SFC9448A

L3 기가비트 매니지먼트 스위치

10G SFP+ 44-슬롯, 40G QSFP28 6-슬롯

웹 사용자 설명서

목 차

1 소개

1.1 제품소개

SFC9448A 스위치는 고대역폭 액세스 및 이더넷 다중 서비스 통합을 제공하도록 설계된 차세대 에너지 절약형 GE 스위치입니다. 최첨단 하드웨어와 VRP(Versatile Routing Platform) 소프트웨어를 기반으로 하는 SFC9448A 스위치는 10Gbit/s 업스트림 전송을 수용하기 위해 대용량 스위칭 용량, 높은 신뢰성(이중 전원 슬롯 및 하드웨어 이더넷 OAM), 고밀도 GE 포트를 제공합니다. 또한 EEE(Energy Efficient Ethernet) 및 iStack 을 지원합니다. SFC9448A 스위치는 광범위한 엔터프라이즈 네트워크 시나리오에서 사용할 수 있습니다. 예를 들어 캠퍼스 네트워크의 집선 스위치로 기능할 수 있습니다.

1.2 제품사양

○ 물리적인 포트

- 1G/10G Base-X 48 슬롯
- 40G QSFP 슬롯 6개
- 스위치 기본 관리 와 설치용 RS-232 콘솔 인터페이스
- 관리 포트(Out-of-band) 10/100/1000Base-T Gigabit RJ45 copper

제품 특징

유연한 이더넷 네트워킹

● 기존의 STP(Spanning Tree Protocol), RSTP(Rapid Spanning Tree Protocol), MSTP(Multiple Spanning Tree Protocol)를 지원하는 것 외에도 스마트 이더넷 보호(기술 및 업계 최신 이더넷 링 보호 스위치)와 함께 설계되었습니다. SEP 는 이더넷 링크 계층 전용 링 보호 프로토콜로, 오픈 링 토폴로지, 폐쇄 링 토폴로지, 계단식 링 토폴로지 등 다양한 링 네트워크 토폴로지에 적용됩니다. 이 프로토콜은 안정적이고 유지 관리가 용이하며 50ms 이내에 빠른 보호 전환을 구현합니다. ERPS 는 ITU-TG.8032 에 정의되어 있으며 기존의 이더넷 MAC 및 브리징 기능을 기반으로 하는 밀리 초 레벨 보호 스위칭을 구현합니다.

● 업링크의 백업을 구현하는 SmartLink 를 지원합니다. 하나의 스위치로 여러 개의 Aggregation 스위치에 연결할 수 있어 액세스 장치의 안정성이 크게 향상됩니다.

● 링크 결함을 빠르게 감지하기 위해 이더넷 OAM(IEEE 802.3ah/802.1ag)을 지원합니다.

다각적인 보안 통제

● 포트별로 802.1X 인증, MAC 주소 인증 및 하이브리드 인증을 지원하며 VLAN IF 인터페이스별로 포털 인증을 지원하며 사용자에게 동적 정책 제공(VLAN, QoS, ACL)을 구현합니다.

● DoS 공격 및 사용자 대상 공격으로부터 방어하는 일련의 메커니즘을 제공합니다. DoS 공격은 스위치를 대상으로 하며 SYN 홍수, Land, 스머프 및 ICMP 홍수 공격이 포함됩니다. 사용자 대상 공격에는 위조 DHCP 서버 공격, IP/MAC 주소 스푸핑, DHCP 요청 플러딩 및 DHCP CHADR 값 변경이 포함됩니다.
● DHCP 스누핑 바인딩 테이블을 설정 및 유지 관리하고 테이블 항목과 일치하지 않는 패킷을 삭제합니다. DHCP 스누핑 신뢰할 수 있는 포트 기능을 사용하면 사용자가 인증된 DHCP 서버에만 연결할 수 있습니다.
● 엄격한 ARP 학습을 지원합니다. 이 기능은 ARP 스푸핑 공격자가 ARP 항목을 모두 소진하지 못하도록 방지합니다. 그리하여 사용자가 인터넷에 정상적으로 연결할 수 있습니다.

간편한 작동 및 유지 관리

● 제로 터치 배포, 추가 구성 없이 결함 있는 장치 교체*, USB 기반 배포*, 배치 장치 구성 및 배치 원격 업그레이드를 제공하는 솔루션인 Easy Operation 을 지원합니다.
Easy Operation 솔루션은 기기 구축, 업그레이드, 서비스 프로비저닝 및 기타 관리 및 유지보수 작업을 촉진하고 O&M 비용을 크게 절감합니다. SNMP(Simple Network Management Protocol) V1, V2 및 V3, CLI(명령줄 인터페이스), 웹 기반 네트워크 관리 시스템 또는 SSH(Secure Shell) V2.0 을 사용하여 관리 및 유지 관리할 수 있습니다. 또한 원격 네트워크 모니터링(RMON), 다중 로그 호스트, 포트 트래픽 통계 수집 및 네트워크 품질 분석을 지원하여 네트워크 최적화 및 재구성을 위한 기반을 마련합니다.
● EasyDeploy 기능을 지원합니다. 특히 Commander는 다운스트림 클라이언트의 토폴로지 정보를 수집하고 토폴로지를 기반으로 클라이언트 시작 정보를 Save(저장)합니다. 클라이언트는 설정 변경 없이 교체할 수 있습니다.
설정 및 스크립트를 일괄적으로 클라이언트에 제공할 수 있습니다. 또한 설정 전송 결과를 조회할 수 있습니다. 또한 Commander는 전체 네트워크에서 전력 소비 정보를 수집하고 표시할 수 있습니다.
● GVRP(GARP VLAN 등록 프로토콜)를 사용하여 VLAN 동적 배포, 등록 및 특성 전파를 구현할 수 있습니다. GVRP는 수동 구성 워크로드를 줄이고 올바른 구성을 보장합니다.
● 주 VLAN과 여러 하위 VLAN을 포함하는 MUX VLAN을 지원합니다.
하위 VLAN은 그룹 VLAN과 개별 VLAN으로 분류됩니다. 기본 VLAN의 포트는 하위 VLAN의 포트와 통신할 수 있습니다. 하위 그룹 VLAN의 포트는 서로 통신할 수 있지만 하위 개별 VLAN의 포트는 서로 통신할 수 없습니다. VLAN VCMP(중앙 관리 프로토콜) 및 VLAN 기반 스패닝 트리(VBST) 프로토콜도 지원합니다.
참고: USB 포트가 있는 스위치만 USB 기반 배포를 수행할 수 있습니다.

스태킹

● 지능형 스택(iStack)을 지원합니다. 이 기술은 여러 스위치를 논리적 스위치로 결합합니다.
스택의 멤버 스위치는 이중화 백업을 구현하여 장치 안정성을 높이고 장치 간 링크 집계를 사용하여 링크 안정성을 향상시킵니다.
● 스태킹은 높은 네트워크 확장성을 제공합니다. 멤버 스위치를 스택에 추가하기만 하면 스택의 포트, 대역폭 및 처리 용량을 늘릴 수 있습니다.
● 스태킹은 또한 기기 구성 및 관리를 단순화합니다. 스택을 설정하면 여러 물리적 스위치가 하나의 논리적 디바이스로 가상화됩니다. 스택의 멤버 스위치에 로그인하여 스택의 모든 멤버 스위치를 관리할 수 있습니다.

뛰어난 네트워크 트래픽 분석

● sFlow 기능을 지원합니다. sFlow 표준에 정의된 방법을 사용하여 통과하는 트래픽을 샘플링하고 샘플링된 트래픽을 수집기로 실시간으로 전송합니다. 수집된 트래픽 통계는 통계 보고서를 생성하는 데 사용되며, 기업이 네트워크를 유지 관리하는 데 도움이 됩니다.

지능형 O&M

● 기기 데이터를 실시간으로 수집하여 네트워크 분석기에 전송할 수 있는 원격 측정 기술을 제공합니다. 네트워크 분석기는 지능적인 장애 식별 알고리즘을 기반으로 네트워크 데이터를 분석하고 실시간 네트워크 상태를 정확하게 표시하여 적시에 결함을 효과적으로 구분하고 찾아냄으로써 사용자 환경에 영향을 미치는 네트워크 문제를 정확하게 파악하여 사용자 경험을 정확하게 보장합니다.

● 향상된 eMDI(Media Delivery Index)를 비롯하여 오디오 및 비디오 서비스를 위한 다양한 지능형 O&M 기능을 지원합니다. 이 eDMI 기능을 통해 스위치는 주기적으로 통계를 수행하고 오디오 및 비디오 서비스 지표를 네트워크 분석기 플랫폼에 보고하는 모니터링 노드 역할을 할 수 있습니다. 이러한 방식으로 네트워크 분석기 플랫폼은 모니터링되는 여러 노드의 결과에 따라 오디오 및 비디오 서비스 품질 결함을 신속하게 식별할 수 있습니다.

OPS

● 스위치는 Python 언어 기반의 개방형 프로그램 가능 시스템인 OPS(Open Programmability System)를 지원합니다. IT 관리자는 Python 스크립트를 통해 스위치의 O&M 기능을 프로그래밍하여 신속하게 기능을 혁신하고 지능형 O&M 을 구현할 수 있습니다.

제품 사양

항목	묘사
메모리(RAM)	4 기가바이트
플래시	총 2GB. 사용 가능한 플래시 메모리 크기를 보려면 **display version** 명령을 실행합니다.
평균 무고장 시간(MTBF)	56.87 년
평균 수리 시간(MTTR)	2 시간
가용도	> 0.99999
서비스 포트 서지 보호	해당 사항 없음
전원 공급 장치 서지 보호	AC 전원 모듈 사용: ±6kV(차동 모드), ±6kV(공통 모드)

항목	묘사
	• DC 전원 모듈 사용: ±2kV(차동 모드), ±4kV(공통 모드)
치수(H x W x D)	• 기본 치수(본체에서 돌출된 부분 제외): 43.6mm x 442.0mm x 420.0mm(1.72 인치 x 17.4 인치 x 16.5 인치) • 최대 치수(깊이는 전면 패널의 포트에서 후면 패널의 핸들까지의 거리): 43.6mm x 442.0mm x 446.0mm(1.72 인치 x 17.4 인치 x 17.6 인치)
무게(포장 포함)	9.2kg(20.28 파운드)
스택 포트	• 모든 10GE SFP+ 포트(최대 16 개의 물리적 포트) • 모든 40GE/100GE QSFP28 포트(최대 6 개의 물리적 포트, 100G 라이선스 별도 구매)
RTC	지원
RPS (RPS)	지원되지 않음
PoE	지원되지 않음
정격 전압 범위	• AC 입력: 100 V AC to 240 V AC, 50/60 Hz • 고전압 DC 입력: 240V DC • DC 입력: -48 V DC to -60 V DC
최대 전압 범위	• AC 입력: 90 V AC 에서 290 V AC, 45 Hz 에서 65 Hz • 고전압 DC 입력: 190 V DC to 290 V DC • DC 입력: -38.4 V DC to -72 V DC
최대 전력 소비(100% 처리량, 팬의 최대 속도)	291 와트
일반 전력 소비(트래픽 부하의 30%, ATIS 표준에 따라 테스트됨)	165 와트

항목	묘사
작동 온도	-5-45°C (23-113°F) @고도 0-1800 미터(0- 5906 피트) **메모:** 고도가 1800-5000m(5906-16404 피트)일 때 고도가 1m(1 피트) 증가할 때마다 최고 작동 온도가 1°C(1.8°F)씩 감소합니다. 주변 온도가 0°C(32°F)보다 낮으면 스위치를 시작할 수 없습니다. 스위치의 작동 온도는 QSFP-5G-ER40 광 모듈을 사용할 때 -23°C - 104°C(100°F - 4°F)입니다.
보관 온도	-40 ° C - 70° C
상온에서의 소음(27°C, 음력)	< 65dB(A)
상대 습도	5% - 95%, 비응축
작동 고도	0-5000m(0-16404 피트)
인증	KC 인증
부품 번호	02352FSF 02352FSF-003 02352FSF-007 02352FSF-009 02352FSF-011 02353FWL 02353FWL-003 02353FWL-005 02353FWL-006

1.3 제품 구성품

- 관리형 기가비트 스위치 X 1
- 콘솔케이블(RS232, RJ45)
- 19’인치 Mount 브라켓, 고정용 나사, 전원 케이블

이들 중 하나라도 누락되거나 손상되어 수리해야 할 경우 박스에 부속품과 제품을 다시 포장하여 본사나 대리점에 문의하십시오.

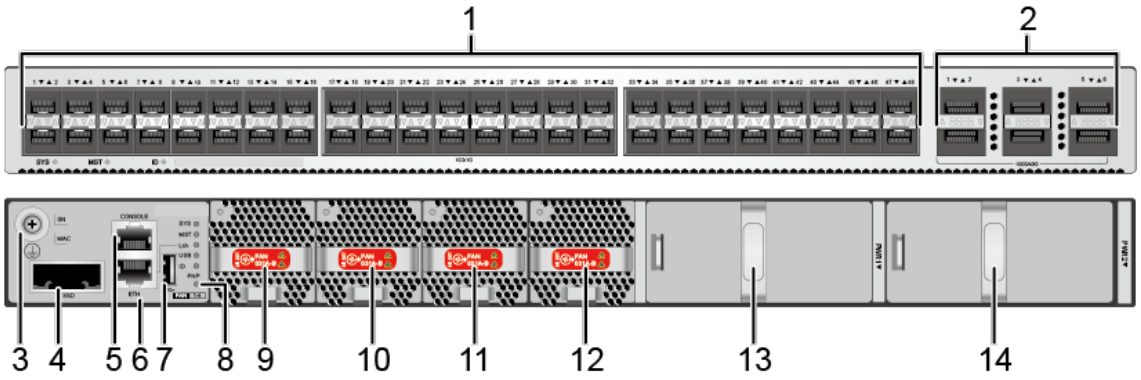
2 외관 설명

2.1 제품의 크기

SFC9448A 스위치의 제품 크기는 442(W) x 420(D) x 43.6(H) 입니다.

2.2 모델 및 외관

Notice : 콘솔 케이블과 터미널 프로그램이 없는 경우, RESET 버튼을 6 초 이상 누르지 마십시오. 다시 구성할 때까지 네트워크 연결이 끊어질 수 있습니다. 그리고 콘솔로만 접속이 가능합니다.



1	10GE SFP+ 포트 48 개 적용 가능한 모듈 및 케이블:	2	40GE/100GE QSFP28 광 포트 6 개 적용 가능한 모듈 및 케이블: 100GE 사용하려면 라이선스를 구매하고 활성화해야 합니다.
3	접지 나사 **메모:** 접지 케이블과 함께 사용됩니다.	4	SSD 카드 슬롯 **메모:** 이 슬롯은 나중에 사용할 수 있도록 예약되어 있습니다.
5	콘솔 포트 (9600, 8, 1, N)	6	ETH 관리 포트
7	USB 포트 1 개(전용 USB 필요)	8	RESET
9	팬 모듈 슬롯 1 **메모:**	10	Fan module slot 2 **메모:**

	적용 가능한 팬 모듈: FAN-031A-B (팬 박스(B,FAN 패널 측 배기))		적용 가능한 팬 모듈: FAN-031A-B (팬 박스(B,FAN 패널 측 배기))
11	팬 모듈 슬롯 3 **메모:** 적용 가능한 팬 모듈: FAN-031A-B (팬 박스(B,FAN 패널 측 배기))	12	팬 모듈 슬롯 4 **메모:** 적용 가능한 팬 모듈: FAN-031A-B (팬 박스(B,FAN 패널 측 배기))
13	전원 모듈 슬롯 1	14	전원 모듈 슬롯 2

■ 콘솔 접속

항목	설정값	비고
속도	9600	
데이터	8	
정지	1	
패리티, 흐름제어	없음	
비밀번호	admin123	

■ 관리 포트(뒷면 ETH포트)

항목	설정값	**비고**
IP	192.168.1.253/24	
계정	admin	
암호	admin123	
접속	SSH, HTTPS	

3 제품 설치

이 섹션에서는 Gigabit Ethernet Switch 를 설치하고 Switch 에 대한 연결 방법에 대해 설명합니다. 다음 항목을 읽고 제시하는 순서의 절차에 따라 수행하십시오. 데스크톱이나 선반에 Gigabit Ethernet Switch 를 설치하려면 다음 단계를 완료하십시오.

3.1 제품 설치방법

1 단계: AC 전원 코드 근처에 스위치가 놓일 수 있는 공간에 설치합니다.

2 단계: Gigabit Ethernet Switch 와 주변 물체 사이에 충분한 통풍공간을 유지하십시오.

3 단계: 네트워크 장치에 Switch 를 연결합니다.

A. Switch 전면에 10/100/1000M RJ-45 및 SFP 광 슬롯에 표준 네트워크 케이블의 한쪽 끝을 연결하십시오.

B. 프린터 서버, 워크 스테이션이나 라우터와 같은 네트워크 장치에 케이블의 한쪽 끝을 연결하십시오.

안내문: Gigabit Ethernet Switch 에 대한 연결은 UTP Category 5 규격 이상 7 미만의 네트워크 케이블이 필요합니다.

4 단계: 스위치의 후면 패널에 있는 AC 소켓에 전원 코드를 연결합니다. Gigabit Ethernet Switch 는 전원을 받으면 전원 LED(Green)가 항상 켜져 있습니다.

안내문: 네트워크가 항상 활성화 상태여야 한다면, 장치에 UPS(무 정전 전원 공급장치)를 사용하는 것을 고려하시기 바랍니다. 네트워크 데이터 손실이나 네트워크 Downtime 을 방지하실 수 있습니다.

안내문: 일부 지역에서는 서지 억제 장치를 설치하는 것을 고려하시기 바랍니다. 스위치가 서지 전류에 의해 손상될 위험이 있습니다.

3.2 SFP 모듈 설치방법

SFP 트랜시버는 hot-pluggable and hot-swappable 입니다. 사용자는 SFP port 에 트랜시버를 탈/부착할 때 Gigabit Ethernet Switch 의 전원을 끄셔야 됩니다.

다른 Switch, 워크 스테이션이나 미디어 컨버터를 연결하기 전에 다음사항을 확인하십시오.

1. SFP 전송의 두 측면은 같은 미디어 유형인지 확인하십시오. 예를 들어:

1000BASE-SX 에는 1000BASE-SX 을, 1000BASE-LX 는, 1000BASE-LX 을 연결해야 합니다.

2. 광섬유 케이블 타입 SFP 전송 모델과 일치하는지 확인하십시오.

-> 1000BASE-SX SFP 전송에 연결하려면 multi-mode fiber 케이블로 duplex LC 커넥터 타입을 사용해야 합니다.

-> 1000BASE-LX SFP 전송에 연결하려면 single mode fiber 케이블로 duplex LC 커넥터 타입을 사용해야 합니다.

3.3 광케이블 연결방법

1. SFP 트랜시버에 네트워크 케이블 duplex LC 커넥터를 연결합니다.
2. SFP 가 설치된 워크 스테이션이나 미디어 컨버터의 fiber NIC 있는 장치에 Switch 케이블의 다른 쪽 끝을 연결합니다.
3. Switch 의 전면에서 SFP 슬롯의 LED LNK/ACT 를 확인하십시오. SFP 트랜시버가 제대로 작동하는지 확인하십시오.
4. 링크가 실패한 경우에는 SFP port 의 연결 모드를 확인합니다. "1000 Force"로 링크 모드 설정을 필요로 하며 일부 fiber NIC 또는 미디어 컨버터와 함께 작동합니다.

3.4 트랜시버 모듈 제거

1. 네트워크 관리자에게 확인하여 어떠한 네트워크 활동이 없는지 확인하십시오. 아니면 사전에 Switch/컨버터의 관리 인터페이스를 통해 port 를 해체하십시오.
2. 부드럽게 fiber 케이블을 제거합니다.
3. 수평으로 SFP 모듈의 손잡이를 잡습니다.
4. 손잡이를 부드럽게 잡아 모듈을 빼냅니다.

4 WEB 기반 구성 가이드

4.1 WEB 로그인

4.1.1 WEB 시스템 로그인 개요

정의

웹 시스템은 장치를 프로비저닝하고 장치 배포 및 관리를 단순화하며 사용자 경험을 개선하는 데 도움이 되는 GUI 기반 장치 관리 도구입니다. CLI 전문 지식 없이도 웹 시스템을 사용하여 구성을 구축하고 장치를 모니터링하고 문제를 해결할 수 있습니다.

목적

웹 시스템 또는 CLI 를 통해 스위치를 관리할 수 있습니다. CLI 를 사용하면 명령을 통해 세분화된 장치 관리를 구현할 수 있습니다. 그러나 명령 구문에 익숙해야 하며 CLI 가 작동하는 방식을 이해해야 합니다. 웹 시스템은 기본적인 일상적인 유지보수 및 관리 기능만을 제공합니다. 관리 요구 사항에 따라 CLI 또는 웹 시스템을 사용할 수 있습니다.
CLI 를 사용하려면 콘솔 포트 또는 미니 USB 포트를 통해 또는 Telnet 또는 STelnet 을 사용하여 스위치에 로그인해야 합니다. 웹 시스템을 사용하려면 HTTPS 를 통해 스위치에 로그인해야 합니다.
콘솔 포트 또는 미니 USB 포트를 통해 또는 Telnet 또는 STelnet 을 사용하여 스위치에 로그인하는 방법에 대한 자세한 내용 은 CLI 로그인 구성을 참조하십시오.

웹 시스템 로그인의 개념

웹 시스템 로그인과 관련된 개념은 다음과 같습니다.

- **HTTP**
  HTTP(Hypertext Transfer Protocol)는 인터넷을 통해 웹 페이지 파일을 전송하는 데 사용됩니다. TCP/IP 프로토콜 스택의 응용 프로그램 계층에서 실행됩니다. 전송 계층은 연결 지향 TCP 프로토콜을 사용합니다. HTTP 의 보안 취약성으로 인해 장치에서는 보다 안전한 HTTPS(Hypertext Transfer Protocol Secure)를 통해서만 웹 시스템에 로그인할 수 있습니다.
- **HTTPS**

HTTPS 는 SSL(Secure Sockets Layer)을 사용하여 클라이언트와 장치 간에 교환되는 데이터를 암호화하고 인증서 속성을 기반으로 액세스 제어 정책을 정의합니다. HTTPS 는 데이터 무결성과 전송 보안을 강화하여 승인된 클라이언트만 장치에 로그인할 수 있도록 합니다.

- **SSL 정책**

  SSL 정책은 시작 중에 장치가 사용하는 매개변수를 정의합니다. HTTPS 구성 전에 SSL 정책을 배포하고 해당 디지털 인증서를 장치에 로드해야 합니다. SSL 정책은 HTTP 와 같은 응용 프로그램 계층 프로토콜에 적용된 후에만 적용됩니다.

- **디지털 인증서**

  디지털 인증서는 인증 기관(CA)에서 발급하고 디지털 서명을 사용하여 공개 키를 ID(인증서를 소유한 신청자)와 바인딩합니다. 전자인증서에는 신청자명, 공개키, 인증기관의 전자서명, 전자인증서의 유효기간 등의 정보가 포함된다. 디지털 인증서는 통신 신뢰성을 향상시키기 위해 두 통신 당사자의 ID 를 검증합니다.

  장치는 PEM, ASN1 및 PFX 형식의 인증서를 지원합니다. 인증서는 형식에 관계없이 동일한 내용을 갖습니다.

  - PEM(.pem) 디지털 인증서가 일반적으로 사용됩니다. 시스템 간의 텍스트 전송에 사용됩니다.
  - ASN1(.der) 형식은 범용 디지털 인증서 형식입니다. 이것은 대부분의 브라우저의 기본 형식입니다.
  - PFX(.pfx) 형식은 범용 디지털 인증서 형식입니다. PEM 또는 ASN1 형식으로 변환할 수 있는 바이너리 형식입니다.

- **CA**

  CA 는 디지털 인증서 소유자의 유효성을 확인하고, 도청 및 변조 방지를 위한 디지털 인증서를 발급하고, 키를 관리하여 디지털 인증서를 발급, 관리 및 취소합니다. 전 세계적으로 신뢰할 수 있는 CA 를 루트 CA 라고 합니다. 루트 CA 는 다른 CA 를 하위 CA 로 인증할 수 있습니다. CA ID 는 확인해야 하며 신뢰할 수 있는 CA 파일에 설명되어 있습니다.

  예를 들어 CA1 은 루트 CA 입니다. CA2 에 대한 인증서를 발급하면 CA3 에 대한 인증서를 발급할 수 있습니다. 이 프로세스는 최종 서버 인증서가 발급될 때까지 계속됩니다.

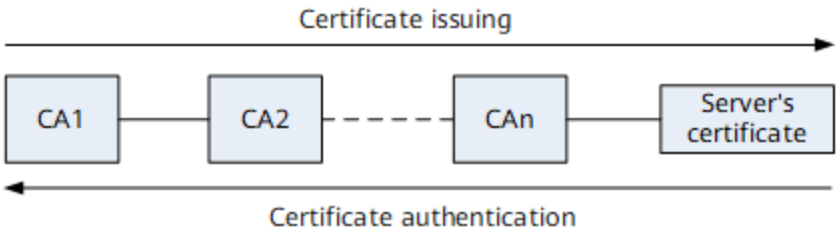
  CA3 가 서버 인증서를 발급한다고 가정합니다. 클라이언트의 인증서 인증 프로세스는 서버 인증서 인증에서 시작됩니다.

  - 클라이언트는 먼저 CA3 인증서를 기반으로 서버 인증서의 유효성을 확인합니다.
  - 그런 다음 클라이언트는 CA2 인증서를 확인하여 CA3 인증서의 유효성을 확인합니다.
  - 그런 다음 클라이언트는 CA1 인증서를 확인하여 CA2 인증서의 유효성을 확인합니다.

- 서버 인증서는 CA2 인증서가 CA1 인증서에 따라 유효한 것으로 확인된 경우에만 인증을 통과합니다.

그림 1 은 인증서 발급 및 인증 프로세스를 보여줍니다.

그림 1 인증서 발급 및 인증



- **인증서 해지 목록(CRL)**

  CRL 은 CA 에서 발급하며 해지된 인증서 목록을 지정합니다.

  각 디지털 인증서에는 제한된 수명이 있으며 CA 는 수명을 단축하기 위해 디지털 인증서를 취소할 수 있습니다. CRL 에 지정된 인증서의 유효 기간이 인증서의 원래 유효 기간보다 짧습니다. CA 가 디지털 인증서를 해지하면 인증서에 정의된 키 쌍은 디지털 인증서가 만료되지 않은 경우에도 더 이상 사용할 수 없습니다. 인증서가 만료되면 CRL 에서 삭제됩니다.

디지털 인증서보다 높은 수준의 CRL 및 인증서(신뢰 인증서)를 PC 에 로드할 수 있습니다. 로드되지 않은 경우 웹 서버와의 연결을 설정할 때 서버를 신뢰하라는 메시지가 표시됩니다. 성공적으로 연결되면 PC 에서 서버의 디지털 인증서를 즉시 확인할 수 없습니다. 그러나 PC 와 서버 간에 전송되는 데이터는 기밀입니다. 유효한 웹 서버에 연결하고 있는지 확인하기 위해 PC 에서 신뢰 인증서와 CRL 을 로드할 수 있습니다. 신뢰 인증서를 로드하는 방법에 대한 자세한 내용은 운영 체제의 도움말 정보를 참조하십시오.

4.1.2 WEB 시스템 로그인 구성

웹 시스템에서 제공하는 GUI 를 통해 스위치를 편리하게 관리하고 유지할 수 있습니다. 웹 시스템 로그인을 구성하기 전에 PC 와 스위치가 서로 라우팅 가능한지 확인하십시오.

공장 초기 설정값

```
!Software Version V200R022C00SPC500
#
sysname Soltech
#
authentication-profile name default_authen_profile
authentication-profile name dot1x_authen_profile
authentication-profile name dot1xmac_authen_profile
authentication-profile name mac_authen_profile
authentication-profile name multi_authen_profile
authentication-profile name portal_authen_profile
#
http server-source all-interface
#
diffserv domain default
#
radius-server template default
#
free-rule-template name default_free_rule
#
portal-access-profile name portal_access_profile
#
drop-profile default
#
aaa
 authentication-scheme default
  authentication-mode local
 authentication-scheme radius
  authentication-mode radius
 authorization-scheme default
  authorization-mode local
 accounting-scheme default
  accounting-mode none
```

```
 local-aaa-user password policy administrator
  password history record number 0
  password expire 0
 domain default
  authentication-scheme radius
  accounting-scheme default
  radius-server default
 domain default_admin
  authentication-scheme default
  accounting-scheme default
 local-user admin password irreversible-cipher admin123
 local-user admin privilege level 15
 local-user admin service-type terminal ssh http
#
interface Vlanif1
#
interface MEth0/0/1
 ip address 192.168.1.253 255.255.255.0
#
interface MEth0/0/2
#
interface XGigabitEthernet0/0/1
#
interface XGigabitEthernet0/0/2
#
interface XGigabitEthernet0/0/3
#
interface XGigabitEthernet0/0/4
#
interface XGigabitEthernet0/0/5
#
interface XGigabitEthernet0/0/6
#
interface XGigabitEthernet0/0/7
#
interface XGigabitEthernet0/0/8
#
interface XGigabitEthernet0/0/9
#
interface XGigabitEthernet0/0/10
```

```
#
interface XGigabitEthernet0/0/11
#
interface XGigabitEthernet0/0/12
#
interface XGigabitEthernet0/0/13
#
interface XGigabitEthernet0/0/14
#
interface XGigabitEthernet0/0/15
#
interface XGigabitEthernet0/0/16
#
interface XGigabitEthernet0/0/17
#
interface XGigabitEthernet0/0/18
#
interface XGigabitEthernet0/0/19
#
interface XGigabitEthernet0/0/20
#
interface XGigabitEthernet0/0/21
#
interface XGigabitEthernet0/0/22
#
interface XGigabitEthernet0/0/23
#
interface XGigabitEthernet0/0/24
#
interface XGigabitEthernet0/0/25
#
interface XGigabitEthernet0/0/26
#
interface XGigabitEthernet0/0/27
#
interface XGigabitEthernet0/0/28
#
interface XGigabitEthernet0/0/29
#
interface XGigabitEthernet0/0/30
```

```
#
interface XGigabitEthernet0/0/31
#
interface XGigabitEthernet0/0/32
#
interface XGigabitEthernet0/0/33
#
interface XGigabitEthernet0/0/34
#
interface XGigabitEthernet0/0/35
#
interface XGigabitEthernet0/0/36
#
interface XGigabitEthernet0/0/37
#
interface XGigabitEthernet0/0/38
#
interface XGigabitEthernet0/0/39
#
interface XGigabitEthernet0/0/40
#
interface XGigabitEthernet0/0/41
#
interface XGigabitEthernet0/0/42
#
interface XGigabitEthernet0/0/43
#
interface XGigabitEthernet0/0/44
#
interface XGigabitEthernet0/0/45
#
interface XGigabitEthernet0/0/46
#
interface XGigabitEthernet0/0/47
#
interface XGigabitEthernet0/0/48
#
interface 40GE0/0/1
#
interface 40GE0/0/2
```

```
#
interface 40GE0/0/3
#
interface 40GE0/0/4
#
interface 40GE0/0/5
#
interface 40GE0/0/6
#
interface NULL0
#
undo icmp name timestamp-request receive
#
stelnet server enable
ssh user admin
ssh user admin authentication-type password
ssh user admin service-type all
ssh server-source all-interface
ssh server cipher aes256_ctr aes128_ctr
ssh server hmac sha2_256
ssh server key-exchange dh_group16_sha512 dh_group15_sha512 dh_group14_sha256
ssh client cipher aes256_ctr aes128_ctr
ssh client hmac sha2_256
ssh client key-exchange dh_group16_sha512 dh_group15_sha512 dh_group14_sha256
ssh server dh-exchange min-len 2048
ssh server publickey rsa_sha2_512 rsa_sha2_256
#
user-interface con 0
 authentication-mode password
 set authentication password admin123
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 15
user-interface vty 16 20
#
wlan
 traffic-profile name default
 security-profile name default
 security-profile name default-wds
 security-profile name default-mesh
```

```
 ssid-profile name default
 vap-profile name default
 wds-profile name default
 mesh-handover-profile name default
 mesh-profile name default
 regulatory-domain-profile name default
 air-scan-profile name default
 rrm-profile name default
 radio-2g-profile name default
 radio-5g-profile name default
 wids-spoof-profile name default
 wids-whitelist-profile name default
 wids-profile name default
 ap-system-profile name default
 port-link-profile name default
 wired-port-profile name default
 ap-group name default
 provision-ap
#
dot1x-access-profile name dot1x_access_profile
#
mac-access-profile name mac_access_profile
#
ops
#
remote-unit
#
return
```

웹 시스템 로그인을 위한 공통 구성

기본적으로 추가 구성 없이 첫 번째 로그인의 사용자 이름과 변경된 비밀번호를 사용하여 스위치에 직접 로그인할 수 있습니다. 웹 사용자를 추가하거나 사용자 정보를 변경하려면 다음 단계를 수행하십시오.

1. 웹 사용자와 로그인 암호를 만듭니다.
2. 웹 사용자에 대한 액세스 유형 및 권한 수준을 구성합니다.

작업 절차

1. 웹 사용자를 만들고 사용자의 로그인 암호를 설정합니다.

```
<Soltech> system-view
[Soltech] aaa
[Soltech-aaa] local-user admin123 password irreversible-cipher abcd@123    //Create a local user admin123 and set the login password to abcd@123.
```

2. 웹 사용자에 대한 액세스 유형 및 권한 수준을 설정합니다.

```
[Soltech-aaa] local-user admin123 privilege level 15    //Set the privilege level of the local user admin123 to 15.
Warning: This operation may affect online users, are you sure to change the user privilege level ?[Y/N]y
[Soltech-aaa] local-user admin123 service-type http    //Set the access type of the local user admin123 to HTTP.
[Soltech-aaa] quit
```

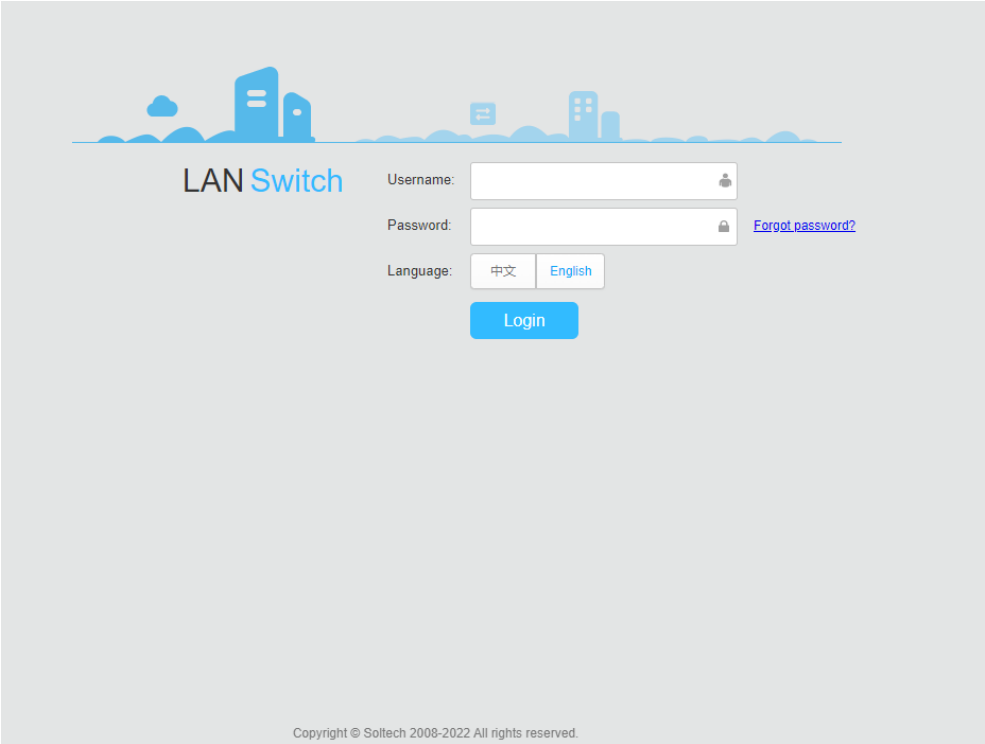
3. HTTPS 서버 정보를 봅니다.

```
[Soltech] display http server
  HTTP Server Status              : enabled
  HTTP Server Port                : 80(80)
  HTTP Timeout Interval           : 20
  Current Online Users            : 3
  Maximum Users Allowed           : 5
  HTTP Secure-server Status       : enabled
  HTTP Secure-server Port         : 443(443)
  HTTP SSL Policy                 : ssl_server
  HTTP IPv6 Server Status         : disabled
  HTTP IPv6 Server Port           : 80(80)
  HTTP IPv6 Secure-server Status  : disabled
  HTTP IPv6 Secure-server Port    : 443(443)
  HTTP server source address      : 0.0.0.0
```

NOTE

장치가 구성 없이 시작되면 HTTP 는 임의로 생성된 자체 서명 인증서를 사용하여 HTTP 를 지원합니다. 자체 서명된 인증서는 위험을 초래할 수 있습니다. 따라서 공식적으로 공인된 디지털 인증서로 교체하는 것이 좋습니다.

4. 웹 시스템을 통해 장치에 로그인합니다.
웹 시스템 로그인의 기본 기능을 설정한 후, PC 에서 웹 브라우저를 열고 주소창에 **https:// *IP 주소*를 입력** 하고 **Enter** 키를 누릅니다. 그러면 웹 시스템 로그인 페이지가 표시됩니다. 그림 1 과 같이 구성된 웹 사용자 이름과 암호를 입력하고 웹 시스템의 언어를 선택합니다.
그림 1 웹 시스템 로그인 페이지



NOTE

- 암호 변경 페이지는 웹 시스템에 처음 로그인할 때 표시됩니다.
- 비밀번호가 만료 예정이거나 만료된 경우에도 비밀번호 변경 페이지가 표시됩니다. 웹 시스템 메인 페이지에 접근하기 위해서는 비밀번호를 변경해야 합니다.
- 보안을 위해 암호에는 소문자, 대문자, 숫자 및 특수 문자(예: ! $ # %) 중 최소 두 가지 유형이 포함되어야 합니다. 또한 암호는 공백이나 작은따옴표(')를 포함할 수 없습니다.
- 웹 사용자가 관리자이고 기본 로컬 사용자가 시스템에 존재하는 경우 시스템은 웹 시스템에 로그인하는 데 사용된 사용자 이름 및 암호에 관계없이 기본 로컬 사용자를 변경하라는 메시지를 사용자에게 표시합니다.

기본 사용자 이름과 암호는 *S 시리즈 스위치 기본 사용자 이름 및 암호* (엔터프라이즈 네트워크 또는 캐리어)에서 사용할 수 있습니다. 문서에 대한 접근 권한을 얻지 못한 경우 웹 사이트의 **도움말**을 참조하여 문서를 얻는 방법을 알아보세요.

웹 시스템 로그인을 위한 기타 구성

- 웹 페이지 파일을 로드합니다.
  일반적으로 웹 페이지 파일은 스위치의 시스템 소프트웨어에 통합되어 로드됩니다. 웹 페이지 파일을 업그레이드해야 하는 경우 Soltech 공식 웹 사이트에 로그인하여 별도의 웹 페이지 파일을 다운로드하여 스위치에 업로드합니다.
  1. 스위치에 웹 페이지 파일을 업로드하십시오.

     NOTE

     웹 페이지 파일을 얻으려면 Soltech 기업 지원 웹사이트(http://support.Soltech.com/enterprise)에 로그인 하여 제품 모델 및 버전을 선택하고 **V 및 R 버전의 공개 패치에서** 패치 버전을 선택하여 필요한 웹 페이지 파일을 다운로드합니다. 파일명은 **product name-software version number.web page 파일 version number.web.7z 형식**입니다.

     각 웹 페이지 파일은 서명 파일에 해당합니다. 서명 파일을 다운로드하는 방법은 웹 페이지 파일을 다운로드하는 방법과 동일합니다.

     필요한 파일을 스위치에 로드하는 방법에 대한 자세한 내용은 **파일 관리**를 참조하십시오.

  2. 웹 페이지 파일을 로드합니다.

     ```
     <Soltech> system-view
     [Soltech] http server load web.7z
     ```

  3. HTTPS 서비스를 활성화합니다.

     ```
     [Soltech] http secure-server enable    //By default, the HTTP IPv4 service function is enabled, and the HTTP IPv6 service function is disabled.
     ```

- 디지털 인증서를 로드하고 SSL 정책을 스위치에 바인딩합니다.
  1. 서버의 디지털 인증서와 개인 키 파일을 스위치에 업로드합니다.

     NOTE

SFTP 를 이용하여 서버의 전자인증서와 개인키 파일을 업로드 할 수 있으며, 전자인증서와 개인키
파일은 **보안** 디렉토리에 Save(저장)됩니다. 스위치에 **보안** 디렉터리 가 없으면 **mkdir security** 명령을 실행하여 만듭니다. 필요한 파일을 스위치에 로드하는 방법에 대한 자세한 내용은 **파일 관리를** 참조하십시오.

서버의 전자인증서와 개인키 파일을 업로드한 후 사용자
보기에서 **dir** 명령어를 실행하여 업로드한 서버의 전자인증서와 개인키 파일의 크기가 파일 서버의 크기와 동일한지 확인한다. 그렇지 않으면 파일 업로드 중에 예외가 발생할 수 있습니다. 파일을 다시 업로드할 수 있습니다.

2. SSL 정책을 만들고 디지털 인증서를 로드합니다. 여기에서는 PEM 디지털 인증서를 예로 사용합니다.

```
[SOLTECH] ssl policy http_server
[Soltech-ssl-policy-http_server] certificate load pem-cert
1_servercert_pem_dsa.pem key-pair dsa key-file 1_serverkey_pem_dsa.pem
auth-code cipher 123456
[HTTPS-Server-ssl-policy-http_server] quit
```

3. SSL 정책을 스위치에 바인딩하고 HTTPS 서비스를 활성화합니다.

```
[Soltech] http secure-server ssl-policy http_server
[Soltech] http secure-server enable
```

4. 로드된 디지털 인증서에 대한 자세한 정보를 봅니다.

```
[Soltech] display ssl policy


      SSL Policy Name: http_server
    Policy Applicants: Config-Webs
       Key-pair Type: DSA
 Certificate File Type: PEM
     Certificate Type: certificate
  Certificate Filename: 1_servercert_pem_dsa.pem
    Key-file Filename: 1_serverkey_pem_dsa.pem
            Auth-code: ******
                  MAC:
             CRL File:
      Trusted-CA File:
          Issuer Name:
   Validity Not Before:
```

```
Validity Not After:
```

관련 명령

자세한 명령 설명은 명령 참조를 참조하십시오.

표 1 공통 명령

기능	명령	설명
로컬 AAA 사용자를 만들고 사용자의 암호를 설정합니다.	**local-user** *user-name* **password irreversible-cipher** *password*	기본 사용자 이름과 암호는 *S 시리즈 스위치 기본 사용자 이름 및 암호* (엔터프라이즈 네트워크 또는 캐리어)에서 사용할 수 있습니다. 문서에 대한 접근 권한을 얻지 못한 경우 웹 사이트의 **도움말**을 참조하여 문서를 얻는 방법을 알아보세요. **노트:** CLI 를 통해 스위치에 로그인하고 기본 사용자의 암호를 변경한 경우 새 암호를 사용하십시오.
로컬 AAA 사용자의 액세스 유형을 설정합니다.	**local-user** *user-name* **service-type http**	기본적으로 로컬 사용자는 액세스 유형을 사용할 수 없습니다.
로컬 사용자의 권한 수준을 설정합니다.	**local-user** *user-name* **privilege level** *level*	기본적으로 로컬 사용자의 권한 수준은 관리자를 나타내는 15 입니다.
웹 페이지 파일을 로드합니다.	**http server load** { *file-name* | **default** }	기본적으로 시스템 소프트웨어에 통합된 웹 페이지 파일은 스위치에 로드됩니다.
SSL 정책을 만들고 SSL 정책 보기를 표시합니다.	**ssl policy** *policy-name*	기본적으로 SSL 정책은 생성되지 않습니다.
SSL 정책을 스위치에 바인딩합니다.	**http secure-server ssl-policy** *policy-name*	기본 SSL 정책은 HTTP 서버에서 사용할 수 있습니다.

표 1 공통 명령

기능	명령	설명
HTTPS 서비스를 활성화합니다.	**http** [**ipv6**] **secure-server enable**	기본적으로 HTTPS IPv4 서비스 기능은 활성화되고 HTTPS IPv6 서비스 기능은 비활성화됩니다.

표 2 기타 명령

기능	명령	설명
웹 페이지 파일의 유효성을 확인하십시오.	**check file-integrity** *filename signature-filename*	확인에 실패하면 시스템 소프트웨어, 패치 파일, 웹 페이지 파일 또는 모드 파일로 사용할 수 없습니다.
HTTPS 서버의 포트 번호를 설정합니다.	**http** [**ipv6**] **secure-server port** *port-number*	기본 포트 번호는 443 입니다.
HTTPS 서버에 대한 소스 인터페이스를 설정합니다.	**http server-source -i loopback** *interface-number*	HTTPS 서버에 대한 소스 인터페이스를 설정하기 전에 소스 인터페이스로 지정할 루프백 인터페이스가 생성되었는지 확인하십시오. 그렇지 않으면 이 명령을 올바르게 실행할 수 없습니다.
HTTPS 세션 비활성 기간을 설정합니다.	**http timeout** *timeout*	기본적으로 HTTPS 세션 비활성 기간은 20 분입니다.
SSL 암호 제품군 정책을 사용자 지정합니다.	**ssl cipher-suite-list** *customization-policy-name*	기본적으로 스위치는 보안 알고리즘만 지원합니다. 이 명령을 실행하여 암호 제품군 정책을 사용자 지정할 수 있습니다.
사용자 정의된 SSL 암호 제품군 정책에 대한 암호 제품군을 설정합니다.	**set cipher-suite** { **tls12_ck_dss_aes_128_gcm_sha256** | **tls12_ck_dss_aes_256_gcm_sha384** | **tls12_ck_rsa_a**	기본적으로 사용자 정의된 SSL 암호 제품군 정책에 대해 암호 제품군이 구성되지 않습니다. 시스템 소프트웨어는 지원하지 않습니다 **tls12_ck_rsa_aes_256_cbc_sha**

표 2 기타 명령

기능	명령	설명
	es_128_gcm_sha256 | **tls12_ck_rsa_aes_256_gcm_sha384** }	**256**, **tls1_ck_dhe_dss_with_aes_128_sha**, **tls1_ck_dhe_dss_with_aes_256_sha**, **tls1_ck_dhe_rsa_with_aes_128_sha**, **tls1_ck_dhe_rsa_with_aes_256_sha**, **tls1_ck_rsa_with_aes_128_sha** 및 **tls1_ck_rsa_with_aes_256_sha 의** 매개 변수를. 이러한 매개변수를 사용하려면 WEAKEA 플러그인을 설치해야 합니다. 보안을 위해 다른 매개변수를 사용하는 것이 좋습니다.
SSL 정책의 최소 SSL 버전을 설정합니다.	**ssl minimum version** { **tls1.1** | **tls1.2** }	SSL 정책의 기본 최소 SSL 버전은 TLS1.2 입니다. 시스템 소프트웨어는 **tls1.0** 매개변수를 지원하지 않습니다. 이 매개변수를 사용하려면 WEAKEA 플러그인을 설치해야 합니다. 보안을 위해 **tls1.2** 매개변수를 지정하는 것이 좋습니다.
지정된 사용자 지정 SSL 암호 제품군 정책을 SSL 정책에 바인딩합니다.	**binding cipher-suite-customization** *customization-policy-name*	기본적으로 각 SSL 정책은 기본 암호 제품군을 사용합니다. SSL 정책에 바인딩된 사용자 지정 암호 제품군 정책의 암호 제품군에 한 가지 유형의 알고리즘(RSA 또는 DSS)만 포함된 경우 성공적인 SSL 협상을 위해 SSL 정책에 대해 해당 인증서를 로드해야 합니다.
PEM 디지털 인증서/인증서 체인을 로드하고 개인 키 파일을 지정합니다.	1. **certificate load pem-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code cipher** *auth-code* 2. **certificate load pem-chain** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-**	하나의 인증서 또는 인증서 체인만 SSL 정책에 로드할 수 있습니다. (인증서 체인은 장치의 인증서에서 시작하여 루트 CA 인증서로 끝나는 신뢰 인증서 목록입니다.) 인증서 또는 인증서 체인이 로드된 경우 **undo certificate load** 명령을 실행 하여 이전 인증서 또는 인증서 체인을 로드 해제하기 전에

표 2 기타 명령

기능	명령	설명
	file *key-filename* **auth-code cipher** *auth-code*	새 로드 중입니다. 인증서 유형에 따라 해당 구성을 선택합니다. PEM 인증서 또는 인증서 체인을 로드할 때 사용자가 CA 에서 디지털 인증서 또는 인증서 체인을 획득하는지 여부에 따라 다음 명령 중 하나를 실행하십시오. 명령 1 은 PEM 디지털 인증서를 로드하고 개인 키 파일을 지정하는 데 사용됩니다. 명령 2 는 PEM 인증서 체인을 로드하고 개인 키 파일을 지정하는 데 사용됩니다.
ASN1 디지털 인증서를 로드하고 개인 키 파일을 지정하십시오.	**certificate load asn1-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename*	
PFX 디지털 인증서를 로드하고 개인 키 파일을 지정합니다.	**certificate load pfx-cert** *cert-filename* **key-pair** { **dsa** | **rsa** } { **mac cipher** *mac-code* | **key-file** *key-filename* } **auth-code cipher** *auth-code*	
지정된 웹 사용자를 강제로 오프라인 상태로 만듭니다.	**free http user-id** *user-id*	현재 스위치는 최대 5 명의 동시 온라인 웹 사용자를 지원합니다.
웹 시스템에서 개인화된 인사말 메시지를 설정합니다.	**web welcome-message** *message*	해당 없음
온라인 웹 사용자 정보를 봅니다.	**display http user** [**username** *username*]	해당 없음

4.2 WEB 시스템 화면 구성

4.2.1 WEB 시스템 클라이언트 사용자 인터페이스

4.2.1.1 창 레이아웃

웹 시스템의 일반적인 작동 사용자 인터페이스는 다음 그림과 같습니다. 그림 1 은 작업 사용자 인터페이스를 보여줍니다.

그림 1 작동 사용자 인터페이스

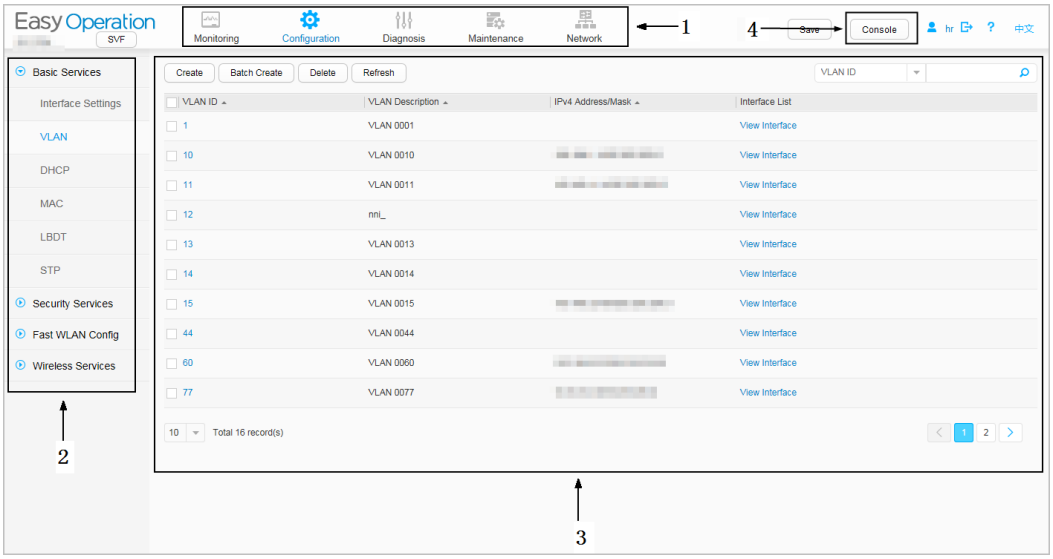


표 1 창 레이아웃

숫자	설명
1	기능 영역. 웹 시스템은 모니터링, 구성, 진단, 유지 관리 및 네트워크의 5 가지 기능을 제공합니다.
2	탐색 트리. 탐색 트리에는 사용 가능한 구성 항목이 나열됩니다.
삼	상태 표시 및 작동 영역. 장치의 현재 상태가 이 영역에 표시되며 이 영역에서 생성, 삭제, 수정, 불러오기, 검색 등의 작업을 수행할 수 있습니다.
4	CLI 스위칭 영역. 이 영역에서 CLI 창을 호출할 수 있으며 사용자는 창에서 명령을 실행하여 장치를 관리하고 유지할 수 있습니다. Microsoft Internet Explorer 를 사용하는 경우 **스크립팅에 안전한 것으로 표시되지 않은 ActiveX 컨트롤 초기화 및 스크립팅**을 **사용** 또는 **확인** 으로 설정해야 합니다. **도구** > **인터넷 옵션** > **보안**을 선택하고 **사용자 지정 수준을** 클릭 **한 다음 스크립팅** 에 **안전하지 않은 것으로 표시된 ActiveX 컨트롤 초기화 및 스크립팅**을 **활성화** 또는 **확인** 으로 **설정합니다**. 이 예에서는 Internet Explorer 8.0 을 사용합니다.

표 1 창 레이아웃

숫자	설명
	노트: ● 이 기능은 운영 체제에서 Telnet 이 활성화되어 있고 운영 체제 사용자에게 관리 권한이 있는 경우에만 사용할 수 있습니다. ● 이 기능은 Telnet 클라이언트만 호출하며 장치 연결 상태를 확인할 수 없습니다. ● 로그인 모드가 URL 주소 또는 장치 IP 주소 및 포트 매핑인 경우 이 기능을 사용할 수 없습니다.

4.2.1.2 탐색 트리

웹 시스템은 모니터링, 구성, 진단, 유지 관리, 네트워크의 5 개 영역으로 구성되며 장치 상태 개요, 인터페이스 관리, VLAN, DHCP, 시스템 관리, 서비스 관리, 진단 도구 및 네트워크 배포 기능을 제공합니다.
표 1 은 4 개 영역의 하위 메뉴를 나열하고 해당 기능을 설명합니다.

NOTE

이 섹션에서 설명하는 메뉴 및 하위 메뉴는 스위치 모델에 따라 약간의 차이가 있기 때문에 참고용으로만 사용됩니다.

표 1 웹 시스템 메뉴 설명

메뉴	하위 메뉴		설명
Monitoring 모니터링	Summary (Standalone) 요약(독립형)		장치 패널, 시스템 설명, 스위치 상태, 상위 5 개 대역폭 사용량, 로그 및 경보를 표시합니다.
	User 사용자		액세스 사용자 정보를 표시합니다.
Configuration 구성	Quick Config 빠른 구성		스위칭 및 라우팅 모드를 빠르게 구성합니다.
	Basic Services 기본 서비스	Interface Settings 인터페이스 설정	인터페이스 구성에는 구성 보기, PC 에 연결, IP 전화에 연결, 스위치에 연결, 라우터에 연결, 인터페이스 활성화/비활성화, 포트 루프백 테스트 및 링크 감지와 같은 구성 페이지가 포함됩니다.
		Transceiver Info	광 모듈 정보를 표시합니다.

표 1 웹 시스템 메뉴 설명

메뉴	하위 메뉴		설명
		트랜시버 정보 보기	
		VLAN	VLAN 구성 및 쿼리, VLAN 수정, VLAN 삭제
		DHCP	전역 주소 풀, VLANIF 인터페이스의 DHCP 주소 풀 및 DHCP 릴레이를 구성하고 쿼리합니다.
		Static Route 정적 경로	고정 경로를 구성합니다.
	고급 서비스	Connecting to Cisco ISE	Cisco ISE 연결 정보를 구성합니다.
		Connecting to Aruba ClearPass	Aruba ClearPass 연결 정보를 구성합니다.
		MQC	MQC 를 구성합니다.
		Voice VLAN 음성 VLAN	음성 VLAN 을 구성합니다.
		MAC	MAC/IP 주소 테이블 쿼리, 고정 MAC 주소 항목 구성, 고정 보안 MAC 주소 구성, 블랙홀 MAC 주소 항목 구성 및 MAC 주소 항목 삭제 기능.
		IP Services IP 서비스	IP 서비스를 구성합니다.
		IP Route IP 경로	IP 경로를 구성합니다.
		VRRP	VRRP 를 구성합니다.
		LBDT	루프백 감지 기능을 구성합니다.
		STP	STP 기능을 구성합니다.
		LLDP	LLDP 기능을 구성합니다.
		IGMP Snooping IGMP 스누핑	IGMP 스누핑을 구성합니다.
		MLD Snooping	MLD 스누핑을 구성합니다.

표 1 웹 시스템 메뉴 설명

메뉴	하위 메뉴		설명
		MLD 스누핑	
		Mirroring 미러링	미러링을 구성합니다.
		Stack 스택	스택을 구성합니다.
	Security Services 보안 서비스	ACL Config ACL 구성	ACL 을 구성합니다.
		ACL Reference ACL 참조	참조 ACL.
		AAA	AAA 를 구성합니다.
		AAA Service App AAA 서비스 앱	AAA 를 신청합니다.
		AAA Profile Mgmt AAA 프로필 관리	AAA 프로필 관리를 제공합니다.
		ACL	패킷을 필터링하도록 인터페이스 ACL 및 VLAN ACL 을 구성합니다.
		User Access Control 사용자 액세스 제어	인증 구성, Portal Server 및 액세스 구성을 구성하여 네트워크에서 보안 관리를 제공합니다.
		QoS Configuration QoS 구성	QoS 를 구성합니다.
		IP Security IP 보안	IP 보안을 구성합니다.
		Storm Control 폭풍 통제	폭풍 제어를 구성합니다.
		Port Isolation 포트 격리	포트 격리를 구성합니다.
Diagnosis 진단	Intelligent Diagnosis 지능형 진단		WLAN 의 스위치, AP 및 STA 에 대한 지능형 진단을 활성화합니다.

표 1 웹 시스템 메뉴 설명

메뉴	하위 메뉴		설명
	One-Click Information Collection 원클릭 정보 수집		구성, 로그 및 오류를 포함하여 장치에 대한 정보를 수집합니다.
	Ping 핑		네트워크 연결 및 호스트 연결 가능성을 확인합니다.
	Trace RouteC 추적 경로 C		패킷이 소스 호스트에서 대상 호스트로 통과하는 게이트웨이를 확인합니다.
	AAA Test AAA 테스트		사용자가 RADIUS 인증을 통과할 수 있는지 확인합니다.
	Configuration Check 구성 확인		AP 와 스위치 간의 버전 매핑, RF 매개변수, 네트워크 매개변수 및 공통 기능을 확인합니다.
Maintenance 유지	System Maintenance 시스템 유지 관리	License 라이선스	라이선스 파일을 로드하고 라이선스 상태를 표시합니다.
		Restart 다시 시작	스위치를 다시 시작하십시오.
		Upgrade 업그레이드	시스템 소프트웨어를 업그레이드하십시오.
		Web File Management 웹 파일 관리	웹 파일을 관리합니다.
		Patch 패치	패치를 업로드, 설치 및 제거합니다.
		Log 로그	최근 300 개의 로그를 표시합니다.
		Alarm & Event 경보 및 이벤트	최근 300 개의 알람을 표시합니다.
		Administrator 관리자	웹 사용자를 관리합니다.
		System 시스템	파일, 시스템 시간, 시스템 정보 및 공장 설정 복구를 포함하여 시스템을 관리합니다.

표 1 웹 시스템 메뉴 설명

메뉴	하위 메뉴		설명
		SNMP	SNMP 에이전트 기능을 구성합니다.
		Electronic Label 전자 라벨	스위치에 elabel 정보를 표시합니다.

4.2.1.3 버튼

표 1 은 버튼을 나열하고 기능을 설명합니다.

표 1 버튼 설명

단추	기능
Delete	선택한 데이터 레코드를 삭제합니다.
ON	기능이 활성화되었는지 여부를 나타냅니다. ON 은 활성화됨을 나타내고 OFF 는 비활성화됨을 나타냅니다. 이 버튼을 전환하여 상태를 변경할 수 있습니다.
Apply	입력한 구성을 제출하고 시스템 디스플레이 정보를 확인합니다. **노트:** 팝업 대화 상자에서 **Apply(적용)을 클릭**하면 대화 상자가 닫히지 않습니다.
Create	현재 페이지에 항목을 만듭니다.
Batch Create	현재 페이지에서 일괄 항목을 만듭니다.
	현재 항목의 값을 검색합니다.
Refresh	현재 페이지를 새로 고칩니다.
Clear	현재 페이지의 모든 기록을 지웁니다.

4.2.1.4 GUI 요소

표 1 은 웹 시스템 GUI 에서 일반적으로 사용하는 요소를 나열합니다.

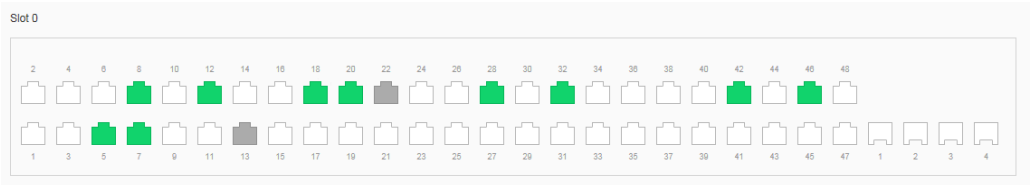
NOTE

이 섹션에서 설명하는 GUI 요소는 다른 스위치 모델의 GUI 요소에 약간의 차이가 있기 때문에 참조용으로만 사용됩니다.

표 1 GUI 요소

이름	요소
단추	OK
온 / 오프 스위치	ON
옵션 버튼	Yes
체크박스	v1
탭	File Management System Time System Info Initialization
텍스트 상자	User-defined file name:
찾아보기 상자	Upgrade file: - Select - ... (Select a *.cc file)
그룹 상자	VLAN ID
드롭다운 목록 상자	Select Select FTP SFTP TFTP
메뉴	View Configuration Connect to PC Connect to IP Phone Connect to Switch Connect to Router
정렬 버튼	기본: 내림차순:

표 1 GUI 요소

이름	요소
	오름차순:
시간 설정	
필수 옵션	
인터페이스 패널	
CLI 전환	Console

4.3 WEB 클라이언트 구성

4.3.1 WEB 사용자 관리

4.3.1.1 사용자 계정 만들기

문맥

스위치에 사용자 계정을 추가하여 로컬 사용자 정보를 기반으로 로그인 사용자를 인증하고 권한을 부여할 수 있습니다. 또한 여러 사용자 계정을 만들고 다른 사용자 수준과 암호를 할당하여 사용자 관리를 세분화할 수 있습니다.
관리 사용자만 사용자 계정을 추가할 수 있습니다.

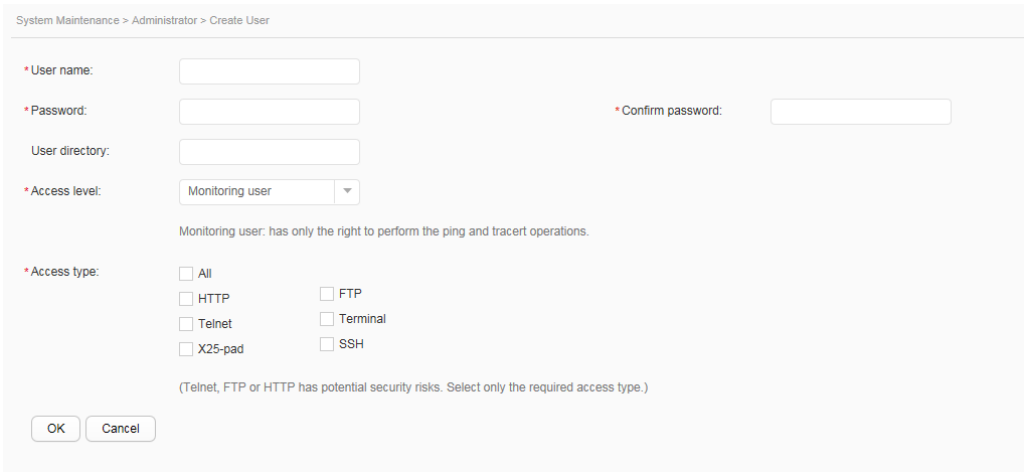
NOTE

동일하거나 더 낮은 수준의 사용자 계정을 만들 수 있습니다.

절차

1. **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > Administrator(관리자)**를 선택합니다.
2. **Create(만들기)**를 클릭합니다. **Create User(사용자 만들기)** 대화 상자가 표시됩니다.
3. **Create User(사용자 만들기)** 페이지에서 **User name(사용자 이름)**, **Password(암호)** 및 **Confirm password(암호 확인)**에 값을 입력하고 그림 1 과 같이 **Access level(접속 수준)** 및 **Access type(접속 유형)**에 대한 값을 선택합니다.

그림 1 사용자 생성



4. Ok(확인)을 클릭합니다.

6.3.1.2 사용자 속성 변경

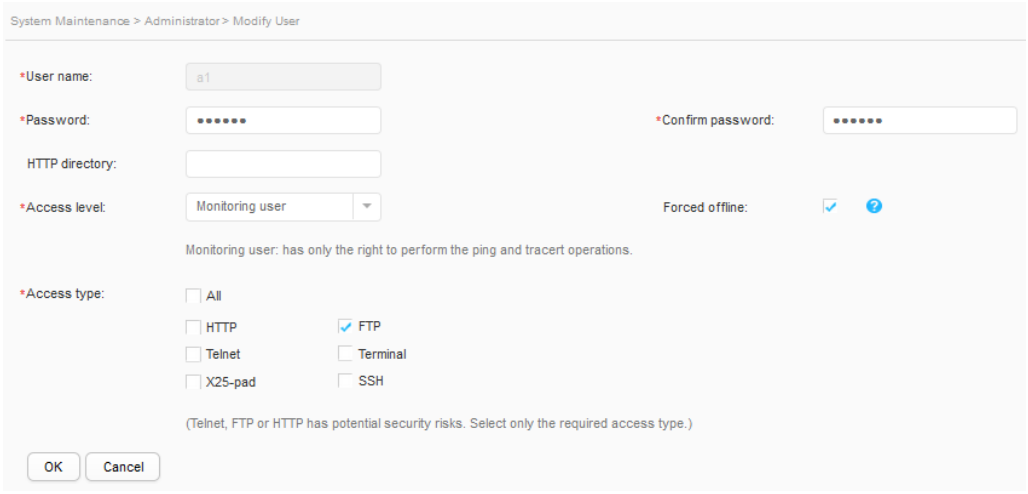
문맥

관리자만 암호와 사용자 수준을 변경할 수 있습니다.

절차

1. **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > Administrator(관리자)**를 선택합니다.
2. **User Name(사용자 이름)** 열 에서 사용자 이름을 클릭하여 사용자 **Modify(수정)** 페이지를 엽니다.
3. **User Modify(사용자 수정)** 페이지에서 **Password(암호)** 및 **Confirm password(암호 확인)**에 값을 입력하고 그림 1 과 같이 **Access level(접속 수준)** 과 **Access type(접속 유형)** 값을 선택합니다.

그림 1 사용자 속성 변경



4. Ok(확인)을 클릭합니다.

6.3.1.3 사용자 속성 변경

문맥

관리 사용자만 사용자 계정을 삭제할 수 있습니다.

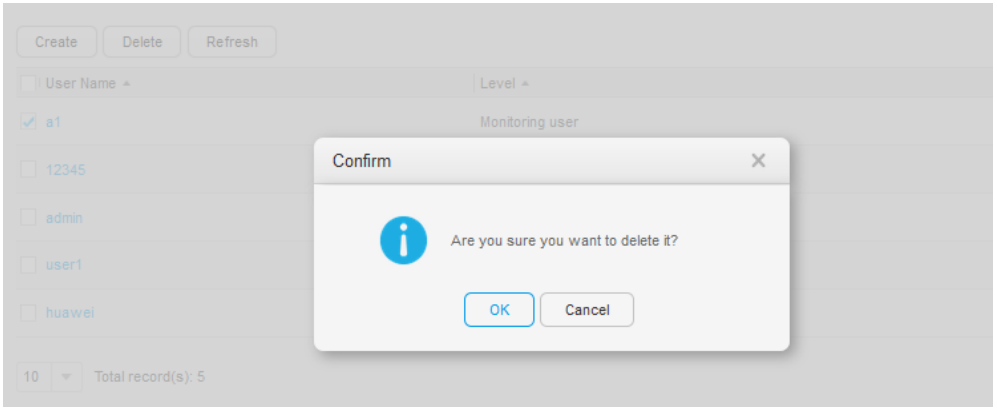
NOTE

- 자신의 사용자 계정을 포함하지 않고 동일하거나 낮은 수준의 사용자 계정을 삭제할 수 있습니다.
- 삭제된 사용자는 복원할 수 없습니다. 삭제할 때 주의하십시오.

절차

1. **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > Administrator(관리자)**를 선택합니다.
2. 삭제할 기록을 선택하고 **Delete(삭제)**를 클릭합니다. 시스템은 그림 1 과 같이 기록 삭제 여부를 묻습니다.

그림 1 사용자 계정 삭제

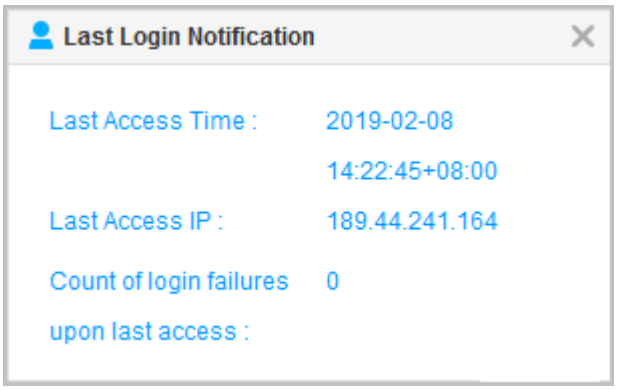


3. Ok(확인)을 클릭합니다.

4.3.2 마지막 로그인 정보

사용자가 웹 시스템에 로그인하면 시스템 은 그림 1 과 같이 페이지 오른쪽 하단에 마지막 로그인 시간, IP 주소 및 로그인 실패 횟수를 자동으로 표시합니다.

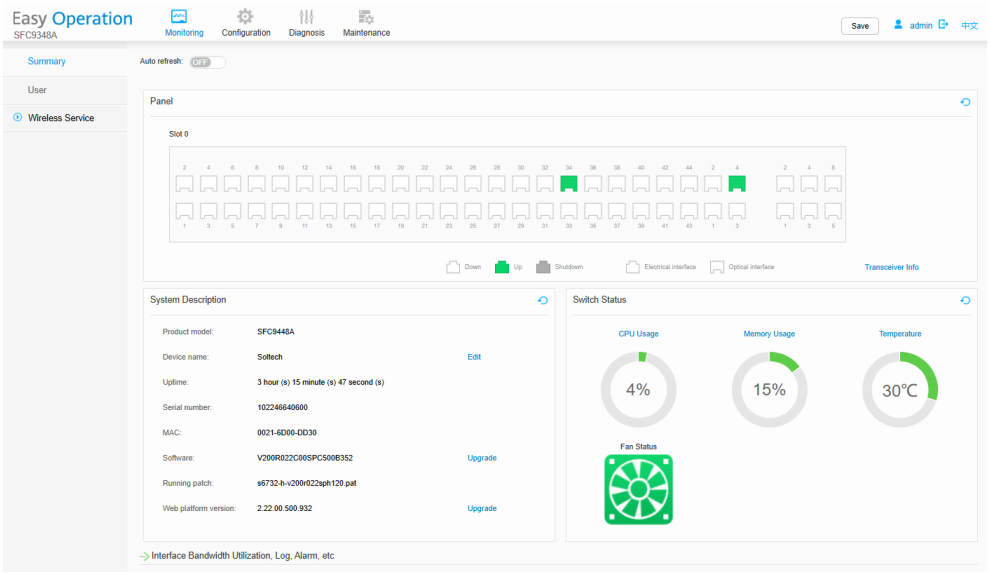
그림 1 마지막 로그인 정보



4.3.3 사용자 시간 초과

웹 시스템 GUI 에서 오랫동안 아무 작업도 수행하지 않으면 로그아웃되고 로그인 페이지가 표시됩니다. 그림 1 은 로그인 페이지를 보여줍니다. 작업을 계속해야 하는 경우 다시 로그인하십시오.

그림 1 로그인 페이지

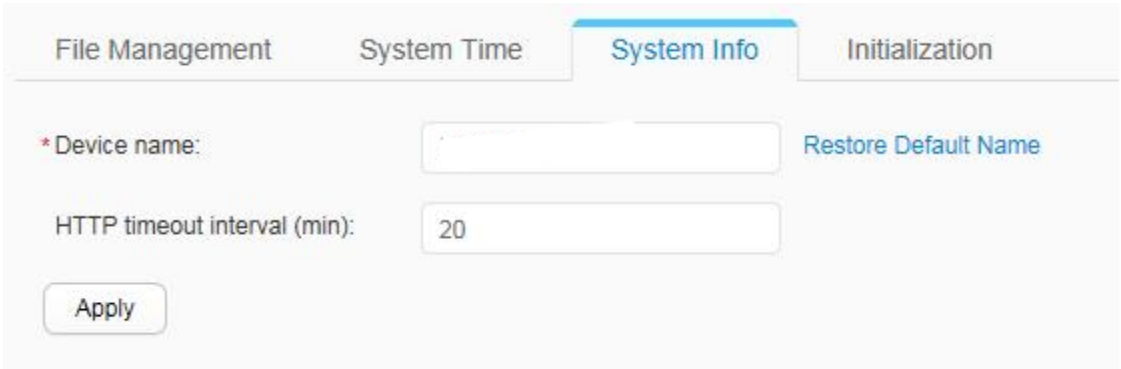


기본적으로 로그인 사용자의 시간 초과 기간은 20 분입니다. **System Info(시스템 정보)** 페이지에서 시간 초과 기간을 변경할 수 있습니다.

시간 초과 기간 변경

Maintenance(유지 관리) > **System Maintenance(시스템 유지 관리)** > **System(시스템)**을 선택하고 그림 2 와 같이 **System Info(시스템 정보)** 페이지에 새로운 타임아웃 기간을 입력합니다. **Apply(적용)**을 클릭합니다.

그림 2 시스템 정보 설정



4.3.4 구성 저장

구성을 수행한 후 구성 데이터를 Save(저장)해야 합니다. 그렇지 않으면 장치가 다시 시작된 후 구성이 손실됩니다.

모든 구성 데이터를 구성 파일에 Save(저장)하려면 오른쪽 상단 모서리에 있는 **Save(저장)**을 클릭합니다.

NOTICE

- 이전 구성 후 오른쪽 상단 모서리에 있는 **Save(저장)**을 클릭합니다. 그렇지 않으면 저장되지 않은 구성이 재부팅 시 손실됩니다.
- 현재 구성 페이지에서 **OK** 또는 **Apply(적용)**을 클릭하면 장치가 작업을 계속하지만 구성을 저장하지 않습니다.

4.3.5 WEB 시스템에서 로그아웃

다음 방법 중 하나로 웹 시스템에서 로그아웃할 수 있습니다.

- 페이지의 오른쪽 상단 모서리를 클릭하여 브라우저를 닫습니다.
- 브라우저의 아무 페이지나 클릭합니다.

NOTE

첫 번째 방법을 사용하는 경우 브라우저를 닫기 전에 구성을 저장하십시오. 그렇지 않으면 구성이 손실됩니다. 두 번째 방법을 사용하는 경우 현재 구성을 저장할 것인지 묻는 메시지가 웹 시스템에 표시됩니다.

4.4 모니터링

4.4.1 패널

문맥

패널 섹션에는 인터페이스 수 및 각 인터페이스의 상태를 포함하여 스위치 패널의 인터페이스에 대한 정보가 표시됩니다. 인터페이스로 마우스를 이동하면 인터페이스 번호와 상태가 표시됩니다.

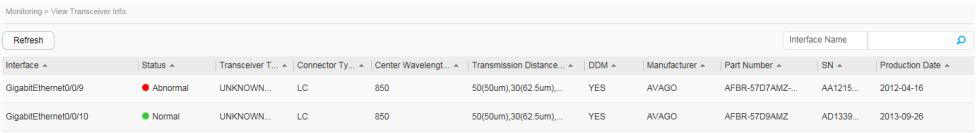
절차

1. 도구 모음에서 **Monitoring(모니터링)**을 클릭합니다. 그림 1 과 같이 패널 다이어그램이 표시됩니다.

   그림 1 패널 다이어그램

2. 장치 패널 아래에서 **View Transceiver Info(트랜시버 정보 보기)**를 클릭합니다. 그림 2 와 같이 광 모듈 정보가 표시됩니다.

