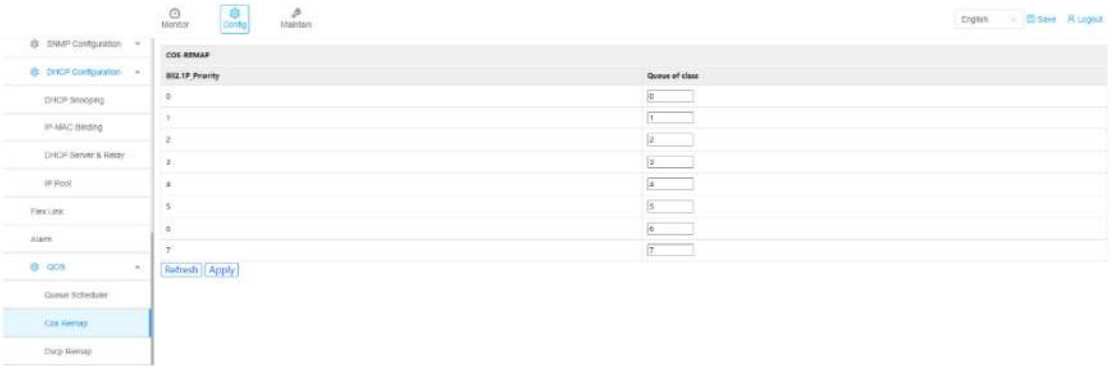

그림 4-15-2 코스 리맵 페이지

이 페이지는 관리자가 IEEE 802.1p 우선순위 값과 내부 스위치 큐 간의 매핑을 구성할 수 있게 합니다. CoS 우선순위를 재매핑함으로써 패킷을 VLAN 우선순위 태그에 따라 서로 다른 포워딩 큐로 분류할 수 있습니다.

이 메커니즘은 트래픽의 차별화된 처리를 가능하게 하고 중요한 애플리케이션의 서비스 품질을 향상시킵니다.

4.15.3 DSCP 재배치

Path:

기본 서비스 > QOS > DSCP 리맵 > 구성

그림 4-15-3 DSCP 리맵 페이지

이 페이지는 관리자가 IP DSCP 값과 내부 스위치 큐 간의 매핑을 구성할 수 있게 합니다. DSCP 값을 재매핑함으로써 IP 패킷은 서비스 클래스에 따라 서로 다른 포워딩 큐로 분류할 수 있습니다.

DSCP 재매핑은 세밀한 트래픽 우선순위 지정을 가능하게 하며, 음성과 비디오와 같은 지연에 민감한 애플리케이션에서 서비스 품질을 보장합니다.

4.16 ERPS 구성

4.16.1 기본 구성

Path:

기본 서비스 > 구성 > ERPS 구성 > 기본 구성

그림 4-16-1 기본 구성 페이지

이 페이지에서는 관리자가 전역 활성화 제어, 인스턴스 생성, 인스턴스 정보 표시 등 기본 ERPS 설정을 구성할 수 있습니다. ERPS 는 ITU-T G.8032 규정을 준수하는 이더넷 링 토폴로지에 대한 빠른 보호 스위칭을 제공합니다.

관리자는 ERPS 인스턴스를 생성하고 설정하기 전에 전 세계적으로 ERPS 를 활성화해야 합니다.

4.16.2 인스턴스 구성

Path:

구성 > 기본 서비스 > ERPS 구성 > 인스턴스 구성

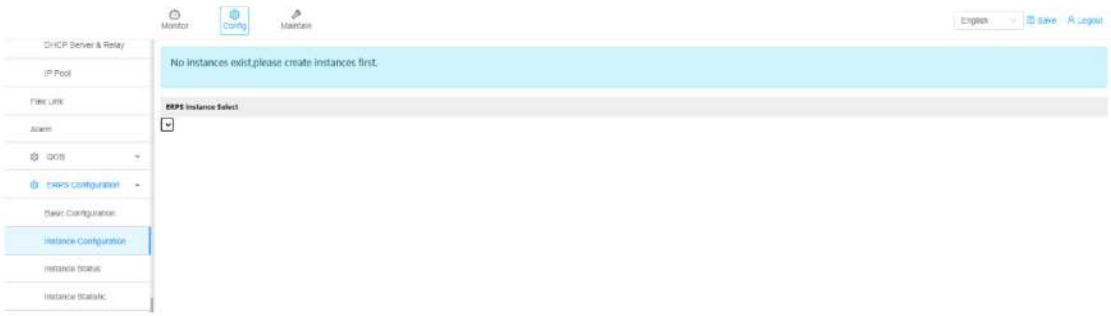

그림 4-16-2 인스턴스 구성 페이지

이 페이지는 관리자가 링 포트, 제어 VLAN, 작업 모드, 타이머 등 ERPS 인스턴스의 상세 매개변수를 설정할 수 있게 합니다.

ERPS 인스턴스가 존재하지 않을 경우, 기본 구성 페이지에서 인스턴스를 먼저 생성해야 한다는 메시지가 표시됩니다.

4.16.3 인스턴스 상태

Path:

Config > Basic Service > ERPS 구성 > 인스턴스 상태

그림 4-16-3 인스턴스 상태 페이지

이 페이지는 링 상태, 보호 상태, 포트 역할을 포함한 ERPS 인스턴스의 실시간 상태를 보여줍니다. 관리자는 이 페이지를 통해 링 상태를 모니터링하고 보호 전환이 발생했는지 확인할 수 있습니다.

4.16.4 인스턴스 통계량

Path:

구성 > 기본 서비스 > ERPS 구성 > 인스턴스 통계

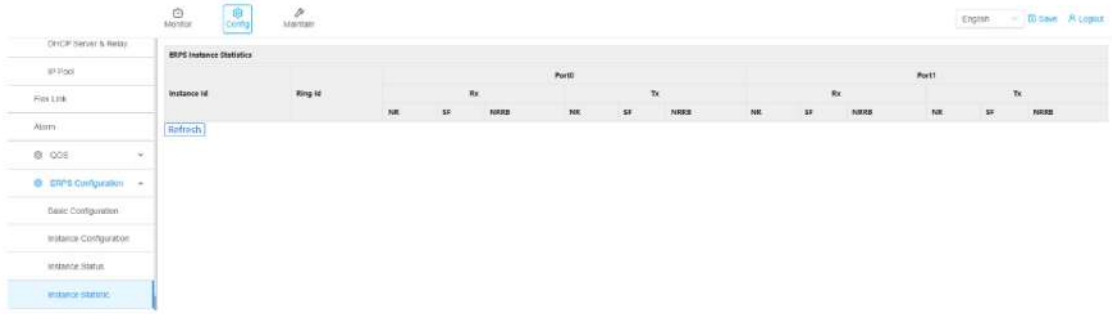

그림 4-16-4 인스턴스 통계 페이지

이 페이지는 각 인스턴스에 대한 ERPS 제어 패킷 통계를 보여주며, 링 포트에서 송수신된 R-APS 메시지를 포함합니다. 이 통계는 관리자가 링 동작을 분석하고 보호 스위칭 이벤트를 진단하는 데

도움을 줍니다.

