U-I-F5010HPA

사용자 매뉴얼

Version 11.0.0

Nov 2021

목차

시작하기 1

이 장에서는 사용자 인터페이스 시작 및 액세스에 대한 개요를 제공합니다. 이 장에는 다음 섹션이 포함되어 있습니다.

- *사용 가능한 출판물 및 온라인 도움말*
- *사용자 인터페이스 이해*
- *웹 관리 인터페이스 개요*
- *웹 브라우저를 사용하여 스위치에 액세스하고 로그인합니다.*
- *SNMP 사용*

Note: 이 설명서에서 다루는 주제에 대한 자세한 내용을 보려면 지원 웹사이트(.com)를 방문하십시오.

Note: 새로운 기능과 버그 수정이 포함된 펌웨어 업데이트는 수시로 .com에서 제공됩니다. 일부 제품은 정기적으로 사이트를 확인하여 새 펌웨어를 다운로드할 수 있거나, 수동으로 새 펌웨어를 확인하고 다운로드할 수 있습니다. 제품의 기능이나 동작이 이 가이드에 설명된 내용과 일치하지 않는 경우 펌웨어를 업데이트해야 할 수도 있습니다.

사용 가능한 출판물 및 온라인 도움말

관리형 스위치에 대해 다양한 출판물을 사용할 수 있습니다.

- *섀시 하드웨어 설치 안내서.*
- *스위치 모듈 설치 안내서.*
- *소프트웨어 설치 설명서.*
- *사용 설명서(본 문서). 스위치에 로그인하면 온라인으로 이 문서에 액세스할 수도 있습니다. 도움말 온라인 도움말 > 사용 설명서를 선택하세요.*
- *명령줄 인터페이스 매뉴얼.*

  명령 구조에 대한 자세한 내용은 Command Line Interface Manual을 참조하십시오. 이는 스위치를 구성하는 데 사용되는 CLI 명령에 대한 정보를 제공합니다. CLI 설명, 구문 및 기본값을 제공합니다.

- *소프트웨어 관리 매뉴얼.*

웹 관리 인터페이스에 로그인하면 온라인 도움말을 사용할 수 있습니다.

사용자 인터페이스 이해

관리형 스위치 소프트웨어에는 다음 방법 중 하나를 사용하여 시스템을 구성하고 모니터링하기 위한 일련의 포괄적인 관리 기능이 포함되어 있습니다.

- 웹 사용자 인터페이스
- 단순 네트워크 관리 프로토콜(SNMP)
- 명령줄 인터페이스(CLI)

각 표준 기반 관리 방법을 사용하면 관리되는 스위치 소프트웨어의 구성 요소를 구성하고 모니터링할 수 있습니다. 시스템 관리에 사용하는 방법은 네트워크 크기와 요구 사항, 선호도에 따라 다릅니다.

시리즈 관리형 스위치 사용자 설명서(이 책)에서는 웹 기반 인터페이스를 사용하여 시스템을 관리하고 모니터링하는 방법을 설명합니다.

웹 관리 인터페이스 개요

관리형 스위치에는 스위치 기능을 관리하고 모니터링하기 위한 내장형 웹 서버와 관리 소프트웨어가 포함되어 있습니다. 관리되는 스위치는 관리 소프트웨어 없이 간단한 스위치로 작동합니다. 그러나 관리 소프트웨어를 사용하여 스위치 효율성과 전체 네트워크 성능을 향상시킬 수 있는 고급 기능을 구성할 수 있습니다.

웹 기반 관리를 사용하면 비싸고 복잡한 SNMP 소프트웨어 제품을 사용하는 대신 표준 웹 브라우저를 사용하여 스위치를 원격으로 모니터링, 구성 및 제어할 수 있습니다. 웹 브라우저에서 스위치 성능을 모니터링하고 네트워크 구성을 최적화할 수 있습니다. 웹 기반 관리 인터페이스를 사용하여 VLAN, QoS, ACL과 같은 모든 스위치 기능을 구성할 수 있습니다.

웹 인터페이스를 사용하기 위한 소프트웨어 요구 사항

웹 브라우저를 사용하여 스위치에 액세스하려면 브라우저가 다음 소프트웨어 요구 사항을 충족해야 합니다.

- HTML 버전 4.0 이상
- HTTP 버전 1.1 이상
- 자바 런타임 환경 1.6 이상

웹 브라우저를 사용하여 스위치에 액세스하고 로그인

웹 브라우저를 사용하여 스위치에 액세스하고 로그인할 수 있습니다. 웹 액세스를 사용하려면 관리 시스템에서 관리형 스위치 관리 인터페이스의 IP 주소를 ping할 수 있어야 합니다.

➢ **브라우저 기반 액세스를 사용하여 스위치에 로그인하려면:**

1. 192.168.10.0 서브넷의 고정 IP 주소(예: 192.168.10.101)를 사용하여 컴퓨터를 준비합니다.
2. 컴퓨터 이더넷 포트의 이더넷 케이블을 스위치의 이더넷 포트에 연결합니다.
3. 웹 브라우저를 시작합니다.
4. 웹 브라우저 주소 필드에 스위치의 IP 주소를 입력합니다.

스위치의 기본 IP 주소는 192.168.10.12입니다.

로그인 화면이 표시됩니다.

5. 사용자 이름과 비밀번호를 입력합니다.

   기본 관리자 사용자 이름은 admin이고 기본 관리자 비밀번호는 비어 있습니다. 즉, 비밀번호를 입력하지 마십시오.

6. 로그인 버튼을 클릭하세요.

   웹 관리 인터페이스 메뉴가 표시됩니다.

웹 인터페이스 버튼 및 사용자 정의 필드

다음 표에는 웹 인터페이스의 화면 전체에서 사용되는 명령 버튼이 나와 있습니다.

Table 1. 웹 인터페이스 명령 버튼

버튼	기능
Add	추가 버튼을 클릭하면 테이블의 제목 행에 구성된 새 항목이 추가됩니다.
Apply	Apply 버튼을 클릭하면 업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.
Cancel	취소 버튼을 클릭하면 화면의 구성이 취소되고 화면의 데이터가 스위치의 이전 값으로 재설정됩니다.
Delete	삭제 버튼을 클릭하면 선택한 항목이 제거됩니다.
Refresh	새로고침 버튼을 클릭하면 장치의 최신 정보로 화면이 새로 고쳐집니다.
Logout	로그아웃 버튼을 클릭하면 세션이 종료됩니다.

사용자 정의 필드에는 구성 웹 화면에 달리 명시되지 않는 한 1~159자가 포함될 수 있습니다. 다음을 제외한 모든 문자를 사용할 수 있습니다(해당 기능에 대해 특별히 언급하지 않는 한).

사용자 정의 필드의 잘못된 문자	
\	<
/	>
*	|
?	

인터페이스 명명 규칙

관리형 스위치는 물리적 및 논리적 인터페이스를 지원합니다. 인터페이스는 해당 유형과 인터페이스 번호로 식별됩니다. 물리적 포트는 기가비트 인터페이스이며 전면 패널에 번호가 지정되어 있습니다. 소프트웨어를 사용하여 논리 인터페이스를 구성합니다.

다음 표에서는 스위치에서 사용할 수 있는 모든 인터페이스의 명명 규칙을 설명합니다.

Table 2. 인터페이스 명명 규칙

인터페이스	설명	예제
Physical	물리적 포트는 기가비트 이더넷 인터페이스이며 1부터 순차적으로 번호가 지정됩니다.	0/1, 0/2, 0/3, and so on
Link aggregation group (LAG)	LAG 인터페이스는 브리징 기능에만 사용되는 논리적 인터페이스입니다.	LAG 1, LAG 2, IAG 3, and so on
CPU management interface	스위치 기본 MAC 주소를 담당하는 내부 스위치 인터페이스입니다. 이 인터페이스는 구성할 수 없으며 항상 MAC 주소 테이블에 나열됩니다.	5/1
Routing VLAN interfaces	라우팅 기능에 사용되는 인터페이스입니다.	VLAN 1, VLAN 2, VLAN 3, and so on

웹 관리 인터페이스 장치 보기

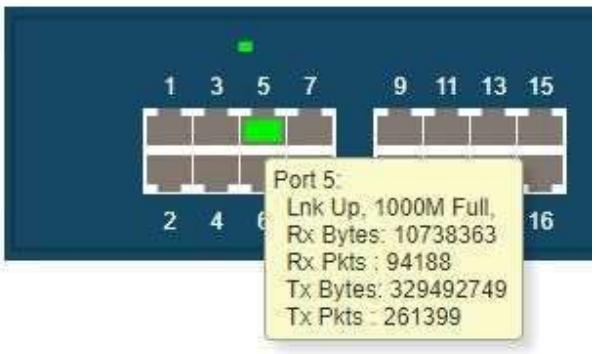
장치 보기는 스위치의 포트를 표시하는 Java® 애플릿입니다. 이 그래픽은 구성 및 모니터링 옵션을 탐색하는 대체 방법을 제공합니다. 그래픽은 또한 장치 포트, 현재 구성 및 상태, 테이블, 기능 구성 요소에 대한 정보를 제공합니다.

- **System > Device View.**
  포트 색상은 포트가 현재 활성 상태인지 여부를 나타냅니다. 녹색은 포트가 활성화되었음을 나타냅니다. 회색은 포트에 오류가 발생했거나 링크가 비활성화되었음을 나타냅니다.

통계 및 구성 옵션을 표시하는 메뉴를 보려면 포트를 클릭하십시오.

메뉴 옵션을 클릭하면 구성 또는 모니터링 옵션이 포함된 화면에 액세스할 수 있습니다.

그래픽을 클릭하고 특정 포트를 클릭하지 않으면 기본 메뉴가 표시됩니다. 이 메뉴에는 화면 상단의 탐색 탭과 동일한 옵션이 포함되어 있습니다.



SNMP 사용

관리형 스위치 소프트웨어는 SNMP 에이전트가 생성하는 트랩을 관리할 수 있는 SNMP 그룹 및 사용자 구성을 지원합니다.

관리형 스위치는 표준 기능을 위한 표준 공용 MIB와 추가 스위치 기능을 지원하는 개인 MIB를 모두 사용합니다. 모든 개인 MIB는 "-" 접두사로 시작됩니다. 인터페이스 구성을 위한 주요 객체는 프라이빗 MIB인 -SWITCHING-MIB에 있습니다. 일부 인터페이스 구성에는 공용 MIB, IF-MIB의 개체도 포함됩니다.

SNMP는 기본적으로 활성화되어 있습니다. 로그인할 때 표시되는 화면인 시스템 정보 화면에는 스위치에 액세스하기 위해 SNMP 관리자를 구성하는 데 필요한 정보가 표시됩니다.

모든 사용자는 SNMP v3 프로토콜을 사용하여 스위치에 연결할 수 있지만 인증 및 암호화를 위해 스위치는 admin이라는 한 명의 사용자만 지원합니다. 따라서 하나의 프로필만 생성하거나 수정할 수 있습니다.

- **SNMP v3 관리자 프로필에 대한 인증 및 암호화 설정을 구성하려면:**

  System > **SNMP** > **SNMP v3** > **User Configuration**.

  사용자 구성 화면이 표시됩니다.

1. 인증을 활성화하려면 MD5 또는 SHA인 인증 프로토콜 옵션을 선택합니다.

2. 암호화를 활성화하려면 암호화 프로토콜 목록에서 DES 옵션을 선택한 다음 암호화 키 필드에 8자 이상의 영숫자 문자로 구성된 암호화 코드를 입력합니다.
3. Apply 버튼을

   클릭하세요. 설정이

   저장되었습니다.

SNMP V1 또는 SNMP V2에 대한 구성 정보에 액세스하려면:
System > **SNMP** > **SNMPv1/v2**
구성할 정보가 포함된 화면을 선택하세요.

시스템 정보 구성 2

이 장에서는 다음 주제를 다룹니다:

- *초기 설정*
- *DHCP 서버 설정 구성*
- *기본 PoE 구성*
- *SNMP 구성*
- *LLDP 개요*
- *ISDP 구성*
- *타이머 일정*

초기 설정

공장 설정이 있는 스위치에 로그인하면 초기 설정 화면이 표시됩니다.

➢ **초기 시스템 구성을 수행하려면:**

1. 192.168.10.0 서브넷의 고정 IP 주소(예: 192.168.10.101)를 사용하여 컴퓨터를 준비합니다.
2. 컴퓨터 이더넷 포트의 이더넷 케이블을 스위치의 이더넷 포트에 연결합니다.
3. 웹 브라우저를 시작합니다.
4. 웹 브라우저 주소 필드에 스위치의 IP 주소를 입력합니다.

   스위치의 기본 IP 주소는 192.168.10.12입니다.
   로그인 화면이 표시됩니다.
5. 사용자 이름과 비밀번호를 입력합니다.

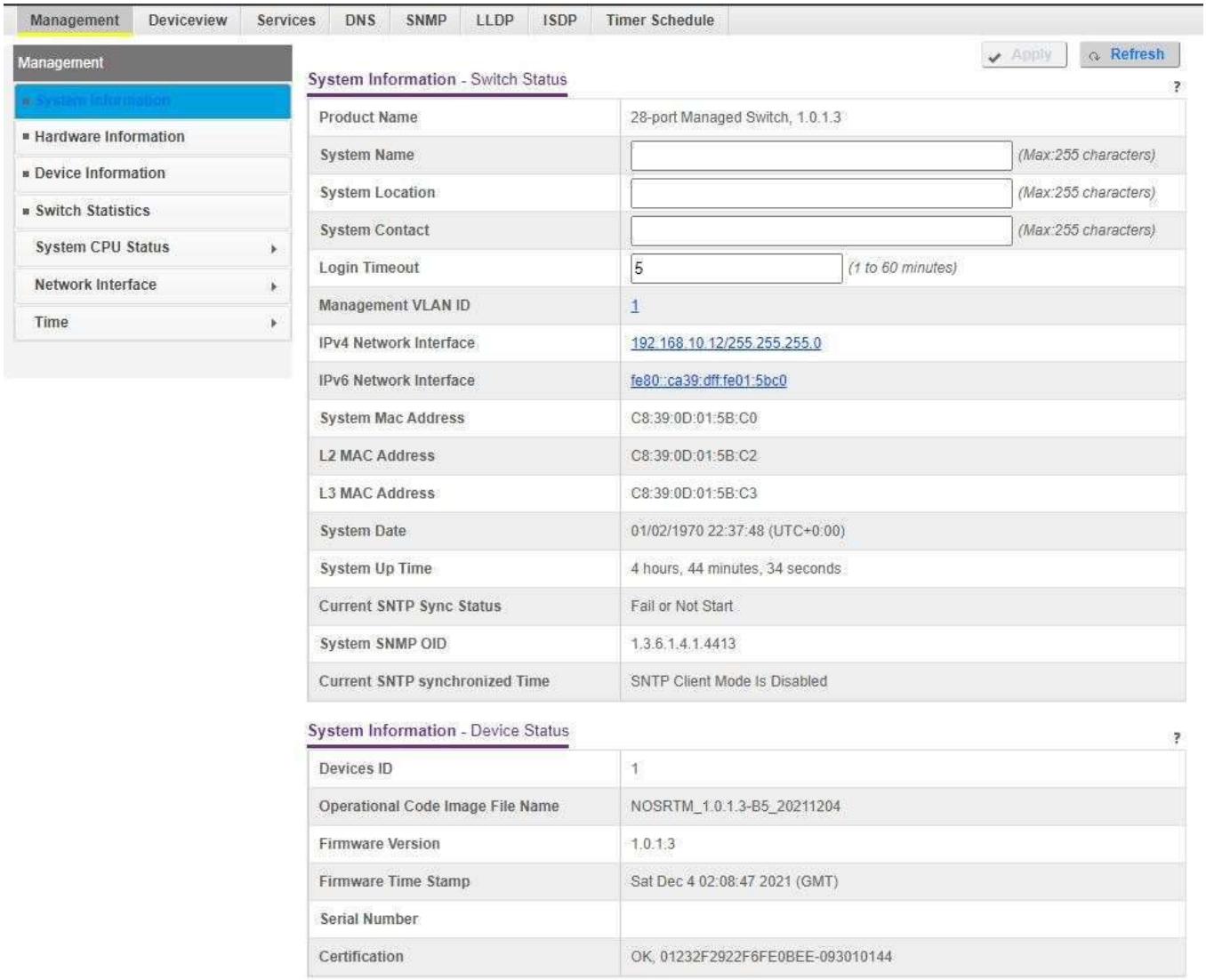
   기본 관리자 사용자 이름은 admin이고 기본 관리자 비밀번호는 비어 있습니다. 즉, 비밀번호를 입력하지 마십시오.
6. 로그인 버튼을 클릭하세요.

   웹 관리 인터페이스 메뉴가 표시됩니다.

시스템 정보 보기 또는 정의

로그인하면 시스템 정보 화면이 표시됩니다. 일반 장치 정보를 구성하고 볼 수 있습니다.

System > **Management** > System information.



1. System Name 필드에 이 스위치를 식별하는 이름을 입력합니다.

   이름은 최대 255자까지 사용할 수 있습니다. 공장 기본값은 공백입니다.

2. System Location 필드에 스위치 위치를 입력합니다.

   위치는 최대 255자까지 사용할 수 있습니다. 공장 기본값은 공백입니다.

3. 이 스위치에 대한 연락 담당자의 이름인 시스템 연락처를 입력합니다.

   연락처 이름은 최대 255자까지 사용할 수 있습니다. 공장 기본값은 공백입니다.

4. Apply 버튼을 클릭하세요.

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

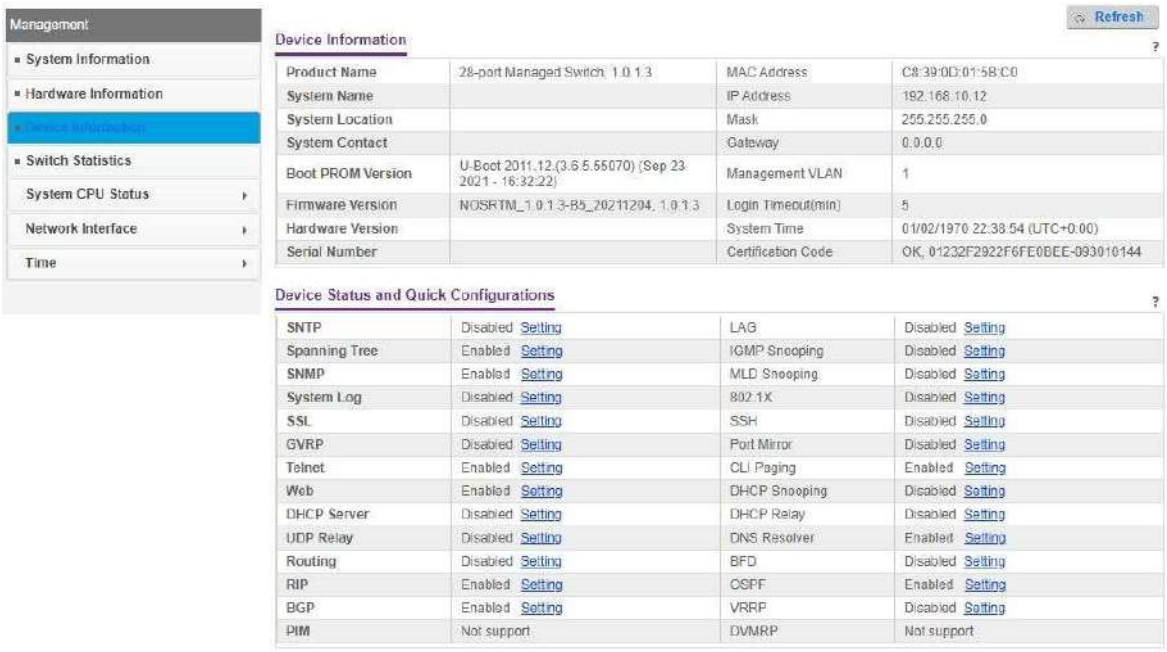
Table 3. 시스템 정보

필드	설명
Product Name	이 스위치의 제품 이름입니다.
IPv4 Management VLAN Interface	관리 VLAN 인터페이스에 할당된 IPv4 주소 및 마스크입니다.
IPv6 Management VLAN Interface	관리 VLAN 인터페이스에 할당된 IPv6 접두사 및 접두사 길이입니다.
Management VLAN ID	스위치의 관리 VLAN ID입니다. 표시된 관리 VLAN ID 값을 클릭하면 구성 화면으로 이동합니다.
IPv4 Service Port Network Interface	서비스 포트 인터페이스에 할당된 IPv4 주소 및 마스크입니다.
IPv6 Service Port Network Interface	서비스 포트 인터페이스에 할당된 IPv6 접두사 및 접두사 길이입니다.
IPv4 Loopback Interface	루프백 인터페이스에 할당된 IPv4 주소 및 마스크입니다.
IPv6 Loopback Interface	루프백 인터페이스에 할당된 IPv6 접두사 및 접두사 길이입니다.
System Date	현재 날짜입니다.
System Up time	마지막 스위치 재부팅 이후의 시간(일, 시간, 분)입니다.
Current SNTP Sync Status	현재 SNTP 동기화 상태입니다.
System SNMP OID	스위치의 엔터프라이즈 MIB에 대한 기본 개체 ID입니다.
System Mac Address	보편적으로 할당된 네트워크 주소입니다.
Service Port MAC Address	대역 외 연결에 사용되는 MAC 주소입니다.
L2 MAC Address	레이어 2 네트워크 세그먼트의 통신에 사용되는 MAC 주소입니다.
L3 MAC Address	레이어 3 네트워크 세그먼트의 통신에 사용되는 MAC 주소입니다.
Supported Java Plugin Version	지원되는 Java 플러그인 버전입니다.
Current SNTP Synchronized Time	SNTP 동기화 시간입니다.

장치 상태 보기

System > **Management** >Device Information

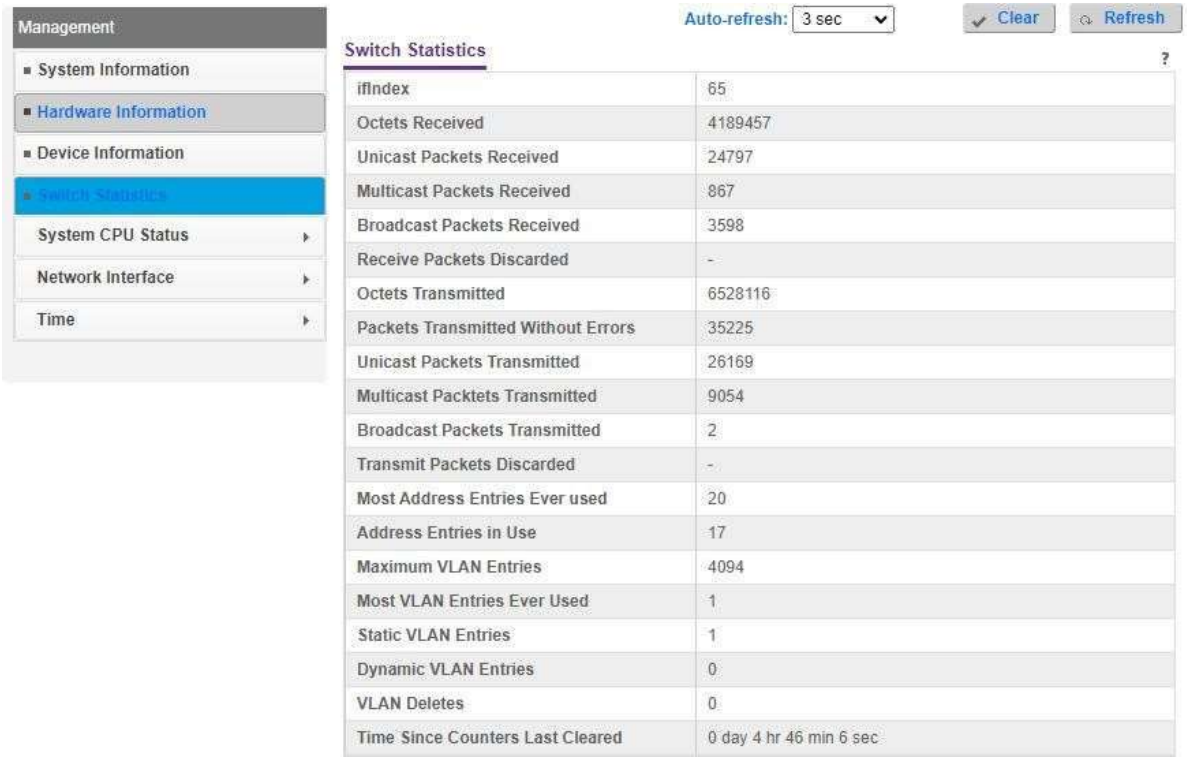
1.5 cm



화면을 새로 고치려면 Refresh버튼을 누르세요

스위치 통계 보기

System > **Management** >Switch Statistics.



1.5 cm

모든 카운터를 지우고 모든 스위치 요약 및 세부 통계를 기본값으로 재설정하려면 Clear 버튼을 클릭하십시오. 버려진 패킷 수는 지울 수 없습니다.

다음 표에서는 스위치 통계 정보에 대해 설명합니다.

Table 9. 스위치 통계 정보

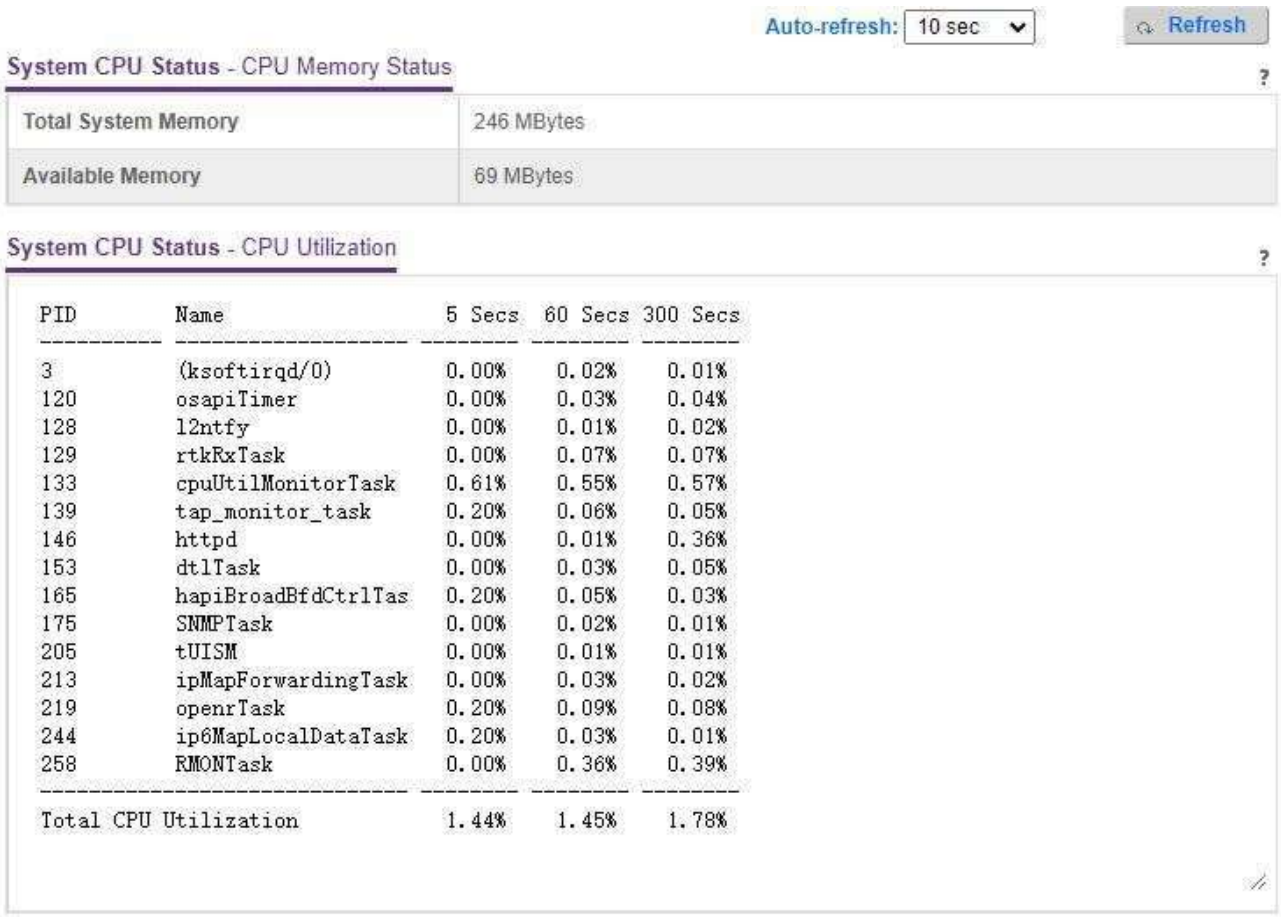
필드	설명
ifIndex	이 스위치의 프로세서와 관련된 인터페이스 테이블 항목의 ifIndex입니다.
Octets Received	프로세서가 수신한 데이터의 총 옥텟 수입니다(프레이밍 비트는 제외하지만 FCS 옥텟은 포함).
Packets Received Without Errors	프로세서가 수신한 총 패킷 수(브로드캐스트 패킷 및 멀티캐스트 패킷 포함)입니다.
Unicast Packets Received	상위 계층 프로토콜로 전달되는 하위 네트워크-유니캐스트 패킷 수입니다.
Multicast Packets Received	멀티캐스트 주소로 전달된 수신 패킷의 총 수입니다. 이 숫자에는 브로드캐스트 주소로 전달되는 패킷이 포함되지 않습니다.
Broadcast Packets Received	브로드캐스트 주소로 전달된 수신 패킷의 총 수입니다. 여기에는 멀티캐스트 패킷이 포함되지 않습니다.
Receive Packets Discarded	상위 계층 프로토콜로 전달되는 것을 방지하기 위해 오류가 감지되지 않았음에도 삭제된 인바운드 패킷 수입니다. 패킷을 삭제하는 가능한 이유는 버퍼 공간을 확보하기 위한 것일 수 있습니다.
Octets Transmitted	프레임 문자를 포함하여 인터페이스 외부로 전송된 총 옥텟 수입니다.
Packets Transmitted Without Errors	인터페이스에서 전송된 총 패킷 수입니다.
Unicast Packets Transmitted	폐기되거나 전송되지 않은 패킷을 포함하여 하위 네트워크-유니캐스트 주소로 전송되는 상위 수준 프로토콜에서 요청한 총 패킷 수입니다.
Multicast Packets Transmitted	삭제되거나 전송되지 않은 패킷을 포함하여 멀티캐스트 주소로 전송되는 상위 수준 프로토콜에서 요청한 총 패킷 수입니다.
Broadcast Packets Transmitted	폐기되거나 전송되지 않은 패킷을 포함하여 브로드캐스트 주소로 전송되는 상위 프로토콜에서 요청한 총 패킷 수입니다.
Transmit Packets Discarded	상위 계층 프로토콜로 전달되는 것을 방지하기 위해 오류가 감지되지 않았음에도 삭제된 아웃바운드 패킷 수입니다. 패킷을 삭제하는 가능한 이유는 버퍼 공간을 확보하기 위한 것일 수 있습니다.

1.5 cm

Most Address Entries Ever Used	가장 최근 재부팅 이후 이 스위치가 학습한 전달 데이터베이스 주소 테이블 항목의 최대 수입니다.
Address Entries in Use	이 스위치에 대한 전달 데이터베이스 주소 테이블의 학습된 정적 항목 수입니다.
Maximum VLAN Entries	이 스위치에 허용되는 최대 가상 LAN(VLAN) 수입니다.
Most VLAN Entries Ever Used	마지막 재부팅 이후 이 스위치에서 활성화된 VLAN의 최대 수입니다.
Static VLAN Entries	정적으로 생성된 이 스위치의 현재 활성 VLAN 항목 수입니다.
Dynamic VLAN Entries	GVRP 등록에 의해 생성된 이 스위치의 현재 활성 VLAN 항목 수입니다.
VLAN Deletes	마지막 재부팅 이후 생성된 후 삭제된 이 스위치의 VLAN 수입니다.
Time Since Counters Last Cleared	이 스위치에 대한 통계가 마지막으로 지워진 이후 경과된 시간(일, 시, 분, 초)입니다.

시스템 CPU 상태 보기

System > **Management** > **System CPU Status**.



메모리 정보, 작업 관련 정보, 작업당 CPU 사용률이 포함된 CPU 사용률 정보를 볼 수 있습니다.

다음 표에는 CPU 메모리 상태 정보가 설명되어 있습니다.

Table 8. CPU 메모리 상태 정보

필드	설명
Total System Memory	스위치의 총 메모리(KB)입니다.
Available Memory	스위치에 사용 가능한 메모리 공간(KB)입니다.

CPU 임계값 구성

CPU 사용률 임계값 알림 기능을 사용하면 임계값을 초과할 경우 알림을 트리거하는 임계값을 구성할 수 있습니다. 알림은 SNMP 트랩 및 syslog 메시지를 통해 수행됩니다.

System > Management > System CPU Status > CPU Threshold

1. 상승 임계값을 구성합니다.

   구성된 기간 동안 총 CPU 사용률이 이 임계값을 초과하면 알림이 생성됩니다. 범위는 1~100입니다.

2. 상승 간격 값을 구성합니다.

   이 사용률 모니터링 기간은 5초의 배수로 5초에서 86400초까지 구성할 수 있습니다.

3. 하강 임계값을 구성합니다.

   구성된 기간 동안 총 CPU 사용률이 이 수준 아래로 떨어지면 알림이 트리거됩니다.

   사용률 하락 임계값은 상승 임계값보다 작거나 같아야 합니다. 사용률 임계값 감소 알림은 이전에 임계값 상승 알림이 완료된 경우에만 이루어집니다. 사용률 감소 임계값 및 기간 구성은 선택 사항입니다. Falling CPU Utilization 매개변수가 구성되지 않은 경우 Rising CPU Utilization 매개변수와 동일한 값을 사용합니다. 범위는 1~100입니다.

4. 하강 간격을 구성합니다.

   사용률 모니터링 기간은 5초에서 86400초까지 5초의 배수로 구성할 수 있습니다.

5. CPU 여유 메모리 임계값을 KB 단위로 구성합니다.

화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

System > Management > Management Interfaces > IPv4 Management VLAN Configuration.

1. 스위치의 관리 VLAN ID를 지정합니다.

   관리 VLAN은 스위치 관리에 사용됩니다. 1~4093 범위의 값으로 구성할 수 있습니다.

Table 17. IPv4 Management VLAN Configuration

Field	Description
MAC Address	VLAN 라우팅 인터페이스에 할당된 MAC 주소입니다.
Routing Interface Status	링크 상태가 작동 중인지 작동 중지인지를 나타냅니다.
Burned-in MAC Address	대역 외 연결에 사용되는 번인된 MAC 주소입니다.
Interface Status	링크 상태가 작동 중인지 작동 중지인지를 나타냅니다.
DHCP Client Identifier	네트워크에서 클라이언트에 할당된 식별 코드입니다. DHCP 서버는 이 코드를 사용하여 이 장치를 식별합니다.

2. 서비스 포트 구성 프로토콜 라디오 버튼을 선택합니다.
   - **BootP**. 다음 부팅 주기 동안 장치의 BootP 클라이언트는 네트워크의 BootP 서버에서 정보를 얻으려는 시도로 BootP 요청을 브로드캐스트합니다.
   - **DHCP**. 다음 부팅 주기 동안 장치의 DHCP 클라이언트는 네트워크의 DHCP 서버에서 정보를 얻으려는 시도로 DHCP 요청을 브로드캐스트합니다.
   - **None**. 장치는 네트워크 정보를 동적으로 획득하려고 시도하지 않습니다.
3. 인터페이스의 IP 주소를 지정합니다.

   공장 기본값은 192.168.10.12입니다.
4. 인터페이스의 IP 서브넷 마스크를 지정합니다.

   공장 기본값은 255.255.0.0입니다.

5. Apply 버튼을 클릭하세요.

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

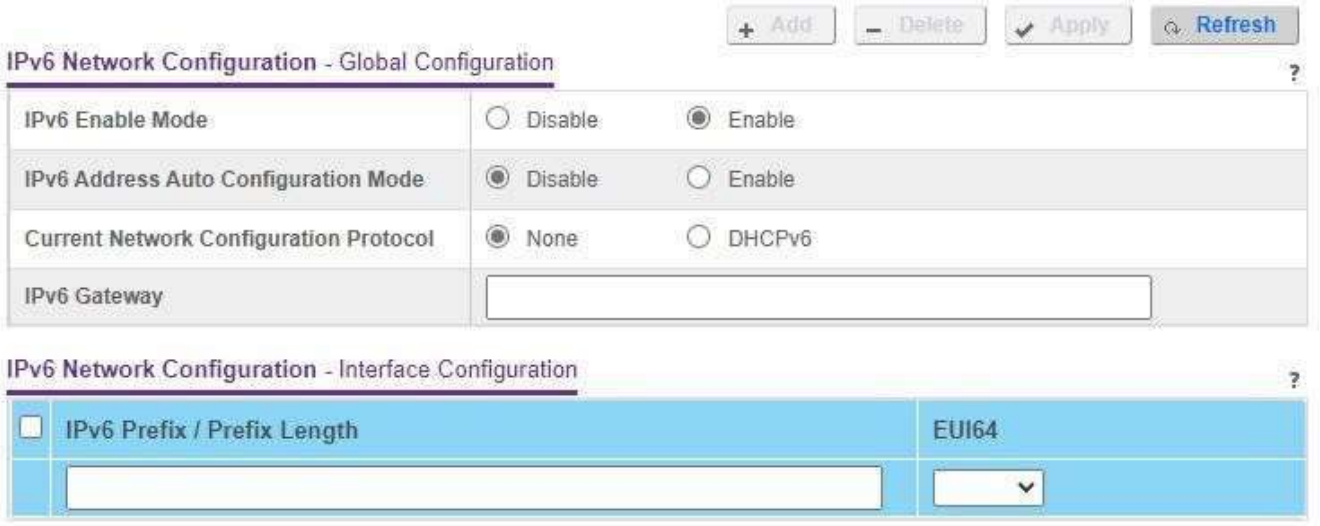
IPv6 서비스 포트 구성

1.5 cm

서비스 포트에 IPv6 네트워크 정보를 구성할 수 있습니다. 서비스 포트는 장치의 대역 외 관리를 위한 전용 이더넷 포트입니다. 이 포트의 트래픽은 스위치 포트의 작동 네트워크 트래픽과 분리되며 작동 네트워크로 전환하거나 라우팅할 수 없습니다..

- **IPv6 서비스 포트를 구성하려면:**

System > Management > Management Interfaces > IPv6 Service Port Configuration.



1. IPv6 모드 Enable 또는 Disable 라디오 버튼을 선택합니다.

   서비스 포트의 IPv6 관리 모드를 지정합니다..

2. 서비스 포트 구성 프로토콜 없음 또는 DHCP 라디오 버튼을 선택합니다.

   장치가 DHCPv6 서버에서 네트워크 정보를 획득하는지 여부를 지정합니다. 없음을 선택하면 서비스 포트에서 DHCPv6 클라이언트가 비활성화됩니다.

3. IPv6 Stateless Address AutoConfig 모드 Enable 또는 Disable 라디오 버튼을 선택합니다.
   - **Enable**. 서비스 포트는 IPv6 NDP(Neighbor Discovery Protocol) 및 라우터 광고 메시지를 통해 IPv6 주소를 획득할 수 있습니다.
   - **Disable**. 서비스 포트는 IPv6 주소를 획득하기 위해 기본 IPv6 주소 자동 구성 기능을 사용하지 않습니다.

   이는 서비스 포트에 IPv6 상태 비저장 주소 자동 구성 모드를 설정합니다.

4. DHCPv6 클라이언트 DUID 필드에는 DHCPv6 서버에 메시지를 보낼 때 DHCPv6 클라이언트(활성화된 경우)에서 사용하는 클라이언트 식별자가 표시됩니다.
5. IPv6 게이트웨이를 구성하려면 IPv6 게이트웨이 변경 check box을

1.5 cm

선택합니다.

IPv6 게이트웨이는 IPv6 서비스 포트 인터페이스의 기본 게이트웨이입니다.

6. IPv6 게이트웨이 필드를 사용하여 IPv6 서비스 포트 인터페이스에 대한 기본 게이트웨이를 지정합니다.

   IPv6 주소 추가/삭제 테이블에는 서비스 포트 인터페이스에서 수동으로 구성된 고정 IPv6 주소가 나열됩니다.

7. 다음을 지정합니다.
   a. IPv6 주소 필드에서 서비스 포트 인터페이스에 추가하거나 제거할 IPv6 주소를 지정합니다.
   b. IPv6 주소에 대해 EUI(확장 범용 식별자) 플래그를 활성화하려면 EUI 플래그 옵션을 선택하고, 플래그를 생략하려면 옵션을 선택 취소하세요.
8. Add 버튼을 클릭합니다.

   서비스 포트 인터페이스에 IPv6 주소가 추가됩니다.

9. 선택한 IPv6 주소를 삭제하려면 Delete 버튼을 클릭하세요.
10. Apply 버튼을 클릭하세요.

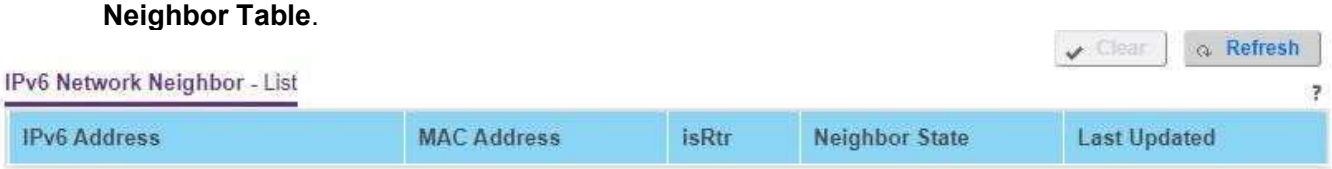
    업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

IPv6 네트워크 인터페이스 인접 테이블 보기

➢ **IPv6 네트워크 이웃 테이블을 보려면:**

Select **System > Management > Management Interfaces > IPv6 Network Interface Neighbor Table**.



다음 표에는 IPv6 네트워크 인터페이스 인접 테이블 정보가 표시되어 있습니다.

Table 15. IPv6 네트워크 인터페이스 인접 테이블 정보

필드	설명
IPv6 address	네트워크 인터페이스에 표시되는 이웃 스위치의 IPv6 주소입니다.

1.5 cm

MAC address	이웃 스위치의 MAC 주소입니다.
IsRtr	**이웃 시스템이 라우터이면 true(1), 그렇지 않으면 false(2)입니다.**
Neighbor State	이웃 스위치의 상태: • **reachable (1)**. 이 스위치로 이웃에 접근할 수 있습니다. • **stale (2)**. 이웃에 대한 정보가 삭제 예정입니다. • **delay (3)**. 지연 기간 동안 이웃으로부터 정보가 수신되지 않았습니다. • **probe (4)**. 스위치가 이 인접 항목을 검색하려고 시도하고 있습니다. • **unknown (6)**. 알 수 없는 상태입니다.
Last Updated	이 네이버가 업데이트된 마지막 sysUpTime입니다.

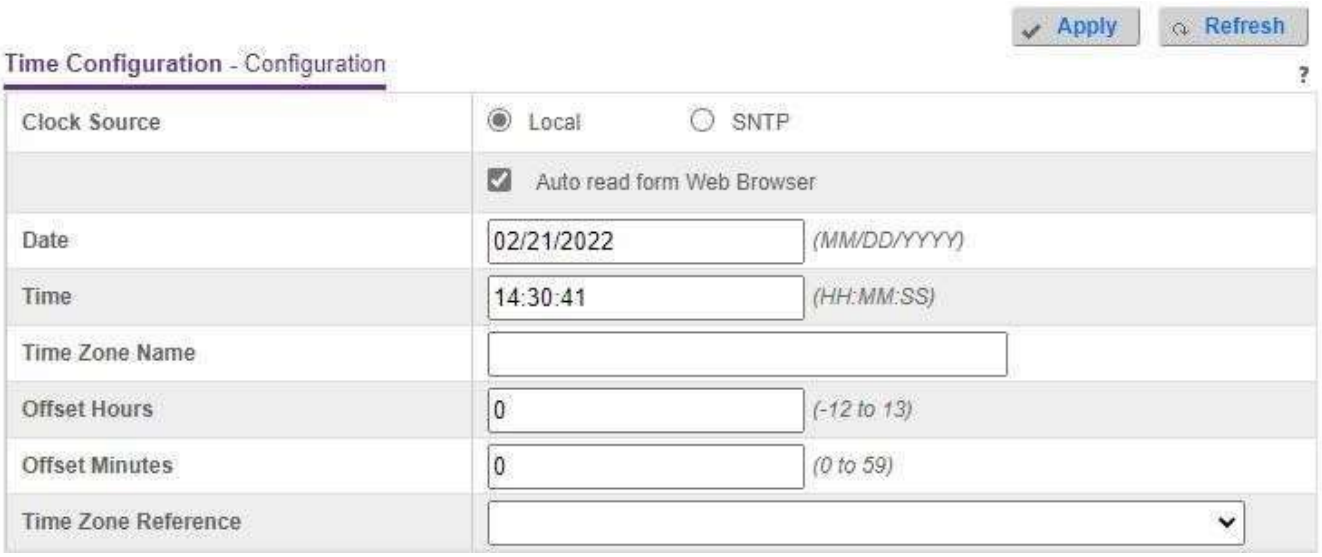
Time

소프트웨어는 SNTP(Simple Network Time Protocol)를 지원합니다. 이름에서 알 수 있듯이 이는 주로 인터넷을 통해 데이터 전송이 처리될 때 네트워크로 연결된 컴퓨터 시스템의 시계를 동기화하는 시스템인 네트워크 시간 프로토콜(Network Time Protocol)의 덜 복잡한 버전입니다.

시간 설정 구성

➢ **시간 설정을 구성하려면:**

System > Management > Time > Time Configuration.



1.5 cm

1. 클럭 소스 Local 또는 SNTP 라디오 버튼을 선택합니다.

   기본값은 SNTP입니다. 다음 두 가지 조건이 충족되는 경우에만 로컬 시계를 SNTP로 설정할 수 있습니다.

   - SNTP 서버가 구성되었습니다.
   - SNTP 마지막 시도 상태가 성공입니다.

2. Date 필드에 현재 날짜를 월, 일, 연도 단위로 지정합니다.
3. Time 필드에 현재 시간을 시, 분, 초 단위로 지정합니다.
4. Apply 버튼을 클릭하세요.

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

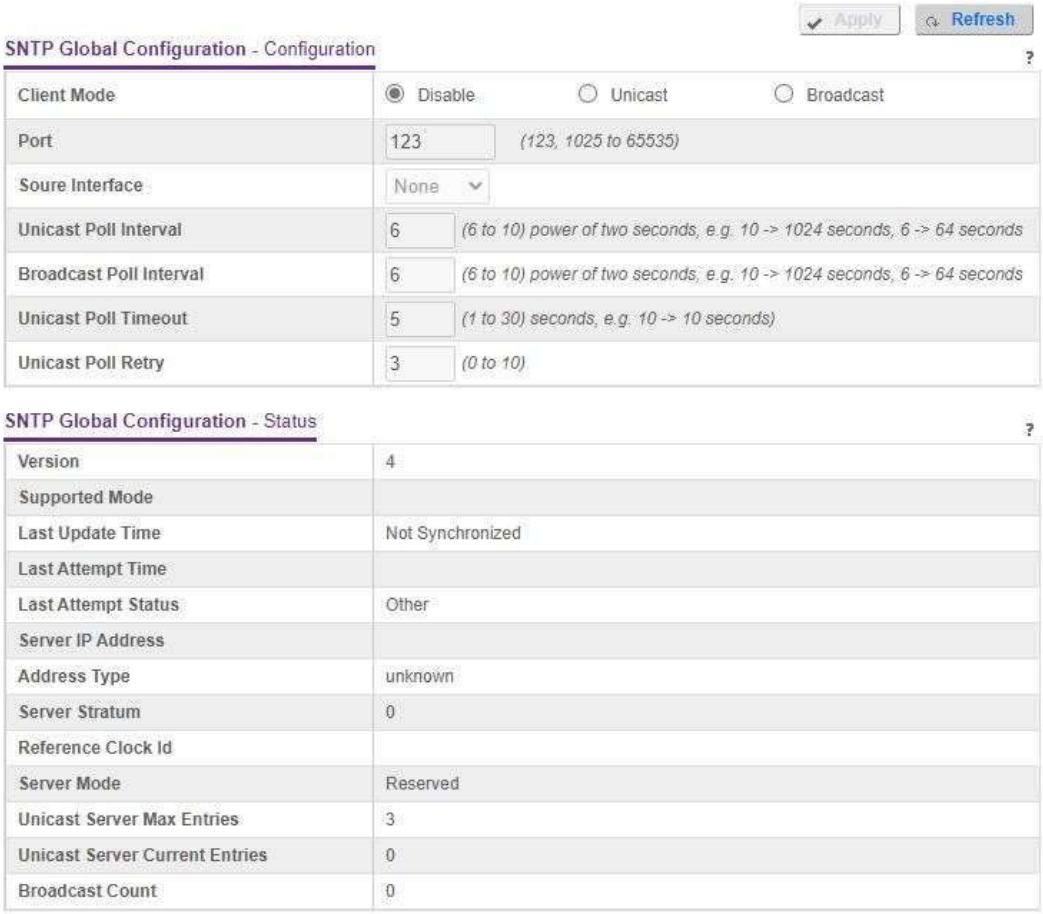
화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

SNTP 전역 설정 구성

➢ **SNTP 전역 설정을 구성하려면:**

System > Management > Time > Time Configuration > SNTP Global Configuration.

SNTP 옵션을 클럭 소스로 선택하면 SNTP 전역 구성 섹션이 화면의 시간 구성 섹션 아래에 표시됩니다.



1. 클라이언트 모드 라디오 버튼을 선택하여 SNTP 클라이언트의 작동 모드를 지정합니다.
   - **Disable**. SNTP가 작동하지 않습니다. SNTP 요청은 클라이언트에서 전송되지 않으며 수신된 SNTP 메시지는 처리되지 않습니다.
   - **Unicast**. SNTP는 지점 간 방식으로 작동합니다. 유니캐스트 클라이언트는 유니캐스트 주소로 지정된 서버에 요청을 보내고 시간과 선택적으로 서버에 대한 왕복 지연 및 로컬 시계 오프셋을 결정할 수 있는 응답을 기대합니다.
   - **Broadcast**. SNTP는 멀티캐스트 모드와 동일한 방식으로 작동하지만 멀티캐스트 주소 대신 로컬 브로드캐스트 주소를 사용합니다. 브로드캐스트 주소에는 단일 서브넷 범위가 있는 반면 멀티캐스트 주소에는 인터넷 전체 범위가 있습니다.

   기본값은 Unicast입니다.
2. 포트 필드에서 SNTP 클라이언트가 서버 패킷을 수신하는 로컬 UDP 포트를 지정합니다.

   허용 범위는 1025~65535이고 값은 123이다. 기본값은 123이다. 기본값을 설정하면 SNTP 패킷에 사용되는 실제 클라이언트 포트 값은 운영체제에 의해 할당됩니다.
3. SNTP 클라이언트에 사용할 Source Interface를 선택합니다.

1.5 cm

가능한 값은 다음과 같습니다.

- None
- VLAN 1
- Routing interface
- Routing VLAN
- Routing loopback interface
- Tunnel interface
- Service port

기본적으로 VLAN 1은 소스 인터페이스로 사용됩니다.

4. Unicast Poll Interval을 지정합니다

   이는 유니캐스트 모드로 구성된 경우 2의 거듭제곱으로 표시되는 유니캐스트 폴링 요청 간의 초 수입니다. 허용되는 범위는 6~10입니다. 기본값은 6입니다.

5. Broadcast Poll Interval을 지정합니다

   이는 브로드캐스트 모드로 구성된 경우 2의 거듭제곱으로 표현되는 브로드캐스트 폴링 요청 간의 초 수입니다. 이 간격이 만료되기 전에 수신된 방송은 삭제됩니다. 허용되는 범위는 6~10입니다. 기본값은 6입니다.

6. Unicast Poll Timeout을 지정합니다

   유니캐스트 모드로 구성되었을 때 SNTP 응답을 기다리는 시간(초)입니다. 허용되는 범위는 1~30입니다. 기본값은 5입니다.

7. Unicast Poll Retry를 지정합니다.

   유니캐스트 모드로 구성된 경우 다음 구성된 서버를 사용하기 전에 첫 번째 시간 초과 후 SNTP 서버에 대한 요청을 재시도하는 횟수입니다. 허용되는 범위는 0~10입니다. 기본값은 1입니다.

8. Apply버튼을 클릭합니다.

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

새로 고침을 하기 위해서는 Refresh 버튼을 클릭하세요

SNTP 글로벌 상태 보기

SNTP 옵션을 클럭 소스로 선택하면 SNTP 전역 상태가 화면의 SNTP 전역 구성 섹션 아래에 표시됩니다.

1.5 cm

- **SNTP 글로벌 상태를 보려면:**

System > Management > Time > Time Configuration > SNTP Global Status

SNTP 옵션을 클럭 소스로 선택하면 SNTP 글로벌 상태가 SNTP 글로벌 구성 섹션 아래에 표시됩니다.

다음 표에는 구성할 수 없는 SNTP 전역 상태 정보가 표시되어 있습니다.

Table 19. SNTP 글로벌 상태

필드	설명
Version	클라이언트가 지원하는 SNTP 버전입니다..
Supported mode	클라이언트가 지원하는 SNTP 모드입니다. 클라이언트는 여러 모드를 지원할 수 있습니다.
Last Update Time	SNTP 클라이언트가 시스템 시계를 마지막으로 업데이트한 현지 날짜 및 시간(UTC)입니다.
Last Attempt Time	마지막 SNTP 요청 또는 원치 않는 메시지 수신의 현지 날짜 및 시간(UTC)입니다.
Last Attempt Status	유니캐스트 및 브로드캐스트 모드 모두에 대한 마지막 SNTP 요청 또는 원치 않는 메시지의 상태입니다. 서버로부터 메시지가 수신되지 않은 경우 기타 상태가 표시됩니다. 이 값은 모든 작동 모드에 적합합니다. • **Other**. 다음 열거형 값이 없습니다. • **Success**. SNTP 작업이 성공했으며 시스템 시간이 업데이트되었습니다. • **Request Timed Out**. SNTP 서버로부터 응답을 받지 못한 채 직접 SNTP 요청 시간이 초과되었습니다. • **Bad Date Encoded**. SNTP 서버에서 제공한 시간이 유효하지 않습니다. • **Version Not Supported**. 서버에서 지원하는 SNTP 버전이 클라이언트에서 지원하는 버전과 호환되지 않습니다. • **Server Unsynchronized**. SNTP 서버는 해당 피어와 동기화되지 않습니다. 이는 SNTP 메시지의 도약 표시 필드를 통해 표시됩니다. • **Server Kiss Of Death**. SNTP 서버에서 이 서버로 더 이상 쿼리가 전송되지 않는다고 표시했습니다. 이는 서버로부터 수신된 메시지에서 0과 동일한 Stratum 필드로 표시됩니다.
Server IP Address	마지막으로 수신된 유효한 패킷에 대한 서버의 IP 주소입니다. 서버로부터 메시지가 수신되지 않으면 빈 문자열이 표시됩니다.
Address Type	마지막으로 수신된 유효한 패킷에 대한 SNTP 서버 주소의 주소 유형입니다.

1.5 cm

Server Stratum	마지막으로 수신된 유효한 패킷에 대해 요청된 서버 계층입니다.
Reference Clock ID	마지막으로 수신된 유효한 패킷에 대한 서버의 참조 시계 식별자입니다.
Server mode	마지막으로 수신된 유효한 패킷에 대한 서버의 모드입니다.
Unicast Server Max Entries	이 클라이언트에 구성할 수 있는 유니캐스트 서버 항목의 최대 수입니다.
Unicast Server Current Entries	이 클라이언트에 대해 구성된 현재 유효한 유니캐스트 서버 항목 수입니다.
Broadcast Count	마지막 재부팅 이후 SNTP 클라이언트가 수신하고 처리한 원치 않는 브로드캐스트 SNTP 메시지 수입니다.

SNTP Server 구성

SNTP는 최대 밀리초까지 정확한 네트워크 장치 시계 시간 동기화를 보장합니다. 시간 동기화는 네트워크 SNTP 서버에 의해 수행됩니다. 소프트웨어는 SNTP 클라이언트로만 작동하며 다른 시스템에 시간 서비스를 제공할 수 없습니다.

시간 소스는 계층별로 설정됩니다. 계층은 참조 시계의 정확도를 정의합니다. 계층이 높을수록(0이 가장 높음) 시계가 더 정확합니다. 장치는 Stratum 2 장치이므로 Stratum 1 이상에서 시간을 수신합니다.

다음은 계층의 예입니다.

- **Stratum 0**. GPS 시스템과 같은 실시간 시계가 시간 소스로 사용됩니다.
- **Stratum 1**. Stratum 0 시간 소스에 직접 연결된 서버가 사용됩니다. Stratum 1 시간 서버는 기본 네트워크 시간 표준을 제공합니다.
- **Stratum 2**. 시간 소스는 네트워크 경로를 통해 Stratum 1 서버와 떨어져 있습니다. 예를 들어 Stratum 2 서버는 Stratum 1 서버에서 NTP를 통해 네트워크 링크를 통해 시간을 수신합니다.

SNTP 서버로부터 수신된 정보는 시간 수준과 서버 유형을 기준으로 평가됩니다.

SNTP 시간 정의는 다음 시간 수준에 따라 평가되고 결정됩니다.

- **T1**. 클라이언트가 원래 요청을 보낸 시간입니다.
- **T2**. 서버가 원래 요청을 수신한 시간입니다.
- **T3**. 서버가 응답을 보낸 시간입니다.
- **T4**. 클라이언트가 서버의 응답을 받은 시간입니다.

1.5 cm

장치는 서버 시간에 대해 유니캐스트 서버 유형을 폴링할 수 있습니다.

유니캐스트 정보에 대한 폴링은 IP 주소가 알려진 서버를 폴링하는 데 사용됩니다. 장치에 구성된 SNTP 서버는 동기화 정보를 위해 폴링되는 유일한 서버입니다. T1~T4는 서버 시간을 결정하는 데 사용됩니다. 이는 가장 안전한 방법이므로 장치 시간을 동기화하는 데 선호되는 방법입니다. 이 방법을 선택하면 SNTP 서버 구성 화면을 사용하여 장치에 정의된 SNTP 서버에서만 SNTP 정보가 허용됩니다.

장치는 적극적으로 정보를 요청하거나 모든 폴링 간격으로 동기화 정보를 검색합니다.

Simple Network Time Protocol SNTP 서버를 추가하고 수정하기 위한 정보를 보고 수정할 수 있습니다.

- **SNTP 서버 설정을 구성하려면:**

  System > Management > Time > SNTP Server Configuration.

1. Server Type 목록에서 구성된 SNTP 서버 주소의 주소 유형을 선택합니다. 가능한 값은 다음과 같습니다.

   - IPv4
   - IPv6
   - DNS

   기본값은 IPv4입니다.

2. Address 필드에 SNTP 서버의 주소를 지정합니다.

   이는 인코딩된 유니캐스트 IP 주소 또는 SNTP 서버의 호스트 이름을 포함하는 최대 64자의 텍스트 문자열입니다. 유니캐스트 SNTP 요청은 이 주소로 전송됩니다. 이 주소가 DNS 호스트 이름인 경우 해당 호스트 이름은 SNTP 요청이 전송될 때마다 IP 주소로 확인됩니다.

1.5 cm

3. SNTP 요청이 전송되는 SNTP 서버의 포트 번호를 입력합니다.

   유효한 범위는 1~65535입니다. 기본값은 123입니다.

4. SNTP 요청이 전송되는 서버 순서를 결정할 때 이 서버 항목의 Priority를 지정합니다.

   클라이언트는 성공적인 응답이 수신되거나 모든 서버가 소진될 때까지 계속해서 다른 서버에 요청을 보냅니다. 우선순위는 서버를 쿼리하는 순서를 나타냅니다. 우선 순위가 1인 서버 항목은 우선 순위가 2인 서버보다 먼저 쿼리됩니다. 둘 이상의 서버가 동일한 우선순위를 갖는 경우 요청 순서는 이 테이블에 있는 항목의 사전순 순서를 따릅니다. 유효한 범위는 1~3입니다. 기본값은 1입니다.

5. 서버에서 실행 중인 NTP Version을 지정합니다.

   범위는 1~4입니다. 기본값은 4입니다.

6. Add 버튼을 클릭합니다.

   SNTP 서버 항목이 추가됩니다. 그러면 업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

7. SNTP 서버를 추가하려면 이전 단계를 반복합니다.

   최대 3개의 SNTP 서버를 구성할 수 있습니다.

8. 기존 SNTP 서버의 설정을 변경하려면 구성된 서버 옆에 있는 check box을 선택하고 사용 가능한 필드에 새 값을 입력합니다.

9. SNTP 서버 항목을 제거하려면 제거할 구성된 서버 옆의 check box을 선택한 다음 Delete 버튼을 클릭합니다.

   항목이 제거되고 장치가 업데이트됩니다.

10. Apply 버튼을 클릭합니다

    업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

새로 고침을 하기 위해서는 Refresh 버튼을 클릭하세요

SNTP 서버 상태 테이블에는 스위치에 구성된 SNTP 서버에 대한 상태 정보가 표시됩니다. 다음 표는 SNTP 서버 상태 정보를 표시합니다.

Table 20. SNTP 서버 상태

필드	설명
Address	모든 기존 서버 주소. 서버 구성이 없으면 SNTP 서버가 없다는 메시지가 화면에 깜박입니다.

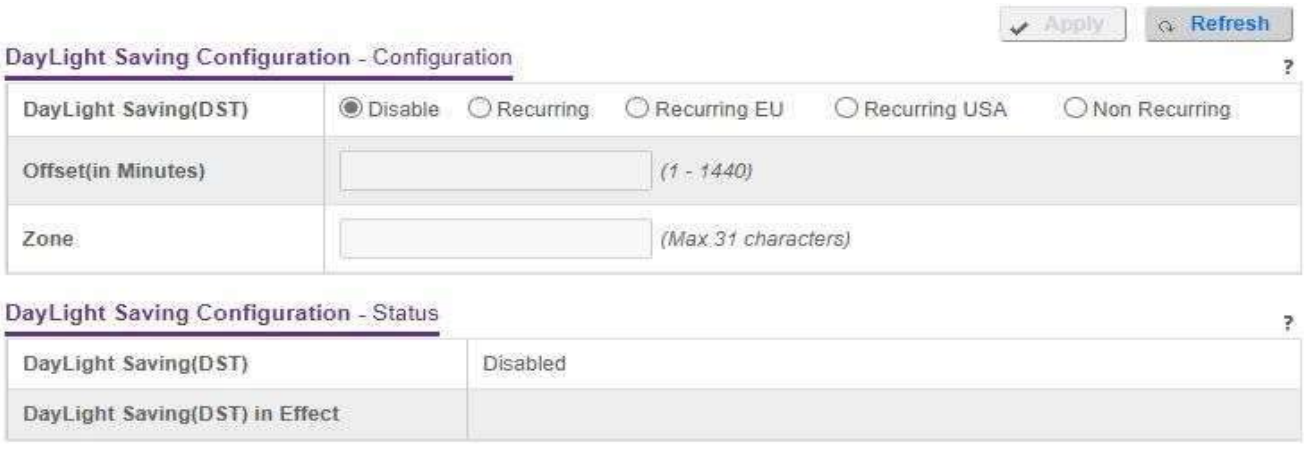
1.5 cm

Last Update Time	이 서버의 응답이 시스템 시계를 업데이트하는 데 사용된 현지 날짜 및 시간(UTC)입니다.
Last Attempt Time	이 SNTP 서버가 마지막으로 쿼리된 현지 날짜 및 시간(UTC)입니다.
Last Attempt Status	이 서버에 대한 마지막 S9 NTP 요청의 상태입니다. 이 서버로부터 패킷이 수신되지 않은 경우 기타 상태가 표시됩니다. • **Other**. 다음 열거형 값이 없습니다. • **Success**. SNTP 작업이 성공했으며 시스템 시간이 업데이트되었습니다. • **Request Timed Out**. SNTP 서버로부터 응답을 받지 못한 채 직접 SNTP 요청 시간이 초과되었습니다. • **Bad Date Encoded**. SNTP 서버에서 제공한 시간이 유효하지 않습니다. • **Version Not Supported**. 서버에서 지원하는 SNTP 버전이 클라이언트에서 지원하는 버전과 호환되지 않습니다. • **Server Unsynchronized**. SNTP 서버는 해당 피어와 동기화되지 않습니다. 이는 SNTP 메시지의 도약 표시 필드를 통해 표시됩니다. • **Server Kiss Of Death**. SNTP 서버에서 이 서버로 더 이상 쿼리가 전송되지 않는다고 표시했습니다. 이는 서버로부터 수신된 메시지에서 0과 동일한 Stratum 필드로 표시됩니다.
Requests	마지막 에이전트 재부팅 이후 이 서버에 대한 SNTP 요청 수입니다.
Failed Requests	마지막 재부팅 이후 이 서버에 대한 실패한 SNTP 요청 수입니다.

일광 절약 시간 설정 구성

➢ **일광 절약 시간 설정을 구성하려면:**

System > Management > Time > Daylight Saving Configuration.



1. 일광 절약 시간(DST) 라디오 버튼을 선택합니다.
   - **Disable.** 일광 절약 시간제를 비활성화합니다.
   - **Recurring**. 반복 일광 절약 시간제를 활성화합니다.
   - **Recurring EU**. 반복되는 EU 일광 절약 시간을 활성화합니다.
   - **Recurring USA**. 반복되는 미국 일광 절약 시간을 활성화합니다.
   - **Non Recurring**. 반복되지 않는 일광 절약 시간을 구성합니다.
2. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표의 필드는 일광 절약 시간이 반복, 반복 EU 또는 반복 USA인 경우에만 표시됩니다.

Table 21. 일광 절약 시간제 - Recurring

필드	설명
Begins At	이 필드는 날짜 및 시간의 시작 값을 구성하는 데 사용됩니다. • **Week**. 시작 주를 구성합니다.. • **Day**. 시작일을 구성합니다. • **Month**. 시작 월을 구성합니다. • **Hours**. 시작 시간(시)을 구성합니다. • **Minutes**. 시작 시간(분)을 구성합니다.
Ends At	이 필드는 날짜 및 시간의 최종 값을 구성하는 데 사용됩니다. • **Week**. 마지막 주를 구성합니다. • **Day**. 종료일을 구성합니다. • **Month**. 종료 월을 구성합니다. • **Hours**. 종료 시간(시)을 구성합니다. • **Minutes**. 종료 시간(분)을 구성합니다.
Offset	몇 분 안에 반복 오프셋을 구성합니다. 유효한 범위는 1~1440분입니다.
Zone	시간대를 구성합니다.

다음 표의 필드는 일광 절약 시간이 반복되지 않는 경우에만 표시됩니다.

Table 22. 일광 절약 시간제 - Non Recurring

필드	설명

1.5 cm

Begins At	이 필드는 날짜 및 시간의 시작 값을 구성하는 데 사용됩니다. • **Week**. 시작 주를 구성합니다.. • **Day**. 시작일을 구성합니다. • **Month**. 시작 월을 구성합니다. • **Hours**. 시작 시간(시)을 구성합니다. • **Minutes**. 시작 시간(분)을 구성합니다.
Ends At	이 필드는 날짜 및 시간의 최종 값을 구성하는 데 사용됩니다. • **Week**. 마지막 주를 구성합니다. • **Day**. 종료일을 구성합니다. • **Month**. 종료 월을 구성합니다. • **Hours**. 종료 시간(시)을 구성합니다. • **Minutes**. 종료 시간(분)을 구성합니다.
Offset	반복되지 않는 오프셋을 몇 분 안에 구성합니다. 유효한 범위는 1~1440분입니다.
Zone	시간대를 구성합니다.

DHCP 서버 설정 구성

DHCP 서버, DHCP 풀, DHCP 바인딩 및 DHCP 릴레이에 대한 설정을 구성할 수 있습니다. DHCP 통계 및 충돌도 볼 수 있습니다.

DHCP 서버 구성

➢ **DHCP 서버를 구성하려면:**

System > Services > DHCP Server > DHCP Server Configuration.

1.5 cm

1. 관리 모드 Disable 또는 Enable 라디오 버튼을 선택합니다.

   DHCP 서비스의 활성화 여부를 지정합니다. 기본값은 Disable입니다.

2. Ping Packet Count를 사용하여 Ping 작업의 일부로 중복을 확인하기 위해 서버가 풀 주소로 보내는 패킷 수를 지정합니다.

   기본값은 2입니다. 유효 범위는 0, 2~10입니다. 값을 0으로 설정하면 기능이 비활성화됩니다.

3. 충돌 로깅 모드 Disable 또는 Enable 라디오 버튼을 선택합니다.

   DHCP 서버의 충돌 로깅을 활성화할지 비활성화할지 여부를 지정합니다. 기본값은 Enable입니다.

4. BootP 자동 모드 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 동적 풀에 대한 BootP를 활성화할지 비활성화할지 여부를 지정합니다. 기본값은 Disable입니다.

5. 주소를 제외하려면 다음을 수행합니다.

   a. IP Range From 필드에 제외할 범위의 가장 낮은 주소 또는 단일 주소를 입력합니다.

   b. IP Range To 필드에 범위를 제외하려면 범위에서 가장 높은 주소를 입력합니다. 단일 주소를 제외하려면 IP Range From 필드에 지정된 것과 동일한 IP 주소를 입력하거나 0.0.0.0으로 그대로 둡니다.

6. Add 버튼을 클릭합니다.

   제외 주소가 스위치에 추가됩니다.

7. 스위치에서 제외 주소를 삭제하려면 Delete 버튼을 클릭하세요.

1.5 cm

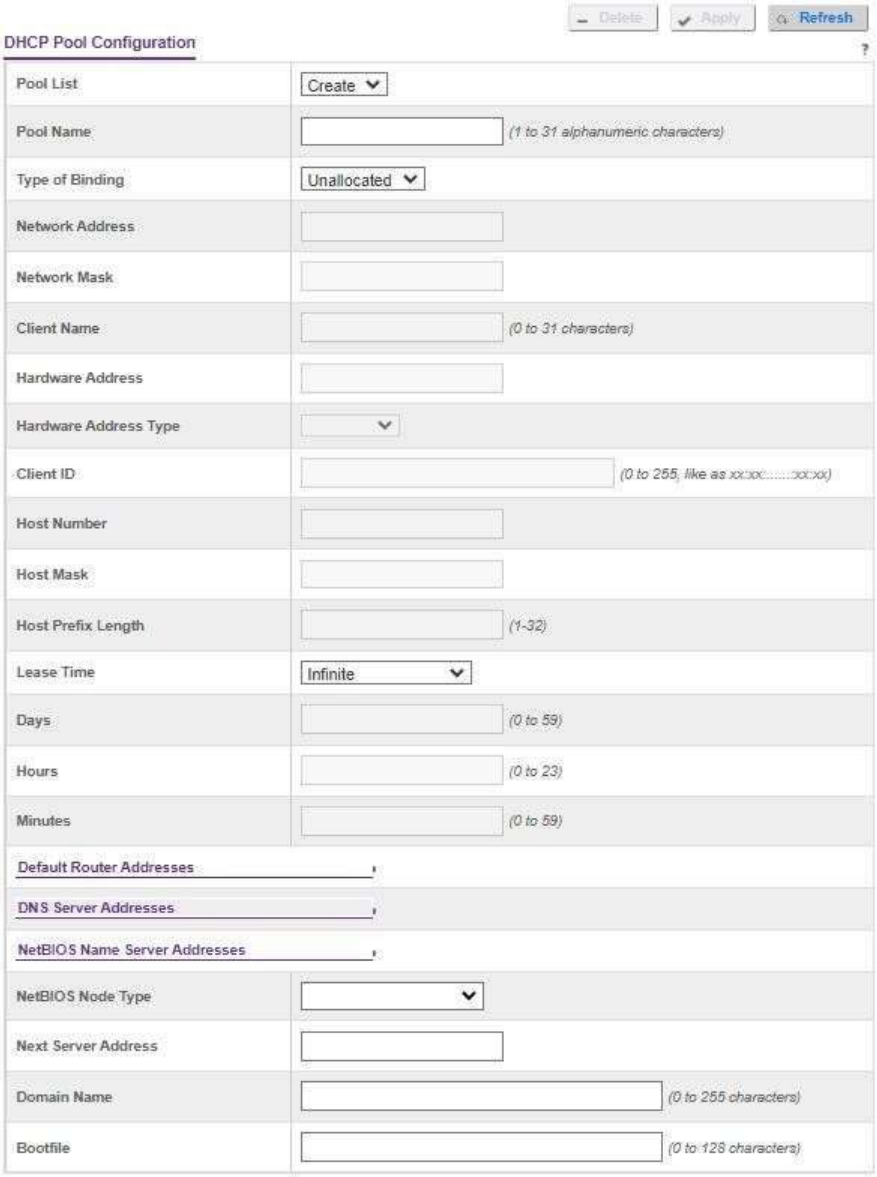
8. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

DHCP 풀 구성

➢ **DHCP 풀을 구성하려면:**

System > Services > DHCP Server > DHCP Pool Configuration.



1. Add 버튼을 클릭합니다.

   풀 구성이 추가됩니다.

2. 풀을 삭제하려면 Delete 버튼을 클릭합니다.

1.5 cm

이 필드는 읽기 전용 권한이 있는 사용자에게 표시되지 않습니다.

3. Apply 버튼을 클릭합니다

업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표에서는 DHCP 풀 구성 필드에 대해 설명합니다.

Table 32. DHCP 풀 구성

필드	설명
Pool Name*	읽기/쓰기 권한이 있는 사용자의 경우 이 필드에는 추가 옵션 만들기와 함께 모든 기존 풀의 이름이 표시됩니다. 사용자가 생성을 선택하면 사용자가 생성할 풀의 이름을 입력할 수 있는 또 다른 텍스트 상자 풀 이름이 나타납니다. 읽기 전용 권한이 있는 사용자의 경우 이 필드에는 기존 풀의 이름만 표시됩니다.
Pool Name	생성할 풀의 이름입니다. 이 필드는 읽기-쓰기 권한이 있는 사용자가 풀 이름 목록*에서 생성을 선택한 경우 나타납니다. 풀 이름은 최대 31자까지 가능합니다.
Type of Binding	풀의 바인딩 유형: • Unallocated • Dynamic • Manual
Network Address	동적 풀의 DHCP 주소에 대한 서브넷 주소입니다.
Network Mask	동적 풀의 DHCP 주소에 대한 서브넷 번호입니다. 네트워크 마스크 또는 접두사 길이 중 하나를 구성하여 서브넷 마스크를 지정할 수 있지만 둘 다 지정할 수는 없습니다.
Network Prefix Length	동적 풀의 DHCP 주소에 대한 서브넷 번호입니다. 네트워크 마스크 또는 접두사 길이 중 하나를 구성하여 서브넷 마스크를 지정할 수 있지만 둘 다 지정할 수는 없습니다. 유효한 범위는 0~32입니다.
Client Name	DHCP 수동 풀의 클라이언트 이름입니다.
Hardware Address	DHCP 클라이언트 하드웨어 플랫폼의 MAC 주소입니다.
Hardware Address Type	DHCP 클라이언트의 하드웨어 플랫폼 프로토콜입니다. 유효한 유형은 이더넷과 ieee802입니다. 기본값은 이더넷입니다.
Client ID	DHCP 수동 풀의 클라이언트 식별자입니다.
Host Number	DHCP 클라이언트에 대한 수동 바인딩을 위한 IP 주소입니다. f 클라이언트 식별자 또는 하드웨어 주소가 지정된 경우에만 호스트를 설정할 수 있습니다. 호스트를 삭제하면 수동 풀의 클라이언트 이름, 클라이언트 ID 및 하드웨어 주소가 삭제되고 풀 유형이 할당되지

1.5 cm

	않음으로 설정됩니다.
Host Mask	DHCP 클라이언트에 대한 수동 바인딩을 위한 서브넷 마스크입니다. 호스트 마스크 또는 접두사 길이 중 하나를 구성하여 서브넷 마스크를 지정할 수 있지만 둘 다 지정할 수는 없습니다.
Host Prefix Length	DHCP 클라이언트에 대한 수동 바인딩을 위한 서브넷 마스크입니다. 호스트 마스크 또는 접두사 길이 중 하나를 구성하여 서브넷 마스크를 지정할 수 있지만 둘 다 지정할 수는 없습니다. 유효한 범위는 0~32입니다.
Lease Time	무한으로 선택하여 임대 시간을 무한으로 지정하거나 지정 기간을 선택하여 특정 임대 기간을 입력할 수 있습니다. 동적 바인딩의 경우 무한은 임대 기간 60일을 의미하고, 수동 바인딩의 경우 무한은 무기한 임대 기간을 의미합니다. 기본값은 지정된 기간입니다.
Days	임대 기간의 일수입니다. 이 필드는 사용자가 지정된 기간을 임대 시간으로 지정한 경우에만 나타납니다. 기본값은 1입니다. 유효한 범위는 0~59입니다.
Hours	임대 기간의 시간입니다. 이 필드는 사용자가 지정된 기간을 임대 시간으로 지정한 경우에만 나타납니다. 유효한 범위는 0~22입니다.
Minutes	임대 기간(분)입니다. 이 필드는 지정된 기간을 임대 시간으로 지정한 경우에만 나타납니다. 유효한 범위는 0~86399입니다.
Default Router Addresses	풀의 기본 라우터 주소 목록입니다. 필드 이름 옆에 있는 화살표를 클릭하면 화면이 확장되고 기본 라우터 주소를 기본 라우터 주소 순으로 최대 8개까지 지정할 수 있는 표가 표시됩니다.
DNS Server Addresses	풀의 DNS 서버 주소 목록입니다. 필드 이름 옆에 있는 화살표를 클릭하면 화면이 확장되고 DNS 서버 주소를 원하는 순서대로 최대 8개까지 지정할 수 있는 표가 표시됩니다.
NetBIOS Name Server Addresses	풀의 NetBIOS 이름 서버 주소 목록입니다. 필드 이름 옆에 있는 화살표를 클릭하면 화면이 확장되고 NetBIOS 이름 서버 주소를 원하는 순서대로 최대 8개까지 지정할 수 있는 테이블이 표시됩니다.
NetBIOS Node Type	DHCP 클라이언트의 NetBIOS 노드 유형: • b-node Broadcast • p-node Peer-to-Peer • m-node Mixed • h-node Hybrid
Next Server Address	풀의 다음 서버 주소입니다.
Domain Name	DHCP 클라이언트의 도메인 이름입니다. 도메인 이름은 최대

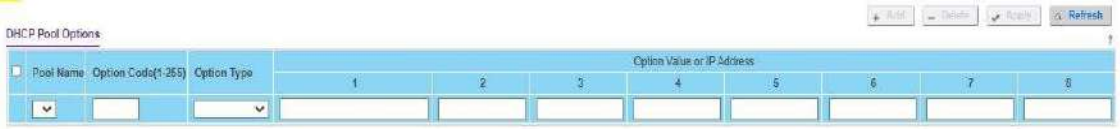
1.5 cm

	255자까지 가능합니다.
Bootfile	DHCP 클라이언트의 기본 부팅 이미지 이름입니다. 파일 이름은 최대 128자까지 가능합니다.

DHCP 풀 옵션 구성

➢ **DHCP 풀 옵션을 구성하려면:**

System > Services > DHCP Server> DHCP Pool Options.



1. Pool Name 목록에서 풀 이름을 선택합니다.
2. Option Code는 선택한 풀에 대해 구성된 옵션 코드를 지정합니다.
3. Option Type을 사용하여 선택한 풀에 대해 구성된 옵션 코드에 대해 옵션 유형을 지정합니다.
   - ASCII
   - Hex
   - IP Address
4. Option Value은 선택한 풀에 대해 구성된 옵션 코드에 대한 값을 지정합니다.
5. Add 버튼을 클릭합니다

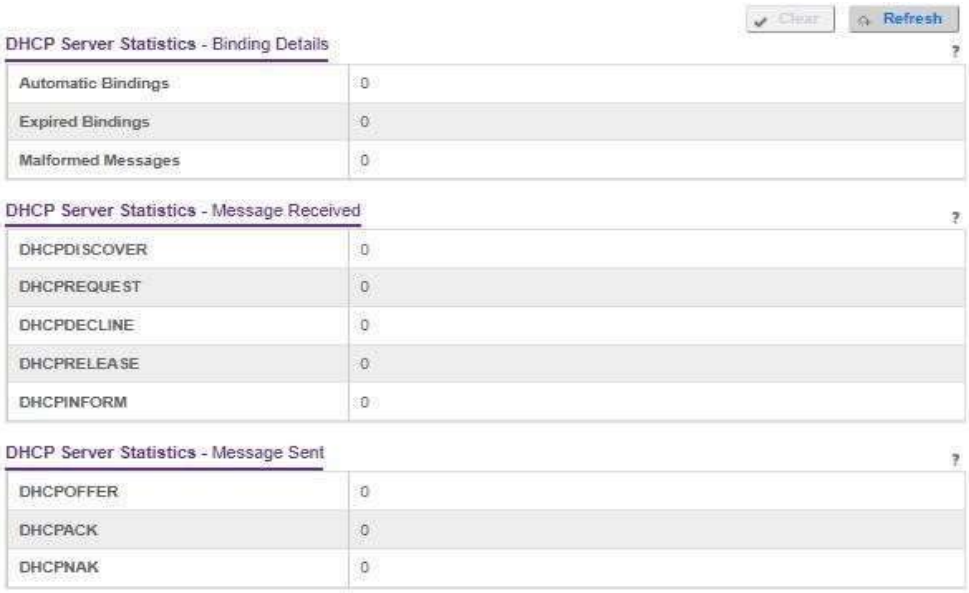
   선택한 풀에 옵션코드가 추가됩니다.
6. 선택한 풀의 옵션 코드를 삭제하려면 Delete 버튼을 클릭하세요.

DHCP 서버 통계 보기

➢ **DHCP 서버 통계를 보려면:**

System > Services > DHCP Server > DHCP Server Statistics.

1.5 cm


Clear
Refresh
DHCP Server Statistics - Binding Details
Automatic Bindings 0
Expired Bindings 0
Malformed Messages 0
DHCP Server Statistics - Message Received
DHCPDISCOVER 0
DHCPREQUEST 0
DHCPDECLINE 0
DHCPRELEASE 0
DHCPINFORM 0
DHCP Server Statistics - Message Sent
DHCPOFFER 0
DHCPACK 0
DHCPNAK 0

다음 표에서는 DHCP 서버 통계 필드에 대해 설명합니다.

Table 33. DHCP 서버 통계

필드	설명
Automatic Bindings	DHCP 서버의 자동 바인딩 수입니다.
Expired Bindings	DHCP 서버에서 만료된 바인딩 수입니다.
Malformed Messages	잘못된 형식의 메시지 수입니다.
DHCPDISCOVER	DHCP 서버가 수신한 DHCPDISCOVER 메시지 수입니다.
DHCPREQUEST	DHCP 서버가 수신한 DHCPREQUEST 메시지 수입니다.
DHCPDECLINE	DHCP 서버가 수신한 DHCPDECLINE 메시지 수입니다.
DHCPRELEASE	DHCP 서버가 수신한 DHCPRELEASE 메시지 수입니다.
DHCPINFORM	DHCP 서버가 수신한 DHCPINFORM 메시지 수입니다.
DHCPOFFER	DHCP 서버가 보낸 DHCPOFFER 메시지 수입니다.
DHCPACK	DHCP 서버가 보낸 DHCPACK 메시지 수입니다.
DHCPNAK	DHCP 서버가 보낸 DHCPNAK 메시지 수입니다.

DHCP 바인딩 정보 보기

➢ **DHCP 바인딩을 보려면:**

System > Services > DHCP Server > DHCP Bindings Information.

1. DHCP 바인딩 정보를 표시하려면 다음 라디오 버튼 중 하나를 선택합니다.
   - **All Dynamic Bindings**. 삭제할 모든 동적 바인딩을 지정합니다.
   - **Specific Dynamic Binding**. 삭제할 특정 동적 바인딩을 지정합니다.

1.5 cm

다음 표에서는 DHCP 바인딩 정보 필드에 대해 설명합니다.

Table 34. DHCP 바인딩 정보

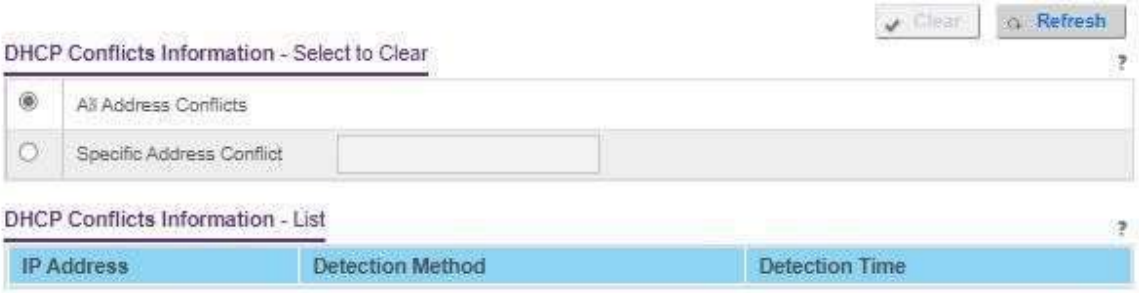
필드	설명
IP Address	클라이언트의 IP 주소입니다.
Hardware Address	클라이언트의 하드웨어 주소입니다.
Lease Time Left	일, 시간, 분 dd:hh:mm 형식의 남은 임대 시간입니다.
Type	바인딩 유형: 동적 또는 수동.

DHCP 충돌 보기

네트워크에서 두 개 이상의 장치에 동일한 IP 주소가 할당되는 경우와 같이 주소 충돌이 있는 호스트에 대한 정보를 볼 수 있습니다.

➢ **DHCP 충돌을 보려면:**

System > Services > DHCP Server > DHCP Conflicts Information.



1. DHCP 충돌 정보를 표시하려면 다음 라디오 버튼 중 하나를 선택합니다.
   - **All Address Conflicts**. 삭제될 모든 주소 충돌을 지정합니다.
   - **Specific Address Conflict**. 삭제할 특정 동적 바인딩을 지정합니다.

다음 표에서는 DHCP 충돌 정보 필드에 대해 설명합니다.

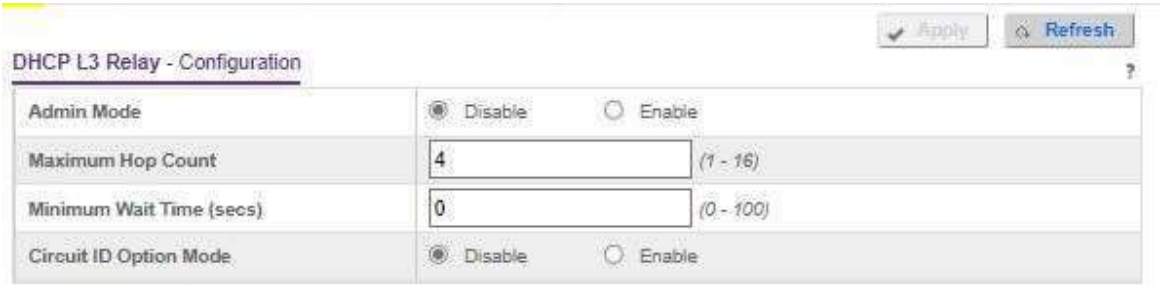
Table 35. DHCP 충돌 정보

필드	설명
IP Address	DHCP 서버에 기록된 호스트의 IP 주소입니다.
Hardware Address	클라이언트의 하드웨어 주소입니다.
Detection Method	DHCP 서버에서 호스트의 IP 주소를 찾은 방식입니다.
Detection Time	시스템 가동 시간을 기준으로 N일 NNh:NNm:NNs 형식으로 충돌이 감지된 시간입니다.

DHCP 릴레이 구성

➢ **DHCP 릴레이를 구성하려면:**

System > Services > DHCP Relay.



1. Maximum Hop Count를 사용하여 클라이언트 요청이 삭제되기 전에 사용할 수 있는 최대 홉 수를 입력합니다.

   범위는 (1~16)입니다. 기본값은 4입니다.

2. Admin Mode를 Disable 또는 Enable 라디오 버튼을 선택합니다.

   활성화를 선택하면 'Server Address' 필드에 입력한 IP 주소로 DHCP 요청이 전달됩니다.

3. Minimum Wait Time을 사용하여 최소 대기 시간을 초 단위로 입력합니다.

   이 값은 클라이언트의 전원이 켜진 이후의 시간을 나타내는 클라이언트 요청 패킷의 타임스탬프와 비교됩니다. 타임스탬프가 최소 대기 시간을 초과하는 경우에만 패킷이 전달됩니다. 범위는 (0~100)입니다.

4. Circuit ID Option mode의 Disable 또는 Enable 라디오 버튼을 선택합니다
   Enable을 선택하면 서버에 전달되기 전에 릴레이 에이전트 옵션이 요청에 추가되고 클라이언트에 전달되기 전에 응답에서 제거됩니다.

다음 표에서는 DHCP 릴레이 통계 필드에 대해 설명합니다.

Table 36. DHCP 릴레이 상태

필드	설명
Requests Received	스위치가 마지막으로 재설정된 이후 모든 클라이언트로부터 수신된 총 DHCP 요청 수입니다.
Requests Relayed	스위치가 마지막으로 재설정된 이후 서버로 전달된 총 DHCP 요청 수입니다.

1.5 cm

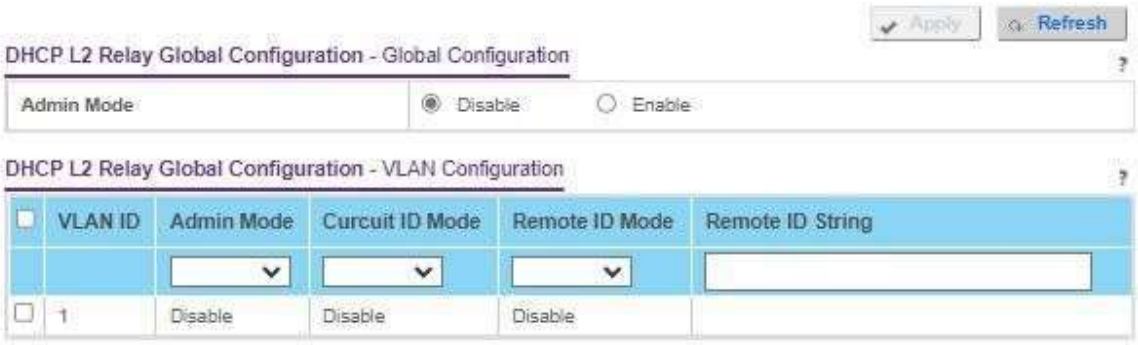
Packets Discarded	스위치가 마지막으로 재설정된 이후 이 릴레이 에이전트가 삭제한 총 DHCP 패킷 수입니다.

DHCP L2 릴레이

글로벌 DHCP L2 릴레이 설정 구성

➢ **글로벌 DHCP L2 릴레이 설정을 구성하려면:**

System > Services > DHCP L2 Relay > DHCP L2 Relay Global Configuration.



1. Admin Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   전역 구성의 경우 스위치에서 DHCP L2 릴레이를 활성화하거나 비활성화합니다. 기본값은 Disable입니다.

2. VLAN 구성의 경우 VLAN ID는 스위치에 구성된 VLAN ID를 표시합니다.

   a. 선택한 VLAN에서 DHCP L2 릴레이를 활성화하거나 비활성화하려면 Admin Mode를 사용하십시오.

   b. Circuit ID Mode를 사용하여 DHCP 옵션-82의 회로 ID 하위 옵션을 활성화하거나 비활성화합니다.

   c. Remote ID Mode가 활성화된 경우 Remote ID String을 사용하여 원격 ID를 지정합니다.

3. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

- 페이지 매김 탐색 메뉴
  - 페이지당 행 수. 화면당 표시되는 테이블 항목 수를 선택합니다. 가능한 값은 20, 50, 100, 200 및 모두입니다.

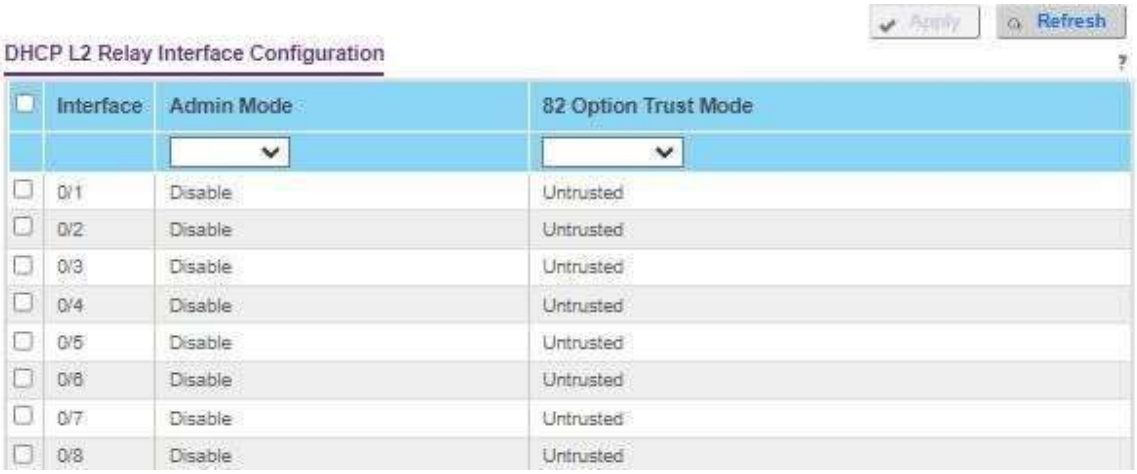
Note: 모두를 선택하면 브라우저에 정보가 표시되는 속도가 느려질 수 있습니다.

- < 테이블 데이터 항목의 이전 페이지를 표시합니다.
- > 테이블 데이터 항목의 다음 페이지를 표시합니다.

DHCP L2 릴레이 인터페이스 구성

➢ **DHCP L2 릴레이를 구성하려면:**

System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration.



1. Admin Mode를 사용하여 선택한 인터페이스에서 DHCP L2 릴레이를 활성화하거나 비활성화합니다.

   기본값은 Disable입니다.

2. 82 Option Trust Mode를 사용하여 수신된 DHCP L2 릴레이(Option-82)에 대해 신뢰할 수 있는 인터페이스를 활성화하거나 비활성화합니다.

DHCP L2 릴레이 인터페이스 통계 보기

➢ **DHCP L2 릴레이 인터페이스 통계를 보려면:**

System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Statistics.

다음 표에서는 DHCP L2 릴레이 인터페이스 통계 필드에 대해 설명합니다.

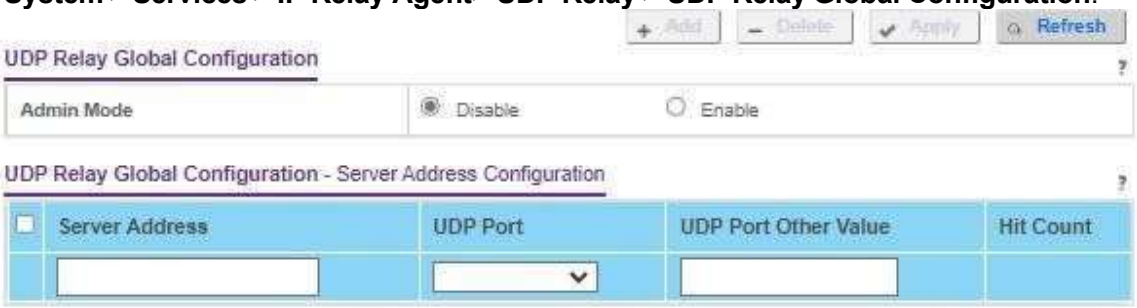
Table 37. DHCP L2 릴레이 인터페이스 통계

필드	설명
Interface	DHCP 메시지가 수신되는 인터페이스를 표시합니다.
UntrustedServerMsgsWithOpt82	신뢰할 수 없는 서버로부터 수신된 option82가 포함된 DHCP 메시지의 수를 표시합니다.
UntrustedClientMsgsWithOpt82	신뢰할 수 없는 클라이언트로부터 수신된 option82가 포함된 DHCP 메시지의 수를 표시합니다.
TrustedServerMsgsWithoutOpt82	신뢰할 수 있는 서버로부터 수신된 option82가 없는 DHCP 메시지의 수를 표시합니다.
TrustedClientMsgsWithoutOpt82	신뢰할 수 있는 클라이언트로부터 수신된 option82가 없는 DHCP 메시지의 수를 표시합니다.

UDP 릴레이 전역 설정 구성

➢ **UDP 릴레이 전역 설정을 구성하려면:**

System > Services > IP Relay Agent> UDP Relay > UDP Relay Global Configuration.



1. Admin Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   스위치의 UDP 릴레이를 활성화하거나 비활성화합니다. 기본값은 Disable입니다.

2. Server Address를 사용하여 UDP 릴레이 서버 주소를 x.x.x.x 형식으로 지정합니다.

3. UDP Port를 사용하여 UDP 대상 포트를 지정합니다.

   지원되는 포트는 다음과 같습니다.

   - **DefaultSet**. UDP 포트 0 패킷을 릴레이합니다. 릴레이 서버 생성 시 UDP 포트를 선택하지 않은 경우 지정됩니다.
   - **dhcp**. DHCP(UDP 포트 67) 패킷을 릴레이합니다.

1.5 cm

- **domain**. DNS(UDP 포트 53) 패킷을 릴레이합니다.
- **isakmp**. ISAKMP(UDP 포트 500) 패킷을 릴레이합니다.
- **mobile-ip**. 모바일 IP(UDP 포트 434) 패킷을 릴레이합니다.
- **nameserver**. IEN-116 이름 서비스(UDP 포트 42) 패킷을 릴레이합니다.
- **netbios-dgm**. NetBIOS 데이터그램 서버(UDP 포트 138) 패킷을 릴레이합니다.
- **netbios-ns**. NetBIOS 이름 서버(UDP 포트 137) 패킷을 릴레이합니다.
- **ntp**. 네트워크 시간 프로토콜(UDP 포트 123) 패킷을 릴레이합니다.
- **pim-auto-rp**. PIM 자동 RP(UDP 포트 496) 패킷을 릴레이합니다.
- **rip**. RIP(Routing Image Protocol)(UDP 포트 520) 패킷을 릴레이합니다.
- **tacacs**. TACACS(UDP 포트 49) 패킷을 릴레이합니다.
- **tftp**. TFTP(UDP 포트 69) 패킷을 릴레이합니다.
- **time**. 시간 서비스(UDP 포트 37) 패킷을 릴레이합니다.
- **Other**. 이 옵션을 선택하면 UDP 포트 기타 값이 활성화됩니다. 이 옵션을 사용하면 UDP 포트 기타 값에 자신의 UDP 포트를 입력할 수 있습니다.

4. UDP Port Other Value을 사용하여 0~65535 사이의 UDP 대상 포트를 지정합니다.
5. Add 버튼을 클릭합니다.

   그러면 지정된 구성으로 UDP 릴레이 테이블에 항목이 생성됩니다.
6. UDP 릴레이 테이블에서 모든 항목 또는 지정된 항목을 제거하려면 Delete 버튼을 클릭합니다.
7. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

Hit Count 필드에는 UDP 포트에 도달하는 UDP 패킷 수가 표시됩니다.

새로 고침을 하기 위해서는 Refresh 버튼을 클릭하세요

UDP 릴레이 인터페이스 설정 구성

➢ **UDP 릴레이 인터페이스 설정을 구성하려면:**

System > Services > UDP Relay > UDP Relay Interface Configuration.

1.5 cm

1. Interface를 사용하여 UDP 릴레이에 대해 활성화할 인터페이스를 선택합니다.
2. Server Address를 사용하여 UDP 릴레이 서버 주소를 x.x.x.x 형식으로 지정합니다.
3. UDP Port를 사용하여 UDP 대상 포트를 지정합니다.

   다음 포트가 지원됩니다:

   - **DefaultSet**. UDP 포트 0 패킷을 릴레이합니다. 릴레이 서버 생성 시 UDP 포트를 선택하지 않은 경우 지정됩니다.
   - **dhcp**. DHCP(UDP 포트 67) 패킷을 릴레이합니다.
   - **domain**. DNS(UDP 포트 53) 패킷을 릴레이합니다.
   - **isakmp**. ISAKMP(UDP 포트 500) 패킷을 릴레이합니다.
   - **mobile-ip**. 모바일 IP(UDP 포트 434) 패킷을 릴레이합니다.
   - **nameserver**. IEN-116 이름 서비스(UDP 포트 42) 패킷을 릴레이합니다.
   - **netbios-dgm**. NetBIOS 데이터그램 서버(UDP 포트 138) 패킷을 릴레이합니다.
   - **netbios-ns**. NetBIOS 이름 서버(UDP 포트 137) 패킷을 릴레이합니다.
   - **ntp**. 네트워크 시간 프로토콜(UDP 포트 123) 패킷을 릴레이합니다.
   - **pim-auto-rp**. PIM 자동 RP(UDP 포트 496) 패킷을 릴레이합니다.
   - **rip**. RIP(UDP 포트 520) 패킷을 릴레이합니다.
   - **tacacs**. TACACS(UDP 포트 49) 패킷을 릴레이합니다.
   - **tftp**. TFTP(UDP 포트 69) 패킷을 릴레이합니다.
   - **time**. 시간 서비스(UDP 포트 37) 패킷을 릴레이합니다.
   - **Other**. 이 옵션을 선택하면 UDP 포트 기타 값이 활성화됩니다. 이 옵션을 사용하면 사용자가 UDP 포트 기타 값에 자신의 UDP 포트를 입력할 수 있습니다.
4. UDP Port Other Value을 사용하여 0~65535 사이의 UDP 대상 포트를 지정합니다.
5. Discard를 사용하여 일치하는 패킷 삭제를 활성화/비활성화합니다.

   활성화는 사용자가 IP 주소 0.0.0.0을 입력한 경우에만 선택할 수 있습니다. 사용자가 IP 주소가 0이 아닌 새 항목을 추가하는 경우 삭제 모드를 비활성화로 설정할 수 있습니다.
6. Add 버튼을 클릭합니다.

1.5 cm

그러면 지정된 구성으로 UDP 릴레이 테이블에 항목이 생성됩니다.

7. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

UDP 릴레이 인터페이스 구성 테이블에서 모든 항목 또는 지정된 항목을 제거하려면 Delete 버튼을 클릭하십시오.

Hit Count 필드에는 UDP 포트에 도달하는 UDP 패킷 수가 표시됩니다.

새로 고침을 하기 위해서는 Refresh 버튼을 클릭하세요

DHCPv6 서버 활성화 또는 비활성화

장치에서 IPv6용 동적 호스트 구성 프로토콜(DHCPv6) 서버 설정을 구성할 수 있습니다. 장치는 IPv6 클라이언트에 네트워크 구성 정보를 할당하는 데 도움이 되는 DHCPv6 서버 또는 DHCPv6 릴레이 에이전트 역할을 할 수 있습니다.

- **DHCP 서비스를 활성화 또는 비활성화하려면:**

System > Services > DHCPv6 Server > DHCPv6 Server Configuration.

1. Admin Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다

   이는 DHCPv6 서비스 관리 모드의 활성화 또는 비활성화 여부를 지정합니다. 기본값은 Disable입니다.

2. DHCPv6 서버 DUID 필드를 사용하여 DHCPv6 서버의 DUID(DHCP 고유 식별자)를 지정합니다.

3. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

DHCPv6 풀 구성

현재 구성된 DHCPv6 서버 풀을 볼 수 있을 뿐만 아니라 풀을 추가 및 제거할 수도 있습니다. DHCPv6 서버 풀은 정보를 요청하는 DHCPv6 클라이언트가 사용할 수 있는 네트워크 구성

1.5 cm

정보 집합입니다.

➢ **DHCPv6 풀 설정을 구성하려면:**

System > Services > DHCPv6 Server > DHCPv6 Pool Configuration.

Pool Name 필드에는 모든 기존 풀의 이름과 Create 옵션이 표시됩니다.

Note: 읽기 전용 권한이 있는 사용자로 로그인한 경우 Pool Name 필드에는 기존 풀 이름만 표시됩니다. 풀을 생성하려면 읽기/쓰기 권한이 있는 admin 사용자 이름으로 로그인해야 합니다.

1. 풀을 생성하려면 Create을 선택하고 생성할 DHCPv6 서버 풀을 식별하는 고유한 이름을 입력합니다.

   이름은 최대 31자의 영숫자 문자일 수 있습니다.

2. Default Router Address 필드를 사용하여 풀의 기본 라우터 주소 목록을 지정합니다.

   사용자는 선호하는 순서대로 최대 8개의 기본 라우터 주소를 지정할 수 있습니다.

3. Domain Name 필드를 사용하여 풀에 있는 DHCPv6 클라이언트의 도메인 이름을 지정합니다.
   도메인 이름의 최대 길이는 영숫자 255자입니다.
   스위치에서 선택한 풀을 삭제하려면 Delete 버튼을 클릭하세요.

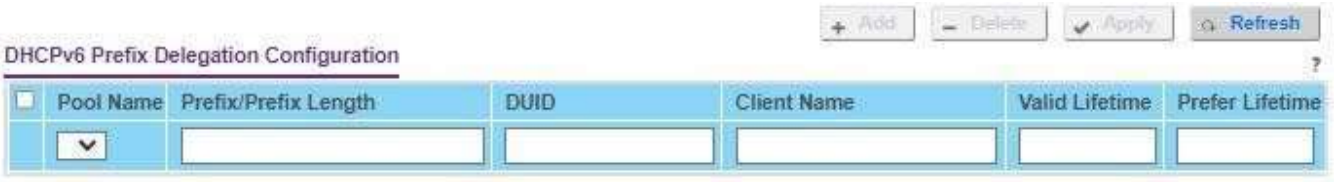
4. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

DHCPv6 접두사 위임 구성

➢ **DHCPv6 접두사 위임 설정을 구성하려면:**

System > Services > DHCPv6 Server > DHCPv6 Prefix Delegation Configuration.



1. 구성된 Pool Name 목록에서 선택합니다.
2. Prefix 및 Prefix Length 필드에서 위임된 IPv6 접두사를 지정합니다.
3. DUID 필드에 클라이언트의 고유 DUID 값을 식별하는 데 사용되는 DUID 식별자를 지정합니다.
4. 로깅 또는 추적에만 유용한 Client Name을 지정합니다.
   이름은 최대 31자의 영숫자 문자일 수 있습니다.
5. 위임된 접두사의 Valid Lifetime(초)을 지정합니다.
   유효한 값은 0~4294967295입니다.
6. 위임된 접두사에 대해 Prefer Lifetime(초)을 지정합니다.
   유효한 값은 0~4294967295입니다.
7. Add 버튼을 클릭합니다
   선택한 풀에 대해 위임된 접두사가 추가됩니다.
8. 선택한 풀에 대해 위임된 접두사를 삭제하려면 Delete 버튼을 클릭합니다.
9. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

DHCPv6 인터페이스 설정 구성

DHCPv6에 대한 인터페이스별 설정을 구성할 수 있습니다. DHCPv6 인터페이스 모드는 상호 배타적입니다. 이 화면에서 구성할 수 있는 필드는 인터페이스에 대해 선택한 모드에 따라 다릅니다.

➢ DHCPv6 인터페이스 설정을 구성하려면:

System > Services > DHCPv6 Server > DHCPv6 Interface Configuration.

1. 보거나 구성할 정보가 있는 인터페이스를 선택합니다. 다음 중 하나를 수행할 수 있습니다.
   a. Go To Interface 필드에 유닛/슬롯/포트 형식의 인터페이스를 입력하고 Go 버튼을 클릭합니다. 지정된 인터페이스에 해당하는 항목이 선택됩니다.
   b. DHCPv6 서버 기능에 대해 구성된 인터페이스 목록에서 check box을 선택합니다.
2. 관리 모드 목록에서 DHCPv6 모드 활성화 또는 비활성화를 선택하여 서버 기능을 구성합니다.

   DHCPv6 서버와 DHCPv6 릴레이 기능은 상호 배타적입니다.
3. Pool Name 필드에서 상태 비저장 및/또는 접두사 위임 매개 변수가 포함된 DHCPv6 풀을 지정합니다.
4. Rapid Commit은 선택적 매개변수입니다. Rapid Commit 목록에서 클라이언트와 서버 간의 단축 교환을 허용하는 Enable 또는 Disable를 선택합니다.
5. 기본 설정 필드에서 클라이언트가 DHCPv6 서버 간의 기본 설정을 결정하는 데 사용하는 기본 설정 값을 지정합니다.

   유효한 값은 0~4294967295입니다. 기본값은 0입니다.
6. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

DHCPv6 바인딩 정보 보기

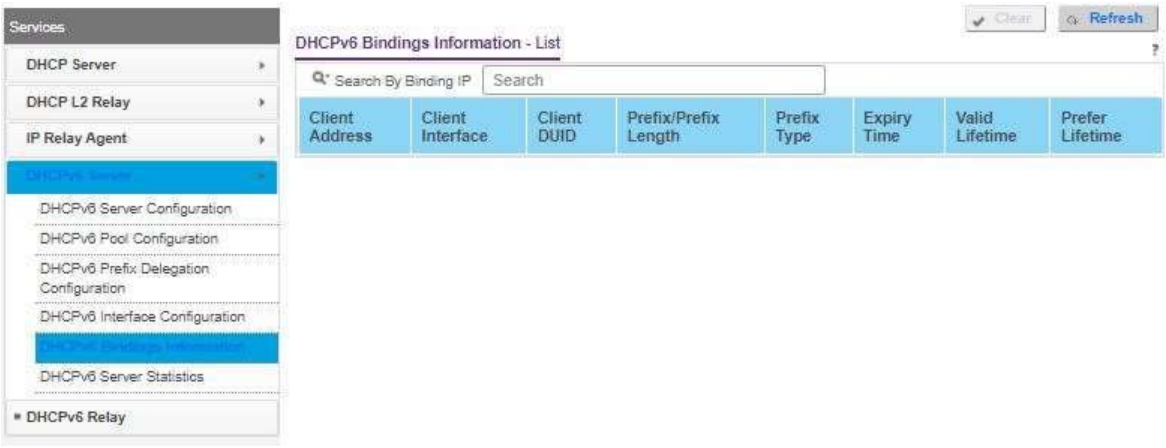
DHCP 바인딩 테이블에서 항목을 볼 수 있습니다. 클라이언트가 DHCPv6 서버에서 IPv6 구성 정보를 얻은 후 서버는 해당 데이터베이스에 항목을 추가합니다. 항목을 바인딩이라고 합니다.

- **DHCPv6 바인딩 정보를 보려면:**

System > Services > DHCPv6 Server > DHCPv6 Bindings Information.

1.5 cm

U-I-F5010HPA



새로 고침을 하기 위해서는 Refresh 버튼을 클릭하세요

다음 표에서는 표시되는 구성할 수 없는 필드에 대해 설명합니다.

Table 38. DHCPv6 바인딩 정보

필드	설명
Client Address	바인딩과 연결된 클라이언트의 IPv6 주소입니다.
Client Interface	클라이언트 바인딩이 발생한 인터페이스 번호입니다.
Client DUID	클라이언트의 DHCPv6 고유 식별자(DUID)입니다. DUID는 클라이언트의 하드웨어 주소와 클라이언트 식별자의 조합입니다.
Prefix	이 바인딩과 연결된 위임된 접두사의 IPv6 주소입니다.
Prefix Length	이 바인딩과 연결된 위임된 접두사의 IPv6 마스크 길이입니다.
Prefix Type	이 바인딩과 연결된 IPv6 접두사의 유형입니다.
Expiry Time	바인딩과 연결된 접두사가 만료될 때까지의 시간(초)입니다.
Valid Lifetime	클라이언트가 접두사를 사용할 수 있는 최대 시간(초)입니다.
Prefer Lifetime	클라이언트가 접두사를 사용하도록 허용되는 기본 시간(초)입니다.

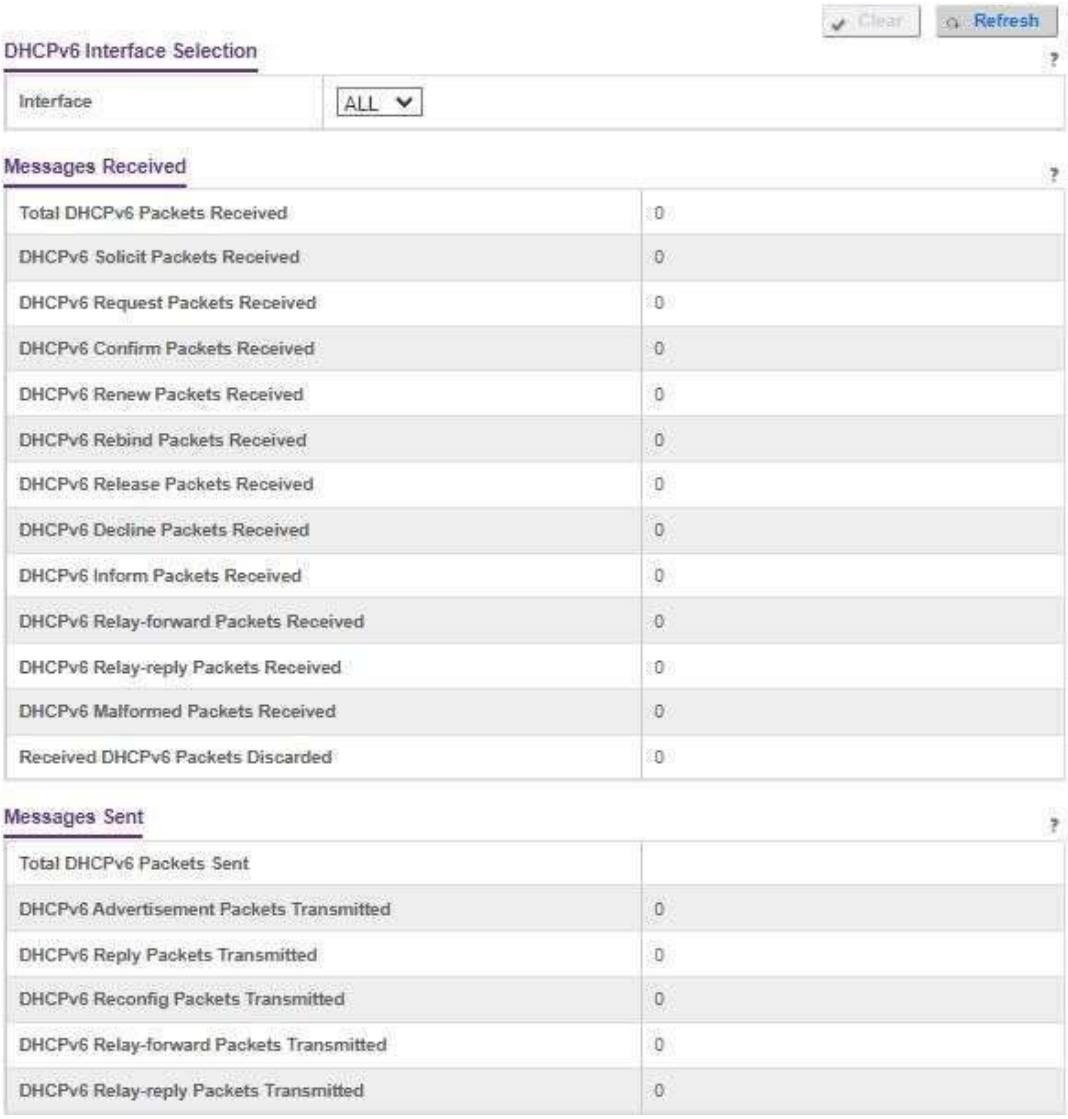
DHCPv6 서버 통계 보기

전역적으로 각 인터페이스에서 전송, 수신 및 삭제된 DHCPv6 메시지에 대한 정보를 포함하여 장치에 대한 DHCPv6 서버 통계를 볼 수 있습니다. 화면의 값은 마지막으로 삭제된 이후 누적된 다양한 카운트를 나타냅니다.