   그림 2 광 모듈 정보



NOTE

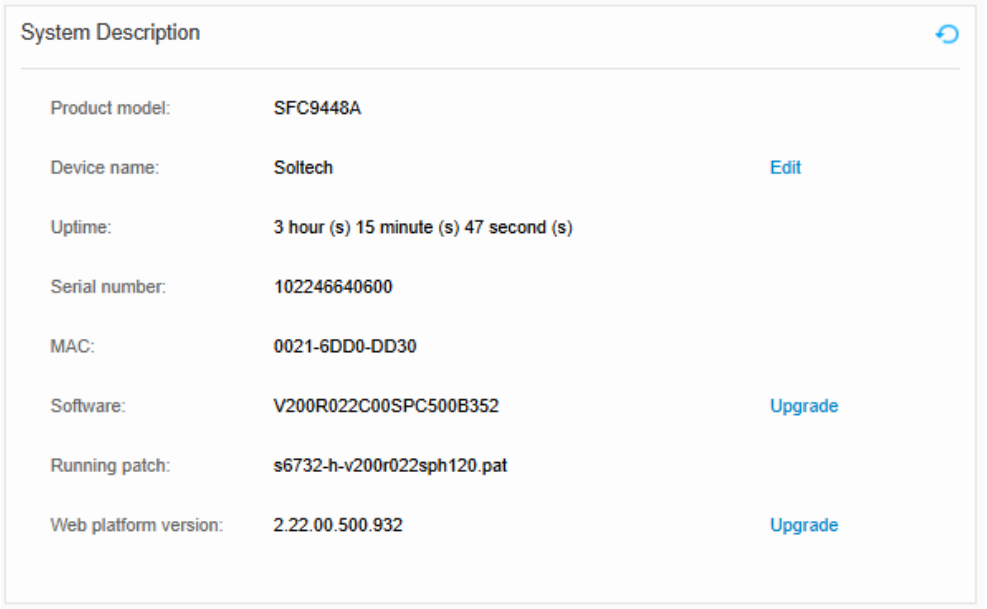
스위치가 스택 모드에 있는 경우 **View Transceiver Info** 매개변수를 사용할 수 없습니다.

4.4.2 시스템 설명

절차

1. 도구 모음에서 **Monitoring(모니터링)**을 클릭합니다. 그림 1 과 같이 스위치의 시스템 설명이 표시됩니다.

그림 1 시스템 설명 섹션



NOTE

여기에 제공된 제품 모델, 소프트웨어 버전 및 기타 제품 정보는 참고용이며 실제 장치 정보와 다를 수 있습니다.

스위치가 NETCONF 모드에 있을 때 장치는 장치 이름을 편집하지 않습니다.

4.4.3 스위치 상태

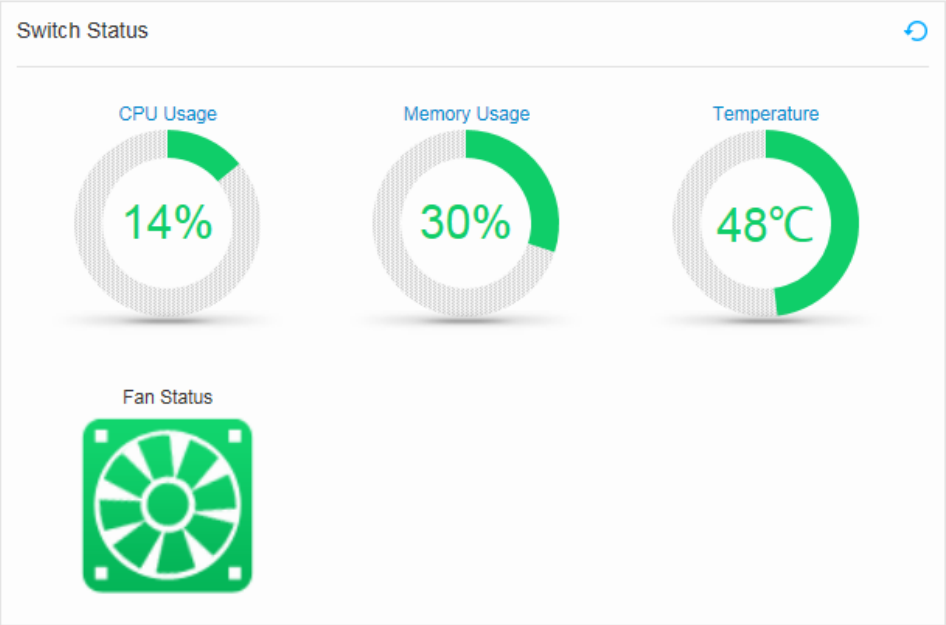
문맥

스위치의 실시간 상태를 보려면 페이지를 새로고침하세요.

절차

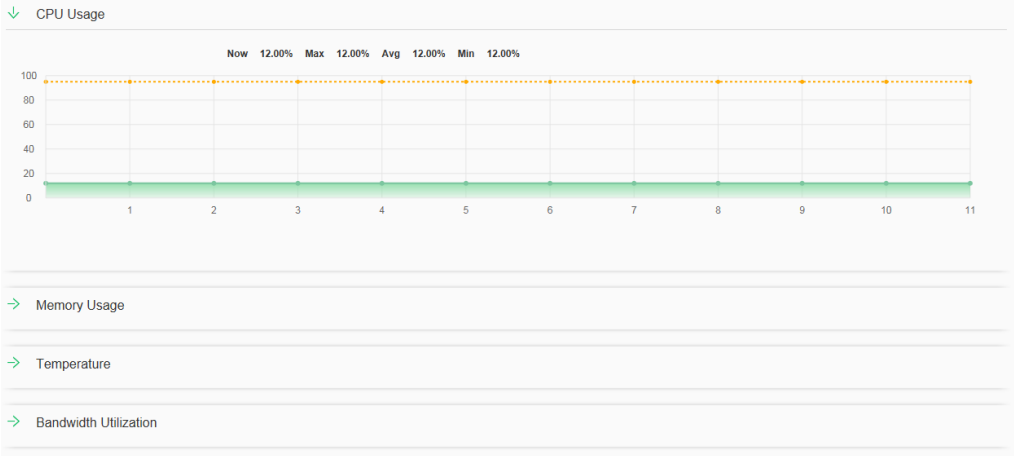
1. 도구 모음에서 **Monitoring(모니터링)**을 클릭합니다. 그림 1 과 같이 스위치 상태가 표시됩니다.

그림 1 스위치 상태 섹션



2. 그림 2 와 같이 **CPU Usage(CPU 사용량)**, **Memory Usage(메모리 사용량)** 및 **Temperature(온도)** 탭을 클릭하여 자세한 상태 정보를 봅니다.

그림 2 상세 상태 정보



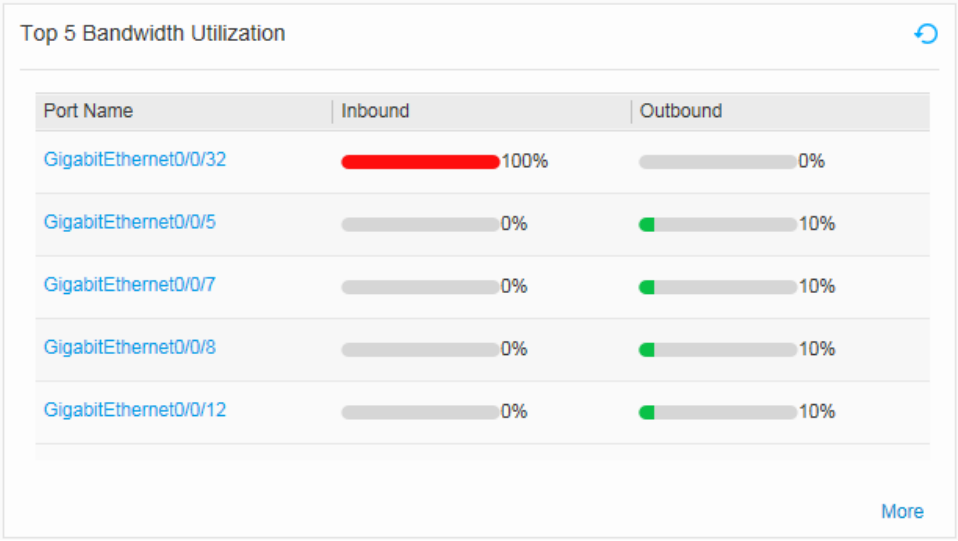
 를 클릭하여 다른 상태 정보 간에 전환할 수 있습니다.

4.4.4 TOP5 대역폭 활용

절차

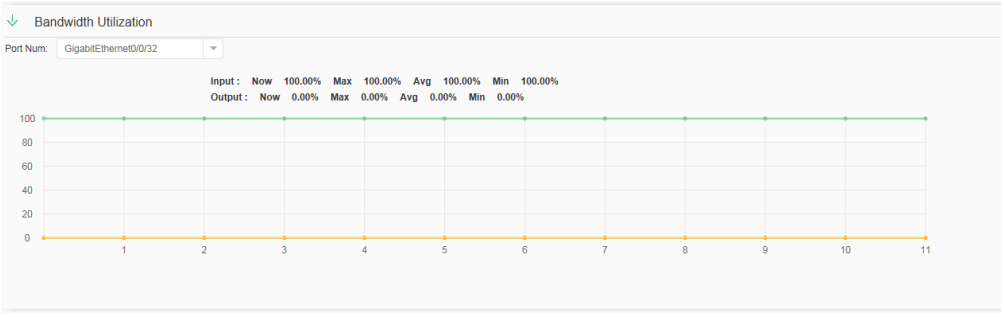
1. **Monitoring(모니터링)**을 클릭하여 **Monitoring(모니터링)** 페이지를 열고 **Interface Bandwidth Utilization, Log, Alarm 등**의 왼쪽에 있는 →을 클릭합니다. 그림 1 과 같이 상위 5 개 인터페이스 대역폭 사용률이 표시됩니다.

   그림 1 상위 5 개 대역폭 사용률



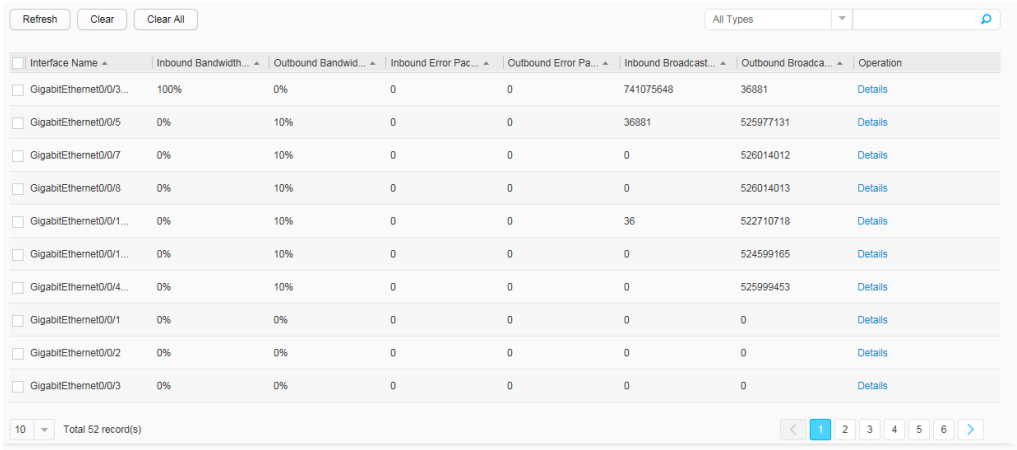
2. 특정 인터페이스의 대역폭 사용률을 보려면 **Port Name(포트 이름)** 아래의 인터페이스를 클릭하십시오. **Bandwidth Utilization(대역폭 사용률)**이 표시됩니다. 페이지에서 그림 2 와 같이 이 인터페이스의 실시간 대역폭 사용률을 볼 수 있습니다.

   그림 2 대역폭 활용



3. 다른 인터페이스의 대역폭 사용률을 보려면 **Top 5 Bandwidth Utilization(상위 5 개 대역폭 사용률)**의 오른쪽 하단 모서리에 있는 **More(자세히)**를 클릭합니다. **Port List(포트 목록)**이 표시됩니다. 그림 3 과 같이 **포트 목록**에서 다른 인터페이스에 대한 자세한 정보를 볼 수 있습니다.

그림 3 포트 목록



다음 방법을 사용하여 **Port List(포트 목록)**에서 특정 인터페이스에 대한 세부 정보를 검색하고 볼 수 있습니다.

a. 드롭다운 목록에서 인터페이스 유형을 선택합니다.

b. 두 번째 검색 상자에 인터페이스 번호를 입력합니다.

c. 을 클릭합니다.

Port List(포트 목록)에서 새로 고침, 지우기 및 모두 지우기 작업을 수행할 수 있습니다.

- 최신 대역폭 사용률을 얻으려면 **Refresh(새로 고침)**을 클릭합니다.
- **Clear(지우기)**를 클릭하여 지정된 인터페이스의 대역폭 사용률을 지우고 페이지를 새로 고칩니다.
- 모든 인터페이스의 대역폭 사용률을 지우고 페이지를 새로 고치려면 **Clear All(모두 지우기)**를 클릭합니다.

표 1 은 **포트 목록**의 매개변수를 설명합니다.

표 1 포트 목록

안건	설명
인터페이스 이름	지정된 유형 및 번호가 있는 인터페이스의 대역폭 사용률입니다.
인바운드 대역폭 사용량	들어오는 트래픽의 대역폭 사용률입니다.
아웃바운드 대역폭 사용량	나가는 트래픽의 대역폭 사용률입니다.
인바운드 오류 패킷	인터페이스에서 수신한 오류 패킷 수입니다.
아웃바운드 오류 패킷	인터페이스에서 보낸 오류 패킷 수입니다.

표 1 포트 목록

안건	설명
인바운드 브로드캐스트 패킷	인터페이스에서 수신한 브로드캐스트 패킷 수입니다.
아웃바운드 브로드캐스트 패킷	인터페이스에서 보낸 브로드캐스트 패킷 수입니다.
작업	**세부 정보**를 클릭하여 인터페이스 및 인터페이스 통계의 실행 상태를 확인합니다.

4.4.5 로그

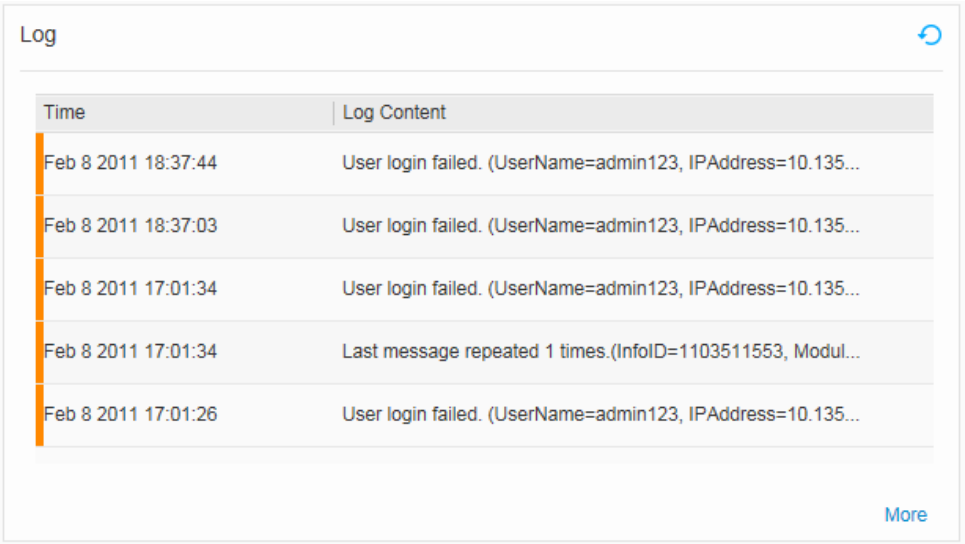
문맥

Moer(더 보기)를 클릭하면 **더** 많은 로그를 볼 수 있습니다.

절차

1. **Monitoring(모니터링)**을 클릭하여 **Monitoring(모니터링)** 페이지를 열고 **Interface Bandwidth Utilization, Log, Alarm 등**의 왼쪽에 있는 →을 클릭합니다. 로그는 그림 1 과 같이 **로그** 섹션에 표시됩니다.

   그림 1 로그 섹션



2. **More(더 보기)**를 클릭하여 **View Log Info(로그 정보 보기)** 페이지를 표시합니다. 이 페이지에서 심각도가 가장 높은 최신 로그를 볼 수 있습니다.

4.4.6 경고

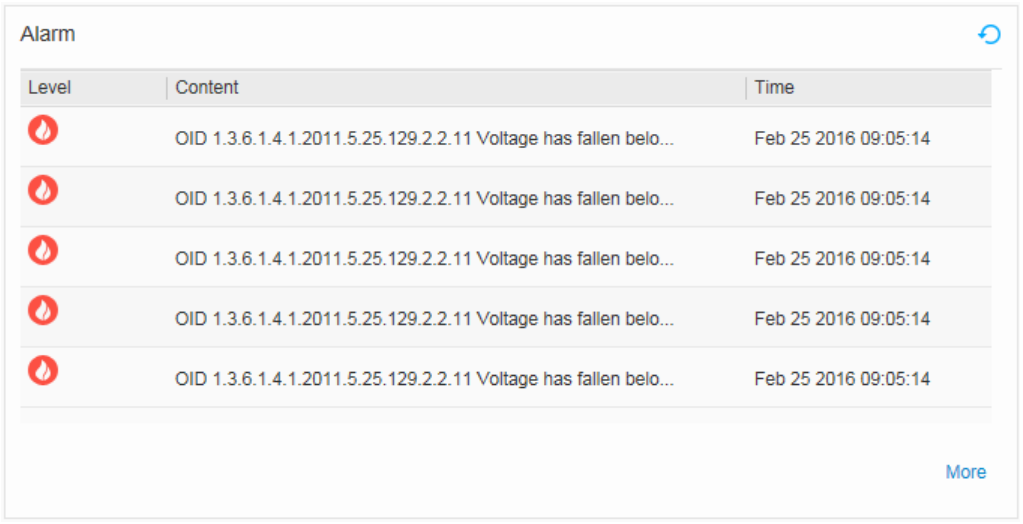
문맥

More(더 보기)를 클릭하면 더 많은 알람을 볼 수 있습니다.

절차

1. **Monitoring(모니터링)**을 클릭하여 **Monitoring(모니터링)** 페이지를 열고 **Interface Bandwidth Utilization, Log, Alarm 등**의 왼쪽에 있는 >을 클릭합니다. 경보는 그림 1 과 같이 **경보** 섹션에 표시됩니다.

그림 1 경보 섹션



2. **More(더 보기)**를 클릭하여 기록 **Historical Alarm & Event(알람 및 이벤트)** 페이지를 표시합니다. 이 페이지에서 최신 알람을 볼 수 있습니다.

4.4.7 전원 상태

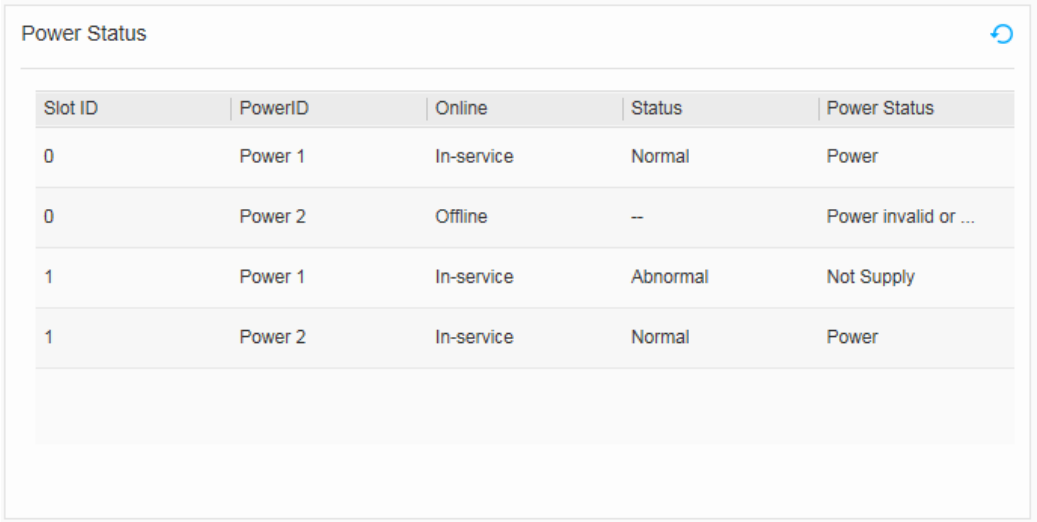
문맥

내부 전원 모듈만 제공하는 비 PoE 장치의 경우 **모니터** 페이지에 **전원 상태** 섹션이 표시되지 않습니다. 장치가 PoE 전원 공급 장치를 지원하지 않는 경우 사용 가능한 총 PoE 전력 및 총 PoE 출력 전력이 **전원 상태** 섹션에 표시되지 않습니다.

절차

1. **Monitoring(모니터링)**을 클릭하여 **Monitoring(모니터링)** 페이지를 열고 **Interface Bandwidth Utilization, Log, Alarm 등**의 왼쪽에 있는을 클릭합니다. 그림 1 과 같이 전원 상태가 표시됩니다.

   그림 1 전원 상태 섹션



4.5 구성

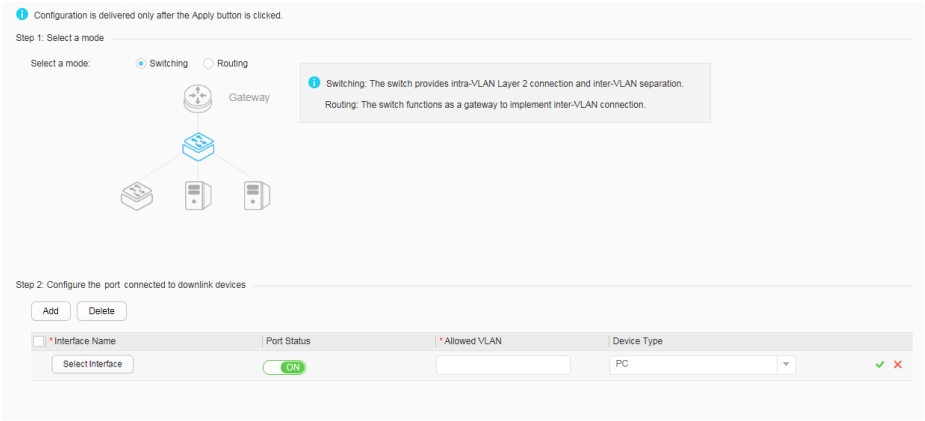
4.5.1 빠른 구성

절차

• 스위칭 모드를 빠르게 구성하십시오.

1. **Configuration(구성)** > **Quick Config(빠른 구성)**을 선택합니다. 그림 1 과 같이 **Select a mode(모드 선택)**에서 **Switching(전환)**을 선택하여 빠른 전환 모드 구성 페이지를 엽니다.

그림 1 빠른 전환 모드 구성



2. **Step 2: Configure the port connected to downlink devices(2 단계 : 다운 링크 장치에 연결된 포트 구성)** 아래의 **Add(추가)**를 클릭하고 매개 변수를 설정한 후 ✔를 클릭합니다.

   표 1 은 표시된 페이지의 매개변수를 설명합니다.

표 1 다운링크 장치에 연결된 포트 구성

매개변수	설명
인터페이스 이름	다운링크 장치에 연결된 인터페이스를 나타냅니다.
포트 상태	선택한 인터페이스의 상태를 나타냅니다. • ON: 인터페이스가 활성화되었음을 나타냅니다. • OFF: 인터페이스가 비활성화되었음을 나타냅니다.
허용된 VLAN	인터페이스가 속한 기본 VLAN 의 ID 를 나타냅니다.
기기 종류	다운스트림 포트에 연결된 장치의 유형을 설정합니다. • PC: 링크 유형은 액세스이며 하나의 VLAN 만 허용됩니다. • 스위치: 링크 유형이 트렁크이며 하나의 VLAN 만 허용됩니다.

NOTE

구성이 완료되면 인터페이스를 클릭하여 구성합니다. 인터페이스를 삭제하려면 **2 단계: 다운링크 장치에 연결된 포트 구성** 아래에서 **삭제를** 클릭합니다.

3. **Step 3: Configure the port connected to the upstream gateway(3 단계: 업스트림 게이트웨이에 연결된 포트 구성)** 아래에서 인터페이스를 선택합니다.

   다음 작업을 선택할 수 있습니다.

- 포트를 선택하려면 하나 이상의 포트 아이콘을 클릭하십시오.
- 마우스를 끌어 연속된 포트를 선택합니다.

표 2 는 표시된 페이지의 매개변수를 설명합니다.

표 2 업스트림 게이트웨이에 연결된 인터페이스 구성

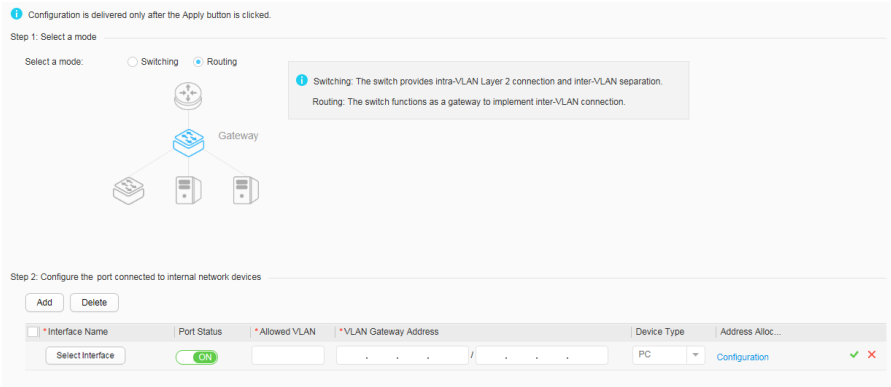
매개변수	설명
포트 상태	선택한 인터페이스의 상태를 나타냅니다. • ON: 인터페이스가 활성화되었음을 나타냅니다. • OFF: 인터페이스가 비활성화되었음을 나타냅니다.
링크 집계	링크 집계가 활성화되었음을 나타냅니다. • ON: 링크 집계가 활성화되었음을 나타냅니다. • OFF: 링크 집계가 비활성화되었음을 나타냅니다.
링크 집계 ID	링크 집계 ID 를 나타냅니다. 이 매개변수는 링크 집계 상태가 **ON 일** 때 유효합니다.
허용된 VLAN	Link Aggregation 유형의 인터페이스가 추가되는 VLAN 을 나타냅니다.

4. 매개변수를 설정한 후 **Apply(적용)을 클릭**합니다.

• 라우팅 모드를 빠르게 구성하십시오.

1. **Configuration(구성)** > **Quick Config(빠른 구성)**을 선택합니다. 그림 2 와 같이 빠른 라우팅 모드 구성 페이지를 열려면 **Select a mode(모드 선택)**에서 **Routing(라우팅)**을 선택합니다.

그림 2 빠른 라우팅 모드 구성



2. **Step 2: Configure the port connected to downlink devices(2 단계 : 다운 링크 장치에 연결된 포트 구성)** 아래의 **Add(추가)**를 클릭하고 매개 변수를 설정한 후 ✔를 클릭합니다.

   표 3 은 표시된 페이지의 매개변수를 설명합니다.

표 3 내부 네트워크 장치에 연결된 포트 구성

매개변수	설명
인터페이스 이름	내부 네트워크 장치에 연결된 인터페이스를 나타냅니다.
포트 상태	선택한 인터페이스의 상태를 나타냅니다. ON: 인터페이스가 활성화되었음을 나타냅니다. OFF: 인터페이스가 비활성화되었음을 나타냅니다.
허용된 VLAN	인터페이스가 속한 기본 VLAN 의 ID 를 나타냅니다.
VLAN 게이트웨이 주소	인터페이스의 IP 주소와 서브넷 마스크를 나타냅니다.
기기 종류	내부 네트워크에 연결된 장치의 종류를 설정합니다. PC: 링크 유형은 액세스이며 하나의 VLAN 만 허용됩니다. 스위치: 링크 유형이 트렁크이며 하나의 VLAN 만 허용됩니다.
터미널에 대한 주소 할당	**구성**을 클릭하여 터미널에 대한 주소 할당 모드를 선택합니다. 공전 DHCP(로컬 서버) DHCP(원격 서버)

NOTE

구성이 완료되면 인터페이스를 클릭하여 구성합니다. 인터페이스를 삭제하려면 **2 단계: 내부 네트워크 장치에 연결된 포트 구성** 아래에서 **삭제를** 클릭합니다.

3. **Step 3: Configure the port connected to the upstream gateway(3 단계: 업스트림 게이트웨이에 연결된 포트 구성)** 아래에서 인터페이스를 선택합니다.

   다음 작업을 선택할 수 있습니다.

   - 포트를 선택하려면 하나 이상의 포트 아이콘을 클릭하십시오.
   - 마우스를 끌어 연속된 포트를 선택합니다.

   표 4 는 표시된 페이지의 매개변수를 설명합니다.

표 4 외부 네트워크를 켜기 위해 연결된 포트 설정

매개변수	설명
포트 상태	선택한 인터페이스의 상태를 나타냅니다. ON: 인터페이스가 활성화되었음을 나타냅니다. OFF: 인터페이스가 비활성화되었음을 나타냅니다.
링크 집계	링크 집계가 활성화되었음을 나타냅니다. ON: 링크 집계가 활성화되었음을 나타냅니다. OFF: 링크 집계가 비활성화되었음을 나타냅니다.
링크 집계 ID	링크 집계 ID 를 나타냅니다. 이 매개변수는 링크 집계 상태가 **ON 일** 때 유효합니다.
허용된 VLAN	Link Aggregation 유형의 인터페이스가 추가되는 VLAN 을 나타냅니다.
연결된 IP 주소/마스크	인터페이스의 IP 주소와 서브넷 마스크를 나타냅니다.
다음 홉	경로의 다음 홉 주소를 나타냅니다.

4. 매개변수를 설정한 후 **Apply(적용)**을 클릭합니다.

4.5.2 기본 서비스

4.5.2.1 인터페이스 설정

4.5.2.1.1 구성 보기

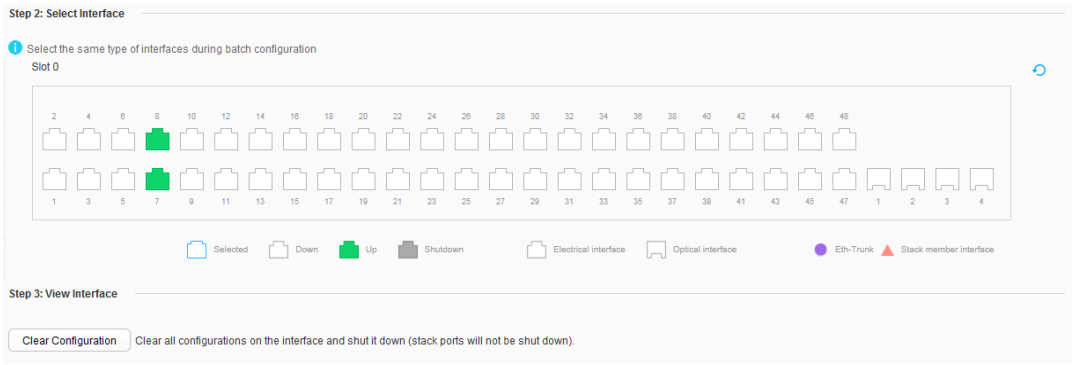
문맥

이 페이지에서 인터페이스 관련 기능을 볼 수 있습니다.

절차

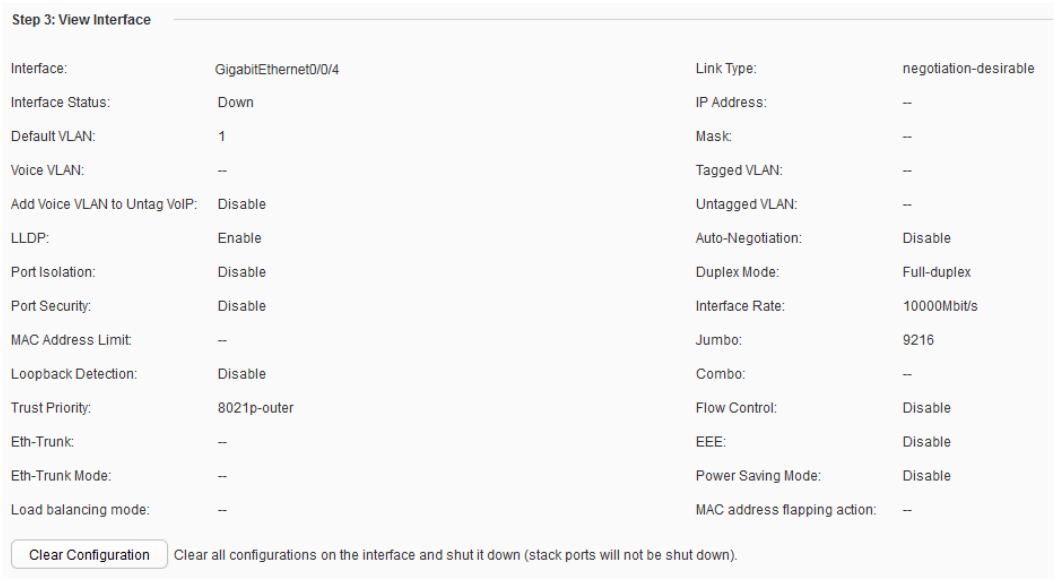
1. 선택 **Configuration(구성) > 기본 서비스** > **인터페이스 설정** > **서비스 인터페이스 설정을** . 그림 1 과 같이 **View Configuration 을** 클릭합니다.

   그림 1 구성 보기



2. 인터페이스 아이콘을 클릭하여 인터페이스를 선택합니다. 한 번에 하나의 인터페이스만 선택할 수 있습니다.
3. 그림 2 와 같이 3 단계에서 인터페이스 기능을 확인합니다.

그림 2 인터페이스 속성 보기



4. 인터페이스의 모든 구성을 삭제하여 기본 설정을 복원하려면 **구성 지우기를** 클릭합니다. 구성이 삭제되면 인터페이스가 비활성화됩니다.

4.5.2.1.2 PC 에 연결

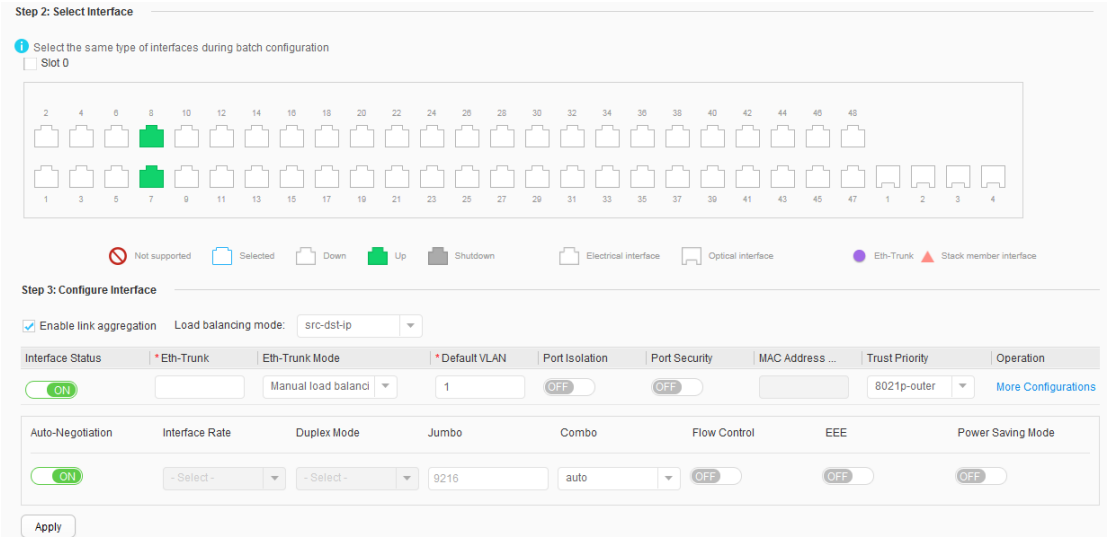
문맥

스위치를 PC 에 연결한 후 서비스 요구 사항에 따라 기본 VLAN, 포트 보안, 포트 격리 등의 기능을 구성할 수 있습니다.

절차

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **Interface Settings(인터페이스 설정)** > **Service Interface Setting(서비스 인터페이스 설정)**을 선택합니다. 그림 1 과 같이 **Connect to PC(PC 에 연결)**을 클릭합니다.

2. **그림 1** PC 에 연결된 포트 설정하기



3. 구성할 포트를 선택합니다. 포트 영역에서 필요에 따라 다음 작업을 수행합니다.
   - 포트 아이콘을 클릭합니다. 포트 선택을 취소하려면 포트 아이콘을 다시 클릭합니다.
   - 커서를 끌어 배치에서 연속 포트를 선택합니다.
   - 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
   - 패널 이 있는 슬롯을 선택합니다. 패널의 모든 포트가 선택됩니다.

4. 포트를 구성합니다.

표 1 은 매개변수와 해당 값을 설명합니다.

표 1 매개변수 및 해당 값

매개변수	설명
부하 분산 모드	Eth-Trunk 로드 밸런싱 모드를 설정합니다. 이 매개변수는 **링크 집계 사용**을 선택한 후에만 유효합니다. dst-ip: 목적지 IP 주소를 기준으로 부하 분산을 수행합니다. dst-mac: 목적지 MAC 주소를 기반으로 부하 분산을 수행합니다. src-ip: 소스 IP 주소를 기반으로 로드 밸런싱을 수행합니다. src-mac: 소스 MAC 주소를 기반으로 로드 밸런싱을 수행합니다. src-dst-ip: 소스와 목적지 IP 주소의 Exclusive-OR 계산 결과를 기반으로 로드 밸런싱을 수행합니다. src-dst-mac: 소스 및 목적지 MAC 주소의 Exclusive-OR 계산 결과를 기반으로 로드 밸런싱을 수행합니다.
인터페이스 상태	인터페이스를 활성화하거나 비활성화합니다. ON: 인터페이스가 활성화됩니다. OFF: 인터페이스가 비활성화됩니다.
E-트렁크	Eth-Trunk 에 인터페이스를 추가합니다. **이 매개변수는 링크 집계 활성화**를 선택한 후에만 설정할 수 있습니다.
이더넷 트렁크 모드	Eth-Trunk 작업 모드를 설정합니다. **이 매개변수는 링크 집계 활성화**를 선택한 후에만 설정할 수 있습니다. 수동 로드 밸런싱(기본값): Eth-Trunk 작업 모드가 수동으로 설정됩니다. Static LACP: Eth-Trunk 작업 모드가 LACP 로 설정됩니다.
기본 VLAN	기본 VLAN 에 인터페이스를 추가합니다. VLAN ID 의 범위는 1~4094 입니다.
포트 격리	포트 격리를 활성화하거나 비활성화합니다. ON: 포트 격리가 활성화됩니다. OFF: 포트 격리가 비활성화됩니다.
항구 보안	포트 보안을 활성화하거나 비활성화합니다. ON: 포트 보안이 활성화됩니다. OFF: 포트 보안이 비활성화됩니다.
MAC 주소 제한	**포트 보안 이 ON** 으로 설정되어 있을 때 유효합니다.

표 1 매개변수 및 해당 값

매개변수	**설명**
	보안 MAC 주소의 최대 수를 설정합니다. 값 범위는 1 ~ 1024 입니다.
루프백 감지	루프백 감지를 활성화하거나 비활성화합니다. **이 매개변수는 링크 집계 사용**을 선택하지 않은 경우에만 설정할 수 있습니다. ON: 루프백 감지가 활성화됩니다. OFF: 루프백 감지가 비활성화됩니다.
신뢰 우선 순위	인터페이스에 대한 신뢰 우선 순위를 구성합니다. **노트:** 값은 스위치 모델에 따라 다릅니다. 스위치의 값은 이 예에서 제공된 값과 다를 수 있습니다.
작업 **추가 구성**을 클릭 하면 다음 매개변수가 유효합니다.	
자동 협상	인터페이스에서 자동 협상을 활성화하거나 비활성화합니다. ON: 자동 협상이 활성화됩니다. OFF: 자동 협상이 비활성화됩니다.
이중 모드	**Auto-Negotiation 이 OFF** 로 설정되어 있을 때 유효합니다. 인터페이스에서 이중 모드를 구성합니다. 전이중 반이중
인터페이스 속도	**Auto-Negotiation 이 OFF** 로 설정되어 있을 때 유효합니다. 인터페이스 속도를 구성합니다. 10Mbit/s 100Mbit/s 1000Mbit/s
커다란 것	점보 프레임 길이를 설정합니다.
콤보	콤보 인터페이스의 작업 모드를 구성합니다. auto: 콤보 인터페이스가 작업 모드를 자동으로 선택합니다. 구리: 콤보 인터페이스는 전기 인터페이스로 작동하며 네트워크 케이블을 사용하여 데이터를 송수신합니다.

표 1 매개변수 및 해당 값

매개변수	**설명**
	광섬유: 콤보 인터페이스는 광학 인터페이스로 작동하며 광섬유를 사용하여 데이터를 송수신합니다.
흐름 제어	흐름 제어 활성화 또는 비활성화: ON: 흐름 제어가 활성화됩니다. OFF: 흐름 제어가 비활성화됩니다.
EEE	이 매개변수는 **자동 협상** 이 **ON** 으로 설정된 경우에 유효 합니다. EEE 기능을 활성화하거나 비활성화합니다. ON: EEE 기능이 활성화됩니다. OFF: EEE 기능이 비활성화됩니다.
절전 모드	절전 모드 활성화 또는 비활성화: ON: 절전 모드가 활성화됩니다. OFF: 절전 모드가 비활성화됩니다.

5. **Apply(적용)**을 클릭하여 구성을 적용합니다.

4.5.2.1.3 IP 전화에 연결

문맥

스위치가 IP 폰에 연결되면 서비스 요구 사항에 따라 기본 VLAN, 음성 VLAN, 포트 보안 및 포트 격리와 같은 기능을 구성할 수 있습니다.

절차

• 전화 모델 기반(자동)

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **Interface Settings(인터페이스 설정)** > **Service Interface Setting(서비스 인터페이스 설정)**을 선택합니다. **Connect to IP Phone(IP Phone 에 연결)**을 클릭하여 **Connect to IP Phone(IP Phone 에 연결)** 페이지를 엽니다.
2. 구성할 포트를 선택합니다. 포트 영역에서 필요에 따라 다음 작업을 수행합니다.
    - 포트 아이콘을 클릭합니다. 포트 선택을 취소하려면 포트 아이콘을 다시 클릭합니다.
    - 커서를 끌어 배치에서 연속 포트를 선택합니다.
    - 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
    - 패널 이 있는 슬롯을 선택합니다. 패널의 모든 포트 가 선택됩니다.
3. **Based On Phone Model (Auto)(기반에 전화 모델 (자동))** 탭을 클릭하고 **Auto Phone Scan(자동 전화 스캔)**을 클릭합니다. 인터페이스가 IP 폰에 연결되어 있는지 확인하십시오. 그림 1 은 인터페이스가 IP 전화에 연결되어 있지 않음을 나타내고 그림 2 는 인터페이스가 IP 전화에 연결되어 있음을 나타냅니다.

그림 1 자동 전화 스캔 결과 - 연결된 IP 전화 없음

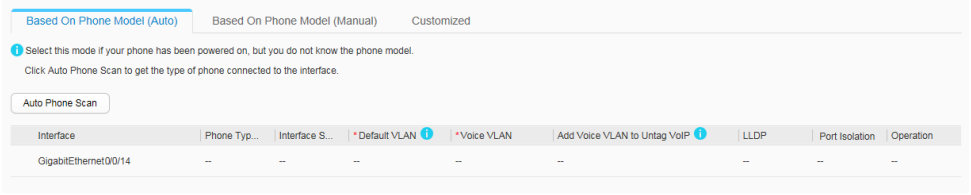


그림 2 자동 전화 스캔 결과 - IP 전화 연결

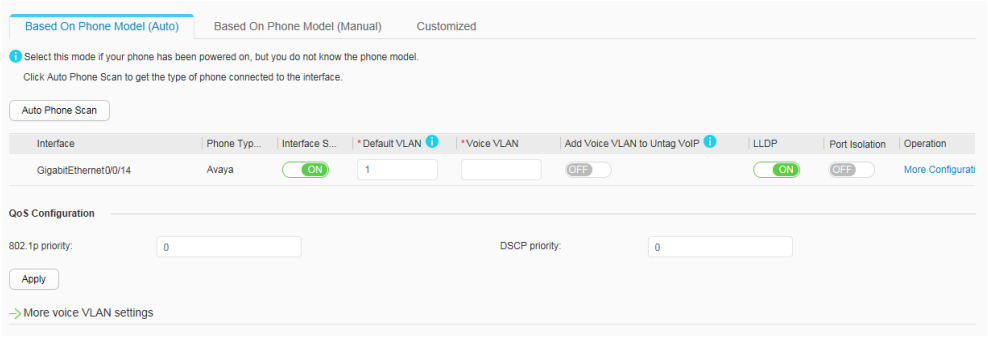


표 1 은 그림 2 의 구성 옵션을 설명합니다.

표 1 자동 전화 스캔 매개변수

매개변수	설명
상호 작용	IP 전화가 스캔되는 인터페이스입니다.
전화 유형	스캔한 인터페이스에 연결된 IP 전화의 유형입니다.
인터페이스 상태	인터페이스를 활성화하거나 비활성화합니다. ON: 인터페이스가 활성화됩니다. OFF: 인터페이스가 비활성화됩니다.
기본 VLAN	기본 VLAN 에 인터페이스를 추가합니다. VLAN ID 의 범위는 1~4094 입니다.
음성 VLAN	음성 VLAN 기능을 활성화하고 VLAN ID 를 지정합니다.
VoIP 태그를 해제하기 위해 음성 VLAN 추가	태그가 지정되지 않은 패킷에 음성 VLAN ID 를 추가하는 기능을 활성화하거나 비활성화합니다. ON: 기능이 활성화됩니다. OFF: 기능이 비활성화됩니다.
LLDP	LLDP 상태: 켜짐: 활성화됨 꺼짐: 비활성화

표 1 자동 전화 스캔 매개변수

매개변수	설명
포트 격리	포트 격리 활성화 또는 비활성화: ON: 포트 격리가 활성화됩니다. OFF: 포트 격리가 비활성화됩니다.
작업 **추가 구성**을 클릭 하면 다음 매개변수가 유효합니다.	
항구 보안	포트 보안 활성화 또는 비활성화: ON: 포트 보안이 활성화됩니다. OFF: 포트 보안이 비활성화됩니다.
MAC 주소 제한	**포트 보안** 이 **ON** 으로 설정되어 있을 때 유효합니다. 보안 MAC 주소의 최대 수를 설정합니다. 값 범위는 1 에서 1024 사이 입니다.
루프백 감지	루프백 감지 활성화 또는 비활성화: ON: 루프백 감지가 활성화됩니다. OFF: 루프백 감지가 비활성화됩니다.
자동 협상	인터페이스에서 자동 협상을 활성화 또는 비활성화합니다. ON: 자동 협상이 활성화됩니다. OFF: 자동 협상이 비활성화됩니다.
이중 모드	**Auto-Negotiation** 이 **OFF** 로 설정되어 있을 때 유효합니다. 인터페이스에서 이중 모드를 구성합니다. 전이중 반이중
인터페이스 속도	**Auto-Negotiation** 이 **OFF** 로 설정되어 있을 때 유효합니다. 인터페이스 속도를 구성합니다. 10Mbit/s 100Mbit/s 1000Mbit/s
커다란 것	점보 프레임 길이를 설정합니다.

표 1 자동 전화 스캔 매개변수

매개변수	설명
콤보	콤보 인터페이스의 작업 모드를 구성합니다. auto: 콤보 인터페이스가 작업 모드를 자동으로 선택합니다. 구리: 콤보 인터페이스는 전기 인터페이스로 작동하며 네트워크 케이블을 사용하여 데이터를 송수신합니다. 광섬유: 콤보 인터페이스는 광학 인터페이스로 작동하며 광섬유를 사용하여 데이터를 송수신합니다.
흐름 제어	흐름 제어 활성화 또는 비활성화: ON: 흐름 제어가 활성화됩니다. OFF: 흐름 제어가 비활성화됩니다.
NS	**Auto-Negotiation** 이 **ON** 으로 설정되어 있을 때 유효합니다. EEE 기능을 활성화하거나 비활성화합니다. ON: EEE 기능이 활성화됩니다. OFF: EEE 기능이 비활성화됩니다.
절전 모드	절전 모드 활성화 또는 비활성화: ON: 절전 모드가 활성화됩니다. OFF: 절전 모드가 비활성화됩니다.
QoS 구성	
802.1p 우선 순위	802.1p 우선 순위를 지정합니다.
DSCP 우선 순위	DSCP 우선 순위를 지정합니다.

4. 매개변수를 설정한 후 **Apply(적용)**을 클릭합니다.
5. **More voice VLAN settings(추가 음성 VLAN 설정)** 왼쪽의 →을 클릭하여 음성 VLAN 구성을 확장합니다. 그림 3 과 같이 **Create(생성)**을 클릭하여 음성 VLAN 의 구성 옵션을 표시합니다.

그림 3 음성 VLAN 구성

표 2 는 표시된 페이지의 매개변수를 설명합니다.

표 2 음성 VLAN 생성 매개변수

매개변수	설명
위	이 매개변수는 필수입니다. 음성 패킷의 MAC 주소를 지정합니다(예: 0812-f231-05e1).
마스크	이 매개변수는 필수입니다. 마스크를 입력합니다(예: ffff-ffff-ffff).
설명	OUI 에 대한 설명을 입력합니다.

매개변수를 설정한 후 ✔을 클릭합니다.

- 전화 모델 기반(수동)

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **Interface Settings(인터페이스 설정)** > **Service Interface Setting(서비스 인터페이스 설정)**을 선택합니다. **Connect to IP Phone(IP Phone 에 연결)**을 클릭하여 **Connect to IP Phone(IP Phone 에 연결)** 페이지를 엽니다.

2. 그림 4 와 같이 **Select Interface(인터페이스 선택)**에서 인터페이스를 선택하고 **Based On Phone Model(Manual)** 탭을 클릭합니다.

그림 4 전화기 종류에 따른(수동)

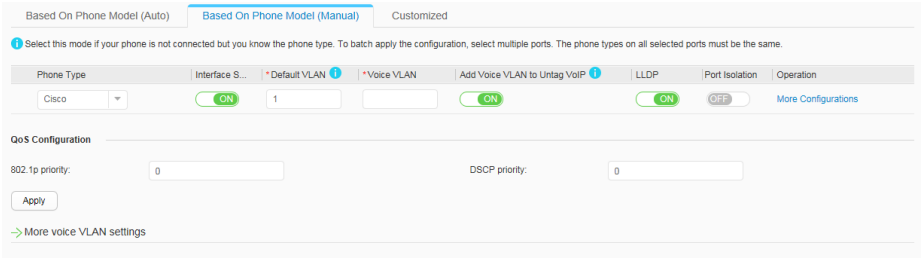


표 3 은 그림 4 의 구성 옵션을 설명합니다.

표 3 전화 유형(수동) 매개변수 기반

매개변수	설명
전화 유형	연결된 전화의 유형입니다.
인터페이스 상태	인터페이스를 활성화하거나 비활성화합니다. ON: 인터페이스가 활성화됩니다.

표 3 전화 유형(수동) 매개변수 기반

매개변수	설명
	OFF: 인터페이스가 비활성화됩니다.
기본 VLAN	기본 VLAN 에 인터페이스를 추가합니다. VLAN ID 의 범위는 1~4094 입니다.
음성 VLAN	음성 VLAN 기능을 활성화하고 VLAN ID 를 지정합니다.
VoIP 태그를 해제하기 위해 음성 VLAN 추가	태그가 지정되지 않은 패킷에 음성 VLAN ID 를 추가하는 기능을 활성화 또는 비활성화합니다. ON: 기능이 활성화됩니다. OFF: 기능이 비활성화됩니다.
LLDP	LLDP 상태: 켜짐: 활성화됨 꺼짐: 비활성화
포트 격리	포트 격리 활성화 또는 비활성화: ON: 포트 격리가 활성화됩니다. OFF: 포트 격리가 비활성화됩니다.
작업 **추가 구성**을 클릭 하면 다음 매개변수가 유효합니다.	
항구 보안	포트 보안 활성화 또는 비활성화: ON: 포트 보안이 활성화됩니다. OFF: 포트 보안이 비활성화됩니다.
MAC 주소 제한	**포트 보안** 이 **ON** 으로 설정되어 있을 때 유효합니다. 보안 MAC 주소의 최대 수를 설정합니다. 값 범위는 1 에서 1024 사이 입니다.
루프백 감지	루프백 감지 활성화 또는 비활성화: ON: 루프백 감지가 활성화됩니다. OFF: 루프백 감지가 비활성화됩니다.
자동 협상	인터페이스에서 자동 협상을 활성화 또는 비활성화합니다. ON: 자동 협상이 활성화됩니다.

표 3 전화 유형(수동) 매개변수 기반

매개변수	설명
	OFF: 자동 협상이 비활성화됩니다.
이중 모드	**Auto-Negotiation** 이 **OFF** 로 설정되어 있을 때 유효합니다. 인터페이스에서 이중 모드를 구성합니다. 전이중 반이중
인터페이스 속도	**Auto-Negotiation** 이 **OFF** 로 설정되어 있을 때 유효합니다. 인터페이스 속도를 구성합니다. 10Mbit/s 100Mbit/s 1000Mbit/s
커다란 것	점보 프레임 길이를 설정합니다.
콤보	콤보 인터페이스의 작업 모드를 구성합니다. auto: 콤보 인터페이스가 작업 모드를 자동으로 선택합니다. 구리: 콤보 인터페이스는 전기 인터페이스로 작동하며 네트워크 케이블을 사용하여 데이터를 송수신합니다. 광섬유: 콤보 인터페이스는 광학 인터페이스로 작동하며 광섬유를 사용하여 데이터를 송수신합니다.
흐름 제어	흐름 제어 활성화 또는 비활성화: ON: 흐름 제어가 활성화됩니다. OFF: 흐름 제어가 비활성화됩니다.
NS	**Auto-Negotiation** 이 **ON** 으로 설정되어 있을 때 유효합니다. EEE 기능을 활성화하거나 비활성화합니다. ON: EEE 기능이 활성화됩니다. OFF: EEE 기능이 비활성화됩니다.
절전 모드	절전 모드 활성화 또는 비활성화: ON: 절전 모드가 활성화됩니다. OFF: 절전 모드가 비활성화됩니다.
QoS 구성	

표 3 전화 유형(수동) 매개변수 기반

매개변수	설명
802.1p 우선 순위	802.1p 우선 순위를 지정합니다.
DSCP 우선 순위	DSCP 우선 순위를 지정합니다.

3. 매개변수를 설정한 후 **Apply(적용)을 클릭**합니다.
4. **More voice VLAN settings(추가 음성 VLAN 설정)** 왼쪽의 →을 클릭하여 음성 VLAN 구성을 확장합니다. **Create(생성)을** 클릭하면 그림 5 와 같이 음성 VLAN 의 구성 옵션이 표시됩니다.

   그림 5 음성 VLAN 구성

   표 4 는 표시된 페이지의 매개변수를 설명합니다.

표 4 음성 VLAN 생성 매개변수

매개변수	설명
위	이 매개변수는 필수입니다. 음성 패킷의 MAC 주소를 지정합니다(예: 0812-f231-05e1).
마스크	이 매개변수는 필수입니다. 마스크를 입력합니다(예: ffff-ffff-ffff).
설명	OUI 에 대한 설명을 입력합니다.

   매개변수를 설정한 후 ✔을 클릭합니다.

• 맞춤형 구성

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **Interface Settings(인터페이스 설정)** > **Service Interface Setting(서비스 인터페이스 설정)**을 선택합니다. **Connect to IP Phone(IP Phone 에 연결)**을 클릭하여 **Connect to IP Phone(IP Phone 에 연결)** 페이지를 엽니다.
2. **Select Interface(인터페이스 선택)**에서 인터페이스를 선택하고 그림 6 과 같이 **Customized** 탭을 클릭합니다.

그림 6 맞춤형 구성

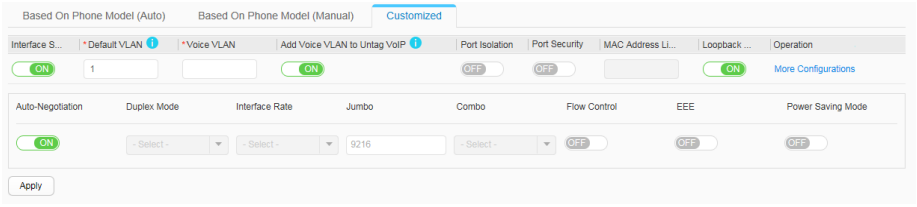


표 5 는 그림 6 의 구성 옵션을 설명합니다.

표 5 사용자 지정 구성 옵션 및의미

매개변수	설명
인터페이스 상태	인터페이스를 활성화하거나 비활성화합니다. • ON: 인터페이스가 활성화됩니다. • OFF: 인터페이스가 비활성화됩니다.
기본 VLAN	기본 VLAN 에 인터페이스를 추가합니다. VLAN ID 의 범위는 1~4094 입니다.
음성 VLAN	음성 VLAN 기능을 활성화하고 VLAN ID 를 지정합니다.
VoIP 태그를 해제하기 위해 음성 VLAN 추가	태그가 지정되지 않은 패킷에 음성 VLAN ID 를 추가하는 기능을 활성화 또는 비활성화합니다. • ON: 기능이 활성화됩니다. • OFF: 기능이 비활성화됩니다.
포트 격리	포트 격리 활성화 또는 비활성화: • ON: 포트 격리가 활성화됩니다. • OFF: 포트 격리가 비활성화됩니다.
항구 보안	포트 보안 활성화 또는 비활성화: • ON: 포트 보안이 활성화됩니다. • OFF: 포트 보안이 비활성화됩니다.
MAC 주소 제한	**포트 보안** 이 **ON** 으로 설정되어 있을 때 유효합니다. 보안 MAC 주소의 최대 수를 설정합니다. 값 범위는 1 에서 1024 사이 입니다.
루프백 감지	루프백 감지 활성화 또는 비활성화: • ON: 루프백 감지가 활성화됩니다. • OFF: 루프백 감지가 비활성화됩니다.

표 5 사용자 지정 구성 옵션 및의미

매개변수	**설명**
작업 **추가 구성**을 클릭 하면 다음 매개변수가 유효합니다.	
자동 협상	인터페이스에서 자동 협상을 활성화 또는 비활성화합니다. • ON: 자동 협상이 활성화됩니다. • OFF: 자동 협상이 비활성화됩니다.
이중 모드	**Auto-Negotiation** 이 **OFF** 로 설정되어 있을 때 유효합니다. 인터페이스에서 이중 모드를 구성합니다. • 전이중 • 반이중
인터페이스 속도	**Auto-Negotiation** 이 **OFF** 로 설정되어 있을 때 유효합니다. 인터페이스 속도를 구성합니다. • 10Mbit/s • 100Mbit/s • 1000Mbit/s
커다란 것	점보 프레임 길이를 설정합니다.
콤보	콤보 인터페이스의 작업 모드를 구성합니다. • auto: 콤보 인터페이스가 작업 모드를 자동으로 선택합니다. • 구리: 콤보 인터페이스는 전기 인터페이스로 작동하며 네트워크 케이블을 사용하여 데이터를 송수신합니다. • 광섬유: 콤보 인터페이스는 광학 인터페이스로 작동하며 광섬유를 사용하여 데이터를 송수신합니다.
흐름 제어	흐름 제어 활성화 또는 비활성화: • ON: 흐름 제어가 활성화됩니다. • OFF: 흐름 제어가 비활성화됩니다.
NS	**Auto-Negotiation** 이 **ON** 으로 설정되어 있을 때 유효합니다. EEE 기능을 활성화하거나 비활성화합니다. • ON: EEE 기능이 활성화됩니다.

표 5 사용자 지정 구성 옵션 및의미

매개변수	설명
	• OFF: EEE 기능이 비활성화됩니다.
절전 모드	절전 모드 활성화 또는 비활성화: • ON: 절전 모드가 활성화됩니다. • OFF: 절전 모드가 비활성화됩니다.

3. 매개변수를 설정한 후 **Apply(적용)**을 클릭합니다.

4.5.2.1.4 스위치에 연결

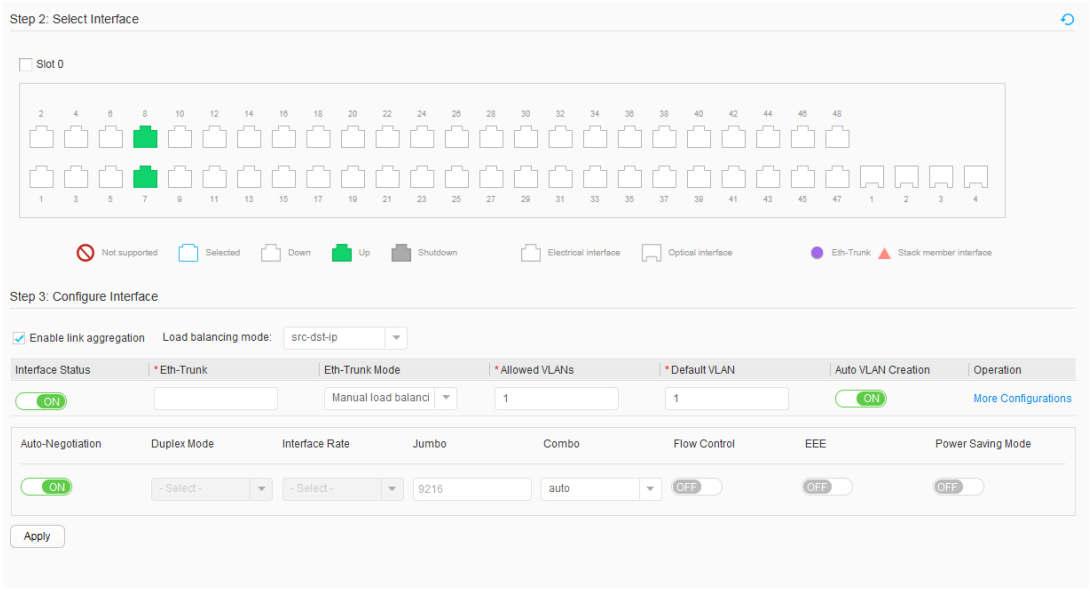
문맥

스위치가 다른 스위치에 연결된 후 서비스 요구 사항에 따라 지정된 VLAN 의 패킷을 허용하도록 스위치 포트를 구성할 수 있습니다.

절차

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **Interface Settings(인터페이스 설정)** > **Service Interface Setting(서비스 인터페이스 설정)**을 선택합니다. 그림 1 과 같이 **Connect to Switch(스위치에 연결)을** 클릭합니다.

그림 1 스위치에 연결된 포트 구성



2. 구성할 포트를 선택합니다. 포트 영역에서 필요에 따라 다음 작업을 수행합니다.

   - 포트 아이콘을 클릭합니다. 포트 선택을 취소하려면 포트 아이콘을 다시 클릭합니다.
   - 커서를 끌어 배치에서 연속 포트를 선택합니다.
   - 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
   - 패널 이 있는 슬롯을 선택합니다. 패널의 모든 포트 가 선택됩니다.

3. 포트를 구성합니다.

표 1 은 매개변수와 해당 값을 설명합니다.

표 1 포트의 매개변수와 값

매개변수	설명
부하 분산 모드	Eth-Trunk 로드 밸런싱 모드를 설정합니다. 이 매개변수는 **링크 집계 활성화**를 선택한 후에만 유효합니다. • dst-ip: 목적지 IP 주소를 기준으로 부하 분산을 수행합니다. • dst-mac: 목적지 MAC 주소를 기반으로 부하 분산을 수행합니다. • src-ip: 소스 IP 주소를 기반으로 로드 밸런싱을 수행합니다. • src-mac: 소스 MAC 주소를 기반으로 로드 밸런싱을 수행합니다.

표 1 포트의 매개변수와 값

매개변수	설명
	• src-dst-ip: 소스 IP 주소와 목적지 IP 주소의 Exclusive-OR 계산 결과를 기반으로 로드 밸런싱을 수행합니다. • src-dst-mac: 소스 및 목적지 MAC 주소의 Exclusive-OR 계산 결과를 기반으로 로드 밸런싱을 수행합니다.
인터페이스 상태	인터페이스를 활성화하거나 비활성화합니다. • ON: 인터페이스가 활성화됩니다. • OFF: 인터페이스가 비활성화됩니다.
E-트렁크	Eth-Trunk 에 인터페이스를 추가합니다. 이 매개변수는 **링크 집계 활성화**를 선택한 후에만 설정할 수 있습니다.
이더넷 트렁크 모드	Eth-Trunk 작업 모드를 설정합니다. 이 매개변수는 **링크 집계 활성화**를 선택한 후에만 설정할 수 있습니다. • 수동 로드 밸런싱(기본값): Eth-Trunk 작업 모드가 수동으로 설정됩니다. • 정적 LACP: Eth-Trunk 작업 모드가 LACP 로 설정됩니다.
허용된 VLAN	인터페이스에서 허용하는 VLAN 을 구성합니다. VLAN ID 의 범위는 1~4094 입니다.
기본 VLAN	트렁크 인터페이스에 대한 기본 VLAN 을 구성합니다. VLAN ID 의 범위는 1~4094 입니다.
자동 VLAN 생성	시스템이 허용된 VLAN 을 자동으로 생성할지 여부를 구성합니다. • 예 • 아니요
작업 **추가 구성**을 클릭 하면 다음 매개변수가 유효합니다.	
자동 협상	인터페이스에서 자동 협상을 활성화 또는 비활성화합니다. • ON: 자동 협상이 활성화됩니다. • OFF: 자동 협상이 비활성화됩니다.
이중 모드	**Auto-Negotiation** 이 **OFF** 로 설정되어 있을 때 유효합니다. 인터페이스에서 이중 모드를 구성합니다. • 전이중

표 1 포트의 매개변수와 값

매개변수	설명
	• 반이중
인터페이스 속도	**Auto-Negotiation** 이 **OFF** 로 설정되어 있을 때 유효합니다. 인터페이스 속도를 구성합니다. • 10Mbit/s • 100Mbit/s • 1000Mbit/s
커다란 것	점보 프레임 길이를 설정합니다.
콤보	콤보 인터페이스의 작업 모드를 구성합니다. • auto: 콤보 인터페이스가 작업 모드를 자동으로 선택합니다. • 구리: 콤보 인터페이스는 전기 인터페이스로 작동하며 네트워크 케이블을 사용하여 데이터를 송수신합니다. • 광섬유: 콤보 인터페이스는 광학 인터페이스로 작동하며 광섬유를 사용하여 데이터를 송수신합니다.
흐름 제어	흐름 제어 활성화 또는 비활성화: • ON: 흐름 제어가 활성화됩니다. • OFF: 흐름 제어가 비활성화됩니다.
NS	**Auto-Negotiation** 이 **ON** 으로 설정되어 있을 때 유효합니다. EEE 기능을 활성화하거나 비활성화합니다. • ON: EEE 기능이 활성화됩니다. • OFF: EEE 기능이 비활성화됩니다.
절전 모드	절전 모드 활성화 또는 비활성화: • ON: 절전 모드가 활성화됩니다. • OFF: 절전 모드가 비활성화됩니다.

4. **Apply(적용)**을 클릭하여 구성을 적용합니다.

4.5.2.1.5 커스터마이징

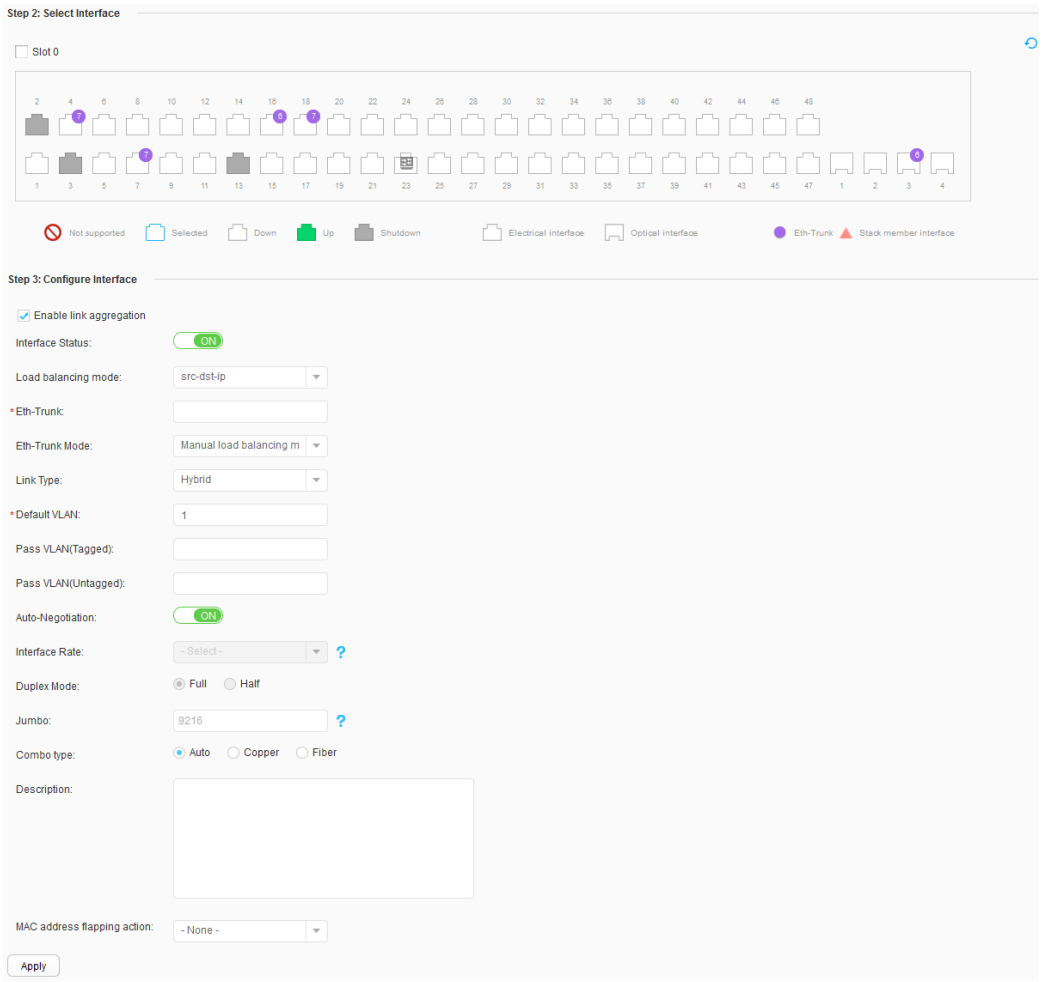
문맥

이 섹션에서는 서비스 요구 사항을 충족하도록 인터페이스 매개변수를 구성하는 방법에 대해 설명합니다.

절차

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **Interface Settings(인터페이스 설정)** > **Service Interface Setting(서비스 인터페이스 설정)**을 선택합니다. 그림 1 과 같이 **Customized(사용자 지정)을** 클릭합니다.

그림 1 맞춤형



2. 구성할 포트를 선택합니다. 포트 영역에서 필요에 따라 다음 작업을 수행합니다.

   - 포트 아이콘을 클릭합니다. 포트 선택을 취소하려면 포트 아이콘을 다시 클릭합니다.
   - 커서를 끌어 배치에서 연속 포트를 선택합니다.
   - 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
   - 패널 이 있는 슬롯을 선택합니다. 패널의 모든 포트 가 선택됩니다.

3. 인터페이스를 구성합니다.

표 1 은 매개변수와 해당 값을 설명합니다.

표 1 사용자 정의 매개변수 설정

매개변수	설명
인터페이스 상태:	인터페이스 상태를 설정합니다. • ON: 현재 인터페이스가 활성화됩니다. • OFF: 현재 인터페이스가 비활성화됩니다.
부하 분산 모드	Eth-Trunk 의 로드 밸런싱 모드를 설정합니다. 이 매개변수는 **링크 집계 사용** 이 선택된 경우에만 사용할 수 있습니다. • dst-ip: 목적지 IP 주소를 기준으로 부하 분산을 수행합니다. • dst-mac: 목적지 MAC 주소를 기반으로 부하 분산을 수행합니다. • src-ip: 소스 IP 주소를 기반으로 로드 밸런싱을 수행합니다. • src-mac: 소스 MAC 주소를 기반으로 로드 밸런싱을 수행합니다. • src-dst-ip: 소스 IP 주소와 목적지 IP 주소의 Exclusive-OR 계산 결과를 기반으로 로드 밸런싱을 수행합니다. • src-dst-mac: 소스 및 목적지 MAC 주소의 Exclusive-OR 계산 결과를 기반으로 로드 밸런싱을 수행합니다.
E-트렁크	인터페이스가 추가되는 Eth-Trunk 의 ID 를 구성합니다. 이 매개변수는 **링크 집계 사용** 이 선택된 경우에만 설정할 수 있습니다.
이더넷 트렁크 모드	Eth-Trunk 작업 모드를 설정합니다. 이 매개변수는 **링크 집계 사용** 이 선택된 경우에만 설정할 수 있습니다. • 수동 로드 밸런싱(기본값): Eth-Trunk 작업 모드가 수동으로 설정됩니다. • 정적 LACP: Eth-Trunk 작업 모드가 LACP 로 설정됩니다.

표 1 사용자 정의 매개변수 설정

매개변수	설명
링크 유형	인터페이스의 링크 유형을 설정합니다. • - 없음 -: 인터페이스의 링크 유형이 협상 가능으로 설정됩니다. • 액세스: 인터페이스의 링크 유형이 액세스로 설정됩니다. • 트렁크: 인터페이스의 링크 유형이 트렁크로 설정됩니다. • 하이브리드: 인터페이스의 링크 유형이 하이브리드로 설정됩니다.
기본 VLAN	인터페이스가 추가되는 기본 VLAN 을 설정합니다. 값 범위는 1~4094 입니다. 이 매개변수는 **Link Type** 이 **Access**, **Trunk** 또는 **Hybrid** 로 설정된 경우에만 설정할 수 있습니다.
VLAN 통과(태그 있음)	태그 모드에서 인터페이스를 통과하도록 VLAN 의 프레임을 구성합니다. 이 매개변수는 **Link Type** 이 **Trunk** 또는 **Hybrid** 로 설정된 경우에만 설정할 수 있습니다.
통과 VLAN(태그 없음)	태그가 지정되지 않은 모드에서 인터페이스를 통과하도록 VLAN 의 프레임을 구성합니다. 이 매개변수는 **링크 유형** 이 **하이브리드** 로 설정된 경우에만 설정할 수 있습니다.
자동 협상	인터페이스에서 자동 협상을 구성합니다. • ON: 자동 협상이 활성화됩니다. • OFF: 자동 협상이 비활성화됩니다.
인터페이스 속도	이 매개변수는 **자동 협상** 이 **OFF** 로 설정된 경우에만 사용할 수 있습니다. 인터페이스 속도를 구성합니다.
이중 모드	이 매개변수는 **자동 협상** 이 **OFF** 로 설정된 경우에만 사용할 수 있습니다. 인터페이스에서 이중 모드를 구성합니다. • 전이중 • 반이중
커다란 것	점보 프레임의 길이를 구성합니다. 1536 에서 12288 사이의 값입니다.
콤보 유형	콤보 인터페이스의 작업 모드를 구성합니다. • 자동: 콤보 인터페이스가 작업 모드를 자동으로 선택합니다. • 구리: 콤보 인터페이스는 전기 인터페이스로 작동하며 네트워크 케이블을 사용하여 데이터를 송수신합니다. • 광섬유: 콤보 인터페이스는 광학 인터페이스로 작동하며 광섬유를 사용하여 데이터를 송수신합니다.

표 1 사용자 정의 매개변수 설정

매개변수	설명
설명	인터페이스 설명을 구성합니다.
MAC 주소 플래핑 동작	인터페이스에서 MAC 주소 플래핑이 감지될 때 인터페이스에서 수행할 작업을 구성합니다. • - 없음 -: 구성된 작업이 없습니다. • error-down: 인터페이스에서 MAC 주소 플래핑이 감지되면 인터페이스를 종료합니다. • quit-vlan: 인터페이스에서 MAC 주소 플랩이 감지될 때 MAC 주소 플랩이 발생하는 VLAN 에서 인터페이스를 제거합니다.

4. **Apply(적용)**을 클릭하여 구성을 적용합니다.

4.5.2.1.6 인터페이스 활성화/비활성화

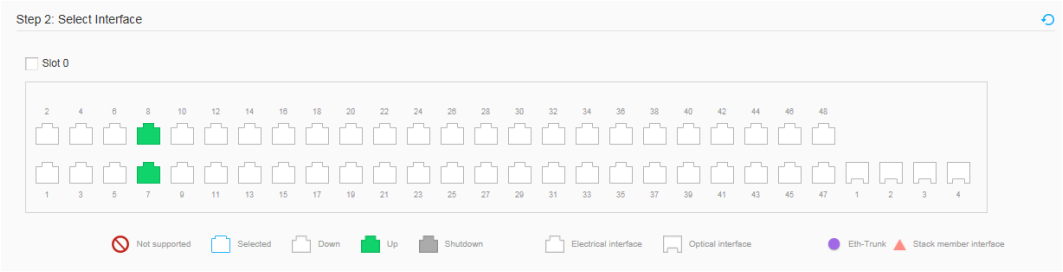
문맥

GUI 에서 케이블이나 광섬유에 연결되지 않은 유휴 인터페이스를 비활성화하여 유휴 인터페이스가 작동 상태에서 다른 인터페이스를 방해하지 않도록 할 수 있습니다.
그림 1 은 인터페이스 상태와 광/전기 인터페이스를 보여줍니다.
그림 1 인터페이스 상태 및 광/전기 인터페이스

절차

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **Interface Settings(인터페이스 설정)** > **Service Interface Setting(서비스 인터페이스 설정)**을 선택합니다. 그림 2 와 같이 **Enable/Disable Interface(인터페이스 활성화/비활성화)**를 클릭합니다.