4.17 LLDP

4.17.1 LLDP 정보

Path:

LLDP > 기본 서비스 > 구성 > LLDP 정보

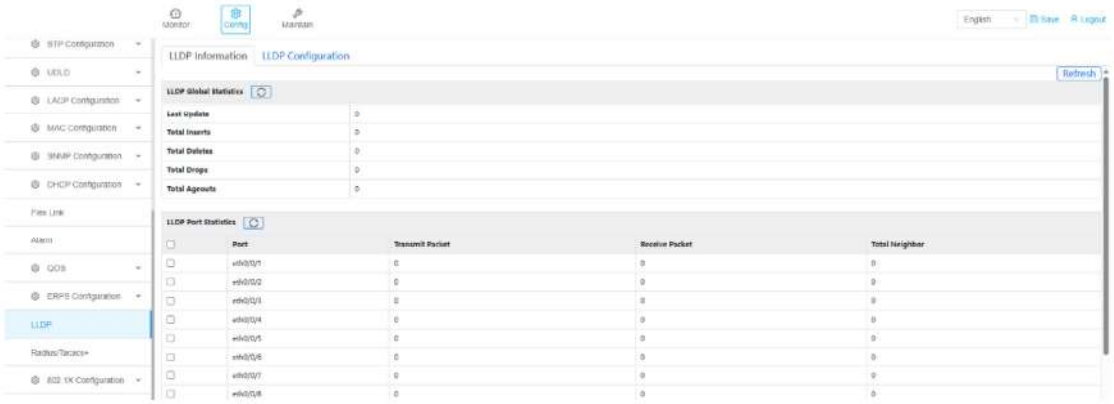

그림 4-17-1 LLDP 정보 페이지

이 페이지는 전역 LLDP 상태와 포트별 LLDP 통계를 보여줍니다. LLDP 는 네트워크 장치가 직접 연결된 이웃에게 자신의 신원과 기능을 광고하고 정보를 학습할 수 있게 합니다. 관리자는 이 페이지를 통해 LLDP 운영 상태, 패킷 전송 및 수신 통계, 그리고 각 포트에서 발견된 이웃 위치를 모니터링할 수 있습니다.

4.17.2 LLDP 구성

Path:

LLDP > LLDP 구성 > 기본 서비스 > 구성

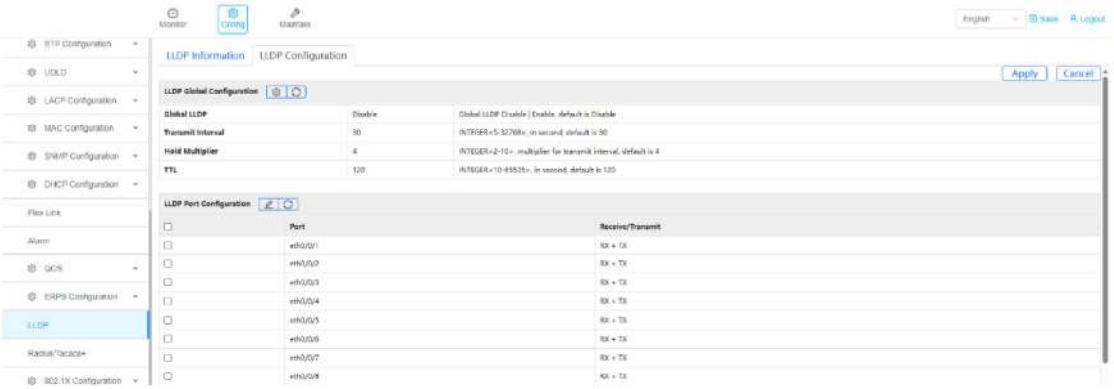

그림 4-17-2 LLDP 구성 페이지

이 페이지는 관리자가 전역 LLDP 매개변수와 포트별 LLDP 수신/송수신 동작을 설정할 수 있게 합니다. LLDP 는 장치가 인접 장치를 발견하고 토폴로지 관리를 위한 정보를 교환할 수 있게 합니다. 관리자는 LLDP 를 전역적으로 활성화하거나 비활성화하고, 전송 간격과 타이머를 조정하며, 개별 포트에서 LLDP 동작을 제어할 수 있습니다.

4.18 radius/Tacacs+

4.18.1 radius 서버

Path:

Radius/Tacacs+ > Radius 서버 > 기본 서비스 > 구성

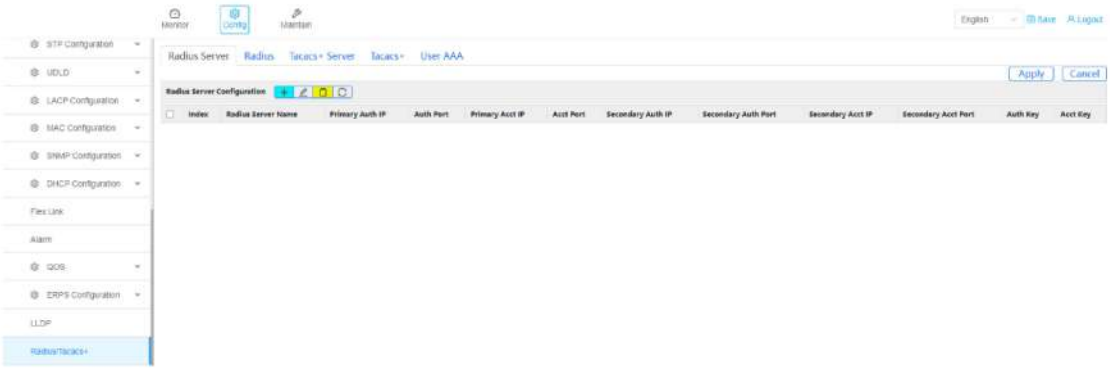

그림 4-18-1 Radius 서버 페이지

이 페이지는 관리자가 인증, 권한 부여 및 회계(AAA)를 위한 RADIUS 서버 매개변수를 설정할 수 있게 합니다. 스위치는 인증 및 회계 요청을 구성된 RADIUS 서버로 전달하여 중앙 집중식 사용자 관리를 가능하게 합니다.

주 및 보조 RADIUS 서버는 신뢰성을 높이기 위해 구성할 수 있습니다.

4.18.2 radius

Path:

기본 서비스 > Radius/Tacacs+ > Radius> 설정

그림 4-18-2 반경 페이지

이 페이지는 관리자가 스위치의 사용자 인증 정책을 설정할 수 있게 해줍니다. 관리자는 RADIUS, TACACS+ 또는 로컬 인증 방식을 선택하여 사용자 접근을 제어할 수 있습니다.

기본 인증 서버가 사용 불가능할 경우 관리 접근 권한을 보장하기 위해 백업 인증 방법을 설정할 수 있습니다.

4.18.3 Tacacs+ 서버

Path:

Config > Basic Service > Radius/Tacacs+ > Tacacs+ Server

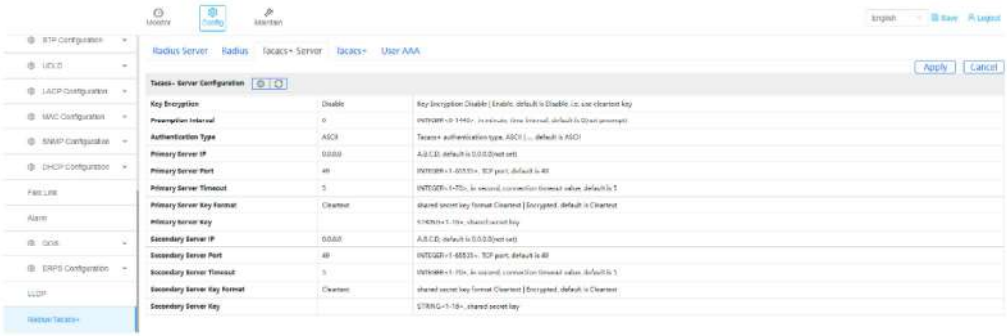

그림 4-18-3 Tacacs+ 서버 페이지

이 페이지는 관리자가 중앙 인증 및 권한을 위해 TACACS+ 서버 매개변수를 설정할 수 있게 합니다. TACACS+는 장치 관리 접근 제어에 일반적으로 사용되며 명령어 수준의 권한 부여를 지원합니다.

주 및 보조 TACACS+ 서버는 신뢰할 수 있는 인증 서비스를 보장하기 위해 구성할 수 있습니다.