- **DHCPv6 서버 통계를 보려면:**

  System > Services > DHCPv6 Server > DHCPv6 Server Statistics.

1.5 cm



1. 인터페이스에 대한 자세한 DHCPv6 통계를 보려면 Interface 목록에서 데이터가 표시될 항목을 선택합니다.

   All을 선택하면 모든 인터페이스에 대한 데이터가 표시됩니다.

하나 이상의 인터페이스에 대한 DHCPv6 카운터를 재설정하려면 재설정할 통계가 있는 각 인터페이스를 선택하고 Clear 버튼을 클릭합니다.

새로 고침을 하기 위해서는 Refresh 버튼을 클릭하세요

다음 표에서는 표시되는 구성할 수 없는 필드에 대해 설명합니다.

1.5 cm

Table 39. DHCPv6 서버 통계

필드	설명
Messages Received	수신된 메시지에 대한 모든 인터페이스 수준 통계의 집계입니다.
Total DHCPv6 Packets Received	인터페이스에서 수신된 DHCPv6 메시지 수입니다. DHCP v6 클라이언트에서 DHCP v6 서버로 전송되는 DHCPv6 메시지에는 요청, 요청, 확인, 갱신, 리바인드, 해제, 거부 및 정보 요청 메시지가 포함됩니다. 또한 DHCP v6 릴레이 에이전트는 릴레이 전달 메시지를 DHCP v6 서버로 전달할 수 있습니다.
DHCPv6 Solicit Packets Received	인터페이스에서 수신된 DHCPv6 Solicit 메시지 수입니다. 이 유형의 메시지는 DHCPv6 서버를 찾기 위해 클라이언트에서 전송됩니다.
DHCPv6 Request Packets Received	요청 수입니다.
DHCPv6 Confirm Packets Received	인터페이스에서 수신된 DHCPv6 확인 메시지 수입니다. 이 유형의 메시지는 해당 구성이 연결된 링크에 유효한지 확인하기 위해 클라이언트에서 모든 DHCPv6 서버로 전송됩니다.
DHCPv6 Renew Packets Received	인터페이스에서 수신된 DHCPv6 갱신 메시지 수입니다. 이 유형의 메시지는 DHCPv6 서버에서 제공하는 구성 정보를 확장하고 업데이트하기 위해 클라이언트에서 전송됩니다.
DHCPv6 Rebind Packets Received	인터페이스에서 수신된 DHCPv6 리바인드 메시지 수입니다. 이 유형의 메시지는 갱신 메시지에 대한 응답을 받지 못한 경우 클라이언트에서 DHCPv6 서버로 전송됩니다.
DHCPv6 Release Packets Received	인터페이스에서 수신된 DHCPv6 해제 메시지 수입니다. 이 유형의 메시지는 할당된 주소가 더 이상 필요하지 않음을 나타내기 위해 클라이언트에서 전송됩니다.
DHCPv6 Decline Packets Received	인터페이스에서 수신된 DHCPv6 거부 메시지 수입니다. 이 유형의 메시지는 할당된 주소가 링크에서 이미 사용 중임을 나타내기 위해 클라이언트에서 DHCPv6 서버로 전송됩니다.
DHCPv6 Inform Packets Received	인터페이스에서 수신된 DHCP v6 정보 요청 메시지 수입니다. 이 유형의 메시지는 IP 주소 할당 이외의 구성 정보를 요청하기 위해 클라이언트에서 전송됩니다.
DHCPv6 Relay-forward Packets Received	인터페이스에서 수신된 DHCPv6 릴레이 전달 메시지 수입니다. 이 유형의 메시지는 메시지를 서버에 전달하기 위해 릴레이 에이전트에 의해 전송됩니다.
DHCPv6 Relay-reply Packets Received	인터페이스에서 수신된 DHCP v6 릴레이 응답 메시지 수입니다. 이 유형의 메시지는 서버에서 DHCP v6 릴레이 에이전트로 전송되며 릴레이 에이전트가 클라이언트에 전달할 메시지를 포함합니다.

1.5 cm

DHCPv6 Malformed Packets Received	인터페이스에서 수신되었지만 형식이 잘못되어 삭제된 DHCPv6 메시지 수입니다.
Received DHCPv6 Packets Discarded	폐기된 패킷 수입니다.
Messages Sent	전송된 메시지에 대한 모든 인터페이스 수준 통계의 집계입니다.
Total DHCPv6 Packets Sent	인터페이스에서 보낸 DHCPv6 메시지 수입니다. DHCPv6 서버에서 DHCPv6 클라이언트로 전송되는 DHCPv6 메시지에는 Advertise, Reply, Reconfigure 및 Relay-Reply 메시지가 포함됩니다.
DHCPv6 Advertisement Packets Transmitted	인터페이스에서 보낸 DHCPv6 Advertise 메시지 수입니다. 이 유형의 메시지는 요청 메시지에 대한 응답으로 서버에서 DHCPv6 클라이언트로 전송되며 서비스에 사용할 수 있음을 나타냅니다.
DHCPv6 Reply Packets Transmitted	요청, 요청, 갱신, 리바인드, 정보 요청, 확인, 해제 또는 거부 메시지에 대한 응답으로 인터페이스에서 DHCPv6 클라이언트로 전송된 DHCPv6 응답 메시지 수입니다.
DHCPv6 Reconfig Packets Transmitted	인터페이스에서 보낸 DHCPv6 재구성 메시지 수입니다. 이 유형의 메시지는 서버에 새 정보나 업데이트된 정보가 있음을 클라이언트에 알리기 위해 서버에서 DHCPv6 클라이언트로 전송됩니다. 그런 다음 클라이언트는 일반적으로 업데이트된 정보를 수신하기 위해 서버와 갱신/응답 또는 정보 요청/응답 트랜잭션을 시작합니다.
DHCPv6 Relay-forward Packets Transmitted	인터페이스에서 보낸 DHCPv6 릴레이 전달 메시지 수입니다. 이 유형의 메시지는 메시지를 서버에 전달하기 위해 릴레이 에이전트에 의해 전송됩니다.
DHCPv6 Relay-reply Packets Transmitted	인터페이스에서 보낸 DHCPv6 릴레이-응답 메시지 수입니다. 이 유형의 메시지는 서버에서 DHCPv6 릴레이 에이전트로 전송되며 릴레이 에이전트가 클라이언트에 전달할 메시지를 포함합니다.

인터페이스에 대한 DHCPv6 릴레이 구성

➢ **인터페이스에 대해 DHCPv6 릴레이를 구성하려면:**

System > Services > DHCPv6 Relay.

1.5 cm

1. 보거나 구성할 정보가 있는 인터페이스를 선택합니다. 다음 중 하나를 수행할 수 있습니다.
   - Go To Interface 필드에 유닛/슬롯/포트 형식의 인터페이스를 입력하고 Go 버튼을 클릭합니다. 지정된 인터페이스에 해당하는 항목이 선택됩니다.
   - DHCPv6 릴레이 기능을 위해 구성된 인터페이스 목록에서 check box을 선택합니다.
2. Admin Mode 필드에서 DHCPv6 모드를 활성화 또는 비활성화하여 지정하여 DHCPv6 릴레이 기능을 구성합니다.

   기본값은 Disable입니다. DHCPv6 서버와 DHCPv6 릴레이 기능은 상호 배타적입니다.
3. Relay Interface 목록에서 릴레이 서버에 연결할 인터페이스를 선택합니다.
4. Destination IP Address에서 릴레이 서버에 연결하기 위한 IPv6 주소를 지정합니다.
5. Remote ID 필드에 릴레이 에이전트 정보 옵션을 지정합니다.

   원격 ID는 DHCPv6 서버 DUID 및 릴레이 인터페이스 번호에서 파생되거나 사용자 정의 문자열로 지정할 수 있습니다.
6. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

DNS 설정 구성

네트워크에서 사용하는 DNS 서버에 대한 정보와 스위치가 DNS 클라이언트로 작동하는 방식을 구성할 수 있습니다.

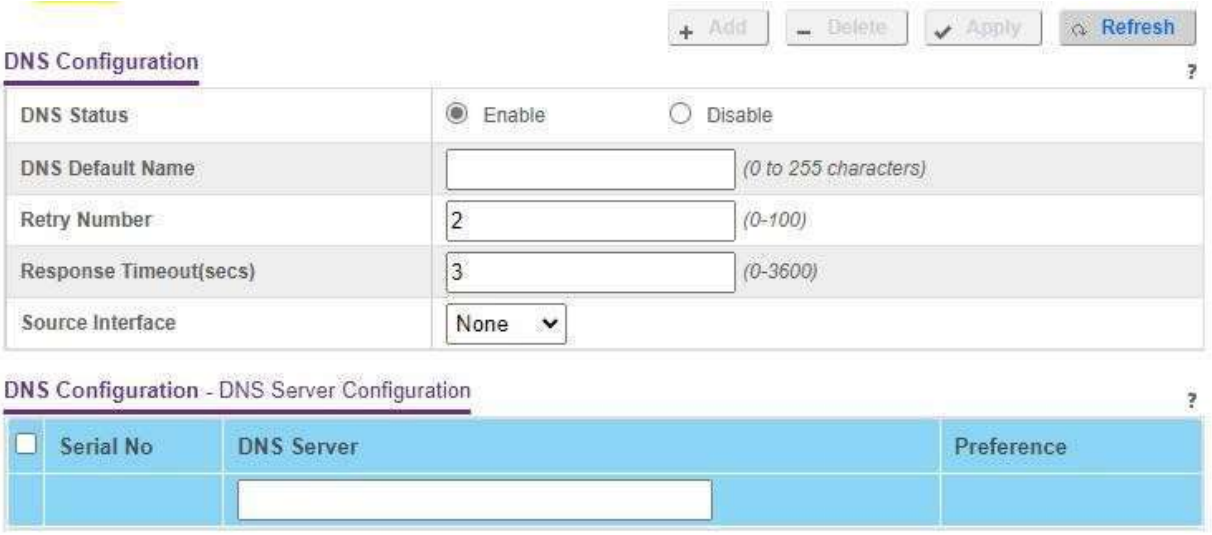
1.5 cm

글로벌 DNS 설정 구성

글로벌 DNS 설정과 DNS 서버 정보를 구성할 수 있습니다.

➢ **글로벌 DNS 설정을 구성하려면:**

System > Management > DNS > DNS Configuration.



1. DNS 상태 Disable 또는 Enable 라디오 버튼을 선택합니다.
   - **Enable**. 스위치가 DNS 쿼리를 DNS 서버에 보내 DNS 도메인 이름을 확인하도록 허용합니다. 기본값은 Enable입니다.
   - **Disable**. 스위치가 DNS 쿼리를 보내지 못하도록 합니다.
2. DNS 쿼리에 포함할 DNS 기본 도메인 이름을 입력합니다.

   시스템이 정규화되지 않은 호스트 이름에 대한 조회를 수행하는 경우 이 필드는 도메인 이름을 제공합니다. 예를 들어 기본 도메인 이름이 .com이고 사용자가 test를 입력하면 이름을 확인하기 위해 test가 test.com으로 변경됩니다.). 이름 길이는 255자를 초과할 수 없습니다.
3. Retry Number를 사용하여 DNS 서버에 DNS 쿼리 전송을 재시도하는 횟수를 지정합니다.

   이 숫자의 범위는 0부터 100까지입니다. 기본값은 2입니다.
4. Response Timeout (secs)를 사용하여 DNS 쿼리에 대한 응답을 기다리는 시간(초)을 지정합니다.

   이 시간 제한 범위는 0~3600입니다. 기본값은 3입니다.
5. DNS에 사용할 Source Interface를 지정합니다.

1.5 cm

가능한 값은 다음과 같습니다.

- None
- VLAN 1
- Routing interface
- Routing VLAN
- Routing loopback interface
- Tunnel interface
- Service port

기본적으로 VLAN 1은 소스 인터페이스로 사용됩니다.

6. 스위치가 DNS 쿼리를 보내는 DNS 서버를 지정하려면 DNS Server Address 필드에 표준 IPv4 점 표기법으로 IP 주소를 입력하고 Add 버튼을 클릭합니다.

   서버가 목록에 나타납니다. 최대 8개의 DNS 서버를 지정할 수 있습니다. 우선순위는 생성된 순서대로 설정됩니다.

7. 목록에서 DNS 서버를 제거하려면 해당 check box을 선택하고 Delete 버튼을 클릭합니다.

   DNS 서버를 선택하지 않고 Delete 버튼을 클릭하면 모든 DNS 서버가 삭제됩니다.

8. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

새로 고침을 하기 위해서는 Refresh 버튼을 클릭하세요

다음 표에는 DNS 서버 구성 정보가 표시되어 있습니다.

Table 24. DNS 서버 구성

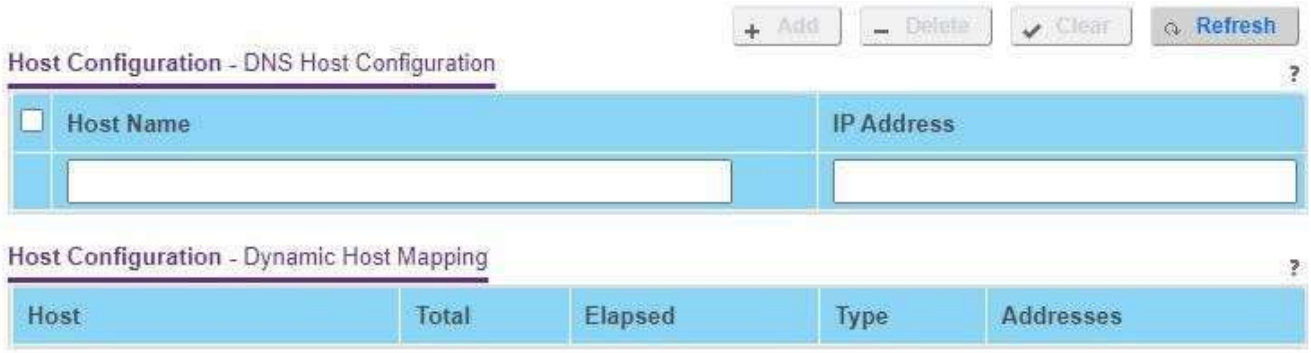
필드	설명
Serial No	DNS 서버의 시퀀스 번호입니다.
Preference	DNS 서버의 기본 설정을 표시합니다. 기본 설정은 입력된 순서에 따라 결정됩니다.

로컬 DNS 테이블에 정적 항목 추가

호스트 이름을 IP 주소에 수동으로 매핑하거나 동적 DNS 매핑을 볼 수 있습니다.

➢ **로컬 DNS 테이블에 정적 항목을 추가하려면:**

System > Management > DNS > Host Configuration.



1. Host Name (1~255자) 필드에 추가할 정적 호스트 이름을 지정합니다.

   길이는 255자를 초과할 수 없으며 필수 필드입니다.

2. IP Address 필드에 호스트 이름과 연결할 IP 주소를 표준 IPv4 점 표기법으로 입력합니다.

3. Add 버튼을 클릭합니다.

   항목이 화면의 목록에 나타납니다.

4. 정적 DNS 테이블에서 항목을 제거하려면 해당 check box을 선택하고 Delete 버튼을 클릭합니다. 목록에서 모든 동적 호스트 이름 항목을 지우려면 Clear버튼을 클릭합니다.

새로 고침을 하기 위해서는 Refresh 버튼을 클릭하세요

동적 호스트 매핑 테이블에는 스위치가 학습한 호스트 이름-IP 주소 항목이 표시됩니다. 다음 표에서는 동적 호스트 필드에 대해 설명합니다.

Table 25. DNS 동적 호스트 매핑

필드	설명
Host	지정된 IP 주소에 할당하는 호스트 이름을 나열합니다.
Total	동적 항목이 테이블에 처음 추가된 이후 경과된 시간입니다.
Elapsed	동적 항목이 마지막으로 업데이트된 이후 경과된 시간입니다.
Type	동적 항목의 유형입니다.
Addresses	호스트 이름과 연관된 IP 주소를 나열합니다.

스위치 데이터베이스 관리 템플릿 기본 설정 구성

SDM(스위치 데이터베이스 관리) 템플릿은 스위치나 라우터가 다양한 기능에 사용할 수 있는 최대 리소스에 대한 설명입니다. 다양한 SDM 템플릿은 다양한 허용을 허용합니다.

스케일링 요소의 조합으로 장치 사용 방법에 따라 리소스를 다르게 할당할 수 있습니다. 즉,

1.5 cm

SDM 템플릿을 사용하면 시스템 리소스를 재할당하여 네트워크 요구 사항에 따라 다양한 기능 조합을 지원할 수 있습니다.

Note: 장치를 스택에 연결했는데 해당 템플릿이 스택의 템플릿과 일치하지 않는 경우 새 장치는 다른 스태킹 구성원이 사용하는 템플릿을 사용하여 자동으로 재부팅됩니다. 자동 재부팅을 방지하려면 먼저 스택의 기존 구성원이 사용하는 SDM 템플릿으로 템플릿을 설정하십시오. 그런 다음 새 장치의 전원을 끄고 스택에 연결한 다음 전원을 켜십시오.

스위치에 대한 SDM 템플릿 기본 설정을 구성할 수 있습니다.

➢ **SDM 템플릿 기본 설정을 구성하려면:**

System > Management > DNS > SDM Template Preference.

1. SDM Next Template ID를 사용하여 다음 활성 템플릿을 구성합니다.

   다음 재부팅 후에만 활성화됩니다. 다음 재부팅 후 기본 템플릿으로 되돌리려면 기본 옵션을 사용하십시오. 가능한 값은 다음과 같습니다.

   - Dual IPv4 and IPv6
   - IPv4 Routing Default
   - IPv4 Data Center
   - IPv4 Data Center Plus
   - Dual IPv4 and IPv6 Data Center

다음 표에는 요약 정보가 표시됩니다.

Table 26. SDM 템플릿 기본 설정 요약

필드	설명
SDM Current Template ID	현재 활성 SDM 템플릿입니다. 가능한 값은 다음과 같습니다: • Dual IPv4 and IPv6 • IPv4-routing Default • IPv4 Data Center
SDM Template	템플릿을 식별합니다. 가능한 값은 다음과 같습니다. • Dual IPv4 and Pv6 • IPv4-routing Default • IPv4 Data Center
ARP Entries	라우팅 인터페이스에 대한 IPv4 ARP(주소 확인 프로토콜) 캐시의 최대 항목 수입니다.
IPv4 Unicast Routes	IPv4 유니캐스트 전달 테이블 항목의 최대 수입니다.

1.5 cm

IPv6 NDP Entries	IPv6 NDP(Neighbor Discovery Protocol) 캐시 항목의 최대 수입니다.
IPv6 Unicast Routes	IPv6 유니캐스트 전달 테이블 항목의 최대 수입니다.
ECMP Next Hops	IPv4 및 IPv6 유니캐스트 전달 테이블에 설치할 수 있는 최대 다음 홉 수입니다.
IPv4 Multicast Routes	IPv4 멀티캐스트 전달 테이블 항목의 최대 수입니다.
IPv6 Multicast Routes	IPv6 멀티캐스트 전달 테이블 항목의 최대 수입니다.

SNMP 구성

SNMP V1/V2 및 SNMPv3에 대한 SNMP 설정을 구성할 수 있습니다.

SNMP V1/V2 커뮤니티 구성

기본적으로 두 개의 SNMP 커뮤니티가 존재합니다.

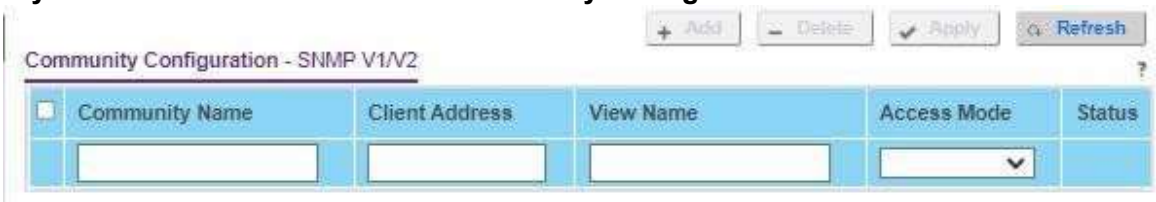
- Private, 읽기/쓰기 권한이 있고 상태가 Enable로 설정되어 있습니다.
- Public, 읽기 전용 권한이 있으며 상태가 Enable로 설정되어 있습니다

이들은 잘 알려진 커뮤니티입니다. 기본값을 변경하거나 다른 커뮤니티를 추가할 수 있습니다. 정의한 커뮤니티만 SNMP V1 및 SNMP V2 프로토콜을 사용하여 스위치에 액세스할 수 있습니다. 읽기/쓰기 수준 액세스 권한이 있는 커뮤니티만 SNMP를 사용하여 구성을 변경하는 데 사용할 수 있습니다.

Note: SNMP v3를 사용하려면 사용자 계정 메뉴를 사용하십시오.

➢ **SNMP V1/V2 커뮤니티를 구성하려면:**

System > SNMP > SNMP V1/V2 > Community Configuration.



1. Community Name을 사용하여 기존 커뮤니티를 재구성하거나 새 커뮤니티를 만듭니다.

   이 메뉴를 사용하여 기존 커뮤니티 이름 중 하나를 선택하거나 '만들기'를 선택하여 새 커뮤니티 이름을 추가하세요. 유효한 항목은 최대 16자의 대소문자 구분 문자열입니다.

2. **Client Address**. 클라이언트 주소와 클라이언트 IP 마스크를 종합하면 SNMP 클라이언트가 해당 커뮤니티를 사용하여 이 장치에 액세스할 수 있는 IP 주소 범위를 나타냅니다.

   (클라이언트 주소 또는 IP 마스크) 값 중 하나가 0.0.0.0이면 모든 IP 주소에서 액세스가 허용됩니다. 그렇지 않은 경우 모든 클라이언트의 주소는 클라이언트 주소와 마찬가지로 마스크와 AND로 연결되며 값이 동일하면 액세스가 허용됩니다. 예를 들어 클라이언트 주소 및 클라이언트 IP 마스크 매개변수가 192.168.1.0/255.255.255.0인 경우 주소가 192.168.1.0부터 192.168.1.255(포함)까지인 모든 클라이언트에 액세스가 허용됩니다. 한 스테이션에서만 액세스를 허용하려면 클라이언트 IP 마스크 값 255.255.255.255를 사용하고 클라이언트 주소에 해당 컴퓨터의 IP 주소를 사용합니다.

3. **Client IP Mask**. 클라이언트 주소와 클라이언트 IP 마스크를 종합하면 SNMP 클라이언트가 해당 커뮤니티를 사용하여 이 장치에 액세스할 수 있는 IP 주소 범위를 나타냅니다.

   (클라이언트 주소 또는 IP 마스크) 값 중 하나가 0.0.0.0이면 모든 IP 주소에서 액세스가 허용됩니다. 그렇지 않은 경우 모든 클라이언트의 주소는 클라이언트 주소와 마찬가지로 마스크와 AND로 연결되며 값이 동일하면 액세스가 허용됩니다. 예를 들어 클라이언트 주소 및 클라이언트 IP 마스크 매개변수가 192.168.1.0/255.255.255.0인 경우 IP 주소가 192.168.1.0~192.168.1.255(포함)인 모든 클라이언트에 액세스가 허용됩니다. 한 스테이션에서만 액세스를 허용하려면 클라이언트 IP 마스크 값 255.255.255.255를 사용하고 클라이언트 주소에 해당 컴퓨터의 IP 주소를 사용합니다.

4. Access Mode 메뉴에서 Read-Write 또는 Read-Only을 선택합니다.

   이는 이 커뮤니티에 대한 액세스 수준을 지정합니다.

5. Status를 사용하여 Enable 또는 Disable를 선택하여 이 커뮤니티의 상태를 지정합니다.

   Enable를 선택하면 커뮤니티 이름은 모든 유효한 커뮤니티 이름 중에서 고유해야 하며 그렇지 않으면 설정 요청이 거부됩니다. Disable를 선택하면 커뮤니티 이름이 유효하지 않게 됩니다.

6. Add 버튼을 클릭합니다.

   그러면 선택한 커뮤니티가 스위치에 추가됩니다.

1.5 cm

7. 선택한 커뮤니티 이름을 삭제하려면 Delete 버튼을 클릭하세요.

SNMP V1/V2 트랩 설정 구성

➢ **SNMP V1/V2 트랩 설정을 구성하려면:**

System > SNMP > SNMP V1/V2 > Trap Configuration.

1. Source Interface 목록에서 SNMP 트랩 수신기에 사용할 소스 인터페이스를 선택합니다.

   가능한 값은 다음과 같습니다.

   - Routing interface
   - Routing VLAN
   - Routing loopback interface
   - Tunnel interface
   - Service port

   VLAN 1은 기본적으로 소스 인터페이스로 사용됩니다.

2. SNMP 트랩을 수신하는 호스트를 추가하려면 다음 단계를 수행하십시오.

   a. **Community Name**. 트랩 관리자로 보낼 SNMP 트랩 패킷의 커뮤니티 문자열을 입력합니다. 이 이름은 최대 16자까지 가능하며 대소문자를 구분합니다.

   b. **Version.** 수신자가 사용할 트랩 버전을 선택하십시오.

      - **SNMP V1.** SNMP V1을 사용하여 수신기에 트랩을 보냅니다.
      - **SNMP V2.** SNMP V2를 사용하여 수신기에 트랩을 보냅니다.

   c. **Protocol**. 수신기에서 사용할 프로토콜을 선택합니다. 수신자 주소가 IPv4 주소인 경우 IPv4를 선택하고, 수신자 주소가 IPv6인 경우 IPv6을 선택합니다.

   d. **Address**. 이 장치에서 SNMP 트랩을 수신하려면 x.x.x.x 형식으로 IPv4 주소를 입력하거나 xxxx:xxxx:xxxx:xxxxx:xxxx:xxxx:xxxx:xxxx 형식으로 IPv6 주소를 입력하십시오.

      주소 길이는 39자를 초과할 수 없습니다.

   e. **Status**. 수신자의 상태를 선택하세요:

      - **Enable**. 수신자에게 트랩을 보냅니다.
      - **Disable**. 수신자에게 트랩을 보내지 않습니다.

1.5 cm

f. Add 버튼을 클릭합니다.

3. 기존 SNMP 수신자에 대한 정보를 수정하려면 수신자에 대한 check box을 선택하고 원하는 필드를 변경합니다.
4. 수신자를 삭제하려면 해당 수신자의 check box을 선택한 후 Delete 버튼을 클릭하세요.
5. Apply 버튼을 클릭합니다

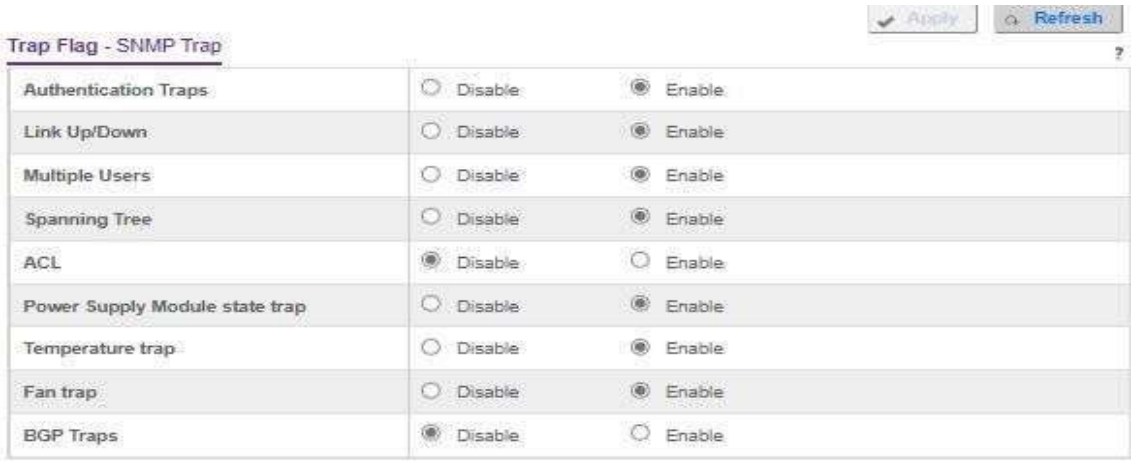
   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

SNMP V1/V2 트랩 플래그 구성

트랩을 활성화하거나 비활성화할 수 있습니다. 스위치에서 활성 트랩으로 식별된 조건이 발생하면 트랩 메시지가 활성화된 모든 SNMP 트랩 수신기로 전송되고 메시지가 트랩 로그에 기록됩니다.

➢ **트랩 플래그를 구성하려면:**

System > SNMP > SNMP V1/V2 > Trap Flags.



1. Authentication Trap의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   인증 실패 트랩의 활성화를 활성화하거나 비활성화합니다. 공장 기본값은 Enable입니다.

2. Link Up/Down의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 링크 상태 트랩의 활성화를 활성화하거나 비활성화합니다. 공장 기본값은 Enable입니다.

3. Multiple Users의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 여러 사용자 트랩의 활성화를 활성화하거나 비활성화합니다. 공장 기본값은 Enable입니다.

1.5 cm

이 트랩은 동일한 사용자 ID가 동시에 두 번 이상 스위치에 로그인될 때(텔넷 또는 직렬 포트를 통해) 트리거됩니다.

4. Spanning Tree 의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 스패닝 트리 트랩의 활성화를 활성화하거나 비활성화합니다. 공장 기본값은 Enable입니다.

5. ACL의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   ACL 트랩 활성화를 활성화하거나 비활성화합니다. 공장 기본값은 Disable입니다.

6. PoE 의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   PoE 트랩 활성화를 활성화하거나 비활성화합니다. 공장 기본값은 Enable입니다.

   PoE 트랩이 전송되는지 여부를 나타냅니다.

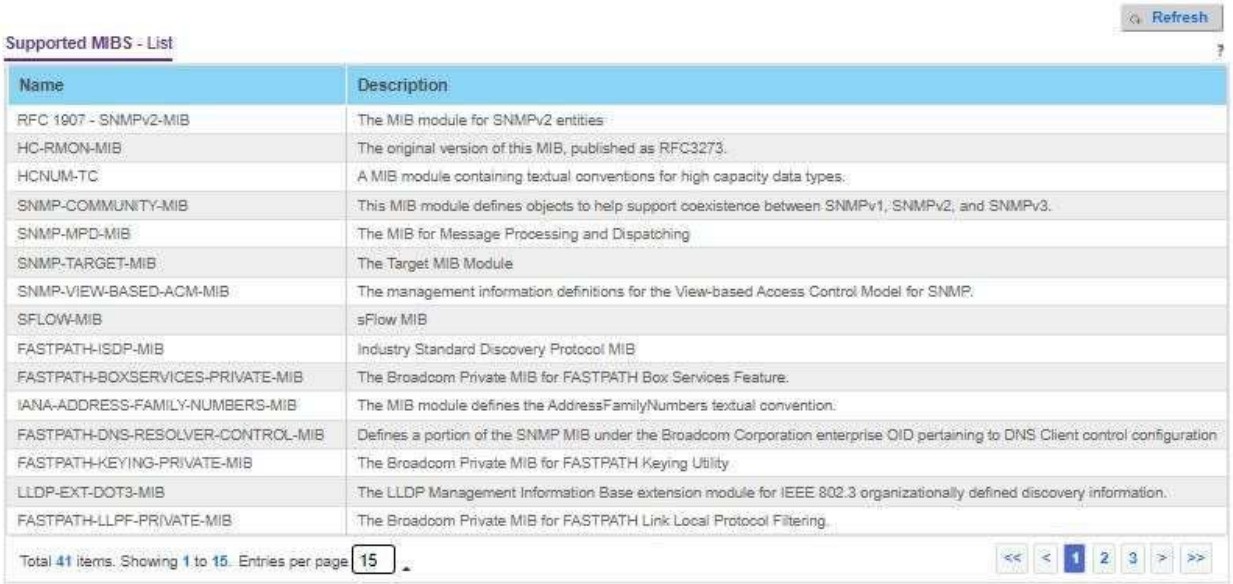
7. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

지원되는 MIB 보기

➢ **스위치가 지원하는 모든 MIB를 보려면:**

System > SNMP > SNMP V1/V2 >Supported MIBs.



다음 표에서는 SNMP 지원 MIB 상태 필드에 대해 설명합니다.

Table 43. SNMP 지원 MIB

필드	설명

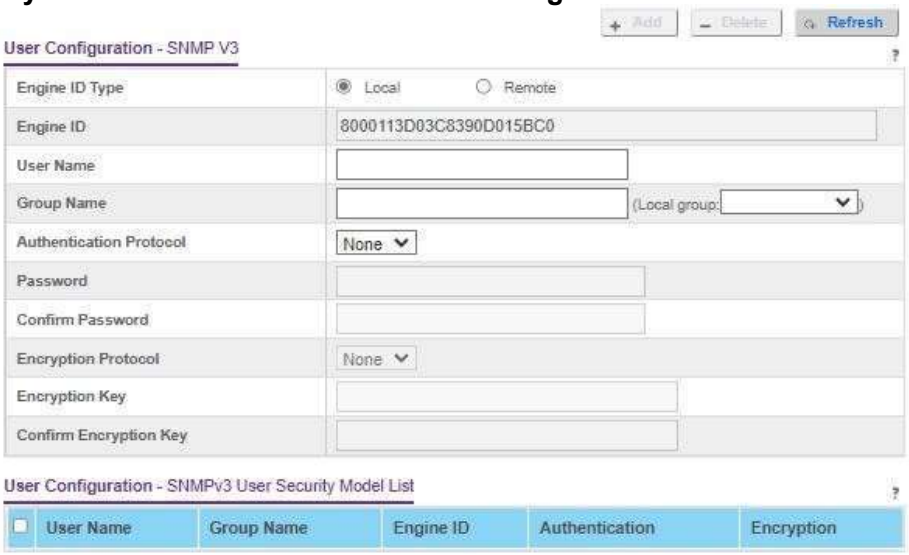
1.5 cm

Name	해당하는 경우 RFC 번호와 MIB의 이름입니다.
Description	RFC 제목 또는 MIB 설명입니다.

Configure SNMP V3 Users

➢ **사용자 계정에 대한 SNMPv3 설정을 구성하려면:**

System > SNMP > SNMP V3 > User Configuration.



1. User Name 목록에서 구성할 사용자 계정을 선택합니다.

   SNMP v3 Access Mode 필드는 사용자 계정에 대한 SNMPv3 액세스 권한을 나타냅니다. 관리자 계정에는 읽기/쓰기 액세스 권한이 있으며 다른 모든 계정에는 읽기 전용 액세스 권한이 할당됩니다.

2. Authentication Protocol 라디오 버튼을 선택합니다.

   유효한 인증 프로토콜은 없음, MD5 또는 SHA입니다.

   - None을 선택하면 사용자는 SNMP 브라우저에서 SNMP 데이터에 액세스할 수 없습니다.
   - MD5 또는 SHA를 선택한 경우 사용자 로그인 비밀번호가 SNMPv3 인증 비밀번호로 사용되므로 비밀번호를 지정해야 하며 길이는 8자여야 합니다.

   선택한 사용자 계정에 대한 SNMPv3 인증 프로토콜 설정을 지정합니다.

3. Encryption Protocol 라디오 버튼을 선택합니다.

   유효한 암호화 프로토콜은 None 또는 DES입니다.

   - DES 프로토콜을 선택한 경우 Encryption Key 필드에 키를 입력해야 합니다.
   - 프로토콜에 None을 지정하면 암호화 키가 무시됩니다.

1.5 cm

선택한 사용자 계정에 대한 SNMPv3 암호화 프로토콜 설정을 지정합니다.

4. Encryption Protocol 필드에서 DES를 선택한 경우 SNMPv3 Encryption Key 필드에 암호화 키를 입력합니다.

   DES를 선택하지 않은 경우 이 필드는 무시됩니다. 유효한 키의 길이는 0~15자입니다.

   암호화 프로토콜 및 암호화 키를 변경하려면 Apply check box을 선택해야 합니다.

5. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

LLDP 개요

IEEE 802.1AB 정의 표준인 LLDP(Link Layer Discovery Protocol)를 사용하면 802 LAN의 스테이션이 주요 기능과 물리적 설명을 광고할 수 있습니다. 네트워크 관리자는 이 정보를 보고 시스템 토폴로지를 식별하고 LAN의 잘못된 구성을 감지합니다.

LLDP는 단방향 프로토콜입니다. 요청/응답 시퀀스가 없습니다. 정보는 전송 기능을 구현하는 스테이션에 의해 광고되고, 수신 기능을 구현하는 스테이션에 의해 수신 및 처리됩니다. 전송 및 수신 기능은 포트별로 별도로 활성화/비활성화할 수 있습니다. 기본적으로 모든 포트에서 전송 및 수신이 모두 비활성화되어 있습니다.
애플리케이션은 포트의 구성된 상태와 작동 상태를 기반으로 각 전송 및 수신 상태 머신을 적절하게 시작하는 역할을 담당합니다.

LLDP-MED(Link Layer Discovery Protocol-Media Endpoint Discovery)는 다음 기능을 갖춘 LLDP의 향상된 기능입니다.

- LAN 정책(예: VLAN, 레이어 2 우선 순위, DiffServ 설정) 자동 검색을 통해 플러그 앤 플레이 네트워킹이 가능합니다.
- 위치 데이터베이스 생성을 위한 장치 위치 검색.
- PoE 엔드포인트의 확장되고 자동화된 전원 관리.
- 재고 관리 - 네트워크 관리자가 네트워크 장치를 추적하고 특성(제조업체, 소프트웨어 및 하드웨어 버전, 일련번호/자산 번호)을 확인할 수 있습니다.

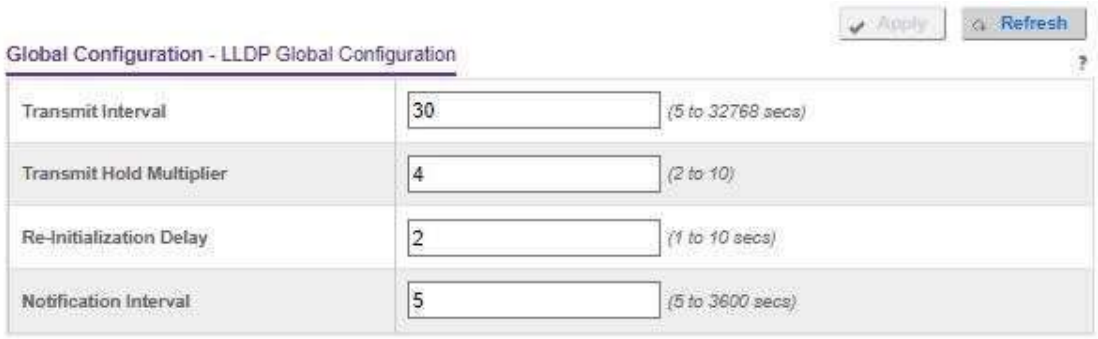
Configure LLDP Global Settings

스위치에 적용되는 LLDP 매개변수를 지정할 수 있습니다.

➢ **글로벌 LLDP 설정을 구성하려면:**

1.5 cm

System > LLDP > Global Configuration.



1. Transmit Interval 필드에 LLDP 프레임을 전송할 간격을 초 단위로 입력합니다.

   범위는 5~32768초입니다. 기본값은 30초입니다.
2. Transmit Hold Multiplier 필드에 전송 간격에 승수를 입력하여 TTL을 할당합니다.

   범위는 2~10초입니다. 기본값은 4입니다.
3. Re-Initialization Delay 필드에 재초기화 전 지연 시간을 입력합니다.

   범위는 1~10초입니다. 기본값은 2초입니다.
4. Notification Interval 필드에 알림 전송 간격을 초 단위로 입력합니다.

   범위는 5~3600초입니다. 기본값은 5초입니다.
5. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 변경 사항은 즉시 적용되지만 저장을 수행하지 않는 한 전원을 껐다 켜도 유지되지 않습니다.

LLDP 인터페이스 구성

➢ **LLDP 인터페이스를 구성하려면:**

System > LLDP > Interface Configuration.

1. Go To Port를 이용하여 유닛/슬롯/포트 형식으로 포트를 입력한 후 Go 버튼을 클릭하세요.
   지정된 포트에 해당하는 항목이 선택됩니다.
2. 포트를 사용하여 LLDP - 802.1AB를 구성할 수 있는 포트 목록을 지정합니다.
   링크 상태 필드는 링크가 작동 중인지 작동 중지되었는지 여부를 나타냅니다.
3. 전송을 사용하여 선택한 인터페이스에 대한 LLDP - 802.1AB 전송 모드를 지정합니다.
4. 수신을 사용하여 선택한 인터페이스에 대한 LLDP - 802.1AB 수신 모드를 지정합니다.
5. 알림을 사용하여 선택한 인터페이스에 대한 LLDP - 802.1AB 알림 모드를 지정합니다.

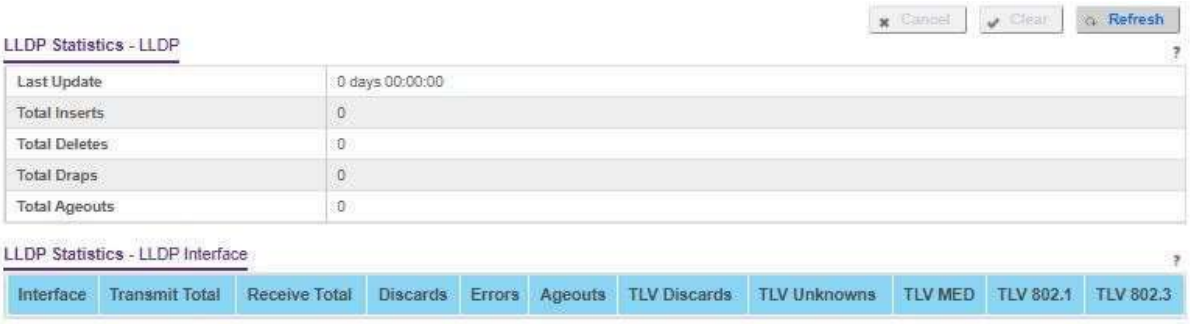
1.5 cm

6. 선택적 TLV(s):
   A. Port Description을 사용하여 LLDP 프레임에 포트 설명 TLV를 포함합니다.
   B. System Name을 사용하여 LLDP 프레임에 시스템 이름 TLV를 포함합니다.
   C. System Description을 사용하여 LLDP 프레임에 시스템 설명 TLV를 포함합니다.
   D. System Capabilities을 사용하여 LLDP 프레임에 시스템 기능 TLV를 포함합니다.
7. Transmit Management Information을 사용하여 선택한 인터페이스에 대해 관리 주소가 LLDP 프레임에서 전송되는지 여부를 지정합니다.

LLDP 통계 보기

➢ **LLDP 통계를 보려면:**

System > LLDP > Statistics.



다음 표에서는 LLDP 통계 필드에 대해 설명합니다.

Table 44. LLDP 통계

필드	설명
Last Update	원격 시스템과 연결된 테이블에서 항목이 생성, 수정 또는 삭제된 시간입니다.
Total Inserts	특정 MSAP(MAC 서비스 액세스 포인트)에서 광고한 전체 정보 세트가 원격 시스템과 연결된 테이블에 삽입된 횟수입니다.
Total Deletes	특정 MSAP(MAC 서비스 액세스 포인트)가 광고한 전체 정보 세트가 원격 시스템과 연결된 테이블에서 삭제된 횟수입니다.
Total Drops	특정 MSAP(MAC 서비스 액세스 포인트)에서 광고하는 전체 정보 세트를 리소스 부족으로 인해 원격 시스템과 연결된 테이블에 입력할 수 없는 횟수입니다.
Total Age outs	정보 적시성 간격이 만료되었기 때문에 특정 MSAP(MAC 서비스 액세스 포인트)에서 광고한 전체 정보 세트가 원격 시스템과 연결된

1.5 cm

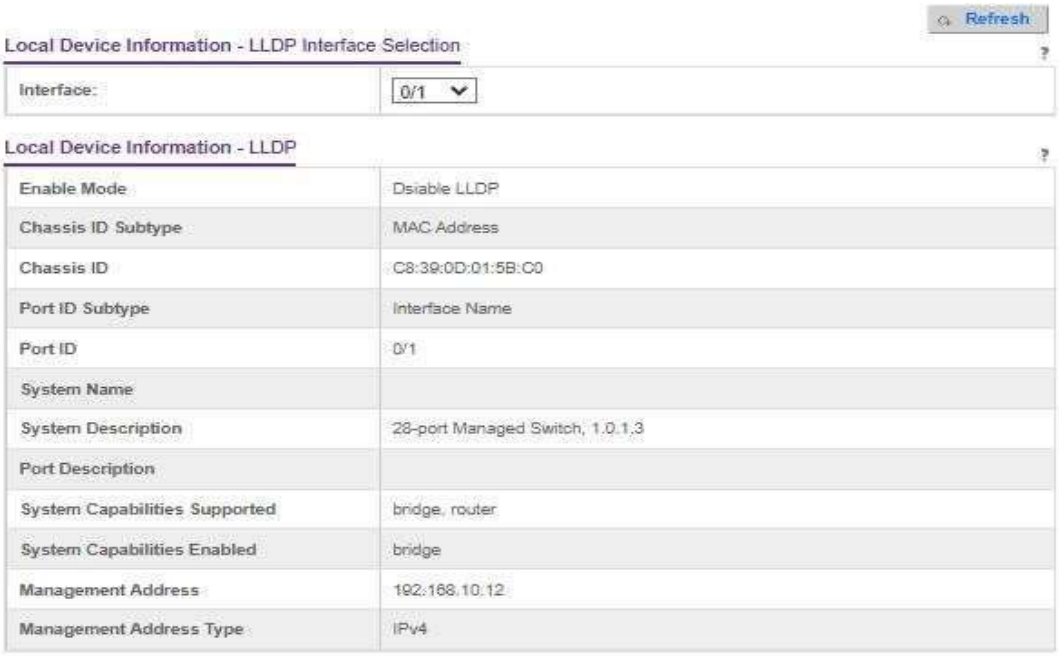
	테이블에서 삭제된 횟수입니다.
Interface	인터페이스의 장치/슬롯/포트입니다.
Transmit Total	해당 포트에서 LLDP 에이전트가 전송한 LLDP 프레임 수입니다.
Receive Total	LLDP 에이전트가 활성화된 동안 해당 포트에서 이 LLDP 에이전트가 수신한 유효한 LLDP 프레임 수입니다.
Discards	해당 포트의 LLDP 에이전트가 어떤 이유로든 폐기한 LLDP TLV 수입니다.
Errors	LLDP 에이전트가 활성화된 동안 해당 포트에서 LLDP 에이전트가 수신한 잘못된 LLDP 프레임 수입니다.
Age outs	특정 포트에서 발생한 만료 횟수입니다. 만료 기간은 정보 적시성 간격이 만료되었기 때문에 특정 MSAP(MAC 서비스 액세스 포인트)에서 광고한 전체 정보 세트가 원격 항목과 연결된 테이블에서 삭제된 횟수입니다.
TLV Discards	해당 포트의 LLDP 에이전트가 어떤 이유로든 폐기한 LLDP TLV 수입니다.
TLV Unknowns	해당 포트의 LLDP 에이전트가 인식하지 못한 로컬 포트에서 수신된 LLDP TLV 수입니다.
TLV MED	로컬 포트에서 수신된 LLDP-MED TLV의 총 수입니다.
TLV 802.1	802.1 유형의 로컬 포트에서 수신된 LLDP TLV의 총 수입니다.
TLV 802.3	802.3 유형의 로컬 포트에서 수신된 LLDP TLV의 총 수입니다.

LLDP 로컬 장치 정보 보기

- **LLDP 로컬 장치 정보를 보려면:**

  System > LLDP > Local Device Information.

1.5 cm



1. Interface 목록에서 LLDP - 802.1AB 프레임이 전송될 수 있는 포트를 선택합니다.

다음 표에서는 LLDP 로컬 장치 정보 필드에 대해 설명합니다.

Table 45. LLDP 로컬 장치 정보

필드	내용
Chassis ID Subtype	섀시 식별자의 소스를 설명하는 문자열입니다.
Chassis ID	로컬 시스템과 연결된 섀시 구성 요소를 식별하는 데 사용되는 문자열 값입니다.
Port ID Subtype	포트 식별자의 소스를 설명하는 문자열입니다.
Port ID	포트 식별자의 소스를 설명하는 문자열입니다.
System Name	로컬 시스템의 시스템 이름입니다.
System Description	로컬 시스템과 연결된 선택된 포트에 대한 설명입니다.
Port Description	로컬 시스템과 연결된 선택된 포트에 대한 설명입니다.
System Capabilities Supported	로컬 시스템의 시스템 기능입니다.
System Capabilities Enabled	지원되고 활성화되는 로컬 시스템의 시스템 기능입니다.
Management Address Type	관리 주소의 유형입니다.
Management Address	로컬 시스템의 공지된 관리 주소입니다.

LLDP 원격 장치 정보 보기

해당 포트에 연결된 원격 장치의 정보를 확인할 수 있습니다.

➢ **LLDP 원격 장치 정보를 보려면:**

System > LLDP > Remote Device Information.

1. 인터페이스를 사용하여 LLDP 프레임을 수신할 수 있는 로컬 포트를 선택합니다.

다음 표에서는 LLDP 원격 장치 정보 필드에 대해 설명합니다.

Table 46. LLDP 원격 장치 정보

필드	설명
Remote ID	원격 ID입니다.
Chassis ID	원격 시스템과 연결된 섀시 구성 요소입니다.
Chassis ID Subtype	섀시 식별자의 소스입니다.
Port ID	원격 시스템과 연결된 포트 구성 요소입니다.
Port ID Subtype	포트 식별자의 소스입니다.
System Name	원격 시스템의 시스템 이름입니다.
System Description	원격 시스템과 연관된 특정 포트에 대한 설명입니다.

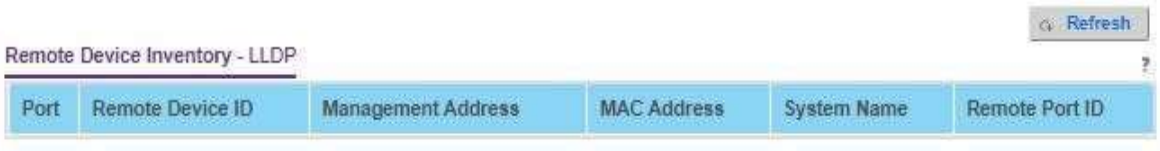
1.5 cm

Port Description	원격 시스템과 연관된 특정 포트에 대한 설명입니다.
System Capabilities Supported	원격 시스템의 시스템 기능입니다.
System Capabilities Enabled	지원되고 활성화되는 원격 시스템의 시스템 기능입니다.
Time to Live	수신된 원격 항목의 TTL(Time To Live) 값(초)입니다.
Management Address Type	관리 주소의 유형입니다.
Management Address	• Management Address. 원격 시스템의 공지된 관리 주소입니다. • Type. 관리 주소의 유형입니다.

LLDP 원격 장치 인벤토리 보기

➢ **LLDP 원격 장치 인벤토리를 보려면:**

System > LLDP > LLDP > Remote Device Inventory.



다음 표에서는 LLDP 원격 장치 인벤토리 필드에 대해 설명합니다.

Table 47. LLDP 원격 장치 인벤토리

필드	설명
Port	LLDP 프레임이 활성화된 모든 포트의 목록입니다.
Remote Device ID	원격 장치 ID입니다.
Management Address	원격 시스템의 공지된 관리 주소입니다.
MAC Address	원격 시스템과 연결된 MAC 주소입니다.
System Name	원격 장치의 모델 이름을 지정합니다.
Remote Port ID	원격 시스템과 연결된 포트 구성 요소입니다.

LLDP-MED 전역 설정 구성

스위치에 적용되는 LLDP-MED 매개변수를 지정할 수 있습니다.

➢ **LLDP-MED 전역 설정을 구성하려면:**

1.5 cm

System > LLDP > LLDP-MED > Global Configuration.

1. Fast Start Repeat Count(빠른 시작 반복 횟수) 필드에 프로토콜이 활성화될 때 전송되는 LLDP PDU 수를 입력합니다.

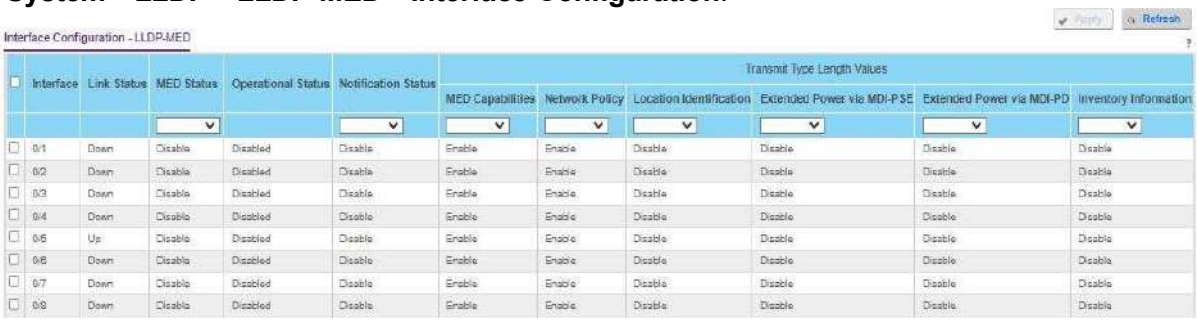
   범위는 (1~10)입니다. 빠른 반복 횟수의 기본값은 3입니다.

   Device Class 필드는 로컬 장치의 MED 분류를 지정합니다. 네 가지 종류의 장치가 있으며 그 중 세 개는 실제 종단점을 나타냅니다(클래스 I 일반 [IP 통신 컨트롤러 등], 클래스 II 미디어[컨퍼런스 브리지 등], 클래스 III 통신[IP 전화 등으로 분류) 에]). 네 번째 장치는 일반적으로 LAN 스위치/라우터, IEEE 802.1 브리지, IEEE 802.11 무선 액세스 포인트 등인 네트워크 연결 장치입니다.

LLDP-MED 인터페이스 구성

➢ **LLDP-MED 인터페이스를 구성하려면 :**

System > LLDP > LLDP-MED > Interface Configuration.



Link Status 필드에는 포트의 링크 상태(작동 또는 작동 중지)가 표시됩니다.

Operational Status 필드에는 LLDP-MED TLV가 이 인터페이스에서 전송되는지 여부가 표시됩니다.

1. Go To Port를 이용하여 유닛/슬롯/포트 형식으로 포트를 입력한 후 Go 버튼을 클릭하세요.

   지정된 포트에 해당하는 항목이 선택됩니다.

2. Interface를 사용하여 LLDP-MED - 802.1AB를 구성할 수 있는 포트 목록을 지정합니다.
3. MED Status를 사용하여 이 인터페이스에서 LLDP-MED 모드를 활성화할지 비활성화할지

1.5 cm

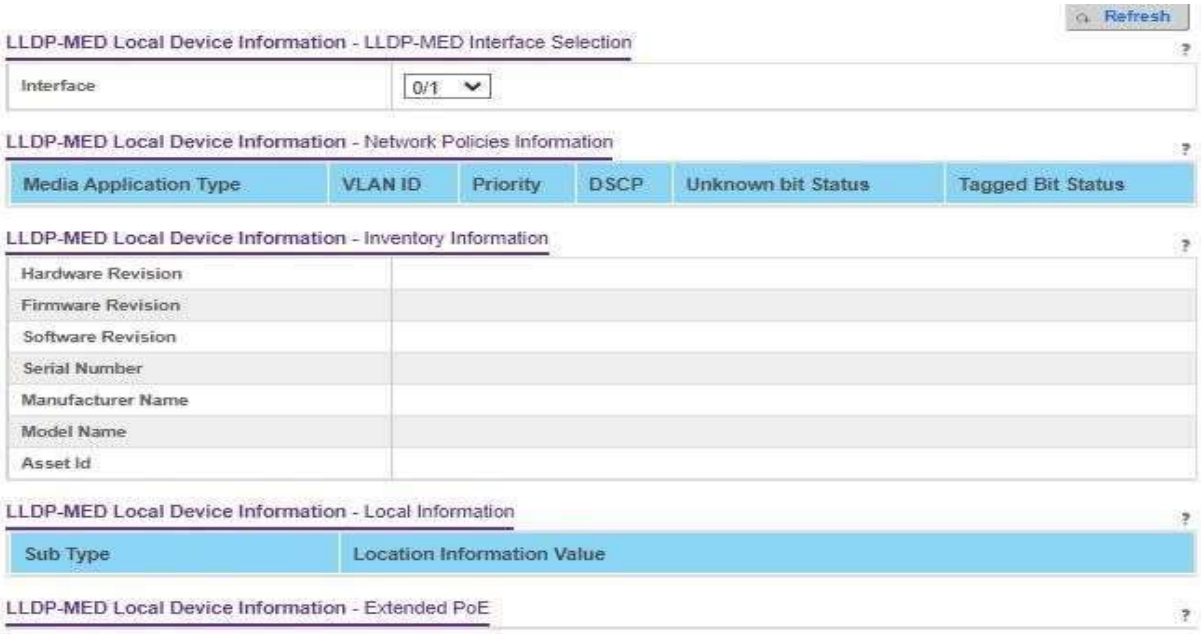
지정합니다.

4. Notification Status를 사용하여 인터페이스의 LLDP-MED 토폴로지 알림 모드를 지정합니다.
5. Transmit Type Length Values을 사용하여 선택한 인터페이스에 대한 LLDP PDU 프레임에서 전송되는 LLDP-MED의 선택적 유형 길이 값(TLV)을 지정합니다.
   - **MED Capabilities**. LLDP 프레임에서 TLV 기능을 전송합니다.
   - **Network Policy**. LLDP 프레임에서 네트워크 정책 TLV를 전송합니다.
   - **Location Identification**. LLDP 프레임에서 위치 TLV를 전송합니다.
   - **Extended Power via MDI - PSE**. 확장된 PSE TLV를 LLDP 프레임으로 전송합니다.
   - **Extended Power via MDI - PD**. 확장된 PD TLV를 LLDP 프레임으로 전송합니다.
   - **Inventory Information**. LLDP 프레임에서 인벤토리 TLV를 전송합니다.

LLDP-MED 로컬 장치 정보 보기

➢ **LLDP-MED 로컬 장치 정보를 보려면:**

System > LLDP > LLDP-MED > Local Device Information.



1. Interface를 사용하여 LLDP-MED 프레임이 전송될 수 있는 포트를 선택합니다.

다음 표에서는 LLDP-MED 로컬 장치 정보 필드에 대해 설명합니다.

1.5 cm

Table 48. LDP-MED 로컬 장치 정보

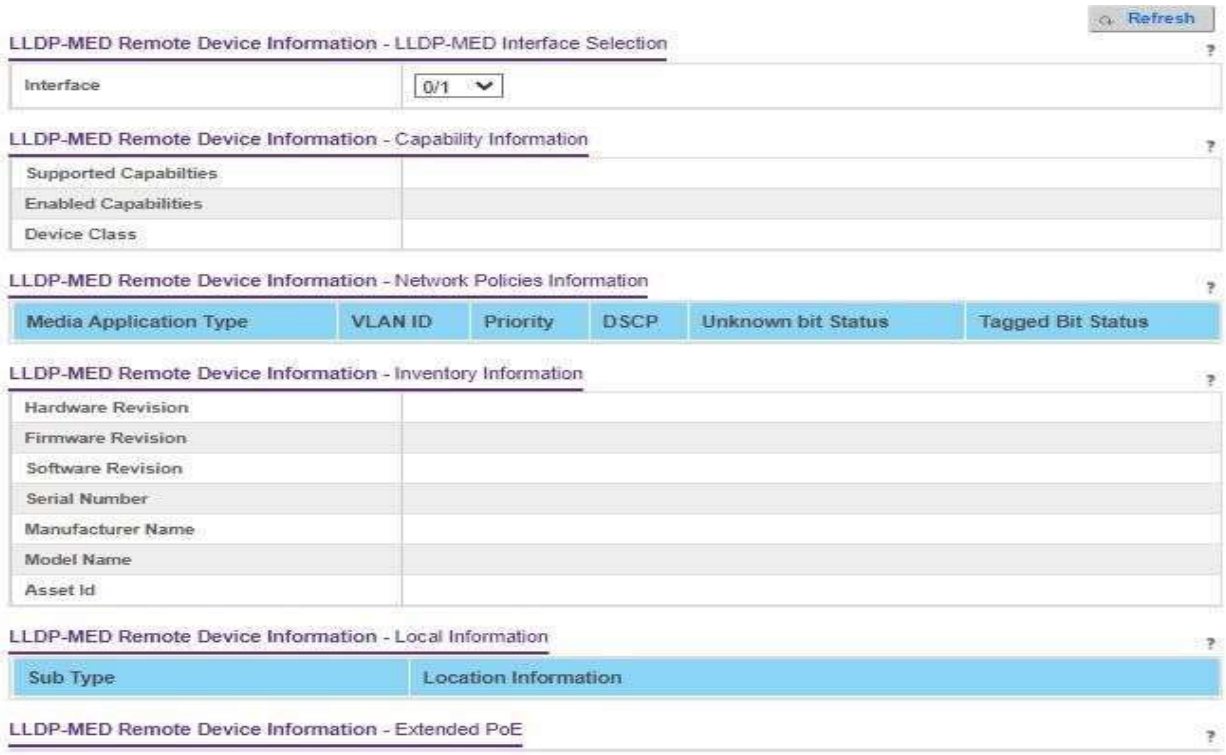
필드	설명
Network Policies Information: LLDP 프레임에 네트워크 정책 TLV가 있는지 여부를 지정합니다.	
Media Application Type	애플리케이션 유형입니다. 애플리케이션 유형의 유형은 알 수 없으며 음성 신호, 게스트 음성, 게스트 음성 신호, 소프트폰 음성, 화상 회의, 스트리밍 비디오, 비디오 신호입니다. 수신된 각 애플리케이션 유형에는 VLAN ID, 우선 순위, DSCP, 태그된 비트 상태 및 알 수 없는 비트 상태가 있습니다. 포트는 그러한 애플리케이션 유형을 하나 이상 수신할 수 있습니다. 네트워크 정책 TLV가 전송된 경우에만 이 정보가 표시됩니다.
Inventory: LLDP 프레임에 인벤토리 TLV가 있는지 여부를 지정합니다.	
Hardware Revision	하드웨어 버전을 지정합니다.
Firmware Revision	펌웨어 버전을 지정합니다.
Software Revision	소프트웨어 버전을 지정합니다.
Serial Number	일련번호를 지정합니다.
Manufacturer Name	제조업체 이름을 지정합니다.
Model Name	모델 이름을 지정합니다.
Asset ID	자산 ID를 지정합니다.
Location Information: LLDP 프레임에 위치 TLV가 있는지 여부를 지정합니다.	
Sub Type	위치 정보의 유형을 지정합니다.
Location Information	특정 유형의 위치 ID에 대한 문자열로 된 위치 정보입니다.

LLDP-MED 원격 장치 정보 보기

- **LLDP-MED 원격 장치 정보를 보려면:**

  System > LLDP > LLDP-MED > Remote Device Information.

1.5 cm



1. Interface를 사용하여 LLDP-MED가 활성화된 포트를 선택합니다.

다음 표에서는 LLDP-MED 원격 장치 정보 필드에 대해 설명합니다.

Table 49. LLDP-MED 원격 장치 정보

필드	설명
Capability Information: 이 포트의 MED TLV에서 수신된 지원 및 활성화된 기능입니다.	
Supported Capabilities	이 포트의 MED TLV에서 수신된 지원 기능을 지정합니다.
Enabled Capabilities	이 포트의 MED TLV에서 수신된 활성화된 기능을 지정합니다.
Device Class	포트에 원격으로 연결된 장치가 광고하는 장치 클래스를 지정합니다.
Network Policy Information: 이 포트의 LLDP 프레임에서 네트워크 정책 TLV가 수신되는지 여부를 지정합니다.	
Media Application Type	애플리케이션 유형입니다. 애플리케이션 유형의 유형은 알 수 없으며 음성 신호, 게스트 음성, 게스트 음성 신호, 소프트폰 음성, 화상 회의, 스트리밍 비디오, 비디오 신호입니다. 수신된 각 애플리케이션 유형에는 VLAN ID, 우선 순위, DSCP, 태그된 비트 상태 및 알 수 없는 비트 상태가 있습니다. 포트는 그러한 애플리케이션 유형을 하나 이상 수신할 수 있습니다. 이 포트에서 네트워크 정책 TLV가 수신된 경우에만 이 정보가 표시됩니다.
VLAN Id	특정 정책 유형과 연관된 VLAN ID입니다.

1.5 cm

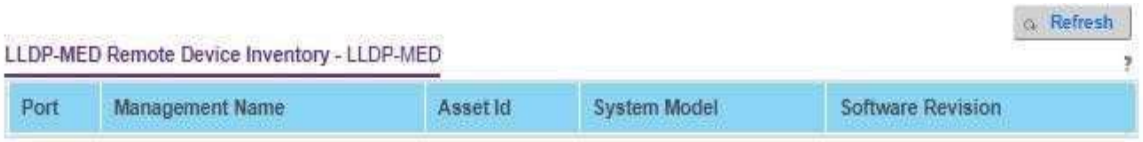
Priority	특정 정책 유형과 관련된 우선순위입니다.
DSCP	특정 정책 유형과 연결된 DSCP입니다.
Unknown Bit Status	특정 정책 유형과 관련된 알 수 없는 비트입니다.
Tagged Bit Status	특정 정책 유형과 관련된 태그가 지정된 비트입니다.
Inventory Information: 이 포트의 LLDP 프레임에서 인벤토리 TLV를 수신할지 여부를 지정합니다.	
Hardware Revision	원격 장치의 하드웨어 버전을 지정합니다.
Firmware Revision	원격 장치의 펌웨어 버전을 지정합니다.
Software Revision	원격 장치의 소프트웨어 버전을 지정합니다.
Serial Number	원격 장치의 일련 번호를 지정합니다.
Manufacturer Name	원격 장치의 제조업체 이름을 지정합니다.
Model Name	원격 장치의 모델 이름을 지정합니다.
Asset ID	원격 장치의 자산 ID를 지정합니다.
Location Information: 이 포트의 LLDP 프레임에서 위치 TLV가 수신되는지 여부를 지정합니다.	
Sub Type	위치 정보의 유형을 지정합니다.
Location Information	특정 유형의 위치 ID에 대한 문자열로 된 위치 정보입니다.
Extended POE: 원격 장치가 PoE 장치인지 여부를 지정합니다.	
Device Type	이 포트에 연결된 원격 장치의 PoE 장치 유형을 지정합니다.
Extended POE PSE: 확장 PSE TLV가 이 포트의 LLDP 프레임에서 수신되는지 여부를 지정합니다.	
Available	원격 포트 PSE 전력 값은 10분의 1와트 단위입니다.
Source	원격 포트 PSE 전원.
Priority	원격 포트 PSE 전원 우선순위입니다.
Extended POE PD: 확장 PD TLV가 이 포트의 LLDP 프레임에서 수신되는지 여부를 지정합니다.	
Required	원격 포트의 PD 전원 요구 사항입니다.
Source	원격 포트의 PD 전원.
Priority	원격 포트의 PD 전원 우선순위입니다.

LLDP-MED 원격 장치 인벤토리 보기

- **LLDP-MED 원격 장치 인벤토리를 보려면:**

  System > LLDP > LLDP-MED > Remote Device Inventory.

1.5 cm



다음 표에서는 LLDP-MED 원격 장치 인벤토리 필드에 대해 설명합니다.

Table 50. LLDP-MED 원격 장치 인벤토리

필드	설명
Port	LLDP-MED가 활성화된 모든 포트의 목록입니다.
Management Address	원격 시스템의 공지된 관리 주소입니다.
MAC Address	원격 시스템과 연결된 MAC 주소입니다.
System Model	원격 장치의 모델 이름을 지정합니다.
Software Revision	원격 장치의 소프트웨어 버전을 지정합니다.

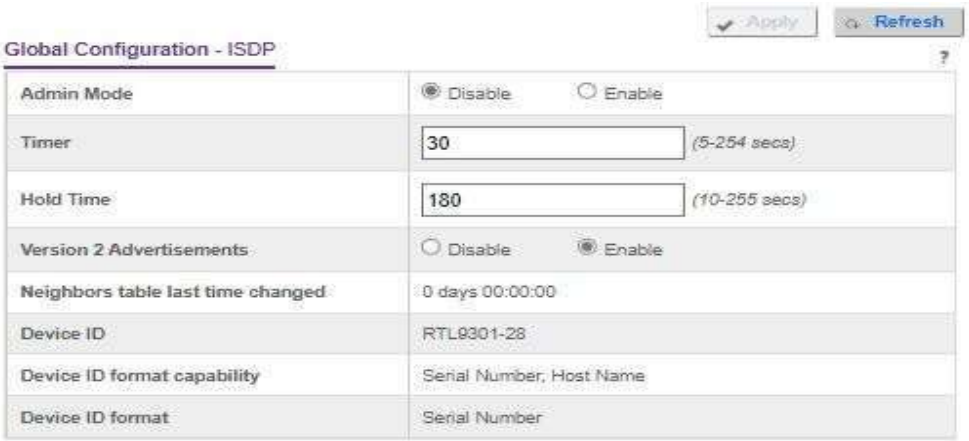
ISDP 구성

ISDP 전역 및 인터페이스 설정을 구성할 수 있습니다.

ISDP 기본 전역 설정 구성

➢ **ISDP 기본 전역 설정을 구성하려면:**

System > ISDP > Basic > Global Configuration.



1. Admin Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다

1.5 cm

ISDP 서비스의 활성화 여부를 지정합니다. 기본값은 활성화입니다.

2. Timer를 사용하여 새 ISDP 패킷 전송 사이의 시간 간격을 지정합니다.

   범위는 5~254초입니다. 기본값은 30초입니다.

3. Hold Time을 사용하여 스위치가 전송하는 ISDP 패킷의 보류 시간을 지정하십시오.

   보류 시간은 수신 장치가 ISDP 패킷을 삭제하기 전에 전송된 정보를 저장해야 하는 기간을 지정합니다. 범위는 10~255초입니다. 기본값은 180초입니다.

4. 버전 2 Advertisements의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 장치에서 ISDP 버전 2 패킷 전송을 활성화하거나 비활성화합니다. 기본값은 Enable입니다.

다음 표에서는 ISDP 기본 전역 구성 필드에 대해 설명합니다.

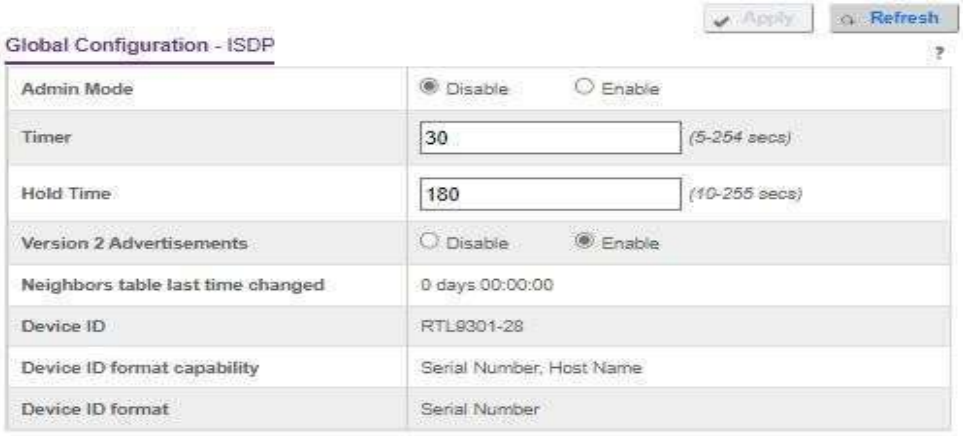
Table 51. ISDP 기본 전역 구성

필드	설명
Neighbors table last time changed	Neighbors 테이블이 마지막으로 변경된 시간을 표시합니다.
Device ID	이 스위치의 장치 ID입니다.
Device ID Format Capability	장치 ID 형식 기능입니다.
Device ID Format	장치 ID 형식입니다.

ISDP 전역 설정 구성

➢ **ISDP 전역 설정을 구성하려면:**

System > ISDP > Advanced > Global Configuration.



1.5 cm

1. Admin Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다

   ISDP 서비스의 활성화 여부를 지정합니다. 기본값은 Enable입니다.
2. Timer 필드에서 새 ISDP 패킷 전송 사이의 시간 간격을 지정합니다.

   범위는 5~254초입니다. 기본값은 30초입니다.
3. Hold Time 필드에서 스위치가 전송하는 ISDP 패킷의 보류 시간을 지정합니다.

   보류 시간은 수신 장치가 ISDP 패킷을 삭제하기 전에 전송된 정보를 저장해야 하는 기간을 지정합니다. 범위는 10~255초입니다. 기본값은 180초입니다.
4. Version 2 Advertisements의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 장치에서 ISDP 버전 2 패킷 전송을 활성화하거나 비활성화합니다. 기본값은 Enable입니다.

다음 표에서는 ISDP 고급 전역 구성 필드에 대해 설명합니다.

Table 52. ISDP 고급 전역 구성

필드	설명
Neighbors table last time changed	Neighbors 테이블이 마지막으로 변경된 시간을 표시합니다.
Device ID	이 스위치의 장치 ID입니다.
Device ID Format Capability	장치 ID 형식 기능입니다.
Device ID Format	장치 ID 형식입니다.

ISDP 인터페이스 구성

➢ **ISDP 인터페이스를 구성하려면:**

System > ISDP > Advanced > Interface Configuration.

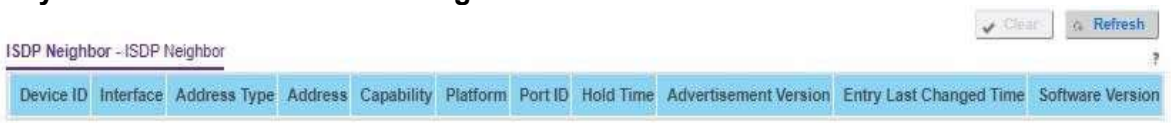
1.5 cm

1. Port를 사용하여 관리 모드가 구성된 포트를 선택합니다.
2. Admin 모드를 사용하여 포트에서 ISDP를 활성화하거나 비활성화합니다. 기본값은 Enable입니다.

ISDP 이웃 보기

➢ **ISDP 이웃을 보려면:**

System > ISDP > Advanced > Neighbor.



다음 표에서는 ISDP 이웃 필드에 대해 설명합니다.

Table 53. ISDP 이웃

필드	설명
Device ID	ISDP 이웃의 장치 ID입니다.
Interface	인접 항목이 검색되는 인터페이스입니다.
Address	이웃의 주소입니다.
Capability	이웃의 능력. 다음이 지원됩니다: • Router • Trans Bridge • Source Route • Switch • Host • IGMP • Repeater

1.5 cm

Platform	이웃의 모델 유형입니다. (0~32)
Port ID	이웃의 포트 ID입니다.
Hold Time	이웃이 전송하는 ISDP 패킷의 보류 시간입니다.
Advertisement Version	이웃에서 보내는 ISDP 버전입니다.
Entry Last Changed Time	마지막 항목 이후의 시간이 변경되었습니다.
Software Version	이웃의 소프트웨어 버전.

ISDP 통계 보기

- **ISDP 통계를 보려면:**

  System > ISDP > Advanced > Statistics.

  다음 표에서는 ISDP 통계 필드에 대해 설명합니다.

Table 54. ISDP 통계

필드	설명
ISDP Packets Received	ISDPv1 및 ISDPv2 패킷을 포함하여 수신된 ISDP 패킷입니다.
ISDP Packets Transmitted	ISDPv1 및 ISDPv2 패킷을 포함하여 전송되는 ISDP 패킷입니다.
ISDPv1 Packets Received	ISDPv1 패킷이 수신되었습니다.
ISDPv1 Packets Transmitted	ISDPv1 패킷이 전송되었습니다.
ISDPv2 Packets Received	ISDPv2 패킷이 수신되었습니다.
ISDPv2 Packets Transmitted	ISDPv2 패킷이 전송되었습니다.
ISDP Bad Header	ISDP 불량 패킷이 수신되었습니다.
ISDP Checksum Error	체크섬 오류의 번호입니다.
ISDP Transmission Failure	전송 실패 횟수입니다.
ISDP Invalid Format	수신된 잘못된 형식의 ISDP 패킷 수입니다.
ISDP Table Full	ISDP 테이블의 테이블 크기입니다.
ISDP Ip Address Table Full	ISDP IP 주소 테이블의 테이블 크기입니다.

1.5 cm

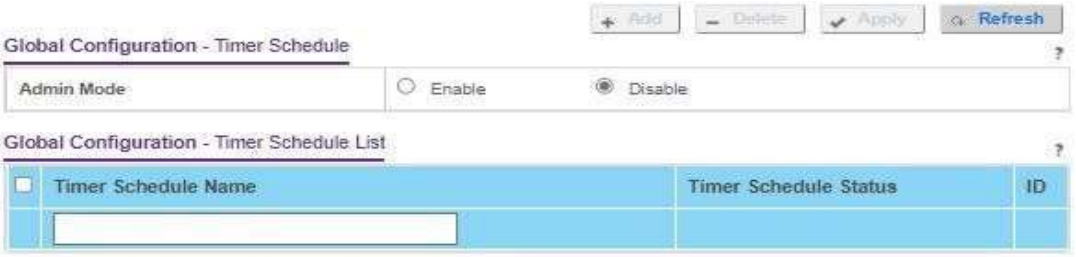
타이머 일정

글로벌 타이머 설정과 타이머 일정을 구성할 수 있습니다.

글로벌 타이머 설정 구성

➢ **글로벌 타이머 설정을 구성하려면:**

System > Timer Schedule > Basic > Global Configuration.



1. Timer Schedule Name을 사용하여 타이머 일정 이름을 지정합니다.
2. Add 버튼을 클릭합니다.

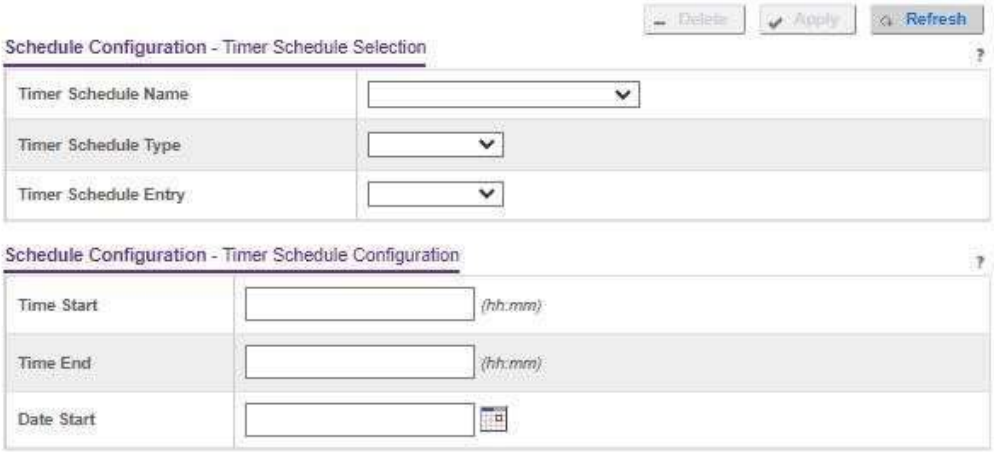
   타이머가 추가됩니다. 구성 변경 사항은 즉시 적용됩니다.
3. 선택한 타이머 일정을 삭제하려면 Delete 버튼을 클릭하세요.

   구성 변경 사항은 즉시 적용됩니다.

Configure the Timer Schedule

➢ **타이머 일정을 구성하려면:**

System > Services > Timer Schedule > Advanced > Schedule Configuration.



1.5 cm

1. Timer Schedule Name 목록에서 타이머 스케줄을 선택하세요.
2. Time Schedule Type에서 Absolute 또는 Periodic을 선택합니다.
3. Timer Schedule Entry 목록에서 구성하거나 추가할 타이머 일정 항목의 개수를 선택하세요.

   항목을 추가하는 경우 new를 선택합니다.
4. Time Start(시간 시작) 필드에 스케줄 작업이 시작되는 시간을 HH:MM 형식으로 입력합니다.

   이 필드는 필수입니다. 시간을 지정하지 않으면 일정이 실행되지 않습니다.
5. Time End 필드에 스케줄 작업이 종료되는 시간을 HH:MM 형식으로 입력합니다.
6. Date Start를 이용하여 스케줄 시작일을 설정하세요.

   날짜를 지정하지 않으면 일정이 즉시 실행되기 시작합니다.
7. Date Stop를 이용하여 스케줄 종료 날짜를 설정하세요.

   종료 날짜 없음을 선택하면 스케줄이 무기한 작동됩니다.
8. Recurrence Pattern을 사용하여 이벤트가 반복되는 기간을 표시합니다.

   반복이 필요하지 않은 경우(타이머 일정은 한 번만 트리거되어야 함) 날짜 중지를 날짜 시작과 동일하게 설정합니다. 가능한 반복 값은 다음과 같습니다.

   - **Daily**. 타이머 일정은 매일 반복됩니다.

     Daily mode. Every WeekDay를 선택하면 월요일부터 금요일까지 매일 스케줄이 실행됩니다. 매일(Every Day)을 선택하면 일정이 정의된 일수마다 트리거된다는 의미입니다. 일수를 지정하지 않으면 매일 스케줄이 트리거됩니다.
   - **Weekly**. 타이머 일정은 매주 반복되도록 작동합니다.

     Every Week(s). 일정이 트리거되는 주 수를 정의합니다. 주 수를 지정하지 않으면 매주 일정이 트리거됩니다.

     WeekDay. 스케줄이 운영되는 요일을 지정합니다.
   - **Monthly**. 타이머 일정은 월별 반복으로 작동합니다.

     Monthly mode. 스케줄이 실행되는 달의 날짜를 표시합니다. 매월 필드는 정의된 개월 수마다 일정이 트리거된다는 의미입니다.
9. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

스위칭 정보 구성 3

이 장에서는 다음 주제를 다룹니다:

- *포트 설정*
- *링크 집합 그룹 설정*
- *VLAN 구성*
- *MAC 주소 테이블 설정*
- *스패닝 트리 프로토콜 설정*
- *멀티캐스트 설정*
- *MVR 구성*
- *자동 VoIP 설정*

포트 설정

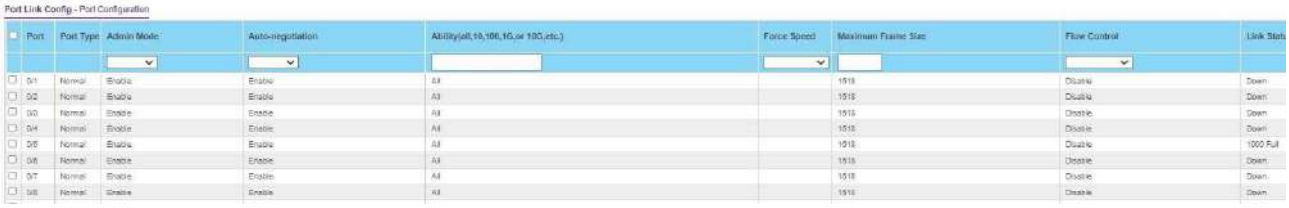
스위치에서 사용 가능한 포트에 대한 물리적 포트 정보를 보고 모니터링할 수 있습니다.

포트 설정 구성

스위치의 물리적 인터페이스를 구성할 수 있습니다.

➢ **포트 설정을 구성하려면:**

Switching > Ports > Port Configuration.



1. Port를 사용하여 인터페이스를 선택합니다.
2. STP 모드를 사용하여 포트 또는 LAG에 대한 스패닝 트리 프로토콜 관리 모드를 선택합니다.

   가능한 값은 다음과 같습니다.

   - **Enable**. 이 포트에 대해 스패닝 트리 프로토콜을 활성화하려면 이를 선택합니다.
   - **Disable.** 이 포트에 대한 스패닝 트리 프로토콜을 비활성화하려면 이를 선택합니다.

   기본값은 Enable입니다.
3. Admin Mode 목록에서 Enable 또는 Disable를 선택합니다.

   포트 제어 관리 모드를 설정합니다. 포트가 네트워크에 참여하려면 Enable를 선택해야 합니다. 공장 기본값은 Enable입니다.
4. LACP Mode 목록에서 Enable 또는 Disable를 선택합니다.

   이는 링크 집계 제어 프로토콜 관리 모드를 선택합니다. 포트가 링크 집계에 참여하려면 모드를 Enable해야 합니다. 공장 기본값은 Enable입니다.
5. Auto-negotiation 목록에서 Enable 또는 Disable를 선택합니다.

   이 포트에 대한 자동 협상 모드를 지정합니다. 기본값은 Enable입니다.

1.5 cm

Note: 자동 협상 모드를 변경한 후 새 설정이 적용되는 동안 몇 초 동안 스위치에 액세스하지 못할 수 있습니다.

6. Speed 목록에서 선택한 포트의 속도 값을 선택합니다.

   가능한 필드 값은 다음과 같습니다.

   - **Auto**. 모든 속도가 지원됩니다.
   - **100**. 100 Mbits/second
   - **10G**. 10 Gbits/second.

   다양한 속도 값을 설정하기 위한 구분 문자는 쉼표(,), 마침표(.) 및 공백( )입니다. 자동 협상 속도를 설정하려면 자동 협상 모드를 Enable로 설정해야 합니다. 기본값은 Auto입니다.

   Note: 속도 값을 변경한 후 새 설정이 적용되는 동안 몇 초 동안 스위치에 액세스하지 못할 수 있습니다.

7. Duplex 모드 목록에서 선택한 포트에 대한 이중 모드를 선택합니다.

   가능한 값은 다음과 같습니다.

   - **Auto**. 자동 협상 프로세스에 의해 속도가 설정됨을 나타냅니다.
   - **Full**. 인터페이스가 장치 간 양방향 전송을 동시에 지원함을 나타냅니다.
   - **Half**. 인터페이스가 한 번에 한 방향으로만 장치 간 전송을 지원함을 나타냅니다.

   기본값은 Auto입니다.

   Note: 이중 모드를 변경한 후 새 설정이 적용되는 동안 몇 초 동안 스위치에 액세스하지 못할 수 있습니다.

8. Link Trap object를 사용하여 링크 상태가 변경될 때 트랩을 보낼지 여부를 결정합니다.

   공장 기본값은 Enable되어 있습니다.

9. Frame Size를 사용하여 이더넷 헤더, CRC 및 페이로드를 포함하여 인터페이스가 지원하거나 사용하도록 구성된 최대 이더넷 프레임 크기를 지정합니다.

   범위는 1518~12288입니다. 기본 최대 프레임 크기는 1518입니다.

10. Debounce Time을 사용하여 100~5000 범위에서 포트 디바운싱에 대한 타이머 값을 100밀리초(msec) 단위로 지정합니다.

    기본 디바운스 타이머 값은 0입니다. 이는 디바운스가 비활성화되었음을 의미합니다.

1.5 cm

11. Flow Control 목록에서 IEEE 802.3 흐름 제어 Enable 또는 Disable를 선택합니다.

    기본값은 Disable입니다. 포트 버퍼가 가득 차면 스위치는 일시 중지 프레임을 보내지 않습니다. 흐름 제어는 포트가 전환되는 프레임 수를 따라잡을 수 없을 때 데이터 손실을 방지하는 데 도움이 됩니다. 활성화되면 포트의 패킷이 사용하는 메모리 양이 사전 구성된 임계값을 초과하고 파트너 장치의 일시 중지 요청에 응답하는 경우 스위치는 일시 중지 프레임을 보내 포트의 트래픽을 중지할 수 있습니다. 일시 중지된 포트는 일시 중지 프레임에 지정된 시간 동안 패킷을 전달하지 않습니다. 일시 중지 프레임 시간이 경과하거나 사용률이 지정된 낮은 임계값으로 돌아가면 스위치는 포트가 프레임을 다시 전송할 수 있도록 합니다. LAG 인터페이스의 경우 흐름 제어를 적용할 수 없으므로 흐름 제어 모드가 공백으로 표시됩니다.

12. Apply 버튼을 클릭합니다

    스위치는 입력한 값으로 업데이트됩니다. 스위치가 전원을 껐다 켜는 동안 새 값을 유지하려면 구성을 저장해야 합니다.

다음 표에서는 표시되는 구성할 수 없는 데이터에 대해 설명합니다.

Table 107. 포트 설정

필드	설명
Media Type	미디어 유형입니다.
Port Type	일반 포트의 경우 이 필드는 Normal입니다. 그렇지 않은 경우 가능한 값은 다음과 같습니다. • **Mirrored**. 포트는 모든 트래픽이 프로브 포트에 복사되는 미러링된 포트입니다. • **Probe**. 이 포트를 사용하여 미러링된 포트를 모니터링합니다. • **Trunk Member**. 포트가 링크 집계 트렁크의 구성원입니다. 자세한 내용은 LAG 화면을 참조하세요.
Admin Status	포트의 관리 모드가 D-Disable인 경우 이 필드는 이유를 나타냅니다. 가능한 이유는 다음과 같습니다. • **STP**. 스패닝 트리 프로토콜 위반. • **UDLD**. UDLD 프로토콜 위반. • **XCEIVER**. 지원되지 않는 SFP/SFP+가 삽입되었습니다.
Physical Status	포트 속도와 이중 모드를 나타냅니다.
Link Status	링크가 작동 중인지 작동 중지되었는지 여부를 나타냅니다.
ifIndex	이 포트와 연관된 인터페이스 테이블 항목의 ifIndex입니다.

포트 설명 구성

➢ **장치의 모든 포트에 대한 설명을 구성하고 표시하려면:**

Switching > **Ports** > **Port Description**.

1. 포트 설명을 사용하여 포트에 연결할 설명 문자열을 입력합니다. 길이는 최대 64자까지 가능합니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 108. 포트 설명

필드	설명
Port	데이터를 표시하거나 구성할 인터페이스를 선택합니다.
MAC Address	지정된 인터페이스의 물리적 주소입니다.
PortList Bit Offset	MIB 객체 유형 PortList를 사용하여 SNMP에서 관리할 때 포트에 해당하는 비트 오프셋 값입니다.
ifIndex	포트와 연결된 인터페이스 인덱스입니다.

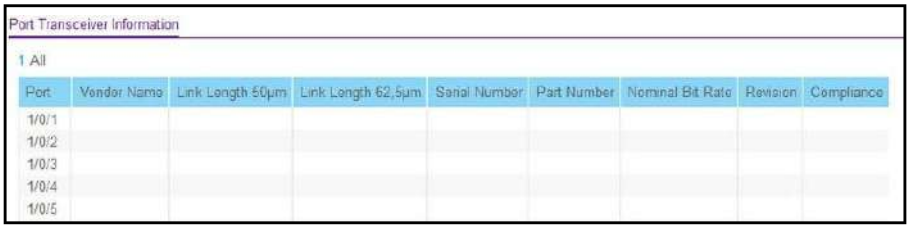
포트 트랜시버 정보 보기

상자에서 모든 광섬유 포트에 대한 트랜시버 정보를 볼 수 있습니다.

➢ **포트 트랜시버 정보를 보려면:**

1.5 cm

Switching > **Ports** > **Port Transceiver**.



1. 선택한 장치의 물리적 포트를 표시하려면 Unit ID를 선택하고, 모든 장치의 물리적 포트를 표시하려면 All를 선택합니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음은 표시되는 구성할 수 없는 데이터에 대해 설명합니다.

Table 109. 포트 트랜시버

필드	설명
Port	데이터가 표시될 인터페이스입니다.
Vendor Name	SFP의 공급업체 이름입니다.
Link Length 50 µm	50µm 광섬유에 지원되는 링크 길이입니다.
Link Length 62, 5 µm	62, 5µm 광섬유에 지원되는 링크 길이입니다.
Serial Number	SFP의 일련 번호입니다.
Part Number	SFP의 부품 번호입니다.
Nominal Bit Rate	SFP의 공칭 신호 속도입니다.
Revision	SFP의 공급업체 개정판입니다.
Compliance	SFP 준수.

PoE

PoE 설정 구성

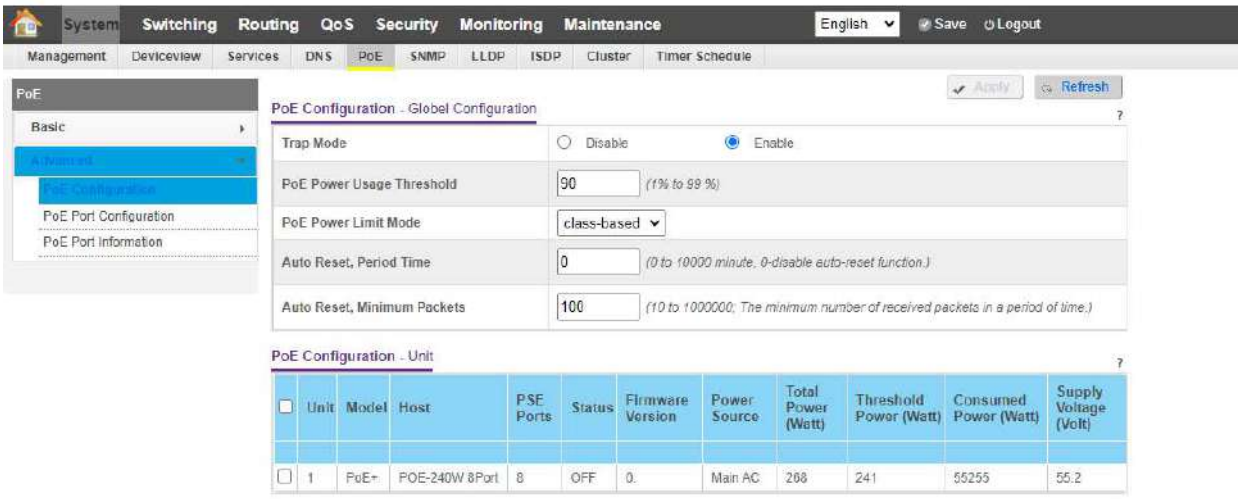
- **PoE 구성 웹 페이지를 표시하려면:**

  System>PoE>Advaced> PoE Configuration

1.5 cm

이 페이지는 PoE 전력 사용량 임계값, PoE 전력 제한 모드, 자동 재설정, 기간 시간,

자동 재설정, 최소 패킷을 구성을 보여줍니다.

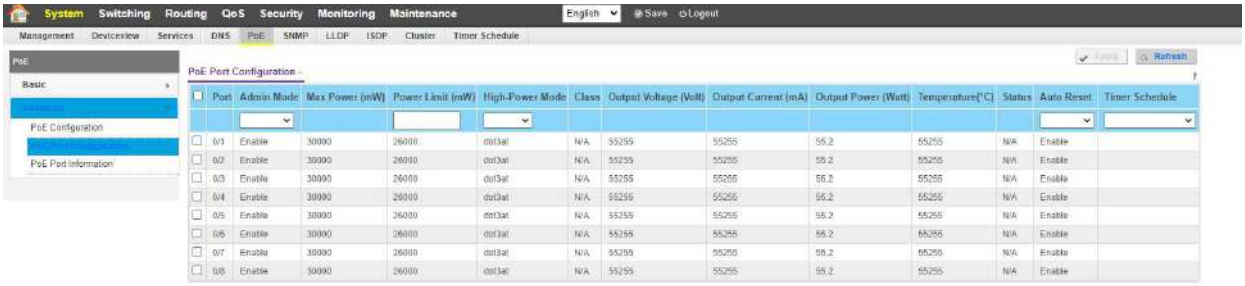


PoE 포트 구성

- **PoE 포트 구성 웹 페이지를 표시하려면:**

System>PoE>Advaced> PoE Port Configuration

이 페이지에는 관리 모드, 전력 제한(mW), 고전력 모드, 자동 재설정이 표시됩니다.



PoE 포트 정보

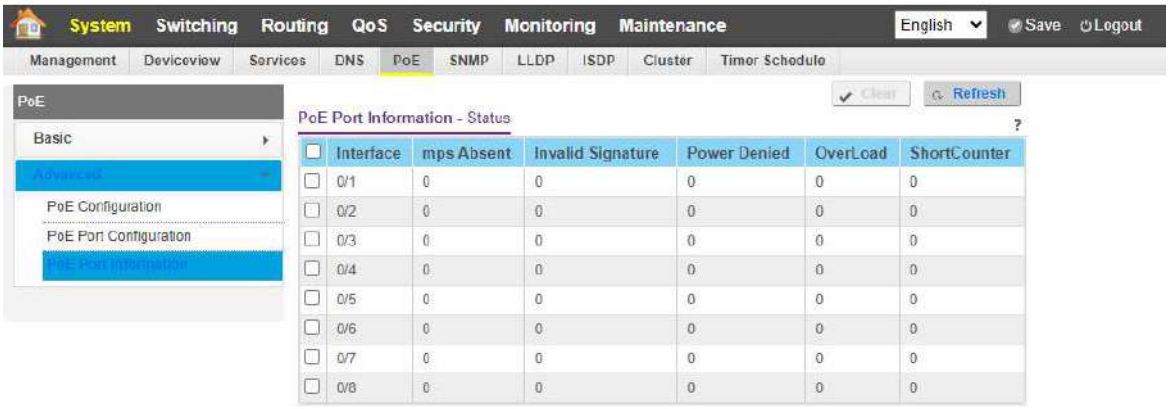
- **To display PoE port information web page:**

System>PoE>Advaced>PoE Port Information

이 페이지에는 인터페이스, mps 부재, 잘못된 서명, 전원 거부, 과부하, ShortCounter가

표시됩니다.

1.5 cm



링크 집계 그룹

포트 채널이라고도 하는 LAG(링크 집계 그룹)를 사용하면 여러 전이중 이더넷 링크를 단일 논리 링크로 결합할 수 있습니다. 네트워크 장치는 집합을 단일 링크인 것처럼 처리하여 내결함성을 높이고 로드 공유를 제공합니다. LAG를 생성한 후 LAG VLAN 멤버십을 할당합니다. 기본적으로 LAG는 관리 VLAN의 구성원이 됩니다.

LAG 인터페이스는 정적이거나 동적일 수 있지만 둘 다일 수는 없습니다. LAG의 모든 구성원은 동일한 프로토콜에 참여해야 합니다. 정적 포트-채널 인터페이스에서는 파트너 시스템이 해당 멤버 포트를 집계할 수 있도록 요구하지 않습니다.

정적 LAG가 지원됩니다. 포트가 LAG에 정적 구성원으로 추가되면 LACPDU를 전송하거나 수신하지 않습니다.

LAG 설정 구성

함께 집계할 하나 이상의 전이중 이더넷 링크를 그룹화하여 포트 채널이라고도 하는 링크 집계 그룹을 형성할 수 있습니다. 스위치는 LAG를 단일 링크인 것처럼 처리합니다.

- **LAG 설정을 구성하려면:**

  Switching > **LAG** > **LAG Configuration**.

1.5 cm

1. LAG Name을 사용하여 LAG에 할당할 이름을 입력합니다.

   최대 15자의 영숫자 문자열을 입력할 수 있습니다. LAG를 생성하려면 유효한 이름을 지정해야 합니다.

2. Admin Mode를 사용하여 Enable 또는 Disable를 선택합니다.

   LAG가 비활성화되면 트래픽 흐름과 LACPDU가 삭제되지 않지만 LAG를 구성하는 링크는 해제되지 않습니다. 공장 기본값은 Enable입니다.

3. Hash Mode를 사용하여 LAG(포트 채널)에 사용되는 load-balancing Mode를 선택합니다.

   특정 패킷을 전송할 채널의 링크 중 하나를 선택하여 포트 채널(LAG)에서 트래픽의 균형이 조정됩니다. 링크는 패킷의 선택된 필드에서 바이너리 패턴을 생성하고 해당 패턴을 특정 링크와 연결하여 선택됩니다.

   - **Src MAC, VLAN, EType, incoming port**. 패킷과 연결된 소스 MAC, VLAN, EtherType 및 수신 포트입니다.
   - **Dest MAC, VLAN, EType, incoming port**. 패킷과 연결된 대상 MAC, VLAN, EtherType 및 수신 포트입니다.
   - **Src/Dest MAC, VLAN, EType, incoming port**. Src/Dest MAC, VLAN, EtherType 및 패킷과 관련된 수신 포트입니다. Incoming port가 기본값입니다.
   - **Src IP** and **Src TCP/UDP Port** fields. 패킷의 소스 IP 및 소스 TCP/UDP 필드입니다.
   - **Dest IP** and **Dest TCP/UDP Port** fields. 패킷의 대상 IP 및 대상 TCP/UDP 포트 필드입니다.
   - **Src/Dest IP** and **TCP/UDP Port Fields**. 패킷의 소스/대상 IP 및 소스/대상 TCP/UDP 포트 필드입니다.
   - **Enhanced hashing Mode**. LAG의 포트 수를 기반으로 하는 MODULO-N 작동, 일반 해시 알고리즘을 사용하는 비유니캐스트 트래픽 및 유니캐스트 트래픽 해싱, 뛰어난 로드 밸런싱 성능 및 패킷 유형에 따른 패킷 속성 선택이 특징입니다.
     - L2 패킷의 경우 소스 및 대상 MAC 주소가 해시 계산에 사용됩니다.

1.5 cm

- L3 패킷의 경우 소스 IP, 대상 IP 주소, TCP/UDP 포트가 사용됩니다.

4. STP Mode를 사용하여 LAG와 관련된 스패닝 트리 프로토콜 관리 모드를 활성화하거나 비활성화합니다.

   가능한 값은 다음과 같습니다.

   - **Disable**. 이 LAG에서는 스패닝 트리가 비활성화되었습니다.
   - **Enable**. 이 LAG에는 스패닝 트리가 활성화되어 있습니다.

     Enable가 기본값입니다.

5. Static Mode를 사용하여 Enable 또는 Disable를 선택합니다.

   LAG가 활성화되면 수신된 LACPDU를 전송하거나 처리하지 않습니다. 즉, 멤버 포트는 LACPDU를 전송하지 않으며 수신할 수 있는 모든 LACPDU는 삭제됩니다. 공장 기본값은 Disable입니다.

6. Link Trap을 사용하여 링크 상태가 변경될 때 트랩을 보낼지 여부를 지정합니다.

   공장 기본값은 트랩이 전송되는 Enable입니다.

7. Local Preference Mode를 사용하여 LAG 인터페이스의 로컬 기본 설정 모드를 Enable 또는 Disable합니다.

   기본값은 Disable입니다.

8. 현재 선택된 구성된 LAG를 제거하려면 Delete 버튼을 클릭합니다.

   이 LAG의 구성원이었던 모든 포트는 LAG에서 제거되고 기본 VLAN에 포함됩니다.

9. Apply 버튼을 클릭합니다

   스위치는 입력한 값으로 업데이트됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 110. LAG 구성

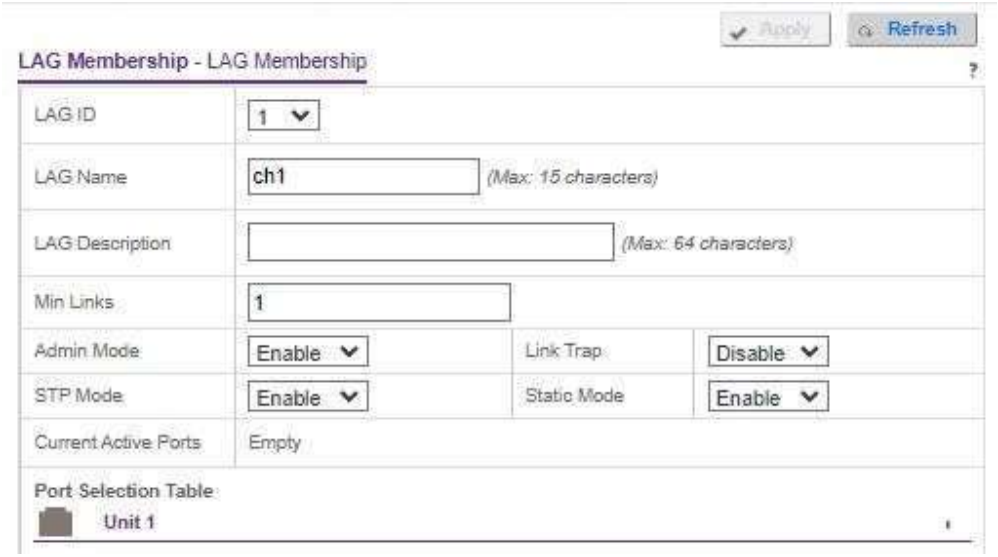
필드	설명
LAG Description	LAG에 첨부할 설명 문자열을 입력합니다. 길이는 최대 64자까지 가능합니다.
LAG ID	LAG 식별.
LAG State	링크가 작동 중인지 작동 중지되었는지 여부를 나타냅니다.
Configured Ports	이 포트 채널의 구성원인 포트를 나타냅니다.
Active Ports	포트 채널에 적극적으로 참여하고 있는 포트를 나타냅니다.

LAG 멤버십 구성

함께 집계할 두 개 이상의 전이중 이더넷 링크를 선택하여 포트 채널이라고도 하는 LAG(링크 집계 그룹)를 형성할 수 있습니다. 스위치는 포트 채널을 단일 링크인 것처럼 처리할 수 있습니다.

➢ **LAG 멤버십을 구성하려면:**

Switching > LAG > LAG Membership.



2. LAG ID를 사용하여 LAG ID를 선택합니다.
3. LAG Name을 사용하여 LAG에 할당할 이름을 입력합니다.

   최대 15자의 영숫자 문자열을 입력할 수 있습니다. LAG를 생성하려면 유효한 이름을 지정해야 합니다.
4. LAG Description을 사용하여 LAG에 첨부할 설명 문자열을 입력합니다.

   길이는 최대 64자까지 가능합니다.
5. Admin Mode를 사용하여 Enable 또는 Disable를 선택합니다.

   LAG가 비활성화되면 트래픽 흐름과 LACPDU가 삭제되지 않지만 LAG를 구성하는 링크는 해제되지 않습니다. 공장 기본값은 Enable입니다.
6. 링크 트랩을 사용하여 링크 상태가 변경될 때 트랩을 보낼지 여부를 지정합니다.

   공장 기본값은 트랩이 전송되는 Enable입니다.
7. STP Mode를 사용하여 LAG와 관련된 스패닝 트리 프로토콜 관리 모드를 활성화하거나 비활성화합니다.

1.5 cm

가능한 값은 다음과 같습니다.

- **Disable**. 이 LAG에서는 스패닝 트리가 비활성화되었습니다.
- **Enable**. 이 LAG에는 스패닝 트리가 활성화되어 있습니다.

  활성화가 기본값입니다.

8. Static Mode를 사용하여 Enable 또는 Disable를 선택합니다.

   LAG가 활성화되면 수신된 LACPDU를 전송하거나 처리하지 않습니다. 즉, 멤버 포트는 LACPDU를 전송하지 않으며 수신할 수 있는 모든 LACPDU는 삭제됩니다. 공장 기본값은 Disable입니다.

9. Hash Mode를 사용하여 LAG(포트 채널)에 사용되는 load-balancing Mode를 선택합니다.

   특정 패킷을 전송할 채널의 링크 중 하나를 선택하여 포트 채널(LAG)에서 트래픽의 균형이 조정됩니다. 링크는 패킷의 선택된 필드에서 바이너리 패턴을 생성하고 해당 패턴을 특정 링크와 연결하여 선택됩니다.

   - **Src MAC,VLAN,EType,incoming port**. 패킷과 연결된 소스 MAC, VLAN, EtherType 및 수신 포트입니다.
   - **Dest MAC,VLAN,EType,incoming port**. 패킷과 연결된 대상 MAC, VLAN, EtherType 및 수신 포트입니다.
   - **Src/Dest MAC,VLAN,EType,incoming port**. 소스/대상 MAC, VLAN, EtherType 및 패킷과 관련된 수신 포트입니다. 이 옵션이 기본값입니다.
   - **Src IP** and **Src TCP/UDP Port** fields. 패킷의 소스 IP 및 소스 TCP/UDP 필드입니다.
   - **Dest IP** and **Dest TCP/UDP Port** fields. 패킷의 대상 IP 및 대상 TCP/UDP 포트 필드입니다.
   - **Src/Dest IP** and **TCP/UDP Port** fields. 패킷의 소스/대상 IP 및 소스/대상 TCP/UDP 포트 필드입니다.
   - **Enhanced Hashing Mode**. LAG의 포트 수를 기반으로 하는 MODULO-N 작동, 일반 해시 알고리즘을 사용하는 비유니캐스트 트래픽 및 유니캐스트 트래픽 해싱, 뛰어난 로드 밸런싱 성능, 패킷 유형에 따른 패킷 속성 선택 기능이 있습니다.
     - L2 패킷의 경우 소스 및 대상 MAC 주소가 해시 계산에 사용됩니다.
     - L3 패킷의 경우 소스 IP, 대상 IP 주소, TCP/UDP 포트가 사용됩니다.

10. Port Selection Table을 사용하여 포트를 LAG의 구성원으로 선택합니다.

VLAN 구성

레이어 2 스위치에 VLAN(가상 LAN) 지원을 추가하면 브리징과 라우팅의 이점 중 일부를 얻을 수 있습니다. 브리지와 마찬가지로 VLAN 스위치는 빠른 레이어 2 헤더를 기반으로 트래픽을 전달하며, 라우터와 마찬가지로 네트워크를 논리적 세그먼트로 분할하여 멀티캐스트 트래픽에 대한 더 나은 관리, 보안 및 관리를 제공합니다.

기본적으로 스위치의 모든 포트는 동일한 브로드캐스트 도메인에 있습니다. VLAN은 동일한 스위치의 포트를 별도의 브로드캐스트 도메인으로 전기적으로 분리하므로 브로드캐스트 패킷이 단일 스위치의 모든 포트로 전송되지 않습니다. VLAN을 사용하면 사용자를 물리적 위치가 아닌 논리적 기능별로 그룹화할 수 있습니다.

네트워크의 각 VLAN에는 VLAN에서 전송되는 패킷의 레이어 2 헤더에 있는 IEEE 802.1Q 태그에 나타나는 관련 VLAN ID가 할당됩니다. 엔드 스테이션은 태그 또는 태그의 VLAN 부분을 생략할 수 있습니다. 이 경우 패킷을 수신하는 첫 번째 스위치 포트는 패킷을 거부하거나 기본 VLAN ID를 사용하여 태그를 삽입할 수 있습니다. 특정 포트는 둘 이상의 VLAN에 대한 트래픽을 처리할 수 있지만 기본 VLAN ID는 하나만 지원할 수 있습니다.

VLAN 멤버십 테이블에 저장된 VLAN 그룹을 정의할 수 있습니다. 제품군의 각 스위치는 최대 1024개의 VLAN을 지원합니다. VLAN 1은 기본적으로 생성되며 모든 포트가 구성원인 기본 VLAN입니다.

기본 VLAN 설정 구성

내부 VLAN은 포트 기반 라우팅 인터페이스에 의해 예약되어 있으며 최종 사용자에게는 보이지 않습니다. 이러한 내부 VLAN은 포트 기반 라우팅 인터페이스에 의해 할당되면 더 이상 사용할 수 없습니다.

라우팅 VLAN 인터페이스에 할당됩니다.

➢ **내부 VLAN 설정을 구성하려면:**

Switching > VLAN > Basic > VLAN Configuration.

1. VLAN 설정을 기본값으로 재설정하려면 구성 재설정 check box을 선택합니다.

   공장 기본값은 다음과 같습니다.

   - 모든 포트는 기본 VLAN 1에 할당됩니다.
   - 모든 포트는 PVID 1로 구성됩니다.
   - 모든 포트는 AdmitAll Frames의 허용 가능한 프레임 유형 값으로 구성됩니다.

1.5 cm

- 모든 포트는 수신 필터링이 비활성화된 상태로 구성됩니다.
- 모든 포트는 태그가 지정되지 않은 프레임만 전송하도록 구성됩니다.
- 모든 포트에서 GVRP가 비활성화되고 모든 동적 항목이 지워집니다.

기본 VLAN을 제외한 모든 VLAN이 삭제됩니다.

2. 내부 VLAN 설정을 지정합니다.

   내부 VLAN 구성 섹션에는 내부 VLAN의 할당 기준과 할당 모드가 표시됩니다.

   a. Internal VLAN Allocation Base을 사용하여 라우팅 인터페이스에 대한 VLAN 할당 기준을 지정합니다.

   내부 VLAN의 기본 기본 범위는 1~4093입니다.

   b. Internal VLAN Allocation Policy의 Ascending 또는 Descending 라디오 버튼을 선택합니다. 내부 VLAN 할당에 대한 정책을 지정합니다.

3. VLAN ID를 사용하여 새 VLAN에 대한 VLAN 식별자를 지정합니다.
   VLAN ID의 범위는 1~4093입니다.

4. VLAN Name (선택 사항) 필드를 사용하여 VLAN의 이름을 지정합니다.

   VLAN 이름은 공백을 포함하여 최대 32자의 영숫자 문자일 수 있습니다. 기본값은 공백입니다. VLAN ID 1은 항상 Default라는 이름을 사용합니다.

5. VLAN Type필드는 구성 중인 VLAN의 유형을 식별합니다.

   기본 VLAN(VLAN ID = 1)의 유형은 변경할 수 없습니다. 항상 기본 유형입니다. 이 화면을 사용하여 VLAN을 생성하면 해당 유형은 항상 정적입니다. GVRP 등록으로 생성된 VLAN은 초기에 Dynamic 유형을 사용합니다. 동적 VLAN을 구성할 때 해당 유형을 Static으로 변경할 수 있습니다.