그림 2 인터페이스 활성화/비활성화



2. 구성할 인터페이스를 선택합니다. 필요에 따라 다음 작업 중 하나를 수행합니다.

   - 인터페이스 아이콘을 클릭하여 인터페이스를 선택합니다.
   - 마우스를 끌어 일괄적으로 여러 개의 연속 인터페이스를 선택합니다.
   - 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
   - 프런트패널의 모든 인터페이스를 선택하려면 프런트패널 이름 앞의 확인란을 클릭합니다.

3. **Configure Interface(인터페이스 구성)**에서 매개변수를 설정합니다. 그림 3 은 **Configure Interface(인터페이스 구성)**을 보여줍니다.

그림 3 인터페이스 구성

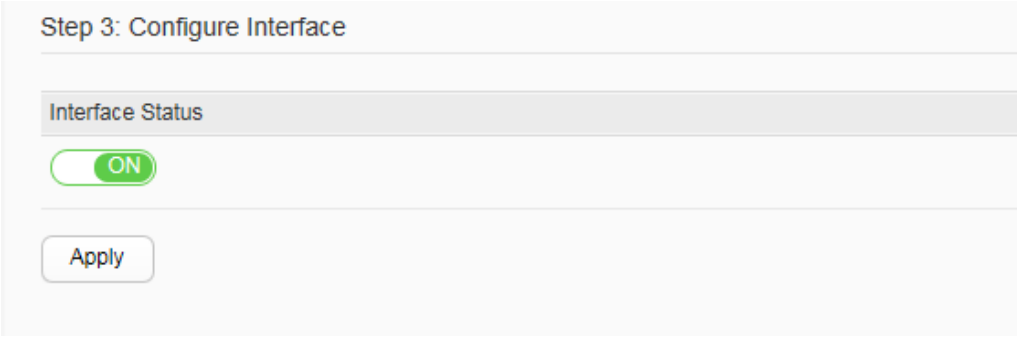


표 1 은 **인터페이스 구성**의 매개변수를 설명합니다.

표 1 인터페이스 구성의 매개변수

안건	설명
인터페이스 상태	인터페이스 상태를 설정합니다. • ON: 현재 인터페이스가 종료되지 않습니다. • OFF: 현재 인터페이스가 종료됩니다.

4. **Apply(적용)**을 클릭하여 구성을 완료합니다.

4.5.2.1.7 링크 감지

문맥

VCT(가상 케이블 테스트) 기술은 TDR(시간 영역 반사 측정)을 사용하여 케이블 상태를 감지합니다. 펄스가 케이블의 끝 또는 케이블의 고장 지점으로 전송될 때 일부 펄스 에너지는 송신단으로 반사됩니다. VCT 알고리즘은 케이블을 통해 펄스를 전송하고 오류 지점에 도달한 후 펄스를 반환하는 데 소요된 시간을 측정합니다. 측정된 시간은 거리로 변환됩니다.

VCT 는 네트워크 케이블의 오류 유형을 감지하고 오류 지점을 식별하여 네트워크 케이블 오류를 찾는 데 도움을 줄 수 있습니다.

VCT 테스트 결과는 참고용일 뿐이며 일부 공급업체의 케이블에서는 정확하지 않을 수 있습니다.

VCT 는 장치에 GE 구리 모듈이 설치되어 있거나 GE 전기 인터페이스가 있는 광학 인터페이스에만 적용됩니다.

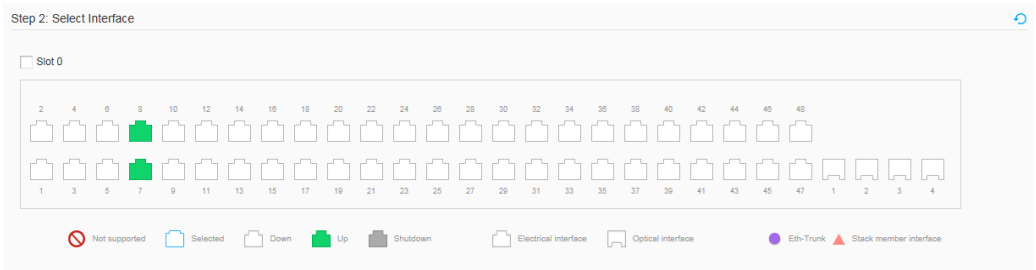
그림 1 은 인터페이스 상태와 광/전기 인터페이스를 보여줍니다.

그림 1 인터페이스 상태 및 광/전기 인터페이스

절차

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **Interface Settings(인터페이스 설정)** > **Service Interface Setting(서비스 인터페이스 설정)**을 선택합니다. 그림 2 와 같이 **Detect Link(링크 감지)**를 클릭합니다.

그림 2 링크 감지



2. 구성할 인터페이스를 선택합니다. 필요에 따라 다음 작업 중 하나를 수행합니다.

   - 인터페이스 아이콘을 클릭하여 인터페이스를 선택합니다.
   - 마우스를 끌어 일괄적으로 여러 개의 연속 인터페이스를 선택합니다.
   - 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
   - 프런트패널의 모든 인터페이스를 선택하려면 프런트패널 이름 앞의 확인란을 클릭합니다.

3. **Apply(적용)**을 클릭합니다. 표시되는 대화 상자에서 **Ok(확인)을 클릭**합니다.

4. **Configure Interface(인터페이스 구성)**에서 확인 결과를 볼 수 있습니다. 그림 3 은 **인터페이스 구성**을 보여줍니다.

그림 3 인터페이스 구성

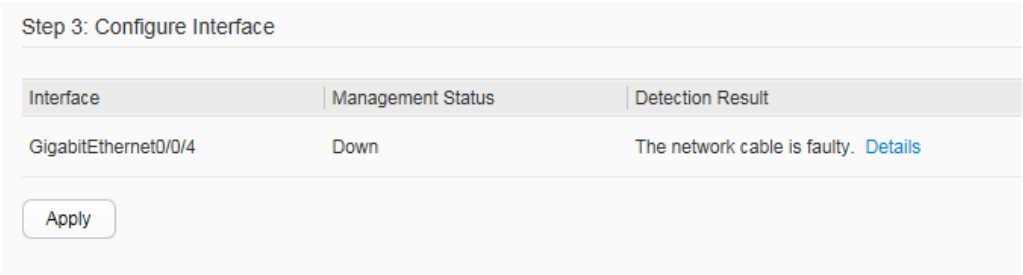


표 1 은 **인터페이스 구성**의 매개변수를 설명합니다.

표 1 인터페이스 구성의 매개변수

안건	설명
상호 작용	링크 감지가 수행되는 인터페이스의 유형 및 번호입니다.
관리 현황	인터페이스의 관리 상태입니다. • 다운: 인터페이스가 비활성화되었습니다. • 위로: 인터페이스가 활성화되었습니다. • 종료: 관리자가 인터페이스 에서 **종료** 명령을 실행했음을 나타냅니다.
탐지 결과	**네트워크 케이블에 결함이** 있거나 **인터페이스가 정상적으로 작동** 하는 링크 감지 결과 . **노트:** 네트워크 케이블 장애가 발생한 경우 **자세히**를 클릭 하면 자세한 감지 결과를 볼 수 있습니다. 표시된 페이지에는 다음 필드가 있습니다. • Pair A/B/C/D: 네트워크 케이블의 4 쌍의 회로를 나타냅니다.

표 1 인터페이스 구성의 매개변수

안건	설명
	• Pair A length: 네트워크 케이블의 길이를 나타냅니다. 오류가 발생하면 이 필드는 인터페이스와 오류 위치 사이의 거리를 나타냅니다. 네트워크 케이블이 제대로 작동하면 이 필드는 케이블의 실제 길이를 나타냅니다. 인터페이스가 네트워크 케이블에 연결되지 않은 경우 기본 길이는 0 미터입니다. • 페어 A 상태: 네트워크 케이블의 상태를 나타냅니다. (**OK** : 정상; **Open** : 개방; **단락** : 단락; **누화** : 잘못된 케이블 시퀀스; **Unknown** : 알 수 없는 오류)

4.5.2.1.8 포트 루프백 테스트

문맥

포트 루프백 테스트는 내부 포워딩 칩이 인터페이스에서 포워딩을 제대로 제어하는지 확인하는 데 사용됩니다.

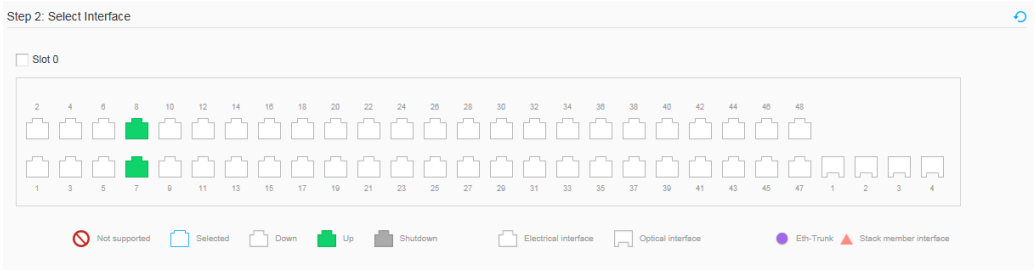
그림 1 은 광학 및 전기 인터페이스의 인터페이스 상태와 기호를 보여줍니다.

그림 1 광 및 전기 포트의 인터페이스 상태 및 기호

절차

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **Interface Settings(인터페이스 설정)** > **Service Interface Setting(서비스 인터페이스 설정)**을 선택합니다. 그림 2 와 같이 **Port Loopback Test** 를 선택 합니다.

그림 2 포트 루프백 테스트



2. 구성할 인터페이스를 선택합니다. 필요에 따라 다음 작업 중 하나를 수행합니다.

   - 인터페이스 아이콘을 클릭하여 인터페이스를 선택합니다.
   - 마우스를 끌어 일괄적으로 여러 개의 연속 인터페이스를 선택합니다.
   - 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
   - 프런트패널의 모든 인터페이스를 선택하려면 프런트패널 이름 앞의 확인란을 클릭합니다.

3. **Apply(적용)**을 클릭합니다. 표시되는 대화 상자에서 **Ok(확인)을 클릭**합니다.
4. 반환된 정보는 그림 3 과 같이 **Configure Interface(인터페이스 구성)**에 표시됩니다.

그림 3 인터페이스 구성

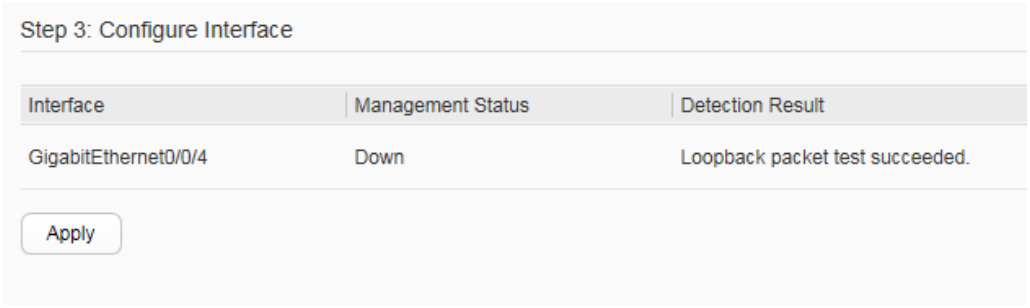


표 1 은 표시된 페이지의 매개변수를 설명합니다.

표 1 인터페이스 매개변수 목록

매개변수	설명
상호 작용	루프백 테스트가 수행되는 인터페이스의 유형 및 번호를 나타냅니다.
관리 현황	관리 상태를 나타냅니다. • Down: 인터페이스가 비활성화되었음을 나타냅니다.

표 1 인터페이스 매개변수 목록

매개변수	설명
	• Up: 인터페이스가 활성화되었음을 나타냅니다. • 종료: **종료** 명령이 인터페이스에서 실행 되었음을 나타냅니다.
탐지 결과	루프백 테스트 결과를 나타냅니다.

4.5.2.2 트랜시버 정보 보기

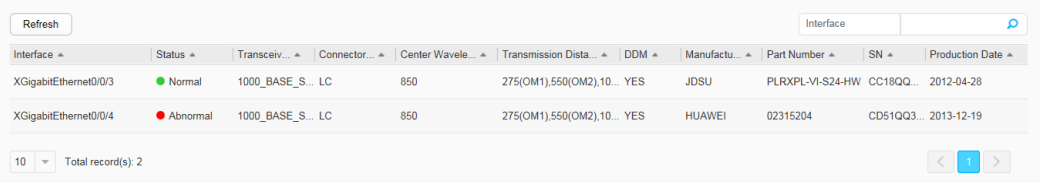
문맥

이 페이지는 스위치가 스택에 합류할 때 표시됩니다.

절차

1. 그림 1 과 같이 **Configuration(구성)** > **Basic Services(기본 서비스)** > **View Transceiver Info(트랜시버 정보 보기)**를 선택합니다.

   그림 1 트랜시버 정보 보기



2. **Refresh(새로 고침)**을 클릭하여 광 모듈 정보 목록을 업데이트합니다.

4.5.2.3 VLAN

4.5.2.3.1 VLAN

문맥

- 스위치는 VLAN 1 에서 VLAN 4094 까지 4094 개의 VLAN 을 지원합니다.
- VLAN 은 서로 통신할 필요가 없는 호스트를 격리하여 브로드캐스트 트래픽을 줄이고 네트워크 보안을 향상시킬 수 있습니다.

절차

• VLAN 생성

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **VLAN** 을 선택합니다.
2. **Create(만들기)를 클릭합니다. VLAN 만들기** 대화 상자가 표시됩니다 같이 그림 1 .

그림 1 VLAN 생성

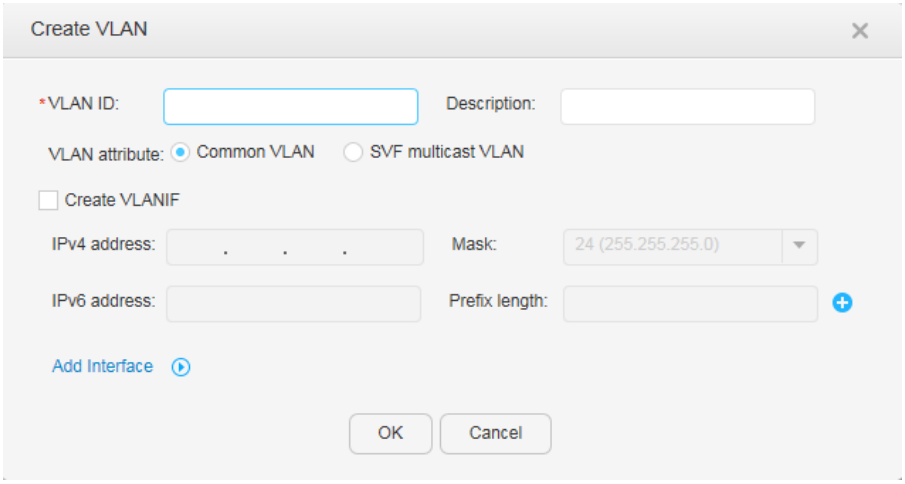


표 1 은 **VLAN 생성** 대화 상자의 매개변수를 설명합니다.

표 1 VLAN 생성을 위한 매개변수

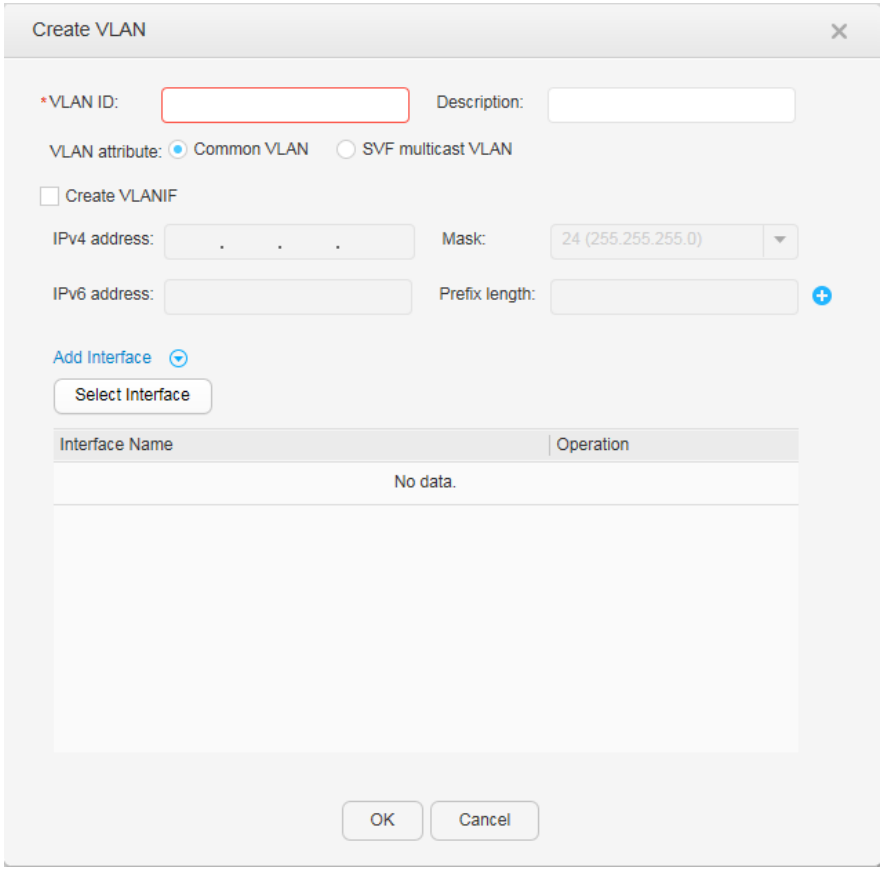
매개변수	설명
VLAN ID	VLAN 의 ID 입니다. 이 매개변수는 필수이며 값 범위는 1 에서 4094 까지입니다. VLAN 1 은 기본 VLAN 이며 시스템은 이를 다시 생성하지 않습니다.
설명	VLAN 에 대한 설명입니다. 이 매개변수는 선택 사항입니다.
VLAN 속성	VLAN 의 속성입니다. 이 매개변수는 필수입니다. 설정 **VLAN 속성** 에 **공통 VLAN** 또는 **SVF 는 VLAN 을 멀티 캐스트** . **노트:** 이 매개변수는 장치가 SVF 로 활성화된 경우에만 사용할 수 있습니다.
IPv4 주소	10.10.10.1 과 같은 VLANIF 인터페이스의 IPv4 주소입니다. 이 매개변수는 선택 사항이며 VLANIF 인터페이스에 대해서만 구성할 수 있습니다.

표 1 VLAN 생성을 위한 매개변수

매개변수	설명
마스크	IP 주소의 서브넷 마스크입니다. 이 매개변수는 선택 사항입니다.
IPv6 주소	IPv6 주소(예: FC00:0:130F:0:0:9C0:876A:130B). 이 매개변수는 선택 사항이며 VLANIF 인터페이스에 대해서만 구성할 수 있습니다.
접두어 길이	주소 접두사의 길이. 이 매개변수는 선택사항이며 값 범위는 1 - 128 입니다.
VLAN 내 프록시 ARP	VLAN 에서 ARP 프록시를 활성화할지 여부를 나타냅니다. • ON: ARP 프록시를 활성화합니다. • OFF: ARP 프록시를 비활성화합니다. **노트:** 중앙 집중식 포워딩에서는 VLAN 에서 ARP 프록시를 활성화해야 합니다.

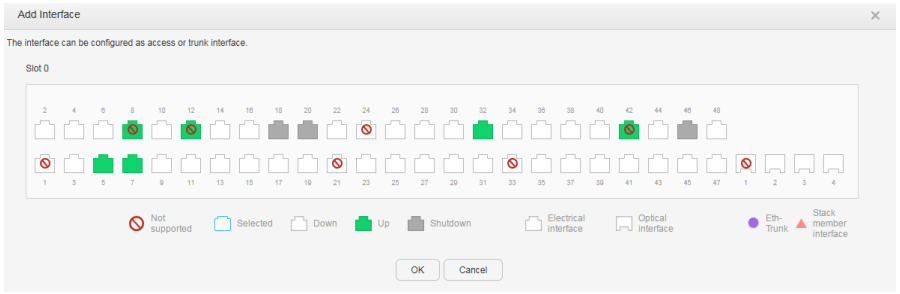
3. 매개변수를 설정합니다.
4. **인터페이스 추가를** 클릭합니다. **추가 인터페이스** 영역이 펼쳐 에서와 같이, 그림 2 .

그림 2 VLAN 에 포트 추가



5. **인터페이스 선택을** 클릭합니다. **추가 인터페이스** 페이지가 표시됩니다 같이 그림 3 .

그림 3 VLAN 에 추가할 포트 선택



6. Ok(확인)을 클릭합니다. **VLAN 만들기** 대화 상자가 표시됩니다.
7. Ok(확인)을 클릭합니다.

• 일괄적으로 VLAN 생성

1. **Configuration(구성) > 기본 서비스 > VLAN 을** 선택 **합니다.**
2. **일괄 생성을** 클릭합니다. **배치는 VLAN 생성**, 표시되는 대화 상자 에서와 같이 그림 4 . 매개변수를 설정합니다.

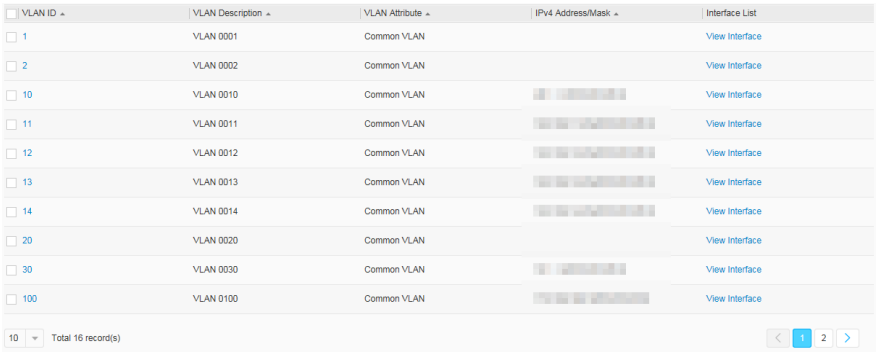
그림 4 일괄 VLAN 생성

3. Ok(확인)을 클릭합니다.

• VLAN 쿼리

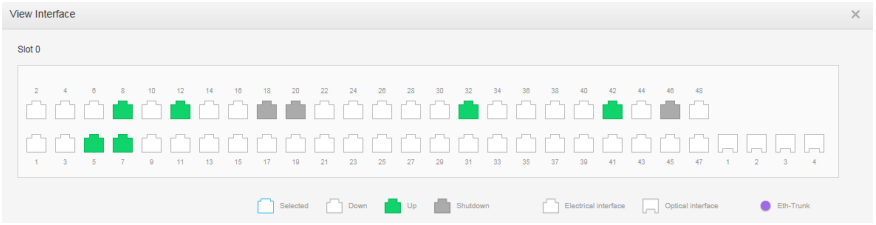
1. **Configuration(구성) > 기본 서비스 > VLAN 을** 선택 **합니다.**
2. 검색 상자에 VLAN ID 를 입력합니다. VLAN ID 를 입력하지 않으면 생성된 모든 VLAN 이 표시됩니다.
3. 을 클릭 합니다. 그림 5 와 같이 VLAN 이 표시됩니다.

그림 5 VLAN 목록



4. **인터페이스 보기를** 클릭합니다. VLAN 에 추가된 인터페이스 는 그림 6 과 같이 표시됩니다.

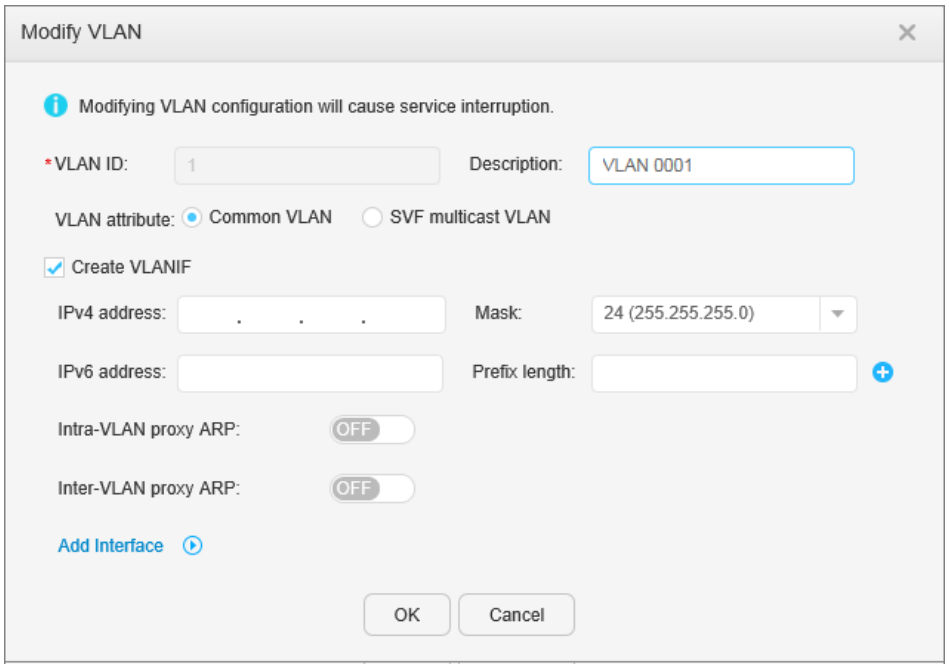
그림 6 보기 인터페이스



• VLAN 수정

1. **Configuration(구성) > 기본 서비스 > VLAN 을** 선택 **합니다.**
2. VLAN ID 를 클릭합니다. **수정 VLAN** 대화 상자가 표시됩니다 같이 그림 7 . 표 1 은 **Modify VLAN** 대화 상자의 매개변수를 설명합니다.

그림 7 VLAN 수정



3. 필요에 따라 매개변수 값을 변경합니다.
4. Ok(확인)을 클릭합니다.

• VLAN 삭제

1. **Configuration(구성) > 기본 서비스 > VLAN 을 선택 합니다.**
2. 삭제할 VLAN 을 선택하고 클릭 **삭제** . 시스템에서 VLAN 을 삭제할지 여부를 묻습니다.

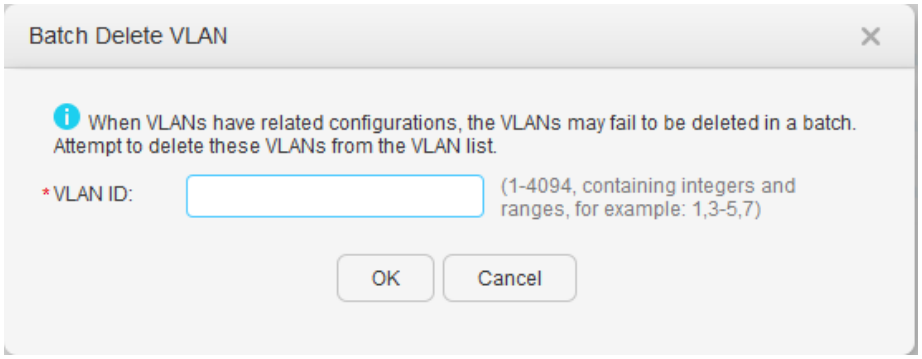
> **NOTE**
>
> VLAN 1 은 기본 VLAN 이며 삭제할 수 없습니다.

3. Ok(확인)을 클릭합니다.

• 일괄 VLAN 삭제

1. **Configuration(구성) > 기본 서비스 > VLAN 을 선택 합니다.**
2. **일괄 삭제를** 클릭합니다. **일괄 삭제 VLAN 의** 대화 상자가 표시됩니다 같이 그림 8 . 매개변수를 설정합니다.

그림 8 일괄 VLAN 삭제



3. **삭제를** 클릭합니다. 시스템에서 VLAN 을 삭제할지 여부를 묻습니다.
4. Ok(확인)을 클릭합니다.

4.5.2.3.2 VLAN 풀

문맥

VLAN 풀은 여러 VLAN 의 조합이며 네트워크 배포를 단순화하는 데 사용됩니다. 관리자는 부서 내 사용자의 VLAN 을 VLAN 풀로 계획합니다. 사용자가 인증을 통과한 후 인증 서버는 사용자에게 VLAN 풀을 승인합니다. 장치는 VLAN 할당 알고리즘을 기반으로 VLAN 풀의 VLAN 을 사용자에게 할당합니다. 이러한 방식으로 각 부서의 사용자 수를 계산할 필요 없이 여러 부서에 대해 VLAN 을 계획할 수 있습니다.

절차

- VLAN 풀을 생성합니다.

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **VLAN** > **VLAN 풀**을 선택합니다.
2. **Create(만들기)를 클릭합니다. VLAN 풀 만들기** 대화 상자가 표시됩니다 같이 그림 1 .

그림 1 VLAN 풀 생성

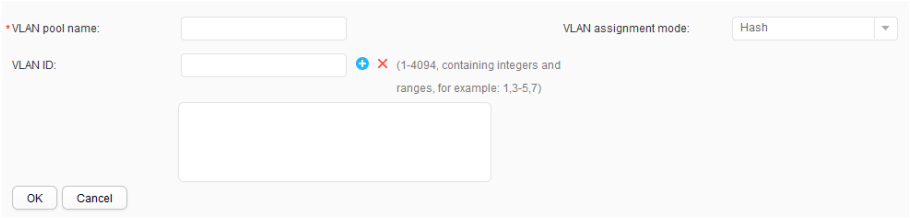


표 1 은 페이지의 매개변수를 설명합니다.

표 1 VLAN 풀 생성

매개변수	설명
VLAN 풀 이름	VLAN 풀의 이름을 지정합니다.
VLAN 할당 모드	VLAN 풀의 VLAN 할당 알고리즘을 해시 또는 짝수로 지정합니다. • VLAN 할당 알고리즘이 **Hash** 로 설정되면 MAC 주소의 해시 결과를 기반으로 VLAN 풀에서 사용자에게 VLAN 이 할당됩니다. VLAN 풀의 VLAN 이 변경되지 않는 한 사용자는 고정 VLAN 을 얻습니다. 사용자는 다른 시간에 온라인에 접속할 때 우선적으로 동일한 IP 주소를 할당받습니다. • VLAN 할당 알고리즘이 **Even** 로 설정 되면 서비스 VLAN 은 사용자가 온라인 상태가 된 순서에 따라 VLAN 풀에서 사용자에게 할당됩니다. 서비스 VLAN 을 매핑하는 주소 풀은 사용자에게 균등하게 IP 주소를 할당합니다. 사용자가 여러 번 온라인 상태가 되면 다른 IP 주소를 얻습니다.
VLAN ID	지정된 VLAN 이 VLAN 풀에 추가되었음을 나타냅니다. **노트:** 이 매개변수는 VLAN ID 를 클릭하고 아래 데이터 영역에 추가한 후에만 구성할 수 있습니다. 또는을 클릭 하여 텍스트 상자의 데이터를 지울 수 있습니다.

3. 매개변수를 설정합니다.

4. Ok(확인)을 클릭합니다.

- VLAN 풀을 수정합니다.

    1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **VLAN** > **VLAN 풀**을 선택합니다.
    2. VLAN 풀 목록에서 VLAN 풀의 이름을 클릭합니다. **VLAN 풀 수정**과 같이 페이지가 표시됩니다 표 1 .
    3. 매개변수를 수정합니다.
    4. Ok(확인)을 클릭합니다.

- VLAN 풀을 삭제합니다.

    1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **VLAN** > **VLAN 풀**을 선택합니다.
    2. 삭제할 VLAN 풀을 선택하고 **삭제**를 클릭합니다. 시스템에서 VLAN 풀을 삭제할지 여부를 묻습니다.
    3. Ok(확인)을 클릭합니다.

- VLAN 풀을 새로 고칩니다.

    1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **VLAN** > **VLAN 풀**을 선택합니다.
    2. **Refresh(새로 고침)**을 클릭합니다.

6.5.2.4 DHCP

4.5.2.4.1 DHCP 주소 풀

문맥

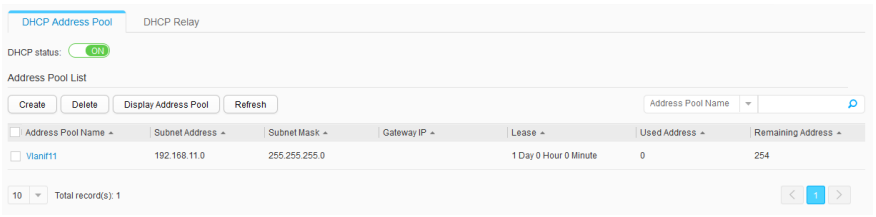
이 섹션에서는 네트워크의 클라이언트에 IP 주소를 동적으로 할당하도록 전역 주소 풀 또는 인터페이스 주소 풀을 구성하는 방법에 대해 설명합니다.

절차

• 전역적으로 DHCP 활성화

1. 그림 1 과 같이 **Configuration(구성)** > **Basic Services(기본 서비스)** > **DHCP** > **DHCP Address Pool 을** 선택합니다.

   그림 1 전역적으로 DHCP 활성화



2. **DHCP 상태**를 **ON** 으로 설정하여 DHCP 를 전 세계적으로 활성화합니다.

• DHCP 주소 풀 생성

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **DHCP** > **DHCP 주소 풀을** 선택합니다.
2. **Address Pool List(주소 풀 목록)**에서, **Create(만들기)**를 클릭합니다. 그림 2 와 같이 **Create DHCP Address Pool(DHCP 주소 풀 생성)** 페이지가 표시됩니다.

그림 2 DHCP 주소 풀 생성

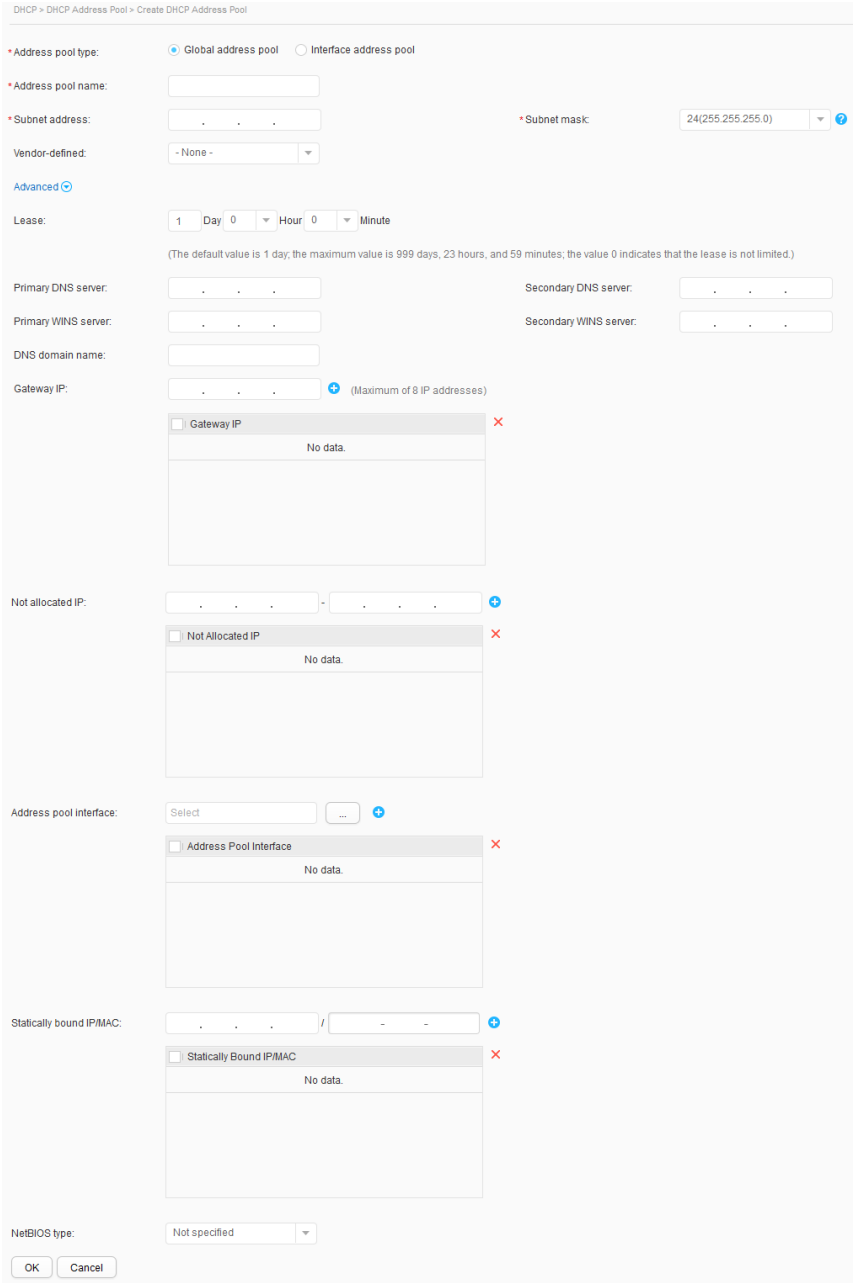


표 1 은 페이지의 매개변수를 설명합니다.

표 1 DHCP 주소 풀 생성을 위한 매개변수

매개변수	설명
주소 풀 유형	생성할 주소 풀의 유형을 지정합니다. 옵션은 다음과 같습니다. 전체 주소 풀 인터페이스 주소 풀

표 1 DHCP 주소 풀 생성을 위한 매개변수

매개변수	**설명**
주소 풀 이름	전역 주소 풀의 이름을 지정합니다. 이 매개변수는 **주소 풀 유형** 이 전체 **주소 풀로** 설정된 경우에만 사용할 수 **있습니다.**
서브넷 주소	전역 주소 풀에서 할당할 수 있는 네트워크 세그먼트 주소를 지정합니다. 이 매개변수는 **주소 풀 유형** 이 전체 **주소 풀로** 설정된 경우에만 사용할 수 **있습니다.**
서브넷 마스크	DHCP 클라이언트에 할당된 IP 주소의 서브넷 마스크를 지정합니다. 이 매개변수는 **주소 풀 유형** 이 전체 **주소 풀로** 설정된 경우에만 사용할 수 **있습니다.**
인터페이스 선택	주소 풀을 구성할 인터페이스를 지정합니다. 이 매개변수는 **주소 풀 유형** 이 **인터페이스 주소 풀로** 설정된 경우에만 사용할 수 **있습니다.**
인터페이스 IP 주소	현재 인터페이스의 IP 주소, 즉 DHCP 클라이언트의 게이트웨이 주소를 지정합니다. 이 매개변수는 **주소 풀 유형** 이 **인터페이스 주소 풀로** 설정된 경우에만 사용할 수 **있습니다.**
마스크	DHCP 클라이언트에 할당된 IP 주소의 서브넷 마스크를 지정합니다. 이 매개변수는 **주소 풀 유형** 이 **인터페이스 주소 풀로** 설정된 경우에만 사용할 수 **있습니다.**
공급업체 정의	주소 풀에 대한 사용자 정의 옵션을 지정합니다. 옵션은 다음과 같습니다. **없음** : 주소 풀에 대해 구성된 사용자 정의 옵션이 **없음을** 나타냅니다. **ascii** : 사용자 정의 옵션이 ASCII 문자열임을 나타냅니다. **cipher** : 사용자 정의 옵션이 암호 문자열임을 나타냅니다. **hex** : 사용자 정의 옵션이 16 진수임을 나타냅니다. **ip-address** : 사용자 정의 옵션이 IP 주소임을 나타냅니다. 1~8 개의 IP 주소를 지정할 수 있습니다.

표 1 DHCP 주소 풀 생성을 위한 매개변수

매개변수	**설명**
	sub-option : 사용자 정의 옵션에 대한 하위 옵션이 구성되었음을 나타냅니다. **하위 옵션**을 선택한경우 **하위** 옵션 매개변수도 설정해야 합니다.
임차권	DHCP 클라이언트에 할당된 IP 주소의 임대를 지정합니다.
기본 DNS 서버	DHCP 클라이언트에 할당된 기본 DNS 서버 주소를 지정합니다.
보조 DNS 서버	DHCP 클라이언트에 할당된 보조 DNS 서버 주소를 지정합니다.
기본 WINS 서버	DHCP 클라이언트에 할당된 기본 WINS 서버 주소를 지정합니다.
보조 WINS 서버	DHCP 클라이언트에 할당된 보조 WINS 서버 주소를 지정합니다.
DNS 도메인 이름	DNS 서버가 DNS 클라이언트에 할당한 도메인 이름 접미사를 지정합니다.
게이트웨이 IP	전역 주소 풀에서 송신 게이트웨이 IP 주소를 지정합니다. 게이트웨이 IP 주소를 생성하려면 게이트웨이 IP 주소를 입력하고을 클릭 ⊕합니다. 이전 작업을 반복하여 최대 8 개의 게이트웨이 IP 주소를 생성할 수 있습니다. 하나 개 이상의 게이트웨이 IP 주소를 삭제하려면, 게이트웨이 IP 주소의 확인란을 선택하거나 옆에있는 확인란을 선택 **게이트웨이 IP**, ❌를 클릭하십시오 . 이 매개변수는 **주소 풀 유형** 이 전체 **주소 풀로** 설정된 경우에만 사용할 수 **있습니다.**
할당되지 않은 IP	클라이언트에 동적으로 할당되지 않을 IP 주소를 지정합니다. 동적으로 할당되지 않을 IP 주소를 생성하려면 시작 및 끝 IP 주소를 입력하고 ⊕을 클릭합니다. 이전 작업을 반복하여 클라이언트에 동적으로 할당되지 않을 여러 IP 주소 또는 IP 주소 세그먼트를 만들 수 있습니다. 원래 동적으로 할당되지 않은 하나 이상의 IP 주소를 삭제하려면 해당 IP 주소의 확인란을 선택하거나 **할당되지 않은 IP** 옆의 확인란을 선택하고 ❌를 클릭합니다.

표 1 DHCP 주소 풀 생성을 위한 매개변수

매개변수	설명
주소 풀 인터페이스	주소 풀의 주소를 사용할 수 있는 인터페이스를 지정합니다. 이 인터페이스를 통해 온라인으로 전환하는 사용자는 전체 주소 풀에서 IP 주소와 같은 구성 정보를 얻을 수 있습니다. 주소 풀의 주소를 사용할 수 있는 인터페이스를 만들려면 인터페이스를 선택하고 ⊕을 클릭합니다. 이전 작업을 반복하여 주소 풀의 주소를 사용할 수 있는 최대 8 개의 인터페이스를 생성할 수 있습니다. 주소 풀의 주소를 사용할 수 있는 하나 이상의 인터페이스를 삭제하려면 인터페이스의 확인란을 선택하거나 **주소 풀 인터페이스** 옆의 확인란을 선택하고 ✕를 클릭합니다. 이 매개변수는 **주소 풀 유형** 이 전체 **주소 풀로** 설정된 경우에만 사용할 수 **있습니다.**
정적으로 바인딩된 IP/MAC	DHCP 클라이언트의 MAC 주소에 동적으로 할당할 수 있는 IP 주소를 정적으로 바인딩합니다. 고정 주소 바인딩 항목을 생성하려면 고정할 IP 주소와 MAC 주소를 입력하고 ⊕을 클릭합니다. 이전 작업을 반복하여 여러 고정 주소 바인딩 항목을 만들 수 있습니다. 하나 이상의 고정 주소 바인딩 항목을 삭제하려면 고정 주소 바인딩 항목의 확인란을 선택하거나 **고정적으로 바인딩된 IP/MAC** 옆의 확인란을 선택하고 ✕를 클릭 합니다.
NetBIOS 유형	DHCP 클라이언트의 NetBIOS 노드 유형을 지정합니다. 옵션은 다음과 같습니다. **지정되지 않음** : NetBIOS 노드 유형이 지정되지 않았음을 나타냅니다. **b-node** : 브로드캐스트 모드의 노드를 나타낸다. b-노드는 브로드캐스트 모드에서 호스트 이름과 IP 주소 간의 매핑을 얻습니다. **p-node** : 하이브리드 모드의 노드를 나타냅니다. p-노드는 P2P 통신 메커니즘으로 활성화된 b-노드입니다. **m-node** : 혼합 모드의 노드를 나타냅니다. m 노드는 일부 브로드캐스트 기능이 있는 p 노드입니다.

표 1 DHCP 주소 풀 생성을 위한 매개변수

매개변수	설명
	h-node : 피어 투 피어 모드의 노드를 나타냅니다. h-노드는 NetBIOS 서버와 통신하여 호스트 이름과 IP 주소 간의 매핑을 얻습니다.

3. 매개변수를 설정합니다.
4. Ok(확인)을 클릭합니다.

• DHCP 주소 풀 수정

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **DHCP** > **DHCP 주소 풀**을 선택합니다.
2. **주소 풀 목록**에서, DHCP 주소 풀의 이름을 클릭합니다. DHCP 주소 풀을 수정하는 페이지가 표시됩니다. 표 1 은 페이지의 매개변수를 설명합니다.
3. 구성 매개변수를 수정하십시오.
4. Ok(확인)을 클릭합니다.

• DHCP 주소 풀 삭제

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **DHCP** > **DHCP 주소 풀**을 선택합니다.
2. **주소 풀 목록**에서 삭제할 DHCP 주소 풀의 체크 박스의 확인란을 선택하고 **삭제**를 클릭합니다. 시스템에서 DHCP 주소 풀을 삭제할지 여부를 묻습니다.
3. Ok(확인)을 클릭합니다.

• 주소 풀 정보 쿼리

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **DHCP** > **DHCP 주소 풀**을 선택합니다.
2. **주소 풀 목록**에서 조회할 DHCP 주소 풀을 선택하고 **표시 주소 풀 표시**를 클릭합니다. 그림 3 과 같이 **주소 풀 정보** 페이지가 표시됩니다.

그림 3 주소 풀 정보 조회

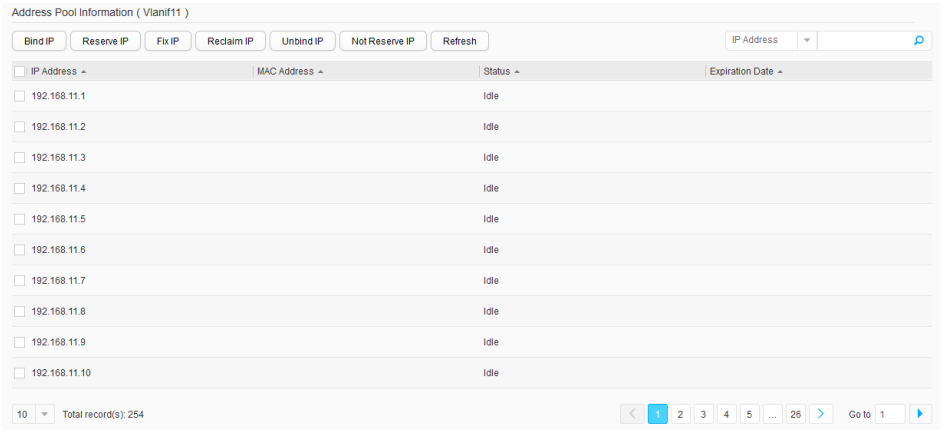


표 2 는 페이지의 매개변수를 설명합니다.

표 2 주소 풀 정보

매개변수	설명
바인드 IP	주소 풀의 IP 주소를 고정 MAC 주소에 바인딩합니다.
IP 예약	주소 풀에서 동적으로 할당되지 않을 IP 주소를 지정합니다.
IP 수정	주소 풀에서 사용 중이거나 만료된 IP 주소를 MAC 주소에 바인딩합니다. IP 주소는 다음에 온라인 상태가 될 때 지정된 클라이언트에 직접 할당됩니다.
IP 회수	사용 중이거나 충돌하거나 주소 풀에서 만료된 IP 주소를 회수합니다. 회수된 IP 주소는 유휴 상태가 되어 클라이언트에 다시 할당될 수 있습니다.
IP 바인딩 해제	MAC 주소에 정적으로 바인딩된 IP 주소를 해제합니다.
IP 를 예약하지 않음	원래 동적으로 할당되지 않은 구성된 IP 주소를 해제합니다.
새로 고치다	페이지에 표시된 정보를 새로 고칩니다.

- DHCP 주소 풀 목록 새로 고침

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **DHCP** > **DHCP 주소 풀**을 선택합니다.
2. **주소 풀 목록**에서 **새로 고침을** 클릭합니다.

4.5.2.4.2 DHCP 릴레이

절차

• DHCP 릴레이 만들기

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **DHCP** > **DHCP 릴레이**를 선택합니다.
2. **Create(만들기)**를 클릭합니다. **DHCP 릴레이 만들기** 페이지가 그림 1 과 같이 표시됩니다.

그림 1 DHCP 릴레이 만들기

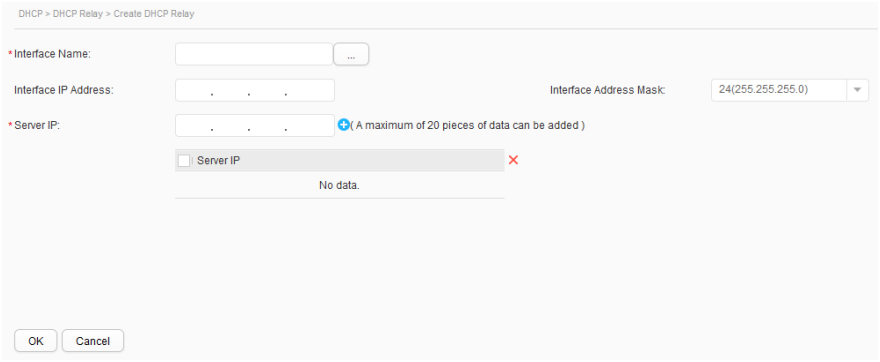


표 1 은 페이지의 매개변수를 설명합니다.

표 1 DHCP 릴레이 생성을 위한 매개변수

매개변수	설명
인터페이스 이름	인터페이스의 이름을 지정합니다.
인터페이스 IP 주소	인터페이스의 IP 주소를 지정합니다.
인터페이스 주소 마스크	서브넷 마스크를 지정합니다.
서버 IP	DHCP 서버의 IP 주소를 지정합니다. DHCP 서버 IP 주소를 생성하려면 DHCP 서버 IP 주소를 입력하고 ⊕을 클릭합니다. 하나 개 이상의 DHCP 서버 IP 주소를 삭제하려면 DHCP 서버 IP 주소의 확인란을 선택하거나 **서버 IP** 옆에 있는 확인란을 선택하고 ✕를 클릭하십시오

3. 매개변수를 설정합니다.
4. Ok(확인)을 클릭합니다.

• DHCP 릴레이 수정

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **DHCP** > **DHCP 릴레이**를 선택합니다.
2. **DHCP 릴레이 목록**에서 인터페이스의 이름을 클릭합니다. DHCP 릴레이를 수정하는 페이지가 표시됩니다. 표 1 은 페이지의 매개변수를 설명합니다.
3. 매개변수 구성을 수정하십시오.
4. Ok(확인)을 클릭합니다.

• DHCP 릴레이 삭제

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **DHCP** > **DHCP 릴레이**를 선택합니다.
2. **DHCP 릴레이 목록**에서 삭제할 DHCP 릴레이의 체크 박스를 선택하고 **삭제**를 클릭합니다. 시스템에서 DHCP 릴레이를 삭제할지 여부를 묻습니다.
3. Ok(확인)을 클릭합니다.

• DHCP 릴레이 목록 새로 고침

1. **Configuration(구성)** > **Basic Services(기본 서비스)** > **DHCP** > **DHCP 릴레이**를 선택합니다.
2. **DHCP 릴레이 목록**에서 **새로 고침**을 클릭합니다.

4.5.2.5 정적 경로

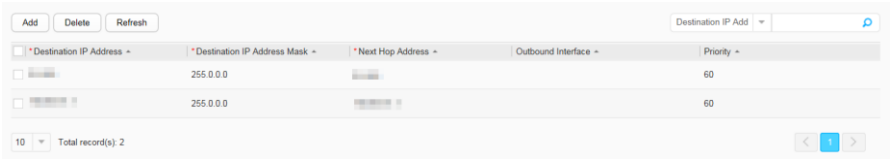
4.5.2.5.1 IPv4 정적 경로

절차

• IPv4 고정 경로를 확인하십시오.

1. 기능 영역에서 **Configuration(구성)**을 클릭합니다. **IPv4 정적 경로** 페이지를 그림 1 과 같이 열기 위해 **Basic Services(기본 서비스)** > **Static Routes(정적 경로)** > **IPv4 Static Routes(IPv4 정적 경로)**를 선택합니다.

   그림 1 IPv4 고정 경로



2. 검색 기준을 설정합니다.

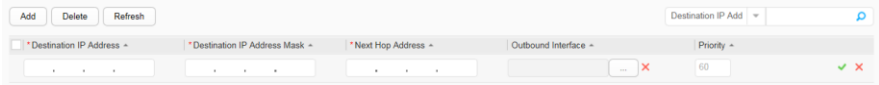
3. 일치하는 모든 레코드를 표시하려면 를 클릭하십시오.

• IPv4 고정 경로를 추가합니다.

1. 기능 영역에서 **Configuration(구성)**을 클릭합니다. **IPv4 정적 경로** 페이지를 그림 1 과 같이 열기 위해 **Basic Services(기본 서비스)** > **Static Routes(정적 경로)** > **IPv4 Static Routes(IPv4 정적 경로)**를 선택합니다.

2. 그림 2 와 같이 **추가**를 클릭하여 IPv4 고정 경로 설정을 표시합니다.

   그림 2 IPv4 고정 경로 추가



3. **대상 IP 주소**, **대상 IP 주소 마스크**, **다음 홉 주소** 및 **우선 순위** 값을 설정합니다. ... 를 클릭하여 **아웃바운드 인터페이스**를 선택합니다.

4. 를 클릭하여 구성을 완료합니다.

• IPv4 고정 경로를 삭제합니다.

1. 기능 영역에서 **Configuration(구성)**을 클릭합니다. **IPv4 정적 경로** 페이지를 그림 1 과 같이 열기 위해 **Basic Services(기본 서비스)** > **Static Routes(정적 경로)** > **IPv4 Static Routes(IPv4 정적 경로)**를 선택합니다.

2. 삭제할 IPv4 의 정적 경로를 선택하고 **삭제**를 클릭합니다.

3. 표시되는 대화 상자에서 **Ok(확인)을 클릭**합니다.

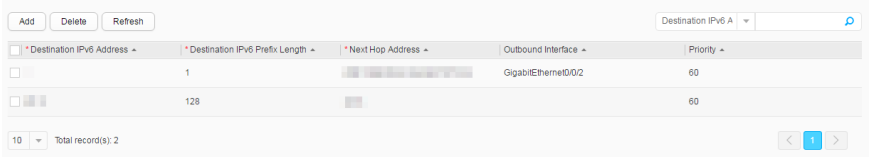
4.5.2.5.2 IPv6 정적 경로

절차

• IPv6 고정 경로를 확인하십시오.

1. 기능 영역에서 **Configuration(구성)**을 클릭합니다. **IPv6 정적 경로** 페이지를 그림 1 과 같이 열기 위해 **Basic Services(기본 서비스)** > **Static Routes(정적 경로)** > **IPv6 Static Routes(IPv6 정적 경로)**를 선택합니다.

그림 1 IPv6 고정 경로



2. 검색 기준을 설정합니다.

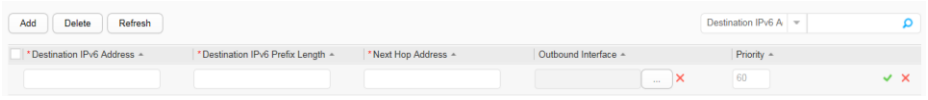
3. 일치하는 모든 레코드를 표시하려면 를 클릭하십시오.

• IPv6 고정 경로를 추가합니다.

1. 기능 영역에서 **Configuration(구성)**을 클릭합니다. **IPv6 정적 경로** 페이지를 그림 1 과 같이 열기 위해 **Basic Services(기본 서비스)** > **Static Routes(정적 경로)** > **IPv6 Static Routes(IPv6 정적 경로)**를 선택합니다.

2. 그림 2 와 같이 **추가**를 클릭하여 IPv6 고정 경로 설정을 표시합니다.

그림 2 IPv6 고정 경로 추가



3. **대상 IPv6 주소**, **대상 IPv6 접두사 길이**, **다음 홉 주소** 및 **우선 순위** 값을 설정합니다. **아웃바운드 인터페이스를** 클릭 ... 하여 선택 합니다.

4. 클릭 하여 구성을 완료합니다.

• IPv6 고정 경로를 삭제합니다.

1. 기능 영역에서 **구성**을 클릭합니다. 선택 **기본 서비스** > **정적 경로** >의 **IPv6 정적 경로를** 열기 위해 **IPv6 의 고정 경로의** 페이지를 같이 그림 1 .

2. 삭제하도록 IPv6 정적 경로를 선택하고 클릭 **삭제** .

3. 표시되는 대화 상자에서 **Ok(확인)을 클릭합니다.**

4.5.3 고급 서비스

4.5.3.1 Cisco ISE 에 연결

문맥

Cisco ISE 에 연결한다는 것은 NAC(네트워크 승인 제어) 네트워크에서 인증 및 권한 부여를 위해 Cisco ISE 서버를 사용하는 것을의미합니다. NAC 는 802.1X, MAC, 포털 인증을 포괄하는 E2E 보안 아키텍처의 일종으로 집계 및 접근 계층 구성을 지원한다. NAC 는 장치 관리자 및 액세스 사용자에 대한 인증, 권한 부여 및 계정을 활성화하여 장치 및 네트워크 보안을 보장합니다.

절차

1. **Configuration(구성)** > **Advanced Services(고급 서비스)** > **Cisco ISE 에 연결을** 선택합니다. 구성 페이지가 표시됩니다.
2. **Select Authentication Interfaces(인증 인터페이스 선택)** 페이지에서 실제 요구 사항에 따라 다음 작업 중 하나를 수행하여 인증 구성에 대한 인터페이스를 선택합니다:
    - 인터페이스 아이콘을 클릭하여 인터페이스를 선택합니다. 아이콘을 다시 클릭하여 인터페이스를 선택 취소할 수 있습니다.
    - 마우스를 끌어 연속 인터페이스를 일괄적으로 선택합니다.
    - 여러 인터페이스 아이콘을 클릭하여 선택합니다. 특정 아이콘을 다시 클릭하여 인터페이스를 선택 해제할 수 있습니다.

    인터페이스를 선택한 후 **인터페이스 인증 구성 지우기**를 클릭하여 인터페이스의 원래 인증 **구성**을 지웁니다.
3. 장치의 모든 인증 구성을 지우려면 **인증 구성 지우기**를 클릭합니다.

4. **인증 방법**에 **802.1X**, **MAC**, 또는 **포털**을 설정합니다.
5. **네트워크 계층**에 **집계 층** 또는 **액세스 계층을** 설정합니다.

> **NOTE**
>
> **네트워크 계층**은 **인증 방법**이 **802.1X** 로 설정된 경우에만 구성할 수 있습니다.

6. 파라미터의 지정 **인증 구성을**, 도시 한 바와 같이 도 1 .

> **NOTE**
>
> **인증 방법**이 **802.1X** 로 설정되고 **네트워크 계층**이 **액세스 계층**으로 설정된 경우에는 인증 구성이 지원되지 않습니다.

그림 1 인증 구성

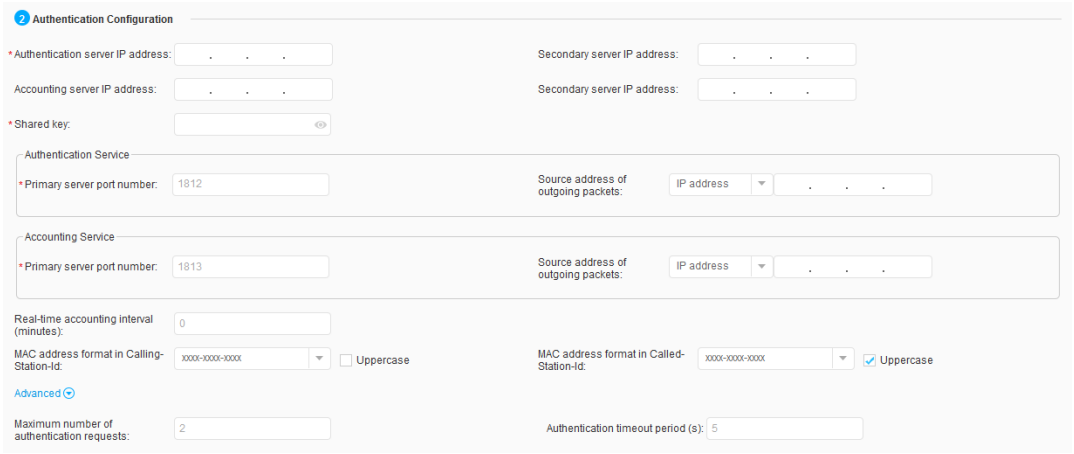


표 1 은 페이지의 매개변수를 설명합니다.

표 1 인증 매개변수 목록

매개변수	설명
인증 서버 IP 주소	RADIUS 인증 서버의 IPv4 주소를 나타냅니다.
보조 서버 IP 주소	보조 RADIUS 인증 서버의 IPv4 주소를 나타냅니다.
회계 서버 IP 주소	RADIUS 계정 서버의 IPv4 주소를 나타냅니다.
보조 서버 IP 주소	보조 RADIUS 계정 서버의 IPv4 주소를 나타냅니다.

표 1 인증 매개변수 목록

매개변수		설명
공용 열쇠		RADIUS 서버의 공유 키를 나타냅니다.
인증 서비스	주 서버 포트 번호	RADIUS 인증 서버의 포트 번호를 나타냅니다.
	나가는 패킷의 소스 주소	스위치에서 RADIUS 인증 서버로 보낸 RADIUS 패킷의 소스 주소를 나타냅니다. • **IP 주소** : 지정된 IPv4 주소입니다. • **VLANIF** : 지정된 VLANIF 인터페이스의 IPv4 주소입니다. • **Loopback** : 지정된 루프백 인터페이스의 IPv4 주소입니다.
	보조 서버 포트 번호	보조 RADIUS 인증 서버의 포트 번호를 나타냅니다. 이 매개변수는 보조 RADIUS 인증 서버의 주소가 구성된 후에만 구성할 수 있습니다.
	보조 서버에서 보낸 패킷의 소스 주소	보조 RADIUS 인증 서버로 전송되는 RADIUS 패킷의 소스 주소를 나타냅니다. • **IP 주소** : 지정된 IPv4 주소입니다. • **VLANIF** : 지정된 VLANIF 인터페이스의 IPv4 주소입니다. • **Loopback** : 지정된 루프백 인터페이스의 IPv4 주소입니다. 이 매개변수는 보조 RADIUS 인증 서버의 주소가 구성된 후에만 구성할 수 있습니다.
회계 서비스	주 서버 포트 번호	RADIUS 계정 서버의 포트 번호를 나타냅니다.
	나가는 패킷의 소스 주소	RADIUS 계정 서버로 전송된 RADIUS 패킷의 소스 주소를 나타냅니다. • **IP 주소** : 지정된 IPv4 주소입니다. • **VLANIF** : 지정된 VLANIF 인터페이스의 IPv4 주소입니다. • **Loopback** : 지정된 루프백 인터페이스의 IPv4 주소입니다.
	보조 서버 포트 번호	보조 RADIUS 계정 서버의 포트 번호를 나타냅니다. 이 매개변수는 보조 RADIUS 계정 서버의 주소가 구성된 후에만 구성할 수 있습니다.
	보조 서버에서 보낸 패킷의 소스 주소	보조 RADIUS 계정 서버로 전송된 RADIUS 패킷의 소스 주소를 나타냅니다. • **IP 주소** : 지정된 IPv4 주소입니다. • **VLANIF** : 지정된 VLANIF 인터페이스의 IPv4 주소입니다. • **Loopback** : 지정된 루프백 인터페이스의 IPv4 주소입니다. 이 매개변수는 보조 RADIUS 계정 서버의 주소가 구성된 후에만 구성할 수 있습니다.
실시간 계산 간격(분)		실시간 계정 간격을 나타냅니다.

표 1 인증 매개변수 목록

매개변수	설명	
Calling-Station-Id 의 MAC 주소 형식	RADIUS 패킷의 Calling-Station-Id(Type 31) 속성에서 MAC 주소의 캡슐화 형식을 나타냅니다.	
Called-Station-Id 의 MAC 주소 형식	RADIUS 패킷의 Called-Station-Id(Type 30) 속성에서 MAC 주소의 캡슐화 형식을 나타냅니다.	
최대 인증 요청 수	802.1X 사용자에 대한 요청 인증 또는 핸드셰이크 패킷의 재전송 시간을 나타냅니다.	이 매개변수는 **인증 방법** 이 **802.1X** 로 설정된 경우에만 구성할 수 있습니다.
인증 시간 초과 기간	클라이언트 인증의 시간 초과 시간을 나타냅니다.	
사용자 이름 모드	MAC 인증 사용자의 사용자 이름 유형을 나타냅니다. • **MAC 주소** : MAC 주소 유형입니다. • **고정 사용자 이름** : 사용자 이름 유형.	이 매개변수는 **인증 방법** 이 **MAC** 으로 설정된 경우에만 구성할 수 있습니다.
MAC 주소	MAC 인증 사용자의 사용자 이름이 MAC 주소임을 나타냅니다. 이 매개변수는 MAC 인증 사용자의 사용자 이름이 MAC 주소 유형으로 설정된 경우에만 구성할 수 있습니다.	
MAC 주소 케이스	MAC 인증 사용자의 사용자 이름이 대문자로 된 MAC 주소임을 나타냅니다. 이 매개변수는 MAC 인증 사용자의 사용자 이름이 MAC 주소 유형으로 설정된 경우에만 구성할 수 있습니다.	
MAC 기반 인증 사용자 이름	MAC 인증 사용자의 사용자 이름이 고정 사용자 이름임을 나타냅니다. 이 매개변수는 MAC 인증 사용자의 사용자 이름이 사용자 이름 유형으로 설정된 경우에만 구성할 수 있습니다.	
MAC 기반 인증 비밀번호	MAC 인증 사용자의 비밀번호를 나타냅니다.	
외부 포털 서버 IP 주소	포털 서버의 IP 주소를 나타냅니다.	
공용 열쇠	포털 서버와의 통신을 위한 공유 키를 나타냅니다.	

표 1 인증 매개변수 목록

매개변수	설명	
SSL 정책	기본 제공 포털 서버에서 사용하는 SSL 정책을 나타냅니다.	이 매개변수는 **인증 방법**이 **포털**로 설정된 경우에만 구성할 수 있습니다.
URL	포털 서버의 리디렉션 URL 을 나타냅니다.	
URL 구분자	URL 의 시작 문자를 따옴표(?)로 바꿉니다.	
LSW IP 주소	URL 에 포함된 AC 의 CAPWAP 게이트웨이 주소를 나타냅니다.	
LSW MAC 주소	URL 에 포함된 AC 의 MAC 주소를 나타냅니다.	
사용자 액세스 URL	사용자가 액세스하고 URL 에 포함된 원래 URL 을 나타냅니다.	
MAC 주소	URL 에 포함된 액세스 사용자의 MAC 주소를 나타냅니다.	
사용자 IP	URL 에 포함된 액세스 사용자의 IP 주소를 나타냅니다.	
시스템 이름	URL 에 포함된 액세스 장치의 시스템 이름을 나타냅니다.	
로그인 URL 키워드/로그인 URL	리디렉션 동안 포털 서버로 전송된 로그인 URL 의 식별 키워드와 액세스 장치의 지정된 URL 을 나타냅니다.	

7. 그림 2 와 같이 **전역 설정**에서 매개 변수를 지정합니다.

NOTE

인증 방법이 **802.1X** 로 설정되고 **네트워크 계층**이 **액세스 계층**으로 설정된 경우에는 전역 설정이 지원되지 않습니다.

그림 2 전역 매개변수 설정

표 2 는 페이지의 매개변수를 설명합니다.

표 2 전역 매개변수 목록

매개변수	설명
사후 인증 도메인에 대한 ACL	전역 ACL 을 나타냅니다.
인증 도메인	인증 도메인을 생성합니다.

8. **802.1X 패킷 투명 전송 구성**에서 매개변수를 지정합니다.

> **NOTE**
>
> **인증 방법**이 **802.1X** 로 설정되고 **네트워크 계층**이 **액세스 계층**으로 설정된 경우 **802.1X 패킷 투명 전송 구성**이 지원됩니다.

인터페이스는 그림 3 에 나와 있습니다.

그림 3 802.1X 투명 전송 구성

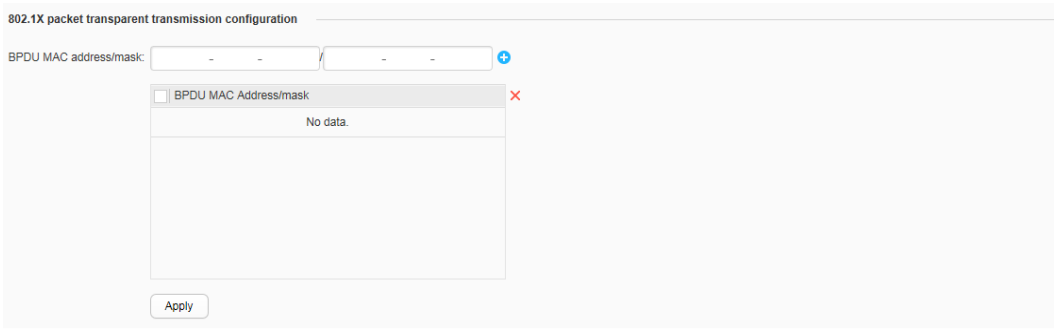


표 3 은 페이지의 매개변수를 설명합니다.

표 3 802.1X 투명 전송 구성

매개변수	설명
투명하게 전송된 802.1X 패킷의 대상 MAC 주소	사용자 정의 프로토콜 패킷의 멀티캐스트 대상 MAC 주소를 나타냅니다.
패킷의 목적지 멀티캐스트 MAC 주소를 대체하는 멀티캐스트 MAC 주소	레이어 2 프로토콜 패킷의 대상 MAC 주소를 대체하는 멀티캐스트 MAC 주소를 나타냅니다.

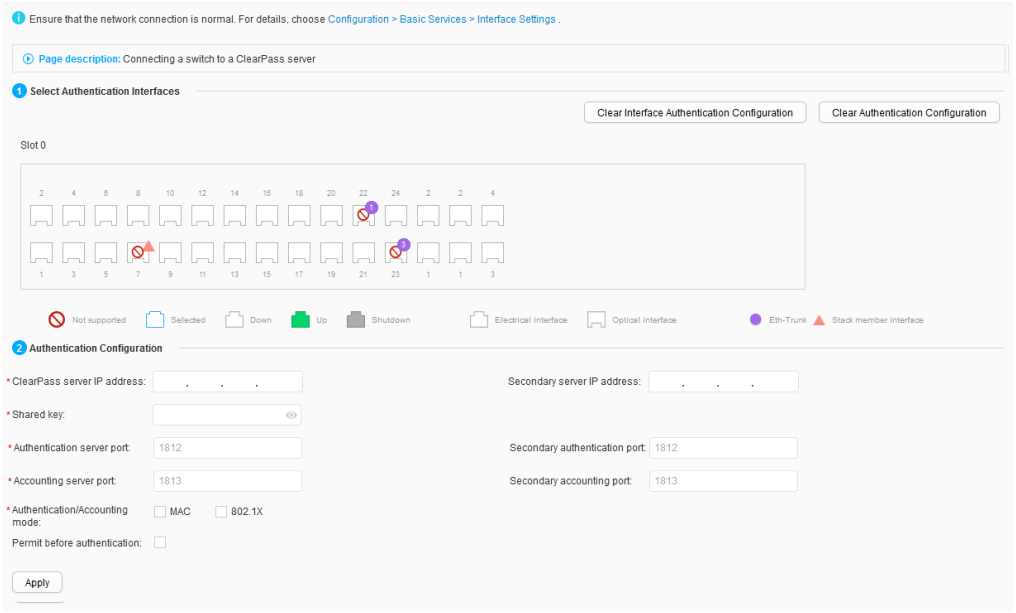
9. **Apply(적용)을 클릭**하여 구성을 완료합니다.

4.5.3.2 Aruba ClearPass 에 연결

절차

1. **Configuration(구성) > Advanced Services(고급 서비스) > Aruba ClearPass 에 연결을** 선택합니다. 그림 1 과 같이 구성 페이지가 표시됩니다.

   그림 1 ClearPass 에 스위치 연결



2. **인증 인터페이스 선택 영역**에서 실제 요구 사항에 따라 다음 작업 중 하나를 수행하여 인증 구성을 위한 인터페이스를 선택합니다.
   - 인터페이스 아이콘을 클릭하여 인터페이스를 선택합니다. 아이콘을 다시 클릭하여 인터페이스를 선택 취소할 수 있습니다.
   - 마우스를 끌어 연속 인터페이스를 일괄적으로 선택합니다.
   - 여러 인터페이스 아이콘을 클릭하여 선택합니다. 특정 아이콘을 다시 클릭하여 인터페이스를 선택 해제할 수 있습니다.
3. (선택 사항) 인터페이스에서 기존 인증 구성을 지우려면 인터페이스를 선택하고 **Clear Interface Authentication Configuration(인터페이스 인증 구성 지우기)을** 클릭합니다.

장치의 모든 인증 구성을 지우려면 **인증 구성 지우기**를 클릭합니다.

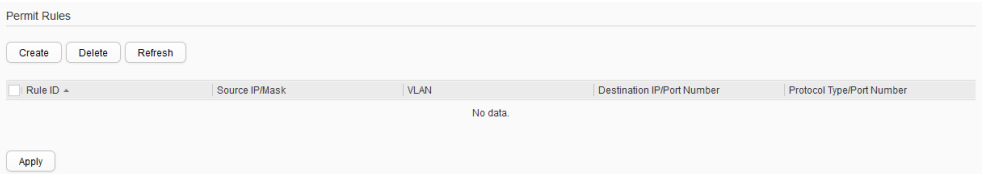
4. 에서 **인증 구성** 영역을 참조하여 인증 파라미터를 설정 표 1 .

표 1 인증 매개변수

매개변수	설명
ClearPass 서버 IP 주소	ClearPass 서버의 IPv4 주소입니다.
보조 서버 IP 주소	ClearPass 서버의 백업 IPv4 주소.
공용 열쇠	ClearPass 서버의 공유 키입니다.
인증 서버 포트	ClearPass 서버의 인증 포트 번호입니다.
2 차 인증 포트	ClearPass 서버의 백업 인증 포트 번호입니다.
회계 서버 포트	ClearPass 서버의 계정 포트 번호입니다.
보조 회계 포트	ClearPass 서버의 백업 계정 포트 번호입니다.
인증/회계 모드	인증 및 계정 모드.
인증 전 허가	무인증 규칙을 구성합니다.

5. **인증 전 허용**을 선택합니다. **허가 규칙** 영역이 그림 2 와 같이 표시됩니다.

그림 2 무인증 규칙 구성



6. **Create(만들기)를 클릭합니다. 허가 규칙 만들기** 대화 상자가 그림 3 과 같이 표시됩니다.

그림 3 무인증 규칙 생성

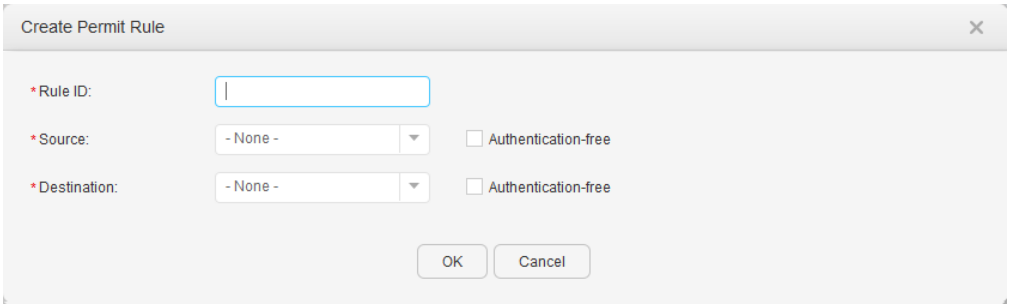


표 2 는 **허가 규칙 생성** 대화 상자의 매개변수를 설명합니다.

