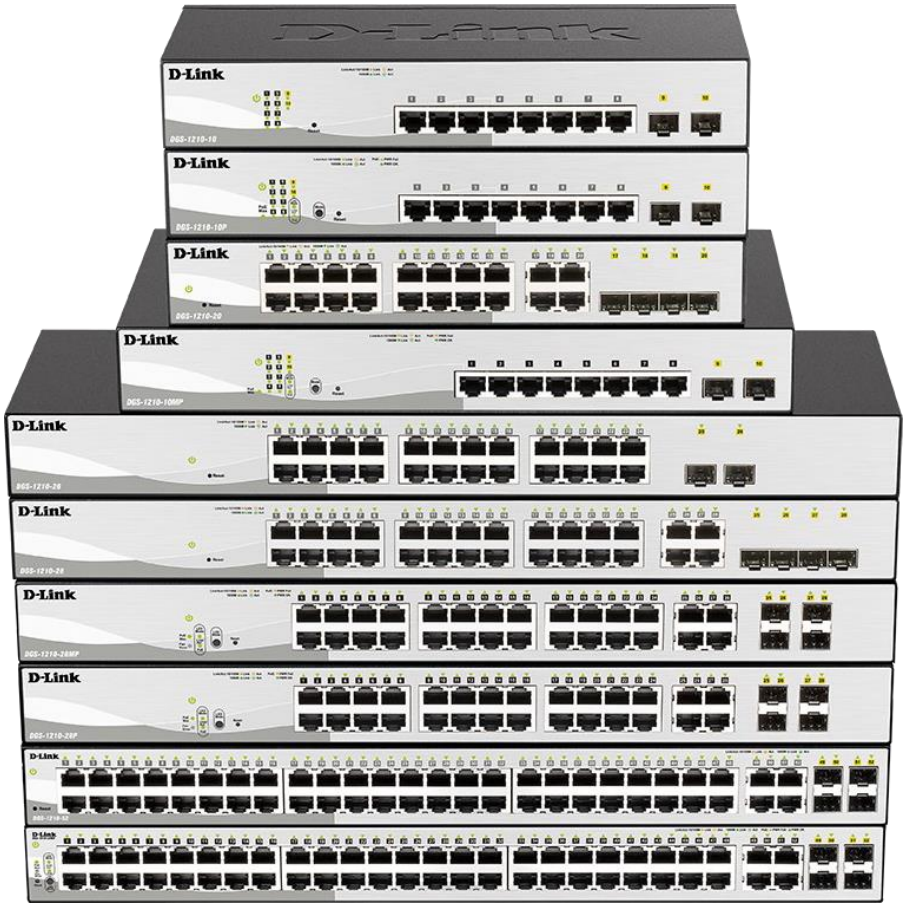
D-Link

버전 6.50 | 3/15/2024



사용자 매뉴얼

Smart Managed Switch

DGS-1210 series

목차

이 가이드에 대하여

이 가이드는 D-Link Smart Managed Switch DGS-1210 시리즈를 설치하고 웹 기반 관리를 단계별로 구성하는 방법에 대한 지침을 제공합니다.

참고: 구매한 모델은 문서에 표시된 그림과 약간 다를 수 있습니다. 스위치, 구성 요소, 네트워크 연결 및 기술 사양에 대한 자세한 내용은 제품 지침 및 기술 사양 섹션을 참조하십시오.

이 가이드는 주로 네 부분으로 나뉩니다.

1. 하드웨어 설치: 단계별 하드웨어 설치 절차
2. 시작하기: 기본 스위치 설치 및 설정을 위한 시작 가이드
3. 웹 구성: 웹을 통한 기능 설명 및 구성 설정에 대한 정보
4. 명령줄 인터페이스: Telnet을 통한 기능 설명 및 구성 설정에 대한 정보.

약관/사용법

이 가이드에서 "스위치"(첫 글자는 대문자)라는 용어는 스마트 스위치를 의미하고 "스위치"(첫 글자는 소문자)는 다른 이더넷 스위치를 의미합니다. 일부 기술은 "스위치", "브리지" 및 "스위칭 허브"라는 용어를 서로 바꿔 부르며, 둘 다 이더넷 스위치에 일반적으로 사용됩니다.

참고는 장치를 더 잘 사용하는 데 도움이 되는 중요한 정보를 나타냅니다.

주의는 잠재적인 재산 피해 또는 개인 상해를 나타냅니다.

저작권 및 상표

1. *제품 소개*

D-Link Smart Managed 스위치 제품을 구매해 주셔서 감사합니다.

D-Link의 차세대 Smart Managed 스위치 시리즈는 플러그 앤 플레이의 간편함과 중소기업(SMB) 네트워킹을 위한 탁월한 가치와 신뢰성을 결합합니다. 모든 모델은 새 스타일의 랙 마운트 금속 케이스에 탑재되어 있으며, 쉽게 볼 수 있는 전면 패널 진단 LED를 갖추고 있으며, 네트워크 보안, 트래픽 분할, QoS 및 다용도의 관리 기능을 포함한 고급 기능을 제공합니다.

유연한 포트 구성. DGS-1210 시리즈는 새로운 세대의 Smart Managed 스위치 시리즈입니다. 8, 16, 24 또는 48개의 10/100/1000Mbps 비 PoE 또는 PoE 포트와 4개의 GE/SFP 포트를 제공합니다. DGS-1210 시리즈의 모든 스위치는 내장된 4개의 기가비트 SFP 업링크를 특징으로 하며, 링, 트리 또는 혼합과 같은 유연한 네트워크 토폴로지 선택을 제공합니다.

D-Link 그린 테크놀러지. D-Link 그린 디바이스는 성능을 저하시키지 않으면서 친환경적인 대안을 제공하는 것을 목표로 합니다. D-Link 그린 테크놀러지에는 DGS-1210 시리즈에서 에너지 소비를 줄이기 위한 여러 혁신이 포함되어 있으며, 예를 들어 포트를 종료하거나 일부 LED 표시등을 끄거나 연결된 이더넷 케이블에 따라 전력 사용을 조정하는 기능 등이 있습니다.

광범위한 레이어 2 기능. 완전한 L2 장치로 구현된 이 스위치들은 IGMP 스누핑, 포트 미러링, 스패닝 트리, 802.3ad LACP 및 루프백 감지와 같은 기능을 포함하여 성능과 네트워크 복원력을 향상시킵니다.

트래픽 분할, QoS 및 자동 감시 VLAN. 스위치는 802.1Q VLAN 표준 태깅을 지원하여 네트워크 보안과 성능을 향상시킵니다. 스위치는 또한 802.1p 우선순위 큐를 지원하여 사용자가 네트워크에서 해당 트래픽의 우선순위를 지정하여 스트리밍 멀티미디어와 같은 대역폭 민감 애플리케이션을 실행할 수 있게 합니다. 이러한 기능은 스위치가 네트워크, 내 VLAN 및 802.1p 트래픽과 원활하게 작동할 수 있도록 합니다. 자동 감시 VLAN은 미리 정의된 IP 감시 장치에서 비디오 트래픽을 높은 우선순위가 할당된 VLAN으로 자동으로 배치하여 일반 데이터 트래픽과 분리될 수 있도록 합니다. 비대칭 VLAN은 서버 또는 게이트웨이 장치와 게이트웨이 같은 공유 자원의 보다 효율적인 사용을 위해 이러한 스위치에 구현되어 있습니다.

네트워크 보안. D-Link의 혁신적인 Safeguard Engine 기능은 바이러스 공격으로 인한 트래픽 플러딩으로부터 스위치를 보호합니다. 802.1X 포트 기반 인증과 같은 추가 기능은 외부 RADIUS 서버와 함께 네트워크 접근 제어를 제공합니다. ACL은 원하지 않는 IP 또는 MAC 트래픽을 차단하는 강력한 도구입니다. Storm Control은 비정상적인 트래픽으로 인해 네트워크가 과부하되는 것을 방지하는 데 도움이 됩니다. 포트 보안은 네트워크 장치의 무결성을 유지하기 위한 또 다른 간단하지만 유용한 인증 방법입니다.

다용도의 관리. 차세대 D-Link Smart Managed 스위치는 성장하는 비즈니스가 네트워크를 간단하고 쉽게 관리할 수

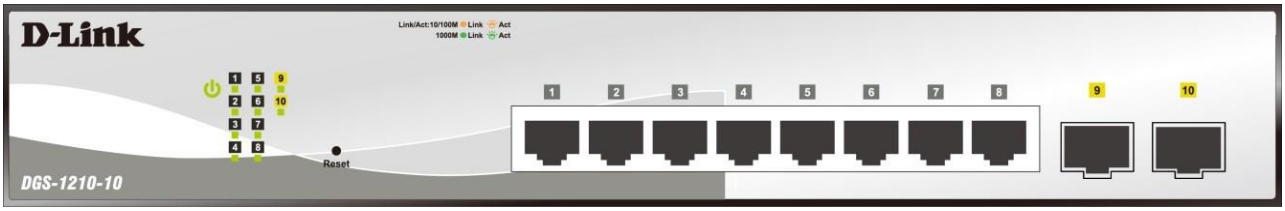
있도록 합니다. 다국어 웹 기반 관리 인터페이스를 통해 관리자는 포트 수준까지 원격으로 네트워크를 제어할 수 있습니다. 직관적인 인터페이스는 고객이 동일한 L2 네트워크 세그먼트에서 여러 D-Link Smart Managed 스위치를 쉽게 발견할 수 있게 합니다. 이 유틸리티를 사용하면 사용자는 PC의 IP 주소를 변경할 필요 없이 스마트 스위치의 초기 설정을 쉽게 할 수 있습니다. 사용자 로컬 PC에 연결된 동일한 L2 네트워크 세그먼트 내의 스위치는 화면에 표시되어 화면에 표시되어 있습니다. 즉시 접근할 수 있습니다. 이는 광범위한 스위치 구성 설정과 비밀번호 변경 또는 펌웨어 업그레이드와 같은 발견된 장치의 기본 구성을 허용합니다.