4.18.4 Tacacs+

Path:

Config > Basic Service > Radius/Tacacs+ > Tacacs+

그림 4-18-4 Tacacs+ 페이지

이 페이지는 관리자가 TACACS+ 기반 사용자 인증, 권한 부여 및 회계 정책을 구성할 수 있게 합니다. 활성화되면 사용자 로그인 인증은 TACACS+ 서버에서 처리됩니다.

TACACS+ 서버가 사용 불가능할 경우 관리 접근 권한을 보장하기 위해 백업 인증 방법을 설정할 수 있습니다.

4.18.5 사용자 AAA

Path:

Radius/Tacacs+ > USER AAA > 기본 서비스 > 구성

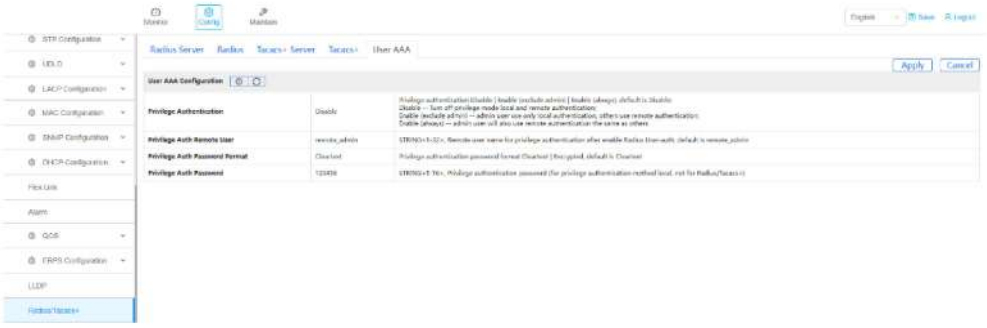

그림 4-18-5 사용자 AAA 페이지

이 페이지는 관리자가 권한 사용자 인증 설정을 구성할 수 있게 해줍니다. 권한 사용자는 일반적으로 고수준 장치 관리 접근에 사용됩니다.

관리자는 권한 인증을 활성화하고, 원격 권한 사용자 이름을 정의하며, 비밀번호 형식을 설정하고, 로컬 권한 비밀번호를 설정할 수 있습니다.

4.19 802.1X 구성

4.19.1 기본 구성

Path:

기본 서비스 > 구성 >802.1X 구성 > 기본 구성

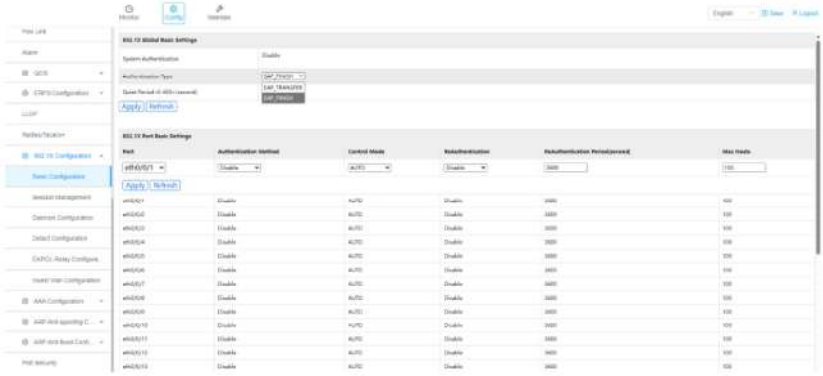

그림 4-19-1 기본 구성 페이지

이 페이지는 관리자가 전역 및 포트 레벨 802.1X 인증 설정을 설정할 수 있게 해줍니다. 802.1X 는 RADIUS 서버를 통해 장치를 인증하여 포트 기반 네트워크 접근 제어를 제공합니다.

관리자는 시스템 인증을 활성화하고, EAP 처리를 구성하며, 인증 전후 포트 동작을 결정할 수 있는

포트 제어 모드를 정의할 수 있습니다.

4.19.2 세션 관리

Path:

구성 > 기본 서비스 >802.1X 세션 관리 > 구성

그림 4-19-2 세션 관리 페이지

이 페이지는 활성 802.1X 인증 세션을 표시하고 관리합니다. 관리자는 포트, VLAN, MAC 주소, 사용자 이름, 로그인 시간 등 인증된 장치를 확인할 수 있습니다.

활성 세션은 수동으로 종료하여 연결된 장치의 재인증을 강제할 수 있습니다.

4.19.3 데몬 구성

Path:

Config > Basic Service >802.1X Configuration > Daemon Configuration

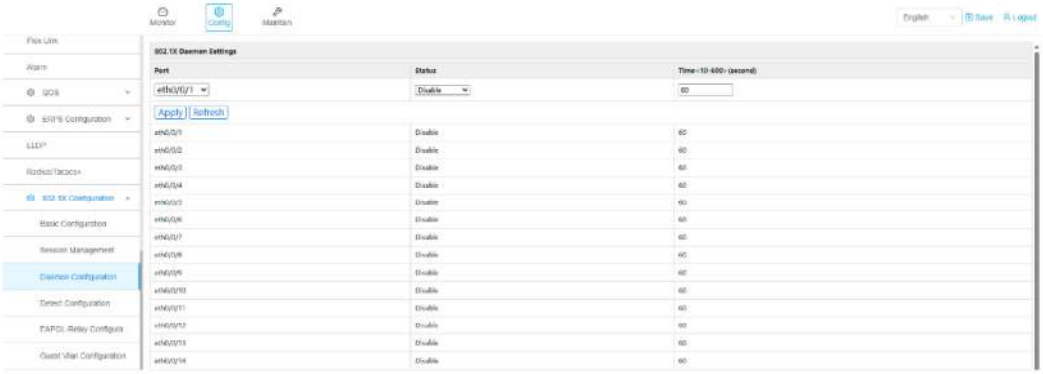

그림 4-19-3 데몬 구성 페이지

이 페이지는 관리자가 각 포트에서 802.1X 데몬 상태와 모니터링 간격을 설정할 수 있게 해줍니다. 데몬은 802.1X 접근 제어의 지속적인 집행을 보장하기 위해 연결된 장치의 인증 상태를 주기적으로 확인합니다.

4.19.4 구성 감지

Path:

구성 > 기본 서비스 >802.1X 구성 > 구성 감지

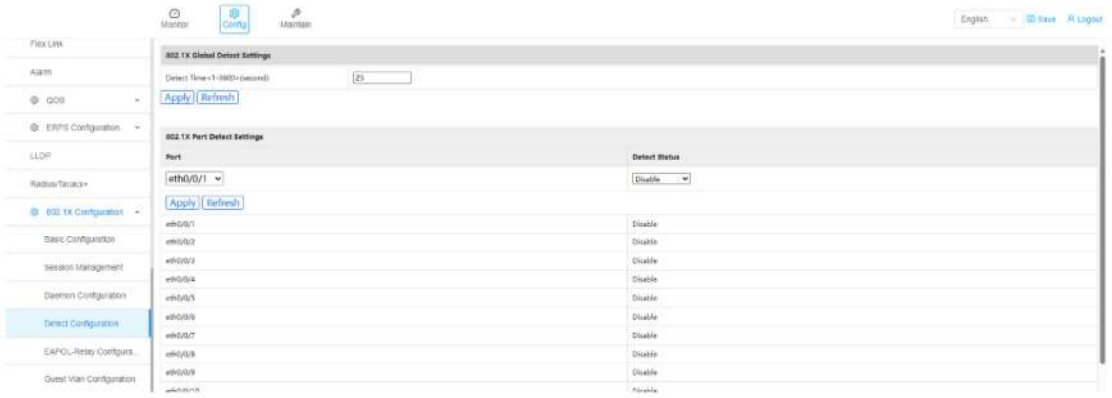

그림 4-19-4 구성 감지 페이지

이 페이지에서는 관리자가 802.1X 에 대해 전역 및 포트별 감지 설정을 설정할 수 있습니다. 탐지 메커니즘은 인증 트리거 또는 재트리거 여부를 주기적으로 포트 상태를 확인합니다. 적절한 감지 구성은 새로 연결되었거나 비정상적인 장치에 대해 신속한 인증을 보장하는 데 도움을 줍니다.