6. Add 버튼을 클릭합니다

   VLAN이 스위치에 추가됩니다.

7. 스위치에서 선택한 VLAN을 삭제하려면 Delete 버튼 을 클릭합니다.

8. Apply 버튼을 클릭합니다

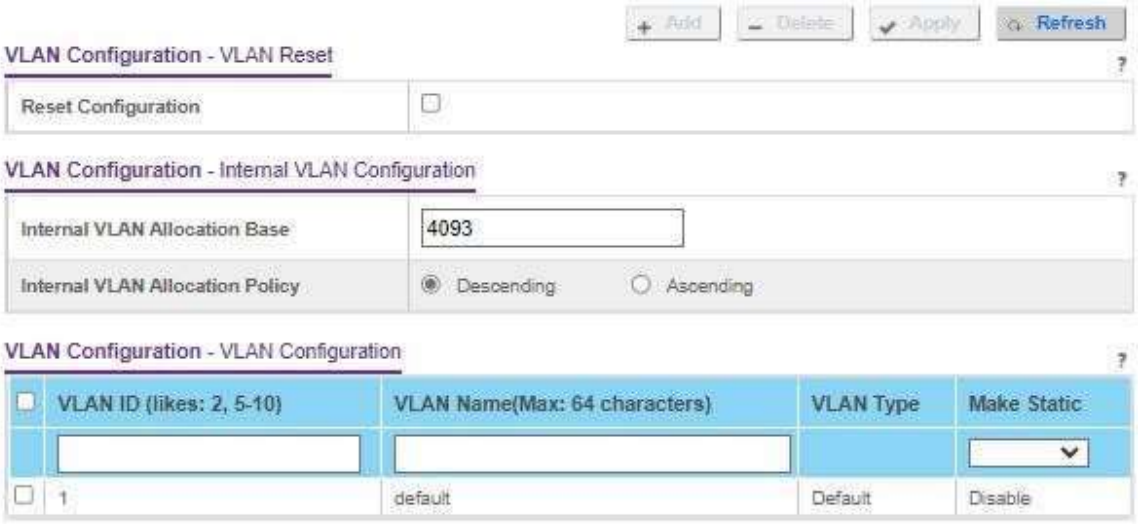
   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

고급 VLAN 구성

1.5 cm

➢ **고급 VLAN을 구성하려면:**

Switching > **VLAN** > **Advanced** > **VLAN Configuration**.



1. **Reset Configuration** - 이 버튼을 선택하고 다음 화면에서 선택을 확인하면 모든 VLAN 구성 매개변수가 공장 기본값으로 재설정됩니다.

   또한 기본 VLAN을 제외한 모든 VLAN이 삭제됩니다. 공장 기본값은 다음과 같습니다.

   - 모든 포트는 기본 VLAN 1에 할당됩니다.
   - 모든 포트는 PVID 1로 구성됩니다.
   - 모든 포트는 AdmitAll Frames의 허용 가능한 프레임 유형 값으로 구성됩니다.
   - 모든 포트는 수신 필터링이 비활성화된 상태로 구성됩니다.
   - 모든 포트는 태그가 지정되지 않은 프레임만 전송하도록 구성됩니다.
   - 모든 포트에서 GVRP가 비활성화되고 모든 동적 항목이 지워집니다.

내부 VLAN 구성

내부 VLAN 섹션에는 내부 VLAN의 할당 기준과 할당 모드가 표시됩니다. 내부 VLAN은 포트 기반 라우팅 인터페이스에 의해 예약되어 있으며 최종 사용자에게는 보이지 않습니다. 이러한 내부 VLAN은 포트 기반 라우팅 인터페이스에 의해 할당되면 라우팅 VLAN 인터페이스에 할당될 수 없습니다.

➢ **내부 VLAN을 구성하려면:**

Switching > **VLAN** > **Advanced** > **VLAN Configuration**.

1.5 cm

1. Internal VLAN Allocation Base 필드에서 라우팅 인터페이스에 대한 VLAN 할당 기준을 지정합니다.

   1부터 4093까지의 값을 입력할 수 있습니다.

2. Internal VLAN Allocation Policy의 Ascending 또는 Descending 라디오 버튼을 선택합니다.

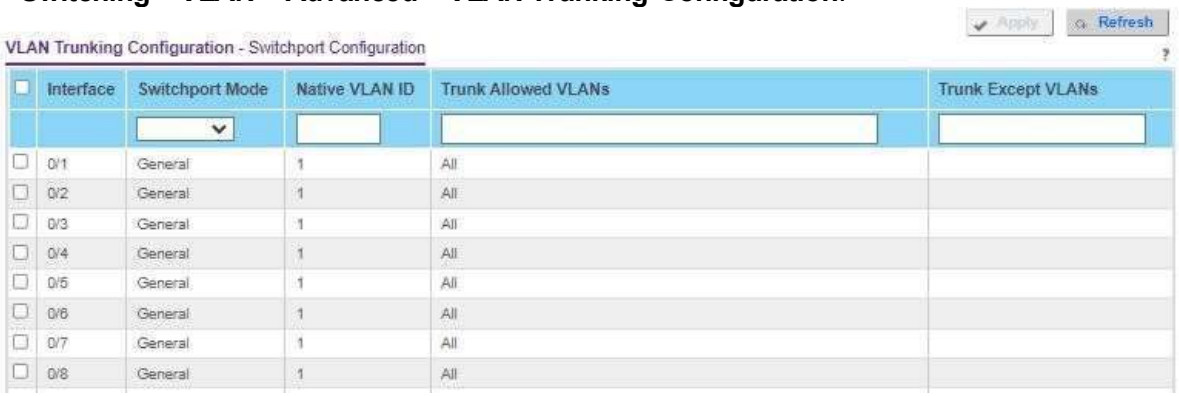
   내부 VLAN 할당에 대한 정책을 지정합니다.

VLAN 트렁킹 구성

인터페이스에서 스위치포트 모드 설정을 구성할 수 있습니다. 스위치 포트 모드는 연결되는 장치 유형에 따라 포트의 목적을 정의하고 이에 따라 포트의 VLAN 구성을 제한합니다. 적절한 스위치포트 모드를 할당하면 VLAN 구성을 단순화하고 오류를 최소화하는 데 도움이 됩니다.

➢ **VLAN 트렁킹을 구성하려면:**

Switching > VLAN > Advanced > VLAN Trunking Configuration.



1. 인터페이스를 선택합니다:
   - 선택한 장치에 대한 물리적 포트 정보를 표시하려면 Unit ID 필드를 선택합니다.
   - LAG만 표시하려면 LAG를 사용합니다.
   - 모든 물리적 포트를 표시하려면 All을 사용합니다.
   - Go To Interface(인터페이스로 이동)를 사용하여 해당 번호를 입력하여 인터페이스를 선택합니다.
   - Interface를 사용하여 데이터가 표시되거나 구성될 인터페이스를 선택합니다.
2. Switchport Mode 목록에서 다음 중 하나를 선택합니다.
   - **Access**. 이 모드는 최종 스테이션이나 최종 사용자에 연결된 포트에 적합합니다.

1.5 cm

액세스 포트는 하나의 VLAN에만 참여합니다. 태그가 있는 패킷과 태그가 없는 패킷을 모두 허용하지만 항상 태그가 없는 패킷을 전송합니다.

- **Trunk**. 이 모드는 다른 스위치에 연결된 포트를 위한 것입니다. 트렁크 포트는 여러 VLAN에 참여할 수 있으며 태그가 지정된 패킷과 태그가 지정되지 않은 패킷을 모두 허용합니다.
- **General**. 이 모드를 사용하면 포트를 사용자 정의 구성할 수 있습니다. 포트 구성 화면의 설정을 사용하여 멤버십, PVID, 태그 지정, 수신 필터 등과 같은 일반 포트 VLAN 속성을 구성합니다. 기본적으로 모든 포트는 처음에 General 모드로 구성됩니다.
- **Host**. 이 모드는 사설 VLAN 구성에 사용됩니다.
- **Promiscuous**. 이 모드는 사설 VLAN 구성에 사용됩니다.

3. 목록에서 선택하여 Access VLAN ID를 구성합니다.

   해당 포트에 대한 액세스 VLAN으로, 포트 스위치포트 모드가 Access인 경우에만 유효합니다.

4. Select from the list to configure the **Native VLAN ID**.

   This is the native VLAN for the port, and is valid only when the port switchport mode is **Trunk**.

5. Trunk Allowed VLAN을 구성합니다.

   이는 트렁크 모드로 구성될 때 포트가 구성원이 될 수 있는 VLAN 세트입니다. 기본적으로 이 목록에는 아직 생성되지 않은 경우에도 가능한 모든 VLAN이 포함됩니다. VLAN ID의 범위는 1~4093입니다. 하이픈(-)을 사용하여 범위를 지정하거나 쉼표(,)를 사용하여 목록에서 VLAN ID를 구분합니다. 공백은 허용되지 않습니다. 0 값은 허용된 VLAN을 지웁니다. All 값은 범위(1~4093)의 모든 VLAN을 설정합니다.

6. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

Native VLAN Tagging 필드에는 Enable 또는 Disable가 표시됩니다.

- VLAN 태그가 활성화된 경우 트렁크 포트가 태그가 지정되지 않은 프레임을 수신하면 VLAN 태그 없이 기본 VLAN에서 해당 프레임을 전달합니다.
- VLAN 태그 지정이 비활성화된 경우 트렁크 포트가 태그 없는 프레임을 수신하면 전달할 때 VLAN 태그에 기본 VLAN ID가 포함됩니다.

1.5 cm

VLAN 멤버십 구성

➢ **VLAN 멤버십을 구성하려면:**

Switching > VLAN > Advanced > VLAN Membership.

1. VLAN ID 목록에서 VLAN ID를 선택합니다.
2. Group Operation 목록에서 모든 포트를 선택하고 구성합니다.
   - **Untag All**. 이 VLAN에 대해 전송된 모든 프레임이 태그 해제된 모든 포트를 선택합니다. 모든 포트는 VLAN에 포함됩니다.
   - **Tag All**. 이 VLAN에 대해 전송된 모든 프레임에 태그가 지정되는 포트를 선택합니다. 모든 포트는 VLAN에 포함됩니다.
   - **Remove All**. GVRP를 통해 이 VLAN에 동적으로 등록할 수 있는 모든 포트입니다. 이 선택은 선택한 VLAN의 모든 포트를 제외합니다.
3. Port 표시에서 포트 번호를 선택하여 이 VLAN에 추가합니다.

   각 포트는 다음 세 가지 모드 중 하나를 사용할 수 있습니다.

   - **T (Tagged)**. 이 VLAN에 대해 전송된 모든 프레임에 태그가 지정되는 포트를 선택합니다. 선택한 포트는 VLAN에 포함됩니다.
   - **U (Untagged)**. 이 VLAN에 대해 전송된 모든 프레임에 태그가 지정되지 않은 포트를 선택합니다. 선택한 포트는 VLAN에 포함됩니다.
   - **BLANK (Autodetect)**. GVRP를 통해 이 VLAN에 동적으로 등록할 수 있는 포트를 선택합니다. 이 선택은 선택한 VLAN에서 포트를 제외합니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 77. 고급 VLAN 멤버십

필드	설명

1.5 cm

VLAN Name	선택한 VLAN의 이름입니다. 공백을 포함하여 최대 32자의 영숫자 문자일 수 있습니다. VLAN ID 1은 항상 Default라는 이름을 사용합니다.
VLAN Type	선택한 VLAN 유형: • **Default** (VLAN ID = 1). 항상 존재합니다. • **Static**. 사용자가 구성한 VLAN. • **Dynamic**. 고정으로 변환하지 않은 GVRP 등록으로 생성된 VLAN이므로 GVRP에서 제거할 수 있습니다.

VLAN 상태 보기

현재 구성된 모든 VLAN의 상태를 볼 수 있습니다.

➢ **VLAN 상태를 보려면:**

Switching > **VLAN** > **Advanced** > **VLAN Status**.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 78. VLAN 상태

필드	설명
VLAN ID	VLAN의 VID(VLAN 식별자)입니다. VLAN ID의 범위는 1~4093입니다.
VLAN Name	VLAN의 이름입니다. VLAN ID 1의 이름은 항상 'Default'입니다.
VLAN Type	VLAN 유형: • **Default** (VLAN ID = 1). 항상 존재합니다. • **Static**. 사용자가 구성한 VLAN. • **Dynamic**. 고정으로 변환하지 않은 GVRP 등록으로 생성된 VLAN이므로 GVRP에서 제거할 수 있습니다.
Routing Interface	VLAN 라우팅이 이 VLAN에 대해 구성된 경우 VLAN과 연결된 인터페이스입니다.
Member Ports	VLAN에 포함된 포트입니다.

포트 PVID 설정 구성

➢ **포트 PVID 설정을 구성하려면:**

Switching > VLAN > Advanced > Port PVID Configuration.

1. 모든 물리적 포트 및 LAG에 대한 정보를 표시하려면 All 버튼을 클릭합니다.
2. Interface를 선택합니다.

   Interface 옆에 있는 Interface check box을 선택합니다. 여러 인터페이스를 선택할 수 있습니다. 모든 인터페이스를 선택하려면 제목 행에서 Interface check box을 선택합니다.
3. PVID 필드에서 이 포트에서 수신된 태그가 지정되지 않았거나 우선 순위가 지정된 프레임에 할당할 VLAN ID를 지정합니다.

   공장 기본값은 1입니다.
4. VLAN Member 필드에서 멤버 포트의 VLAN ID 또는 VLAN 목록을 지정합니다.

   VLAN ID 범위는 1~4093입니다. 공장 기본값은 1입니다. 하이픈(-)을 사용하여 범위를 지정하거나 쉼표(,)를 사용하여 목록에서 VLAN ID를 구분합니다. 공백과 0은 허용되지 않습니다.
5. VLAN Tag 필드에서 태그가 지정된 포트의 VLAN ID 또는 VLAN 목록을 지정합니다.

   VLAN ID 범위는 1~4093입니다. 범위를 지정하려면 하이픈(-)을 사용하고, 목록에서 VLAN ID를 구분하려면 쉼표(,)를 사용하세요. 공백과 0은 허용되지 않습니다. VLAN 태그 구성을 기본값으로 재설정하려면 None 키워드를 사용하십시오. VLAN에 대한 포트 태그 지정은 포트가 이 VLAN의 구성원인 경우에만 설정할 수 있습니다.
6. Acceptable Frame Type 목록에서 이 포트에서 수신할 수 있는 프레임 유형을

지정합니다.

옵션은 VLAN Only 및 Admit All입니다.

- VLAN Only으로 설정된 경우 이 포트에서 수신된 태그가 지정되지 않은 프레임 또는 우선순위 태그가 지정된 프레임이 삭제됩니다.
- Admit All으로 설정하면 이 포트에서 수신된 태그 없는 프레임 또는 우선 태그가 있는 프레임이 허용되고 이 포트에 대한 포트 VLAN ID 값이 할당됩니다. 두 옵션 중 하나를 사용하면 VLAN 태그가 지정된 프레임이 802.1Q VLAN 사양에 따라 전달됩니다.

7. Configured Ingress Filtering 필드에서 Enable 또는 Disable을 선택합니다.
   - 활성화되면 이 포트가 이 프레임과 연결된 VLAN의 구성원이 아닌 경우 프레임이 삭제됩니다. 태그가 지정된 프레임에서 VLAN은 VLAN으로 식별됩니다.

     태그에 ID가 있습니다. 태그가 지정되지 않은 프레임에서 VLAN은 이 프레임을 수신한 포트에 대해 지정된 포트 VLAN ID입니다.
   - 비활성화되면 모든 프레임이 802.1Q VLAN 브리지 사양에 따라 전달됩니다. 공장 기본값은 비활성화되어 있습니다.
8. Port Priority 필드에서 포트에 도착하는 태그가 지정되지 않은 패킷에 할당된 기본 802.1p 우선 순위를 지정합니다.

   0부터 7까지의 숫자를 입력할 수 있습니다.

MAC 기반 VLAN 구성

MAC 기반 VLAN 기능을 사용하면 태그가 지정되지 않은 수신 패킷을 VLAN에 할당하여 패킷의 소스 MAC 주소를 기반으로 트래픽을 분류할 수 있습니다.

MAC-VLAN 테이블의 항목을 구성하여 MAC-VLAN 매핑을 정의합니다. 항목은 소스 MAC 주소와 원하는 VLAN ID를 통해 지정됩니다. MAC-VLAN 구성은 장치의 모든 포트에서 공유됩니다(즉, MAC 주소-VLAN ID 매핑이 포함된 시스템 전체 테이블이 있습니다).

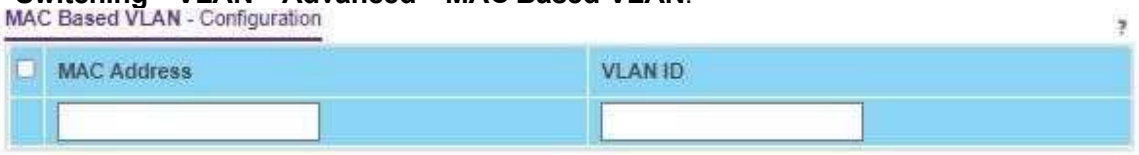
태그가 지정되지 않았거나 우선적으로 태그가 지정된 패킷이 스위치에 도착하고 MAC-VLAN 테이블에 항목이 있으면 패킷의 소스 MAC 주소를 조회합니다. 항목이 발견되면 해당 VLAN ID가 패킷에 할당됩니다. 패킷에 이미 우선순위 태그가 지정되어 있으면 이 값을 유지합니다. 그렇지 않으면 우선순위가 0으로 설정됩니다. 할당된 VLAN ID는 VLAN 테이블에 대해 확인됩니다. VLAN이 유효한 경우 패킷에 대한 수신 처리가 계속됩니다. 그렇지 않으면

1.5 cm

패킷이 삭제됩니다. 이는 사용자가 시스템에서 생성되지 않은 VLAN에 대한 MAC 주소 매핑을 구성할 수 있음을 의미합니다.

➢ **MAC 기반 VLAN을 구성하려면:**

Switching > VLAN > Advanced > MAC Based VLAN.



1. MAC Address 필드에 VLAN ID에 바인딩할 유효한 MAC 주소를 입력합니다.

   이 필드는 MAC 기반 VLAN이 생성된 경우에만 구성할 수 있습니다.

2. VLAN ID 필드에 1~4093 범위의 VLAN ID를 지정합니다.
3. Add 버튼을 클릭합니다.

   MAC 주소가 VLAN 매핑에 추가됩니다.

4. VLAN 매핑에서 MAC 주소를 삭제하려면 Delete 버튼을 클릭합니다.

프로토콜 기반 VLAN 그룹 구성

프로토콜 기반 VLAN을 사용하여 태그가 지정되지 않은 패킷에 대한 필터링 기준을 정의할 수 있습니다. 기본적으로 포트 기반(IEEE 802.1Q) 또는 프로토콜 기반 VLAN을 구성하지 않으면 태그가 지정되지 않은 패킷이 VLAN 1에 할당됩니다. 포트 기반 VLAN 또는 프로토콜 기반 VLAN을 정의하여 이 동작을 재정의할 수 있습니다. 둘 다. 태그가 지정된 패킷은 항상 IEEE 802.1Q 표준에 따라 처리되며 프로토콜 기반 VLAN에 포함되지 않습니다.

특정 프로토콜에 대한 프로토콜 기반 VLAN에 포트를 할당하는 경우 해당 프로토콜에 대해 해당 포트에서 수신된 태그가 지정되지 않은 프레임에는 프로토콜 기반 VLAN ID가 할당됩니다. 다른 프로토콜에 대해 포트에서 수신된 태그가 지정되지 않은 프레임에는 포트 VLAN ID, 기본 PVID(1) 또는 포트 VLAN 구성 화면을 사용하여 포트에 특별히 할당한 PVID가 할당됩니다.

그룹을 생성하여 프로토콜 기반 VLAN을 정의합니다. 각 그룹은 VLAN ID와 일대일 관계를 가지며, 1~3개의 프로토콜 정의를 포함할 수 있고, 여러 포트를 포함할 수 있습니다. 그룹을 생성할 때 이름을 지정하면 그룹 ID가 자동으로 할당됩니다.

➢ **프로토콜 기반 VLAN 그룹을 구성하려면:**

1.5 cm

Switching > **VLAN** > **Advanced** > **Protocol Based VLAN Group Configuration**.

1. Group Name 필드에 새 그룹의 이름을 입력합니다.

   최대 16자까지 입력할 수 있습니다.

2. Protocol 필드에서 그룹과 연결할 프로토콜을 선택합니다.

   구성 가능한 프로토콜은 세 가지가 있습니다.

   - **IP**. IP는 데이터 전달을 위해 비연결 서비스를 제공하는 네트워크 계층 프로토콜입니다.
   - **ARP**. ARP(주소 확인 프로토콜)는 네트워크 계층 주소를 물리적 MAC(매체 액세스 제어) 주소에 동적으로 매핑하는 하위 수준 프로토콜입니다.
   - **IPX**. IPX(Internetwork Packet Exchange)는 네트워크를 통해 데이터를 전달하는 연결 없는 데이터그램 네트워크 계층 프로토콜입니다.

3. VLAN ID 필드에서 VLAN ID를 선택합니다.

   1~4093 범위의 숫자일 수 있습니다. 그룹의 모든 포트는 이 그룹에 포함된 프로토콜에 대해 수신된 태그가 지정되지 않은 패킷에 이 VLAN ID를 할당합니다.

4. Add 버튼을 클릭합니다

   프로토콜 기반 VLAN 그룹이 스위치에 추가됩니다.

5. Group ID 필드의 값으로 식별된 프로토콜 기반 VLAN 그룹을 제거하려면 Delete 버튼을 클릭합니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 79. 프로토콜 기반 VLAN 그룹

필드	설명
Group ID	사용자가 생성한 그룹을 식별하는 데 사용되는 번호입니다. 그룹 ID는 사용자가 그룹을 생성할 때 자동으로 할당됩니다.
Ports	그룹에 속한 모든 멤버 포트를 표시합니다.

1.5 cm

프로토콜 기반 VLAN 그룹 멤버십 구성

➢ **프로토콜 기반 VLAN 그룹 멤버십을 구성하려면:**

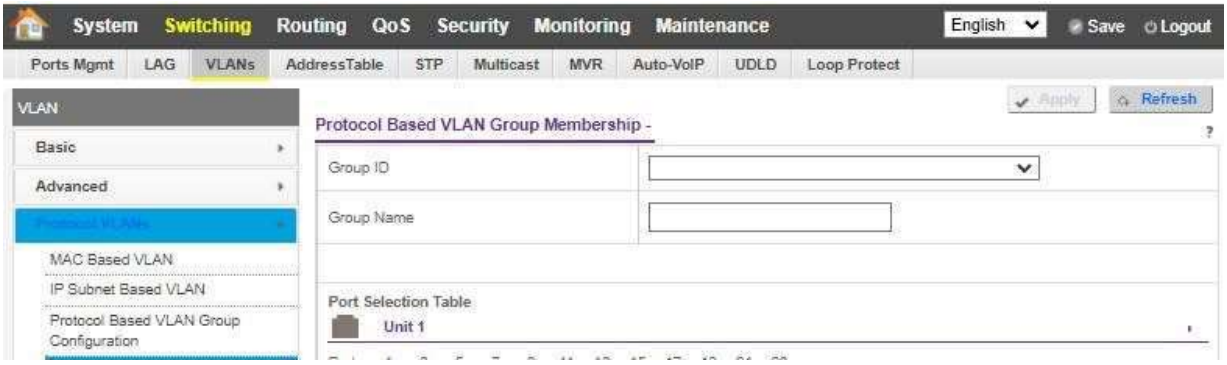
1. 192.168.10.0 서브넷의 고정 IP 주소(예: 192.168.10.101)를 사용하여 컴퓨터를 준비합니다.
2. 컴퓨터 이더넷 포트의 이더넷 케이블을 스위치의 이더넷 포트에 연결합니다.
3. 웹 브라우저를 시작합니다.
4. 웹 브라우저 주소 필드에 스위치의 IP 주소를 입력합니다.

   스위치의 기본 IP 주소는 192.168.10.12입니다.

   로그인 화면이 표시됩니다.
5. 사용자 이름과 비밀번호를 입력합니다.

   기본 관리자 사용자 이름은 admin이고 기본 관리자 비밀번호는 비어 있습니다. 즉, 비밀번호를 입력하지 마십시오.
6. Login 버튼을 클릭하세요.

   웹 관리 인터페이스 메뉴가 표시됩니다.
7. **Switching > VLAN > Advanced > Protocol Based VLAN Group Membership.**를 선택하세요.



8. Group ID 목록에서 프로토콜 기반 VLAN 그룹 ID를 선택합니다.
9. 포트 번호(1, 2, 3 등)를 선택하여 이 프로토콜 기반 VLAN 그룹에 추가할 포트를 선택합니다.

   인터페이스는 특정 프로토콜에 대해 하나의 그룹에만 속할 수 있습니다. IP용 그룹에 이미 포트를 추가한 경우 IPX용 새 그룹에는 추가할 수 있지만 IP도 포함하는 다른 그룹에는 추가할 수 없습니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

1.5 cm

Table 80. 프로토콜 기반 VLAN 그룹 멤버십

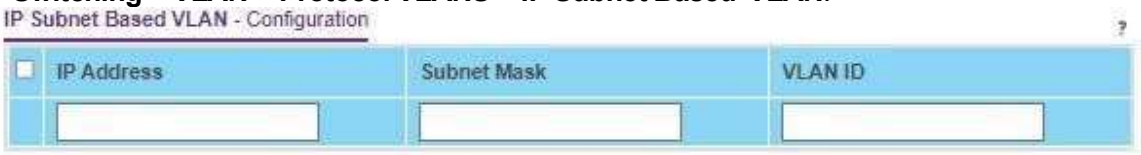
필드	설명
Group Name	이 필드는 선택한 프로토콜 기반 VLAN의 이름을 식별합니다. 공백을 포함하여 최대 32자의 영숫자 문자일 수 있습니다.
Current Members	이 버튼을 클릭하면 선택한 프로토콜 기반 VLAN 그룹의 현재 번호가 표시됩니다.

IP 서브넷 기반 VLAN 구성

IP 서브넷-VLAN 매핑은 IP 서브넷-VLAN 테이블의 항목을 구성하여 정의됩니다. 항목은 소스 IP 주소, 네트워크 마스크 및 원하는 VLAN ID를 통해 지정됩니다. VLAN 구성에 대한 IP 서브넷은 장치의 모든 포트에서 공유됩니다.

- **IP 서브넷 기반 VLAN을 구성하려면:**

Switching > VLAN > Protocol VLANS > IP Subnet Based VLAN.



1. IP Address 필드에서 VLAN ID에 바인딩된 유효한 IP 주소를 지정합니다.
   점으로 구분된 십진수 표기법으로 IP 주소를 입력합니다.
2. Subnet Mask 필드에서 IP 주소의 유효한 서브넷 마스크를 지정합니다.

   점으로 구분된 십진수 표기법으로 서브넷 마스크를 입력합니다.
3. VLAN ID 필드에서 (1~4093) 범위의 VLAN ID를 지정합니다.
4. Add 버튼을 클릭합니다

   IP 서브넷 기반 VLAN이 추가됩니다.
5. 선택한 IP 서브넷 기반 VLAN을 삭제하려면 Delete 버튼을 클릭합니다.

포트 DVLAN 구성

1.5 cm

➢ **포트 DVLAN을 구성하려면:**

Switching > VLAN > 802.1Q TUNNELING > Port DVLAN Configuration.

1. Interface check box을 선택하여 물리적 인터페이스를 선택합니다.

   모든 포트를 선택하려면 열 상단의 Interface check box을 선택하세요.

2. Admin Mode 필드에서 Enable 또는 Disable를 선택합니다.

   이는 이중 VLAN 래깅을 활성화하거나 비활성화할 수 있는 관리 모드를 지정합니다. 기본값은 Disable입니다.

3. Global EtherType 필드에서 DVLAN 태그의 처음 16비트를 지정합니다.
   - **802.1Q Tag**. 0x8100을 나타내는 일반적으로 사용되는 태그입니다.
   - **vMAN Tag**. 0x88A8을 나타내는 일반적으로 사용되는 태그입니다.
   - **Custom Tag**. 0~65535 범위에서 EtherType을 구성합니다.

GARP 스위치 설정 구성

Note: GARP 구성 변경 사항이 적용되는 데 최대 10초가 걸릴 수 있습니다.

➢ **GARP 스위치 설정을 구성하려면:**

Switching > VLAN > Advanced > GARP Switch Configuration.

1. GVRP 모드 Disable 또는 Enable 라디오 버튼을 선택합니다.

   스위치에 대한 GARP VLAN 등록 프로토콜 관리 모드를 선택합니다. 공장 기본값은 Disable입니다.

2. GMRP 모드 Disable 또는 Enable 라디오 버튼을 선택합니다.

   스위치에 대한 GARP 멀티캐스트 등록 프로토콜 관리 모드를 선택합니다. 공장 기본값은 Disable입니다.

GARP 포트 구성

Note: GARP 구성 변경 사항이 적용되는 데 최대 10초가 걸릴 수 있습니다.

➢ **GARP 포트를 구성하려면:**

Switching > **VLAN** > **Advanced** > **GARP Port Configuration**.

GARP Port Configuration -

	Interface	Port GVRP Mode	Port GMRP Mode	Join Timer(centisecs)	Leave Timer (centisecs)	Leave All Timer(centisecs)
☐	0/1	Disable	Disable	20	60	1000
☐	0/2	Disable	Disable	20	60	1000
☐	0/3	Disable	Disable	20	60	1000
☐	0/4	Disable	Disable	20	60	1000
☐	0/5	Disable	Disable	20	60	1000
☐	0/6	Disable	Disable	20	60	1000
☐	0/7	Disable	Disable	20	60	1000
☐	0/8	Disable	Disable	20	60	1000

1. Interface를 사용하여 데이터를 표시하거나 구성할 물리적 인터페이스를 선택합니다.
2. Port GVRP Mode 필드에서 Enable 또는 Disable를 선택합니다.

   이는 포트에 대한 GARP VLAN 등록 프로토콜 관리 모드를 지정합니다. 비활성화를 선택하면 프로토콜이 활성화되지 않으며 참여 시간, 종료 시간 및 항상 종료 시간이 적용되지 않습니다. 공장 기본값은 Disable입니다.

3. Port GMRP Mode 필드에서 Enable 또는 Disable를 선택합니다.

   이는 포트에 대한 GARP 멀티캐스트 등록 프로토콜 관리 모드를 지정합니다. 비활성화를 선택하면 프로토콜이 활성화되지 않으며 참여 시간, 퇴장 시간 및 항상 퇴장 시간이 적용되지 않습니다. 공장 기본값은 Disable입니다.

4. Join Time(centiseconds) 필드에서 VLAN 또는 멀티캐스트 그룹에 대한 멤버십을 등록(또는 재등록)하는 GARP PDU 전송 사이의 시간을 센티초 단위로 지정합니다.

   10~100(0.1~1.0초) 사이의 숫자를 입력하세요. 공장 기본값은 20센티초(0.2초)입니다. 이 타이머의 인스턴스는 각 포트의 각 GARP 참가자에 대해 존재합니다.

5. Leave Time(centiseconds) 필드에서 VLAN 또는 멀티캐스트 그룹에 대한 등록 취소 요청을 받은 후 연결된 항목을 삭제하기 전까지 기다리는 시간(센티초)을 지정합니다.

   이는 중단 없는 서비스를 유지하기 위해 다른 스테이션이 동일한 속성에 대한 등록을 주장할 시간을 허용합니다. 20~600(0.2~6.0초) 사이의 숫자를 입력하세요. 공장 기본값은 60센티초(0.6초)입니다. 이 타이머의 인스턴스는 각 포트의 각 GARP 참가자에 대해 존재합니다.

1.5 cm

6. Leave All Time(센티초)을 사용하여 LeaveAll PDU가 생성되는 빈도를 제어합니다.

   LeaveAll PDU는 모든 등록이 곧 취소될 것임을 나타냅니다. 등록을 유지하려면 참가자가 다시 가입해야 합니다. 전체 휴가 기간 타이머는 LeaveAllTime ~ 1.5*LeaveAllTime 범위의 임의 값으로 설정됩니다. 타이머는 100분의 1초 단위로 지정됩니다. 200~6000(2~60초) 사이의 숫자를 입력하세요. 공장 기본값은 1000센티초(10초)입니다. 이 타이머의 인스턴스는 각 포트의 각 GARP 참가자에 대해 존재합니다.

VoiceVLAN 구성

음성 VLAN 구성에 대한 매개변수를 구성할 수 있습니다. 읽기/쓰기 액세스 권한이 있는 사용자만 이 화면의 데이터를 변경할 수 있습니다.

➢ **음성 VLAN을 구성하려면:**

Switching > VLAN > Advanced > Voice VLAN Configuration.

Voice VLAN Configuration - Global Admin

Admin mode	Disable	Enable

Voice VLAN Configuration - Ports Configuration

Interface	Interface Mode	Vlan ID/Priority	CoS Override Mode	Operational State
0/1	Disable		Disable	Disabled
0/2	Disable		Disable	Disabled
0/3	Disable		Disable	Disabled
0/4	Disable		Disable	Disabled
0/5	Disable		Disable	Disabled
0/6	Disable		Disable	Disabled
0/7	Disable		Disable	Disabled
0/8	Disable		Disable	Disabled

1. Admin Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다

   스위치의 음성 VLAN에 대한 관리 모드를 지정합니다. 기본값은 비활성화입니다.

2. Interface를 사용하여 물리적 인터페이스를 선택합니다.
3. Interface Mode를 사용하여 선택한 인터페이스에 대한 음성 VLAN 모드를 선택합니다.
   - **Disable**. 이것이 기본값입니다.
   - **None**. IP 전화가 자체 구성을 사용하여 태그가 지정되지 않은 음성 트래픽을 보낼 수 있도록 허용합니다.
   - **VLAN ID**. 태그가 지정된 음성 트래픽을 보내도록 전화기를 구성합니다.

1.5 cm

- **dot1p** 음성 트래픽에 대한 음성 VLAN 802.1p 우선순위 태그를 구성합니다. 이를 선택한 경우 값 필드에 dot1p 값을 입력합니다.
- **Untagged**. 태그가 지정되지 않은 음성 트래픽을 보내도록 전화기를 구성합니다.

4. Value를 사용하여 VLAN ID 또는 dot1p 값을 입력합니다.

   VLAN ID 또는 dot1p 값을 사용하여 값을 입력합니다.

5. CoS Override Mode 필드에서 Disable 또는 Enable를 선택합니다.

   기본값은 Disable입니다.

6. Authentication Mode 필드에서 Enable 또는 Disble를 선택합니다.

   기본값은 Enable입니다. 인증 모드가 활성화되면 승인되지 않은 음성 VLAN 포트에서 음성 트래픽이 허용됩니다. 인증 모드가 비활성화되면 장치는 dot1x를 통해 인증됩니다.

   Note: dot1x를 통한 인증은 dot1x가 활성화된 경우에만 가능합니다.

7. DSCP Value 필드에서 포트에 대한 음성 VLAN DSCP 값을 구성합니다.

   유효한 범위는 0~64입니다. 기본값은 0입니다.

Operational State(작동 상태) 필드에는 해당 인터페이스의 음성 VLAN 작동 상태가 표시됩니다.

MAC 주소 테이블

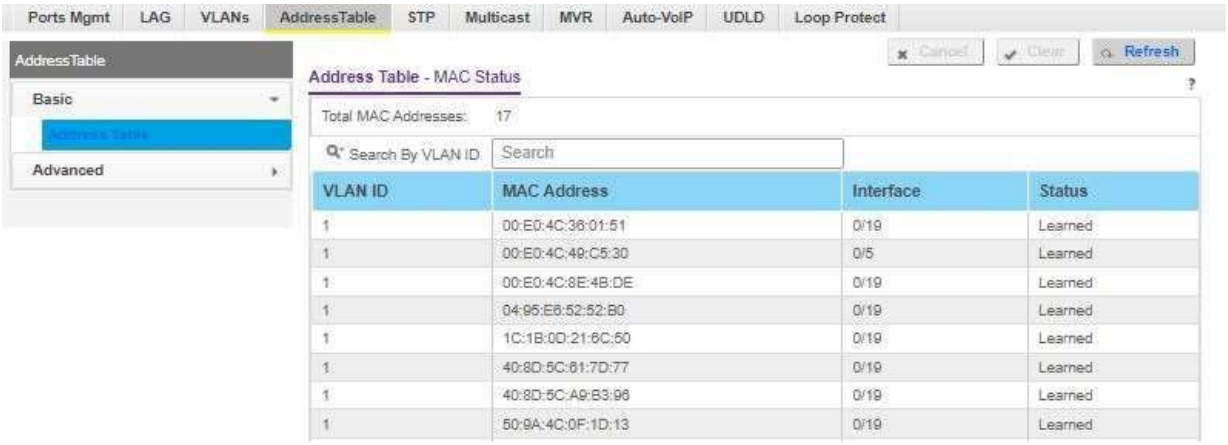
MAC 주소 테이블을 보거나 구성할 수 있습니다. 이 테이블에는 스위치에 전달 또는 필터링 정보가 있는 유니캐스트 항목에 대한 정보가 포함되어 있습니다. 이 정보는 수신된 프레임을 전파하는 방법을 결정할 때 투명 브리징 기능에 의해 사용됩니다.

MAC 주소 테이블 구성

➢ **MAC 주소 테이블을 구성하려면:**

1.5 cm

Switching > Address Table> Basic > **Address Table**.



1. 검색 기준을 사용하여 MAC 주소, VLAN ID 또는 포트별로 MAC 주소를 검색합니다.
   - **Searched by MAC Address**. MAC Address를 선택하고 6바이트 16진수 MAC 주소를 콜론으로 구분된 두 자리 그룹으로 입력합니다(예: 01:23:45:67:89:AB). 그런 다음 이동 버튼을 클릭하세요. 주소가 존재하는 경우 해당 항목은 다음과 같습니다.

     첫 번째 항목으로 표시되고 그 뒤에 나머지(더 큰) MAC 주소가 표시됩니다. 정확하게 일치해야 합니다.
   - **Searched by VLAN ID**. VLAN ID를 선택하고 VLAN ID(예: 100)를 입력한 다음 이동 버튼을 클릭합니다. 주소가 존재하는 경우 해당 항목은 첫 번째 항목으로 표시되고 그 뒤에 나머지(더 큰) MAC 주소가 표시됩니다.
   - **Searched by Port**. Port를 선택하고 장치/슬롯/포트 형식으로 포트 ID를 입력합니다(예: 2/1/1). 그런 다음 이동 버튼을 클릭하세요. 주소가 존재하는 경우 해당 항목은 첫 번째 항목으로 표시되고 그 뒤에 나머지(더 큰) MAC 주소가 표시됩니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 106. 기본 주소 테이블

필드	설명
Total MAC Address	학습되거나 구성된 총 MAC 주소 수를 표시합니다.
MAC Address	스위치에 전달 및/또는 필터링 정보가 있는 유니캐스트 MAC 주소입니다. 형식은 콜론으로 구분된 6바이트 MAC 주소입니다(예: 01:23:45:67:89:AB).
VLAN ID	MAC 주소와 연결된 VLAN ID입니다.
Port	이 주소가 학습된 포트입니다.

1.5 cm

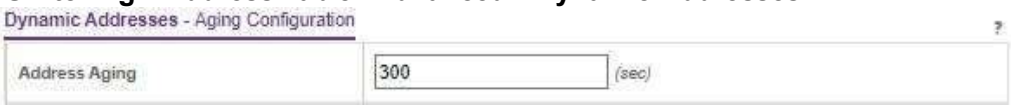
Status	이 항목의 상태입니다. 값의 의미는 다음과 같습니다. • Static. 해당 인스턴스의 값은 시스템이나 사용자에 의해 추가된 것이므로 다시 학습할 수 없습니다. • Learned. 해당 인스턴스의 값을 학습하여 사용하고 있습니다. • Management. 해당 인스턴스의 값은 dot1dStaticAddress의 기존 인스턴스 값이기도 합니다.

동적 주소 에이징 간격 설정

지정된 전달 데이터베이스에 대한 주소 에이징 간격을 설정할 수 있습니다.

➢ **주소 에이징 간격을 설정하려면,**

Switching > Address Table> Advanced > Dynamic Addresses.



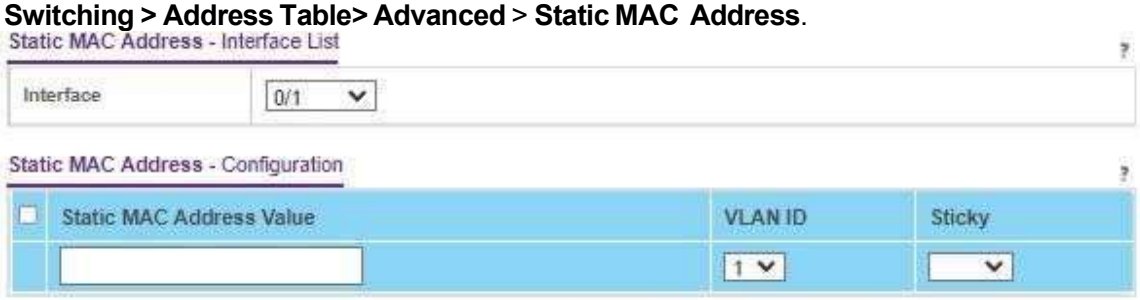
1. 동적으로 학습된 전달 정보의 만료 기간을 초 단위로 지정하려면 Address Aging Timeout(seconds)을 사용합니다.

   802.1D-1990에서는 기본값으로 300초를 권장합니다. 값은 10초에서 1000000초 사이의 숫자로 지정할 수 있습니다. 공장 기본값은 300입니다.

정적 MAC 주소 구성

➢ **정적 MAC 주소를 구성하려면:**

Switching > Address Table> Advanced > Static MAC Address.



1. Interface를 사용하여 물리적 인터페이스/LAG를 선택합니다.
2. Static MAC Address 필드에 MAC 주소를 입력합니다.

1.5 cm

3. MAC 주소와 연결된 VLAN ID를 선택합니다.
4. Add 버튼을 클릭합니다

   정적 MAC 주소가 스위치에 추가됩니다.

스위치에서 기존 고정 MAC 주소를 삭제하려면 Delete 버튼을 클릭하세요.

스패닝 트리 프로토콜

STP(Spanning Tree Protocol)는 모든 브리지 배열에 대한 트리 토폴로지를 제공합니다. STP는 또한 네트워크의 최종 스테이션 간에 단일 경로를 제공하여 루프를 제거합니다. 지원되는 스패닝 트리 버전에는 Common STP, Multiple STP 및 Rapid STP가 포함됩니다.

클래식 STP는 엔드 스테이션 간의 단일 경로를 제공하여 루프를 피하고 제거합니다. 공통 STP 구성에 대한 자세한 내용은 236페이지의 CST 포트 설정 구성을 참조하십시오.

MSTP(다중 스패닝 트리 프로토콜)는 스패닝 트리의 여러 인스턴스를 지원하여 다양한 인터페이스를 통해 VLAN 트래픽을 효율적으로 전달합니다. 스패닝 트리의 각 인스턴스는 IEEE 802.1w, RSTP(Rapid Spanning Tree)에 지정된 방식으로 작동하며 작업에는 약간의 수정이 있지만 최종 효과는 없습니다(효과 중 가장 중요한 것은 포트가 전달로 빠르게 전환된다는 것입니다). . RSTP와 기존 STP(IEEE 802.1D)의 차이점은 전이중 연결과 엔드 스테이션에 연결된 포트를 구성하고 인식하여 포트를 Forwarding 상태로 빠르게 전환하고 토폴로지 변경을 억제하는 기능입니다. 공고. 이러한 기능은 pointtopoint 및 edgeport 매개변수로 표시됩니다. MSTP는 RSTP 및 STP와 모두 호환됩니다. STP 및 RSTP 브리지에 적절하게 작동합니다. MSTP 브리지는 완전히 RSTP 브리지 또는 STP 브리지로 작동하도록 구성할 수 있습니다.

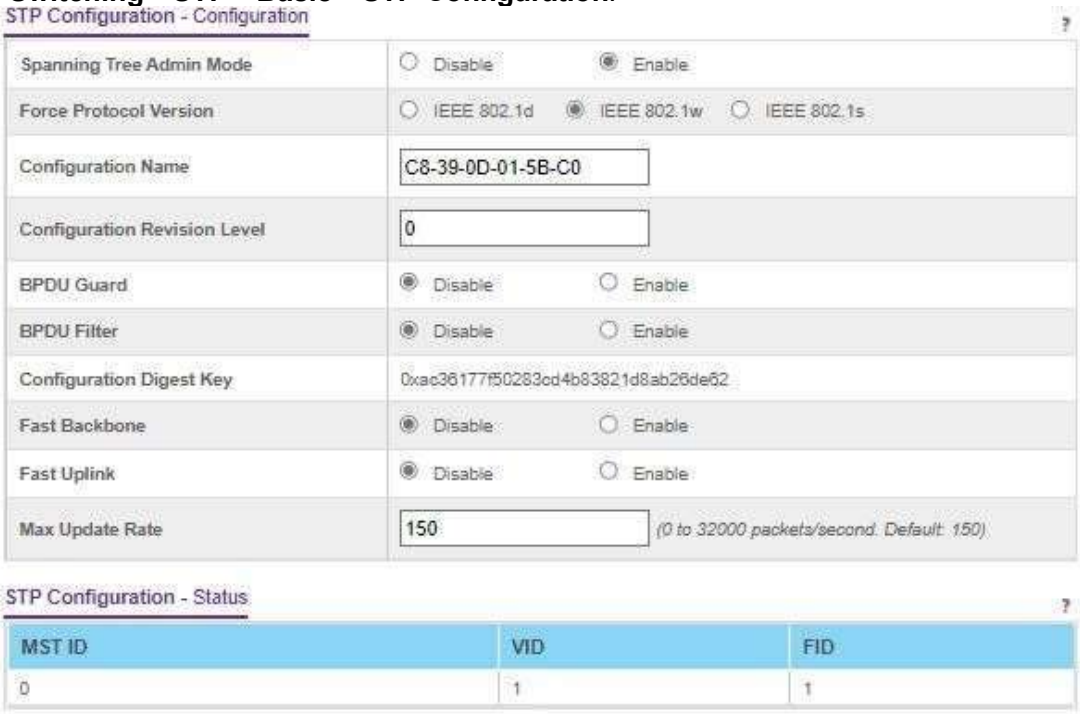
Note: 두 브리지가 동일한 지역에 있으려면 강제 버전이 802.1s여야 하며 해당 구성 이름, 다이제스트 키 및 개정 수준이 일치해야 합니다. 지역과 네트워크 토폴로지에 미치는 영향에 대한 추가 정보는 IEEE 802.1Q 표준을 참조하세요.

기본 STP 설정 구성

➢ **STP 기본 설정을 구성하려면:**

1.5 cm

Switching > STP > Basic > STP Configuration.



1. Spanning Tree Management Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   스위치에서 스패닝 트리 작업을 활성화할지 여부를 지정합니다.

2. Force Protocol Version을 사용하여 스위치에 대한 강제 프로토콜 버전 매개변수를 지정합니다.

   옵션은 IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, PVST 및 RPVST입니다.

3. Configuration Name을 사용하여 현재 사용 중인 구성을 식별하는 데 사용되는 식별자를 지정합니다.

   최대 32자의 영숫자 문자를 사용할 수 있습니다.

4. Configuration Revision Level을 사용하여 현재 사용 중인 구성을 식별하는 데 사용되는 식별자를 지정합니다.

   허용되는 값은 0에서 65535 사이입니다. 기본값은 0입니다.

5. STP가 비활성화된 동안 Forward BPDU의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 스위치에서 스패닝 트리가 비활성화된 동안 스패닝 트리 BPDU가 전달되는지 여부를 지정합니다.

6. BPDU Guard의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   BPDU 가드 기능의 활성화 여부를 지정합니다. STP BPDU 가드를 사용하면 네트워크 관리자는 STP 도메인 경계를 적용하고 활성 토폴로지를 일관되고 예측 가능하게 유지할

1.5 cm

수 있습니다. STP BPDU 가드가 활성화된 에지 포트 뒤의 스위치는 전체 STP 토폴로지에 영향을 미치지 않습니다. BPDU 수신 시 BPDU 가드 동작은 이 옵션으로 구성된 포트를 비활성화하고 해당 포트를 비활성화 상태로 전환합니다. 이로 인해 포트가 관리적으로 비활성화됩니다.

7. BPDU Filter의 Disable 또는 Eneable 라디오 버튼을 선택합니다.

   BPDU 필터 기능의 활성화 여부를 지정합니다. STP BPDU 필터링은 모든 작동 에지 포트에 적용됩니다. 작동 상태의 엣지 포트는 일반적으로 BPDU를 삭제하는 호스트에 연결되어야 합니다. 작동 중인 에지 포트가 BPDU를 수신하면 즉시 작동 상태를 잃습니다. 이 경우 이 포트에서 BPDU 필터링이 활성화되면 이 포트에서 수신된 BPDU를 삭제합니다.

8. Fast Backbone Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다. (PVSTP에만 해당됩니다.)

   간접 링크가 실패할 경우 새 간접 링크를 선택하려면 이 옵션을 사용하십시오. 시스템은 802.1d에서처럼 하위 BPDU를 무시하지 않습니다. 오히려 시스템은 BPDU를 사용하여 BPDU를 수신한 포트를 만료시킵니다. 나중에 시스템은 지정되지 않은 다른 포트에 루트 링크 쿼리를 보냅니다. 응답을 기반으로 그 중 적어도 하나에 대해 긍정적인 응답이 있으면 새로운 간접 링크를 선택합니다. 빠른 백본 모드는 기본적으로 비활성화되어 있습니다.

9. Fast Uplink Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다. (PVSTP에만 해당됩니다.)

   이 옵션을 사용하면 기본 루트 포트가 다운된 경우 새 루트 포트를 선택하는 복구 시간이 단축됩니다. 빠른 업링크 모드는 기본적으로 비활성화되어 있습니다.

10. Max Update Rate 필드를 사용하여 빠른 업링크 최대 업데이트 속도를 구성합니다.

    빠른 업링크 모드가 활성화되면 구성을 위해 이 필드가 활성화됩니다. 허용되는 값은 초당 0~32000개의 패킷입니다. 기본값은 150입니다.

11. Apply 버튼을 클릭합니다

    업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표에서는 구성할 수 없는 필드에 대해 설명합니다.

Table 85. STP 구성

필드	설명
Configuration Digest Key	현재 사용 중인 구성을 식별하는 데 사용되는 식별자입니다.
Configuration Format Selector	BPDU 교환에 사용되는 구성 형식의 버전입니다.

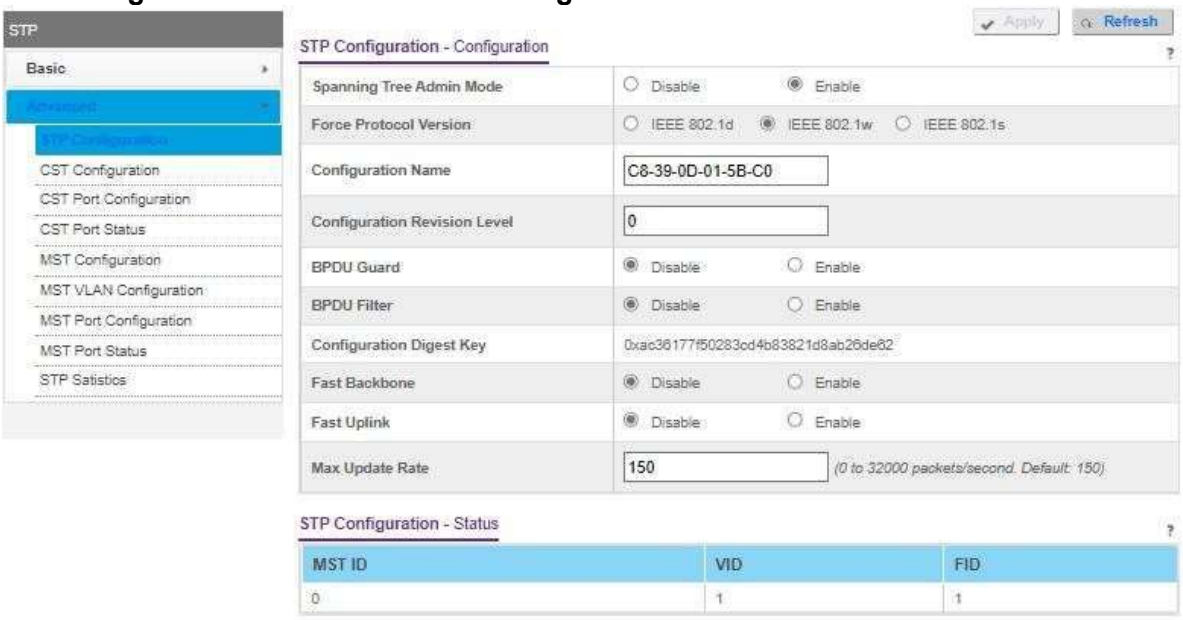
1.5 cm

MST ID	MST 인스턴스(CST 포함) 및 각 인스턴스와 연결된 해당 VLAN ID로 구성된 테이블입니다.
VID ID	VLAN ID 및 각 ID와 연결된 해당 FID로 구성된 테이블입니다.
FID ID	FID 및 각 FID와 연결된 해당 VLAN ID로 구성된 테이블입니다.

고급 STP 설정 구성

➢ **고급 STP 설정을 구성하려면:**

Switching > STP > Advanced > STP Configuration.



1. Admin Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다

   스위치에서 스패닝 트리 작업을 활성화할지 여부를 지정합니다. 기본값은 Enable입니다.

2. Force Protocol Version을 사용하여 스위치에 대한 강제 프로토콜 버전 매개변수를 지정합니다.

   옵션은 IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, PVST 및 RPVST입니다. 기본값은 IEEE 802.1w입니다.

3. Configuration Name을 사용하여 현재 사용 중인 구성을 식별하는 데 사용되는 식별자를 지정합니다.

   최대 32자의 영숫자 문자를 사용할 수 있습니다.

4. Configuration Revision Level을 사용하여 현재 사용 중인 구성을 식별하는 데 사용되는

1.5 cm

식별자를 지정합니다.

허용되는 값은 0에서 65535 사이입니다. 기본값은 0입니다.

5. STP가 비활성화된 동안 Forward BPDU이 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 스위치에서 스패닝 트리가 비활성화된 동안 스패닝 트리 BPDU가 전달되는지 여부를 지정합니다. 기본값은 Disable입니다.

6. BPDU Guard의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   BPDU 가드 기능의 활성화 여부를 지정합니다. STP BPDU 가드를 사용하면 네트워크 관리자는 STP 도메인 경계를 적용하고 활성 토폴로지를 일관되고 예측 가능하게 유지할 수 있습니다. STP BPDU 가드가 활성화된 에지 포트 뒤의 스위치는 전체 STP 토폴로지에 영향을 미치지 않습니다. BPDU 수신 시 BPDU 가드 동작은 이 옵션으로 구성된 포트를 비활성화하고 해당 포트를 비활성화 상태로 전환합니다. 이로 인해 포트가 관리적으로 비활성화됩니다.

7. BPDU Filter의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   BPDU 필터 기능의 활성화 여부를 지정합니다. STP BPDU 필터링은 모든 작동 에지 포트에 적용됩니다. 작동 상태의 엣지 포트는 일반적으로 BPDU를 삭제하는 호스트에 연결되어야 합니다. 작동 중인 에지 포트가 BPDU를 수신하면 즉시 작동 상태를 잃습니다. 이 경우 이 포트에서 BPDU 필터링이 활성화되면 이 포트에서 수신된 BPDU를 삭제합니다.

8. Fast Backbone Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다. (PVSTP에만 해당됩니다.)

   간접 링크가 실패할 경우 새 간접 링크를 선택하려면 이 옵션을 사용하십시오. 시스템은 802.1d에서처럼 하위 BPDU를 무시하지 않습니다. 오히려 시스템은 BPDU를 사용하여 BPDU를 수신한 포트를 만료시킵니다. 나중에 시스템은 지정되지 않은 다른 포트에 루트 링크 쿼리를 보냅니다. 응답을 기반으로 그 중 적어도 하나에 대해 긍정적인 응답이 있으면 새로운 간접 링크를 선택합니다. 빠른 백본 모드는 기본적으로 비활성화되어 있습니다.

9. Fast Uplink Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다. (PVSTP에만 해당됩니다.)

   이 옵션을 사용하면 기본 루트 포트가 다운된 경우 새 루트 포트를 선택하는 복구 시간이 단축됩니다. 빠른 업링크 모드는 기본적으로 비활성화되어 있습니다.

10. Max Update Rate 필드를 사용하여 빠른 업링크 최대 업데이트 속도를 구성합니다.

    빠른 업링크 모드가 활성화되면 구성을 위해 이 필드가 활성화됩니다. 허용되는 값은 초당 0~32000개의 패킷입니다. 기본값은 150입니다.

1.5 cm

11. Apply 버튼을 클릭합니다

업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 86. STP 구성

필드	설명
Configuration Digest Key	현재 사용 중인 구성을 식별하는 데 사용되는 MST 구성 테이블(VLAN ID-MST ID 매핑)에서 생성된 HMAC-MD5 유형의 16바이트 서명입니다.
Configuration Format Selector	BPDU 교환에 사용되는 구성 형식의 버전입니다.
STP 상태	
MST ID	MST 인스턴스(CST 포함) 및 각 인스턴스와 연결된 해당 VLAN ID로 구성된 테이블입니다.
VID ID	VLAN ID 및 각 ID와 연결된 해당 FID로 구성된 테이블입니다.
FID ID	FID 및 각 FID와 연결된 해당 VLAN ID로 구성된 테이블입니다.

CST 설정 구성

스위치에서 CST(Common Spanning Tree) 및 내부 스패닝 트리(Internal Spanning Tree)를 구성할 수 있습니다.

➢ **CST 설정을 구성하려면:**

Switching > STP > Advanced > CST Configuration.

1. 해당 필드에 CST 값을 지정합니다.
   - **Bridge Priority**. 스위치나 브리지가 STP를 실행하는 경우 각각에 우선 순위가 할당됩니다. BPDU를 교환한 후 우선순위 값이 가장 낮은 스위치가 루트 브리지가 됩니다. 공통 및 내부 스패닝 트리(CST)에 대한 브리지 우선순위 값을 지정합니다. 유효한 범위는 0~61440입니다. 브리지 우선순위는 4096의 배수입니다. 4096의 배수가 아닌 우선순위를 지정하면 우선순위는 자동으로 4096의 배수인 다음으로 낮은 우선순위로 설정됩니다. 예를 들어 우선순위를 다음으로 설정하려고 하면 0에서 4095 사이의 값은 0으로 설정됩니다. 기본 우선순위는 32768입니다.
   - **Bridge Max Age (secs)**. 공통 및 내부 스패닝 트리(CST)에 대한 브리지 최대 수명 시간은 토폴로지 변경을 구현하기 전에 브리지가 대기하는 시간(초)을 나타냅니다.

1.5 cm

유효한 범위는 6~40이고 값은 (2 * 브리지 전달 지연) - 1보다 작거나 같고 2 * (브리지 헬로우 시간 +1)보다 크거나 같아야 합니다. 기본값은 20입니다.

- **Bridge Hello Time (secs)**. 공통 및 내부 스패닝 트리(CST)에 대한 브리지 헬로우 시간은 루트 브리지가 구성 메시지 사이에 대기하는 시간(초)을 나타냅니다. 값은 2초로 고정됩니다. 값은 (Bridge Max Age / 2) - 1보다 작거나 같아야 합니다. 기본 안녕하세요 시간 값은 2입니다.
- **Bridge Forward Delay (secs).** 브리지 전달 지연 시간은 브리지가 패킷을 전달하기 전에 청취 및 학습 상태를 유지하는 시간(초)을 나타냅니다. 값은 (Bridge MaxAge / 2) + 1보다 크거나 같아야 합니다. 시간 범위는 4초~30초입니다. 기본값은 15초입니다.
- **Spanning Tree Maximum Hops**. 특정 CST 인스턴스에 대한 정보가 삭제되기 전에 이동할 수 있는 최대 브리지 홉 수입니다. 유효한 범위는 6~40입니다. 기본값은 20홉입니다.
- **Spanning Tree Tx Hold Count**. Hello 시간 창 내에서 브리지가 전송할 수 있는 최대 bpdus 수를 구성합니다. 유효한 범위는 1~10입니다. 기본값은 6입니다.

2. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표에서는 표시되는 CST 상태 정보에 대해 설명합니다.

Table 87. STP 고급 CST 구성

필드	설명
Bridge identifier	CST의 브리지 식별자입니다. 브리지 우선순위와 브리지의 기본 MAC 주소를 사용하여 구성됩니다.
Time since topology change	CST의 토폴로지가 마지막으로 변경된 이후의 시간(초)입니다.
Topology change count	CST에 대해 토폴로지가 변경된 횟수입니다.
Topology change	CST에 할당된 포트에서 토폴로지 변경이 진행 중인지 여부를 나타내는 스위치의 토폴로지 변경 매개변수 값입니다. True 또는 False인 경우 값을 취합니다.
Designated root	루트 브리지의 브리지 식별자입니다. 이는 브리지 우선순위와 브리지의 기본 MAC 주소로 구성됩니다.
Root Path Cost	CST의 지정된 루트에 대한 경로 비용입니다.

1.5 cm

Root Port Identifier	CST의 지정 루트에 접근하기 위한 포트입니다.
Max Age(secs)	CST의 지정된 루트에 대한 경로 비용입니다.
Forward Delay(secs)	루트 포트 브리지 전달 지연 매개변수의 파생 값입니다.
Hold Time(secs)	구성 BPDU 전송 사이의 최소 시간입니다.
CST Regional Root	CST 지역 루트의 우선순위 및 기본 MAC 주소입니다.
CST Path Cost	CST 트리 지역 루트에 대한 경로 비용입니다.

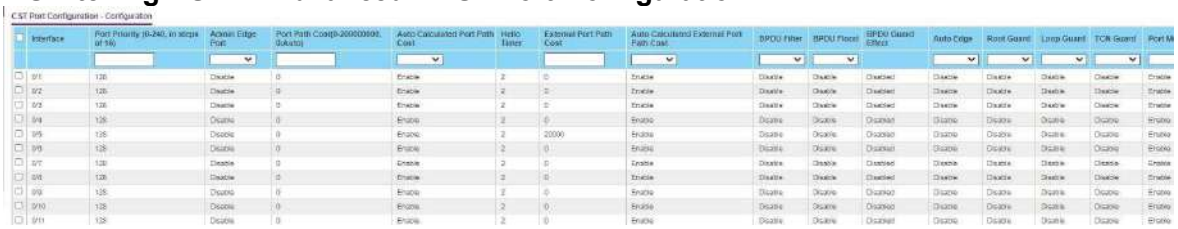
CST 포트 설정 구성

스위치의 특정 포트에서 CST(공통 스패닝 트리) 및 내부 스패닝 트리를 구성할 수 있습니다.

DOT1S에 심각한 오류 조건이 발생하면 포트는 진단적으로 비활성화(D-Disable)될 수 있습니다. 가장 일반적인 원인은 DOT1S 소프트웨어에 BPDU 플러딩이 발생하는 경우입니다. 플러딩 기준은 DOT1S가 3초 간격으로 15개 이상의 BPDU를 수신하는 것입니다. DOT1S D-Disable의 다른 원인은 극히 드뭅니다.

- **CST 포트 설정을 구성하려면:**

  Switching > STP > Advanced > CST Port Configuration.



1. Interface를 선택합니다.

   CST와 연결된 VLAN과 연결된 물리적 또는 포트 채널 인터페이스를 선택할 수 있습니다.

2. Port Priority를 사용하여 CST 내의 특정 포트에 대한 우선 순위를 지정합니다.

포트 우선순위는 16의 배수로 설정됩니다. 예를 들어 우선순위를 0~15 사이의 값으로 설정하려고 하면 0으로 설정됩니다. 16~(2*) 사이의 값으로 설정하려고 하면 0으로 설정됩니다. 16-1) 16으로 설정되어 있습니다. 기본값은 128입니다.

3. Admin Edge Port를 사용하여 지정된 포트가 CIST 내의 에지 포트인지 지정합니다.

   메뉴를 사용하여 Disable 또는 Enable를 선택합니다. 기본값은 Disable입니다.

4. Port Path Cost을 사용하여 공통 및 내부 스패닝 트리에서 지정된 포트에 대한 경로 비용을 새 값으로 설정합니다.

   1~200000000 범위의 값을 사용합니다. 기본값은 0입니다.

5. External Port Path Cost을 사용하여 스패닝 트리의 지정된 포트에 대한 외부 경로 비용을 새 값으로 설정합니다.

   1~200000000 범위의 값을 사용합니다. 기본값은 0입니다.

6. BPDU Filter를 사용하여 이 포트에서 STP가 활성화되면 이 포트의 BPDU 트래픽을 필터링하는 BPDU 필터를 구성합니다.

   가능한 값은 Enable 또는 Disable입니다. 기본값은 Disable입니다.

7. BPDU Flood를 사용하여 이 포트에서 STP가 비활성화된 경우 이 포트에 도착하는 BPDU 트래픽을 플러딩하는 BPDU Flood를 구성합니다.

   가능한 값은 Enable 또는 Disable입니다. 기본값은 Disable입니다.

8. Auto Edge를 사용하여 포트의 자동 에지 모드를 구성합니다. 그러면 포트가 일정 기간 동안 BPDU가 표시되지 않는 경우 에지 포트가 될 수 있습니다.

   가능한 값은 Enable 또는 Disable입니다. 기본값은 Enable입니다.

9. Root Guard를 사용하여 포트에서 수신한 모든 상위 정보를 폐기하도록 포트를 설정하고 장치의 루트가 변경되지 않도록 보호하는 루트 가드 모드를 구성합니다.

   포트는 폐기 상태가 되며 어떤 패킷도 전달하지 않습니다. 가능한 값은 Enable 또는 Disable입니다. 기본값은 Disable입니다.

10. Loop Guard를 사용하여 레이어 2 전달 루프를 보호하기 위해 포트의 루프 가드를 Enable하거나 Disable합니다.

    루프 가드가 활성화되면 포트는 수신/학습/전달 상태 대신 STP 루프 불일치 차단 상태로 전환됩니다. 기본값은 Disable입니다.

1.5 cm

11. TCN Guard를 사용하여 포트가 해당 포트를 통해 수신된 토폴로지 변경 정보를 전파하지 못하도록 제한하는 포트에 대해 TCN Guard를 구성합니다.

    가능한 값은 Enable 또는 Disable입니다. 기본값은 Disable입니다.

12. Port Mode를 사용하여 포트 또는 포트 채널과 관련된 스패닝 트리 프로토콜 관리 모드를 Enable하거나 Disable합니다.

    가능한 값은 Enable또는 Disable입니다. 기본값은 Disable입니다.

13. Apply 버튼을 클릭합니다

    업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 88. CST 포트 구성

필드	설명
Auto Calculated Port Path Cost	경로 비용이 자동으로 계산되는지(활성화) 또는 계산되지 않는지(비활성화)를 표시합니다. 포트 경로 비용에 대해 구성된 값이 0인 경우 경로 비용은 포트의 링크 속도를 기준으로 계산됩니다.
Hello Timer	CST에 대한 매개변수 값입니다.
Auto Calculated External Port Path Cost	외부 경로 비용이 자동으로 계산되는지(활성화) 또는 계산되지 않는지(비활성화)를 표시합니다. 외부 포트 경로 비용에 대해 구성된 값이 0인 경우 외부 경로 비용은 포트의 링크 속도를 기준으로 계산됩니다.
BPDU Guard Effect	BPDU 가드 효과를 표시하면 BPDU 패킷을 수신하는 에지 포트가 비활성화됩니다. 가능한 값은 활성화 또는 비활성화입니다.
Port Forwarding State	이 포트의 전달 상태입니다.

CST 포트 상태 보기

스위치의 특정 포트에서 CST(Common Spanning Tree) 및 내부 스패닝 트리(Internal Spanning Tree)를 볼 수 있습니다.

➢ **CST 포트 상태를 보려면:**

Switching > STP > Advanced > CST Port Status.

1.5 cm

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표에서는 화면에 표시되는 CST 상태 정보에 대해 설명합니다.

Table 89. CST 포트 상태

필드	설명
Interface	CST와 연결된 VLAN과 연결된 물리적 또는 포트 채널 인터페이스를 식별합니다.
Port ID	CST 내에서 지정된 포트에 대한 포트 식별자입니다. 포트 우선순위와 포트의 인터페이스 번호로 구성됩니다.
Port Forwarding State	이 포트의 전달 상태입니다.
Port Role	활성화된 각 MST 브리지 포트에는 각 스패닝 트리에 대한 포트 역할이 할당됩니다. 포트 역할은 루트 포트, 지정된 포트, 대체 포트, 백업 포트, 마스터 포트 또는 비활성화된 포트 값 중 하나입니다.
Designated Root	CST용 루트 브리지. 브리지 우선순위와 브리지의 기본 MAC 주소를 사용하여 구성됩니다.
Designated Cost	지정된 포트가 LAN에 제공하는 경로 비용입니다.
Designated Bridge	지정된 포트가 있는 브리지의 브리지 식별자입니다. 브리지 우선순위와 브리지의 기본 MAC 주소를 사용하여 구성됩니다.
Designated Port	LAN에 가장 낮은 비용을 제공하는 지정 브리지의 포트 식별자입니다. 포트 우선순위와 포트의 인터페이스 번호로 구성됩니다.
Topology Change Acknowledge	이 포트에 대해 전송될 다음 BPDU에 대해 토폴로지 변경 확인 플래그가 설정되어 있는지 여부를 식별합니다. True 또는 False입니다.
Edge port	포트가 에지 포트로 활성화되었는지 여부를 나타냅니다. 활성화 또는 비활성화 값을 사용합니다.
Point-to-point MAC	지점 간 상태의 파생 값입니다.
CST Regional Root	CST 지역 루트의 브리지 식별자입니다. 브리지 우선순위와 브리지의 기본 MAC 주소를 사용하여 구성됩니다.
CST Path Cost	CST 지역 루트에 대한 경로 비용입니다.
Port Up Time Since Counters Last Cleared	카운터가 마지막으로 지워진 이후의 시간이 일, 시, 분, 초로 표시됩니다.

1.5 cm

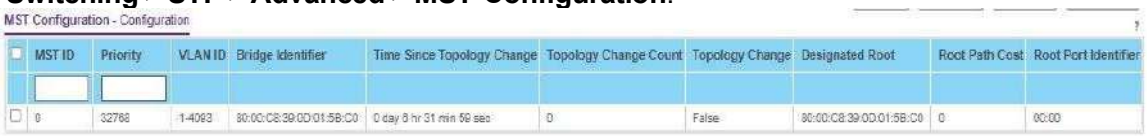
Loop Inconsistent State	이 매개변수는 포트가 루프 불일치 상태에 있는지 여부를 식별합니다.
Transitions Into Loop Inconsistent State	이 인터페이스가 루프 불일치 상태로 전환된 횟수입니다.
Transitions Out Of Loop Inconsistent State	이 인터페이스가 루프 불일치 상태에서 전환된 횟수입니다.

MST 설정 구성

스위치에서 다중 스패닝 트리(MST)를 구성할 수 있습니다.

➢ **MST 인스턴스를 구성하려면:**

Switching > STP > Advanced > MST Configuration.



1. MST 값을 구성합니다.
   - **MST ID**. 생성할 MST의 ID를 지정합니다. 이에 대한 유효한 값은 1~4094입니다. 이는 MST ID 선택 상자의 선택 옵션이 선택된 경우에만 표시됩니다.
   - **Priority**. MST의 브리지 우선순위 값입니다. 스위치나 브리지가 STP를 실행하는 경우 각각에 우선 순위가 할당됩니다. BPDU를 교환한 후 우선순위 값이 가장 낮은 스위치가 루트 브리지가 됩니다. 브리지 우선순위는 4096의 배수입니다. 4096의 배수가 아닌 우선순위를 지정하면 우선순위는 자동으로 4096의 배수인 다음으로 낮은 우선순위로 설정됩니다. 예를 들어 우선순위를 설정하려고 시도하는 경우 0~4095 사이의 값이면 0으로 설정됩니다. 기본 우선순위는 32768입니다. 유효한 범위는 0~61440입니다.
   - **VLAN ID**. 이는 스위치의 각 VLAN에 대한 콤보 상자를 제공합니다. VLAN과 MST 인스턴스의 연결을 재구성하기 위해 이를 선택하거나 선택 취소할 수 있습니다.
2. Add 버튼을 클릭합니다

   이렇게 하면 구성한 새 MST가 생성됩니다.
3. MST 인스턴스를 수정하려면:
   a. 인스턴스 옆의 check box을 선택합니다. (여러 개의 check box을 선택하여 선택한 모든 포트에 동일한 설정을 적용할 수 있습니다.)
   b. 값을 업데이트합니다.
   c. Apply 버튼을 클릭합니다

1.5 cm

4. MST 인스턴스를 삭제하려면 해당 인스턴스의 check box을 선택하고 Delete 버튼을 클릭합니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

구성된 각 인스턴스에 대해 다음 표에 설명된 정보가 화면에 표시됩니다.

Table 90. MST 구성

필드	설명
Bridge Identifier	선택한 MST 인스턴스의 브리지 식별자입니다. 브리지 우선순위와 브리지의 기본 MAC 주소를 사용하여 구성됩니다.
Time Since Topology Change	선택한 MST 인스턴스의 토폴로지가 마지막으로 변경된 이후 n초가 경과한 시간입니다.
Topology Change Count	선택한 MST 인스턴스에 대해 토폴로지가 변경된 횟수입니다.
Topology Change	선택한 MST 인스턴스에 할당된 포트에서 토폴로지 변경이 진행 중인지 여부를 나타내는 스위치의 토폴로지 변경 매개변수 값입니다. True 또는 False인 경우 값을 취합니다.
Designated Root	루트 브리지의 브리지 식별자입니다. 브리지 우선순위와 브리지의 기본 MAC 주소로 구성됩니다.
Root Path Cost	이 MST 인스턴스의 지정 루트에 대한 경로 비용입니다.
Root PortIdentifier	이 MST 인스턴스의 지정 루트에 액세스하기 위한 포트입니다.

스패닝 트리 MST 포트 상태 보기

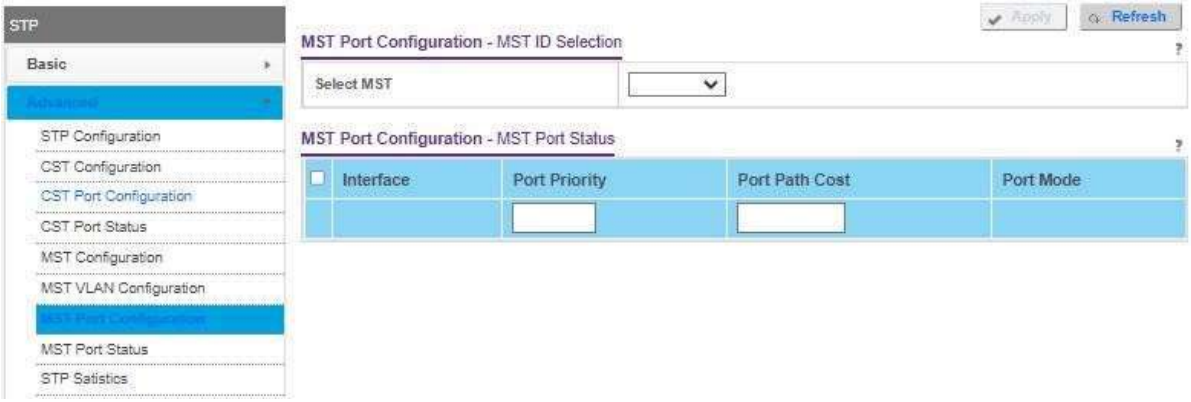
스위치의 특정 포트에 대한 다중 스패닝 트리(MST) 설정을 구성하고 표시할 수 있습니다.

DOT1S에 심각한 오류 조건이 발생하면 포트는 진단적으로 비활성화(D-Disable)될 수 있습니다. 가장 일반적인 원인은 DOT1S 소프트웨어에 BPDU 플러딩이 발생하는 경우입니다. 플러딩 기준은 DOT1S가 3초 간격으로 15개 이상의 BPDU를 수신하는 것입니다. DOT1S D-Disable의 다른 원인은 극히 드뭅니다.

- **스패닝 트리 MST 포트 상태를 보려면:**

Switching > STP > Advanced > MST Port Status.

1.5 cm



Note: 스위치에 MST 인스턴스가 구성되지 않은 경우 화면에 No MSTs Available 메시지가 표시되고 다음 필드 설명 테이블에 표시된 필드가 표시되지 않습니다.

1. MST ID를 이용하여 기존 MST 인스턴스 중 하나의 MST 인스턴스를 선택합니다.
2. Interface를 사용하여 선택한 MST 인스턴스와 연결된 VLAN과 연결된 물리적 또는 포트 채널 인터페이스 중 하나를 선택합니다.
3. Port Priority를 사용하여 선택한 MST 인스턴스 내의 특정 포트에 대한 우선 순위를 지정합니다.

   포트 우선순위는 16의 배수로 설정됩니다. 예를 들어 우선순위를 0~15 사이의 값으로 설정하려고 하면 0으로 설정됩니다. 16~(2*) 사이의 값으로 설정하려고 하면 0으로 설정됩니다. 16-1) 16으로 설정되어 있습니다.

4. Port Path Cost을 사용하여 선택한 MST 인스턴스의 지정된 포트에 대한 경로 비용을 새 값으로 설정합니다.

   1~200000000 범위의 값을 사용합니다.

5. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표에서는 Spanning Tree CST Configuration(스패닝 트리 CST 구성) 화면에 표시되는 읽기 전용 MST 포트 구성 정보에 대해 설명합니다.

Table 91. MST 포트 상태

필드	설명
Auto Calculated Port Path Cost	경로 비용이 자동으로 계산되는지(활성화) 또는 계산되지 않는지(비활성화)를 표시합니다. 포트 경로 비용에 대해 구성된 값이 0인 경우 경로 비용은 포트의 링크 속도를 기준으로 계산됩니다.

1.5 cm

Port ID	선택한 MST 인스턴스 내에서 지정된 포트에 대한 포트 식별자입니다. 포트 우선순위와 포트의 인터페이스 번호로 구성됩니다.
Port Uptime Since Last Clear Counters	카운터가 마지막으로 지워진 이후의 시간이 일, 시, 분, 초로 표시됩니다.
Port Mode	스패닝 트리 프로토콜(Spanning Tree Protocol) 관리 모드는 포트 또는 포트 채널과 연결됩니다. 가능한 값은 활성화 또는 비활성화입니다.
Port Forwarding State	이 포트의 전달 상태입니다.
Port Role	활성화된 각 MST 브리지 포트에는 각 스패닝 트리에 대한 포트 역할이 할당됩니다. 포트 역할은 루트 포트, 지정된 포트, 대체 포트, 백업 포트, 마스터 포트 또는 비활성화된 포트 값 중 하나입니다.
Designated Root	선택한 MST 인스턴스에 대한 루트 브리지입니다. 브리지 우선순위와 브리지의 기본 MAC 주소를 사용하여 구성됩니다.
Designated Cost	지정된 포트가 LAN에 제공하는 경로 비용입니다.
Designated Bridge	지정된 포트가 있는 브리지의 브리지 식별자입니다. 브리지 우선순위와 브리지의 기본 MAC 주소를 사용하여 구성됩니다.
Designated Port	LAN에 가장 낮은 비용을 제공하는 지정 브리지의 포트 식별자입니다. 포트 우선순위와 포트의 인터페이스 번호로 구성됩니다.

STP 통계 보기

각 포트에서 전송 및 수신되는 BPDU(브리지 프로토콜 데이터 단위)의 수와 유형에 대한 정보를 볼 수 있습니다.

- **To view Spanning Tree statistics:**

Switchi 스패닝 트리 통계를 보려면:ng > STP > Advanced > STP Statistics.

STP Satistics - Status

Interface	STP BPDUs Received	STP BPDUs Transmitted	RSTP BPDUs Received	RSTP BPDUs Transmitted	MSTP BPDUs Received	MSTP BPDUs Transmitted
0/1	0	0	0	0	0	0
0/2	0	0	0	0	0	0
0/3	0	0	0	0	0	0
0/4	0	0	0	0	0	0
0/5	0	0	0	11778	0	0
0/6	0	0	0	0	0	0
0/7	0	0	0	0	0	0
0/8	0	0	0	0	0	0

스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

1.5 cm

다음 표에서는 STP 통계 화면에서 사용할 수 있는 정보에 대해 설명합니다.

Table 92. STP 통계

필드	설명
Interface	스위치의 물리적 또는 포트 채널 인터페이스 중 하나를 선택합니다.
STP BPDUs Received	선택한 포트에서 수신된 STP BPDU 수입니다.
STP BPDUs Transmitted	선택한 포트에서 전송된 STP BPDU 수입니다.
RSTP BPDUs Received	선택한 포트에서 수신된 RSTP BPDU 수입니다.
RSTP BPDUs Transmitted	선택한 포트에서 전송된 RSTP BPDU 수입니다.
MSTP BPDUs Received	선택한 포트에서 수신된 MSTP BPDU 수입니다.
MSTP BPDUs Transmitted	선택한 포트에서 전송된 MSTP BPDU 수입니다.

멀티캐스트

멀티캐스트 IP 트래픽은 호스트 그룹으로 향하는 트래픽입니다. 호스트 그룹은 224.0.0.0에서 239.255.255.255 범위의 클래스 D IP 주소로 식별됩니다.

MFDB 테이블 보기

멀티캐스트 전달 데이터베이스는 모든 활성 멀티캐스트 주소 항목에 대한 포트 멤버십 정보를 보유합니다. 항목의 키는 VLAN ID와 MAC 주소 쌍으로 구성됩니다. 항목에는 둘 이상의 프로토콜에 대한 데이터가 포함될 수 있습니다.

- **MFDB 테이블을 보려면:**

Switching > Multicast > MFDB > MFDB Table.

1. MAC 주소로 검색을 사용하여 MAC 주소를 입력하세요.

   6개의 2자리 16진수 숫자를 콜론으로 구분하여 입력하세요(예: 00:01:23:43:45:67).

2. GO 버튼을 클릭하세요.

   주소가 있으면 해당 항목이 표시됩니다. 정확하게 일치해야 합니다.

1.5 cm

Table 96. MFDB 테이블

필드	설명
MAC Address	데이터를 요청한 멀티캐스트 MAC 주소입니다.
VLAN ID	멀티캐스트 MAC 주소와 관련된 VLAN ID입니다.
Type	항목의 유형이 표시됩니다. 정적 항목은 최종 사용자가 구성한 항목입니다. 학습 프로세스나 프로토콜의 결과로 동적 항목이 테이블에 추가됩니다.
Component	이는 멀티캐스트 전달 데이터베이스에서 이 항목을 담당하는 구성 요소입니다. 가능한 값은 IGMP 스누핑, GMRP, 정적 필터링 및 MLD 스누핑입니다.
Description	이 멀티캐스트 테이블 항목에 대한 텍스트 설명입니다. 가능한 값은 관리 구성, 네트워크 구성 및 네트워크 지원입니다.
Forwarding Interfaces	결과 전달 목록은 모든 전달 인터페이스를 결합하고 정적 필터링 인터페이스로 나열된 인터페이스를 제거하여 파생됩니다.

MFDB 통계 보기

➢ **MFDB 통계를 보려면:**

Switching > Multicast > MFDB > MFDB Statistics.

다음 표에서는 MFDB 통계 필드에 대해 설명합니다.

Table 97. MFDB 통계

필드	설명
Max MFDB Table Entries	멀티캐스트 전달 데이터베이스 테이블이 보유할 수 있는 최대 항목 수입니다.
Most MFDB Entries Since Last Reset	마지막 재설정 이후 멀티캐스트 전달 데이터베이스 테이블에 있었던 최대 항목 수입니다. 이 값은 MFDB 최고 수위 표시라고도 합니다.
Current Entries	멀티캐스트 전달 데이터베이스 테이블의 현재 항목 수입니다.

IGMP 스누핑

IGMP(인터넷 그룹 관리 프로토콜) 스누핑은 스위치가 스위치에서 멀티캐스트 트래픽을 지능적으로 전달할 수 있도록 하는 기능입니다. 멀티캐스트 IP 트래픽은 호스트 그룹으로 향하는 트래픽입니다. 호스트 그룹은 클래스 D IP 주소로 식별됩니다.

224.0.0.0 ~ 239.255.255.255. 스위치는 IGMP 쿼리 및 보고 메시지를 기반으로 멀티캐스트 트래픽을 요청하는 포트에만 트래픽을 전달합니다. 이렇게 하면 스위치가 트래픽을 모든 포트에 브로드캐스팅하여 네트워크 성능에 영향을 미칠 수 있는 것을 방지할 수 있습니다.

동일한 공유 미디어에 너무 많은 장치를 배치하는 것을 방지하기 위해 기존 이더넷 네트워크를 여러 네트워크 세그먼트로 분리할 수 있습니다. 브리지와 스위치는 이러한 세그먼트를 연결합니다. 브로드캐스트 또는 멀티캐스트 대상 주소가 있는 패킷이 수신되면 스위치는 IEEE MAC 브리지 표준에 따라 복사본을 나머지 네트워크 세그먼트 각각에 전달합니다. 결국, 패킷은 네트워크에 연결된 모든 노드에 액세스할 수 있게 됩니다.

이 접근 방식은 연결된 모든 노드에서 보거나 처리하도록 의도된 브로드캐스트 패킷에 적합합니다. 그러나 멀티캐스트 패킷의 경우 이 접근 방식은 특히 패킷이 소수의 노드만을 대상으로 하는 경우 네트워크 대역폭을 덜 효율적으로 사용할 수 있습니다. 패킷은 패킷을 수신하는 노드가 없는 네트워크 세그먼트로 플러딩됩니다. 노드는 요청되지 않은 그룹 주소로 주소가 지정된 패킷을 필터링하기 위해 처리 오버헤드를 거의 발생시키지 않지만 멀티캐스트 패킷이 플러딩되는 기간 동안 공유 미디어에 새 패킷을 전송할 수 없습니다. 대역폭 낭비 문제는 예를 들어 전이중 링크에서와 같이 LAN 세그먼트가 공유되지 않을 때 더욱 악화됩니다.

스위치가 IGMP 패킷을 스누핑하도록 허용하는 것은 이 문제를 해결하기 위한 창의적인 노력입니다. 스위치는 네트워크 전체에 전달되는 IGMP 패킷의 정보를 사용하여 그룹 주소로 전달되는 패킷을 수신하는 세그먼트를 결정합니다.

IGMP 스누핑 구성

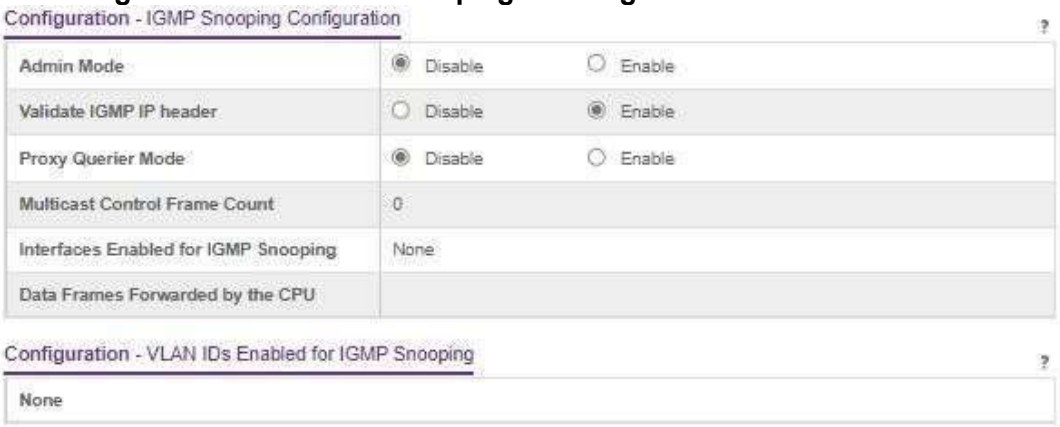
멀티캐스트 트래픽에 대한 전달 목록을 작성하는 데 사용되는 IGMP 스누핑에 대한 매개변수를 구성할 수 있습니다.

Note: 이 화면의 데이터를 변경하려면 읽기/쓰기 권한이 있는 관리자로

로그인해야 합니다.

➢ **IGMP 스누핑을 구성하려면:**

Switching > Multicast > IGMP Snooping > Configuration.



1. Admin Mode의 Enable 또는 Disable 라디오 버튼을 선택합니다.

   이는 스위치에 대한 IGMP 스누핑을 위한 관리 모드를 지정합니다. 기본값은 Disable입니다.

2. Validate IGMP IP header 옵션을 사용하여 모든 IGMP 버전에 대한 헤더 유효성 검사를 Enable하거나 Disable합니다.

   IGMP IP 헤더 확인이 활성화된 경우 IGMP IP 헤더는 라우터 경고 옵션, ToS 및 TTL을 확인합니다. 기본값은 Enable입니다.

3. Proxy Querier 모드의 Enable 또는 Disable 라디오 버튼을 선택합니다.

   이는 시스템에서 IGMP 프록시 쿼리기를 활성화하거나 비활성화합니다. 비활성화된 경우 소스 IP가 0.0.0.0인 IGMP 프록시 쿼리는 IGMP 탈퇴 패킷에 대한 응답으로 전송되지 않습니다. 기본값은 Enable입니다.

4. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

다음 표는 글로벌 IGMP 스누핑 상태 및 통계에 대한 정보를 화면에 표시합니다.

Table 98. IGMP 스누핑 구성

필드	설명
Multicast Control Frame Count	CPU에서 처리되는 멀티캐스트 제어 프레임 수입니다.

1.5 cm

Interfaces Enabled for IGMP Snooping	현재 IGMP 스누핑이 활성화된 모든 인터페이스 목록입니다.
VLAN IDs Enabled For IGMP Snooping	IGMP 스누핑이 활성화된 VLAN ID를 표시합니다.

인터페이스에 대한 IGMP 스누핑 구성

➢ **인터페이스에 대한 IGMP 스누핑을 구성하려면:**

Switching > Multicast > IGMP Snooping > Interface Configuration.

Interface Configuration - IGMP Snooping Interface Configuration

Interface	Admin Mode	Group Membership Interval (2-3600 secs)	Max Response Time (1-25 secs)	Present Expiration Time (0-3600 secs)	Fast Leave Admin Mode
0/1	Disable	260	10	0	Disable
0/2	Disable	260	10	0	Disable
0/3	Disable	260	10	0	Disable
0/4	Disable	260	10	0	Disable
0/5	Disable	260	10	0	Disable
0/6	Disable	260	10	0	Disable
0/7	Disable	260	10	0	Disable
0/8	Disable	260	10	0	Disable

화면에는 모든 물리적 인터페이스, VLAN 및 LAG 인터페이스가 나열됩니다.

1. Interface check box을 사용하여 인터페이스를 선택합니다.
2. Admin Mode 필드에서 Disable 또는 Enable를 선택합니다.

   스위치의 IGMP 스누핑을 위해 선택한 인터페이스의 인터페이스 모드를 지정합니다. 기본값은 Disable입니다.

3. Group Membership Interval을 사용하여 스위치가 그룹에서 해당 인터페이스를 삭제하기 전에 특정 인터페이스의 특정 그룹에 대한 보고서를 기다리는 시간을 지정합니다.

   1~3600초 사이의 값을 입력하세요. 기본값은 260초입니다.

4. Max Response Time을 사용하여 해당 인터페이스의 특정 그룹에 대한 보고서를 수신하지 못했기 때문에 스위치가 인터페이스에 쿼리를 보낸 후 대기하는 시간을 지정합니다.

   1보다 크거나 같고 그룹 구성원 간격(초)보다 작은 값을 입력하십시오. 기본값은 10초입니다. 구성된 값은 그룹 멤버십 간격보다 작아야 합니다.

5. Present Expiration Time을 사용하여 스위치가 멀티캐스트 라우터가 연결된 인터페이스

1.5 cm

목록에서 인터페이스를 제거하기 전에 인터페이스에 대한 쿼리를 수신하기 위해 기다리는 시간을 지정합니다.

0~3600초 사이의 값을 입력하세요. 기본값은 0초입니다. 0 값은 무한 시간 제한, 즉 만료 없음을 나타냅니다.

6. 빠른 나가기 관리 모드를 사용하여 특정 인터페이스에 대한 빠른 나가기 모드를 선택합니다.

   기본값은 Disable입니다.

7. Proxy Querier 모드를 사용하여 특정 인터페이스에 대한 프록시 쿼리기 모드를 선택합니다.

   비활성화된 경우 소스 IP 0.0.0.0을 사용하는 IGMP 프록시 쿼리는 IGMP 탈퇴 패킷에 대한 응답으로 전송되지 않습니다. 기본값은 Enable입니다.

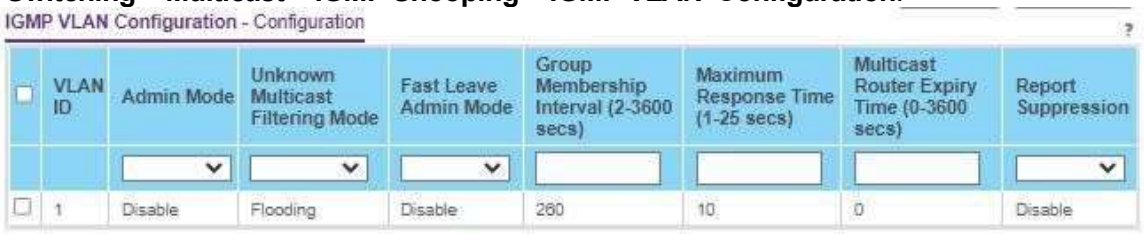
8. Apply 버튼을 클릭합니다

   설정이 스위치에 적용됩니다. 구성 변경 사항은 즉시 적용됩니다.

VLAN에 대한 IGMP 스누핑 구성

➢ **VLAN에 대한 IGMP 스누핑 설정을 구성하려면:**

Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration.



1. VLAN에서 IGMP 스누핑을 활성화하려면 VLAN ID를 입력하고 IGMP 스누핑 값을 구성합니다.
   - Admin Mode를 사용하여 지정된 VLAN ID에 대한 IGMP 스누핑을 Enable하거나 Disable합니다.
   - Fast Leave Admin Mode를 사용하여 지정된 VLAN ID에 대한 IGMP 스누핑 빠른 나가기 모드를 Enable하거나 Disable합니다.
   - Group Membership Interval을 사용하여 지정된 VLAN ID에 대한 IGMP 스누핑의 그룹 멤버십 간격 값을 설정합니다. 유효한 범위는 최대 응답 시간 + 1~3600초입니다.
   - 지정된 VLAN ID에 대한 IGMP 스누핑의 최대 응답 시간 값을 설정하려면 Maximum

1.5 cm

Response Time을 사용합니다. 유효한 범위는 1부터 그룹 구성원 간격 - 1까지입니다. 해당 값은 그룹 구성원 간격 값보다 커야 합니다.

- Multicast Router Expiry Time을 사용하여 지정된 VLAN ID에 대한 IGMP 스누핑의 멀티캐스트 라우터 만료 시간 값을 설정합니다. 유효한 범위는 0~3600초입니다.
- Report Suppression Mode를 사용하여 지정된 VLAN ID에 대한 IGMP 스누핑 보고서 억제 모드를 활성화하거나 비활성화합니다. IGMP 스누핑 보고서 억제를 사용하면 레이어 3 멤버십 테이블을 구축하여 멀티캐스트 호스트가 보낸 IGMP 보고서를 억제할 수 있으므로 멀티캐스트 트래픽을 수신하기 위해 꼭 필요한 보고서만 IGMP 라우터에 보냅니다. 결과적으로 IGMP 라우터로 전송되는 멀티캐스트 보고서 트래픽이 줄어듭니다.
- 지정된 VLAN ID에 대한 Proxy Querier 모드를 Enable하거나 Disable합니다. 프록시 쿼리기 모드가 비활성화된 경우 소스 IP가 0.0.0.0인 IGMP 프록시 쿼리는 IGMP 탈퇴 패킷에 대한 응답으로 전송되지 않습니다. 기본값은 Enable입니다.

2. VLAN에서 IGMP 스누핑을 비활성화하고 목록에서 제거하려면:
   a. VLAN ID 옆의 check box을 선택합니다.
   b. Delete 버튼을 클릭합니다
3. VLAN에 대한 IGMP 스누핑 설정을 수정하려면:
   a. VLAN ID 옆의 check box을 선택합니다.
   b. 값을 업데이트합니다
   c. Apply 버튼을 클릭합니다

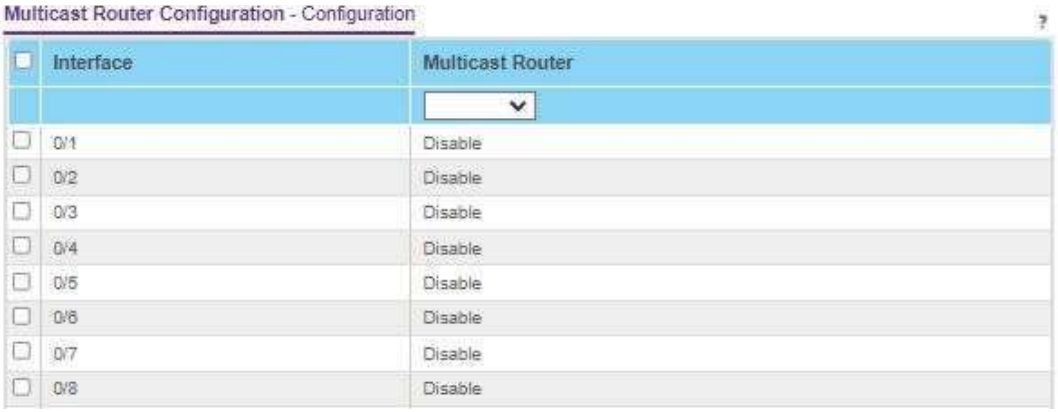
   설정이 스위치로 전송됩니다.

멀티캐스트 라우터 구성

멀티캐스트 라우터가 연결된 인터페이스로 인터페이스를 구성할 수 있습니다. 스위치에 의해 스누핑된 모든 IGMP 패킷은 이 인터페이스에서 연결할 수 있는 멀티캐스트 라우터로 전달됩니다. 스위치가 멀티캐스트 라우터를 자동으로 감지하고 이에 따라 IGMP 패킷을 전달하므로 대부분의 경우 구성이 필요하지 않습니다. 멀티캐스트 라우터가 복잡한 네트워크의 스위치로부터 항상 IGMP 패킷을 수신하도록 하려는 경우에만 필요합니다.

➢ **멀티캐스트 라우터를 구성하려면:**

Switching > Multicast > IGMP Snooping > Multicast Router Configuration.



1. Interface를 사용하여 물리적 인터페이스를 선택합니다.
2. Multicast Router 필드에서 Enable 또는 Disable를 선택합니다.
3. Apply 버튼을 클릭합니다

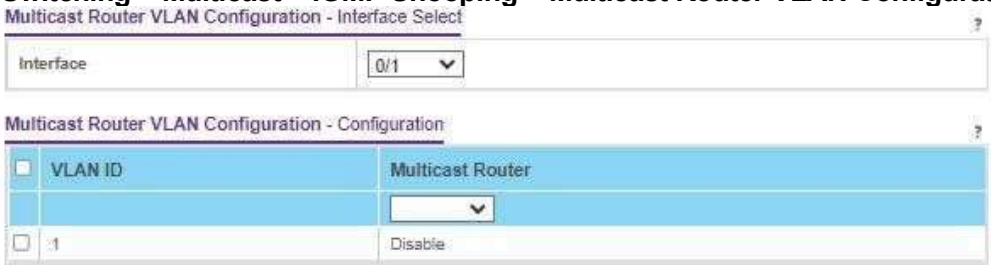
   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

멀티캐스트 라우터 VLAN 구성

VLAN ID(<VLANID>)에서 들어오는 스누핑된 IGMP 패킷만 이 인터페이스에 연결된 멀티캐스트 라우터로 전달하도록 인터페이스를 구성할 수 있습니다. 스위치가 자동으로 멀티캐스트 라우터를 감지하고 이에 따라 IGMP 패킷을 전달하므로 대부분의 경우 구성이 필요하지 않습니다. 멀티캐스트 라우터가 복잡한 네트워크의 스위치로부터 항상 IGMP 패킷을 수신하도록 하려는 경우에만 필요합니다.

➢ **멀티캐스트 라우터 VLAN을 구성하려면:**

Switching > Multicast > IGMP Snooping > Multicast Router VLAN Configuration.



1. Interface를 사용하여 인터페이스를 선택합니다.
2. VLAN ID를 사용하여 VLAN ID를 선택합니다.

3. Multicast Router 필드에서 Enable 또는 Disable를 선택합니다.
4. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

IGMP 스누핑 쿼리기 개요

IGMP 스누핑을 사용하려면 하나의 중앙 스위치 또는 라우터가 정기적으로 네트워크의 모든 최종 장치에 쿼리하여 멀티캐스트 멤버십을 알려야 합니다. 이 중앙 장치는 IGMP 쿼리기입니다. IGMP 보고서로 알려진 IGMP 쿼리 응답은 포트별로 현재 멀티캐스트 그룹 구성원 자격으로 스위치를 업데이트합니다. 스위치가 적시에 업데이트된 멤버십 정보를 수신하지 못하면 최종 장치가 있는 포트로의 멀티캐스트 전달을 중지합니다.

네트워크 및 VLAN에서 별도로 IGMP 스누핑 쿼리기에 대한 정보를 구성하고 표시할 수 있습니다.

IGMP 스누핑 쿼리기 구성

IGMP 스누핑 쿼리기에 대한 매개변수를 구성할 수 있습니다. 읽기/쓰기 액세스 권한이 있는 사용자만 이 화면의 데이터를 변경할 수 있습니다.

➢ **IGMP 스누핑 쿼리어 설정을 구성하려면:**

Switching > Multicast > IGMP Snooping > Querier Configuration.

Querier Configuration - IGMP Snooping Querier Configuration

Querier Admin Mode	◉ Disable ○ Enable
Querier IP Address	0.0.0.0
IGMP Version	2
Query Interval(secs)	60 (1-1800)
Query Expiry Interval(secs)	125 (60-300)
VLANs Enabled for IGMP Snooping Querier	

1. Querier Admin Mode를 사용하여 스위치에 대한 IGMP 스누핑을 위한 관리 모드를 선택합니다.

   기본값은 Disable입니다.

2. Snooping Querier IP Address 필드에 IP 주소를 입력합니다.

이는 정기적인 IGMP 쿼리에서 소스 주소로 사용될 스누핑 쿼리어 주소를 지정합니다. 이 주소는 쿼리가 전송되는 VLAN에 주소가 구성되어 있지 않을 때 사용됩니다.

3. IGMP Version을 사용하여 정기적인 IGMP 쿼리에 사용되는 IGMP 프로토콜 버전을 지정합니다.

   범위는 1~2입니다. 기본값은 2입니다.

4. Query Interval(secs)을 사용하여 스누핑 쿼리 수행자가 보낸 주기적 쿼리 사이의 시간 간격(초)을 지정합니다.

   쿼리 간격은 1~1800 범위의 값이어야 합니다. 기본값은 60입니다.

5. Querier Expiry Interval(secs)을 사용하여 마지막 쿼리기 정보가 제거된 후의 시간 간격(초)을 지정합니다.

   쿼리 실행자 만료 간격은 60~300 범위의 값이어야 합니다. 기본값은 125입니다.

6. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

   화면에는 IGMP 스누핑 쿼리기에 대해 활성화된 VLAN ID가 표시됩니다.

VLAN에 대한 IGMP 스누핑 쿼리기 구성

네트워크의 VLAN과 함께 사용할 IGMP 쿼리기를 구성할 수 있습니다.

➢ **쿼리어 VLAN 설정을 구성하려면:**

Switching > Multicast > IGMP Snooping > Querier VLAN Configuration.

Querier VLAN Configuration - IGMP Snooping

	VLAN ID	Admin Mode	Querier Election Participate Mode	Querier VLAN Address	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time
☐	1	Disable	Disable	0.0.0.0	Disabled	2			

1. IGMP 스누핑을 위한 새 VLAN ID를 생성하려면 VLAN ID 필드에서 New Entry을 선택하고 다음 필드를 완성합니다.

   사전 구성 가능한 스누핑 쿼리어 매개변수를 설정할 수도 있습니다.

   - **VLAN ID**. IGMP 스누핑 쿼리기를 활성화할 VLAN ID입니다.
   - **Querier Election Participate Mode**. 쿼리어 참여 모드를 Enable하거나 Disable합니다.

- **Disabled**. VLAN에서 동일한 버전의 다른 쿼리어를 발견하면 스누핑 쿼리어는 쿼리어가 없는 상태로 이동합니다.
- **Enabled**. 스누핑 쿼리어는 쿼리어 선택에 참여합니다. 이 경우 가장 적은 IP 주소가 해당 VLAN에서 쿼리어로 작동합니다. 다른 쿼리자는 쿼리자가 아닌 상태로 이동합니다.

- **Snooping Querier VLAN Address**. 지정된 VLAN에서 전송되는 주기적인 IGMP 쿼리에서 소스 주소로 사용할 스누핑 쿼리어 IP 주소를 지정합니다.

2. Apply 버튼을 클릭합니다

   설정이 스위치에 적용됩니다. 구성 변경 사항이 즉시 적용됩니다.

3. VLAN에서 스누핑 쿼리어를 비활성화하려면 VLAN ID를 선택하고 Delete 버튼을 클릭합니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 99. 쿼리어 VLAN 구성

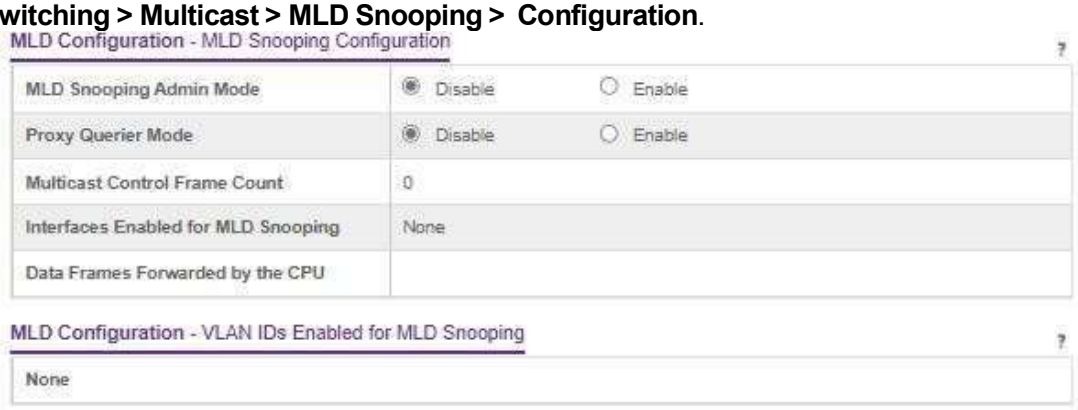
필드	설명
Operational State	VLAN에서 IGMP 스누핑 쿼리기의 작동 상태입니다. 다음 상태 중 하나일 수 있습니다. • **Querier**: 스누핑 스위치는 VLAN의 쿼리어입니다. 스누핑 스위치는 구성된 쿼리어 쿼리 간격과 동일한 시간 간격으로 정기적인 쿼리를 보냅니다. 스누핑 스위치가 VLAN에서 더 나은 쿼리어를 찾으면 비쿼리어 모드로 전환됩니다. • **Non-Querier**: 스누핑 스위치는 VLAN에서 innNon-querier 모드입니다. 쿼리어 만료 간격 타이머가 만료되면 스누핑 스위치는 쿼리어 모드로 전환됩니다. • **Disabled**: 스누핑 쿼리어는 VLAN에서 작동하지 않습니다. 스누핑 쿼리기는 VLAN에서 IGMP 스누핑이 작동하지 않거나 쿼리기 주소가 구성되지 않았거나 네트워크 관리 주소도 구성되지 않은 경우 비활성화 모드로 전환됩니다.
Operational Version	쿼리어의 작동 가능한 IGMP 프로토콜 버전입니다.
Last Querier Address	VLAN에서 쿼리가 스누핑된 마지막 쿼리기의 IP 주소입니다.
Last Querier Version	VLAN에서 쿼리가 스누핑된 마지막 쿼리기의 IGMP 프로토콜 버전입니다.
Operational Max Response Time	스누핑 쿼리어가 보낸 쿼리에 사용할 최대 응답 시간을 표시합니다.

MLD 스누핑 구성

멀티캐스트 트래픽에 대한 전달 목록을 작성하는 데 사용되는 MLD 스누핑에 대한 매개변수를 구성할 수 있습니다. 읽기/쓰기 액세스 권한이 있는 사용자만 이 화면의 데이터를 변경할 수 있습니다.

➢ **MLD 스누핑을 구성하려면:**

Switching > Multicast > MLD Snooping > Configuration.



1. MLD Snooping Admin Mode를 사용하여 스위치에 대한 MLD 스누핑 관리 모드를 선택합니다.

   기본값은 Disable입니다.

2. Proxy Querier Mode의 Enable 또는 Disable 라디오 버튼을 선택합니다.

   이는 시스템에서 MLD 프록시 쿼리기를 활성화하거나 비활성화합니다. 비활성화된 경우 소스 IP가 0::0인 MLD 프록시 쿼리는 MLD 탈퇴 패킷에 대한 응답으로 전송되지 않습니다. 활성화된 경우 MLD 프록시 쿼리가 전송됩니다. 기본값은 Enable입니다.

3. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표에서는 구성할 수 없는 MLD 스누핑 구성 필드에 대해 설명합니다.

Table 100. MLD 스누핑 구성

필드	설명
Multicast Control Frame Count	CPU에서 처리되는 멀티캐스트 제어 프레임 수입니다.

Interfaces Enabled for MLD Snooping	현재 MLD 스누핑이 활성화된 모든 인터페이스 목록입니다.
VLAN IDs Enabled For MLD Snooping	MLD 스누핑이 활성화된 VLAN ID를 표시합니다.

MLD 스누핑 인터페이스 구성

➢ **MLD 스누핑 인터페이스를 구성하려면:**

Switching > Multicast > MLD Snooping > Interface Configuration.

Interface Configuration - MLD Snooping Interface Configuration

Interface	Admin Mode	Group Membership Interval (2-3600 secs)	Max Response Time (1-25 secs)	Present Expiration Time (0-3600 secs)	Fast Leave Admin Mode
0/1	Disable	260	10	0	Disable
0/2	Disable	260	10	0	Disable
0/3	Disable	260	10	0	Disable
0/4	Disable	260	10	0	Disable
0/5	Disable	260	10	0	Disable
0/6	Disable	260	10	0	Disable
0/7	Disable	260	10	0	Disable
0/8	Disable	260	10	0	Disable

모든 물리적, VLAN 및 LAG 인터페이스가 표시됩니다.

1. Interface check box을 사용하여 인터페이스를 선택합니다.
2. Admin Mode를 사용하여 스위치의 MLD 스누핑을 위해 선택한 인터페이스에 대한 인터페이스 모드를 선택합니다.

   기본값은 비활성화입니다.
3. Group Membership Interval(secs)을 사용하여 스위치가 그룹에서 해당 인터페이스를 삭제하기 전에 특정 인터페이스의 특정 그룹에 대한 보고서를 기다리는 시간을 지정합니다.

   유효한 범위는 2~3600초입니다. 구성된 값은 최대 응답 시간보다 커야 합니다. 기본값은 260초입니다.
4. Max Response Time(secs)을 사용하여 해당 인터페이스의 특정 그룹에 대한 보고서를 수신하지 못했기 때문에 스위치가 인터페이스에 쿼리를 보낸 후 기다리는 시간을 지정합니다.

   1보다 크거나 같고 그룹 멤버십 간격(초)보다 작은 값을 입력하십시오. 기본값은 10초입니다. 구성된 값은 그룹 멤버십 간격보다 작아야 합니다.

5. Present Expiration Time을 사용하여 스위치가 멀티캐스트 라우터가 연결된 인터페이스 목록에서 인터페이스를 제거하기 전에 인터페이스에 대한 쿼리를 수신하기 위해 기다리는 시간을 지정합니다.

   0~3600초 사이의 값을 입력하세요. 기본값은 0초입니다. 0 값은 무한 시간 제한, 즉 만료가 없음을 나타냅니다.

6. Fast Leave Admin Mode를 사용하여 특정 인터페이스에 대한 빠른 나가기 모드를 선택합니다.

   기본값은 Disable입니다.

7. Proxy Querier Mode를 선택하여 시스템에서 MLD 프록시 쿼리기를 Enable하거나 Disable합니다.

   비활성화된 경우 소스 IP가 0::0인 MLD 프록시 쿼리는 MLD 탈퇴 패킷에 대한 응답으로 전송되지 않습니다. 활성화된 경우 MLD 프록시 쿼리가 전송됩니다. 기본값은 Enable입니다.

MLD VLAN 설정 구성

➢ **MLD VLAN 설정을 구성하려면:**

Switching > Multicast > MLD Snooping > MLD VLAN Configuration.

MLD VLAN Configuration - Configuration

	VLAN ID	Admin Mode	Unknown Multicast Filtering Mode	Fast Leave Admin Mode	Group Membership Interval (2-3600 secs)	Maximum Response Time (1-25 secs)	Multicast Router Expiry Time (0-3600 secs)	Report Suppression
☐	1	Disable	Flooding	Disable	260	10	0	Disable

1. VLAN ID를 사용하여 MLD 스누핑이 활성화된 VLAN ID를 설정합니다.
2. Admin Mode를 사용하여 지정된 VLAN ID에 대해 MLD 스누핑을 활성화합니다.
3. Fast Leave Admin Mode를 사용하여 지정된 VLAN ID에 대해 MLD 스누핑 빠른 나가기 모드를 Enable하거나 Disable합니다.
4. Group Membership Interval을 사용하여 지정된 VLAN ID에 대한 MLD 스누핑의 그룹 멤버십 간격 값을 설정합니다.

   유효한 범위는 (최대 응답 시간 + 1) ~ 3600입니다.

5. Maximum Response Time을 사용하여 지정된 VLAN ID에 대한 MLD 스누핑의 최대 응답 시간 값을 설정합니다.

유효한 범위는 1부터 (그룹 구성원 간격 -1)까지입니다. 해당 값은 그룹 구성원 간격 값보다 작아야 합니다.