사용자는 Telnet을 통해 스위치에 접근할 수도 있습니다. 스위치의 IP 주소 변경, 설정을 공장 초기값으로 재설정, 관리자 비밀번호 설정, 스위치 재부팅 또는 스위치 펌웨어 업그레이드와 같은 기본 작업을 명령줄 인터페이스(CLI)를 사용하여 수행할 수 있습니다.

또한, 사용자는 SNMP MIB(Management Information Base)를 활용하여 스위치의 상태에 대한 정보를 폴링하거나 비정상적인 이벤트의 트랩을 보낼 수 있습니다. SNMP 지원을 통해 사용자는 SNMP가 지원되는 환경에서 다른 서드파티 장치와 스위치를 통합하여 관리할 수 있습니다. D-Link Smart Managed Switches는 사용하기 쉬운 그래픽 인터페이스를 제공하여 운영 효율성을 향상시킵니다.

DGS - 1210-10

8포트 10/100/1000Mbps 및 SFP 포트 2개(100/1000Mbps) 스마트 매니지드 스위치.



전면 패널

그림 1.1 - DGS-1210-10 전면 패널

DGS-1210-10 스위치의 전면 패널은 다음과 같이 구성됩니다.

- **Power LED** : 스위치가 전원에 연결되면 Power LED가 켜집니다.
- **포트 링크/작동/속도 LED (1-8):** 링크/작동/속도 LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트에 호박색 빛이 있을 경우, 포트가 10M 또는 100M에서 작동 중임을 나타냅니다. 녹색 빛이 있을 경우, 1000M에서 작동 중임을 나타냅니다.
- **포트 링크/작동/속도 LED(9F, 10F):** 링크/작동/속도 LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트 LED가 호박색으로 빛나면 포트가 100M에서 작동 중임을 나타냅니다. 포트 LED가 녹색으로 빛나면 1000Mbps에서 작동 중임을 나타냅니다.
- **재설정:** Reset 버튼을 1-5초 동안 누르면 장치가 재부팅됩니다. 6-10초 동안 누르면 스위치가 기본 설정으로 재설정되며 LED가 2초 동안 호박색으로 지속적으로 켜집니다. 또는 Reset 버튼을 11초 이상 누르면 장치가 재부팅된 후 로더 모드로 들어가며 LED가 2초 동안 녹색으로 지속적으로 켜집니다. 장치가 이미지 1 및 이미지 2를 통해 스위치를 재부팅 할 수 없으면 자동으로 로더 모드로 들어갑니다.

주의: 이 제품은 UL 인증을 받은 광 트랜시버 제품(정격 DC3.3V, 레이저 클래스 I)과 함께 사용하기 위한 것입니다.

주의: 장비 전원 공급 코드는 접지 연결이 있는 소켓-아웃렛에 연결되어야 합니다.

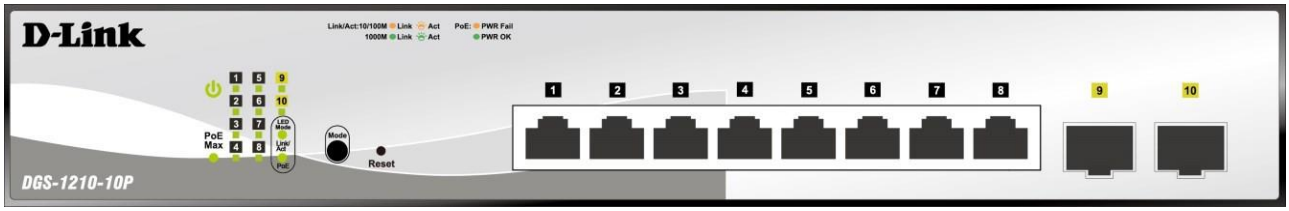
후면 패널

그림 1.2 - DGS-1210-10 후면 패널

Power: 제공된 AC 전원 케이블을 이 포트에 연결합니다.

DGS-1210-10P

8포트 10/100/1000Mbps 및 SFP 포트 2개(100/1000Mbps) 스마트 관리형 PoE 스위치.



전면 패널

그림 1.3 – DGS-1210-10P 전면 패널

DGS-1210-10P 스위치의 전면 패널은 다음과 같이 구성됩니다.

- **Power LED:** 스위치가 전원에 연결되면 Power LED가 켜집니다.
- **PoE Max:** PoE Max LED는 관리자가 웹 GUI의 PoE 시스템 설정 페이지를 통해 정의한 최대 전력 예산 또는 기본 전력 예산 65W에 도달하면 호박색으로 지속적으로 켜집니다.
- **포트 링크/작동/속도 LED (1-8):** 링크/작동/속도 LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트에 호박색 빛이 있을 경우, 포트가 10M 또는 100M에서 작동 중임을 나타냅니다. 녹색 빛이 있을 경우, 1000M에서 작동 중임을 나타냅니다.
- **포트 링크/작동/속도 LED(9F, 10F):** 링크/작동/속도 LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트 LED가 호박색으로 빛나면 포트가 100M에서 작동 중임을 나타냅니다. 포트 LED가 녹색으로 빛나면 1000Mbps에서 작동 중임을 나타냅니다.
- **LED Mode:** 포트 LED의 모드를 선택하기 위해, 모드 버튼 아래의 Link/Act 및 PoE LED가 선택된 모드를 나타내기 위해 지속적으로 녹색으로 켜집니다.
- **Mode:** Mode 버튼을 눌러 포트 LED를 Link/Act 모드와 PoE 모드 사이에서 전환할 수 있습니다.
- **재설정:** Reset 버튼을 1-5초 동안 누르면 장치가 재부팅됩니다. 6-10초 동안 누르면 스위치가 기본 설정으로 재설정되며 LED가 2초 동안 호박색으로 지속적으로 켜집니다. 또는 Reset 버튼을 11초 이상 누르면 장치가 재부팅된 후 로더 모드로 들어가며 LED가 2초 동안 녹색으로 지속적으로 켜집니다. 장치가 이미지 1 및 이미지 2를 통해 스위치를 재부팅 할 수 없으면 자동으로 로더 모드로 들어갑니다.

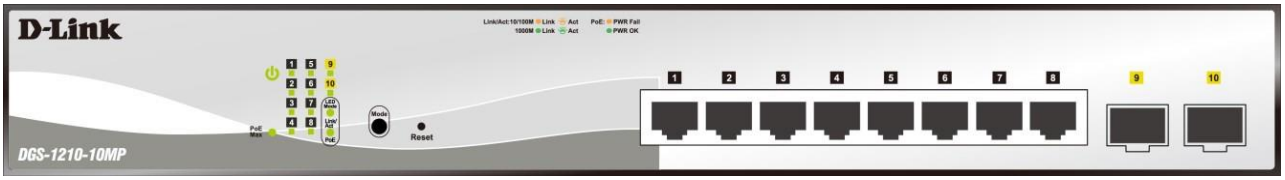
후면 패널

그림 1.4 – DGS-1210-10P 후면 패널

Power: 제공된 DC 외부 전원 54V/1.574A 케이블을 이 포트에 연결합니다.

DGS-1210-10MP

8포트 10/100/1000Mbps 및 SFP 포트 2개(100/1000Mbps) 스마트 관리형 PoE 스위치.

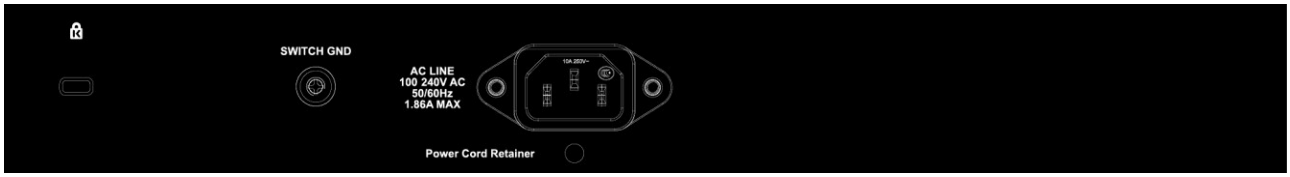


전면 패널

그림 1.5 - DGS-1210-10MP 전면 패널

DGS-1210-10MP 스위치의 전면 패널은 다음과 같이 구성됩니다.