4.19.5 EAPOL-릴레이 구성

Path:

Config > Basic Service >802.1X Configuration > EAPOL-Relay Configuration

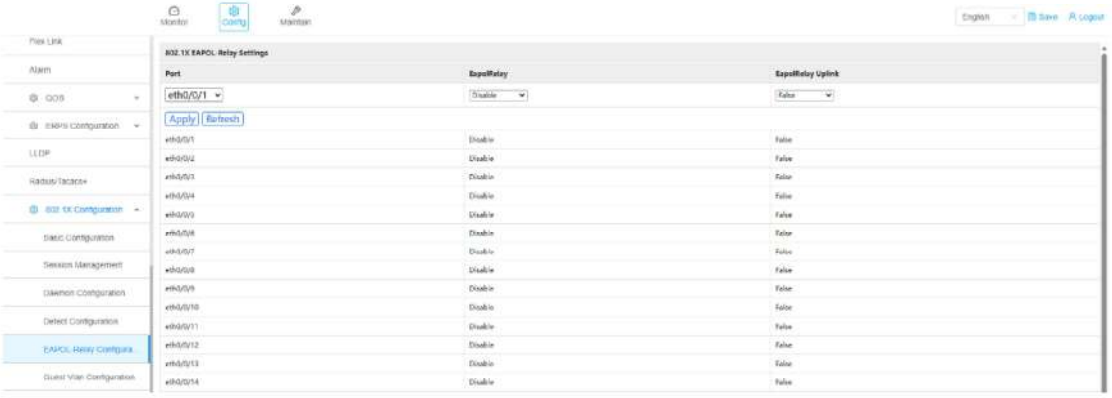

그림 4-19-5 EAPOL-릴레이 구성 페이지

이 페이지는 관리자가 EAPOL 릴레이 설정을 설정할 수 있게 해줍니다. EAPOL 릴레이는 중앙 인증 배포에서 802.1X 인증 패킷을 액세스 포트와 업링크 포트 간에 전달할 수 있게 합니다. 관리자는 어떤 포트가 EAPOL 패킷을 중계하고 어떤 포트가 인증 트래픽의 업링크 역할을 하는지 정의할 수 있습니다.

4.19.6 게스트 VLAN 구성

Path:

Config > Basic Service >802.1X Configuration > Guest Vlan Configuration

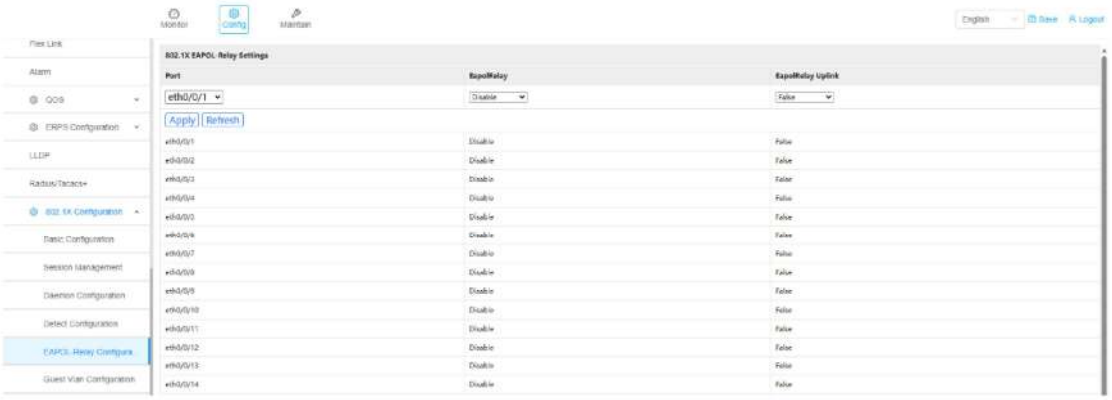

그림 4-19-6 게스트 VLAN 구성 페이지

이 페이지에서는 관리자가 802.1X 용 게스트 VLAN 설정을 구성할 수 있습니다. 장치가 인증되지 않았거나 802.1X 를 지원하지 않을 때, 제한적인 네트워크 접근을 제공하기 위해 일시적으로 게스트 VLAN 에 배치할 수 있습니다.

인증이 성공하면 포트는 게스트 VLAN 에서 권한이 부여된 VLAN 으로 전환됩니다.

4.20 AAA 구성

4.20.1 도메인 구성

Path:

구성 > 기본 서비스 > AAA 구성 > 도메인 구성

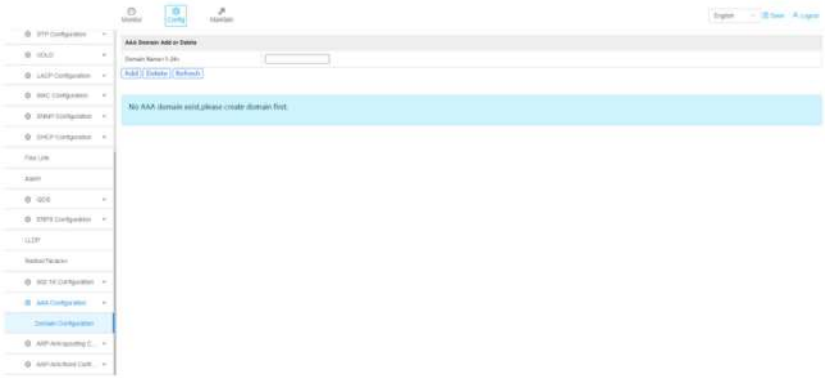

그림 4-20-1 도메인 구성 페이지

이 페이지는 관리자가 AAA 도메인을 생성하고 관리할 수 있게 해줍니다. AAA 도메인은 인증, 권한 부여 및 회계 정책에 대한 논리적 범위를 정의합니다.

AAA 관련 기능을 구성하기 전에 최소 하나의 AAA 도메인을 생성해야 합니다.

4.21 ARP 안티 스푸핑 구성

4.21.1 기본 구성

Path:

기본 서비스 > 구성 > ARP 안티 스푸핑 구성 > 기본 구성

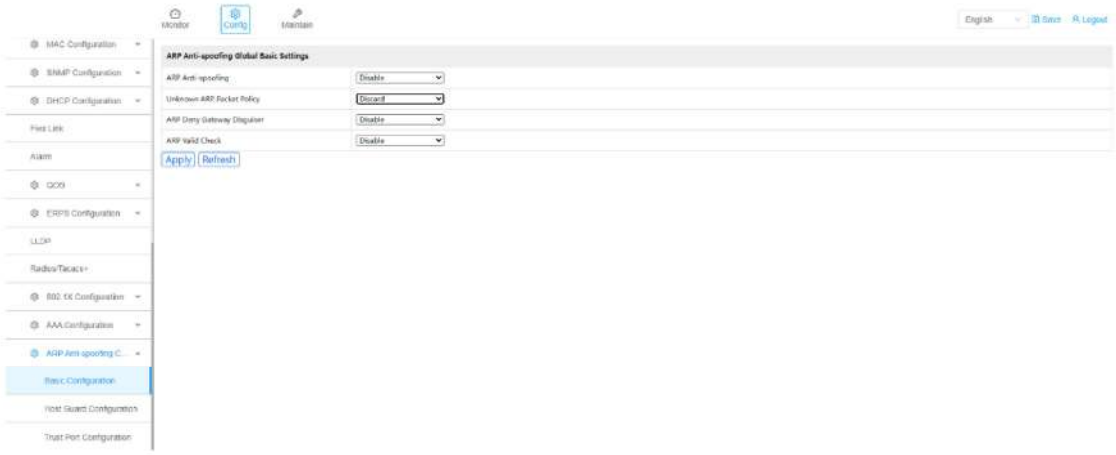

그림 4-21-1 기본 구성 페이지

이 페이지에서는 관리자가 전역 ARP 안티스푸핑 설정을 설정할 수 있습니다. ARP 안티 스푸핑은 ARP 스푸핑 공격, 게이트웨이 사칭, 중간자 위협으로부터 네트워크를 보호합니다.