표 2 무인증 규칙 매개변수

매개변수	설명
규칙 ID	인증이 필요 없는 규칙의 ID 입니다.
원천	인증되기 전에 일부 리소스에 액세스할 수 있는 사용자의 IP 주소입니다. • - 없음 - • 모든 IP 주소 • 지정 **Source** 가 **Authentication-free 로** 설정되어 있으면 모든 사용자가 액세스할 수 있습니다.
소스 IP 주소	소스 IP 주소. 이 매개변수는 **소스** 가 **지정됨** 으로 설정된 경우에만 구성할 수 있습니다.
마스크	소스 IP 주소의 마스크입니다. 이 매개변수는 **소스** 가 **지정됨** 으로 설정된 경우에만 구성할 수 있습니다.
VLAN	소스 패킷의 VLAN ID 입니다. 이 매개변수는 **소스** 가 **모든 IP 주소** 또는 **지정됨으로** 설정된 경우에만 구성할 수 있습니다.
목적지	사용자가 인증 없이 액세스할 수 있는 대상 네트워크 리소스입니다. • - 없음 - • 모든 IP 주소 • 지정 때 사용자가 인증없이 액세스 할 수있는 대상 네트워크 리소스 **대상이** 설정되어 **인증이없는** .
대상 IP 주소	대상 IP 주소. 이 매개변수는 **대상** 이 **지정됨** 으로 설정된 경우에만 구성할 수 있습니다.
마스크	대상 IP 주소의 마스크입니다. 이 매개변수는 **대상** 이 **지정됨** 으로 설정된 경우에만 구성할 수 있습니다.
프로토콜 유형	사용자가 인증 없이 모든 대상 네트워크 리소스에 액세스하는 데 사용하는 프로토콜입니다. 이 매개변수는 **대상** 이 **지정됨** 으로 설정된 경우에만 구성할 수 있습니다.
대상 포트 번호	UDP 또는 TCP 대상 포트 번호입니다. 이 매개변수는 **대상** 이 **지정됨** 으로 설정된 경우에만 구성할 수 있습니다.

7. Ok(확인)을 클릭합니다.

8. **Apply(적용)을 클릭**하여 구성을 완료합니다.

4.5.3.3 MCQ

4.5.3.3.1 MQC 구성

절차

- 트래픽 분류기 만들기

1. **Configuration(구성) > Advanced Services(고급 서비스) > MQC > MQC 구성을** 선택하십시오. 구성 페이지가 표시됩니다.
2. **트래픽 분류자** 영역에서 **Create(만들기)를 클릭합니다.** 그림 1 과 같이 **트래픽 분류 자 만들기** 페이지가 표시됩니다.

그림 1 트래픽 분류기 생성

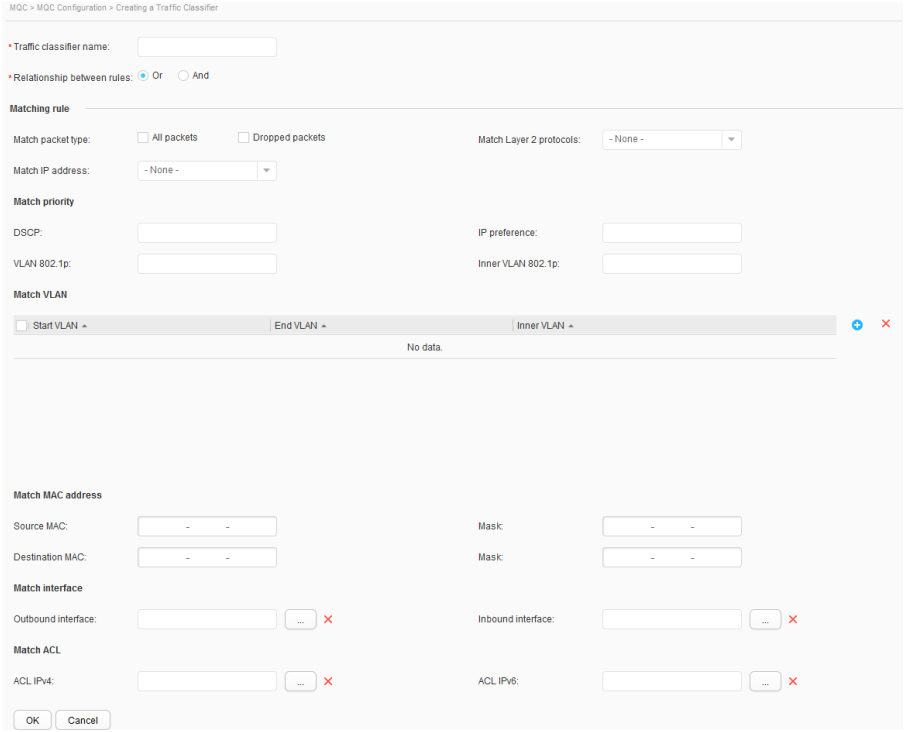


표 1 은 페이지의 매개변수를 설명합니다.

표 1 트래픽 분류기 생성

매개변수	설명
트래픽 분류자 이름	트래픽 분류기의 이름을 나타냅니다.
규칙 간의 관계	트래픽 분류기의 규칙 간의 논리적 관계를 나타냅니다. • **Or** : 규칙 간의 OR 관계. • **And** : 규칙 간의 AND 관계.
일치 규칙	
패킷 유형 일치	모든 데이터 패킷 또는 폐기된 패킷을 기반으로 트래픽 분류를 수행할지 여부를 지정합니다. • **모든 패킷** : 모든 데이터 패킷을 기반으로 하는 트래픽 분류. • **삭제된 패킷** : 폐기된 패킷을 기반으로 하는 트래픽 분류.
레이어 2 프로토콜 일치	트래픽 분류를 위한 레이어 2 캡슐화된 프로토콜 필드를 기반으로 한 일치 규칙을 나타냅니다.

표 1 트래픽 분류기 생성

매개변수	설명
	• **- 없음 -** : Layer 2 캡슐화 프로토콜 필드를 지정하지 않고 트래픽 분류를 수행합니다. • **ARP** : ARP 프로토콜 필드를 기반으로 트래픽 분류를 수행합니다. • **IP** : IP 프로토콜 필드를 기반으로 트래픽 분류를 수행합니다. • **MPLS** : MPLS 프로토콜 필드를 기반으로 트래픽 분류가 수행됩니다. • **RARP** : RARP 프로토콜 필드를 기반으로 트래픽 분류를 수행합니다.
IP 주소 일치	트래픽 분류를 위한 프로토콜을 기반으로 한 일치 규칙을 나타냅니다. • **- 없음 -** : 프로토콜을 지정하지 않고 트래픽 분류를 수행합니다. • **IPv4** : IPv4 프로토콜을 기반으로 트래픽 분류를 수행합니다. • **IPv6** : IPv6 프로토콜을 기반으로 트래픽 분류를 수행합니다.
일치 우선 순위	
DSCP	패킷의 DSCP 우선 순위를 기반으로 트래픽 분류를 구성합니다.
IP 기본 설정	패킷의 IP 기본 설정을 기반으로 트래픽 분류를 구성합니다.
VLAN 802.1p	VLAN 패킷의 802.1p 우선 순위를 기반으로 트래픽 분류를 구성합니다.
VLAN 일치 **노트:** 여러 일치 VLAN 을 구성할 수 있습니다.	
VLAN 시작	VLAN ID 를 기반으로 트래픽 분류를 위한 외부 시작 VLAN 을 구성합니다.
끝 VLAN	VLAN ID 를 기반으로 트래픽 분류를 위해 외부 종단 VLAN 을 구성합니다.

표 1 트래픽 분류기 생성

매개변수	설명
MAC 주소 일치	
소스 MAC	트래픽 분류기의 소스 MAC 주소를 나타냅니다.
마스크	트래픽 분류기에서 소스 MAC 주소의 마스크를 나타냅니다.
대상 MAC	트래픽 분류기의 대상 MAC 주소를 나타냅니다.
마스크	트래픽 분류기에서 MAC 주소의 대상 마스크를 나타냅니다.
경기 인터페이스	
인바운드 인터페이스	트래픽 분류기에서 패킷의 인바운드 인터페이스를 나타냅니다.
ACL 일치	
ACL IPV4	트래픽 분류기의 IPv4 ACL 을 나타냅니다.
ACL IPV6	트래픽 분류기의 IPv6 ACL 을 나타냅니다.

3. 매개변수를 지정합니다.

4. **Ok(확인)을 클릭**하여 구성을 완료합니다.

- 트래픽 분류기 수정

1. **Configuration(구성) > Advanced Services(고급 서비스) > MQC > MQC 구성을** 선택하십시오. 구성 페이지가 표시됩니다.

2. **트래픽 분류자** 영역에서 항목을 클릭합니다. 트래픽 분류자를 수정할 수 있는 페이지가 표시됩니다. 표 1 은 페이지의 매개변수를 설명합니다.

   트래픽 분류자 이름 및 **규칙 간의 관계는** 수정할 수 없습니다.

3. 매개변수를 수정합니다.

4. **Ok(확인)을 클릭**하여 구성을 완료합니다.

- 트래픽 분류기 삭제

1. **Configuration(구성) > Advanced Services(고급 서비스) > MQC > MQC 구성을** 선택하십시오. 구성 페이지가 표시됩니다.
2. **트래픽 분류자** 영역에서 삭제할 항목을 선택하고 **삭제를** 클릭합니다. 그런 다음 확인 메시지가 표시됩니다.
3. **Ok(확인)을 클릭**하여 구성을 완료합니다.

- 트래픽 분류기 새로 고침

1. **Configuration(구성) > Advanced Services(고급 서비스) > MQC > MQC 구성을** 선택하십시오. 구성 페이지가 표시됩니다.
2. **트래픽 분류자** 영역에서 **새로 고침**을 클릭합니다.

- 교통 행동 만들기

1. **Configuration(구성) > Advanced Services(고급 서비스) > MQC > MQC 구성을** 선택하십시오. 구성 페이지가 표시됩니다.
2. **트래픽 동작** 영역에서 **Create(만들기)를 클릭합니다.** 그림 2 와 같이 **교통 동작 만들기** 페이지가 표시됩니다.

그림 2 트래픽 동작 생성

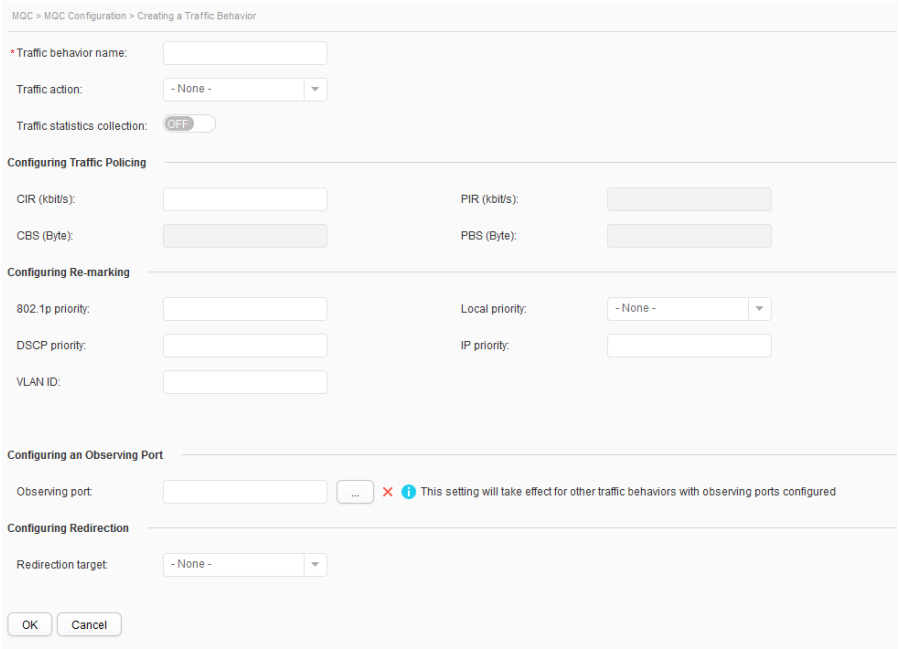


표 2 는 페이지의 매개변수를 설명합니다.

표 2 트래픽 동작 생성

매개변수	설명
교통 행동 이름	트래픽 동작의 이름을 나타냅니다.
교통 행동	교통 행동을 나타냅니다. - **없음** - : 트래픽 분류에 따른 서비스 패킷에 대한 접근 제어를 수행하지 않습니다. **Permit** : 트래픽 분류 규칙과 일치하는 패킷을 원래 정책에 따라 전달합니다. **Deny** : 트래픽 분류 규칙과 일치하는 서비스 흐름은 통과할 수 없습니다.
트래픽 통계 수집	트래픽 통계 수집을 활성화하거나 비활성화합니다.
트래픽 정책 구성	
CIR(kbit/s)	커밋된 정보 속도(CIR)를 나타냅니다.
PIR(kbit/s)	피크 정보 속도(PIR)를 나타냅니다.
CBS(바이트)	커밋된 버스트 크기(CBS)를 나타냅니다.

표 2 트래픽 동작 생성

매개변수	**설명**
PBS(바이트)	피크 버스트 크기(PBS)를 나타냅니다.
녹색 패킷 노란색 패킷 레드 패킷 리마킹 우선순위 유형 802.1p 우선 순위 DSCP 우선 순위	다른 색상의 패킷에 대해 수행할 트래픽 정책 작업, 다시 표시할 우선 순위 유형 및 해당 우선 순위 값을 나타냅니다. 스택에 대한 장치 지원 은 Command Reference 에서 **car(교통 행동 보기)**를 참조하십시오.
재마킹 구성	
802.1p 우선 순위	트래픽 동작에서 VLAN 패킷의 802.1p 우선 순위를 표시합니다.
지역 우선순위	트래픽 동작에서 패킷의 내부 우선 순위를 표시합니다. **노트:** **802.1p 우선 순위** 와 **로컬 우선 순위** 는 동일한 트래픽 동작에 대해 동시에 구성할 수 없습니다.
DSCP 우선 순위	트래픽 동작에서 IP 패킷의 DSCP 우선 순위를 표시합니다.
IP 우선 순위	트래픽 동작에서 패킷의 IP 우선 순위를 표시합니다. **노트:** **DSCP 우선 순위** 와 **IP 우선 순위** 는 동일한 트래픽 동작에 대해 동시에 구성할 수 없습니다.
VLAN ID	트래픽 동작에서 VLAN 패킷의 VLAN ID 를 표시합니다.
관찰 포트 구성	
관찰 포트	관찰 포트를 나타냅니다.
리디렉션 구성	
리디렉션 대상	트래픽 동작에서 패킷 리디렉션 작업을 생성할지 여부를 지정합니다. - **없음** - : 트래픽 동작에서 패킷 리디렉션 작업을 생성하지 않습니다. 인터페이스: 트래픽 동작에서 지정된 인터페이스로 패킷을 리디렉션하는 작업을 만듭니다.

표 2 트래픽 동작 생성

매개변수	설명
	다음 홉 IPv4 주소 : 트래픽 동작에서 패킷을 다음 홉 IPv4 주소로 리디렉션하는 작업을 만듭니다. **다음 홉 IPv6 주소** : 트래픽 동작에서 패킷을 다음 홉 IPv6 주소로 리디렉션하는 작업을 만듭니다.
대상 인터페이스	트래픽 동작에서 패킷이 리디렉션되는 인터페이스를 나타냅니다.
다음 홉 IPv4 주소	트래픽 동작에서 패킷이 리디렉션되는 다음 홉 IPv4 주소를 나타냅니다.
다음 홉 IPv6 주소	트래픽 동작에서 패킷이 리디렉션되는 다음 홉 IPv6 주소를 나타냅니다.
강제 리디렉션	강제 리디렉션을 나타냅니다.

3. 매개변수를 지정합니다.
4. **Ok(확인)을 클릭**하여 구성을 완료합니다.

- 트래픽 동작 수정

1. **Configuration(구성) > Advanced Services(고급 서비스) > MQC > MQC 구성을** 선택하십시오. 구성 페이지가 표시됩니다.
2. **교통 행동** 영역에서 항목을 클릭합니다. 트래픽 동작을 수정할 수 있는 페이지가 표시됩니다. 표 2 는 페이지의 매개변수를 설명합니다.

   트래픽 동작 이름 은 수정할 수 없습니다.
3. 매개변수를 수정합니다.
4. **Ok(확인)을 클릭**하여 구성을 완료합니다.

- 트래픽 동작 삭제

1. **Configuration(구성) > Advanced Services(고급 서비스) > MQC > MQC 구성을** 선택하십시오. 구성 페이지가 표시됩니다.
2. **트래픽 동작** 영역에서 삭제할 항목을 선택하고 **삭제를** 클릭합니다. 그런 다음 확인 메시지가 표시됩니다.
3. **Ok(확인)을 클릭**하여 구성을 완료합니다.

- 트래픽 동작 새로 고침

1. **Configuration(구성) > Advanced Services(고급 서비스) > MQC > MQC 구성을** 선택하십시오. 구성 페이지가 표시됩니다.
2. **트래픽 동작** 영역에서 **새로 고침**을 클릭합니다.

• 트래픽 정책 만들기

1. **Configuration(구성) > Advanced Services(고급 서비스) > MQC > MQC 구성을** 선택하십시오. 구성 페이지가 표시됩니다.
2. **트래픽 정책** 영역에서 **Create(만들기)를 클릭합니다.** 그림 3 과 같이 **교통 정책 만들기** 페이지가 표시됩니다.

   그림 3 트래픽 정책 생성

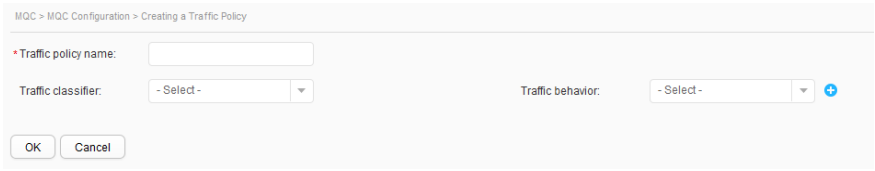


   표 3 은 페이지의 매개변수를 설명합니다.

표 3 트래픽 정책 생성

매개변수	설명
트래픽 정책 이름	트래픽 정책의 이름을 나타냅니다.
트래픽 분류기	트래픽 정책에서 트래픽 분류자를 바인딩합니다.
교통 행동	트래픽 정책에서 트래픽 동작을 바인딩합니다.

3. 매개변수를 지정합니다.

   ⊕를 클릭하면 트래픽 정책에서 여러 트래픽 분류자와 트래픽 동작을 바인딩할 수 있습니다.
4. **Ok(확인)을 클릭**하여 구성을 완료합니다.

• 트래픽 정책 수정

1. **Configuration(구성) > Advanced Services(고급 서비스) > MQC > MQC 구성을** 선택하십시오. 구성 페이지가 표시됩니다.
2. **트래픽 정책** 영역에서 항목을 클릭합니다. 트래픽 정책을 수정할 수 있는 페이지가 표시됩니다. 표 3 은 페이지의 매개변수를 설명합니다.

   트래픽 정책 이름 은 수정할 수 없습니다.

3. 매개변수를 수정합니다.
4. **Ok(확인)을 클릭**하여 구성을 완료합니다.

- 트래픽 정책 삭제

1. **Configuration(구성) > Advanced Services(고급 서비스) > MQC > MQC 구성을** 선택하십시오. 구성 페이지가 표시됩니다.
2. **트래픽 정책** 영역에서 삭제할 항목을 선택하고 **삭제를** 클릭합니다. 그런 다음 확인 메시지가 표시됩니다.
3. **Ok(확인)을 클릭**하여 구성을 완료합니다.

- 트래픽 정책 새로 고침

1. **Configuration(구성) > Advanced Services(고급 서비스) > MQC > MQC 구성을** 선택하십시오. 구성 페이지가 표시됩니다.
2. **트래픽 정책** 영역에서 **새로 고침**을 클릭합니다.

4.5.3.4 음성 VLAN

4.5.3.4.1 OUI 구성

문맥

OUI 를 미리 설정할 수 있습니다. OUI 는 MAC 주소의 처음 24 비트입니다. IEEE(Institute of Electrical and Electronics Engineers)는 각 공급업체에 OUI 를 할당하고 OUI 를 기반으로 장치 공급업체를 식별할 수 있습니다. 당신은에 OUI 의 마스크를 설정할 수있는 스위치 하는 MAC 주소의 길이를 조절하는 스위치가 되면 OUI 와 일치합니다.

절차

• OUI 를 만듭니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > 음성 VLAN > OUI 구성을** 선택하여 **OUI 구성** 페이지에 접근합니다.

2. 그림 1 과 같이 **Create(만들기)를 클릭합니다.**

   그림 1 OUI 만들기

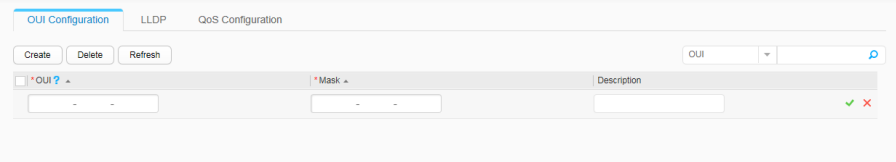
   

   표 1 은 **OUI 구성** 페이지의 매개변수를 설명합니다.

   표 1 OUI 구성 페이지의 매개변수 설명

매개변수	설명
위	이 매개변수는 필수입니다. 음성 패킷의 MAC 주소를 지정합니다(예: **0812-f231-05e1**) .
마스크	이 매개변수는 필수입니다. 마스크를 입력하십시오(예: **ffff-ffff-ffff**) .
설명	OUI 에 대한 설명을 입력합니다.

3. 매개변수를 설정합니다.

4. ✔을 클릭합니다.

   NOTE

   OUI 구성이 완료된 후 OUI 의 설명을 수정할 수 있습니다.

• OUI 를 삭제합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > 음성 VLAN > OUI 구성을** 선택하여 **OUI 구성** 페이지에 접근합니다.
2. 삭제할 데이터를 선택하고 **삭제**를 클릭합니다. 시스템에서 데이터 삭제 여부를 묻습니다.
3. Ok(확인)을 클릭합니다.

- OUI 를 새로 고칩니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > 음성 VLAN > OUI 구성을** 선택하여 **OUI 구성** 페이지에 접속합니다.
2. 갱신할 데이터를 선택하고 **새로 고침**을 클릭합니다.

4.5.3.4.2 LLDP

문맥

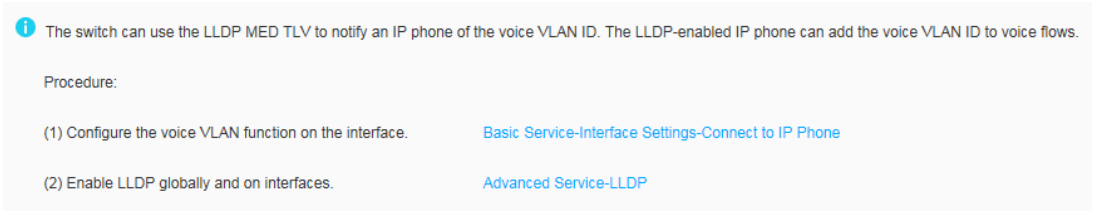
스위치는 LLDP MED TLV 와 함께 LLDPDU 를 전송하여 연결된 IP 전화에 음성 VLAN ID 를 알립니다. IP 전화는 LLDP MED TLV 와 함께 LLDPDU 를 수신한 후 LLDPDU 에 음성 VLAN ID 를 추가합니다.

절차

1. **Configuration(구성) > Advanced Services(고급 서비스) > 음성**

   VLAN > **LLDP** 를 선택하여 그림 1 과 같이 **LLDP** 페이지에 접근합니다.

   그림 1 LLDP



2. 기본 서비스-인터페이스 설정-IP 전화에 연결을 클릭하여 IP 전화에 연결 페이지에 접근하여 음성 VLAN 구성을 완료합니다.

3. 고급 서비스-LLDP 를 클릭하여 **LLDP** 페이지에 액세스하고 스위치 및 인터페이스에서 LLDP 구성을 완료합니다. LLDP 기반의 음성 VLAN 이 구성됩니다.

4.5.3.4.3 QoS 구성

문맥

음성 VLAN 기능이 구축된 네트워크에서 음성 서비스는 데이터 서비스보다 실시간성이 높습니다. 음성 데이터는 전송 중 지연을 최소화하기 위해 다른 서비스 데이터보다 우선 순위가 높아야 합니다. 음성 VLAN 의 802.1p 또는 DSCP 우선 순위는 음성 데이터가 더 높은 우선 순위로 전송되도록 조정됩니다.

NOTE

인터페이스 설정 > IP 전화에 연결을 통해 스위치 인터페이스에 VLAN 이 구성되었고 음성 VLAN 기능이 활성화되었음을 입력합니다. 그렇지 않으면 QoS 구성이 유효하지 않습니다.

절차

1. **Configuration(구성) > Advanced Services(고급 서비스) > 음성 VLAN** >의 **QoS 구성**을 선택하여 그림 1 과 같이 **QoS 구성** 페이지에 접근합니다.

   그림 1 QoS 구성

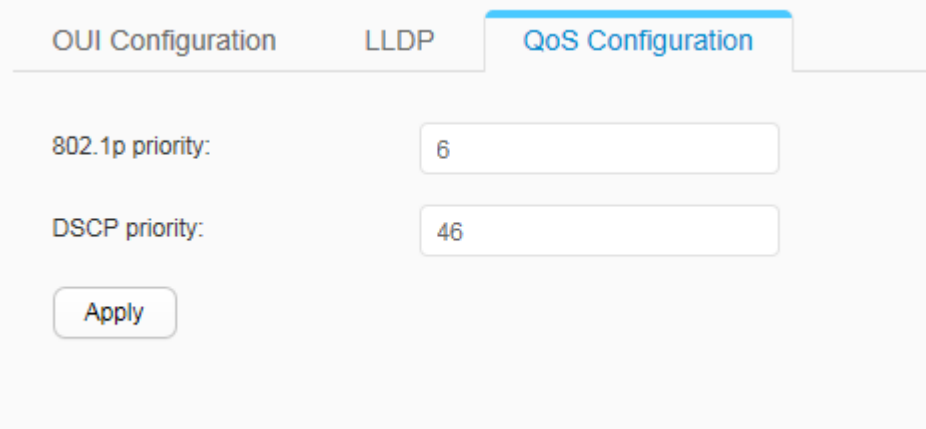


   표 1 은 **QoS 구성** 페이지의 매개변수를 설명합니다.

표 1 QoS 구성

매개변수	설명
802.1p 우선 순위	802.1p 우선 순위를 지정합니다. 값은 0 에서 7 사이의 정수입니다. 기본값은 6 입니다. 값이 클수록 우선 순위가 높습니다.
DSCP 우선 순위	DSCP 우선 순위를 지정합니다. 값은 0 에서 63 사이의 정수입니다. 기본값은 46 입니다.

2. 매개변수를 설정하고 **Apply(적용)을 클릭**합니다.

4.5.3.5 MAC

문맥

각 스위치는 MAC 주소 테이블을 유지 관리합니다. MAC 테이블은 학습된 MAC 주소, VLAN ID 및 아웃바운드 인터페이스를 기록합니다. 데이터를 전달하기 위해 스위치는 패킷에 대한 아웃바운드 인터페이스를 결정하기 위해 패킷에 포함된 대상 MAC 주소 및 VLAN ID 를 기반으로 MAC 테이블을 검색합니다. 따라서 브로드캐스트 트래픽이 감소합니다. 다음 MAC 주소 유형 및 기능을 구성합니다.

- 인터페이스는 소스 MAC 주소 학습을 기반으로 동적 항목을 얻습니다. 동적 항목은 에이징될 수 있습니다.
- 정적 MAC 항목은 수동으로 구성되며 에이징되지 않습니다. 자세한 내용 은 정적 MAC 구성을 참조하십시오.
- 블랙홀 MAC 항목은 지정된 소스 또는 대상 MAC 주소가 있는 데이터 프레임을 삭제하는 데 사용됩니다. 블랙홀 MAC 항목은 수동으로 구성되며 에이징되지 않습니다. 자세한 내용 은 블랙홀 MAC 주소 항목 구성을 참조하십시오.
- ARP 항목 수정은 ARP 주소 스푸핑 공격을 방어하도록 구성할 수 있습니다. 자세한 내용은 ARP 항목 수정 구성을 참조하십시오.
- 포트 보안은 인터페이스에서 학습된 MAC 주소를 보안 MAC 주소로 만들어 보안 MAC 주소와 정적 MAC 주소가 있는 호스트만 인터페이스를 통해 스위치와 통신할 수 있도록 하여 스위치 보안을 향상시킵니다. 자세한 내용은 포트 보안 구성을 참조하십시오.

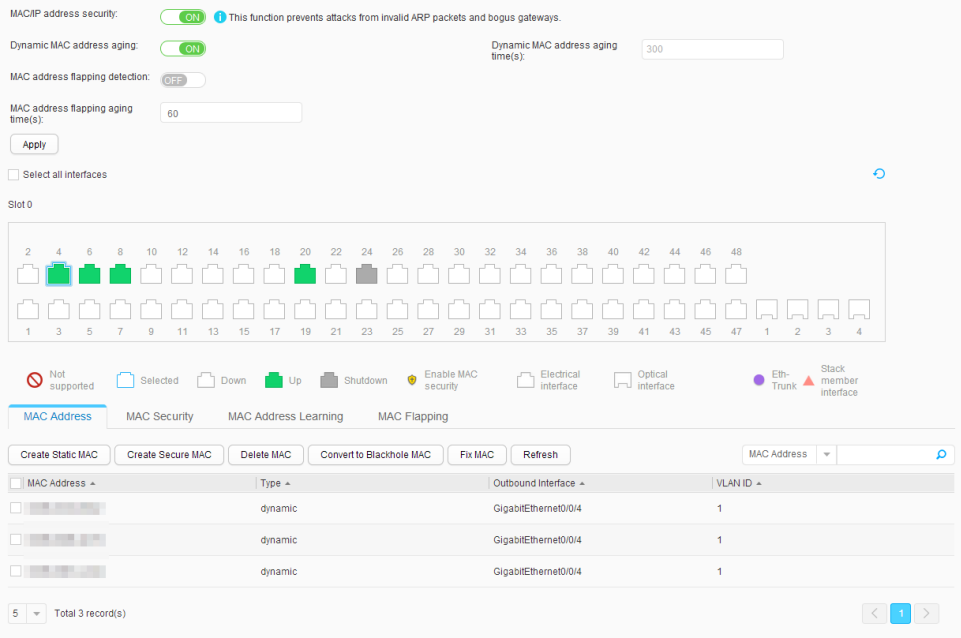
절차

- MAC/IP 주소 보안 구성 및 동적 MAC 주소의 에이징 시간

1. 그림 1 과 같이 **Configuration** > **Advanced**

   Services > **MAC 을** 선택합니다.

그림 1 MAC 주소 항목 쿼리



[표 1](#) 은 페이지의 매개변수를 설명합니다.

표 1 MAC 주소 에이징 및 MAC 주소 플래핑 감지 구성

매개변수	설명
MAC/IP 주소 보안	ARP 게이트웨이 충돌 방지 기능을 활성화할지 여부를 지정합니다.
동적 MAC 주소 에이징	MAC 주소 항목의 에이징 시간을 구성할지 여부를 지정합니다.
동적 MAC 주소 에이징 시간	동적 MAC 주소 항목의 에이징 시간을 지정합니다.
MAC 주소 플래핑 감지	전역 MAC 주소 플래핑 감지를 구성할지 여부를 지정합니다.
MAC 주소 플래핑 에이징 시간	MAC 주소 항목 플랩의 에이징 시간을 지정합니다.

2. 매개변수를 설정합니다.

3. **Apply(적용)을 클릭**합니다.

- MAC 주소 항목 쿼리

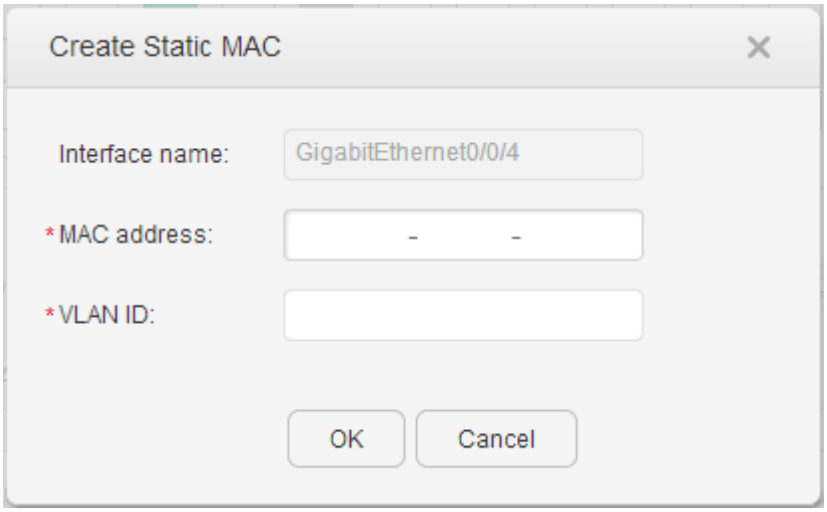
1. [그림 1](#) 과 같이 **Configuration** > **Advanced Services** > **MAC 을** 선택합니다.

2. **MAC 주소** 탭을 클릭하고 인터페이스를 선택합니다. **MAC 주소** 탭 페이지가 표시됩니다.
3. **새로 고침**을 클릭하여 MAC 주소 목록의 항목을 새로 고칩니다.
4. **MAC 주소**, **유형**, **아웃바운드 인터페이스** 및 **VLAN ID 를** 기반으로 MAC 주소 항목을 조회하기 위한 검색 항목을 설정합니다.
5. 을 클릭합니다. 검색 결과가 표시됩니다.

- 정적 사용자 구성

1. 그림 1 과 같이 **Configuration** > **Advanced Services** > **MAC 을** 선택합니다.
2. **MAC 주소** 탭을 클릭하고 인터페이스를 선택합니다. **MAC 주소** 탭 페이지가 표시됩니다.
3. **정적 MAC 생성을** 클릭합니다. 그림 2 와 같이 **정적 MAC 작성** 페이지가 표시됩니다.

그림 2 정적 Mac 만들기



4. 매개변수를 설정합니다.
5. Ok(확인)을 클릭합니다.

- 고정 보안 MAC 주소 생성

1. 그림 1 과 같이 **Configuration** > **Advanced Services** > **MAC 을** 선택합니다.
2. **MAC 주소** 탭을 클릭하고 인터페이스를 선택합니다. **MAC 주소** 탭 페이지가 표시됩니다.

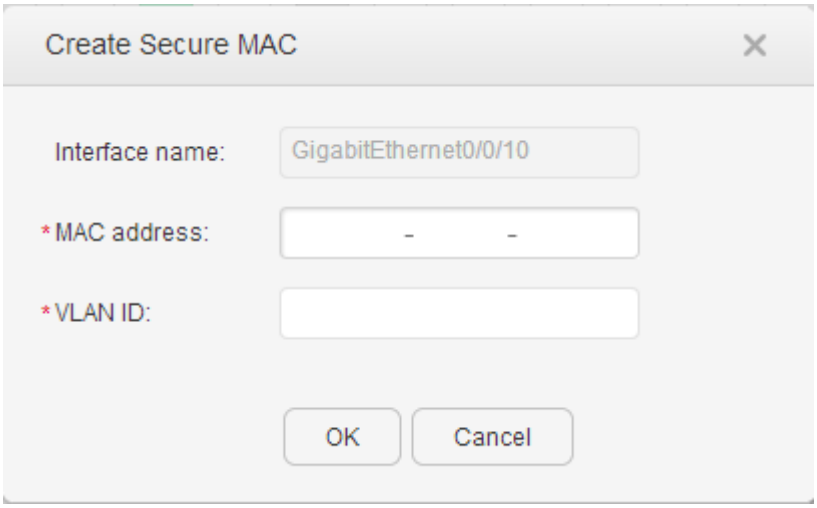
NOTE

고정 보안 MAC 주소를 생성하기 전에 포트 보안 구성을 참조하여 포트 보안을 활성화하십시오.

포트 보안이 활성화되면 인터페이스 옆에 노란색 실드 식별자가 표시됩니다.

3. **보안 MAC 생성을** 클릭합니다. 그림 3 과 같이 **보안 만들기 MAC 의** 페이지가 표시됩니다.

   그림 3 보안 MAC 주소 생성



4. 매개변수를 설정합니다.
5. Ok(확인)을 클릭합니다.

- MAC 주소 항목 삭제

1. 그림 1 과 같이 **Configuration** > **Advanced Services** > **MAC 을** 선택합니다.
2. **MAC 주소** 탭을 클릭하고 인터페이스를 선택합니다. **MAC 주소** 탭 페이지가 표시됩니다.
3. 항목을 선택하고 **MAC 삭제를** 클릭합니다. 시스템에서 항목을 삭제할지 여부를 묻습니다.
4. Ok(확인)을 클릭합니다.

- 블랙홀 MAC 주소 항목 구성

1. 그림 1 과 같이 **Configuration** > **Advanced Services** > **MAC 을** 선택합니다.
2. **MAC 주소** 탭을 클릭하고 인터페이스를 선택합니다. **MAC 주소** 탭 페이지가 표시됩니다.
3. 항목을 선택하고 **Blackhole MAC 으로 변환을** 클릭합니다. 시스템은 항목을 블랙홀 MAC 주소 항목으로 구성할지 여부를 묻습니다.

NOTE

동적 MAC 주소 항목만 블랙홀 MAC 주소 항목으로 구성할 수 있습니다.

동적 MAC 주소 항목이 블랙홀 MAC 주소 항목으로 구성된 후 MAC 주소 목록에 표시될 수 있도록 **모든 인터페이스** 선택을 **선택**합니다.

4. Ok(확인)을 클릭합니다.

• ARP 항목 수정 구성

1. 그림 1 과 같이 **Configuration** > **Advanced Services** > **MAC 을** 선택합니다.
2. **MAC 주소** 탭을 클릭하고 인터페이스를 선택합니다. **MAC 주소** 탭 페이지가 표시됩니다.
3. 항목을 선택하고 **MAC 수정을** 클릭합니다. 시스템에서 MAC 주소 항목을 수정할지 여부를 묻습니다.

NOTE

동적 MAC 주소 항목만 수정할 수 있습니다.

4. Ok(확인)을 클릭합니다.

• 포트 보안 구성

1. 그림 1 과 같이 **Configuration** > **Advanced Services** > **MAC 을** 선택합니다.
2. **MAC 보안** 탭을 클릭합니다. **MAC 보안** 탭 페이지가 표시됩니다.
3. 그림 4 와 같이 포트를 선택합니다.

그림 4 포트 보안 구성

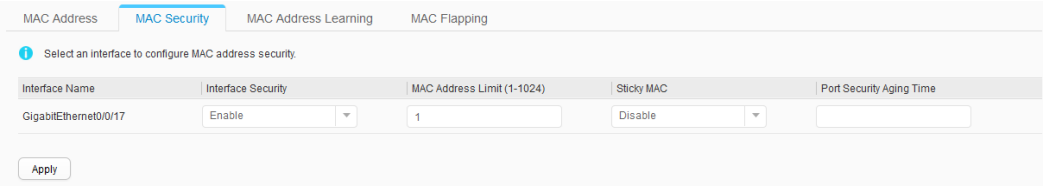


표 2 는 **MAC 보안** 탭 페이지의 매개변수를 설명합니다.

표 2 포트 보안 구성

매개변수	설명
인터페이스 이름	-
인터페이스 보안	네트워크에 높은 액세스 보안이 필요한 경우 지정된 포트에서 포트 보안을 구성할 수 있습니다. 이 포트에서 학습한 MAC 주소는 동적 보안 MAC 주소 또는 고정 MAC 주소로 변경됩니다. 학습된 MAC 주소의 수가 제한에 도달하면

표 2 포트 보안 구성

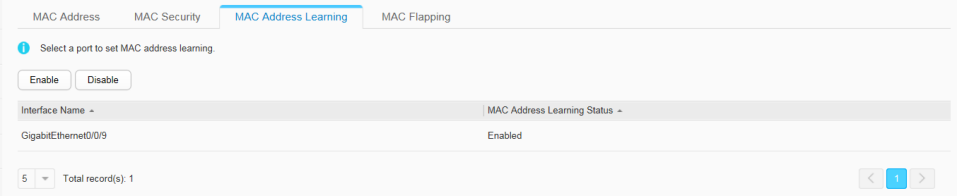
매개변수	설명
	포트는 새 MAC 주소를 학습하지 않습니다. 이렇게 하면 신뢰할 수 없는 MAC 주소를 가진 장치가 이러한 포트에 연결되는 것을 방지하여 장치와 네트워크의 보안이 향상됩니다.
MAC 주소 제한 (1-1024)	포트에서 학습할 수 있는 최대 MAC 주소 수입니다.
스티키 맥	고정 MAC 주소는 만료되지 않으며 장치가 다시 시작된 후에도 존재합니다.
포트 보안 에이징 시간	인터페이스에서 보안 동적 MAC 주소의 에이징 시간입니다.

4. 매개변수를 설정합니다.
5. **Apply(적용)을 클릭**합니다.

- MAC 주소 학습 구성

1. 그림 1 과 같이 **Configuration** > **Advanced Services** > **MAC 을** 선택합니다.
2. **MAC 주소 학습** 탭을 클릭하여 **학습 MAC 주소** 페이지에 접근하고 그림 5 와 같이 인터페이스 선택 영역에서 구성할 인터페이스를 선택합니다.

   그림 5 MAC 주소 학습 구성

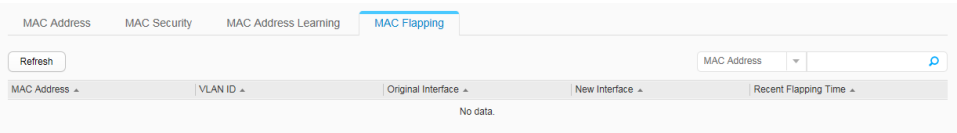


3. **활성화** 또는 **비활성화**를 클릭하여 인터페이스에서 MAC 주소 학습을 활성화하거나 비활성화합니다.

- MAC 주소 플랩 정보 확인

1. 그림 1 과 같이 **Configuration** > **Advanced Services** > **MAC 을** 선택합니다.
2. **MAC Flapping** 탭을 클릭하여 그림 6 과 같이 **MAC Flapping** 페이지에 접근합니다.

   그림 6 MAC 플래핑 페이지



3. **새로 고침**을 클릭하여 MAC 주소 플랩 정보를 새로 고칩니다.

4.5.3.6 IP 서비스

4.5.3.6.1 ARP

문맥

근거리 통신망(LAN)에서 호스트 또는 네트워크 장치는 데이터를 보내기 전에 대상 호스트 또는 장치의 IP 주소를 알아야 합니다. 또한 IP 패킷은 물리적 네트워크를 통한 전송을 위해 프레임으로 캡슐화되어야 하므로 호스트 또는 네트워크 장치는 대상 호스트 또는 장치의 물리적 주소(MAC 주소)를 알아야 합니다. 따라서 IP 주소에서 물리적 주소로의 매핑이 필요합니다. ARP(Address Resolution Protocol)는 IP 주소를 물리적 주소(이더넷 MAC 주소)에 매핑하기 위해 도입되었습니다.

절차

- 고정 ARP 항목을 만듭니다.

  1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > ARP > 정적 ARP 를** 선택하여 **정적 ARP** 페이지에 접근합니다.
  2. 그림 1 과 같이 **Create(만들기)를 클릭합니다.**

그림 1 고정 ARP 항목 만들기

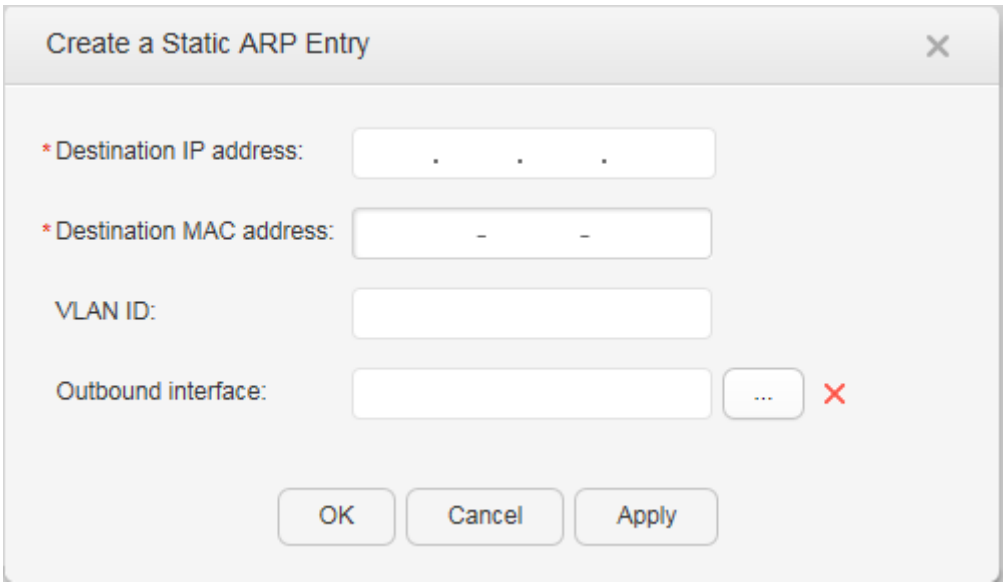


표 1 은 페이지의 매개변수를 설명합니다.

표 1 고정 ARP 항목 생성

매개변수	설명
대상 IP 주소	대상 IP 주소를 입력합니다(예: **10.10.10.1**) . **노트:** 이 매개변수는 VLANIF 인터페이스에 구성된 VRRP 그룹의 가상 IP 주소로 설정할 수 없습니다. 그렇지 않으면 잘못된 호스트 경로가 생성되어 전달 오류가 발생합니다.
대상 MAC 주소	IP 주소를 매핑하는 이더넷 MAC 주소를 입력합니다(예: **0812-f231-05e1**) .
VLAN ID	IP 주소에 해당하는 VLAN ID 를 입력합니다. **노트:** • VLAN ID 를 입력하면 생성된 ARP 항목이 지정된 VLAN 에 있습니다. • VLAN 의 VLANIF 인터페이스는 대상 IP 주소와 동일한 네트워크 세그먼트에 있어야 합니다.
아웃바운드 인터페이스	... ARP 패킷의 아웃바운드 인터페이스를 선택 하려면 클릭 합니다(예: GigabitEthernet 0 /0/1). **노트:** 인터페이스는 지정된 VLAN 의 구성원이어야 합니다.

3. 매개변수를 설정합니다.

NOTE

목적지 IP 주소와 아웃바운드 인터페이스의 IP 주소는 동일한 네트워크 세그먼트에 있어야 합니다.

4. Ok(확인)을 클릭합니다.

- 고정 ARP 항목을 수정합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > ARP > 정적 ARP 를** 선택하여 **정적 ARP** 페이지에 접근합니다.
2. 그림 2 와 같이 고정 ARP 항목 목록에서 대상 IP 주소를 클릭하여 해당 고정 ARP 항목 수정 페이지에 액세스합니다.

그림 2 고정 ARP 항목 수정

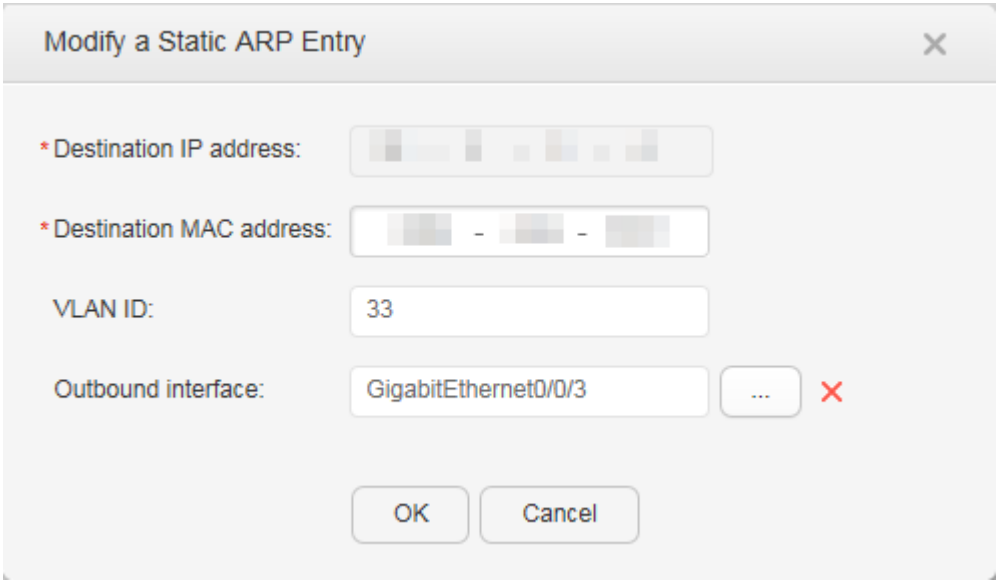


표 1 은 페이지의 매개변수를 설명합니다.

NOTE

대상 IP 주소는 수정할 수 없습니다.

3. 매개변수 구성을 수정합니다.
4. Ok(확인)을 클릭합니다.

- 고정 ARP 항목을 삭제합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > ARP > 정적 ARP 를** 선택하여 **정적 ARP** 페이지에 접근합니다.

2. 삭제할 기록을 선택하고 **삭제를** 클릭합니다. 시스템에서 레코드를 삭제할지 여부를 묻습니다.
3. Ok(확인)을 클릭합니다.

- 모든 고정 ARP 항목을 지웁니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > ARP > 정적 ARP 를** 선택하여 **정적 ARP** 페이지에 접근합니다.
2. **모든 고정 ARP 항목 지우기를** 클릭합니다. 시스템은 모든 고정 ARP 항목을 삭제할지 여부를 묻습니다.
3. Ok(확인)을 클릭합니다.

- 고정 ARP 항목을 업데이트합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > ARP > 정적 ARP 를** 선택하여 **정적 ARP** 페이지에 접근합니다.
2. **새로 고침을** 클릭합니다.

- 동적 ARP 항목을 삭제합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > ARP > 정적 ARP 를** 선택하여 **정적 ARP** 페이지에 접근합니다.
2. 삭제할 기록을 선택하고 **삭제를** 클릭합니다. 시스템에서 레코드를 삭제할지 여부를 묻습니다.
3. Ok(확인)을 클릭합니다.

- 모든 동적 ARP 항목을 지웁니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > ARP > 정적 ARP 를** 선택하여 **정적 ARP** 페이지에 접근합니다.
2. **모든 동적 ARP 항목 지우기를** 클릭합니다. 시스템은 모든 동적 ARP 항목을 삭제할지 여부를 묻습니다.
3. Ok(확인)을 클릭합니다.

- 동적 ARP 항목을 업데이트합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > ARP > 정적 ARP 를** 선택하여 **정적 ARP** 페이지에 접근합니다.
2. **새로 고침을** 클릭합니다.

4.5.3.6.2 ND

문맥

유효하지 않은 패킷을 필터링하기 위해 ND 항목을 생성하여 이러한 유효하지 않은 패킷의 대상 IPv6 주소를 존재하지 않는 MAC 주소에 바인딩할 수 있습니다.

절차

- 정적 ND 항목을 만듭니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > ND > 정적 ND** 를 선택하여 **정적 ND** 페이지에 접근합니다.

2. 그림 1 과 같이 **Create(만들기)를 클릭합니다.**

그림 1 정적 ND 항목 만들기

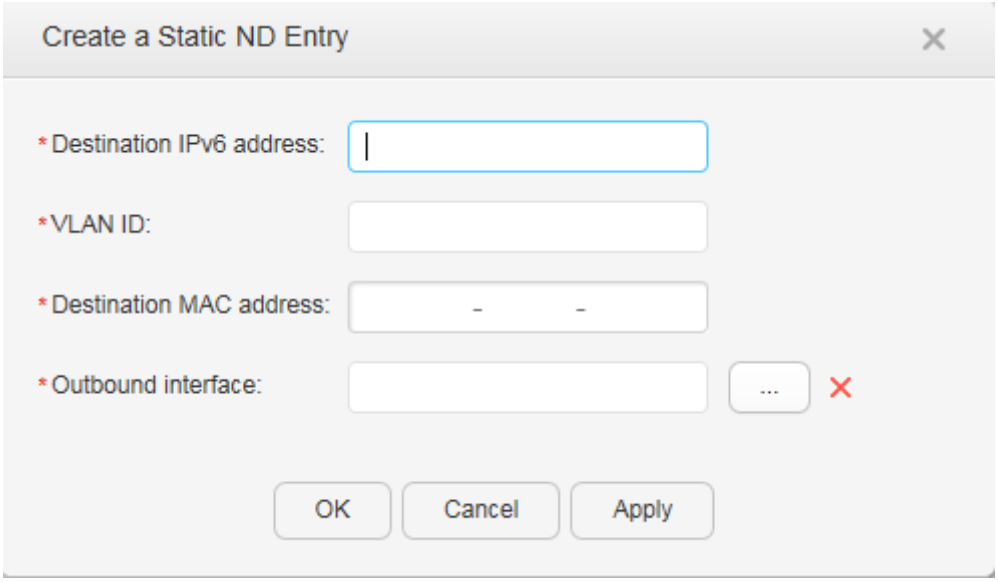


표 1 은 페이지의 매개변수를 설명합니다.

표 1 정적 ND 항목 생성

매개변수	설명
대상 IPv6 주소	고정 ND 항목에 대상 IPv6 주소를 지정합니다.
VLAN ID	인터페이스가 속한 외부 VLAN 의 ID 를 지정합니다.
대상 MAC 주소	고정 ND 항목에 대상 MAC 주소를 지정합니다.
아웃바운드 인터페이스	... ND 패킷의 아웃바운드 인터페이스를 선택 하려면 클릭합니다. **노트:** 인터페이스는 지정된 VLAN 의 구성원이어야 합니다.

3. 매개변수를 설정합니다.

4. Ok(확인)을 클릭합니다.

- 정적 ND 항목을 수정합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > ND > 정적 ND** 를 선택하여 **정적 ND** 페이지에 접근합니다.

2. 그림 2 와 같이 고정 ND 항목 목록에서 대상 IPv6 주소를 클릭하여 해당하는 고정 ND 항목 수정 페이지에 액세스합니다.

그림 2 정적 ND 항목 수정

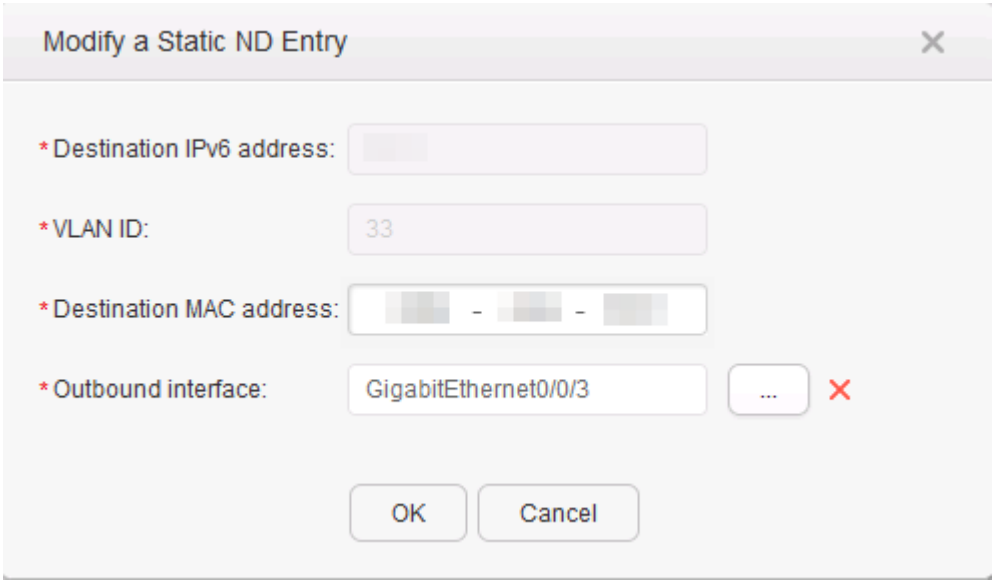


표 1 은 페이지의 매개변수를 설명합니다.

NOTE

대상 IPv6 주소 및 VLAN ID 는 수정할 수 없습니다.

3. 구성 매개변수를 수정합니다.
4. Ok(확인)을 클릭합니다.

- 정적 ND 항목을 삭제합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > ND > 정적 ND** 를 선택하여 **정적 ND** 페이지에 접근합니다.
2. 삭제할 기록을 선택하고 **삭제를** 클릭합니다. 시스템에서 레코드를 삭제할지 여부를 묻습니다.
3. Ok(확인)을 클릭합니다.

- 모든 정적 ND 항목을 지웁니다.

    1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > ND > 정적 ND** 를 선택하여 **정적 ND** 페이지에 접근합니다.
    2. **모든 정적 ND 항목 지우기를** 클릭합니다. 시스템은 모든 고정 ND 항목을 삭제할지 여부를 묻습니다.
    3. Ok(확인)을 클릭합니다.

- 정적 ND 항목을 업데이트합니다.

    1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > ND > 정적 ND** 를 선택하여 **정적 ND** 페이지에 접근합니다.
    2. **새로 고침을** 클릭합니다.

- 모든 동적 ND 항목을 지웁니다.

    1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > ND > 정적 ND** 를 선택하여 **정적 ND** 페이지에 접근합니다.
    2. **모든 동적 ND 항목 지우기를** 클릭합니다. 시스템은 모든 동적 ND 항목을 삭제할지 여부를 묻습니다.
    3. Ok(확인)을 클릭합니다.

- 동적 ND 항목을 업데이트합니다.

1. **Configuration(구성)** > **Advanced Services(고급 서비스)** > **IP 서비스** > **ND** > **정적 ND** 를 선택하여 **정적 ND** 페이지에 접근합니다.

2. **새로 고침을** 클릭합니다.

4.5.3.6.3 DNS

문맥

TCP/IP 는 IP 주소 외에 문자열을 사용하여 호스트를 식별하는 DNS(Domain Name System)를 제공합니다. DNS 는 계층적 명명 체계를 사용하여 네트워크 장치에의미 있는 이름을 지정합니다. 도메인 이름과 IP 주소 간의 매핑은 DNS 서버에서 설정됩니다. DNS 를 통해 사용자는 IP 주소 대신의미 있고 기억하기 쉬운 도메인 이름을 사용하여 장치를 식별할 수 있습니다.

절차

- 고정 DNS

1. 고정 DNS 항목을 만듭니다.

   a. **Configuration(구성)** > **Advanced Services(고급 서비스)** > **IP 서비스** > **DNS** > **정적 DNS** 를 선택하여 그림 1 과 같이 **정적 DNS** 페이지에 접근합니다.

그림 1 고정 DNS

b. 그림 2 와 같이 **Create(만들기)를 클릭합니다.**

그림 2 고정 DNS 항목 만들기

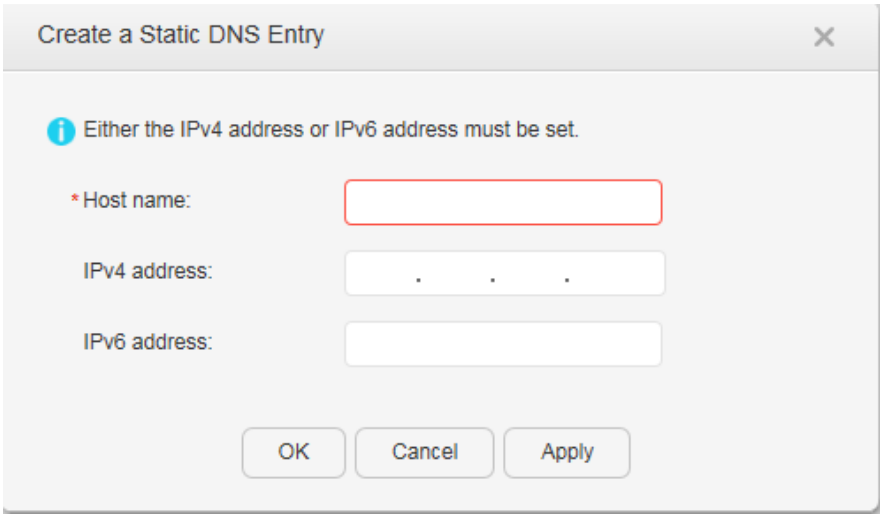


표 1 은 페이지의 매개변수를 설명합니다.

표 1 고정 DNS 항목 생성

매개변수	설명
호스트 이름	도메인 이름을 지정합니다.
IPv4 주소	도메인 이름을 매핑하는 IPv4 주소를 지정합니다.
IPv6 주소	도메인 이름을 매핑하는 IPv6 주소를 지정합니다.

c. 매개변수를 설정합니다.

d. Ok(확인)을 클릭합니다.

2. 고정 DNS 항목을 삭제합니다.

a. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > DNS > 정적 DNS** 를 선택하여 그림 1 과 같이 **정적 DNS** 페이지에 접근합니다.

b. 삭제할 기록을 기록을 선택하고 **삭제를** 클릭합니다. 시스템에서 레코드를 삭제할지 여부를 묻습니다.

c. Ok(확인)을 클릭합니다.

3. 고정 DNS 항목을 업데이트합니다.

a. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > DNS > 정적 DNS** 를 선택하여 그림 1 과 같이 **정적 DNS** 페이지에 접근합니다.

b. **새로 고침을** 클릭합니다.

- 동적 DNS

1. 동적 도메인 이름 확인 기능을 구성합니다.

a. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > DNS > 동적 DNS** 를 선택하여 그림 3 과 같이 **동적 DNS** 페이지에 접근합니다.

그림 3 동적 DNS

b. **동적 도메인 이름 확인 설정**합니다.

2. 동적 DNS 목록을 만듭니다.

a. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > DNS > 동적 DNS** 를 선택하여 그림 3 과 같이 **동적 DNS** 페이지에 접근합니다.

b. **동적 DNS 목록** 영역에서 **Create(만들기)를 클릭합니다. 동적 DNS 엔트리 작성** 페이지가 표시되고 도시 된 바와 같이, 도 4 .

그림 4 동적 DNS 목록 만들기

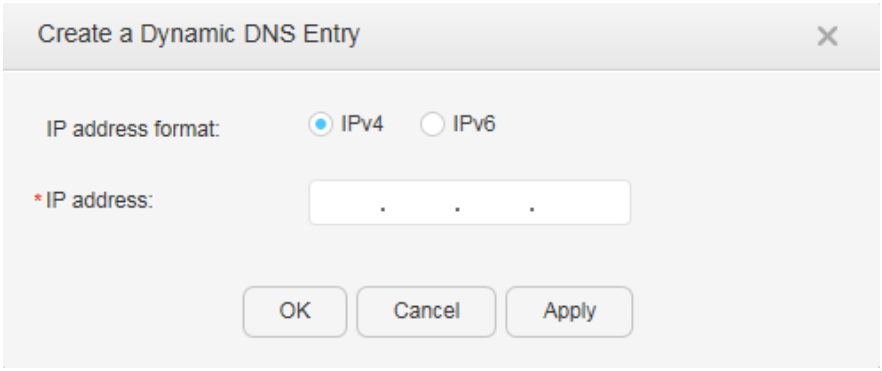


표 2 는 페이지의 매개변수를 설명합니다.

표 2 동적 DNS 목록 생성

매개변수	설명
IP 주소 형식	IP 주소 형식을 선택합니다. • IPv4 • IPv6
IP 주소	DNS 서버의 IP 주소를 지정합니다.
인터페이스 이름	이 매개변수는 **IP 주소 형식** 이 **IPv6** 으로 설정된 경우에만 유효 **합니다.** ... DNS 서버와의 통신을 위한 아웃바운드 인터페이스를 선택 하려면 클릭합니다. **노트:** 자세한 규칙을 보려면 마우스를 오른쪽으로 이동하십시오.

c. 매개변수를 설정합니다.

d. Ok(확인)을 클릭합니다.

3. 동적 DNS 항목을 삭제합니다.

a. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > DNS > 동적 DNS** 를 선택하여 그림 3 과 같이 **동적 DNS** 페이지에 접근합니다.

b. **동적 DNS 목록** 영역에서 삭제할 기록을 선택하고 **삭제를 클릭합니다**. 시스템에서 레코드를 삭제할지 여부를 묻습니다.

c. Ok(확인)을 클릭합니다.

4. 동적 DNS 항목을 업데이트합니다.

   a. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > DNS > 동적 DNS** 를 선택하여 그림 3 과 같이 **동적 DNS** 페이지에 접근합니다.

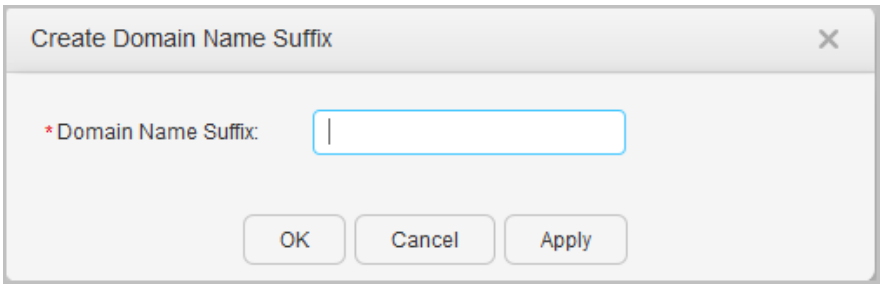
   b. **동적 DNS 목록** 영역에서 **새로 고침**을 클릭합니다.

5. 도메인 이름 접미사 목록을 만듭니다.

   a. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > DNS > 동적 DNS** 를 선택하여 그림 3 과 같이 **동적 DNS** 페이지에 접근합니다.

   b. **도메인 이름 접미사 목록** 영역에서 **Create(만들기)를 클릭합니다.** 그림 5 과 같이 **도메인 이름 접미어 생성** 페이지가 표시됩니다.

      그림 5 도메인 이름 접미사 생성

   c. 도메인 이름 접미사를 설정합니다.

   d. Ok(확인)을 클릭합니다.

6. 도메인 이름 접미사 항목을 삭제합니다.

    a. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > DNS > 동적 DNS** 를 선택하여 그림 3 과 같이 **동적 DNS** 페이지에 접근합니다.

    b. **도메인 이름 접미사 목록** 영역에서 삭제할 기록을 선택하고 **삭제**를 클릭합니다. 시스템에서 레코드를 삭제할지 여부를 묻습니다.

    c. Ok(확인)을 클릭합니다.

7. 도메인 이름 접미사 항목을 지웁니다.

    a. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > DNS > 동적 DNS** 를 선택하여 그림 3 과 같이 **동적 DNS** 페이지에 접근합니다.

    b. **도메인 이름 접미사 목록** 영역에서 삭제할 기록을 선택하고 **삭제**를 클릭합니다. 시스템에서 레코드를 삭제할지 여부를 묻습니다.

    c. Ok(확인)을 클릭합니다.

8. 도메인 이름 접미사 항목을 업데이트합니다.

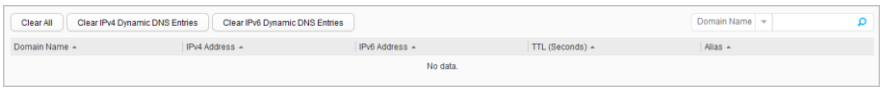
a. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > DNS > 동적 DNS** 를 선택하여 그림 3 과 같이 **동적 DNS** 페이지에 접근합니다.

b. **도메인 이름 접미사 목록** 영역에서 **새로 고침**을 클릭합니다.

- 동적 DNS 항목

1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > DNS > 동적 DNS** 를 선택하여 그림 6 과 같이 **동적 DNS** 페이지에 접근합니다.

그림 6 동적 DNS 항목



2. **모두 지우기, IPv4 동적 DNS 항목 지우기** 또는 **IPv6 동적 DNS 항목 지우기를** 클릭합니다. 시스템에서 기록을 지울지 여부를 묻습니다.

3. Ok(확인)을 클릭합니다.

4.5.3.6.4 루프백 인터페이스

문맥

TCP/IP 프로토콜 제품군에 따르면 네트워크 세그먼트 127.0.0.0 의 IP 주소는 루프백 주소입니다. 이러한 주소로 구성된 인터페이스는 루프백 인터페이스입니다. 시작하는 동안 시스템은 루프백 주소 127.0.0.1 을 사용하여 로컬 스위치로 전송된 모든 패킷을 수신하는 인터페이스를 자동으로 생성합니다.

절차

- 루프백 인터페이스를 만듭니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > 루프백 인터페이스**를 선택하여 **루프백 인터페이스** 페이지에 접근합니다.
2. 그림 1 과 같이 **Create(만들기)를 클릭합니다.**

그림 1 루프백 인터페이스 만들기

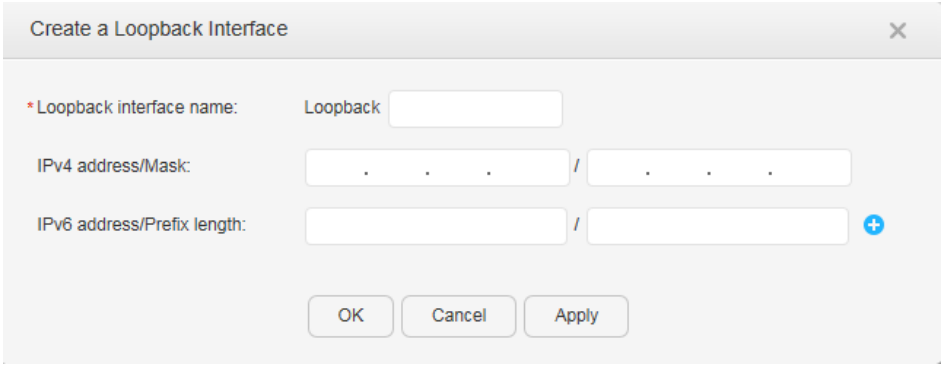


표 1 은 페이지의 매개변수를 설명합니다.

표 1 루프백 인터페이스 생성

매개변수	설명
루프백 인터페이스 이름	루프백 인터페이스의 번호를 입력합니다. 이 매개변수는 필수입니다.

표 1 루프백 인터페이스 생성

매개변수	설명
IPv4 주소/마스크	루프백 인터페이스의 IPv4 주소와 서브넷 마스크를 입력합니다.
IPv6 주소/접두사 길이	IPv6 주소(예: FC00:0:130F:0:0:9C0:876A:130B) 및 접두사 길이(1~128 범위)를 입력합니다. 를 클릭 하여 IPv6 주소를 추가하거나를 클릭 하여 IPv6 주소를 삭제할 수 있습니다.

3. 매개변수를 설정합니다.

4. Ok(확인)을 클릭합니다.

- 루프백 인터페이스를 수정합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > 루프백 인터페이스**를 선택하여 **루프백 인터페이스** 페이지에 접근합니다.

2. 루프백 인터페이스 목록에서 루프백 인터페이스 이름을 클릭하면 그림 2 와 같이 해당 루프백 인터페이스 수정 페이지에 액세스할 수 있습니다.

그림 2 루프백 인터페이스 수정

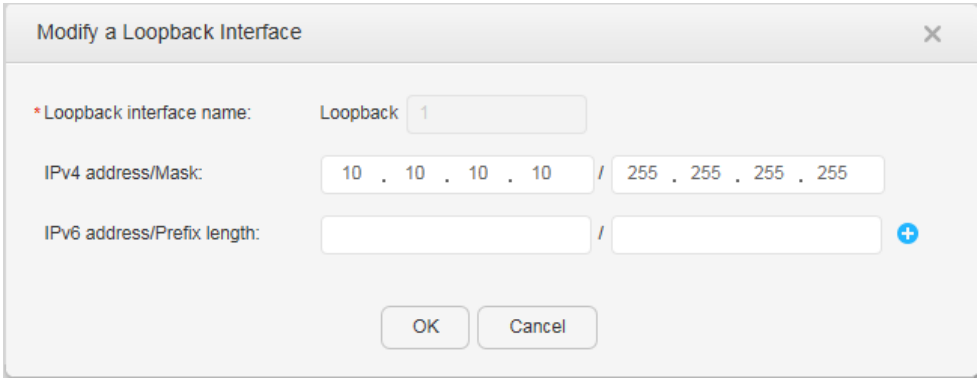


표 1 은 페이지의 매개변수를 설명합니다.

> **NOTE**
>
> 루프백 인터페이스 이름은 수정할 수 없습니다.

3. 구성 매개변수를 수정하십시오.
4. Ok(확인)을 클릭합니다.

- 루프백 인터페이스를 삭제합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > 루프백 인터페이스**를 선택하여 **루프백 인터페이스** 페이지에 접근합니다.
2. 삭제할 기록을 선택하고 **삭제**를 클릭합니다. 시스템에서 레코드를 삭제할지 여부를 묻습니다.
3. Ok(확인)을 클릭합니다.

- 루프백 인터페이스를 업데이트합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > IP 서비스 > 루프백 인터페이스**를 선택하여 **루프백 인터페이스** 페이지에 접근합니다.
2. **새로 고침**을 클릭합니다.

4.5.3.7 IP 라우팅

4.5.3.7.1 OSPF

절차

- OSPF 를 생성합니다.

1. 탐색 트리에서 **Configuration(구성) > Advanced Services(고급 서비스) > IP 경로 > OSPF** 를 선택하여 **OSPF** 페이지를 엽니다. 그림 1 과 같이 **Create(만들기)**를 클릭합니다.

그림 1 OSPF 구성 페이지

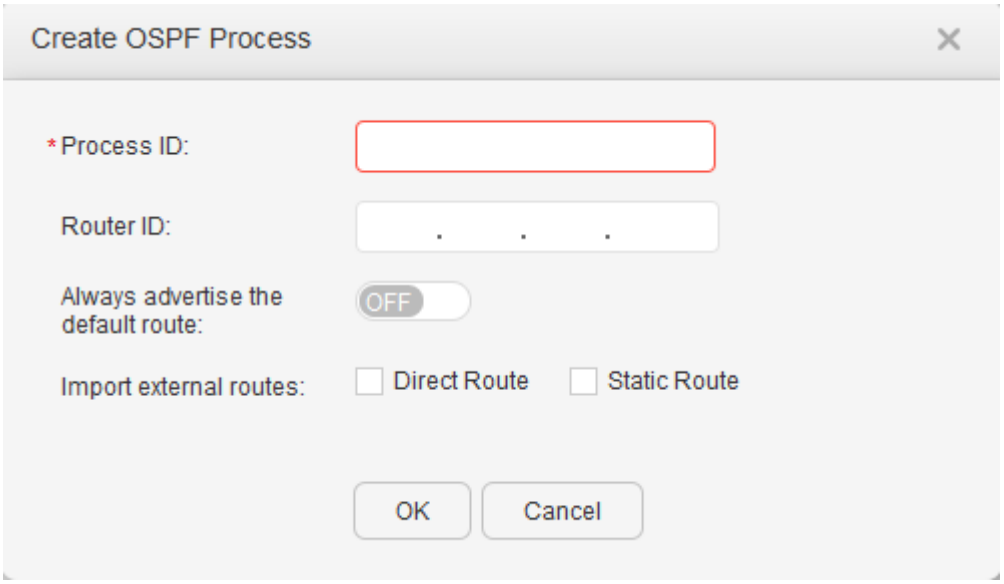


표 1 은 페이지의 매개변수를 설명합니다.

표 1 OSPF 매개변수

매개변수	설명
프로세스 ID	OSPF 프로세스 ID 를 지정합니다.

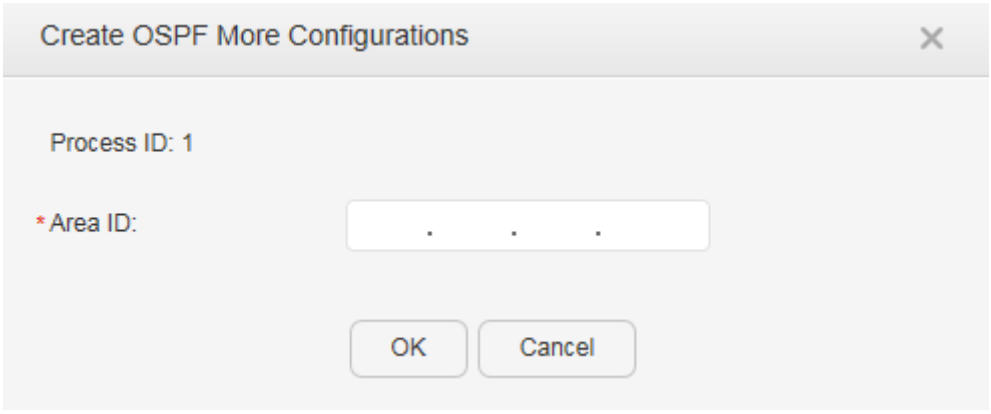
표 1 OSPF 매개변수

매개변수	설명
라우터 ID	라우터 ID 를 지정합니다.
항상 기본 경로를 알립니다.	공통 OSPF 영역에 기본 경로를 광고하는 기능이 다음과 같은지 여부를 나타냅니다. • 에 • 끄다
외부 경로 가져오기	다른 라우팅 프로토콜에서 학습한 경로를 가져옵니다. • 직항로 • 정적 경로

2. 매개변수를 설정합니다. **Ok(확인)을 클릭**하여 구성을 완료합니다.

3. **OSPF 목록** 데이터의 오른쪽에 있는 **추가 구성**을 클릭하여 구성 페이지를 엽니다. 그림 2 와 같이 **Create(만들기)**를 클릭합니다.