- **Power LED:** 스위치가 전원에 연결되면 Power LED가 켜집니다.
- **PoE Max:** 스위치가 관리자가 웹 GUI의 PoE 시스템 설정 페이지를 통해 정의한 최대 전력 예산 또는 기본 전력 예산인 130W에 도달하면 PoE Max LED가 호박색으로 지속적으로 켜집니다.
- **포트 링크/작동/속도 LED (1-8):** 링크/작동/속도 LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트에 호박색 빛이 있을 경우, 포트가 10M 또는 100M에서 작동 중임을 나타냅니다. 녹색 빛이 있을 경우, 1000M에서 작동 중임을 나타냅니다.
- **포트 링크/작동/속도 LED(9F, 10F):** 링크/작동/속도 LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트 LED가 호박색으로 빛나면 포트가 100M에서 작동 중임을 나타냅니다. 포트 LED가 녹색으로 빛나면 1000Mbps에서 작동 중임을 나타냅니다.
- **LED Mode:** 포트 LED의 모드를 선택하기 위해, 모드 버튼 아래의 Link/Act 및 PoE LED가 선택된 모드를 나타내기 위해 지속적으로 녹색으로 켜집니다.
- **Mode:** Mode 버튼을 눌러 포트 LED를 Link/Act 모드와 PoE 모드 사이에서 전환할 수 있습니다.
- **재설정:** Reset 버튼을 1-5초 동안 누르면 장치가 재부팅됩니다. 6-10초 동안 누르면 스위치가 기본 설정으로 재설정되며 LED가 2초 동안 호박색으로 지속적으로 켜집니다. 또는 Reset 버튼을 11초 이상 누르면 장치가 재부팅된 후 로더 모드로 들어가며 LED가 2초 동안 녹색으로 지속적으로 켜집니다. 장치가 이미지 1 및 이미지 2를 통해 스위치를 재부팅 할 수 없으면 자동으로 로더 모드로 들어갑니다.



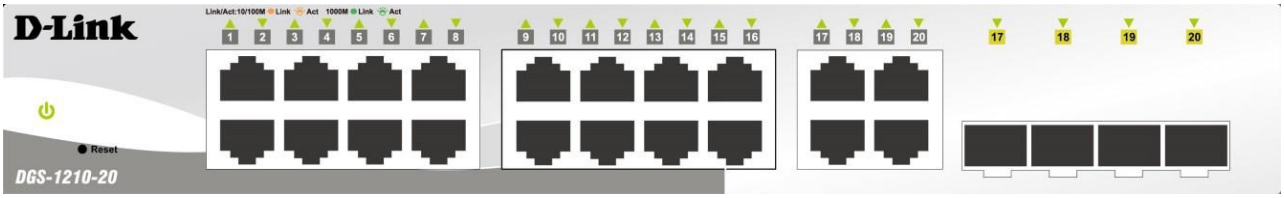
후면 패널

그림 1.6 – DGS-1210-10MP 후면 패널

Power: 제공된 AC 전원 케이블을 이 포트에 연결합니다.

DGS-1210-20

16포트 10/100/1000Mbps 및 4콤보 GE/SFP 슬롯 스마트 매니지드 스위치.

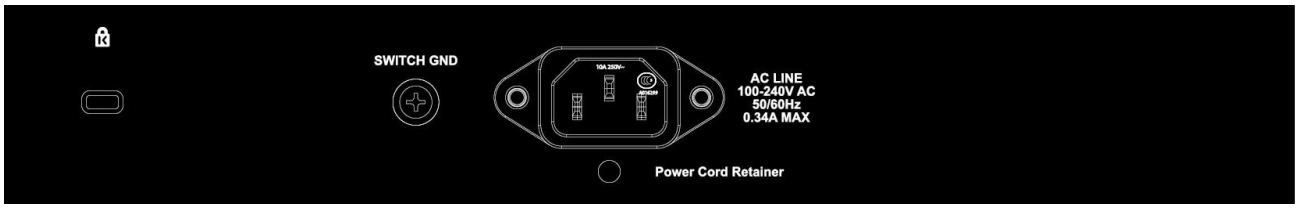


전면 패널

그림 1.7 - DGS-1210-20 전면 패널

DGS-1210-20 스위치의 전면 패널은 다음과 같이 구성됩니다.

- **Power LED:** 스위치가 전원에 연결되면 Power LED가 켜집니다.
- **Port Link/Act/Speed LED (1-16):** Link/Act/Speed LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트에 호박색 빛이 있을 경우, 포트가 10M 또는 100M에서 작동 중임을 나타냅니다. 녹색 빛이 있을 경우, 1000M에서 작동 중임을 나타냅니다.
- **포트 링크/작동/속도 LED (17F, 18F, 19F, 20F, 17T, 18T, 19T, 20T):** 링크/작동/속도 LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트 LED가 호박색으로 빛나면 포트가 100M에서 작동 중임을 나타냅니다. 포트 LED가 녹색으로 빛나면 1000Mbps에서 작동 중임을 나타냅니다.
- **재설정:** Reset 버튼을 1-5초 동안 누르면 장치가 재부팅됩니다. 6-10초 동안 누르면 스위치가 기본 설정으로 재설정되며 LED가 2초 동안 호박색으로 지속적으로 켜집니다. 또는 Reset 버튼을 11초 이상 누르면 장치가 재부팅된 후 로더 모드로 들어가며 LED가 2초 동안 녹색으로 지속적으로 켜집니다. 장치가 이미지 1 및 이미지 2를 통해 스위치를 재부팅 할 수 없으면 자동으로 로더 모드로 들어갑니다.



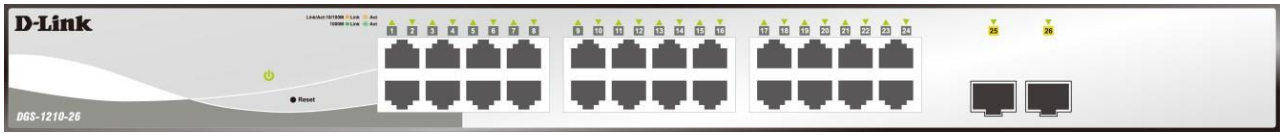
후면 패널

그림 1.8 – DGS-1210-20 후면 패널

Power: 제공된 AC 전원 케이블을 이 포트에 연결합니다.

DGS-1210-26

24포트 10/100/1000Mbps 및 2개의 SFP 포트(100/1000Mbps) 스마트 매니지드 스위치.



전면 패널

그림 1.9 – DGS-1210-26 전면 패널

DGS-1210-26 스위치의 전면 패널은 다음과 같이 구성됩니다.

- **Power LED:** 스위치가 전원에 연결되면 Power LED가 켜집니다.
- **Port Link/Act/Speed LED (1-24):** Link/Act/Speed LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트에 호박색 빛이 있을 경우, 포트가 10M 또는 100M에서 작동 중임을 나타냅니다. 녹색 빛이 있을 경우, 1000M에서 작동 중임을 나타냅니다.
- **포트 링크/작동/속도 LED(25F, 26F):** 링크/작동/속도 LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트 LED가 호박색으로 빛나면 포트가 100M에서 작동 중임을 나타냅니다. 포트 LED가 녹색으로 빛나면 1000Mbps에서 작동 중임을 나타냅니다.
- **재설정:** Reset 버튼을 1-5초 동안 누르면 장치가 재부팅됩니다. 6-10초 동안 누르면 스위치가 기본 설정으로 재설정되며 LED가 2초 동안 호박색으로 지속적으로 켜집니다. 또는 Reset 버튼을 11초 이상 누르면 장치가 재부팅된 후 로더 모드로 들어가며 LED가 2초 동안 녹색으로 지속적으로 켜집니다. 장치가 이미지 1 및 이미지 2를 통해 스위치를 재부팅 할 수 없으면 자동으로 로더 모드로 들어갑니다.

후면 패널

그림 1.10 – DGS-1210-26 후면 패널

Power: 제공된 AC 전원 케이블을 이 포트에 연결합니다.

DGS - 1210-28

24포트 10/100/1000Mbps 및 4콤보 GE/SFP 슬롯 스마트 매니지드 스위치.

전면 패널

그림 1.11 - DGS-1210-28 전면 패널

DGS-1210-28 스위치의 전면 패널은 다음과 같이 구성됩니다.

- **Power LED :** 스위치가 전원에 연결되면 Power LED가 켜집니다.
- **Port Link/Act/Speed LED (1-24):** Link/Act/Speed LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트에 호박색 빛이 있을 경우, 포트가 10M 또는 100M에서 작동 중임을 나타냅니다. 녹색 빛이 있을 경우, 1000M에서 작동 중임을 나타냅니다.
- **포트 링크/작동/속도 LED (25F, 26F, 27F, 28F, 25T, 26T, 27T, 28T):** 링크/작동/속도 LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트 LED가 호박색으로 빛나면 포트가 100M에서 작동 중임을 나타냅니다. 포트 LED가 녹색으로 빛나면 1000Mbps에서 작동 중임을 나타냅니다.
- **재설정:** Reset 버튼을 1-5초 동안 누르면 장치가 재부팅됩니다. 6-10초 동안 누르면 스위치가 기본 설정으로 재설정되며 LED가 2초 동안 호박색으로 지속적으로 켜집니다. 또는 Reset 버튼을 11초 이상 누르면 장치가 재부팅된 후 로더 모드로 들어가며 LED가 2초 동안 녹색으로 지속적으로 켜집니다. 장치가 이미지 1 및 이미지 2를 통해 스위치를 재부팅 할 수 없으면 자동으로 로더 모드로 들어갑니다.