6. 멀티캐스트 라우터 만료 시간을 사용하여 지정된 VLAN ID에 대한 MLD 스누핑의 멀티캐스트 라우터 만료 시간 값을 설정합니다. 유효한 범위는 0~3600입니다.
7. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다.

인터페이스에서 멀티캐스트 라우터 활성화 또는 비활성화

➢ **인터페이스에서 멀티캐스트 라우터를 활성화하거나 비활성화하려면:**

Switching > Multicast > MLD Snooping > Multicast Router Configuration.

Multicast Router Configuration - MLD Configuration

Interface	Multicast Router
0/1	Disable
0/2	Disable
0/3	Disable
0/4	Disable
0/5	Disable
0/6	Disable
0/7	Disable
0/8	Disable

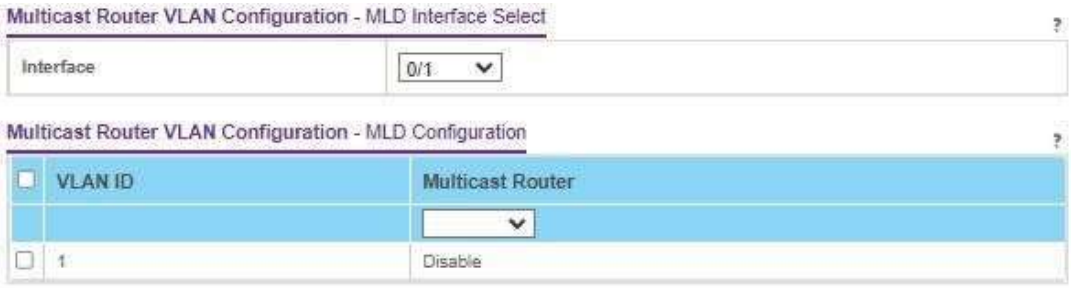
1. **Interface**: 인터페이스를 선택합니다.
2. Multicast Router를 사용하여 선택한 인터페이스에서 멀티캐스트 라우터를 Enable하거나 Disable합니다.
3. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다.

멀티캐스트 라우터 VLAN 설정 구성

➢ **멀티캐스트 라우터 VLAN 설정을 구성하려면:**

Switching > Multicast > MLD Snooping > Multicast Router VLAN Configuration.



1. Interface를 사용하여 인터페이스를 선택합니다.
2. VLAN ID를 사용하여 VLAN ID를 선택합니다.
3. Multicast Router를 사용하여 VLAN ID에 대한 멀티캐스트 라우터를 Enable하거나 Disable합니다.
4. Apply 버튼을 클릭합니다

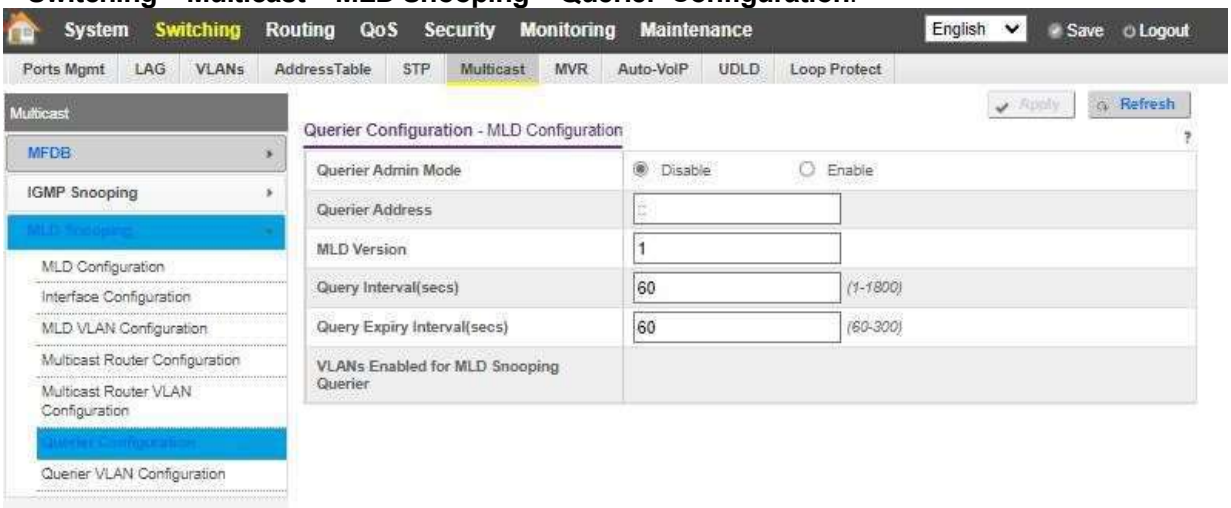
   업데이트된 구성이 스위치로 전송됩니다.

MLD 스누핑 쿼리기 구성

MLD 스누핑 쿼리기에 대한 매개변수를 구성할 수 있습니다. 읽기/쓰기 액세스 권한이 있는 사용자만 이 화면의 데이터를 변경할 수 있습니다.

➢ **MLD 스누핑 쿼리어를 구성하려면:**

Switching > Multicast > MLD Snooping > Querier Configuration.



1. Querier Amin Mode를 사용하여 스위치에 대한 MLD 스누핑에 대한 관리 모드를 선택합니다.

   기본값은 비활성화입니다.

2. 정기적인 MLD 쿼리에서 소스 주소로 사용할 스누핑 쿼리어 주소를 지정하려면 Querier Address를 사용합니다.

   이 주소는 쿼리가 전송되는 VLAN에 주소가 구성되어 있지 않을 때 사용됩니다. 지원되는 IPv6 형식은 x:x:x:x:x:x:x:x 및 x::x입니다.

3. MLD Version을 사용하여 정기적인 MLD 쿼리에 사용되는 MLD 프로토콜 버전을 지정합니다.
4. Query Interval(secs)을 사용하여 스누핑 쿼리 수행자가 보낸 주기적 쿼리 사이의 시간 간격(초)을 지정합니다.

   쿼리 간격은 1~1800 범위의 값이어야 합니다. 기본값은 60입니다.

5. Querier Expiry Interval(secs)을 사용하여 마지막 쿼리기 정보가 제거된 후의 시간 간격(초)을 지정합니다.

   쿼리 실행자 만료 간격은 60~300 범위의 값이어야 합니다. 기본값은 60입니다.

   화면에는 MLD 스누핑 쿼리기에 대해 활성화된 VLAN ID가 표시됩니다.

MLD 스누핑 쿼리어 VLAN 설정 구성

➢ **MLD 스누핑 쿼리어 VLAN 설정을 구성하려면:**

Switching > Multicast > MLD Snooping > Querier VLAN Configuration.

1. VLAN ID를 사용하여 MLD 스누핑 쿼리기가 관리상 활성화되고 VLAN 데이터베이스에 VLAN이 존재하는 VLAN ID를 선택합니다.
2. Querier Election Participate Mode를 사용하여 선택 모드에서 MLD 스누핑 쿼리어 참여를 Enable하거나 Disable합니다.

   이 모드가 비활성화되면 VLAN에서 동일한 버전의 다른 쿼리어가 감지되면 스누핑 쿼리어가 쿼리어가 아닌 상태로 전환됩니다. 이 모드가 활성화되면 스누핑 쿼리어는 가장 낮은 IP 주소가 쿼리어 선택에서 승리하고 해당 VLAN에서 쿼리어로 작동하는 쿼리어 선택에 참여합니다. 다른 쿼리자는 쿼리자가 아닌 상태로 이동합니다.

3. Querier VLAN Address를 사용하여 지정된 VLAN에서 전송되는 주기적인 MLD 쿼리에서 소스 주소로 사용할 스누핑 쿼리어 주소를 지정합니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 101. 쿼리어 VLAN 구성

필드	설명
Operational State	VLAN에서 MLD 스누핑 쿼리기의 작동 상태입니다. 다음 상태 중 하나일 수 있습니다. • **Querier**: 스누핑 스위치는 VLAN의 쿼리어입니다. 스누핑 스위치는 구성된 쿼리어 쿼리 간격과 동일한 시간 간격으로 정기적인 쿼리를 보냅니다. 스누핑 스위치가 VLAN에서 더 나은 쿼리어를 발견하면 비쿼리어 모드로 이동합니다. • **Non-Querier**: 스누핑 스위치는 VLAN에서 비쿼리어 모드입니다. 쿼리어 만료 간격 타이머가 만료되면 스누핑 스위치는 쿼리어 모드로 전환됩니다. • **Disabled**: 스누핑 쿼리어가 VLAN에서 작동하지 않습니다. 스누핑 쿼리기는 VLAN에서 MLD 스누핑이 작동하지 않거나 쿼리기 주소가 구성되지 않았거나 네트워크 관리 주소도 구성되지 않은 경우 비활성화 모드로 전환됩니다.
Operational Version	쿼리어의 작동 가능한 MLD 프로토콜 버전입니다.
Last Querier Address	VLAN에서 쿼리가 스누핑된 마지막 쿼리기의 IP 주소입니다.
Last Querier Version	VLAN에서 쿼리가 스누핑된 마지막 쿼리기의 MLD 프로토콜 버전입니다.
Operational Max Response Time	스누핑 쿼리어가 보낸 쿼리에 사용할 최대 응답 시간을 표시합니다.

MVR 구성

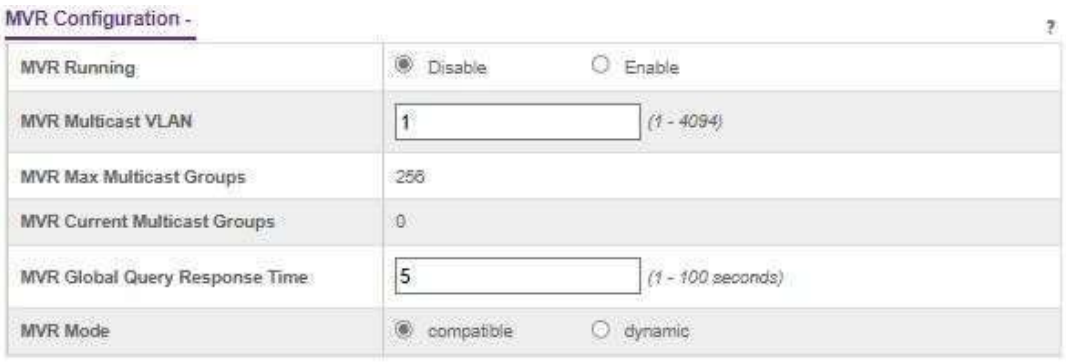
기본, 고급, 그룹, 인터페이스 또는 그룹 멤버십 설정을 구성할 수 있습니다.

기본 MVR 설정 구성

➢ **기본 MVR 설정을 구성하려면:**

Switching > MVR > Basic > MVR Configuration.

U-I-F5010HPA



1. MVR Running을 사용하여 MVR 기능을 Enable하거나 Disable합니다.
   공장 기본값은 비활성화입니다.

2. MVR 멀티캐스트 VLAN을 사용하여 MVR 멀티캐스트 데이터가 수신되는 VLAN을 지정합니다.

   모든 소스 포트는 이 VLAN에 속합니다. 값은 1~4093 범위에서 설정할 수 있습니다.
   기본값은 1입니다.

3. MVR Global Query Response Time을 사용하여 수신기 포트에서 IGMP 보고서
   멤버십을 기다리는 최대 시간을 설정합니다.

   이 시간은 수신자 포트 나가기 처리에만 적용됩니다. IGMP 쿼리가 수신기 포트에서
   전송되면 스위치는 멀티캐스트 그룹 멤버십에서 포트를 제거하기 전에 IGMP 그룹
   멤버십 보고서에 대한 기본 또는 구성된 MVR 쿼리 시간을 기다립니다. 값은 1/10초와
   같습니다. 범위는 1에서 100까지입니다. 공장 기본값은 5/10 또는 1/2입니다.

4. MVR Mode를 사용하여 MVR 작동 모드를 지정합니다.

   가능한 값은 호환 가능 또는 동적입니다. 공장 기본값은 호환 가능합니다.

5. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

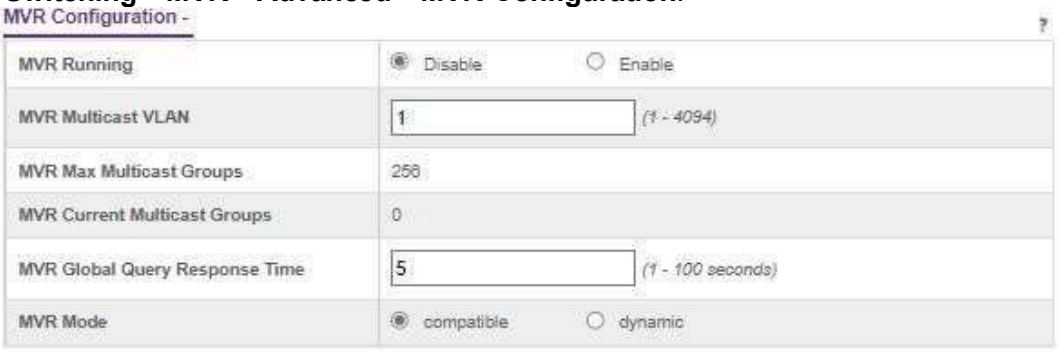
Table 102. MVR 구성

필드	설명
MVR Max Multicast Groups	MVR이 지원하는 최대 멀티캐스트 그룹 수입니다.
MVR Current Multicast Groups	현재 할당된 MVR 그룹의 수를 표시합니다.

고급 MVR 설정 구성

➢ **고급 MVR 설정을 구성하려면:**

Switching > MVR > Advanced > MVR Configuration.



1. MVR Running의 Enable 또는 Disable 라디오 버튼을 선택합니다.

   공장 기본값은 비활성화입니다.

2. MVR Multicast VLAN을 사용하여 MVR 멀티캐스트 데이터가 수신되는 VLAN을 지정합니다.

   모든 소스 포트는 이 VLAN에 속합니다. 값은 1~4094 범위에서 설정할 수 있습니다. 기본값은 1입니다.

3. MVR Global query response time을 사용하여 수신기 포트에서 IGMP 보고서 멤버십을 기다리는 최대 시간을 설정합니다. 이 시간은 수신자 포트 나가기 처리에만 적용됩니다. IGMP 쿼리가 수신기 포트에서 전송되면 스위치는 멀티캐스트 그룹 멤버십에서 포트를 제거하기 전에 IGMP 그룹 멤버십 보고서에 대한 기본 또는 구성된 MVR 쿼리 시간을 기다립니다. 값은 1/10초와 같습니다. 범위는 1에서 100까지입니다. 공장 기본값은 5/10 또는 1/2입니다.

4. MVR Mode 라디오 버튼을 선택하여 MVR 작동 모드를 지정합니다.

   공장 기본값은 호환 가능합니다.

5. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 103. 고급 MVR 구성

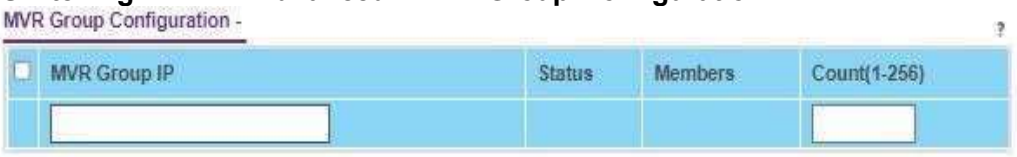
필드	설명

MVR Max Multicast Groups	MVR이 지원하는 최대 멀티캐스트 그룹 수입니다.
MVR Current Multicast Groups	현재 할당된 MVR 그룹 수를 표시합니다.

MVR 그룹 구성

➢ **MVR 그룹을 구성하려면:**

Switching > MVR > Advanced > MVR Group Configuration.



1. MVR Group IP를 사용하여 새 MVR 그룹의 IP 주소를 지정합니다.
2. Count를 사용하여 연속 MVR 그룹 수를 지정합니다.

   이는 Add 버튼을 한 번 클릭하여 여러 MVR 그룹을 생성하는 데 도움이 됩니다. 필드가 비어 있는 경우 버튼을 클릭하면 새 그룹이 하나만 생성됩니다. 필드는 각 특정 그룹에 대해 비어 있는 것으로 표시됩니다. 범위는 1~256입니다.
3. 추가 버튼을 클릭합니다.

   MVR 그룹이 추가됩니다.
4. 선택한 MVR 그룹을 삭제하려면 Delete 버튼을 클릭하세요.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 104. MVR 그룹 구성

필드	설명
Status	특정 MVR 그룹의 상태입니다.
Members	특정 MVR 그룹에 참여하는 포트 목록입니다.

MVR 인터페이스 구성

➢ **MVR 인터페이스를 구성하려면:**

Switching > MVR > Advanced > MVR Interface Configuration.

MVR Interface Configuration -

	Interface	Admin Mode	Type	Immediate Leave	Status
	0/1	Disable	none	Disable	INACTIVE/InVLAN
	0/2	Disable	none	Disable	INACTIVE/InVLAN
	0/3	Disable	none	Disable	INACTIVE/InVLAN
	0/4	Disable	none	Disable	INACTIVE/InVLAN
	0/5	Disable	none	Disable	ACTIVE/InVLAN
	0/6	Disable	none	Disable	INACTIVE/InVLAN
	0/7	Disable	none	Disable	INACTIVE/InVLAN
	0/8	Disable	none	Disable	INACTIVE/InVLAN

각 포트의 상태가 표시됩니다.

1. Interface를 사용하여 인터페이스를 선택합니다.
2. Admin를 사용하여 포트의 MVR을 Enable 또는 Disable합니다.

   공장 기본값은 Disable입니다.
3. Type을 사용하여 포트를 MVR 수신기 포트 또는 소스 포트로 구성합니다.

   기본 포트 유형은 none입니다.
4. Immediate Leave를 사용하여 포트에서 MVR의 Immediate Leave 기능을 Enable 또는 Disable합니다.

   공장 기본값은 Disable입니다.
5. Apply 버튼을 클릭합니다

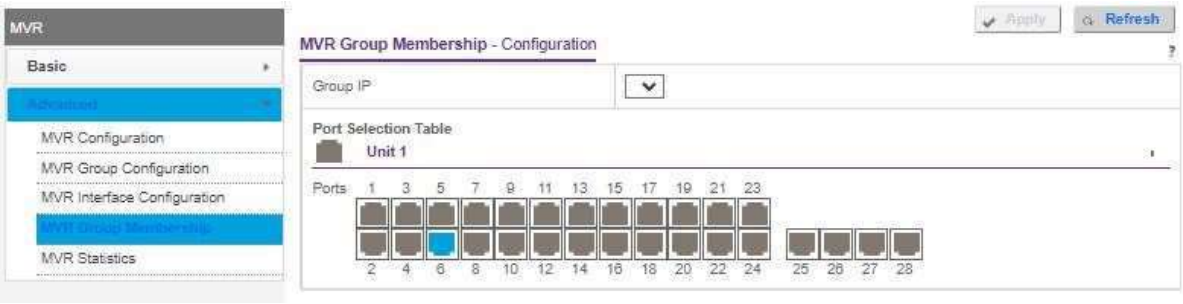
   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

MVR 그룹 멤버십 구성

➢ **MVR 그룹 멤버십을 구성하려면:**

Switching > MVR > Advanced > MVR Group Membership.



1. Group IP를 사용하여 MVR 그룹의 IP 멀티캐스트 주소를 지정합니다.
2. Port List을 사용하여 선택한 MVR 그룹의 구성원 구성 목록을 봅니다.

   이 포트 목록을 사용하여 선택한 포트를 이 MVR 그룹에 추가할 수 있습니다.
3. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

MVR 통계 보기

➢ **MVR 통계를 보려면:**

Switching > MVR > Advanced > MVR Statistics.

MVR Statistics - Status

IGMP Query Received	0
IGMP Report V1 Received	0
IGMP Report V2 Received	0
IGMP Leave Received	0
IGMP Query Transmitted	0
IGMP Report V1 Transmitted	0
IGMP Report V2 Transmitted	0
IGMP Leave Transmitted	0
IGMP Packet Receive Failures	0
IGMP Packet Transmit Failures	0

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 105. MVR 통계

필드	설명
IGMP Query Received	수신된 IGMP 쿼리 수입니다.
IGMP Report V1 Received	수신된 IGMP 보고서 수 V1.
IGMP Report V2 Received	수신된 IGMP 보고서 수 V2.
IGMP Leave Received	수신된 IGMP 나뭇잎 수입니다.
IGMP Query Transmitted	전송된 IGMP 쿼리 수입니다.
IGMP Report V1 Transmitted	전송된 IGMP 보고서의 수 V1.
IGMP Report V2 Transmitted	전송된 IGMP 보고서의 수 V2.
IGMP Leave Transmitted	전송된 IGMP 리프 수입니다.
IGMP Packet Receive Failures	IGMP 패킷 수신 실패 횟수입니다.
IGMP Packet Transmit Failures	IGMP 패킷 전송 실패 횟수입니다.

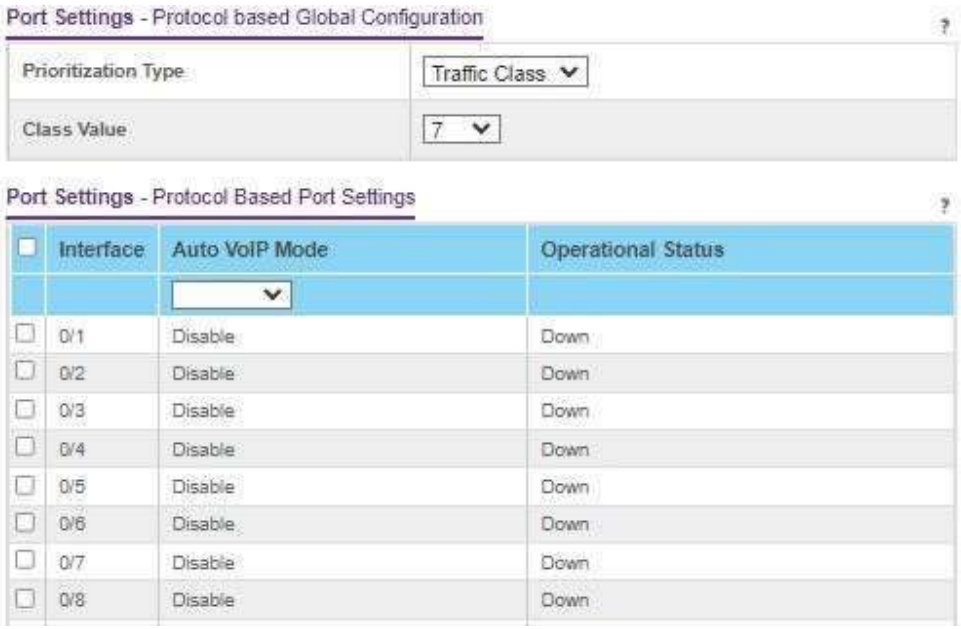
Auto-VoIP

프로토콜 기반 포트 설정 및 OUI 설정을 구성할 수 있습니다.

프로토콜 기반 포트 설정 구성

➢ **프로토콜 기반 포트 설정을 구성하려면:**

Switching > Auto-VoIP > Protocol-based > Port Settings.



1. Prioritization Type에서 Traffic Class 또는 Remark을 선택합니다.

   우선순위 유형을 지정합니다.

2. Class Value 목록에서 Remark CoS가 활성화된 경우 음성 VLAN에서 수신된 패킷에 대해 재할당할 CoS 태그 값을 지정합니다.

3. Apply 버튼을 클릭합니다

   스위치는 입력한 값으로 업데이트됩니다. 스위치가 전원을 껐다 켜는 동안 새 값을 유지하려면 저장을 수행해야 합니다.

Auto VoIP OUI 기반 속성 구성

➢ **자동 VoIP OUI 기반 속성을 구성하려면:**

Switching > Auto-VoIP > OUI-based> Properties.

1. VoIP VLAN ID 필드에 스위치의 VoIP VLAN ID를 입력합니다.

   자동 VoIP에는 기본 VLAN이 없으므로 먼저 VLAN을 생성해야 합니다.

2. OUI 기반 우선순위 목록에서 스위치의 OUI 기반 우선순위를 선택합니다.

   기본값은 7입니다.

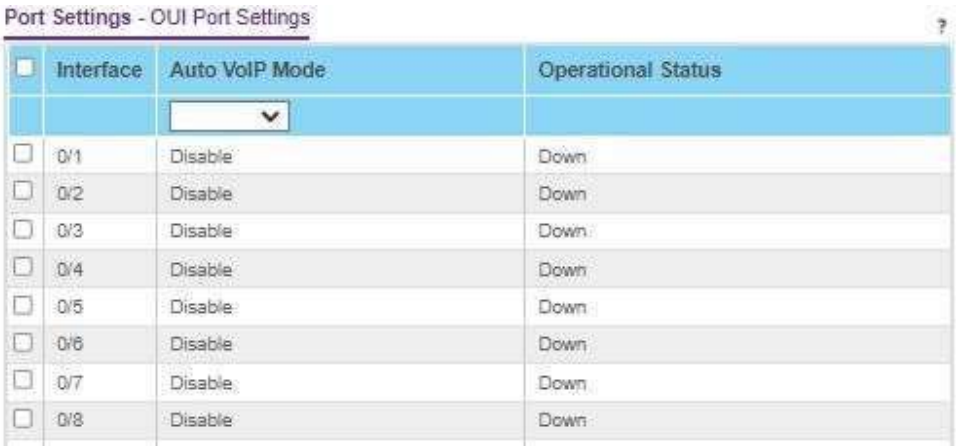
3. Apply 버튼을 클릭합니다

   스위치는 입력한 값으로 업데이트됩니다. 스위치가 전원을 껐다 켜는 동안 새 값을 유지하려면 저장을 수행해야 합니다.

OUI 기반 포트 설정

➢ **자동 VoIP OUI 기반 포트 설정을 구성하려면:**

Switching > Auto-VoIP > OUI-based > Port Settings.



Operational Status 필드에는 각 인터페이스의 현재 작동 상태가 표시됩니다.

1. 인터페이스 check box을 사용하여 인터페이스를 선택합니다.
2. Auto VoIP 모드 필드에서 Disable 또는 Enable를 선택합니다.

   자동 VoIP는 기본적으로 Disable되어 있습니다.

3. Go To Interface(인터페이스로 이동)를 사용하여 해당 번호를 입력하여 인터페이스를 선택합니다.
4. Apply 버튼을 클릭합니다

   스위치는 입력한 값으로 업데이트됩니다. 스위치가 전원을 껐다 켜는 동안 새 값을 유지하려면 저장을 수행해야 합니다.

OUI 테이블 구성

➢ **OUI 테이블을 구성하려면:**

Switching > Auto-VoIP > OUI-based > OUI Table.

OUI Table - Configuration

	Telephony OUI (xx:xx:xx)	Description (0-32 characters)
☐	00:01:E3	SIEMENS
☐	00:03:6B	CISCO1
☐	00:12:43	CISCO2
☐	00:0F:E2	H3C
☐	00:60:B9	NITSUKO
☐	00:D0:1E	PINTEL
☐	00:E0:75	VERILINK
☐	00:E0:BB	3COM
☐	00:04:0D	AVAYA1
☐	00:1B:4F	AVAYA2
☐	00:04:13	SNOM

1. Telephony OUI 필드에서 AA:BB:CC 형식으로 추가할 VoIP OUI 접두사를 지정합니다.

   최대 128개의 OUI를 구성할 수 있습니다.

2. Description 필드에 OUI에 대한 설명을 입력합니다.

   설명의 최대 길이는 32자입니다. 기본적으로 구성에는 다음 OUI가 있습니다.

   - 00:01:E3 - SIEMENS
   - 00:03:6B - CISCO1
   - 00:12:43 - CISCO2
   - 00:0F:E2 - H3C
   - 00:60:B9 - NITSUKO
   - 00:D0:1E - PINTEL
   - 00:E0:75 - VERILINK
   - 00:E0:BB - 3COM
   - 00:04:0D - AVAYA1
   - 00:1B:4F - AVAYA2

3. Add 버튼을 클릭합니다.

   전화 통신 OUI 항목이 추가됩니다.

4. 생성된 항목을 삭제하려면 삭제 버튼을 클릭하세요.

Auto VoIP 상태 보기

➢ **자동 VoIP 상태를 보려면:**

Switching > Auto-VoIP > Auto-VoIP Status.

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표에서는 구성할 수 없는 자동 VoIP 상태 정보에 대해 설명합니다.

Table 81. 자동 VoIP 상태

필드	설명
Auto-VoIP VLAN ID	자동 VoIP VLAN ID입니다.
Maximum Number of Voice Channels Supported	지원되는 최대 음성 채널 수입니다.
Number of Voice Channels Detected	VoIP 채널의 우선순위가 성공적으로 지정되었습니다.

라우팅 4

이 장에서는 다음 주제를 다룹니다.

- *경로 관리*
- *라우터 IP 구성*
- *스위치에 대한 라우팅 매개변수 구성*
- *IPv6*
- *VLAN 개요*
- *주소 확인 프로토콜 개요*

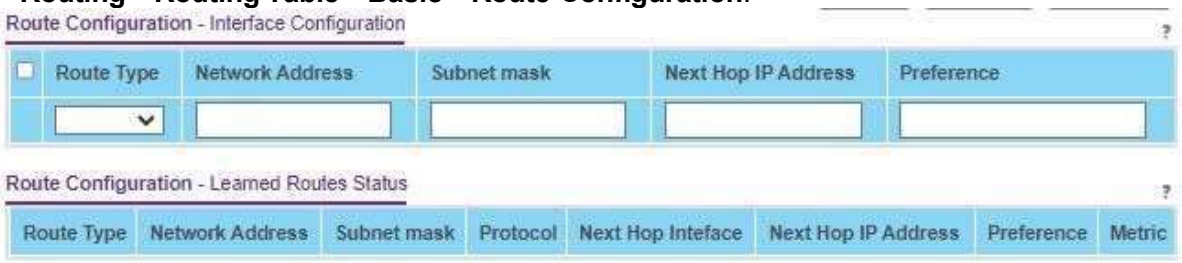
경로 관리

라우팅 테이블은 정적 경로와 로컬 경로 등 여러 소스에서 경로를 수집합니다. 라우팅 테이블은 여러 소스에서 동일한 대상으로 향하는 여러 경로를 학습할 수 있습니다. 라우팅 테이블에는 모든 경로가 나열됩니다.

기본 경로 구성

➢ **기본 경로를 구성하려면:**

Routing > **Routing Table** > **Basic** > **Route Configuration**.



1. Route Type 목록에서 다음 경로 유형 중 하나를 선택합니다.
   - **Default**. 기본 경로를 생성하려면 다음 홉 주소와 기본 설정만 지정해야 합니다.
   - **Static**. 고정 경로를 생성하려면 네트워크 주소, 서브넷 마스크, 다음 홉 주소 및 기본 설정을 지정합니다.
   - **Static Reject**. 정적 거부 경로를 생성하려면 네트워크 주소, 서브넷 마스크 및 기본 설정을 지정합니다.
2. **Network Address** 대상의 IP 경로 접두사가 표시됩니다.
3. **Subnet Mask** 연결된 네트워크를 식별하는 IP 인터페이스 주소 부분을 나타냅니다.

   이를 서브넷/네트워크 마스크라고도 합니다.
4. **Next Hop IP Address** 대상으로 향하는 경로의 다음 라우터(있는 경우)로 트래픽을 전달할 때 사용할 나가는 라우터 IP 주소를 표시합니다.

   다음 라우터는 항상 인접한 이웃 중 하나이거나 직접 연결된 네트워크에 대한 로컬 인터페이스의 IP 주소입니다.

5. **Preference** 1부터 255까지의 정수 값을 표시합니다.

   개별 정적 경로의 기본 설정 값(관리 거리라고도 함)을 지정할 수 있습니다. 동일한 목적지로 가는 경로 중 선호도 값이 가장 낮은 경로가 포워딩 데이터베이스에 입력된 경로입니다. 사용자는 정적 경로의 기본 설정을 지정하여 정적 경로가 동적 라우팅 프로토콜의 경로보다 선호되는지 여부를 제어합니다. 또한 기본 설정은 동일한 대상에 대한 다른 정적 경로보다 정적 경로를 선호하는지 여부를 제어합니다.

6. 설명을 사용하여 경로를 식별하는 이 경로에 대한 설명을 지정합니다.

   설명은 영숫자, 하이픈 또는 밑줄 문자로 구성되어야 하며 최대 31자까지 가능합니다.

7. Add 버튼을 클릭합니다.

   고정 경로가 스위치에 추가됩니다.

8. 스위치에서 기존 고정 경로 항목을 삭제하려면 Delete 버튼을 클릭합니다.

9. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표에서는 표시되는 구성할 수 없는 데이터에 대해 설명합니다.

Table 121. 라우팅 테이블 기본 경로 구성

필드	설명
Network Address	대상의 IP 경로 접두사입니다.
Subnet Mask	서브넷/네트워크 마스크라고도 하며 연결된 네트워크를 식별하는 IP 인터페이스 주소 부분을 나타냅니다.
Protocol	이 필드는 지정된 경로를 생성한 프로토콜을 알려줍니다. 가능성은 다음 중 하나입니다. • Local • Static
Route Type	이 필드는 프로토콜에 따라 연결됨, 정적 또는 동적일 수 있습니다.
Next Hop Interface	트래픽을 대상으로 전달할 때 사용할 나가는 라우터 인터페이스입니다.
Next Hop Address	대상으로 향하는 경로의 다음 라우터(있는 경우)로 트래픽을 전달할 때 사용할 나가는 라우터 IP 주소입니다. 다음 라우터는 항상 인접한 이웃

	중 하나이거나 직접 연결된 네트워크에 대한 로컬 인터페이스의 IP 주소입니다.
Preference	기본 설정은 (0~255)의 정수 값입니다. 사용자는 개별 고정 경로의 기본 설정 값(관리 거리라고도 함)을 지정할 수 있습니다. 동일한 목적지로 가는 경로 중 선호도 값이 가장 낮은 경로가 포워딩 데이터베이스에 입력된 경로입니다. 사용자는 정적 경로의 기본 설정을 지정하여 정적 경로가 동적 라우팅 프로토콜의 경로보다 선호되는지 여부를 제어합니다. 또한 기본 설정은 동일한 대상에 대한 다른 정적 경로보다 정적 경로를 선호하는지 여부를 제어합니다.
Metric	목적지까지의 경로에 대한 관리 비용. 값을 입력하지 않을 경우 기본값은 1입니다. 범위는 0~255입니다.

고급 경로 구성

➢ **고급 경로를 구성하려면:**

Routing > Routing Table> Advanced > Route Configuration.

1. Route Type 필드를 사용하여 기본 또는 정적 거부 경로를 지정합니다.

   기본 경로를 생성하는 경우 다음 홉 IP 주소만 지정해야 합니다. 그렇지 않으면 각 필드를 작성해야 합니다.

2. **Network Address** 대상의 IP 경로 접두사가 표시됩니다.
3. **Subnet Mask** 연결된 네트워크를 식별하는 IP 인터페이스 주소 부분을 나타냅니다.

   이를 서브넷/네트워크 마스크라고도 합니다.

4. **Next Hop IP Address** 대상으로 향하는 경로의 다음 라우터(있는 경우)로 트래픽을 전달할 때 사용할 나가는 라우터 IP 주소를 표시합니다.

   다음 라우터는 항상 인접한 이웃 중 하나이거나 직접 연결된 네트워크에 대한 로컬

인터페이스의 IP 주소입니다.

5. **Preference** 1부터 255까지의 정수 값을 표시합니다.

   개별 정적 경로의 기본 설정 값(관리 거리라고도 함)을 지정할 수 있습니다. 동일한 목적지로 가는 경로 중 선호도 값이 가장 낮은 경로가 포워딩 데이터베이스에 입력된 경로입니다. 사용자는 정적 경로의 기본 설정을 지정하여 정적 경로가 동적 라우팅 프로토콜의 경로보다 선호되는지 여부를 제어합니다. 또한 기본 설정은 동일한 대상에 대한 다른 정적 경로보다 정적 경로를 선호하는지 여부를 제어합니다.

6. 설명을 사용하여 경로를 식별하는 이 경로에 대한 설명을 지정합니다.

   설명은 영숫자, 하이픈 또는 밑줄 문자로 구성되어야 하며 최대 31자까지 가능합니다.

7. Add 버튼을 클릭합니다

   고정 경로가 스위치에 추가됩니다.

8. 스위치에서 선택한 고정 경로 항목을 삭제하려면 Delete 버튼을 클릭합니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 122. 경로 구성 - 학습된 경로

필드	설명
Network Address	대상의 IP 경로 접두사입니다.
Subnet Mask	서브넷/네트워크 마스크라고도 하며 연결된 네트워크를 식별하는 IP 인터페이스 주소 부분을 나타냅니다.
Protocol	이 필드는 지정된 경로를 생성한 프로토콜을 알려줍니다. 가능성은 다음 중 하나입니다. • Local • Static
Route Type	이 필드는 기본값이거나 정적일 수 있습니다.
Next Hop Interface	트래픽을 대상으로 전달할 때 사용할 나가는 라우터 인터페이스입니다.
Next Hop IP Address	대상으로 향하는 경로의 다음 라우터(있는 경우)로 트래픽을 전달할 때 사용할 나가는 라우터 IP 주소입니다. 다음 라우터는 항상 인접한 이웃 중 하나이거나 직접 연결된 네트워크에 대한 로컬 인터페이스의 IP 주소입니다.

Preference	기본 설정은 0~255 사이의 정수 값입니다. 사용자는 개별 고정 경로의 기본 설정 값(관리 거리라고도 함)을 지정할 수 있습니다. 동일한 목적지로 가는 경로 중 선호도 값이 가장 낮은 경로가 포워딩 데이터베이스에 입력된 경로입니다. 사용자는 정적 경로의 기본 설정을 지정하여 정적 경로가 동적 라우팅 프로토콜의 경로보다 선호되는지 여부를 제어합니다. 또한 기본 설정은 동일한 대상에 대한 다른 정적 경로보다 정적 경로를 선호하는지 여부를 제어합니다.
Metric	목적지까지의 경로에 대한 관리 비용. 값을 입력하지 않을 경우 기본값은 1입니다. 범위는 0~255입니다.

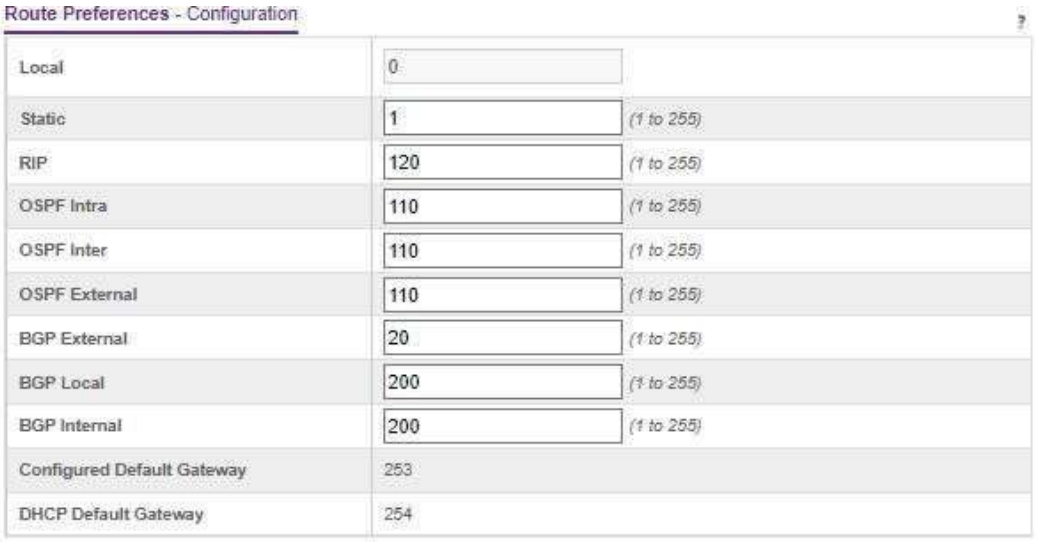
경로 기본 설정 지정

각 프로토콜에 대한 기본 기본 설정을 구성할 수 있습니다(예: 고정 경로의 경우 60, RIP의 경우 120). 이러한 값은 1~255 범위의 임의 값이며 경로 메트릭과 무관합니다. 대부분의 라우팅 프로토콜은 경로 메트릭을 사용하여 다른 프로토콜과 관계없이 프로토콜에 알려진 최단 경로를 결정합니다.

선호도 값이 가장 낮은 경로를 선택하여 목적지까지 최적의 경로를 선택합니다.
목적지까지의 경로가 여러 개인 경우 기본 설정 값을 사용하여 기본 경로를 결정합니다.
여전히 동점인 경우 경로 메트릭이 가장 좋은 경로가 선택됩니다. 일치하지 않는 메트릭(예: RIP 및 OSPF(Open Shortest Path First) 메트릭과 같이 직접 비교할 수 없음) 문제를 방지하려면 각 프로토콜에 대해 서로 다른 기본 설정 값을 구성해야 합니다.

- **경로 기본 설정을 지정하려면:**

  Routing > Routing Table > Advanced > Route Preferences.



1. Static을 사용하여 라우터의 고정 경로 기본 설정 값을 지정합니다.

   기본값은 1입니다. 범위는 1~255입니다.

2. 라우터에서 RIP 경로 기본 설정 값을 지정합니다.
   기본값은 120입니다. 범위는 1~255입니다.

3. 라우터에서 OSPF 내부 경로 기본 설정 값을 지정합니다.

   기본값은 110입니다. 범위는 1~255입니다. OSPF 사양(RFC 2328)에 따르면 OSPF를 통해 학습된 경로에 대해 다음 순서로 기본 설정을 제공해야 합니다.

4. 라우터에서 OSPF 내부 경로 기본 설정 값을 지정합니다.

   기본값은 110입니다. 범위는 1~255입니다. OSPF 사양(RFC 2328)에 따르면 OSPF를 통해 학습된 경로에 대해 다음 순서로 기본 설정을 제공해야 합니다.

5. 라우터에서 OSPF 외부 경로 기본 설정 값을 지정합니다.

   기본값은 110입니다. 범위는 1~255입니다. OSPF 사양(RFC 2328)에 따르면 type1/type2/nssa1/nssa2와 같은 모든 OSPF 외부 경로 유형에 대해 기본 설정 값이 동일해야 합니다.

6. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

로컬 필드에는 로컬 경로 기본 설정 값이 표시됩니다.

라우터 IP 구성

인터페이스와 달리 스위치에 대한 라우팅 매개변수를 구성할 수 있습니다.

➢ **라우터 IP를 구성하려면:**

Routing > IP > Basic > IP Configuration.

1. Routing Mode를 사용하여 Enable 또는 Disable를 선택합니다.

   인터페이스를 통해 라우팅하려면 먼저 스위치에 대한 라우팅을 활성화해야 합니다. 기본값은 Disable입니다.

2. ICMP Echo Replies을 사용하여 Enable 또는 Disable를 선택합니다.

   활성화를 선택하면 라우터만 ECHO 응답을 보낼 수 있습니다. 기본적으로 ICMP 에코 응답은 에코 요청에 대해 전송됩니다.

3. ICMP Redirects을 사용하여 Enable 또는 Disable를 선택합니다.

   이것이 전역적으로 그리고 인터페이스 수준에서 활성화되면 라우터만 ICMP 리디렉션을 보낼 수 있습니다.

4. ICMP Rate Limit Interval을 사용하면 버스트 간격당 허용되는 ICMP 오류 패킷 수를 지정하여 ICMP 오류 패킷을 제어할 수 있습니다.

   기본적으로 속도 제한은 100패킷/초입니다(버스트 간격은 1000밀리초). ICMP 속도 제한을 비활성화하려면 이 필드를 0으로 설정합니다. 유효한 속도 간격은 0~2147483647입니다.

5. ICMP Rate Limit Burst를 사용하면 버스트 간격당 허용되는 ICMP 오류 패킷 수를 지정하여 ICMP 오류 패킷을 제어할 수 있습니다.

   기본적으로 버스트 크기는 100패킷입니다. 버스트 간격이 0이면 이 필드를 구성하는 것은 유효한 작업이 아닙니다. 유효한 버스트 크기 범위는 1~200입니다.

6. Select to configure Global Default Gateway를 사용하여 Global Default Gateway 필드를 편집합니다.

7. Global Default Gateway를 사용하여 글로벌 기본 게이트웨이를 수동으로 구성된 값으로 설정합니다. 이 명령으로 구성된 기본 게이트웨이는 DHCP 서버에서 학습된 기본 게이트웨이보다 더 선호됩니다. 기본 게이트웨이는 하나만 구성할 수 있습니다. 이 명령을 여러 번 호출하면 각 명령이 이전 값을 대체합니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 123. 라우팅 IP 구성

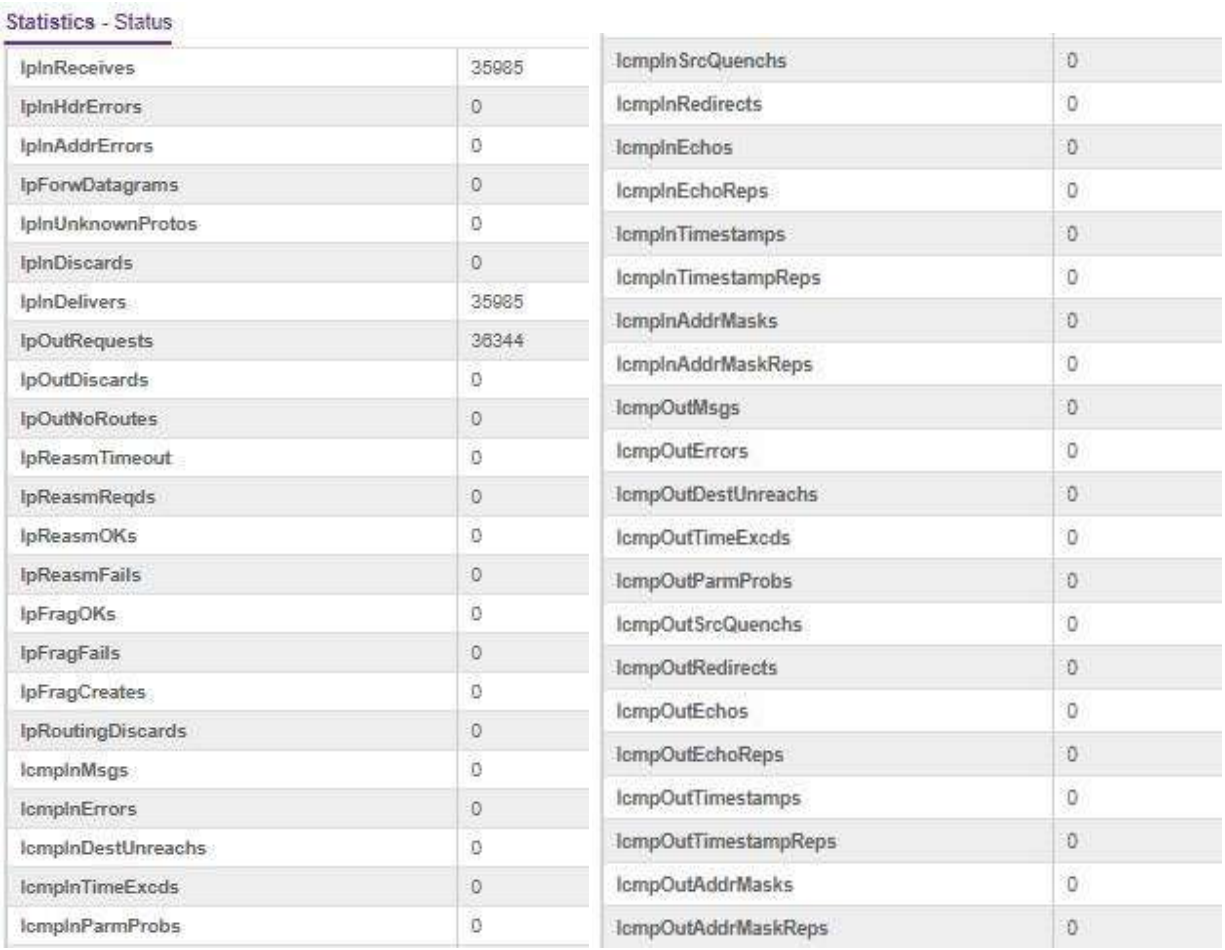
필드	설명
Default Time to Live	전송 계층 프로토콜에서 TTL 값을 제공하지 않는 경우 스위치에서 생성된 데이터그램의 IP 헤더에 있는 TTL(Time-To-Live) 필드에 삽입되는 기본값입니다.
Maximum Next Hops	스위치가 지원하는 최대 홉 수입니다. 이는 컴파일 타임 상수입니다.
Maximum Routes	스위치가 지원하는 최대 경로 수(라우팅 테이블 크기)입니다. 이는 컴파일 타임 상수입니다.

통계 보기

이 화면에 보고된 통계는 RFC 1213에 지정된 대로입니다.

- **통계를 보려면:**

  Routing > IP > Basic > Statistics.



다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 124. IP 기본 통계

필드	설명
IpInReceives	오류로 수신된 데이터그램을 포함하여 인터페이스에서 수신된 입력 데이터그램의 총 수입니다.
IpInHdrErrors	잘못된 체크섬, 버전 번호 불일치, 기타 형식 오류, TTL(time-to-live) 초과, IP 옵션 처리 중 발견된 오류 등을 포함하여 IP 헤더의 오류로 인해 삭제된 입력 데이터그램 수입니다.
IpInAddrErrors	IP 헤더의 대상 필드에 있는 IP 주소가 이 엔터티에서 수신할 수 있는 유효한 주소가 아니기 때문에 삭제된 입력 데이터그램 수입니다. 이 수에는 잘못된 주소(예: 0.0.0.0)와 지원되지 않는 클래스(클래스 E)의 주소가 포함됩니다. IP 게이트웨이가 아니므로 데이터그램을 전달하지 않는 엔터티의 경우 이 카운터에는 대상 주소가 로컬 주소가 아니기 때문에 삭제된 데이터그램이 포함됩니다.

IpForwDatagrams	이 엔터티가 최종 IP 대상이 아니어서 해당 최종 대상으로 전달하기 위한 경로를 찾으려고 시도한 입력 데이터그램의 수입니다. IP 게이트웨이 역할을 하지 않는 엔터티에서 이 카운터에는 IP 게이트웨이 역할을 한 패킷만 포함됩니다.
IpInUnknownProtos	성공적으로 수신되었지만 알 수 없거나 지원되지 않는 프로토콜로 인해 삭제된 로컬 주소가 지정된 데이터그램의 수입니다.
IpInDiscards	지속적인 처리를 방지하기 위해 문제가 발생하지 않았지만 버퍼 공간 부족으로 인해 삭제된 입력 IP 데이터그램 수입니다. 이 카운터에는 재조립을 기다리는 동안 폐기된 데이터그램이 포함되지 않습니다.
IpInDelivers	IP 사용자 프로토콜(ICMP 포함)에 성공적으로 전달된 총 입력 데이터그램 수입니다.
IpOutRequests	로컬 IP 사용자 프로토콜(ICMP 포함)이 전송 요청 시 IP에 제공한 총 IP 데이터그램 수입니다. 이 카운터에는 ipForwDatagrams에서 계산된 데이터그램이 포함되지 않습니다.
IpOutDiscards	대상으로의 전송을 방지하기 위해 문제가 발생하지 않았지만 버퍼 공간 부족 등의 이유로 폐기된 출력 IP 데이터그램의 수입니다. 이 카운터에는 해당 패킷이 이 (임의) 폐기 기준을 충족하는 경우 ipForwDatagrams에서 계산된 데이터그램이 포함됩니다.
IpOutNoRoutes	대상으로 전송할 경로를 찾을 수 없어 삭제된 IP 데이터그램 수입니다. 이 카운터에는 이 경로 없음 기준을 충족하는 ipForwDatagrams에서 계산된 모든 패킷이 포함됩니다. 여기에는 모든 기본 게이트웨이가 다운되어 호스트가 라우팅할 수 없는 모든 데이터그램이 포함됩니다.
IpReasmTimeout	수신된 조각이 이 엔터티에서 재조립을 기다리는 동안 보관되는 최대 시간(초)입니다.
IpReasmReqds	이 엔터티에서 재조립되어 수신된 IP 조각 수입니다.
IpReasmOKs	성공적으로 재조립된 IP 데이터그램의 수입니다.
IpReasmFails	IP 재조립 알고리즘에 의해 감지된 실패 수(이유에 관계없이: 시간 초과, 오류 등). 일부 알고리즘은 조각이 수신될 때 조각을 결합하여 조각 수를 추적하지 못할 수 있으므로 이는 폐기된 IP 조각의 개수일 필요는 없습니다.
IpFragOKs	이 엔터티에서 조각화된 IP 데이터그램 수입니다.
IpFragFails	이 엔터티에서 조각화해야 했지만 조각화하지 않음 플래그가 설정된 등의 이유로 조각화할 수 없어 삭제된 IP 데이터그램 수입니다.

IpFragCreates	이 엔터티의 조각화 결과로 생성된 IP 데이터그램 조각 수입니다.
IpRoutingDiscards	유효함에도 불구하고 삭제된 라우팅 항목의 수입니다. 이러한 항목을 삭제하는 한 가지 가능한 이유는 다른 라우팅 항목을 위한 버퍼 공간을 확보하는 것일 수 있습니다.
IcmpInMsgs	엔터티가 수신한 총 ICMP 메시지 수입니다. 이 카운터에는 icmpInErrors로 계산된 모든 항목이 포함됩니다.
IcmpInErrors	엔터티가 수신했지만 ICMP 관련 오류(잘못된 ICMP 체크섬, 잘못된 길이 등)가 있는 것으로 확인된 ICMP 메시지 수입니다.
IcmpInDestUnreachs	수신된 ICMP 대상에 연결할 수 없는 메시지 수입니다.
IcmpInTimeExcds	수신된 ICMP 시간 초과 메시지 수입니다.
IcmpInParmProbs	수신된 ICMP 매개변수 문제 메시지 수입니다.
IcmpInSrcQuenchs	수신된 ICMP 소스 퀀치 메시지 수입니다.
IcmpInRedirects	수신된 ICMP 리디렉션 메시지 수입니다.
IcmpInEchos	수신된 ICMP 에코(요청) 메시지 수입니다.
IcmpInEchoReps	수신된 ICMP 에코 응답 메시지 수입니다.
IcmpInTimestamps	수신된 ICMP 타임스탬프(요청) 메시지 수입니다.
IcmpInTimestampReps	수신된 ICMP 라임스탬프 응답 메시지 수입니다.
IcmpInAddrMasks	수신된 ICMP 주소 마스크 요청 메시지 수입니다.
IcmpInAddrMaskReps	수신된 ICMP 주소 마스크 응답 메시지 수입니다.
IcmpOutMsgs	이 엔터티가 보내려고 시도한 총 ICMP 메시지 수입니다. 이 카운터에는 icmpOutErrors로 계산된 모든 항목이 포함됩니다.
IcmpOutErrors	버퍼 부족 등 ICMP 내에서 발견된 문제로 인해 이 엔터티가 보내지 않은 ICMP 메시지 수입니다. 이 값에는 IP가 결과 데이터그램을 라우팅할 수 없는 등 ICMP 계층 외부에서 발견된 오류는 포함되지 않습니다. 일부 구현에서는 이 카운터 값에 영향을 미치는 오류 유형이 없을 수 있습니다.
IcmpOutDestUnreachs	전송된 ICMP 대상에 연결할 수 없는 메시지 수입니다.
IcmpOutTimeExcds	전송된 ICMP 시간 초과 메시지 수입니다.
IcmpOutParmProbs	전송된 ICMP 매개변수 문제 메시지 수입니다.
IcmpOutSrcQuenchs	전송된 ICMP 소스 퀀치 메시지 수입니다.
IcmpOutRedirects	전송된 ICMP 리디렉션 메시지 수입니다. 호스트의 경우 호스트가

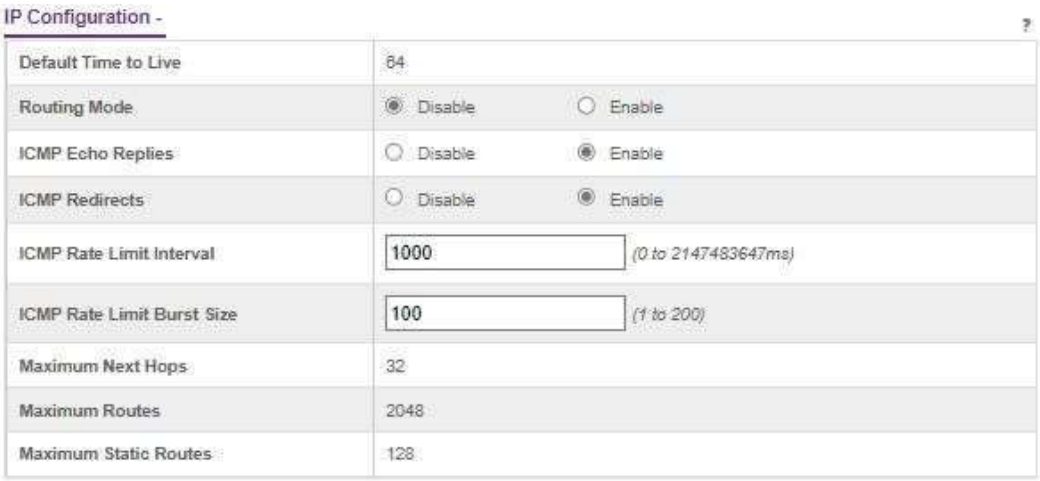
	리디렉션을 보내지 않으므로 이는 항상 0입니다.
IcmpOutEchos	전송된 ICMP 에코(요청) 메시지 수입니다.
IcmpOutEchoReps	전송된 ICMP 에코 응답 메시지 수입니다.
IcmpOutTimestamps	ICMP 타임스탬프(요청) 메시지 수입니다.
IcmpOutTimestampReps	전송된 ICMP 타임스탬프 응답 메시지 수입니다.
IcmpOutAddrMasks	전송된 ICMP 주소 마스크 요청 메시지 수입니다.

스위치에 대한 라우팅 매개변수 구성

인터페이스와 반대로 스위치에 대한 라우팅 매개변수를 구성할 수 있습니다.

➢ **스위치에 대한 라우팅 매개변수를 구성하려면:**

Routing > IP > Advanced > IP Configuration.



1. Routing Mode를 사용하여 Enable 또는 Disable를 선택합니다.

   인터페이스를 통해 라우팅하려면 먼저 스위치에 대한 라우팅을 활성화해야 합니다.

   기본값은 비활성화입니다.

2. ICMP Echo Replies을 사용하여 Enable 또는 Disable를 선택합니다.

   활성화를 선택하면 라우터만 ECHO 응답을 보낼 수 있습니다. 기본적으로 ICMP 에코 응답은 에코 요청에 대해 전송됩니다.

3. ICMP Redirects을 사용하여 Enable 또는 Disable를 선택합니다.

전역적으로 인터페이스 수준에서 활성화된 경우 라우터만 ICMP 리디렉션을 보낼 수 있습니다.

4. ICMP Rate Limit Interval을 사용하면 버스트 간격당 허용되는 ICMP 오류 패킷 수를 지정하여 ICMP 오류 패킷을 제어할 수 있습니다.

   기본적으로 속도 제한은 100패킷/초입니다(버스트 간격은 1000밀리초). ICMP 속도 제한을 비활성화하려면 이 필드를 0으로 설정하십시오. 유효한 속도 간격의 범위는 0~2147483647입니다..

5. ICMP Rate Limit Burst Size를 사용하면 버스트 간격당 허용되는 ICMP 오류 패킷 수를 지정하여 ICMP 오류 패킷을 제어할 수 있습니다.

   기본적으로 버스트 크기는 100패킷입니다. 버스트 간격이 0이면 이 필드를 구성하는 것은 유효한 작업이 아닙니다. 유효한 버스트 크기는 1~200입니다.

6. Select to Configure Global Default Gateway를 사용하여 Global Default Gateway필드를 편집합니다.

7. Global Default Gateway를 사용하여 글로벌 기본 게이트웨이를 수동으로 구성된 값으로 설정합니다.

   이 명령으로 구성된 기본 게이트웨이는 DHCP 서버에서 학습된 기본 게이트웨이보다 더 선호됩니다. 기본 게이트웨이는 하나만 구성할 수 있습니다. 이 명령을 여러 번 호출하면 각 명령이 이전 값을 대체합니다.

8. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 125. 라우팅 IP 구성

필드	설명
Default Time to Live	전송 계층 프로토콜에서 TTL 값을 제공하지 않는 경우 스위치에서 생성된 데이터그램의 IP 헤더에 있는 TTL(Time-To-Live) 필드에 삽입되는 기본값입니다.
Maximum Next Hops	스위치가 지원하는 최대 홉 수입니다. 이는 컴파일 타임 상수입니다.
Maximum Routes	스위치가 지원하는 최대 경로 수(라우팅 테이블 크기)입니다. 이는 컴파일 타임 상수입니다.

Maximum Static Routes	스위치가 지원하는 최대 고정 경로 수입니다.

IP 통계 보기

이 화면에 보고된 통계는 RFC 1213에 지정된 대로입니다.

➢ **IP 통계를 보려면:**

Routing > IP > Advanced > Statistics.

Statistics - Status

IpInReceives	36175
IpInHdrErrors	0
IpInAddrErrors	0
IpForwDatagrams	0
IpInUnknownProtos	0
IpInDiscards	0
IpInDelivers	36175
IpOutRequests	36534
IpOutDiscards	0
IpOutNoRoutes	0
IpReasmTimeout	0
IpReasmReqds	0
IpReasmOKs	0
IpReasmFails	0
IpFragOKs	0
IpFragFails	0
IpFragCreates	0
IpRoutingDiscards	0
IcmpInMsgs	0
IcmpInErrors	0
IcmpInDestUnreachs	0
IcmpInTimeExcds	0
IcmpInParmProbs	0
IcmpInSrcQuenchs	0
IcmpInRedirects	0
IcmpInEchos	0
IcmpInEchoReps	0
IcmpInTimestamps	0
IcmpInTimestampReps	0
IcmpInAddrMasks	0
IcmpInAddrMaskReps	0
IcmpOutMsgs	0
IcmpOutErrors	0
IcmpOutDestUnreachs	0
IcmpOutTimeExcds	0
IcmpOutParmProbs	0
IcmpOutSrcQuenchs	0
IcmpOutRedirects	0
IcmpOutEchos	0
IcmpOutEchoReps	0
IcmpOutTimestamps	0
IcmpOutTimestampReps	0
IcmpOutAddrMasks	0
IcmpOutAddrMaskReps	0

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 126. IP 통계

필드	설명
IpInReceives	오류로 수신된 데이터그램을 포함하여 인터페이스에서 수신된 입력 데이터그램의 총 수입니다.

IpInHdrErrors	잘못된 체크섬, 버전 번호 불일치, 기타 형식 오류, TTL(time-to-live) 초과, IP 옵션 처리 중 발견된 오류 등을 포함하여 IP 헤더의 오류로 인해 폐기된 입력 데이터그램 수
IpInAddrErrors	IP 헤더의 대상 필드에 있는 IP 주소가 이 엔터티에서 수신할 수 있는 유효한 주소가 아니기 때문에 삭제된 입력 데이터그램 수입니다. 이 수에는 잘못된 주소(예: 0.0.0.0)와 지원되지 않는 클래스(예: 클래스 E)의 주소가 포함됩니다. IP 게이트웨이가 아니므로 데이터그램을 전달하지 않는 엔터티의 경우 이 카운터에는 대상 주소가 로컬 주소가 아니기 때문에 삭제된 데이터그램이 포함됩니다.
IpForwDatagrams	이 엔터티가 최종 IP 대상이 아니어서 해당 최종 대상으로 전달하기 위한 경로를 찾으려고 시도한 입력 데이터그램의 수입니다. IP 게이트웨이 역할을 하지 않는 엔터티에서 이 카운터에는 이 엔터티를 통해 소스 라우팅되었으며 소스 경로 옵션 처리가 성공한 패킷만 포함됩니다.
IpInUnknownProtos	성공적으로 수신되었지만 알 수 없거나 지원되지 않는 프로토콜로 인해 삭제된 로컬 주소가 지정된 데이터그램의 수입니다.
IpInDiscards	지속적인 처리를 방지하기 위해 문제가 발생하지 않았지만 버퍼 공간 부족 등의 이유로 폐기된 입력 IP 데이터그램의 수입니다. 이 카운터에는 재조립을 기다리는 동안 폐기된 데이터그램이 포함되지 않습니다.
IpInDelivers	IP 사용자 프로토콜(ICMP 포함)에 성공적으로 전달된 총 입력 데이터그램 수입니다.
IpOutRequests	로컬 IP 사용자 프로토콜(ICMP 포함)이 전송 요청 시 IP에 제공한 총 IP 데이터그램 수입니다. 이 카운터에는 ipForwDatagrams에서 계산된 데이터그램이 포함되지 않습니다.
IpOutDiscards	대상으로의 전송을 방지하기 위해 문제가 발생하지 않았지만 버퍼 공간 부족 등의 이유로 폐기된 출력 IP 데이터그램의 수입니다. 이 카운터에는 해당 패킷이 이 (임의) 폐기 기준을 충족하는 경우 ipForwDatagrams에서 계산된 데이터그램이 포함됩니다.
IpOutNoRoutes	대상으로 전송할 경로를 찾을 수 없어 삭제된 IP 데이터그램 수입니다. 이 카운터에는 이 경로 없음 기준을 충족하는 ipForwDatagrams에서 계산된 모든 패킷이 포함됩니다. 여기에는 모든 기본 게이트웨이가 다운되어 호스트가 라우팅할 수 없는 모든 데이터그램이 포함됩니다.
IpReasmTimeout	수신된 조각이 이 엔터티에서 재조립을 기다리는 동안 보관되는 최대 시간(초)입니다.

IpReasmReqds	이 엔터티에서 재조립해야 하는 수신된 IP 조각 수입니다.
IpReasmOKs	성공적으로 재조립된 IP 데이터그램의 수입니다.
IpReasmFails	IP 리어셈블리 알고리즘에 의해 감지된 실패 수(이유: 시간 초과, 오류 등). 일부 알고리즘은 조각이 수신될 때 조각을 결합하여 조각 수를 추적하지 못할 수 있으므로 이는 폐기된 IP 조각의 개수일 필요는 없습니다.
IpFragOKs	이 엔터티에서 조각화된 IP 데이터그램 수입니다.
IpFragFails	이 엔터티에서 조각화해야 했지만 조각화할 수 없어 삭제된 IP 데이터그램 수입니다. 예를 들어 조각화 안 함 플래그가 설정되었기 때문에 이런 일이 발생할 수 있습니다.
IpFragCreates	이 엔터티의 조각화 결과로 생성된 IP 데이터그램 조각 수입니다.
IpRoutingDiscards	유효함에도 불구하고 삭제된 라우팅 항목의 수입니다. 이러한 항목을 삭제하는 한 가지 가능한 이유는 다른 라우팅 항목을 위한 버퍼 공간을 확보하는 것일 수 있습니다.
IcmpInMsgs	엔터티가 수신한 총 ICMP 메시지 수입니다. 이 카운터에는 icmpInErrors로 계산된 모든 항목이 포함됩니다.
IcmpInErrors	엔터티가 수신했지만 ICMP 관련 오류(잘못된 ICMP 체크섬, 잘못된 길이 등)가 있는 것으로 확인된 ICMP 메시지 수입니다.
IcmpInDestUnreachs	수신된 ICMP 대상에 연결할 수 없는 메시지 수입니다.
IcmpInTimeExcds	수신된 ICMP 시간 초과 메시지 수입니다.
IcmpInParmProbs	수신된 ICMP 매개변수 문제 메시지 수입니다.
IcmpInSrcQuenchs	수신된 ICMP 소스 퀀치 메시지 수입니다.
IcmpInRedirects	수신된 ICMP 리디렉션 메시지 수입니다.
IcmpInEchos	수신된 ICMP 에코(요청) 메시지 수입니다.
IcmpInEchoReps	수신된 ICMP 에코 응답 메시지 수입니다.
IcmpInTimestamps	수신된 ICMP 타임스탬프(요청) 메시지 수입니다.
IcmpInTimestampReps	수신된 ICMP 타임스탬프 응답 메시지 수입니다.
IcmpInAddrMasks	수신된 ICMP 주소 마스크 요청 메시지 수입니다.
IcmpInAddrMaskReps	수신된 ICMP 주소 마스크 응답 메시지 수입니다.
IcmpOutMsgs	이 엔터티가 보내려고 시도한 총 ICMP 메시지 수입니다. 이 카운터에는 icmpOutErrors로 계산된 모든 항목이 포함됩니다.

IcmpOutErrors	버퍼 부족 등 ICMP 내에서 발견된 문제로 인해 이 엔터티가 보내지 않은 ICMP 메시지 수입니다. 이 값에는 IP가 결과 데이터그램을 라우팅할 수 없는 등 ICMP 계층 외부에서 발견된 오류는 포함되지 않습니다. 일부 구현에서는 이 카운터 값에 영향을 미치는 오류 유형이 없을 수 있습니다.
IcmpOutDestUnreachs	전송된 ICMP 대상에 연결할 수 없는 메시지 수입니다.
IcmpOutTimeExcds	전송된 ICMP 시간 초과 메시지 수입니다.
IcmpOutParmProbs	전송된 ICMP 매개변수 문제 메시지 수입니다.
IcmpOutSrcQuenchs	전송된 ICMP 소스 퀀치 메시지 수입니다.
IcmpOutRedirects	전송된 ICMP 리디렉션 메시지 수입니다. 호스트의 경우 호스트가 리디렉션을 보내지 않으므로 이는 0입니다.
IcmpOutEchos	전송된 ICMP 에코(요청) 메시지 수입니다.
IcmpOutEchoReps	전송된 ICMP 에코 응답 메시지 수입니다.
IcmpOutTimestamps	ICMP 타임스탬프(요청) 메시지 수입니다.
IcmpOutTimestampReps	전송된 ICMP 타임스탬프 응답 메시지 수입니다.
IcmpOutAddrMasks	전송된 ICMP 주소 마스크 요청 메시지 수입니다.
IcmpOutAddrMaskReps	전송된 ICMP 주소 마스크 응답 메시지 수입니다.

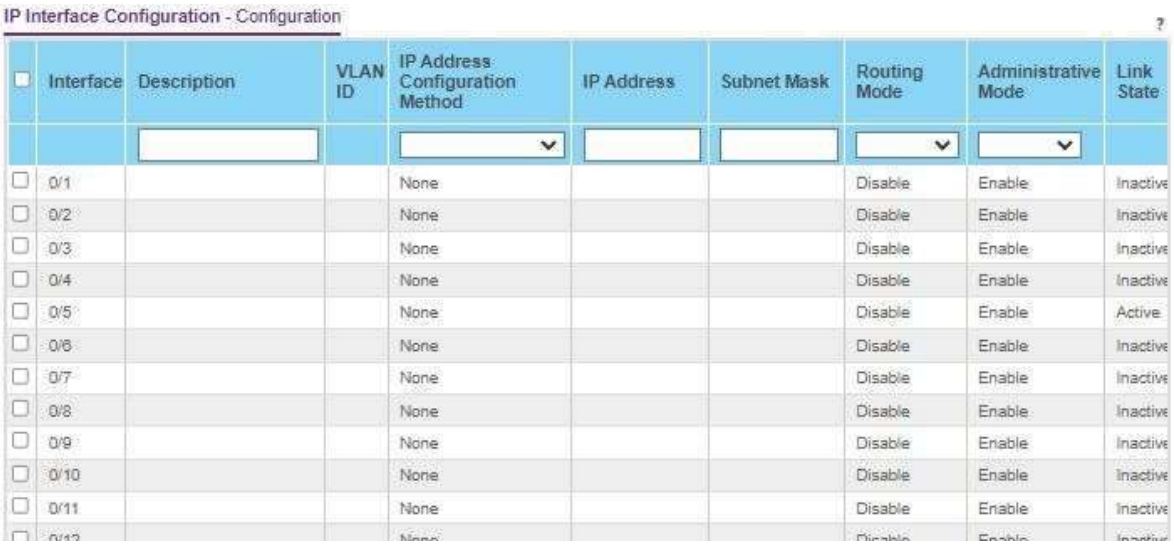
IP 인터페이스 구성

이 스위치에 대한 IP 인터페이스 데이터를 업데이트할 수 있습니다.

- **IP 인터페이스를 구성하려면:**

  Routing > IP > Advanced > IP Interface Configuration.

  화면은 세 부분으로 표시됩니다.


IP Interface Configuration - Configuration

Interface	Description	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routing Mode	Administrative Mode	Link State
0/1			None			Disable	Enable	Inactive
0/2			None			Disable	Enable	Inactive
0/3			None			Disable	Enable	Inactive
0/4			None			Disable	Enable	Inactive
0/5			None			Disable	Enable	Active
0/6			None			Disable	Enable	Inactive
0/7			None			Disable	Enable	Inactive
0/8			None			Disable	Enable	Inactive
0/9			None			Disable	Enable	Inactive
0/10			None			Disable	Enable	Inactive
0/11			None			Disable	Enable	Inactive

1. Go To Interface를 이용하여 유닛/슬롯/포트 형식의 인터페이스에 진입한 후 Go 버튼을 클릭합니다.
   지정된 인터페이스에 해당하는 항목이 선택됩니다.
2. Interface를 사용하여 인터페이스를 선택합니다.
3. Description을 사용하여 인터페이스에 대한 설명을 입력합니다.
4. IP Address Configuration Method를 사용하여 인터페이스에서 IP 주소를 구성하는 방법을 입력합니다.

   None, Manual, DHCP의 세 가지 방법이 있습니다. 기본적으로 이 방법은 None입니다. DHCP 방법을 재설정하려면 None 방법을 사용하십시오.

   Note: 구성 방법이 DHCP에서 None으로 변경되면 화면이 새로 고쳐지기 전에 약간의 지연이 발생합니다.
5. IP Address를 사용하여 인터페이스의 IP 주소를 입력합니다.
6. Subnet Mask를 사용하여 인터페이스의 서브넷 마스크를 입력합니다.

   이는 서브넷/네트워크 마스크라고도 하며 연결된 네트워크를 식별하는 데 사용되는 인터페이스의 IP 주소 부분을 정의합니다.
7. Routing Mode 목록에서 Enable 또는 Disable를 선택합니다.
   기본값은 Enable입니다.
8. Administrative Mode를 사용하여 인터페이스의 관리 모드를 Enable하거나 Disable합니다.
   기본값은 Enable입니다. 이 모드는 논리적 VLAN 인터페이스에는 지원되지 않습니다.

9. Forward Net Directed Broadcasts를 사용하여 네트워크 지향 브로드캐스트 패킷을 처리하는 방법을 선택합니다.

   활성화를 선택하면 네트워크 지향 브로드캐스트가 전달됩니다.

   비활성화를 선택하면 삭제됩니다. 기본값은 비활성화입니다.

10. Encapsulation Type을 사용하여 지정된 인터페이스에서 전송되는 패킷에 대한 링크 계층 캡슐화 유형을 선택합니다.

    가능한 값은 Ethernet과 SNAP입니다. 기본값은 Ethernet입니다.

11. Proxy Arp를 사용하여 지정된 인터페이스에 대해 프록시 ARP를 Disable하거나 Enable합니다.

12. Local Proxy Arp를 사용하여 지정된 인터페이스에 대해 로컬 프록시 ARP를 Disable하거나 Enable합니다.

13. Bandwidth(kbps)을 사용하여 이 인터페이스에 구성된 대역폭을 지정합니다.

    이 매개변수는 인터페이스 속도를 더 높은 수준의 프로토콜에 전달합니다. OSPF는 대역폭을 사용하여 링크 비용을 계산합니다. 유효한 범위는 1~10000000입니다.

14. ICMP Destination Unreachable을 사용하여 이 인터페이스에서 ICMP 대상 도달 불가능을 보내는 모드를 지정합니다.

    비활성화된 경우 이 인터페이스는 ICMP 대상에 연결할 수 없음을 보내지 않습니다. 기본적으로 대상 도달 불가 모드가 활성화되어 있습니다.

15. ICMP 리디렉션을 사용하여 ICMP 리디렉션 모드를 Enable하거나 Disable합니다.

    라우터는 전역적으로나 인터페이스에서 리디렉션이 활성화된 경우에만 인터페이스에서 ICMP 리디렉션을 보냅니다. 기본적으로 ICMP 리디렉션 모드가 활성화되어 있습니다.

16. IP MTU를 사용하여 인터페이스에서 전송되는 IP 패킷의 최대 크기를 지정합니다.

    유효한 범위는 링크 MTU의 68바이트입니다. 기본값은 0입니다. 값 0은 IP MTU가 구성되지 않았음을 나타냅니다. IP MTU가 구성 해제되면 라우터는 링크 MTU를 IP MTU로 사용합니다. IP MTU는 최대 프레임 크기에서 레이어 2 헤더의 길이를 뺀 값입니다.

17. 선택한 인터페이스에서 IP 주소를 삭제하려면 Delete 버튼을 클릭합니다.

18. Apply 버튼을 클릭합니다

    업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표에서는 표시되는 구성할 수 없는 데이터에 대해 설명합니다.

Table 127. IP 인터페이스 구성

필드	설명
VLAN ID	인터페이스의 VLAN ID입니다.
OSPF Admin Mode	인터페이스의 OSPF 관리 모드를 표시합니다. 기본값은 비활성화입니다.
Link State	지정된 인터페이스의 상태는 활성 또는 비활성입니다. 링크가 작동 중이고 전달 상태인 경우 인터페이스는 활성 상태로 간주됩니다.
Routing Interface Status	링크 상태가 작동 중인지 작동 중지인지를 나타냅니다.

보조 IP 주소 구성

➢ **보조 IP 주소를 구성하려면:**

Routing > IP > Advanced > Secondary IP.

1. Routing Interface 목록에서 인터페이스를 선택합니다.
2. Secondary IP Address 필드에서 선택한 인터페이스에 보조 IP 주소를 추가합니다.
3. Secondary IP Subnet Mask 필드에 보조 IP 주소와 연결된 서브넷 마스크를 입력합니다.

   이는 서브넷/네트워크 마스크라고도 하며 연결된 네트워크를 식별하는 데 사용되는 인터페이스의 IP 주소 부분을 정의합니다. 이 값은 구성된 후에는 읽기 전용입니다.
4. Add 버튼을 클릭합니다.

   선택한 인터페이스의 보조 IP 주소가 추가됩니다.
5. 선택한 인터페이스에서 보조 IP 주소를 삭제하려면 Delete 버튼을 클릭합니다.

다음 표에서는 표시되는 구성할 수 없는 데이터에 대해 설명합니다.

Table 128. 보조 IP

필드	설명
VLAN ID	표시되거나 구성된 인터페이스와 연결된 VLAN ID입니다.
Primary IP Address	인터페이스의 기본 IP 주소입니다.

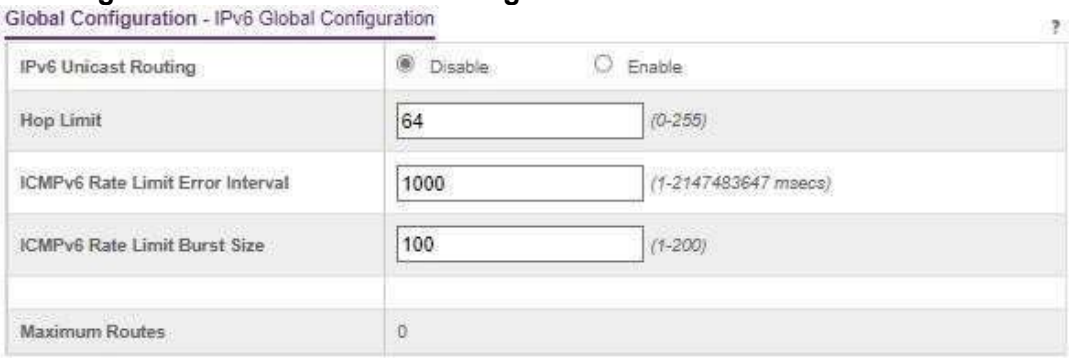
IPv6

IPv6 전역 설정 구성

인터페이스와 달리 스위치에 대한 IPv6 라우팅 매개변수를 구성할 수 있습니다.

➢ **IPv6 전역 설정을 구성하려면:**

Routing > IPv6 > Basic > Global Configuration.



1. IPv6 unicast Routing 필드에서 IPv6 유니캐스트 라우팅을 전역적으로 Enable 또는 Disable하는 옵션을 선택합니다.
2. Hop Limit 필드에 노드에서 시작된 IPv6 패킷에 사용되는 유니캐스트 홉 수 값을 입력합니다.

   이 값은 라우터 광고에도 포함됩니다. 홉의 유효한 값은 1~255입니다. 기본값은 구성되지 않음입니다. 이는 라우터 광고에서 0 값이 전송됨을 의미합니다.

3. ICMPv6 Rate Limit Error Interval 필드에서 버스트 간격당 허용되는 ICMP 오류 패킷 수를 지정합니다.

   이 값은 ICMPv6 오류 패킷을 제어합니다. 기본 속도 제한은 초당 100패킷입니다. 이는

버스트 간격이 1000밀리초임을 의미합니다. ICMP 속도 제한을 비활성화하려면 이 필드를 0으로 설정합니다. 유효한 속도 간격은 0~2147483647밀리초 범위에 있어야 합니다.

4. ICMPv6 Rate Limit Burst Size 필드에서 버스트 간격당 허용되는 ICMP 오류 패킷 수를 지정합니다.

   이 값은 ICMP 오류 패킷을 제어합니다. 기본 버스트 크기는 100패킷입니다. 버스트 간격이 0이면 이 필드를 구성하는 것은 유효한 작업이 아닙니다. 유효한 버스트 크기는 1~200입니다.

5. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

IPv6 경로 테이블 보기

➢ **IPv6 라우팅 테이블을 보려면:**

Routing > IPv6 > Basic > Route Table.

1. Routes Displayed 목록에서 다음 중 하나를 선택합니다.
   - **All Routes**. 모든 활성 IPv6 경로를 표시합니다.
   - **Best Routes Only**. 가장 좋은 활성 경로만 표시합니다.
   - **Configured Routes Only**. 사용자가 구성한 경로를 표시합니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표에서는 표시되는 구성할 수 없는 데이터에 대해 설명합니다.

Table 129. IPv6 경로 테이블

필드	설명
Number of Routes	경로 테이블의 총 활성 경로 수입니다.

IPv6 Prefix	활성 경로의 네트워크 접두사입니다.
Prefix Length	활성 경로의 접두사 길이입니다.
Protocol	활성 경로의 프로토콜 유형입니다.
Next Hop Interface	경로가 활성화된 인터페이스입니다. 거부 경로의 경우 다음 홉은 Null0 인터페이스가 됩니다.
Next Hop IP Address	활성 경로에 대한 다음 홉 IPv6 주소입니다.
Preference	구성된 경로의 경로 기본 설정입니다.

IPv6 인터페이스 설정 구성

➢ **IPv6 인터페이스 설정 구성:**

Routing > IPv6 > Advanced > Interface Configuration.

1. Go To Interface를 이용하여 유닛/슬롯/포트 형식의 인터페이스에 진입한 후 Go 버튼을 클릭합니다.

   지정된 인터페이스에 해당하는 항목이 선택됩니다.

2. Interface 옆에 있는 check box을 선택하여 선택합니다.
   모든 물리적 인터페이스가 유효합니다.

3. IPv6 Mode 목록에서 Enable 또는 Disable를 선택합니다.

   IPv6 모드가 활성화되면 인터페이스는 전역 주소 없이 IPv6 작업을 수행할 수 있습니다. 이 경우 EUI-64 기반의 링크-로컬 주소가 사용됩니다. 기본값은 Disable입니다.

4. DHCPv6 클라이언트 모드 목록에서 인터페이스의 DHCPv6 클라이언트 모드 Enable 또는 Disable를 선택합니다.

   언제든지 하나의 인터페이스만 클라이언트 역할을 할 수 있습니다. 기본값은 Disable입니다.

5. Stateless Address AutoConfig Mode(상태 비저장 주소 자동 구성 모드) 목록에서 인터페이스의 Stateless Address AutoConfig(상태 비저장 주소 자동 구성 모드) Enable 또는 Disable를 선택합니다.

   기본값은 Disable입니다.

6. Routing Mode 목록에서 인터페이스의 라우팅 모드를 Enable 또는 Disable하도록 선택합니다.

   기본값은 Disable입니다.

7. Admin Mode 목록에서 IPv6 모드 Enable 또는 Disable를 선택합니다.

   기본값은 Disable입니다. IPv6 모드가 활성화되면 인터페이스는 전역 주소 없이 IPv6 작업을 수행할 수 있습니다. 이 경우 EUI-64 기반의 링크-로컬 주소가 사용됩니다.

8. MTU 필드에서 인터페이스의 최대 전송 단위를 지정합니다.

   값이 0이면 이 인터페이스는 라우팅에 대해 활성화되지 않습니다. 라우팅이 활성화된 경우 이 값을 0으로 설정하는 것은 유효하지 않습니다. MTU 범위는 1280~1500입니다. 기본값은 1500입니다.

9. Duplicate Address Detection Transmits 필드에서 인터페이스의 DAD(중복 주소 감지) 전송 수를 지정합니다.

   DAD 전송 값은 0~600 범위에 있어야 합니다. 기본값은 1입니다.

10. 인터페이스에서 전송된 router advertisement Life Time Interval을 지정합니다.

    이 값은 최대 광고 간격보다 크거나 같아야 합니다. 0은 라우터를 기본 라우터로 사용하지 않음을 의미합니다. 라우터 수명 범위는 0~9000입니다. 기본값은 1800입니다.

11. Adv NS Interval 필드에서 인터페이스에서 보낸 라우터 광고의 재전송 시간 필드를 지정합니다..

    값이 0이면 라우터에 간격이 지정되지 않았음을 의미합니다. 인접 요청 간격의 범위는 1000~4294967295입니다. 기본값은 0입니다.

12. Adv Reachable Interval 필드에서 라우터 광고 시간을 지정합니다.

    이는 ND 확인 후 도달 가능한 이웃을 고려하기 위해 할당된 시간입니다. 도달 가능한 시간의 범위는 0~3600000 입니다. 기본값은 0 입니다.

13. Adv Interval 필드를 사용하여 인터페이스에서 라우터 광고 전송 사이에 허용되는 최대 시간을 지정합니다.

최대 광고 간격의 범위는 4~1800입니다. 기본값은 600입니다.

14. Adv Other Config Flag 목록에서 Enable 또는 Disable를 선택하여 라우터 광고 기타 상태 저장 구성 플래그를 지정합니다.

    기타 구성 플래그의 기본값은 비활성화입니다.

15. Adv Suppress Flag 목록에서 인터페이스에 대한 라우터 광고 억제를 Enable 또는 Disable하도록 선택합니다.

    억제 플래그의 기본값은 Disable입니다.

16. Destination Unreachable 목록에서 이 인터페이스에서 ICMPv6 대상에 연결할 수 없는 항목을 보내는 모드를 Enable 또는 Disable하도록 선택합니다.

    비활성화된 경우 이 인터페이스는 ICMPv6 예측 도달 불가능 항목을 보내지 않습니다. 기본적으로 IPv6 대상 도달 불가 모드가 Enable되어 있습니다.

17. Apply 버튼을 클릭합니다

    업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표에서는 표시되는 구성할 수 없는 데이터에 대해 설명합니다.

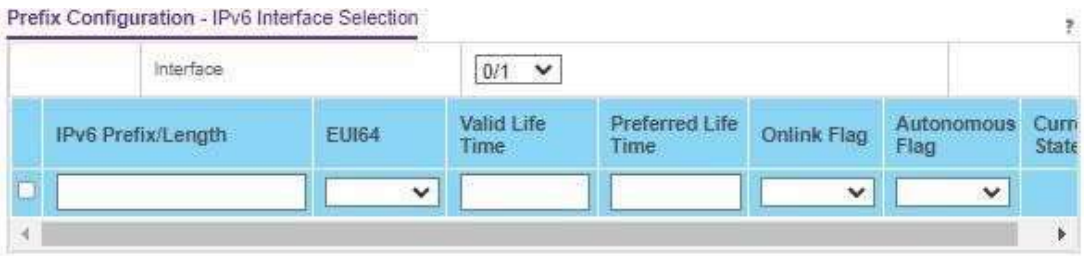
Table 130. IPv6 고급 인터페이스 구성

필드	설명
Operational Mode	인터페이스의 작동 상태를 지정합니다. 기본값은 비활성화입니다.
Link State	링크가 작동 중인지 작동 중지되었는지 여부를 나타냅니다.

IPv6 접두사 구성

➢ **IPv6 접두사 구성을 구성합니다:**

Routing > IPv6 > Advanced > Prefix Configuration.



1. Interface 목록에서 인터페이스를 선택합니다.

   선택 사항이 변경되면 화면 업데이트가 발생하여 새로 선택한 포트에 대해 모든 필드가 업데이트됩니다. 모든 물리적 인터페이스가 유효합니다.

2. IPv6 Prefix 필드에서 인터페이스의 IPv6 접두사를 지정합니다.
3. Prefix Length 필드에서 인터페이스의 IPv6 접두사 길이를 지정합니다.
4. EUI64 목록에서 지정된 64비트 유니캐스트 접두사를 Enable 또는 Disable하도록 선택합니다.
5. Valid Life Time 필드에서 접두사 시간당 라우터 광고를 지정합니다.

   이는 온링크 결정을 위해 유효한 접두어를 고려하는 데 허용되는 시간입니다. 유효한 수명 시간은 0~4294967295입니다.

6. Preferred Life Time 필드에서 접두사 시간별로 라우터 광고를 지정합니다.

   이 접두사에서 생성된 자동 구성된 주소가 선호됩니다. 기본 수명 시간은 0~4294967295 범위에 있어야 합니다.

7. Onlink Flag 목록에서 Enable 또는 Disable를 선택합니다.

   선택한 접두어를 온링크 결정에 사용할 수 있는지 여부를 지정합니다. 기본값은 Enable입니다.

8. Autonomouse Flag 목록에서 Enable 또는 Disable를 선택합니다.

   선택한 접두사를 자율 주소 구성에 사용할 수 있는지 여부를 지정합니다. 기본값은 Enable입니다.

9. Add 버튼을 클릭합니다.

   IPv6 주소가 인터페이스에 추가됩니다.

10. 인터페이스에서 기존 IPv6 주소 항목을 삭제하려면 Delete 버튼을 클릭합니다..
11. Apply 버튼을 클릭합니다

    업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

현재 상태 필드에는 IPV6 주소의 상태가 표시됩니다. 라우팅이 비활성화되거나 DAD가 실패하는 경우 상태는 TENT입니다. 인터페이스가 활성이고 DAD가 성공한 경우 상태는 활성입니다.

IPv6 통계 보기

- **IPv6 인터페이스 통계를 보려면:**
  Routing > IPv6 > Advanced > Statistics.

Statistics - IPv6 Statistics

Interface	ALL
Total Datagrams Received	0
Received Datagrams Locally Delivered	0
Received Datagrams Discarded Due To Header Errors	0
Received Datagrams Discarded Due To MTU	0
Received Datagrams Discarded Due To No Route	0
Received Datagrams With Unknown Protocol	0
Received Datagrams Discarded Due To Invalid Address	0
Received Datagrams Discarded Dut To Truncated Data	0
Received Datagrams Discarded Other	0
Received Datagrams Reassembly Required	0
Datagrams Successfully Reassembled	0
Datagrams Failed To Reassemble	0
Datagrams Forwarded	0
Datagrams Locally Trasmitted	0
Datagrams Transmit Failed	0
Datagrams Successfully Fragmented	0
Datagrams Failed To Fragment	0
Datagrams Fragments Created	0
Multicast Datagrams Received	0
Multicast Datagrams Transmitted	0

Statistics - ICMPv6 Statistics

Total ICMPv6 Messages Received	0
ICMPv6 Messages With Errors Received	0
ICMPv6 Destination Unreachable Messages Received	0
ICMPv6 Messages Prohibited Administratively Received	0
ICMPv6 Time Exceeded Messages Received	0
ICMPv6 Parameter Problem Messages Received	0
ICMPv6 Packet Too Big Messages Received	0
ICMPv6 Echo Request Messages Received	0
ICMPv6 Echo Reply Messages Received	0
ICMPv6 Router Solicit Messages Received	0
ICMPv6 Router Advertisement Messages Received	0
ICMPv6 Neighbor Solicit Messages Received	0
ICMPv6 Neighbor Advertisement Messages Received	0
ICMPv6 Redirect Messages Received	0
ICMPv6 Group Membership Query Messages Received	0
ICMPv6 Group Membership Response Messages Received	0
ICMPv6 Group Membership Reduction Messages Received	0
Total ICMPv6 Messages Transmitted	0
ICMPv6 Messages Not Transmitted Due To Error	0

ICMPv6 Destination Unreachable Messages Transmitted	0
ICMPv6 Messages Prohibited Administratively Transmitted	0
ICMPv6 Time Exceeded Messages Transmitted	0
ICMPv6 Parameter Problem Messages Transmitted	0
ICMPv6 Packet Too Big Messages Transmitted	0
ICMPv6 Echo Request Messages Transmitted	0
ICMPv6 Echo Reply Messages Transmitted	0
ICMPv6 Router Solicit Messages Transmitted	0
ICMPv6 Router Advertisement Messages Transmitted	0
ICMPv6 Neighbor Solicit Messages Transmitted	0
ICMPv6 Neighbor Advertisement Messages Transmitted	0
ICMPv6 Redirect Messages Transmitted	0
ICMPv6 Group Membership Query Messages Transmitted	0
ICMPv6 Group Membership Response Messages Transmitted	0
ICMPv6 Group Membership Reduction Messages Transmitted	0
ICMPv6 Duplicate Address Detects	0

1. 인터페이스 목록에서 인터페이스를 선택합니다.

   선택 사항이 변경되면 화면 새로 고침이 발생하여 새로 선택한 포트에 대해 모든 필드가

업데이트됩니다

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표에서는 표시되는 구성할 수 없는 데이터에 대해 설명합니다.

Table 131. IPv6 고급 인터페이스 통계

필드	설명
Total Datagrams Received	오류로 수신된 데이터그램을 포함하여 인터페이스에서 수신된 입력 데이터그램의 총 수입니다.
Received Datagrams Locally Delivered	IPv6 사용자 프로토콜(ICMP 포함)에 성공적으로 전달된 총 데이터그램 수입니다. 이 카운터는 이러한 데이터그램이 지정된 인터페이스에서 증가하며, 이는 일부 데이터그램에 대한 입력 인터페이스가 아닐 수도 있습니다.
Received Datagrams Discarded Due To Header Errors	버전 번호 불일치, 기타 형식 오류, 홉 수 초과, IPv6 옵션 처리 중 발견된 오류 등을 포함하여 IPv6 헤더의 오류로 인해 삭제된 입력 데이터그램 수입니다.
Received Datagrams Discarded Due To MTU	크기가 나가는 인터페이스의 링크 MTU를 초과하여 전달할 수 없는 입력 데이터그램 수입니다.
Received Datagrams Discarded Due To No Route	대상으로 전송할 경로를 찾을 수 없어 삭제된 입력 데이터그램 수입니다.
Received Datagrams With Unknown Protocol	성공적으로 수신되었지만 알 수 없거나 지원되지 않는 프로토콜로 인해 삭제된 로컬 주소가 지정된 데이터그램의 수입니다. 이 카운터는 이러한 데이터그램이 지정된 인터페이스에서 증가하며, 이는 일부 데이터그램에 대한 입력 인터페이스가 아닐 수도 있습니다.
Received Datagrams Discarded Due To Invalid Address	IPv6 헤더 대상 필드의 IPv6 주소가 이 엔터티에서 수신할 수 있는 유효한 주소가 아니기 때문에 삭제된 입력 데이터그램 수입니다. 이 수에는 잘못된 주소(예: ::0) 및 지원되지 않는 주소(예: 할당되지 않은 접두사가 있는 주소)가 포함됩니다. IPv6 라우터가 아니므로 데이터그램을 전달하지 않는 엔터티의 경우 이 카운터에는 대상 주소가 없기 때문에 삭제된 데이터그램이 포함됩니다. 현지 주소.
Received Datagrams Discarded Dut To Truncated Data	데이터그램 프레임에 충분한 데이터가 전달되지 않아 삭제된 입력 데이터그램 수입니다.
Received Datagrams Discarded Other	지속적인 처리를 방지하기 위해 문제가 발생하지 않았지만 버퍼 공간 부족 등의 이유로 폐기된 입력 IPv6 데이터그램 수입니다. 이 카운터에는 재조립을 기다리는 동안 폐기된 데이터그램이 포함되지 않습니다.

Received Datagrams Reassembly Required	이 인터페이스에서 재조립해야 하는 수신된 IPv6 조각 수입니다. 이 카운터는 이러한 조각이 처리된 인터페이스에서 증가하며, 이는 일부 조각의 입력 인터페이스가 아닐 수도 있습니다.
Datagrams Successfully Reassembled	성공적으로 재조립된 IPv6 데이터그램 수입니다. 이 카운터는 이러한 데이터그램이 처리된 인터페이스에서 증가하며, 이는 일부 조각의 입력 인터페이스일 필요는 없습니다.
Datagrams Failed To Reassemble	IPv6 리어셈블리 알고리즘에 의해 감지된 실패 횟수(이유에 관계없이: 시간 초과, 오류 등). 일부 알고리즘(특히 RFC 815의 알고리즘)은 조각이 수신될 때 조각을 결합하여 조각 수를 추적하지 못할 수 있으므로 이는 폐기된 IPv6 조각의 개수일 필요는 없습니다. 이 카운터는 이러한 조각이 처리된 인터페이스에서 증가하며, 이는 일부 조각의 입력 인터페이스가 아닐 수도 있습니다.
Datagrams Forwarded	이 엔터티가 수신하여 최종 대상으로 전달한 출력 데이터그램 수입니다. IPv6 라우터 역할을 하지 않는 엔터티에서 이 카운터에는 이 엔터티를 통해 소스 라우팅되었으며 소스 경로 처리가 성공한 패킷만 포함됩니다. 성공적으로 전달된 데이터그램의 경우 나가는 인터페이스의 카운터가 증가됩니다.
Datagrams Locally Transmitted	이 엔터티가 이 출력 인터페이스에서 성공적으로 전송한 데이터그램 수입니다.
Datagrams Transmit Failed	이 엔터티가 성공적으로 전송하지 못한 데이터그램 수입니다.
Datagrams Successfully Fragmented	이 출력 인터페이스에서 조각화된 IPv6 데이터그램 수입니다.
Datagrams Failed To Fragment	이 인터페이스에서 조각화할 수 없는 출력 데이터그램 수입니다.
Datagrams Fragments Created	이 출력 인터페이스에서 조각화의 결과로 생성된 출력 데이터그램 조각 수입니다.
Multicast Datagrams Received	인터페이스가 수신한 멀티캐스트 패킷 수입니다.
Multicast Datagrams Transmitted	인터페이스에서 전송된 멀티캐스트 패킷 수입니다.

다음 표에서는 표시되는 구성할 수 없는 데이터에 대해 설명합니다.

Table 132. ICMPv6 통계

필드	설명
Total ICMPv6 Messages Received	인터페이스에서 수신한 총 ICMP 메시지 수입니다. 여기에는 IPv6IfIcmpInErrors로 계산된 모든 메시지가 포함됩니다. 이 인터페이스는

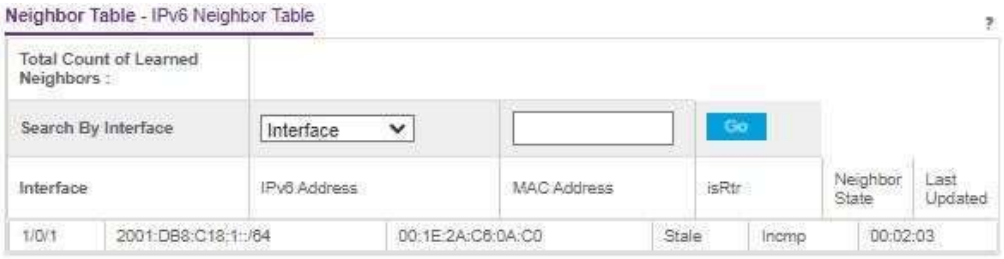
	ICMP 메시지가 처리된 인터페이스이며 메시지의 입력 인터페이스가 아닐 수도 있습니다.
ICMPv6 Messages With Errors Received	인터페이스가 수신했지만 ICMP 관련 오류(잘못된 ICMP 체크섬, 잘못된 길이 등)가 있는 것으로 확인된 ICMP 메시지 수입니다.
ICMPv6 Destination Unreachable Messages Received	인터페이스에서 수신한 ICMP 대상에 연결할 수 없는 메시지 수입니다.
ICMPv6 Messages Prohibited Administratively Received	인터페이스에서 수신한 ICMP 대상 도달 불가/통신 관리상 금지된 메시지 수입니다.
ICMPv6 Time Exceeded Messages Received	인터페이스에서 수신한 ICMP 시간 초과 메시지 수입니다.
ICMPv6 Parameter Problem Messages Received	인터페이스에서 수신한 ICMP 매개변수 문제 메시지 수입니다.
ICMPv6 Packet Too Big Messages Received	인터페이스에서 수신한 ICMP 패킷이 너무 큼 메시지 수입니다.
ICMPv6 Echo Request Messages Received	인터페이스에서 수신한 ICMP 에코(요청) 메시지 수입니다.
ICMPv6 Echo Reply Messages Received	인터페이스에서 수신한 ICMP 에코 응답 메시지 수입니다.
ICMPv6 Router Solicit Messages Received	인터페이스에서 수신한 ICMP Router Solicit 메시지 수입니다.
ICMPv6 Router Advertisement Messages Received	인터페이스에서 수신한 ICMP 라우터 알림 메시지 수입니다.
ICMPv6 Neighbor Solicit Messages Received	인터페이스에서 수신한 ICMP Neighbor Solicit 메시지 수입니다.
ICMPv6 Neighbor Advertisement Messages Received	인터페이스에서 수신한 ICMP 인접 광고 메시지 수입니다.
ICMPv6 Redirect Messages Received	인터페이스에서 수신한 ICMPv6 리디렉션 메시지 수입니다.
ICMPv6 Group Membership Query Messages Received	인터페이스에서 수신한 ICMPv6 그룹 멤버십 쿼리 메시지 수입니다.
ICMPv6 Group Membership Response Messages Received	인터페이스가 수신한 ICMPv6 그룹 멤버십 응답 메시지 수입니다.
ICMPv6 Group Membership Reduction Messages Received	인터페이스에서 수신한 ICMPv6 그룹 멤버십 감소 메시지 수입니다.
Total ICMPv6 Messages Transmitted	이 인터페이스가 전송을 시도한 총 ICMP 메시지 수입니다. 이 카운터에는 icmpOutErrors로 계산된 모든 항목이 포함됩니다.
ICMPv6 Messages Not Transmitted Due To Error	버퍼 부족 등 ICMP 내에서 발견된 문제로 인해 이 인터페이스가 전송하지 못한 ICMP 메시지 수입니다. 이 값에는 IPv6가 결과 데이터그램을 라우팅할 수 없는 것과 같이 ICMP 계층 외부에서 발견된 오류는 포함되지 않습니다. 일부 구현에서는 이 카운터 값에 영향을

	미치는 오류 유형이 없을 수 있습니다.
ICMPv6 Destination Unreachable Messages Transmitted	인터페이스에서 보낸 ICMP 대상에 연결할 수 없는 메시지 수입니다.
ICMPv6 Messages Prohibited Administratively Transmitted	전송된 ICMP 대상에 연결할 수 없음/관리적으로 금지된 통신 메시지 수입니다.
ICMPv6 Time Exceeded Messages Transmitted	인터페이스에서 보낸 ICMP 시간 초과 메시지 수입니다.
ICMPv6 Parameter Problem Messages Transmitted	인터페이스에서 보낸 ICMP 매개변수 문제 메시지 수입니다.
ICMPv6 Packet Too Big Messages Transmitted	인터페이스에서 보낸 ICMP 패킷이 너무 큼 메시지 수입니다.
ICMPv6 Echo Request Messages Transmitted	인터페이스에서 보낸 ICMP 에코(요청) 메시지 수입니다.
ICMPv6 Echo Reply Messages Transmitted	인터페이스에서 보낸 ICMP 에코 응답 메시지 수입니다.
ICMPv6 Router Solicit Messages Transmitted	인터페이스에서 보낸 ICMP 이웃 요청 메시지 수입니다.
ICMPv6 Router Advertisement Messages Transmitted	인터페이스에서 보낸 ICMP 라우터 알림 메시지 수입니다.
ICMPv6 Neighbor Solicit Messages Transmitted	인터페이스에서 보낸 ICMP 이웃 요청 메시지 수입니다.
ICMPv6 Neighbor Advertisement Messages Transmitted	인터페이스에서 보낸 ICMP 인접 광고 메시지 수입니다.
ICMPv6 Redirect Messages Transmitted	전송된 리디렉션 메시지 수입니다.
ICMPv6 Group Membership Query Messages Transmitted	전송된 ICMPv6 그룹 멤버십 쿼리 메시지 수입니다.
ICMPv6 Group Membership Response Messages Transmitted	전송된 ICMPv6 그룹 멤버십 응답 메시지 수입니다.
ICMPv6 Group Membership Reduction Messages Transmitted	전송된 ICMPv6 그룹 멤버십 감소 메시지 수입니다.
ICMPv6 Duplicate Address Detects	인터페이스가 감지한 중복 주소 수입니다.

IPv6 인접 테이블 보기

- **IPv6 인접 테이블을 보려면:**

  Routing > IPv6 > Advanced > Neighbor Table.



1. Search By Interface 필드를 사용하여 IPv6 주소 또는 인터페이스별로 IPv6 경로를 검색합니다.
   - IPv6 주소로 검색하려면 검색 기준 목록에서 IPv6 주소를 선택하세요. 128바이트 16진수 IPv6 주소를 콜론으로 구분된 4자리 그룹으로 입력합니다(예: 2001:231F:::1). 그런 다음 이동 버튼을 클릭하세요. 주소가 있으면 해당 항목이 표시됩니다. 정확하게 일치해야 합니다.
   - 인터페이스별로 검색하려면 검색 기준 목록에서 인터페이스를 선택하고 인터페이스 ID를 유닛/슬롯/포트 형식으로 입력합니다(예: 2/1/1). 그런 다음 이동 버튼을 클릭하세요. 주소가 있으면 해당 항목이 표시됩니다.

선택한 인터페이스 또는 모든 인터페이스에서 IPv6 인접 항목을 지우려면 Clear 버튼을 클릭합니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

다음 표에서는 표시되는 구성할 수 없는 데이터에 대해 설명합니다.

Table 133. IPv6 고급 이웃 테이블

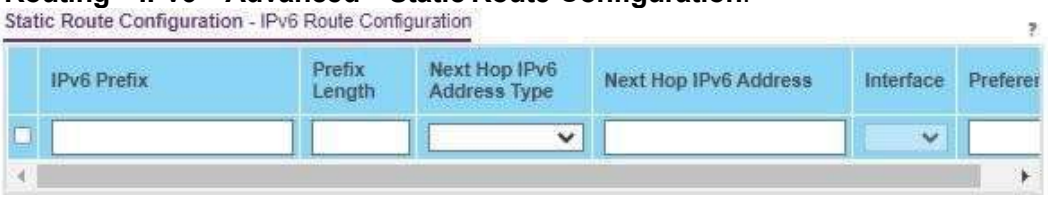
필드	설명
Interface	현재 테이블 행에 설정이 표시되는 인터페이스입니다.
IPv6 Address	이웃 또는 인터페이스의 IPv6 주소입니다.
MAC Address	인터페이스와 연결된 MAC 주소를 지정합니다.
isRtr	이웃이 라우터인지 여부를 나타냅니다. 이웃이 라우터인 경우 값은 True입니다. 이웃이 라우터가 아닌 경우 값은 False입니다.
Neighbor State	인접 캐시 항목의 상태입니다. 다음은 IPv6 인접 검색 캐시의 동적 항목 상태입니다. • **Incmp**. 항목에서 주소 확인이 수행되고 있습니다. 이웃 요청 메시지가 대상의 요청된 노드 멀티캐스트 주소로 전송되었지만 해당 이웃 광고 메시지가 아직 수신되지 않았습니다. • **Reach**. 이웃에 대한 전달 경로가 제대로 작동하고 있다는 긍정적인 확인이 마지막 연결 가능 시간(밀리초) 내에 수신되었습니다. REACH 상태에 있는 동안 장치는 패킷이 전송될 때 특별한 조치를

	취하지 않습니다. • **Stale**. 전달 경로가 제대로 작동하고 있다는 마지막 긍정적인 확인을 받은 이후 ReachableTime 밀리초 이상이 경과되었습니다. STALE 상태에 있는 동안 장치는 패킷이 전송될 때까지 아무런 조치도 취하지 않습니다. • **Delay**. 전달 경로가 제대로 작동하고 있다는 마지막 긍정적인 확인을 받은 이후 ReachableTime 밀리초 이상이 경과되었습니다. 마지막 DELAY_FIRST_PROBE_TIME초 내에 패킷이 전송되었습니다. DELAY 상태로 진입한 후 DELAY_FIRST_PROBE_TIME초 이내에 연결 가능성 확인이 수신되지 않으면 이웃 요청 메시지를 보내고 상태를 PROBE로 변경합니다. • **Probe**. 연결 가능성 확인이 수신될 때까지 RetransTimer 밀리초마다 이웃 요청 메시지를 다시 보내 연결 가능성 확인을 적극적으로 찾습니다.
Last Updated	주소에 접속 가능한 것으로 확인된 이후의 시간입니다.

IPv6 정적 경로 구성

➢ **IPv6 고정 경로를 구성합니다:**

Routing > IPv6 > Advanced > Static Route Configuration.



1. IPv6 Prefix 필드에서 구성된 경로에 대한 IPv6 접두사를 지정합니다.
2. Prefix Length 필드에서 구성된 경로에 대한 IPv6 접두사 길이를 지정합니다.
3. Next Hop IPv6 Address Type 목록에서 다음 옵션 중 하나를 선택합니다.
   - **Global IPv6 Address**.
   - **Link-Local** IPv6 address. 지정된 다음 홉 IPv6 주소가 링크-로컬 IPv6 주소인 경우 링크-로컬 IPv6 다음 홉 주소에 대한 인터페이스를 지정합니다.
   - **Static-Reject**. 대상 접두사에 대한 정적 거부 경로를 생성하려면 정적 거부를 선택합니다. 이 경우 다음 홉 주소가 지정되지 않습니다.
4. 구성된 경로에 대한 Next Hop IPv6 Address를 입력합니다.

5. Interface 목록에서 선택하여 유닛/슬롯/포트 형식으로 링크-로컬 IPv6 다음 홉 주소를 지정합니다.

   이 필드는 Link-Local이 선택된 경우에만 활성화됩니다.

6. 구성된 경로의 Preference 설정을 지정합니다.
7. Add 버튼을 클릭합니다

   경로가 추가됩니다.

8. 선택한 경로를 삭제하려면 삭제 버튼을 클릭하세요.

IPv6 경로 테이블 구성

➢ **IPv6 라우팅 테이블을 구성하려면:**

Routing > IPv6 > Advanced > Route Table.

1. 표시된 경로 필드의 다음 목록에서 표시할 경로를 선택합니다.
   - **All Routes**. 모든 활성 IPv6 경로를 표시합니다.
   - **Best Routes Only**. 가장 좋은 활성 경로만 표시합니다.
   - **Configured Routes Only**. 사용자가 구성한 경로를 표시합니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표에서는 표시되는 구성할 수 없는 데이터에 대해 설명합니다.

Table 134. IPv6 고급 경로 테이블

필드	설명
Number of Routes	경로 테이블의 총 활성 경로 수입니다.
IPv6 Prefix	활성 경로의 네트워크 접두사입니다.
Prefix Length	활성 경로의 접두사 길이입니다.
Protocol	활성 경로의 프로토콜 유형입니다.

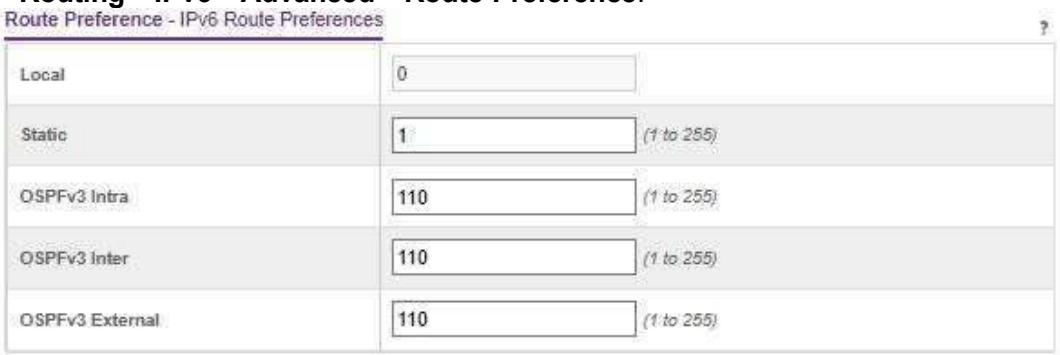
Next Hop Interface	경로가 활성화된 인터페이스입니다. 거부 경로의 경우 다음 홉은 Null0 인터페이스가 됩니다.
Next Hop IP Address	활성 경로에 대한 다음 홉 IPv6 주소입니다.
Preference	구성된 경로의 경로 기본 설정입니다.

IPv6 경로 기본 설정

이 화면을 사용하여 각 프로토콜에 대한 기본 기본 설정을 구성합니다. 이러한 값은 1~255 범위의 임의 값이며 경로 메트릭과 무관합니다. 대부분의 라우팅 프로토콜은 경로 메트릭을 사용하여 다른 프로토콜과 관계없이 프로토콜에 알려진 최단 경로를 결정합니다. 선호도 값이 가장 낮은 경로를 선택하여 목적지까지 최적의 경로를 선택합니다. 목적지까지의 경로가 여러 개인 경우 기본 설정 값을 사용하여 기본 경로를 결정합니다. 여전히 동점인 경우 경로 메트릭이 가장 좋은 경로가 선택됩니다. 메트릭 불일치 문제를 방지하려면 각 프로토콜에 대해 서로 다른 기본 설정 값을 구성해야 합니다.

➢ **IPv6 경로 기본 설정을 구성합니다.**

Routing > IPv6 > Advanced > Route Preference.