   그림 2 추가 구성



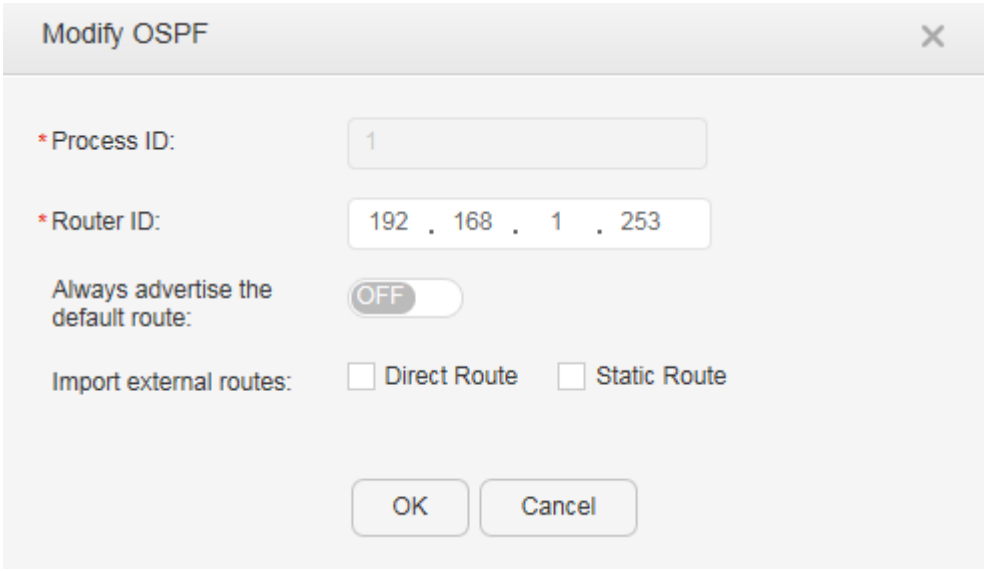
4. **Area ID** 의 텍스트 상자에, 영역 ID 를 점으로 구분된 십진수 표기법으로 입력합니다. OK 를 클릭합니다.

- OSPF 를 수정합니다.

1. 탐색 트리에서 **Configuration(구성) > Advanced Services(고급 서비스) > IP 경로 > OSPF** 를 선택하여 **OSPF** 페이지를 엽니다.

2. **OSPF 목록**에서 해당 데이터의 오른쪽에 있는 **수정**을 클릭하여 그림 3 과 같이 **OSPF 수정** 페이지를 엽니다.

   그림 3 OSPF 수정



3. 표 1 은 페이지의 매개변수를 설명합니다. 필요에 따라 매개변수를 수정한 다음 **Ok(확인)을 클릭**합니다.

- OSPF 를 삭제합니다.

1. 탐색 트리에서 **Configuration(구성) > Advanced Services(고급 서비스) > IP 경로 > OSPF** 를 선택하여 **OSPF** 페이지를 엽니다.

2. 데이터 항목을 선택하고 **삭제를** 클릭합니다. 표시되는 대화 상자에서 **Ok(확인)을 클릭**합니다.

- OSPF 를 업데이트합니다.

1. 탐색 트리에서 **Configuration(구성) > Advanced Services(고급 서비스) > IP 경로 > OSPF** 를 선택하여 **OSPF** 페이지를 엽니다.

2. **새로 고침**을 클릭하여 OSPF 목록을 업데이트합니다.

4.5.3.7.2 OSPFv3

절차

- OSPFv3 을 만듭니다.

1. 탐색 트리에서 **Configuration(구성) > Advanced Services(고급 서비스) > IP 경로 > OSPFv3** 을 선택하여 **OSPFv3** 페이지를 엽니다. 그림 1 과 같이 **Create(만들기)**를 클릭합니다.

그림 1 OSPFv3 구성 페이지

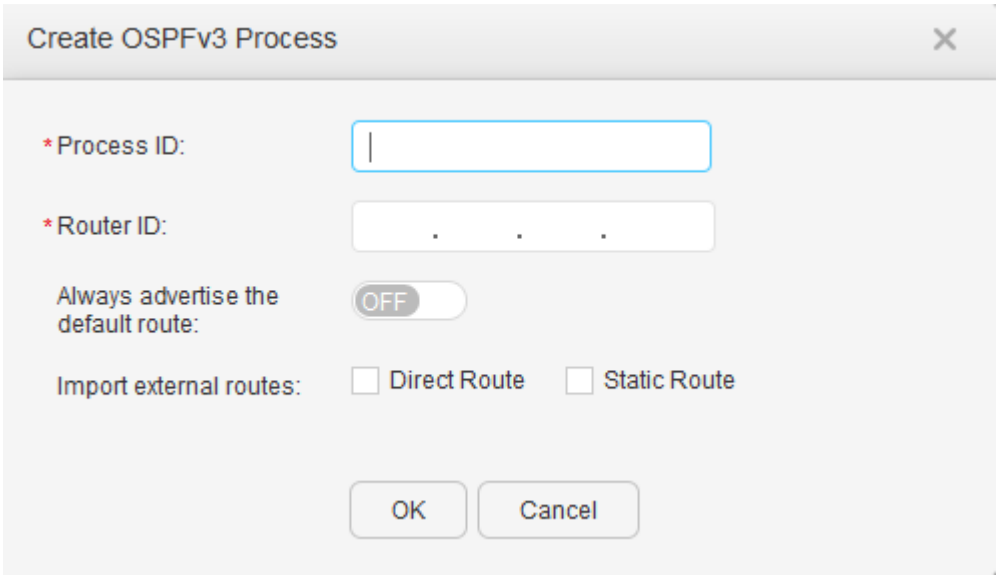


표 1 은 페이지의 매개변수를 설명합니다.

표 1 OSPFv3 매개변수

매개변수	설명
프로세스 ID	OSPFv3 프로세스 ID 를 지정합니다.
라우터 ID	라우터 ID 를 지정합니다.
항상 기본 경로를 알립니다.	공통 OSPF 영역에 기본 경로를 광고하는 기능이 다음과 같은지 여부를 나타냅니다. • 에 • 끄다
외부 경로 가져오기	다른 라우팅 프로토콜에서 학습한 경로를 가져옵니다. • 직항로 • 정적 경로

2. 매개변수를 설정하고 **Ok(확인)을 클릭합니다.**

3. **OSPFv3 목록** 데이터의 오른쪽에 있는 **추가 구성**을 클릭하여 구성 페이지를 엽니다. 그림 2 와 같이 **Create(만들기)**를 클릭합니다.

그림 2 추가 구성

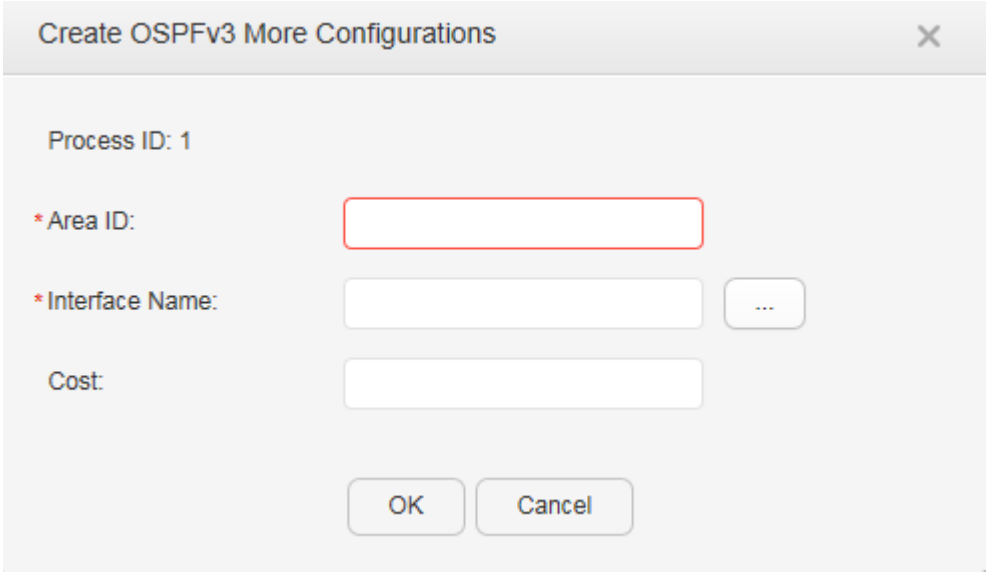


표 2 는 페이지의 매개변수를 설명합니다.

표 2 OSPFv3 매개변수

매개변수	설명
프로세스 ID	OSPFv3 프로세스 ID 를 지정합니다.
지역 ID	영역 ID 를 지정합니다.
인터페이스 이름	OSPFv3 인터페이스를 나타냅니다. 클릭 ... 하여 OSPFv3 인터페이스를 선택할 수 있습니다.
비용	인터페이스에 대한 링크 비용을 설정합니다.

4. 매개변수를 설정하고 **Ok(확인)을 클릭합니다.**

- OSPFv3 을 수정합니다.

1. 탐색 트리에서 **Configuration(구성) > Advanced Services(고급 서비스) > IP 경로 > OSPFv3** 을 선택하여 **OSPFv3** 페이지를 엽니다.

2. **OSPFv3 목록**에서 해당 데이터의 오른쪽에 있는 **수정**을 클릭하여 그림 3 과 같이 **OSPFv3 수정** 페이지를 엽니다.

그림 3 OSPFv3 수정

3. 표 1 은 페이지의 매개변수를 설명합니다. 필요에 따라 매개변수를 수정한 다음 **Ok(확인)을 클릭**합니다.

- OSPFv3 을 삭제합니다.

1. 탐색 트리에서 **Configuration(구성) > Advanced Services(고급 서비스) > IP 경로 > OSPFv3** 을 선택하여 **OSPFv3** 페이지를 엽니다.
2. 데이터 항목을 선택하고 **삭제를** 클릭합니다. 표시되는 대화 상자에서 **Ok(확인)을 클릭합니다.**

- OSPFv3 을 업데이트합니다.

1. 탐색 트리에서 **Configuration(구성) > Advanced Services(고급 서비스) > IP 경로 > OSPFv3** 을 선택하여 **OSPFv3** 페이지를 엽니다.
2. **새로 고침**을 클릭하여 OSPFv3 목록을 업데이트합니다.

4.5.3.8 VRRP

4.5.3.8.1 IPv4

절차

- VRRP 항목을 만듭니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > VRRP** >의 **IPv4** 를 선택하여 **IPv4** 페이지를 엽니다. 그림 1 과 같이 **Create(만들기)**를 클릭합니다.

그림 1 VRRP 항목 만들기

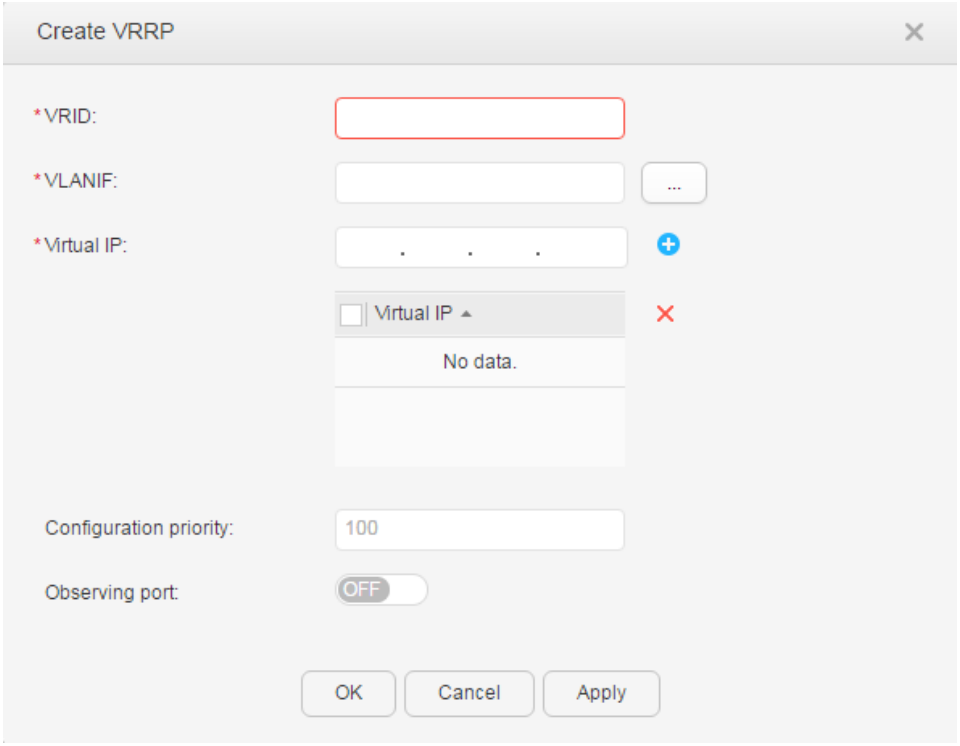


표 1 은 매개변수를 설명합니다.

표 1 VRRP 매개변수

매개변수	설명
VRID	VRRP 그룹의 VRID 를 나타냅니다.
VLANIF	VRRP 그룹이 생성되는 VLANIF 인터페이스를 지정하려면 ... 를 클릭합니다.
가상 IP	VRRP 그룹의 가상 IP 주소를 나타냅니다. 가상 IP 주소를 추가하려면 ⊕ 를 클릭합니다. **노트:**

표 1 VRRP 매개변수

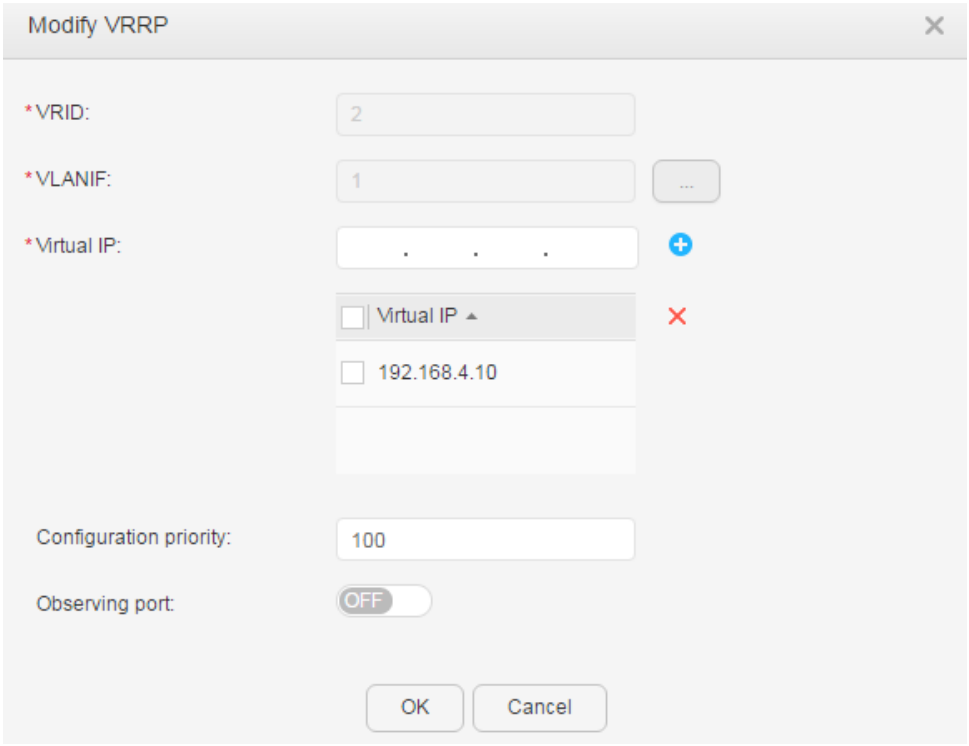
매개변수	설명
	가상 IP 주소는 VLANIF 인터페이스의 IP 주소와 동일한 네트워크 세그먼트에 있어야 합니다.
구성 우선 순위	VRRP 그룹에 있는 장치의 우선 순위를 나타냅니다. 값이 클수록 우선 순위가 높음을 나타냅니다.
관찰 포트	VRRP 와 인터페이스 상태 간의 연결을 활성화할지 여부를 나타냅니다. ON: VRRP 와 인터페이스 상태 간의 연결이 활성화됩니다. OFF: VRRP 와 인터페이스 상태 간의 연결이 비활성화됩니다.
인터페이스 이름	연결된 인터페이스를 지정하려면 ... 를 클릭합니다. **노트:** 이 파라미터는 **Observing 포트** 값 이 **ON 일** 때만 사용 가능합니다.
우선 사항	연결된 인터페이스의 우선 순위가 증가하거나 감소하는 값을 나타냅니다. 값을 지정하려면 ⊕ 를 클릭합니다. **노트:** 이 파라미터는 **Observing 포트** 값 이 **ON 일** 때만 사용 가능합니다.

2. 매개변수를 설정하고 **Ok(확인)을 클릭합니다.**

- VRRP 항목을 수정합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > VRRP** >의 **IPv4** 를 선택하여 **IPv4** 페이지를 엽니다.
2. 그림 2 와 같이 데이터 항목 옆에 있는 **수정을** 클릭하여 **VRRP 수정** 페이지에 액세스합니다.

그림 2 VRRP 수정 페이지



3. 매개변수를 수정하고 **Ok(확인)을 클릭**합니다.

- VRRP 항목을 삭제합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > VRRP** >의 **IPv4** 를 선택하여 **IPv4** 페이지를 엽니다.

2. 삭제할 데이터를 선택하고 **삭제**를 클릭합니다. 표시되는 대화 상자에서 **Ok(확인)을 클릭**합니다.

- VRRP 정보를 새로 고칩니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > VRRP** >의 **IPv4** 를 선택하여 **IPv4** 페이지를 엽니다.

2. **새로 고침**을 클릭하여 VRRP 목록을 새로 고 **칩니다.**

4.5.3.8.2 IPv6

절차

- VRRP6 항목을 만듭니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > VRRP** >의 **IPv6** 를 선택하여 **IPv6** 페이지를 엽니다. 그림 1 과 같이 **Create(만들기)**를 클릭합니다.

그림 1 VRRP6 항목 만들기

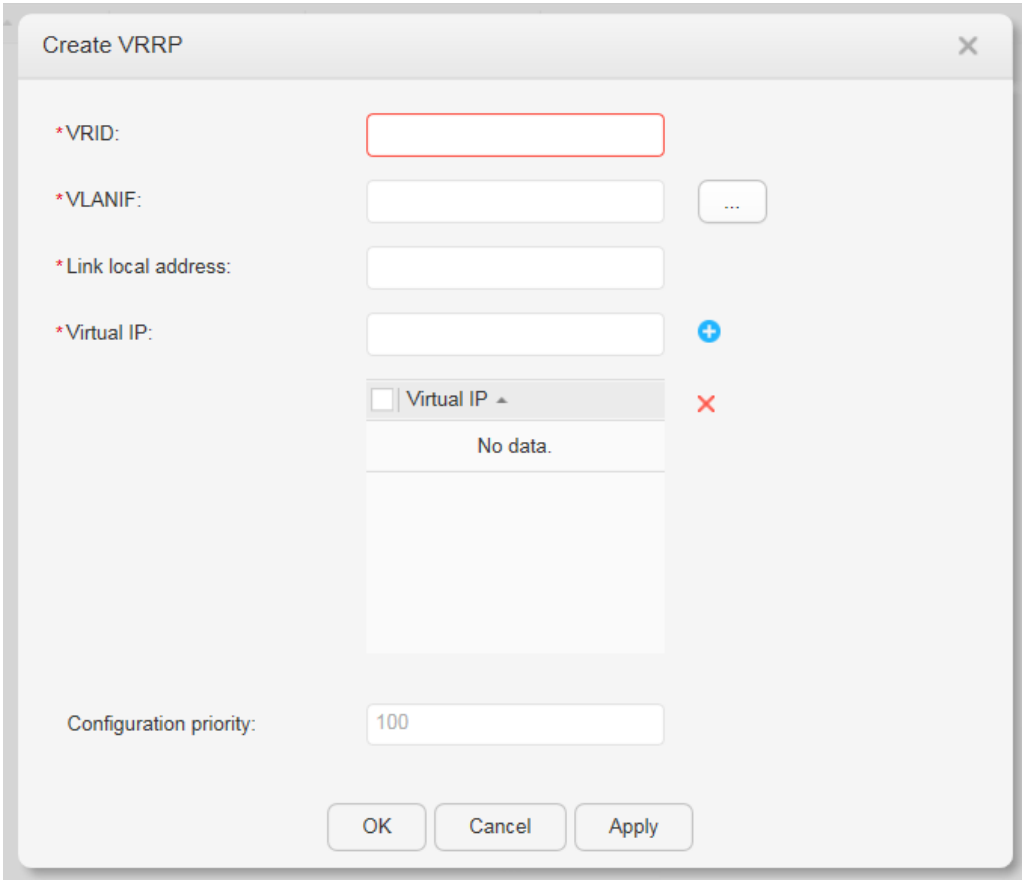


표 1 은 매개변수를 설명합니다.

표 1 VRRP6 매개변수

매개변수	설명
VRID	VRRP6 그룹의 VRID 를 나타냅니다.
VLANIF	VRRP6 그룹이 생성되는 VLANIF 인터페이스를 지정하려면 ... 를 클릭합니다.
로컬 주소 연결	링크 로컬 주소를 나타냅니다.
가상 IP	VRRP6 그룹의 가상 IP 주소를 나타냅니다. 가상 IP 주소를 추가하려면 ⊕ 를 클릭합니다. **노트:** 가상 IP 주소는 VLANIF 인터페이스의 IP 주소와 동일한 네트워크 세그먼트에 있어야 합니다.

표 1 VRRP6 매개변수

매개변수	설명
	VRRP6 그룹의 첫 번째 가상 IPv6 주소는 링크 로컬 주소여야 합니다.
구성 우선 순위	VRRP6 그룹에서 장치의 우선 순위를 나타냅니다. 값이 클수록 우선 순위가 높음을 나타냅니다.

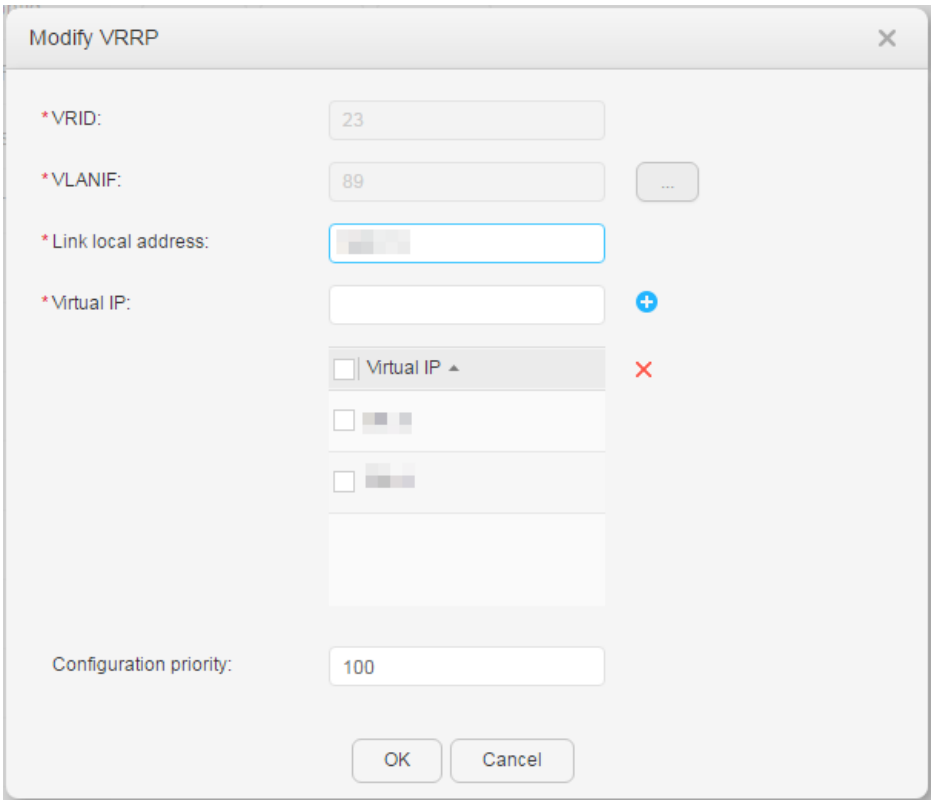
2. 매개변수를 설정하고 **Ok(확인)을 클릭합니다.**

- VRRP6 항목을 수정합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > VRRP** >의 **IPv6** 를 선택하여 **IPv6** 페이지를 엽니다.

2. 그림 2 와 같이 데이터 항목 옆에 있는 **수정을** 클릭하여 **VRRP6 수정** 페이지에 액세스합니다.

그림 2 VRRP6 수정 페이지



3. 매개변수를 수정하고 **Ok(확인)을 클릭합니다.**

- VRRP6 항목을 삭제합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > VRRP** >의 **IPv6** 를 선택하여 **IPv6** 페이지를 엽니다.

2. 삭제할 데이터를 선택하고 **삭제**를 클릭합니다. 표시되는 대화 상자에서 **Ok(확인)을 클릭**합니다.

- VRRP6 정보를 새로 고칩니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > VRRP** >의 **IPv6** 를 선택하여 **IPv6** 페이지를 엽니다.

2. **새로 고침**을 클릭하여 VRRP6 목록을 새로 고 **칩니다.**

4.5.3.9 LBDT

문맥

네트워크에서 루프가 발생하면 브로드캐스트, 멀티캐스트 및 알 수 없는 유니캐스트 패킷이 네트워크에서 반복적으로 전송됩니다. 이는 네트워크 리소스를 낭비하거나 전체 네트워크에서 서비스 중단을 유발합니다. 장치가 계층 2 네트워크의 루프를 적시에 감지하고 네트워크가 루프에의해 심각하게 영향을 받는 것을 방지하려면 루프백 감지를 구성하십시오. 루프백 감지를 통해 장치는 루프백 감지 패킷을 주기적으로 보내 루프를 감지할 수 있습니다. 인터페이스에서 루프가 감지되면 장치는 루프를 제거하기 위해 인터페이스를 종료하거나 차단합니다. 장치가 인터페이스의 루프가 제거되었음을 감지하면 인터페이스를 복원할 수 있습니다.

절차

1. 그림 1 과 같이 **Configuration(구성) > Advanced Services(고급 서비스) > LBDT** 를 선택하여 **LBDT** 페이지 에 액세스합니다.

그림 1 루프백 감지 구성 페이지

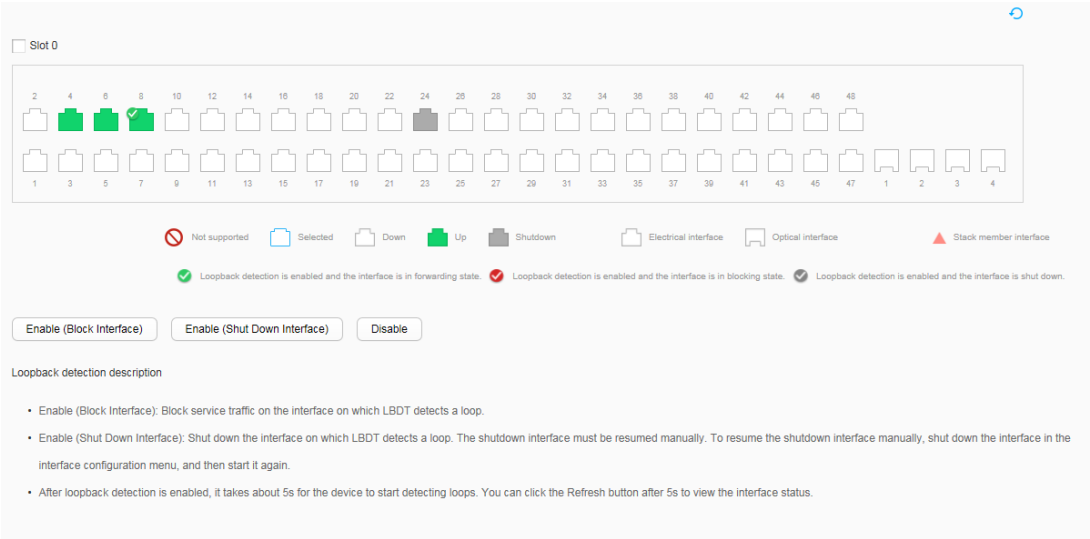


표 1 은 루프백 감지 구성 페이지의 매개변수를 설명합니다.

표 1 루프백 감지 구성 페이지의 매개변수

매개변수	설명
활성화(블록 인터페이스)	인터페이스에서 루프백 감지를 활성화하고 작업을 **block 으로** 설정합니다. 루프가 감지되면 장치는 인터페이스를 차단하고 BPDU 만 전달합니다.
활성화(종료 인터페이스)	인터페이스에서 루프백 감지를 활성화하고 작업을 **shutdown 으로** 설정합니다. 루프가 감지되면 장치가 인터페이스를 종료합니다.
장애를 입히다	인터페이스에서 루프백 감지를 비활성화합니다.

2. 구성할 인터페이스를 선택합니다.

다음 작업 중 하나를 수행합니다.

- 인터페이스 아이콘을 클릭하여 하나 이상의 인터페이스를 선택합니다.
- 마우스를 끌어 배치에서 연속 인터페이스를 선택합니다.
- 장치 패널 및 모든 인터페이스를 선택 합니다.

3. **Enable(인터페이스 차단)** 또는 **Enable(인터페이스 종료)을** 클릭하여 인터페이스에서 루프백 감지를 활성화하고 루프가 감지될 때 수행할 작업을 설정합니다.

   기본적으로 루프백 감지는 인터페이스에서 비활성화되어 있습니다.

   NOTE

   경우 **사용 (아래 인터페이스를 종료)** 루프가 감지되면 선택, 인터페이스는 종료됩니다. 종료 인터페이스는 **Interface Settings** > **Enable/Disable Interface** 에서 다시 시작할 수 있습니다. 자세한 내용은 인터페이스 활성화/비활성화를 참조하십시오.

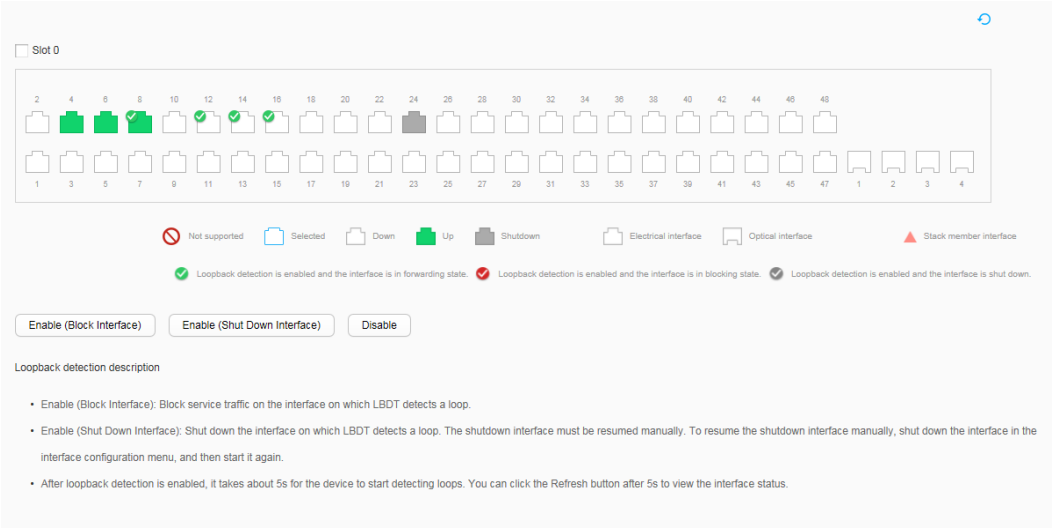
4. 구성을 확인하십시오.

   루프백 감지 상태는 그림 2 와 같이 루프백 감지를 활성화해야 하는 모든 인터페이스에 표시되며 구성이 성공한 것입니다. 그렇지 않으면 구성이 실패합니다.

   NOTE

   라인 루프백 감지가 활성화된 후 시스템은 약 5 초 후에 루프를 감지합니다. 5 초 후 인터페이스 상태를 보려면 클릭하십시오.

그림 2 루프백 감지 구성 결과



4.5.3.10 STP

4.5.3.10.1 STP 요약

절차

- STP 를 전역적으로 활성화합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > STP > STP 요약**을 클릭하여 **STP 요약** 페이지에 액세스합니다.

2. **글로벌 STP 상태**를 **ON** 으로 설정하여 STP 에게 전 세계적으로 활성화합니다.

> **NOTE**
>
> **STP 전역 설정** 및 **인터페이스 상태** 매개 변수는 STP 가 전 세계적으로 활성화된 경우에만 사용할 수 있습니다.

- 글로벌 STP 기능을 구성합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > STP > STP 요약**을 선택하여 그림 1 과 같이 **STP 요약** 페이지를 엽니다.

그림 1 STP 구성

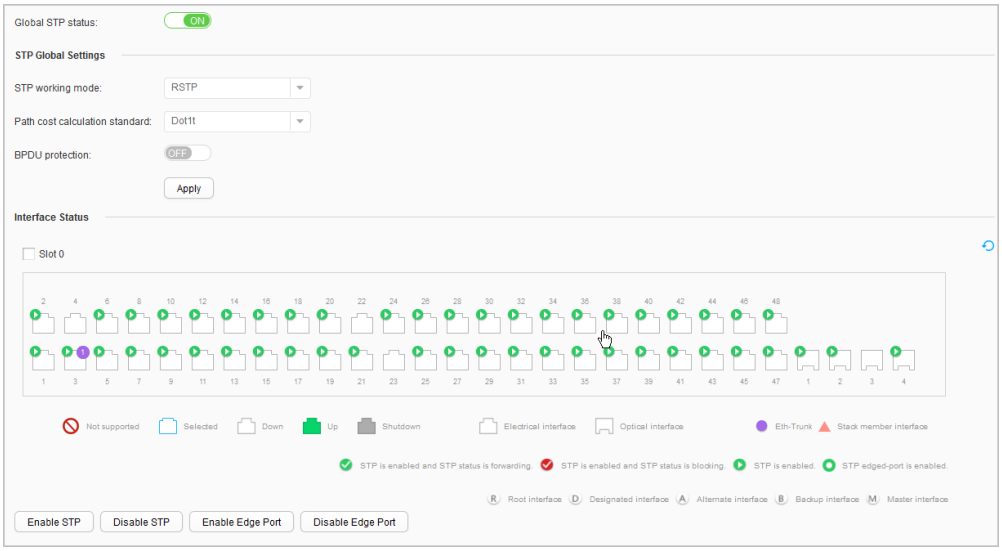


표 1 은 **STP 요약** 페이지의 매개변수를 설명합니다.

표 1 STP 요약 페이지의 매개변수 설명

매개변수	설명
STP 작동 모드	STP 의 작동 모드: MSTP: 스위치가 MSTP BPDU 를 보냅니다. RSTP: 스위치가 RSTP BPDU 를 보냅니다. STP: 스위치가 STP BPDU 를 보냅니다. VBST: 스위치가 VBST BPDU 를 보냅니다. **노트:** SVF 에서 값은 기본적으로 RSTP 이며 변경할 수 없습니다.
경로 비용 계산 기준	경로 비용 계산 방법: Dot1d-1998: IEEE 802.1d-1998 표준 방법을 사용하여 경로 비용을 계산합니다. Dot1t: IEEE 802.1t 표준 방법을 사용하여 경로 비용을 계산합니다.

표 1 STP 요약 페이지의 매개변수 설명

매개변수	설명
	레거시: Soltech 의 방법을 사용하여 경로 비용을 계산합니다.
BPDU 보호	BPDU 보호 활성화 여부: ON: BPDU 보호가 활성화됩니다. 꺼짐: BPDU 보호가 비활성화됩니다.

2. 매개변수를 설정하고 **Apply(적용)을 클릭**합니다.

- 포트 상태를 구성합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > STP > STP 요약**을 선택하여 그림 1 과 같이 **STP 요약** 페이지를 엽니다.
2. **인스턴스** 텍스트 상자에 인스턴스 ID 를 입력합니다.
3. 구성할 포트를 선택합니다.

   다음 작업 중 하나를 수행합니다.

   - 포트 아이콘을 클릭하여 하나 이상의 포트를 선택하십시오.
   - 마우스를 끌어 배치에서 연속 포트를 선택합니다.
   - 모든 포트를 선택하려면 장치 패널을 선택하십시오.
4. **STP 활성화**, **비활성화 STP 를**, **에지 포트 사용** 또는 **사용 안 함 에지 포트**를 클릭하여 선택한 포트를 설정합니다.

4.5.3.10.2 MST 지역 구성

문맥

NOTE

스위치가 SVF(Super Virtual Fabric) 모드에서 작동하는 경우 이 기능이 지원되지 않습니다.

이 기능은 **STP 작업 모드** 가 **MSTP** 로 설정된 경우에만 지원됩니다.

절차

- MST 지역을 구성합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > STP > MST 영역 구성**을 선택하여 그림 1 과 같이 **MST 영역 구성** 페이지를 엽니다.

그림 1 MST 지역 구성 페이지

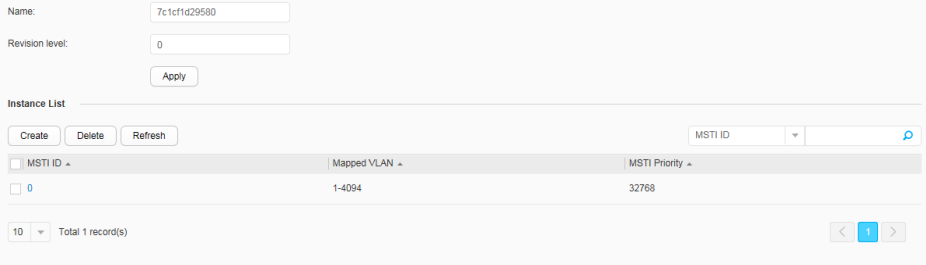


표 1 은 **MST 지역 구성** 페이지의 매개변수를 설명합니다.

표 1 MSTP 지역 구성 페이지의 매개변수 설명

매개변수	설명
이름	MST 지역의 이름을 입력합니다.

표 1 MSTP 지역 구성 페이지의 매개변수 설명

매개변수	설명
개정 수준	MSTP 개정 수준을 입력합니다. MST 지역 이름, VLAN 매핑 테이블 및 MSTP 개정 수준은 스위치가 속한 MST 지역을 식별합니다.

2. 매개변수를 설정하고 **Apply(적용)을 클릭**합니다.

- MSTI 목록을 만듭니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > STP > MST 영역 구성**을 선택하여 그림 1 과 같이 **MST 영역 구성** 페이지를 엽니다.

2. 그림 2 와 같이 **Create** 를 클릭하여 **Create MSTI** 페이지에 액세스합니다.

그림 2 MSTI 생성 페이지

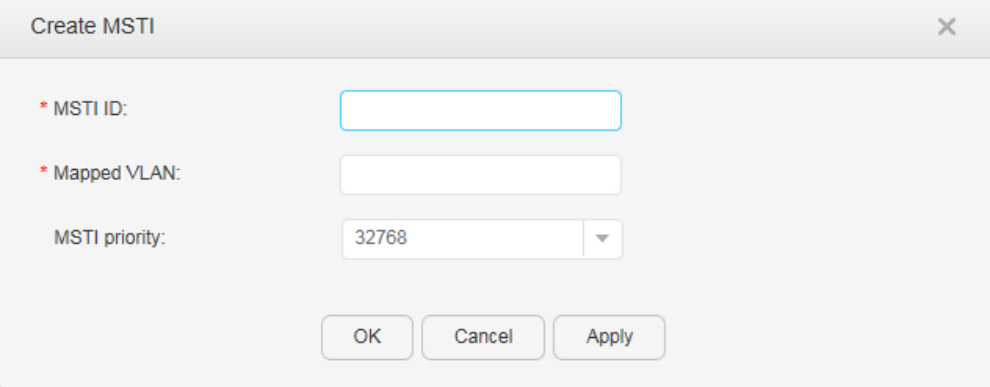


표 2 는 **MSTI 생성** 페이지의 매개변수에 대해 설명합니다.

표 2 Create MSTI 페이지의 매개변수 설명

매개변수	설명
MSTI ID	MSTI 의 ID 를 입력합니다.
매핑된 VLAN	지정된 MSTI 에 매핑되는 VLAN ID 범위를 입력합니다.

표 2 Create MSTI 페이지의 매개변수 설명

매개변수	설명
MSTI 우선 순위	지정된 MSTI 에서 장치의 우선 순위를 선택합니다.

3. 매개변수를 설정하고 **Ok(확인)을 클릭합니다.**

- MSTI 를 삭제합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > STP > MST 영역 구성**을 선택하여 그림 1 과 같이 **MST 영역 구성** 페이지를 엽니다.

2. 삭제하는 MSTI 를 선택하고 **삭제**를 클릭합니다. 표시되는 대화 상자에서 **Ok(확인)을 클릭**합니다.

- MSTI 목록을 새로 고칩니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > STP > MST 영역 구성**을 선택하여 그림 1 과 같이 **MST 영역 구성** 페이지를 엽니다.

2. **새로 고침**을 클릭하여 MSTI 목록을 새로 고칩니다.

4.5.3.10.3 VBST 구성

문맥

NOTE

스위치가 SVF(Super Virtual Fabric) 모드에서 작동하는 경우 이 기능이 지원되지 않습니다.

이 기능은 **STP 작업 모드** 가 **VBST** 로 설정된 경우에만 지원됩니다.

절차

- VLAN 에서 VBST(VLAN 기반 스패닝 트리)를 활성화합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > STP > VBST 구성**을 선택하여 **VBST 구성** 페이지를 엽니다.

2. 그림 1 과 같이 **Enable** 을 클릭하여 **Enable VBST in VLANs** 페이지를 표시합니다.

그림 1 VLAN 에서 VBST 활성화

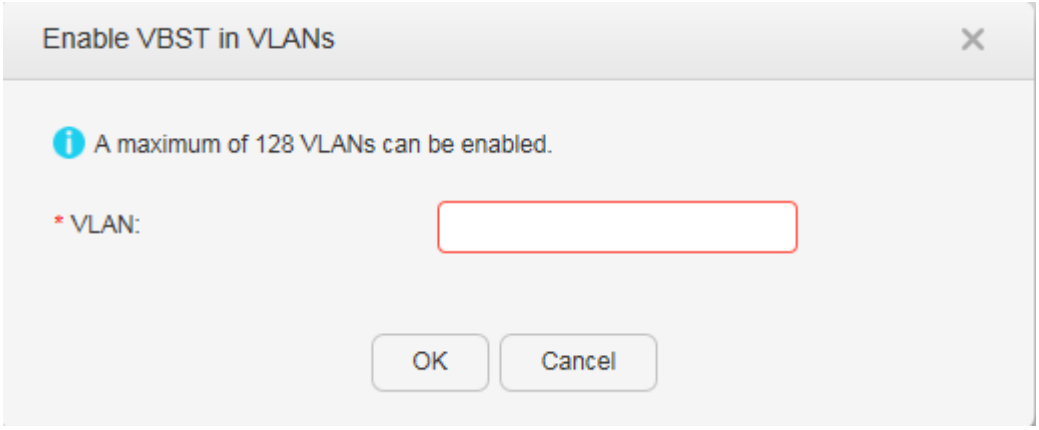


표 1 은 페이지의 매개변수를 설명합니다.

표 1 VLAN 에서 VBST 를 활성화하기 위한 매개변수

매개변수	설명
VLAN	VBST 를 활성화해야 하는 VLAN 의 ID 를 나타냅니다.

3. 매개변수를 설정하고 **Ok(확인)을 클릭합니다.**

- VLAN 우선 순위를 변경합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > STP > VBST 구성**을 선택하여 **VBST 구성** 페이지를 엽니다.

2. VBST 목록에서 우선 순위를 변경해야 하는 VLAN 의 ID 를 클릭합니다. 그림 2 와 같이 **수정 VLAN 우선** 페이지가 표시됩니다.

   그림 2 VLAN 우선 순위 변경

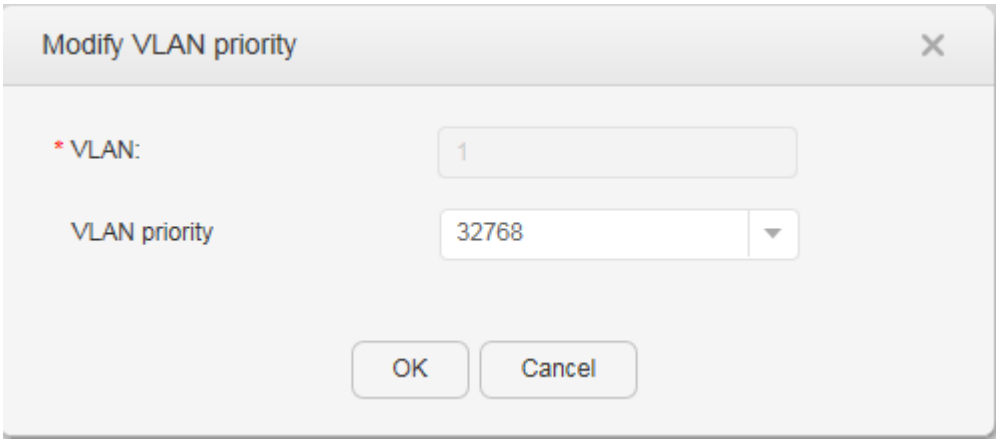


   표 2 는 페이지의 매개변수를 설명합니다.

   표 2 VLAN 우선 순위 변경을 위한 매개변수

매개변수	설명
VLAN	우선 순위를 변경해야 하는 VLAN 의 ID 를 나타냅니다. 값을 수정할 수 없습니다.
VLAN 우선 순위	VLAN 의 우선 순위를 나타냅니다. 값이 작을수록 우선 순위가 높음을 나타냅니다.

3. 매개변수를 설정하고 **Ok(확인)을 클릭합니다.**

- VLAN 에서 VBST 를 비활성화합니다.

1. **Configuration(구성)** > **Advanced Services(고급 서비스)** > **STP** > **VBST 구성**을 선택하여 **VBST 구성** 페이지를 엽니다.

2. VBST 를 비활성화해야 하는 VLAN 을 선택하고 비활성화를 클릭합니다. 표시되는 대화 상자에서 **Ok(확인)을 클릭**합니다.

- VBST 목록을 업데이트합니다.

1. **Configuration(구성)** > **Advanced Services(고급 서비스)** > **STP** > **VBST 구성**을 선택하여 **VBST 구성** 페이지를 엽니다.

2. **새로 고침**을 클릭하여 VBST 목록을 업데이트합니다.

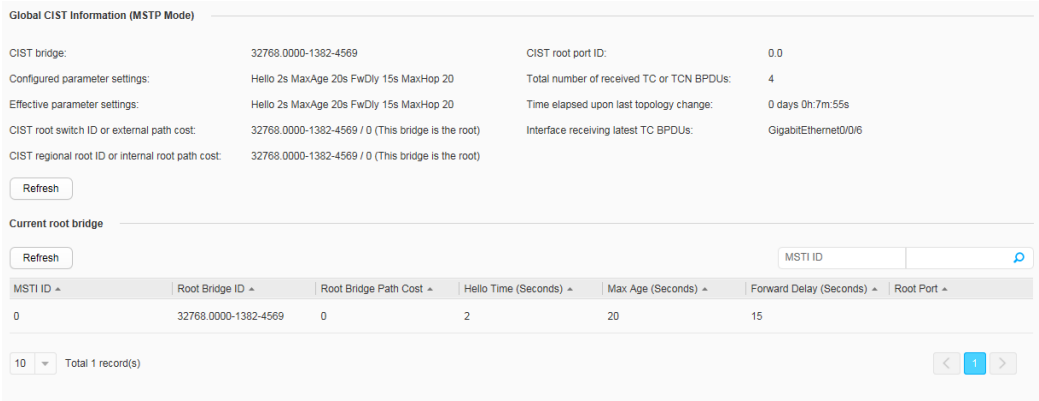
4.5.3.10.4 다중 인스턴스

절차

- CIST 에 대한 글로벌 정보를 확인하세요.

1. **Configuration(구성)** > **Advanced Services(고급 서비스)** > **STP** > **다중 인스턴스**를 선택하여 그림 1 과 같이 **다중 인스턴스** 페이지를 엽니다.

그림 1 다중 인스턴스 페이지



2. CIST 정보를 새로 고치려면 **현재 루트 브리지** 위의 **새로 고침을** 클릭합니다.

- 현재 루트 브리지를 확인합니다.

1. **Configuration(구성) > Advanced Services(고급 서비스) > STP > 다중 인스턴스**를 선택하여 **다중 인스턴스** 페이지를 엽니다.

2. **현재 루트 브리지**에서 **새로 고침**을 클릭하여 **현재 루트 브리지**에 대한 정보를 새로 고칩니다.

NOTE

MSTI ID 옆에 **MSTI ID** 를 입력하고 를 클릭하면 MSTI 정보를 조회할 수 있습니다.

4.5.3.11 LLDP

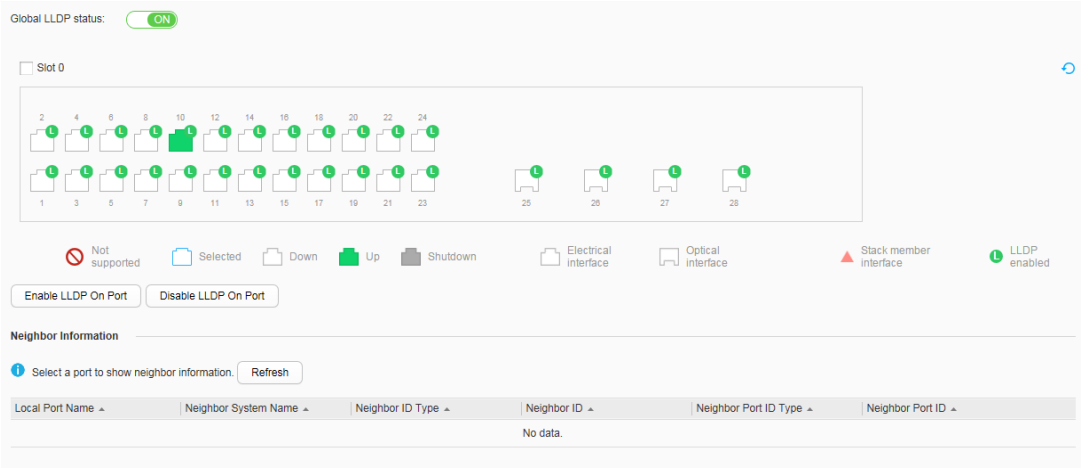
문맥

네트워크 장치 간의 계층 2 링크 상태를 보고 네트워크 토폴로지를 분석하려면 LLDP(Link Layer Discovery Protocol)를 활성화하십시오.

절차

1. **Configuration(구성) > Advanced Services(고급 서비스) > LLDP** 를 선택하여 그림 1 과 같이 LLDP 구성 페이지를 표시합니다.

   그림 1 LLDP 구성 페이지



2. **글로벌 LLDP 상태**를 **ON** 으로 설정하여 LLDP 를 모든 인터페이스에서 활성화되도록 합니다.

3. 구성할 인터페이스를 선택합니다.

   다음 방법 중 하나를 사용하여 인터페이스를 선택합니다.

   - 인터페이스 아이콘을 클릭하여 하나 이상의 인터페이스를 선택합니다.
   - 여러 인접 인터페이스를 선택하려면 마우스를 끕니다.
   - 패널의 모든 인터페이스를 선택하려면 패널의 확인란을 선택합니다.

4. **LLDP 포트 활성화** 또는 **비활성화 LLDP 포트**를 클릭하여 선택한 인터페이스를 LLDP 활성화 또는 비활성화 할 수 있습니다. **새로 고침**을 클릭하여 선택한 인터페이스의 인접 항목에 대한 정보를 새로 고칩니다.

4.5.3.12 IGMP 스누핑

4.5.3.12.1 IGMP 스누핑 구성

문맥

VLAN 에서 기본 IGMP 스누핑 기능을 구성하면 스위치가 레이어 2 멀티캐스트 전달 테이블을 만들고 유지 관리할 수 있으며, 이를 기반으로 멀티캐스트 데이터 패킷이 데이터 링크 레이어를 통해 수신기로 정확하게 전달될 수 있습니다.

NOTE

알 수 없는 멀티캐스트 흐름은 멀티캐스트 전달 테이블의 항목과 일치하지 않거나 비어 있는 아웃바운드 인터페이스 목록과 멀티캐스트 전달 항목과 일치하는 흐름입니다. 이러한 흐름은 사용자가 요청하지 않습니다. 스위치가 알 수 없는 IPv4 멀티캐스트 흐름을 처리하는 데 사용하는 기본 방법은 레이어 2

멀티캐스트가 활성화되었는지 여부와 어떤 레이어 2 멀티캐스트 전달 모드가 사용되는지에 따라 다릅니다.

- 스위치에서 레이어 2 멀티캐스트가 활성화되지 않은 경우 스위치는 해당 VLAN 에서 알 수 없는 멀티캐스트 흐름을 브로드캐스트합니다.
- 레이어 2 멀티캐스트가 활성화된 경우 MAC 주소 기반 전달 모드에서 해당 VLAN 의 알 수 없는 멀티캐스트 흐름을 브로드캐스트하고 IP 주소 기반 전달 모드에서 알 수 없는 멀티캐스트 흐름을 삭제합니다.

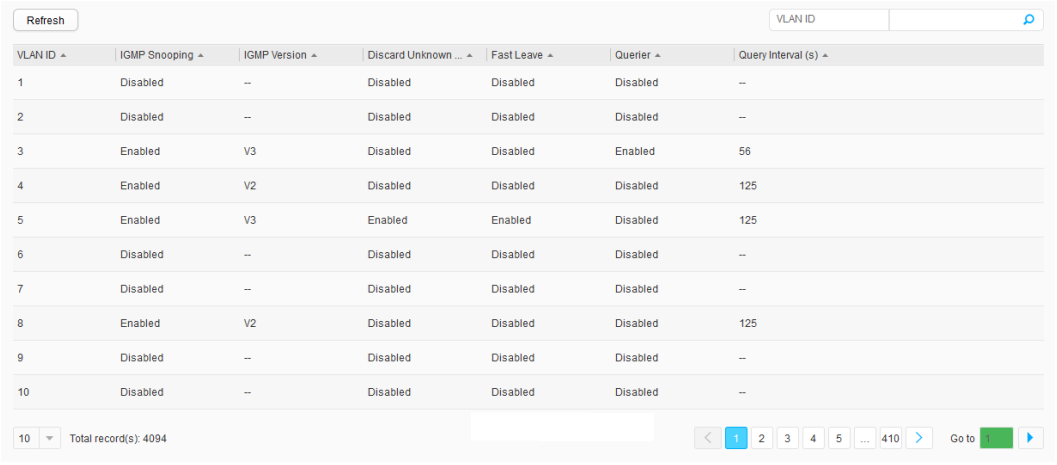
스위치가 VLAN 에서 알 수 없는 멀티캐스트 흐름을 브로드캐스트하는 경우 알 수 없는 멀티캐스트 흐름을 삭제하도록 스위치를 구성하여 즉각적인 대역폭 사용을 줄일 수 있습니다.

절차

1. **Configuration(구성) > Advanced Services(고급 서비스) > IGMP 스누핑을** 선택하고 **IGMP 스누핑 구성** 탭을 클릭합니다.

2. VLAN 의 구성 레코드를 클릭하면 그림 1 과 같이 편집 상태로 들어갑니다.

그림 1 IGMP 스누핑 구성



3. **IGMP 스누핑** 및 **IGMP 버전** 과 같은 IGMP 스누핑 매개변수를 설정합니다.

4. 클릭 ✔하여 구성을 완료합니다.

4.5.3.12.1 그룹 구성원 포트

절차

- 정적 사용자를 만듭니다.

  1. 그림 1 과 같이 **Configuration** > **Advanced Services** > **IGMP Snooping** 을 선택하고 **Group Member Ports** 탭을 클릭합니다.

     그림 1 그룹 구성원 포트

2. 그림 2 와 같이 **정적 사용자 만들기**를 클릭하여 **정적 사용자 생성** 페이지를 표시합니다.

그림 2 정적 사용자 생성

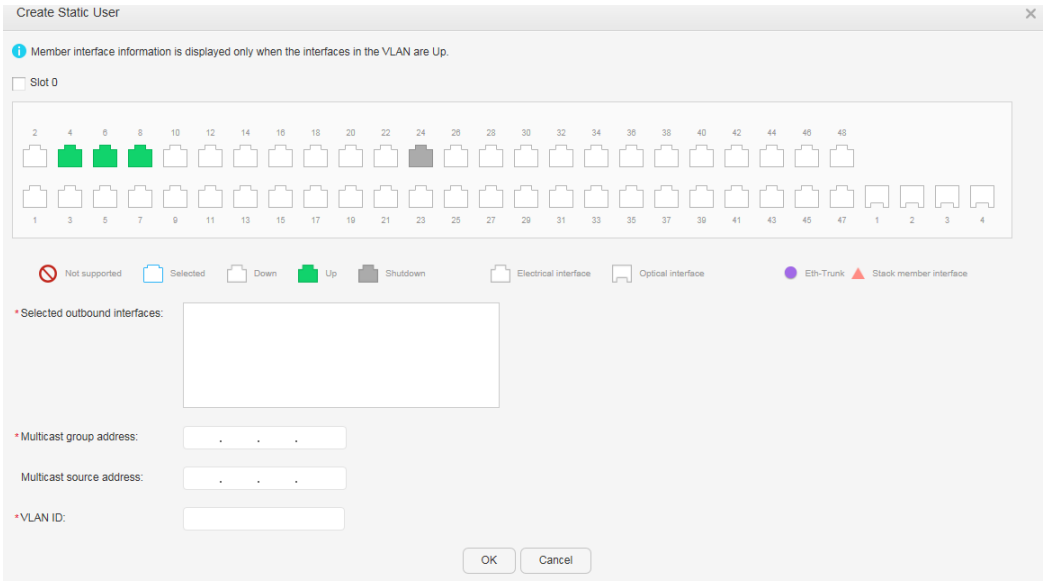


표 1 은 **정적 사용자 생성** 페이지의 매개변수를 설명합니다.

표 1 정적 사용자 생성 페이지의 매개변수

매개변수	설명
선택된 아웃바운드 인터페이스	패널에서 선택한 인터페이스를 나열합니다.
멀티캐스트 그룹 주소	인터페이스를 바인딩할 멀티캐스트 그룹의 IP 주소를 입력합니다.
멀티캐스트 소스 주소	멀티캐스트 소스 주소를 입력하십시오.
VLAN ID	인터페이스의 VLAN ID 를 입력합니다. 값은 1 에서 4094 사이의 정수입니다.

3. 매개변수를 설정합니다.

4. Ok(확인)을 클릭합니다.

- 정적 사용자를 삭제합니다.

1. 그림 1 과 같이 **Configuration** > **Advanced Services** > **IGMP Snooping** 을 선택하고 **Group Member Ports** 탭을 클릭합니다.

2. 그림 3 과 같이 **정적 사용자 삭제**를 클릭하여 **정적 사용자 삭제** 페이지를 표시합니다.

   그림 3 정적 사용자 삭제

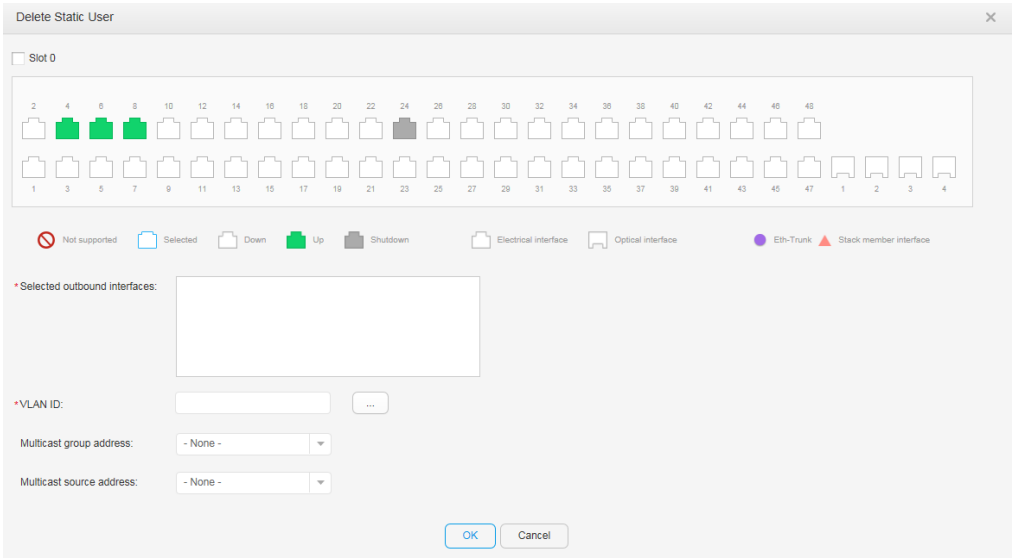


   표 2 는 **정적 사용자 삭제** 페이지의 매개변수를 설명합니다.

표 2 정적 사용자 삭제 페이지의 매개변수

매개변수	설명
선택된 아웃바운드 인터페이스	패널에서 선택한 인터페이스를 나열합니다.
VLAN ID	VLAN ID 를 선택하여 지정된 VLAN 의 그룹에서 인터페이스를 제거합니다.
멀티캐스트 그룹 주소	인터페이스를 제거할 멀티캐스트 그룹의 IP 주소를 입력합니다.
멀티캐스트 소스 주소	멀티캐스트 소스 주소를 입력하십시오.

3. 매개변수를 설정합니다.

4. Ok(확인)을 클릭합니다.

- 동적 멀티캐스트 항목을 삭제합니다.

1. 그림 1 과 같이 **Configuration** > **Advanced Services** > **IGMP Snooping 을** 선택하고 **Group Member Ports** 탭을 클릭합니다.
2. 삭제를 클릭 할 동적 멀티 캐스트 항목을 선택하고 **동적 멀티 캐스트 항목 삭제**를 클릭합니다. 시스템에서 항목을 삭제할지 여부를 묻습니다.
3. Ok(확인)을 클릭합니다.

4.5.3.13 MLD 스누핑

4.5.3.13.1 MLD 스누핑 구성

문맥

MLD 스누핑이 구성되면 스위치는 사용자 호스트와 라우터 간에 교환되는 MLD 메시지를 분석하여 레이어 2 멀티캐스트 포워딩 테이블을 생성하고 유지할 수 있습니다. 이러한 방식으로 멀티캐스트 데이터 패킷은 브로드캐스트되는 대신 레이어 2 멀티캐스트 포워딩 테이블을 기반으로 포워딩됩니다.

NOTE

멀티캐스트 흐름은 멀티캐스트 전달 테이블의 항목과 일치하지 않거나 비어 있는 아웃바운드 인터페이스 목록이 있는 멀티캐스트 전달 항목과 일치하는 경우 알 수 없는 것으로 간주됩니다. 이러한 흐름은

사용자가 요청하지 않습니다. 스위치가 알 수 없는 IPv6 멀티캐스트 흐름을 처리하는 데 사용하는 기본 방법은 레이어 2 멀티캐스트가 활성화되었는지 여부와 어떤 레이어 2 멀티캐스트 전달 모드가 사용되는지에 따라 다릅니다.

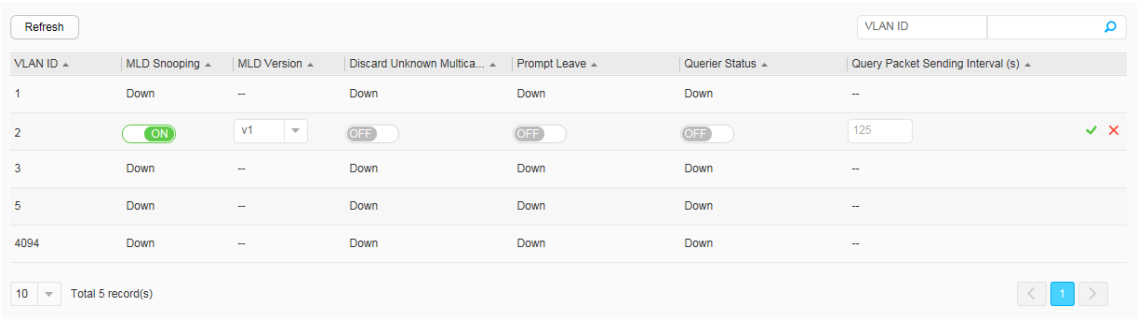
- 스위치에서 레이어 2 멀티캐스트가 활성화되지 않은 경우 스위치는 알 수 없는 멀티캐스트 흐름을 브로드캐스트합니다.
- 레이어 2 멀티캐스트가 스위치에서 활성화된 경우 스위치는 어떤 레이어 2 멀티캐스트 전달 모드가 사용되는지에 관계없이 VLAN 에서 알 수 없는 멀티캐스트 흐름을 브로드캐스트합니다.

절차

1. **Configuration(구성) > Advanced Services(고급 서비스) > MLD 스누핑을** 선택하고 **MLD 스누핑 구성** 탭을 클릭합니다.

2. VLAN 의 구성 레코드를 클릭하면 그림 1 과 같이 편집 상태로 들어갑니다.

그림 1 MLD 스누핑 구성



3. **MLD 스누핑** 및 **MLD 버전** 과 같은 MLD 스누핑 매개변수를 설정합니다.

4. ✔를 클릭하여 구성을 완료합니다.

4.5.3.13.2 그룹 구성원 포트

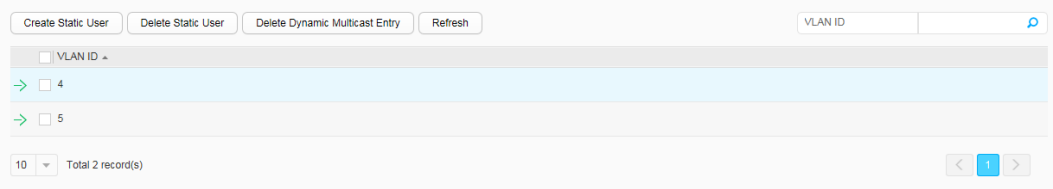
절차

- 정적 사용자를 만듭니다.

1. 그림 1 과 같이 **Configuration** > **Advanced Services** > **MLD**

   Snooping 을 선택하고 **Group Member Ports** 탭을 클릭합니다.

   그림 1 그룹 구성원 포트



2. 그림 2 와 같이 **정적 사용자 만들기**를 클릭하여 **정적 사용자 생성** 페이지를

   표시합니다.

그림 2 정적 사용자 생성

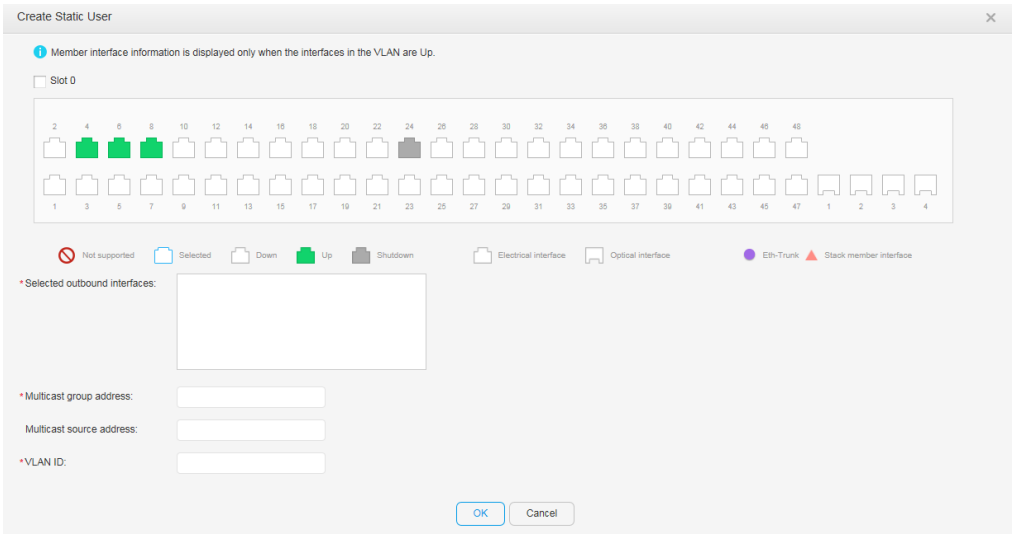


표 1 은 **정적 사용자 생성** 페이지의 매개변수를 설명합니다.

표 1 정적 사용자 생성 페이지의 매개변수

매개변수	설명
선택된 아웃바운드 인터페이스	패널에서 선택한 인터페이스를 나열합니다.
멀티캐스트 그룹 주소	인터페이스를 바인딩할 멀티캐스트 그룹의 IP 주소를 입력합니다.
멀티캐스트 소스 주소	멀티캐스트 소스 주소를 입력하십시오.
VLAN ID	인터페이스의 VLAN ID 를 입력합니다. 값은 1 에서 4094 사이의 정수입니다.

3. 매개변수를 설정합니다.

4. Ok(확인)을 클릭합니다.

- 정적 사용자를 삭제합니다.

1. 그림 1 과 같이 **Configuration** > **Advanced Services** > **MLD Snooping 을** 선택하고 **Group Member Ports** 탭을 클릭합니다.

2. 그림 3 과 같이 **정적 사용자 삭제**를 클릭하여 **삭제 정적 사용자** 페이지를 표시합니다.

그림 3 정적 사용자 삭제

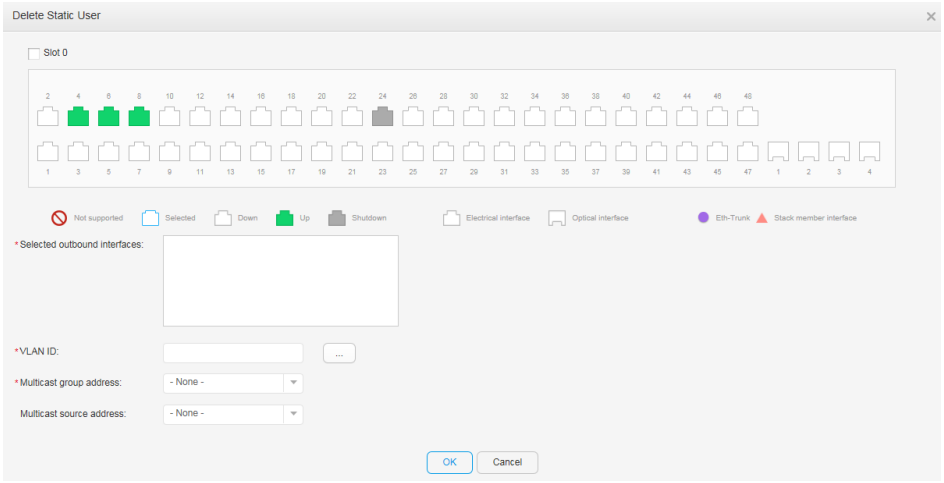


표 2 는 **정적 사용자 삭제** 페이지의 매개변수를 설명합니다.

표 2 정적 사용자 삭제 페이지의 매개변수

매개변수	설명
선택된 아웃바운드 인터페이스	패널에서 선택한 인터페이스를 나열합니다.
VLAN ID	VLAN ID 를 선택하여 지정된 VLAN 의 그룹에서 인터페이스를 제거합니다.
멀티캐스트 그룹 주소	인터페이스를 제거할 멀티캐스트 그룹의 IP 주소를 입력합니다.
멀티캐스트 소스 주소	멀티캐스트 소스 주소를 입력하십시오.

3. 매개변수를 설정합니다.

4. Ok(확인)을 클릭합니다.

- 동적 멀티캐스트 항목을 삭제합니다.

  1. 그림 1 과 같이 **Configuration** > **Advanced Services** > **MLD Snooping 을** 선택하고 **Group Member Ports** 탭을 클릭합니다.
  2. 삭제할 동적 멀티 캐스트 항목을 선택하고 **삭제 동적 멀티 캐스트 항목**을 클릭합니다. 시스템에서 항목을 삭제할지 여부를 묻습니다.
  3. Ok(확인)을 클릭합니다.

6.5.3.14 PoE

문맥

NOTE

스위치가 PoE 를 지원하는지 여부는 하드웨어에 따라 다릅니다. Non-PoE 스위치는 소프트웨어 업그레이드를 통해 PoE 스위치로 변경할 수 없습니다. 다음 조건 중 하나를 충족하는 스위치가 PoE 스위치입니다.

- 장치 이름에 PWR 또는 PWH 가 포함되어 있습니다.
- 스위치는 V200R013C02 이상 버전으로 출시되었으며 새로운 다운링크 인터페이스 유형 UM, P 또는 U 를 제공합니다.

절차

1. **Configuration(구성) > Advanced Services(고급 서비스) > PoE** 를 선택합니다.

2. 그림 1 과 같이 전역 설정을 수행하고 **Apply(적용)을 클릭**합니다.

그림 1 전역 설정

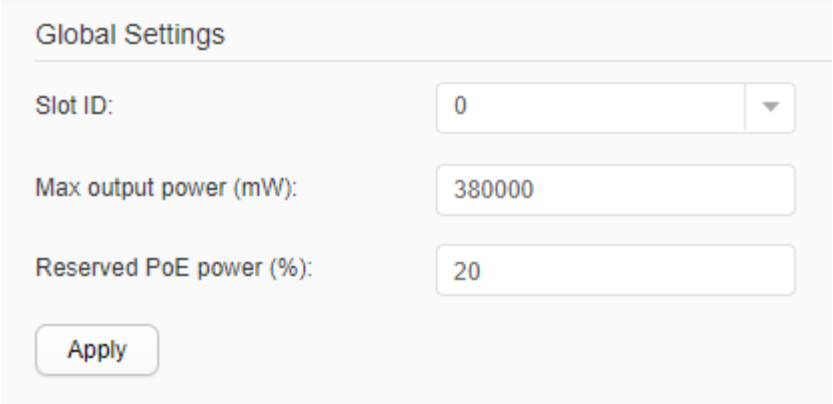


표 1 은 **전역 설정**의 매개변수를 설명합니다.

표 1 전역 설정의 매개변수

안건	설명
슬롯 ID	단일 보드를 선택합니다.
전원 공급 관리 모드	스위치의 전원 공급 관리 모드를 구성합니다. • 자동 • 설명서
최대 출력 전력(mW) MCU1 최대 출력 전력(mW) MCU2 최대 출력 전력(mW)	스위치의 최대 출력 전력을 mW 단위로 설정합니다.
예약 PoE 전력(%) MCU1 예약 PoE 전력(%) MCU2 예약 PoE 전력(%)	총 PoE 전력에 대한 예비 PoE 전력의 백분율을 설정합니다.

3. 구성할 포트를 선택합니다. 포트 영역에서 필요에 따라 다음 작업을 수행합니다.

- 포트 아이콘을 클릭합니다. 포트 선택을 취소하려면 포트 아이콘을 다시 클릭합니다.
- 커서를 끌어 배치에서 연속 포트를 선택합니다.
- 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
- 패널 이 있는 슬롯을 선택합니다. 패널의 모든 포트 가 선택됩니다.

4. 인터페이스를 구성합니다.

그림 4 인터페이스 설정

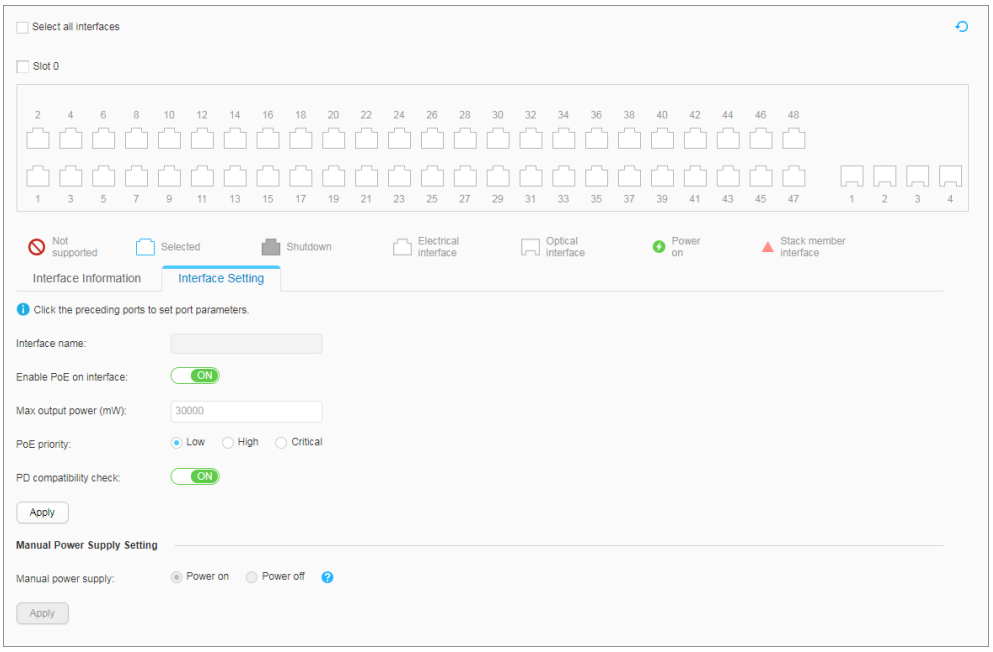


표 2 는 **인터페이스 설정**의 매개변수를 설명합니다.

표 2 인터페이스 설정 파라미터

안건	설명
인터페이스 이름	현재 구성된 인터페이스 이름을 나타냅니다. 이 매개변수는 수정할 수 없습니다.
인터페이스에서 PoE 활성화	PoE 기능을 활성화할지 여부를 나타냅니다. • ON: PoE 기능을 활성화합니다. • OFF: PoE 기능을 비활성화합니다.
최대 출력 전력(mW)	인터페이스의 최대 출력 전력을 mW 단위로 설정합니다.
PoE 우선 순위	인터페이스에 대한 전원 공급 장치 우선 순위를 구성합니다. • 낮음: 가장 낮은 우선 순위 • 높음: 두 번째로 높은 우선 순위 • 중요: 가장 높은 우선 순위
수동 전원 공급 장치	수동 전원 공급 모드를 구성합니다. • 전원 켜기: 인터페이스의 전원이 수동으로 켜집니다. • 전원 끄기: 인터페이스의 전원이 수동으로 꺼집니다.
PD 호환성 체크	인터페이스에서 비표준 PD 호환성 검사를 활성화할지 여부를 나타냅니다. • ON: 비표준 PD 호환성 검사를 활성화합니다. • OFF: 비표준 PD 호환성 검사를 비활성화합니다.