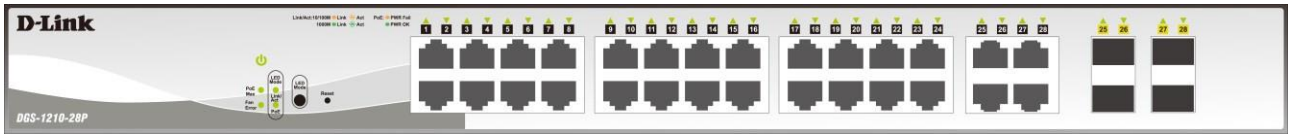
후면 패널

그림 1.12 - DGS-1210-28 후면 패널

Power: 제공된 AC 전원 케이블을 이 포트에 연결합니다.

DGS-1210-28P

24포트 10/100/1000Mbps 및 4콤보 GE/SFP 스마트 관리형 PoE 스위치.



전면 패널

그림 1.13 - DGS-1210-28P 전면 패널

DGS-1210-28P 스위치의 전면 패널은 다음과 같이 구성됩니다.

- **Power LED :** 스위치가 전원에 연결되면 Power LED가 켜집니다.
- **Fan Error:** FAN LED는 팬의 상태를 표시합니다. 불이 꺼져 있으면 모든 팬이 정상적으로 작동함을 나타내며, 빨간불은 하나 이상의 팬이 비정상적으로 작동하고 있음을 나타냅니다.
- **PoE Max:** 스위치가 관리자가 웹 GUI의 PoE 시스템 설정 페이지를 통해 정의한 최대 전력 예산 또는 기본 전력 예산인 193W에 도달하면 PoE Max LED가 호박색으로 지속적으로 켜집니다.
- **LED Mode:** 포트 LED의 모드를 선택하기 위해, 모드 버튼 아래의 Link/Act 및 PoE LED가 선택된 모드를 나타내기 위해 지속적으로 녹색으로 켜집니다.
- **Port Link/Act/Speed LED (1-24):** Link/Act/Speed LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트에 호박색 빛이 있을 경우, 포트가 10M 또는 100M에서 작동 중임을 나타냅니다. 녹색 빛이 있을 경우, 1000M에서 작동 중임을 나타냅니다.
- **포트 링크/작동/속도 LED (25F, 26F, 27F, 28F, 25T, 26T, 27T, 28T):** 링크/작동/속도 LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트 LED가 호박색으로 빛나면 포트가 100M에서 작동 중임을 나타냅니다. 포트 LED가 녹색으로 빛나면 1000Mbps에서 작동 중임을 나타냅니다.
- **재설정:** Reset 버튼을 1-5초 동안 누르면 장치가 재부팅 됩니다. 6-10초 동안 누르면 스위치가 기본 설정으로 재설정되며 LED가 2초 동안 호박색으로 지속적으로 켜집니다. 또는 Reset 버튼을 11초 이상 누르면 장치가 재부팅 된 후 로더 모드로 들어가며 LED가 2초 동안 녹색으로 지속적으로 켜집니다. 장치가 이미지 1 및 이미지 2를 통해 스위치를 재부팅 할 수 없으면 자동으로 로더 모드로 들어갑니다.
- **LED Mode:** Mode 버튼을 눌러 포트 LED를 Link/Act 모드와 PoE 모드 사이에서 전환할 수 있습니다.

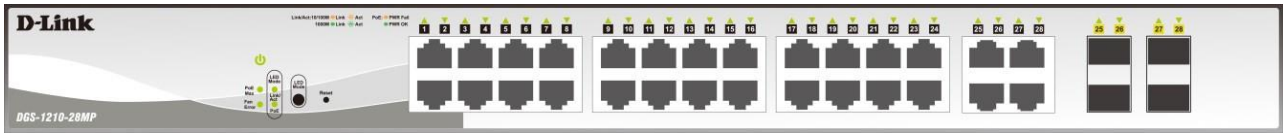
후면 패널

그림 1.14 – DGS-1210-28P 후면 패널

Power: 제공된 AC 전원 케이블을 이 포트에 연결합니다.

DGS-1210-28P

24포트 10/100/1000Mbps 및 4콤보 GE/SFP 슬롯 스마트 관리형 PoE 스위치.



전면 패널

그림 1.15 - DGS-1210-28MP 전면 패널

DGS-1210-28MP 스위치의 전면 패널은 다음과 같이 구성됩니다.

- **Power LED:** 스위치가 전원에 연결되면 Power LED가 켜집니다.
- **Fan Error:** FAN LED는 팬의 상태를 표시합니다. 불이 꺼져 있으면 모든 팬이 정상적으로 작동함을 나타내며, 빨간 불은 하나 이상의 팬이 비정상적으로 작동하고 있음을 나타냅니다.
- **PoE Max:** 스위치가 관리자가 웹 GUI의 PoE 시스템 설정 페이지를 통해 정의한 최대 전력 예산 또는 기본 전력 예산인 370W에 도달하면 PoE Max LED가 호박색으로 지속적으로 켜집니다.
- **LED Mode:** 포트 LED의 모드를 선택하기 위해, 모드 버튼 아래의 Link/Act 및 PoE LED가 선택된 모드를 나타내기 위해 지속적으로 녹색으로 켜집니다.
- **Port Link/Act/Speed LED (1-24):** Link/Act/Speed LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트에 호박색 빛이 있을 경우, 포트가 10M 또는 100M에서 작동 중임을 나타냅니다. 녹색 빛이 있을 경우, 1000M에서 작동 중임을 나타냅니다.
- **포트 링크/작동/속도 LED (25F, 26F, 27F, 28F, 25T, 26T, 27T, 28T):** 링크/작동/속도 LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트 LED가 호박색으로 빛나면 포트가 100M에서 작동 중임을 나타냅니다. 포트 LED가 녹색으로 빛나면 1000Mbps에서 작동 중임을 나타냅니다.
- **재설정:** Reset 버튼을 1-5초 동안 누르면 장치가 재부팅 됩니다. 6-10초 동안 누르면 스위치가 기본 설정으로 재설정되며 LED가 2초 동안 호박색으로 지속적으로 켜집니다. 또는 Reset 버튼을 11초 이상 누르면 장치가 재부팅 된 후 로더 모드로 들어가며 LED가 2초 동안 녹색으로 지속적으로 켜집니다. 장치가 이미지 1 및 이미지 2를 통해 스위치를 재부팅 할 수 없으면 자동으로 로더 모드로 들어갑니다.
- **LED Mode:** Mode 버튼을 눌러 포트 LED를 Link/Act 모드와 PoE 모드 사이에서 전환할 수 있습니다.

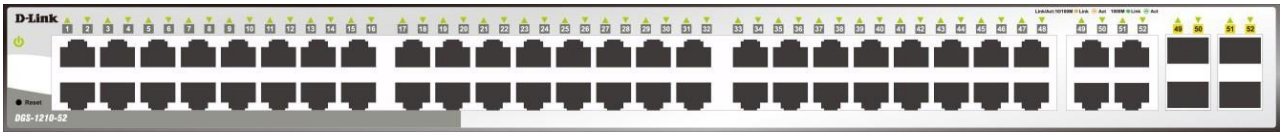
후면 패널

그림 1.16 - DGS-1210-28MP 후면 패널

Power: 제공된 AC 전원 케이블을 이 포트에 연결합니다.

DGS - 1210-52

48포트 10/100/1000Mbps 및 4콤보 GE/SFP 슬롯 스마트 매니지드 스위치.



전면 패널

그림 1.17 - DGS-1210-52 전면 패널

DGS-1210-52 스위치의 전면 패널은 다음과 같이 구성됩니다.

- **Power LED:** 스위치가 전원에 연결되면 Power LED가 켜집니다.
- **Port Link/Act/Speed LED (1-48):** Link/Act/Speed LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트에 호박색 빛이 있을 경우, 포트가 10M 또는 100M에서 작동 중임을 나타냅니다. 녹색 빛이 있을 경우, 1000M에서 작동 중임을 나타냅니다.
- **포트 링크/작동/속도 LED (49F, 50F, 51F, 52F, 49T, 50T, 51T, 52T):** 링크/작동/속도 LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트 LED가 호박색으로 빛나면 포트가 100M에서 작동 중임을 나타냅니다. 포트 LED가 녹색으로 빛나면 1000Mbps에서 작동 중임을 나타냅니다.
- **재설정:** Reset 버튼을 1-5초 동안 누르면 장치가 재부팅 됩니다. 6-10초 동안 누르면 스위치가 기본 설정으로 재설정되며 LED가 2초 동안 호박색으로 지속적으로 켜집니다. 또는 Reset 버튼을 11초 이상 누르면 장치가 재부팅 된 후 로더 모드로 들어가며 LED가 2초 동안 녹색으로 지속적으로 켜집니다. 장치가 이미지 1 및 이미지 2를 통해 스위치를 재부팅 할 수 없으면 자동으로 로더 모드로 들어갑니다.