1. Static 필드에서 라우터에 대한 정적 경로 기본 설정 값을 지정합니다.
   범위는 1~255입니다. 기본값은 1입니다.

2. OSPFv3 Intra 필드에서 라우터의 OSPFv3 인트라 경로 기본 설정 값을 지정합니다.
   범위는 1~255입니다. 기본값은 110입니다.

3. OSPFv3 Inter 필드에서 라우터의 OSPFv3 Inter 경로 기본 설정 값을 지정합니다.
   범위는 1~255입니다. 기본값은 110입니다.

4. OSPFv3 External 필드에서 라우터의 OSPFv3 외부 경로 기본 설정 값을 지정합니다.

범위는 1~255입니다. 기본값은 110입니다.

5. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

   Local 필드에는 로컬 기본 설정이 표시됩니다.

IPv6 터널 구성

터널을 생성, 구성 및 삭제할 수 있습니다.

➢ **IPv6 터널을 구성하려면:**

Routing > IPv6 > Advanced > Tunnel Configuration.

1. Tunnel ID 필드의 사용 가능한 터널 ID 목록에서 선택합니다.
2. Mode 목록에서 지원되는 모드를 선택합니다.
   - 6-in-4-configured
   - 6-to-4
3. 목록에서 IPv6 Mode를 선택합니다.
4. IPv6 주소를 사용하여 이 인터페이스에서 IPv6을 Enable합니다.

   이 옵션은 명시적인 IPv6 주소를 지정할 때까지만 구성할 수 있습니다.

5. IPv6 Unreachable 항목 목록에서 Enable 또는Disable를 선택합니다.

   이는 이 인터페이스에서 ICMPv6 대상 연결 불가 항목을 보내는 모드를 지정합니다. 비활성화를 선택하면 이 인터페이스는 ICMPv6 대상에 연결할 수 없음을 보내지 않습니다. 기본적으로 IPv6 대상 도달 불가 모드가 Enable되어 있습니다.

6. IPv6 주소/접두사 길이 필드에 선택한 인터페이스에 대해 구성된 IPv6 주소를 입력합니다.

   주소는 접두사/길이 형식으로 입력해야 합니다.

7. EUI64 목록에서 64비트 확장 고유 식별자(EUI-64)를 Enable 또는 Disable 하도록 선택합니다.

6to4 터널의 경우 2002:tunnel-source-IPv4-address::/48 형식의 첫 번째 48비트로 IPv6 주소를 구성합니다.

8. 이 터널에 대해 원하는 소스 주소를 지정합니다.

   이 값은 점으로 구분된 십진수 표기법으로 입력해야 합니다.

9. 이 터널의 Source Interface를 선택합니다.

   선택한 인터페이스와 연결된 주소가 소스 주소로 사용됩니다.

10. 점으로 구분된 십진수 표기법으로 이 터널의 대상 주소를 입력합니다.
11. Add 버튼을 클릭합니다.

    터널이 추가됩니다.

12. 선택한 터널을 삭제하려면 Delete 버튼을 클릭합니다.
13. Apply 버튼을 클릭합니다

    업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

Interface Link Status 필드는 터널 인터페이스가 작동 중인지 작동 중지되었는지 여부를 나타냅니다.

VLAN 개요

VLAN을 지원하는 일부 포트와 라우팅을 지원하는 일부 포트로 소프트웨어를 구성할 수 있습니다. VLAN의 트래픽이 마치 VLAN이 라우터 포트인 것처럼 처리되도록 소프트웨어를 구성할 수도 있습니다.

포트가 라우팅이 아닌 브리징(기본값)에 대해 활성화되면 인바운드 패킷에 대해 모든 일반 브리지 처리가 수행된 다음 VLAN과 연결됩니다. MAC 대상 주소(MAC DA)와 VLAN ID는 MAC 주소 테이블을 검색하는 데 사용됩니다. VLAN에 대해 라우팅이 활성화되고 인바운드 유니캐스트 패킷의 MAC DA가 내부 브리지-라우터 인터페이스의 MAC DA인 경우 패킷이 라우팅됩니다. 인바운드 멀티캐스트 패킷은 VLAN의 모든 포트와 내부 브리지-라우터 인터페이스(라우팅된 VLAN에서 수신된 경우)로 전달됩니다.

포트는 둘 이상의 VLAN에 속하도록 구성될 수 있으므로 포트의 모든 VLAN 또는 하위 집합에 대해 VLAN 라우팅이 활성화될 수 있습니다. VLAN 라우팅을 사용하면 둘 이상의 물리적 포트가 동일한 서브넷에 상주할 수 있습니다. VLAN이 여러 물리적 네트워크에 걸쳐 있거나

추가 분할 또는 보안이 필요한 경우에도 사용할 수 있습니다. 이 섹션에서는 VLAN 라우팅을 지원하도록 스위치를 구성하는 방법을 보여줍니다. 포트는 VLAN 포트 또는 라우터 포트일 수 있지만 둘 다일 수는 없습니다. 그러나 VLAN 포트는 라우터 포트인 VLAN의 일부일 수 있습니다.

VLAN 라우팅 구성

➢ **VLAN 라우팅을 구성하려면:**

Routing > VLAN > VLAN Routing.

1. VLAN ID를 선택합니다.

   이 필드에는 이 스위치에 구성된 모든 VLAN의 ID가 표시됩니다.

2. IP Address를 사용하여 VLAN 라우팅 인터페이스에 대해 구성할 IP 주소를 입력합니다.
3. Subnet Mask를 사용하여 VLAN 라우팅 인터페이스에 대해 구성할 서브넷 마스크를 입력합니다.
4. Add 버튼을 클릭합니다.

   선택한 VLAN ID에 대해 VLAN 라우팅 인터페이스가 추가됩니다.

5. VLAN ID 필드에서 선택한 VLAN 라우팅 인터페이스를 제거하려면 Delete 버튼을 클릭합니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 135. VLAN 라우팅 구성

필드	설명
Port	라우팅을 위해 VLAN에 할당된 인터페이스입니다.
MAC Address	VLAN 라우팅 인터페이스에 할당된 MAC 주소입니다.

ARP (주소 확인 프로토콜) 개요

ARP(주소 확인 프로토콜)는 레이어 2 MAC 주소를 레이어 3 IPv4 주소와 연결합니다. 소프트웨어는

동적 및 수동 ARP 구성을 모두 제공합니다. 수동 ARP 구성을 사용하면 ARP 테이블에 항목을 정적으로 추가할 수 있습니다.

ARP는 인터넷 프로토콜(IP)의 필수 부분이며 IP 주소를 이더넷과 같은 근거리 통신망(LAN)에서 정의하는 미디어(MAC) 주소로 변환하는 데 사용됩니다. IP 패킷을 보내야 하는 스테이션은 IP 대상의 MAC 주소 또는 대상이 동일한 서브넷에 없는 경우 다음 홉 라우터의 MAC 주소를 알아야 합니다. 이는 의도된 수신자가 MAC 주소가 포함된 ARP 응답을 유니캐스팅하여 응답하는 ARP 요청 패킷을 브로드캐스트함으로써 달성됩니다. 학습된 MAC 주소는 IP 패킷 앞에 추가된 계층 2 헤더의 대상 주소 필드에 사용됩니다.

ARP 캐시는 네트워크의 각 스테이션에서 로컬로 유지 관리되는 테이블입니다. ARP 캐시 항목은 ARP 요청인지 응답인지에 관계없이 ARP 패킷 페이로드 필드의 소스 정보를 검사하여 학습됩니다. 따라서 ARP 요청이 LAN 세그먼트 또는 가상 LAN(VLAN)의 모든 스테이션에 브로드캐스트되면 각 수신자는 발신자의 IP 및 MAC 주소를 해당 ARP 캐시에 저장할 수 있습니다. 유니캐스트인 ARP 응답은 일반적으로 ARP 캐시에 보낸 사람 정보를 저장하는 요청자에게만 표시됩니다. 최신 정보는 항상 ARP 캐시의 기존 콘텐츠를 대체합니다.

지원되는 ARP 항목 수는 플랫폼에 따라 다릅니다.

장치는 네트워크에서 이동할 수 있습니다. 즉, 한때 특정 MAC 주소와 연결되었던 IP 주소가 이제 다른 MAC을 사용하여 발견되거나 네트워크에서 완전히 사라졌습니다(예: 재구성, 연결 해제, 또는 전원이 꺼져 있음). 이로 인해 네트워크에 표시되는 새로운 정보에 대한 반응으로 항목이 업데이트되거나, 주소가 여전히 존재하는지 확인하기 위해 주기적으로 새로 고쳐지거나, 항목이 ARP 패킷의 보낸 사람으로 식별된 경우 캐시에서 제거되지 않는 한 ARP 캐시에 오래된 정보가 발생합니다. 일반적으로 구성을 통해 지정되는 만료 기간 동안입니다.

기본 ARP 캐시 구성

이 화면을 사용하여 ARP 캐시의 ARP 항목을 표시합니다.

- **ARP 캐시에 ARP 항목을 표시하려면:**
  Routing > ARP > Basic > ARP Cache.

1. IP Address는 시스템의 MAC 주소와 연관된 IP 주소를 표시합니다.

   스위치의 기존 라우팅 인터페이스 중 하나에 연결된 서브넷에 있는 장치의 IP 주소여야 합니다.

2. Port 필드에는 연결의 관련 장치/슬롯/포트가 표시됩니다.

3. MAC Address는 장치의 유니캐스트 MAC 주소를 표시합니다. 주소는 콜론으로 구분된 6개의 2자리 16진수입니다(예: 00:06:29:32:81:40).

스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

페이지 매김 탐색 메뉴

- Rows per screen — 화면당 표시되는 테이블 항목 수를 선택합니다. 가능한 값은 50, 100, 500, 1000 및 모두입니다.

  Note: 모두를 선택하면 브라우저에 정보가 표시되는 속도가 느려질 수 있습니다.

- < 테이블 데이터 항목의 이전 화면을 표시합니다.
- > 테이블 데이터 항목의 다음 화면을 표시합니다.

ARP 테이블에 항목 추가

ARP(주소 확인 프로토콜) 테이블에 항목을 추가할 수 있습니다.

➢ **ARP 테이블에 항목을 추가하려면:**

Routing > ARP > Advanced > ARP Create.

1. IP Address를 이용하여 추가할 IP 주소를 입력하세요.

스위치의 기존 라우팅 인터페이스 중 하나에 연결된 서브넷에 있는 장치의 IP 주소여야 합니다.

2. MAC Address를 사용하여 장치의 유니캐스트 MAC 주소를 지정합니다.

   콜론으로 구분된 6개의 2자리 16진수로 주소를 입력합니다(예: 00:06:29:32:81:40).

3. Add 버튼을 클릭합니다.

   고정 ARP 항목이 스위치에 추가됩니다.

4. 스위치에서 선택한 고정 ARP 항목을 삭제하려면 Delete 버튼을 클릭합니다.

5. Apply 버튼을 클릭합니다

   IP에 대한 MAC 주소 매핑이 변경됩니다. 구성 변경 사항은 즉시 적용됩니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 136. ARP 캐시

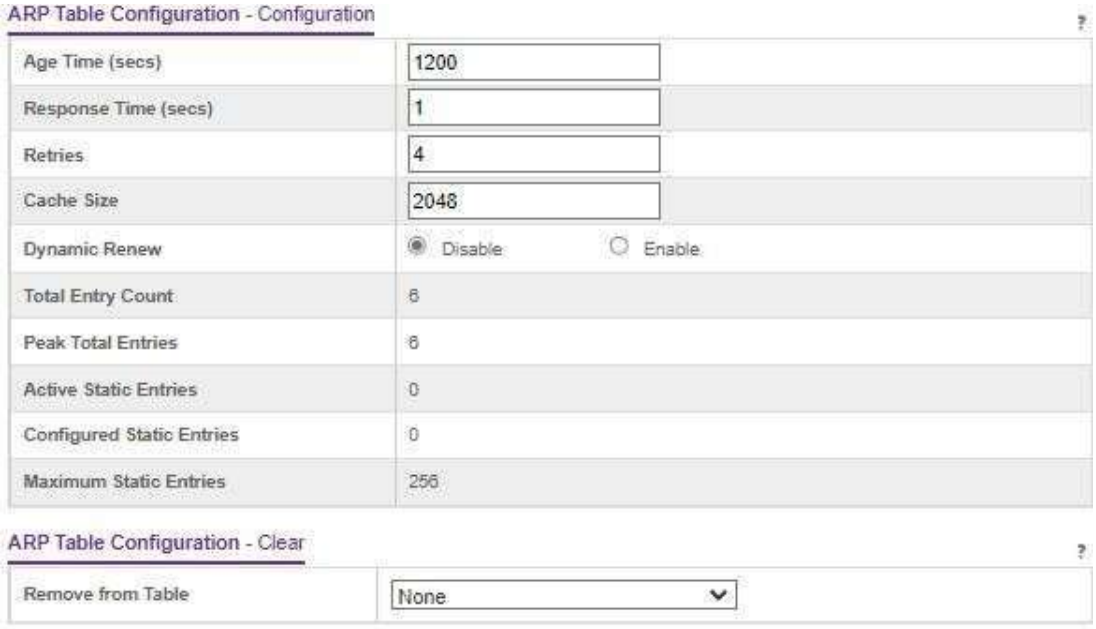
필드	설명
Port	연결의 관련 장치/슬롯/포트입니다.
IP Address	IP 주소입니다. 스위치의 기존 라우팅 인터페이스 중 하나에 연결된 서브넷에 있는 장치의 IP 주소여야 합니다.
Port	연결의 관련 장치/슬롯/포트입니다.
MAC Address	장치의 유니캐스트 MAC 주소입니다. 주소는 콜론으로 구분된 6개의 2자리 16진수입니다(예: 00:06:29:32:81:40).
Type	ARP 항목의 유형입니다. 가능한 값은 다음과 같습니다. • **Local**. 스위치의 라우팅 인터페이스 MAC 주소 중 하나와 연결된 ARP 항목입니다. • **Gateway**. IP 주소가 라우터의 주소인 동적 ARP 항목입니다. • **Static**. 사용자가 구성한 ARP 항목입니다.. • **Dynamic**. 라우터가 학습한 ARP 항목입니다.
Age	ARP 테이블에서 항목이 마지막으로 새로 고쳐진 이후의 경과 기간(초)입니다.

ARP 테이블 보기 또는 구성

ARP(주소 확인 프로토콜) 테이블의 구성 매개변수를 변경할 수 있습니다. 이 화면을 사용하여 테이블의 내용을 표시할 수도 있습니다.

➢ **ARP 테이블을 구성하려면:**

Routing > ARP > Advanced > ARP Table Configuration.



1. Age Time을 사용하여 ARP 항목 만료 시간에 사용할 스위치 값을 입력합니다.

   ARP 항목이 만료되는 데 걸리는 시간(초)을 나타내는 유효한 정수를 입력해야 합니다. 이 필드의 범위는 15~21600초입니다. 보존 시간의 기본값은 1200초입니다.

2. Response Time(응답 시간)을 사용하여 ARP 응답 시간 초과에 사용할 스위치 값을 입력합니다.

   스위치가 ARP 요청에 대한 응답을 기다리는 시간(초)을 나타내는 유효한 정수를 입력해야 합니다. 이 필드의 범위는 1~10초입니다. 기본값은 1초입니다.

3. Retries를 사용하여 ARP 요청이 재시도되는 최대 횟수를 지정하는 정수를 입력합니다.

   이 필드의 범위는 0~10입니다. 재시도의 기본값은 4입니다.

4. Cache Size를 사용하여 ARP 캐시의 최대 항목 수를 지정하는 정수를 입력합니다.

   이 필드의 범위는 64~6144입니다. 캐시 크기의 기본값은 2000입니다.

5. Dynamic Renew을 사용하여 ARP 구성 요소가 만료된 동적 유형의 ARP 항목을 자동으로 갱신하려고 시도할지 여부를 제어합니다.

   기본 설정은 Enable입니다.

6. Remove from table을 사용하여 ARP 테이블에서 삭제할 특정항목을 제거합니다

   나열된 선택 사항은 삭제할 ARP 항목의 유형을 지정합니다.
   - **All Dynamic Entries**
   - **All Dynamic and Gateway Entries**
   - **Specific Dynamic/Gateway Entry**. 이를 선택하면 사용자가 필요한 IP 주소를 지정할 수 있습니다.
   - **Specific Static Entry**. 이를 선택하면 사용자가 필요한 IP 주소를 지정할 수 있습니다.
   - **None.** 사용자가 ARP 테이블에서 항목을 삭제하지 않으려는 경우 선택됩니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 137. ARP 테이블 구성

필드	설명
Total Entry Count	ARP 테이블의 총 항목 수입니다.
Peak Total Entries	총 항목 수에 도달한 최고 값입니다. 이 카운터 값은 ARP 테이블 캐시 크기 값이 변경될 때마다 다시 시작됩니다.
Active Static Entries	ARP 테이블의 총 활성 정적 항목 수입니다.
Configured Static Entries	ARP 테이블에 구성된 정적 항목의 총 개수입니다.
Maximum Static Entries	정의할 수 있는 최대 정적 항목 수입니다.

서비스 품질 구성 5

이 장에서는 다음 주제를 다룹니다.

- *QoS 개요*
- *서비스 등급*
- *차별화된 서비스 개요*

QoS 개요

일반적인 스위치에서 각 물리적 포트는 연결된 네트워크에서 패킷을 전송하기 위한 하나 이상의 대기열로 구성됩니다. 사용자 정의 기준에 따라 다른 패킷보다 특정 패킷에 우선권을 부여하기 위해 포트당 여러 대기열이 제공되는 경우가 많습니다. 패킷이 전송을 위해 포트에 대기할 때 서비스되는 속도는 대기열이 구성된 방식과 포트의 다른 대기열에 있는 트래픽 양에 따라 달라집니다. 지연이 필요한 경우 스케줄러가 대기열에 전송을 승인할 때까지 패킷은 대기열에 보관됩니다. 대기열이 가득 차면 전송을 위해 패킷을 보관할 수 없으며 스위치에서 삭제됩니다.

QoS는 엄격한 타이밍 요구 사항이 있는 패킷과 지연을 더 잘 견딜 수 있는 패킷을 구별하여 일관되고 예측 가능한 데이터 전달을 제공하는 수단입니다. 엄격한 타이밍 요구 사항이 있는 패킷은 QoS 가능 네트워크에서 특별하게 처리됩니다. 이를 염두에 두고 네트워크의 모든 요소는 QoS를 지원해야 합니다. QoS를 지원하지 않는 노드가 하나 이상 있으면 네트워크 경로에 결함이 발생하고 전체 패킷 흐름의 성능이 저하됩니다.

서비스 등급

CoS(서비스 클래스) 대기열 기능을 사용하면 스위치 대기열의 특정 측면을 직접 구성할 수 있습니다. 이는 DiffServ의 복잡성이 필요하지 않은 경우 다양한 유형의 네트워크 트래픽에 대해 원하는 QoS 동작을 제공합니다. 인터페이스에 도착하는 패킷의 우선 순위는 매핑 테이블을 통해 패킷을 적절한 아웃바운드 CoS 대기열로 조정하는 데 사용될 수 있습니다. 최소 보장 대역폭, 전송 속도 조절 등 대기열 매핑에 영향을 미치는 CoS 대기열 특성은 대기열(또는 포트) 수준에서 사용자가 구성할 수 있습니다.

포트당 8개의 대기열이 지원됩니다.

CoS를 사용하여 인터페이스의 서비스 클래스 신뢰 모드를 설정합니다. 스위치의 각 포트는 패킷 필드(802.1p 또는 IP DSCP) 중 하나를 신뢰하거나 패킷의 우선 순위 지정을 신뢰하지 않도록(신뢰할 수 없는 모드) 구성될 수 있습니다. 포트가 신뢰할 수 있는 모드로 설정된 경우 사용 중인 신뢰할 수 있는 필드에 적합한 매핑 테이블을 사용합니다. 이 매핑 테이블은 해당 송신 포트에서 패킷이 전달되는 CoS 대기열을 나타냅니다. 물론 매핑 테이블을 사용하려면 패킷에 신뢰할 수 있는 필드가 있어야 하므로 그렇지 않은 경우 기본 작업이 수행됩니다. 이러한 작업에는 현재 802.1p 매핑 테이블에 의해 트래픽 클래스에 매핑된 기존 포트 기본

1.5 cm

우선 순위를 기반으로 수신 포트 전체에 대해 구성된 특정 CoS 수준으로 패킷을 보내는 작업이 포함됩니다.

또는 포트가 신뢰할 수 없음으로 구성되면 들어오는 패킷 우선 순위 지정을 신뢰하지 않고 대신 포트 기본 우선 순위 값을 사용합니다. 신뢰할 수 없는 포트의 수신에 도착하는 모든 패킷은 수신 포트에 구성된 기본 우선 순위에 따라 적절한 송신 포트의 특정 CoS 대기열로 전달됩니다. 이 프로세스는 IP DSCP 값을 신뢰하도록 구성된 포트에 비IP 패킷이 도착하는 경우와 같이 신뢰할 수 있는 포트 매핑을 적용할 수 없는 경우에도 사용됩니다.

글로벌 CoS 설정 구성

➢ **글로벌 CoS 설정을 구성하려면:**

QoS > Basic > CoS Configuration.

Note: 다음을 선택하여 이 화면으로 이동할 수도 있습니다. **QoS > CoS > Advanced > CoS Configuration**.

1. Global을 사용하여 CoS 구성 가능 인터페이스를 모두 지정합니다.

   글로벌 옵션은 가장 최근의 글로벌 구성 설정을 나타냅니다.

2. Interface를 사용하여 인터페이스별로 CoS 구성 설정을 지정합니다.

3. Global Trust Mode를 사용하여 수신 시 특정 패킷 표시를 신뢰할지 여부를 지정합니다.

   글로벌 신뢰 모드는 다음 중 하나일 수 있습니다.
   - untrusted
   - trust dot1p
   - trust ip-dscp

   기본값은 trust dot1p입니다.

4. Interface Trust Mode를 사용하여 수신 시 특정 패킷 표시를 신뢰할지 여부를 지정합니다.

   인터페이스 신뢰 모드는 다음 중 하나일 수 있습니다.
   - untrusted

1.5 cm

- trust dot1p
- trust ip-dscp

기본값은 untrusted입니다.

5. Apply 버튼을 클릭합니다

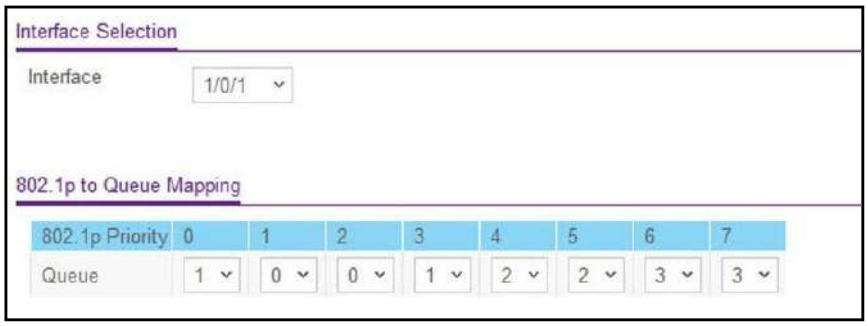
   업데이트된 구성이 스위치로 전송됩니다.

802.1p 우선순위를 대기열에 매핑

802.1p 대 대기열 매핑 화면에는 현재 802.1p 우선 순위 매핑 테이블도 표시됩니다.

➢ **802.1p 우선순위를 대기열에 매핑하려면:**

QoS > CoS > Advanced > 802.1p to Queue Mapping.



1. Interface를 사용하여 인터페이스를 선택합니다.

   인터페이스별로 또는 모든 CoS 구성 가능 인터페이스에 대해 CoS 구성 설정을 지정할 수 있습니다.

2. 해당 802.1p 값을 매핑할 내부 트래픽 클래스를 지정합니다.

   대기열 번호는 특정 하드웨어에 따라 다릅니다. 802.1p 우선 순위 행에는 매핑할 8개의 802.1p 우선 순위 각각에 대한 트래픽 클래스 선택기가 포함되어 있습니다. 우선순위는 낮음(0)에서 높음(3)으로 지정됩니다. 예를 들어 우선순위가 0인 트래픽은 대부분의 데이터 트래픽에 대한 것이며 최선을 다해 전송됩니다. 3과 같이 우선순위가 더 높은 트래픽은

   음성이나 영상과 같이 시간에 민감한 트래픽입니다.

   각 목록의 값은 트래픽 클래스를 나타냅니다. 트래픽 클래스는 포트의 하드웨어 대기열입니다. 트래픽 클래스 값이 높을수록 대기열 위치가 더 높다는 것을 나타냅니다.

1.5 cm

낮은 대기열의 트래픽이 전송되기 전에 상위 대기열의 트래픽이 전송될 때까지 기다려야 합니다.

3. Apply 버튼을 클릭합니다

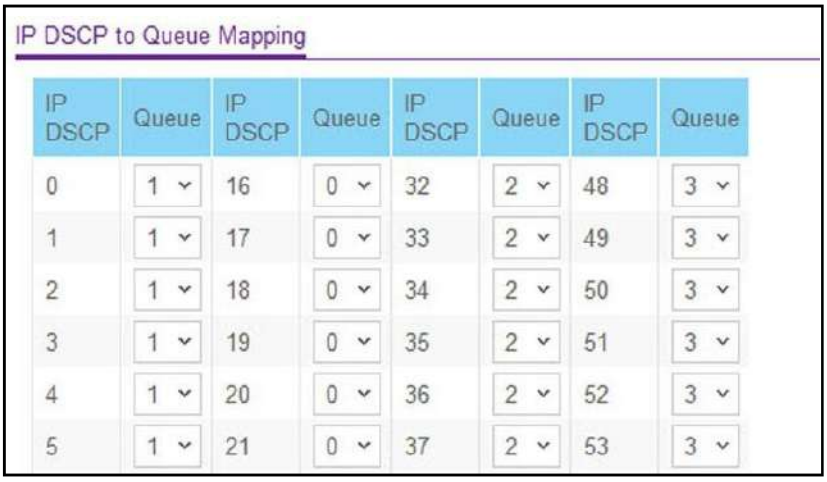
   업데이트된 구성이 스위치로 전송됩니다.

DSCP 값을 대기열에 매핑

해당 DSCP 값을 매핑할 내부 트래픽 클래스를 지정할 수 있습니다.

➢ **DSCP 값을 대기열에 매핑하려면:**

QoS > CoS > Advanced > IP DSCP to Queue Mapping.



IP DSCP 필드에는 0부터 63까지의 IP DSCP 값이 표시됩니다.

1. 각 DSCP 값에 대해 해당 IP DSCP 값을 매핑할 내부 트래픽 클래스를 지정합니다.

   대기열 번호는 특정 하드웨어에 따라 다릅니다.

2. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

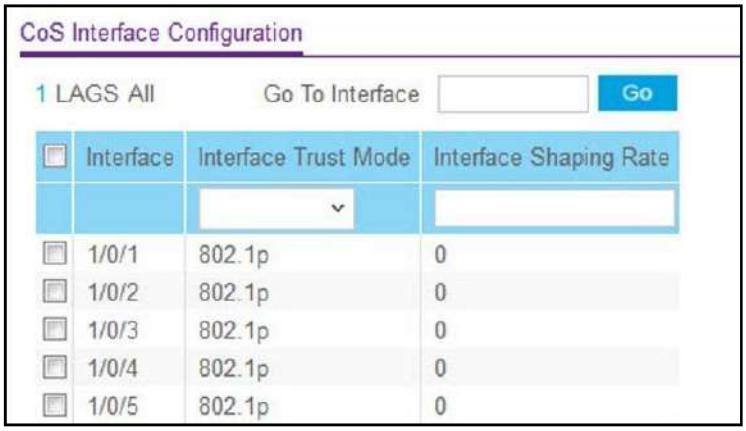
인터페이스에 대한 CoS 인터페이스 설정 구성

모든 인터페이스 또는 특정 인터페이스에 인터페이스 형성 속도를 적용할 수 있습니다.

1.5 cm

- **인터페이스에 대한 CoS 설정을 구성하려면:**

  QoS > CoS> Advanced > CoS Interface Configuration.



1. 모든 LAG 인터페이스 목록을 표시하려면 LAG를 선택합니다.
2. 모든 물리적 인터페이스와 LAG 인터페이스 목록을 표시하려면 All를 선택합니다.
3. 모든 CoS 구성 가능 인터페이스의 인터페이스 목록에서 Interface를 선택합니다.
4. Go To Interface 필드를 사용하여 장치/슬롯/포트 형식의 인터페이스를 입력하고 Go 버튼을 클릭합니다.

   지정된 인터페이스에 해당하는 항목이 선택됩니다.

5. Interface Trust Mode를 사용하여 수신 시 특정 패킷 표시를 신뢰할지 여부를 지정합니다.

   인터페이스 신뢰 모드는 다음 중 하나일 수 있습니다.

   - Untrusted
   - 802.1p
   - IP DSCP

   기본값은 802.1p입니다.

6. Interface Shaping Rate를 사용하여 허용되는 최대 대역폭을 지정합니다.

   이는 일반적으로 아웃바운드 전송 속도를 형성하는 데 사용됩니다. 이 값은 큐당 최대 대역폭 구성과 독립적으로 제어됩니다. 이는 사실상 두 번째 수준의 성형 메커니즘입니다. 기본값은 0입니다. 유효 범위는 0~100이며 1씩 증가합니다. 값 0은 최대값이 무제한임을 의미합니다.

7. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

1.5 cm

인터페이스에 대한 CoS 대기열 설정 구성

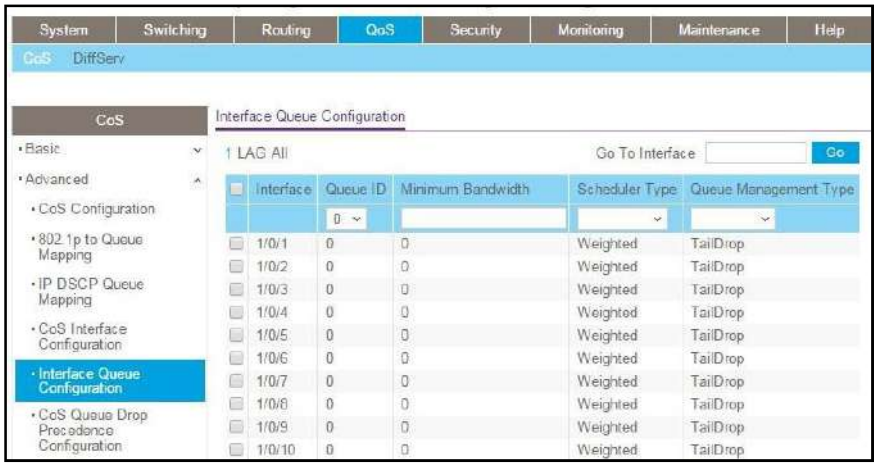
스위치 송신 대기열을 구성하여 특정 대기열이 수행하는 작업을 정의할 수 있습니다.

사용자가 구성할 수 있는 매개변수는 대기열에서 사용하는 대역폭의 양, 혼잡 시간 동안의 대기열 깊이 및 포트의 모든 대기열 집합에서 패킷 전송 일정을 제어합니다. 각 포트에는 자체 CoS 대기열 관련 구성이 있습니다.

각 CoS 대기열 매개변수를 전역적으로 또는 포트별로 구성할 수 있으므로 구성 프로세스가 단순화됩니다. 전역 구성 변경 사항은 시스템의 모든 포트에 자동으로 적용됩니다.

➢ **인터페이스에 대한 CoS 대기열 설정을 구성하려면 다음을 수행하십시오.**

QoS > CoS >Advanced > Interface Queue Configuration.



1. 구성할 포트 또는 LAG 옆의 check box을 선택합니다.

   여러 포트와 LAG를 선택하여 선택한 인터페이스에 동일한 설정을 적용할 수 있습니다. 모든 인터페이스에 신뢰 모드 또는 속도를 적용하려면 제목 행의 check box을 선택합니다.

2. Queue ID 메뉴를 사용하여 구성할 대기열(플랫폼 기반)을 선택합니다.
3. Minimum Bandwidth을 사용하여 이 대기열에 할당된 최소 보장 대역폭을 지정합니다.

   이 값을 해당 최대 대역폭보다 높게 설정하면 자동으로 최대값이 동일한 값으로 늘어납니다. 기본값은 0입니다. 유효 범위는 0~100이며 1씩 증가합니다. 값 0은 최소값이 보장되지 않음을 의미합니다. 선택한 인터페이스의 모든 대기열에 대한 개별 최소 대역폭 값의 합계는 정의된 최대값(100)을 초과할 수 없습니다.

4. Queue Management Type은 이 인터페이스의 대기열에 사용되는 대기열 깊이 관리 기술을 표시합니다.

   이는 장치가 대기열별로 독립적인 설정을 지원하는 경우에만 사용됩니다. 대기열 관리 유형

1.5 cm

메뉴에서 TailDrop 또는 WRED를 선택합니다. 기본값은 TailDrop입니다.

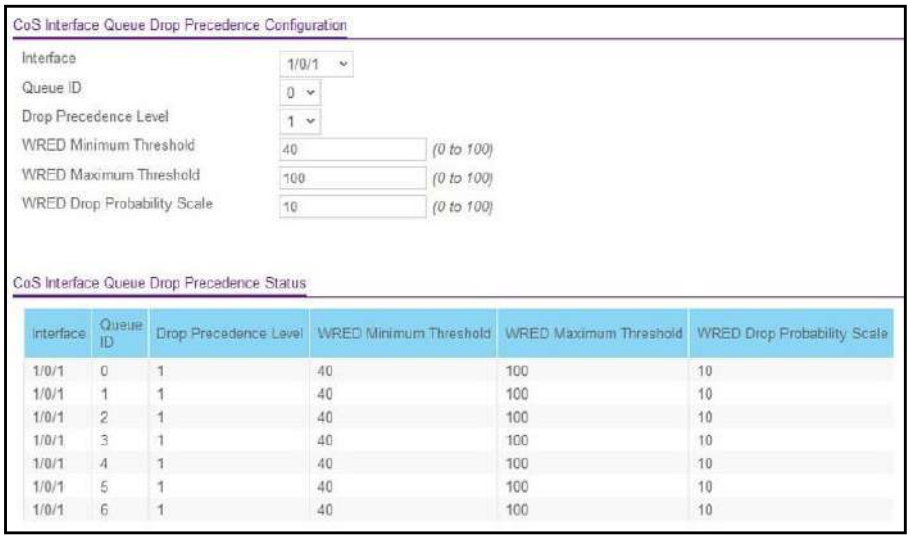
5. Apply 버튼을 클릭합니다

   변경 사항이 시스템에 적용됩니다.

CoS 삭제 우선순위 설정 구성

➢ **CoS 삭제 우선 순위 설정을 구성하려면:**

QoS > CoS> Advanced > CoS Queue Drop Precedence Configuration.



1. Interface를 사용하여 CoS 구성 가능 인터페이스를 모두 지정합니다.
2. Queue ID를 사용하여 사용 가능한 모든 대기열을 지정합니다.

   유효한 값은 0~6입니다. 기본값은 0입니다.
3. Drop Precedence Level을 사용하여 사용 가능한 모든 삭제 우선 순위 수준을 지정합니다.

   유효한 값은 1~4입니다. 기본값은 1입니다.
4. WRED Minimum Threshold을 사용하여 현재 삭제 우선 순위 수준에 대해 패킷이 삭제되지 않는 가중치 RED 최소 대기열 임계값을 지정합니다.

   범위는 0~100입니다. 기본값은 40입니다.
5. WRED Maximum Threshold을 사용하여 현재 삭제 우선 순위 수준에 대해 모든 패킷이 삭제되는 가중치 RED 최대 대기열 임계값을 지정합니다.

   범위는 0~100입니다. 기본값은 100입니다.

1.5 cm

6. WRED Drop Probability Scale를 사용하여 현재 삭제 우선 순위 수준에 대한 패킷 삭제 확률을 결정합니다.

   범위는 0~100입니다. 기본값은 10입니다.

7. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표에서는 표시되는 구성할 수 없는 데이터에 대해 설명합니다.

Table 198. CoS 인터페이스 대기열 삭제 우선 순위 상태

필드	설명
Interface	CoS 구성 가능 인터페이스.
Queue ID	대기열 ID입니다.
Drop Precedence Level	삭제 우선순위 수준입니다.
WRED Minimum Threshold	가중치가 부여된 RED 최소 대기열 임계값입니다.
WRED Maximum Threshold	가중치가 부여된 RED 최대 대기열 임계값입니다.
WRED Drop Probability Scale	패킷 삭제 확률 값입니다.

차별화된 서비스 개요

QoS 기능에는 트래픽을 스트림으로 분류하고 정의된 홉별 동작에 따라 특정 QoS 처리를 제공할 수 있는 DiffServ(차별화된 서비스) 지원이 포함되어 있습니다.

표준 IP 기반 네트워크는 최선의 데이터 전달 서비스를 제공하도록 설계되었습니다. 최선의 노력 서비스는 보장은 없지만 네트워크가 적시에 데이터를 전달한다는 것을 의미합니다. 혼잡 중에는 패킷이 지연되거나 산발적으로 전송되거나 삭제될 수 있습니다. 이메일 및 파일 전송과 같은 일반적인 인터넷 응용 프로그램의 경우 서비스의 약간의 저하가 허용되며 대부분의 경우 눈에 띄지 않습니다. 반대로, 서비스 저하로 인해 음성이나 멀티미디어와 같이 타이밍 요구 사항이 엄격한 애플리케이션에는 바람직하지 않은 영향을 미칩니다.

QoS용 DiffServ를 사용하려면 먼저 다음 범주와 해당 기준을 정의해야 합니다.

1. Class - 클래스를 만들고 클래스 기준을 정의합니다.
2. Policy - 정책을 생성하고, 클래스를 정책과 연결하고, 정책 설명을 정의합니다.
3. Service - 인바운드 인터페이스에 정책을 추가합니다.

1.5 cm

패킷은 정의된 기준에 따라 분류되고 처리됩니다. 분류 기준은 클래스별로 정의됩니다. 처리는 정책 속성에 의해 정의됩니다. 정책 속성은 클래스 인스턴스별로 정의할 수 있으며 일치가 발생할 때 적용되는 속성입니다. 정책에는 여러 클래스가 포함될 수 있습니다. 정책이 활성화되면 수행되는 작업은 패킷과 일치하는 클래스에 따라 달라집니다.

패킷 처리는 패킷의 클래스 일치 기준을 테스트하는 것으로 시작됩니다. 해당 정책 내에서 클래스 일치가 발견되면 해당 패킷에 정책이 적용됩니다.

DiffServ 마법사 개요

DiffServ 마법사는 트래픽 클래스를 생성하고 트래픽 클래스를 정책에 추가한 다음 선택한 포트에 정책을 추가하여 스위치에서 DiffServ를 활성화합니다. DiffServ 마법사는 다음을 수행합니다.

- DiffServ Class를 생성하고 들어오는 트래픽이 클래스의 구성원이 되기 위한 요구 사항을 충족하는지 확인하기 위해 필터로 사용되는 일치 기준을 정의합니다.
- Traffic Type 선택에 따라 DiffServ Class 일치 기준을 다음과 같이 설정합니다.
  - **VOIP**. 일치 기준을 UDP 프로토콜로 설정합니다.
  - **HTTP**. 일치 기준을 HTTP 대상 포트로 설정합니다.
  - **FTP**. 일치 기준을 FTP 대상 포트로 설정합니다.
  - **Telnet**. 일치 기준을 Telnet 대상 포트로 설정합니다.
  - **Every**. 모든 트래픽에 대한 일치 기준을 설정합니다.
- Diffserv Policy을 생성하고 생성된 DiffServ Class에 추가합니다.
- Policing이 YES로 설정된 경우 DiffServ Policy 스타일은 Simple으로 설정됩니다. 클래스 Match 기준을 준수하는 트래픽은 Outbound Priority 선택에 따라 처리됩니다. Outbound Priority는 다음과 같이 적합한 트래픽 처리를 구성합니다.
  - **High**. 정책 조치를 markdscp ef로 설정합니다.
  - **Med**. 정책 조치를 markdscp af31로 설정합니다.
  - **Low**. 보낼 정책 조치를 설정합니다.
- Policing이 NO로 설정된 경우 모든 트래픽은 다음과 같이 표시됩니다.
  - **High**. 정책 표시를 ipdscp ef로 설정합니다.
  - **Med**. 정책 표시를 ipdscp af31로 설정합니다.
  - **Low**. 정책 표시를 pdscp be로 설정합니다.

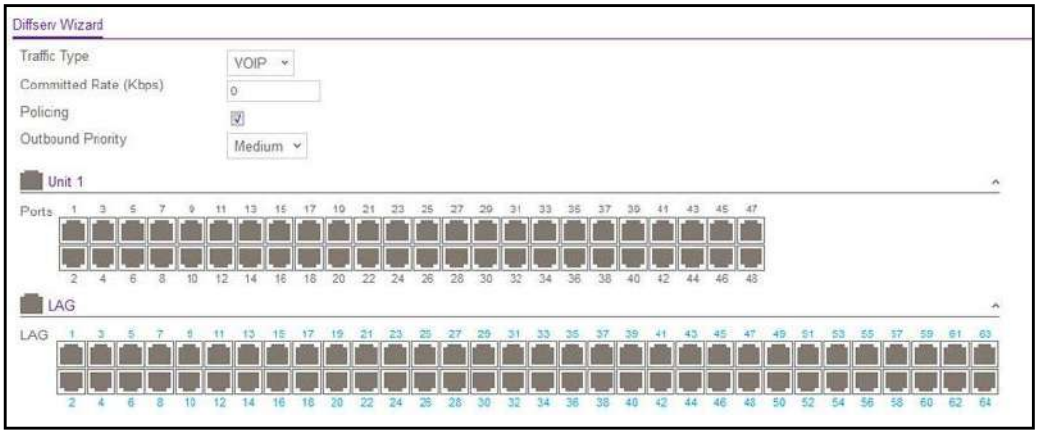
1.5 cm

- 선택한 각 포트가 생성된 정책에 추가됩니다.

DiffServ 마법사 사용

➢ **DiffServ 마법사를 사용하려면:**

QoS > DiffServ > DiffServ Wizard.



1. Traffic Type을 사용하여 DiffServ 클래스를 정의합니다.

   트래픽 유형 옵션은 VOIP, HTTP, FTP, Telnet 및 Every입니다.

2. 포트에는 DiffServ 정책을 지원하도록 구성할 수 있는 포트가 표시됩니다.

   DiffServ 정책이 선택한 포트에 추가됩니다.

3. Enable Policing를 사용하여 DiffServ 정책에 정책을 추가합니다.
   적용할 치안율입니다.

4. 약정 비율을 지정합니다.
   - Policing이 활성화되면 커밋된 비율이 정책에 적용되고 폴리싱 작업이 이를 따르도록 설정됩니다.
   - Policing이 비활성화되면 커밋 속도가 적용되지 않고 정책이 markdscp로 설정됩니다.

5. 아웃바운드 우선순위를 지정합니다.
   - Policing이 활성화되면 Outbound Priority는 폴리싱 준수 작업 유형을 정의합니다. 여기서 High는 작업을 markdscp ef로 설정하고, Med는 작업을 markdscp af31로 설정하고, Low는 작업을 전송으로 설정합니다

1.5 cm

- Policing이 비활성화되면 아웃바운드 우선 순위는 다음과 같은 정책을 정의합니다. 높음은 ipdscp ef를 표시하도록 정책을 설정하고, Med는 ipdscp af31을 표시하도록 정책을 설정하고, 낮음은 ipdscp be를 표시하도록 정책을 설정합니다.

기본 DiffServ 설정 구성

패킷은 정의된 기준에 따라 필터링되고 처리됩니다. 필터링 기준은 클래스별로 정의됩니다. 처리는 정책 속성에 의해 정의됩니다. 정책 속성은 클래스 인스턴스별로 정의할 수 있으며 일치가 발생할 때 적용되는 속성입니다.

구성 프로세스는 클래스에 대해 하나 이상의 일치 기준을 정의하는 것으로 시작됩니다. 그런 다음 하나 이상의 클래스가 정책에 추가됩니다. 그런 다음 인터페이스에 정책이 추가됩니다.

패킷 처리는 패킷의 일치 기준을 테스트하는 것으로 시작됩니다. 모든 클래스 유형 옵션은 패킷이 해당 클래스와 일치하려면 클래스 내의 각 일치 기준이 true로 평가되어야 함을 지정합니다. 모든 클래스 유형 옵션은 패킷이 해당 클래스와 일치하려면 하나 이상의 일치 기준이 true로 평가되어야 함을 지정합니다. 클래스는 정책에 추가된 순서대로 테스트됩니다. 해당 정책 내에서 클래스 일치가 발견되면 해당 패킷에 정책이 적용됩니다.

➢ **기본 DiffServ 설정을 구성하려면:**

QoS > DiffServ > Basic > DiffServ Configuration.

다음 표에서는 표시되는 구성할 수 없는 데이터에 대해 설명합니다.

1.5 cm

Table 199. DiffServ 구성

필드	설명
DiffServ Admin Mode	DiffServ의 옵션 모드입니다. 기본값은 활성화입니다. 비활성화된 동안 DiffServ 구성은 저장 시 유지되며 변경할 수 있지만 활성화되지는 않습니다. 활성화되면 Diffserv 서비스가 활성화됩니다.
Class table	스위치에 허용되는 총계 중에서 구성된 DiffServ 클래스 수입니다.
Class Rule table	스위치에 허용되는 총 클래스 규칙 중 구성된 클래스 규칙의 수입니다.
Policy table	스위치에 허용되는 총 정책 중 구성된 정책 수입니다.
Policy Instance table	스위치에 허용되는 총계 중 구성된 정책 클래스 인스턴스의 수입니다.
Policy Attributes table	스위치에 허용되는 총계 중에서 구성된 정책 속성(정책 클래스 인스턴스에 연결됨)의 수입니다.
Service table	스위치에 허용되는 전체 서비스 중 구성된 서비스(지정된 인터페이스의 정책에 연결됨) 수입니다.

전역 DiffServ 설정 구성

패킷은 정의된 기준에 따라 필터링되고 처리됩니다. 필터링 기준은 클래스별로 정의됩니다. 처리는 정책 속성에 의해 정의됩니다. 정책 속성은 클래스 인스턴스별로 정의할 수 있으며 일치가 발생할 때 적용되는 속성입니다.

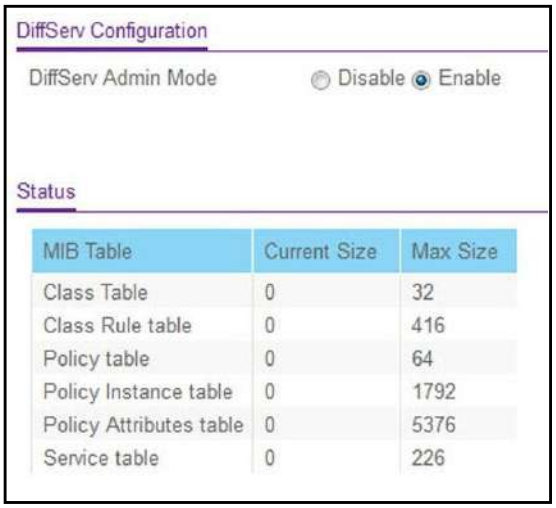
구성 프로세스는 클래스에 대해 하나 이상의 일치 기준을 정의하는 것으로 시작됩니다. 그런 다음 하나 이상의 클래스가 정책에 추가됩니다. 그런 다음 인터페이스에 정책이 추가됩니다.

패킷 처리는 패킷의 일치 기준을 테스트하는 것으로 시작됩니다. 모든 클래스 유형 옵션은 패킷이 해당 클래스와 일치하려면 클래스 내의 각 일치 기준이 true로 평가되어야 함을 지정합니다. 모든 클래스 유형 옵션은 패킷이 해당 클래스와 일치하려면 하나 이상의 일치 기준이 true로 평가되어야 함을 지정합니다. 클래스는 정책에 추가된 순서대로 테스트됩니다. 해당 정책 내에서 클래스 일치가 발견되면 해당 패킷에 정책이 적용됩니다.

- **글로벌 DiffServ 모드를 구성하려면:**

  QoS > DiffServ > Advanced > Diffserv Configuration.

1.5 cm



1. DiffServ에 대한 Admin Mode를 선택합니다.
   - **Enable**. 차별화된 서비스가 활성화되어 있습니다.
   - **Disable**. DiffServ 구성은 유지되고 변경될 수 있지만 활성화되지 않습니다.
2. Apply 버튼을 클릭합니다

   설정이 시스템에 적용됩니다.

다음 표에서는 DiffServ 구성 화면의 상태 테이블에 표시되는 정보에 대해 설명합니다.

Table 200. DiffServ 상태

필드	설명
Class Table	스위치에 허용되는 총계 중에서 구성된 DiffServ 클래스 수입니다.
Class Rule table	스위치에 허용되는 총 클래스 규칙 중 구성된 클래스 규칙의 수입니다.
Policy table	스위치에 허용되는 총 정책 중 구성된 정책 수입니다.
Policy Instance table	스위치에 허용되는 총계 중 구성된 정책 클래스 인스턴스의 수입니다.
Policy Attributes table	스위치에 허용되는 총계 중에서 구성된 정책 속성(정책 클래스 인스턴스에 연결됨)의 수입니다.
Service table	스위치에 허용되는 전체 서비스 중 구성된 서비스(지정된 인터페이스의 정책에 연결됨) 수입니다.

DiffServ 클래스 구성

새 DiffServ 클래스 이름을 추가하거나 기존 클래스의 이름을 바꾸거나 삭제할 수 있습니다. DiffServ 클래스와 연결할 기준을 정의할 수도 있습니다. 패킷이 수신되면 이러한 DiffServ 클래스를 사용하여 패킷의 우선 순위를 지정합니다. 클래스에서 여러 일치 기준을 사용할 수 있습니다. 논리는 이 기준에 대한 부울 논리 AND입니다. 수업을 생성한 후 수업 링크를 클릭하면 수업 화면으로 이동합니다.

➢ **DiffServ 클래스를 구성하려면:**

QoS > DiffServ > Advanced > Class Configuration.

1. 새로운 클래스를 생성하려면 Class Name을 입력하고 Class Type을 선택한 후 Add 버튼을 클릭하세요.

   이 필드에는 선택할 수 있는 모든 기존 DiffServ 클래스 이름도 나열됩니다. 스위치는 Class Type 값 All만 지원합니다. 이는 클래스에 대해 정의된 모든 다양한 일치 기준이 패킷 일치에 대해 충족됨을 의미합니다. 모두는 모든 일치 기준의 논리적 AND를 나타냅니다. 새 클래스를 생성할 때만 클래스 유형을 선택할 수 있습니다. 클래스가 생성되면 클래스 유형 필드를 구성할 수 없게 됩니다.

2. 기존 클래스의 이름을 바꾸려면 구성된 클래스 옆에 있는 check box을 선택하고 이름을 업데이트합니다. Apply 버튼을 클릭합니다

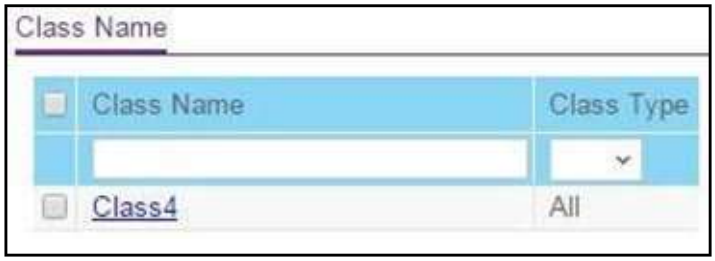
   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

3. 클래스를 제거하려면 클래스 이름 check box을 선택하고 Delete 버튼을 클릭합니다.

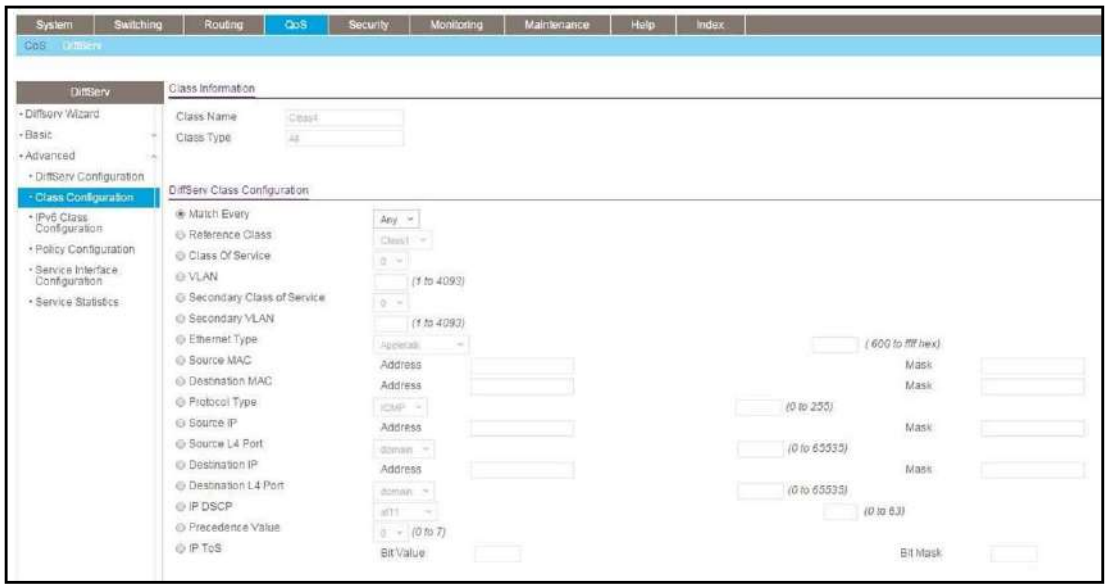
   스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

4. 클래스 생성 후 클래스 링크를 클릭하면 클래스 화면으로 이동합니다.

5. 기존 Class의 클래스 이름을 클릭합니다.



클래스 이름은 하이퍼링크입니다. 다음 그림은 클래스의 구성 필드를 보여줍니다.



6. 수업 세부정보를 구성하려면 다음 필드를 완성하세요.
   - **Class Name** - 구성된 DiffServ 클래스의 이름입니다.
   - **Class Type** - DiffServ 클래스 유형입니다.

     새 클래스를 생성할 때만 클래스 유형을 선택할 수 있습니다. 클래스를 생성한 후 이 필드에 클래스 유형이 표시되지만 이를 변경할 수는 없습니다.

7. DiffServ 클래스와 연결할 기준을 정의합니다.
   - **Match Every**. 이는 지정된 클래스 정의에 모든 패킷이 클래스에 속하는 것으로 간주되는 일치 조건을 추가합니다.
   - **Reference Class**. 현재 클래스에 참조 클래스로 할당할 수 있는 클래스를 나열합니다.
   - **Class of Service**. 여기에는 선택할 수 있는 0~7 범위의 서비스 클래스 일치 기준에

대한 모든 값이 나열됩니다.

- **VLAN**. 0~4093 범위의 값입니다.
- **Secondary Class of Service**. 이더넷 프레임 헤더의 CoS(서비스 클래스) 값이 지정된 CoS 값과 일치하도록 하려면 이 옵션을 선택하십시오.
- **Secondary VLAN**. 패킷의 VLAN ID가 연속 범위 내의 보조 VLAN ID 또는 보조 VLAN ID와 일치하도록 요구하려면 이 옵션을 선택합니다. 범위를 구성하는 경우 패킷의 보조 VLAN ID가 범위 내의 보조 VLAN ID와 동일하면 일치가 발생합니다. 이 옵션을 선택한 후 다음 필드를 사용하여 보조 VLAN 일치 기준을 구성하십시오.
  - **Secondary VLAN ID Start**. 일치시킬 보조 VLAN ID 또는 VLAN 범위 내에서 가장 낮은 값을 가진 보조 VLAN ID입니다.
  - **Secondary VLAN ID End**. VLAN 범위 내에서 가장 높은 값을 갖는 보조 VLAN ID입니다. 일치 기준이 단일 VLAN ID인 경우 이 필드는 필요하지 않습니다.
- **Ethernet Type**. 선택할 수 있는 Ethertype에 대한 키워드가 나열됩니다.
- **Source MAC Address**. 이는 콜론으로 구분된 6개의 2자리 16진수 숫자로 지정된 소스 MAC 주소입니다.
- **Source MAC Mask**. 이는 패킷 콘텐츠와 일치하는 데 사용할 소스 MAC 주소 부분을 나타내는 MAC 주소와 동일한 형식의 비트 마스크입니다.
- **Destination MAC Address**. 이는 콜론으로 구분된 6개의 2자리 16진수 숫자로 지정된 대상 MAC 주소입니다.
- **Destination MAC Mask**. 이는 패킷 내용과 일치하는 데 사용할 대상 MAC 주소의 부분을 나타내는 MAC 주소와 동일한 형식의 비트 마스크입니다.
- **Protocol Type**. 여기에는 선택할 수 있는 레이어 4 프로토콜에 대한 키워드가 나열되어 있습니다. 목록에는 나머지 값에 대한 옵션으로 'other'가 포함됩니다.
- **Source IP Address**. 이는 점으로 구분된 십진수 형식의 유효한 소스 IP 주소입니다.
- **Source Mask**. 이는 패킷 콘텐츠와 일치하는 데 사용할 소스 IP 주소의 부분을 나타내는 IP 점으로 구분된 십진수 형식의 비트 마스크입니다.
- **Source L4 Port**. 여기에는 선택할 수 있는 알려진 소스 레이어 4 포트에 대한 키워드가 나열됩니다. 목록에는 이름이 지정되지 않은 포트에 대한 옵션으로 '기타'가 포함되어 있습니다.
- **Destination IP Address**. 이는 점으로 구분된 십진수 형식의 유효한 대상 IP

주소입니다.

- **Destination Mask**. 이는 패킷 콘텐츠와 일치하는 데 사용할 대상 IP 주소의 부분을 나타내는 IP 점으로 구분된 10진수 형식의 비트 마스크입니다.
- **Destination L4 Port**. 여기에는 선택할 수 있는 알려진 대상 레이어 4 포트에 대한 키워드가 나열됩니다. 목록에는 이름이 지정되지 않은 포트에 대한 옵션으로 'other'가 포함되어 있습니다.
- **IP DSCP**. 여기에는 선택할 수 있는 알려진 DSCP 값에 대한 키워드가 나열됩니다. 목록에는 나머지 값에 대한 옵션으로 'other'가 포함됩니다.
- **Precedence Value**. 여기에는 0~7 범위의 IP 우선순위 값에 대한 키워드가 나열됩니다.
- **IP ToS**. IP ToS 필드를 구성합니다.
  - **ToS Bits**. 비교할 00~ff 범위의 서비스 유형 옥텟 값입니다.
  - **ToS Mask**. 이는 서비스 유형 값과 비교 대상인 ToS 비트를 나타냅니다.

8. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표에서는 DiffServ 고급 클래스 구성 화면 하단의 클래스 요약에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 201. DiffServ 클래스 구성 - 클래스 요약

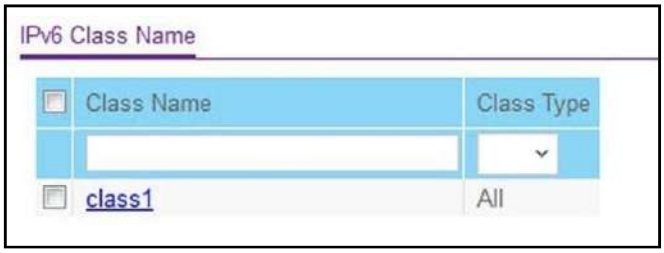
필드	설명
Match Criteria	지정된 클래스에 대해 구성된 일치 기준입니다.
Values	구성된 일치 기준의 값입니다.

DiffServ IPv6 클래스 설정 구성

새 IPv6 DiffServ 클래스 이름을 추가하거나 기존 클래스의 이름을 바꾸거나 삭제할 수 있습니다. DiffServ 클래스와 연결할 기준을 정의할 수도 있습니다. 패킷이 수신되면 이러한 DiffServ 클래스를 사용하여 패킷의 우선 순위를 지정합니다. 클래스에서 여러 일치 기준을 사용할 수 있습니다. 논리는 이 기준에 대한 부울 논리 AND입니다. 수업을 생성한 후 수업 링크를 클릭하면 수업 화면으로 이동합니다.

➢ **DiffServ IPv6 클래스 설정을 구성하려면:**

QoS > DiffServ > Advanced > IPv6 Class Configuration.



1. 새로운 클래스를 생성하려면 Class Name을 입력하고 Class Type을 선택한 후 Add 버튼을 클릭하세요.

   이 필드에는 선택할 수 있는 모든 기존 DiffServ 클래스 이름도 나열됩니다. 스위치는 클래스 Type 값 All만 지원합니다. 이는 클래스에 대해 정의된 모든 다양한 일치 기준이 패킷 일치에 대해 충족됨을 의미합니다. 모두는 모든 일치 기준의 논리적 AND를 나타냅니다. 새 클래스가 생성된 경우에만 이 필드는 선택기 필드입니다. 클래스 생성 후에는 구성된 클래스 유형을 표시하는 구성 불가능한 필드가 됩니다.

2. 기존 클래스의 이름을 바꾸려면 구성된 클래스 옆의 check box을 선택하고 이름을 업데이트합니다.

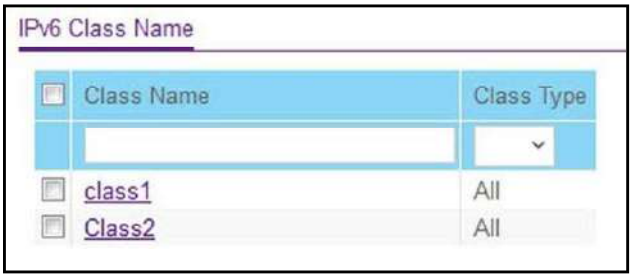
3. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

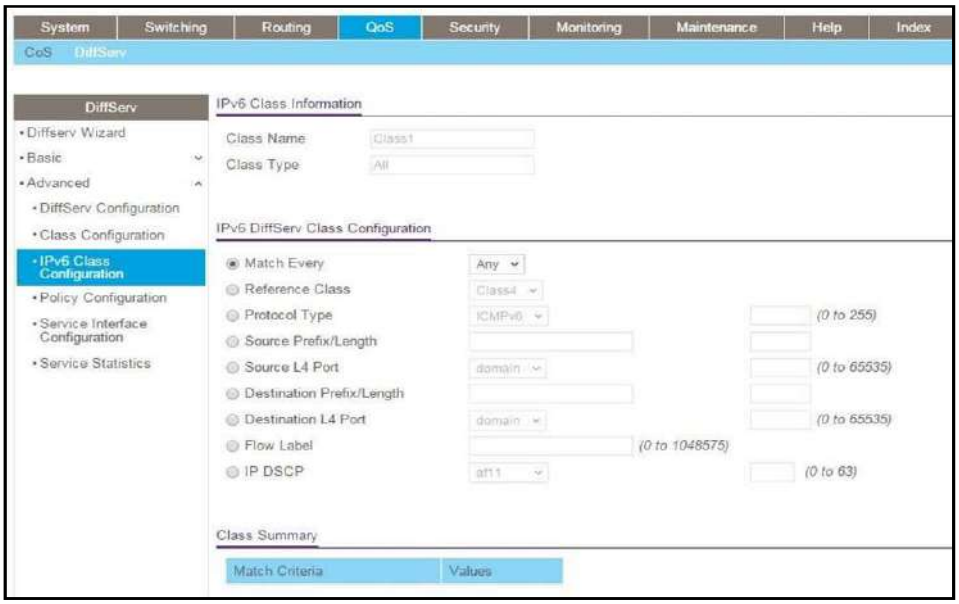
4. 클래스를 제거하려면 Class Name check box을 선택한 다음 Delete 버튼을 클릭합니다.

   스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

5. 클래스 생성 후 기존 클래스의 Class Name을 클릭합니다.



   클래스 이름은 하이퍼링크입니다. 다음 그림은 클래스의 구성 필드를 보여줍니다.



6. IPv6 클래스를 구성하려면 다음 필드를 완성합니다.
   - **Class Name** - 구성된 DiffServ 클래스의 이름입니다.
   - **Class Type** - DiffServ 클래스 유형입니다.
   - **Options**: All

   새 클래스를 생성할 때만 클래스 유형을 지정할 수 있습니다. 클래스가 생성된 후 이 필드에 클래스 유형이 표시되지만 이를 변경할 수는 없습니다.

7. DiffServ 클래스와 연결할 기준을 정의합니다.
   - **Match Every** - 이는 지정된 클래스 정의에 모든 패킷이 클래스에 속하는 것으로 간주되는 일치 조건을 추가합니다.
   - **Reference Class** - 현재 클래스에 참조 클래스로 할당할 수 있는 클래스를 나열합니다.
   - **Protocol Type** - 여기에는 선택할 수 있는 레이어 4 프로토콜에 대한 키워드가 나열되어 있습니다. 목록에는 나머지 값에 대한 옵션으로 'other'가 포함됩니다.
   - **Source Prefix Length** - 이는 IPv6 패킷과 비교할 유효한 소스 IPv6 접두사입니다. 접두사는 항상 접두사 길이로 지정됩니다. 접두어는 0~FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 범위로 입력할 수 있으며, 접두어 길이는 0~128 범위에서 입력할 수 있습니다.
   - **Source L4 Port** - 여기에는 선택할 수 있는 알려진 소스 레이어 4 포트에 대한 키워드가 나열됩니다. 목록에는 이름이 지정되지 않은 포트에 대한 옵션으로

'other'가 포함되어 있습니다.

- **Destination Prefix/Length** - 이는 IPv6 패킷과 비교할 수 있는 유효한 대상 IPv6 접두사입니다. 접두사는 항상 접두사 길이로 지정됩니다. 접두어는 0~FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 범위로 입력할 수 있으며, 접두어 길이는 0~128 범위에서 입력할 수 있습니다.
- **Destination L4 Port** - 여기에는 선택할 수 있는 알려진 대상 레이어 4 포트에 대한 키워드가 나열됩니다. 목록에는 이름이 지정되지 않은 포트에 대한 옵션으로 '기타'가 포함되어 있습니다.
- **Flow Label** - 이는 IPv6 패킷에 고유한 20비트 숫자로, 라우터에서 서비스 품질 처리를 나타내기 위해 최종 스테이션에서 사용됩니다. 흐름 레이블은 0~1048575 범위에서 지정할 수 있습니다.
- **IP DSCP** - 알려진 DSCP 값에 대한 키워드를 선택할 수 있습니다. 목록에는 나머지 값에 대한 옵션으로 기타가 포함되어 있습니다.

8. **Match Criteria** - 지정된 클래스에 대해 구성된 일치 기준을 표시합니다.
9. **Values** - 구성된 일치 기준의 값을 표시합니다.
10. Apply 버튼을 클릭합니다

    업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표에서는 DiffServ 고급 IPv6 클래스 구성 화면 하단의 클래스 요약에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 202. DiffServ IPv6 클래스 구성 - 클래스 요약

필드	설명
Match Criteria	지정된 클래스에 대해 구성된 일치 기준입니다.
Values	구성된 일치 기준의 값입니다.

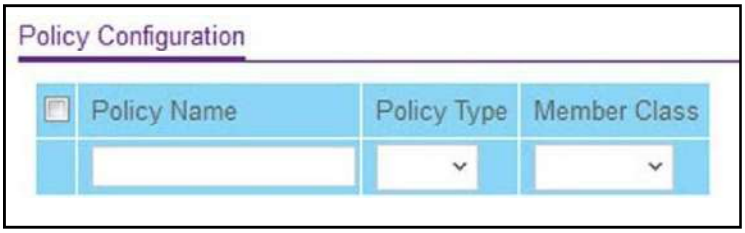
DiffServ 정책 구성

클래스 컬렉션을 하나 이상의 정책 설명과 연결할 수 있습니다. 정책을 생성한 후 정책 링크를 클릭하면 정책 화면으로 이동합니다.

➢ **DiffServ 정책을 구성하려면:**

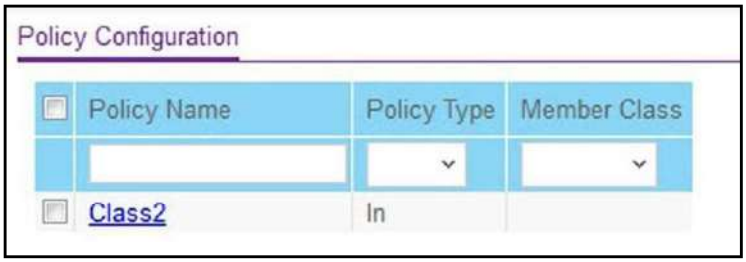
1.5 cm

QoS > DiffServ > Advanced > Policy Configuration.



1. Policy Name을 사용하면 1~31자의 대소문자 구분 영숫자 문자열을 사용하여 정책을 고유하게 식별할 수 있습니다.
2. Member Class 목록에서 DiffServ 클래스를 선택합니다.
   여기에는 현재 지정된 정책의 구성원으로 정의된 모든 기존 DiffServ 클래스가 나열됩니다. 이 목록은 새 클래스가 정책에 추가되거나 제거될 때 자동으로 업데이트됩니다.
   이 필드는 기존 정책 클래스 인스턴스를 제거할 경우에만 선택기 필드입니다. 정책 클래스 인스턴스를 제거한 후에는 구성할 수 없는 필드가 됩니다.
3. **Policy Type** - 유형이 인바운드 트래픽 방향과 관련되어 있음을 나타냅니다.
4. Add 버튼을 클릭합니다.

   새 정책이 스위치에 추가됩니다.
5. 스위치에서 현재 선택된 정책을 삭제하려면 Delete 버튼을 클릭합니다.
6. 정책 속성을 구성하려면 정책 이름을 클릭합니다.



정책 이름은 하이퍼링크입니다. 다음 그림은 정책의 구성 필드를 보여줍니다.

7. 이 정책 클래스의 패킷이 할당되는 Assign Queue을 선택합니다.
   이는 0~6 범위의 정수 값입니다.
8. 정책 속성을 구성합니다.
   - **Drop** - 드롭 라디오 버튼을 선택합니다. 이 플래그는 정책 속성이 모든 인바운드 패킷을 삭제하도록 정의되었음을 나타냅니다.
   - **Mark VLAN CoS** - VLAN 우선순위를 설정하기 위한 0~7 범위의 정수 값입니다.
   - **Mark CoS as Secondary Cos** - 이 옵션은 모든 패킷의 외부 VLAN 태그 우선순위 비트를 내부 VLAN 태그 우선순위로 표시합니다. 이는 본질적으로 내부 VLAN 태그 CoS가 외부 VLAN 태그 CoS로 복사됨을 의미합니다.
   - **Mark IP Precedence** - 이는 0~7 범위의 IP 우선순위 값입니다.
   - **Mirror**
   - **Redirect**
   - **Two Rate Policy** - 2단계 폴리서를 사용하면 커밋 속도와 최대 속도라는 두 가지 속도에 따라 트래픽 정책을 시행할 수 있습니다.
   - **Mark IP DSCP** - 여기에는 선택할 수 있는 알려진 DSCP 값에 대한 키워드가 나열됩니다. 목록에는 나머지 값에 대한 옵션으로 'other'가 포함됩니다.
   - **Simple Policy** - 이 속성을 사용하여 지정된 클래스에 대한 트래픽 정책 스타일을 설정합니다. 이 명령은 단일 데이터 속도와 버스트 크기를 사용하여 두 가지 결과(준수 및 위반)를 생성합니다.

9. Simple Policy 속성을 선택하면 다음 필드를 구성할 수 있습니다.
   - **Color Mode** - 색상 모드가 나열됩니다. 기본값은 'Color Blind'입니다.
     - **Color Blind**
     - **Color Aware**
       Color Aware 모드를 사용하려면 이 정책 인스턴스에 사용할 수 있는 색상 클래스가 하나 이상 있어야 합니다. 유효한 색상 클래스에는 단일, 다음 필드 중 하나에 대한 제외되지 않은 일치 기준(필드가 정책 인스턴스 자체의 분류자와 충돌하지 않는 경우):
     - **CoS**
     - **IP DSCP**
     - **IP Precedence**
   - **Committed Rate** - 이 값은 1~4294967295Kbps(초당 킬로비트) 범위로 지정됩니다.
   - **Committed Burst Size** - 이 값은 1~128KB 범위에서 지정됩니다. 커밋된 버스트 크기는 허용되는 트래픽 양을 결정하는 데 사용됩니다.
   - **Conform Action** - 여기에는 선택할 수 있는 정책 측정 기준에 따라 패킷 준수에 대해 취해야 할 조치가 나열되어 있습니다. 기본값은 send입니다.
   - **Violate Action** - 여기에는 선택할 수 있는 정책 측정 기준에 따라 위반 패킷에 대해 취해야 할 조치가 나열되어 있습니다. 기본값은 send입니다.
   - 각 작업 선택기에 대해 다음 작업 중 하나를 수행할 수 있습니다.
     - **Drop** - 이러한 패킷은 즉시 삭제됩니다.
     - **Mark IP DSCP** - 이러한 패킷은 시스템 전달 요소에 제공되기 전에 지정된 DSCP 값으로 DiffServ에 의해 표시됩니다. 이렇게 선택하려면 DSCP 필드를 설정해야 합니다.
     - **Mark CoS** - 이러한 패킷은 시스템 전달 요소에 제공되기 전에 지정된 CoS 값으로 DiffServ에 의해 표시됩니다. 이 선택을 위해서는 Mark CoS 필드를 설정해야 합니다.
     - **Send** - 이러한 패킷은 DiffServ에 의해 수정되지 않은 상태로 시스템 전달 요소에 제공됩니다.
     - **Mark IP Precedence** - 이러한 패킷은 시스템 전달 요소에 제공되기 전에 지정된 IP 우선 순위 값으로 DiffServ에 의해 표시됩니다. 이 선택을 위해서는 Mark IP Precedence 필드가 설정되어 있어야 합니다.

10. Two Rate를 선택하면 추가 필드(단순 정책과 동일한 필드)를 구성할 수 있습니다.
11. Apply 버튼을 클릭합니다

    업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 203. DiffServ 정책 구성 - 정책 속성

필드	설명
Policy Name	DiffServ 정책의 이름을 표시합니다.
Policy Type	정책 유형을 In으로 표시합니다.
Member Class Name	정책 내의 각 클래스 인스턴스 이름을 표시합니다.

DiffServ 서비스 인터페이스 구성

➢ **DiffServ 서비스 인터페이스를 구성하려면:**

QoS > DiffServ > Advanced > Service Interface Configuration.

1. Interface를 사용하여 DiffServ 서비스에 대한 인터페이스를 선택합니다.
2. **Policy Name** - 선택할 수 있는 모든 정책 이름을 나열합니다.

   인바운드 서비스 정책 첨부가 플랫폼에서 지원되지 않는 읽기/쓰기 사용자에게는 이 필드가 표시되지 않습니다.

Table 204. 서비스 인터페이스 구성

필드	설명

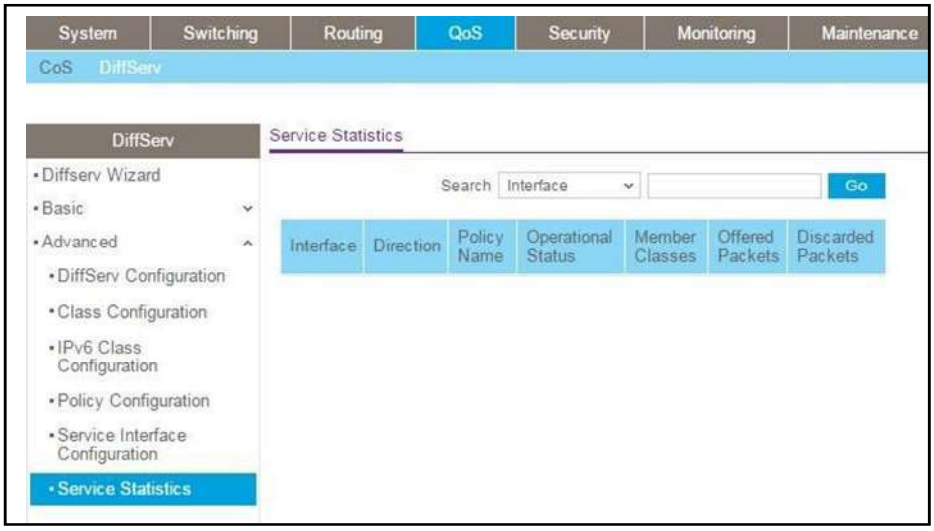
Direction	이 서비스 인터페이스의 트래픽 방향이 In임을 표시합니다.
Operational Status	이 서비스 인터페이스의 작동 상태(작동 또는 작동 중지)를 표시합니다.

DiffServ 서비스 통계 보기

해당 화면은 인터페이스와 방향에 따라 지정된 정책에 대한 클래스별 통계정보를 표시하는 화면입니다. 멤버 클래스 목록은 지정된 인터페이스와 방향 및 그에 따른 첨부된 정책(있는 경우)을 기반으로 채워집니다. 멤버 클래스 이름을 강조 표시하면 지정된 인터페이스 및 방향에 대한 정책 클래스 인스턴스의 통계 정보가 표시됩니다.

➢ **DiffServ 서비스 통계를 보려면:**

QoS > DiffServ > Advanced > Service Statistics.



1. Search 메뉴를 사용하여 MAC 인터페이스 또는 이웃 IP별로 이웃 항목을 검색합니다.
2. 인터페이스별로 검색하려면 Interface를 선택하고 장치/슬롯/포트 형식으로 인터페이스를 입력합니다(예: 1/0/13). 그런 다음 Go 버튼을 클릭하세요.

   인접 항목이 있는 경우 해당 항목이 첫 번째 항목으로 표시되고 그 뒤에 나머지 항목이 표시됩니다.
3. 회원 등급별로 검색하려면 Member Class을 선택하고 회원 등급을 입력한 후 Go 버튼을 클릭하세요.

   일치하는 구성원 클래스가 있는 항목이 있는 경우 해당 항목이 첫 번째 항목으로 표시되고 나머지 항목이 표시됩니다. 정확하게 일치해야 합니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

다음 표에서는 서비스 통계 화면에서 사용할 수 있는 정보에 대해 설명합니다.

Table 205. DiffServ 서비스 통계

필드	설명
Interface	현재 In 방향으로 연결된 DiffServ 정책이 있는 시스템의 모든 유효한 슬롯 번호 및 포트 번호 조합 목록입니다.
Direction	인터페이스의 트래픽 방향 목록을 In으로 표시합니다. DiffServ 정책이 현재 연결된 방향만 표시합니다.
Policy Name	현재 지정된 인터페이스 및 방향에 연결된 정책의 이름입니다.
Operational Status	지정된 인터페이스 및 방향에 현재 연결된 정책의 작동 상태입니다. 값은 위 또는 아래입니다.
Member Classes	현재 선택한 정책 이름의 구성원으로 정의된 모든 DiffServ 클래스 목록입니다. 통계를 표시하려면 멤버 클래스 이름을 선택하세요. 선택한 정책과 연결된 클래스가 없으면 목록에 아무것도 채워지지 않습니다.
Offered Packets	정의된 DiffServ 처리가 적용되기 전에 이 서비스 정책의 모든 클래스 인스턴스에 제공되는 총 패킷 수입니다. 인터페이스별, 방향별 전체 개수입니다.
Discarded Packets	DiffServ 처리로 인해 어떤 이유로든 이 서비스 정책의 모든 클래스 인스턴스에 대해 삭제된 총 패킷 수입니다. 인터페이스별, 방향별 전체 개수입니다. 삭제된 패킷은 인바운드 방향에서는 지원되지만 아웃바운드 방향에서는 지원되지 않습니다.

장치 보안 관리 6

이 장에서는 다음 주제를 다룹니다.

- *관리 보안 설정*
- *TACACS 개요*
- *관리 액세스 구성*
- *포트 인증*
- *교통 통제*
- *포트 보안*
- *DHCP 스누핑*
- *액세스 제어 목록 구성*

관리 보안 설정

로그인 비밀번호, RADIUS(Remote Authorization Dial-In User Service) 설정, TACACS(Terminal Access Controller Access Control System) 설정 및 인증 목록을 구성할 수 있습니다.

사용자 구성

기본적으로 두 개의 사용자 계정이 존재합니다.

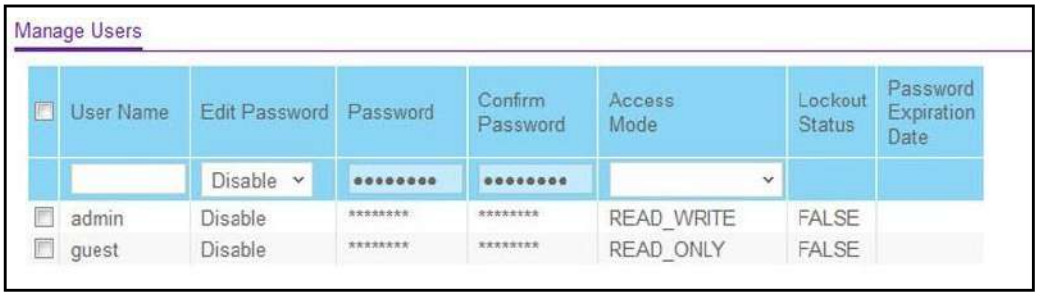
- admin, 읽기/쓰기 권한이 있습니다.
- guest, 읽기 전용 권한이 있습니다.

기본적으로 두 계정 모두 암호는 비어 있습니다. 이름은 대소문자를 구분하지 않습니다.

읽기/쓰기 권한이 있는 사용자 계정(admin)으로 로그인하면 기본 계정에 대해 비밀번호를 할당하고 보안 매개변수를 설정할 수 있으며, 계정(admin 이외)을 최대 6개까지 추가 및 삭제할 수 있습니다. 읽기/쓰기 권한이 있는 사용자만 웹 인터페이스 화면의 데이터를 수정할 수 있으며, 읽기/쓰기 권한이 있는 계정은 하나만 생성할 수 있습니다.

➢ **사용자를 구성하려면:**

Security > Management Security > Local User > User Management.



1. User Name 필드에 새 계정의 이름을 입력합니다.

   계정을 생성할 때만 새 사용자 이름을 입력할 수 있습니다. 사용자 이름은 최대 64자이며 대소문자를 구분하지 않습니다. 유효한 문자에는 모든 영숫자 문자와 하이픈(-) 및 밑줄(_) 문자가 포함됩니다. 사용자 이름 기본값이 유효하지 않습니다. 한번 생성된 사용자 이름은 변경하거나 수정할 수 없습니다.

2. 비밀번호를 변경할 때만 Edit Password 필드를 Enable로 설정합니다.

   기본값은 Disable입니다.

3. Password 필드에 계정의 비밀번호를 입력하세요.

   문자는 입력한 대로 표시되지 않습니다. 별표(*)만 표시됩니다. 비밀번호는 최대 8자리 영숫자이며 대소문자를 구분합니다.

4. Confirm Password 필드에 비밀번호를 다시 입력하여 비밀번호를 올바르게 입력했는지 확인하세요.

   이 필드에는 입력된 비밀번호가 표시되지 않지만 별표(*)가 표시됩니다.

   Access Mode 필드에는 사용자의 액세스 모드가 표시됩니다. 관리자 계정에는 항상 읽기/쓰기 액세스 권한이 있으며 다른 모든 계정에는 읽기 전용 액세스 권한이 할당됩니다. 기본값은 읽기 전용입니다.

   Lockout Status 필드는 사용자 계정이 잠겨 있는지 여부(TRUE 또는 FALSE)를 나타냅니다.

   Password Expiration Date 필드는 현재 비밀번호 만료 날짜를 나타냅니다.

5. Add 버튼을 클릭합니다.

   사용자 계정이 추가됩니다.

6. 선택한 사용자 계정을 삭제하려면 Delete 버튼을 클릭하세요.

   관리자 읽기/쓰기 사용자는 삭제할 수 없습니다.

사용자 비밀번호 구성

➢ **사용자 비밀번호를 구성하려면:**

Security > Management Security > Local User > User Password Configuration.

1. Password Minimum Length 필드에 모든 새 로컬 사용자 비밀번호의 최소 문자 길이를 입력하십시오.
2. Password Aging(day) 필드에 비밀번호가 설정된 시간부터 사용자 비밀번호가 유효한 최대 시간(일)을 입력합니다.

   비밀번호가 만료되면 사용자는 비밀번호 만료 후 처음 로그인할 때 새 비밀번호를 입력해야 합니다. 값 0은 비밀번호가 만료되지 않음을 나타냅니다.

3. Password History 필드에 비밀번호 재사용 방지를 위해 저장할 이전 비밀번호

수를 입력합니다.

이렇게 하면 각 사용자가 비밀번호를 자주 재사용하지 않게 됩니다. 0 값은 이전 비밀번호가 저장되지 않았음을 나타냅니다.

4. Lockout Attempts 필드에서 사용자 계정이 잠기기 전에 허용되는 로컬 인증 시도 실패 횟수를 지정합니다.

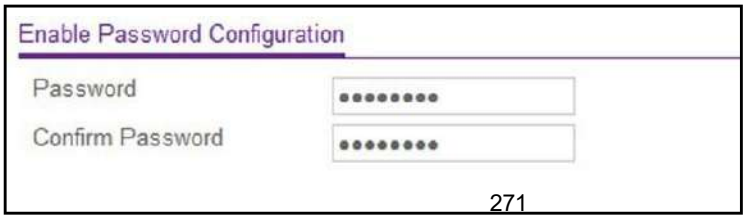
   값 0은 사용자 계정이 잠기지 않음을 나타냅니다.

비밀번호 구성 활성화

권한 있는 EXEC 비밀번호를 변경할 수 있습니다. 비밀번호는 최대 64자의 영숫자입니다. 비밀번호는 대소문자를 구분합니다.

➢ **비밀번호 구성을 활성화하려면:**

Security > Management Security > Enable Password.



1. Password 필드에 비밀번호를 입력하세요.

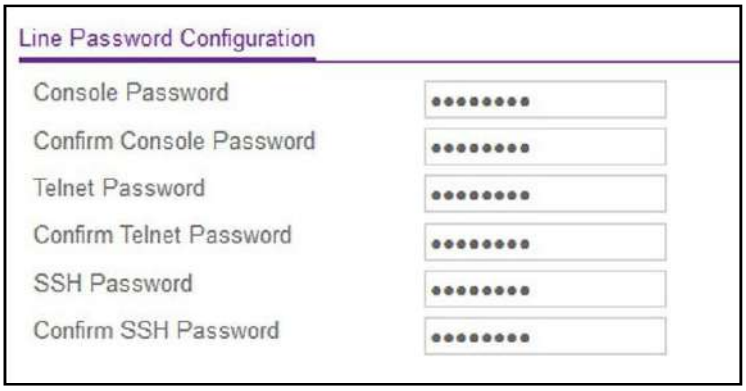
   비밀번호는 최대 64자의 영숫자입니다.

2. Confirm Password 필드에 비밀번호를 다시 입력하여 비밀번호를 올바르게 입력했는지 확인하세요.

회선 비밀번호 구성

➢ **회선 비밀번호를 구성하려면:**

Security > Management Security > Line Password.



1. Console Password 필드에 콘솔 비밀번호를 입력합니다.

   비밀번호는 최대 64자의 영숫자입니다.

2. Confirm Console Password 필드에 비밀번호를 다시 입력하여 올바르게 입력했는지 확인합니다.
3. Telnet Password(텔넷 비밀번호) 필드에 Telnet 비밀번호를 입력합니다.

   비밀번호는 최대 64자의 영숫자입니다.

4. Confirm Telnet Password 필드에 비밀번호를 다시 입력하여 비밀번호를 올바르게 입력했는지 확인합니다.
5. SSH Password 필드에 SSH 비밀번호를 입력합니다.

   비밀번호는 최대 64자의 영숫자입니다.

6. Confirm SSH Password 필드에 비밀번호를 다시 입력하여 비밀번호를 올바르게 입력했는지 확인합니다.

RADIUS 개요

RADIUS 서버는 네트워크에 추가 보안을 제공합니다. RADIUS 서버는 사용자별 인증 정보가 포함된 사용자 데이터베이스를 유지 관리합니다. 스위치는 네트워크 사용을 승인하기 전에 사용자 이름과 암호를 인증할 수 있는 구성된 RADIUS 서버에 정보를 전달합니다. RADIUS 서버는 다음에 대한 중앙 집중식 인증 방법을 제공합니다.

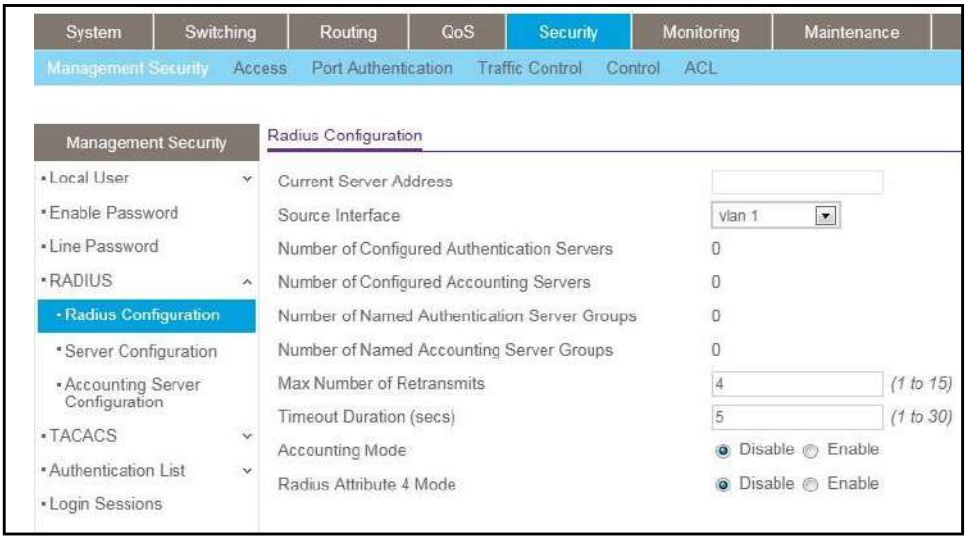
- Web access
- Access control port (802.1X)

글로벌 RADIUS 서버 설정 구성

네트워크에 있는 하나 이상의 RADIUS 서버에 대한 정보를 추가할 수 있습니다.

➢ **글로벌 RADIUS 서버 설정을 구성하려면:**

Security > Management Security > RADIUS > Radius Configuration.



구성된 서버가 없으면 Current Server Address 필드는 비어 있습니다(RADIUS 서버 구성 참조). 스위치는 구성된 RADIUS 서버를 최대 3개까지 지원합니다. 둘 이상의 RADIUS 서버가 구성된 경우 현재 서버가 기본 서버입니다. 기본 서버로 구성된 서버가 없는 경우 현재 서버는 가장 최근에 추가된 RADIUS 서버입니다.

1. Source Interface 목록에서 RADIUS에 사용할 인터페이스를 선택합니다.

   가능한 값은 다음과 같습니다.
   - **None**
   - **Routing interface**
   - **Routing VLAN**
   - **Routing loopback interface**
   - **Service Port**

   기본적으로 VLAN 1은 소스 인터페이스로 사용됩니다.

2. Max Number of Retransmit 필드에서 요청 패킷이 RADIUS 서버로 재전송되는 최대 횟수를 지정합니다.

   유효한 범위는 1~15입니다. 기본값은 4입니다.

   RADIUS 최대 재전송 및 RADIUS 시간 제한을 구성할 때 최대 지연 시간을 고려하십시오. 여러 RADIUS 서버가 구성된 경우 다음 서버를 시도하기 전에 각 서버의 최대 재전송

값이 소진됩니다. 해당 서버에 구성된 시간 초과 값이 RADIUS 서버의 응답 없이 전달될 때까지 재전송이 발생하지 않습니다. 따라서 RADIUS 애플리케이션으로부터 응답을 수신할 때의 최대 지연 시간은 구성된 모든 서버의 재전송 시간 초과 시간과 같습니다. RADIUS 요청이 사용자 로그인 시도에 의해 생성된 경우 RADIUS 애플리케이션이 응답을 반환할 때까지 모든 사용자 인터페이스가 차단됩니다.

3. Timeout Duration 필드에서 요청 재전송에 대한 시간 초과 값(초)을 지정합니다.

   유효한 범위는 1~30입니다. 기본값은 5입니다.

   RADIUS 최대 재전송 및 RADIUS 시간 제한을 구성할 때 최대 지연 시간을 고려하십시오. 여러 RADIUS 서버가 구성된 경우 다음 서버를 시도하기 전에 각 서버의 최대 재전송 값이 소진됩니다. 해당 서버에 구성된 시간 초과 값이 RADIUS 서버의 응답 없이 전달될 때까지 재전송이 발생하지 않습니다. 따라서 RADIUS 애플리케이션으로부터 응답을 수신할 때의 최대 지연 시간은 구성된 모든 서버의 재전송 시간 초과 시간과 같습니다. RADIUS 요청이 사용자 로그인 시도에 의해 생성된 경우 RADIUS 애플리케이션이 응답을 반환할 때까지 모든 사용자 인터페이스가 차단됩니다.

4. Accounting Mode에서 Disable 또는 Enable 라디오 버튼을 선택합니다.

   현재 서버에서 RADIUS 계정 모드를 활성화할지 비활성화할지 여부를 지정합니다.

5. RADIUS Attribute 4 Mode에서 Disable 또는 Enable 라디오 버튼을 선택합니다.

   RADIUS Attribute 4를 활성화하거나 비활성화합니다. 기본값은 Disable입니다. Radius Attribute 4 값은 선택 사항 필드이며 RADIUS Attribute 4 모드가 활성화된 경우에만 볼 수 있습니다. xx.xx.xx.xx 형식의 IP 주소 값을 사용합니다.

Table 206. Radius 구성

필드	설명
Current Server Address	현재 서버의 주소입니다. 구성된 서버가 없으면 이 필드는 비어 있습니다.
Number of Configured Authentication Servers	구성된 인증 RADIUS 서버 수입니다. 값의 범위는 0에서 32까지입니다.
Number of Configured Accounting Servers	구성된 RADIUS 계정 서버 수입니다. 값의 범위는 0에서 32까지입니다.
Number of Named Authentication Server Groups	구성된 명명된 RADIUS 서버 인증 그룹의 수입니다.
Number of Named Accounting Server Groups	구성된 명명된 RADIUS 서버 계정 그룹의 수입니다.

RADIUS 서버 구성

➢ **RADIUS 서버를 구성하려면:**

Security > Management Security> RADIUS > Server Configuration.

1. RADIUS 서버를 추가하려면 다음 설정을 지정합니다.
   - Radius Server IP Address 필드에 RADIUS 서버의 IP 주소를 지정합니다.
   - Radius Server Name 필드에 서버 이름을 지정합니다.
   - Port를 사용하여 이 서버에서 사용하는 UDP 포트를 지정합니다. 유효한 범위는 0~65535입니다.
   - Secret Configured. 이 옵션이 Yes인 경우에만 비밀이 적용됩니다. 옵션이 아니요인 경우 비밀 필드에 입력한 내용은 아무 효과가 없으며 유지되지 않습니다.
   - Secret을 사용하여 이 서버에 대한 공유 비밀을 지정합니다.
   - Primary Server를 사용하여 선택한 서버를 기본 또는 보조 서버로 설정합니다.
   - Message Authenticator를 사용하여 선택한 서버에 대한 메시지 인증자 속성을 Enable하거나 Disable합니다.
2. Add 버튼을 클릭합니다.

   서버가 스위치에 추가됩니다.

   이 버튼은 읽기-쓰기 권한이 있는 admin 사용자 이름으로 로그인한 경우에만 사용할 수 있습니다. 이러한 변경 사항은 저장을 수행하지 않는 한 전원을 껐다 켜도 유지되지 않습니다.
3. 구성에서 선택한 서버를 제거하려면 Delete 버튼을 클릭합니다.

   이 버튼은 읽기-쓰기 권한이 있는 admin 사용자 이름으로 로그인한 경우에만 사용할 수 있습니다. 이러한 변경 사항은 저장을 수행하지 않는 한 전원을 껐다 켜도 유지되지 않습니다.

Current 필드는 이 서버가 현재 인증 서버로 사용되고 있는지 여부를 나타냅니다. 인증 서버

및 RADIUS 통계를 기본값으로 재설정하려면 화면 하단에 있는 Clear Counter 버튼을 클릭하세요.

다음 표에서는 화면에 표시되는 RADIUS 서버 통계에 대해 설명합니다.

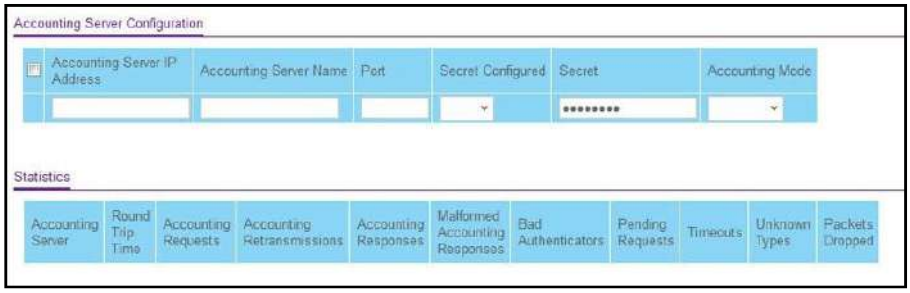
Table 207. RADIUS 통계

필드	설명
Radius Server	통계가 표시되는 RADIUS 서버의 주소 또는 RADIUS 서버의 이름입니다.
Round Trip Time	가장 최근의 액세스 응답/액세스 챌린지와 이 RADIUS 인증 서버에서 일치하는 액세스 요청 사이의 시간 간격(100분의 1초)입니다.
Access Requests	이 서버로 전송된 RADIUS 액세스 요청 패킷 수입니다. 이 숫자에는 재전송이 포함되지 않습니다.
Access Retransmissions	이 서버로 재전송된 RADIUS 액세스 요청 패킷 수입니다.
Access Accepts	유효한 패킷과 잘못된 패킷을 모두 포함하여 이 서버에서 수신된 RADIUS 액세스 허용 패킷 수입니다.
Access Rejects	유효한 패킷과 잘못된 패킷을 모두 포함하여 이 서버에서 수신된 RADIUS 액세스 거부 패킷 수입니다.
Access Challenges	유효한 패킷과 잘못된 패킷을 모두 포함하여 이 서버에서 수신된 RADIUS 액세스 시도 패킷 수입니다.
Malformed Access Responses	이 서버에서 수신된 잘못된 RADIUS 액세스 응답 패킷 수입니다. 잘못된 패킷에는 잘못된 길이의 패킷이 포함됩니다. 잘못된 인증자, 서명 속성 또는 알 수 없는 유형은 잘못된 액세스 응답에 포함되지 않습니다.
Bad Authenticators	이 서버에서 수신된 유효하지 않은 인증자 또는 서명 속성을 포함하는 RADIUS 액세스-응답 패킷 수입니다.
Pending Requests	이 서버로 향하지만 아직 시간 초과되지 않았거나 응답을 받지 못한 RADIUS 액세스 요청 패킷 수입니다.
Timeouts	이 서버에 대한 인증 시간 초과 횟수입니다.
Unknown Types	인증 포트를 통해 이 서버로부터 수신된 알 수 없는 유형의 RADIUS 패킷 수입니다.
Packets Dropped	인증 포트를 통해 이 서버로부터 수신되었지만 다른 이유로 인해 삭제된 RADIUS 패킷 수입니다.

RADIUS 계정 서버 구성

➢ **RADIUS 계정 서버를 구성하려면:**

Security > Management Security > RADIUS > Accounting Server Configuration.



1. Accounting Server IP Address 필드에 RADIUS 계정 서버의 IP 주소를 지정합니다.
2. Accounting Server Name 필드에 계정 서버의 이름을 입력합니다.
3. Port 필드에서 서버가 RADIUS 계정 서버를 확인하는 데 사용하는 UDP 포트 번호를 지정합니다.

   유효한 범위는 0~65535입니다. 사용자에게 읽기 전용 액세스 권한이 있는 경우 값이 표시되지만 변경할 수는 없습니다.
4. 구성된 Secret 목록에서 예를 선택하여 다음 필드에 RADIUS 비밀을 추가합니다.

   RADIUS 계정 서버를 추가한 후 이 필드는 이 서버에 대한 공유 암호가 구성되었는지 여부를 나타냅니다.
5. Secret 필드에 지정된 계정 서버와 함께 사용할 공유 비밀을 입력합니다.
6. Accounting 모드 목록에서 RADIUS 계정 모드를 Enable하거나 Disable합니다.
7. 구성된 RADIUS 계정 서버를 삭제하려면 Delete 버튼을 클릭합니다.

계정 서버 통계를 지우려면 Clear Counters 버튼을 클릭하세요.
다음 표에서는 화면에서 확인할 수 있는 RADIUS 계정 서버 통계에 대해 설명합니다.

Table 208. RADIUS 계정 서버 통계

필드	설명
Accounting Server Address	통계와 관련된 회계 서버입니다.
Round Trip Time(secs)	가장 최근의 계정 응답과 이 RADIUS 계정 서버에서 일치하는 계정 요청 사이의 시간 간격(100분의 1초)입니다.

Accounting Requests	재전송을 포함하지 않고 전송된 RADIUS 계정 요청 패킷 수입니다.
Accounting Retransmissions	이 RADIUS 계정 서버로 재전송된 RADIUS 계정 요청 패킷 수입니다.
Accounting Responses	이 서버의 계정 포트에서 수신된 RADIUS 패킷 수입니다.
Malformed Accounting Responses	이 서버에서 수신된 잘못된 RADIUS 계정 응답 패킷 수입니다. 잘못된 패킷에는 잘못된 길이의 패킷이 포함됩니다. 잘못된 인증자 및 알 수 없는 유형은 잘못된 계정 응답으로 포함되지 않습니다.
Bad Authenticators	이 계정 서버에서 수신한 잘못된 인증자가 포함된 RADIUS 계정 응답 패킷 수입니다.
Pending Requests	이 서버로 전송되었지만 아직 시간 초과되지 않았거나 응답을 받지 못한 RADIUS 계정 요청 패킷 수입니다.
Timeouts	이 서버에 대한 계정 시간 초과 횟수입니다.
Unknown Types	계정 포트를 통해 이 서버로부터 수신된 알 수 없는 유형의 RADIUS 패킷 수입니다.
Packets Dropped	계정 포트를 통해 이 서버로부터 수신되었다가 다른 이유로 인해 삭제된 RADIUS 패킷 수입니다.

TACACS 개요

TACACS는 중앙 집중식 사용자 관리 시스템을 제공하는 동시에 RADIUS 및 기타 인증 프로세스와의 일관성을 유지합니다. TACACS는 다음과 같은 서비스를 제공합니다.

- **Authentication**. 로그인 중, 사용자 이름 및 사용자 정의 비밀번호를 통해 인증을 제공합니다.
- **Authorization**. 로그인 시 수행됩니다. 인증 세션이 완료되면 인증된 사용자 이름을 사용하여 인증 세션이 시작됩니다. TACACS 서버는 사용자 권한을 확인합니다.

ACACS 프로토콜은 장치와 TACACS 서버 간의 암호화된 프로토콜 교환을 통해 네트워크 보안을 보장합니다.

글로벌 TACACS 설정 구성

인밴드 관리 포트를 통해 구성한 TACACS 서버와 스위치 간의 통신을 위한 TACACS 설정을 구성할 수 있습니다.

➢ **글로벌 TACACS 설정을 구성하려면:**

Security > **Management Security** > **TACACS** > **TACACS Configuration**.

1. Key String(키 문자열) 필드에서 스위치와 TACACS 서버 간의 TACACS 통신을 위한 인증 및 암호화 키를 지정합니다.

   유효한 범위는 0~128입니다. 키는 TACACS 서버에 구성된 키와 일치해야 합니다.

2. Connection Timeout 필드에서 관리되는 스위치와 TACACS 서버 사이에 TCP 연결을 설정하는 데 허용되는 최대 시간(초)을 지정합니다.

3. Source Interface 목록에서 TACACS의 소스를 선택합니다.

   가능한 값은 다음과 같습니다.

   - None
   - Routing interface
   - Routing VLAN
   - Routing loopback interface
   - Service port

   기본적으로 VLAN 1은 소스 인터페이스로 사용됩니다.

4. Apply 버튼을 클릭합니다

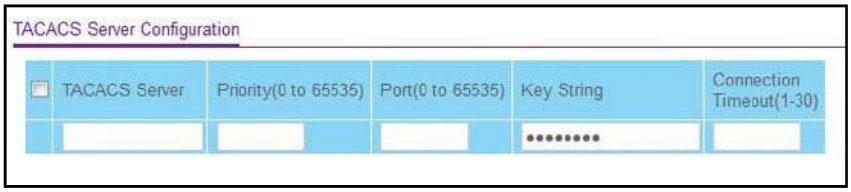
   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

TACACS 서버 설정 구성

스위치가 통신할 수 있는 TACACS 서버를 최대 5개까지 구성할 수 있습니다.

➢ **TACACS 서버 설정을 구성하려면:**

Security > Management Security> TACACS > TACACS Server Configuration.



1. TACACS 서버를 사용하여 TACACS 서버 IP 주소를 구성합니다.
2. Priority를 사용하여 TACACS 서버가 사용되는 순서를 지정합니다.

   유효한 범위는 0~65535입니다.
3. Port를 사용하여 인증 포트를 지정합니다. 0~65535 범위 내에 있어야 합니다.
4. Key String을 사용하여 장치와 TACACS 서버 간의 TACACS 통신을 위한 인증 및 암호화 키를 지정합니다.

   유효한 범위는 0~128입니다. 키는 TACACS 서버에서 사용되는 키와 일치해야 합니다.
5. Connection Timeout를 사용하여 장치와 TACACS 서버 간의 연결 시간이 초과되기 전까지 경과되는 시간을 지정합니다.

   범위는 1~30입니다.
6. Add 버튼을 클릭합니다.

   서버가 스위치에 추가됩니다.

   이 버튼은 읽기/쓰기 사용자만 사용할 수 있습니다. 이러한 변경 사항은 저장을 수행하지 않는 한 전원을 껐다 켜도 유지되지 않습니다.
7. 구성에서 선택한 서버를 삭제하려면 Delete 버튼을 클릭합니다.

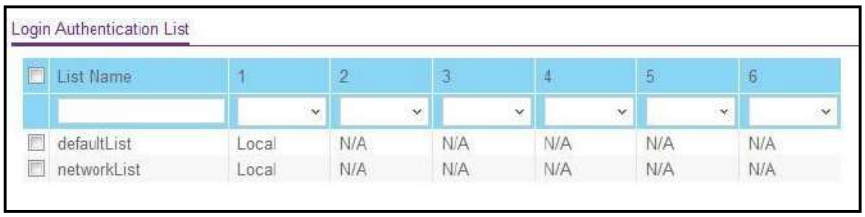
로그인 인증 목록 구성

로그인 목록은 목록과 연결된 사용자의 스위치 또는 포트 액세스를 확인하는 데 사용되는 인증 방법을 지정합니다. 사전 구성된 사용자인 admin 및 guest는 삭제할 수 없는 defaultList라는 사전 구성된 목록에 할당됩니다. 새로 생성된 모든 사용자는 다른 목록에 특별히 할당할 때까지 defaultList에도 할당됩니다.

DefaultList와 networkList라는 두 가지 기본 목록이 있습니다.

➢ **로그인 인증 목록을 구성하려면:**

Security > Management Security > Authentication List > Login Authentication List.



1. 새 로그인 목록을 생성하려면 List Name 필드에 이름을 입력하세요.

   이름은 최대 15자의 영숫자 문자일 수 있으며 대소문자를 구분하지 않습니다.

2. 번호가 매겨진 목록(1, 2, 3, 4, 5, 6)에서 선택한 인증 활성화 목록에 가장 먼저 나타날 방법을 선택합니다.

   옵션은 다음과 같습니다:

   - **Enable**. 권한 있는 EXEC 비밀번호가 인증에 사용됩니다.
   - **Line**. 회선 비밀번호는 인증에 사용됩니다.
   - **None**. 사용자를 인증할 수 없습니다.
   - **RADIUS**. 사용자 이름과 비밀번호는 로컬 서버 대신 RADIUS 서버를 사용하여 인증됩니다.
   - **TACACS**. 사용자 이름과 비밀번호는 TACACS 서버를 통해 인증됩니다.
   - **Deny**. 인증은 항상 실패합니다.

3. Add 버튼을 클릭합니다.

   로그인 목록이 스위치에 추가됩니다.

4. 선택한 인증 로그인 목록을 구성에서 제거하려면 Delete 버튼을 클릭합니다.

   선택한 로그인 목록이 시스템 로그인을 위해 임의의 사용자(기본 사용자 포함)에게 할당된 경우 삭제가 실패합니다. 읽기/쓰기 권한이 있는 admin 사용자로 로그인한 경우에만 이 버튼을 사용할 수 있습니다. 저장을 수행하지 않으면 전원을 껐다 켜도 변경 사항이 유지되지 않습니다.

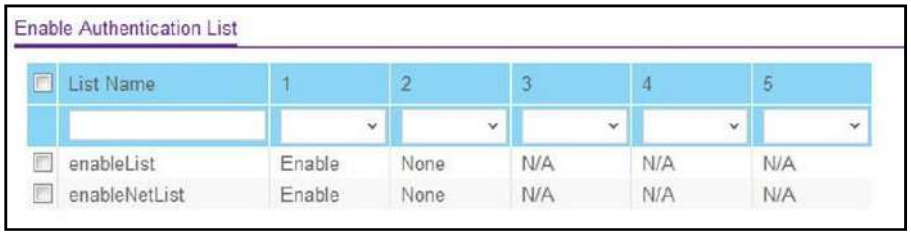
인증 활성화 목록 구성

활성화 목록은 목록과 연결된 사용자에 대해 권한 있는 EXEC 액세스를 검증하는 인증 방법을 지정합니다. 사전 구성된 사용자인 admin 및 guest는 삭제할 수 없는 defaultList라는 사전 구성된 목록에 할당됩니다. 새로 생성된 모든 사용자는 다른 목록에 특별히 할당할 때까지 defaultList에도 할당됩니다. 두 개의 기본 목록(enableList 및 enableNetList)이

있습니다.

➢ **활성화 인증 목록을 구성하려면:**

Security > Management Security > Authentication List > Enable Authentication List.



1. 새 활성화 목록을 생성하려면 목록 이름 필드에 이름을 입력합니다.

   최대 15자의 영숫자까지 가능하며 대소문자를 구분하지 않습니다.

2. 번호가 매겨진 목록(1, 2, 3, 4, 5, 6)에서 선택한 인증 활성화 목록에 가장 먼저 나타날 방법을 선택합니다.

   옵션은 다음과 같습니다:

   - **Enable**. 권한 있는 EXEC 비밀번호가 인증에 사용됩니다.
   - **Line**. 회선 비밀번호는 인증에 사용됩니다.
   - **None**. 사용자를 인증할 수 없습니다.
   - **RADIUS**. 사용자 이름과 비밀번호는 로컬 서버 대신 RADIUS 서버를 사용하여 인증됩니다.
   - **TACACS**. 사용자 이름과 비밀번호는 TACACS 서버를 통해 인증됩니다.
   - **Deny**. 인증은 항상 실패합니다.

3. Add 버튼을 클릭합니다.

   로그인 목록이 스위치에 추가됩니다.

4. 선택한 인증 활성화 목록을 구성에서 제거하려면 삭제 버튼을 클릭합니다.

   읽기/쓰기 권한이 있는 경우에만 이 버튼을 사용할 수 있습니다. 저장을 수행하지 않으면 전원을 껐다 켜도 변경 사항이 유지되지 않습니다.

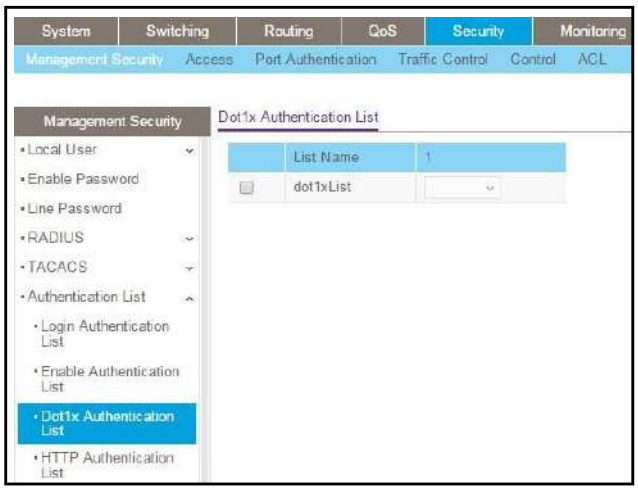
Dot1x 인증 목록 구성

dot1x 목록을 구성할 수 있습니다. dot1x 목록은 목록과 연결된 사용자의 포트 액세스를 확인하는 인증 방법을 지정합니다. dot1x 방법은 하나만 지원될 수 있습니다.

기본 목록은 dot1xList입니다.

➢ **dot1x 인증 목록을 구성하려면:**

Security > Management Security > Authentication List > Dot1x Authentication List.



1. List Name 필드에서 dot1x 목록 이름을 선택합니다.
2. 선택한 인증 로그인 목록에 가장 먼저 나타날 방법을 선택하세요.

   옵션은 다음과 같습니다:

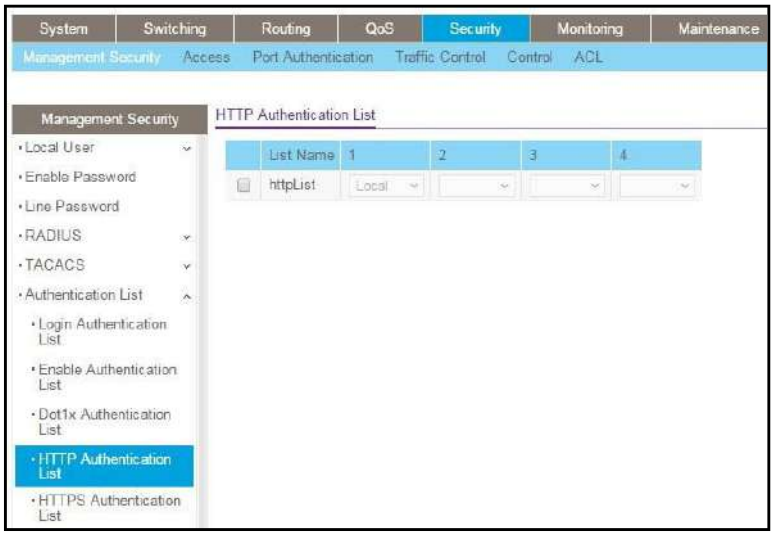
   - **IAS**. 인증은 내부 인증 서버 데이터베이스에 있는 사용자 ID와 비밀번호를 사용합니다.
   - **Local**. 인증에는 사용자의 로컬에 저장된 ID와 비밀번호가 사용됩니다.
   - **RADIUS**. 사용자 ID와 비밀번호는 로컬 인증이 아닌 RADIUS서버를 통해 인증됩니다.
   - **None**. 사용자 이름과 비밀번호 없이 사용자가 인증되었습니다.