관리자는 전역 ARP 안티 스푸핑을 활성화하고, 알 수 없는 ARP 패킷 처리 방식을 정의하며, 추가적인 ARP 검증 메커니즘을 활성화할 수 있습니다.

4.21.2 호스트 가드 구성

Path:

구성 > 기본 서비스 > ARP 안티 스푸핑 구성 > 호스트 가드 구성

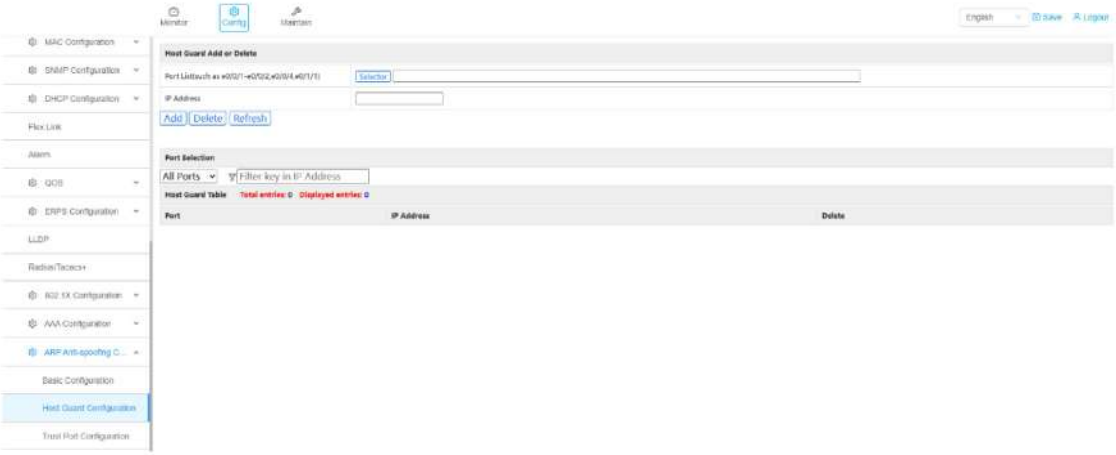

그림 4-21-2 호스트 가드 구성 페이지

이 페이지는 관리자가 ARP 호스트 가드 규칙을 구성할 수 있게 해줍니다. 호스트 가드는 특정 IP 주소를 지정된 포트에 묶어, 호스트가 IP 주소를 스푸핑하거나 ARP 공격을 실행하는 것을 방지합니다. 설정된 포트-IP 바인딩과 일치하는 ARP 패킷만 허용됩니다.

4.21.3 트러스트 포트 구성

Path:

Config > 기본 서비스 > ARP 안티스푸핑 구성 > Trust Port Configuration

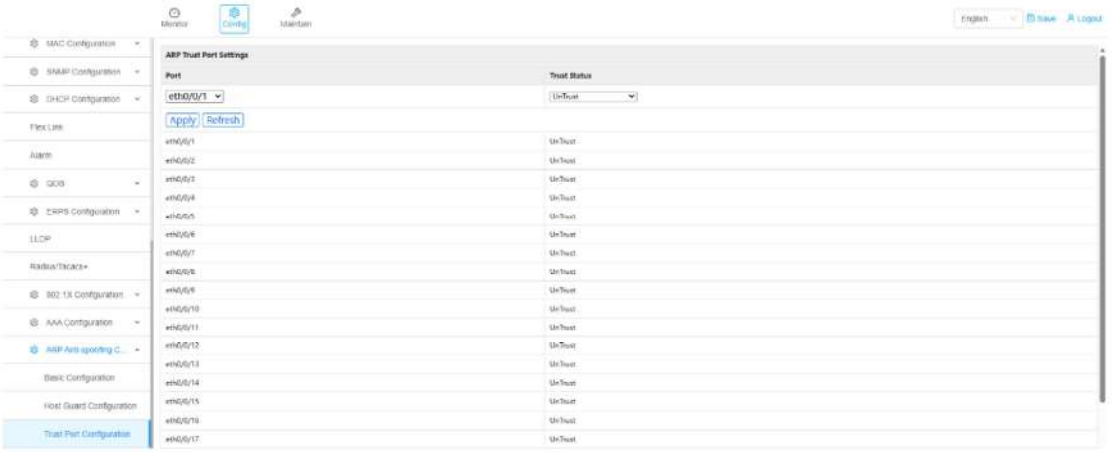

그림 4-21-3 트러스트 포트 구성 페이지

이 페이지는 관리자가 ARP 안티스푸핑을 위해 신뢰할 수 있는 포트를 설정할 수 있게 해줍니다. 신뢰할 수 있는 포트에서 수신된 ARP 패킷은 합법적인 것으로 간주되며 엄격한 ARP 검사의 대상이 아닙니다.

신뢰 포트는 일반적으로 게이트웨이, 라우터 또는 기타 신뢰할 수 있는 네트워크 장치에 연결된 업링크 포트입니다.

4.22 ARP Anti-flood 구성

4.22.1 기본 구성

Path:

기본 서비스 > 구성 > ARP 안티 스푸핑 구성 > 기본 구성

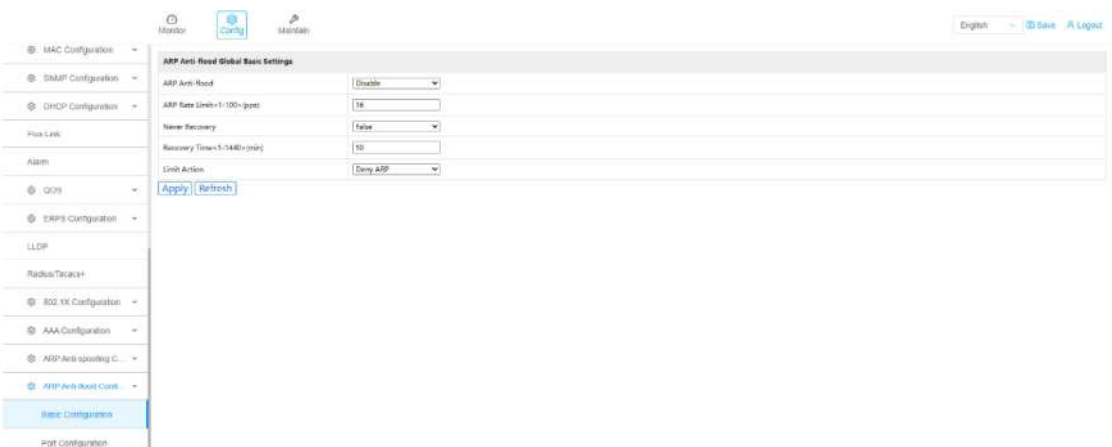

그림 4-22-1 기본 구성 페이지

이 페이지에서는 관리자가 전역 ARP Anti-flood 설정을 구성할 수 있습니다. ARP 안티플러드는 잘못된 호스트나 악의적인 공격으로 인해 발생할 수 있는 과도한 ARP 트래픽으로부터 스위치를 보호합니다. 관리자는 ARP 속도 제한을 활성화하고, 복구 동작을 정의하며, 속도 한도를 초과할 때 행동을 지정할 수 있습니다.