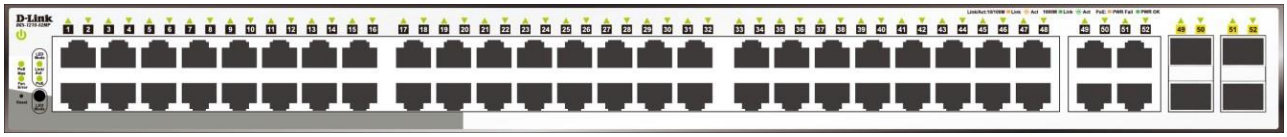
후면 패널

그림 1.18 – DGS-1210-52 후면 패널

Power: 제공된 AC 전원 케이블을 이 포트에 연결합니다.

DGS-1210-52MP

48포트 10/100/1000Mbps 및 4콤보 GE/SFP 스마트 관리형 PoE 스위치.



전면 패널

그림 1.19 - DGS-1210-52MP 전면 패널

DGS-1210-52MP 스위치의 전면 패널은 다음과 같이 구성됩니다.

- **Power LED :** 스위치가 전원에 연결되면 Power LED가 켜집니다.
- **Fan Error:** FAN LED는 팬의 상태를 표시합니다. 불이 꺼져 있으면 모든 팬이 정상적으로 작동함을 나타내며, 빨간불은 하나 이상의 팬이 비정상적으로 작동하고 있음을 나타냅니다.
- **PoE Max:** 스위치가 관리자가 웹 GUI의 PoE 시스템 설정 페이지를 통해 정의한 최대 전력 예산 또는 기본 전력 예산인 370W에 도달하면 PoE Max LED가 호박색으로 지속적으로 켜집니다.
- **LED Mode:** 포트 LED의 모드를 선택하기 위해, 모드 버튼 아래의 Link/Act 및 PoE LED가 선택된 모드를 나타내기 위해 지속적으로 녹색으로 켜집니다.
- **Port Link/Act/Speed LED (1-48):** Link/Act/Speed LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트에 호박색 빛이 있을 경우, 포트가 10M 또는 100M에서 작동 중임을 나타냅니다. 녹색 빛이 있을 경우, 1000M에서 작동 중임을 나타냅니다.
- **포트 링크/작동/속도 LED (49F, 50F, 51F, 52F, 49T, 50T, 51T, 52T):** 링크/작동/속도 LED가 깜빡이며 해당 포트를 통한 네트워크 링크를 나타냅니다. 깜빡임은 스위치가 포트로 데이터를 보내거나 받고 있음을 의미합니다. 포트 LED가 호박색으로 빛나면 포트가 100M에서 작동 중임을 나타냅니다. 포트 LED가 녹색으로 빛나면 1000Mbps에서 작동 중임을 나타냅니다.
- **재설정:** Reset 버튼을 1-5초 동안 누르면 장치가 재부팅 됩니다. 6-10초 동안 누르면 스위치가 기본 설정으로 재설정되며 LED가 2초 동안 호박색으로 지속적으로 켜집니다. 또는 Reset 버튼을 11초 이상 누르면 장치가 재부팅 된 후 로더 모드로 들어가며 LED가 2초 동안 녹색으로 지속적으로 켜집니다. 장치가 이미지 1 및 이미지 2를 통해 스위치를 재부팅 할 수 없으면 자동으로 로더 모드로 들어갑니다.
- **LED Mode:** Mode 버튼을 눌러 포트 LED를 Link/Act 모드와 PoE 모드 사이에서 전환할 수 있습니다.

후면 패널

그림 1.20 – DGS-1210-52MP 후면 패널

Power: 제공된 AC 전원 케이블을 이 포트에 연결합니다.

LED 표시등

스위치는 각 포트에 대한 전원, 팬 및 링크/활동용 LED 표시기를 지원합니다.

다음은 DGS-1210 시리즈 Smart Managed 스위치의 LED 표시와 각 표시에 대한 설명을 보여줍니다.

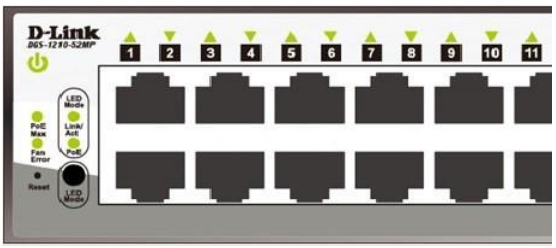


그림 1.21 - DGS-1210 시리즈의 LED 표시등

위치	LED 표시	색깔	상태	설명
장치당	힘	초록	점등	전원 켜짐
			꺼짐	전원 꺼짐
	팬 오류 (DGS-1210-28P/28MP/52MP의 경우)	빨강	점등	팬에 런타임 오류가 발생하여 오프라인 상태로 전환되었습니다.
	PoE 최대 (DGS-1210-10P / 10MP / 28P / 28MP / 52MP의 경우)	주황	점등	스위치의 총 PoE 출력이 DGS-1210-10P의 경우 65W, DGS-1210-10MP의 경우 130W, DGS-1210-28P의 경우 193W, 그리고 DGS-1210-28MP/52MP의 경우 370W에 도달하거나 이를 초과하면 PoE Max LED가 켜집니다. 이 상태에서는 추가적인 PoE 장치를 지원할 수 없습니다.
			점멸	스위치의 총 PoE 출력이 가드 밴드 모드에 도달했습니다. (최대 PoE 예산 < 7 W)
			꺼짐	시스템 전력 사용량이 가드 밴드 범위에 도달하지 않을 때
10/100/1000Mbps 구리 포트당 LED	링크/행위	초록/주황	초록 점등	포트 중 하나에서 안정적인 1000Mbps 이더넷 연결(또는 링크)이 있을 때
			초록 점멸	1000Mbps 이더넷 연결 포트에서 데이터의 수신 또는 전송(즉, 활동—Act)이 발생할 때
			주황 점등	포트 중 하나에서 안정적인 10/100Mbps 이더넷 연결(또는 링크)이 있을 때
			주황 점멸	10/100Mbps 이더넷 연결 포트에서 데이터의 수신 또는 전송(즉, 활동—Act)이 발생할 때..
			꺼짐	링크 없음
	PoE 모드	초록	점등	전력 공급 중
		주황	점등	오류 상태
		꺼짐	꺼짐	전력 공급 없음
100/1000Mbps SFP 포트당 LED	링크/행위	초록/주황	초록 점등	포트 중 하나에서 안정적인 1000Mbps 이더넷 연결(또는 링크)이 있을 때
			초록 점멸	포트가 1000Mbps 이더넷에 연결되어 있을 때 데이터의 수신 또는 전송(즉, 활동—Act)이 발생할 때
			주황 점등	포트 중 하나에서 안정적인 100Mbps 이더넷 연결(또는 링크)이 있을 때
			주황 점멸	포트가 100Mbps 이더넷에 연결되어 있을 때 데이터의 수신 또는 전송(즉, 활동—Act)이 발생할 때
		꺼짐	꺼짐	링크 없음

2. *하드웨어 설치*

이 장에서는 D-Link Smart Managed Switch의 개봉 및 설치 정보를 제공합니다.

안전 주의 사항

신체 상해, 감전, 화재 및 장비 손상의 위험을 줄이기 위해 다음 예방 조치를 준수하십시오.