HTTP 인증 목록 구성

HTTP 목록을 구성할 수 있습니다. HTTP 목록은 HTTP를 통한 스위치 또는 포트 액세스를 검증하는 인증 방법을 지정합니다.

➢ **HTTP 인증 목록을 구성하려면:**

Security > Management Security > Authentication List > HTTP Authentication List.



1. List Name을 사용하여 HTTP 목록 이름을 선택합니다.
2. 번호가 매겨진 목록(1, 2, 3, 4)에서 선택한 인증 활성화 목록에 가장 먼저 나타날 방법을 선택합니다.

   옵션은 다음과 같습니다:

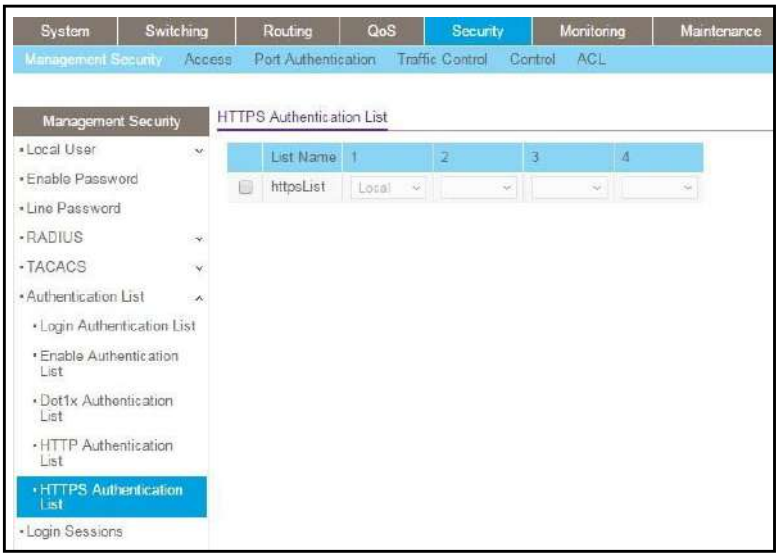
   - **Enable**. 권한 있는 EXEC 비밀번호가 인증에 사용됩니다.
   - **None**. 사용자를 인증할 수 없습니다.
   - **RADIUS**. 사용자 이름과 비밀번호는 로컬 서버 대신 RADIUS 서버를 사용하여 인증됩니다.
   - **TACACS**. 사용자 이름과 비밀번호는 TACACS 서버를 통해 인증됩니다.

HTTPS 인증 목록 구성

HTTPS 목록을 구성할 수 있습니다. 로그인 목록은 목록과 연결된 사용자에 대해 HTTPS를 통해 스위치 또는 포트 액세스를 검증하는 인증 방법을 지정합니다. 기본 목록은 httpsList입니다.

➢ **HTTPS 인증 목록을 구성하려면:**

Security > Management Security > Authentication List > HTTPS Authentication List.



1. HTTPS 목록 이름에 대한 목록 이름 check box을 선택합니다.
2. 번호가 매겨진 목록(1, 2, 3, 4, 5, 6)에서 선택한 인증 활성화 목록에 가장 먼저 나타날 방법을 선택합니다.

   옵션은 다음과 같습니다:

   - **Enable**. 권한 있는 EXEC 비밀번호가 인증에 사용됩니다.
   - **None**. 사용자를 인증할 수 없습니다.
   - **RADIUS**. 사용자 이름과 비밀번호는 로컬 서버 대신 RADIUS 서버를 사용하여 인증됩니다.
   - **TACACS**. 사용자 이름과 비밀번호는 TACACS 서버를 통해 인증됩니다.

로그인 세션 보기

➢ **로그인 세션을 보려면:**

Security > Management Security > Login Sessions.

Table 209. 로그인 세션

필드	설명
ID	이 행의 ID를 식별합니다.
User Name	세션이 열려 있는 사용자의 이름입니다.
Connection From	사용자가 연결된 시스템입니다.
Idle Time	유휴 세션 시간입니다.
Session Time	총 세션 시간입니다.
Session Type	세션 유형: Telnet, Serial 또는 SSH

관리 액세스 구성

스위치 관리 인터페이스에 대한 HTTP 및 보안 HTTP 액세스를 구성할 수 있습니다.

HTTP 서버 설정 구성

웹 브라우저를 사용하여 스위치에 접속하려면 먼저 IP 정보(IP 주소, 서브넷 마스크, 기본 게이트웨이)로 스위치를 구성해야 합니다. 다음 중 하나를 사용하여 IP 정보를 구성할 수 있습니다.

- BOOTP
- DHCP
- Terminal interface through the EIA-232 port

대역 내 연결을 설정한 후에는 웹 기반 관리를 사용하여 IP 정보를 변경할 수 있습니다.

➢ **HTTP 서버 설정을 구성하려면:**

Security > Access> HTTP > HTTP Configuration.

1. HTTP Access 필드에서 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 웹 브라우저에서 스위치에 액세스할 수 있는지 여부를 지정합니다. 웹 모드를 활성화하면 웹 브라우저에서 스위치를 관리할 수 있습니다. 공장 기본값은 Enable입니다.

2. HTTP Port 필드에 HTTP 포트 번호를 입력합니다.

   유효한 범위는 80과 1025~65535입니다. 기본값은 80입니다.

3. Java Mode에서 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이렇게 하면 시스템 탭의 장치 보기 탭에 스위치 그림을 표시하는 Java 애플릿이 활성화되거나 비활성화됩니다. 애플릿을 실행하면 화면 왼쪽의 탐색 트리를 사용하는 대신 스위치 그림을 클릭하여 구성 화면을 선택할 수 있습니다. 공장 기본값은 Enable입니다.

4. HTTP Session Soft Timeout(Minutes) 필드에서 HTTP 세션에 대한 비활성 시간 초과를 설정합니다.

   값은 1~60분 범위에 있어야 합니다. 기본값은 5분입니다. 현재 구성된 값이 표시됩니다.

5. HTTP Session Hard Timeout(Hours) 필드에서 HTTP 세션에 대한 하드 시간 초과를 설정합니다.

   이 시간 초과는 세션의 활동 수준에 영향을 받지 않습니다. 값은 1~168시간 범위에 있어야 합니다. 기본값은 24시간입니다. 현재 구성된 값이 표시됩니다.

6. Maximum Number of HTTP Sessions 필드에서 허용되는 최대 HTTP 세션 수를 설정합니다.

   값은 0~16 범위에 있어야 합니다. 기본값은 16입니다. 현재 구성된 값이 표시됩니다.

   Authentication List 필드에는 HTTP가 사용하는 목록이 표시됩니다.

HTTPS 구성

보안 HTTP를 사용하면 암호화된 SSL(Secure Sockets Layer) 또는 TLS(전송 계층 보안) 연결을 통해 HTTP를 전송할 수 있습니다. 웹 인터페이스를 사용하여 스위치를 관리하는 경우 보안 HTTP는 관리 시스템과 스위치 간의 통신을 도청 및 중간자 공격으로부터 보호하는 데 도움이 될 수 있습니다.

관리 스테이션과 스위치 간의 HTTPS 통신 설정을 구성할 수 있습니다.

➢ **HTTPS 설정을 구성하려면:**

Security > Access > HTTPS > HTTPS Configuration.

1. HTTPS Admin Mode에서 Disable 또는 Enable 라디오 버튼을 선택합니다.

   보안 HTTPS의 관리 모드를 활성화하거나 비활성화합니다. 현재 구성된 값이 표시됩니다. 기본값은 비활성화입니다. HTTPS 관리 모드가 비활성화된 경우에만 SSL 인증서를 다운로드할 수 있습니다. HTTPS 관리 모드는 장치에 인증서가 있는 경우에만 활성화할 수 있습니다.

2. SSL Version 3에서 Disable 또는 Enable 라디오 버튼을 선택합니다.

   SSL(Secure Sockets Layer) 버전 3.0을 활성화하거나 비활성화합니다. 현재 구성된 값이 표시됩니다. 기본값은 Enable입니다.

3. TLS Version 1에서 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 Transport Layer Security 버전 1.0을 활성화하거나 비활성화합니다. 현재 구성된 값이 표시됩니다. 기본값은 Enable입니다.

4. HTTPS Port 필드에 HTTPS 포트 번호를 입력합니다.

   The value must be in the range of 1025 to 65535. Port 443 is the default value. The

currently configured value is displayed.

5. HTTPS Session Soft Timeout(Minutes) 필드에 HTTPS 세션에 대한 비활성 시간 초과를 입력합니다.

   값은 1~60분 범위에 있어야 합니다. 기본값은 5분입니다. 현재 구성된 값이 표시됩니다.

6. HTTPS Session Hard Timeout(Hours) 필드에서 HTTPS 세션에 대한 하드 시간 초과를 설정합니다.

   이 시간 초과는 세션의 활동 수준에 영향을 받지 않습니다. 값은 1~168시간 범위에 있어야 합니다. 기본값은 24시간입니다. 현재 구성된 값이 표시됩니다.

7. Maximum Number of HTTPS Sessions 필드에 허용되는 최대 HTTPS 세션 수를 입력합니다.

   값은 0~16 범위에 있어야 합니다. 기본값은 16입니다. 현재 구성된 값이 표시됩니다.

   Authentication List 필드에는 HTTPS에 대한 인증 목록이 표시됩니다.

인증서 관리

인증서를 생성하거나 삭제할 수 있습니다.

➢ **인증서를 관리하려면:**

Security > Access > HTTPS > Certificate Management.

Certificate Present 필드에는 장치에 인증서가 있는지 여부가 표시됩니다.

1. 다음 라디오 버튼 중 하나를 선택합니다.

   - **None**. 인증서 관리와 관련하여 별도로 수행할 수 있는 작업은 없습니다. 이것이 기본 선택입니다.

- **Generate Certificates**. 인증서 파일 생성을 시작합니다.
- **Delete Certificates**. 해당 인증서 파일이 있는 경우 삭제합니다.

Certificate Generation Status 필드에는 SSL 인증서 생성 상태가 표시됩니다.

인증서 다운로드

인증서 파일을 스위치로 전송할 수 있습니다.

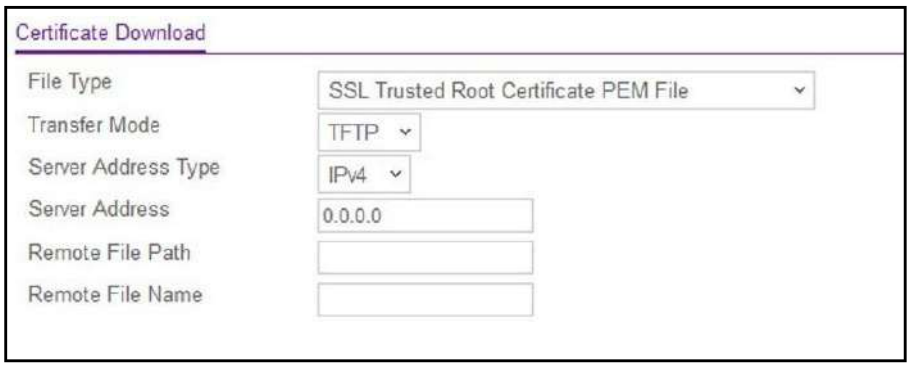
스위치의 웹 서버가 관리 스테이션의 HTTPS 연결을 수락하려면 웹 서버에 공개 키 인증서가 필요합니다. 외부에서(예: 오프라인) 인증서를 생성하고 스위치에 다운로드할 수 있습니다.

스위치에 파일을 다운로드하기 전에 다음 조건이 충족되어야 합니다.

- TFTP 서버에서 다운로드할 파일은 서버의 해당 디렉터리에 있습니다.
- 파일 형식이 올바른지 확인하세요.
- 스위치에는 TFTP 서버에 대한 경로가 있습니다.

➢ **인증서를 다운로드하려면:**

Security > Access > HTTPS > Certificate Download.



1. 파일 형식 목록에서 전송할 파일 형식을 지정합니다.
   - **SSL Trusted Root Certificate PEM File**. SSL 신뢰할 수 있는 루트 인증서 파일(PEM 인코딩)
   - **SSL Server Certificate PEM File**. SSL 서버 인증서 파일(PEM 인코딩)
   - **SSL DH Weak Encryption Parameter PEM File**. SSL Diffie-Hellman 약한 암호화 매개변수 파일(PEM 인코딩)
   - **SSL DH Strong Encryption Parameter PEM File**. SSL Diffie-Hellman 강력한 암호화 매개변수 파일(PEM 인코딩)

2. Transfer Mode 목록에서 파일 전송에 사용할 프로토콜을 지정합니다.
   - **TFTP**. Trivial File Transfer Protocol
   - **SFTP**. Secure File Transfer Protocol
   - **SCP**. Secure Copy Protocol
3. Server Address Type 목록에서 IPv4, IPv6 또는 DNS를 지정하여 TFTP/SFTP/SCP 서버 주소 필드의 형식을 나타냅니다.

   공장 기본값은 IPv4입니다.
4. Server Address 필드에 서버 주소 유형에 표시된 형식에 따라 서버의 IP 주소 또는 DNS 호스트 이름을 입력합니다.

   공장 기본값은 IPv4 주소 0.0.0.0입니다.
5. Remote File Path 필드에 다운로드할 파일의 경로를 입력합니다.

   최대 96자까지 입력할 수 있습니다. 공장 기본값은 공백입니다.
6. Remote File Name 필드에 다운로드할 TFTP 서버의 파일 이름을 입력합니다.

   최대 32자까지 입력할 수 있습니다. 공장 기본값은 공백입니다.

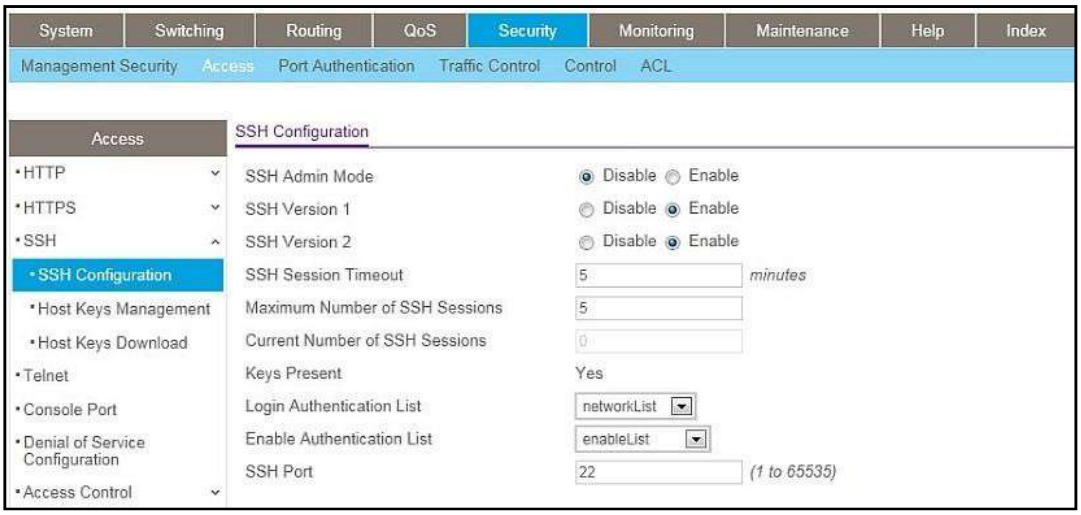
SSH 설정 구성

장치의 SSH(Secure Shell) 서버 설정을 보고 수정할 수 있습니다. SSH는 원격 관리 시스템에서 SSH 클라이언트를 사용하여 CLI 관리 인터페이스에 액세스할 수 있게 해주는 네트워크 프로토콜입니다. SSH는 Telnet보다 더 안전한 액세스 방법입니다.

관리 시스템과 장치 간의 통신을 암호화하기 때문입니다. 안전한 CLI 기반 관리를 위해 SSH 호스트 키를 다운로드하거나 생성할 수 있습니다.

➢ **SSH 설정을 구성하려면:**

Security > Access > SSH > SSH Configuration.



1. SSH Admin Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   SSH 서버 관리 모드를 활성화하거나 비활성화합니다. 이 모드가 활성화되면 원격 시스템에서 SSH 클라이언트를 사용하여 장치에 액세스할 수 있습니다. 현재 구성된 값이 표시됩니다. 기본값은 Disable입니다.

2. SSH Version 1의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   SSH에 대한 프로토콜 수준 1을 활성화하거나 비활성화합니다. 활성화를 선택하면 장치의 SSH 서버가 프로토콜 수준 1을 사용하여 SSH 클라이언트의 연결을 수락할 수 있습니다.

   SSH(SSH-1)의 경우. 비활성화를 선택하면 장치는 SSH-1 프로토콜을 사용하는 클라이언트의 연결을 허용하지 않습니다. 현재 구성된 값이 표시됩니다. 기본값은 Enable입니다.

3. SSH Version 2의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   SSH에 대한 프로토콜 수준 2를 활성화하거나 비활성화합니다. 활성화를 선택하면 장치의 SSH 서버는 SSH용 프로토콜 수준 2(SSH-2)를 사용하여 SSH 클라이언트의 연결을 수락할 수 있습니다. 비활성화를 선택하면 장치는 SSH-2 프로토콜을 사용하는 클라이언트의 연결을 허용하지 않습니다. 현재 구성된 값이 표시됩니다. 기본값은 Enable입니다.

4. SSH Session Timeout를 사용하여 스위치로 들어오는 SSH 세션에 대한 SSH 세션 비활성 시간 초과 값을 구성합니다.

   이 시간 동안 SSH 활동을 나타내지 않는 연결된 사용자는 장치에서 자동으로 연결이 끊어집니다. 이 필드에 허용되는 범위는 1~5분입니다.

5. Maximum Number Of SSH Sessions를 사용하여 장치에 동시에 연결할 수 있는 최대

인바운드 SSH 세션 수를 구성합니다.

현재 구성된 값이 표시됩니다. 이 필드에 허용되는 범위는 0~5입니다.

6. Login Authentication List을 이용하여 인증 목록을 선택하세요.

   이 목록은 스위치에 로그인을 시도하는 사용자를 인증하는 데 사용됩니다.

7. Enable Authentication List를 사용하여 인증 목록을 선택합니다.

   이 목록은 활성화 수준 권한을 얻으려는 사용자를 인증하는 데 사용됩니다.

8. SSH Port를 사용하여 1~65535 사이의 포트 범위를 입력합니다.

   기본값은 22입니다.

9. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

Table 210. SSH 구성

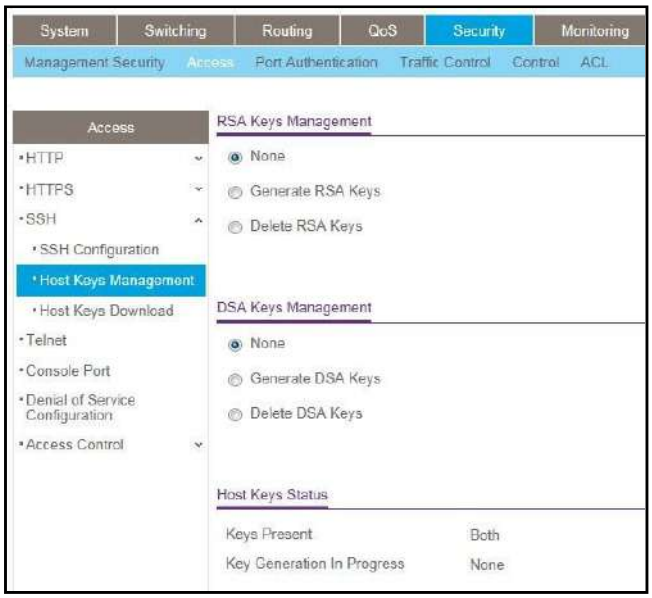
필드	설명
Current Number of SSH Sessions	원격 SSH 클라이언트와 장치의 SSH 서버 간의 활성 SSH 세션 수입니다.
Keys Present	다음 키 중 하나 또는 둘 다(있는 경우)가 장치에 있는지 여부를 Yes 또는 No로 표시합니다. • SSH-1 RSA(Rivest-Shamir-Adelman) 키 파일 또는 SSH-2 RSA 키 파일(PEM 인코딩) • SSH-2 디지털 서명 알고리즘(DSA) 키 파일(PEM 인코딩)

호스트 키 관리

RSA 및 DSA 키를 생성하거나 삭제할 수 있습니다.

➢ **호스트 키를 관리하려면:**

Security > Access > SSH > Host Keys Management.



1. RSA Keys Management 라디오 버튼을 선택합니다.
   - **None**. 이것이 기본 선택입니다.
   - **Generate RSA Keys**. RSA 호스트 키 생성을 시작합니다. SSH 키 파일을 생성하려면 SSH를 관리적으로 비활성화해야 하며 활성 SSH 세션이 없어야 합니다.
   - **Delete RSA Keys**. 해당 RSA 키 파일이 있으면 삭제합니다.
2. DSA 키 관리 라디오 버튼을 선택합니다.
   - **None**. 이것이 기본 선택입니다.
   - **Generate DSA Keys**. DSA 호스트 키 생성을 시작합니다.

     SSH 키 파일을 생성하려면 SSH를 관리적으로 비활성화해야 하며 활성 SSH 세션이 없어야 합니다.
   - **Delete DSA Keys**. 해당 DSA 키 파일이 있으면 삭제합니다.
3. Apply 버튼을 클릭합니다

   호스트 키 파일 다운로드가 시작됩니다. SSH 키 파일을 다운로드하려면 SSH를 관리상 비활성화해야 하며 활성 SSH 세션이 없어야 합니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

Table 211. RSA 키 관리

필드	설명

Keys Present	다음 중 장치에 있는 키 또는 둘 다(있는 경우)를 표시합니다. • SSH-1 RSA(Rivest-Shamir-Adelman) 키 파일 또는 SSH-2 RSA 키 파일(PEM 인코딩) • SSH-2 디지털 서명 알고리즘(DSA) 키 파일(PEM 인코딩)
Key Generation In Progress	생성되는 키(있는 경우), RSA, DSA 또는 없음을 표시합니다.

호스트 키 다운로드

SSH-1 RSA, SSH-2 RSA 또는 SSH-2 DSA 키 파일을 원격 시스템에서 장치로 다운로드할 수 있습니다.

➢ **호스트 키를 다운로드하려면:**

Security > Access > SSH > Host Keys Download.

1. File Type목록에서 전송할 파일 유형을 선택합니다.
   - **SSH-1 RSA Key File**. SSH-1 RSA(Rivest-Shamir-Adelman) 키 파일
   - **SSH-2 RSA Key PEM File**. SSH-2 RSA(Rivest-Shamir-Adelman) 키 파일(PEM 인코딩)
   - **SSH-2 DSA Key PEM File**. SSH-2 디지털 서명 알고리즘(DSA) 키 파일(PEM 인코딩)
2. 전송 모드 목록에서 파일 전송에 사용할 프로토콜을 선택합니다.
   - **TFTP**. Trivial File Transfer Protocol
   - **SFTP**. Secure File Transfer Protocol
   - **SCP**. Secure Copy Protocol
3. Server Address Type 필드에서 IPv4, IPv6 또는 DNS를 지정합니다.

   TFTP/SFTP/SCP 서버 주소 필드의 형식을 지정합니다. 공장 기본값은 IPv4입니다.
4. Server Address 필드에 서버 주소 유형에 표시된 형식에 따라 서버의 IP 주소 또는

DNS 호스트 이름을 입력합니다.

공장 기본값은 IPv4 주소 0.0.0.0입니다.

5. Remote File Path 필드에 다운로드할 파일의 경로를 입력합니다.

   최대 96자까지 입력할 수 있습니다. 공장 기본값은 공백입니다.

6. Remote File Name 필드에 다운로드할 TFTP 서버의 파일 이름을 입력합니다.

   최대 32자까지 입력할 수 있습니다. 공장 기본값은 공백입니다.

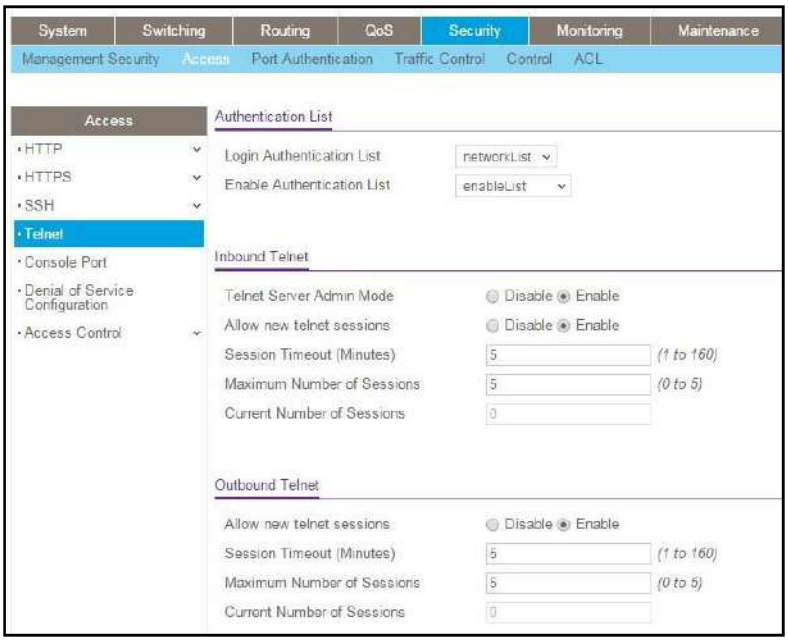
7. Apply 버튼을 클릭합니다

   호스트 키 파일 다운로드가 시작됩니다. SSH 키 파일을 다운로드하려면 SSH를 관리적으로 비활성화해야 하며 활성 SSH 세션이 없어야 합니다.

텔넷 설정 구성

➢ **Telnet 설정을 구성하려면:**

Security > Access > Telnet.



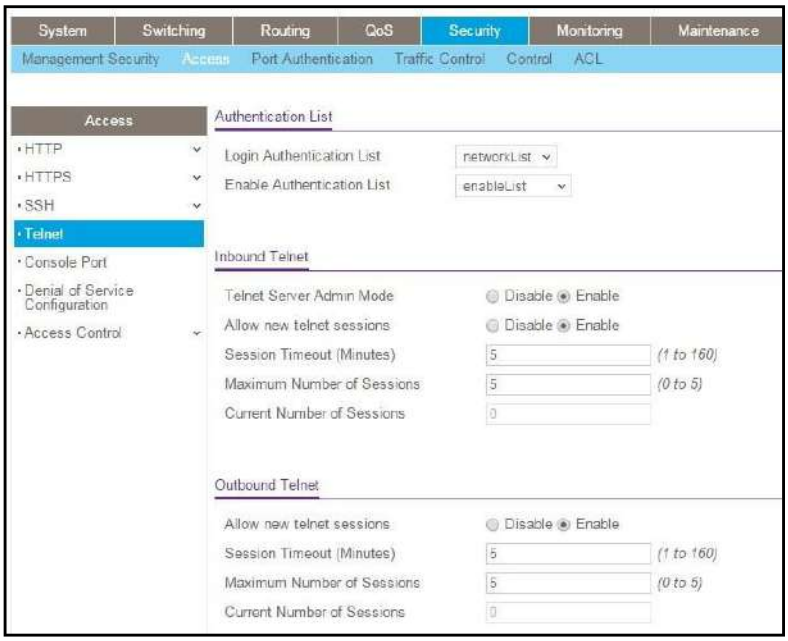
Telnet 인증 목록 구성

사용 가능한 로그인 및 인증 활성화 목록을 선택할 수 있습니다. 로그인 목록은 연결된 사용자의 스위치 또는 포트 액세스를 확인하는 데 사용할 인증 방법을 지정합니다.

목록. 활성화 목록은 목록과 연결된 사용자에 대해 권한 있는 EXEC 액세스를 검증하는 데 사용할 인증 방법을 지정합니다. 이러한 목록은 관리 보안 아래의 인증 목록 링크를 통해 생성할 수 있습니다.

➢ **Telnet 인증 목록을 구성하려면:**

Security > Access > Telnet.



1. Login Authentication List을 사용하여 Telnet을 통해 로그인할 때 사용할 인증 목록을 지정합니다.

   기본값은 networkList입니다.

2. 권한 있는 EXEC 모드로 들어갈 때 사용할 인증 목록을 지정하려면 Enable Authentication List를 사용합니다.

   기본값은 활성화NetList입니다.

3. 인바운드 Telnet 설정을 구성하려면 다음을 지정합니다.

   - Telnet Server Admin Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다.

     이는 Telnet 서버의 관리 모드를 활성화하거나 비활성화합니다. 기본값은 Enable입니다.

   - Allow new telnet Sessions의 Disable 또는 Enable 라디오 버튼을 선택합니다.

     이는 새 인바운드 Telnet 세션의 활성화 또는 비활성화 여부를 지정합니다. 기본값은 사용 가능이므로 더 이상 사용 가능한 세션이 없을 때까지 새 인바운드 Telnet 세션을 설정할 수 있습니다. 비활성화된 경우 새 인바운드 Telnet 세션이 설정되지 않습니다.

설정된 세션은 세션이 종료되거나 비정상적인 네트워크 오류로 인해 세션이 종료될 때까지 활성 상태로 유지됩니다.

- Sesstion Timeout를 사용하여 세션이 로그오프되기 전에 Telnet 세션에서 몇 분 동안 활동이 없는지 지정합니다.
- 1~160 사이의 숫자를 입력할 수 있습니다. 공장 기본값은 5분입니다.
- Maximum Number of Sessions를 사용하여 허용되는 동시 Telnet 세션 수를 지정합니다. 최대값은 5이며 이는 공장 기본값이기도 합니다.

Current Number of Sessions 필드에는 현재 세션 수가 표시됩니다.

4. outbound Telnet 설정을 구성하려면 다음을 지정합니다.

- Allow New Telnet Sessions을 비활성화 또는 활성화 라디오 버튼을 선택합니다

  이는 새 아웃바운드 Telnet 세션의 활성화 또는 비활성화 여부를 지정합니다. 기본값은 사용 가능이므로 더 이상 사용 가능한 세션이 없을 때까지 새 아웃바운드 Telnet 세션을 설정할 수 있습니다. 새 텔넷 세션 허용이 비활성화된 경우 새 아웃바운드 텔넷 세션이 설정되지 않습니다. 설정된 세션은 세션이 종료되거나 비정상적인 네트워크 오류로 인해 세션이 종료될 때까지 활성 상태로 유지됩니다.

- Session Timeout를 사용하여 아웃바운드 Telnet 로그인 비활성 시간 초과를 분 단위로 지정합니다.

  기본값은 5분입니다. 유효한 범위는 1~160입니다.

- Maximum Number of Sessions를 사용하여 허용되는 아웃바운드 텔넷 세션의 최대 수를 지정합니다.

  기본값은 5입니다. 유효한 범위는 0~5입니다.

Current Number of Sessions 필드에는 현재 세션 수가 표시됩니다.

콘솔 포트 구성

➢ **콘솔 포트를 구성하려면:**

Security > Access > Console Port.

1. Serial Port Login Timeout(minutes) 필드에 생하는 시간(분)을 지정합니다.

   0~160 사이의 숫자를 입력합니다. 공장 기본값은 5입니다. 0을 입력하면 시간 초과가 비활성화됩니다.

2. Baud Rate(bps) 연결에 대한 기본 전송 속도를 선택합니다.

   1200, 2400, 4800, 9600, 19200, 38400, 57600 및 115200 보드 중에서 선택할 수 있습니다. 공장 기본값은 115200 보드입니다.

3. Login Authentication List에서 Telnet을 통해 로그인할 때 사용할 인증 목록을 선택합니다.

   기본값은 defaultList입니다.

4. Enable Authentication List에서 권한 있는 EXEC 모드로 들어갈 때 사용할 인증 목록을 선택합니다.

   기본값은 활성화 목록입니다.

다음 표에서는 표시되는 구성할 수 없는 데이터에 대해 설명합니다.

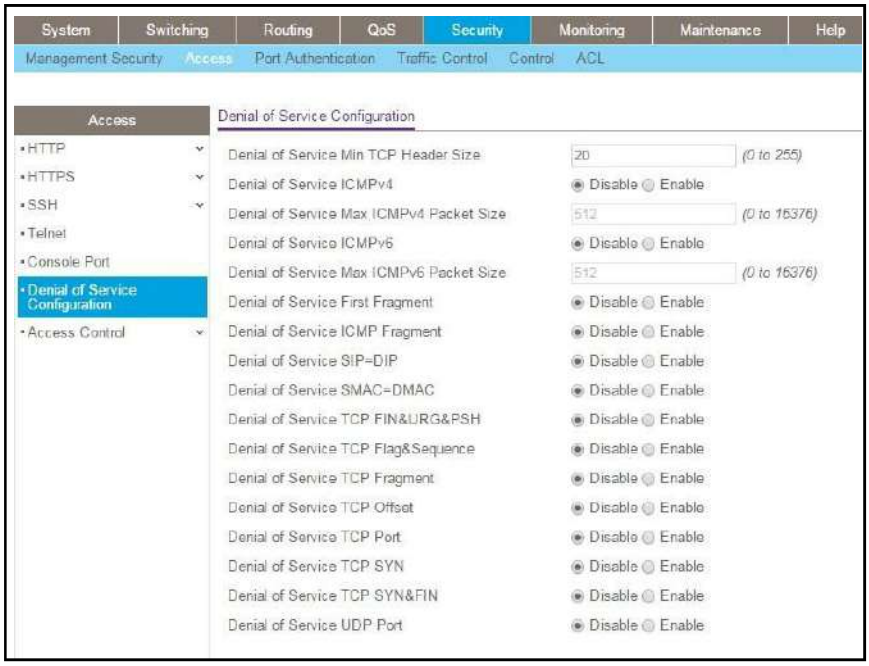
Table 212. 콘솔 포트

필드	설명
Character Size (bits)	문자의 비트 수입니다. 이것은 항상 8입니다.
Flow Control	하드웨어 흐름 제어가 활성화되었는지 또는 비활성화되었는지 여부입니다. 항상 비활성화되어 있습니다.
Stop Bits	문자당 정지 비트 수입니다. 항상 1입니다.
Parity	직렬 포트에 사용되는 패리티 방법입니다. 항상 없음입니다.

서비스 거부 설정 구성

➢ **서비스 거부 설정을 구성하려면:**

Security > Denial of Service Configuration.



1. Denial of Service Min TCP Header Size 필드에서 허용되는 최소 TCP 헤더 크기를 지정합니다.

   DoS TCP 조각이 활성화된 경우 스위치는 다음 패킷을 삭제합니다.

   - TCP 페이로드가 있는 첫 번째 TCP 조각: IP_Payload_Length - IP_Header_Size < Min_TCP_Header_Size.
   - 범위는 0~255입니다. 기본값은 20입니다.

2. Denial of Service ICMPv4의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   ICMPv4 DoS 방지를 활성화하면 스위치는 유형이 ECHO_REQ(ping)로 설정되고 크기가 구성된 ICMPv4 패킷 크기보다 큰 ICMPv4 패킷을 삭제합니다.

   공장 기본값은 Disable입니다.

3. Denial of Service Max ICMPv4 Packet Size를 지정합니다.

   이는 허용되는 최대 ICMPv4 패킷 크기입니다. ICMPv4 DoS 방지가 활성화된 경우 스위치는 구성된 최대 ICMPv4 패킷 크기보다 큰 크기의 IPv4 ICMP ping 패킷을 삭제합니다. 범위는 0~16376입니다. 기본값은 512입니다.

4. Denial of Service ICMPv6을 사용하여 ICMPv6 DoS 방지를 활성화합니다.

이로 인해 스위치는 유형이 ECHO_REQ(ping)로 설정되고 크기가 구성된 ICMPv6 패킷 크기보다 큰 ICMPv6 패킷을 삭제합니다. 공장 기본값은 Disable입니다.

5. Denial of Service Max ICMPv6 Packet Size를 사용하여 허용되는 최대 IPv6 ICMP 패킷 크기를 지정합니다.

   ICMPv6 DoS 방지가 활성화된 경우 스위치는 구성된 최대 ICMPv6 패킷 크기보다 큰 크기의 IPv6 ICMP ping 패킷을 삭제합니다. 범위는 0~16376입니다. 기본값은 512입니다.

6. Denial of Service First Fragment의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이를 통해 스위치가 조각화된 IP 패킷을 수신할 때 스위치가 첫 번째 조각 IP 패킷에 대한 DoS 옵션을 확인하도록 하는 첫 번째 조각 DoS 방지가 활성화됩니다. 그렇지 않으면 스위치는 첫 번째 조각 IP 패키지를 무시합니다. 공장 기본값은 Disable입니다.

7. Denial of Service ICMP Fragment의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   ICMP 조각 DoS 방지를 활성화하면 스위치가 ICMP 조각화된 패킷을 삭제합니다. 공장 기본값은 Disable입니다.

8. Denial of Service SIP=DIP의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   SIP=DIP 활성화 DoS 방지는 스위치가 대상 IP 주소와 동일한 소스 IP 주소를 가진 패킷을 삭제하도록 합니다. 공장 기본값은 Disable입니다.

9. Denial of Service SMAC=DMAC의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   SMAC=DMAC DoS 방지를 활성화하면 스위치는 소스 MAC 주소가 대상 MAC 주소와 동일한 패킷을 삭제합니다. 공장 기본값은 Disable입니다.

10. Denial of Service TCP FIN & URG & PSH의 Disable 또는 Enable 라디오 버튼을 선택합니다.

    TCP FIN & URG & PSH DoS 방지를 활성화하면 스위치는 TCP 플래그 FIN, URG 및 PSH가 설정되고 TCP 시퀀스 번호=0인 패킷을 삭제합니다. 공장 기본값은 Disable입니다.

11. Denial of Service TCP Flag & Sequence의 Disable 또는 Enable 라디오 버튼을 선택합니다.

    TCP 플래그 DoS 방지를 활성화하면 스위치는 TCP 제어 플래그가 0으로 설정되고 TCP 시퀀스 번호가 0으로 설정된 패킷을 삭제합니다. 공장 기본값은 Disable입니다.

12. Denial of Service TCP Fragment의 Disable 또는 Enable 라디오 버튼을 선택합니다.

    TCP 조각 DoS 방지를 활성화하면 스위치가 다음과 같이 패킷을 삭제합니다.

    TCP 페이로드가 있는 첫 번째 TCP 조각: IP_Payload_Length - IP_Header_Size < Min_TCP_Header_Size.

공장 기본값은 비활성화입니다.

13. Denial of Service TCP Offset의 Disable 또는 Enable 라디오 버튼을 선택합니다.

    TCP 오프셋 DoS 방지를 활성화하면 스위치가 TCP 헤더 오프셋=1인 패킷을 삭제합니다. 공장 기본값은 Disable입니다.

14. Denial of Service TCP Port의 Disable 또는 Enable 라디오 버튼을 선택합니다.

    TCP 포트 DoS 방지를 활성화하면 스위치가 TCP 소스 포트가 TCP 대상 포트와 동일한 패킷을 삭제합니다. 공장 기본값은 Disable입니다.

15. Denial of Service TCP SYN의 Disable 또는 Enable 라디오 버튼을 선택합니다.

    TCP SYN DoS 방지를 활성화하면 스위치는 TCP 플래그 SYN이 설정된 패킷을 삭제합니다. 공장 기본값은 Disable입니다.

16. Denial of Service TCP SYN & FIN의 Disable 또는 Enable 라디오 버튼을 선택합니다.

    TCP SYN 및 FIN DoS 방지를 활성화하면 스위치는 TCP 플래그 SYN 및 FIN이 설정된 패킷을 삭제합니다. 공장 기본값은 Disable입니다.

17. Denial of Service UDP Port의 Disaable 또는 Enable 라디오 버튼을 선택합니다.

    UDP 포트 DoS 방지를 활성화하면 스위치가 UDP 대상 포트와 동일한 UDP 소스 포트를 사용하는 패킷을 삭제합니다. 공장 기본값은 Disable입니다.

포트 인증

포트 기반 인증에서 802.1X가 포트에서 전역적으로 활성화되면 포트에 연결된 요청자 중 하나가 성공적으로 인증되면 모든 사용자가 제한 없이 포트를 사용할 수 있습니다. 주어진 시간에 단 한 명의 신청자만이 이 모드의 포트에서 인증을 시도할 수 있습니다. 이 모드의 포트는 양방향 제어를 받습니다. 이는 기본 인증 모드입니다.

802.1X 네트워크에는 세 가지 구성 요소가 있습니다.

- **Authenticators**. 시스템 접근을 허용하기 전에 인증되는 포트입니다.
- **Supplicants**. 시스템 서비스에 대한 액세스를 요청하는 인증된 포트에 연결된 호스트입니다.
- **Authentication Server**. 외부 서버(예: 인증자를 대신하여 인증을 수행하고 사용자에게 시스템 서비스에 액세스할 권한이 있는지 여부를 나타내는 RADIUS 서버).

글로벌 802.1X 설정 구성

➢ **글로벌 802.1X 설정을 구성하려면:**

Security > Port Authentication > Basic > 802.1X Configuration.

1. Administrative Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 스위치의 802.1X 관리 모드를 활성화하거나 비활성화합니다.

   - **Enable**. 스위치에서는 포트 기반 인증이 허용됩니다.

     802.1X가 활성화된 경우 RADIUS 서버에서 인증이 수행됩니다. 이는 기본 인증 방법이 RADIUS여야 함을 의미합니다. 방법을 설정하려면 Security > Management Security > Authentication List을 선택하고 defaultList의 방법 1로 RADIUS를 선택합니다. 자세한 내용은 로그인 인증 목록 구성을 참조하십시오.

   - **Disable**. 포트가 인증된 사용자만 허용하도록 구성된 경우에도 스위치는 포트에서 트래픽을 허용하기 전에 802.1X 인증을 확인하지 않습니다. 기본값입니다.

2. VLAN Assignment Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   기본값은 Disable입니다.

3. EAPOL Flood Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   기본값은 Disable입니다.

4. Dynamic VLAN Creation Mode를 사용하여 Disable 또는 Enable를 선택합니다.

   기본값은 Disable입니다.

5. Monitor Mode를 사용하여 Disable 또는 Enable를 선택합니다.

   기본값은 Disalbe입니다. 이 기능은 dot1x 인증 프로세스를 모니터링하고 인증 실패

사례를 진단하는 데 도움을 줍니다.

6. User를 사용하여 802.1x 포트 보안을 위해 선택한 로그인 목록에 대한 사용자 이름을 선택합니다.
7. Login을 사용하여 지정된 사용자에게 적용할 로그인 목록을 선택합니다.

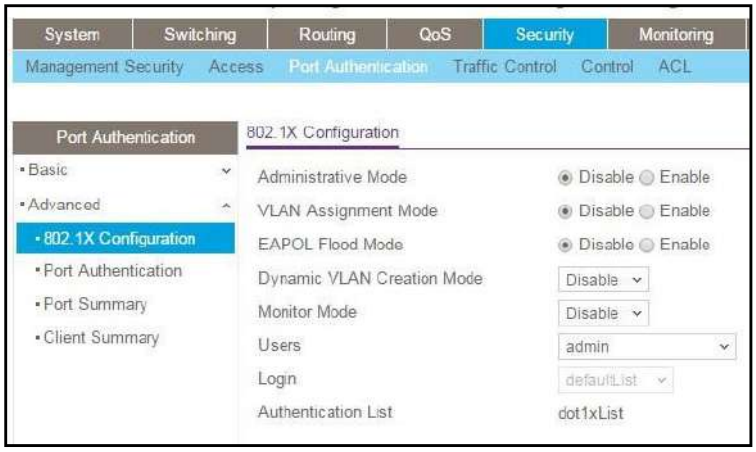
   구성된 모든 로그인 목록이 표시됩니다. 인증 목록 필드에는 802.1X에서 사용되는 인증 목록이 표시됩니다.

802.1X 설정 구성

시스템에서 802.1X 액세스 제어를 활성화하거나 비활성화할 수 있습니다.

➢ **802.1X 설정을 구성하려면:**

Security > Port Authentication > Advanced > 802.1X Configuration.



1. Administrative Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   기본값은 Disable입니다.

2. VLAN Assignment Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   기본값은 Disable입니다.

3. EAPOL Flood Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   기본값은 Disable입니다.

4. Dynamic VLAN Creation Mode를 사용하여 Disable 또는 Enable를 선택합니다.

   기본값은 Disable입니다.

5. Monitor Mode를 사용하여 Disable 또는 Enable를 선택합니다.

기본값은 Disable입니다. 이 기능은 dot1x 인증 프로세스를 모니터링하고 인증 실패 사례를 진단하는 데 도움을 줍니다.

6. Users를 사용하여 802.1x 포트 보안을 위해 선택한 로그인 목록에 대한 사용자 이름을 선택합니다.
7. Login을 사용하여 지정된 사용자에게 적용할 로그인 목록을 선택합니다.

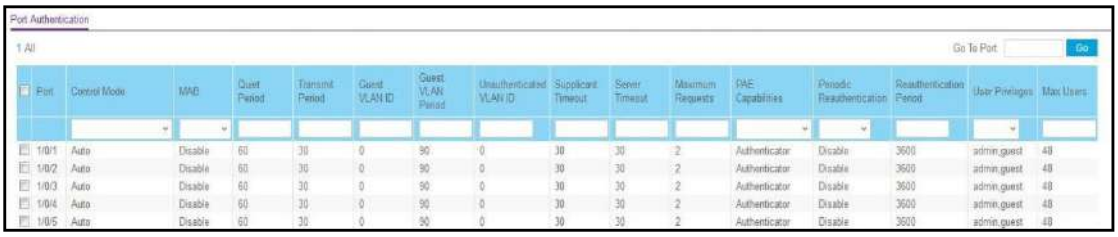
   구성된 모든 로그인 목록이 표시됩니다. Authentication List 필드에는 802.1X에서 사용되는 목록이 표시됩니다.

포트 인증 구성

하나 이상의 포트에서 포트 액세스 제어를 활성화하고 구성할 수 있습니다.

➢ **포트에 대한 802.1X 설정을 구성하려면:**

Security > Port Authentication > Advanced > Port Authentication.



Note: 모든 필드를 보려면 화면 하단의 가로 스크롤 막대를 사용하세요.

1. 구성할 Port 옆의 check box을 선택합니다.

   또한 여러 check box을 선택하여 선택한 포트에 동일한 설정을 적용하거나 제목 행의 check box을 선택하여 모든 포트에 동일한 설정을 적용할 수도 있습니다.

2. 선택한 포트에 대해 다음 설정을 지정합니다.
   - **Control Mode**. 제어 모드에 대한 옵션을 선택합니다. 제어 모드는 포트의 링크 상태가 Link Up인 경우에만 설정됩니다. 옵션은 다음과 같습니다:
     - **Force unauthorized**. 인증자 포트 액세스 엔터티(PAE)는 제어된 포트를 무조건 무단으로 설정합니다.
     - **Force authorized**. 인증자 PAE는 제어되는 포트를 무조건 인증됨으로 설정합니다.
     - **Auto**. 인증자 PAE는 신청자, 인증자 및 인증 서버 간의 인증 교환 결과를 반영하도록 제어된 포트 모드를 설정합니다.
     - **MAC Based**. 인증자 PAE는 신청자별로 신청자, 인증자 및 인증 서버 간의 인증

교환 결과를 반영하도록 제어된 포트 모드를 설정합니다.

- **N/A**. 제어 모드를 적용할 수 없습니다.

- MAB를 사용하여 MAC 기반을 Enable하거나 Disable합니다. 기본 선택은 Disable입니다. 인증자 PAE는 신청자별로 신청자, 인증자 및 인증 서버 간의 인증 교환 결과를 반영하도록 제어된 포트 모드를 설정합니다.
- **Quiet Period**. 이 입력 필드를 사용하면 선택한 포트의 침묵 기간을 구성할 수 있습니다. 이 명령은 신청자를 획득하려고 시도하지 않는 기간을 정의하기 위해 이 포트의 인증자 상태 시스템이 사용하는 타이머의 값을 초 단위로 설정합니다. 침묵 기간은 신청자와의 인증 교환이 실패한 후 인증자가 신청자를 획득하려고 시도하지 않는 기간입니다. 침묵 기간은 0에서 65535 사이의 숫자여야 합니다. 침묵 기간 값이 0이면 인증자 상태 시스템이 신청자를 획득하지 않는다는 의미입니다. 기본값은 60입니다. 값을 변경하면 Apply 버튼을 클릭할 때까지 구성이 변경되지 않습니다.
- **Transmit Period**. 이 입력 필드를 사용하면 선택한 포트의 전송 기간을 구성할 수 있습니다. 전송 기간은 신청자에게 EAPOL EAP 요청/식별 프레임을 보낼 시기를 결정하기 위해 지정된 포트의 인증자 상태 시스템이 사용하는 타이머의 값(초)입니다. 전송 기간은 1~65535 범위의 숫자여야 합니다. 기본값은 30입니다. 값을 변경하면 Apply 버튼을 클릭할 때까지 구성이 변경되지 않습니다.
- **GuestVLAN ID**. 이 필드를 사용하면 인터페이스에서 게스트 VLAN ID를 구성할 수 있습니다. 유효한 범위는 0~4093입니다. 기본값은 0입니다. 값을 변경해도 Apply 버튼을 클릭할 때까지 구성이 변경되지 않습니다. 인터페이스에서 게스트 VLAN ID를 지우려면 0을 입력합니다.
- **Guest VLAN Period**. 이 입력 필드를 사용하면 사용자는 선택한 포트에 대한 게스트 VLAN 기간을 입력할 수 있습니다. 게스트 VLAN 기간은 게스트 VLAN 인증을 위한 타이머의 값(초)입니다. 게스트 VLAN 시간 초과 값은 1~300이어야 합니다.

  기본값은 90입니다. 값을 변경해도 Apply 버튼을 클릭할 때까지 구성이 변경되지 않습니다.
- **Unauthenticated VLAN ID**. 선택한 포트에 대해 인증되지 않은 VLAN ID를 입력하세요. 유효한 범위는 0~4093입니다. 기본값은 0입니다. 값을 변경해도 Apply 버튼을 클릭할 때까지 구성이 변경되지 않습니다. 인터페이스에서 인증되지 않은 VLAN ID를 지우려면 0을 입력합니다.
- **Supplicant Timeout**. 선택한 포트에 대한 신청자 시간 초과를 입력합니다. 신청자 시간 초과는 신청자를 시간 초과하기 위해 이 포트의 인증자 상태 시스템이 사용하는 타이머 값(초)입니다. 신청자 시간 제한은 1~65535 범위에 있어야 합니다. 기본값은

30입니다. 값을 변경하면 Apply 버튼을 클릭할 때까지 구성이 변경되지 않습니다.

- **Server Timeout**. 선택한 포트에 대한 서버 시간 초과를 입력합니다. 서버 시간 초과는 인증 서버의 시간 초과를 위해 이 포트의 인증자가 사용하는 타이머의 값(초)입니다. 서버 시간 제한은 1~65535 범위에 있어야 합니다. 기본값은 30입니다. 값을 변경하면 Apply 버튼을 클릭할 때까지 구성이 변경되지 않습니다.
- **Maximum Requests**. 선택한 포트에 대한 최대 요청 수를 입력합니다. 최대 요청 값은 신청자 시간이 초과되기 전에 이 포트의 인증자 상태 시스템이 EAPOL EAP 요청/ID를 재전송하는 최대 횟수입니다. 최대 요청 값은 1~10 범위에 있어야 합니다. 기본값은 2입니다. 값을 변경하면 Apply 버튼을 클릭할 때까지 구성이 변경되지 않습니다.
- **PAE Capabilities**. 선택한 포트의 PAE(포트 액세스 엔터티) 기능을 선택합니다. 가능한 값은 Authenticator 또는 Supplicant입니다.
- **Periodic Reauthentication**. 지정된 포트에 대한 신청자의 재인증을 활성화하거나 비활성화합니다. 선택 가능한 값은 활성화 또는 비활성화입니다. 값이 활성화되면 재인증이 발생합니다. 그렇지 않으면 재인증이 허용되지 않습니다. 기본값은 Disable입니다. 선택 사항을 변경해도 Apply 버튼을 클릭할 때까지 구성이 변경되지 않습니다.
- **Reauthentication Period**. 선택한 포트의 재인증 기간을 입력하세요. 재인증 기간은 신청자의 재인증이 발생하는 시기를 결정하기 위해 이 포트의 인증자 상태 시스템에 대한 타이머 값(초)입니다. 재인증 기간은 1~65535 범위의 값이어야 합니다. 기본값은 3600입니다. 값을 변경하면 Apply 버튼을 클릭할 때까지 구성이 변경되지 않습니다.
- **User Privileges**. 지정된 포트 또는 모든 포트에 접근할 수 있는 사용자 목록에 지정된 사용자를 추가합니다.
- **Max Users**. 지정된 인터페이스의 신청자 수 제한을 입력합니다.

3. 선택한 포트에서 초기화 시퀀스를 시작하려면 Initialize 버튼을 클릭합니다.

   초기화 시퀀스가 시작됩니다.

   제어 모드가 자동인 경우에만 이 버튼을 클릭할 수 있습니다. 버튼을 사용할 수 없는 경우 회색으로 표시됩니다. 이 버튼을 클릭하면 즉시 작업이 수행됩니다. 작업이 발생하기 위해 Apply 버튼을 클릭할 필요는 없습니다.

4. Reauthentication 버튼을 클릭합니다.

   재인증 시퀀스는 선택한 포트에서 시작됩니다.

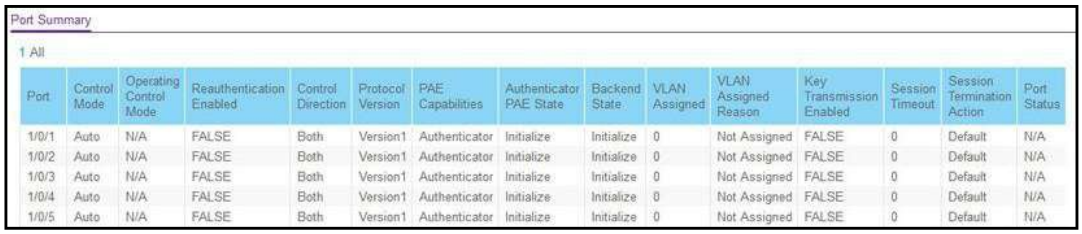
제어 모드가 자동인 경우에만 이 버튼을 클릭할 수 있습니다. 버튼을 사용할 수 없는 경우 회색으로 표시됩니다. 이 버튼을 클릭하면 즉시 작업이 수행됩니다. 작업이 발생하기 위해 Apply 버튼을 클릭할 필요는 없습니다.

포트 요약 보기

특정 포트의 포트 접근 제어 설정에 대한 정보를 볼 수 있습니다.

➢ **포트 요약을 보려면:**

Security > Port Authentication > Advanced > Port Summary.


Port Summary

1 All

Port	Control Mode	Operating Control Mode	Reauthentication Enabled	Control Direction	Protocol Version	PAE Capabilities	Authenticator PAE State	Backend State	VLAN Assigned	VLAN Assigned Reason	Key Transmission Enabled	Session Timeout	Session Termination Action	Port Status
1/0/1	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A
1/0/2	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A
1/0/3	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A
1/0/4	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A
1/0/5	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A

다음 표에서는 포트 요약 화면의 필드에 대해 설명합니다.

Table 214. 포트 요약

필드	설명
Port	현재 테이블 행에 설정이 표시되는 포트입니다.
Control Mode	이 필드는 포트에 대해 구성된 제어 모드를 나타냅니다. 가능한 값은 다음과 같습니다. • **Force Unauthorized**. 인증자 포트 액세스 엔터티(PAE)는 제어된 포트를 무조건 무단으로 설정합니다. • **Force Authorized**. 인증자 PAE는 제어되는 포트를 무조건 인증됨으로 설정합니다. • **Auto**. 인증자 PAE는 신청자, 인증자 및 인증 서버 간의 인증 교환 결과를 반영하도록 제어 포트 모드를 설정합니다. • **MAC Based**. 인증자 PAE는 신청자별로 신청자, 인증자 및 인증 서버 간의 인증 교환 결과를 반영하도록 제어된 포트 모드를 설정합니다.
Operating Control Mode	포트가 실제로 작동하는 제어 모드입니다. 가능한 값은 다음과 같습니다. • ForceUnauthorized • ForceAuthorized • Auto

	• MAC Based • N/A: 포트가 Detached 상태인 경우 포트 접근 제어에 참여할 수 없습니다.
Reauthentication Enabled	이 필드는 지정된 포트에 대한 신청자의 재인증이 허용되는지 여부를 표시합니다. 가능한 값은 True와 False입니다. 값이 True이면 재인증이 발생합니다. 그렇지 않으면 재인증이 허용되지 않습니다.
Control Direction	지정된 포트에 대한 제어 방향입니다. 제어 방향은 신청자와 인증자 간에 프로토콜 교환이 이루어지는 정도를 나타냅니다. 이는 승인되지 않은 제어 포트가 양방향(들어오는 프레임과 나가는 프레임 모두 비활성화) 또는 들어오는 방향(들어오는 프레임의 수신만 비활성화)의 통신에 대한 제어를 행사하는지 여부에 영향을 줍니다. 일부 플랫폼에서는 이 필드를 구성할 수 없습니다.
Protocol Version	선택한 포트와 관련된 프로토콜 버전입니다. 유일하게 가능한 값은 802.1x 사양의 첫 번째 버전에 해당하는 1입니다. 이 필드는 구성할 수 없습니다.
PAE Capabilities	선택한 포트의 PAE(포트 액세스 엔터티) 기능입니다. 가능한 값은 인증자 또는 신청자입니다. 이 필드는 구성할 수 없습니다.
Authenticator PAE State	인증자 PAE 상태 시스템의 현재 상태입니다. 가능한 값은 다음과 같습니다. • Initialize • Disconnected • Connecting • Authenticating • Authenticated • Aborting • Held • ForceAuthorized • ForceUnauthorized
Backend State	백엔드 인증 상태 머신의 현재 상태입니다. 가능한 값은 다음과 같습니다. • Request • Response • Success • Fail • Timeout • Initialize • Idle
VLAN Assigned	인증자가 선택한 인터페이스에 할당한 VLAN ID입니다. 이 필드는 선택한 인터페이스의 포트 제어 모드가 MAC 기반이 아닌 경우에만 표시됩니다. 이 필드는 구성할 수 없습니다.
VLAN Assigned Reason	인증자가 선택한 인터페이스에 할당한 VLAN ID의 이유입니다. 이 필드는 선택한 인터페이스의 포트 제어 모드가 MAC 기반이 아닌

	경우에만 표시됩니다. 이 필드는 구성할 수 없습니다. 가능한 값은 다음과 같습니다. • Radius • Unauth • Default • Not Assigned
Key Transmission Enabled	이 필드는 선택한 포트에서 키 전송이 활성화되었는지 여부를 표시합니다. 이는 구성 가능한 필드가 아닙니다. 가능한 값은 True와 False입니다. 값이 False이면 키 전송이 발생하지 않습니다. 그렇지 않으면 선택한 포트에서 키 전송이 지원됩니다.
Session Timeout	선택한 포트에 대해 RADIUS 서버에서 설정한 세션 종료 시간입니다. 이 필드는 선택한 포트의 포트 제어 모드가 MAC 기반이 아닌 경우에만 표시됩니다.
Session Termination Action	선택한 포트에 대해 RADIUS 서버가 설정한 종료 동작입니다. 이 필드는 선택한 포트의 포트 제어 모드가 MAC 기반이 아닌 경우에만 표시됩니다. 가능한 값은 다음과 같습니다. • Default • Reauthenticate 종료 작업이 기본값으로 설정된 경우 세션이 끝나면 클라이언트 세부 정보가 초기화됩니다. 그렇지 않으면 재인증이 시도됩니다.
Port Status	지정된 포트의 인증 상태입니다. 가능한 값은 승인됨, 승인되지 않음 및 해당 없음입니다. 포트가 분리된 상태인 경우 해당 포트는 포트 액세스 제어에 참여할 수 없으므로 값은 N/A입니다.

클라이언트 요약 보기

➢ **클리아언트 요약을 보려면:**

Security > Port Authentication > Advanced > Client Summary.

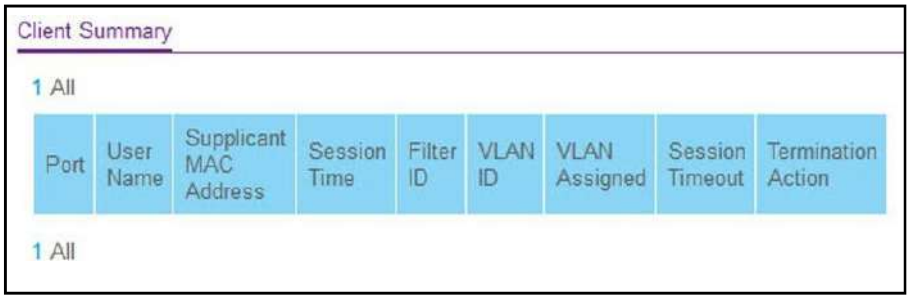


Table 215. 클라이언트 요약

필드	설명
Port	표시할 포트입니다.
User Name	신청자 장치의 ID를 나타내는 사용자 이름입니다.
Supplicant Mac Address	신청자의 장치 MAC 주소입니다.
Session Time	신청자가 로그인한 이후의 시간(초)입니다.
Filter ID	인증자가 신청자 장치에 할당한 정책 필터 ID입니다.
VLAN ID	인증자가 신청자 장치에 할당한 VLAN ID입니다.
VLAN Assigned	인증자가 신청자 장치에 할당한 VLAN ID의 이유입니다.
Session Timeout	RADIUS 서버가 신청자 장치에 설정한 세션 시간 제한입니다.
Termination Action	RADIUS 서버가 신청자 장치에 설정한 종료 작업입니다.

트래픽 제어

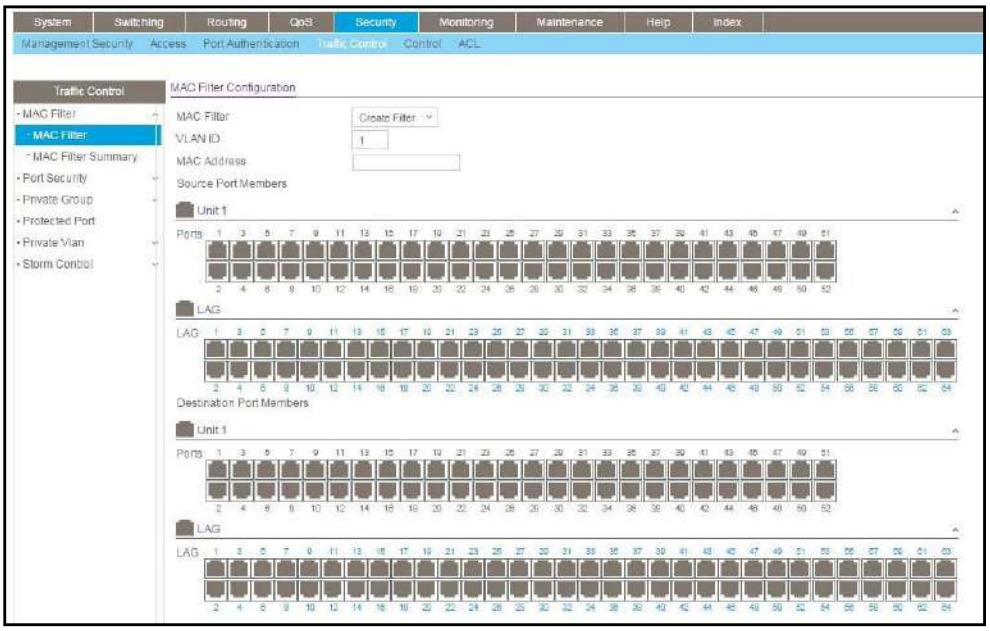
MAC 필터, 스톰 제어, 포트 보안 및 보호된 포트 설정을 구성할 수 있습니다.

MAC 필터링 구성

시스템의 지정된 포트로 들어오고 나가는 트래픽을 제한하는 MAC 필터를 만들 수 있습니다.

- **MAC 필터 설정을 구성하려면:**

  Security > Traffic Control > MAC Filter.



구성된 모든 필터에 대한 MAC 주소 및 VLAN ID 쌍 목록입니다.

1. 기존 필터의 포트 마스크를 변경하려면 항목을 선택합니다.
2. 새 필터를 추가하려면 MAC Filter List에서 Create Filter을 선택합니다.
3. VLAN ID 목록에서 필터링할 패킷을 완전히 식별하기 위해 MAC 주소와 함께 사용할 VLAN을 선택합니다.

   MAC Filter 목록에서 Create Filter를 선택한 경우에만 이 필드를 변경할 수 있습니다.
4. MAC Address 필드에서 필터의 MAC 주소를 00:01:1A:B2:53:4D 형식으로 지정합니다.

   필터 생성 옵션을 선택할 때 이 필드를 변경할 수 있습니다.

   다음 MAC 주소에 대해서는 필터를 정의할 수 없습니다.
   - 00:00:00:00:00:00
   - 01:80:C2:00:00:00 to 01:80:C2:00:00:0F
   - 01:80:C2:00:00:20 to 01:80:C2:00:00:21
   - FF:FF:FF:FF:FF:FF
5. Source Port Members을 사용하여 인바운드 필터에 포함될 포트를 나열합니다.

   선택한 MAC 주소와 VLAN ID를 가진 패킷이 목록에 없는 포트에서 수신되면 해당 패킷은 삭제됩니다.
6. Destination Port Member을 사용하여 아웃바운드 필터에 포함될 포트를 나열합니다.

   선택한 MAC 주소와 VLAN ID가 포함된 패킷은 목록에 있는 포트에서만 전송됩니다. 대상 포트는 멀티캐스트 필터에만 포함될 수 있습니다.
7. 구성된 MAC 필터를 삭제하려면 해당 필터를 선택한 다음 Delete 버튼을 클릭합니다.

8. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

MAC 필터 요약

➢ **MAC 필터 요약을 보려면:**

Security > Traffic Control > MAC Filter > MAC Filter Summary.

다음 표에서는 화면에 표시되는 정보에 대해 설명합니다.

Table 216. MAC 필터 요약

필드	설명
MAC Address	00:01:1A:B2:53:4D 형식의 필터 MAC 주소.
VLAN ID	필터와 연결된 VLAN ID입니다.
Source Port Members	인바운드 패킷 필터링에 사용할 포트 목록입니다.
Destination Port Members	아웃바운드 패킷을 필터링하는 데 사용할 포트 목록입니다.

포트 보안

포트 보안 설정을 구성할 수 있습니다.

글로벌 포트 보안 모드 구성

시스템에서 하나 이상의 포트를 잠글 수 있습니다. 포트가 잠겨 있으면 허용되는 소스 MAC 주소가 있는 패킷만 전달할 수 있습니다. 다른 모든 패킷은 삭제됩니다.

➢ **글로벌 포트 보안 모드를 구성하려면:**

Security > Traffic Control > Port Security > Port Administration.

1. Port Security Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다.

포트 보안 위반 테이블에는 포트 보안이 활성화된 포트에서 발생한 위반에 대한 정보가 표시됩니다. 다음 표에서는 포트 보안 위반 테이블의 필드에 대해 설명합니다.

Table 217. 포트 보안 위반

필드	설명
Port	물리적 인터페이스.
Last Violation MAC	잠긴 포트에서 버려진 마지막 패킷의 소스 MAC 주소입니다.
VLAN ID	마지막 위반 MAC 주소에 해당하는 VLAN ID입니다.

포트 보안 인터페이스 구성

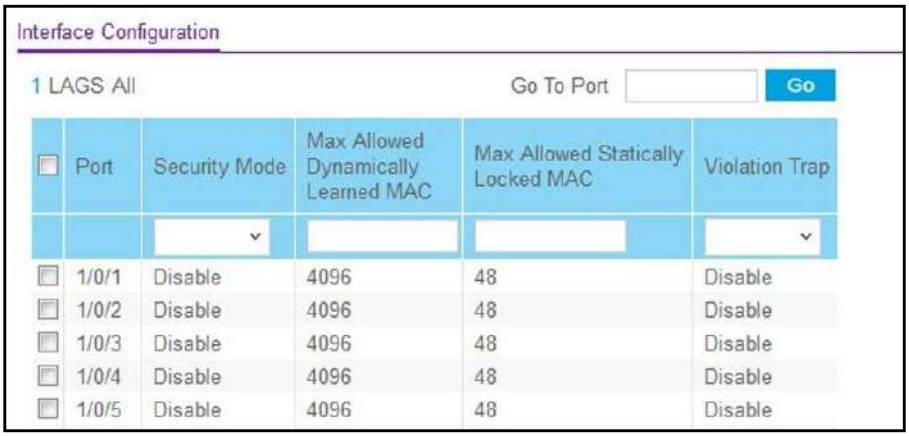
MAC 주소는 동적 또는 정적으로 두 가지 방법 중 하나로 허용되도록 정의할 수 있습니다. 포트가 잠겨 있을 때 두 가지 방법이 동시에 사용됩니다.

동적 잠금은 포트 보안을 위한 선착순 메커니즘을 구현합니다. 잠긴 포트에서 학습할 수 있는 주소 수를 지정합니다. 제한에 도달하지 않은 경우 소스 MAC 주소를 알 수 없는 패킷이 학습되어 정상적으로 전달됩니다. 제한에 도달하면 포트에서 더 이상 주소가 학습되지 않습니다. 아직 학습되지 않은 소스 MAC 주소가 있는 모든 패킷은 삭제됩니다. 허용되는 동적 항목 수를 0으로 설정하면 동적 잠금을 효과적으로 비활성화할 수 있습니다.

정적 잠금을 사용하면 포트에 허용되는 MAC 주소 목록을 지정할 수 있습니다. 패킷의 동작은 동적 잠금과 동일합니다. 허용되는 소스 MAC 주소가 있는 패킷만 전달할 수 있습니다.

➢ **포트 보안 설정을 구성하려면:**

Security > Traffic Control > Port Security > Interface Configuration.



1. 구성할 포트 또는 LAG 옆의 check box을 선택합니다.

   선택한 모든 인터페이스에 동일한 설정을 적용하려면 여러 check box을 선택합니다. 모든 인터페이스에 동일한 설정을 적용하려면 제목 행의 check box을 선택합니다.

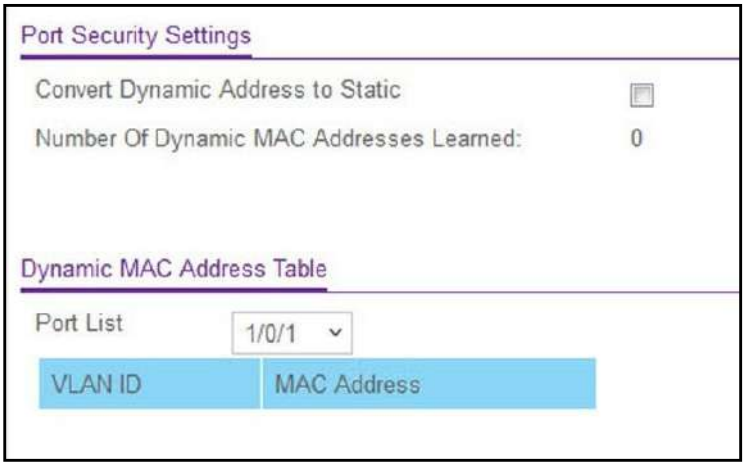
2. 다음 설정을 지정합니다.
   - **Security Mode**. 선택한 인터페이스에 대한 포트 보안 기능을 활성화하거나 비활성화합니다.
   - **Max Allowed Dynamically Learned MAC**. 선택한 인터페이스에서 동적으로 학습된 MAC 주소의 최대 수를 설정합니다.
   - **Max Allowed Statically Locked MAC**. 선택한 인터페이스에서 정적으로 잠긴 MAC 주소의 최대 수를 설정합니다.
   - **Violation Traps**. 허용되지 않는 MAC 주소가 있는 패킷이 잠긴 포트에서 수신될 때를 지정하는 새로운 위반 트랩 전송을 활성화하거나 비활성화합니다.

학습된 MAC 주소를 정적 주소로 변환

동적으로 학습된 MAC 주소를 정적으로 잠긴 주소로 변환할 수 있습니다.

➢ **학습된 MAC 주소를 변환하려면:**

Security > Traffic Control > Port Security > Dynamic MAC Address.



1. Port List을 사용하여 물리적 인터페이스를 선택합니다.
2. Convert Dynamic Address to Static을 사용하여 동적으로 학습된 MAC 주소를 정적으로 잠긴 주소로 변환합니다.

   동적 MAC 주소 항목은 정적 제한에 도달할 때까지 숫자 오름차순으로 정적 MAC 주소 항목으로 변환됩니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

다음 표에는 선택한 포트에서 학습된 MAC 주소와 관련 VLAN이 나와 있습니다. 인터페이스를 선택하려면 Port List 메뉴를 사용하십시오.

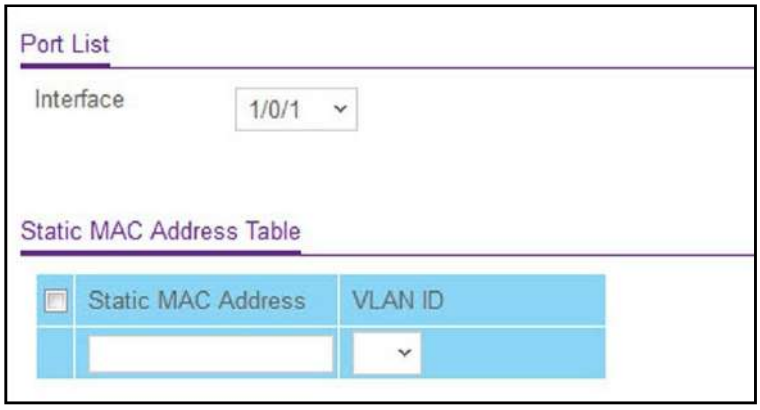
Table 218. 동적 MAC 주소

필드	설명
Number of Dynamic MAC Addresses Learned	특정 포트에서 동적으로 학습된 MAC 주소의 수입니다.
VLAN ID	MAC 주소에 해당하는 VLAN ID입니다.
MAC Address	특정 포트에서 학습된 MAC 주소입니다.

정적 MAC 주소 구성

➢ **정적 MAC 주소를 구성하려면:**

Security > Traffic Control > Port Security > Static MAC Address.



1. Interface를 사용하여 물리적 인터페이스를 선택합니다.
2. Static MAC Address. 추가할 MAC 주소에 대한 사용자 입력을 허용합니다.
3. VLAN ID를 사용하여 추가 중인 MAC 주소에 해당하는 VLAN ID를 선택합니다.
4. Add 버튼을 클릭합니다.

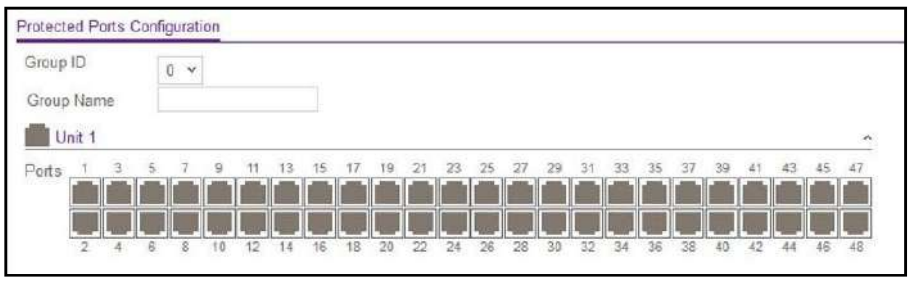
   정적 MAC 주소가 스위치에 추가됩니다.
5. 스위치에서 기존 고정 MAC 주소를 삭제하려면 Delete 버튼을 클릭합니다.

보호된 포트 구성

포트가 보호되도록 구성된 경우 스위치의 다른 보호된 포트로는 트래픽을 전달하지 않지만 보호되지 않는 포트로는 트래픽을 전달합니다. 포트를 보호되거나 보호되지 않도록 구성할 수 있습니다. 구성을 수정하려면 읽기-쓰기 액세스 권한이 필요합니다.

➢ **보호된 포트를 구성하려면:**

Security > Traffic Control > Protected Ports.



1. Group ID 목록에서 논리적 그룹으로 결합할 수 있는 보호 포트 그룹을 선택합니다.

   트래픽은 서로 다른 그룹에 속하는 보호된 포트 간에 흐를 수 있지만 동일한 그룹 내에서는 흐를 수 없습니다. 목록에는 현재 플랫폼에 대해 지원되는 가능한 모든 보호

포트 그룹 ID가 포함됩니다. Group ID의 유효한 범위는 0~2입니다.

2. 선택적인 Group Name 필드를 사용하여 이름을 보호된 포트 그룹(식별 목적으로 사용)과 연결합니다.

   공백을 포함하여 최대 32자의 영숫자 문자일 수 있습니다. 기본값은 공백입니다. 이 필드는 선택 사항입니다.

3. 주황색 막대를 클릭하여 사용 가능한 포트를 표시합니다.
4. 보호 포트로 구성할 각 포트 아래의 확인란을 선택합니다.

   선택 목록은 보호되는 포트와 보호되지 않는 포트로 구성됩니다. 보호되는 포트는 구별하기 위해 체크 표시가 되어 있습니다. 보호된 두 포트 사이에는 트래픽 전달이 불가능합니다. 구성되지 않은 채로 두면 기본 상태는 보호되지 않습니다.

5. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

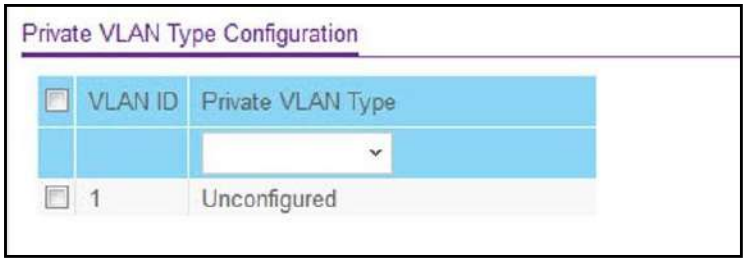
스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

프라이빗 VLAN 구성

사설 VLAN에는 서로 통신할 수 없지만 다른 네트워크에 액세스할 수 있는 스위치 포트가 포함되어 있습니다. 이러한 포트를 개인 포트라고 합니다. 각 사설 VLAN에는 하나 이상의 사설 포트와 단일 업링크 포트 또는 업링크 집계 그룹이 포함되어 있습니다. 개인 포트 간의 모든 트래픽은 레이어 2 트래픽뿐만 아니라 FTP, HTTP, Telnet과 같은 트래픽도 모든 레이어에서 차단됩니다.

➢ **사설 VLAN 유형을 구성하려면:**

Security > Traffic Control > Private VLAN > Private VLAN Type Configuration.



1. Private VLAN Type을 사용하여 Private VLAN 유형을 선택합니다.

공장 기본값은 Unconfigured입니다.

2. Apply 버튼을 클릭합니다

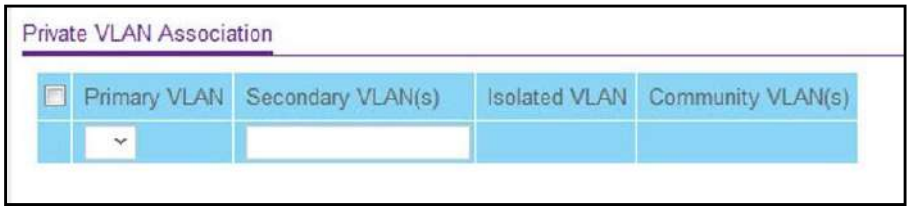
   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

   VLAN ID 필드는 사설 VLAN 유형이 설정되는 VLAN ID를 지정합니다. 공장 기본값은 Unconfigured입니다.

사설 VLAN 연결 설정 구성

➢ **사설 VLAN 연결을 구성하려면:**

Security > Traffic Control > Private VLAN > Private VLAN Association Configuration.



1. Primary VLAN을 사용하여 도메인의 기본 VLAN ID를 선택합니다.

   이는 보조 VLAN을 도메인과 연결하는 데 사용됩니다.

2. Secondary VLAN을 사용하여 정적으로 생성된 모든 VLAN을 표시합니다 (기본 및 기본 VLAN 제외).

   이 컨트롤은 VLAN을 선택한 기본 VLAN과 연결하는 데 사용됩니다.

3. 스위치에서 IP 서브넷 기반 VLAN을 삭제하려면 Delete 버튼을 클릭합니다.

4. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

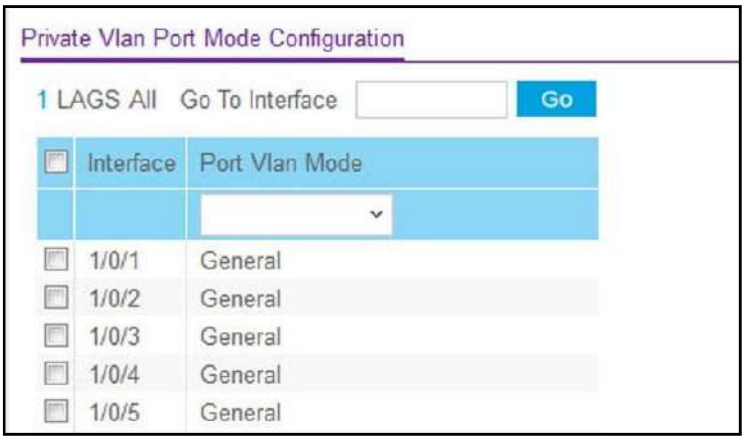
Table 220. 사설 VLAN 연관

필드	설명
Isolated VLAN	선택한 기본 VLAN과 연결된 격리된 VLAN입니다.
Community VLAN(s)	선택한 기본 VLAN과 연결된 커뮤니티 VLAN 목록입니다.

사설 VLAN 포트 모드 구성

➢ **사설 VLAN 포트 모드를 구성하려면:**

Security > Traffic Control > Private VLAN > Private VLAN Port Mode Configuration.



1. 스위치 포트 모드를 사용하여 스위치 포트 모드를 선택합니다.
   - **General**: 포트를 일반 모드로 설정합니다.
   - **Host**: 호스트 모드에서 포트를 설정합니다. 사설 VLAN 구성에 사용됩니다.
   - **Promiscuous**: 포트를 무차별 모드로 설정합니다. 사설 VLAN 구성에 사용됩니다.

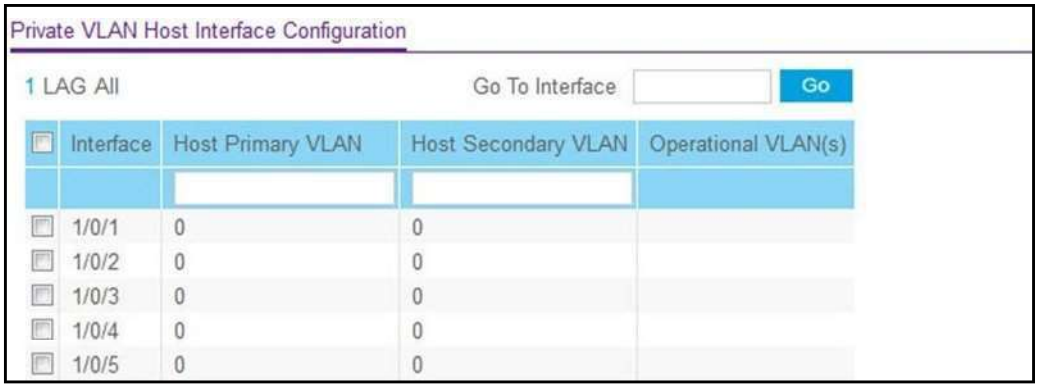
   공장 기본값은 General입니다.
2. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

사설 VLAN 호스트 인터페이스 구성

➢ **개인 VLAN 호스트 인터페이스를 구성하려면:**

Security > Traffic Control > Private VLAN > Private VLAN Host Interface Configuration.



1. Host Primary VLAN 필드에서 호스트 연결 모드에 대한 기본 VLAN ID를 설정합니다.

   VLAN ID의 범위는 2~4093입니다.

2. Host Secondary VLAN을 사용하여 호스트 연결 모드에 대한 보조 VLAN ID를 설정합니다.
   VLAN ID의 범위는 2~4093입니다..

3. 스위치에서 IP 서브넷 기반 VLAN을 삭제하려면 Delete 버튼을 클릭합니다.
4. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

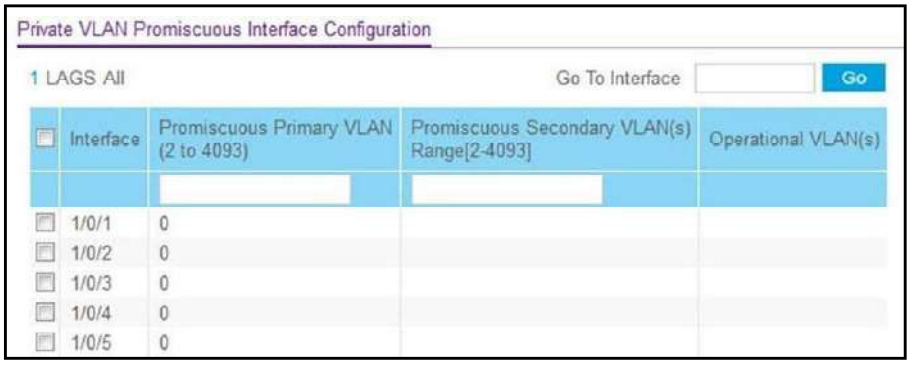
Table 221. 사설 VLAN 호스트 인터페이스 구성

필드	설명
Interface	물리적 또는 LAG 인터페이스를 선택합니다.
Operational VLAN(s)	작동 VLAN.

프라이빗 VLAN 무차별 인터페이스 구성

➢ **사설 VLAN 무차별 인터페이스를 구성하려면:**

Security > Traffic Control > Private VLAN > Private VLAN Promiscuous Interface Configuration.



1. Promiscuous Primary VLAN을 사용하여 무차별 연결 모드에 대한 기본 VLAN ID를 설정합니다.

   VLAN ID의 범위는 2~4093입니다.

2. Promiscuous Secondary VLAN ID를 사용하여 무차별 연결 모드에 대한 보조 VLAN ID 목록을 설정합니다.

   이 필드는 단일 VLAN ID, VLAN ID 범위 또는 ','로 구분된 순서대로 두 가지의 조합을 허용할 수 있습니다. 개별 VLAN ID(예: 10)를 지정할 수 있습니다. VLAN 범위 값을 하이픈으로 구분하여 지정할 수 있습니다(예: 10-13). 두 가지 조합을 쉼표로 구분하여 지정할 수 있습니다. 예를 들면 다음과 같습니다.

   12,15,40–43,1000–1005, 2000. VLAN ID의 범위는 2–4093입니다.

   Note: 이 컨트롤에 제공된 VLAN ID 목록은 연결에 구성된 보조 VLAN 목록을 대체합니다.

3. Click the **Delete** button to delete the IP subnet-based VLAN from the switch.
4. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 222. 사설 VLAN 무차별 인터페이스 구성

필드	설명
Interface	물리적 또는 LAG 인터페이스 선택
Operational VLAN(s)	작동 VLAN.

Storm 컨트롤

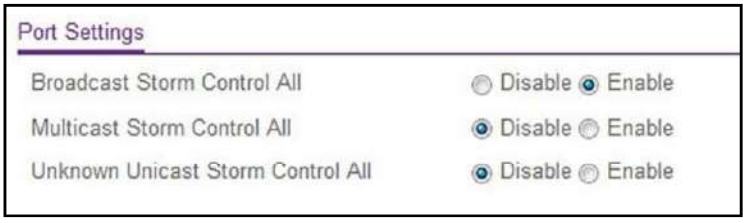
브로드캐스트 폭풍은 단일 포트를 통해 네트워크를 통해 동시에 전송되는 과도한 수의 브로드캐스트 메시지로 인해 발생합니다. 전달된 메시지 응답으로 인해 네트워크 리소스가 과부하되거나 네트워크 시간 초과가 발생할 수 있습니다.

스위치는 포트당 들어오는 브로드캐스트/멀티캐스트/알 수 없는 유니캐스트 패킷 속도를 측정하고 속도가 정의된 값을 초과하면 패킷을 삭제합니다. 스톰 제어는 패킷 유형과 패킷 전송 속도를 정의하여 인터페이스별로 활성화됩니다.

전역 폭풍 제어 설정 구성

➢ **전역 폭풍 제어 설정을 구성하려면:**

Security > Traffic Control > Storm Control > Storm Control Global Configuration.



다음 세 가지 컨트롤은 각 유형의 패킷을 글로벌 방식으로 모든 포트에서 속도 제한하도록 활성화하거나 비활성화하는 쉬운 방법을 제공합니다. 각 포트의 효과적인 스톰 제어 상태는 포트 구성 화면으로 이동하여 확인할 수 있습니다.

1. Broadcast Strom Control All의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 모든 포트에서 브로드캐스트 스톰 복구 모드를 활성화하거나 비활성화합니다. 활성화를 지정하고 이더넷 포트의 브로드캐스트 트래픽이 구성된 임계값을 초과하면 스위치는 브로드캐스트 트래픽을 차단(폐기)합니다. 공장 기본값은 Enable입니다.

2. Multicast Storm Control All의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 모든 포트에서 멀티캐스트 스톰 복구 모드를 활성화하거나 비활성화합니다. 활성화를 지정하고 이더넷 포트의 멀티캐스트 트래픽이 구성된 임계값을 초과하면 스위치는 멀티캐스트 트래픽을 차단(폐기)합니다. 공장 기본값은 Disable입니다.

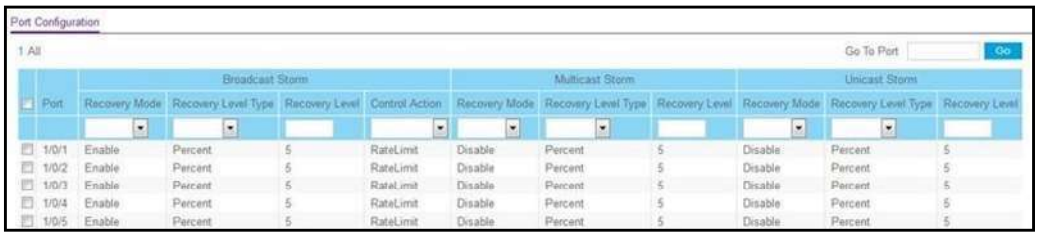
3. Unknown Unicast Storm Control All의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 모든 포트에서 유니캐스트 스톰 복구 모드를 활성화하거나 비활성화합니다. 활성화를 지정하고 이더넷 포트의 유니캐스트 트래픽이 구성된 임계값을 초과하면 스위치는 유니캐스트 트래픽을 차단(폐기)합니다. 공장 기본값은 Disable입니다.

폭풍 제어 인터페이스 구성

➢ **폭풍 제어 인터페이스를 구성하려면:**

Security > Traffic Control > Storm Control > Storm Control Interface Configuration.



다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 223. 폭풍 제어 인터페이스 구성

필드	설명
Broadcast Storm Recovery Mode	드롭다운 입력 필드에서 해당 라인을 선택하여 이 옵션을 활성화하거나 비활성화합니다. 브로드캐스트 스톰 복구에 대해 활성화를 지정하고 지정된 이더넷 포트의 브로드캐스트 트래픽이 구성된 임계값을 초과하면 스위치는 브로드캐스트 트래픽을 차단(폐기)합니다. 공장 기본값은 활성화입니다.
Broadcast Storm Recovery Level Type	브로드캐스트 폭풍 복구 수준을 링크 속도의 백분율이나 초당 패킷 수로 지정합니다.
Broadcast Storm Recovery Level	폭풍 제어가 활성화되는 임계값을 지정합니다. 공장 기본값은 pps 유형의 경우 포트 속도의 5%입니다.
Broadcast Storm Control Action	브로드캐스트 스톰 복구 기능의 구성된 임계값이 위반되면 포트를 종료하는 구성 기능을 제공합니다. ShutDown 또는 RateLimit 모드 옵션을 선택합니다. 기본값은 RateLimit입니다.
Multicast Storm Recovery Mode	목록에서 해당 라인을 선택하여 이 옵션을 활성화하거나 비활성화합니다. 멀티캐스트 스톰 복구에 대해 활성화를 지정하고 지정된 이더넷 포트의 멀티캐스트 트래픽이 구성된 임계값을 초과하면 스위치는 멀티캐스트 트래픽을 차단(폐기)합니다. 공장 기본값은 비활성화입니다.
Multicast Storm Recovery Level Type	멀티캐스트 폭풍 복구 수준을 링크 속도의 백분율이나 초당 패킷 수로 지정합니다.
Multicast Storm Recovery Level	폭풍 제어가 활성화되는 임계값을 지정합니다. 공장 기본값은 pps 유형의 경우 포트 속도의 5%입니다.

Unicast Storm Recovery Mode	이 옵션을 활성화하거나 비활성화합니다. 유니캐스트 스톰 복구에 대해 활성화를 지정하고 지정된 이더넷 포트의 유니캐스트 트래픽이 구성된 임계값을 초과하면 스위치는 유니캐스트 트래픽을 차단(폐기)합니다. 공장 기본값은 비활성화입니다.

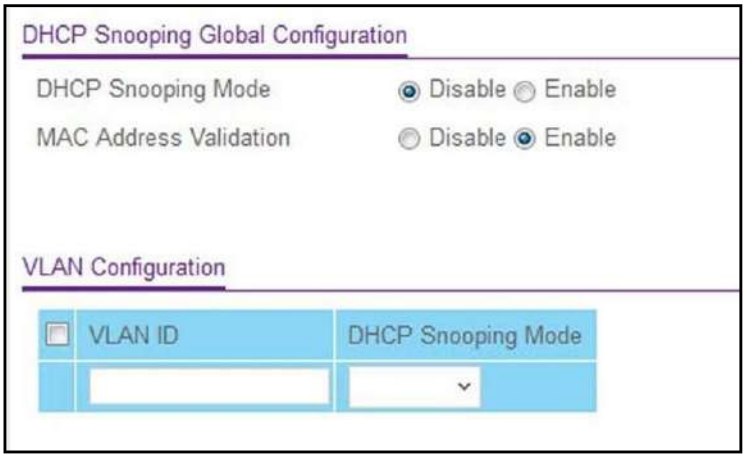
DHCP 스누핑

DHCP 스누핑 전역 및 인터페이스 설정을 구성할 수 있습니다.

DHCP 스누핑 전역 설정 구성

➢ **DHCP 스누핑 전역 설정을 구성하려면:**

Security > Control > DHCP Snooping > Global Configuration.



1. DHCP Snooping Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   공장 기본값은 Disable입니다.

2. MAC Address Validation의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 DHCP 스누핑을 위한 발신자 MAC 주소 검증을 활성화하거나 비활성화합니다. 공장 기본값은 Enable입니다.

3. VLAN ID를 사용하여 DHCP 스누핑 모드를 활성화할 VLAN을 입력합니다.

4. DHCP Snooping Mode를 사용하여 입력된 VLAN에 대한 DHCP 스누핑 기능을 Enable하거나 Disable합니다.

   공장 기본값은 Disable입니다.

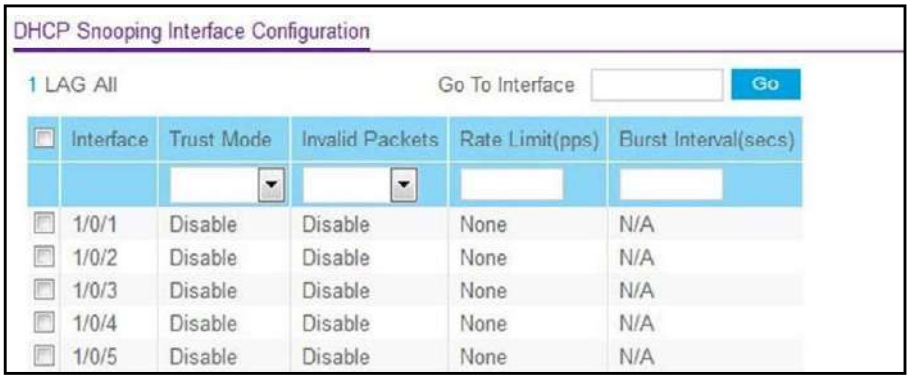
5. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 이러한 변경 사항은 구성 저장을 수행하지 않는 한 전원을 껐다 켜도 유지되지 않습니다.

DHCP 스누핑 인터페이스 구성

➢ **DHCP 스누핑 인터페이스를 구성하려면:**

Security > Control > DHCP Snooping > Interface Configuration.



1. Interface check box을 사용하여 인터페이스를 선택합니다.
2. Trust Mode가 활성화된 경우 DHCP 스누핑 애플리케이션은 해당 포트를 신뢰할 수 있는 것으로 간주합니다.

   공장 기본값은 Disable입니다.

3. Invalid Packets이 활성화된 경우 DHCP 스누핑 애플리케이션은 이 인터페이스에 잘못된 패킷을 기록합니다.

   공장 기본값은 Disable입니다.

4. Rate Limit(pps)을 사용하여 DHCP 스누핑 목적에 대한 비율 제한 값을 지정합니다.

   DHCP 패킷의 수신 속도가 연속 버스트 간격(초) 동안 이 값을 초과하면 포트가 종료됩니다. 이 값이 N/A이면 버스트 간격은 의미가 없으므로 비활성화됩니다. 기본값은 해당 없음입니다. N/A를 의미하는 –1 값으로 설정할 수 있습니다. 속도 제한의 범위는 0~300입니다.

5. Burst Interval(secs)을 사용하여 이 인터페이스의 속도 제한 목적을 위한 버스트 간격 값을 지정합니다.

   속도 제한이 N/A인 경우 버스트 간격은 의미가 없으며 N/A입니다. 기본값은 해당 없음입니다. N/A를 의미하는 –1로 설정할 수 있습니다. 버스트 간격의 범위는

1~15입니다.

DHCP 스누핑 바인딩 구성

➢ **스누핑 바인딩을 구성하려면:**

Security > Control > DHCP Snooping > Binding Configuration.

1. 정적 바인딩을 구성하려면 다음을 지정합니다.
   a. Interface check box을 사용하여 인터페이스를 선택합니다.
   b. MAC Address를 사용하여 추가할 바인딩 항목의 MAC 주소를 지정합니다.

      이는 바인딩 데이터베이스의 키입니다.

   c. VLAN ID를 사용하여 바인딩 규칙 목록에서 VLAN을 선택합니다.

      VLAN ID의 범위는 1~4093입니다.
   d. IP Address를 사용하여 바인딩 규칙에 유효한 IP 주소를 지정합니다.
   e. Add 버튼을 클릭합니다.

      DHCP 스누핑 바인딩 항목이 데이터베이스에 추가됩니다.

   f. 데이터베이스에서 선택한 정적 항목을 삭제하려면 Delete 버튼을 클릭합니다.
2. 동적 바인딩을 구성하려면 다음을 지정합니다.
   a. Interface check box을 사용하여 인터페이스를 선택합니다.
   b. MAC Address를 사용하여 바인딩 데이터베이스의 바인딩에 대한 MAC 주소를 표시합니다.
   c. VLAN ID를 사용하여 바인딩 데이터베이스의 바인딩 항목에 대한 VLAN을 표시합니다. VLAN ID의 범위는 1~4093입니다.
   d. IP Address. 바인딩 데이터베이스의 바인딩 항목에 대한 IP 주소를 표시합니다.

e. Lease Time. 동적 항목의 남은 임대 시간입니다.

f. 모든 DHCP 스누핑 바인딩 항목을 삭제하려면 Clear 버튼을 클릭하세요.

스누핑 영구 설정 구성

➢ **스누핑 영구 설정을 구성하려면:**

Security > Control > DHCP Snooping > Persistent Configuration.

1. Store에 대해 Local 또는 Remote 라디오 버튼을 선택합니다.

   로컬을 선택하면 Remote 필드 Remote File Name 및 Remote IP Address가 Disable됩니다.

2. Remote을 선택한 경우 다음을 수행합니다.

   a. Remote IP Addres 필드에 스누핑 데이터베이스가 저장된 원격 IP 주소를 입력하십시오.

   b. Remote File Name 필드에 데이터베이스를 저장할 원격 파일 이름을 입력합니다.

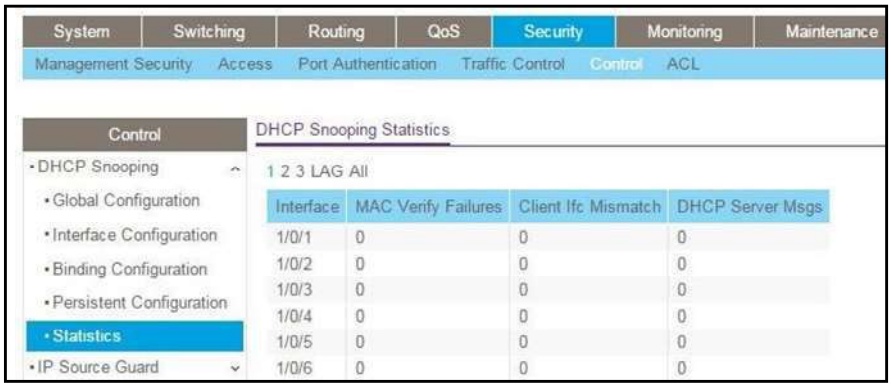
3. Write Delay 필드에 데이터베이스를 로컬 또는 원격에 쓰기 위한 최대 쓰기 시간(secs)을 입력합니다.

   범위는 15~86400입니다.

DHCP 스누핑 통계 보기

➢ **DHCP 스누핑 통계를 보려면:**

Security > Control > DHCP Snooping > Statistics.



모든 인터페이스 통계를 지우려면 Clear 버튼을 클릭합니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

다음 표에는 DHCP 스누핑 통계가 설명되어 있습니다.

Table 224. DHCP 스누핑 통계

필드	설명
Interface	통계를 표시할 신뢰할 수 없고 스누핑이 활성화된 인터페이스입니다.
MAC Verify Failures	일치하는 DHCP 스누핑 바인딩 항목이 없기 때문에 DHCP 스누핑에 의해 삭제된 패킷 수입니다.
Client Ifc Mismatch	소스 MAC 주소 및 클라이언트 HW 주소 확인을 기반으로 삭제되는 DHCP 메시지 수입니다.
DHCP Server Msgs	신뢰할 수 없는 포트에서 삭제된 서버 메시지 수입니다.

IP 소스 가드 인터페이스 구성

각 인터페이스에서 IP 소스 가드(IPSG)를 구성할 수 있습니다. IPSG는 소스 ID를 기반으로 IP 패킷을 필터링하는 보안 기능입니다. 이 기능은 IP 주소 스푸핑을 사용하여 네트워크를 손상시키거나 압도하는 공격으로부터 네트워크를 보호하는 데 도움이 됩니다. 소스 ID는 소스 IP 주소이거나 소스 IP 주소와 소스 MAC 주소 쌍일 수 있습니다. DHCP 스누핑 바인딩 데이터베이스는 데이터베이스의 IPSG 항목과 함께 인증된 소스 ID를 식별합니다. DHCP 스누핑이 비활성화되어 있거나 DHCP 스누핑이 활성화되어 있지만 포트를 신뢰할 수 있는 포트에서 IPSG를 활성화하면 관리자가 구성한 IPSG 항목에 따라 해당 포트에서 수신된 모든 IP 트래픽이 삭제됩니다. 또한 IPSG는 포트 MAC 잠금이라고도 하는 포트 보안과 상호 작용하여 수신된 패킷에 소스 MAC 주소를 적용합니다. 포트 보안은 레이어 2 전달 데이터베이스(MAC 주소 테이블)에서 학습하는 소스 MAC 주소를 제어합니다. 이전에

학습되지 않은 소스 MAC 주소로 프레임이 수신되면 포트 보안은 IPSG 기능을 쿼리하여 MAC 주소가 유효한 바인딩에 속하는지 확인합니다.

➢ **IP 소스 가드 인터페이스 설정을 구성하려면:**

Security > Control > IP Source Guard > Interface Configuration.

1. Interface check box을 사용하여 인터페이스를 선택합니다.
2. IPSG Mode 목록에서 Disable 또는 Enable를 선택합니다.

   인터페이스에서 IPSG의 관리 모드를 설정합니다. IPSG 모드가 활성화되면 이 인터페이스의 보낸 사람 IP 주소가 DHCP 스누핑 바인딩 데이터베이스에 대해 검증됩니다. IPSG가 활성화된 경우 보낸 사람 IP 주소가 DHCP 스누핑 바인딩 데이터베이스에 없으면 패킷이 전달되지 않습니다. 공장 기본값은 Disable입니다.

3. IPSG Port Security목록에서 비활성화 또는 활성화를 선택합니다.

   선택한 인터페이스에서 IPSG 포트 보안의 관리 모드를 활성화하거나 비활성화합니다. 이 기능이 활성화되면 보낸 사람 MAC 주소가 전달 데이터베이스(FDB) 테이블이나 DHCP 스누핑 바인딩 데이터베이스에 없으면 패킷이 전달되지 않습니다. MAC 주소를 기반으로 필터링을 시행하려면 기타 필수 구성은 다음과 같습니다.

   - 전역적으로 포트 보안을 활성화합니다.
   - 인터페이스 수준에서 포트 보안을 활성화합니다.

   IPSG가 비활성화된 경우 IPSG 포트 보안을 활성화할 수 없습니다. 공장 기본값은 Disable입니다. 또한 IPv6SG가 활성화된 동안에는 IPv6SG 포트 보안을 끌 수 없습니다.

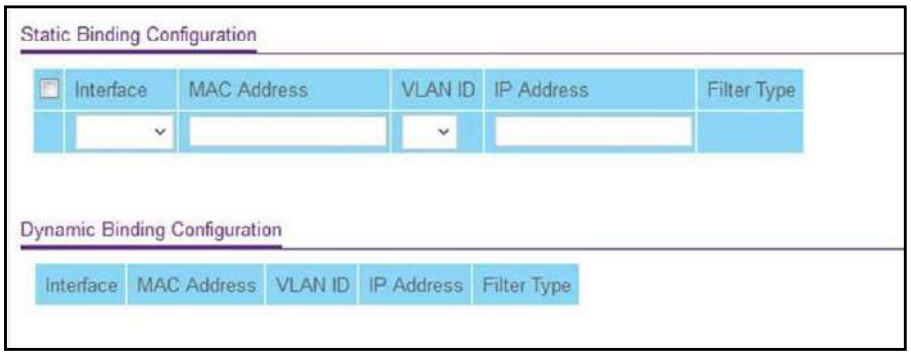
4. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

IP 소스 가드 바인딩 설정 구성

➢ **IP 소스 가드 정적 바인딩 설정을 구성하려면:**

Security > Control > IP Source Guard > Binding Configuration.



1. Interface check box을 사용하여 인터페이스를 선택합니다.
2. MAC Address 필드에 바인딩을 위한 MAC 주소를 입력합니다.
3. VLAN ID 목록에서 바인딩 규칙에 대한 VLAN을 선택합니다.
4. IP Address 필드에서 바인딩 규칙에 대한 유효한 IP 주소를 지정합니다.
5. Add 버튼을 클릭합니다.

   IPSG 정적 바인딩 항목이 데이터베이스에 추가됩니다.
6. 데이터베이스에서 선택한 정적 항목을 삭제하려면 Delete 버튼을 클릭합니다.

모든 동적 바인딩 항목을 지우려면 Clear 버튼을 클릭하세요.

다음 표에서는 표시되는 구성할 수 없는 IP 소스 가드 동적 바인딩 구성 정보에 대해 설명합니다.

Table 225. IP 소스 가드 동적 바인딩 구성

필드	설명
Interface	IPSG 데이터베이스에 바인딩을 추가할 인터페이스입니다.
MAC Address	바인딩 항목의 MAC 주소입니다.
VLAN ID	바인딩 항목의 VLAN입니다.
IP Address	바인딩 항목에 대한 유효한 IP 주소를 표시합니다.
Filter Type	인터페이스에 사용되는 필터 유형입니다. 하나는 소스 IP 주소 필터 유형이고, 다른 하나는 소스 IP 주소 및 MAC 주소 필터 유형입니다.

동적 ARP Inspection 구성

➢ **동적 ARP Inspection (DAI)를 구성하려면:**

Security > Control > Dynamic ARP Inspection > DAI Configuration.

1. Validate Source MAC의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 스위치에 대한 DAI 소스 MAC 검증 모드를 지정합니다. 활성화를 선택하면 ARP 패킷에 대한 보낸 사람 MAC 검증이 활성화됩니다. 공장 기본값은 Disable입니다.

2. Validate Destination MAC의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 스위치에 대한 DAI 대상 MAC 검증 모드를 지정합니다. 활성화를 선택하면 ARP 응답 패킷에 대한 대상 MAC 검증이 활성화됩니다. 공장 기본값은 Disable입니다.

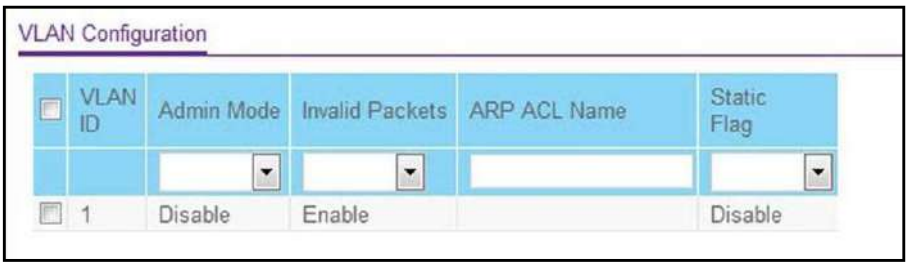
3. Validate IP의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   이는 스위치에 대한 DAI IP 검증 모드를 지정합니다. 활성화를 선택하면 ARP 패킷에 대한 IP 주소 유효성 검사가 활성화됩니다. 공장 기본값은 Disable입니다.

DAI VLAN 구성

➢ **DAI VLAN을 구성하려면:**

Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration.



1. VLAN ID check box을 사용하여 DAI 지원 VLAN을 선택합니다.
2. Admin Mode 목록에서 Enable 또는 Disable를 선택합니다.

   이는 이 VLAN에서 동적 ARP 검사가 활성화되어 있는지 여부를 나타냅니다. 활성화로 설정되면 동적 ARP 검사가 활성화됩니다. 비활성화로 설정되면 동적 ARP 검사가

비활성화됩니다. 기본값은 Disable입니다.

3. Invalid Packets을 사용하여 이 VLAN에서 동적 ARP 검사 로깅이 활성화되었는지 여부를 나타냅니다.

   활성화로 설정하면 유효하지 않은 ARP 패킷 정보가 기록됩니다. 비활성화로 설정된 경우 동적 ARP 검사 로깅이 비활성화됩니다. 기본값은 Enable입니다.

4. ARP ACL Name을 사용하여 ARP 액세스 목록의 이름을 지정합니다.

   규칙이 포함된 이 ARP ACL을 ARP 패킷 검증을 위한 필터로 사용하도록 VLAN을 구성할 수 있습니다. 이름에는 최대 31자의 영숫자가 포함될 수 있습니다. N/A를 지정하면 ARP ACL 이름이 삭제됩니다.

5. ARP ACL 규칙이 일치하지 않는 경우 Static Flag를 사용하여 DHCP 스누핑 데이터베이스를 사용하여 ARP 패킷을 검증해야 하는지 여부를 결정합니다.

   플래그가 활성화되면 ARP 패킷은 ARP ACL 규칙에 의해서만 검증됩니다. 플래그가 비활성화된 경우 DHCP 스누핑 항목을 사용하여 ARP 패킷을 추가로 검증해야 합니다. 공장 기본값은 Disable입니다.

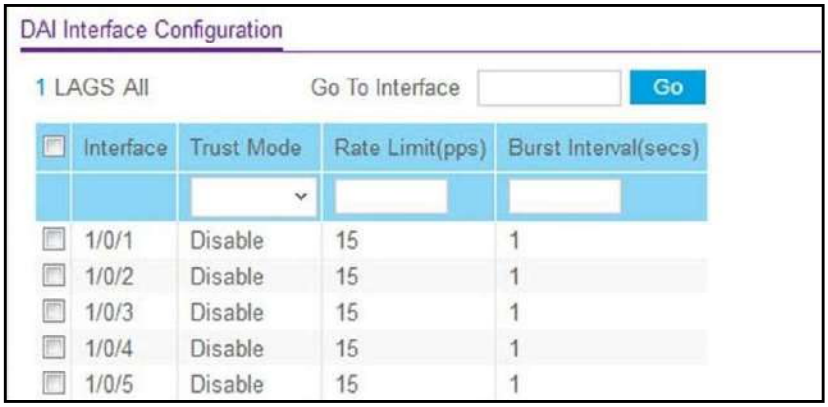
6. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

DAI 인터페이스 구성

➢ **DAI 인터페이스를 구성하려면:**

Security > Control > Dynamic ARP Inspection > DAI Interface Configuration.



1. Interface check box을 사용하여 물리적 인터페이스를 선택합니다.
2. Trust Mode를 사용하여 동적 ARP 검사 목적으로 인터페이스를 신뢰할 수 있는지 여부를 나타냅니다.

   활성화로 설정되면 해당 인터페이스는 신뢰할 수 있습니다. 이 인터페이스로 들어오는 ARP 패킷은 확인 없이 전달됩니다. 비활성화로 설정된 경우 인터페이스를 신뢰할 수 없습니다. 이 인터페이스로 들어오는 ARP 패킷은 ARP 검사를 받습니다. 공장 기본값은 Disable입니다.
3. Rate Limit(pps)을 사용하여 동적 ARP 검사 목적에 대한 속도 제한 값을 지정합니다.

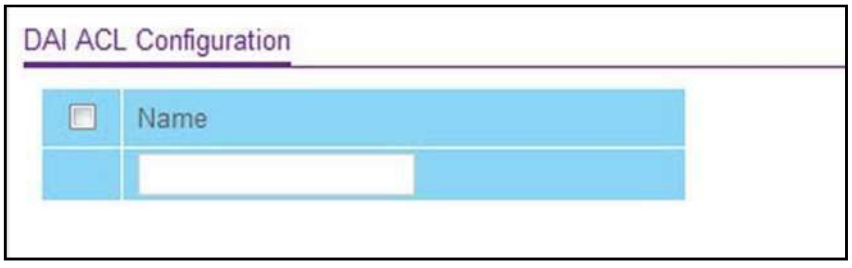
   ARP 패킷의 수신 속도가 연속 버스트 간격(초) 동안 이 값을 초과하면 ARP 패킷이 삭제됩니다. 이 값이 N/A이면 제한이 없습니다. 그만큼

   값은 N/A를 의미하는 –1로 설정될 수 있습니다. 범위는 0~300입니다. 공장 기본값은 15pps(초당 패킷 수)입니다.
4. Burst Interval(secs)을 사용하여 이 인터페이스의 속도 제한 목적을 위한 버스트 간격 값을 지정합니다. 속도 제한이 None이면 버스트 간격은 의미가 없으며 N/A로 표시됩니다. 공장 기본값은 1초입니다.