4.22.2 포트 구성

Path:

구성 > 기본 서비스 > ARP 안티스푸핑 구성 > 포트 구성

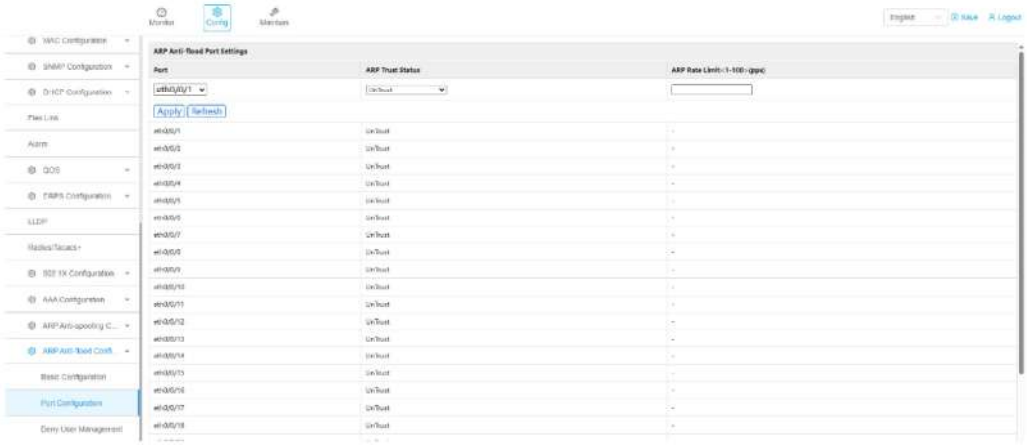

그림 4-22-2 포트 구성 페이지

이 페이지에서는 관리자가 포트 레벨 ARP 안티플러드 설정을 구성할 수 있습니다. 관리자는 신뢰할 수 있는 포트와 신뢰할 수 없는 포트를 정의할 수 있으며, 선택적으로 포트별 ARP 속도 제한을 적용할 수 있습니다.

포트 수준 속도 제한은 설정 시 전역 설정을 무시합니다.

4.22.3 사용자 관리 거부

Path:

Config > Basic Service > ARP 안티스푸핑 구성 > 사용자 관리 거부

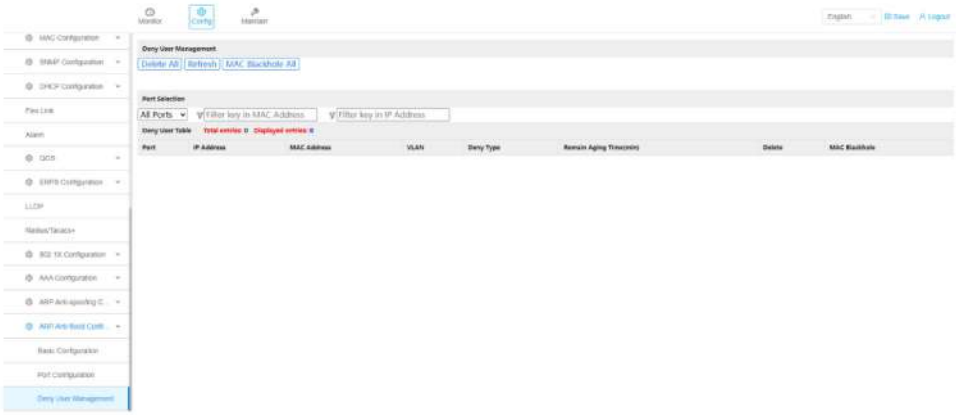

그림 4-22-3 사용자 관리 거부 페이지

이 페이지는 ARP Anti-flood 때문에 접근이 거부된 사용자를 표시하고 관리합니다. 관리자는 거부된 사용자를 확인하거나, 거부 항목을 삭제하거나, 장기 차단을 위해 MAC 주소를 블랙리스트에 추가할 수 있습니다.

4.23 포트 보안

Path:

기본 서비스 > 포트 보안 > 구성

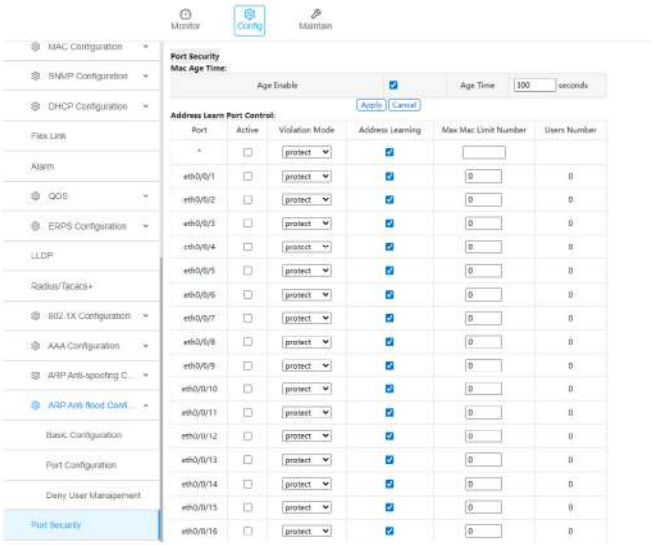

그림 4-23 포트 보안 페이지

이 페이지는 관리자가 포트 보안 설정을 설정할 수 있게 해줍니다. 포트 보안은 한 포트에서 학습되는 MAC 주소 수를 제한하고, 무단 장치가 네트워크에 접근하는 것을 방지합니다.

MAC 노화 및 위반 처리는 보안과 운영 안정성을 모두 보장하기 위해 구성할 수 있습니다.

5. Advanced Service

5.1 DNS 클라이언트

Path:

Config > Advanced Service > DNS 클라이언트

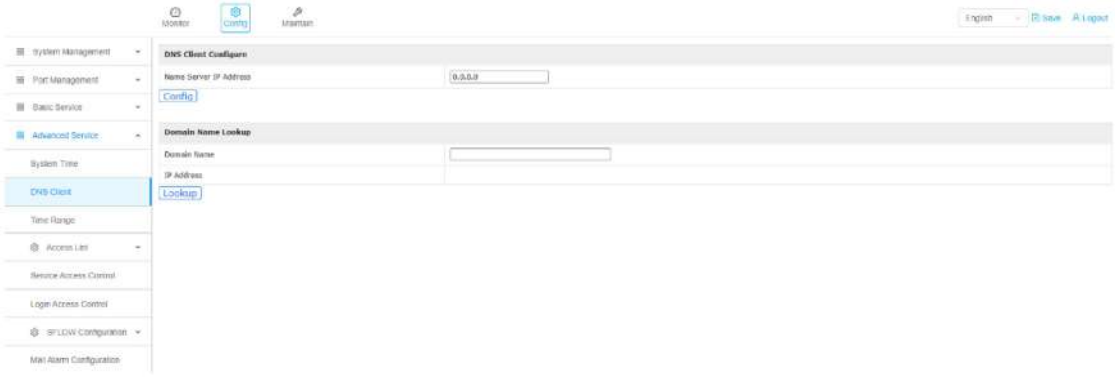

그림 5-1 DNS 클라이언트 페이지

이 페이지는 관리자가 스위치의 DNS 클라이언트 설정을 설정할 수 있게 해줍니다. DNS 클라이언트는 스위치가 도메인 이름을 IP 주소로 분해하여 시스템 관리 및 문제 해결 목적을 제공합니다. 관리자는 DNS 서버를 구성하고 기기에서 직접 도메인 이름 조회를 수행할 수 있습니다.