- 서비스 표시 준수
  - 시스템 문서에 설명된 경우를 제외하고는 어떤 제품도 서비스하지 마십시오.
  - 번개 모양의 삼각형 기호가 표시된 커버를 열거나 제거하면 감전될 수 있습니다.
- 숙련된 서비스 기술자만 이러한 내부 구성 요소에 대한 서비스를 제공해야 합니다.
- 다음 사항 중 하나가 발생하면 제품을 전원 콘센트에서 분리하고 부품을 교체하거나 숙련된 서비스 제공 업체에 연락하십시오.
  - 전원 케이블, 연장 케이블 또는 플러그가 손상된 경우
  - 물체가 제품 내부로 떨어진 경우
  - 제품이 물에 노출된 경우
  - 제품이 떨어지거나 손상된 경우
  - 작동 지침을 준수했지만 제품이 동작하지 않는 경우.
- 시스템을 라디에이터 및 열원에서 멀리 유지하고, 냉각 통풍구를 막지 마십시오.
- 시스템의 개방부에 물체를 밀어 넣지 마십시오. 이는 내부 구성 요소의 단락으로 인해 화재 또는 감전의 원인이 될 수 있습니다
- 시스템 구성 요소에 음식물이나 액체를 쏟지 마십시오. 절대로 젖은 환경에서 제품을 작동하지 마십시오. 시스템이 젖은 경우, 훈련된 서비스 제공업체에 연락하십시오.
- 제품은 승인된 장비와만 사용하십시오.
- 커버를 제거하거나 내부 구성 요소를 만지기 전에 제품이 식도록 하십시오.
- 전기 등급 라벨에 표시된 유형의 외부 전원 소스에서만 제품을 작동하십시오. 필요한 전원 소스 유형이 확실하지 않으면 서비스 제공업체나 지역 전력 회사에 문의하십시오.
- 연결된 장치가 위치에서 사용 가능한 전원으로 작동하도록 전기적으로 평가되었는지 확인하십시오.
- 시스템에 대한 전원 케이블이 제공되지 않았거나 시스템용으로 의도된 AC 전원 옵션이 있는 경우, 해당 국가에서 사용이 승인된 전원 케이블을 구입하십시오. 전원 케이블은 제품의 전기 등급 라벨에 표시된 전압 및 전류에 맞게 평가되어야 합니다. 케이블의 전압 및 전류 등급은 제품에 표시된 등급보다 커야 합니다.
- 시스템 및 주변 장치의 전원 케이블을 적절히 접지된 전기 콘센트에 연결하십시오.
- 이 케이블은 적절한 접지를 보장하기 위해 3구 플러그가 장착되어 있습니다. 어댑터 플러그를 사용하거나 케이블의 접지 핀을 제거하지 마십시오. 연장 케이블을 사용해야 하는 경우, 적절히 접지된 플러그가 있는 3선 케이블을 사용하십시오.
- 연장 케이블 또는 전원 스트립에 연결된 모든 제품의 총 암페어 등급이 연장 케이블 또는 전원 스트립의 암페어 등급 한도를 80% 초과하지 않도록 하십시오.
- 갑작스러운 일시적인 전력 증감으로부터 시스템을 보호하기 위해 서지 억제기, 라인 컨디셔너 또는 무정전 전원

공급장치(UPS)를 사용하십시오.

- 시스템 케이블 및 전원 케이블을 주의 깊게 배치하십시오. 케이블이 히밟거나 걸려 넘어지지 않도록 경로를 정하십시오. 케이블 위에 아무것도 놓지 않도록 하십시오.
- 전원 케이블이나 플러그를 수정하지 마십시오. 현장 수정을 위해서는 면허가 있는 전기기사나 전력 회사에 문의하십시오.
- 항상 지역/국가의 배선 규칙을 준수하십시오
- 시스템에 제공되는 경우, 핫 플러그 가능한 전원 공급 장치의 전원을 연결하거나 분리할 때 다음 지침을 준수하십시오.
  - 전원 공급 장치를 설치한 후 전원 케이블을 전원 공급 장치에 연결하십시오.
  - 전원 공급 장치를 제거하기 전에 전원 케이블을 분리하십시오.
  - 시스템에 여러 전원 공급원이 있는 경우, 모든 전원 케이블을 전원 공급 장치에서 분리하여 시스템의 전원을 차단하십시오.
- 제품을 조심스럽게 이동시키고, 모든 캐스터 및/또는 안정 장치가 시스템에 단단히 연결되어 있는지 확인하십시오. 갑작스러운 정지와 고르지 않은 표면을 피하십시오.

1단계: 개봉

배송 상자를 열고 내용을 주의 깊게 개봉하십시오. 모든 항목이 누락되지 않고 손상되지 않았는지 확인하려면 사용자 매뉴얼에 있는 포장 목록을 참조하십시오. 항목이 누락되었거나 손상된 경우, 지역 D-Link 리셀러에 연락하여 교체하십시오.

- 하나의 D-Link DGS-1210 스마트 관리형 스위치
- 하나의 빠른 시작 가이드
- 전원 코드 및 전원 코드 고정 장치 또는 외부 전원 어댑터(DGS-1210-10P 전용)
- 랙 마운트 키트 및 고무 발

항목이 누락되었거나 손상된 경우, 지역 리셀러에 연락하여 교체하십시오.

2단계: 스위치 설치

안전한 스위치 설치 및 작동을 위해 다음을 권장합니다.

- 전원 코드가 교류 전원 커넥터에 완전히 연결되어 있는지 육안으로 검사하십시오.
- 스위치 주변에 적절한 열 방산 및 충분한 환기가 있는지 확인하십시오.
- 스위치 위에 무거운 물체를 놓지 마십시오.

데스크톱 또는 선반 설치

스위치를 데스크톱이나 선반에 설치할 때, 장치와 함께 제공된 고무 발을 장치 베이스의 각 모서리에 부착해야 합니다. 장치와 주변 물체 사이에 충분한 환기 공간을 확보하십시오.

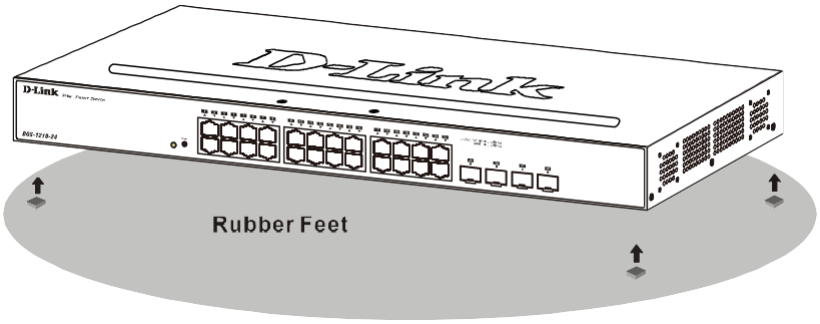


그림 2.1 – 하단에 접착식 고무 패드를 부착

랙 설치

스위치는 EIA 표준 크기 19인치 랙에 장착할 수 있으며, 이는 다른 장비와 함께 배선 클로젯에 배치할 수 있습니다. 설치하려면, 장착 브래킷을 스위치의 측면 패널(양쪽 각각 하나)에 부착하고 제공된 나사로 고정하십시오(이 브래킷은 손바닥 크기의 스위치를 위한 것이 아님을 유의하십시오).

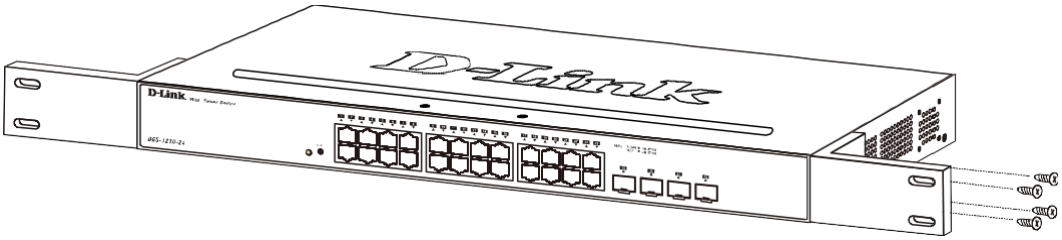


그림 2.2 - 스위치에 장착 브래킷 부착

그런 다음, 장비 랙과 함께 제공된 나사를 사용하여 스위치를 랙에 장착하십시오.

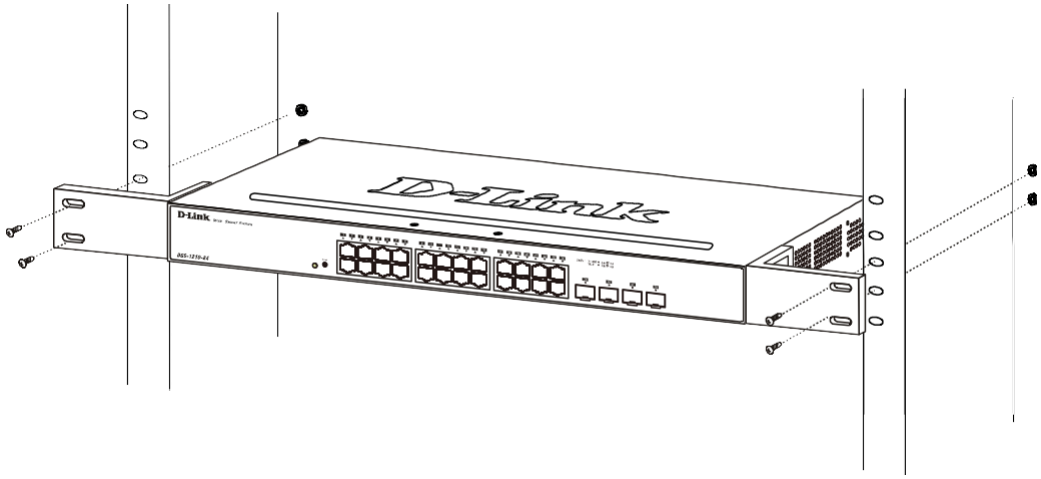


그림 2.3 - 랙 또는 섀시에 스위치 장착

설치 시 다음 안전 지침을 준수하십시오.