DAI ACL 구성

➢ **DAI ACL을 구성하려면:**

Security > Control > Dynamic ARP Inspection > DAI ACL Configuration.



1. Name을 사용하여 DAI용 ARP ACL을 생성합니다.
2. Add 버튼을 클릭합니다

   DAI ACL이 스위치 구성에 추가됩니다.

3. 스위치 구성에서 현재 선택된 DAI ACL을 제거하려면 Delete 버튼을 클릭합니다.

DAI ACL 규칙 구성

➢ **DAI ACL 규칙을 구성하려면:**

Security > Control > Dynamic ARP Inspection > DAI ACL Rule Configuration.

1. ACL Name 필드에서 DAI ARP ACL을 선택합니다.
2. Add 버튼을 클릭합니다.

   선택한 ACL에 규칙이 추가됩니다.
3. 선택한 ACL에서 현재 선택한 규칙을 제거하려면 삭제 버튼을 클릭합니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

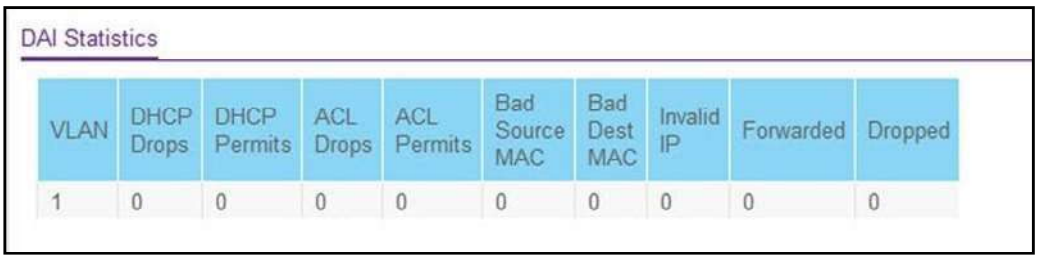
Table 227. DAI ACL 규칙 구성

필드	설명
Source IP Address	이는 DAI ARP ACL에 대한 발신자 IP 주소 일치 값을 나타냅니다.
Source MAC Address	DAI ARP ACL에 대한 발신자 MAC 주소 일치 값을 나타냅니다.

DAI 통계 보기

➢ **DAI 통계를 보려면:**

Security > Control > Dynamic ARP Inspection > DAI Statistics.



DAI 통계를 지우려면 Clear 버튼을 클릭하세요.

스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 228. DAI 통계

필드	설명
VLAN	통계가 표시될 활성화된 VLAN ID입니다.
DHCP Drops	일치하는 DHCP 스누핑 바인딩 항목이 없기 때문에 DAI가 삭제한 ARP 패킷 수입니다.
DHCP Permits	일치하는 DHCP 스누핑 바인딩 항목이 발견되어 DAI가 전달한 ARP 패킷 수입니다.
ACL Drops	이 VLAN에 대해 일치하는 ARP ACL 규칙이 없고 이 VLAN에 정적 플래그가 설정되어 있기 때문에 DAI에서 삭제한 ARP 패킷 수입니다.
ACL Permits	이 VLAN에 대해 일치하는 ARP ACL 규칙이 발견되었기 때문에 DAI에서 허용한 ARP 패킷 수입니다.
Bad Source MAC	ARP 패킷의 보낸 사람 MAC 주소가 이더넷 헤더의 소스 MAC 주소와 일치하지 않아 DAI가 삭제한 ARP 패킷 수입니다.
Bad Dest MAC	ARP 응답 패킷의 대상 MAC 주소가 이더넷 헤더의 대상 MAC 주소와 일치하지 않아 DAI가 삭제한 ARP 패킷 수입니다.
Invalid IP	ARP 패킷의 보낸 사람 IP 주소 또는 ARP 응답 패킷의 대상 IP 주소가 잘못되어 DAI에서 삭제한 ARP 패킷 수입니다. 잘못된 주소에는 0.0.0.0, 255.255.255.255, IP 멀티캐스트 주소, 클래스 E 주소(240.0.0.0/4), 루프백 주소(127.0.0.0/8)가 포함됩니다.
Forwarded	DAI가 전달한 유효한 ARP 패킷 수입니다.
Dropped	DAI가 삭제한 잘못된 ARP 패킷 수입니다.
Unicast Storm Recovery Level Type	유니캐스트 폭풍 복구 수준을 링크 속도의 백분율 또는 초당 패킷 수로 지정합니다.

Unicast Storm Recovery Level	폭풍 제어가 활성화되는 임계값을 지정합니다. 공장 기본값은 pps 유형의 경우 포트 속도의 5%입니다.

액세스 제어 목록 구성

ACL(액세스 제어 목록)은 승인된 사용자만 특정 리소스에 액세스할 수 있도록 보장하는 동시에 네트워크 리소스에 접근하려는 부당한 시도를 차단합니다. ACL은 트래픽 흐름 제어를 제공하고, 라우팅 업데이트 내용을 제한하고, 전달 또는 차단할 트래픽 유형을 결정하고, 무엇보다도 네트워크에 보안을 제공하는 데 사용됩니다. ProSafe 매니지드 스위치의 소프트웨어는 IPv4, IPv6 및 MAC ACL을 지원합니다.

먼저 IPv4 기반, IPv6 기반 또는 MAC 기반 ACL ID를 생성합니다. 그런 다음 규칙을 생성하고 이를 고유한 ACL ID에 할당합니다. 다음으로 프로토콜, 소스, 대상 IP 및 MAC 주소와 기타 패킷 일치 기준을 식별할 수 있는 규칙을 정의합니다. 마지막으로 ID 번호를 사용하여 ACL을 포트 또는 LAG에 할당합니다.

기본 MAC ACL 구성

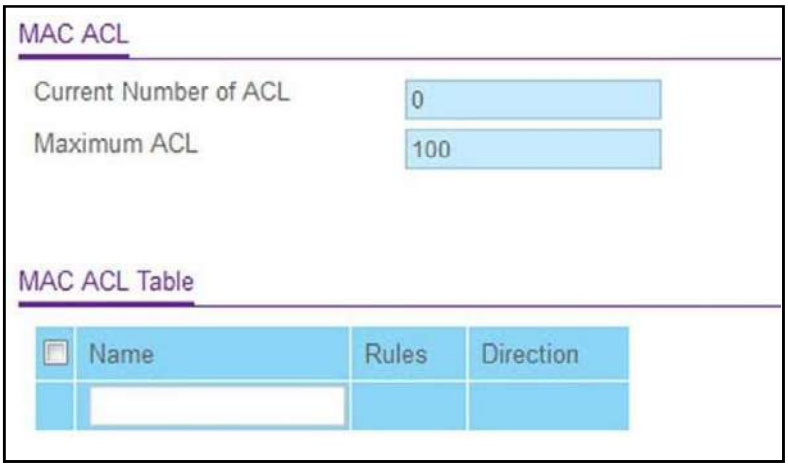
MAC ACL은 패킷과 순차적으로 일치하는 규칙 세트로 구성됩니다. 패킷이 규칙의 일치 기준을 충족하면 지정된 규칙 작업(허용/거부)이 수행되고 추가 규칙의 일치 여부는 확인되지 않습니다. MAC ACL 규칙은 MAC ACL 규칙 구성 화면을 사용하여 지정/생성됩니다.

MAC ACL을 정의하고 이를 스위치에 적용하는 데는 여러 단계가 포함됩니다.

1. ACL Name을 생성합니다.
2. ACL에 대한 규칙을 생성합니다.
3. 이름별로 ACL을 포트에 할당합니다.
4. 선택적으로 MAC 바인딩 테이블 화면에서 MAC ACL 바인딩 보기 또는 삭제를 사용하여 구성을 봅니다.

➢ **MAC ACL을 구성하려면:**

Security > ACL > Basic > MAC ACL.



MAC ACL 화면에는 현재 스위치에 구성된 ACL 수와 구성할 수 있는 최대 ACL 수가 표시됩니다. 현재 숫자는 구성된 IPv4 및 IPv6 ACL 수에 구성된 MACACL 수를 더한 것과 같습니다.

1. Name 필드에 MAC ACL의 이름을 지정합니다.

   이름 문자열에는 알파벳, 숫자, 하이픈, 밑줄 또는 공백 문자만 포함될 수 있습니다. 이름은 영문자로 시작해야 합니다.

   구성된 각 ACL에는 다음 정보가 표시됩니다.

   - **Rules**. MAC ACL에 대해 현재 구성된 규칙 수입니다.
   - **Direction**. MAC ACL의 영향을 받는 패킷 트래픽 방향(인바운드 또는 공백일 수 있음)

2. Add 버튼을 클릭합니다.

   MAC ACL이 스위치 구성에 추가됩니다.

3. MAC ACL의 이름을 변경하려면 Name 필드에서 이름을 업데이트한 다음 Apply 버튼을 클릭합니다.
4. 선택한 MAC ACL을 삭제하려면 Delete 버튼을 클릭합니다.

MAC ACL 규칙 구성

MAC 기반 ACL에 대한 규칙을 정의할 수 있습니다. 액세스 목록 정의에는 기준과 일치하는 트래픽을 정상적으로 전달할지 아니면 삭제할지를 지정하는 규칙이 포함되어 있습니다.
기본 모든 거부 규칙은 모든 목록의 마지막 규칙입니다.

➢ **MAC ACL 규칙을 구성하려면:**

Security > ACL> Basic > MAC Rules.

1. ID를 이용하여 1~1023 범위의 정수를 입력하여 규칙을 식별합니다.
2. Action을 사용하여 패킷이 규칙 기준과 일치하는 경우 수행할 작업을 지정합니다.

   선택 사항은 Permit 또는 Deny입니다.
3. Assign Queue ID을 사용하여 이 ACL 규칙과 일치하는 모든 패킷을 처리하는 데 사용되는 하드웨어 송신 대기열 식별자를 지정합니다.

   유효한 대기열 ID 범위는 0~7입니다.
4. Mirror Interface는 장치에 의해 정상적으로 전달되는 것 외에도 일치하는 트래픽 스트림이 복사되는 특정 송신 인터페이스를 지정합니다.

   ACL 규칙에 대해 리디렉션 인터페이스가 이미 구성된 경우 이 필드를 설정할 수 없습니다. 이 필드는 허용 작업에 대해 표시됩니다.
5. Redirect Interface를 사용하여 일치하는 트래픽 스트림이 강제로 적용되는 특정 송신 인터페이스를 지정하고 장치에서 일반적으로 수행되는 전달 결정을 우회합니다.

   ACL 규칙에 대해 미러 인터페이스가 이미 구성된 경우 이 필드를 설정할 수 없습니다.
6. 모든 레이어 2 MAC 패킷과 일치하는 표시를 지정하려면 Match Every를 사용합니다.

   유효한 값은 다음과 같습니다.

   - **True**. 모든 패킷이 선택한 ACL 규칙과 일치하는 것으로 간주됨을 나타냅니다.
   - **False**. 모든 패킷이 선택한 ACL 규칙과 일치할 필요가 없음을 나타냅니다.
7. CoS를 사용하여 이더넷 프레임과 비교할 802.1p 사용자 우선 순위를 지정합니다.

   유효한 값 범위는 0~7입니다.
8. Destination MAC를 사용하여 이더넷 프레임과 비교할 대상 MAC 주소를 지정합니다. 유효한 형식은 xx:xx:xx:xx:xx:xx입니다.

   BPDU 키워드는 대상 MAC 주소 01:80:C2:xx:xx:xx를 사용하여 지정할 수 있습니다.

9. Destination MAC Mask를 사용하여 이더넷 프레임과 비교할 대상 MAC의 비트를 지정하는 대상 MAC 주소 마스크를 지정합니다.

   유효한 형식은 xx:xx:xx:xx:xx:xx입니다. BPDU 키워드는 대상 MAC 마스크 00:00:00:ff:ff:ff를 사용하여 지정할 수 있습니다.

10. EtherType Key를 사용하여 이더넷 프레임과 비교할 EtherType 값을 지정합니다.

    유효한 값은 다음과 같습니다.

    - Appletalk
    - ARP
    - IBM SNA
    - IPv4
    - IPv6
    - IPX
    - MPLS multicast
    - MPLS unicast
    - NetBIOS
    - Novell
    - PPPoE
    - Reverse ARP
    - User Value

11. EtherType User Value을 사용하여 이더넷 프레임과 비교하기 위해 사용자 값을 EtherType 키로 선택할 때 사용할 사용자 정의 사용자 정의 EtherType 값을 지정합니다.

    유효한 값 범위는 0x0600~0xFFFF입니다.

12. Source MAC을 사용하여 이더넷 프레임과 비교할 소스 MAC 주소를 지정합니다.

    유효한 형식은 xx:xx:xx:xx:xx:xx입니다.

13. Source MAC Mask를 사용하여 이더넷 프레임과 비교할 소스 MAC의 비트를 지정하는 소스 MAC 주소 마스크를 지정합니다.

    유효한 형식은 xx:xx:xx:xx:xx:xx입니다.

14. VLAN을 사용하여 이더넷 프레임과 비교할 VLAN ID를 지정합니다.

    유효한 값 범위는 1~4095입니다. VLAN 범위 또는 VLAN을 구성할 수 있습니다.

15. Logging을 사용하여 로깅을 Enable하거나 Disable합니다.

    활성화로 설정하면 이 ACL 규칙에 대한 로깅이 활성화됩니다(장치의 리소스 가용성에

따라 다름). 액세스 목록 트랩 플래그도 활성화된 경우 현재 보고 간격 동안 이 규칙이 적중된 횟수를 나타내는 주기적 트랩이 생성됩니다. 전체 시스템에 대해 고정된 5분 보고 간격이 사용됩니다. 현재 간격 동안 ACL 규칙 적중 횟수가 0이면 트랩이 발행되지 않습니다. 이 필드는 거부 작업에만 지원됩니다.

16. Rate Limit Conform Data Rate를 사용하여 MAC ACL 규칙의 준수 데이터 속도 값을 지정합니다.

    유효한 값은 1~4294967295(Kbps)입니다.

17. Rate Limit Burst Size를 사용하여 MAC ACL 규칙의 버스트 크기를 지정합니다.

    유효한 값은 1~128KB(KB)입니다.

18. Time Range를 사용하여 MAC ACL 규칙과 관련된 시간 범위의 이름을 입력합니다.

    ACL 규칙이 활성인지 비활성인지 규칙 상태가 표시됩니다. 이 필드가 비어 있으면 타이머 일정이 규칙에 할당되지 않은 것입니다.

19. 규칙을 삭제하려면 해당 규칙과 관련된 확인란을 선택하고 Delete 버튼을 클릭합니다.
20. 규칙을 변경하려면 규칙과 관련된 check box을 선택하고 원하는 필드를 변경합니다.
21. Apply 버튼을 클릭합니다

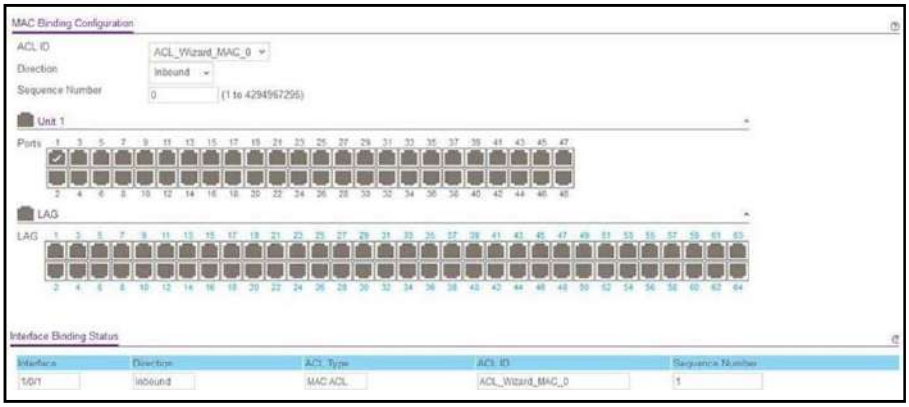
    업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

MAC 바인딩 구성

ACL이 인터페이스에 바인딩되면 정의된 모든 규칙이 선택한 인터페이스에 적용됩니다. MAC 바인딩 구성 화면을 사용하여 MAC ACL 목록을 ACL 우선 순위 및 인터페이스에 할당합니다.

- **MAC 바인딩을 구성하려면:**

  Security > ACL > Basic > MAC Binding Configuration.



1. ACL ID 목록에서 MAC ACL을 선택합니다.

   하나를 선택하여 인터페이스에 바인딩할 수 있습니다.

   ACL에 대한 패킷 필터링 Direction은 인바운드입니다. 이는 MAC ACL 규칙이 포트에 들어오는 트래픽에 적용된다는 의미입니다.

2. 이 인터페이스 및 방향에 이미 할당된 다른 액세스 목록과 관련하여 이 액세스 목록의 순서를 나타내려면 선택적 Sequence Number를 지정합니다.

   숫자가 낮을수록 우선순위가 높다는 것을 나타냅니다. 이 인터페이스 및 방향에 대해 시퀀스 번호가 이미 사용 중인 경우 지정된 액세스 목록은 해당 시퀀스 번호를 사용하여 현재 연결된 액세스 목록을 대체합니다. 시퀀스 번호를 지정하지 않으면 현재 이 인터페이스 및 방향에 사용되는 가장 높은 시퀀스 번호보다 1 큰 시퀀스 번호가 사용됩니다. 유효한 범위는 1~4294967295입니다.

3. Port Selection Table은 ACL 바인딩에 사용할 수 있는 모든 유효한 인터페이스 목록을 제공합니다. 모든 비라우팅 물리적 인터페이스 VLAN 인터페이스와 LAG에 참여하는 인터페이스가 나열됩니다.
   - 선택한 ACL을 포트 또는 LAG에 추가하려면 포트 또는 LAG 번호 바로 아래에 있는 상자를 클릭하여 상자에 X가 나타나도록 하십시오.
   - 포트 또는 LAG에서 선택한 ACL을 제거하려면 포트 또는 LAG 번호 바로 아래에 있는 상자를 클릭하여 선택 항목을 지웁니다. 상자 안의 X는 ACL이 인터페이스에 적용되었음을 나타냅니다.

4. Apply 버튼을 클릭하여 실행 중인 구성에 대한 변경 사항을 저장합니다.

다음 표에는 인터페이스 바인딩 상태에 표시되는 정보가 설명되어 있습니다.

Table 232. 인터페이스 바인딩 상태

필드	설명
Interface	할당된 ACL의 인터페이스입니다.
Direction	ACL에 대해 선택된 패킷 필터링 방향을 표시합니다.
ACL Type	선택한 인터페이스 및 방향에 할당된 ACL 유형입니다.
ACL ID	선택한 인터페이스 및 방향에 할당된 ACL을 식별하는 ACL 번호(IP ACL의 경우) 또는 ACL 이름(MAC ACL의 경우)입니다.
Sequence Number	선택한 인터페이스 및 방향에 할당된 다른 ACL을 기준으로 지정된 ACL의 순서를 나타내는 시퀀스 번호입니다.

MAC 바인딩 테이블에서 MAC ACL 바인딩 보기 또는 삭제

MAC 바인딩 테이블에서 MAC ACL 바인딩을 보거나 삭제할 수 있습니다.

- **To view or delete MAC ACL bindings:**
  Security > ACL > Basic > MAC Binding Table.

MAC ACL-인터페이스 바인딩을 삭제하려면 인터페이스 옆에 있는 확인란을 선택하고 Delete 버튼을 클릭합니다.

다음 표에서는 MAC 바인딩 테이블에 표시되는 정보에 대해 설명합니다.

Table 233. MAC 바인딩 테이블

필드	설명
Interface	할당된 ACL의 인터페이스입니다.
Direction	ACL에 대해 선택된 패킷 필터링 방향입니다.
ACL Type	선택한 인터페이스 및 방향에 할당된 ACL 유형입니다.
ACL ID	선택한 인터페이스 및 방향에 할당된 ACL을 식별하는 ACL 이름입니다.

Sequence Number	선택한 인터페이스 및 방향에 할당된 다른 ACL을 기준으로 지정된 ACL의 순서를 나타내는 시퀀스 번호입니다.

IP ACL 구성

IP 또는 IPv6 ACL은 패킷과 순차적으로 일치하는 규칙 세트로 구성됩니다. 패킷이 규칙의 일치 기준을 충족하면 지정된 규칙 작업(허용/거부)이 수행되고 추가 규칙의 일치 여부는 확인되지 않습니다. IP ACL이 적용되는 인터페이스와 인바운드 또는 아웃바운드 트래픽에 적용되는지 여부를 지정해야 합니다. IP ACL에 대한 규칙은 IPv6 ACL 규칙 구성 화면을 사용하여 지정하거나 생성됩니다.

➢ **IP ACL을 구성하려면:**

Security > ACL > Advanced > IP ACL.

P ACL 화면에는 ACL 테이블의 현재 크기와 ACL 테이블의 최대 크기가 표시됩니다. 현재 크기는 구성된 IPv4 및 IPv6 ACL 수에 구성된 MAC ACL 수를 더한 것과 같습니다. 최대 크기는 100입니다.

Current Number of ACL 필드에는 스위치에 구성된 모든 ACL의 현재 수가 표시됩니다.

Maximum ACL은 하드웨어에 따라 스위치에 구성할 수 있는 최대 IP ACL 수를 표시합니다.

1. IP ACL 필드에서 IP ACL 유형에 따라 ACL ID 또는 IP ACL 이름을 지정합니다.

   IP ACL ID는 다음 범위의 정수입니다.

   - **1–99**: 소스 IP 주소의 트래픽을 허용하거나 거부할 수 있는 IP 기본 ACL을 생성합니다.
   - **100–199**: 소스 IP 주소에서 대상 IP 주소로의 특정 유형의 레이어 3 또는 레이어 4 트래픽을 허용하거나 거부할 수 있는 IP 확장 ACL을 생성합니다. 이 유형의 ACL은

표준 IP ACL보다 더 세밀하고 필터링 기능을 제공합니다.

- **IP ACL Name**: 최대 31자의 영숫자를 포함하는 IPv4 ACL 이름 문자열을 생성합니다. 이름은 영문자로 시작해야 합니다.

구성된 각 ACL에는 다음 정보가 표시됩니다.

- **Rules**. IP ACL에 대해 현재 구성된 규칙 수입니다.
- **Type**. ACL을 기본 IP ACL(1~99의 ID), 확장 IP ACL(100~199의 ID) 또는 명명된 IP ACL로 식별합니다.

2. IP ACL을 삭제하려면 IP ACL ID 필드 옆에 있는 확인란을 선택한 다음 Delete 버튼을 클릭합니다.
3. Add 버튼을 클릭합니다.

   IP ACL이 스위치 구성에 추가됩니다.

4. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

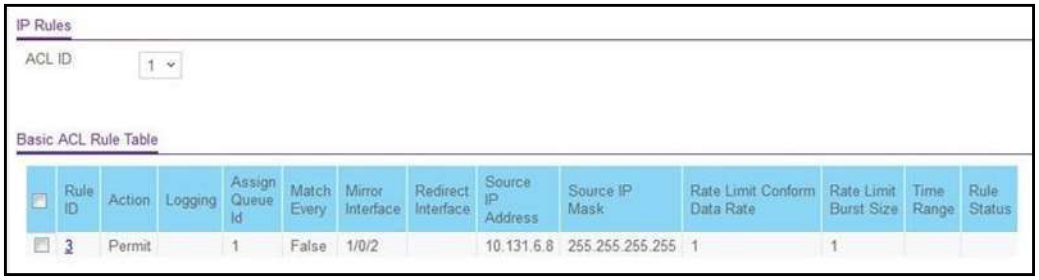
IP ACL에 대한 규칙 구성

생성한 IP ACL(액세스 제어 목록)에 대한 규칙을 표시할 수 있습니다. 이 화면에 표시되는 내용은 규칙 구성 프로세스의 현재 단계에 따라 다릅니다.

Note: ACL 목록 끝에는 암시적인 모든 거부 규칙이 있습니다. 즉, ACL이 패킷에 적용되고 명시적 규칙 중 일치하는 규칙이 없으면 최종 암시적 모든 거부 규칙이 적용되고 패킷이 삭제됩니다.

➢ **IP ACL에 대한 규칙을 구성하려면:**

Security > ACL > Advanced > IP Rules.



1. IP ACL 규칙을 추가하려면 ACL ID를 선택하고 다음 목록에 설명된 필드를 완성한 후 Add 버튼을 클릭합니다.

   (1부터 99까지의 ACL ID만 표시합니다.)

   - **Rule ID.** 규칙을 식별하는 데 사용되는 1~1023 범위의 정수를 입력하세요. IP ACL에는 최대 1023개의 규칙이 있을 수 있습니다.
   - **Action**. 패킷이 규칙 기준과 일치하는 경우 수행할 작업을 지정합니다. 선택 사항은 허용 또는 거부입니다.
   - **Logging**. 활성화로 설정하면 이 ACL 규칙에 대한 로깅이 활성화됩니다(장치의 리소스 가용성에 따라 다름). 액세스 목록 트랩 플래그도 활성화된 경우 현재 보고 간격 동안 이 규칙이 적중된 횟수를 나타내는 주기적 트랩이 생성됩니다. 전체 시스템에 대해 고정된 5분 보고 간격이 사용됩니다. 현재 간격 동안 ACL 규칙 적중 횟수가 0이면 트랩이 발행되지 않습니다. 이 필드는 거부 작업에 대해 표시됩니다.
   - **Assign Queue ID**. 이 IP ACL 규칙과 일치하는 모든 패킷을 처리하는 데 사용되는 하드웨어 송신 대기열 식별자입니다. 유효한 대기열 ID 범위는 0~6입니다. 이 필드는 작업으로 허용을 선택한 경우 표시됩니다.
   - **Match Every.** True 또는 False을 선택합니다. True는 모든 패킷이 선택한 IP ACL 및 규칙과 일치해야 하며 허용되거나 거부됨을 의미합니다. 이 경우 모든 패킷이 규칙과 일치하므로 다른 일치 기준을 구성하는 옵션은 제공되지 않습니다. 규칙에 대한 특정 일치 기준을 구성하려면 규칙을 제거하고 다시 생성하거나 다른 일치 기준이 표시되도록 모든 일치를 False로 다시 구성합니다.
   - **Mirror Interface.** 장치에 의해 정상적으로 전달되는 것 외에도 일치하는 트래픽 스트림이 복사되는 특정 송신 인터페이스입니다. ACL 규칙에 대해 리디렉션 인터페이스가 이미 구성된 경우 이 필드를 설정할 수 없습니다. 이 필드는 허용 작업에 대해 표시됩니다.
   - **Redirect Interface**. 장치에서 일반적으로 수행되는 전달 결정을 우회하여 일치하는 트래픽 스트림이 강제되는 특정 송신 인터페이스입니다. ACL 규칙에 대해 미러 인터페이스가 이미 구성된 경우 이 필드를 설정할 수 없습니다. 이 필드는 허용 작업에 대해 활성화됩니다.
   - **Source IP Address**. 선택한 IP ACL 규칙에 대한 일치 기준으로 패킷의 소스 IP 주소와 비교할 IP 주소를 점으로 구분된 십진수 표기법으로 입력합니다.
   - **Source IP Mask**. 소스 IP 주소 값과 함께 사용할 IP 마스크를 점으로 구분된 십진수 표기법으로 지정합니다.

- **Rate Limit Conform Data Rate**. 속도 제한 준수 데이터 속도 값은 IP ACL 규칙의 준수 데이터 속도를 지정합니다. 유효한 값은 1~4294967295(Kbps)입니다.
- **Rate Limit Burst Size**. 속도 제한 버스트 크기 값은 IP ACL 규칙의 버스트 크기를 지정합니다. 유효한 값은 1~128KB(KB)입니다.
- **Time Range.** IP ACL 규칙과 연결된 시간 범위의 이름입니다.
- **Rule Status**. ACL 규칙이 활성인지 비활성인지 표시합니다. 공백은 규칙에 타이머 일정이 할당되지 않았음을 의미합니다.

2. IP ACL 규칙을 삭제하려면 규칙 확인란을 선택한 후 Delete 버튼을 클릭합니다.
3. IP ACL 규칙을 업데이트하려면 규칙 확인란을 선택하고 원하는 필드를 업데이트한 후 Apply 버튼을 클릭하세요

   기존 IP 규칙의 규칙 ID는 수정할 수 없습니다.
4. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.
5. 기존 IP 확장 ACL 규칙을 수정하려면 Rule ID를 클릭합니다.

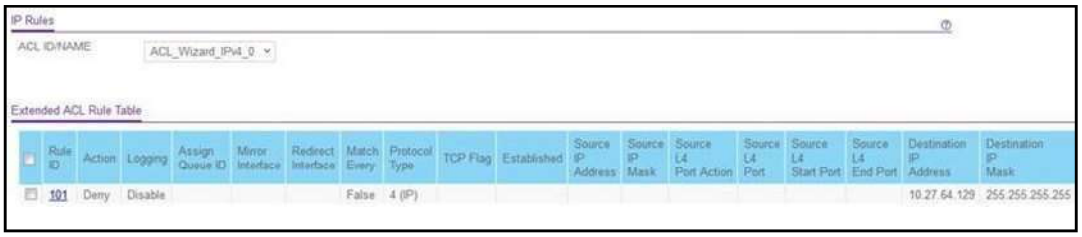
   번호는 확장 ACL 규칙 구성 화면에 대한 하이퍼링크입니다.

확장 IP ACL에 대한 규칙 구성

생성한 IP 액세스 제어 목록에 대한 규칙을 볼 수 있습니다. 이 화면에 표시되는 내용은 규칙 구성 프로세스의 현재 단계에 따라 다릅니다.

Note: ACL 목록 끝에는 암시적인 모든 거부 규칙이 있습니다. 즉, ACL이 패킷에 적용되고 명시적 규칙 중 일치하는 규칙이 없으면 최종 암시적 모든 거부 규칙이 적용되고 패킷이 삭제됩니다.

➢ **To configure rules for an extended IP ACL:**
Security > ACL > Advanced > IP Extended Rules.



1. **ACL ID/Name** - 규칙을 생성하거나 업데이트할 IP ACL을 선택합니다.
2. 규칙을 식별하는 데 사용되는 1~1023 범위의 정수를 입력하여 Rule ID를 구성합니다.

   IP ACL에는 최대 1023개의 규칙이 있을 수 있습니다.
3. Action 목록에서 패킷이 규칙 기준과 일치하는 경우 수행할 동작을 지정합니다.

   The choices are Permit or Deny.
4. Logging을 Enable로 설정합니다.

   이렇게 하면 이 ACL 규칙에 대한 로깅이 활성화됩니다(장치의 리소스 가용성에 따라 다름). 액세스 목록 트랩 플래그도 활성화된 경우 현재 보고 간격 동안 이 규칙이 적중된 횟수를 나타내는 주기적 트랩이 생성됩니다. 전체 시스템에 대해 고정된 5분 보고 간격이 사용됩니다. 현재 간격 동안 ACL 규칙 적중 횟수가 0이면 트랩이 발행되지 않습니다. 이 필드는 거부 작업에 대해 표시됩니다.
5. Assign Queue ID에서 이 IP ACL 규칙과 일치하는 모든 패킷을 처리하는 데 사용되는 하드웨어 송신 대기열 식별자를 지정합니다.

   유효한 대기열 ID 범위는 0~6입니다.
6. Mirror Interface 필드를 사용하여 장치에 의해 정상적으로 전달되는 것 외에도 일치하는 트래픽 스트림이 복사되는 특정 송신 인터페이스를 지정합니다.

   ACL 규칙에 대해 리디렉션 인터페이스가 이미 구성된 경우 이 필드를 설정할 수 없습니다. 이 필드는 허용 작업에 대해 표시됩니다.
7. Redirect Interface 필드를 사용하여 일치하는 트래픽 스트림이 강제로 적용되는 특정 송신 인터페이스를 지정하고 장치에서 일반적으로 수행되는 전달 결정을 우회합니다.

   ACL 규칙에 대해 미러 인터페이스가 이미 구성된 경우 이 필드를 설정할 수 없습니다. 이 필드는 허용 작업에 대해 활성화됩니다.
8. Match Every 목록에서 True 또는 False를 선택합니다.

   True는 모든 패킷이 선택한 IP ACL 및 규칙과 일치해야 하며 허용되거나 거부됨을

의미합니다. 이 경우 모든 패킷이 규칙과 일치하므로 옵션은 다음과 같습니다.

다른 일치 기준 구성은 제공되지 않습니다. 규칙에 대한 특정 일치 기준을 구성하려면 규칙을 제거하고 다시 생성하거나 다른 일치 기준이 표시되도록 모든 일치를 False로 다시 구성합니다.

9. Protocol Type 필드를 사용하여 패킷의 IP 프로토콜이 선택한 IP ACL 규칙에 대한 일치 조건임을 지정합니다.

   가능한 값은 ICMP, IGMP, IP, TCP, UDP, EIGRP, GRE, IPINIP, OSPF 및 PIM입니다.

10. TCP Flag 필드에서 패킷의 TCP 플래그가 선택한 IP ACL 규칙에 대한 일치 조건임을 지정합니다.

    TCP 플래그 값은 URG, ACK, PSH, RST, SYN 및 FIN입니다. 각 TCP 플래그는 별도로 설정할 수 있습니다. 가능한 값은 다음과 같습니다.

    - **Ignore**. 패킷은 이 패킷의 TCP 플래그 설정 여부에 관계없이 이 ACL 규칙과 일치합니다.
    - **Set (+)**. 이 패킷의 TCP 플래그가 설정되면 패킷은 이 ACL 규칙과 일치합니다.
    - **Clear (-)**. 이 패킷의 TCP 플래그가 설정되지 않은 경우 패킷은 이 ACL 규칙과 일치합니다.

11. Established이 지정된 경우 RST 또는 ACK 지정 비트가 TCP 헤더에 설정되면 일치가 발생합니다. 이 필드는 TCP 프로토콜이 선택된 경우에만 활성화됩니다.

12. Src 필드에 점으로 구분된 십진수 표기법을 사용하여 선택한 IP ACL 규칙에 대한 일치 기준으로 패킷의 소스 IP 주소와 비교할 소스 IP 주소를 입력합니다.

    a. IPAddress 옵션을 선택하고 관련 와일드카드 마스크와 함께 IP 주소를 입력하여 이 기준을 적용하십시오. 이 필드를 비워 두면 모든 것을 의미합니다.

    b. Host 옵션을 선택하면 와일드카드 마스크가 0.0.0.0으로 구성됩니다. 이 필드를 비워 두면 모든 것을 의미합니다.

    와일드카드 마스크는 사용되는 비트와 무시되는 비트를 결정합니다. 0.0.0.0의 와일드카드 마스크는 어떤 비트도 중요하지 않음을 나타냅니다. 255.255.255.255의 와일드카드는 모든 비트가 중요함을 나타냅니다.

13. Source L4 Port Action을 사용하여 현재 확장 ACL 규칙의 L4 포트 번호에 대한 관련 일치 조건을 지정합니다.

    - **Equal**. IP ACL 규칙은 레이어 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키와 동일한 경우에만 일치합니다.

- **Less Than**. IP ACL 규칙은 레이어 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키보다 작은 경우 일치합니다.
- **Greater Than**. IP ACL 규칙은 레이어 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키보다 큰 경우 일치합니다.
- **Not Equal**. IP ACL 규칙은 레이어 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키와 동일하지 않은 경우에만 일치합니다.

14. Src L4 Port 및 Src L4 Range 옵션은 프로토콜이 TCP 또는 UDP로 설정된 경우에만 사용할 수 있습니다. 포트 옵션을 선택한 경우 목록에서 포트 키를 선택하거나 포트 번호를 직접 입력하세요.
    - 소스 IP TCP 포트 이름은 bgp, domain, echo, ftp, ftpdata, http, smtp, snmp, Telnet, www, pop2, pop3입니다.
    - 소스 IP UDP 포트 이름은 domain, echo, ntp, rip, snmp, tftp, time, who입니다.

    이러한 각 값은 해당 포트 번호로 변환되며, 이는 포트 범위의 시작과 끝으로 사용됩니다.

    포트 키 목록에서 기타를 선택한 경우에만 자신의 포트 번호를 입력할 수 있습니다. 기타 필드를 비워 두면 모든 것을 의미합니다.

15. Range 옵션을 선택하면 레이어 4 포트 번호가 지정된 포트 범위 내에 있는 경우에만 IP ACL 규칙이 일치합니다.

    시작 포트 및 끝 포트 매개변수는 포트 범위의 일부인 첫 번째 포트와 마지막 포트를 식별합니다. 값의 범위는 0에서 65535까지입니다.

    자신의 포트 번호를 입력하는 기능은 포트 키 목록에서 기타를 선택한 경우에만 사용할 수 있습니다. 시작 포트, 끝 포트 및 그 사이의 모든 포트는 계층 4 포트 범위의 일부입니다. 이 필드를 비워 두면 모든 것을 의미합니다.

    와일드카드 마스크는 사용되는 비트와 무시되는 비트를 결정합니다. 0.0.0.0의 와일드카드 마스크는 어떤 비트도 중요하지 않음을 나타냅니다. 255.255.255.255의 와일드카드는 모든 비트가 중요함을 나타냅니다.

16. Dst 필드에서 점으로 구분된 십진수 표기법과 관련 와일드카드 마스크를 사용하여 대상 IP 주소를 지정합니다.

    이는 선택한 확장 IP ACL 규칙에 대한 일치 기준으로 패킷의 대상 IP 주소와 비교됩니다.

17. IP Address 옵션을 선택하고 관련 와일드카드 마스크와 함께 IP 주소를 입력하여 이 기준을 적용합니다.

이 필드를 비워 두면 모든 것을 의미합니다.

18. Host 옵션을 선택하면 와일드카드 마스크가 0.0.0.0으로 구성됩니다. 이 필드를 비워 두면 모든 것을 의미합니다.
19. Destination IP Mask 필드에서 대상 IP 주소 값과 함께 사용할 IP 마스크를 점으로 구분된 십진수 표기법으로 지정합니다.
20. Dst L4 Port and Dst L4 Range 필드에서 선택한 확장 IP ACL 규칙에 대한 레이어 4 대상 포트 일치 조건을 지정합니다.

    이러한 옵션은 프로토콜이 TCP 또는 UDP로 설정된 경우에만 사용할 수 있습니다.

    포트 키 목록에서 기타를 선택한 경우에만 자신의 포트 번호를 입력할 수 있습니다. 기타 필드를 비워 두면 모든 것을 의미합니다.

    - 대상 IP TCP의 가능한 포트 이름은 bgp, domain, echo, ftp, ftp-data, http, smtp, Telnet, www, pop2, pop3입니다.
    - 대상 IP UDP 가능한 포트 이름은 domain, echo, ntp, rip, snmp, tftp, time, who입니다.

    이러한 각 값은 해당 포트 번호로 변환되며, 이는 포트 범위의 시작과 끝으로 사용됩니다. 이는 선택적 구성입니다.

21. Destination L4 Port Action을 사용하여 현재 확장 ACL 규칙의 L4 포트 번호에 대한 관련 일치 조건을 지정합니다.
    - **Equa**l. IP ACL 규칙은 계층 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키와 동일한 경우에만 일치합니다.
    - **Less Than**. IP ACL 규칙은 레이어 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키보다 작은 경우 일치합니다.
    - **Greater Than**. IP ACL 규칙은 레이어 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키보다 큰 경우 일치합니다.
    - **Not Equal**. IP ACL 규칙은 레이어 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키와 동일하지 않은 경우에만 일치합니다.
22. Range 옵션을 선택하면 레이어 4 포트 번호가 지정된 포트 범위 내에 있는 경우에만 IP ACL 규칙이 일치합니다.

    시작 포트 및 끝 포트 매개변수는 포트 범위의 일부인 첫 번째 포트와 마지막 포트를 식별합니다. 값의 범위는 0에서 65535까지입니다.

자신의 포트 번호를 입력하는 기능은 포트 키 목록에서 기타를 선택한 경우에만 사용할 수 있습니다. 대상 L4 시작 포트, 대상 L4 종료 포트 및 그 사이의 모든 포트는 계층 4 포트 범위의 일부입니다. 이 필드를 비워 두면 모든 것을 의미합니다.

23. **IGMP Type** - IGMP 유형이 지정되면 IP ACL 규칙은 지정된 IGMP 메시지 유형과 일치합니다.

    가능한 값은 0~255 범위에 있습니다. 이 필드가 비어 있으면 임의를 의미합니다.

24. **ICMP Type** and **ICMP Code** - ICMP 유형 및 ICMP 코드 필드는 프로토콜이 ICMP인 경우에만 활성화됩니다. ICMP 유형 및 ICMP 코드 필드를 사용하여 ICMP 패킷에 대한 일치 조건을 지정합니다.
    - ICMP 유형 옵션을 선택하면 IP ACL 규칙이 지정된 ICMP 메시지 유형과 일치합니다. 가능한 유형 번호의 범위는 0~255입니다.
    - ICMP 코드 옵션이 지정된 경우 IP ACL 규칙은 지정된 ICMP 메시지 코드와 일치합니다. 코드에 가능한 값은 0에서 255 사이일 수 있습니다.
    - 이 필드가 비어 있으면 모든 것을 의미합니다.
    - 메시지 옵션을 선택한 경우 선택한 IP ACL 규칙과 일치하는 ICMP 메시지 유형을 선택합니다. 메시지를 지정한다는 것은 ICMP 유형과 ICMP 코드가 모두 지정됨을 의미합니다. ICMP 메시지는 해당 ICMP 유형 및 해당 ICMP 유형 내의 ICMP 코드로 디코딩됩니다. IPv4 ICMP 메시지 유형은 다음과 같습니다: echo, echo-reply, 호스트 리디렉션, 모바일 리디렉션, net-redirect, net-unreachable, 리디렉션, packet-too-big, port-unreachable, source-quench, router-solicitation, router- 광고, 시간 초과, TTL 초과, 도달 불가.

25. **Service Type** - 확장 IP ACL 규칙에 대한 서비스 유형 일치 조건을 선택합니다.

    가능한 값은 IP 헤더의 동일한 서비스 유형 필드에 대한 일치 기준을 지정하는 대체 방법인 IP DSCP, IP 우선 순위 및 IP TOS입니다. 그러나 각각은 다른 사용자 표기법을 사용합니다. 선택한 후 적절한 값을 지정할 수 있습니다.

    - **IP DSCP.** IP DiffServ 코드 포인트(DSCP) 필드를 지정합니다. DSCP는 IP 헤더에 있는 서비스 유형 옥텟의 상위 6비트로 정의됩니다. 이는 선택적 구성입니다. 0~63 사이의 정수를 입력합니다. IP DSC를 선택하려면 목록에서 DSCP 키워드 중 하나를 선택합니다. 숫자 값을 지정하여 값을 선택하려면 기타를 선택하면 DSCP의 숫자 값을 입력할 수 있는 필드가 표시됩니다.
    - **IP Precedence**. 패킷의 IP 우선 순위 필드는 IP 헤더에 있는 서비스 유형 옥텟의

상위 3비트로 정의됩니다. 이는 선택적 구성입니다. 0~7 사이의 정수를 입력하세요.

- **IP TOS**. 패킷의 IP TOS 필드는 IP 헤더에 있는 서비스 유형 옥텟의 8비트 모두로 정의됩니다. TOS 비트 값은 00부터 09까지, aa부터 ff까지의 16진수입니다. ToS 마스크 값은 00부터 FF까지의 16진수입니다. ToS 마스크는 패킷의 IP TOS 필드와 비교하는 데 사용되는 TOS 비트 값의 비트 위치를 나타냅니다. 예를 들어 비트 7과 5가 설정되고 비트 1이 지워진(비트 7이 가장 중요한) IP ToS 값을 확인하려면 TOS 비트 값 0xA0과 TOS 마스크 0xFF를 사용합니다. 이는 선택적 구성입니다.

26. **Rate Limit Conform Data Rate** - IP ACL 규칙에 맞는 데이터 속도를 지정합니다.

    유효한 값은 1~4294967295(Kbps)입니다.

27. **Rate Limit Burst Size** - IP ACL 규칙의 버스트 크기를 지정합니다. 유효한 값은 1~128KB(KB)입니다.
28. **Time Range** - IP 확장 ACL 규칙과 연결된 시간 범위의 이름입니다.

    ACL 규칙이 활성인지 비활성인지 여부가 Rule Status필드에 표시됩니다. 공백은 규칙에 타이머 일정이 할당되지 않았음을 의미합니다.

29. 기존 IP 확장 ACL 규칙을 수정하려면 Rule ID를 클릭합니다.

    이 번호는 확장 ACL 규칙 구성 100-199 화면에 대한 하이퍼링크입니다. IP 확장 규칙 화면에서 Add 버튼을 클릭하세요.

30. 표준 ACL 규칙 구성(1~99)의 경우 IP 규칙 화면에서 Add 버튼을 클릭합니다.
31. IP ACL 규칙을 삭제하려면 해당 규칙의 확인란을 선택한 다음 Delete 버튼을 클릭합니다.

IPv6 ACL 구성

IP 또는 IPv6 ACL은 패킷과 순차적으로 일치하는 규칙 세트로 구성됩니다. 패킷이 규칙의 일치 기준을 충족하면 지정된 규칙 작업(허용/거부)이 수행되고 추가 규칙의 일치 여부는 확인되지 않습니다. 이 화면에서는 IP ACL이 적용되는 인터페이스와 인바운드 또는 아웃바운드 트래픽에 적용되는지 여부를 지정해야 합니다.

➢ **IPv6 ACL을 구성하려면:**

Security > **ACL** > **Advanced** > **IPv6 ACL**.

1. IPv6 ACL을 지정합니다.

   이는 최대 31자의 영숫자 문자만 포함하는 IPv6 ACL 이름 문자열입니다. 이름은 영문자로 시작해야 합니다.

2. Add 버튼을 클릭합니다.

   IPv6 ACL이 스위치 구성에 추가됩니다.

3. 스위치 구성에서 현재 선택된 IPv6 ACL을 제거하려면 삭제 버튼을 클릭합니다.

4. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 234. IPv6 ACL

필드	설명
Current Number of ACL	스위치에 구성된 현재 IP ACL 수입니다.
Maximum ACL	하드웨어에 따라 스위치에 구성할 수 있는 최대 IP ACL 수입니다.
Rules	IP ACL과 연관된 규칙의 수입니다.
Type	유형은 IPv6 ACL입니다.

IPv6 규칙 구성

이 화면을 사용하여 IPv6 액세스 제어 목록 구성 화면을 사용하여 생성된 IPv6 액세스 제어 목록에 대한 규칙을 표시합니다. 기본적으로 IPv6 ACL 규칙에는 특정 값이 적용되지

않습니다.

- **ACL IPv6 규칙을 구성합니다:**

  Security > ACL > Advanced > IPv6 Rules.

  1. Rule ID를 사용하여 규칙을 식별하는 데 사용되는 1~1023 범위의 정수를 입력합니다.

     An IP ACL can have up to 1023 rules.

  2. Action을 사용하여 패킷이 규칙 기준과 일치하는 경우 수행할 작업을 지정합니다. 선택 사항은 Permit 또는 Deny입니다.

  3. Logging을 사용하여 이 ACL 규칙에 대한 로깅을 활성화합니다(장치의 리소스 가용성에 따라 다름).

     액세스 목록 트랩 플래그도 활성화된 경우 현재 보고 간격 동안 이 규칙이 적중된 횟수를 나타내는 주기적 트랩이 생성됩니다. 전체 시스템에 대해 고정된 5분 보고 간격이 사용됩니다. 현재 간격 동안 ACL 규칙 적중 횟수가 0이면 트랩이 발행되지 않습니다. 이 필드는 거부 작업에 대해 표시됩니다.

  4. Assigned Queue ID 할당을 사용하여 이 IPv6 ACL 규칙과 일치하는 모든 패킷을 처리하는 데 사용되는 하드웨어 송신 대기열 식별자를 지정합니다.

     유효한 대기열 ID 범위는 0~7입니다. 이 필드는 허용 작업에 대해 표시됩니다.

  5. Mirror Interface를 사용하여 일치하는 트래픽 스트림이 장치에 의해 정상적으로 전달되는 것 외에 복사되는 특정 송신 인터페이스를 지정합니다.

     ACL 규칙에 대해 리디렉션 인터페이스가 이미 구성된 경우 이 필드를 설정할 수 없습니다. 이 필드는 허용 작업에 대해 표시됩니다.

  6. Redirect Interface를 사용하여 일치하는 트래픽 스트림이 강제로 적용되는 특정 송신 인터페이스를 지정하고 장치에서 일반적으로 수행되는 전달 결정을 우회합니다.

     ACL 규칙에 대해 미러 인터페이스가 이미 구성된 경우 이 필드를 설정할 수 없습니다. 이 필드는 허용 작업에 대해 표시됩니다.

  7. Match Every 필드에서 True 또는 False를 선택합니다.

     True는 모든 패킷이 선택한 IPv6 ACL 및 규칙과 일치해야 하며 허용되거나 거부됨을 의미합니다. 이 경우 모든 패킷이 규칙과 일치하므로 다른 일치 기준을 구성하는 옵션은 제공되지 않습니다. 규칙에 대한 특정 일치 기준을 구성하려면 규칙을 제거하고 다시 생성하거나 다른 일치 기준이 표시되도록 모든 일치를 False로 다시 구성합니다.

  8. IPv6 프로토콜 유형을 구성하는 방법에는 두 가지가 있습니다.

- 프로토콜 키워드 other를 선택한 후 1~255 범위의 정수를 지정합니다. 이 숫자는 IP 프로토콜을 나타냅니다.
- 기존 인터넷 프로토콜(IPv6), 전송 제어 프로토콜(TCP), 사용자 데이터그램 프로토콜(UDP) 및 인터넷 제어 메시지 프로토콜(ICMPv6) 목록에서 프로토콜 이름을 선택합니다.

9. TCP Flag를 사용하여 패킷의 TCP 플래그가 선택한 IPv6 ACL 규칙에 대한 일치 조건임을 지정합니다.

   TCP 플래그 값은 URG, ACK, PSH, RST, SYN, FIN입니다. 각 TCP 플래그는 별도로 설정할 수 있습니다. 가능한 값은 다음과 같습니다.

   - **Ignore**. 패킷은 이 패킷의 TCP 플래그 설정 여부에 관계없이 이 ACL 규칙과 일치합니다.
   - **Set (+)**. 이 패킷의 TCP 플래그가 설정되면 패킷은 이 ACL 규칙과 일치합니다.
   - **Clear (-)**. 이 패킷의 TCP 플래그가 설정되지 않은 경우 패킷은 이 ACL 규칙과 일치합니다.
   - Established이 지정된 경우 RST 또는 ACK 지정 비트가 TCP 헤더에 설정되면 일치가 발생합니다.
   - 다음 필드는 TCP 프로토콜을 선택한 경우에만 활성화됩니다.
     - **Protocol**. IPv6 프로토콜을 구성하는 방법에는 두 가지가 있습니다.

       프로토콜 키워드 other를 선택한 후 1~255 범위의 정수를 지정합니다. 이 숫자는 IP 프로토콜을 나타냅니다.

       인터넷 프로토콜(IPv6), 전송 제어 프로토콜(TCP), 사용자 데이터그램 프로토콜(UDP) 및 인터넷 제어 메시지 프로토콜(ICMPv6)의 기존 목록에서 프로토콜 이름을 선택합니다.

     - **Src**. 선택한 IPv6 ACL 규칙과 일치하도록 소스 IPv6 주소를 지정합니다.

       IPv6 주소 라디오 버튼을 선택한 경우 IPv6 ACL 규칙과 일치하는 접두사 길이로 IPv6 주소를 입력합니다. 이 필드를 비워 두면 모든 것을 의미합니다.

       호스트 라디오 버튼을 선택한 경우 지정된 IPv6 주소와 일치하는 호스트 소스 IPv6 주소를 입력합니다. 이 필드를 비워 두면 모든 것을 의미합니다.

   이 소스 IPv6 주소 인수는 주소가 콜론 사이의 16비트 값을 사용하여 16진수로 지정되는 RFC 2373에 문서화된 형식이어야 합니다.

10. Src L4 Port 옵션은 TCP 또는 UDP 프로토콜에 대해서만 활성화됩니다.
    - 소스 L4 TCP 포트 이름은 bgp, domain, echo, ftp, ftpdata, http, smtp, Telnet, www, pop2, pop3입니다.
    - 소스 L4 UDP 포트 이름은 domain, echo, ntp, rip, snmp, tftp, time, who입니다.

    포트 옵션을 선택한 경우 목록에서 포트 키를 선택하거나 포트 번호를 입력하세요. 포트 키 목록에서 기타를 선택한 경우에만 자신의 포트 번호를 입력할 수 있습니다. 이 필드를 비워 두면 모든 것을 의미합니다.

11. Source L4 Port Action은 현재 확장 규칙의 레이어 4 포트 번호에 대한 관련 일치 조건을 지정합니다.
    - **Equal**. IPv6 ACL 규칙은 레이어 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키와 동일한 경우에만 일치합니다.
    - **Less Than**. IPv6 ACL 규칙은 레이어 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키보다 작은 경우 일치합니다.
    - **Greater Than**. IPv6 ACL 규칙은 레이어 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키보다 큰 경우 일치합니다.
    - **Not Equal**. IPv6 ACL 규칙은 레이어 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키와 동일하지 않은 경우에만 일치합니다.

12. Dst L4 Port Option은 TCP 또는 UDP 프로토콜에 대해서만 활성화됩니다.
    - 대상 L4 TCP 포트 이름은 bgp, domain, echo, ftp, ftpdata, http, smtp, Telnet, www, pop2, pop3입니다.
    - 대상 L4 UDP 포트 이름은 domain, echo, ntp, rip, snmp, tftp, time, who입니다.

    포트 옵션을 선택한 경우 목록에서 포트 키를 선택하거나 포트 번호를 입력하세요. 포트 키 목록에서 기타를 선택한 경우에만 자신의 포트 번호를 입력할 수 있습니다. 이 필드를 비워 두면 모든 것을 의미합니다.

13. Destination L4 Port Action은 현재 확장 ACL 규칙의 레이어 4 포트 번호에 대한 관련 일치 조건을 지정합니다.
    - **Equal**. IPv6 ACL 규칙은 레이어 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키와 동일한 경우에만 일치합니다.
    - **Less Than**. IPv6 ACL 규칙은 레이어 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키보다 작은 경우 일치합니다.

- **Greater Than**. IPv6 ACL 규칙은 레이어 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키보다 큰 경우 일치합니다.
- **Not Equal**. IPv6 ACL 규칙은 레이어 4 소스 포트 번호가 지정된 포트 번호 또는 포트 키와 동일하지 않은 경우에만 일치합니다.

14. **Fragments**. 초기가 아닌 조각(조각 비트 어설션)인 패킷을 일치시키는 규칙입니다.

    이 옵션은 TCP 포트 번호와 같은 L4 정보와 일치하는 규칙에는 유효하지 않습니다. 해당 정보는 초기 패킷에 포함되어 있기 때문입니다.

15. **Routing**. 라우팅 확장 헤더를 포함하는 패킷을 일치시키는 규칙입니다.

16. **ICMPv6 Type**. ICMP 패킷의 일치 조건을 지정합니다.

    유형 라디오 버튼을 선택하면 IPv6 ACL 규칙이 지정된 ICMPv6 메시지 유형과 일치합니다. 가능한 유형 번호의 범위는 0~255입니다. ICMPv6 코드가 지정되면 IP ACL 규칙은 지정된 ICMPv6 메시지 코드와 일치합니다. 가능한 값은 0~255 범위입니다. 이 필드를 비워 두면 임의를 의미합니다.

17. 메시지 라디오 버튼이 선택되면 선택한 IPv6 ACL 규칙과 일치하는 ICMPv6 메시지 유형을 선택합니다.
    메시지를 지정하면 ICMPv6 유형과 ICMPv6 코드가 모두 지정됨을 의미합니다. ICMPv6 메시지는 해당 ICMPv6 유형 내의 ICMPv6 코드와 해당 ICMPv6 유형으로 디코딩됩니다. IPv6 ICMPv6 메시지 유형은 대상 연결 불가, 에코 응답, 에코 요청, 헤더, 홉 제한, mld-query, mld-reduction, mld-report, nd-na, nd-ns, next-header, no-admin입니다. , 경로 없음, 패킷이 너무 큼, 포트에 연결할 수 없음, 라우터 요청, 라우터 광고, 라우터 번호 다시 매기기, 시간 초과 및 연결할 수 없음.

    Note: 다음 필드는 프로토콜이 ICMPv6인 경우에만 활성화됩니다.

18. **Flow Label**. 흐름 레이블은 IPv6 패킷에 고유한 20비트 숫자로, 라우터에서 서비스 품질 처리를 나타내기 위해 최종 스테이션에서 사용됩니다.

    흐름 레이블은 0~1048575 범위 내에서 지정할 수 있습니다.

19. IPv6 DSCP Service를 사용하여 IP DiffServ 코드 포인트(DSCP) 필드를 지정합니다.

    DSCP는 IPv6 헤더에 있는 서비스 유형 옥텟의 상위 6비트로 정의됩니다. 이는 선택적 구성입니다. 0~63 사이의 정수를 입력하세요. IPv6 DSCP를 선택하려면 DSCP 키워드 중 하나를 선택하세요. 숫자 값을 지정하여 값을 선택하려면 기타를 선택하면 DSCP의 숫자

값을 입력할 수 있는 필드가 나타납니다.

20. **Rate Limit Conform Data Rate**. IPv6 ACL 규칙에 맞는 데이터 속도를 지정합니다.

    유효한 값은 1~4294967295(Kbps)입니다.

21. **Rate Limit Burst Size**. IPv6 ACL 규칙의 버스트 크기를 지정합니다.

    유효한 값은 1~128KB(KB)입니다.

22. **Time Range**. IPv6 ACL 규칙과 연결된 시간 범위의 이름입니다.
23. **Rule Status**. ACL 규칙이 활성인지 비활성인지 표시합니다.

    공백은 규칙에 타이머 일정이 할당되지 않았음을 의미합니다.

24. IP 확장 ACL 규칙을 수정하려면 Rule ID를 클릭합니다.

    이 번호는 확장 IPv6 ACL 규칙 구성(100-199) 화면에 대한 하이퍼링크입니다. IP 확장 규칙 화면에서 Add 버튼을 클릭하세요.

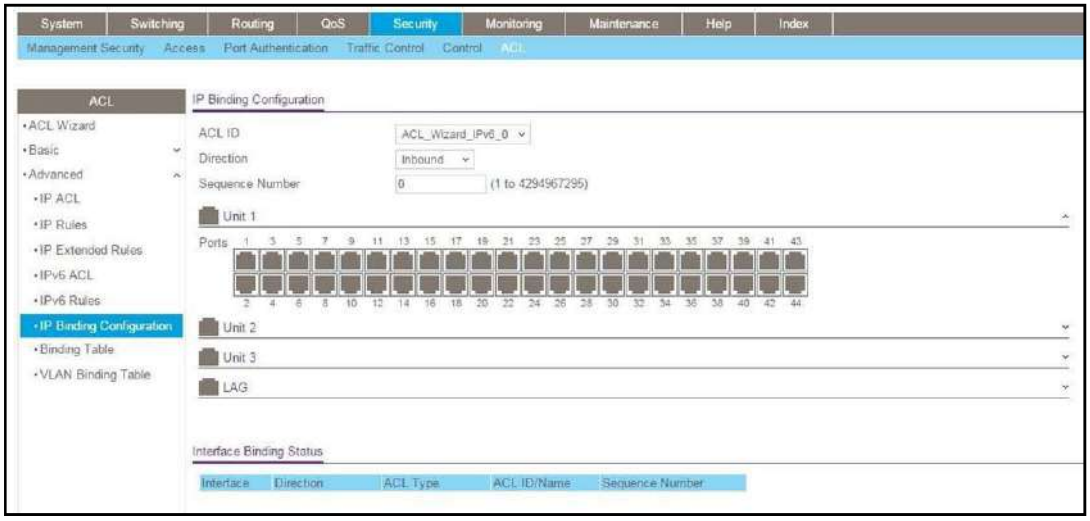
25. 표준 ACL 규칙 구성(1~99)의 경우 IPv6 규칙 화면에서 Add 버튼을 클릭합니다.
26. 규칙을 삭제하려면 해당 확인란을 선택하고 Delete 버튼을 클릭합니다.

IP ACL 인터페이스 바인딩 구성

ACL이 인터페이스에 바인딩되면 정의된 모든 규칙이 선택한 인터페이스에 적용됩니다. ACL 목록을 ACL 우선순위 및 인터페이스에 할당할 수 있습니다.

➢ **IP ACL 인터페이스 바인딩을 구성하려면:**

Security > **ACL** > **Advanced** > **IP Binding Configuration**.



1. ACL ID 메뉴에서 IP ACL을 선택합니다.

Note: 시스템에 새 ACL을 바인딩할 리소스가 없으면 인터페이스에 ACL 바인딩이 실패합니다. IPv4 ACL과 IPv6 ACL은 동시에 인터페이스에 바인딩될 수 없습니다.

2. ACL에 대한 패킷 필터링 Direction을 선택합니다.

   유효한 방향은 인바운드 또는 아웃바운드입니다. ACL의 패킷 필터링 방향은 인바운드입니다. 이는 IP ACL 규칙이 포트로 들어오는 트래픽에 적용된다는 의미입니다.

3. 이 인터페이스 및 방향에 이미 할당된 다른 액세스 목록과 관련하여 이 액세스 목록의 순서를 나타내려면 선택적 Sequence Number를 지정합니다.

   숫자가 낮을수록 우선순위가 높다는 것을 나타냅니다. 이 인터페이스 및 방향에 대해 시퀀스 번호가 이미 사용 중인 경우 지정된 액세스 목록은 해당 시퀀스 번호를 사용하여 현재 연결된 액세스 목록을 대체합니다. 시퀀스 번호를 지정하지 않으면(값이 0임을 의미) 현재 이 인터페이스 및 방향에 사용되는 가장 높은 시퀀스 번호보다 1 큰 시퀀스 번호가 사용됩니다. 유효한 범위는 1~4294967295입니다.

4. Port Selection Table에는 ACL 매핑에 사용할 수 있는 유효한 인터페이스가 모두 나열됩니다.

   모든 비라우팅 물리적 인터페이스와 LAG에 참여하는 인터페이스가 나열됩니다. 적절한 장치 이름을 클릭하여 사용 가능한 포트 또는 LAG를 표시합니다.

   - 선택한 ACL을 포트 또는 LAG에 추가하려면 포트 또는 LAG 번호 바로 아래에 있는

상자를 클릭하여 상자에 X가 나타나도록 하십시오.

- 포트 또는 LAG에서 선택한 ACL을 제거하려면 포트 또는 LAG 번호 바로 아래에 있는 상자를 클릭하여 선택 항목을 지웁니다. 상자 안의 X는 ACL이 인터페이스에 적용되었음을 나타냅니다.

5. Apply 버튼을 클릭하여 실행 중인 구성에 대한 변경 사항을 저장합니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 235. IP 바인딩 구성

필드	설명
Interface	선택한 인터페이스를 표시합니다.
Direction	ACL에 대해 선택한 패킷 필터링 방향을 표시합니다.
ACL Type	선택한 인터페이스 및 방향에 할당된 ACL 유형입니다.
ACL ID/Name	선택한 인터페이스 및 방향에 할당된 ACL을 식별하는 ACL 번호(IP ACL의 경우) 또는 ACL 이름(명명된 IP ACL 및 IPv6 ACL의 경우)입니다.
Sequence Number	선택한 인터페이스 및 방향에 할당된 다른 ACL을 기준으로 지정된 ACL의 순서를 나타내는 시퀀스 번호입니다.

IP ACL 바인딩 테이블에서 IP ACL 바인딩 보기 또는 삭제

➢ **To view or delete IP ACL bindings:**

Security > ACL > Advanced > Binding Table.

1. IP ACL-인터페이스 바인딩을 삭제하려면 인터페이스 옆에 있는 확인란을 선택하고 Delete 버튼을 클릭합니다.

다음 표에서는 IP ACL 바인딩 테이블에 표시되는 정보를 설명합니다.

Table 236. IP ACL 바인딩 테이블

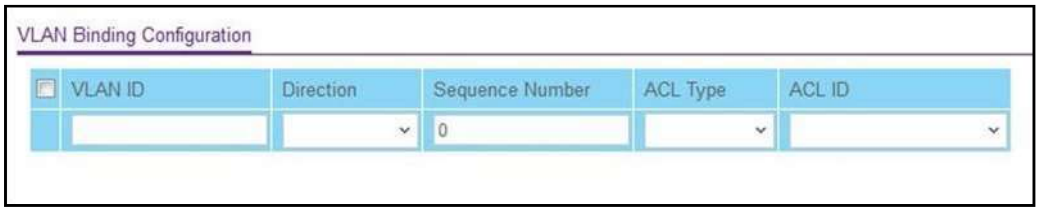
필드	설명

Interface	선택한 인터페이스를 표시합니다.
Direction	ACL에 대해 선택한 패킷 필터링 방향을 표시합니다.
ACL Type	선택한 인터페이스 및 방향에 할당된 ACL 유형입니다.
ACL ID/Name	선택한 인터페이스 및 방향에 할당된 ACL을 식별하는 ACL 번호(IP ACL의 경우) 또는 ACL 이름(명명된 IP ACL 및 IPv6 ACL의 경우)입니다.
Sequence Number	선택한 인터페이스 및 방향에 할당된 다른 ACL을 기준으로 지정된 ACL의 순서를 나타내는 시퀀스 번호입니다.

VLAN 바인딩 테이블에서 VLAN ACL 바인딩 보기 또는 삭제

➢ **VLAN ACL 바인딩을 보거나 삭제하려면:**

Security > ACL> Advanced > VLAN Binding Table.



1. ACL 유형을 사용하여 ACL 유형을 지정합니다.

   유효한 ACL 유형에는 IP ACL, MAC ACL 및 IPv6 ACL이 포함됩니다.

2. ACL ID를 사용하여 선택한 ACL 유형에 따라 구성된 모든 ACL을 표시합니다.
3. Add 버튼을 클릭하여 선택한 ACL ID에 VLAN ID를 추가합니다.
4. VLAN ACL-인터페이스 바인딩을 삭제하려면 인터페이스 확인란을 선택하고 Delete 버튼을 클릭합니다.

다음 표에서는 ACL VLAN 바인딩 테이블에 표시되는 정보를 설명합니다.

Table 237. ACL VLAN 바인딩 테이블

필드	설명
Direction	ACL의 패킷 필터링 방향입니다.
VLAN ID	ACL 매핑을 위한 VLAN ID입니다.

Sequence Number	이 VLAN 및 방향에 이미 할당된 다른 액세스 목록과 관련하여 이 액세스 목록의 순서를 나타내기 위해 선택적 시퀀스 번호를 지정할 수 있습니다. 숫자가 낮을수록 우선순위가 높다는 의미입니다. 이 VLAN 및 방향에 대해 시퀀스 번호가 이미 사용 중인 경우 지정된 액세스 목록은 해당 시퀀스 번호를 사용하여 현재 연결된 액세스 목록을 대체합니다. 사용자가 시퀀스 번호를 지정하지 않은 경우(값은 0) 현재 이 VLAN 및 방향에 사용 중인 가장 높은 시퀀스 번호보다 1 큰 시퀀스 번호가 사용됩니다. 유효한 범위는 1~4294967295입니다.

시스템 모니터링 7

이 장에서는 다음 주제를 다룹니다.

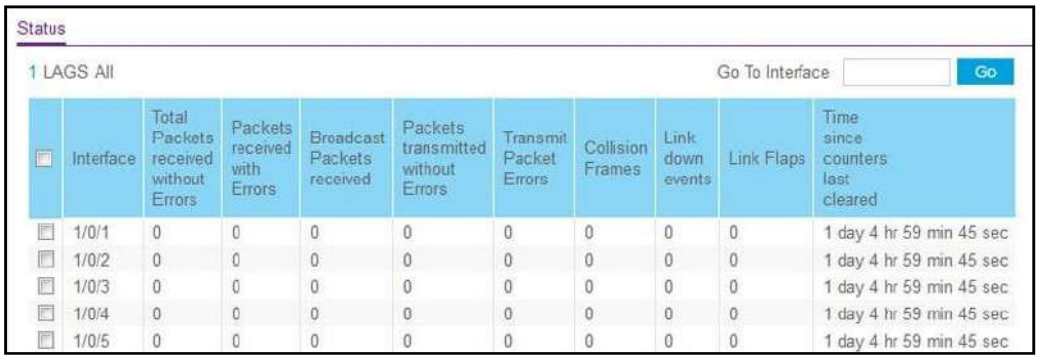
- *포트 통계 보기*
- *로그 관리*
- *다중 포트 미러링 구성*
- *RSPAN VLAN 구성*
- *sFlow 구성*

포트 통계 보기

스위치의 포트별 트래픽 통계 요약을 볼 수 있습니다.

➢ **포트 통계를 보려면:**

Monitoring > **Ports > Port Statistics**.



화면 하단에 있는 버튼을 사용하여 다음 작업을 수행합니다.

- 스위치의 모든 포트에 대한 모든 카운터를 지우려면 행 제목의 확인란을 선택하고 지우기 버튼을 클릭합니다.
- 특정 포트에 대한 카운터를 지우려면 해당 포트의 확인란을 선택하고 Clear 버튼을 클릭합니다.
- 스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표는 화면에 표시되는 포트별 통계를 설명합니다.

Table 238. 포트 통계

필드	설명
Interface	이 개체는 어댑터의 이 포트와 연결된 인터페이스 테이블 항목의 인터페이스를 나타냅니다.
Total Packets Received Without Errors	오류 없이 수신된 총 패킷 수입니다.
Packets Received With Error	상위 계층 프로토콜로 전달할 수 없도록 하는 오류가 포함된 인바운드 패킷 수입니다.
Broadcast Packets Received	브로드캐스트 주소로 전달된 수신된 양호한 패킷의 총 수입니다. 여기에는 멀티캐스트 패킷이 포함되지 않습니다.
Packets Transmitted Without Errors	이 포트에서 해당 세그먼트로 전송된 프레임 수입니다.

Transmit Packet Errors	오류로 인해 전송할 수 없는 아웃바운드 패킷 수입니다.
Collision Frames	이 이더넷 세그먼트의 총 충돌 수에 대한 최선의 추정치입니다.
Number of Link Down Events	물리적 포트의 총 링크 다운 이벤트 수입니다.
Link Flaps	디바운싱 시간 동안 링크 업 이벤트(1개의 링크 플랩 생성)에 대한 링크 다운의 총 발생 횟수입니다.
Time Since Counters Last Cleared	이 포트에 대한 통계가 마지막으로 지워진 이후 경과된 시간(일, 시간, 분, 초)입니다.

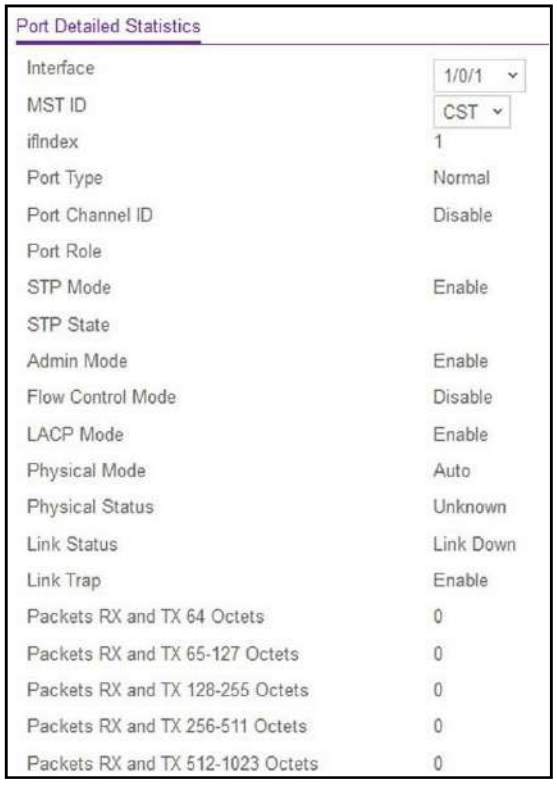
자세한 포트 통계 보기

다양한 포트별 트래픽 통계를 볼 수 있습니다.

- **자세한 포트 통계를 보려면:**

  Monitoring > Ports > Port Detailed Statistics.

  다음 그림은 포트 상세 통계 화면의 필드 중 일부를 보여줍니다.



  화면 하단에 있는 버튼을 사용하여 다음 작업을 수행합니다.

- 모든 카운터를 지우려면 지우기 버튼을 클릭합니다. 그러면 이 포트에 대한 모든 통계가 기본값으로 재설정됩니다.
- 스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

다음 표에서는 화면에 표시되는 자세한 포트 정보를 설명합니다. 다른 포트에 대한 정보를 보려면 인터페이스 메뉴에서 포트 번호를 선택하십시오.

Table 239. 포트 상세 통계

필드	설명
MST ID	인터페이스와 연관된 MST 인스턴스를 표시합니다.
ifIndex	이 객체는 어댑터의 이 포트와 연관된 인터페이스 테이블 항목의 ifIndex를 나타냅니다.
Port Type	일반 포트의 경우 이 필드는 정상입니다. 그렇지 않은 경우 가능한 값은 다음과 같습니다. • **Mirrored**. 이 포트는 미러링된 포트로 포트 미러링에 참여하는 포트입니다. 자세한 내용은 포트 미러링 화면을 참조하십시오. • **Probe**. 이 포트는 프로브 포트로 포트 미러링에 참여하는 포트입니다. 자세한 내용은 포트 미러링 화면을 참조하십시오. • **Trunk Member**. 포트가 링크 집계 트렁크의 구성원입니다. 자세한 내용은 포트 채널 화면을 참조하십시오.
Port Channel ID	포트가 포트 채널의 구성원인 경우 포트 채널의 인터페이스 ID와 이름이 표시됩니다. 그렇지 않으면 비활성화가 표시됩니다.
Port Role	활성화된 각 MST 브리지 포트에는 각 스패닝 트리에 대한 포트 역할이 할당됩니다. 포트 역할은 루트, 지정, 대체, 백업, 마스터 또는 비활성화됨 값 중 하나입니다.
STP Mode	포트 또는 포트 채널과 연관된 스패닝 트리 프로토콜 관리 모드입니다. 가능한 값은 다음과 같습니다. • Enable. 이 포트에 스패닝 트리가 활성화되어 있습니다. • Disable. 이 포트에는 스패닝 트리가 비활성화되어 있습니다.
STP State	포트의 현재 스패닝 트리 상태. 이 상태는 프레임 수신 시 포트가 수행하는 작업을 제어합니다. 브리지가 오작동하는 포트를 감지하면 해당 포트를 손상된 상태로 전환합니다. 상태는 IEEE 802.1D에 정의되어 있습니다. • Disabled • Blocking • Listening • Learning • Forwarding • Broken
Admin Mode	포트 제어 관리 상태입니다. 네트워크에 허용되려면 포트를 활성화해야

	합니다. 공장 기본값은 활성화되어 있습니다.
Flow Control Mode	포트에 대한 흐름 제어의 활성화 또는 비활성화 여부를 나타냅니다. 이 필드는 LAG 인터페이스에는 유효하지 않습니다.
LACP Mode	링크 집계 제어 프로토콜 관리 상태를 나타냅니다. 포트가 링크 집계에 참여하려면 모드를 활성화해야 합니다.
Physical Mode	포트 속도와 이중 모드를 나타냅니다. 자동 협상 모드에서는 이중 모드와 속도가 자동 협상 프로세스에서 설정됩니다.
Physical Status	포트 속도와 이중 모드를 나타냅니다.
Link Status	링크가 작동 중인지 작동 중지되었는지 여부를 나타냅니다.
Link Trap	링크 상태가 변경될 때 포트가 트랩을 보낼지 여부를 나타냅니다.
Packets RX and TX 64 Octets	길이가 64옥텟인(프레이밍 비트 제외, FCS 옥텟 포함) 수신 또는 전송된 총 패킷 수(불량 패킷 포함)입니다.
Packets RX and TX 65-127 Octets	길이가 65~127옥텟(프레이밍 비트는 제외, FCS 옥텟 포함)인 수신 또는 전송된 총 패킷 수(불량 패킷 포함)입니다.
Packets RX and TX 128-255 Octets	길이가 128~255옥텟인(프레이밍 비트 제외, FCS 옥텟 포함) 수신 또는 전송된 총 패킷 수(불량 패킷 포함)입니다.
Packets RX and TX 256-511 Octets	길이가 256~511옥텟(프레이밍 비트는 제외하지만 FCS 옥텟 포함)인 수신 또는 전송된 총 패킷 수(불량 패킷 포함)입니다.
Packets RX and TX 512-1023 Octets	길이가 512~1023옥텟인 수신 또는 전송된 총 패킷 수(불량 패킷 포함)입니다(프레이밍 비트 제외, FCS 옥텟 포함).
Packets RX and TX 1024-1518 Octets	길이가 1024~1518 옥텟(프레이밍 비트는 제외, FCS 옥텟 포함)인 수신 또는 전송된 총 패킷 수(불량 패킷 포함)입니다.
Packets RX and TX 1519-2047 Octets	길이가 1519~2047옥텟인 수신 또는 전송된 총 패킷 수(불량 패킷 포함)(프레이밍 비트 제외, FCS 옥텟 포함)입니다.
Packets RX and TX 2048-4095 Octets	길이가 2048~4095 옥텟(프레이밍 비트는 제외하지만 FCS 옥텟 포함)인 수신 또는 전송된 총 패킷 수(불량 패킷 포함)입니다.
Packets RX and TX 4096-9216 Octets	길이가 4096~9216 옥텟(프레이밍 비트는 제외, FCS 옥텟 포함)인 수신 또는 전송된 총 패킷 수(불량 패킷 포함)입니다.
Octets Received	네트워크에서 수신된 데이터의 총 옥텟 수(잘못된 패킷의 옥텟 포함)입니다(프레이밍 비트는 제외, FCS 옥텟 포함). 이 개체는 이더넷 활용도를 합리적으로 추정하는 데 사용될 수 있습니다. 더 높은 정밀도가 필요한 경우 etherStatsPkts 및 etherStatsOctets 개체는 공통 간격 전후에 샘플링되어야 합니다.
Packets Received 64 Octets	길이가 64옥텟(프레이밍 비트는 제외하지만 FCS 옥텟 포함)인 수신된 패킷(불량 패킷 포함)의 총 수입니다.

Packets Received 65-127 Octets	길이가 65~127옥텟인 수신된 패킷(불량 패킷 포함)의 총 수입니다(프레이밍 비트 제외, FCS 옥텟 포함).
Packets Received 128-255 Octets	길이가 128~255옥텟(프레이밍 비트는 제외, FCS 옥텟 포함)인 수신된 총 패킷 수(불량 패킷 포함)입니다.
Packets Received 256-511 Octets	길이가 256~511옥텟(프레이밍 비트는 제외, FCS 옥텟 포함)인 수신된 총 패킷 수(불량 패킷 포함)입니다.
Packets Received 512-1023 Octets	길이가 512~1023 옥텟인 수신된 총 패킷 수(불량 패킷 포함)입니다(프레이밍 비트 제외, FCS 옥텟 포함).
Packets Received 1024-1518 Octets	길이가 1024~1518 옥텟(프레이밍 비트는 제외, FCS 옥텟 포함)인 수신된 총 패킷 수(불량 패킷 포함)입니다.
Packets Received > 1518 Octets	1518옥텟(프레이밍 비트 제외, FCS 옥텟 포함)보다 길고 형식이 올바른 수신된 총 패킷 수입니다.
Total Packets Received Without Errors	오류 없이 수신된 총 패킷 수입니다.
Unicast Packets Received	상위 계층 프로토콜로 전달되는 하위 네트워크-유니캐스트 패킷 수입니다.
Multicast Packets Received	멀티캐스트 주소로 전달된 수신된 양호한 패킷의 총 수입니다. 이 숫자에는 브로드캐스트 주소로 전달되는 패킷이 포함되지 않습니다.
Broadcast Packets Received	브로드캐스트 주소로 전달된 수신된 양호한 패킷의 총 수입니다. 여기에는 멀티캐스트 패킷이 포함되지 않습니다.
Receive Packets Discarded	상위 계층 프로토콜로 전달되는 것을 방지하기 위해 오류가 감지되지 않았음에도 삭제된 인바운드 패킷 수입니다. 패킷을 삭제하는 가능한 이유는 버퍼 공간을 확보하기 위한 것일 수 있습니다.
Total Packets Received with MAC Errors	상위 계층 프로토콜로 전달할 수 없도록 하는 오류가 포함된 인바운드 패킷의 총 수입니다.
Jabbers Received	1518 옥텟(프레이밍 비트 제외, FCS 옥텟 포함)보다 길고 정수 옥텟 수의 잘못된 FCS(프레임 검사 시퀀스)(FCS 오류) 또는 잘못된 FCS가 있는 수신된 총 패킷 수입니다. 정수가 아닌 옥텟 수(정렬 오류). 이 Jabber 정의는 IEEE-802.3 섹션의 정의와 다릅니다.
Fragments Received	8.2.1.5(10BASE5) 및 섹션 10.3.1.4(10BASE2). 이 문서에서는 Jabber를 패킷이 20ms를 초과하는 조건으로 정의합니다. 재버를 감지할 수 있는 허용 범위는 20ms에서 150ms 사이입니다.
Undersize Received	ERROR CRC(프레이밍 비트 제외, FCS 옥텟 포함)가 포함된 길이가 64옥텟 미만인 수신된 총 패킷 수입니다.
Alignment Errors	GOOD CRC를 사용하여 길이가 64옥텟 미만인 수신된 총 패킷 수입니다(프레이밍 비트는 제외하지만 FCS 옥텟 포함).

Rx FCS Errors	64~1518 옥텟 길이(프레이밍 비트 제외, FCS 옥텟 포함)로 수신된 총 패킷 수이지만 옥텟 수가 정수가 아닌 잘못된 FCS(프레임 검사 시퀀스)가 있습니다.
Overruns	64~1518 옥텟 길이(프레이밍 비트 제외, FCS 옥텟 포함)로 수신되었지만 정수 옥텟 수의 잘못된 FCS(프레임 검사 시퀀스)가 있는 수신된 패킷의 총 수
Total Received Packets Not Forwarded	이 포트가 수신 패킷으로 과부하되어 유입을 따라잡지 못해 삭제된 총 프레임 수입니다.
802.3x Pause Frames Received	전달 프로세스에서 삭제(즉, 필터링)된 유효한 프레임 수입니다.
Unacceptable Frame Type	허용되지 않는 프레임 유형으로 인해 이 포트에서 삭제된 프레임 수입니다.
Total Packets Transmitted (Octets)	네트워크에서 전송된 데이터의 총 옥텟 수(불량 패킷 포함)(프레이밍 비트 제외, FCS 옥텟 포함). 이 개체는 이더넷 활용도를 합리적으로 추정하는 데 사용될 수 있습니다. 더 높은 정밀도가 필요한 경우 etherStatsPkts 및 etherStatsOctets 개체는 공통 간격 전후에 샘플링되어야 합니다.
Packets Transmitted 64 Octets	길이가 64옥텟(프레이밍 비트는 제외하지만 FCS 옥텟 포함)인 수신된 패킷(불량 패킷 포함)의 총 수입니다.
Packets Transmitted 65-127 Octets	길이가 65~127옥텟인 수신된 패킷(불량 패킷 포함)의 총 수입니다(프레이밍 비트 제외, FCS 옥텟 포함).
Packets Transmitted 128-255 Octets	길이가 128~255옥텟(프레이밍 비트는 제외, FCS 옥텟 포함)인 수신된 총 패킷 수(불량 패킷 포함)입니다.
Packets Transmitted 256-511 Octets	길이가 256~511옥텟(프레이밍 비트는 제외, FCS 옥텟 포함)인 수신된 총 패킷 수(불량 패킷 포함)입니다.
Packets Transmitted 512-1023 Octets	길이가 512~1023 옥텟인 수신된 총 패킷 수(불량 패킷 포함)입니다(프레이밍 비트 제외, FCS 옥텟 포함).
Packets Transmitted 1024-1518 Octets	길이가 1024~1518 옥텟(프레이밍 비트는 제외, FCS 옥텟 포함)인 수신된 총 패킷 수(불량 패킷 포함)입니다.
Packets Transmitted > 1518 Octets	1518옥텟(프레이밍 비트는 제외, FCS 옥텟 포함)보다 길고 형식이 올바른 전송된 총 패킷 수입니다. 이 카운터의 최대 증가율은 10Mb/s에서 초당 815카운트입니다.
Maximum Frame Size	이더넷 헤더, CRC 및 페이로드를 포함하여 인터페이스가 지원하거나 사용하도록 구성된 최대 이더넷 프레임 크기입니다. (1518년부터 9216년까지). 기본 최대 프레임 크기는 1518입니다.
Total Packets Transmitted Successfully	이 포트에서 해당 세그먼트로 전송된 프레임 수입니다.
Unicast Packets Transmitted	폐기되거나 전송되지 않은 패킷을 포함하여 상위 수준 프로토콜이 하위 네트워크-유니캐스트 주소로 전송되도록 요청한 총 패킷 수입니다.

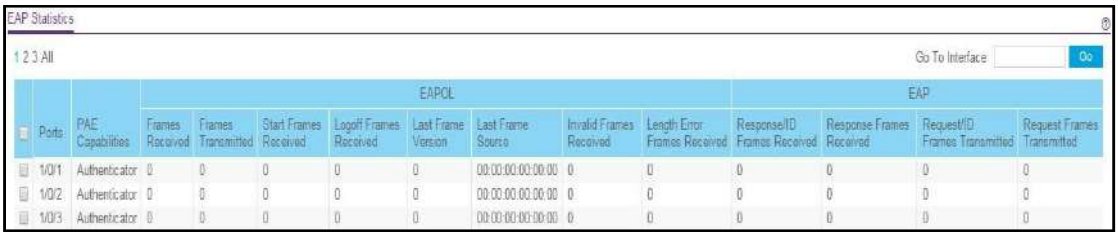
Multicast Packets Transmitted	폐기되거나 전송되지 않은 패킷을 포함하여 상위 수준 프로토콜이 멀티캐스트 주소로 전송하도록 요청한 총 패킷 수입니다.
Broadcast Packets Transmitted	삭제되거나 전송되지 않은 패킷을 포함하여 상위 수준 프로토콜이 브로드캐스트 주소로 전송되도록 요청한 총 패킷 수입니다.
Total Transmit Errors	단일 충돌, 다중 충돌, 과도한 충돌의 합입니다.
Total Transmit Packets Discarded	삭제된 단일 충돌 프레임, 삭제된 여러 충돌 프레임 및 삭제된 초과 프레임의 합계입니다.
Single Collision Frames	정확히 한 번의 충돌로 인해 전송이 금지된 특정 인터페이스에서 성공적으로 전송된 프레임 수입니다.
Multiple Collision Frames	둘 이상의 충돌로 인해 전송이 금지된 특정 인터페이스에서 성공적으로 전송된 프레임 수입니다.
Excessive Collision Frames	과도한 충돌로 인해 특정 인터페이스에서 전송이 실패한 프레임 수입니다.
STP BPDUs Received	선택한 포트에서 수신된 STP BPDU 수입니다.
STP BPDUs Transmitted	선택한 포트에서 전송된 STP BPDU 수입니다.
RSTP BPDUs Received	선택한 포트에서 수신된 RSTP BPDU 수입니다.
RSTP BPDUs Transmitted	선택한 포트에서 전송된 RSTP BPDU 수입니다.
MSTP BPDUs Received	선택한 포트에서 수신된 MSTP BPDU 수입니다.
MSTP BPDUs Transmitted	선택한 포트에서 전송된 MSTP BPDU 수입니다.
802.3x Pause Frames Transmitted	PAUSE 작업을 나타내는 opcode와 함께 이 인터페이스에서 전송된 MAC 제어 프레임의 수입니다. 인터페이스가 반이중 모드에서 작동하는 경우 이 카운터는 증가하지 않습니다.
GVRP PDUs Received	GARP 계층에서 수신된 GVRP PDU의 수입니다.
GVRP PDUs Transmitted	GARP 계층에서 전송된 GVRP PDU의 개수입니다.
GVRP Failed Registrations	GVRP 등록 시도 횟수를 완료하지 못했습니다.
GMRP PDUs Received	GARP 계층으로부터 수신된 GMRP PDU의 수입니다.
GMRP PDUs Transmitted	GARP 계층에서 전송된 GMRP PDU의 개수입니다.
GMRP Failed Registrations	GMRP 등록 시도 횟수를 완료하지 못했습니다.
EAPOL Frames Received	이 인증자가 수신한 모든 유형의 유효한 EAPOL 프레임 수입니다.
EAPOL Frames Transmitted	이 인증자가 전송한 모든 유형의 EAPOL 프레임 수입니다.
Time Since Counters Last Cleared	이 포트에 대한 통계가 마지막으로 지워진 이후 경과된 시간(일, 시간, 분, 초)입니다.

EAP 통계 보기

특정 포트에서 수신된 EAP 패킷에 대한 정보를 표시할 수 있습니다.

➢ **EAP 통계를 보려면:**

Monitoring > Ports > EAP Statistics.



화면 하단에 있는 버튼을 사용하여 다음 작업을 수행합니다.

- 스위치의 모든 포트에 대한 모든 EAP 카운터를 지우려면 행 제목의 확인란을 선택하고 Clear 버튼을 클릭합니다. 버튼을 클릭하면 모든 포트에 대한 모든 통계가 기본값으로 재설정됩니다.
- 특정 포트에 대한 카운터를 지우려면 해당 포트와 관련된 확인란을 선택하고 Clear 버튼을 클릭합니다.
- 스위치의 최신 정보로 화면을 새로 고칩니다.

다음 표에서는 화면에 표시되는 EAP 통계에 대해 설명합니다. 업데이트 버튼을 클릭하세요.

Table 240. EAP 통계

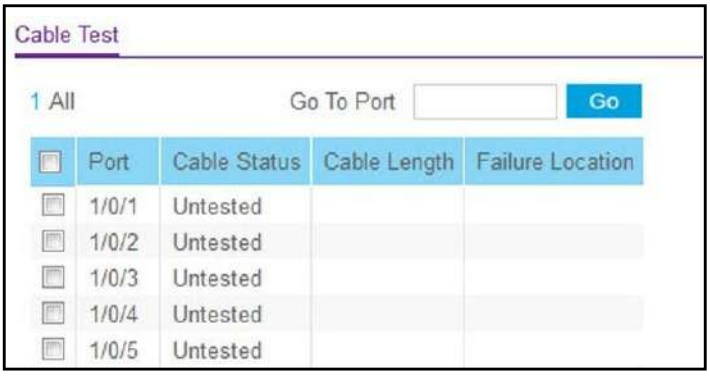
필드	설명
Port	표시할 포트를 선택합니다. 선택 사항이 변경되면 화면 업데이트가 발생하여 새로 선택한 포트에 대해 모든 필드가 업데이트됩니다. 모든 물리적 인터페이스가 유효합니다.
PAE Capabilities	선택한 포트의 PAE 기능이 표시됩니다.
EAPOL Frames Received	이 인증자가 수신한 모든 유형의 유효한 EAPOL 프레임 수가 표시됩니다.
EAPOL Frames Transmitted	이는 이 인증자가 전송한 모든 유형의 EAPOL 프레임 수를 표시합니다.
EAPOL Start Frames Received	이 인증자가 수신한 EAPOL 시작 프레임 수가 표시됩니다.
EAPOL Logoff Frames Received	이 인증자가 수신한 EAPOL 로그오프 프레임 수가 표시됩니다.
EAPOL Last Frame Version	가장 최근에 수신된 EAPOL 프레임에 포함된 프로토콜 버전 번호를 표시합니다.

EAPOL Last Frame Source	가장 최근에 수신된 EAPOL 프레임에 전달된 소스 MAC 주소를 표시합니다.
EAPOL Invalid Frames Received	이 인증자가 수신한 프레임 유형이 인식되지 않는 EAPOL 프레임 수를 표시합니다.
EAPOL Length Error Frames Received	이 인증자가 수신한 프레임 유형이 인식되지 않는 EAPOL 프레임 수를 표시합니다.
EAP Response/ID Frames Received	이 인증자가 수신한 EAP 응답/신원 프레임 수가 표시됩니다.
EAP Response Frames Received	이는 이 인증자가 수신한 유효한 EAP 응답 프레임(resp/ID 프레임 제외)의 수를 표시합니다.
EAP Request/ID Frames Transmitted	이 인증자가 전송한 EAP 요청/ID 프레임 수가 표시됩니다.
EAP Request Frames Transmitted	이 인증자가 전송한 EAP 요청 프레임(요청/ID 프레임 제외) 수가 표시됩니다.

케이블 테스트 수행

- **To perform a cable test:**

  Monitoring > Ports > Cable Test.



1. **Port**. 테스트할 케이블이 연결된 인터페이스를 나타냅니다.
2. Apply 버튼을 클릭합니다

   선택한 인터페이스에서 케이블 테스트가 수행됩니다. 케이블 테스트를 완료하는 데 최대 2초가 걸릴 수 있습니다. 포트에 활성 링크가 있는 경우 케이블 상태는 항상 정상입니다. 이 기능이 현재 링크 속도에 대해 PHY에서 지원되는 경우 명령은 케이블 길이 추정치를 반환합니다. 링크가 다운되고 케이블이 10/100 이더넷 어댑터에 연결된 경우 일부 이더넷 어댑터는 사용하지 않는 와이어 쌍을 종단되지 않거나 접지된 상태로 두기 때문에 케이블 상태가 개방형 또는 단락일 수 있습니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 241. 케이블 테스트

필드	설명
Cable Status	이는 케이블 상태를 Normal, Open 또는 Short로 표시합니다. • Normal: 케이블이 올바르게 작동하고 있습니다. • Open: 케이블이 연결되지 않았거나 커넥터에 결함이 있습니다. • Short: 케이블에 전기적 단락이 있습니다. • Cable Test Failed: 케이블 상태를 확인할 수 없습니다. 케이블이 실제로 작동할 수도 있습니다. • Untested: 케이블은 아직 테스트되지 않았습니다. • Invalid cable type: 지원되지 않는 케이블 유형입니다.
Cable Length	케이블의 예상 길이(미터)입니다. 길이는 가장 짧은 예상 길이와 가장 긴 예상 길이 사이의 범위로 표시됩니다. 케이블 길이를 확인할 수 없으면 알 수 없음이 표시됩니다. 케이블 길이는 케이블 상태가 정상인 경우에만 표시됩니다.
Failure Location	케이블 끝에서 오류 위치까지의 예상 거리(미터)입니다. 오류 위치는 케이블 상태가 Open(개방) 또는 Short(단락)인 경우에만 표시됩니다.

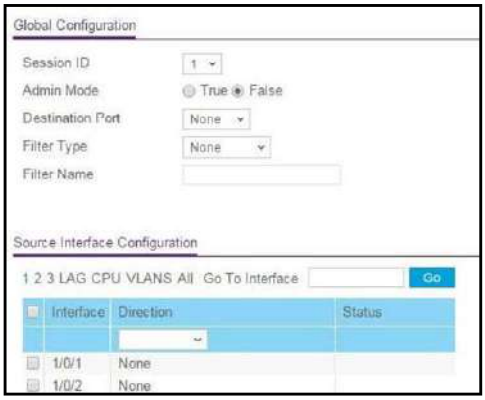
다중 포트 미러링 구성

포트 미러링은 네트워크 분석기에서 분석할 네트워크 트래픽을 선택합니다. 이는 스위치의 특정 포트에 대해 수행됩니다. 이처럼 많은 스위치 포트가 소스 포트로 구성되고, 하나의 스위치 포트가 대상 포트로 구성됩니다. 소스 포트에서 트래픽이 미러링되는 방식을 구성할 수 있습니다. 소스 포트에서 수신되거나, 포트에서 전송되거나, 수신 및 전송되는 패킷은 대상 포트로 미러링될 수 있습니다.

대상 포트로 복사된 패킷은 회선의 원본 패킷과 동일한 형식입니다. 즉, 미러가 수신된 패킷을 복사하는 경우 복사된 패킷은 소스 포트에서 수신되었으므로 VLAN 태그가 지정되거나 태그가 지정되지 않습니다. 미러가 전송된 패킷을 복사하는 경우 복사된 패킷은 소스 포트에서 전송되므로 VLAN 태그가 지정되거나 태그가 지정되지 않습니다.

➢ **다중 포트 미러링을 전역적으로 구성하려면:**

Monitoring > Mirroring > Multiple Port Mirroring.



1. Session ID 목록에서 세션 번호를 선택하세요.
2. Admin Mode에서 True(활성화) 또는 False(비활성화) 라디오 버튼을 선택합니다.

   선택한 세션에 대해 관리 모드를 활성화하려면 True 옵션을 선택하십시오. 특정 세션이 활성화되면 세션의 소스 포트에 들어가거나 나가는 모든 트래픽이 해당 대상 포트 또는 RSPAN(원격 교환 포트 분석기) VLAN에 복사(미러링)됩니다. 기본적으로 관리 모드는 비활성화되어 있습니다(False).

3. Destination Port 목록에서 포트 트래픽을 복사할 대상 인터페이스를 선택합니다.

   시스템에서는 하나의 대상 포트만 구성할 수 있습니다. 이는 프로브 포트 역할을 하며 구성된 미러링 포트에서 모든 트래픽을 수신합니다. 값이 구성되지 않은 경우 None으로 표시됩니다. 기본값은 None입니다.

4. Filter Type 목록에서 허용 규칙과 일치하는 트래픽을 미러링할 수 있는 IP 또는 MAC ACL을 선택합니다.

   가능한 값은 다음과 같습니다.

   - **None**. 세션에 대해 구성된 필터가 없습니다.
   - **IP ACL**. IP ACL을 구성합니다.
   - **MAC ACL.** MAC ACL을 구성합니다.

   기본값은 None입니다.

5. Filter Name 필드에 해당 세션에 대해 필터가 구성된 경우 필터 이름을 입력합니다.
6. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

7. Source Interface Configuration Section에서 다음 선택 방법을 사용합니다.

- 선택한 장치의 물리적 포트를 표시하려면 Unit ID를 선택합니다.
- LAG 목록만 표시하려면 LAG를 선택합니다.
- CPU 목록만 표시하려면 CPU를 선택합니다.
- VLAN을 선택하여 사용 가능한 VLAN 목록을 표시합니다.
- 모든 물리적 포트, LAG, CPU 및 VLAN 목록을 표시하려면 All을 선택합니다.
- Go To Interface 필드에 해당 번호를 입력하여 특정 인터페이스를 선택합니다.
- Interface를 사용하여 구성된 포트를 미러링된 포트로 지정합니다. 구성된 포트의 트래픽이 프로브 포트로 전송됩니다.

8. Direction 필드에서 구성된 미러링 포트에서 미러링할 트래픽 방향을 지정합니다.

   값이 구성되지 않은 경우 없음으로 표시됩니다. 기본값은 없음입니다. Direction 옵션은 다음과 같습니다.

   - **None**. 값이 구성되지 않았습니다.
   - **Tx and Rx**. 전송 및 수신된 패킷을 모니터링합니다.
   - **Tx**. 전송된 패킷만 모니터링합니다.
   - **Rx**. 수신된 패킷만 모니터링합니다.

   Note: VLAN의 경우에만 Tx, Rx 및 None 옵션을 적용할 수 있습니다.

   - **Tx and Rx.** VLAN을 소스 VLAN으로 지정합니다.
   - **None.** 지정된 소스 VLAN을 제거합니다.

   VLAN이 소스 VLAN으로 구성된 경우 해당 방향은 빈 필드로 표시됩니다.

9. Apply 버튼을 클릭합니다
   설정이 시스템에 적용됩니다. 포트가 소스 포트로 구성된 경우 Mirroring Port 필드 값은 Mirroring입니다.

   Status 필드는 인터페이스 상태를 나타냅니다.

   Note: 여러 오류 메시지가 있는 오류 대화 상자의 경우 이를 해결하여 나머지 오류 세트(있는 경우)를 가져옵니다.

RSPAN VLAN 구성

RSPAN(원격 스위치 포트 분석기) VLAN을 사용하도록 VLAN을 구성할 수 있습니다. RSPAN을 사용하면 여러 네트워크 장치의 여러 소스 포트(또는 VLAN의 구성원인 모든 포트)의 트래픽을 미러링하고 미러링된 트래픽을 원격 장치의 대상 포트(네트워크 분석기에 연결된 프로브 포트)로 보낼 수 있습니다. 미러링된 트래픽에는 RSPAN VLAN ID 태그가 지정되고 RSPAN VLAN의 트렁크 포트를 통해 전송됩니다.

➢ **RSPAN VLAN을 구성하려면:**

Monitoring > Mirroring > RSPAN VLAN.

VLAN ID 열에는 장치의 모든 VLAN이 나열됩니다.

1. RSPAN VLAN으로 사용할 VLAN을 선택합니다.
2. Admin 목록에서 해당 VLAN에 대한 RSPAN 지원 Enable 또는 Disable를 선택합니다.

   기본값은 Disable입니다.
3. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

RSPAN 소스 스위치 구성

➢ **RSPAN 소스 스위치를 구성하려면:**

Monitoring > Mirroring > RSPAN Source Switch Configuration.

1. 목록에서 Session ID 번호를 선택하세요.
2. 선택한 세션에 대해 Admin Mode의 True(활성화) 또는 False(비활성화) 라디오 버튼을 선택합니다.

   특정 세션이 활성화되면 세션의 소스 포트에 들어가거나 나가는 모든 트래픽이 해당 대상 포트 또는 RSPAN(원격 교환 포트 분석기) VLAN에 복사(미러링)됩니다. 기본적으로 관리 모드는 False되어 있습니다.
3. available VLAN ID 목록에서 RSPAN Source VLAN을 선택합니다.
4. Reflector Port Interface 목록에서 RSPAN Reflector Port를 선택합니다.
5. Filter Type 목록에서 선택하여 허용 규칙과 일치하는 트래픽을 미러링할 수 있는 IP 또는 MAC ACL을 구성합니다.

   가능한 값은 다음과 같습니다.

   - **None**.
   - **IP ACL**. IP ACL을 구성합니다.
   - **MAC ACL**. MAC ACL을 구성합니다.
6. 세션에 필터가 구성된 경우 Filter Name을 입력합니다.
7. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

➢ **RSPAN 소스 인터페이스를 구성하려면:**

1. 선택한 장치에 대한 물리적 포트 목록을 표시하려면 Unit ID(1, 2, 3)를 선택하십시오.
2. LAG만 표시하려면 LAG를 선택합니다.
3. CPU만 표시하려면 CPU를 선택합니다.
4. VLAN을 선택하여 사용 가능한 VLAN ID 목록을 표시합니다.
5. 모든 물리적 포트, LAG, CPU 및 VLAN을 표시하려면 All을 선택합니다.
6. Go To Interface필드에 인터페이스 번호를 입력하여 인터페이스를 선택합니다.
7. 인터페이스 목록에서 구성된 포트를 미러링 포트로 지정할 인터페이스를 선택합니다.

   구성된 포트의 트래픽이 프로브 포트로 전송됩니다.
8. Direction 목록에서 선택하여 구성된 미러링 포트에서 미러링할 트래픽 방향을 지정합니다.

   값이 구성되지 않은 경우 없음이 표시됩니다. 기본값은 None입니다.

   - **None**. 값이 구성되지 않았습니다.
   - **Tx and Rx**. 전송 및 수신된 패킷을 모니터링합니다.
   - **Tx**. 전송된 패킷만 모니터링합니다.
   - **Rx**. 수신된 패킷만 모니터링합니다.

Status 필드는 인터페이스 상태를 나타냅니다.

RSPAN 대상 스위치 구성

➢ **RSPAN 대상 스위치를 구성하려면:**

Monitoring > Mirroring > RSPAN Destination Switch Configuration.

1. Session ID 목록에서 세션 ID를 선택하세요.
2. 선택한 세션에 대해 Admin Mode에서 True(활성화) 또는 False(비활성화) 라디오 버튼을 선택합니다.

   특정 세션이 활성화되면 세션의 소스 포트에 들어가거나 나가는 모든 트래픽이 해당 대상 포트 또는 RSPAN(원격 교환 포트 분석기) VLAN에 복사(미러링)됩니다. 기본적으로 관리 모드는 False되어 있습니다.
3. available VLAN ID 목록에서 RSPAN Source VLAN을 선택합니다.
4. Destination Interface 목록에서 RSPAN Destination VLAN을 선택합니다.
5. Filter Type을 구성합니다.

   IP 또는 MAC ACL은 허용 규칙과 일치하는 트래픽을 미러링합니다. 가능한 값은 다음과 같습니다.

   - **None**. 세션에 대해 구성된 필터가 없습니다.
   - **IP ACL**. IP ACL을 구성합니다.
   - **MAC ACL**. MAC ACL을 구성합니다.
6. 세션에 대해 구성된 경우 Filter Name을 입력합니다.
7. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

sFlow 구성

기본 또는 고급 sFlow 설정을 구성할 수 있습니다.

기본 sFlow 에이전트 정보 구성

➢ **To configure basic sFlow agent information:**

Monitoring > sFlow > Basic > sFlow Agent Information.

1. Source Interface 목록에서 sFlow Agent에 사용되는 관리 인터페이스를 선택합니다.

   가능한 값은 다음과 같습니다.
   - None
   - Routing interface
   - Routing VLAN
   - Routing loopback interface
   - Tunnel interface
   - Service port

   기본적으로 VLAN 1은 소스 인터페이스로 사용됩니다.

2. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.The 다음 표에서는 구성할 수 없는 정보에 대해 설명합니다.

Table 245. sFlow 기본 에이전트 정보

필드	설명
Agent Version	이 MIB의 버전과 구현을 고유하게 식별합니다. 버전 문자열은 다음 구조를 사용해야 합니다. MIB 버전;조직;소프트웨어 개정: • MIB Version: 예를 들어 1.3은 이 MIB 버전입니다. • Organization: Inc. • Revision: 1.0
Agent Address	이 에이전트와 연결된 IP 주소입니다.

sFlow 에이전트 고급 설정 구성

➢ **sFlow 에이전트 고급 설정을 구성하려면:**

Monitoring > **sFlow** > **Advanced** > **sFlow Agent Information**.

1. Source Interface 목록에서 sFlow Agent에 사용할 관리 인터페이스를 선택합니다.

   가능한 값은 다음과 같습니다.
   - None
   - Routing interface
   - Routing VLAN
   - Routing loopback interface
   - Tunnel interface
   - Service port

   기본적으로 VLAN 1은 소스 인터페이스로 사용됩니다.

2. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표에서는 구성할 수 없는 정보에 대해 설명합니다.

Table 246. sFlow 고급 에이전트 정보

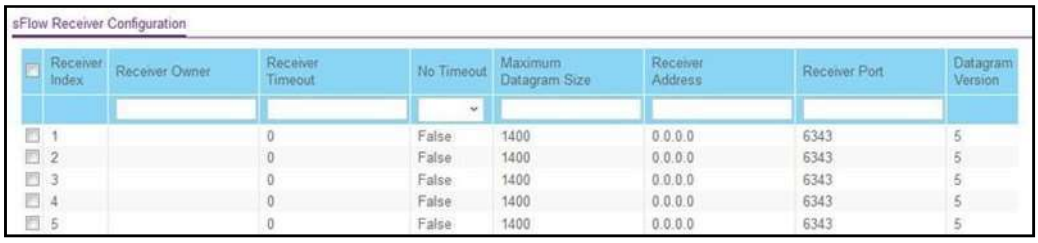
필드	설명

Agent Version	이 MIB의 버전과 구현을 고유하게 식별합니다. 버전 문자열은 다음 구조를 사용해야 합니다. MIB 버전;조직;소프트웨어 개정: • MIB Version: '1.3', 이 MIB 버전 • Organization: Inc. • Revision: 1.0
Agent Address	이 에이전트와 연결된 IP 주소입니다.

sFlow 수신기 구성

➢ **sFlow 수신기를 구성하려면:**

Monitoring > sFlow > Advanced > sFlow Receiver Configuration.



1. Receiver Owner를 지정합니다.

   이는 이 sFlowRcvrTable 항목을 사용하는 엔터티입니다. 빈 문자열은 항목이 현재 요청되지 않았으며 수신자 구성이 기본값으로 재설정되었음을 나타냅니다. sFlowRcvrTable 항목을 요청하려는 엔터티는 항목을 요청하기 전에 항목이 요청 취소되었는지 확인해야 합니다. 항목은 소유자 문자열을 설정하여 주장됩니다. 다른 샘플러 개체를 변경하려면 먼저 항목을 요청해야 합니다.

2. **Receiver Timeout** - 샘플러가 해제되고 샘플링이 중지되기까지 남은 시간(초)입니다.

   샘플러의 제어를 유지하려는 관리 주체는 이전 값이 만료되기 전에 새 값을 설정해야 할 책임이 있습니다. 유효한 범위는 0~2147483647입니다. 값이 0이면 선택한 수신기 구성이 기본값으로 설정됩니다.

3. No Timeout을 사용하여 True 또는 False를 선택하여 수신기에 대한 시간 초과 샘플링 없음을 설정합니다.

   No Timeout 선택 항목이 True가 될 때까지 샘플링은 중지되지 않습니다. 기본값은 False입니다.

4. **Maximum Datagram Size** - 단일 샘플 데이터그램으로 전송할 수 있는 최대 데이터 바이트 수입니다.

   sFlow 데이터그램의 조각화를 방지하려면 이 값을 설정하십시오. 기본값: 1400. 허용되는 범위는 200~9116입니다.

5. **Receiver Address. sFlow 수집기의 IP 주소입니다.**

   0.0.0.0으로 설정하면 sFlow 데이터그램이 전송되지 않습니다.

6. **Receiver Port. sFlow 데이터그램의 대상 포트입니다.**

   허용되는 범위는 1~65535입니다.

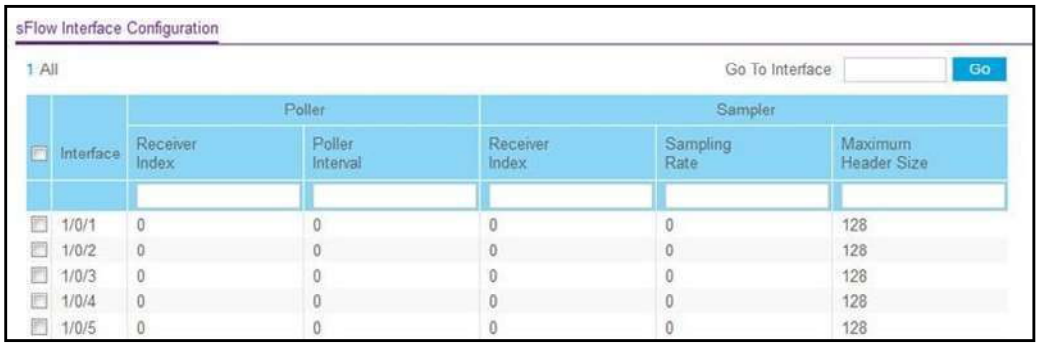
Receiver Datagram Version 필드에는 전송될 sFlow 데이터그램 버전이 표시됩니다.

sFlow 인터페이스 구성

sFlow 에이전트는 전환된 흐름의 통계적 패킷 기반 샘플링을 수집하여 구성된 수신기로 보냅니다. 흐름 샘플을 수집하도록 구성된 데이터 소스를 샘플러라고 합니다. sFlow 에이전트는 또한 네트워크 인터페이스 통계의 시간 기반 샘플링을 수집하여 구성된 sFlow 수신기로 보냅니다. 카운터 샘플을 수집하도록 구성된 데이터 소스를 폴러라고 합니다.

➢ **sFlow 인터페이스를 구성하려면:**

Monitoring > sFlow > Advanced > sFlow Interface Configuration.



1. Interface는 이 플로우 폴러와 샘플러에 대한 인터페이스를 표시합니다.

   이 에이전트는 물리적 포트만 지원합니다.

2. Poller Receiver Index를 사용하여 이 카운터 폴러와 연결된 sFlow 수신기에 대해 허용되는 범위를 지정합니다.

허용되는 범위는 1~8입니다.

3. Poller Interval을 사용하여 이 데이터 소스와 관련된 카운터의 연속 샘플 사이의 최대 시간(초)을 지정합니다.

   샘플링 간격이 0이면 카운터 샘플링이 비활성화됩니다.

   허용되는 범위는 0~86400초입니다.

4. Sampler Receiver Index을 사용하여 이 흐름 샘플러에 대한 sFlow 수신기를 지정합니다.

   0으로 설정하면 샘플러 구성이 기본값으로 설정되고 샘플러가 삭제됩니다.

   활성 수신기만 설정할 수 있습니다. 수신기가 만료되면 수신기와 연결된 모든 샘플러도 만료됩니다. 허용되는 범위는 1~8입니다.

5. Sampling Rate를 사용하여 이 소스의 패킷 샘플링에 대한 통계 샘플링 속도를 지정합니다. 샘플링 속도 1은 모든 패킷을 계산합니다. 샘플링 속도가 0이면 샘플링이 비활성화됩니다. 허용되는 범위는 1024~65536입니다.

6. Maximum Header Size를 사용하여 샘플링된 패킷에서 복사할 최대 바이트 수를 지정합니다.

   허용되는 범위는 20~256입니다.

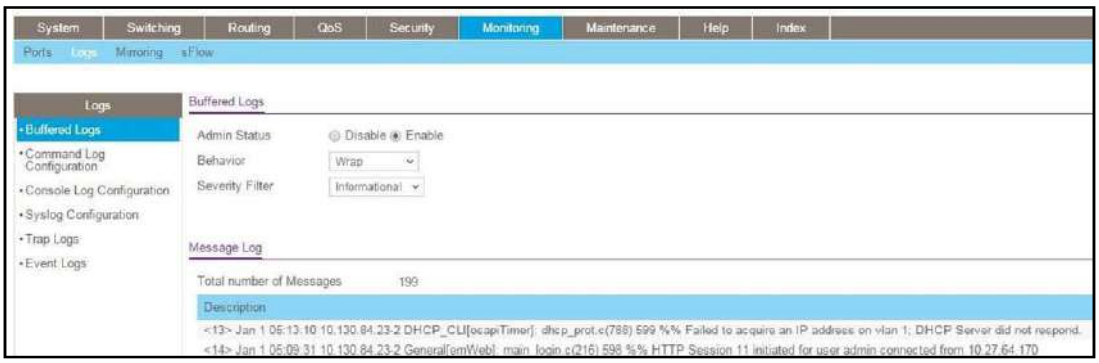
로그 관리

스위치는 플랫폼에서 발생하는 이벤트, 오류 또는 오류는 물론 구성 변경이나 기타 발생에 대한 응답으로 메시지를 생성합니다. 이러한 메시지는 로컬에 저장되며 모니터링 목적이나 장기 보관 저장소를 위해 하나 이상의 중앙 집중식 수집 지점으로 전달될 수 있습니다. 로깅 기능의 로컬 및 원격 구성에는 심각도 및 생성 구성 요소를 기반으로 기록되거나 전달된 메시지 필터링이 포함됩니다.