5.2 시간 범위

Path:

Config > Advanced Service > Time Range

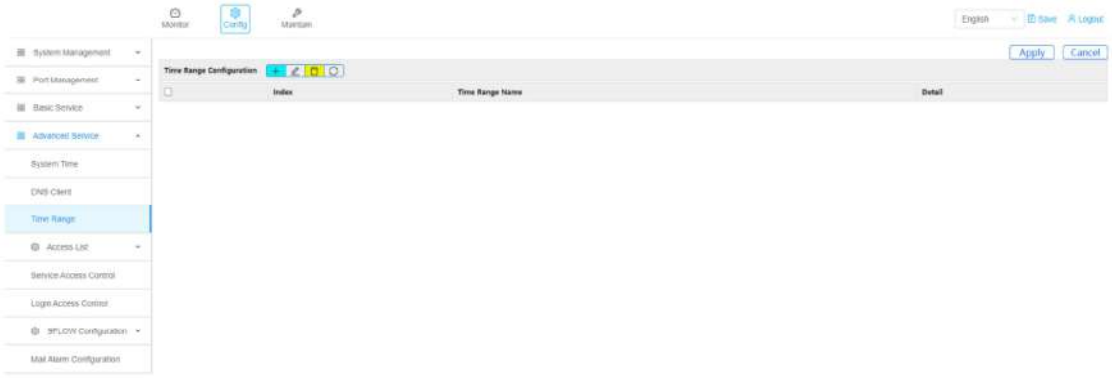

그림 5-2 시간 범위 페이지

이 페이지는 관리자가 시간 범위 객체를 생성하고 관리할 수 있게 해줍니다. 시간 범위는 정책이나 서비스가 활성화되는 특정 기간을 정의합니다. 시간 범위는 ACL, 접근 제어, 로그인 정책 등 다른 기능으로 참조하여 시간 기반 제어를 가능하게 합니다.

5.3 접근 목록

5.3.1 분류자

Path:

Config > Advanced Service > Access List > Classifier

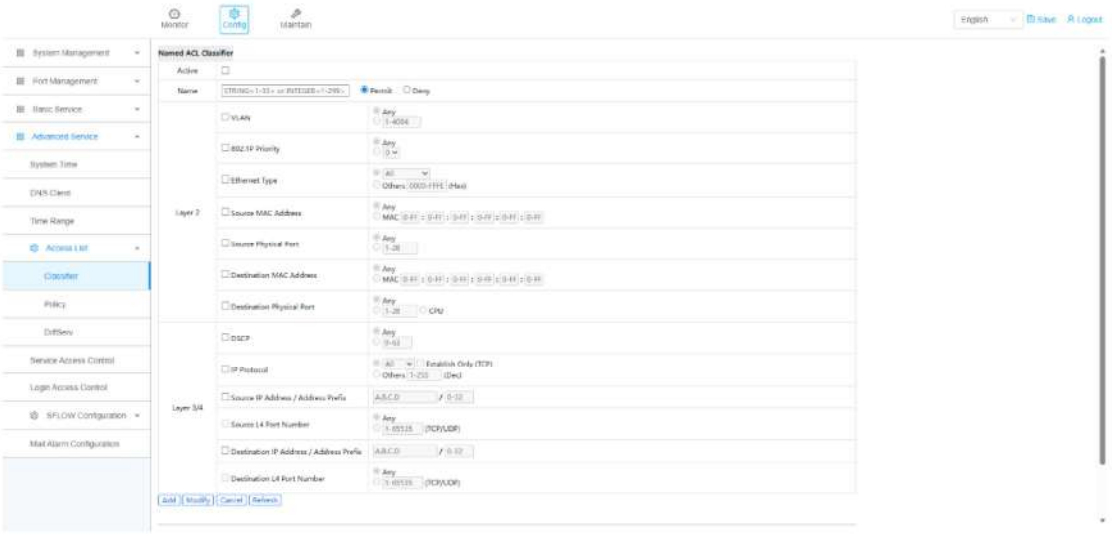

그림 5-3-1 분류기 페이지

이 페이지는 관리자가 2 계층 및 3/4 계층 필드를 기반으로 트래픽을 매칭하는 데 사용되는 ACL 분류기를 정의할 수 있게 합니다. 분류기는 특정 트래픽 흐름을 식별하며, 효과를 내기 위해 정책에 바인딩되어야 합니다.

5.3.2 정책

Path:

Config > Advanced Service > Access List > Policy

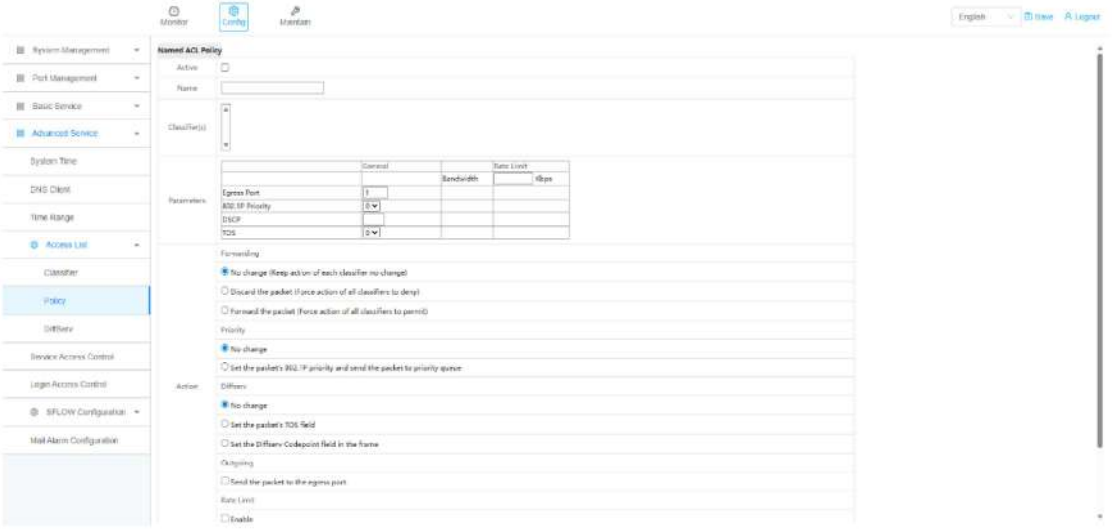

그림 5-3-2 정책 페이지

이 페이지는 관리자가 ACL 정책을 구성할 수 있게 해줍니다. 정책은 하나 이상의 분류기를 결합하여

전달, 폐기, 우선순위 표시, 매칭된 트래픽에 대한 속도 제한과 같은 동작을 정의합니다.

정책은 ACL 의 실행 구성 요소로, 매칭된 트래픽을 어떻게 처리하는지를 결정합니다.

5.3.3 DiffServ

Path:

Config > Advanced Service > Access List > DiffServ

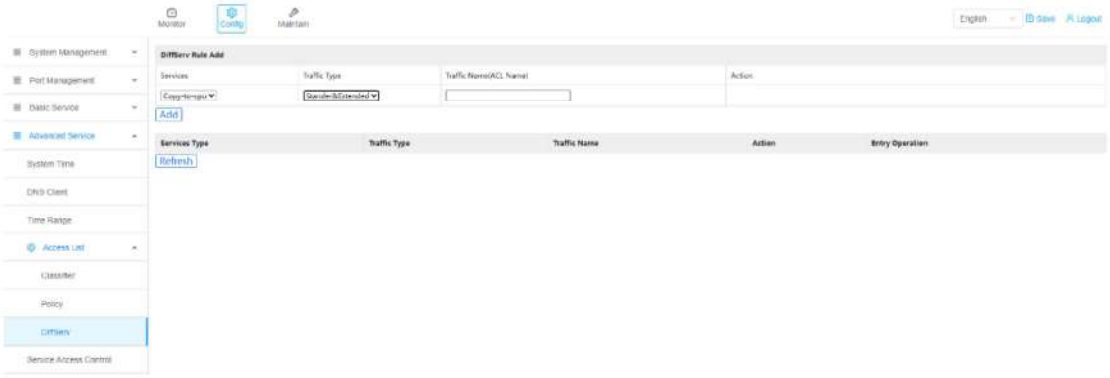

그림 5-3-3 DiffServ 페이지

이 페이지는 관리자가 DiffServ 규칙을 설정할 수 있게 해줍니다. DiffServ 규칙은 CPU 로 패킷을 복사하거나, 트래픽을 리디렉션하거나, VLAN 태그를 삽입하거나 재작성하거나, 통계 수집과 같은 특정 동작을 분류된 트래픽에 적용합니다.