하나) 고온 작동 환경 - 밀폐형 또는 다중 유닛 랙 어셈블리에 설치된 경우, 랙 환경의 작동 온도가 실내 온도보다 높을 수 있습니다. 따라서 제조업체가 지정한 최대 환경 온도(Tma)와 호환되는 환경에 장비를 설치하는 것을 고려하십시오.

둘)공기 흐름 감소 - 랙에 장비를 설치할 때, 장비의 안전한 작동에 필요한 공기 흐름량이 저해되지 않도록 해야 합니다.

셋)기계적 하중 - 랙에 장비를 장착할 때, 고르지 않은 기계적 하중으로 인해 위험한 상태가 발생하지 않도록 해야 합니다.

넷) 회로 과부하 - 장비를 공급 회로에 연결할 때, 회로의 과부하가 과전류 보호 및 공급 배선에 미칠 영향을 고려해야 합니다. 이 문제를 해결할 때 장비 명판 등급을 적절히 고려해야 합니다.

다섯) 신뢰할 수 있는 접지 - 랙에 장착된 장비의 신뢰할 수 있는 접지를 유지해야 합니다. 브랜치 회로에 직접 연결되지 않은 공급 연결(예: 전원 스트립 사용)에 특히 주의하십시오.

3단계: 전원 코드 및 전원 코드 클립 연결

AC 전원 코드가 우발적으로 분리되는 것을 방지하기 위해, 전원 코드 클립을 전원 코드와 함께 설치하는 것이 권장됩니다.

하나) 거친 면이 아래로 향하게 하여 타이 랩을 전원 소켓 아래의 구멍에 삽입하십시오.

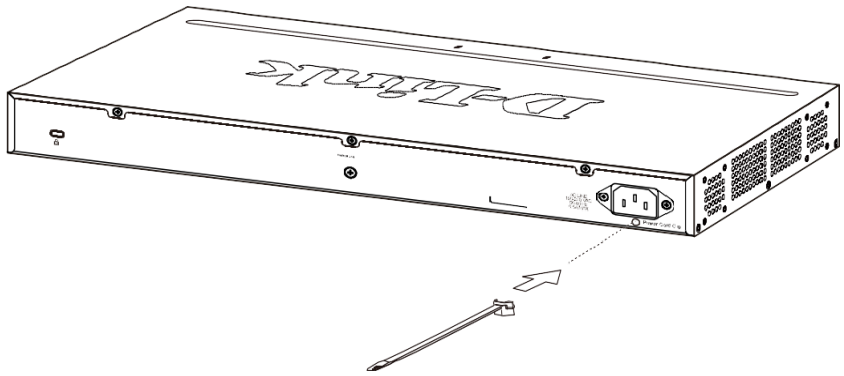


그림 2.4 - 스위치에 타이 랩 삽입

둘) AC 전원 코드를 스위치의 전원 소켓에 연결하십시오.

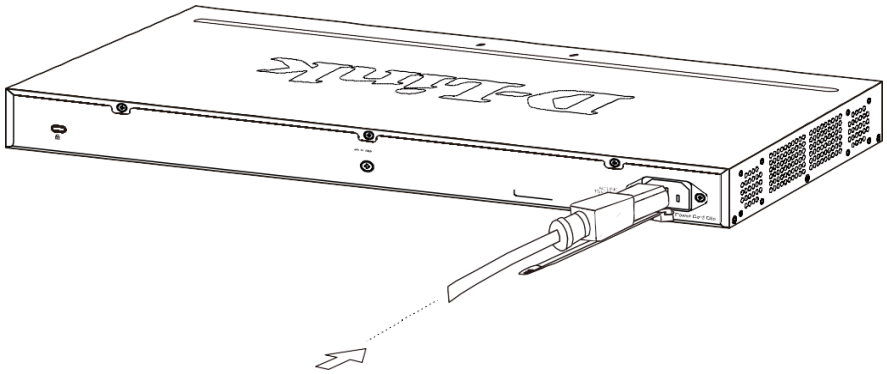


그림 2.5 - 전원 코드를 스위치에 연결

셋)리테이너를 타이 랩을 통해 코드 끝까지 미끄러뜨리십시오.

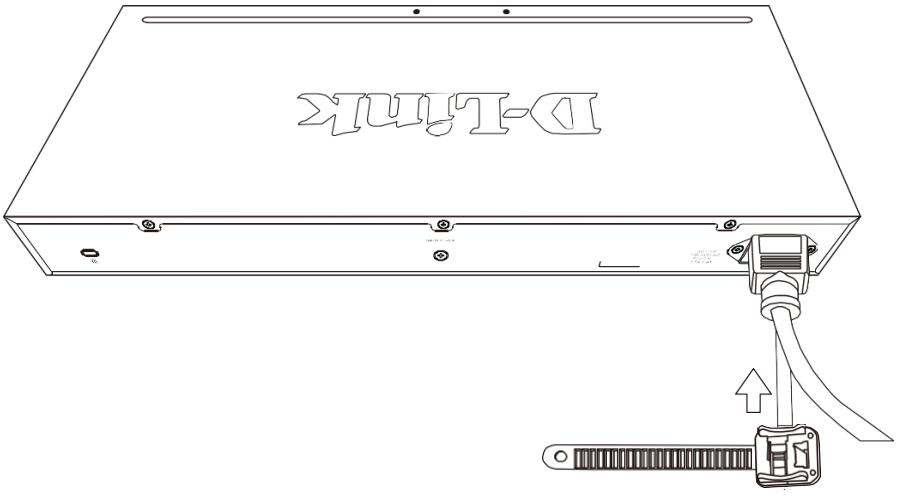


그림 2.6 - 리테이너를 타이 랩을 통해 미끄러뜨리기

넷)리테이너의 타이를 전원 코드 주위로 돌려 리테이너의 잠금장치에 넣으십시오.

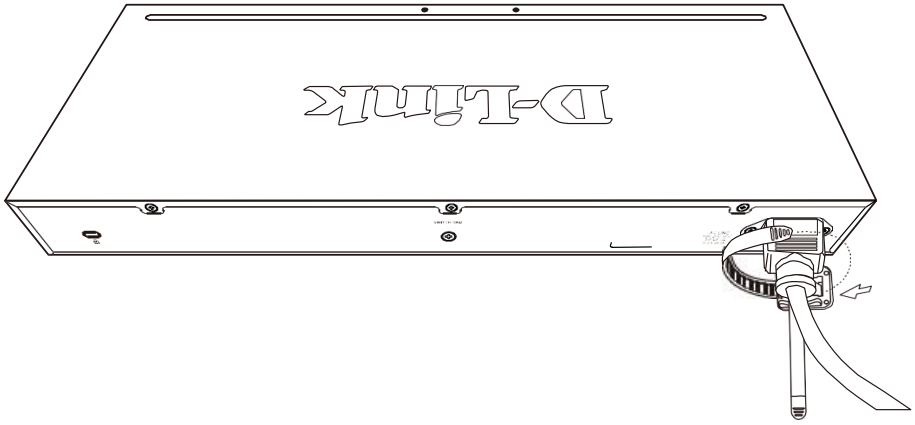


그림 2.7 - 전원 코드 주위로 돌리기

다섯) 리테이너의 타이를 고정하여 전원 코드가 고정되도록 하십시오.

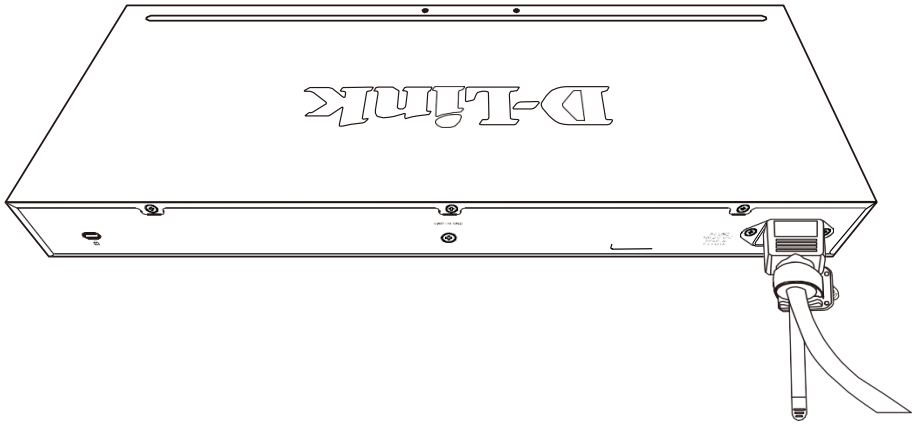


그림 2.8 - 전원 코드 고정

여섯) 이제 사용자는 AC 전원 코드를 전기 콘센트(가능하면 접지 및 서지 보호가 되는)로 연결할 수 있습니다.