5. **Apply(적용)을 클릭**하여 구성을 적용합니다.

4.5.3.15 미러링

4.5.3.15.1 포트 미러링 디스플레이

절차

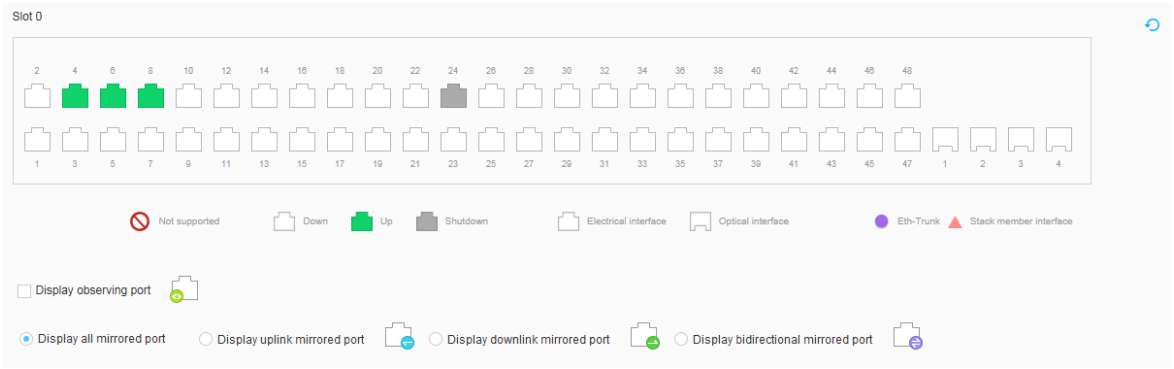
1. **Configuration(구성) > Advanced Services(고급 서비스)**

   > 미러링을 선택하여 **미러링** 페이지를 엽니다.

2. 그림 1 과 같이 **포트 미러링 디스플레이** 탭을 클릭하여 **포트 미러링**

   디스플레이 페이지를 엽니다.

   그림 1 포트 미러링 표시 페이지



3. **관찰 포트 표시** 확인란을 선택하여 **관찰 포트**를 확인합니다.

4. **미러링된 포트 모두 표시** 확인란을 선택하여 **미러링된 모든 포트를** 확인합니다.

5. **업링크 미러링 포트 표시** 확인란을 선택하여 인바운드 미러링 포트를 확인합니다.

6. **다운링크 미러링 포트 표시** 확인란을 선택하여 미러링된 아웃바운드 포트를 확인합니다.

7. **양방향 미러링 포트 표시** 확인란을 선택하여 **양방향 미러링 포트**를 확인합니다.

4.5.3.13.2 포트 미러링 구성

문맥

포트 미러링에서 미러링된 포트를 통과하는 패킷은 복사된 다음 분석 및 Monitoring(모니터링)을 위해 지정된 관찰 포트로 전송됩니다.

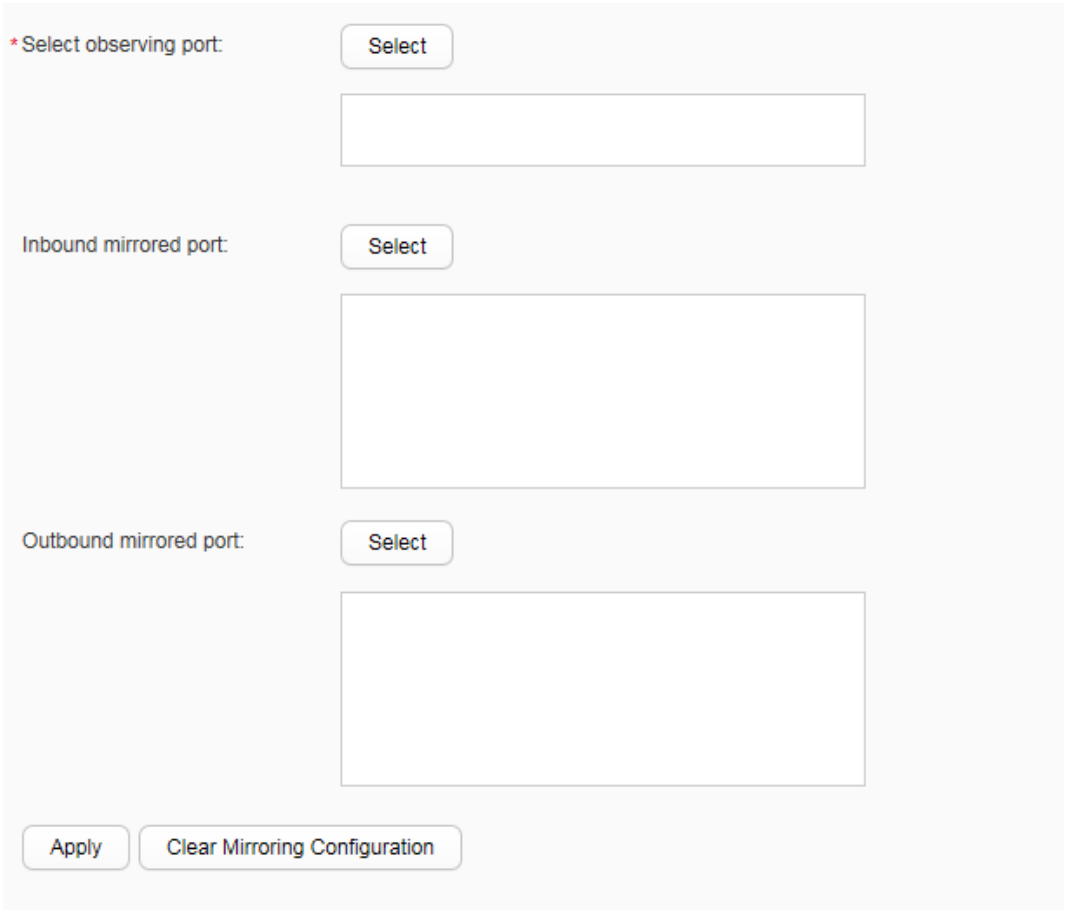
NOTE

- 물리적 포트는 관찰 포트와 미러링 포트 모두로 구성할 수 없습니다.

절차

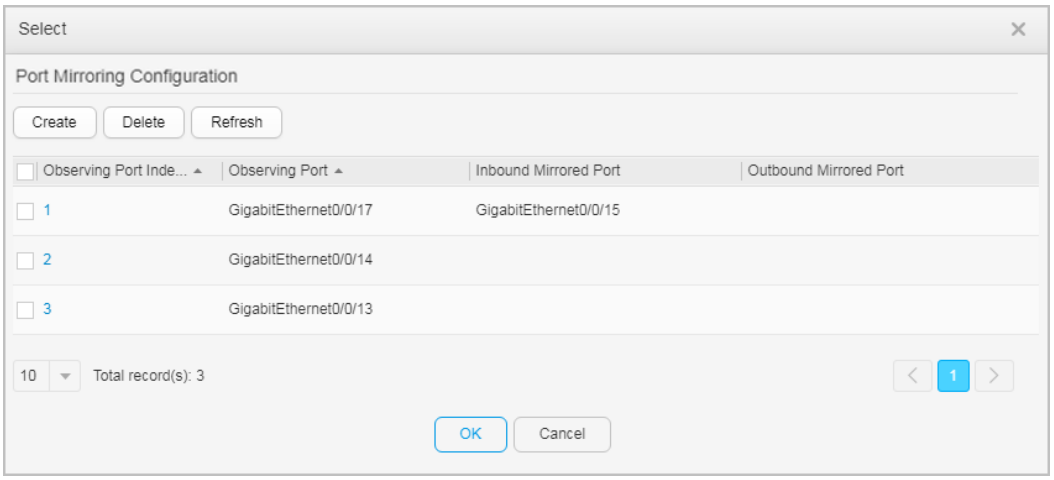
1. **Configuration(구성) > Advanced Services(고급 서비스)** > **미러링을** 선택합니다. **미러링** 페이지가 표시됩니다.
2. **포트 미러링 구성** 탭을 클릭합니다. 그림 1 과 같이 **포트 미러링 구성** 페이지가 표시됩니다.

그림 1 포트 미러링 구성 페이지



3. **관찰 포트 선택** 옆에 있는 **선택**을 클릭합니다. 그림 2 와 같이 관찰 포트를 선택하는 대화 상자가 표시됩니다.

그림 2 포트 구성 관찰

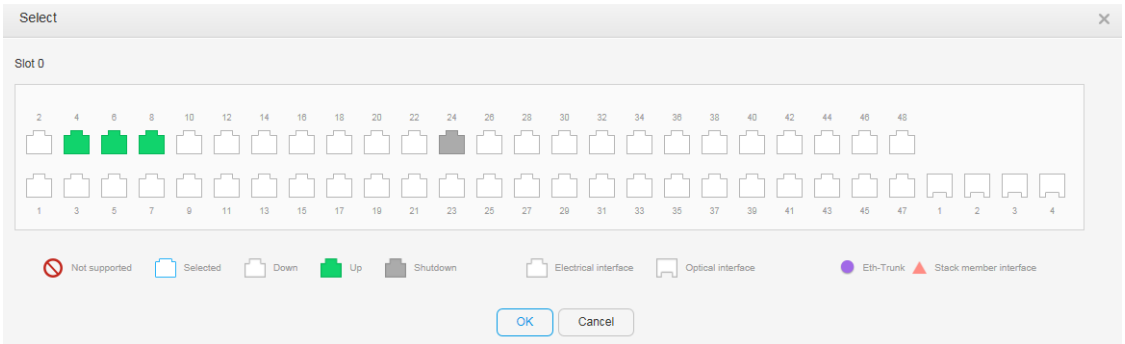


4. 원하는 관찰 포트를 선택하고 **Ok(확인)을 클릭합니다.**

> **NOTE**
>
> **생성**을 클릭하여 포트를 관찰 포트로 구성할 수도 있습니다. 관찰 포트의 인덱스를 클릭하여 인덱스를 수정할 수 있습니다.

5. **인바운드 미러링 포트** 및 **아웃바운드 미러링 포트** 옆에 있는 **선택을 차례로** 클릭합니다. 그림 3 과 같이 포트 구성 페이지가 표시됩니다.

그림 3 포트 구성 페이지



> **NOTE**

앞의 순서대로 포트를 구성하지 않으면 선택한 포트가 구성되지 않은 첫 번째 포트로 자동 구성됩니다. 예를 들어 **아웃바운드 미러링 포트**가 지정되었지만 **관찰 포트 선택** 및 **인바운드 미러링 포트**가 구성되지 않은 경우 지정된 포트는 **관찰 포트 선택**으로 자동 구성됩니다.

6. 인바운드 미러링 포트 또는 아웃바운드 미러링 포트로 구성할 인터페이스의 아이콘을 선택하고 **Ok(확인)을 클릭**합니다.
7. **Apply(적용)**을 클릭합니다. 표시되는 대화 상자에서 **Ok(확인)**을 클릭하여 구성을 완료합니다.
8. 이전 포트 미러링 **구성**을 지우려면 **미러링 구성 지우기**를 클릭합니다.

4.5.3.16 스택

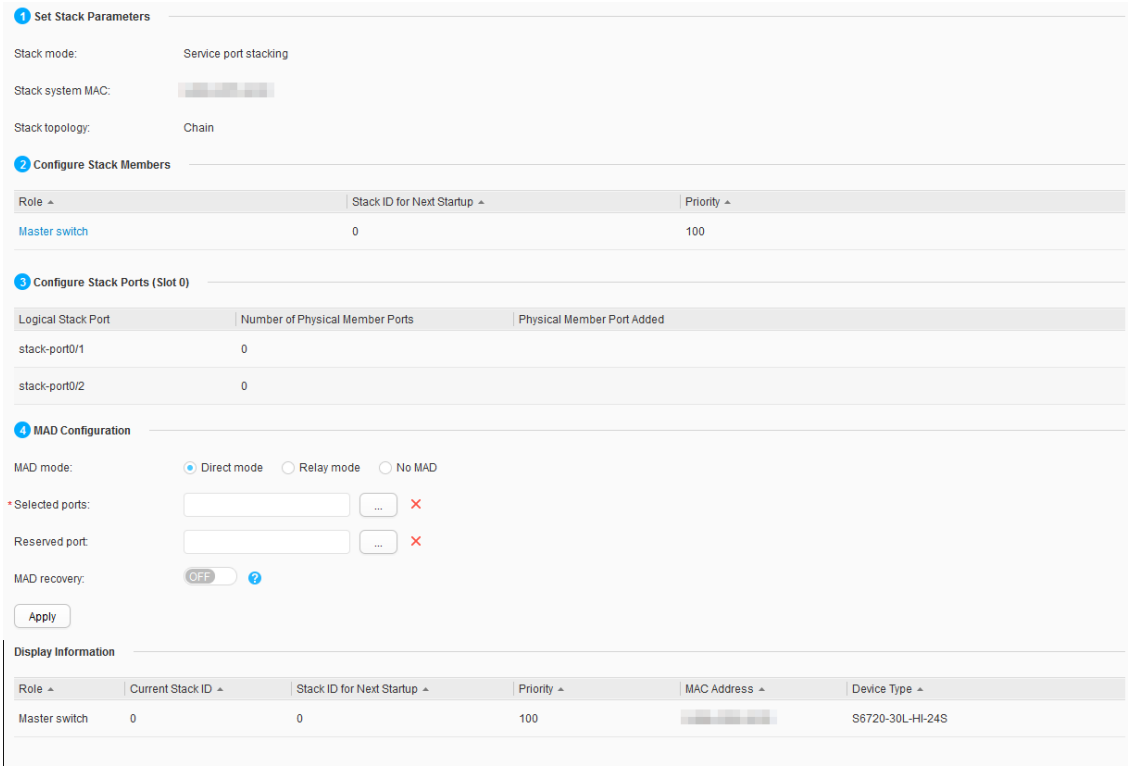
문맥

서비스 포트 연결 또는 스택 카드 연결을 사용하여 스택을 설정할 수 있습니다.

절차

1. 그림 1 과 같이 탐색 트리에서 **Configuration(구성) > Advanced Services(고급 서비스) > 스택**을 선택하여 **스택** 페이지를 엽니다.

그림 1 스택 구성 페이지



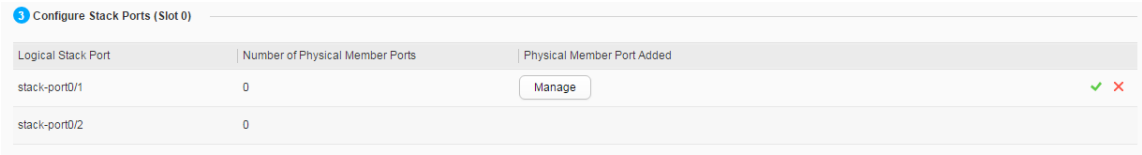
2. 그림 2 와 같이 **Configure Stack Members** 아래의 데이터 라인을 클릭하여 **마스터 스위치, 대기 스위치** 또는 **슬레이브 스위치**를 구성합니다. 매개변수를 설정하고 ✔을 클릭합니다.

> **NOTE**
>
> **Standby 스위치** 또는 **Slave 스위치**는 **스위치** 가 스택에 합류할 때만 표시됩니다.

그림 2 스택 구성원 구성 페이지

3. **Configure Stack Members** 아래에 있는 **Master 스위치, Standby 스위치** 또는 **Slave 스위치를** 클릭하여 **Configure Stack Ports (Slot ID)** 페이지를 열고 적절한 데이터 라인을 선택하면 그림 3 과 같이 **Manage** 가 나타납니다.

그림 3 스택 포트 구성 페이지



4. **관리를** 클릭합니다. 표시된 페이지에서 스택 멤버 포트를 선택하고 ✔를 클릭합니다.

> **NOTE**
>
> 스택 구성원 포트를 철회하려면 **관리를** 클릭하고 표시된 페이지에서 이 포트의 선택을 취소하고 ✔을 클릭합니다.

5. **MAD 구성**에서 **MAD 모드**를 지정하여 그림 4 와 같이 다중 활성 검출(MAD)을 구성합니다.

그림 4 MAD 구성

표 1 은 페이지의 매개변수를 설명합니다.

표 1 MAD 구성

구성 항목	설명
매드 모드	MAD 모드를 지정합니다. • **다이렉트 모드** : **다이렉트 모드의** MAD • **릴레이 모드** : **릴레이 모드의** MAD • **매드 없음**
선택한 포트	감지할 포트를 구성합니다.

표 1 MAD 구성

구성 항목	설명
CSS/스택 이더넷 트렁크	**선택한 포트** 는 **MAD 모드** 가 **Direct 모드** 로 설정된경우에만 구성할 수 **있습니다.** **CSS/Stack Eth-Trunk** 는 **MAD 모드** 가 **릴레이 모드** 로 설정된경우에만 구성할 수 **있습니다.**
예약된 포트	후속 MAD 동안 비활성화되지 않는 예약된 포트를 지정합니다. 이 매개변수는 **MAD 모드** 가 **Direct 모드** 또는 **Relay 모드로** 설정된 경우에만 구성할 수 **있습니다.**
매드 리커버리	스택 분할 후 복구 상태가 된 장치의 비활성화된 모든 포트를 복구할지 여부를 지정합니다. • **ON** : 스택 분할 후 복구 상태가 된 장치의 비활성화된 모든 포트를 복구합니다. • **OFF** : 스택 분할 후 복구 상태로 들어가는 장치의 비활성화된 포트를 복구하지 않습니다. 이 매개변수는 **MAD 모드** 가 **Direct 모드** 또는 **Relay 모드로** 설정된 경우에만 구성할 수 **있습니다.**

6. **Apply(적용)**을 클릭합니다. 표시되는 대화 상자에서 **Ok(확인)**을 클릭합니다. 정보 **표시** 아래의 스택 정보를 확인하십시오.

4.5.4 보안 서비스

4.5.4.1 ACL

4.5.4.1.1 인터페이스 ACL

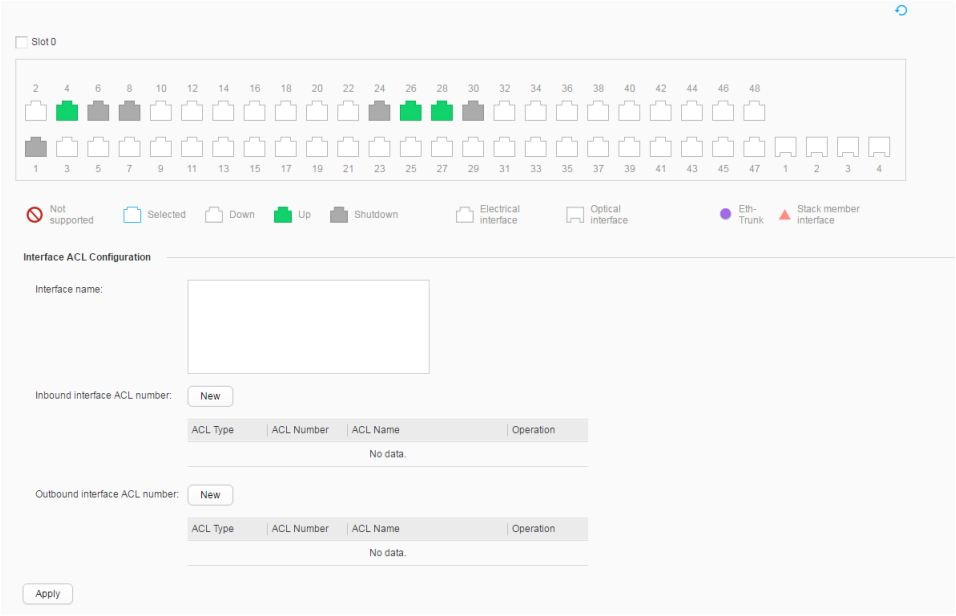
문맥

ACL 을 생성한 후 인터페이스에 적용하여 인터페이스를 기반으로 패킷을 필터링합니다.

절차

1. 그림 1 과 같이 **Configuration** > **Security Services** > **ACL Reference** 를 선택하고 **Interface ACL** 탭을 클릭합니다.

그림 1 인터페이스 ACL



2. 구성할 포트를 선택합니다. 포트 영역에서 필요에 따라 다음 작업을 수행합니다.

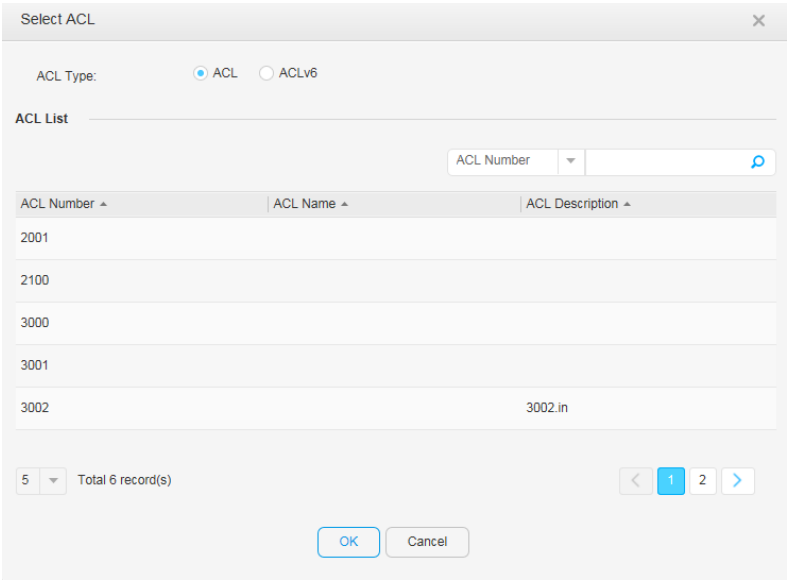
- 포트 아이콘을 클릭합니다. 포트 선택을 취소하려면 포트 아이콘을 다시 클릭합니다.
- 커서를 끌어 배치에서 연속 포트를 선택합니다.
- 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
- 패널이 있는 슬롯을 선택합니다. 패널의 모든 포트 가 선택됩니다.

3. 인바운드 및 아웃바운드 ACL 번호를 구성합니다.

a. **새로 만들기**를 클릭합니다.

b. 표시되는 대화 상자에서 그림 2 와 같이 ACL 번호를 선택하고 **확인**을 클릭합니다.

그림 2 ACL 선택



4. 매개변수를 설정한 후 Apply(**적용**)을 클릭합니다.

4.5.4.1.2 VLAN ACL

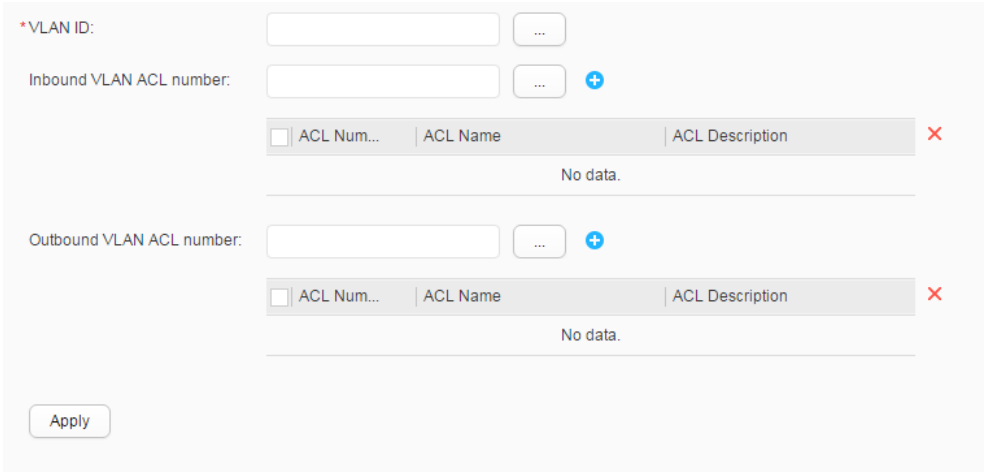
문맥

ACL 을 생성한 후 VLAN 에 적용하여 VLAN 을 기반으로 패킷을 필터링합니다.

절차

1. 그림 1 과 같이 **Configuration** > **Security Services** > **ACL Reference** 를 선택하고 **VLAN ACL** 탭을 클릭합니다.

그림 1 VLAN ACL



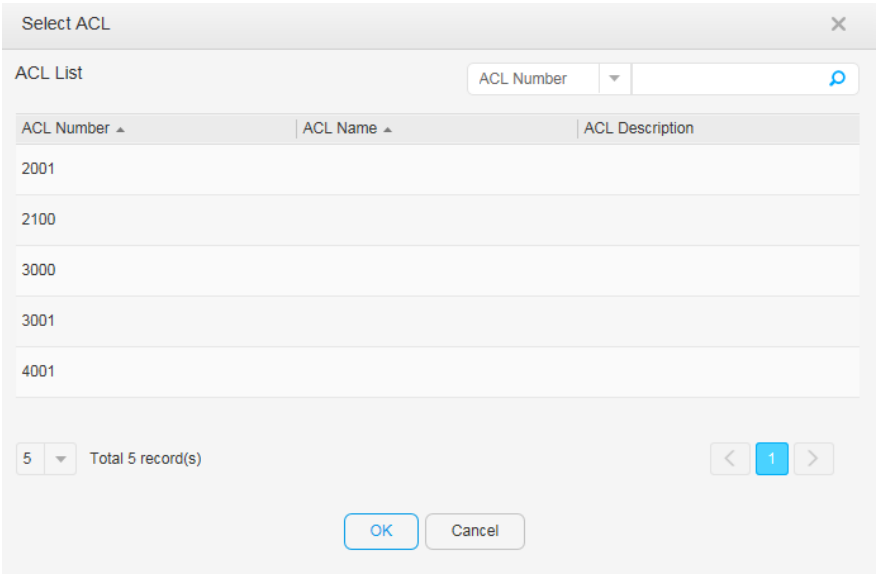
2. VLAN ID 옆에 있는 ... 을 클릭하여 **VLAN ID** 를 선택합니다.

3. 인바운드 및 아웃바운드 VLAN ACL 번호를 구성합니다.

   a. ... 을 클릭합니다.

   b. 표시되는 대화 상자에서 그림 2 와 같이 ACL 번호를 선택하고 **확인**을 클릭합니다.

   그림 2 ACL 선택



   c. ACL 을 VLAN 에 적용하려면 클릭합니다.

4. 매개변수를 설정한 후 **Apply(적용)**을 클릭합니다.

4.5.4.2 사용자 액세스 제어

4.5.4.2.1 인증 구성

문맥

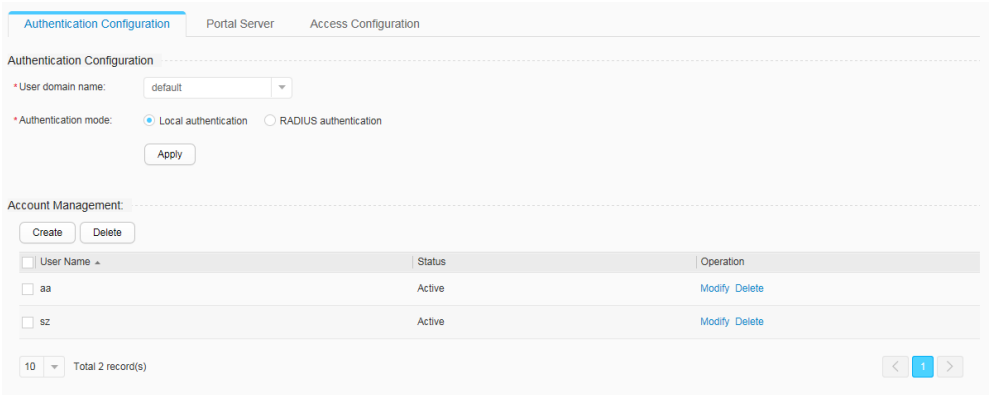
인증 구성에는 로컬 및 RADIUS 인증 모드의 구성이 포함됩니다. 로컬 인증 모드를 사용하는 경우 스위치에서 사용자 계정을 생성하고 비밀번호를 설정해야 합니다. RADIUS 인증 모드를 사용하는 경우 RADIUS 서버의 IP 주소, 포트 번호, 공유 키를 설정해야 합니다. 로컬 사용자 생성 또는 수정 시 설정한 비밀번호가 기본 비밀번호와 같으면 보안상 위험하다.

절차

- 로컬 인증 구성

1. **구성**을 클릭 하여 **구성** 페이지 를 표시합니다.
2. 탐색 트리에서 **보안 서비스** > **사용자 액세스 제어** 를 선택 하여 **사용자 액세스 제어** 페이지를 표시하십시오.
3. **인증 구성** 탭을 클릭하여 인증 **구성** 페이지를 표시하십시오.
4. **인증 구성 영역의 사용자 도메인 이름** 드롭다운 목록 상자에서 옵션을 선택합니다.
5. 그림 1 과 같이 **인증 모드** 에 대해 **로컬 인증**을 선택 합니다.

그림 1 로컬 인증 구성



6. **적용**을 클릭합니다.

7. **계정 관리** 영역 에서 로컬 인증을 위한 사용자 계정 정보를 구성합니다.

- 사용자 계정을 만듭니다.

  a. 그림 2 와 같이 **Create** 를 클릭 하여 **Create User** 페이지 를 표시합니다.

  그림 2 사용자 생성

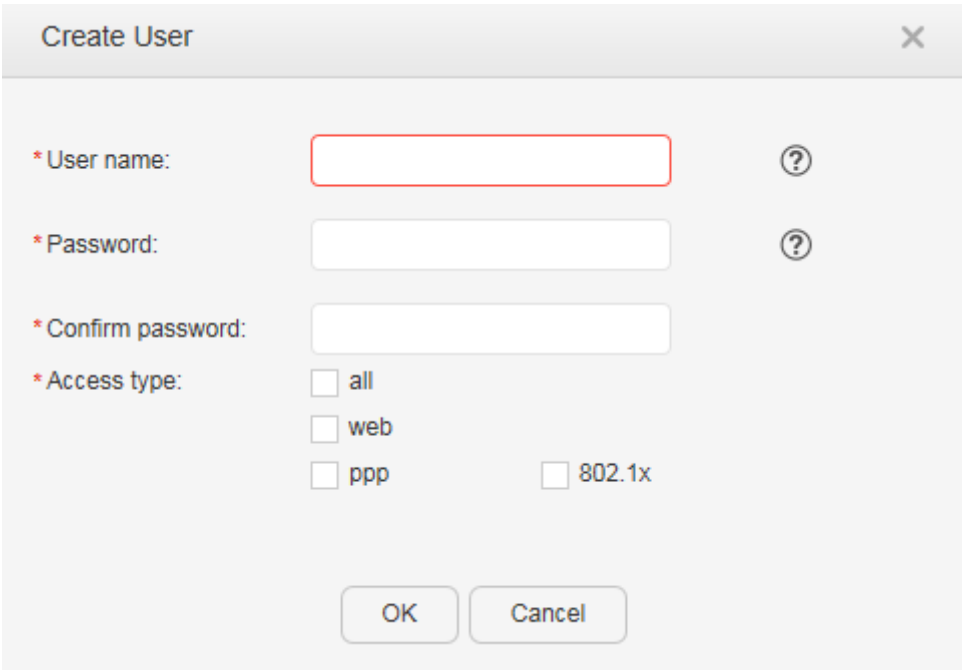


  표 1 은 사용자 생성을 위한 매개변수를 설명합니다.

표 1 사용자 생성/사용자 수정

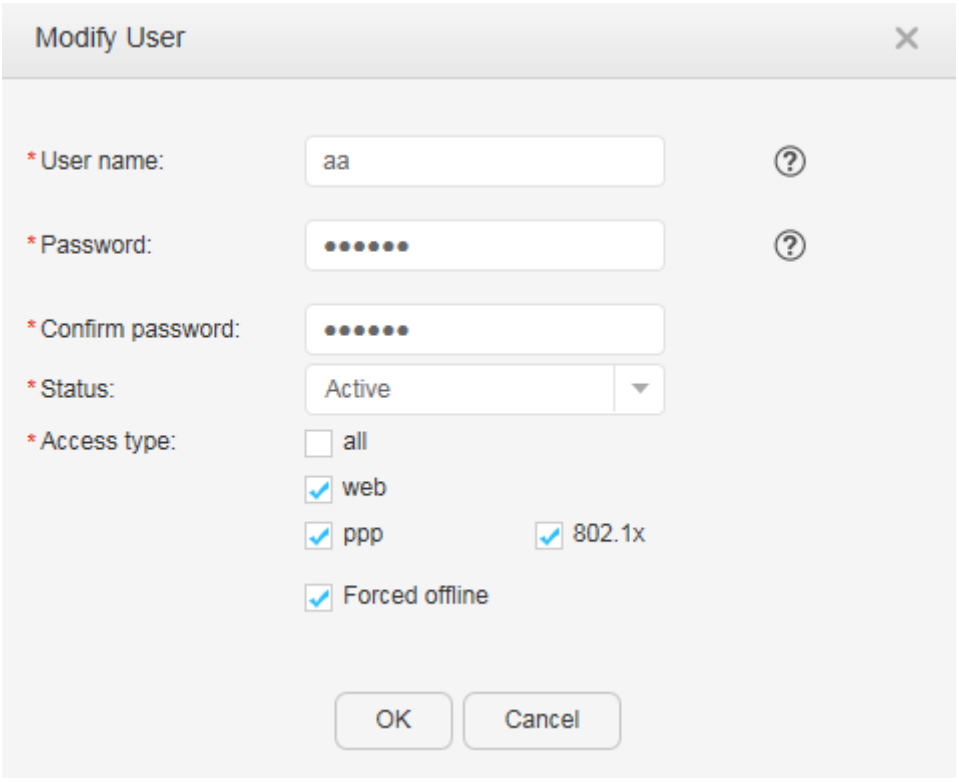
매개변수	설명
사용자 이름	새 사용자 이름을 나타냅니다. 사용자 이름에는 ₩ / : * ? " < > | ' 또는 %이며 @로 시작할 수 없습니다.
비밀번호	사용자 암호를 나타냅니다. 보안 암호는 소문자, 대문자, 숫자, 특수 문자(예: ! $ # %) 중 최소 두 가지 유형을 포함해야 합니다. 또한 암호는 공백이나 작은따옴표(')를 포함할 수 없습니다.
비밀번호 확인	확인 암호를 나타냅니다. 형식은 **Password** 의 형식과 동일 합니다.
상태	사용자 상태를 설정합니다. 사용자 상태에는 활성 및 차단이 포함됩니다. 상태가 차단으로 설정된 경우 장치는 사용자의 인증 요청을 거부하고 사용자는 암호를 변경할 수 없습니다. **노트:** 이 매개변수는 사용자 수정 페이지에만 표시됩니다.
액세스 유형	사용자 액세스 유형을 설정합니다.
강제 오프라인	사용자가 네트워크에서 강제로 연결 해제되었는지 여부를 나타냅니다. **노트:** 이 매개변수는 사용자 수정 페이지에만 표시됩니다.

b. 매개변수를 설정합니다. **확인**을 클릭합니다.

- 사용자 계정을 수정합니다.

a. 그림 3 과 같이 수정할 AAA 계정 옆에 있는 **수정**을 클릭 하여 **사용자 수정** 페이지 를 표시합니다.

그림 3 사용자 수정



NOTE

- 매개변수 설명은 표 1 을 참조하십시오 .
- 사용자 이름은 고정되어 있으며 변경할 수 없습니다.

b. 매개변수를 설정합니다. **확인**을 클릭합니다.

- 사용자 계정을 삭제합니다.

a. 다음 방법 중 하나를 사용하여 사용자 계정을 삭제할 수 있습니다.

- 삭제할 AAA 계정 옆에 있는 **삭제** 를 클릭합니다.
- 삭제할 AAA 계정의 기록을 선택하고 **생성** 옆에 있는 **삭제** 를 클릭

하여 AAA 계정을 일괄 삭제합니다.

a. **삭제** 를 클릭 하면 시스템에서 삭제 작업을 확인하는 메시지를 표시합니다. **확인**을 클릭합니다.

- RADIUS 인증 구성

1. **구성**을 클릭 하여 **구성** 페이지 를 표시합니다.
2. 탐색 트리에서 **보안 서비스** > **사용자 액세스 제어** 를 선택 하여 **사용자 액세스 제어** 페이지를 표시하십시오.
3. **인증 구성** 탭을 클릭하여 인증 **구성** 페이지를 표시하십시오.
4. **인증 구성 영역의 사용자 도메인 이름** 드롭다운 목록 상자에서 옵션을 선택합니다.
5. 그림 4 와 같이 **인증 모드 로 RADIUS 인증**을 선택 합니다.

그림 4 RADIUS 인증 구성

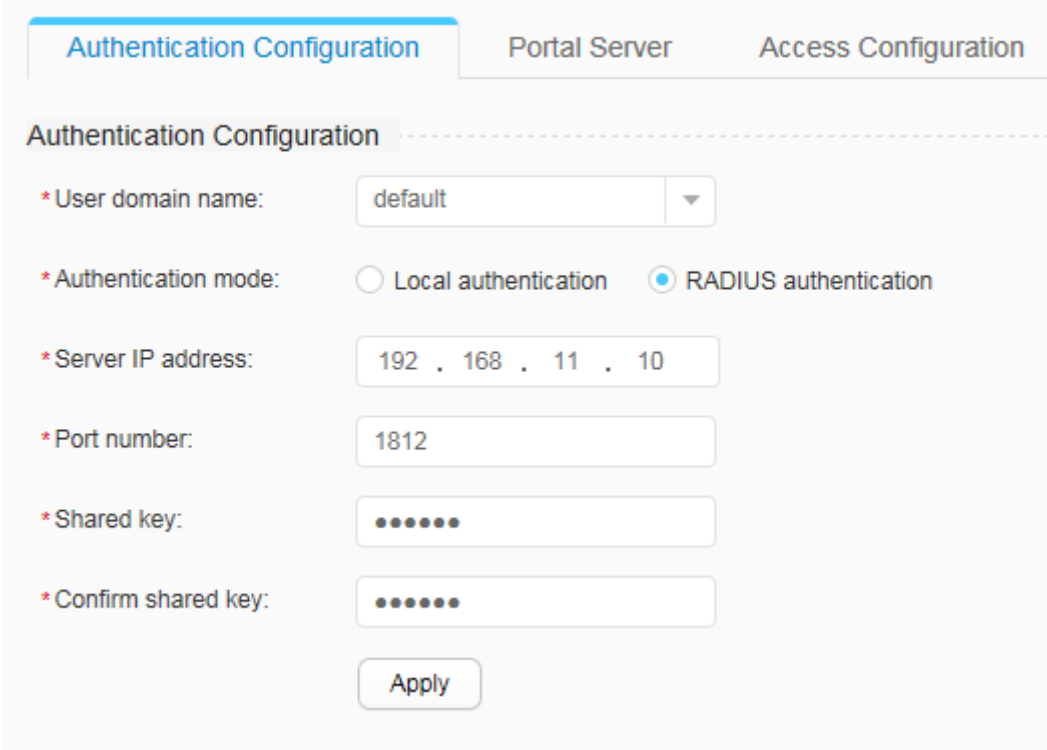


표 2 는 RADIUS 인증을 위한 매개변수를 설명합니다.

표 2 RADIUS 인증 구성을 위한 매개변수

매개변수	설명
서버 IP 주소	RADIUS 서버의 IP 주소를 나타냅니다(예: 10.10.10.1). 서버 IP 주소에는 스위치에 연결할 수 있는 경로가 있어야 합니다.
포트 번호	RADIUS 서버의 UDP 포트 번호를 나타냅니다.
공용 열쇠	스위치와 RADIUS 서버 간의 통신에 사용되는 공유 키를 나타냅니다. RADIUS 서버와 통신할 때 스위치는 공유 키를 사용하여 사용자 암호를 암호화하여 데이터 전송 중 암호 보안을 보장합니다. 값은 공백, 작은따옴표(') 및 질문 마스크(?) 없이 대소문자를 구분하는 1~128 자의 문자열입니다.
공유 키 확인	확인 공유 키를 나타냅니다. 형식은 공유 키의 형식과 동일합니다.

6. 매개변수를 설정합니다.

7. **적용**을 클릭합니다.

4.5.4.2.2 포털 서버

문맥

스위치와 Portal 서버 간의 통신을 보장하려면 스위치와 Portal 서버 간의 정보 교환에 대한 Portal 서버 IP 주소 및 매개변수(Port 번호 및 Portal 서버의 공유 키 포함)를 구성하고 인터페이스를 Portal 에 바인딩해야 합니다.

NOTE

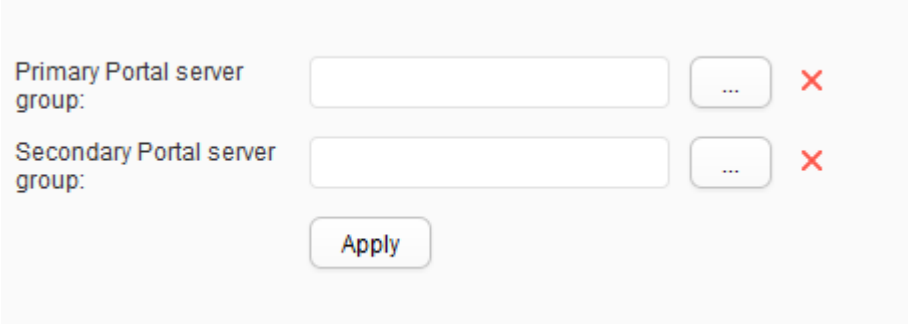
포털 인증을 구성한 후 인증 구성을 수행합니다. 두 기능은 사용자 인증을 함께 구현합니다.

절차

- 포털 서버를 구성합니다.

1. **구성을** 클릭합니다. **구성** 페이지가 표시됩니다.
2. 탐색 트리에서 **보안 서비스** > **사용자 액세스 제어**를 선택합니다. **사용자 액세스 제어** 페이지가 표시됩니다.
3. **포털 서버** 탭을 클릭합니다. **포털 서버** 탭 페이지가 표시됩니다 같이 그림 1 .

   그림 1 포털 서버 구성

4. 를 클릭 ... 하고 서버 이름을 선택합니다.
5. **Apply(적용)을 클릭**합니다.

- 포털 인증 서버를 만듭니다.

1. **구성을** 클릭합니다. **구성** 페이지가 표시됩니다.
2. 탐색 트리에서 **보안 서비스** > **사용자 액세스 제어**를 선택합니다. **사용자 액세스 제어** 페이지가 표시됩니다.
3. **포털 서버** 탭을 클릭합니다. **포털 서버** 탭 페이지가 표시됩니다.

4. 을 클릭 ... 합니다. **포털 인증 서버 목록** 페이지가 표시됩니다.

5. **Create(만들기)를 클릭합니다. 포털 인증 서버 목록** 페이지가 표시됩니다 같이 그림 2 .

그림 2 포털 인증 서버 생성

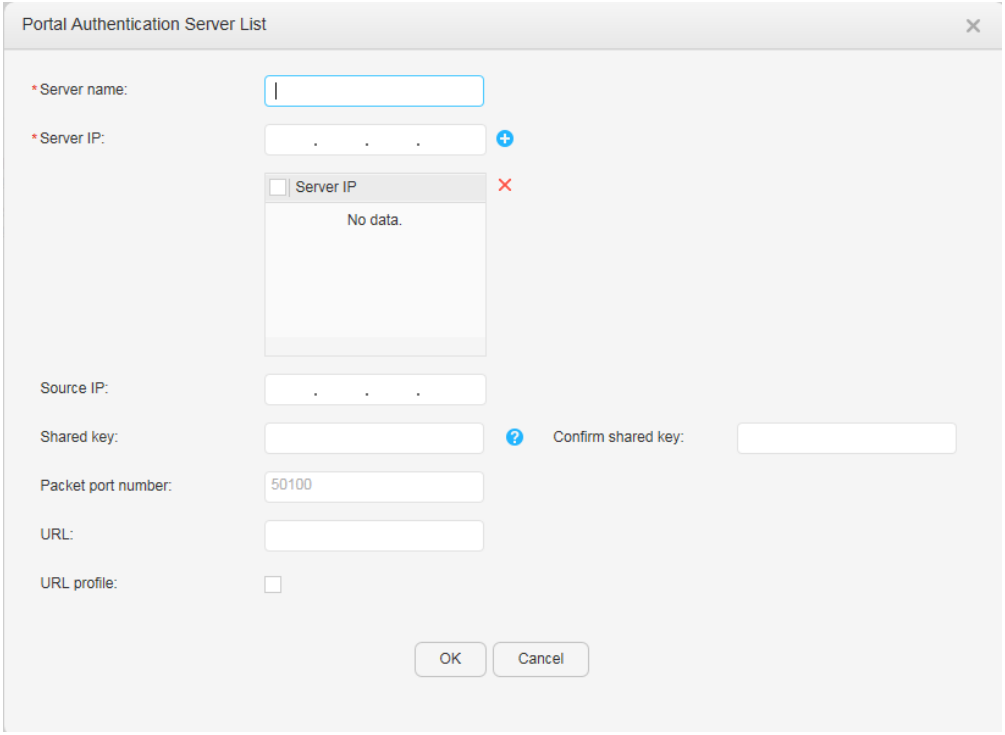


표 1 은 포털 인증 서버를 생성하기 위한 매개변수를 설명합니다.

표 1 포털 인증 서버 생성을 위한 매개변수

매개변수	설명
서버 이름	포털 인증 서버의 이름을 나타냅니다.
서버 IP	포털 서버의 IP 주소를 나타냅니다.
소스 IP	포털 서버와 통신하는 장치의 소스 IP 주소를 나타냅니다.
공용 열쇠	장치가 포털 서버와 정보를 교환하는 데 사용하는 공유 키를 나타냅니다.
공유 키 확인	공유 키를 다시 입력하십시오.

표 1 포털 인증 서버 생성을 위한 매개변수

매개변수	설명
패킷 포트 번호	장치가 포털 프로토콜 패킷을 수신 대기하는 데 사용하는 포트 번호를 나타냅니다.
URL	포털 서버의 URL 을 나타냅니다.
URL 프로필 **URL 프로필**을 선택 하면 다음 매개변수가 유효합니다.	
URL	리디렉션 URL 또는 푸시된 URL 을 나타냅니다.
사용자 액세스 URL	URL 에 포함된 사용자가 액세스하는 원래 URL 을 나타냅니다.
사용자 MAC	URL 에 포함된 사용자 MAC 주소를 나타냅니다.
사용자 IP	URL 에 포함된 사용자 IP 주소를 나타냅니다.
시스템 이름	URL 에 포함된 장치 시스템 이름을 나타냅니다.
MAC 주소 형식	• 구분 기호 없음 • normal: MAC 주소 형식을 XXXX-XXXX-XXXX 로 설정합니다. 문자를 구분 기호로 지정할 수 있습니다. • Compact: MAC 주소 형식을 XX-XX-XX-XX-XX-XX 로 설정합니다. 문자를 구분 기호로 지정할 수 있습니다.
분리 기호	하나의 문자를 포함하는 구분 기호를 나타냅니다.

6. Ok(확인)을 클릭합니다.

- 포털 인증 서버 수정.

1. **구성을** 클릭합니다. **구성** 페이지가 표시됩니다.

2. 탐색 트리에서 **보안 서비스** > **사용자 액세스 제어**를 선택합니다. **사용자 액세스 제어** 페이지가 표시됩니다.
3. **포털 서버** 탭을 클릭합니다. **포털 서버** 탭 페이지가 표시됩니다.
4. ... 을 클릭합니다. **포털 인증 서버 목록** 페이지가 표시됩니다.
5. 수정할 인증 서버의 이름을 클릭합니다. 인증 서버 수정 페이지가 표시됩니다.
6. 인증 서버에 대한 매개변수를 수정합니다. 표 1 은 매개변수를 설명합니다.
7. Ok(확인)을 클릭합니다.

- 포털 인증 서버를 삭제합니다.

1. **구성을** 클릭합니다. **구성** 페이지가 표시됩니다.
2. 탐색 트리에서 **보안 서비스** > **사용자 액세스 제어**를 선택합니다. **사용자 액세스 제어** 페이지가 표시됩니다.
3. **포털 서버** 탭을 클릭합니다. **포털 서버** 탭 페이지가 표시됩니다.
4. ... 을 클릭합니다. **포털 인증 서버 목록** 페이지가 표시됩니다.
5. 인증 서버 이름을 선택하고 **삭제를** 클릭합니다. 시스템에서 레코드를 삭제할지 여부를 묻습니다.

NOTE

- 레코드를 선택하려면 레코드의 확인란을 클릭합니다.
- 레코드를 일괄 삭제하려면 레코드의 확인란을 클릭합니다.

6. Ok(확인)을 클릭합니다.

4.5.4.2.3 액세스 구성

문맥

장치는 두 가지 구성 모드를 지원합니다. 기본적으로 통합 모드가 사용됩니다. **undo authentication 통합 모드** 명령을 실행하여 구성 모드를 공통 모드로 전환할 수 있습니다.

- 공통 모드에서 액세스 구성에는 인증 없음, 802.1X 인증, MAC 주소 인증, MAC 주소 우회 인증이 포함됩니다. 마지막 인증 모드는 802.1X 인증과 MAC 주소 인증의 조합입니다.
  - 인증 없음: 사용자가 인증 없이 네트워크에 액세스할 수 있습니다.
  - 802.1X 인증: 802.1X 프로토콜을 기반으로 하는 레이어 2 인증 모드입니다. 이 모드에서는 사용자 단말기에 802.1X 클라이언트 소프트웨어가 설치되어 있어야 하며 EAP(Extensible Authentication Protocol)를 사용하여 클라이언트와 서버 간에 사용자 ID 인증이 수행됩니다.
  - MAC 주소 인증: 사용자의 MAC 주소를 식별 정보로 사용합니다. 이 모드에서는 802.1X 클라이언트 소프트웨어를 사용자 터미널에 설치할 필요가 없습니다.
  - MAC 주소 우회 인증: 이 모드에서는 802.1X 인증이 먼저 수행되고 MAC 주소 우회 인증을 위한 지연 타이머가 동시에 활성화됩니다. 지연 시간이 만료된 후에도 802.1X 인증이 계속 실패하면 MAC 주소 인증이 트리거됩니다.

접근 설정을 할 때는 먼저 인증 기능을 활성화한 후 접근 설정이 적용되는 인터페이스를 선택하고 인증 모드를 선택해야 합니다.

- 통합 모드에서 액세스 구성에는 인증 없음, 802.1X 인증, MAC 주소 인증 및 포털 인증이 포함됩니다.

NOTE

액세스 구성을 수행한 후 인증 구성을 수행합니다. 두 기능은 사용자 인증을 함께 구현합니다.

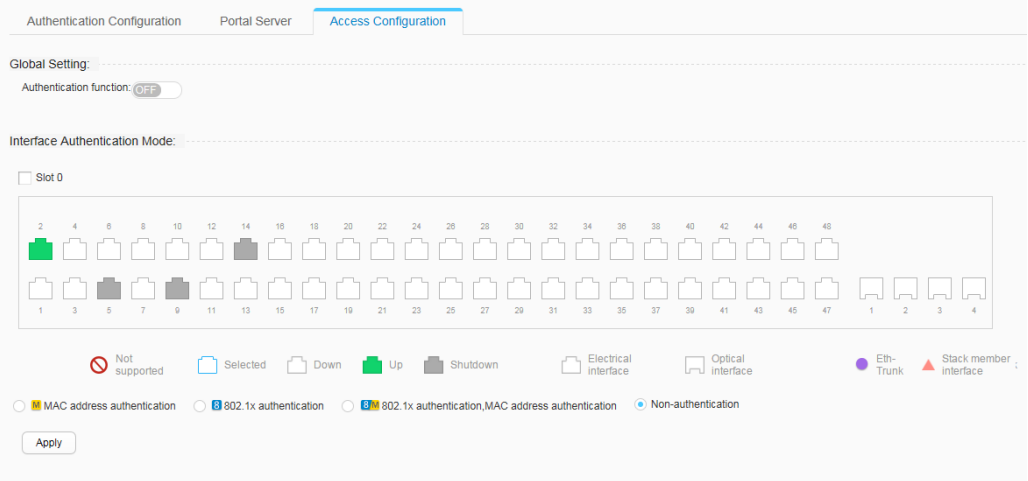
비인증이 구성된 경우 사용자는 사용자 이름 또는 암호를 사용하여 인증을 통과합니다. 따라서 장치 또는 네트워크 보안을 보호하기 위해 인증된 사용자만 장치 또는 네트워크에 액세스할 수 있도록 인증을 활성화하는 것이 좋습니다.

절차

- 공통 모드:

1. **구성**을 클릭하여 **구성** 페이지를 표시합니다.
2. 탐색 트리에서 **보안 서비스** > **사용자 액세스 제어** 를 선택 하여 **사용자 액세스 제어** 페이지를 표시하십시오.
3. 그림 1 과 같이 **액세스 구성** 탭을 클릭하여 액세스 **구성** 페이지를 표시합니다.

그림 1 액세스 구성



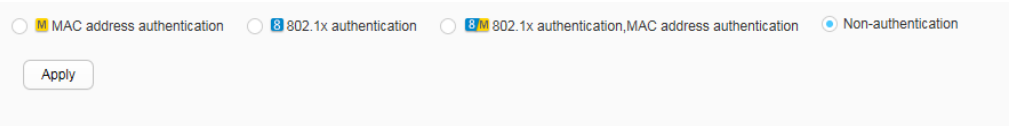
4. **인증 기능**을 **ON** 으로 설정 하고 확인을 **클릭** 합니다.

5. 인증 기능을 활성화해야 하는 인터페이스를 선택합니다. 필요에 따라 다음 작업을 수행할 수 있습니다.

   - 단일 인터페이스의 아이콘을 클릭하거나 여러 인터페이스의 아이콘을 클릭합니다.
   - 여러 인접 인터페이스를 선택하려면 마우스를 끕니다.
   - 장치 패널 이름을 클릭하고 모든 인터페이스를 선택합니다.

6. 그림 2 와 같이 인터페이스 인증 방법을 선택합니다.

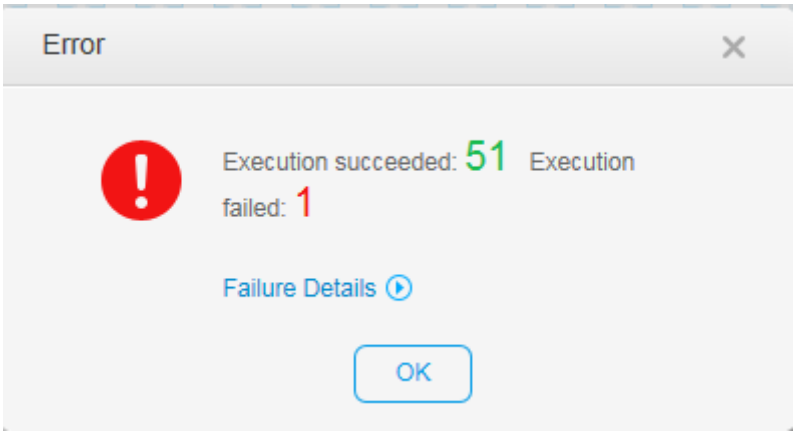
   그림 2 인터페이스 인증 모드



7. **적용**을 클릭합니다.

인터페이스에서 인증에 실패하면 그림 3 과 같이 오류 페이지가 표시됩니다.

그림 3 인터페이스 인증 활성화 결과

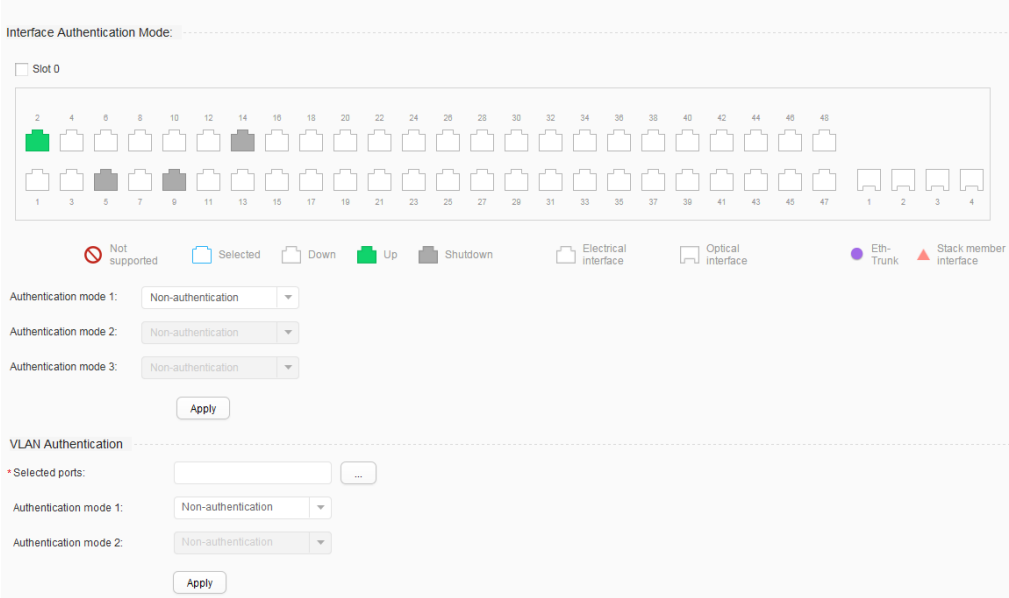


대화 상자에서 **실행 성공** 은 인터페이스 인증 기능이 성공적으로 적용된 인터페이스의 수를 나타냅니다. **Execution failed** 는 인터페이스 인증 기능이 적용되지 않은 인터페이스의 개수를 나타냅니다.

- 통합 모드.

1. **구성**을 클릭 하여 **구성** 페이지 를 표시합니다.
2. 탐색 트리에서 **보안 서비스** > **사용자 액세스 제어** 를 선택 하여 **사용자 액세스 제어** 페이지를 표시하십시오.
3. 그림 4 와 같이 **Access Configuration** 탭을 클릭하여 Access **Configuration** 페이지를 표시합니다.

그림 4 액세스 구성



4. 인증 기능을 활성화해야 하는 인터페이스를 선택합니다. 필요에 따라 다음 작업을 수행할 수 있습니다.

   - 단일 인터페이스의 아이콘을 클릭하거나 여러 인터페이스의 아이콘을 클릭합니다.
   - 여러 인접 인터페이스를 선택하려면 마우스를 끕니다.
   - 장치 패널 이름을 클릭하고 모든 인터페이스를 선택합니다.

5. **MAC 주소 인증**, **802.1X 인증** 및 **포털 인증**을 포함한 인터페이스 인증 모드를 선택합니다. **적용**을 클릭합니다.

> **NOTE**
>
> 802.1X 인증이 인증 모드 1 로 구성되고 MAC 주소 인증이 인증 모드 2 로 구성된 경우 MAC 주소 우회 인증 기능이 활성화됩니다.

MAC 주소 인증이 인증 모드 1 로 구성되고 802.1X 인증이 인증 모드 2 로 구성된 경우 MAC 주소 우회 인증 중에 MAC 주소 인증이 먼저 수행됩니다.

6. **VLAN 인증** 영역에서 ... 를 클릭하여 인터페이스를 추가하고 인터페이스 인증 모드를 선택한 다음 **적용**을 클릭합니다.

4.5.4.3 QoS 구성

4.5.4.3.1 포트 우선 순위

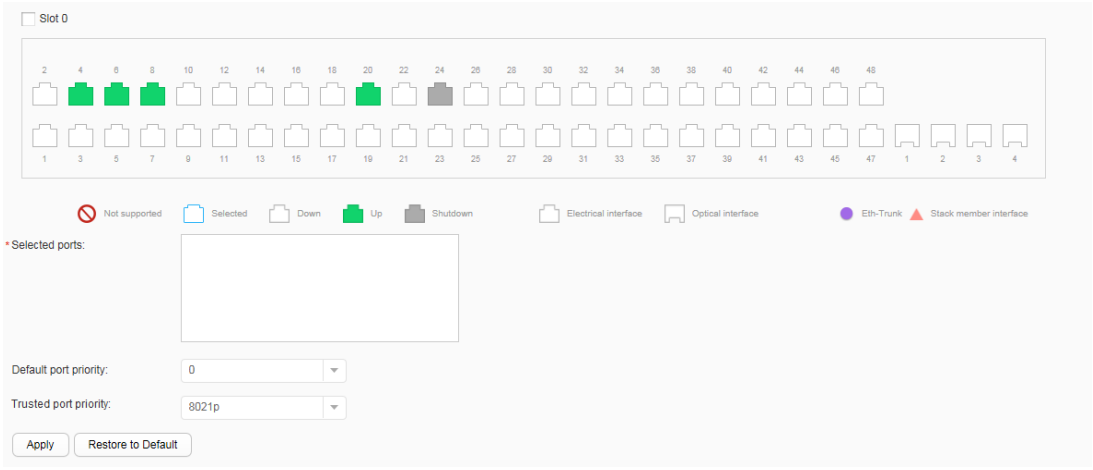
문맥

스위치는 패킷의 우선 순위 또는 인터페이스의 우선 순위에 따라 우선 순위 매핑을 수행합니다. 그런 다음 스위치는 패킷 우선 순위 또는 인터페이스의 우선 순위에 따라 수신된 패킷의 대기열 및 출력 우선 순위를 결정합니다. 이를 통해 스위치는 차별화된 서비스를 제공합니다.

절차

1. 그림 1 과 같이 **Configuration** > **Security Services** > **QoS Configuration** 을 선택하고 **Port Priority** 탭을 클릭합니다.

그림 1 포트 우선 순위



2. 구성할 포트를 선택합니다. 포트 영역에서 필요에 따라 다음 작업을 수행합니다.

   - 포트 아이콘을 클릭합니다. 포트 선택을 취소하려면 포트 아이콘을 다시 클릭합니다.
   - 커서를 끌어 배치에서 연속 포트를 선택합니다.
   - 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
   - 패널 이 있는 슬롯을 선택합니다. 패널의 모든 포트 가 선택됩니다.

3. **기본 포트 우선 순위** 드롭다운 목록 상자 에서 인터페이스 우선 순위를 선택합니다.

4. **신뢰할 수 있는 포트 우선 순위** 드롭다운 목록 상자 에서 신뢰할 수 있는 우선 순위를 선택합니다. 그런 다음 스위치는 우선 순위에 따라 패킷을 매핑합니다.

   - **8021p** : 스위치는 802.1p 우선 순위에 따라 패킷을 매핑합니다.
   - **8021p-inner** : 스위치는 내부 802.1p 우선 순위에 따라 패킷을 매핑합니다.
   - **8021p-outer** : 스위치는 외부 802.1p 우선 순위에 따라 패킷을 매핑합니다.

- **DSCP** : 스위치는 DSCP 우선 순위에 따라 패킷을 매핑합니다.
- **없음** : 스위치가 패킷 우선 순위를 신뢰하지 않습니다.

5. **Apply(적용)을 클릭**합니다.

4.5.4.3.2 혼잡 관리

문맥

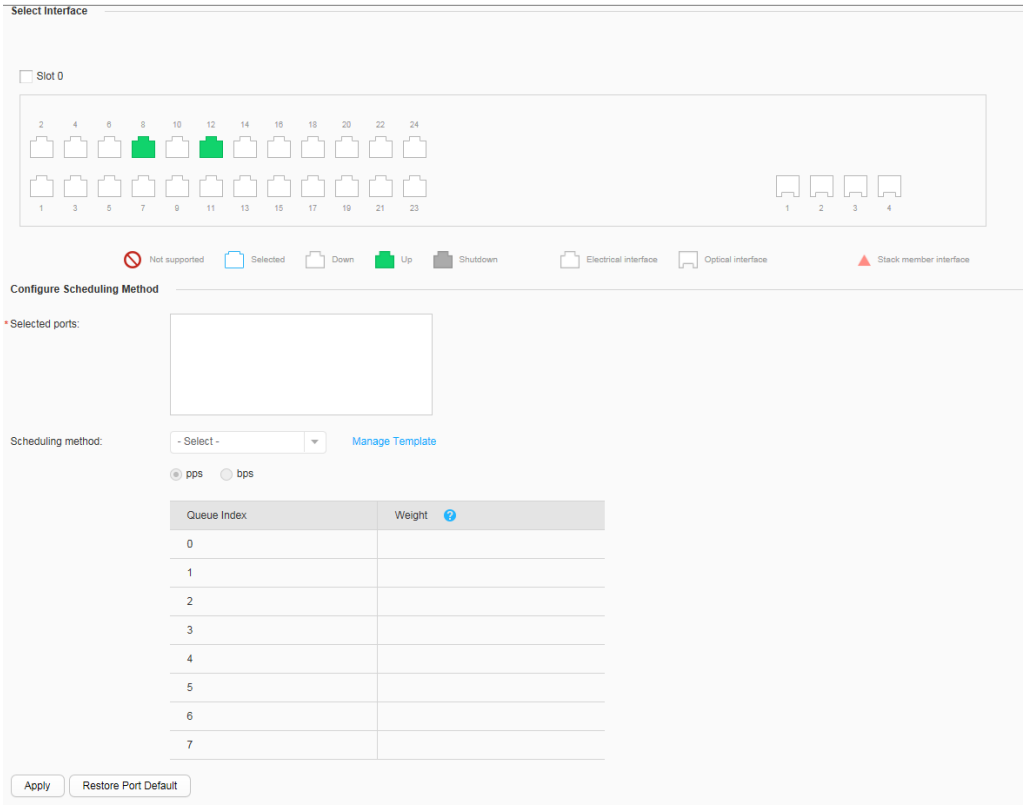
네트워크에서 혼잡이 발생하면 혼잡 관리로 구성된 스위치는 정의된 스케줄링 정책에 따라 패킷이 전달되는 순서를 결정하고 우선 순위가 높은 패킷이 우선적으로 스케줄링되도록 합니다.

절차

1. 그림 1 과 같이 **Configuration** > **Security Services** > **QoS**

   Configuration 을 선택하고 **Congestion Management** 탭을 클릭합니다.

그림 1 혼잡 관리



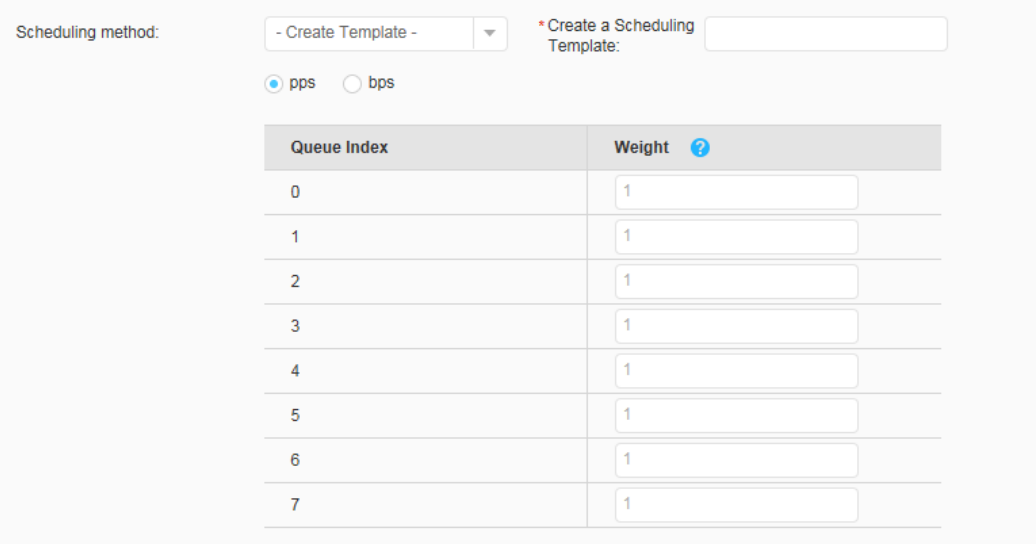
2. 구성할 포트를 선택합니다. 포트 영역에서 필요에 따라 다음 작업을 수행합니다.

   - 포트 아이콘을 클릭합니다. 포트 선택을 취소하려면 포트 아이콘을 다시 클릭합니다.
   - 커서를 끌어 배치에서 연속 포트를 선택합니다.
   - 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
   - 패널 이 있는 슬롯을 선택합니다. 패널의 모든 포트 가 선택됩니다.

3. **Scheduling 메소드**의 인터페이스에서 대기열 스케줄링 모드를 구성하십시오.

   a. 그림 2 와 같이 드롭다운 목록 상자에서 **템플릿 만들기를** 선택 합니다.

그림 2 템플릿 생성



b. 일정 템플릿 **만들기 에 일정 템플릿**의 이름을 입력합니다.

c. 인터페이스 대기열의 스케줄링 모드를 선택합니다.

- **pps** : WRR 스케줄링을 나타냅니다.
- **bps** : WDRR 스케줄링을 나타냅니다.

d. 각 대기열의 가중치를 설정합니다.

NOTE

큐의 가중치가 0 으로 설정되면 큐는 PQ 스케줄링을 사용합니다. 이 경우 PQ+WRR 또는 PQ+WDRR 이 사용됩니다.

4. **Apply(적용)을 클릭**합니다.

4.5.4.3.3 속도 제한 및 형성

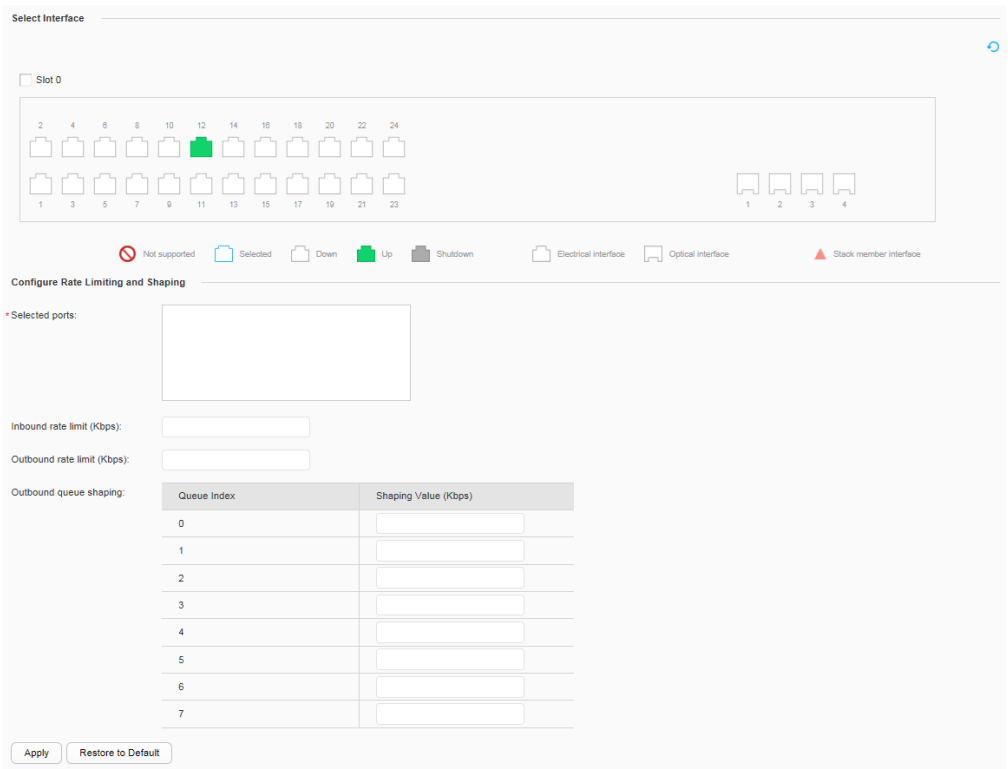
문맥

인터페이스 기반 속도 제한은 대역폭이 허용 범위 내에 있도록 인터페이스를 통과하는 모든 패킷의 속도를 제한합니다. 인터페이스에서 수신된 패킷은 우선 순위 매핑에 따라 다른 대기열에 들어갑니다. 스위치는 우선 순위가 다른 대기열에 대해 서로 다른 트래픽 형성 매개변수를 설정하여 차별화된 서비스를 제공합니다.

절차

1. 그림 1 과 같이 **Configuration** > **Security Services** > **QoS Configuration** 을 선택하고 **Rate Limiting And Shaping** 탭을 클릭합니다.

그림 1 속도 제한 및 형성 페이지



2. 구성할 포트를 선택합니다. 포트 영역에서 필요에 따라 다음 작업을 수행합니다.

- 포트 아이콘을 클릭합니다. 포트 선택을 취소하려면 포트 아이콘을 다시 클릭합니다.
- 커서를 끌어 배치에서 연속 포트를 선택합니다.
- 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
- 패널 이 있는 슬롯을 선택합니다. 패널 의 모든 포트 가 선택됩니다.

3. **인바운드 속도 제한(Kbps)** 및 **아웃바운드 속도 제한(Kbps)을** 설정합니다.

   값의 범위는 64 에서 1000000 입니다.

4. **아웃바운드 대기열 형성** 에서 대기열 인덱스 ID 에 해당하는 트래픽 형성 값을 설정합니다.

   값의 범위는 64 에서 1000000 입니다.

5. **적용**을 클릭합니다.

4.5.4.4 IP 보안

4.5.4.4.1 DHCP 스누핑

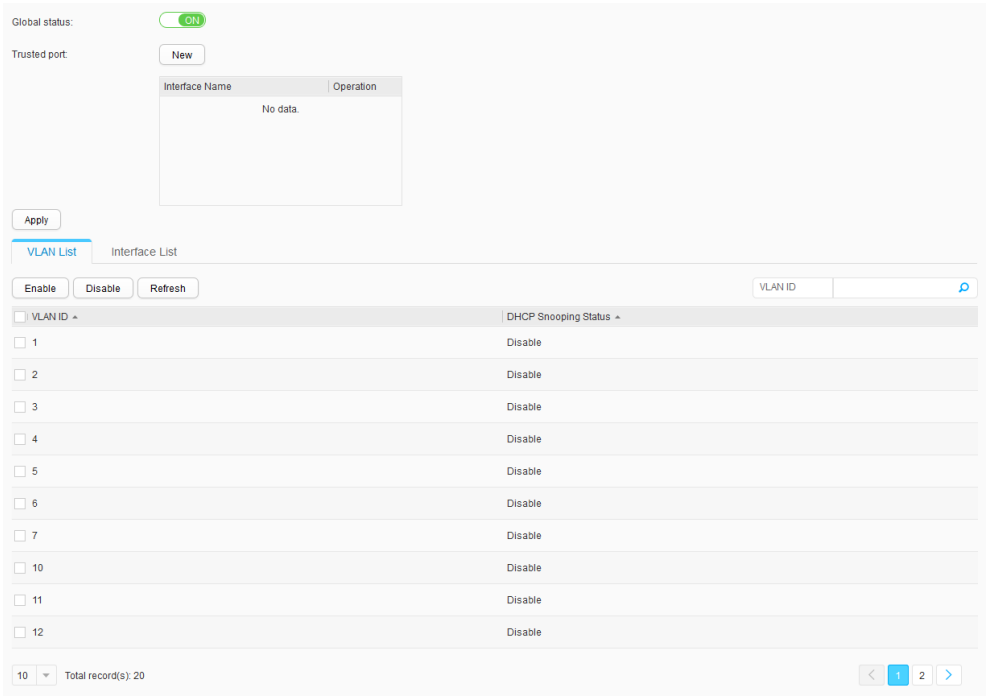
문맥

DHCP 스누핑을 통해 클라이언트는 승인된 DHCP 서버에서 IP 주소를 얻을 수 있습니다. DHCP 스누핑이 활성화된 장치는 DHCP 클라이언트의 IP 및 MAC 주소를 기반으로 바인딩 항목을 생성할 수 있습니다.

절차

1. 그림 1 과 같이 **Configuration** > **Security Services** > **IP Security** 를 선택 하고 **DHCP Snooping** 탭을 클릭합니다.

   그림 1 DHCP 스누핑 구성



2. DHCP 스누핑을 전역적으로 활성화하려면 **전역 상태** 를 켜십시오.

   기본적으로 DHCP 스누핑은 전역적으로 활성화되어 있지 않습니다.

3. **새로 만들기**를 클릭하고 표시된 대화 상자에서 신뢰할 수 있는 인터페이스를 선택합니다.

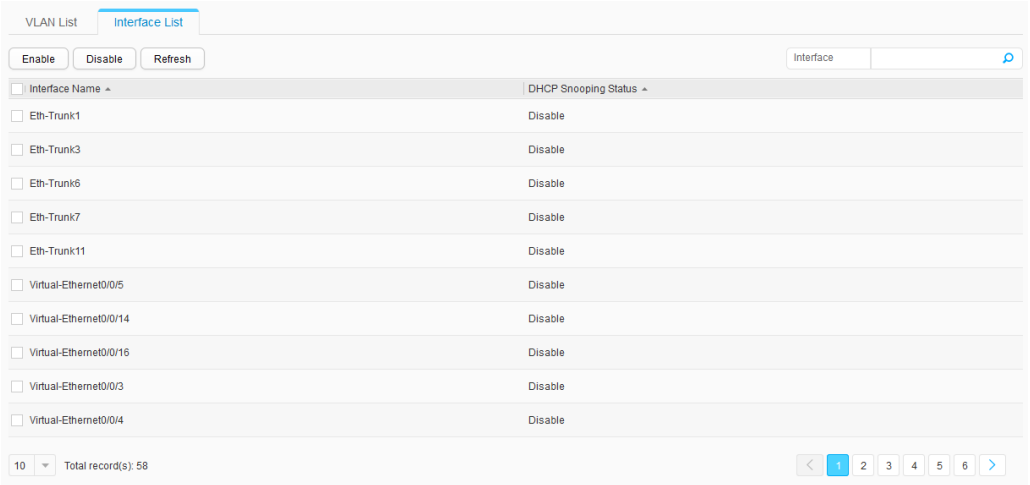
4. **적용**을 클릭하여 선택한 인터페이스를 신뢰할 수 있는 인터페이스로 구성합니다.