DiffServ 는 ACL 분류기와 협력하여 차별화된 서비스 처리를 제공합니다.

5.4 로그인 접근 제어

Path:

Config > Advanced Service > Access List > 로그인 접근 제어

그림 5-4 로그인 접근 제어 페이지

로그인 접근 제어 구성

이 페이지는 관리자가 로그인 접근 제어 규칙을 설정할 수 있게 해줍니다. 관리자는 소스 IP 주소와

서비스 유형을 지정함으로써 SNMP, 웹, 텔넷과 같은 관리 인터페이스를 통해 어떤 호스트가 장치에 접근할 수 있는지 제한할 수 있습니다.

로그인 접근 제어는 무단 관리 접근을 방지하여 기기 보안을 강화합니다.

5.5 SFLOW 구성

5.5.1 수집기 구성

Path:

구성 > 고급 서비스 > SFLOW 구성 > 수집기 구성

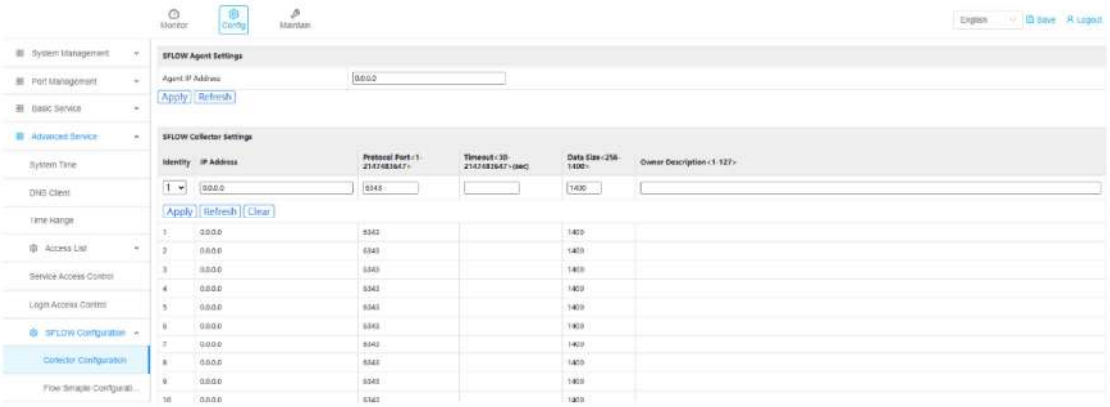

그림 5-5-1 컬렉터 구성 페이지

이 페이지는 관리자가 sFlow 에이전트 설정과 sFlow 수집기를 구성할 수 있게 해줍니다. 장치는 교통 데이터를 샘플링하여 하나 이상의 구성된 수집기로 전송하여 트래픽 분석 및 모니터링을 수행합니다.

5.5.2 플로우 스메이플 구성

Path:

Config > Advanced Service > SFLOW Configuration > Flow Smaple Configuration

그림 5-5-2 플로우 스맵플 구성 페이지

이 페이지는 관리자가 포트별로 플로우 샘플링을 구성할 수 있게 해줍니다. 활성화되면 장치는 지정된 샘플링 속도에 따라 트래픽을 샘플링하고, 샘플링된 데이터를 구성된 sFlow 수집기로 전송합니다.

5.5.3 카운터 구성

Path:

Config > Advanced Service > SFLOW Configuration > Counter Configuration

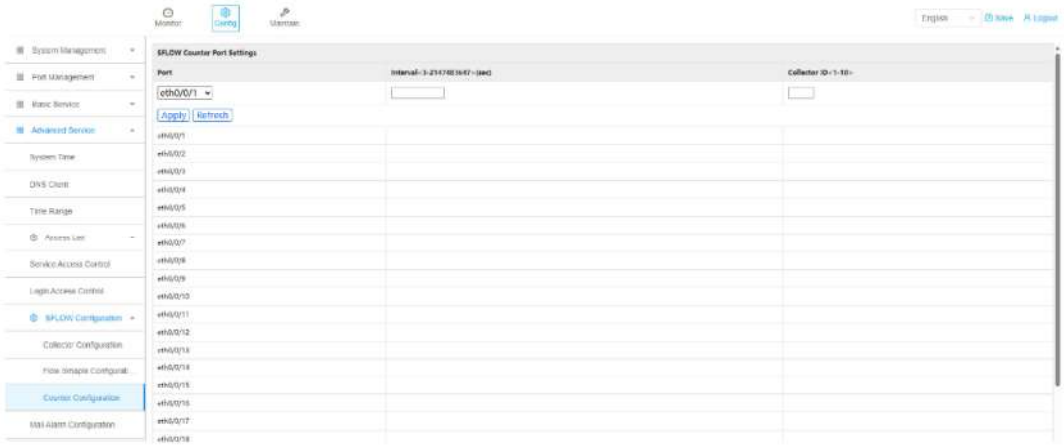

그림 5-5-3 카운터 구성 페이지

이 페이지는 관리자가 포트별로 카운터 샘플링을 구성할 수 있게 합니다. 장치는 주기적으로 포트 카운터 통계를 수집하여 지정된 간격에 맞게 구성된 sFlow 수집기로 전송합니다.

카운터 샘플링은 패킷 샘플링 없이 장기 트래픽 통계를 제공합니다.

5.6 메일 알람 구성

Path:

구성 > 고급 서비스 > SFLOW 구성 > 메일 알람 구성

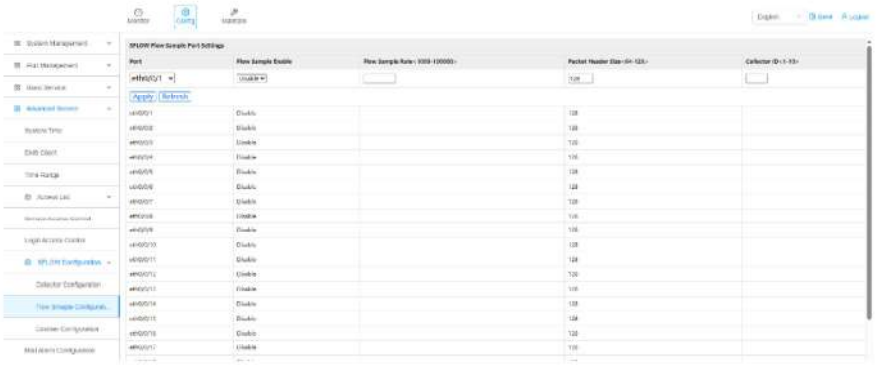

그림 5-6 우편 경보 구성 페이지

이 페이지는 관리자가 포트별로 플로우 샘플링을 구성할 수 있게 해줍니다. 플로우 샘플링이 활성화되면, 장치는 지정된 샘플링 속도에 따라 패킷을 샘플링하여 구성된 sFlow 수집기로 샘플링한 데이터를 전송합니다.

플로우 샘플링은 트래픽 분석과 네트워크 모니터링에 사용되며, 정상적인 포워딩 성능에는 영향을

주지 않습니다.