버퍼링된 로그 보기

➢ **버퍼링된 로그를 보려면:**

Monitoring > Logs > Buffered Logs.



버퍼링된 로그 구성

이 로그는 메시지 구성 요소 및 심각도 설정에 따라 메시지를 메모리에 저장합니다. 섀시 시스템에서 이 로그는 섀시 플랫폼 상단에만 존재합니다. 섀시의 다른 플랫폼은 해당 메시지를 섀시 로그 상단으로 전달합니다.

➢ **버퍼링된 로그를 구성하려면:**

1. Admin Status의 Enable 또는 Disable 라디오 버튼을 선택합니다.

   비활성화된 로그는 메시지를 기록하지 않습니다.

2. Behavior을 사용하여 로그가 가득 찼을 때의 동작을 지정합니다.

   로그 공간이 채워지면 순환되거나 중지될 수 있습니다.

3. Severity Filter목록에서 심각도 옵션을 선택합니다.

   로그는 구성된 심각도 임계값과 같거나 그 이상의 메시지를 기록합니다. 심각도 수준은 다음과 같습니다.

   - **Emergency (0)**. 시스템을 사용할 수 없습니다.
   - **Alert (1)**. 즉시 조치를 취해야 합니다.
   - **Critical (2)**. 심각한 조건.
   - **Error (3)**. 오류 조건.
   - **Warning (4)**. 경고 조건.
   - **Notice (5)**. 정상적이지만 중요한 상태.
   - **Informational (6)**. 정보 메시지.

- **Debug (7)**. 디버그 수준 메시지.

스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

4. 메모리에 버퍼링된 로그를 지우려면 Clear 버튼을 클릭하세요.
5. Apply 버튼을 클릭합니다

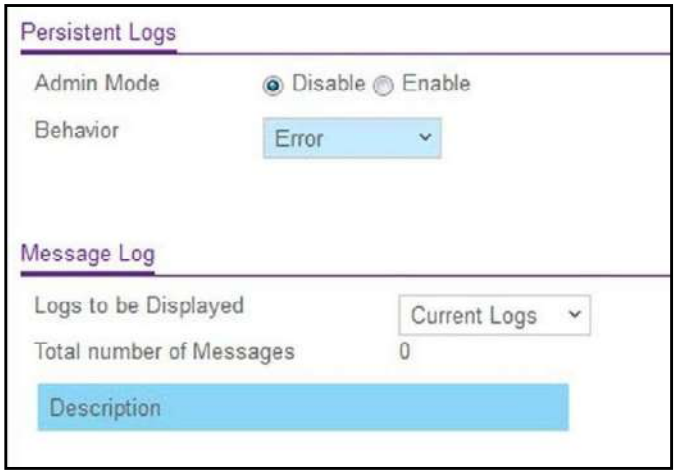
업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

영구 로그 구성(및 전용)

영구 로그는 영구 저장소에 저장되는 로그입니다. 영구 스토리지는 플랫폼 재부팅 후에도 유지됩니다. 첫 번째 로그 유형은 시스템 시작 로그입니다. 시스템 시작 로그는 시스템 재부팅 후 수신된 처음 N개의 메시지를 저장합니다. 두 번째 로그 유형은 시스템 작업 로그입니다. 시스템 작동 로그에는 시스템 작동 중에 수신된 마지막 N개 메시지가 저장됩니다.

➢ **영구 로그를 구성하려면:**

Monitoring > Logs > Persistent Logs.



비활성화된 로그는 메시지를 기록하지 않습니다.

1. Admin Mode의 Disable 또는 Enable 라디오 버튼을 선택합니다

2. Behavior 목록에서 심각도 수준을 선택합니다.

   로그는 구성된 심각도 임계값과 같거나 그 이상의 메시지를 기록합니다. 다음 심각도 수준을 사용할 수 있습니다.

   - **Emergency (0)**. 시스템을 사용할 수 없습니다.
   - **Alert (1)**. 즉시 조치를 취해야 합니다
   - **Critical (2)**. 중요한 조건
   - **Error (3)**. 오류 조건
   - **Warning (4)**. 경고 조건
   - **Notice (5)**. 정상이지만 중요한 상태
   - **Informational (6)**. 정보 메시지
   - **Debug (7)**. 디버그 수준 메시지

스위치에 대한 최신 정보로 화면을 새로 고치려면 새로 고침 버튼을 클릭하세요.

메시지 형식

- Total number of messages: Number of persistent log messages displayed on the switch.
- <15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry

이 예는 섀시가 아니며 mstp_api 파일의 라인 318에 의해 8월 24일 05:34:05에 스레드 ID 2110에서 실행되는 구성 요소 MSTP에 의해 생성된 시스템의 심각도 7(디버그)이 있는 사용자 수준 메시지(1)를 나타냅니다. 기음. 237번째 메시지가 기록되었습니다. syslog를 통해 수집기 또는 릴레이에 기록되는 메시지는 이전 메시지와 동일한 형식을 사용합니다.

메시지 로그 형식

이 주제는 메시지 로그, 지속성 로그 또는 콘솔 로그에 대해 표시되는 모든 기록된 메시지의 형식에 적용됩니다.

syslog를 통해 수집기 또는 릴레이에 기록되는 메시지는 동일한 형식을 사용합니다.

- <15>Aug 24 05:34:05 0.0.0.0-1 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry.

  This example indicates a message with severity 7 (15 mod 8) (debug) on a chassis and generated by component MSTP running in thread ID 2110 on Aug 24 05:34:05 by line 318 of file mstp_api.c. This is the 237th message logged with system IP 0.0.0.0 and task-ID 1.

- <15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry.

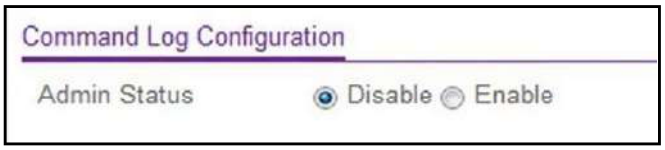
  이 예는 섀시가 아니며 mstp_api 파일의 라인 318에 의해 8월 24일 05:34:05에 스레드 ID 2110에서 실행되는 구성 요소 MSTP에 의해 생성된 시스템의 심각도 7(디버그)이 있는 사용자 수준 메시지(1)를 나타냅니다. 기음. 237번째 메시지가 기록되었습니다. syslog를 통해 수집기 또는 릴레이에 기록되는 메시지는 이전 메시지와 동일한 형식을 사용합니다.

- **Total number of Messages**: 메시지 로그의 경우 최신 200개 항목만 화면에 표시됩니다.

명령 로그 활성화 또는 비활성화

➢ **명령 로그를 활성화하거나 비활성화하려면:**

Monitoring > Logs > Command Log Configuration.



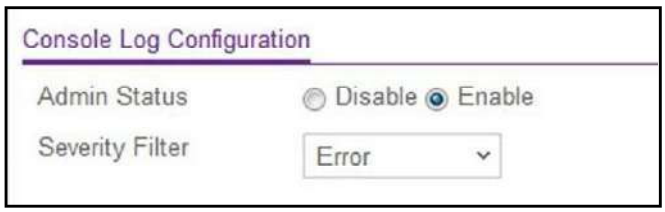
1. Admin Mode를 사용하면 해당 라디오 버튼을 선택하여 CLI 명령 로깅 작업을 Enable/Disable할 수 있습니다.

콘솔 로깅 활성화 또는 비활성화

이를 통해 호스트에 연결된 모든 직렬 장치에 로깅할 수 있습니다.

➢ **콘솔 로깅을 활성화하거나 비활성화하려면:**

Monitoring > Logs > Console Log Configuration.



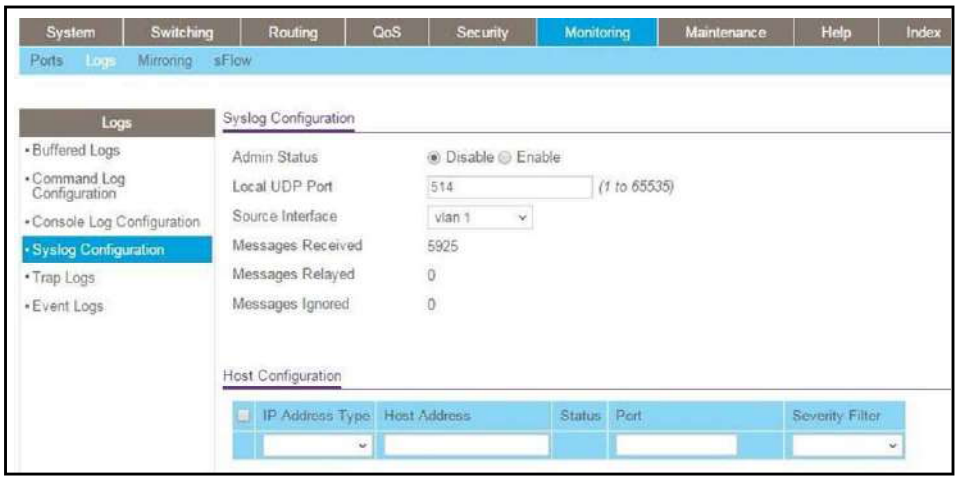
1. Admin Status의 Disable 또는 Enable 라디오 버튼을 선택합니다.

   비활성화된 로그는 메시지를 기록하지 않습니다.

Syslog 호스트 설정 구성

➢ **syslog를 구성하려면:**

Monitoring > Logs > Syslog Configuration.



Status 필드에는 호스트가 적극적으로 로깅하도록 구성되었는지 여부가 표시됩니다.

1. Admin Status의 Disable 또는 Enable 라디오 버튼을 선택합니다.
   구성된 syslog 호스트에 대한 로깅을 활성화하거나 비활성화합니다. 이를 비활성화로 설정하면 모든 syslog 호스트에 대한 로깅이 중지되므로 메시지가 수집기나 릴레이로 전송되지 않습니다.
   활성화는 각 수집기 또는 릴레이에 대해 구성된 값을 사용하여 구성된 수집기 또는 릴레이로 메시지가 전송됨을 의미합니다.

2. Local UDP Port를 사용하여 syslog 메시지가 전송되는 로컬 호스트의 포트를 지정합니다.
   기본 포트는 514입니다.

3. syslog에 사용할 소스 인터페이스를 지정합니다.
   가능한 값은 다음과 같습니다.
   - None
   - Routing interface
   - Routing VLAN
   - Routing loopback interface
   - Tunnel interface
   - Service port

   기본적으로 VLAN 1은 소스 인터페이스로 사용됩니다.

4. IP Address Type을 사용하여 호스트의 주소 유형을 지정합니다.
   다음 중 하나일 수 있습니다.
   - IPv4
   - IPv6
   - DNS

5. In the **Host Address** - 이는 syslog용으로 구성된 호스트의 주소입니다.

6. Port 필드에서 syslog 메시지가 전송되는 호스트의 포트를 지정합니다.

   기본 포트는 514입니다.

7. Severity Filter 목록에서 심각도 옵션을 선택합니다.

   로그는 구성된 심각도 임계값과 같거나 그 이상의 메시지를 기록합니다. 다음 심각도 수준을 사용할 수 있습니다.

   - **Emergency (0)**. 시스템을 사용할 수 없습니다.
   - **Alert (1)**. 즉시 조치를 취해야 합니다
   - **Critical (2)**. 중요한 조건
   - **Error (3)**. 오류 조건
   - **Warning (4)**. 경고 조건
   - **Notice (5)**. 정상이지만 중요한 상태
   - **Informational (6)**. 정보 메시지
   - **Debug (7)**. 디버그 수준 메시지

다음 표에서는 구성할 수 없는 데이터에 대해 설명합니다.

Table 242. Syslog 구성

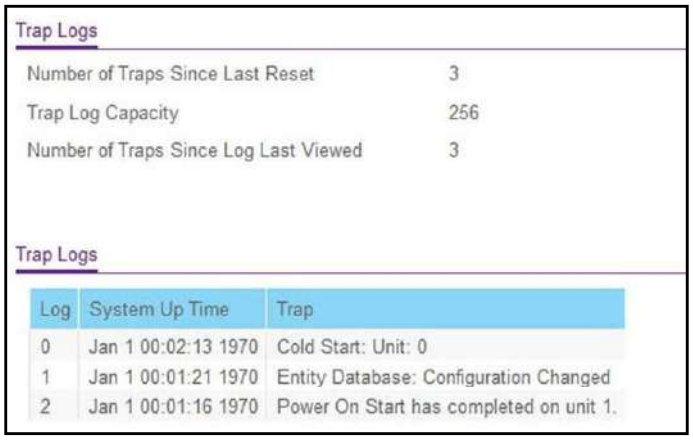
필드	설명
Messages Received	로그 프로세스에서 수신한 메시지 수입니다. 여기에는 삭제되거나 무시된 메시지가 포함됩니다.
Messages Relayed	릴레이된 syslog 메시지 수입니다.
Messages Ignored	무시된 syslog 메시지 수입니다.

트랩 로그 보기

트랩 로그의 항목을 볼 수 있습니다. 정보는 파일로 검색할 수 있습니다.

- **트랩 로그 보기:**

Monitoring > Logs > Trap Logs.



화면에는 전송된 트랩에 대한 정보도 표시됩니다.

모든 카운터를 지우려면 Clear 버튼을 클릭하세요. 그러면 트랩 로그에 대한 모든 통계가 기본값으로 재설정됩니다.

다음 표는 화면에 표시되는 트랩 로그 정보에 대해 설명합니다.

Table 243. 트랩 로그

필드	설명
Number of Traps Since Last Reset	스위치가 마지막으로 재부팅된 이후 발생한 트랩 수입니다.
Trap Log Capacity	로그에 저장된 최대 트랩 수입니다. 트랩 수가 용량을 초과하면 항목이 가장 오래된 항목을 덮어씁니다.

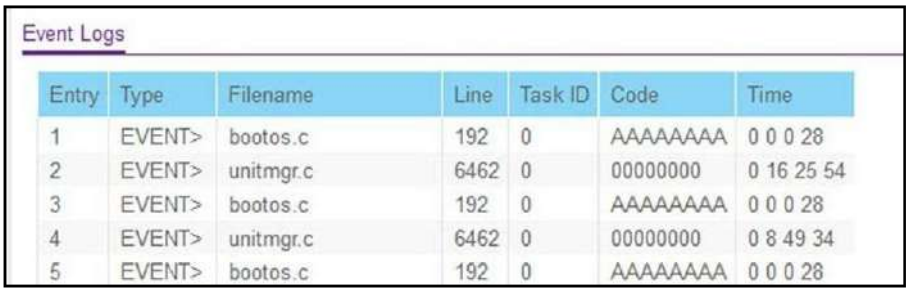
Number of Traps since log last viewed	트랩이 마지막으로 표시된 이후 발생한 트랩 수입니다. 어떤 방법(터미널 인터페이스 표시, 웹 표시, 스위치에서 파일 업로드 등)으로 트랩을 표시하면 이 카운터가 0으로 지워집니다.
Log	이 트랩의 시퀀스 번호입니다.
System Up Time	스위치를 마지막으로 재부팅한 이후 이 트랩이 발생한 시간으로, 일, 시간, 분, 초로 표시됩니다.
Trap	트랩을 식별하는 정보입니다.

이벤트 로그 보기

시스템의 오류 메시지가 포함된 이벤트 로그를 볼 수 있습니다. 시스템 재설정 시 이벤트 로그는 지워지지 않습니다.

➢ **To view the event log:**

Monitoring > Logs > Event Logs.



화면 하단에 있는 버튼을 사용하여 다음 작업을 수행합니다.

- 이벤트 로그에서 메시지를 지우려면 Clear 버튼을 클릭합니다.
- 스위치에 대한 최신 정보로 화면을 새로 고치려면 Refresh 버튼을 클릭하세요.

다음 표에서는 화면에 표시되는 이벤트 로그 정보에 대해 설명합니다.

Table 244. Event Logs

Field	Description
Entry	The sequence number of the event.
Type	The type of the event.
File Name	The file in which the event originated.

Line	The line number of the event.
Task Id	The task ID of the event.

Table 244. Event Logs

Field	Description
Code	The event code.
Time	The time this event occurred.

유지보수 8

이 장에서는 다음 주제를 다룹니다.

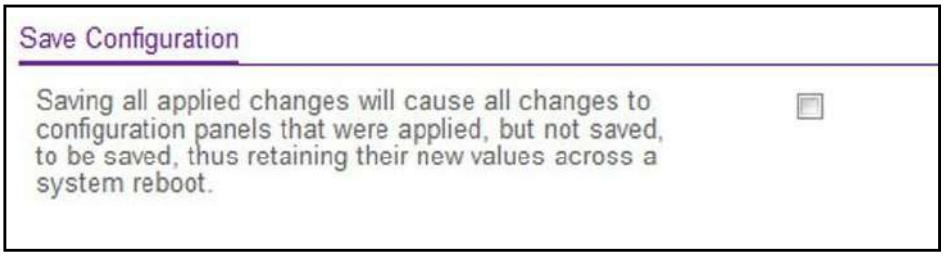
- *구성 저장*
- *자동 저장 모드 구성*
- *스위치 재부팅*
- *스위치 전원을 껐다 켜십시오.*
- *스위치를 공장 기본 설정으로 재설정*
- *모든 사용자 비밀번호를 기본 설정으로 재설정*
- *스위치에서 파일 업로드*
- *스위치에 파일 다운로드*
- *파일 관리*
- *문제 해결*

구성 저장

구성을 저장하면 스위치를 재부팅해도 변경 사항이 유지됩니다. 구성을 수동으로 저장하거나 자동 저장을 설정할 수 있습니다.

➢ **구성을 저장하려면:**

Maintenance > Save Config > Save Configuration.



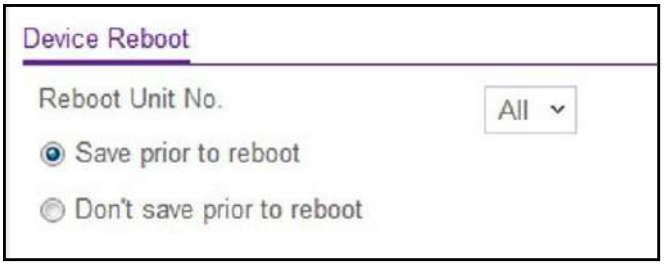
1. Check box을 선택합니다.
2. Apply 버튼을 클릭합니다

   구성 변경 사항은 시스템 재부팅 시 저장됩니다. 이전 저장 또는 시스템 재부팅 이후 제출된 모든 변경 사항은 스위치에 의해 유지됩니다.

스위치 재부팅

➢ **스위치를 재부팅하려면:**

Maintenance > Reset > Device Reboot.



1. Reboot Unit No. 필드에서 재설정할 장치를 선택합니다.

여러 장치가 섀시에 연결된 경우 All을 선택하여 스택의 모든 장치(즉, 전체 섀시)를 재설정하거나 장치 번호를 선택하여 특정 장치만 재설정합니다.

2. 라디오 버튼을 선택합니다:
   - **Save prior to reboot**. 현재 구성이 저장되고 스위치가 재부팅됩니다.
   - **Don't save prior to reboot**. 현재 구성을 저장하지 않고 스위치가 재부팅됩니다.
3. Apply 버튼을 클릭합니다

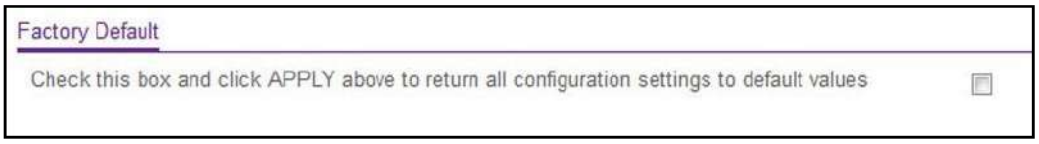
   저장 옵션을 선택한 경우 구성이 저장됩니다. 스위치가 재부팅됩니다.

스위치를 공장 기본 설정으로 재설정

Note: 스위치를 기본 구성으로 재설정하면 IP 주소가 192.168.10.12로 재설정되고 DHCP 클라이언트가 활성화됩니다.

➢ **스위치를 공장 기본 설정으로 재설정하려면:**

Maintenance > Reset > Factory Default.



Check box을 선택합니다.

1. Apply 버튼을 클릭합니다

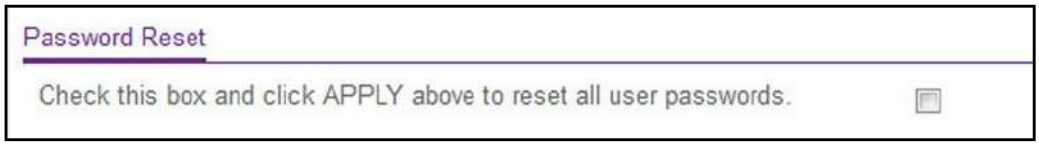
   확인 화면이 표시됩니다.
2. 예를 클릭하여 확인합니다.

   모든 구성 매개변수가 공장 기본값으로 재설정됩니다. 저장을 실행했더라도 변경한 내용은 모두 그대로 유지됩니다.

모든 사용자 비밀번호를 기본 설정으로 재설정

➢ **To reset all user passwords to their default settings:**

Maintenance > Reset > Password Reset.



1. Check box을 선택합니다.
2. Apply 버튼을 클릭합니다

   모든 사용자 비밀번호는 공장 기본값으로 재설정됩니다.

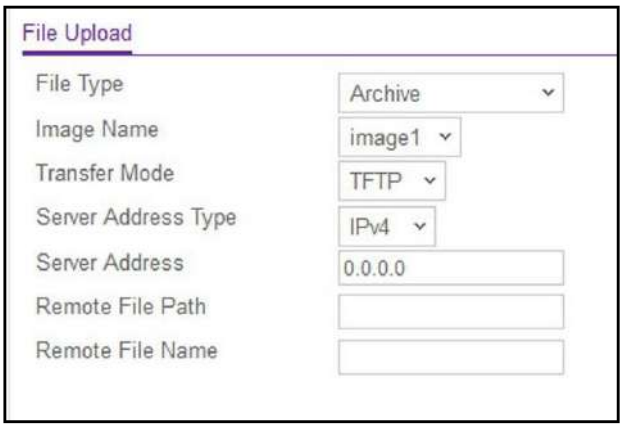
스위치에서 파일 업로드

스위치에서 TFTP 서버로 구성(ASCII), 로그(ASCII) 및 이미지(바이너리) 파일을 업로드할 수 있습니다.

TFTP 서버에 파일 업로드

➢ **스위치에서 TFTP 서버로 파일을 업로드하려면:**

Maintenance > **Upload** > **File Upload**.



1. 파일 유형을 사용하여 업로드할 파일 유형을 지정합니다.
   - **Archive**. 작동 중인 플래시에서 검색할 아카이브(STK) 코드를 지정합니다.
   - **CLI Banner**. CLI 배너 파일을 검색하려면 CLI 배너를 지정하십시오.
   - **Text Configuration**. 저장된 구성을 검색하려면 텍스트 모드에서 구성을 지정하세요.
   - **Script File**. 저장된 구성을 검색하려면 스크립트 파일을 지정하세요.
   - **Error Log**. 이벤트 로그라고도 하는 시스템 오류(지속) 로그를 검색하려면 오류 로그를 지정합니다.
   - **Trap Log**. 시스템 트랩 레코드를 검색하려면 트랩 로그를 지정하십시오.
   - **Buffered Log**. 시스템 버퍼링(메모리 내) 로그를 검색하려면 버퍼링 로그를 지정합니다.
   - **Tech Support**. 문제 해결에 필요한 스위치 정보를 검색하려면 기술 지원을 지정하십시오.
   - **Crash Logs**. 충돌 로그를 검색하려면 충돌 로그를 지정하세요.

   공장 기본값은 Archive입니다.

2. Image Name 필드는 선택한 파일 유형이 아카이브인 경우에만 표시됩니다.

   스위치 이미지(아카이브)를 업로드하는 경우 Image Name 목록을 사용하여 관리 시스템에 업로드할 스위치의 소프트웨어 이미지를 선택합니다.

   - **image1.** image1을 업로드하려면 image1을 선택하세요.
   - **image2**. image2를 업로드하려면 image2를 선택하세요.

3. Transfer Mode를 사용하여 파일 전송에 사용할 프로토콜을 지정합니다.
   - **TFTP**. Trivial File Transfer Protocol
   - **SFTP**. Secure File Transfer Protocol
   - **SCP**. Secure Copy Protocol
   - **FTP**. File Transfer Protocol

4. Server Address Type 사용하여 IPv4, IPv6 또는 DNS를 지정하여 서버 주소 필드의 형식을 나타냅니다. 공장 기본값은 IPv4입니다.
5. Server Address를 이용하여 시어 주소 유형에 표시된 형식에 맞춰 서버의 IP 주소를 입력합니다.

   공장 기본값은 IPv4 주소 0.0.0.0입니다.
6. Remote File Path를 사용하여 파일을 업로드할 경로를 입력하세요.

   파일 경로에는 알파벳, 숫자, 슬래시, 점 또는 밑줄 문자만 포함될 수 있습니다. 최대 160자까지 입력할 수 있습니다. 공장 기본값은 공백입니다.
7. Remote File Name을 사용하여 서버에서 다운로드할 파일 이름을 입력합니다. 최대 32자까지 입력할 수 있습니다.

   공장 기본값은 공백입니다.
8. Local File Name을 사용하여 업로드할 로컬 스크립트 파일 이름을 지정합니다.

   이 필드는 파일 유형이 스크립트 파일인 경우에만 표시됩니다.
9. User Name을 사용하여 파일이 전송되는 SFTP/SCP 서버에 원격 로그인하기 위한 사용자 이름을 입력합니다.

   이 필드는 SFTP 또는 SCP 전송 모드를 선택한 경우에만 표시됩니다.
10. Password를 사용하여 파일이 전송되는 SFTP/SCP 서버에 원격 로그인하기 위한 비밀번호를 입력합니다.

    이 필드는 SFTP 또는 SCP 전송 모드를 선택한 경우에만 표시됩니다.

테이블의 마지막 행은 파일 전송 진행 상황에 대한 정보를 표시하는 데 사용됩니다.

HTTP 파일 업로드

➢ **HTTP 파일 업로드를 사용하려면:**

Maintenance > Upload > HTTP File Upload.

1. File Type을 사용하여 업로드할 파일 유형을 지정합니다.
   - **Archive**. 작동 중인 플래시에서 검색할 아카이브(STK) 코드를 지정합니다.
   - **Image Name**. 목록에서 이미지 중 하나를 선택하십시오.
     - **Image1**. 검색할 코드 image1을 지정합니다.
     - **Image2**. 검색할 코드 image2를 지정합니다.
   - **CLI Banner**. CLI 배너 파일을 검색하려면 CLI 배너를 지정하십시오.
   - **Text Configuration**. 저장된 구성을 검색하려면 텍스트 모드에서 구성을 지정하세요.
   - **Script File**. 저장된 구성을 검색하려면 스크립트 파일을 지정하세요.
   - **Error Log**. 이벤트 로그라고도 하는 시스템 오류(지속) 로그를 검색하려면 오류 로그를 지정합니다.
   - **Trap Log**. 시스템 트랩 레코드를 검색하려면 트랩 로그를 지정하십시오.
   - **Buffered Log**. 시스템 버퍼링(메모리 내) 로그를 검색하려면 버퍼링 로그를 지정합니다.
   - **Tech Support.** 문제 해결에 필요한 스위치 정보를 검색하려면 기술 지원을 지정하십시오.
   - **Crash Logs**. 시스템 충돌 로그를 검색하려면 충돌 로그를 지정하십시오.

   공장 기본값은 Archive입니다.
2. Local File Name을 사용하여 업로드할 로컬 스크립트 파일 이름을 지정합니다.

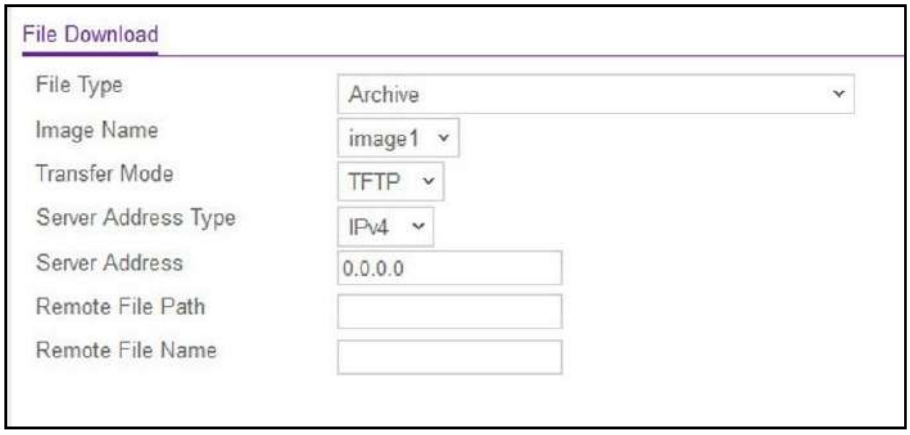
스위치에 파일 다운로드

스위치는 TFTP 또는 HTTP를 사용하여 원격 시스템에서 스위치로의 시스템 파일 다운로드를 지원합니다.

파일 다운로드

➢ **파일을 다운로드하려면:**

Maintenance > File Export > File Export.



1. File Type을 사용하여 전송할 파일 유형을 지정합니다.
   - **Archive**. 작동 가능한 플래시를 업그레이드하기 위한 아카이브(STK) 코드입니다.
   - **Text Configuration**. 스위치 구성을 업데이트하기 위한 텍스트 모드의 구성입니다. 파일에 오류가 있으면 업데이트가 중지됩니다.
   - **SSH-1 RSA Key File**. SSH-1 RSA(Rivest-Shamir-Adelman) 키 파일.
   - **SSH-2 RSA Key PEM File**. SSH-2 RSA(Rivest-Shamir-Adelman) 키 파일(PEM 인코딩).
   - **SSH-2 DSA Key PEM File**. SSH-2 디지털 서명 알고리즘(DSA) 키 파일(PEM 인코딩).
   - SSL Trusted Root Cetificate FEM File을 사용하여 SSL 신뢰할 수 있는 루트 인증서 파일(PEM 인코딩)을 지정합니다.
   - SSL Server Certificate PEM File을 사용하여 SSL 서버 인증서 파일(PEM 인코딩)을 지정합니다.
   - SSL DH Weak Encryption Parameter PEM File을 사용하여 SSL Diffie-Hellman 약한 암호화 매개변수 파일(PEM 인코딩)을 지정합니다.
   - SSL DH Strong Encryption PEM File을 사용하여 SSL Diffie-Hellman 강력한 암호화 매개변수 파일(PEM 인코딩)을 지정합니다.
   - Script File을 사용하여 스크립트 구성 파일을 지정합니다.
   - **CLI Banner**. 로그인 프롬프트 전에 배너를 표시하려면 CLI Banner를 지정하십시오.

- IAS Users를 사용하여 내부 인증 서버 사용자 데이터베이스 파일을 지정합니다.

공장 기본값은 Archive입니다.

Note: SSH 키 파일을 다운로드하려면 SSH를 관리적으로 비활성화해야 하며 활성 SSH 세션이 없어야 합니다.

Note: SSL PEM 파일을 다운로드하려면 관리상 SSL을 비활성화해야 하며 활성 SSH 세션이 없어야 합니다.

Image Name 필드는 파일 유형 아카이브를 선택한 경우에만 표시됩니다.

2. Image Name을 사용하여 목록에서 이미지 중 하나를 선택합니다.
   - **Image1**. 검색할 코드 image1을 지정합니다.
   - **Image2**. 검색할 코드 image2를 지정합니다.
3. Transfer Mode를 사용하여 파일 전송에 사용할 프로토콜을 지정합니다.
   - **TFTP**. Trivial File Transfer Protocol
   - **SFTP**. Secure File Transfer Protocol
   - **SCP**. Secure Copy Protocol
   - **FTP**. File Transfer Protocol
4. Server Address Type을 사용하여 IPv4, IPv6 또는 DNS를 지정하여 TFTP/SFTP/SCP 서버 주소 필드의 형식을 나타냅니다.

   공장 기본값은 IPv4입니다.
5. Server Address를 사용하여 서버 주소 유형에 표시된 형식(예: x.x.x.x 형식의 IP 주소)에 따라 TFTP 서버의 IP 주소를 입력합니다.

   공장 기본값은 IPv4 주소 0.0.0.0입니다.
6. Remote File Path를 이용하여 다운로드할 파일의 경로를 입력하세요.

   파일 경로에는 다음 기호를 포함할 수 없습니다: ' \:*?”<>| '. 최대 160자까지 입력할 수 있습니다. 공장 기본값은 공백입니다.
7. Remote File Name을 사용하여 서버에서 다운로드할 파일 이름을 입력합니다.

   파일 경로에는 다음 기호를 포함할 수 없습니다: ' \:*?”<>| '. 최대 32자까지 입력할 수

있습니다. 공장 기본값은 공백입니다.

8. 사용자 이름을 사용하여 파일이 있는 SFTP/SCP 서버에 원격 로그인하기 위한 사용자 이름을 입력합니다.

   이 필드는 SFTP 또는 SCP 전송 모드를 선택한 경우에만 표시됩니다.

9. Password를 사용하여 파일이 있는 SFTP/SCP 서버에 원격 로그인하기 위한 비밀번호를 입력합니다.

   이 필드는 SFTP 또는 SCP 전송 모드를 선택한 경우에만 표시됩니다.

   테이블의 마지막 행에는 파일 전송 진행률에 대한 정보가 표시됩니다. 프로세스가 시작된 후에만 표시됩니다. 파일 전송이 완료될 때까지 화면이 자동으로 새로 고쳐집니다.

10. Apply 버튼을 클릭합니다

    업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

HTTP를 사용하여 스위치에 파일 다운로드

HTTP 세션을 사용하여(예: 웹 브라우저를 통해) 다양한 유형의 파일을 스위치에 다운로드할 수 있습니다.

➢ **HTTP를 사용하여 스위치에 파일을 다운로드하려면:**

Maintenance > File Export> HTTP File Export.

1. File Type을 사용하여 전송할 파일 유형을 지정합니다.
   - **Archive**. 작동 가능한 플래시를 업그레이드하기 위한 아카이브(STK) 코드입니다.
   - Image Name 필드는 파일 유형 보관을 선택한 경우에만 표시됩니다.

     Image Name을 사용하여 목록에서 이미지 중 하나를 선택하세요.
     - **Image1**. 다운로드할 코드 image1을 지정합니다.
     - **Image2**. 다운로드할 코드 image2를 지정합니다.
   - **Text Configuration**. 구성은 스위치 구성을 업데이트하기 위한 텍스트 모드입니다. 파일에 오류가 있으면 업데이트가 중지됩니다.
   - SSH-1 RSA Key File을 사용하여 SSH-1 RSA(Rivest-Shamir-Adelman) 키 파일을 지정합니다.
   - SSH-2 RSA Key PEM File을 사용하여 SSH-2 RSA(Rivest-Shamir-Adelman) 키 파일(PEM 인코딩)을 지정합니다.
   - SSH-2 DSA Key PEM File을 사용하여 SSH-2 디지털 서명 알고리즘(DSA) 키 파일(PEM 인코딩)을 지정합니다.
   - SSL Trusted Root Certificate PEM File을 사용하여 SSL 신뢰할 수 있는 루트 인증서 파일(PEM 인코딩)을 지정합니다.
   - SSL Server Certificate PEM File을 사용하여 SSL 서버 인증서 파일(PEM 인코딩)을 지정합니다.
   - SSL DH Seak Encryption Parameter PEM File을 사용하여 SSL Diffie-Hellman 약한 암호화 매개변수 파일(PEM 인코딩)을 지정합니다.
   - SSL DH Strong Encryption Parameter PEM File을 사용하여 SSL Diffie-Hellman 강력한 암호화 매개변수 파일(PEM 인코딩)을 지정합니다.
   - Config Script를 사용하여 스크립트 구성 파일을 지정합니다.
   - **CLI Banner**. 로그인 프롬프트 전에 배너가 표시될 경우 CLI Banner를 지정하십시오.
   - IAS Users를 사용하여 내부 인증 서버 사용자 데이터베이스 파일을 지정합니다.

   공장 기본값은 Archive입니다.

   Note: SSH 키 파일을 다운로드하려면 SSH를 관리적으로 비활성화해야 하며 활성 SSH 세션이 없어야 합니다.

   Note: SSL PEM 파일을 다운로드하려면 관리상 SSL을 비활성화해야 하며 활성 SSH 세션이 없어야 합니다.

2. Select File을 사용하여 다운로드할 파일의 경로와 함께 이름을 찾아 입력합니다.
   최대 80자까지 입력할 수 있습니다. 공장 기본값은 공백입니다.

3. 찾아보기를 클릭하여 다운로드할 파일을 찾습니다.
   공장 기본값은 공백입니다.

4. Apply 버튼을 클릭합니다
   다운로드가 시작됩니다.
   다운로드 Status 필드는 파일을 스위치로 전송하는 동안의 상태를 표시합니다.

Note: 파일 전송이 시작된 후 화면이 새로 고쳐질 때까지 기다리세요.
화면이 새로 고쳐지면 파일 선택 옵션이 숨겨집니다. 이는 파일 전송이 완료되었음을 나타냅니다.

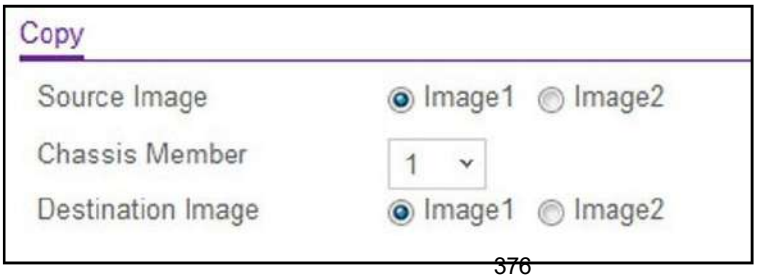
파일 관리

시스템은 영구 저장 장치에 두 가지 버전의 소프트웨어를 유지합니다. 한 이미지는 활성 이미지이고 두 번째 이미지는 백업 이미지입니다. 이후 스위치를 다시 시작하는 동안 활성 이미지가 로드됩니다. 이 기능은 소프트웨어를 업그레이드하거나 다운그레이드할 때 스위치를 끄는 시간을 줄여줍니다.

이미지 복사

➢ **이미지를 복사하려면:**

Maintenance > File Management > Copy.



1. Source Image를 사용하여 이미지1 또는 이미지2를 원본 이미지(복사할 이미지)로 선택합니다.
2. Chassis Member를 사용하여 슈퍼바이저에서 복사할 대상 장치를 선택합니다.
3. Destination Image를 사용하여 image1 또는 image2를 대상 이미지로 선택합니다.
4. Apply 버튼을 클릭합니다

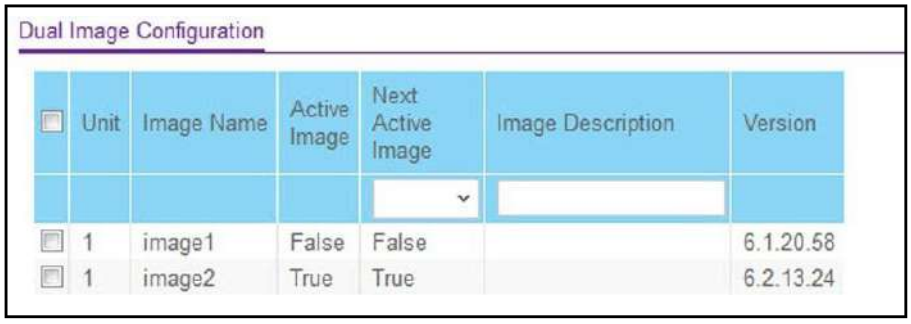
   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

듀얼 이미지 설정 구성

듀얼 이미지 기능을 사용하면 스위치가 두 개의 이미지를 영구 저장 장치에 보관할 수 있습니다. 관리자는 이후 스위치를 다시 시작할 때 로드할 활성 이미지로 image1 또는 image2를 지정할 수 있습니다. 이 기능은 소프트웨어 이미지를 업그레이드하거나 다운그레이드할 때 스위치 다운 시간을 줄여줍니다.

➢ **듀얼 이미지 설정을 구성하려면:**

Maintenance > File Management > Dual Image Configuration.



1. Unit을 사용하여 코드 이미지를 활성화, 업데이트 또는 삭제할 유닛 ID를 선택합니다.
2. Next Active Image를 사용하여 선택한 이미지를 이 장치의 후속 재부팅을 위한 다음 활성 이미지로 만듭니다.
3. Image Description을 사용하여 선택한 이미지에 대한 설명을 지정합니다.
4. Delete 버튼을 클릭하면 스위치의 영구 저장 장치에서 선택한 이미지가 삭제됩니다.
5. Apply 버튼을 클릭합니다

   업데이트된 구성이 스위치로 전송됩니다. 구성 변경 사항은 즉시 적용됩니다.

Note: 이미지를 활성화한 후 스위치의 시스템 재설정을 수행하여 새 코드를 실행해야 합니다.

다음 표에서는 화면에 표시되는 구성할 수 없는 정보에 대해 설명합니다.

Table 247. 듀얼 이미지 구성

필드	설명
Image Name	선택한 장치의 이미지 이름이 표시됩니다.
Active Image	선택한 장치의 현재 활성 이미지입니다.
Version	image1 코드 파일의 버전입니다.

문제 해결

Ping 또는 Traceroute를 사용할 수 있으며 메모리 덤프를 수행할 수 있습니다.

Ping IPv4

스위치에 지정된 IP 주소로 ping 요청을 보내도록 지시할 수 있습니다. 스위치가 특정 IP 스테이션과 통신할 수 있는지 확인할 수 있습니다. Apply 버튼을 클릭하면 스위치가 지정된 수의 ping 요청을 보내고 결과가 표시됩니다.

핑에 대한 응답이 수신되지 않으면 다음 메시지가 표시됩니다.

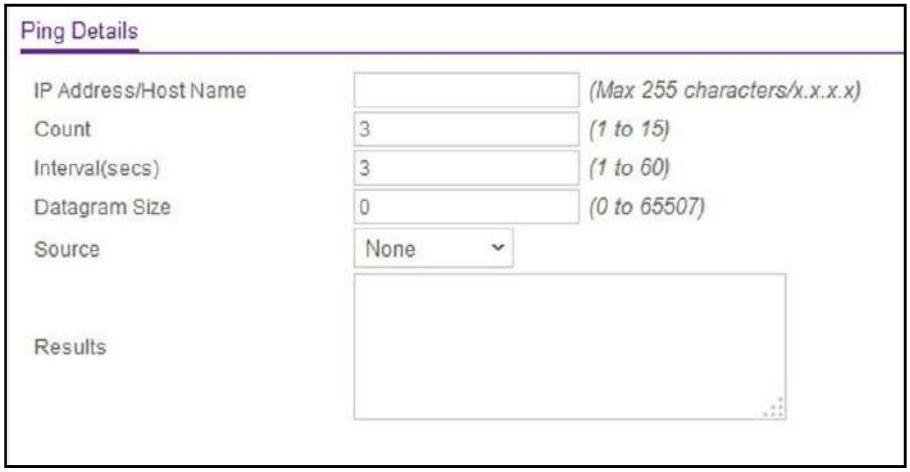
```
Tx = Count, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec
```

If a reply to the ping is received, the following message displays:

```
Reply From a.b.c.d: icmp_seq = 0. time= xyz usec.
Reply From a.b.c.d: icmp_seq = 1. time= abc usec.
Reply From a.b.c.d: icmp_seq = 2. time= def usec.
Tx = count, Rx = count Min/Max/Avg RTT = xyz/abc/def msec
```

➢ **설정을 구성하고 네트워크의 호스트를 핑하려면:**

Maintenance > Troubleshooting > Ping IPv4.



1. IP Address/Host Name을 사용하여 ping할 스위치에 대한 스테이션의 IP 주소 또는 호스트 이름을 입력합니다.

   초기값은 비어 있습니다.

2. 개수 필드에 보낼 에코 요청 수를 입력합니다.

   기본값은 3입니다. 범위는 1~15입니다.

3. ping 패킷 사이의 간격을 초 단위로 입력합니다.

   기본값은 3초입니다. 범위는 1~60입니다.

4. 핑 패킷의 Datagram Size를 입력합니다.

   기본값은 0바이트입니다. 범위는 0~65507입니다.

5. 에코 요청 패킷을 보낼 때 사용할 Source IP Address 또는 Interface를 입력합니다.

   소스가 필요하지 않은 경우 소스 옵션으로 None을 선택하세요. 가능한 값은 다음과 같습니다.

   - **None**. ping 패킷의 소스 주소는 기본 발신 인터페이스의 주소입니다.
   - **IP Address**. 에코 요청 패킷을 보낼 때 사용할 소스 IP 주소입니다. 이 필드는 소스 옵션으로 IP 주소를 선택한 경우 표시됩니다.
   - **Interface**. 에코 요청 패킷을 보낼 때 사용할 인터페이스입니다. 이 필드는 인터페이스가 소스 옵션으로 선택된 경우 표시됩니다.

   Note: 이 화면의 필드에 구성된 값은 스위치에 저장되지 않습니다. 결과적으로 화면을 새로 고치면 이러한 필드가 기본값으로 설정됩니다.

6. Apply 버튼을 클릭합니다

핑은 지정된 주소로 전송됩니다. 스위치는 Count 필드에 지정된 수의 핑을 전송하고 결과는 결과 영역의 구성 가능한 데이터 아래에 표시됩니다.

화면에서 작업을 취소하고 화면의 데이터를 스위치의 최신 값으로 재설정하려면 Cancel 버튼을 클릭하세요.

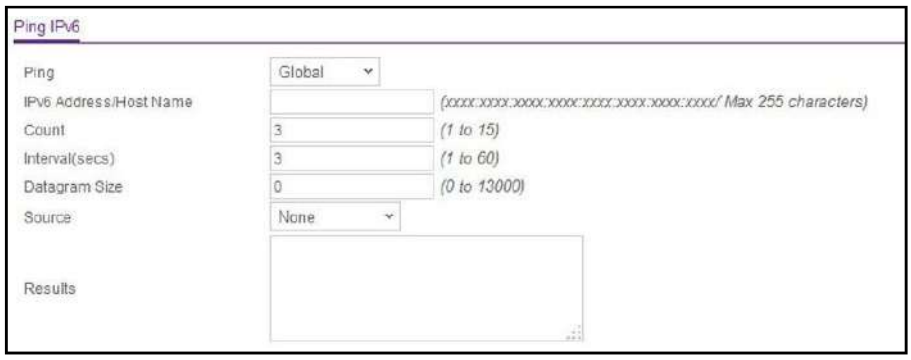
Ping IPv6

이 화면은 지정된 호스트 이름이나 IPv6 주소로 ping 요청을 보내는 데 사용됩니다. 이를 사용하여 스위치가 특정 IPv6 스테이션과 통신할 수 있는지 확인할 수 있습니다. Apply 버튼을 클릭하면 스위치는 지정된 수의 ping 요청을 보내고 결과는 구성 가능한 데이터 아래에 표시됩니다. 출력에는 다음이 표시됩니다.

```
Send count=n, Receive count=n from (IPv6 Address). Average round trip time
= n ms.
```

➢ **Ping IPv6를 사용하려면:**

Maintenance > Troubleshooting > Ping IPv6.



1. 목록에서 Ping 유형을 선택합니다.

   가능한 값은 다음과 같습니다.

   - **Global**. 글로벌 IPv6 주소를 ping합니다.
   - **Link Local**. 지정된 인터페이스를 통해 링크-로컬 IPv6 주소를 ping합니다. 이 필드는 ping 옵션으로 인터페이스를 선택한 경우 표시됩니다.

2. IPv6 Address/Host Name을 사용하여 ping할 스위치에 대한 스테이션의 IPv6 주소 또는 호스트 이름을 입력합니다.

   초기값은 비어 있습니다. 형식은 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx입니다. 최대

문자 수는 255자입니다.

3. Count를 사용하여 전송되는 에코 요청 수를 입력합니다.

   범위는 1~15입니다. 기본값은 3입니다.

4. 핑 패킷 사이의 간격(초)을 입력합니다.

   범위는 1~60입니다. 기본값은 3입니다.

5. Datagram Size를 사용하여 데이터그램 크기를 입력합니다.

   유효한 범위는 0~13000입니다. 기본값은 0바이트입니다.

6. 에코 요청 패킷을 보낼 때 사용할 Source IP Address 또는 Interface를 입력합니다.

   소스가 필요하지 않은 경우 소스 옵션으로 없음을 선택하세요. 가능한 값은 다음과 같습니다.

   - **None**. ping 패킷의 소스 주소는 기본 발신 인터페이스의 주소입니다.
   - **IPv6 Address**. 에코 요청 패킷을 보낼 때 사용할 소스 IPv6 주소입니다. 이 필드는 IPv6 주소가 소스 옵션으로 선택된 경우 표시됩니다.
   - **Interface**. 에코 요청 패킷을 보낼 때 사용할 인터페이스입니다. 이 필드는 인터페이스가 소스 옵션으로 선택된 경우 표시됩니다.

   Note: 이 화면의 필드에 구성된 값은 스위치에 저장되지 않습니다. 결과적으로 화면을 새로 고치면 이러한 필드가 기본값으로 설정됩니다.

7. Apply 버튼을 클릭합니다

   Ping은 지정된 IPv6 주소 또는 호스트 이름으로 전송됩니다. 스위치는 Count 필드에 지정된 수의 핑을 전송하고 결과는 결과 영역의 구성 가능한 데이터 아래에 표시됩니다.

Traceroute IPv4

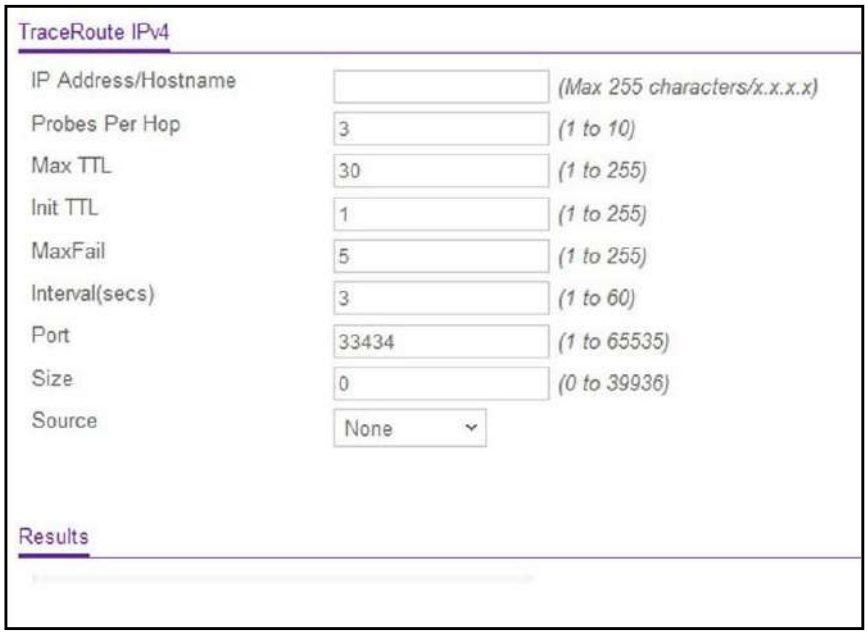
이 화면을 사용하여 스위치가 지정된 IP 주소 또는 호스트 이름으로 경로 추적 요청을 보내도록 지시합니다. 이를 사용하여 패킷이 원격 대상으로 이동하는 경로를 검색할 수 있습니다. 적용 버튼을 클릭하면 스위치가 경로 추적을 전송하고 결과가 구성 가능한 데이터 아래에 표시됩니다.

Traceroute에 대한 응답이 수신되면 다음 메시지가 표시됩니다.

```
1 e.f.g.h 9869 usec 9775 usec 10584 usec
2 0.0.0.0 0 usec * 0 usec * 0 usec *
3 0.0.0.0 0 usec * 0 usec * 0 usec *
Hop Count = j Last TTL = k Test attempt = m Test Success = n.
```

- **경로 추적 설정을 구성하고 프로브 패킷을 보내 네트워크의 호스트에 대한 경로를 검색하려면:**

  Maintenance > Troubleshooting > Traceroute IPv4.



1. IP Address/Host Name을 사용하여 경로를 검색하려는 스테이션의 IP 주소 또는 호스트 이름을 입력합니다.

   기본값은 공백입니다.

2. Probes Per Hop를 입력합니다.

   기본값은 3입니다. 범위는 1~10입니다.

3. 대상의 Max TTL을 입력합니다.

   기본값은 30입니다. 범위는 1~255입니다.

4. 사용할 Initial TTL을 입력합니다.

   기본값은 1입니다. 범위는 1~255입니다.

5. 세션에 허용되는 Max Failures를 입력합니다.

   기본값은 5입니다. 범위는 1~255입니다.

6. Interval (secs). 프로브 사이의 시간을 초 단위로 입력합니다.

기본값은 3입니다. 범위는 1~60입니다.

7. 프로브 패킷에 UDP 대상 Port를 입력합니다.

   기본값은 33434입니다. 범위는 1~65535입니다.

8. 프로브 패킷의 Size를 입력합니다.

   기본값은 0입니다. 범위는 0~39936입니다.

9. 에코 요청 패킷을 보낼 때 사용할 Source IP Address 또는 Interface를 입력합니다.

   소스가 필요하지 않은 경우 소스 옵션으로 None을 선택하세요. 가능한 값은 다음과 같습니다.

   - **None**. ping 패킷의 소스 주소는 기본 발신 인터페이스의 주소입니다.
   - **IP Address**. 에코 요청 패킷을 보낼 때 사용할 소스 IP 주소입니다. 이 필드는 소스 옵션으로 IP 주소를 선택한 경우 표시됩니다.
   - **Interface**. 에코 요청 패킷을 보낼 때 사용할 인터페이스입니다. 이 필드는 인터페이스가 소스 옵션으로 선택된 경우 표시됩니다.

   Note: 이 화면의 필드에 구성된 값은 스위치에 저장되지 않습니다. 결과적으로 화면을 새로 고치면 이러한 필드가 기본값으로 설정됩니다.

10. Apply 버튼을 클릭합니다

    Traceroute 요청은 지정된 IP 주소 또는 호스트 이름으로 전송됩니다. 결과는 TraceRoute 결과 영역의 구성 가능한 데이터 아래에 표시됩니다.

    결과 필드에는 스위치가 지정된 IP 주소 또는 호스트 이름으로 경로 추적 요청을 보낸 후 경로 추적 IPv4 결과가 표시됩니다.

Traceroute IPv6

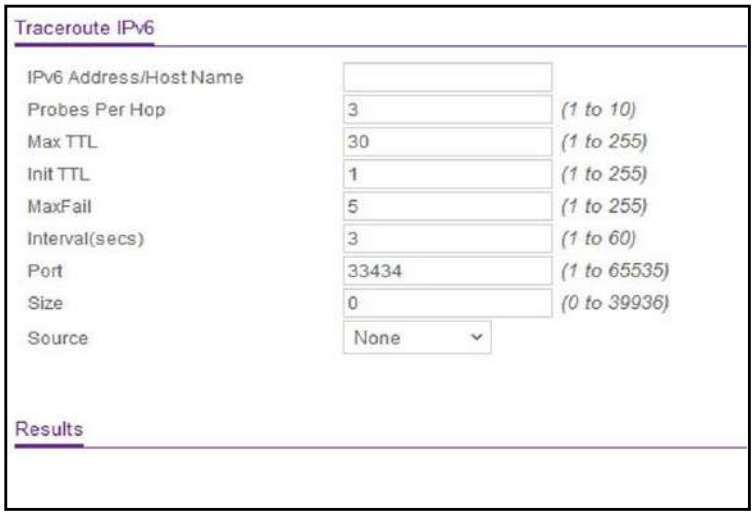
이 화면을 사용하여 스위치가 지정된 IPv6 주소 또는 호스트 이름으로 경로 추적 요청을 보내도록 지시합니다. 이를 사용하여 패킷이 원격 대상으로 이동하는 경로를 검색할 수 있습니다. 적용 버튼을 클릭하면 스위치가 경로 추적을 전송하고 결과가 구성 가능한 데이터 아래에 표시됩니다.

Traceroute에 대한 응답이 수신되면 다음 메시지가 표시됩니다.

```
1 a:b:c:d:e:f:g 9869 usec 9775 usec 10584 usec
2 0:0:0:0:0:0:0:0 0 usec * 0 usec * 0 usec *
Hop Count = p Last TTL = q Test attempt = r Test Success = s.
```

- **추적 경로 IPv6를 사용하려면:**

  Maintenance > **Troubleshooting** > **Traceroute IPv6**.



1. IPv6 Address/Host Name 필드에 스위치가 경로를 검색할 스테이션의 IPv6 주소 또는 호스트 이름을 입력합니다.

   초기값은 비어 있습니다. 입력한 IPv6 주소 또는 호스트 이름은 전원을 껐다 켜도 유지되지 않습니다.

2. Probe Per Hop를 입력합니다.

   기본값은 3입니다. 범위는 1~10입니다.

3. 대상의 Maximum TTL을 입력합니다.

   기본값은 30입니다. 범위는 1~255입니다. 입력한 MaxTTL은 전원을 껐다 켜도 유지되지 않습니다.

4. 사용할 Initial TTL을 입력합니다.

   기본값은 1입니다. 범위는 1~255입니다. 입력한 InitTTL은 전원을 껐다 켜도 유지되지 않습니다.

5. 세션에 허용되는 Maximum Failures를 입력합니다.

   기본값은 5입니다. 범위는 1~255입니다. 입력한 MaxFail은 전원을 껐다 켜도 유지되지 않습니다.

6. **Interval (secs)** - 프로브 사이의 시간을 초 단위로 입력합니다.

   기본값은 3입니다. 범위는 1~60입니다. 입력한 간격은 전원을 껐다 켜도 유지되지 않습니다.

7. 프로브 패킷에 UDP 대상 Port를 입력합니다.

   기본값은 33434입니다. 범위는 1~65535입니다. 입력한 포트는 전원을 껐다 켜도 유지되지 않습니다.

8. 프로브 패킷의 Size를 입력합니다.

   기본값은 0입니다. 범위는 0~39936입니다. 입력한 크기는 전원을 껐다 켜도 유지되지 않습니다.

9. 에코 요청 패킷을 보낼 때 사용할 Source IP Address 또는 Interface를 입력합니다.

   소스가 필요하지 않은 경우 소스 옵션으로 None을 선택하세요. 가능한 값은 다음과 같습니다.

   - **None**. ping 패킷의 소스 주소는 기본 발신 인터페이스의 주소입니다.
   - **IP Address**. 에코 요청 패킷을 보낼 때 사용할 소스 IP 주소입니다. 이 필드는 소스 옵션으로 IP 주소를 선택한 경우 표시됩니다.
   - **Interface**. 에코 요청 패킷을 보낼 때 사용할 인터페이스입니다. 이 필드는 인터페이스가 소스 옵션으로 선택된 경우 표시됩니다.

   Note: 이 화면의 필드에 구성된 값은 스위치에 저장되지 않습니다. 결과적으로 화면을 새로 고치면 이러한 필드가 기본값으로 설정됩니다.

10. Apply 버튼을 클릭합니다

    추적 경로가 시작됩니다. 결과는 TraceRoute 영역에 표시됩니다.

    결과 필드에는 스위치가 지정된 IP 주소 또는 호스트 이름으로 경로 추적 요청을 보낸 후 경로 추적 IPv6 결과가 표시됩니다.

기본 설정 A

이 부록에서는 다양한 관리 스위치 소프트웨어 기능의 기본 설정을 설명합니다.

Table 248. 기본 설정

필드	기본값
IP address	192.168.10.12
Subnet mask	255.255.0.0
Default gateway	0.0.0.0
Protocol	DHCP
Management VLAN ID	1
Minimum password length	Eight characters
IPv6 management Mode	None
SNTP client	Enabled
SNTP server	Not configured
Global logging	Enabled
CLI command logging	Disabled
Console logging	Enabled (Severity level: debug and above)
RAM logging	Enabled (Severity level: debug and above)
Persistent (FLASH) logging	Disabled
DNS	Enabled (No servers configured)
SNMP	Enabled (SNMPv1/SNMPv2, SNMPv3)
SNMP Traps	Enabled
Auto Install	Enabled
Auto Save	Disabled
sFlow	Enabled
ISDP	Enabled (Versions 1 and 2)
RMON	Enabled
TACACS	Not configured
RADIUS	Not configured

SSH/SSL	Disabled
Telnet	Enabled
Denial of Service Protection	Disabled
Captive Portal	Disabled
Dot1x Authentication (IEEE 802.1X)	Disabled
MAC-based port security	All ports are unlocked
Access control lists (ACL)	None configured
IP source guard (IPSG)	Disabled
DHCP snooping	Disabled
Dynamic ARP inspection	Disabled
Protected ports	None
Private groups	None
Flow control support (IEEE 802.3x)	Disabled
Head of line blocking prevention	Disabled
Maximum frame size	1518 bytes
Auto-MDI/MDIX support	Enabled
Auto-negotiation	Enabled
Advertised port speed	Maximum Capacity
Broadcast storm control	Enabled
Port mirroring	Disabled
LLDP	Enabled
LLDP-MED	Enabled
MAC table address aging	300 seconds (dynamic addresses)
DHCP Layer 2 relay	Disabled
Default VLAN ID	1
Default VLAN name	Default
GVRP	Disabled
GARP timers	Leave: 60 centiseconds Leave All: 1000 centiseconds Join: 20 centiseconds
Voice VLAN	Disabled
Guest VLAN	Disabled
RADIUS-assigned VLANs	Disabled
Double VLANs	Disabled
Spanning Tree Protocol (STP)	Enabled
STP operation mode	IEEE 802.1s RSTP

Optional STP features	Disabled
STP bridge priority	32768
Multiple Spanning Tree	Disabled
Link aggregation	No Link Aggregation Groups (LAGs) configured
LACP system priority	1
Routing mode	Disabled
IP helper and UDP relay	Disabled
Tunnel and loopback interfaces	None
DiffServ	Enabled
Auto VoIP	Disabled
Auto VoIP traffic class	6
MLD snooping	Disabled
IGMP snooping	Disabled
IGMP snooping querier	Disabled
GMRP	Disabled

구성 예

B

이 부록에는 다음 기능을 구성하는 방법에 대한 정보가 포함되어 있습니다.

- *VLAN(가상 근거리 통신망)*
- *액세스 제어 목록(ACL)*
- *차별화된 서비스(DiffServ)*
- *802.1X*
- *MSTP*

VLAN(가상 근거리 통신망)

LAN(Local Area Network)은 일반적으로 브로드캐스트 도메인으로 정의될 수 있습니다. 동일한 물리적 세그먼트에 있는 허브, 브리지 또는 스위치는 모든 최종 노드 장치를 연결합니다. 엔드 노드는 라우터 없이도 서로 통신할 수 있습니다. 라우터는 LAN을 함께 연결하여 트래픽을 적절한 포트로 라우팅합니다.

가상 LAN(VLAN)은 지리적 위치 이외의 기준(예: 부서, 사용자 유형 또는 기본 응용 프로그램 기준)으로 워크스테이션을 매핑하는 정의가 있는 근거리 통신망입니다. VLAN 간에 트래픽이 흐르도록 하려면 마치 VLAN이 두 개의 별도 LAN에 있는 것처럼 트래픽이 라우터를 통과해야 합니다.

VLAN은 단일 네트워크 세그먼트에 연결되어 있지 않더라도 마치 단일 네트워크 세그먼트에 연결된 것처럼 동작하는 PC, 서버 및 기타 네트워크 리소스의 그룹입니다. 예를 들어 모든 마케팅 담당자가 건물 전체에 분산되어 있을 수 있습니다. 하지만 모두 단일 VLAN에 할당되면 마치 동일한 세그먼트에 연결된 것처럼 리소스와 대역폭을 공유할 수 있습니다. IT 관리자가 VLAN을 설정한 방법에 따라 다른 부서의 리소스는 마케팅 VLAN 구성원에게 보이지 않거나, 모두가 액세스할 수 있거나, 특정 개인만 액세스할 수 있습니다.

VLAN은 다음과 같은 여러 가지 장점을 제공합니다.

- 네트워크 분할이 용이하다. 서로 가장 자주 통신하는 사용자는 물리적 위치에 관계없이 공통 VLAN으로 그룹화될 수 있습니다. 각 그룹의 트래픽은 대부분 VLAN 내에 포함되어 외부 트래픽을 줄이고 전체 네트워크의 효율성을 향상시킵니다.
- 관리가 쉽습니다. 노드 추가, 이동 및 기타 변경 사항은 배선실이 아닌 관리 인터페이스에서 빠르고 편리하게 처리할 수 있습니다.
- 향상된 성능을 제공합니다. VLAN은 노드 간 및 네트워크 전체의 브로드캐스트 트래픽을 제한하여 대역폭을 확보합니다.
- 향상된 네트워크 보안을 보장합니다. VLAN은 라우터를 통해서만 교차할 수 있는 가상 경계를 만듭니다. 따라서 표준 라우터 기반 보안 조치를 사용하여 각 VLAN에 대한 액세스를 제한할 수 있습니다.

스위치가 수신한 패킷은 다음과 같은 방식으로 처리됩니다.

- 태그가 지정되지 않은 패킷이 포트에 들어오면 자동으로 포트의 기본 VLAN ID 태그 번호로 태그가 지정됩니다. 각 포트에는 사용자가 구성할 수 있는 기본 VLAN ID 설정이 있습니다(기본 설정은 1). 각 포트의 기본 VLAN ID 설정은 Port PVID Configuration(포트

PVID 구성) 화면에서 변경할 수 있습니다. 포트 PVID 설정 구성을 참조하십시오.

- 태그가 지정된 패킷이 포트에 들어갈 때 해당 패킷의 태그는 기본 VLAN ID 설정의 영향을 받지 않습니다. 패킷은 VLAN ID 태그 번호로 지정된 VLAN으로 진행됩니다.
- 패킷이 입력된 포트가 VLAN ID 태그에 지정된 VLAN의 구성원이 아닌 경우 패킷이 삭제됩니다.
- 포트가 패킷의 VLAN ID로 지정된 VLAN의 구성원인 경우 패킷은 동일한 VLAN ID를 가진 다른 포트로 전송될 수 있습니다.
- 스위치에서 나가는 패킷은 해당 포트의 VLAN 멤버십 속성 설정에 따라 태그가 지정되거나 태그가 지정되지 않습니다. 특정 포트에 대한 U는 해당 포트에서 스위치를 떠나는 패킷에 태그가 지정되지 않음을 의미합니다. 반대로 특정 포트에 대한 T는 해당 포트에서 스위치를 떠나는 패킷이 해당 포트와 연결된 VLAN ID로 태그 지정됨을 의미합니다.

이 섹션에 제공된 예는 태그가 지정된 VLAN에 대한 이해를 돕기 위해 광범위한 구성을 설명하는 여러 단계로 구성됩니다.

VLAN 구성 예

이 예에서는 VLAN 사용에 대한 여러 시나리오를 보여주고 스위치가 태그가 지정된 트래픽과 태그가 지정되지 않은 트래픽을 처리하는 방법을 설명합니다.

이 예에서는 두 개의 새 VLAN을 생성하고, 기본 VLAN 1의 포트 멤버십을 변경하고, 두 개의 새 VLAN에 포트 멤버를 할당합니다.

1. 기본 VLAN 구성 화면(VLAN 구성 참조)에서 다음 VLAN을 생성합니다.
   - VLAN ID가 10인 VLAN.
   - VLAN ID가 20인 VLAN.
2. VLAN 멤버십 화면(VLAN 멤버십 구성 참조)에서 다음과 같이 VLAN 멤버십을 지정합니다.
   - VLAN ID 1이 있는 기본 VLAN의 경우 포트 7(U) 및 포트 8(U) 멤버를 지정합니다.
   - VLAN ID가 10인 VLAN의 경우 포트 1(U), 포트 2(U), 포트 3(T) 멤버를 지정합니다..
   - VLAN ID가 20인 VLAN의 경우 포트 4(U), 포트 5(T) 및 포트 6(U) 멤버를 지정합니다.
3. 포트 PVID 구성 화면(포트 PVID 설정 구성 참조)에서 포트 g1 및 g4에 대한 PVID를 지정하여 해당 포트에 들어오는 패킷이 포트 VLAN ID로 태그 지정되도록 합니다.
   - Port g1: PVID 10

- Port g4: PVID 20

4. 설정한 VLAN 구성을 사용하면 다음 상황에서 설명한 대로 결과가 생성됩니다.
   - 태그가 지정되지 않은 패킷이 포트 1에 들어가면 스위치는 해당 패킷에 VLAN ID 10으로 태그를 지정합니다. 패킷은 포트 2와 포트 3에 액세스할 수 있습니다. 나가는 패킷에서 태그가 제거되어 포트 2가 태그가 지정되지 않은 패킷으로 남습니다. 포트 3의 경우 나가는 패킷은 VLAN ID 10의 태그가 지정된 패킷으로 남습니다.
   - VLAN ID 10이 포함된 태그가 지정된 패킷이 포트 3에 들어가면 해당 패킷은 포트 1과 포트 2에 액세스할 수 있습니다. 패킷이 포트 1이나 포트 2를 떠나면 해당 태그가 제거되어 태그가 지정되지 않은 패킷으로 스위치에 남습니다.
   - 태그가 지정되지 않은 패킷이 포트 4에 들어가면 스위치는 해당 패킷에 VLAN ID 20으로 태그를 지정합니다. 패킷은 포트 5와 포트 6에 액세스할 수 있습니다. 나가는 패킷은 포트 6을 떠날 때 태그가 제거되어 태그가 지정되지 않은 패킷이 됩니다. 5에서 나가는 패킷은 VLAN ID 20의 태그가 지정된 패킷으로 남습니다.

액세스 제어 목록(ACL)

ACL은 승인된 사용자만 특정 리소스에 액세스할 수 있도록 하는 동시에 네트워크 리소스에 접근하려는 부당한 시도를 차단합니다.

ACL은 트래픽 흐름 제어를 제공하고, 라우팅 업데이트 내용을 제한하고, 전달 또는 차단할 트래픽 유형을 결정하고, 네트워크에 보안을 제공하는 데 사용됩니다. ACL은 일반적으로 내부 네트워크와 인터넷과 같은 외부 네트워크 사이에 위치한 방화벽 라우터에 사용됩니다. 또한 내부 네트워크의 특정 부분으로 들어오거나 나가는 트래픽을 제어하기 위해 네트워크의 두 부분 사이에 위치한 라우터에서 사용할 수도 있습니다. ACL 기능에 필요한 추가 패킷 처리는 스위치 성능에 영향을 주지 않습니다. 즉, ACL 처리는 회선 속도로 발생합니다.

액세스 목록은 허용 및 거부 조건의 순차적 모음입니다. 필터링 기준으로 알려진 이러한 조건 모음은 스위치나 라우터에서 처리되는 각 패킷에 적용됩니다. 패킷 전달 또는 삭제는 패킷이 지정된 기준과 일치하는지 여부에 따라 결정됩니다.

트래픽 필터링에는 다음 두 가지 기본 단계가 필요합니다.

1. 액세스 목록 정의를 생성합니다.

   액세스 목록 정의에는 기준과 일치하는 트래픽을 정상적으로 전달할지 아니면 삭제할지를 지정하는 규칙이 포함되어 있습니다. 또한 기준과 일치하는 트래픽을 특정 대기열에 할당하거나 트래픽을 특정 포트로 리디렉션할 수 있습니다. 기본 모든 거부 규칙은 모든 목록의 마지막 규칙입니다.

2. 인바운드 방향의 인터페이스에 액세스 목록을 적용합니다.

ACL이 물리적 포트 및 LAG에 바인딩되도록 허용합니다. 스위치 소프트웨어는 MAC ACL 및 IP ACL을 지원합니다.

MAC ACL 샘플 구성

다음 예에서는 지정된 포트에서 영업 부서의 이더넷 트래픽을 허용하고 해당 포트의 다른 모든 트래픽을 거부하는 MAC 기반 ACL을 생성하는 방법을 보여줍니다.

1. MAC ACL 화면에서 네트워크의 영업 부서에 대해 Sales_ACL이라는 이름의 ACL을 생성합니다(기본 MAC ACL 구성 참조).

   기본적으로 이 ACL은 인바운드 방향으로 바인딩됩니다. 즉, 스위치가 포트에 들어갈 때 트래픽을 검사한다는 의미입니다.

2. MAC 규칙 화면에서 다음 설정을 사용하여 Sales_ACL에 대한 규칙을 생성합니다.
   - ID: 1
   - Action: Permit
   - Assign Queue ID: 0
   - Match Every: False
   - CoS: 0
   - Destination MAC: 01:02:1A:BC:DE:EF
   - Destination MAC Mask: 00:00:00:00:FF:FF
   - EtherType User Value:
   - Source MAC: 02:02:1A:BC:DE:EF
   - Source MAC Mask: 00:00:00:00:FF:FF
   - VLAN ID: 2

   MAC ACL 규칙에 대한 자세한 내용은 MAC ACL 규칙 구성을 참조하십시오.

3. MAC 바인딩 구성 화면에서 Sales_ACL을 인터페이스 기가비트 포트 6, 7, 8에 할당한 다음 적용 버튼을 클릭합니다(MAC 바인딩 구성 참조).

   이 인터페이스 및 방향에 이미 할당된 다른 액세스 목록을 기준으로 이 액세스 목록의 순서를 표시하기 위해 선택적 시퀀스 번호를 할당할 수 있습니다.

4. MAC 바인딩 테이블에는 인터페이스와 MAC ACL 바인딩 정보가 표시됩니다(MAC 바인딩 테이블에서 MAC ACL 바인딩 보기 또는 삭제 참조).

Sales_ACL이라는 ACL은 규칙에 정의된 대상 및 소스 MAC 주소와 MAC 마스크가 있는 이더넷 프레임을 찾습니다. 또한 프레임에는 영업 부서 VLAN인 VLAN ID 2 태그가 지정되어야 합니다. 프레임의 CoS 값은 0이어야 하며, 이는 이더넷 프레임의 기본값입니다.

이 기준과 일치하는 프레임은 인터페이스 6, 7, 8에서 허용되며 기본 대기열인 하드웨어 송신 대기열 0에 할당됩니다. 다른 모든 트래픽은 이러한 인터페이스에서 명시적으로 거부됩니다. 추가 트래픽이 이러한 포트에 진입하도록 허용하려면 원하는 일치 기준을 사용하여 새 허용 규칙을 추가하고 해당 규칙을 인터페이스 6, 7, 8에 바인딩해야 합니다.

표준 IP ACL 샘플 구성

다음 예에서는 재무 부서의 IP 트래픽이 다른 부서와 연결된 포트에서 허용되지 않도록 방지하는 IP 기반 ACL을 생성하는 방법을 보여줍니다. 재무 부서의 트래픽은 각 패킷의 네트워크 IP 주소로 식별됩니다.

1. IP ACL 화면에서 IP ACL ID가 1인 새 IP ACL을 생성합니다(IP ACL 구성 참조).
2. IP 규칙 화면에서 다음 설정을 사용하여 IP ACL 1에 대한 규칙을 생성합니다.
   - Rule ID: 1
   - Action: Deny
   - Assign Queue ID: 0 (optional: 0 is the default value)
   - Match Every: False
   - Source IP Address: 192.168.187.0
   - Source IP Mask: 255.255.255.0

   IP ACL 규칙에 대한 추가 정보는 IP ACL에 대한 규칙 구성을 참조하십시오.
3. Add 버튼을 클릭합니다
4. IP 규칙 화면에서 다음 설정을 사용하여 IP ACL 1에 대한 두 번째 규칙을 만듭니다.
   - Rule ID: 2
   - Action: Permit
   - Match Every: True
5. Add 버튼을 클릭합니다.
6. IP 바인딩 구성 화면에서 ACL ID 1을 인터페이스 기가비트 포트 2, 3, 4에 할당하고 시퀀스 번호 1을 할당합니다(IP ACL 인터페이스 바인딩 구성 참조).

   기본적으로 이 IP ACL은 인바운드 방향으로 바인딩되므로 스위치에 들어갈 때 트래픽을 검사합니다.
7. Apply 버튼을 클릭합니다
   IP 바인딩 테이블 화면을 사용하여 인터페이스 및 IP ACL 바인딩 정보를 확인합니다(참조: IP ACL 바인딩 테이블에서 IP ACL 바인딩 보기 또는 삭제)

이 예의 IP ACL은 모든 패킷을 재무 부서 네트워크의 소스 IP 주소 및 서브넷 마스크와 일치시키고 스위치의 이더넷 인터페이스 2, 3, 4에서 이를 거부합니다. 두 번째 규칙은

포트의 모든 비금융 트래픽을 허용합니다. 우선순위가 가장 낮은 규칙으로 명시적인 모든 거부 규칙이 있으므로 두 번째 규칙이 필요합니다.

차별화된 서비스(DiffServ)

표준 IP 기반 네트워크는 최선의 데이터 전달 서비스를 제공하도록 설계되었습니다. 최선의 노력 서비스는 네트워크가 적시에 데이터를 전달한다는 것을 의미하지만 반드시 그럴 것이라는 보장은 없습니다. 혼잡 중에는 패킷이 지연되거나 산발적으로 전송되거나 삭제될 수 있습니다. 이메일 및 파일 전송과 같은 일반적인 인터넷 응용 프로그램의 경우 서비스의 약간의 저하가 허용되며 대부분의 경우 눈에 띄지 않습니다. 그러나 서비스 저하는 음성이나 멀티미디어와 같이 타이밍 요구 사항이 엄격한 애플리케이션에 바람직하지 않은 영향을 미칩니다.

QoS(서비스 품질)는 타이밍 요구 사항이 엄격한 패킷과 지연을 더 잘 견디는 패킷을 구별하여 일관되고 예측 가능한 데이터 전달을 제공할 수 있습니다. 엄격한 타이밍 요구 사항이 있는 패킷은 QoS 가능 네트워크에서 특별하게 처리됩니다. 이를 염두에 두고 네트워크의 모든 요소는 QoS를 지원해야 합니다. 한 노드가 필요한 타이밍 요구 사항을 충족할 수 없는 경우 네트워크 경로에 결함이 발생하고 전체 패킷 흐름의 성능이 저하됩니다.

QoS에는 두 가지 기본 유형이 있습니다.

- **Integrated Services**: 네트워크 리소스는 요청에 따라 할당되며 네트워크 관리 정책(예: RSVP)에 따라 예약됩니다(리소스 예약).
- **Differentiated Services**: 네트워크 리소스는 트래픽 분류 및 우선순위에 따라 할당되어 엄격한 타이밍 요구 사항이 있는 데이터를 우선적으로 처리합니다.

관리형 스위치 스위치는 DiffServ를 지원합니다.

DiffServ 기능에는 차별화된 서비스 네트워크를 구성하는 데 사용할 수 있는 다양한 개념적 QoS 구성 요소가 포함되어 있습니다. 이러한 동일한 블록을 다양한 방식으로 사용하여 다른 유형의 QoS 아키텍처를 구축하십시오.

DiffServ를 구성하는 데 필요한 3가지 주요 QoS 구성 요소가 있습니다.

- Class
- Policy
- Service (the assignment of a policy to a directional interface)

클래스

패킷에 대한 다음 정보를 검사하여 레이어 2, 3, 4에서 들어오는 패킷을 분류할 수 있습니다.

- Source/destination MAC address
- EtherType
- Class of Service (802.1p priority) value (first/only VLAN tag)
- VLAN ID range (first/only VLAN tag)
- Secondary 802.1p priority value (second/inner VLAN tag)
- Secondary VLAN ID range (second/inner VLAN tag)
- IP Service Type octet (also known as: ToS bits, Precedence value, DSCP value)
- Layer 4 protocol (TCP, UDP and so on)
- Layer 4 source/destination ports
- Source/destination IP address

DiffServ 관점에서 볼 때 클래스에는 두 가지 유형이 있습니다.

- DiffServ traffic classes
- DiffServ service levels/forwarding classes

DiffServ 트래픽 클래스

DiffServ를 사용하면 수신 인터페이스에서 추적할 트래픽 클래스를 정의할 수 있습니다. 단순 BA 분류자(DSCP)와 다양한 다중 필드(MF) 분류자를 정의할 수 있습니다.

- Layer 2; Layers 3, 4 (IP only)
- Protocol-based
- Address-based

이러한 분류자를 논리적 AND 또는 OR 연산과 결합하여 복잡한 구조를 구축할 수 있습니다.

MF 분류자(각각 all 또는 any 클래스 유형 지정) 즉, 단일 클래스 내에서 정의된 클래스 유형에 따라 여러 일치 기준이 AND 표현식 또는 순차 OR 표현식으로 함께 그룹화됩니다. 동일한 유형의 클래스만 중첩될 수 있습니다. 클래스 중첩은 참조된 클래스의 부정(제외 옵션)을 허용하지 않습니다.

DiffServ를 구성하려면 서비스 수준, 즉 송신 인터페이스에서 특정 DSCP 값으로 식별되는 전달 클래스/PHB를 정의해야 합니다. 이러한 서비스 수준은 각각에 대한 BA 클래스를 구성하여 정의됩니다.

정책 만들기

DiffServ 정책을 사용하여 구성하는 클래스 컬렉션을 하나 이상의 QoS 정책 설명과 연결합니다. 이 연관의 결과를 정책이라고 합니다.

DiffServ 관점에서 볼 때 다음과 같은 두 가지 유형의 정책이 있습니다.

- **Traffic Conditioning Policy**: DiffServ 트래픽 클래스에 적용되는 정책
- **Service Provisioning Policy**: DiffServ 서비스 수준에 적용되는 정책

원하는 TCS(트래픽 조절 사양) 및 SLS(서비스 수준 사양) 작업을 각각 달성하려면 트래픽 조절 및 서비스 프로비저닝 정책에 사용되는 다양한 명령문과 규칙을 수동으로 구성해야 합니다.

교통 상황 정책

트래픽 조절은 수신 트래픽에 대해 수행되는 작업과 관련됩니다. 트래픽 조절과 관련된 몇 가지 고유한 QoS 작업이 있습니다.

- **Dropping**. 도착 시 패킷을 버리십시오. 이는 특히 DiffServ와 ACL이 동일한 인터페이스에 공존할 수 없는 경우 DiffServ를 사용하여 액세스 제어 목록 작업을 에뮬레이션하는 데 유용합니다.
- **Marking IP DSCP or IP Precedence**. 특정 DiffServ 트래픽 클래스와 관련된 서비스 수준을 나타내는 DSCP 값을 사용하여 패킷의 DiffServ 코드 포인트를 표시/재표시합니다. 또는 패킷의 IP 우선순위 값을 표시/재표시할 수 있습니다.
- **Marking CoS (802.1p)**. 트래픽 클래스에 대해 패킷이 전송될 때 첫 번째/유일한 802.1p 헤더의 3비트 우선 순위 필드를 지정된 값으로 설정합니다. 802.1p 헤더가 아직 없으면 삽입됩니다. 이는 DiffServ 전달 클래스(예: DSCP 또는 IP 우선 순위 값) 정의를 기반으로 계층 2 우선 순위 수준을 할당하여 IP 헤더에서 DSCP 값을 정기적으로 확인하지 않는 다운스트림 스위치에 일부 QoS 특성을 전달하는 데 유용합니다.
- **Policing**. TCS의 조건을 준수하도록 특정 클래스와 연관된 수신 트래픽을 제한하는 방법입니다. 적합성 사양을 초과하거나 부적합한 프로파일 외부 패킷에는 특별한 처리가 적용될 수 있습니다. DiffServ 기능은 다음 유형의 트래픽 정책 처리(작업)를 지원합니다.
  - drop. 패킷이 삭제되었습니다.
  - mark cos. 802.1p 사용자 우선순위 비트가 (재)표시되어 전달됩니다.
  - mark dscp. 패킷 DSCP가 (재)표시되어 전달됩니다.
  - mark prec. 패킷 IP 우선순위가 (재)표시되어 전달됩니다.
  - send: 패킷은 DiffServ 수정 없이 전달됩니다.

Color Mode Awareness. DiffServ 기능의 정책은 색맹 또는 색 인식 모드를 사용합니다. 색맹 모드는 수신 패킷의 색상(표시)을 무시합니다. 색상 인식 모드는 정책 결과를 결정할 때 현재 패킷 표시를 고려합니다. 보조 트래픽 클래스는 정책 정의와 함께 사용되어 적합한 색상으로 사용될 수신 색상 값을 지정하는 802.1p, 보조 802.1p, IP DSCP 또는 IP 우선 순위 필드 중 하나에 대한 값을 지정합니다. 초과 트래픽의 색상도 선택적으로 지정할 수 있습니다.

- **Counting**. DiffServ 내의 트래픽 경로를 따라 데이터 처리를 추적하기 위해 옥텟 및 패킷 통계를 업데이트합니다. 이 DiffServ 기능에서 카운터는 사용자가 명시적으로 구성하지 않지만 생성되는 DiffServ 정책을 기반으로 시스템에 설계됩니다. 자세한 내용은 이 문서의 통계 섹션을 참조하세요.
- **Assigning QoS Queue**. 트래픽 스트림을 지정된 QoS 대기열로 보냅니다. 이를 통해 트래픽 분류자는 지원되는 하드웨어 대기열 중 어느 것이 클래스에 속하는 패킷을 처리하는 데 사용되는지 지정할 수 있습니다.
- **Redirecting**. 분류된 트래픽 스트림을 지정된 송신 포트(물리적 또는 LAG)로 강제 적용합니다. 이는 표시 또는 단속 조치에 추가로 발생할 수 있습니다. QoS 대기열 할당과 함께 지정할 수도 있습니다.

DiffServ 예시 구성

DiffServ 클래스/정책을 생성하여 스위치 인터페이스에 연결하려면 다음 단계를 따르십시오.

1. QoS 클래스 구성 화면에서 다음 설정을 사용하여 새 클래스를 생성합니다.
   - Class Name: Class1
   - Class Type: All

   이 화면에 대한 자세한 내용은 DiffServ 클래스 구성을 참조하십시오.
2. Class1 하이퍼링크를 클릭하면 이 클래스에 대한 DiffServ 클래스 구성 화면을 볼 수 있습니다.
3. Class1에 대해 다음 설정을 구성합니다.
   - Protocol Type: UDP
   - Source IP Address: 192.12.1.0
   - Source Mask: 255.255.255.0
   - Source L4 Port: Other, and enter 4567 as the source port value
   - Destination IP Address: 192.12.2.0
   - Destination Mask: 255.255.255.0
   - Destination L4 Port: Other, and enter 4568 as the destination port value

이 화면에 대한 자세한 내용은 DiffServ 클래스 구성을 참조하십시오.

4. Apply 버튼을 클릭합니다
5. 정책 구성 화면에서 다음 설정을 사용하여 새 정책을 만듭니다.
   - Policy Selector: Policy1
   - Member Class: Class1

   이 화면에 대한 자세한 내용은 DiffServ 정책 구성을 참조하십시오.
6. Add 버튼을 클릭합니다.

   정책이 추가됩니다.
7. 이 정책에 대한 정책 클래스 구성 화면을 보려면 Policy1 하이퍼링크를 클릭합니다.
8. 다음과 같이 정책 속성을 구성합니다.
   - Assign Queue: 3
   - Policy Attribute: Simple Policy
   - Color Mode: Color Blind
   - Committed Rate: 1000000 Kbps
   - Committed Burst Size: 128 KB
   - Confirm Action: Send
   - Violate Action: Drop

   이 화면에 대한 자세한 내용은 DiffServ 정책 구성을 참조하십시오.
9. 서비스 구성 화면에서 인터페이스 g7 및 g8 옆에 있는 확인란을 선택하여 이러한 인터페이스에 정책을 연결한 다음 적용 버튼을 클릭합니다(DiffServ 서비스 인터페이스 구성 참조).

모든 UDP 패킷 흐름은 다음의 IP 소스 주소를 사용하여 192.12.2.0 네트워크로 향합니다.

포트 7과 8에 있는 이 스위치의 레이어 4 소스 포트 4567과 대상 포트 4568을 포함하는 192.12.1.0 네트워크는 하드웨어 대기열 3에 할당됩니다.

이 네트워크에서 스트리밍 애플리케이션의 트래픽은 UDP 포트 4567을 소스로 사용하고 4568을 대상으로 사용합니다. 이 실시간 트래픽은 시간에 민감하므로

우선순위가 높은 하드웨어 대기열. 기본적으로 데이터 트래픽은 최선형 대기열로 지정된 하드웨어 대기열 0을 사용합니다.

또한 이 흐름에서 확인된 작업은 1000000Kbps의 커밋 속도와 128KB의 버스트 크기로 패킷을 보내는 것입니다. 커밋된 속도와 버스트 크기를 위반하는 패킷은 삭제됩니다.

802.1X

근거리 통신망(LAN)은 승인되지 않은 장치가 LAN 인프라에 물리적으로 연결되거나 승인되지 않은 사용자가 이미 연결된 장비를 통해 LAN에 액세스하도록 허용하는 환경에 배포되는 경우가 많습니다. 이러한 환경에서는 LAN에서 제공하는 서비스에 대한 액세스를 해당 서비스를 사용하도록 허용된 사용자 및 장치로 제한할 수 있습니다.

포트 기반 네트워크 액세스 제어는 LAN 인프라의 물리적 특성을 활용하여 지점 간 연결 특성이 있는 LAN 포트에 연결된 장치를 인증 및 권한 부여하고 다음과 같은 경우 해당 포트에 대한 액세스를 방지하는 수단을 제공합니다. 인증 및 권한 부여 프로세스가 실패합니다. 이러한 맥락에서 포트는 MAC 브리지의 포트, IEEE 802.11 무선 LAN의 스테이션 또는 액세스 포인트 간의 연결과 같은 LAN에 대한 단일 연결 지점입니다.

IEEE 802.11 표준은 인증 및 그에 따른 조치가 이루어지는 아키텍처 프레임워크를 설명합니다. 또한 인증자(인증 요청을 인증 서버에 전달하는 시스템)와 신청자(인증을 요청하는 시스템) 사이는 물론 인증자와 인증 서버 사이의 프로토콜에 대한 요구 사항도 설정합니다.

관리형 스위치 스위치는 인증되지 않은 사용자가 네트워크 리소스에 대한 제한된 액세스를 허용하는 게스트 VLAN을 지원합니다.

Note: QoS 기능을 사용하여 게스트 VLAN에 속도 제한을 제공하여 게스트 VLAN이 제공하는 네트워크 리소스를 제한할 수 있습니다.

802.1X의 또 다른 기능은 EAPoL 패킷 전달 지원을 활성화/비활성화하도록 포트를 구성하는 기능입니다. 장치에서 802.1X가 비활성화된 경우 EAPoL 전달을 비활성화하거나 활성화할 수 있습니다.

802.1X 인증 스위치의 포트는 LAN을 통해 연결할 수 있는 다른 시스템에 서비스를 제공할 수 있는 수단을 제공합니다. 포트 기반 네트워크 액세스 제어를 사용하면 스위치 포트의 작동을 제어하여 해당 서비스에 대한 액세스가 승인된 시스템에서만 허용되도록 할 수 있습니다.

포트 액세스 제어는 시스템이 제공하는 서비스에 대한 신청자의 무단 액세스를 방지하는 수단을 제공합니다. 공개적으로 액세스 가능한 브리지 포트에 대한 액세스를 제한하거나 부서별 LAN에 대한 액세스를 제한하려는 경우 스위치 및 스위치가 연결된 LAN에 대한 액세스를 제어하는 것이 바람직할 수 있습니다.

액세스 제어는 인증자의 제어 포트에 연결된 신청자의 인증을 시행하여 달성됩니다. 인증 프로세스의 결과에 따라 신청자가 해당 제어 포트의 서비스에 액세스할 수 있는 권한이

있는지 여부가 결정됩니다.

포트 액세스 엔터티(PAE)는 액세스 제어 상호 작용 내에서 두 가지 고유한 역할 중 하나를 채택할 수 있습니다.

1. **Authenticator**: 해당 포트를 통해 사용 가능한 서비스에 대한 액세스를 허용하기 전에 인증을 시행하는 포트입니다.
2. **Supplicant:** 인증자가 제공하는 서비스에 액세스를 시도하는 포트입니다.

또한 세 번째 역할도 있습니다.

3. **Authentication server**: 인증자를 대신하여 신청자의 자격 증명을 확인하는 데 필요한 인증 기능을 수행합니다.

인증 교환을 완료하려면 세 가지 역할이 모두 필요합니다.

관리형 스위치 스위치는 PAE가 신청자와의 통신을 담당하는 인증자 역할만 지원합니다. 또한 인증자 PAE는 자격 증명을 확인하기 위해 요청자로부터 받은 정보를 인증 서버에 제출하여 포트의 인증 상태를 결정하는 역할도 합니다. Authenticator PAE는 RADIUS 기반 인증 프로세스의 결과에 따라 제어되는 포트의 승인/비인증 상태를 제어합니다.

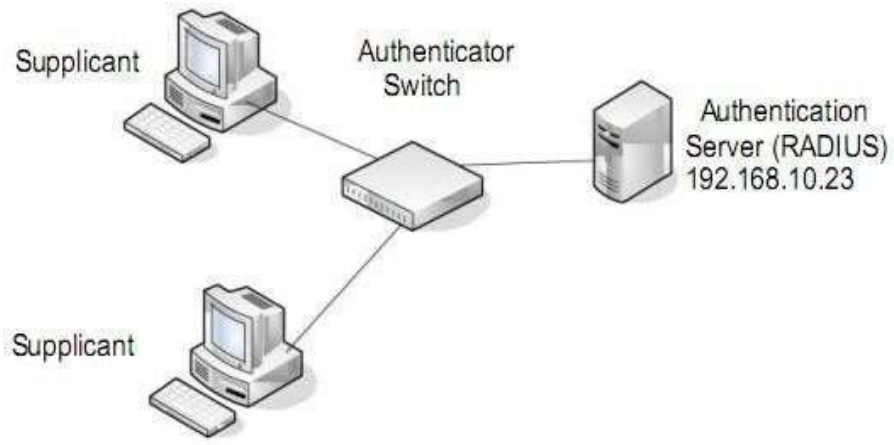


Figure 1. 802.1X Authentication Roles

802.1X 구성 예

이 예에서는 회사 회의실(1/0/5~1/0/8)의 포트에 802.1X 기반 인증이 필요하도록 스위치를 구성하는 방법을 보여줍니다. 이러한 포트는 방문자가 사용할 수 있으며 네트워크에 대한 액세스 권한을 부여하기 전에 인증을 받아야 합니다. 인증은 외부 RADIUS 서버에 의해 처리됩니다. 방문자가 성공적으로 인증되면 트래픽이 자동으로 게스트 VLAN에 할당됩니다. 이 예에서는 VLAN이 VLAN ID 150과 VLAN 이름 Guest로 구성되었다고 가정합니다.

1. 포트 인증 화면에서 포트 1/0/5, 1/0/6, 1/0/7 및 1/0/8을 선택합니다.
2. 포트 제어 메뉴에서 인증되지 않음을 선택합니다.

   인증이 필요하지 않은 다른 모든 포트에 대한 포트 제어 설정은 승인되어야 합니다. Port Control 설정이 Authorized인 경우, 포트는 무조건 강제 Authorized 상태가 되며 어떠한 인증도 필요하지 않습니다. 포트 제어 설정이 자동인 경우 인증자 PAE는 제어된 포트 모드를 설정합니다.

3. 포트 1/0/5~1/0/8의 게스트 VLAN 필드에 150을 입력하여 해당 포트를 게스트 VLAN에 할당합니다.

   포트를 통해 네트워크에 대한 액세스를 제어하기 위해 추가 설정을 구성할 수 있습니다. 설정에 대한 자세한 내용은 포트 보안 인터페이스 구성을 참조하십시오.

4. Apply 버튼을 클릭합니다
5. 802.1X 구성 화면에서 포트 기반 인증 상태 및 게스트 VLAN 모드를 활성화로 설정한 다음 적용 버튼을 클릭합니다(전역 포트 보안 모드 구성 참조).

   이 예에서는 포트 인증 설정에 기본값을 사용하지만 구성할 수 있는 몇 가지 추가 설정이 있습니다. 예를 들어 EAPOL 플러드 모드 필드를 사용하면 장치에서 802.1X가 비활성화된 경우 EAPoL 프레임 전달을 활성화할 수 있습니다.

6. RADIUS 서버 구성 화면에서 다음 설정으로 RADIUS 서버를 구성합니다.
   - Server Address: 192.168.10.23
   - Secret Configured: Yes
   - Secret: secret123
   - Active: Primary

   자세한 내용은 RADIUS 개요를 참조하십시오.

7. Add 버튼을 클릭합니다.
8. 인증 목록 화면에서 RADIUS를 첫 번째 인증 방법으로 사용하도록 기본 목록을 구성합니다(로그인 인증 목록 구성 참조).

이 예에서는 802.1X 기반 포트 보안을 활성화하고 포트 g5-g8에 연결된 호스트에 802.1X 기반 인증을 요청하는 메시지를 표시합니다. 스위치는 구성된 RADIUS 서버에 인증 정보를 전달합니다.

MSTP

STP(Spanning Tree Protocol)는 브리지된 네트워크에서 실행되어 루프를 제거하는 데

도움이 됩니다. 브리지 루프가 발생하면 네트워크에 트래픽이 넘칠 수 있습니다. IEEE 802.1s 다중 스패닝 트리 프로토콜(MSTP)은 스패닝 트리의 여러 인스턴스를 지원하여 다양한 인터페이스를 통해 VLAN 트래픽을 효율적으로 전달합니다. 스패닝 트리의 각 인스턴스는 작업에 약간의 수정이 있지만 최종 효과는 아닌 IEEE 802.1w, Rapid Spanning Tree에 지정된 방식으로 동작합니다(효과 중 가장 중요한 것은 포트가 전달 상태로 빠르게 전환된다는 것입니다).

RSTP와 기존 STP(IEEE 802.1D)의 차이점은 전이중 연결과 엔드 스테이션에 연결된 포트를 구성하고 인식하여 포트를 전달 상태로 빠르게 전환하고 토폴로지 변경을 억제하는 기능입니다. 공고. 이러한 기능은 pointtopoint 및 edgeport 매개변수로 표시됩니다. MSTP는 RSTP 및 STP와 모두 호환됩니다. STP 및 RSTP 브리지에 적절하게 작동합니다.

MSTP 브리지는 완전히 RSTP 브리지 또는 STP 브리지로 작동하도록 구성할 수 있습니다. 따라서 IEEE 802.1s 브리지는 본질적으로 IEEE 802.1w 및 IEEE 802.1D도 지원합니다.

MSTP 알고리즘 및 프로토콜은 각각 MSTP, STP 또는 RSTP를 작동하는 임의로 상호 연결된 네트워킹 장치로 구성된 브리지 LAN 전체에서 특정 VLAN에 할당된 프레임에 대해 간단하고 완전한 연결을 제공합니다. MSTP를 사용하면 서로 다른 VLAN에 할당된 프레임이 LAN 및/또는 MSTP 브리지로 구성된 다중 스패닝 트리(MST) 영역 내에서 각각 독립적인 다중 스패닝 트리 인스턴스(MSTI)를 기반으로 하는 별도의 경로를 따라갈 수 있습니다. 이러한 지역과 기타 브리지 및 LAN은 단일 CST(공통 스패닝 트리)로 연결됩니다. [IEEE 초안 P802.1s/D13]

MSTP는 단일 CIST(공통 및 내부 스패닝 트리)를 사용하여 모든 브리지와 LAN을 연결합니다. CIST는 가능한 최대 범위를 선택하여 각 MST 영역의 자동 결정을 지원합니다. CIST에 대해 계산된 연결성은 이러한 지역을 상호 연결하기 위한 CST와 각 지역 내의 내부 스패닝 트리(IST)를 제공합니다. MSTP는 주어진 VLAN ID를 가진 프레임이 지역 내의 MSTI 또는 IST 중 하나에만 할당되고, 할당이 지역의 모든 네트워킹 장치 간에 일관되며, 각 MSTI 및 IST의 안정적인 연결을 보장합니다. 지역의 경계는 CST의 경계와 일치합니다. 특정 VLAN에 속하는 것으로 일관되게 분류된 프레임과 관련하여 브리지 LAN의 안정적인 활성 토폴로지는 네트워크 전체에 걸쳐 모든 LAN과 네트워킹 장치를 간단하고 완전하게 연결합니다. 단, 서로 다른 VLAN에 속한 프레임은 IEEE에 따라 모든 지역 내에서 서로 다른 경로를 사용할 수 있습니다. 초안 P802.1s/D13.

STP, RSTP 또는 MSTP를 사용하는 모든 브리지는 BPDU(Bridge Protocol Data Unit)를 통해 구성 메시지의 정보를 전송하여 하나 이상의 스패닝 트리를 기반으로 완전하고 간단하게 연결된 활성 토폴로지에서 각 포트의 참여를 결정하는 포트 역할을 할당합니다. 전달되는 정보는 스패닝 트리 우선순위 벡터로 알려져 있습니다. 이러한 서로 다른 프로토콜 각각에 대한 BPDU 구조는 다릅니다. MSTP 브리지는 특정 포트에서 수신된 BPDU 유형에

따라 적절한 BPDU를 전송합니다.

MST 지역은 동일한 MST 구성 식별자를 갖고 동일한 MSTI를 사용하며 MSTP BPDU를 수신 및 전송할 수 없는 연결된 브리지가 없는 하나 이상의 MSTP 브리지로 구성됩니다. MST 구성 식별자에는 다음 구성 요소가 있습니다.

1. 구성 식별자 형식 선택기
2. 구성 이름
3. 구성 개정 수준
4. 구성 다이제스트: MST 구성 테이블에서 생성된 HMAC-MD5 유형의 16바이트 서명(MSTID에 대한 VLAN ID 매핑)

스패닝 트리의 여러 인스턴스가 있으므로 포트별, 인스턴스별로(또는 VLAN별로 포트별로 유지되는 MSTP 상태가 있습니다. 모든 VLAN은 하나의 MSTI 또는 CIST에만 있을 수 있기 때문입니다) 예를 들어, 포트 A는 인스턴스 1을 전달하고 인스턴스 2를 삭제할 수 있습니다. 포트 상태는 IEEE 802.1D 사양 이후 변경되었습니다.

다중 스패닝 트리를 지원하려면 스패닝 트리에 대한 VLAN ID(VID)를 명확하게 할당하여 MSTP 브리지를 구성해야 합니다. 이는 다음을 통해 달성됩니다.

1. FID에 대한 VID 할당이 모호하지 않은지 확인합니다.
2. 브리지에서 지원하는 각 FID가 정확히 하나의 스패닝 트리 인스턴스에 할당되었는지 확인합니다.

VID에서 FID로, FID에서 MSTI로의 할당 조합은 MST 구성 테이블에 표시된 스패닝 트리 인스턴스에 대한 VID 매핑을 정의합니다.

이 할당을 통해 모든 VLAN이 단 하나의 MSTI에만 할당되도록 합니다. CIST는 MSTID가 0인 스패닝 트리의 인스턴스이기도 합니다.

VID가 할당되지 않은 인스턴스가 발생할 수 있지만 모든 VLAN은 스패닝 트리의 다른 인스턴스 중 하나에 할당되어야 합니다.

동일한 MST 지역의 두 브리지를 연결하는 네트워크의 활성 토폴로지 부분은 해당 지역의 MST 브리지 및 LAN만 통과하며 지역 외부의 어떤 종류의 브리지도 통과하지 않습니다. 즉, 지역 내의 연결은 외부와 연결과 독립적입니다.

MSTP 예시 구성

이 예에서는 스위치에서 MSTP 인스턴스를 생성하는 방법을 보여줍니다. 예제

네트워크에는 네트워크의 서로 다른 위치에 서비스를 제공하는 세 가지가 있습니다. 이 예에서 포트 1/0/1-1/0/5는 호스트 스테이션에 연결되므로 해당 링크는 네트워크 루프의 영향을 받지 않습니다. 포트 1/0/6~1/0/8은 스위치 1, 2, 3에 걸쳐 연결됩니다.

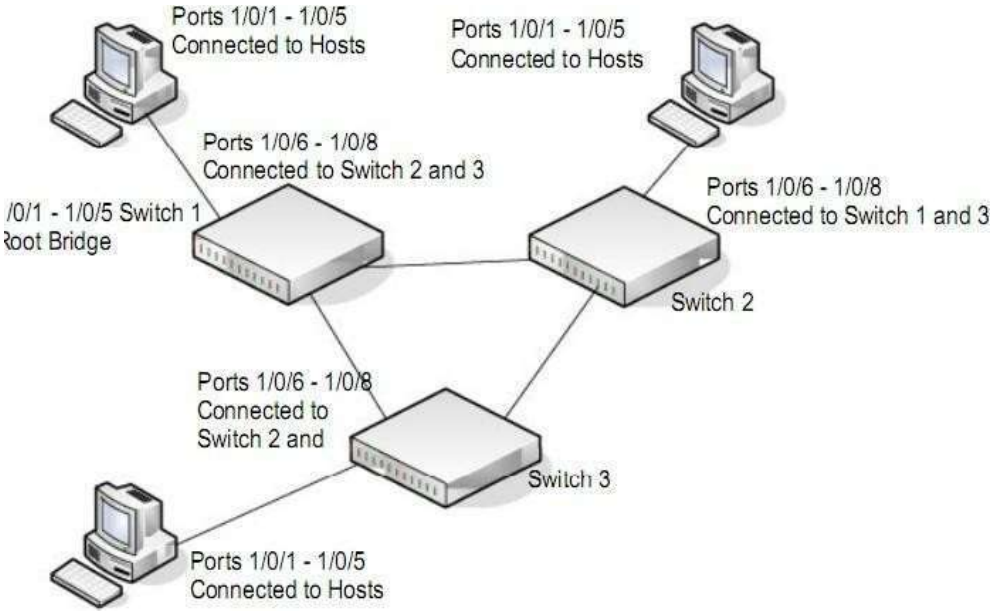


Figure 2. MSTP sample configuration

MSTP를 구성하려면 각 스위치에서 다음 절차를 수행하십시오.

1. VLAN 구성 화면을 사용하여 VLAN 300 및 500을 생성합니다(기본 VLAN 설정 구성 참조).
2. VLAN 멤버십 화면을 사용하여 VLAN 300 및 VLAN 500의 태그가 있는(T) 또는 태그가 없는(U) 멤버로 포트 1/0/1~1/0/8을 포함합니다(기본 VLAN 설정 구성 참조).
3. STP 구성 화면에서 스패닝 트리 상태 옵션을 활성화합니다(고급 STP 설정 구성 참조).

   나머지 STP 구성 설정에는 기본값을 사용합니다. 기본적으로 STP 작동 모드는 MSTP이고 구성 이름은 스위치 MAC 주소입니다.
4. CST 구성 화면에서 스위치 1이 루트 브리지가 되도록 세 스위치 각각에 대한 브리지 우선 순위 값을 설정합니다.
   - Switch 1: 4096
   - Switch 2: 12288
   - Switch 3: 20480

Note: 브리지 우선순위 값은 4096의 배수입니다.

루트 브리지를 지정하지 않고 모든 스위치에 동일한 브리지 우선 순위 값이 할당된 경우 MAC 주소가 가장 낮은 스위치가 루트 브리지로 선택됩니다(CST 설정 구성 참조).

5. CST 포트 구성 화면에서 포트 1/0/1~1/0/8을 선택하고 STP 상태 메뉴에서 활성화를 선택합니다(CST 포트 설정 구성 참조).
6. Apply 버튼을 클릭합니다
7. 포트 1/0/1~1/0/5(에지 포트)를 선택하고 빠른 링크 메뉴에서 활성화를 선택합니다.

   에지 포트는 네트워크 루프의 위험이 없으므로 빠른 링크가 활성화된 포트는 전달 상태로 직접 전환됩니다.
8. Apply 버튼을 클릭합니다

   CST 포트 상태 화면을 사용하여 각 포트에 대한 스패닝 트리 정보를 볼 수 있습니다.
9. MST 구성 화면에서 다음 설정을 사용하여 MST 인스턴스를 생성합니다.
   - MST ID: 1
   - Priority: Use the default (32768)
   - VLAN ID: 300

   자세한 내용은 MST 설정 구성을 참조하십시오.
10. Add 버튼을 클릭합니다.
11. 다음 설정을 사용하여 두 번째 MST 인스턴스를 생성합니다.
    - MST ID: 2
    - Priority: 49152
    - VLAN ID: 500
12. Add 버튼을 클릭합니다.

이 예에서는 스위치 1이 MST 인스턴스 1의 루트 브리지가 되고 스위치 2가 MST 인스턴스 2의 루트 브리지가 되었다고 가정합니다. 스위치 3에는 영업 부서에 호스트가 있습니다(포트 1/0/1, 1/ 0/2 및 1/0/3) 및 HR 부서(포트 1/0/4 및 1/0/5)에 있습니다. 스위치 1과 2에는 영업 및 인사 부서의 호스트도 포함됩니다. 스위치 2에서 연결된 호스트는 VLAN 500, MST 인스턴스 2를 사용하여 스위치 3의 호스트와 직접 통신합니다. 마찬가지로 스위치 1의 호스트는 VLAN 300, MST 인스턴스 1을 사용하여 스위치 3의 호스트와 직접 통신합니다.

호스트는 MSTP의 다양한 인스턴스를 사용하여 스위치 전체의 링크를 효과적으로 사용합니다. 동일한 개념이 다른 스위치 및 더 많은 MSTP 인스턴스로 확장될 수 있습니다.

약어 C

대부분의 경우 두문자어와 약어는 이 문서에서 처음 사용할 때 정의됩니다. 두문자어와 약어도 다음 표에 정의되어 있습니다.

Table 249. 약어

약어	설명
802.1x	IEEE 802.1x Authentication Protocol Standard
ACE	Access Control Entry
ACL	Access Control List
API	Application Programming Interface
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
CLI	Command Line Interface
CoS	Class of Service
Default Gateway	The IP address of a router that a host can use as its first hop when the host does not know a more specific route to a given destination.
Default Route	A manually configured (*static*) route whose destination is 0.0.0.0/0.0.0.0 and therefore matches every packet's destination. A router uses a default route to forward packets that do not match a more specific route.
DHCP	Dynamic Host Configuration Protocol (RFC 2131, RFC3315). A mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
DHCP Server	Dynamic Host Configuration Protocol Servers are servers that grant the address and do parameter assignment to requested clients in the network. Current interest is that these servers provide TFTP server and boot file information.
DLL	Data Link Layer
DNS Server	Domain Name System servers that provide the IP address mapping to the name of the hosts.
DSCP	Differentiated Services Code Point
EAP	Extensible Authentication Protocol

413

EAPOL	Extensible Authentication Protocol over LAN
ECMP	Equal Cost Multiple Paths
EEE	Energy Efficient Ethernet (from the IEEE 802.3az Energy Efficient Ethernet Task Force and IEEE 802.3az Energy Efficient Ethernet Study Group).
Host Interface	An IP interface that is not a routing interface. Only locally-originated packets are sent on a host interface. Only packets with a local destination are received. Host interfaces do not participate in dynamic routing protocols.
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS	Internal Authentication Server
IGMP	Internet Group Management Protocol
In-band Interface	An IP interface that could be used for in-band management. Any IP interface other than the Out-of-Band port.
IP	Internet Protocol
IP Address Owner	The VRRP router that has the virtual router's IP address(es) as real interface address(es). This is the router that, when up, will respond to packets addressed to one of these IP addresses for ICMP pings, TCP connections, and so on
IP Interface	An interface configured as an IP interface rather than a Layer 2 switching interface. An IP interface must be assigned one or more IP addresses. Also called a *Layer 3 interface*.
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISDP	Industry Standard Discovery Protocol
ISID	Initiator-defined session identifier
L2	Layer 2 (networking)
L3	Layer 3 (networking)
LAG	Link Aggregation Group (IEEE standard)
LLDP	Link Layer Discovery Protocol
Local Route	A route to an attached subnet. A router creates a local route for each active, locally-configured IP address and uses the local route to reach other stations on the attached subnet.
LPI	Low-power Idle
MAB	MAC Authentication Bypass
MAC	Media Access Control
Management Interface	An external IP interface used to send and receive IP packets to configure and monitor the device.
Management VLAN	A VLAN configured to be used for management rather than control or data traffic.
MFDB	Multicast Forwarding Database
MIB	Management Information Base

414

MLAG	Multi-chassis Link Aggregation
MPLS	Multiprotocol Label Switching: A standard involving IP quality.
MVR	Multicast VLAN Registration
N/A	not applicable
NSF	Nonstop Forwarding
PAE	Port Access Entity
PDU	Protocol Data Unit
PIM-DM	Protocol-Independent Multicast Dense mode
PIM-SM	Protocol-Independent Multicast Sparse mode
Primary IP Address	An IP address selected from the set of real interface addresses. One possible selection algorithm is to always select the first address. VRRP advertisements are always sent using the primary IP address as the source of the IP packet.
PoE	Power over Ethernet. Corresponds to the IEEE 802.3AF standard which supports power delivery of up to 15.4W per port.
PoE+	Power over Ethernet Plus. Corresponds to the IEEE 802.3AT standard which supports power delivery of up to 34.2W per port.
PSE	Power Sourcing Equipment
QoS	Quality of Service
RADIUS	Remote Authentication Dial-in User Service
Routing Interface	An IP interface whose physical ports are front panel ports and associated with a VLAN. Packets received on a routing interface can be transmitted on a different VLAN than they were received on.
SDM	Switch Database Management
Service Port	An IP interface on an Ethernet interface that is separate from the front panel ports. The service port is dedicated to management. The service port has its own independent interface to the IP stack. The service port is a host interface.
SM	state machine
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
TFTP	Trivial File Transfer Protocol
TFTP Server	Trivial File Transfer Protocol Servers are servers that hold the requested configuration and/or image files for requested clients.
TLV	Type-Length-Value
UDLD	Uni-Directional Link Detection
UI	User Interface
UPoE	Universal Power over Ethernet. No IEEE standard exists yet for UPoE. UPoE supports power delivery of up to 60W per port.
USB	Universal Serial Bus

415

Virtual Router	An abstract object managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a virtual router identifier and a set of associated IP address(es) across a common LAN. A VRRP router can backup one or more virtual routers
Virtual Router Backup	The set of VRRP routers available to assume forwarding responsibility for a virtual router if the current Master fails.
Virtual Router Master	The VRRP router that is assuming the responsibility of forwarding packets sent to the IP address(es) associated with the virtual router, and answering ARP requests for these IP addresses. Note that if the IP address owner is available, then it will always become the Master.
VLAN	Virtual Local Area Network
VRRP Router	A router running the Virtual Router Redundancy Protocol. It can participate in one or more virtual routers.

416