5. **VLAN 목록**에서 레코드를 클릭하여 DHCP 스누핑 상태를 편집합니다. **DHCP 스누핑 상태**를 켜고 ✔를 클릭하여 구성을 완료합니다.

> **NOTE**
>
> 여러 레코드를 선택하고 **활성화** 또는 **비활성화**를 클릭하여 DHCP 스누핑 상태를 일괄적으로 설정할 수도 있습니다.

6. 그림 2 와 같이 **Configuration** > **Security Services** > **IP Security** > **DHCP Snooping** 을 선택 하고 **Interface List** 탭을 클릭합니다.

그림 2 인터페이스 목록 탭 페이지



7. **Interface List** (인터페이스 목록) 탭 페이지에서 인터페이스를 선택하고 DHCP 스누핑 상태를 편집합니다. **DHCP 스누핑 상태** 를 켜고 ✔를 클릭하여 구성을 완료합니다.

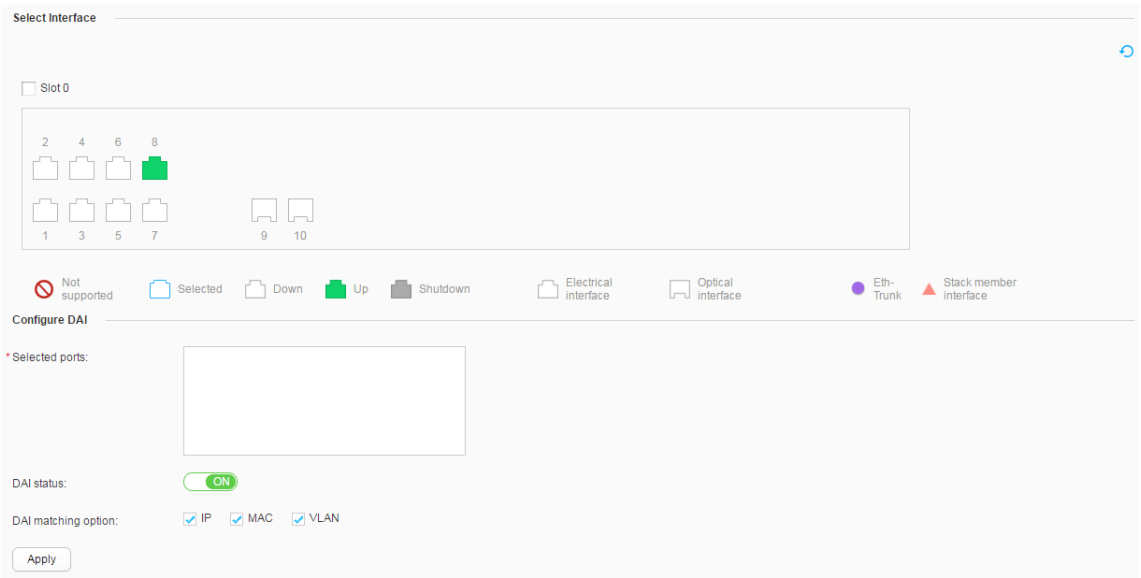
4.5.4.4.2 DAI

절차

1. 그림 1 과 같이 **Configuration** > **Security Services** > **IP**

   Security 를 선택하고 **DAI** 탭을 클릭합니다.

   그림 1 DAI 구성



2. 구성할 포트를 선택합니다. 포트 영역에서 필요에 따라 다음 작업을 수행합니다.

   - 포트 아이콘을 클릭합니다. 포트 선택을 취소하려면 포트 아이콘을 다시 클릭합니다.
   - 커서를 끌어 배치에서 연속 포트를 선택합니다.
   - 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
   - 패널 이 있는 슬롯을 선택합니다. 패널의 모든 포트 가 선택됩니다.

3. **DAI 상태를** 켭니다.

4. **DAI 매칭 옵션** 에서 ARP 패킷 체크 항목을 **선택** 합니다.

5. **Apply(적용)을 클릭**하여 구성을 완료합니다.

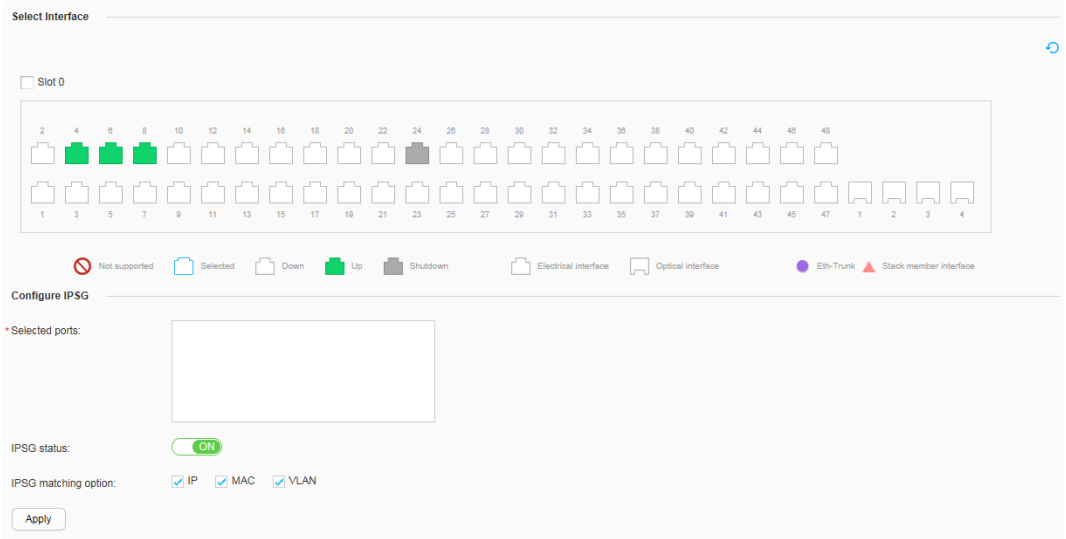
4.5.4.4.3 IPSG

절차

1. 그림 1 과 같이 **Configuration** > **Security Services** > **IP**

   Security 를 선택하고 **IPSG** 탭을 클릭합니다.

   그림 1 IPSG 구성



2. 구성할 포트를 선택합니다. 포트 영역에서 필요에 따라 다음 작업을 수행합니다.

   - 포트 아이콘을 클릭합니다. 포트 선택을 취소하려면 포트 아이콘을 다시 클릭합니다.
   - 커서를 끌어 배치에서 연속 포트를 선택합니다.

- 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
- 패널 이 있는 슬롯을 선택합니다. 패널의 모든 포트 가 선택됩니다.

3. **IPSG 상태를** 켭니다.
4. **IPSG 매칭 옵션**에서 IP 패킷 체크 항목을 선택합니다.
5. **Apply(적용)**을 클릭하여 구성을 완료합니다.

4.5.4.4.4 정적 바인딩 테이블

문맥

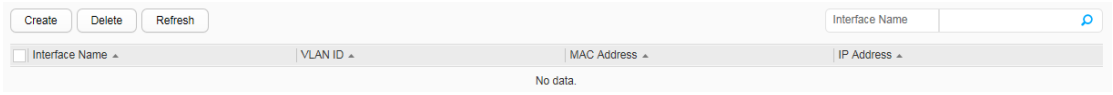
정적 바인딩 테이블을 기반으로 하는 IPSG 는 신뢰할 수 없는 인터페이스에서 수신한 IP 패킷을 필터링하여 훔친 IP 주소를 사용하는 악의적인 호스트의 네트워크 액세스를 방지합니다.

절차

- 정적 바인딩 항목을 만듭니다.

1. 그림 1 과 같이 **Configuration** > **Security Services** > **IP Security** 를 선택 하고 **Static Binding Table** 탭을 클릭합니다.

그림 1 정적 바인딩 테이블



2. **만들기** 를 클릭하여 그림 2 와 같이 **Bing 항목 만들기** 페이지를 엽니다.

그림 2 Binging 항목 만들기

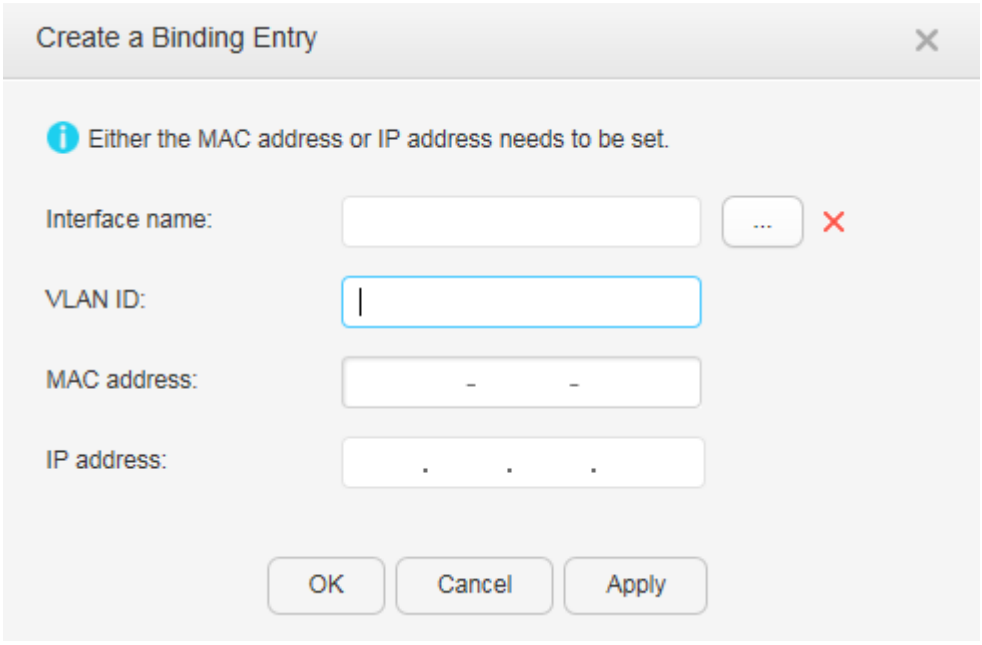


표 1 은 표시된 페이지의 매개변수를 설명합니다.

표 1 Bing 항목 만들기

매개변수	설명
인터페이스 이름	사용자에게 연결된 인터페이스를 나타냅니다.
VLAN ID	사용자 VLAN 의 ID 를 지정합니다. 값 범위는 1~4094 입니다.
MAC 주소	사용자의 MAC 주소를 나타냅니다.
IP 주소	사용자의 고정 IP 주소를 지정합니다.

3. 필요한 매개변수를 설정합니다.

4. **확인**을 클릭합니다.

- 정적 바인딩 항목을 삭제합니다.

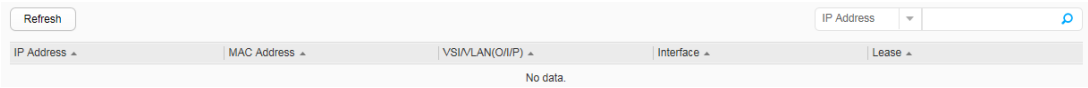
1. 그림 1 과 같이 **Configuration** > **Security Services** > **IP Security** 를 선택 하고 **Static Binding Table** 탭을 클릭합니다.
2. 삭제할 레코드를 선택하고 **삭제**를 클릭합니다. 시스템에서 레코드 삭제 여부를 묻습니다.
3. **확인**을 클릭합니다.

4.5.4.4.5 동적 바인딩 테이블

절차

1. 그림 1 과 같이 **Configuration** > **Security Services** > **IP Security** 를 선택하고 **Dynamic Binding Table** 탭을 클릭합니다.

그림 1 동적 바인딩 테이블



2. **새로 고침**을 클릭하여 동적 바인딩 항목을 업데이트합니다.

4.5.4.4.6 원 클릭 바인딩

문맥

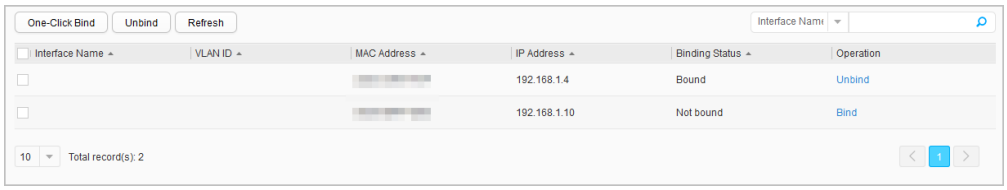
원 클릭 바인딩이 구성된 후 스위치는 ARP 항목 정보를 기반으로 정적 사용자 바인딩 항목을 생성할 수 있습니다. 이 기능은 사용자 정적 바인딩 항목 생성의 효율성을 향상시킵니다.

절차

- ARP 항목 정보를 기반으로 정적 사용자 바인딩 항목을 구성합니다.

  1. **구성** > **보안 서비스** > **IP 보안** > **원 클릭 바인딩을** 선택 합니다. 그림 1 과 같이 **원 클릭 바인딩** 페이지가 표시됩니다.

     그림 1 원 클릭 바인딩

  2. ARP 항목을 기반으로 하나의 정적 사용자 바인딩 항목을 바인딩하려면 바인딩을 클릭합니다. ARP 항목을 기반으로 여러 정적 사용자 바인딩 항목을 바인딩하려면 바인딩할 항목을 선택하고 **원 클릭 바인딩을** 클릭합니다.

- ARP 항목을 기반으로 생성된 사용자 정적 바인딩 항목을 삭제합니다.

  1. **구성** > **보안 서비스** > **IP 보안** > **원 클릭 바인딩을** 선택합니다. 그림 1 과 같이 **원 클릭 바인딩** 페이지가 표시됩니다.

2. 하나의 정적 사용자 바인딩 항목을 바인딩 해제하려면 바인딩 해제를 클릭합니다. 여러 정적 사용자 바인딩 항목을 바인딩 해제하려면 바인딩 해제할 항목을 선택하고 **원 클릭 바인딩 해제**를 클릭합니다.

4.5.4.5 폭풍 통제

4.5.4.5.1 폭풍 억제

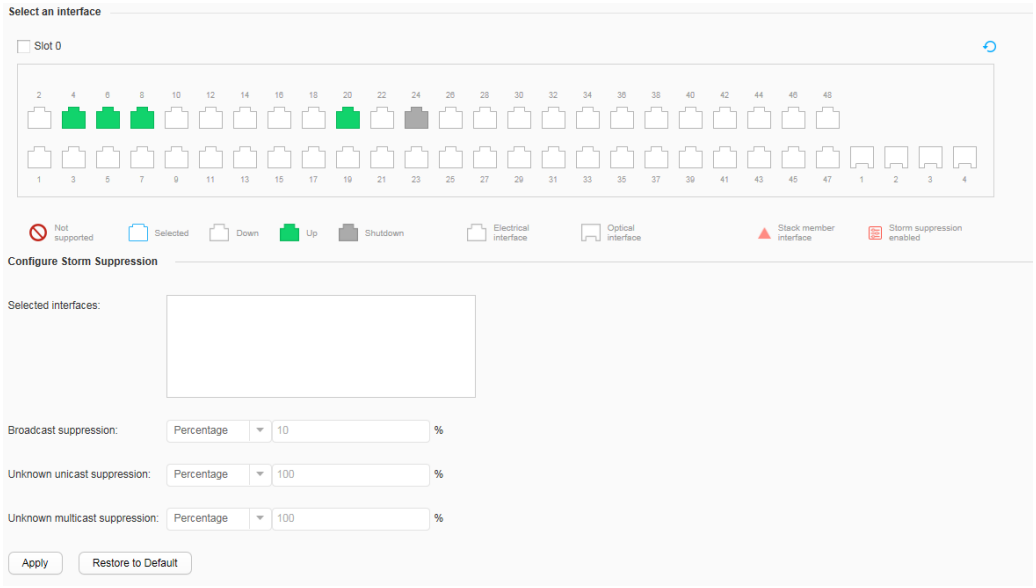
문맥

인바운드 및 아웃바운드 인터페이스의 과도한 브로드캐스트, 알 수 없는 멀티캐스트 및 알 수 없는 유니캐스트 패킷은 브로드캐스트 스톰을 유발합니다. 브로드캐스트 스톰을 방지하려면 인터페이스에서 해당 유형의 패킷에 대한 억제를 구성하십시오.

절차

1. 그림 1 과 같이 **Configuration** > **Security Services** > **Storm Control** 을 선택하고 **Storm Suppression** 탭을 클릭합니다.

그림 1 폭풍 진압



2. 구성할 포트를 선택합니다. 포트 영역에서 필요에 따라 다음 작업을 수행합니다.

   - 포트 아이콘을 클릭합니다. 포트 선택을 취소하려면 포트 아이콘을 다시 클릭합니다.
   - 커서를 끌어 배치에서 연속 포트를 선택합니다.
   - 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
   - 패널 이 있는 슬롯을 선택합니다. 패널의 모든 포트 가 선택됩니다.

3. 인터페이스에서 브로드캐스트 패킷에 대한 속도 제한을 설정하려면 **브로드캐스트 억제** 에서 매개변수를 설정합니다.

4. 인터페이스에서 **알 수 없는 유니** 캐스트 패킷에 대한 속도 제한을 설정하려면 **알 수 없는 유니캐스트 억제** 에서 매개변수를 설정합니다.

5. 인터페이스에서 **알 수 없는 멀티** 캐스트 패킷에 대한 속도 제한을 설정하려면 **알 수 없는 멀티캐스트 억제** 에서 매개변수를 설정합니다.

6. **Apply(적용)을 클릭**하여 구성을 완료합니다.

4.5.4.5.2 폭풍 제어

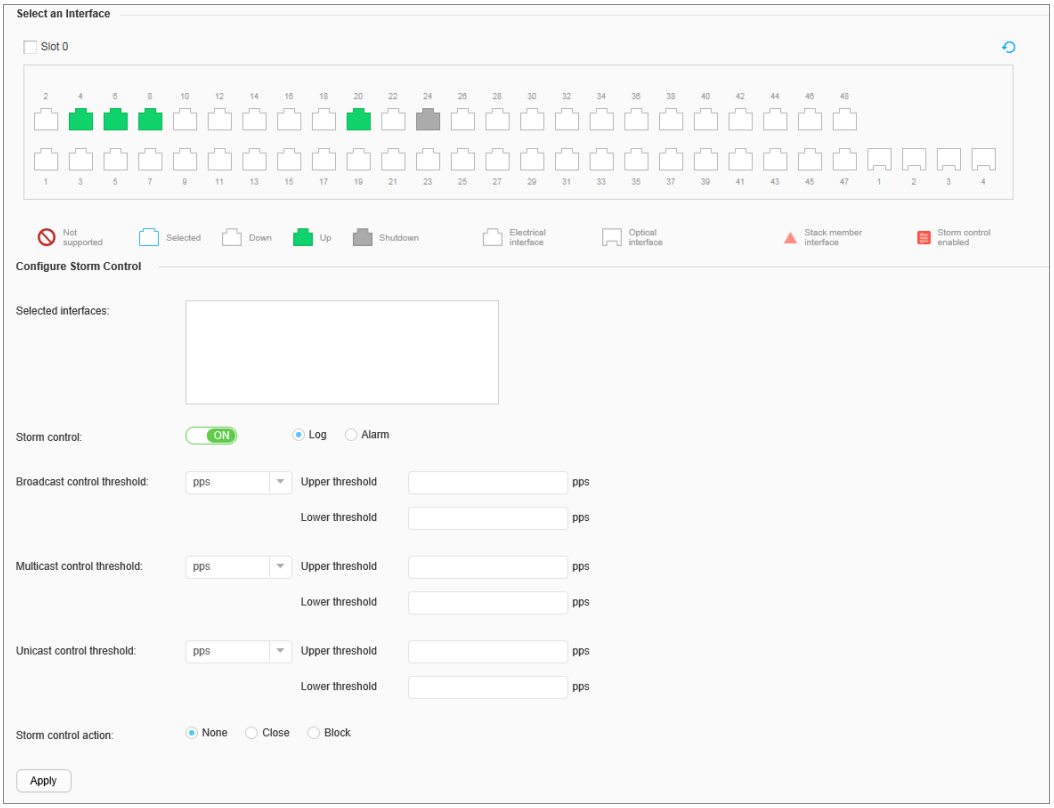
문맥

인바운드 인터페이스에서 브로드캐스트, 알 수 없는 멀티캐스트 또는 알 수 없는 유니캐스트 패킷의 비율을 제한하고 장치에서 과도한 트래픽을 방지하려면 인바운드 인터페이스에서 해당 패킷 유형에 대한 폭풍 제어를 구성하십시오.

절차

1. 그림 1 과 같이 **Configuration** > **Security Services** > **Storm Control** 을 선택하고 **Storm Control** 탭을 클릭합니다.

그림 1 폭풍 제어



2. 구성할 포트를 선택합니다. 포트 영역에서 필요에 따라 다음 작업을 수행합니다.

- 포트 아이콘을 클릭합니다. 포트 선택을 취소하려면 포트 아이콘을 다시 클릭합니다.
- 커서를 끌어 배치에서 연속 포트를 선택합니다.
- 여러 포트 아이콘을 클릭하여 이러한 포트를 선택하고 포트 아이콘을 다시 클릭하여 포트 선택을 취소합니다.
- 패널 이 있는 슬롯을 선택합니다. 패널의 모든 포트 가 선택됩니다.

3. **폭풍 제어를** 켜고 **폭풍 제어에** 대한 로그 또는 경보를 활성화합니다.

기본적으로 폭풍우 제어에 대한 로그 및 알람은 비활성화되어 있습니다.

4. **브로드캐스트 제어 임계값** 에서 선택한 인터페이스에서 수신된 브로드캐스트 패킷에 대한 스톰 제어를 구성 합니다.

- **상한 임계값** : pps, 바이트 또는 백분율 모드에서 상한을 지정합니다.
- **하한 임계값** : pps, 바이트 또는 백분율 모드에서 하한을 지정합니다.

5. **멀티캐스트 제어 임계값** 에서 선택한 인터페이스에서 수신된 알 수 없는 멀티캐스트 패킷에 대한 폭풍 제어를 구성 합니다.

- **상한 임계값** : pps, 바이트 또는 백분율 모드에서 상한을 지정합니다.
- **하한 임계값** : pps, 바이트 또는 백분율 모드에서 하한을 지정합니다.

6. **Unicast 제어 임계값** 에서 선택한 인터페이스에서 수신된 알 수 없는 유니캐스트 패킷에 대한 폭풍 제어를 구성 합니다.

- **상한 임계값** : pps, 바이트 또는 백분율 모드에서 상한을 지정합니다.
- **하한 임계값** : pps, 바이트 또는 백분율 모드에서 하한을 지정합니다.

7. 폭풍우 통제 동작에서 **폭풍우 통제 동작을** 설정합니다.

- **없음** : 폭풍우 제어 조치가 구성되지 않았음을 나타냅니다.
- **비활성화** : 인터페이스를 종료함을 나타냅니다.
- **차단** : 패킷을 폐기함을 나타냅니다.

8. **Apply(적용)을 클릭**하여 구성을 완료합니다.

4.5.4.6 포트 격리

4.5.4.6.1 양방향 격리

절차

- 양방향 격리를 만듭니다.

    1. **Configuration(구성) > 보안 서비스 > 포트 격리를** 선택하고 **양방향 격리** 탭을 클릭합니다.

    2. 그림 1 과 같이 **Create** 를 클릭하여 양방향 격리를 생성 합니다.

        그림 1 양방향 격리 생성

    3. **인터페이스 선택을** 클릭하여 양방향 격리를 구성해야 하는 **인터페이스**를 선택하고 **Ok(확인)을 클릭합니다.**

    4. ✔를 클릭하여 구성을 완료합니다.

- 양방향 격리를 삭제합니다.

    1. **Configuration(구성) > 보안 서비스 > 포트 격리를** 선택하고 **양방향 격리** 탭을 클릭합니다.

2. 삭제하고 클릭합니다하는 격리 그룹 선택 **삭제를** . 시스템에서 그룹을 삭제할지 여부를 묻습니다.

3. Ok(확인)을 클릭합니다.

4.5.4.6.2 단방향 격리

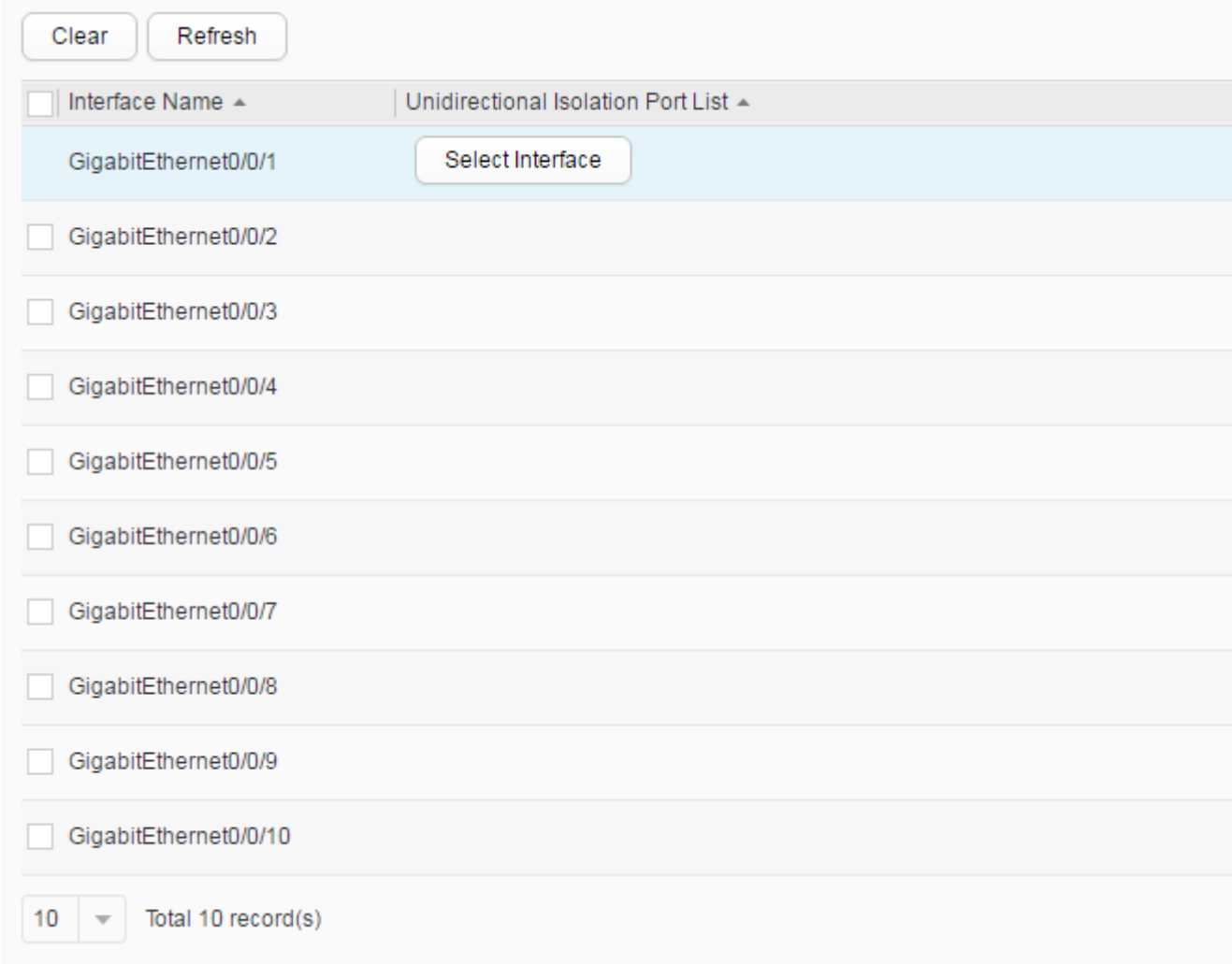
절차

- 단방향 격리를 만듭니다.

1. **구성** > **보안 서비스** > **포트 격리** 를 선택 하고 **단방향 격리** 탭을 클릭합니다.

2. 필요한 인터페이스의 기록을 클릭합니다. **Select Interface** 버튼은 그림 1 과 같이 **Interface Name** 열 에서 사용할 수 있습니다.

그림 1 단방향 격리 생성



3. **인터페이스 선택**을 클릭하여 단방향 격리를 구성해야 하는 인터페이스를 선택하고 **확인**을 클릭합니다.

4. ✔를 클릭하여 구성을 완료합니다.

- 단방향 격리를 삭제합니다.

1. **구성** > **보안 서비스** > **포트 격리** 를 선택 하고 **단방향 격리** 탭을 클릭합니다

2. 삭제할 데이터를 선택하고 **지우기**를 클릭합니다. 시스템에서 그룹을 삭제할지 여부를 묻습니다.

3. **확인**을 클릭합니다.

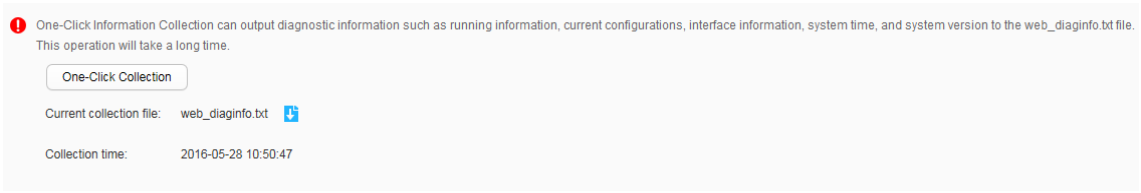
4.5.5 진단

4.5.5.1 원 클릭 정보 수집

절차

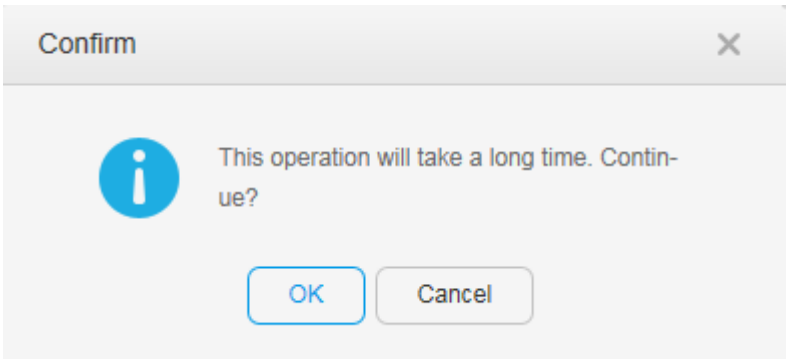
1. **진단** > **원 클릭 정보 수집**을 선택하여 그림 1 과 같이 **원 클릭 정보 수집** 페이지에 액세스합니다.

그림 1 원클릭 정보 수집



2. 원 클릭 **컬렉션**을 클릭합니다. 시스템은 그림 2 와 같이 계속할지 여부를 묻는 메시지를 표시합니다. **확인**을 클릭합니다.

그림 2 확인



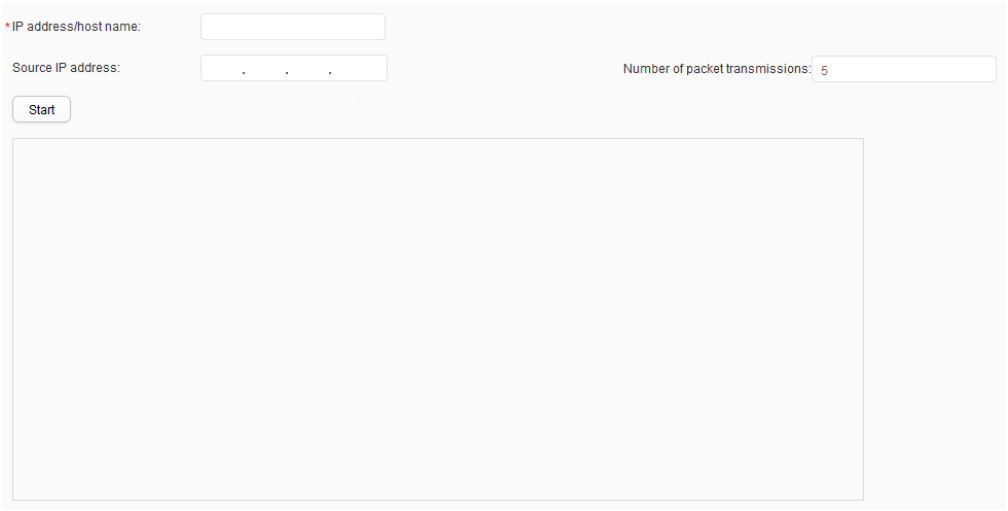
3. 정보 수집이 완료되면 시스템은 작업이 성공했음을 나타내는 메시지를 표시합니다. **확인**을 클릭하고 아이콘을 클릭하여 파일을 다운로드합니다.

4.5.5.2 핑

절차

1. 그림 1 과 같이 **진단** > **Ping** 을 선택 하여 **Ping** 페이지 에 액세스합니다.

그림 1 핑



2. **IP 주소/호스트 이름** , **소스 IP 주소** , **패킷 전송 횟수를 설정** 하고 **시작**을 클릭합니다. 네트워크 연결 정보가 표시됩니다.

NOTE

시간 초과 간격 내에 응답 패킷이 수신되지 않으면 다음 정보가 표시됩니다. **요청 시간 초과** . 앞의 정보는 링크에 결함이 있음을 보여줍니다.

4.5.5.3 경로 추적

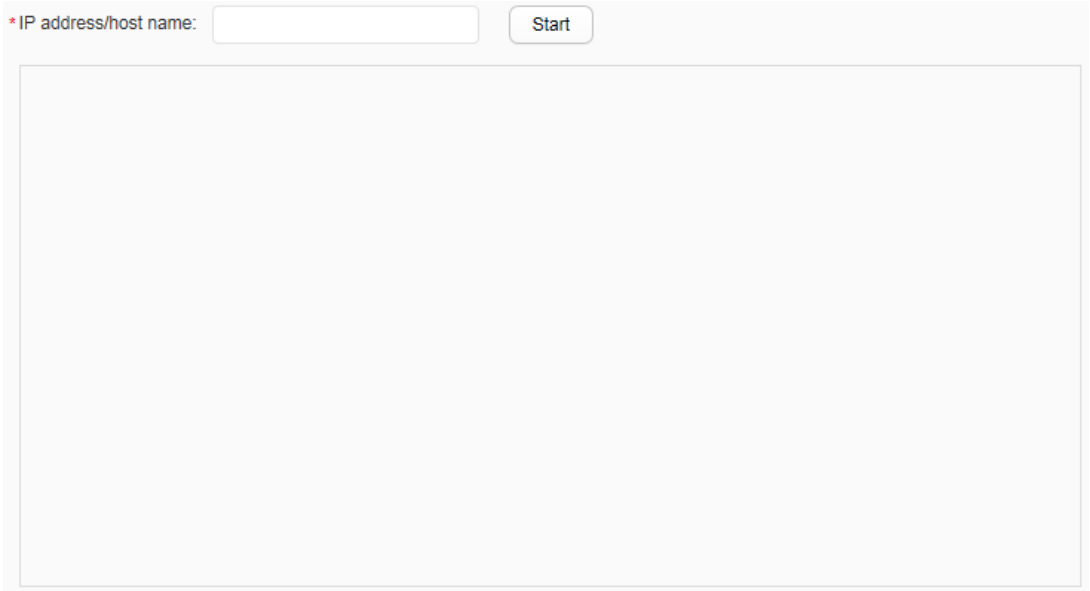
문맥

Trace Route 라고도 하는 **Tracert** 명령을 사용하면 IP 주소와 소스와 대상 간의 게이트웨이 수를 확인할 수 있습니다. Tracert 는 네트워크 연결을 확인하고 네트워크 오류를 찾는 데 사용됩니다.

절차

1. 그림 1 과 같이 **진단** > **경로 추적을** 선택하여 **경로 추적** 페이지 에 액세스합니다.

그림 1 추적 경로



2. **경로 추적** 텍스트 상자 에 IP 주소를 입력하고 **시작을** 클릭합니다. 패킷이 소스 호스트와 대상 호스트 사이를 통과하는 레이어 3 장치가 표시됩니다.

NOTE

- **tracert** 명령의 출력 에는 패킷이 대상에 도달하는 모든 게이트웨이의 IP 주소가 포함됩니다. 하나의 게이트웨이가 TTL 타임아웃을 나타내는 패킷을 되돌려 보내면 * 가 표시됩니다.
- 추적 테스트는 시간이 오래 걸릴 수 있습니다.

4.5.5.4 AAA 테스트

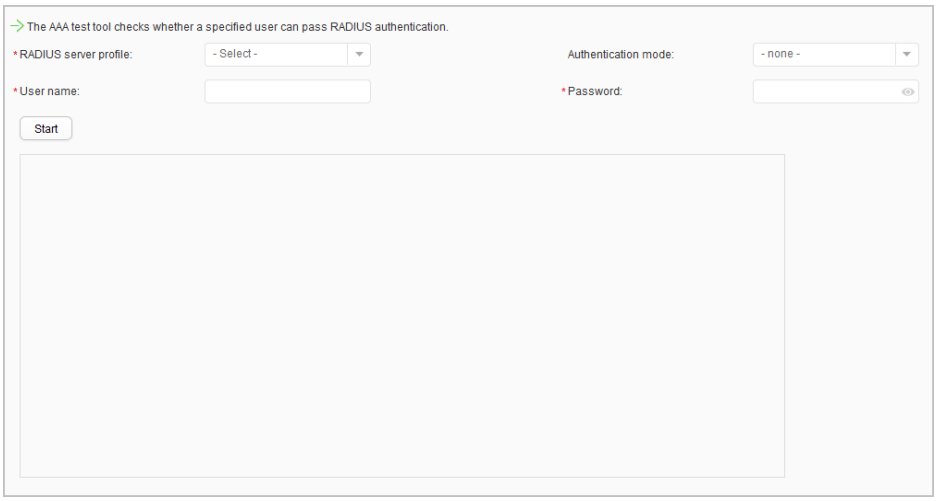
문맥

AAA 테스트 도구는 지정된 사용자가 RADIUS 인증을 통과할 수 있는지 여부를 확인합니다.

절차

1. 그림 1 과 같이 **진단** > **AAA 테스트**를 선택하여 **AAA 테스트** 페이지 에 액세스합니다.

그림 1 AAA 테스트



2. RADIUS 서버 프로필, 인증 모드, 사용자 이름 및 암호와 같은 매개변수를 입력합니다. 매개변수 정보는 표 1 을 참조하십시오.

표 1 AAA 테스트 매개변수

매개변수	설명
RADIUS 서버 프로필	인증에 사용되는 RADIUS 서버 템플릿입니다.
인증 모드	인증에 사용되는 인증 모드입니다.
사용자 이름	테스트할 사용자의 사용자 이름입니다.
비밀번호	테스트할 사용자의 비밀번호입니다.

3. **시작을** 클릭합니다.

AAA 테스트가 수행된 후 테스트 결과가 표시됩니다.

4.5.6 시스템 유지관리

4.5.5.1 재부팅

문맥

다음 시작을 위해 시스템 소프트웨어, 구성 파일 및 패치 파일을 지정한 후 파일을 적용하려면 장치를 다시 시작해야 합니다. 웹 시스템은 즉시 다시 시작과 시간 지정 다시 시작이라는 두 가지 다시 시작 모드를 제공합니다. 장치를 다시 시작하면 서비스가 중단됩니다. 따라서 장치가 유휴 상태일 때 장치를

다시 시작해야 합니다. 장치가 현재 유휴 상태이면 즉시 장치를 다시 시작하십시오. 장치가 서비스를 처리 중이면 장치가 유휴 상태일 때 예약된 시간에 장치를 다시 시작하십시오.

NOTICE

장치를 다시 시작하기 전에 현재 구성을 저장하는 것이 좋습니다. 그렇지 않으면 구성이 손실될 수 있습니다.

시스템 소프트웨어 및 구성 파일은 참조용입니다. 실제 출력 정보는 앞의 정보와 다를 수 있습니다.

절차

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 재부팅**을 선택하여 **재부팅** 페이지 에 액세스합니다.

그림 1 재부팅

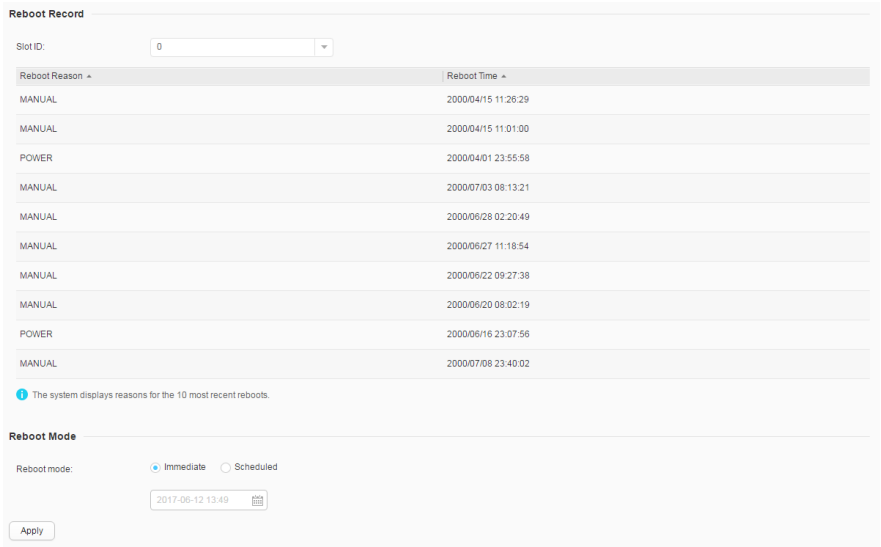


표 1 은 페이지의 매개변수를 설명합니다.

표 1 재부팅 페이지의 매개변수

안건	설명
재부팅 기록	슬롯 ID 드롭다운 목록에서 슬롯 ID 를 선택하여 재부팅 레코드를 표시합니다.
재부팅 모드	재시작 모드를 나타냅니다. 장치는 즉시 다시 시작 및 예약된 다시 시작을 지원합니다. **노트:** 시간은 현재 시간 이후 720 시간을 초과할 수 없습니다. 스위치가 NETCONF 모드에 있는 경우 장치는 예약된 다시 시작을 지원하지 않습니다.

1. **재부팅 모드** 섹션에서 다시 시작 모드를 선택하고 적용을 클릭합니다. **즉시**를 선택 하면 구성을 저장할 것인지 묻는 메시지가 표시됩니다. **저장 및 재부팅**을 클릭하면 장치가 즉시 다시 시작되고 웹 연결이 종료됩니다. **예약됨**을 선택한 경우 특정 다시 시작 시간을 입력합니다. 장치는 지정된 시간에 다시 시작됩니다.

6.5.5.2 업그레이드

문맥

장치의 시스템 소프트웨어를 업그레이드하려면 업그레이드 파일을 장치에 업로드하고 다음 시작을 위한 파일을 지정하고 장치를 다시 시작하여 업그레이드 파일이 적용되도록 해야 합니다. 웹 시스템을 사용하면 GUI 에서 시스템 소프트웨어를 업그레이드하여 업그레이드 작업을 단순화하고 효율성을 높일 수 있습니다.

NOTICE

- 시스템 소프트웨어를 업그레이드하기 전에 구성이 저장되었는지 확인하십시오.
- 업그레이드하는 동안 장치의 전원을 끄지 마십시오.
- 시스템 소프트웨어를 장치에 업로드하는 데 시간이 오래 걸립니다. 따라서 시스템 소프트웨어를 업그레이드하기 전에 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 시스템 > 시스템 정보를 선택하고 HTTP 시간 초과 간격(분)**을 60 분으로 설정하십시오.
- 시스템 소프트웨어 및 구성 파일은 참조용입니다. 실제 출력 정보는 앞의 정보와 다를 수 있습니다.

절차

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 업그레이드**를 선택하여 **업그레이드** 페이지 에 액세스합니다.

그림 1 업그레이드

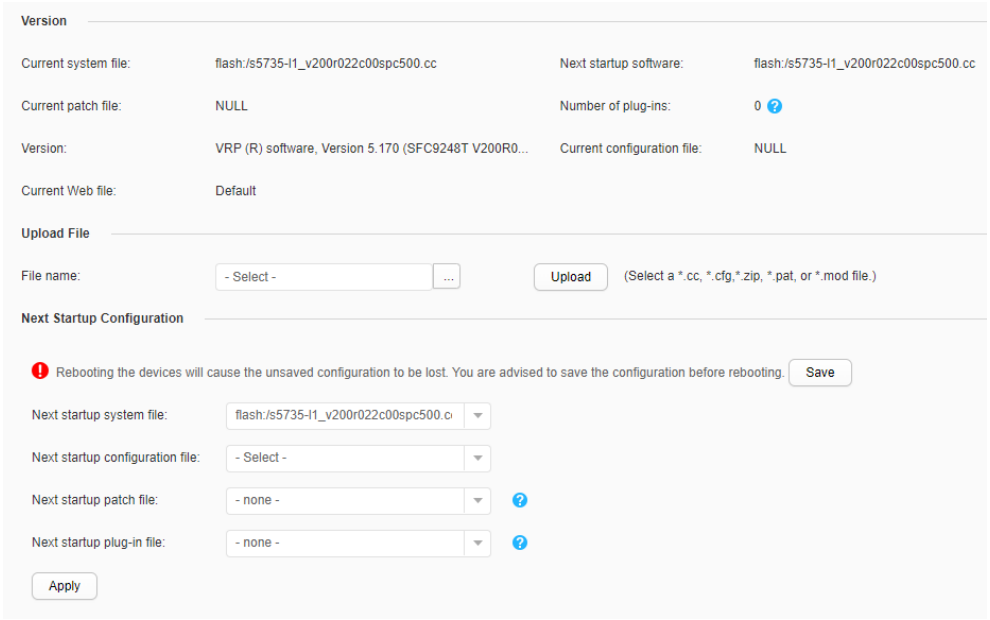


표 1 은 표시된 페이지의 구성 항목을 설명합니다.

표 1 업그레이드 페이지

안건	설명
버전	현재 시스템 파일, 다음 시작 소프트웨어, 현재 패치 파일 및 현재 웹 파일과 같은 시스템 파일에 대한 정보가 페이지에 표시됩니다.
파일 업로드	업로드할 파일을 선택합니다.
다음 시작 구성	선택한 **다음 시작 시스템 파일**, **다음 시작 구성 파일** 및 **다음 시작 패치 파일** 드롭 다운 목록에서합니다. **노트:** 장치가 플러그인을 지원하는 경우 드롭다운 목록에서 다음 시작을 위한 플러그인 파일을 선택합니다. 스위치가 NETCONF 모드인 경우 구성 파일을 저장할 수 없으며 다음 시작을 위한 구성 파일을 설정할 수 없습니다.

2. **파일 업로드** 옵션을 클릭합니다. 업그레이드 파일을 선택하고 **업로드**를 클릭하여 파일을 업로드합니다.

3. **다음 시작 구성** 옵션의 드롭다운 목록에서 다음 시작을 위한 파일을 선택하고 **저장**을 클릭합니다.

4. **Apply(적용)**을 클릭합니다.

6.5.5.3 웹 파일 관리

절차

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 웹 파일 관리** 를 선택 하여 **웹 파일 관리** 페이지 에 액세스합니다.

그림 1 웹 파일 관리

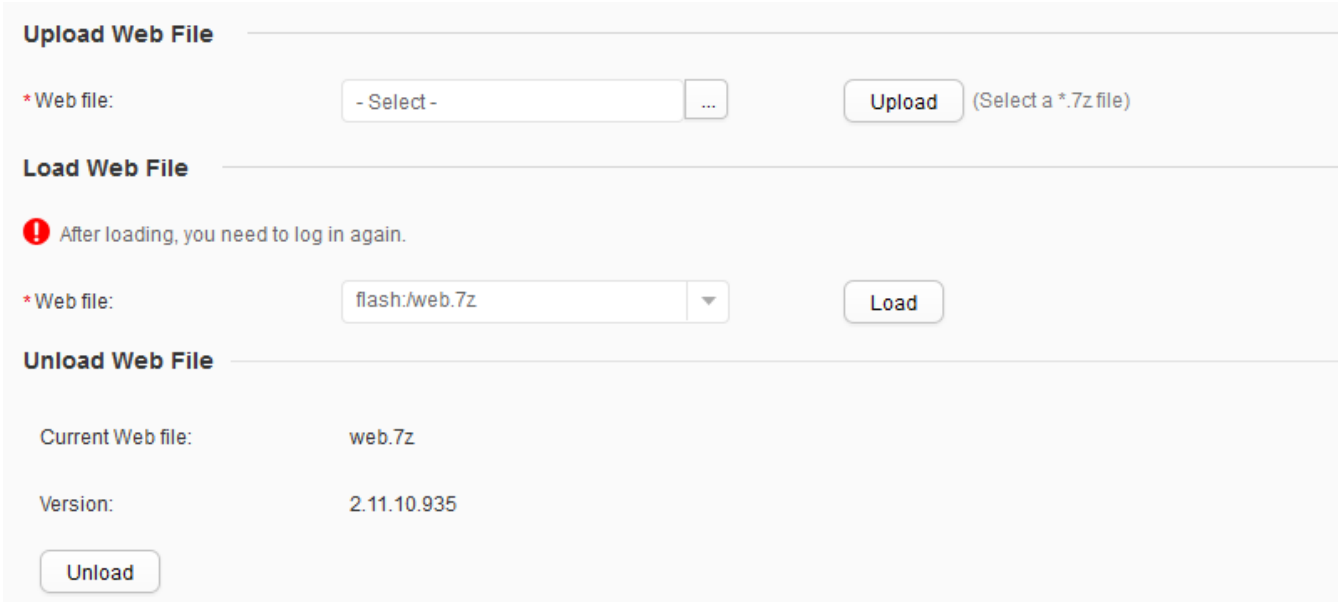


표 1 은 페이지의 매개변수를 설명합니다.

표 1 웹 파일 관리 페이지 의 매개변수

안건	설명
웹 파일 업로드	업로드할 웹 파일을 선택합니다.
웹 파일 로드	로드할 웹 파일을 선택합니다.
웹 파일 언로드	다음을 포함하여 웹 파일에 대한 정보가 페이지에 표시됩니다. 현재 웹 파일 버전 **노트:** 웹 패키지를 시스템 소프트웨어 패키지에 포함된 웹 파일로 복원하려면 **언로드** 를 클릭합니다.

2. ... 을 클릭하고 업로드할 웹 파일을 선택한 다음 업로드를 클릭합니다.

3. 로드할 웹 파일을 선택하고 로드를 클릭합니다. 표시되는 대화 상자에서 **확인**을 클릭합니다.

   그런 다음 다시 로그인해야 합니다.

6.5.5.4 패치

문맥

패치에는 콜드 패치와 핫 패치의 두 가지 유형이 있습니다. 콜드 패치는 스위치가 다시 시작된 후에만 적용되고 핫 패치는 스위치에 로드된 직후에 적용됩니다.

- 패치는 시스템 소프트웨어와 호환되는 일종의 소프트웨어입니다. 시스템 소프트웨어의 중요한 버그를 제거하는 데 사용됩니다. 패치 파일의 확장명은 **.pat** 입니다.

- 패치를 로드하기 전에 스위치의 저장 장치에 패치 파일을 저장해야 합니다. 패치 파일은 HTTP 를 사용하여 스위치에 업로드됩니다.
- 패치를 제거한 후 메모리에서 패치를 삭제합니다.

절차

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 패치**를 선택하여 **패치** 페이지 에 액세스합니다.

그림 1 패치

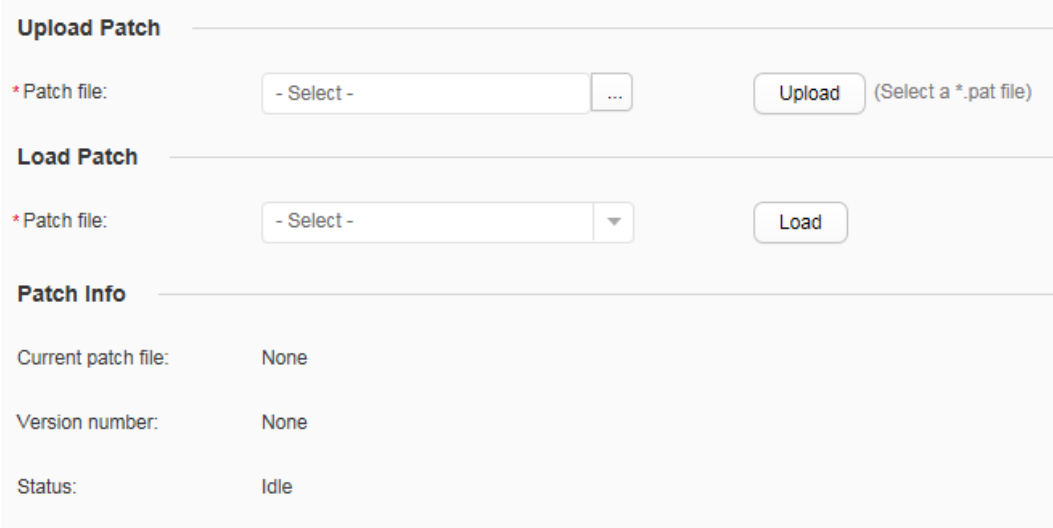


표 1 은 페이지의 매개변수를 설명합니다.

표 1 패치 페이지의 매개변수

안건	설명
패치 업로드	업로드할 패치 파일을 선택할 수 있습니다.
패치 로드	로드할 패치 파일을 선택할 수 있습니다.
패치 정보	패치 정보를 나타냅니다. 현재 패치 파일

표 1 패치 페이지의 매개변수

안건	설명
	버전 번호 상태 **노트:** 설치된 패치를 삭제하려면 **제거**를 클릭합니다.

2. ...를 클릭하여 업로드 할 수 있는 패치 파일을 선택하고 **업로드**를 클릭합니다.

3. 로드 할 수 있는 패치 파일을 선택하고 **로드**를 클릭합니다. 시스템은 현재 로드된 패치 파일을 **Patch Info** 에 표시합니다.

6.5.5.5 플러그인 관리

문맥

소프트웨어 업그레이드는 새로운 기능과 서비스를 추가할 수 있습니다. 그러나 소프트웨어 업그레이드는 복잡하며 서비스에 영향을 미칠 수 있습니다. 이러한 문제를 해결하기 위해 플러그인 관리 기능을 사용하여 지정된 모듈을 로드할 수 있습니다. 이것은 온라인 서비스 또는 기능 로딩을 구현합니다.

절차

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리)** > **플러그인 관리** 를 선택 하여 **플러그인 관리** 페이지 에 액세스합니다.

그림 1 플러그인 관리

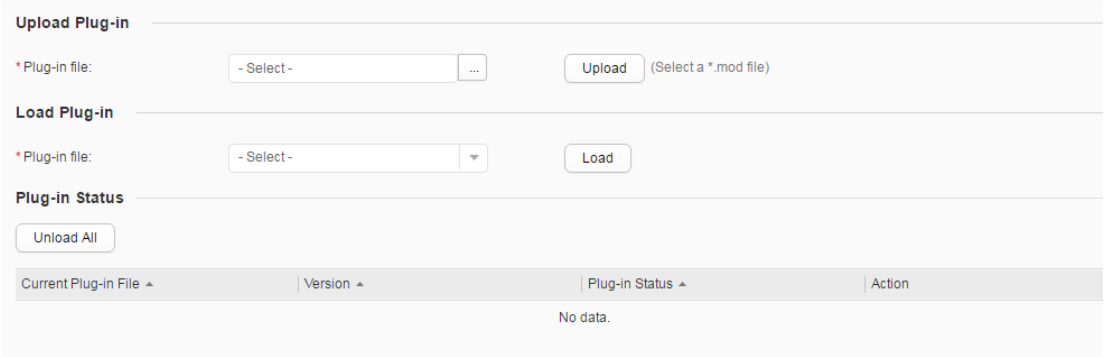


표 1 은 페이지의 매개변수를 설명합니다.

표 1 플러그인 관리 페이지의 매개변수

안건	설명
플러그인 업로드	업로드할 플러그인을 선택할 수 있습니다.
플러그인 로드	로드할 플러그인을 선택할 수 있습니다.

표 1 플러그인 관리 페이지의 매개변수

안건	설명
플러그인 상태	플러그인 정보를 나타냅니다. 현재 플러그인 파일 버전 플러그인 상태 동작

2. ...를 클릭하고 업로드할 플러그인을 선택합니다.

NOTE

- 업로드된 플러그인 파일 이름 확장자는 **.MOD** 여야 합니다.
- 로드된 플러그인 파일 버전은 실행 중인 시스템 소프트웨어 버전과 동일해야 합니다. 그렇지 않으면 로드에 실패합니다.

3. 로드할 플러그인을 선택하고 **로드**를 클릭합니다.

4. 플러그인 파일이 로드된 후 **플러그인 상태** 목록에서 로드된 플러그인 파일의 상태를 확인합니다.

   플러그인 파일을 제거하려면 해당 플러그인 파일의 **언로드**를 클릭하거나 **모두 언로드**를 클릭하여 모든 플러그인 파일을 제거합니다.

6.5.5.6 로그

4.5.5.6.1 로그 정보 보기

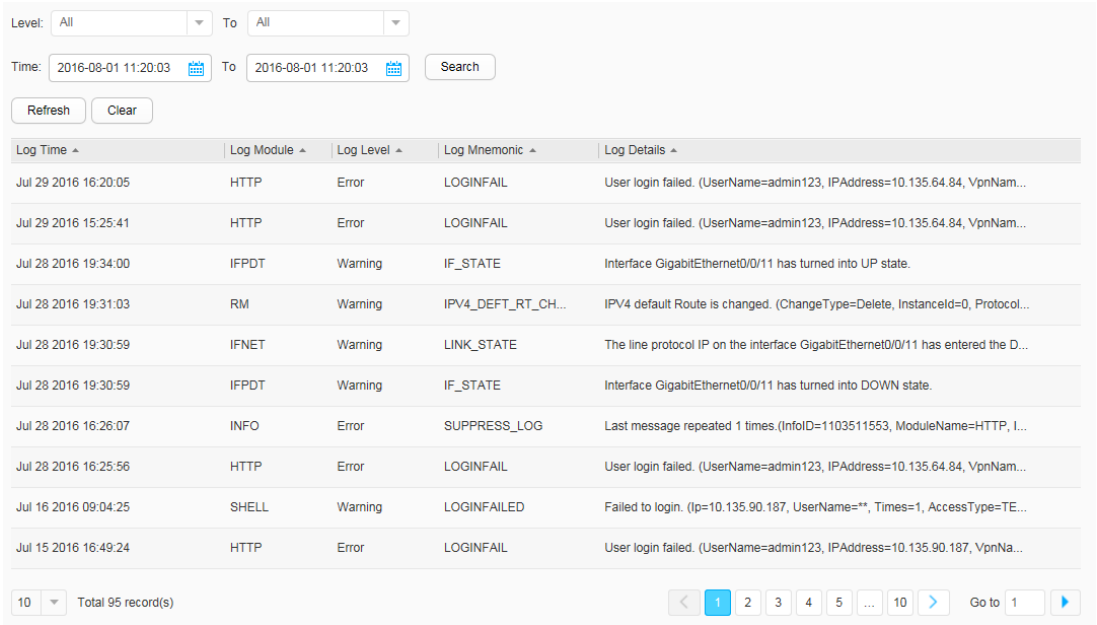
문맥

로그 관리 기능은 사용자 동작을 기록하고 시스템 보안을 모니터링하며 시스템 진단 및 유지 관리를 위한 정보를 제공합니다.

절차

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 로그** 를 선택 하고 **로그 정보 보기** 탭을 클릭합니다.

   그림 1 로그 보기



2. 지정된 로그를 검색하려면 **레벨** 및 **시간**을 설정합니다.

3. 모든 로그 정보를 지우려면 **지우기**를 클릭하십시오.

4.5.5.6.2 매개변수 설정

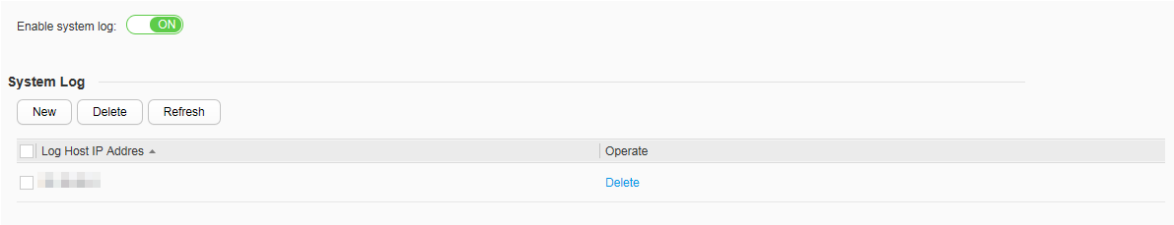
문맥

로그 호스트에 로그를 출력하도록 장치를 설정한 후, 로그 호스트에 저장된 로그를 확인하여 장치 실행 상태를 모니터링할 수 있습니다.

절차

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 로그** 를 선택 하고 **매개변수 설정** 탭을 클릭합니다.

   그림 1 매개변수 설정



2. 정보 센터를 활성화하려면 **시스템 로그 활성화** 를 켜십시오 .

3. **새로 만들기** 를 클릭하고 표시된 대화 상자에 로그 호스트 IP 주소를 입력합니다.

4. **확인**을 클릭합니다.

4.5.5.6.3 LSW 로그

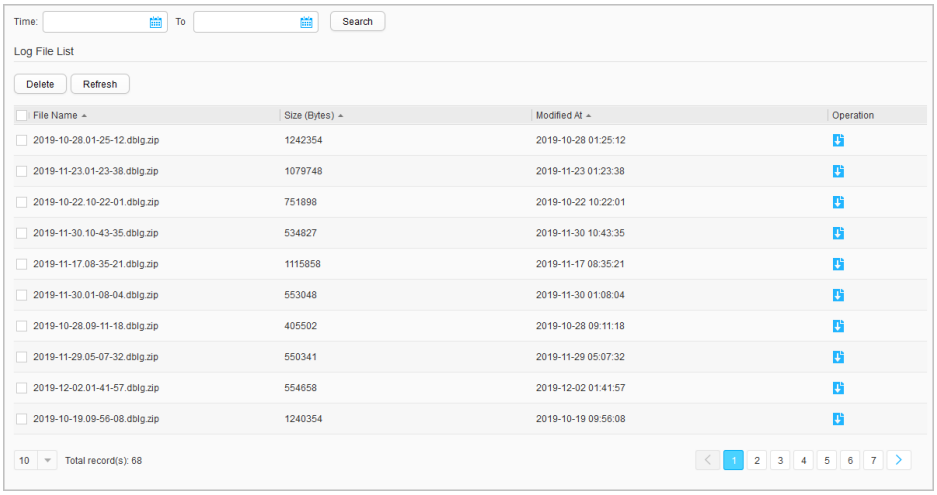
문맥

스위치에서 생성되는 로그 파일에는 사용자 로그 파일과 진단 로그 파일이 포함됩니다. 사용자 로그 파일은 중요한 작업(예: 장치 다시 시작) 및 트랩 정보를 기록합니다. 진단 로그 파일은 서비스 처리 및 오류 정보를 기록합니다. 서비스 요구 사항에 따라 로그 파일을 관리할 수 있습니다.

절차

1. **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 로그** 를 선택합니다. 그림 1 과 같이 **LSW 로그** 페이지가 표시됩니다.

   그림 1 LSW 로그



2. 지정된 기간 동안 생성된 로그 파일을 조회할 시간 범위를 설정합니다.

3. 로그 파일의 줄에서 을 클릭하여 다운로드합니다.

4. 원하는 로그 파일을 선택하고 **삭제**를 클릭하면 로그 파일이 삭제됩니다.

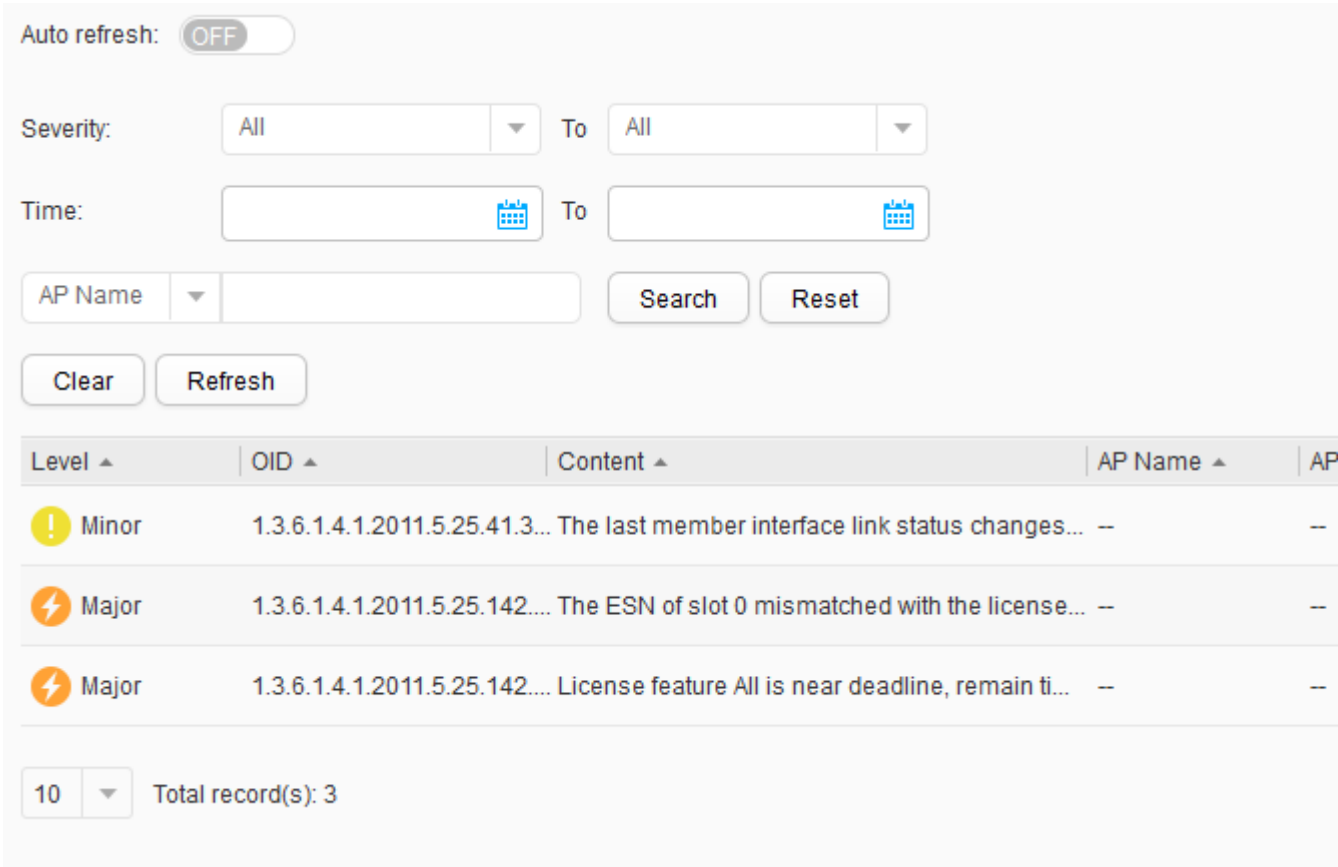
4.5.5.7 알람 및 이벤트

4.5.5.7.1 활성 알람

절차

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 경보 및 이벤트 > 활성 알람**를 선택 하여 **활성 알람** 페이지에 액세스합니다.

그림 1 활성 알람



2. **Severity** , **Time** , **AP Name** , **AP MAC** , **IP Address** , **Keyword** 를 설정하여 지정된 알람을 검색합니다.

3. 모든 알람 정보를 지우려면 **지우기**를 클릭 하십시오.

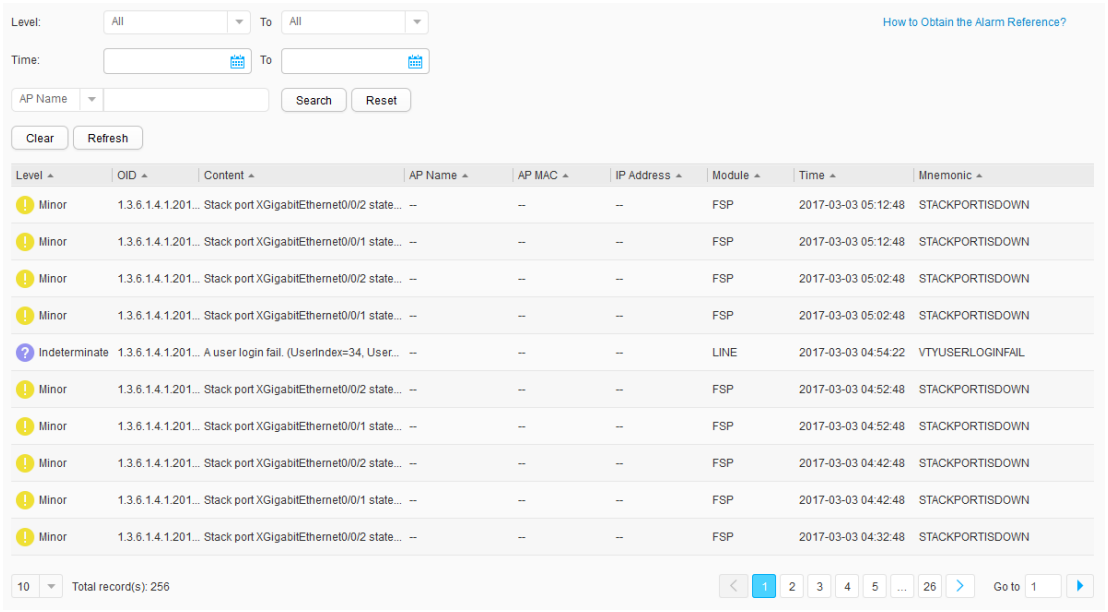
4. **경보 참조를 얻는 방법을** 클릭하십시오. 알람 참조를 얻는 방법을 확인합니다.

4.5.5.7.2 이력 알람 및 이벤트

절차

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 알람 및 이벤트 > 알람 및 이벤트 기록**을 선택하여 **알람 및 이벤트 기록** 페이지에 액세스합니다.

그림 1 이력 알람 및 이벤트



2. **레벨** , **시간** , **AP 이름** , **AP MAC** , **IP 주소** , **키워드** 를 설정 하여 지정된 알람을 검색합니다.

3. 모든 알람 정보를 지우 려면 **지우기**를 클릭하십시오.

4. **경보 참조를 얻는 방법**을 클릭하십시오. 알람 참조를 얻는 방법을 확인합니다.

4.5.5.8 관리자

4.5.5.8.1 관리자

문맥

사용자 관리에는 로컬 사용자 계정(액세스 유형이 HTTP 인 웹 플랫폼 사용자) 생성 및 기존 사용자 계정 수정 또는 삭제가 포함됩니다.

기본적으로 **admin** 이라는 로컬 사용자가 시스템에 존재합니다. 사용자 액세스 유형은 HTTP 및 터미널입니다. (기본 비밀번호는 admin123 입니다.)

NOTE

사용자 액세스 유형이 Telnet, FTP 또는 HTTP 로 설정된 경우 보안 위험이 존재합니다. 필요한 액세스 모드만 구성하는 것이 좋습니다.

단순한 암호는 보안 위험을 초래합니다. 기본 계정으로 웹 네트워크 관리 시스템에 로그인한 후 비밀번호를 복잡한 비밀번호로 변경하는 것을 권장합니다. 암호는 8 자 이상이어야 하며 소문자, 대문자, 숫자, 특수 문자(예: ! $ # %) 중 2 가지 이상을 포함해야 합니다. 암호는 공백과 작은따옴표(')를 포함할 수 없습니다. 또한 암호는 사용자 이름 또는 미러 사용자 이름과 같을 수 없습니다.

로컬 사용자 생성 또는 수정 시 설정한 비밀번호가 기본 비밀번호와 같으면 보안상 위험하다. 기기 보안을 위해 주기적으로 비밀번호를 변경하세요.

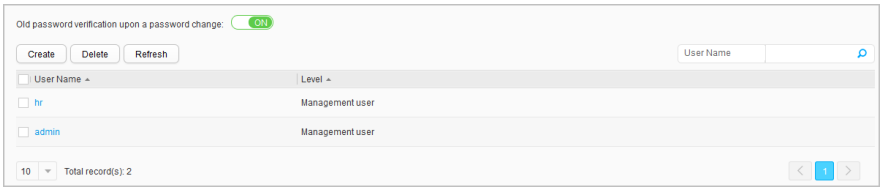
사용자 목록에는 사용자 유형이 FTP, HTTP, SSH, Telnet, Terminal 또는 x25-pad 인 사용자에 대한 정보가 포함됩니다. 생성된 사용자의 접근 유형은 FTP, HTTP, SSH, Telnet, Terminal 또는 x25-pad 가 될 수 있습니다.

절차

- 사용자 계정을 만듭니다.

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 관리자** 를 선택 하고 **관리자** 탭을 클릭합니다.

그림 1 관리자



2. 그림 2 와 같이 **Create** 를 클릭 하여 **Create User** 페이지 를 표시합니다.

그림 2 사용자 생성

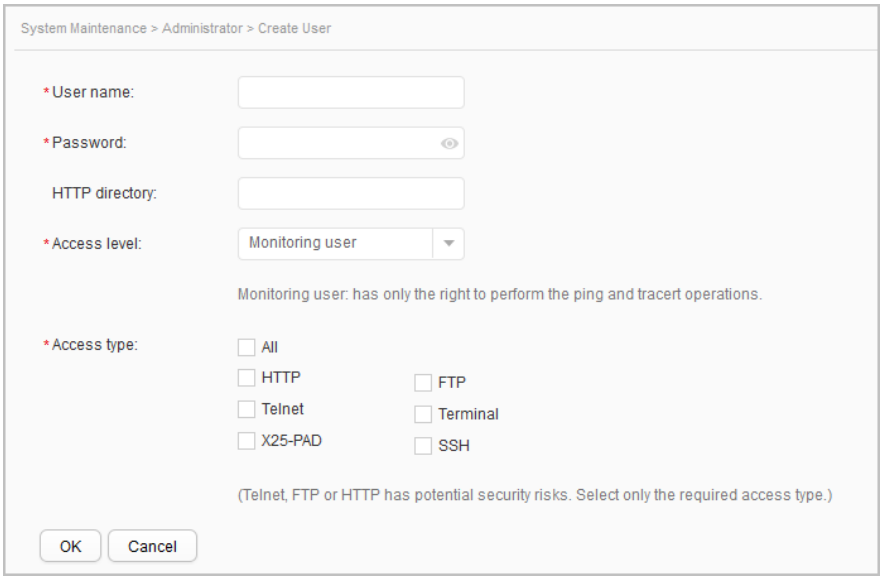


표 1 은 사용자 생성을 위한 매개변수를 설명합니다.

표 1 사용자 생성/사용자 수정

매개변수	설명
사용자 이름	새 사용자 이름을 나타냅니다. 사용자 이름은 물음표(?) 또는 공백을 포함할 수 없습니다.
기존 비밀번호	현재 웹 시스템 로그인 암호를 나타냅니다. **노트:** 이 옵션은 현재 로그인한 사용자의 수정 페이지에서만 사용할 수 있습니다. **이 매개변수는 비밀번호 변경 시 이전 비밀번호 확인 이 ON** 으로 설정된 경우에만 구성할 수 있습니다.
비밀번호	사용자 암호를 나타냅니다.
HTTP 디렉토리	HTTP 사용자가 액세스할 수 있는 디렉토리를 나타냅니다.
액세스 수준	사용자 레벨을 나타냅니다. 오름차순으로 두 가지 사용자 수준이 있습니다. 모니터링 사용자와 관리 사용자입니다.
액세스 유형	사용자 액세스 유형을 나타냅니다.
강제 오프라인	사용자가 네트워크에서 강제로 연결 해제되었는지 여부를 나타냅니다. **노트:** 이 매개변수는 사용자 수정 페이지에만 표시됩니다.
SSH 사용자 구성 **노트:** **이 매개변수는 액세스 유형** 이 **SSH** 로 설정된 경우에만 구성할 수 있습니다.	
인증 모드	SSH 사용자의 인증 모드를 나타냅니다.
서비스 종류	SSH 사용자의 서비스 유형을 나타냅니다.
승인된 디렉토리	SSH 사용자에 대한 SFTP 서비스 인증 디렉토리를 나타냅니다.

3. 매개변수를 설정합니다.

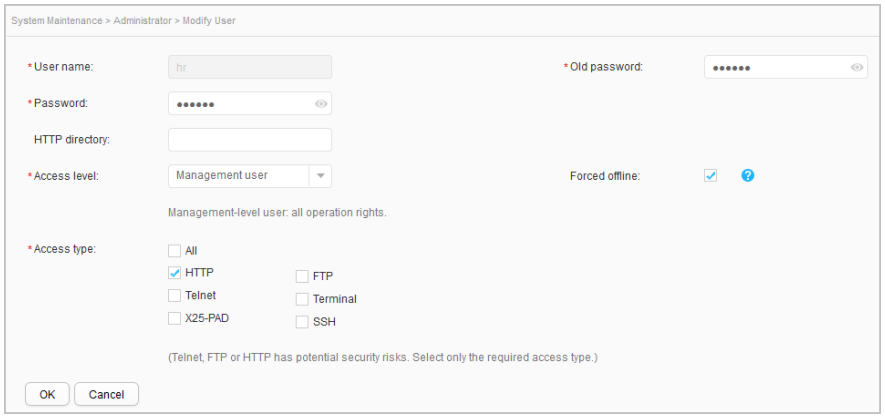
4. **확인**을 클릭합니다.

• 사용자 정보를 수정합니다.

1. **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 관리자** 를 선택 하고 **관리자** 탭을 클릭합니다.

2. 그림 3 과 같이 수정할 사용자 계정을 클릭하여 사용자 **수정** 페이지 에 액세스합니다.

그림 3 사용자 수정



NOTE

- 표 1 은 사용자 정보를 수정하기 위한 매개변수를 설명합니다. 사용자 속성이 변경된 후 사용자 수준은 관리 수준 사용자의 경우 3 이고 모니터링 수준 사용자의 경우 1 입니다.
- 사용자 속성을 수정한 후에는 로그아웃한 다음 다시 로그인해야 수정 사항이 적용됩니다.
- 사용자 이름은 고정되어 있으며 변경할 수 없습니다.

3. 매개변수를 설정합니다.

4. **확인**을 클릭합니다.

• 사용자 계정을 삭제합니다.

1. **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 관리자** 를 선택 하고 **관리자** 탭을 클릭합니다.
2. 삭제할 사용자 계정을 선택하고 삭제 를 클릭합니다.
3. 표시되는 대화 상자에서 **확인**을 클릭합니다.

4.5.5.8.2 비밀번호 정책

절차

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 관리자를** 선택하고 **암호 정책** 탭을 클릭합니다.

그림 1 암호 정책

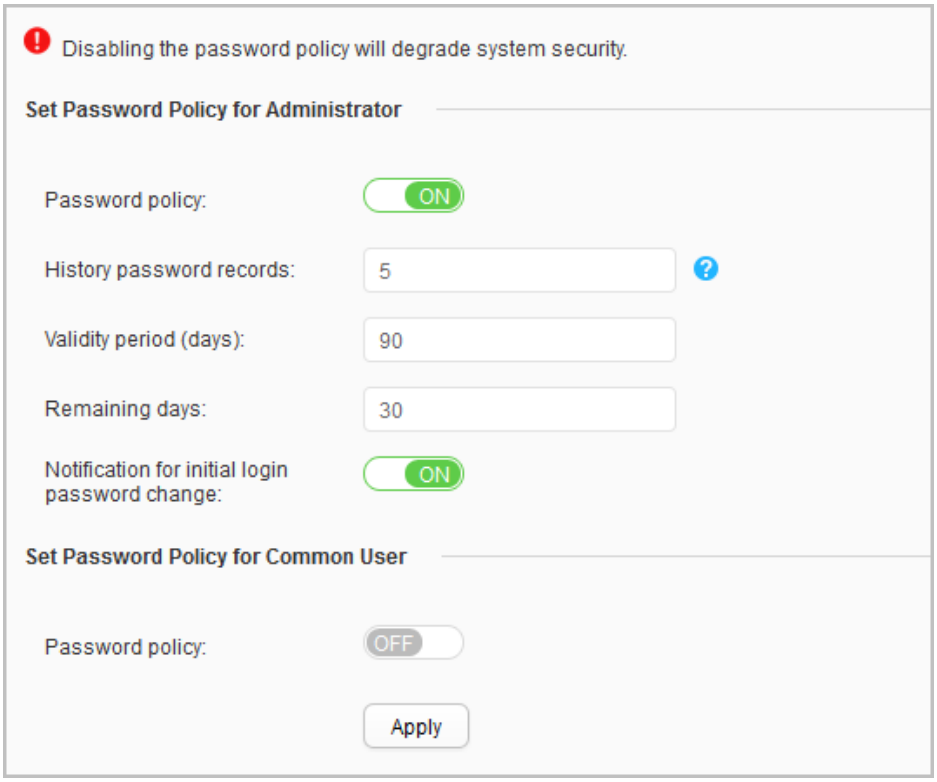


표 1 은 페이지의 매개변수를 설명합니다.

표 1 비밀번호 정책

안건	설명
관리자에 대한 암호 정책 설정	
비밀번호 정책	로컬 관리자에 대한 암호 정책을 활성화할지 여부입니다.
기록 비밀번호 기록	로컬 관리자에 대해 기록된 암호의 최대 수를 나타냅니다.
유효기간(일)	암호 유효 기간(일)을 나타냅니다.
남은 일수	암호가 만료되기 전에 시스템이 프롬프트를 표시하는 시간을 나타냅니다.
초기 로그인 비밀번호 변경 알림	사용자에게 초기 암호를 변경하라는 메시지를 표시하도록 장치를 활성화할지 여부입니다.
일반 사용자에 대한 암호 정책 설정	
비밀번호 정책	로컬 사용자에 대한 암호 정책을 활성화할지 여부입니다.

표 1 비밀번호 정책

안건	설명
기록 비밀번호 기록	로컬 관리자에 대해 기록된 암호의 최대 수를 나타냅니다. 값은 0 에서 12 사이의 정수입니다. 기본값은 5 입니다.

2. 매개변수를 설정합니다.

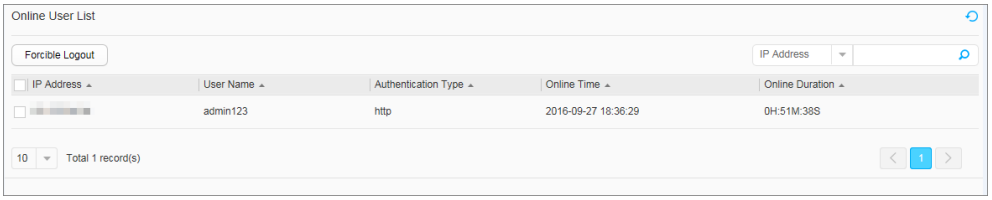
3. **Apply(적용)**을 클릭합니다.

4.5.5.8.3 온라인 관리자

절차

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 관리자를** 선택하고 **온라인 관리자** 탭을 클릭합니다.

그림 1 온라인 사용자 목록



2. 한 명 이상의 사용자를 선택하고 **강제 로그아웃**을 클릭하여 사용자를 강제로 오프라인 상태로 만듭니다.

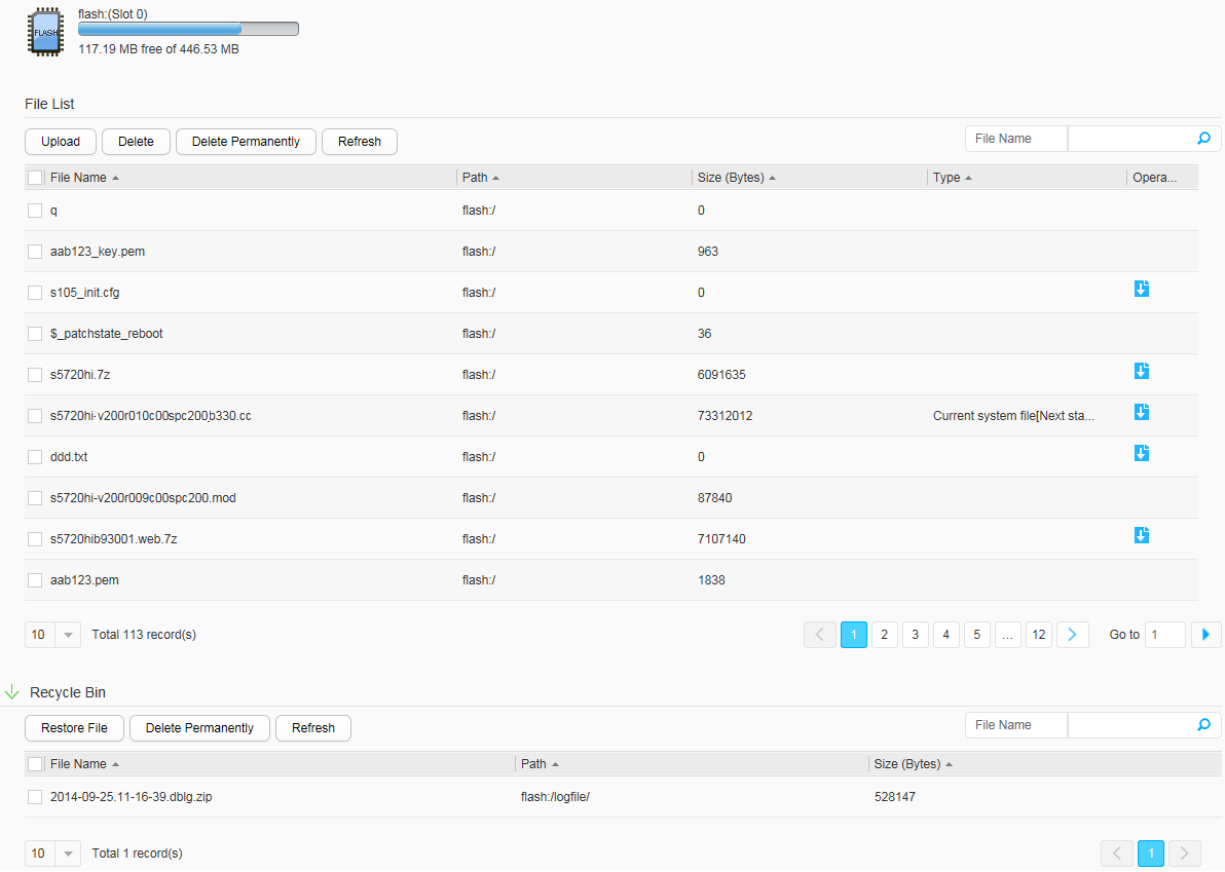
4.5.5.9 시스템

4.5.5.9.1 파일 관리

문맥

웹 시스템은 사용자 작업을 용이하게 하기 위해 파일 관리 기능을 제공합니다. 그림 1 은 **파일 관리** 페이지를 보여줍니다.

그림 1 파일 관리 페이지



절차

- 파일 업로드

로컬 파일을 스위치에 업로드할 수 있습니다.

1. **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 시스템**을 선택하고 **파일 관리** 탭을 클릭합니다.
2. **업로드**를 클릭합니다.
3. 업로드할 로컬 파일을 선택하고 확인을 클릭합니다. 파일이 업로드된 후 시스템은 성공적인 업로드를 나타내는 메시지를 표시합니다.

NOTE

- **파일 관리**에 있는 파일과 이름이 같은 파일은 업로드할 수 없습니다.
- 다음 파일 이름 확장명을 가진 파일만 업로드할 수 있습니다: .cc, .pat, .zip, .7z, .txt, .log, .dblg, .cfg, .dat, .bat, .jpg, .jpeg, .png, .pem, .p12, .cer, .bin, .mod 및 .xml.
- 웹 브라우저의 보안 수준이 너무 높을 경우 그림 2 와 같이 파일 업로드를 시도할 때 "브라우저의 보안 수준이 너무 높음"이라는 메시지가 표시될 수 있습니다. 이 경우 **인터넷 옵션 > 보안을 선택하고 사용자 지정 수준**을 클릭 합니다. 표시된 대화 상자 에서 그림 3 및 그림 4 와 같이 **ActiveX 컨트롤 초기화 및 스크립팅을 스크립팅에 안전하지 않은 것으로 표시** 하고 **서버에 파일을 업로드할 때 로컬 디렉터리 경로 포함**을 **활성화** 로 설정합니다.

그림 2 웹에 표시되는 예외 메시지

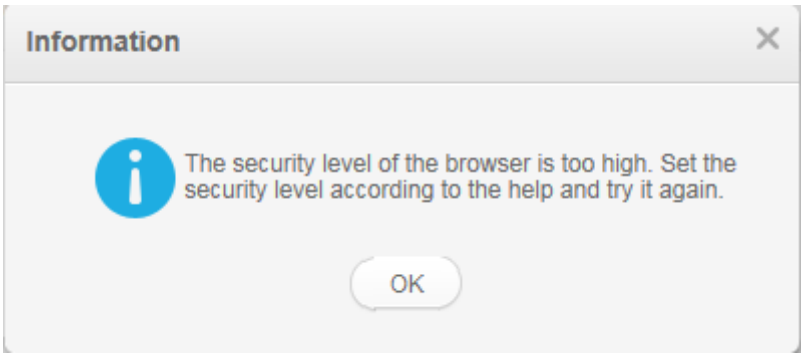


그림 3 "스크립팅에 안전한 것으로 표시되지 않은 ActiveX 컨트롤 초기화 및 스크립팅" 활성화

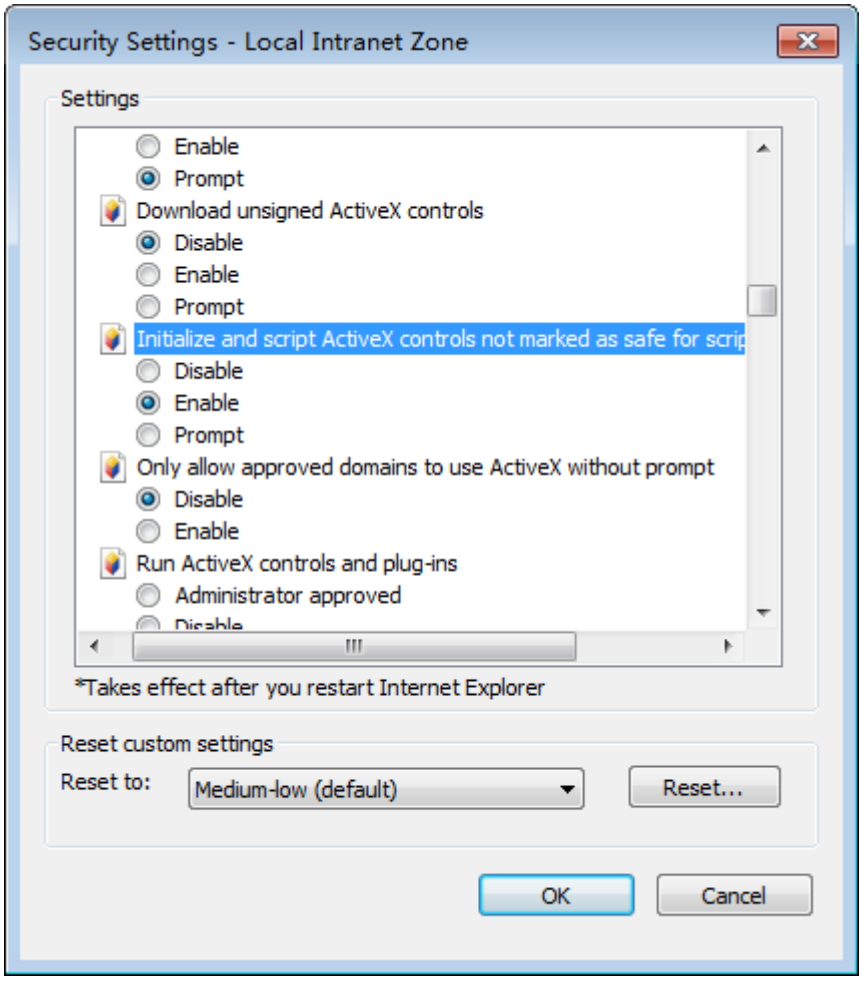
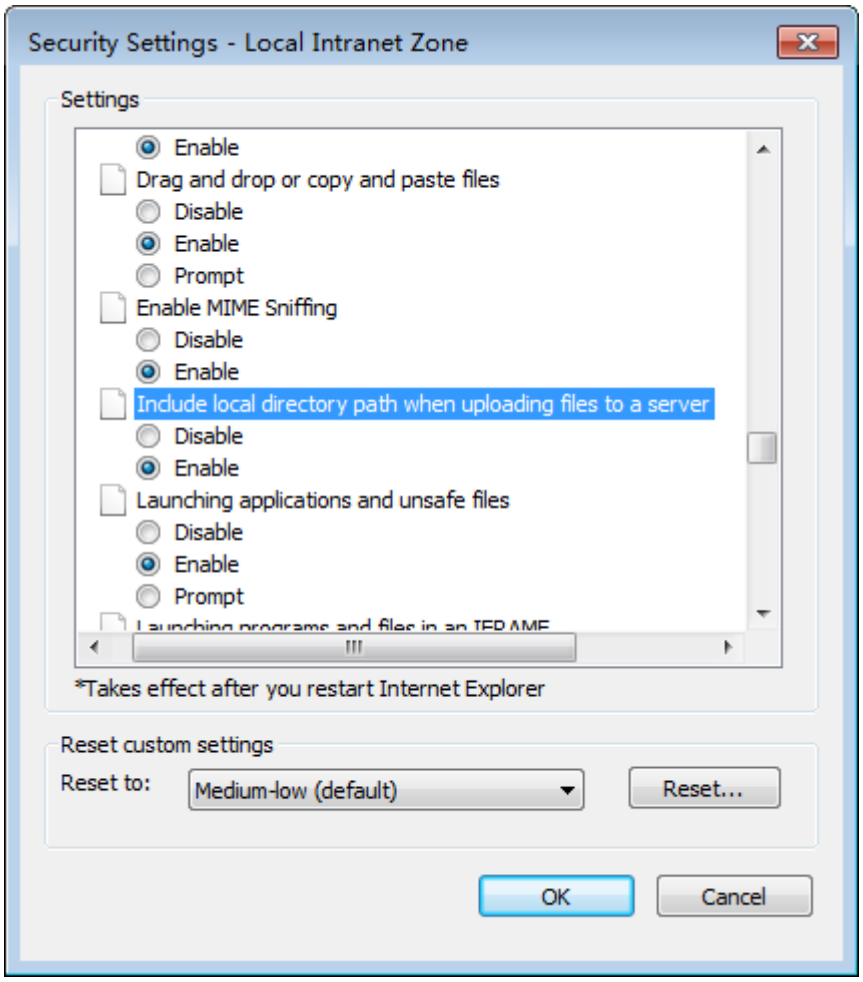


그림 4 "서버에 파일을 업로드할 때 로컬 디렉토리 경로 포함" 활성화



• 파일 다운로드

스위치에서 로컬 장치로 파일을 다운로드할 수 있습니다.

1. **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 시스템**을 선택 하고 **파일 관리** 탭을 클릭합니다.

2. 파일 옆에 있는 을 클릭하여 파일을 다운로드합니다.

NOTE

다음 파일 이름 확장명을 가진 파일만 업로드할 수 있습니다: .cc, .pat, .zip, .7z, .txt, .log, .dblg, .cfg, .dat, .bat, .jpg, .jpeg, .png, .pem, .p12, .cer, .bin, .mod 및 .xml.

- 휴지통으로 파일 이동

파일이 휴지통으로 이동된 후에도 여전히 스위치에 존재합니다. 휴지통에 있는 파일을 복원할 수 있습니다.

1. **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 시스템**을 선택하고 **파일 관리** 탭을 클릭합니다.
2. 삭제할 파일을 선택합니다.
3. **삭제**를 클릭합니다.
4. 표시되는 대화 상자에서 **확인**을 클릭합니다.

- 파일을 영구적으로 삭제합니다.

스위치에서 파일을 영구적으로 삭제할 수 있습니다.

NOTICE

영구적으로 삭제된 파일은 복구할 수 없습니다.

1. **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 시스템**을 선택하고 **파일 관리** 탭을 클릭합니다.

2. 삭제할 파일을 선택합니다.

3. **영구 삭제**를 클릭합니다.

4. 표시되는 대화 상자에서 **확인**을 클릭합니다.

- 파일을 복원합니다.

  휴지통에 있는 파일을 저장 장치로 복원할 수 있습니다.

  1. **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 시스템**을 선택 하고 **파일 관리** 탭을 클릭합니다.

  2. 복원할 파일을 선택합니다.

  3. 파일 복원을 클릭하여 **파일**을 복원합니다. 파일이 휴지통에서 제거됩니다.

- 휴지통에서 파일을 삭제합니다.

  휴지통에 있는 파일은 여전히 저장 공간을 차지합니다. 불필요한 파일을 휴지통에서 영구적으로 삭제하여 저장 공간을 절약할 수 있습니다.

  1. **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 시스템**을 선택 하고 **파일 관리** 탭을 클릭합니다.

  2. 영구적으로 삭제할 파일을 선택합니다.

  3. **영구 삭제**를 클릭합니다.

  4. 표시되는 대화 상자에서 **확인**을 클릭합니다.

4.5.5.9.2 시스템 시간

문맥

일반적으로 DST(일광 절약 시간)는 여름에 구성되며 DST 는 1 일에서 1 년 사이입니다. 따라서 일광 절약 시간제의 종료 시간은 시작 시간보다 하루 이상 1 년 이상 늦어야 합니다.

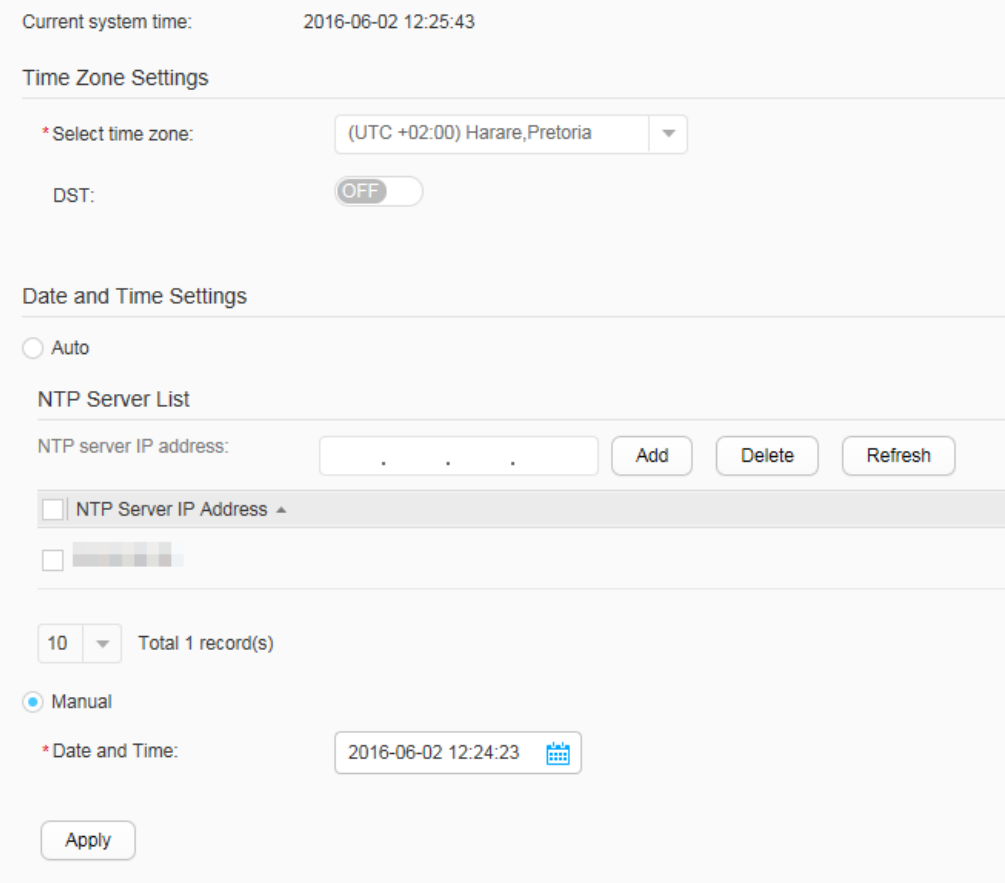
스위치와 다른 장치 간의 효과적인 통신을 위해 시스템 시간을 올바르게 설정하십시오.

절차

- 시간대 설정

1. 그림 1 과 같이 **Maintenance(유지 관리)** > **System Maintenance(시스템 유지 관리)** > **시스템**을 선택 하고 **시스템 시간** 탭을 클릭합니다.

그림 1 시스템 시간



2. 그림 2 와 같이 **Select time** zone 에서 시간대를 선택하고 **DST** 를 **ON** 으로 설정합니다.

그림 2 DST 설정

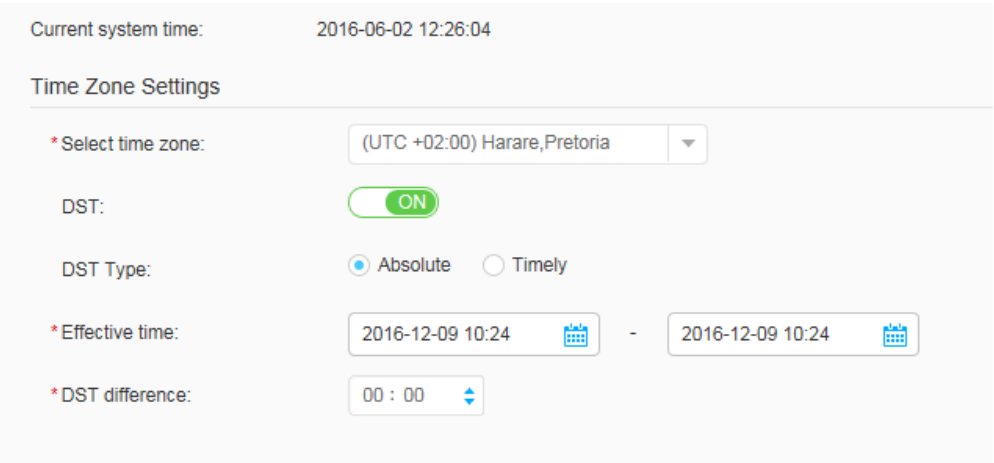


표 1 은 페이지의 매개변수를 설명합니다.

표 1 DST 매개변수

매개변수	설명
다음 매개변수는 **DST 유형** 이 **Absolute** 로 설정된 경우에만 유효합니다.	
유효 시간	절대 DST 의 시작 및 종료 시간을 지정합니다.
DST 차이	DTS 차이를 지정합니다.
다음 매개변수는 **DST 유형** 이 **Timely** 로 설정된 경우에만 유효합니다.	
시작 시간	DST 시작 시간을 설정하려면 **주별** 또는 **날짜별**을 선택 합니다.
종료 시간	DST 종료 시간을 설정하려면 **주별** 또는 **날짜별**을 선택 합니다.
DST 차이	DTS 차이를 지정합니다.
시작 및 종료 연도	주기적 DST 의 시작 및 종료 연도를 지정합니다.

3. 매개변수를 설정한 후 **적용**을 클릭합니다.

- 날짜 및 시간 설정

그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 시스템**을 선택 하고 **시스템 시간** 탭을 클릭합니다.

현재 시스템 시간 은 현재 날짜와 시간을 표시합니다.

- 자동 동기화

1. **자동**을 클릭합니다.
2. **NTP 서버 IP 주소** 를 설정 하고 **추가** 를 클릭 하여 원격 NTP 서버를 지정합니다.

3. **적용**을 클릭 하여 구성을 완료합니다.

- 수동 설정

1. **수동**을 클릭합니다.

2. **날짜 및 시간** 설정 .

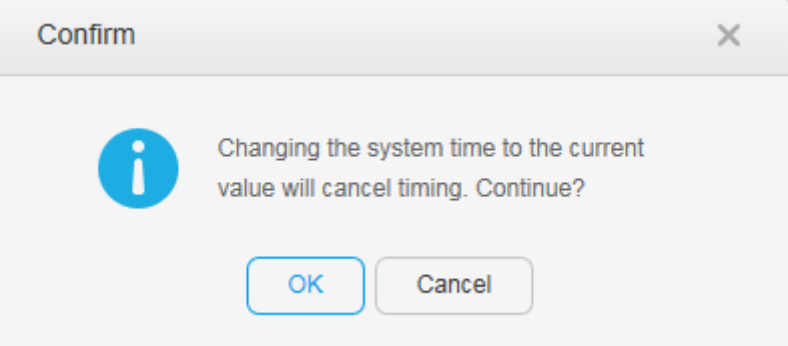
3. **적용**을 클릭 하여 구성을 완료합니다.

새로운 날짜와 시간이 표시됩니다.

- 새 시간이 예정된 재부팅 시간보다 10 분 늦거나 720 시간 빠른 경우

시스템은 그림 3 과 같이 예약된 재시작 기능을 비활성화할 것인지 묻는 메시지를 표시합니다.

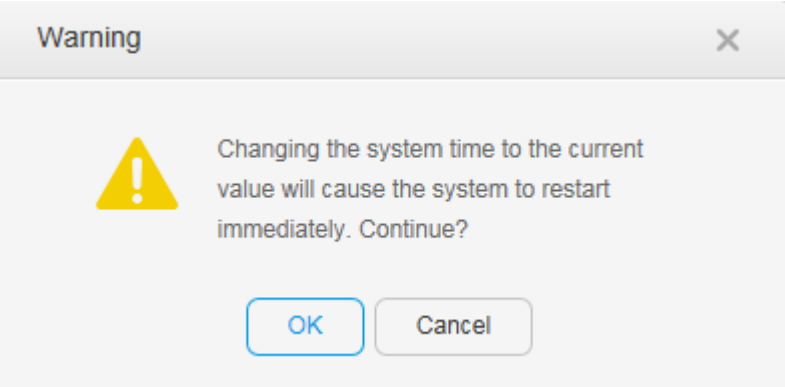
그림 3 정보 페이지



- 시스템 시간이 예정된 다시 시작 시간보다 10 분 이상 늦지 않도록 변경되면

시스템은 그림 4 와 같이 장치를 즉시 다시 시작할 것인지 묻는 메시지를 표시합니다.

그림 4 경고 페이지


Warning
Changing the system time to the current value will cause the system to restart immediately. Continue?
OK
Cancel

4.5.5.9.3 시스템 정보

절차

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 시스템**을 선택 하고 **시스템 정보** 탭을 클릭합니다.

   그림 1 시스템 정보

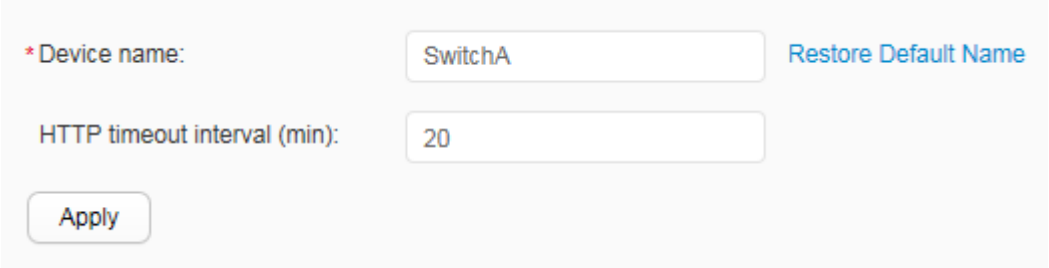


   표 1 은 **시스템 정보** 페이지 의 매개변수를 설명합니다.

   표 1 시스템 정보 페이지 의 매개변수

안건	설명
장치 이름	장치 이름을 나타냅니다. 이것은 필수 매개변수입니다. **기본 이름 복원**을 클릭 하여 기본 장치 이름을 복원할 수 있습니다.
HTTP 시간 초과 간격(분)	HTTP 연결의 시간 초과 간격을 지정합니다.

2. 매개변수를 설정합니다.

3. **적용**을 클릭하여 구성을 완료합니다.

4.5.5.9.4 초기화

문맥

스위치에서 잘못된 구성을 수행한 경우 스위치의 공장 설정을 복원할 수 있습니다.

NOTICE

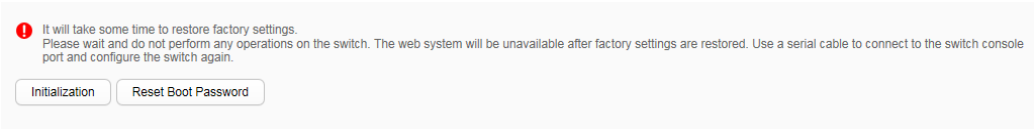
초기화를 클릭하면 스위치에서 수행한 모든 구성이 삭제되고 복원할 수 없습니다. 원래 관리 IP 주소가 무효화되고 웹 시스템을 사용할 수 없습니다. 직렬 케이블을 사용하여 스위치의 콘솔 인터페이스와 PC 를 연결하여 스위치를 재구성합니다.

절차

- 공장 설정을 복원합니다.

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 시스템**을 선택 하고 **초기화** 탭을 클릭합니다.

   그림 1 초기화

2. **초기화**를 클릭합니다.

3. 표시되는 대화 상자에서 **확인**을 클릭합니다.

- 부팅 암호를 재설정합니다.

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 시스템**을 선택 하고 **초기화** 탭을 클릭합니다.

2. **루트 암호 재설정**을 클릭하여 BootLoad 암호를 기본값으로 복원합니다.

3. 표시되는 대화 상자에서 **확인**을 클릭합니다.

4.5.5.9.5 서비스 관리

절차

• 텔넷 서비스를 구성합니다.

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 시스템**을 선택 하고 **서비스 관리** 탭을 클릭합니다.

   그림 1 서비스 관리

2. Telnet 상태를 **ON** 또는 **OFF** 로 설정합니다.

3. **적용**을 클릭하고 표시된 대화 상자에서 **확인을 클릭하여 Telnet 서비스를 활성화 또는 비활성화합니다.**

• STelnet 서비스를 구성합니다.

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 시스템**을 선택 하고 **서비스 관리** 탭을 클릭합니다.

2. STelnet 상태를 **ON** 또는 **OFF** 로 설정합니다.

3. **적용**을 클릭하고 표시된 대화 상자에서 **확인을 클릭하여 STelnet 서비스를 활성화 또는 비활성화합니다.**

- SFTP 서비스를 구성합니다.

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 시스템**을 선택 하고 **서비스 관리** 탭을 클릭합니다.

2. SFTP 상태를 **ON** 또는 **OFF** 로 설정합니다.

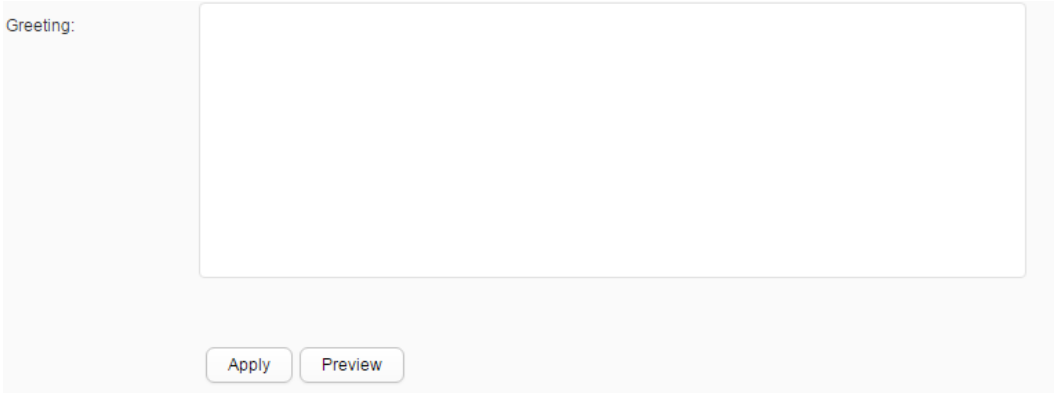
3. **적용**을 클릭하고 표시된 대화 상자에서 **확인을 클릭하여 SFTP 서비스를 활성화하거나 비활성화합니다.**

4.5.5.9.6 인사말 구성

절차

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > 시스템**을 선택하고 **인사말 구성** 탭을 클릭합니다.

   그림 1 인사말 구성



2. 텍스트 상자에 인사말을 입력합니다.

> **NOTE**
>
> **Greeting** 의 값은 1~242 자의 문자열입니다.

3. 웹 페이지에서 인사말을 미리 보려면 **미리 보기**를 클릭합니다.

4. **적용**을 클릭합니다. 표시되는 대화 상자에서 확인을 클릭합니다.

4.5.5.10 SNMP

4.5.5.10.1 전역 구성

문맥

SNMP 에이전트는 관리되는 장치의 에이전트 프로그램입니다. SNMP 에이전트는 관리되는 장치에 대한 정보를 유지 관리하고, NMS 의 요청에 응답하고, 관리 데이터를 NMS 로 보냅니다. NMS 가 SNMP 를 통해 장치를 관리하기 전에 장치에서 SNMP 에이전트를 활성화하고 적절한 SNMP 버전을 선택해야 합니다.

웹 시스템은 SNMPv1, SNMPv2c 및 SNMPv3 을 지원합니다. 장치와 NMS 는 동일한 SNMP 버전을 사용해야 합니다.

NOTE

장치가 다른 SNMP 버전을 실행하는 여러 NMS 에의해 관리되는 경우 장치가 이러한 NMS 와 통신할 수 있도록 장치에 모든 SNMP 버전을 설정해야 합니다.

표 1 SNMP 사용 시나리오

버전	사용 시나리오
SNMPv1	네트워크가 단순하고 보안 요구 사항이 낮은 소규모 네트워크 또는 캠퍼스 네트워크 및 소규모 기업 네트워크와 같이 보안 및 안정성이 우수한 소규모 네트워크에 적용할 수 있습니다.
SNMPv2c	보안 요구 사항이 낮거나 보안이 우수하지만 서비스가 너무 많아 트래픽 정체가 발생할 수 있는 중대형 네트워크에 적용할 수 있습니다.
SNMPv3	다양한 규모의 네트워크, 특히 보안 요구 사항이 엄격하고 승인된 네트워크 관리자만 관리할 수 있는 네트워크에 적용할 수 있습니다. 예를 들어, SNMPv3 는 NMS 와 관리 대상 장치 간의 데이터를 공용 네트워크를 통해 전송해야 하는 경우 사용할 수 있습니다.

절차

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택하고 **전역 구성** 탭을 클릭합니다.

그림 1 전역 구성

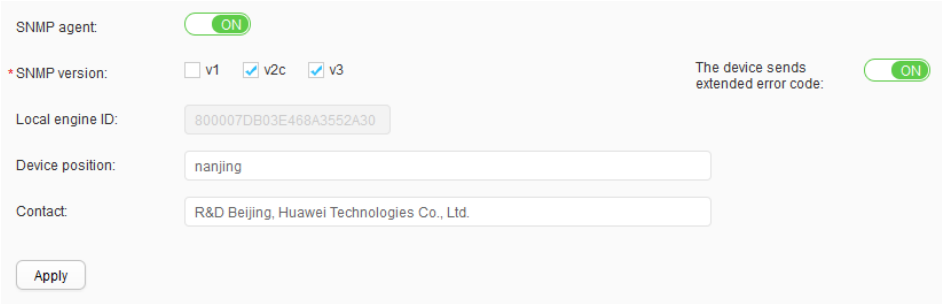


표 2 는 전역 구성 매개변수를 설명합니다.

표 2 전역 구성 매개변수

매개변수	설명
SNMP 에이전트	SNMP 에이전트 기능을 활성화할지 여부를 지정합니다.
SNMP 버전	SNMP 버전을 지정합니다.
장치가 확장 오류 코드를 보냅니다.	장치에서 확장 오류 코드를 NMS 로 보낼 수 있는지 여부를 지정합니다.
로컬 엔진 ID	로컬 SNMP 엔티티의 엔진 ID 를 표시합니다. 이 매개변수는 수정할 수 없습니다.
장치 위치	장치의 위치를 지정합니다.
연락하다	유지 관리 연락처 정보를 지정합니다.

2. 매개변수를 설정합니다.

3. **Apply(적용)을 클릭**하여 구성을 완료합니다.

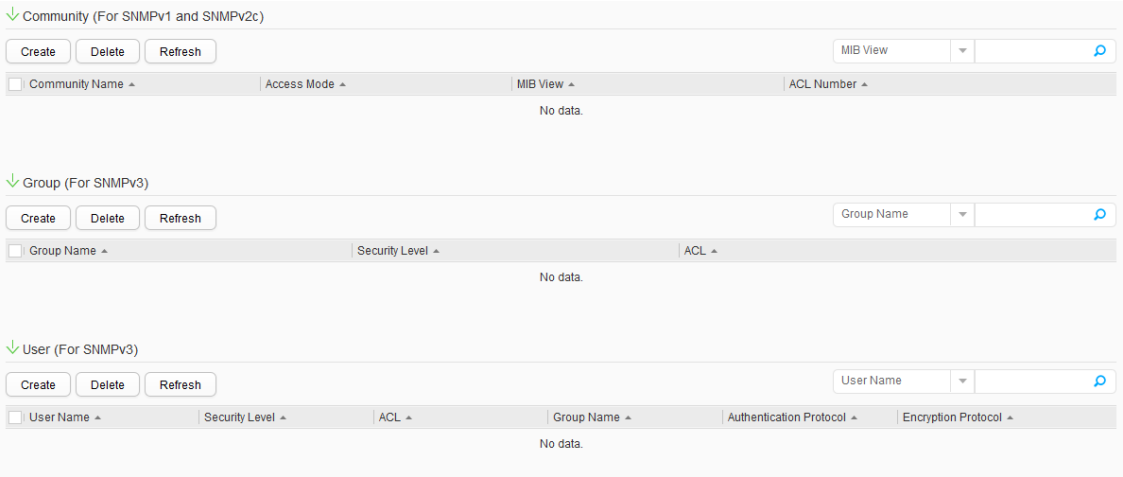
4.5.5.10.2 커뮤니티/그룹 관리

절차

• 커뮤니티 만들기

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택 하고 **커뮤니티/그룹 관리** 탭을 클릭합니다.

그림 1 커뮤니티/그룹 관리



2. **커뮤니티(SNMPv1 및 SNMPv2c 용)** 영역에서 **만들기** 를 클릭 합니다. 그림 2 와 같이 Create **Community** 대화 상자가 표시됩니다.

그림 2 커뮤니티 만들기

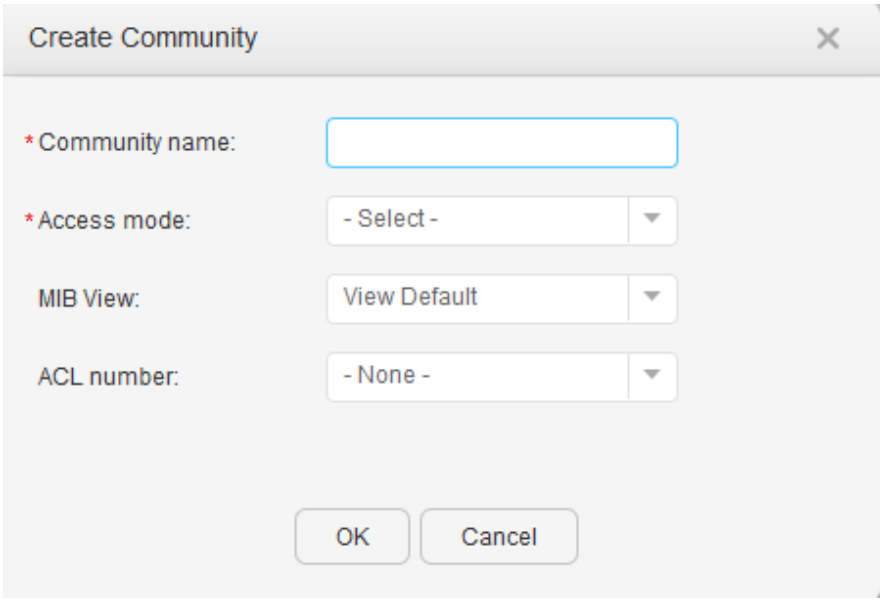


표 1 은 대화 상자의 매개변수를 설명합니다.

표 1 커뮤니티 매개변수

매개변수	설명
커뮤니티 이름	커뮤니티 이름을 지정합니다.
액세스 모드	커뮤니티 이름에 대해 지정된 MIB 보기에 대한 권한을 지정합니다. 읽기 전용 읽기-쓰기
MIB 보기	커뮤니티 이름이 액세스할 수 있는 MIB 보기를 지정합니다.
ACL 번호	커뮤니티 이름과 일치하는 ACL 번호를 지정합니다.

3. 매개변수를 설정합니다.
4. **확인**을 클릭합니다.

- 커뮤니티 삭제

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택 하고 **커뮤니티/그룹 관리** 탭을 클릭합니다.
2. 삭제할 커뮤니티를 선택하고 삭제 를 클릭 **합니다.** 시스템에서 커뮤니티 삭제 여부를 묻습니다.
3. **확인**을 클릭합니다.

- 커뮤니티 정보 업데이트

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택 하고 **커뮤니티/그룹 관리** 탭을 클릭합니다.
2. **커뮤니티(SNMPv1 및 SNMPv2c** 의 경우) 영역에서 **새로 고침**을 클릭합니다.

- 그룹 만들기

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택 하고 **커뮤니티/그룹 관리** 탭을 클릭합니다.
2. **그룹(SNMPv3** 의 경우) 영역에서 **만들기** 를 클릭합니다. 그림 3 과 같이 Create **Group** 대화 상자가 표시됩니다.

그림 3 그룹 생성

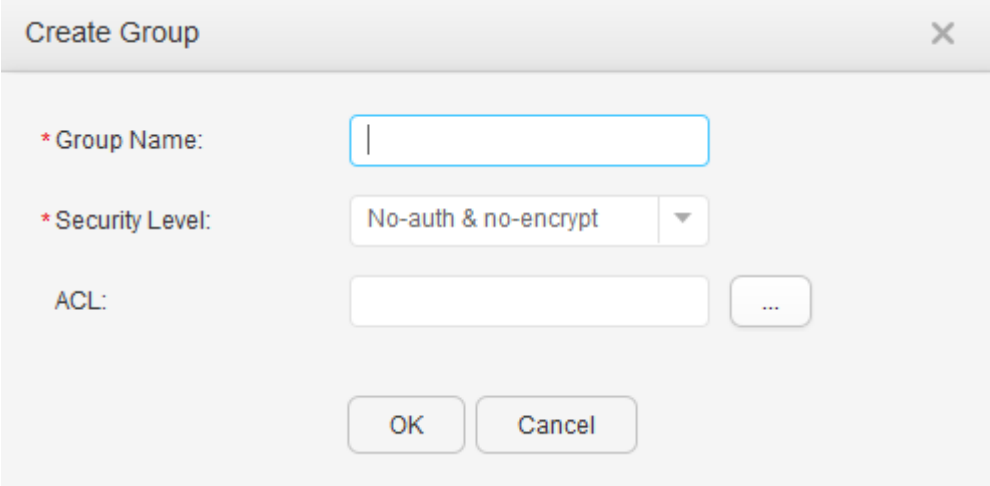


표 2 는 대화 상자의 매개변수를 설명합니다.

표 2 그룹 매개변수

매개변수	설명
그룹 이름	그룹 이름을 지정합니다.
보안 레벨	SNMP 그룹의 보안 수준을 지정합니다.
ACL	그룹과 일치하는 ACL 번호를 지정합니다. 을 클릭 ... 하고 대화 상자에서 ACL 을 선택합니다.

- 그룹 수정

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택 하고 **커뮤니티/그룹 관리** 탭을 클릭합니다.
2. 그룹 이름을 클릭하여 그룹 **수정** 페이지에 액세스합니다. 표 2 는 페이지의 매개변수를 설명합니다.
3. 구성 매개변수를 수정합니다. **그룹 이름** 은 수정할 수 없습니다.

4. **확인**을 클릭합니다.

• 그룹 삭제

1. **확인**을 클릭합니다.
2. 삭제할 그룹을 선택하고 삭제 를 클릭 **합니다.** 시스템에서 그룹을 삭제할지 여부를 묻습니다.
3. **확인**을 클릭합니다.

• 그룹 정보 업데이트

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택 하고 **커뮤니티/그룹 관리** 탭을 클릭합니다.
2. **그룹(SNMPv3** 의 경우) 영역에서 **새로 고침**을 클릭합니다.

• 사용자 생성

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택 하고 **커뮤니티/그룹 관리** 탭을 클릭합니다.
2. **사용자(SNMPv3** 의 경우) 영역에서 **만들기** 를 클릭합니다. 그림 4 와 같이 Create **User** 대화 상자가 표시됩니다.

그림 4 사용자 생성

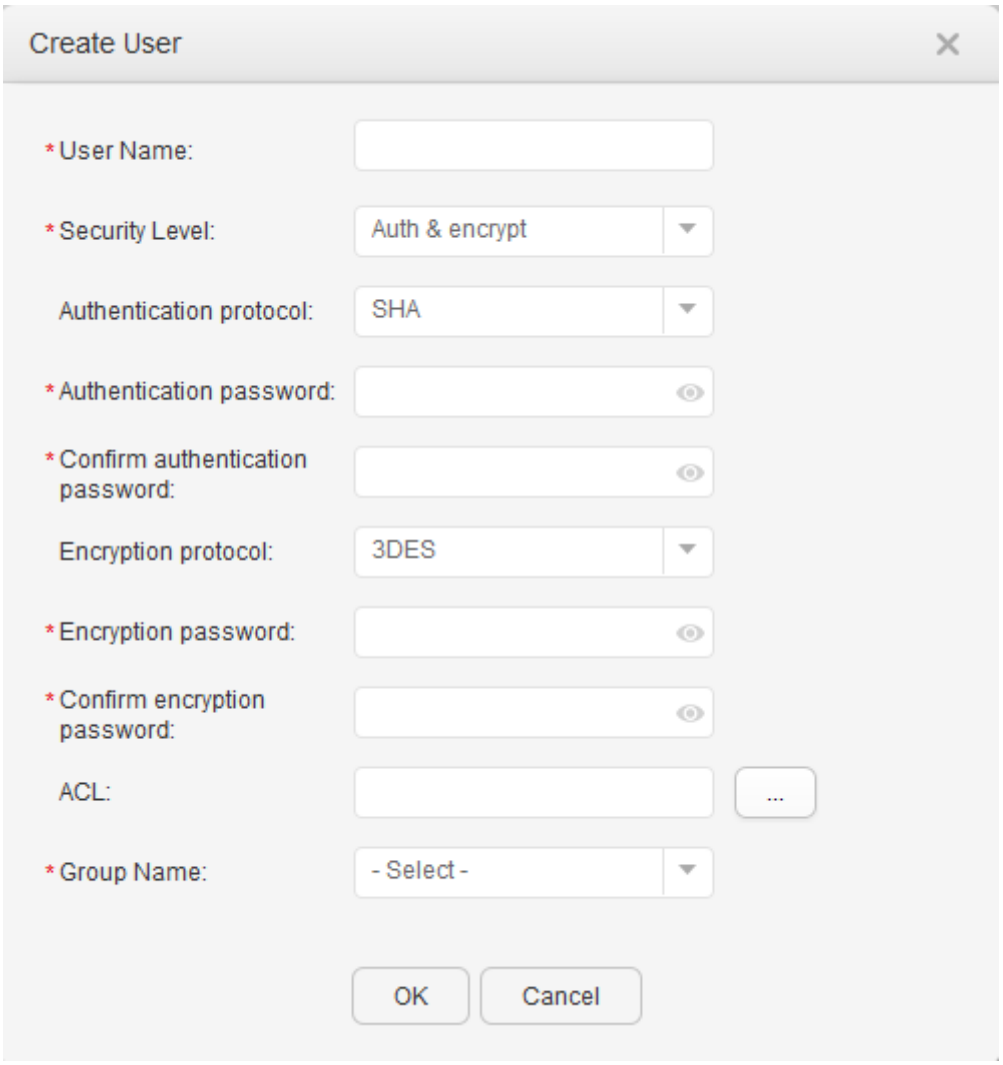


표 3 은 대화 상자의 매개변수를 설명합니다.

표 3 사용자 매개변수

매개변수	설명
사용자 이름	사용자 이름을 지정합니다.
보안 레벨	사용자의 보안 수준을 지정합니다.
인증 프로토콜	인증 프로토콜을 SHA 또는 MD5 로 설정합니다. **이 매개변수는 보안 수준** 이 **Auth & no-encrypt** 또는 **Auth & encrypt** 로 설정된 경우에만 사용할 수 있습니다.
인증 비밀번호	사용자의 인증 암호를 지정합니다. **이 매개변수는 보안 수준** 이 **Auth & no-encrypt** 또는 **Auth & encrypt** 로 설정된 경우에만 사용할 수 있습니다.

표 3 사용자 매개변수

매개변수	설명
인증 비밀번호 확인	인증 비밀번호를 확인합니다. **이 매개변수는 보안 수준** 이 **Auth & no-encrypt** 또는 **Auth & encrypt** 로 설정된 경우에만 사용할 수 있습니다.
암호화 프로토콜	암호화 프로토콜을 DES-56, AES-128, AES-192, AES-256 또는 3DES 로 설정합니다. **이 매개변수는 보안 수준** 이 **인증 및 암호화** 로 설정된 경우에만 사용할 수 있습니다.
암호화 비밀번호	사용자의 암호화 암호를 지정합니다. **이 매개변수는 보안 수준** 이 **인증 및 암호화** 로 설정된 경우에만 사용할 수 있습니다.
암호화 비밀번호 확인	암호화 암호를 확인합니다. **이 매개변수는 보안 수준** 이 **인증 및 암호화** 로 설정된 경우에만 사용할 수 있습니다.
ACL	사용자와 일치하는 ACL 번호를 지정합니다. 을 클릭 ... 하고 대화 상자에서 ACL 을 선택합니다.
그룹 이름	SNMP 그룹 이름을 지정합니다.

- 사용자 수정

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택 하고 **커뮤니티/그룹 관리** 탭을 클릭합니다.
2. 사용자 이름을 클릭하여 사용자 **수정** 페이지에 액세스합니다. 표 3 은 페이지의 매개변수를 설명합니다.
3. 구성 매개변수를 수정합니다. **사용자 이름** 은 수정할 수 없습니다.
4. **확인**을 클릭합니다.

• 사용자 삭제

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택 하고 **커뮤니티/그룹 관리** 탭을 클릭합니다.
2. 삭제할 사용자를 선택하고 삭제 를 클릭 **합니다.** 시스템에서 사용자를 삭제할지 여부를 묻습니다.
3. **확인**을 클릭합니다.

• 사용자 정보 업데이트

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택 하고 **커뮤니티/그룹 관리** 탭을 클릭합니다.
2. **사용자(SNMPv3** 의 경우) 영역에서 **새로 고침**을 클릭합니다.

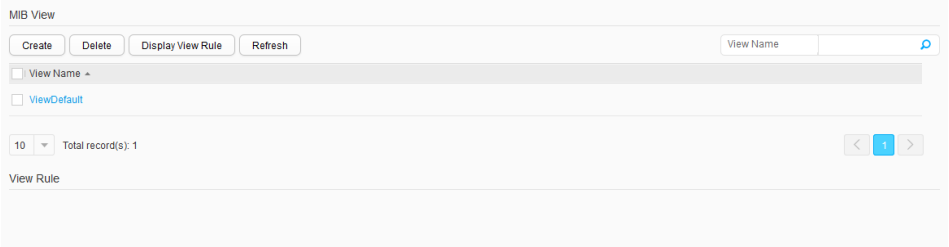
4.5.5.10.3 MIB 보기

절차

• MIB 보기 만들기

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택 하고 **MIB 보기** 탭을 클릭합니다.

그림 1 MIB 보기 페이지



2. **MIB 보기** 영역에서 만들기를 클릭합니다. 그림 2 와 같이 Create **View Rule** 대화 상자가 표시됩니다.

그림 2 보기 규칙 만들기

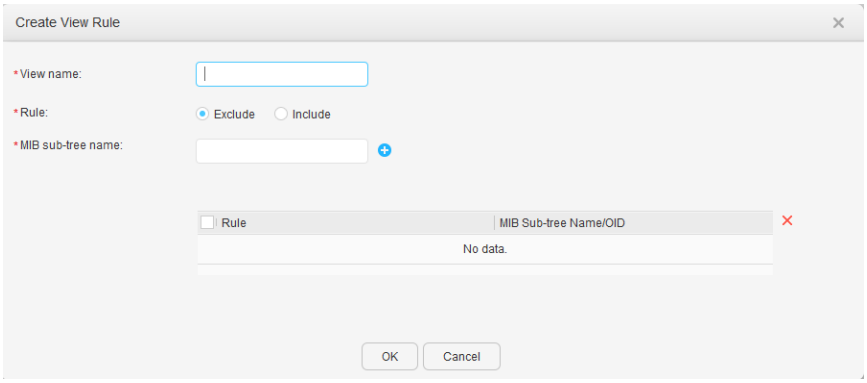


표 1 은 **보기 규칙 생성** 대화 상자 의 매개변수를 설명합니다.

표 1 규칙 매개변수 보기

매개변수	설명
보기 이름	MIB 보기의 이름을 지정합니다.
규칙	MIB 하위 트리에서 MIB 보기의 권한을 지정합니다.
MIB 하위 트리 이름	MIB 하위 트리의 OID 를 지정합니다. 이 OID 는 하위 트리의 OID(예: 1.4.5.3.1) 또는 이름(예: 시스템)일 수 있습니다.

NOTE

데이터 레코드를 추가하려면 을 클릭합니다. 여러 데이터 레코드를 추가할 수 있습니다. 데이터 레코드를 삭제하려면 해당 레코드를 선택하고 을 클릭합니다.

3. 매개변수를 설정합니다.

4. **확인**을 클릭합니다.

• MIB 보기 수정

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택 하고 **MIB 보기** 탭을 클릭합니다.

2. **MIB 보기 수정** 페이지 에 액세스하려면 MIB 보기 이름을 클릭 하십시오. 표 1 은 페이지의 매개변수를 설명합니다.

3. 구성 매개변수를 수정합니다. **보기 이름** 은 수정할 수 없습니다.

4. **확인**을 클릭합니다.

• MIB 보기 삭제

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택 하고 **MIB 보기** 탭을 클릭합니다.

2. 삭제할 MIB 보기를 선택하고 삭제 를 클릭 **하십시오** . 시스템에서 MIB 보기를 삭제할지 여부를 묻습니다.

3. **확인**을 클릭합니다.

• 보기 규칙 표시

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택 하고 **MIB 보기** 탭을 클릭합니다.

2. 표시할 MIB 보기를 선택하고 **보기 규칙** 표시 를 클릭하십시오. 시스템은 MIB 보기의 보기 규칙을 표시합니다.

• 보기 규칙 업데이트

1. 그림 1 과 같이 **Maintenance(유지 관리) > System Maintenance(시스템 유지 관리) > SNMP** 를 선택 하고 **MIB 보기** 탭을 클릭합니다.

2. **MIB 보기** 영역에서 **새로 고침**을 클릭합니다.

4.5.5.10.4 트랩 설정

문맥

NOTE

이 페이지는 SNMP 설정 의 SNMP 에이전트 상태 가 **ON** 으로 설정된 경우에만 표시됩니다.

트랩은 네트워크 오류를 관리자에게 알리기 위해 관리되는 장치에서 NMS 로 보내는 경보 메시지입니다. 관리되는 장치에서 트랩을 수신한 후 NMS 는 응답할 필요가 없습니다.

절차

- 트랩 기능을 구성합니다.

1. 그림 1 과 같이 유지 **관리** > **시스템 유지 관리** > **SNMP** 를 선택 하고 **트랩 설정** 탭을 클릭합니다.

그림 1 트랩 설정

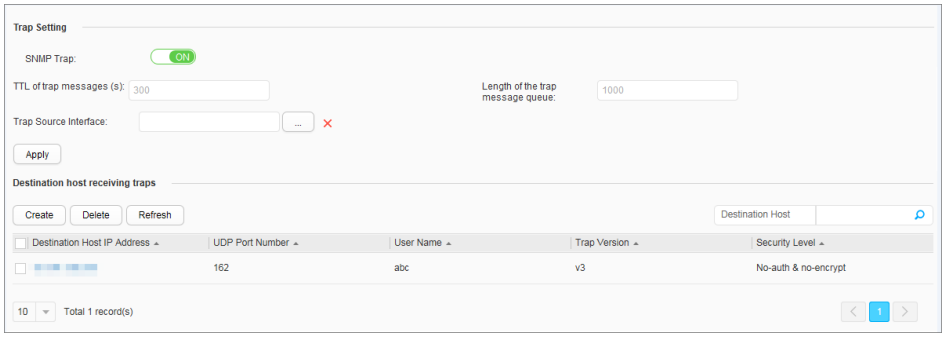


표 1 은 **트랩 설정** 영역 의 매개변수를 설명 합니다.

표 1 트랩 매개변수

매개변수	설명
SNMP 트랩	NMS 에 트랩을 보낼 수 있도록 스위치를 활성화할지 여부를 지정합니다.
트랩 메시지의 TTL	트랩의 TTL 을 설정합니다. TTL 이 만료되면 트랩이 삭제됩니다.
트랩 메시지 대기열의 길이	대상 호스트로 보낸 트랩의 대기열 길이를 지정합니다.
트랩 소스 인터페이스	트랩을 보내기 위한 소스 포트를 지정합니다.

2. 매개변수를 설정합니다.

3. **적용**을 클릭 하여 구성을 완료합니다.

- 트랩 대상 호스트를 생성합니다.

1. 그림 1 과 같이 유지 **관리** > **시스템 유지 관리** > **SNMP** 를 선택 하고 **트랩 설정** 탭을 클릭합니다.

2. 그림 2 와 같이 **트랩을 수신하는 대상 호스트 에서 생성**을 클릭 하여 **트랩 호스트 생성** 페이지 를 엽니다.

그림 2 트랩 대상 호스트 생성

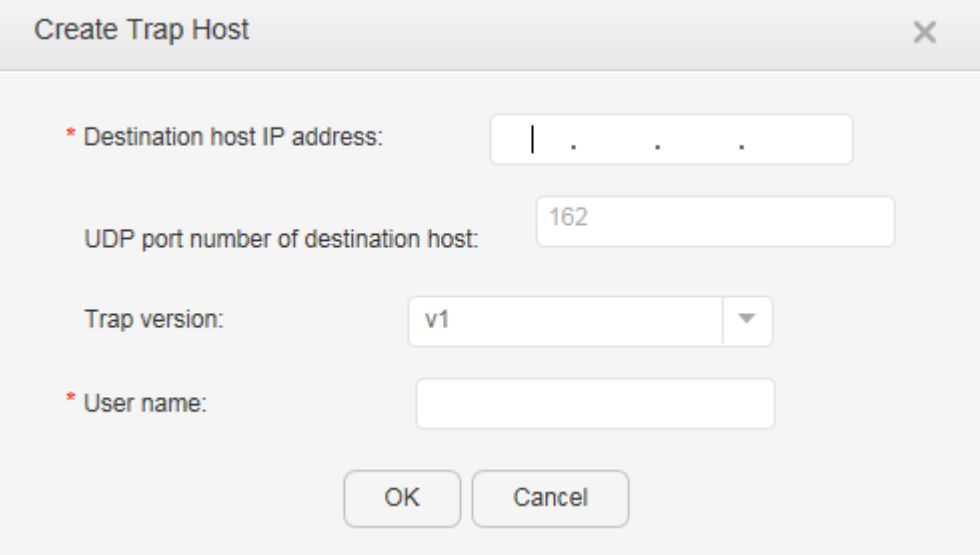


표 2 는 **트랩 호스트 생성** 대화 상자 의 매개변수에 대해 설명 합니다.

표 2 트랩 호스트 매개변수

매개변수	설명
대상 호스트 IP 주소	대상 호스트의 IP 주소를 지정합니다.
목적지 호스트의 UDP 포트 번호	대상 호스트에서 트랩을 수신하기 위한 포트 번호를 지정합니다.
트랩 버전	다음을 포함하여 트랩 메시지와 일치하는 SNMP 버전을 지정합니다. • v1: SNMPv1. • v2c: SNMPv2c. • v3: SNMPv3.
사용자 이름	NMS 에 표시되는 사용자 이름을 지정합니다.
보안 레벨	트랩 버전이 v3 인 경우 이 매개변수는 필수입니다. 보안 수준에는 다음이 포함됩니다. • 인증 없음(&N) 암호화 • 인증(&N) 암호화 • 인증(&E) 암호화

3. 매개변수를 설정합니다.

4. **확인**을 클릭합니다. 구성이 완료되었습니다.

- 트랩 대상 호스트를 수정합니다.

1. 그림 1 과 같이 유지 **관리** > **시스템 유지 관리** > **SNMP** 를 선택 하고 **트랩 설정** 탭을 클릭합니다.
2. 수정하려는 트랩 대상 호스트의 IP 주소를 눌러 **트랩 호스트 수정** 페이지에 액세스합니다. 표 2 는 페이지의 매개변수를 설명합니다.
3. 구성 매개변수를 수정합니다. **대상 호스트 IP 주소** 및 **사용자 이름** 은 수정할 수 없습니다.
4. **확인**을 클릭합니다.

- 트랩 대상 호스트를 삭제합니다.

1. 그림 1 과 같이 유지 **관리** > **시스템 유지 관리** > **SNMP** 를 선택 하고 **트랩 설정** 탭을 클릭합니다.
2. 삭제할 트랩 대상 호스트를 선택하고 삭제 를 클릭 **합니다.** 시스템에서 트랩 대상 호스트를 삭제할지 여부를 묻습니다.
3. **확인**을 클릭합니다.

- 트랩 대상 호스트 정보를 업데이트합니다.

1. 그림 1 과 같이 유지 **관리** > **시스템 유지 관리** > **SNMP** 를 선택 하고 **트랩 설정** 탭을 클릭합니다.

2. 트랩을 수신 하는 **대상 호스트** 영역에서 **새로 고침**을 클릭합니다.

4.5.5.11 전자 라벨

절차

1. 그림 1 과 같이 **Maintenance(유지 관리)** > **System Maintenance(시스템 유지 관리)** > **전자 라벨**을 선택하여 **전자 라벨** 페이지에 액세스합니다.

그림 1 전자 라벨

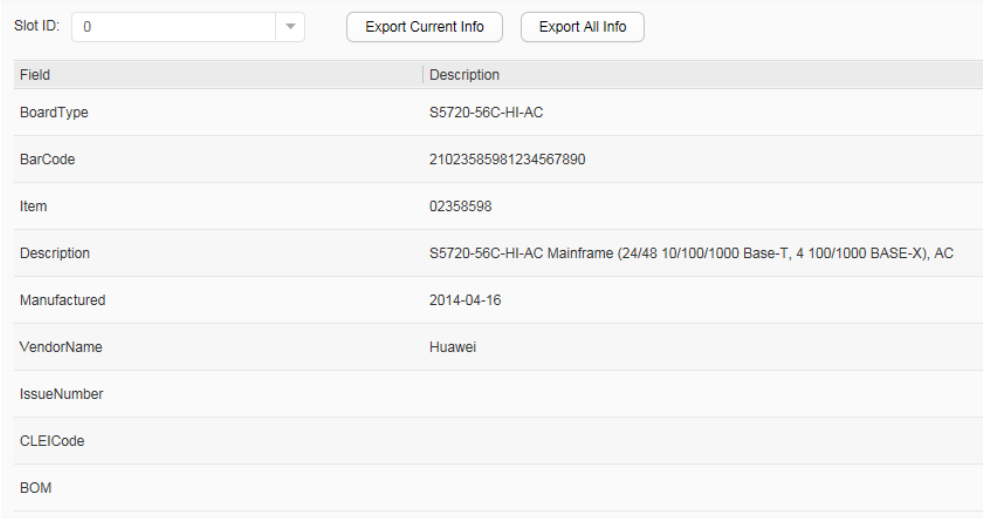


표 1 은 페이지의 매개변수를 설명합니다.

표 1 전자 라벨 페이지의 매개변수

안건	설명
슬롯 ID	스위치가 있는 슬롯입니다.

표 1 전자 라벨 페이지의 매개변수

안건	설명
보드타입	지정된 구성 요소의 보드 모델입니다.
바코드	지정된 구성 요소의 바코드입니다.
안건	지정된 구성요소의 BOM 코드입니다.
설명	지정된 구성 요소에 대한 영어 설명입니다.
제조	지정된 구성 요소의 생산 날짜입니다.
공급업체 이름	지정된 구성 요소의 공급업체 이름입니다.
발행 번호	지정된 구성 요소의 발행 번호입니다.
CLEI 코드	지정된 구성 요소의 CLEI 코드입니다.
봄	지정된 구성요소의 판매 BOM 코드입니다.

기초 명령어

■ 기본 구성

명령	설명
System-view	구성 모드로 진입
sysname Soltech	시스템 이름 설정
telnet server enable	텔넷 서버 활성화
telnet server-source all-interface	텔넷 액세스를 위한 모든 인터페이스
http server-source all-interface	http 액세스를 위한 모든 모든 인터페이스
pnp-button mode reset-system	전면 리셋버튼에 구성을 리셋하는 기능을 활성화
aaa	aaa 구성 모드로 들어갑니다.
local-user admin password admin123	로컬 사용자 및 암호를 구성합니다. (암호화되지 않음)
local-user *admin123* password irreversible-cipher *abcd@123*	로컬 사용자 및 암호를 구성하고 비밀번호를 해시(hash)방식으로 암호화 저장합니다. (암호길이 8~128 글자)
local-user admin privilege level 15	관리자의 로컬 사용자 권한을 구성합니다.
local-user admin service-type telnet terminal ssh http	로컬 사용자 서비스 액세스 유형을 허용합니다.
undo local-user admin123	사용자 계정을 지웁니다.
quit	AAA 구성 모드에서 나옵니다.
interface Vlanif1	VLAN 인터페이스 구성 모드로 들어갑니다.
ip address 192.168.0.1 255.255.255.0	IP 주소 및 서브넷 마스크를 구성합니다.
stelnet server enable	SSH(Stelnet) 서버를 활성화합니다.
ssh user admin	SSH 에 대한 사용자 이름을 구성합니다.
ssh user admin authentication-type password	SSH 사용자에 대한 인증 유형을 구성합니다.
ssh user admin service-type all	SSH 사용자에 대한 서비스 유형을 구성합니다.
ssh server-source all-interface	SSH 액세스를 위한 소스 인터페이스를 구성합니다.
user-interface con 0	콘솔 인터페이스 구성 모드 진입
authentication-mode aaa	콘솔에 대한 인증 모드를 AAA 로 구성합니다.
user-interface vty 0 4	가상 인터페이스(Telnet/SSH) 구성 모드
authentication-mode aaa	VTY 에 대한 인증 모드를 AAA 로 구성합니다.
user privilege level 15 protocol inbound all	인바운드 VTY 액세스에 대한 권한 수준을 구성합니다.

♣ 주의사항

공장 설정을 완전히 초기화하고 스위치를 재설정하려면 버튼을 6 초 이상 누르십시오.

RESET 스위치를 재설정하면 네트워크 서비스 및 Web/SSH/Telnet 관리접속이 중단됩니다.

RESET 버튼을 누를 때 주의하십시오.

■ 공통 명령 뷰

이름	참가 방법	기능
사용자 뷰 user View	사용자가 장치에 로그인하면 사용자 보기로 들어가고 다음 프롬프트가 표시됩니다. <Soltech>	사용자 보기에서 장치의 실행 상태 및 통계를 볼 수 있습니다.
시스템 뷰 System-view	system-view 명령을 실행하고 사용자 보기에서 Enter 키를 누릅니다. 시스템 보기가 표시됩니다. <Soltech> system-view Enter system view, return user view with Ctrl+Z. [Soltech]	시스템 보기에서 장치의 시스템 매개변수를 설정하고 이 보기에서 다른 기능 보기를 입력할 수 있습니다.
인터페이스 뷰 Interface view	interface 명령을 실행하고 인터페이스 유형 및 번호를 지정하여 인터페이스 보기로 들어갑니다. [Soltech] interface gigabitethernet X/Y/Z [Soltech-GigabitEthernetX/Y/Z] X/Y/Z 는 지정해야 하는 인터페이스의 수를 나타냅니다. 스택 ID/카드 번호/인터페이스 시퀀스 번호 형식입니다. GigabitEthernet 인터페이스가 예로 사용됩니다.	인터페이스 보기에서 인터페이스 매개 변수를 구성할 수 있습니다. 인터페이스 매개 변수에는 물리적 속성, 링크 레이어 프로토콜 및 IP 주소가 포함됩니다.

■ 인터페이스 & VLAN 구성

명령	설명
User authentication	
Username: admin	
Password: admin123	초기 설정값
<Soltech>	유저뷰
<Soltech> system-view	관리자모드 <Soltech>에서 구성 모드 [Soltech]로 들어갑니다.
[Soltech] interface GigabitEthernet 1/0/1	물리적 인터페이스 구성 모드로 들어갑니다.
[Soltech-XGigabitEthernet0/0/1] description *Test*	인터페이스에 대한 설명이 구성됩니다.
[Soltech-XGigabitEthernet0/0/1] shutdown	인터페이스를 비활성화합니다.
Soltech-XGigabitEthernet0/0/1] no shutdown	인터페이스를 활성화합니다. 모든 인터페이스는 기본적으로 활성화되어 있습니다.
Soltech-XGigabitEthernet0/0/1] quit	인터페이스 모드를 종료합니다.
[Soltech]vlan batch 2	VLAN 2 만들기
[Soltech]vlan batch 3 to 4	VLAN 3~4 생성
[Soltech-XGigabitEthernet0/0/1] port link-type access	이더넷 인터페이스는 액세스 인터페이스로 구성됩니다.
[Soltech-XGigabitEthernet0/0/1] port default vlan *vlan-id*	인터페이스에 대해 기본 VLAN 이 구성됩니다.
[Soltech-XGigabitEthernet0/0/1] quit	인터페이스 모드를 종료합니다.
[Soltech] interface XGigabitEthernet0/0/3	물리적 인터페이스 구성 모드로 들어갑니다.
[Soltech-XGigabitEthernet0/0/3] port link-type trunk	이더넷 인터페이스는 트렁크 인터페이스로 구성됩니다.
[Soltech-XGigabitEthernet0/0/3] display this	이 인터페이스의 디스플레이 구성
[Soltech-XGigabitEthernet0/0/3] port trunk pvid vlan vlan-id	기본 VLAN 은 트렁크 인터페이스에 대해 구성됩니다.(선택 사항)
[Soltech-XGigabitEthernet0/0/3] quit	
[Soltech]interface Eth-Trunk 1	Link Aggregation 그룹 생성
[Soltech-Eth-Trunk1]quit	
[Soltech]interface GigabitEthernet 0/0/1	GigabitEthernet 0/0/1 진입
[Soltech-GigabitEthernet0/0/1]eth-trunk 1 mode active	Eth-trunk 1 에 Active 모드로 설정
[Soltech-GigabitEthernet0/0/1]quit	

[Soltech]interface GigabitEthernet 0/0/2	GigabitEthernet 0/0/2 진입
[Soltech-GigabitEthernet0/0/2]eth-trunk 1 mode active	Eth-trunk 1 에 Active 모드로 설정
[Soltech-GigabitEthernet0/0/2]quit	
[Soltech] display Eth-Trunk 1	Eth-trunk 1 상태 표시

■ L3 인터페이스, 정적 라우트 & NTP 구성

명령	**설명**
<Soltech> system-view	
[Soltech] interface vlanif *vlan-id*	VLANIF 인터페이스 보기가 표시됩니다.
[Soltech-Vlanif2] description description	(선택 사항) 설명 추가
[Soltech-Vlanif2] ip address *ip-address* { mask | mask-length } [sub]	VLANIF 인터페이스가 레이어 3 연결을 구현하도록 IP 주소가 구성됩니다. 각 VLANIF 인터페이스는 하나의 기본 IP 주소와 최대 31 개의 보조(하위 키워드 포함) IP 주소로 구성할 수 있습니다.(sub 키워드 사용)
[Soltech-Vlanif2] quit	
[Soltech] ip route-static 0.0.0.0 0.0.0.0 x.x.x.x	게이트웨이 주소를 구성합니다.
[Soltech] ntp-service refclock-master	자체(스위치)를 NTP 마스터 클록으로 지정합니다.
[Soltech] undo ntp-service server disable	NTP 서버를 활성화합니다.
[Soltech] quit	구성 모드(system-view)에서 나옵니다.
<Soltech> display current-configuration	현재 운영중인 구성정보를 표시합니다.
<Soltech> display version	이것은 관리자 모드에서 버전을 표시합니다.
<Soltech> dis ntp status	NTP 상태를 표시합니다.
<Soltech> display interface brief	물리적 포트 정보를 표시합니다.
<Soltech> display local-user	현재 구성되어 있는 사용자 정보를 표시합니다.
<Soltech> dis interface	vlan-id 정보를 표시합니다.
<Soltech> dis interface *vlan-id*	vlan-id 정보를 표시합니다.
<Soltech> dis interface Vlanif	레이어 3 인터페이스에 IP 정보를 출력합니다.
<Soltech>display ip route	
<Soltech> Save	구성 저장

<Soltech> quit	관리자모드에서 로그아웃 합니다.

품질보증

- 본 제품에 대한 보증기간은 1 년입니다.
- 정상적으로 사용 중 수리를 요하는 경우

보증기간 내 : 무상수리 / 보증기간 경과 후 : 유상수리

- 소비자의 과실 및 천재지변에 의한 고장 : 유상수리

[사용자 안내문]

A 급 기기(업무용 방송통신기기)

이 기기는 업무용(A 급)으로 전자파적합등록을 한 기기 이오니 판매자 또는

사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는 것을 목적

으로 합니다.

A/S 연락처

주소: 서울시 영등포구 당산로 41 길 11, SK V1 CENTER W 동 215 호
전화: 070-4106-6200 E-mail: as@soltech.co.kr