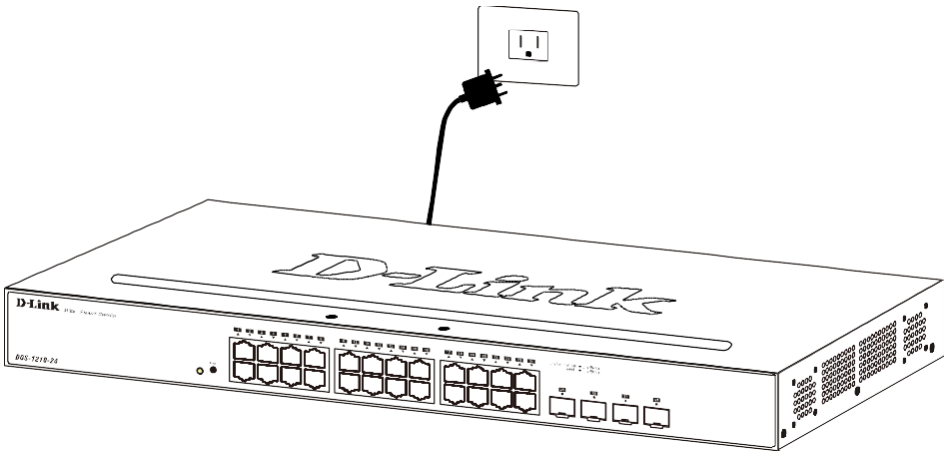


그림 2.9 - 스위치를 콘센트에 연결

전원 장애

예방 조치로, 정전 시 스위치를 분리해야 합니다. 전원이 복구되면 스위치를 다시 연결하십시오.

스위치 접지

이 섹션에서는 DGS-1210 시리즈 스위치를 접지하는 방법을 설명합니다. 스위치를 전원에 연결하기 전에 다음 절차를 수행해야 합니다.

필요한 도구 및 장비

- 접지 나사 (액세서리 키트에 포함됨): M4 x 6 mm (미터법) 팬헤드 나사 하나.
- 접지 케이블 (액세서리 키트에 포함되지 않음): 접지 케이블은 지역 및 국가 설치 요구 사항에 따라 크기가 지정되어야 합니다. 전원 공급 장치 및 시스템에 따라 미국 설치의 경우 12에서 6 AWG 구리 도체가 필요합니다. 시판되는 6 AWG 와이어를 권장합니다. 케이블의 길이는 스위치가 적절한 접지 시설과 얼마나 가까운지에 따라 다릅니다.
- 드라이버 (액세서리 키트에 포함되지 않음)

스위치를 보호 접지에 연결하는 단계

1단계: 시스템 전원이 꺼져 있는지 확인하십시오.

Step 2: 접지 케이블을 사용하여 그림 아래와 같이 #8 터미널 러그 링을 접지 나사 개구부 위에 놓으십시오.

Step 3: 접지 나사를 접지 나사 개구부에 삽입하십시오.

Step 4: 드라이버를 사용하여 접지 나사를 조여 접지 케이블을 스위치에 단단히 고정하십시오.

Step 5: 접지 케이블의 다른 쪽 끝에 있는 터미널 러그 링을 스위치가 설치된 랙의 적절한 접지 스터드 또는 볼트에 부착하십시오.

Step 6: 스위치와 랙의 접지 커넥터에서 연결이 단단히 고정되었는지 확인하십시오.

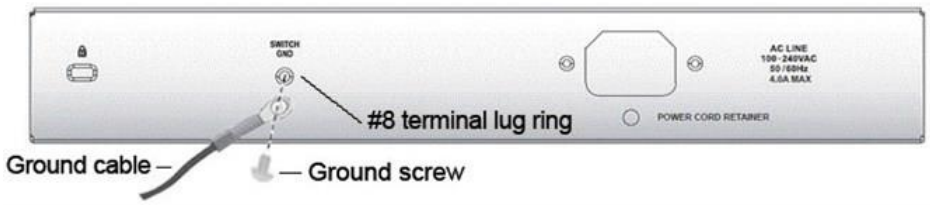


그림 2.10 - 접지 케이블 연결

3. *시작하기*

이 장에서는 D-Link Smart Managed Switch의 관리 인터페이스를 소개합니다.

관리 옵션

D-Link 스마트 관리 스위치는 웹 기반 관리를 사용하여 장치의 모든 포트를 통해 관리할 수 있습니다.

각 스위치는 웹 기반 관리 또는 SNMP 네트워크 관리자와 통신에 사용되는 고유한 IP 주소를 할당받아야 합니다. PC는 스위치와 동일한 범위의 IP 주소를 가져야 합니다. 각 스위치는 최대 네 명의 사용자가 동시에 웹 기반 관리에 액세스할 수 있습니다. 웹 기반 관리에 대한 설치 지침은 다음을 참조하십시오.

웹 기반 관리 사용하기

스위치는 웹 브라우저를 통해 관리, 구성 및 모니터링이 가능합니다.

지원되는 웹 브라우저

임베디드 웹 기반 관리는 현재 다음 웹 브라우저를 지원합니다.

IE8(또는 그 이후 버전), Firefox, Chrome 및 Safari

스위치 연결

다음 장비가 필요합니다.

일. RJ-45 이더넷 연결이 있는 PC

이. 표준 이더넷 케이블

스위치 전면 패널의 포트 중 하나에 이더넷 케이블을 연결하고 PC의 이더넷 포트에도 연결하십시오.

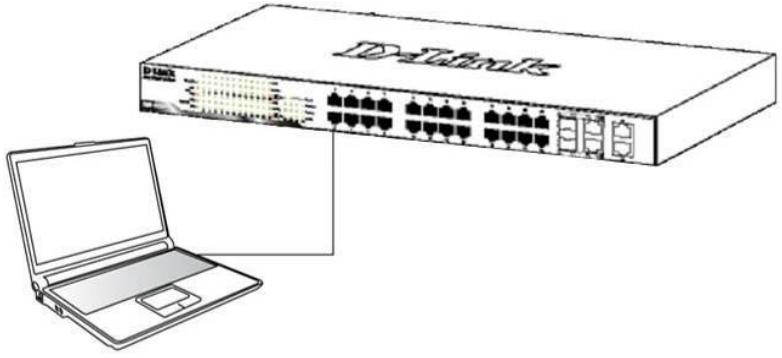


그림 3.1 - 이더넷 케이블 연결

웹 기반 관리에 로그인하기

이더넷 연결을 통해 스위치에 로그인하고 구성하기 위해서는 PC가 스위치와 동일한 서브넷에 있는 IP 주소를 가져야 합니다. 예를 들어, 스위치의 IP 주소가 10.90.90.90이면, PC는 10.x.y.z (여기서 x/y는 0~254 사이의 숫자이고 z는 1~254 사이의 숫자)의 IP 주소와 255.0.0.0의 서브넷 마스크를 가져야 합니다. 웹 기반 관리를 시작하는 두 가지 방법이 있습니다: 스마트콘솔 유틸리티 상단의 웹 액세스 버튼을 클릭하거나 웹 브라우저를 열고 주소 표시줄에 10.90.90.90(공장 기본 IP 주소)을 입력한 후 <Enter>를 누릅니다.

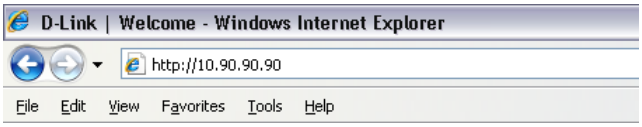


그림 3.2 - 웹 브라우저 주소창에 IP 주소 10.90.90.90을 입력

참고: 스위치의 출고 시 기본 IP 주소는 10.90.90.90이며, 서브넷 마스크는 255.0.0.0이고 기본 게이트웨이는 0.0.0입니다.

웹 구성은 SmartConsole 유틸리티를 통해서도 접근할 수 있습니다. SmartConsole 유틸리티를 열고 모니터 목록에 나타나는 스위치를 더블 클릭하십시오. 이렇게 하면 웹 브라우저에서 자동으로 웹 구성이 로드됩니다.

다음 로그인 대화 상자가 나타나면 비밀번호를 입력하고 웹 기반 관리 인터페이스의 언어를 선택한 다음 **OK**를 클릭하십시오.

스위치는 영어, 번체 중국어, 간체 중국어, 독일어, 스페인어, 프랑스어, 이탈리아어, 포르투갈어, 일본어 및 러시아어를 포함한 10개 언어를 지원합니다. 기본적으로 비밀번호는 admin이며 언어는 영어입니다.

그림 3.3 - 로그인 박스

스마트 마법사

로그인에 성공한 후, 스마트 마법사가 사용자를 D-Link 스마트 관리 스위치의 필수 설정으로 안내할 것입니다. 자세한 내용은 해당 섹션을 참조해 주세요.

웹 기반 관리

스마트 마법사의 종료 버튼을 클릭하면 사용자는 웹 기반 관리 인터페이스로 이동합니다.

자세한 지침은 챕터 4 웹 기반 스위치 구성을 참조하세요.

4. 웹 기반 스위치 구성

D-Link 스마트 매니지드 스위치의 기능과 기능은 웹 기반 관리 유틸리티를 통해 최적 사용을 위해 구성할 수 있습니다.

스마트 마법사 구성

스마트 마법사는 웹 UI에 처음 접속할 때 시작되는 구성 유틸리티입니다. 사용자는 스위치 모드, 관리 IP, 비밀번호 및 SNMP와 같은 기본 설정을 구성할 수 있습니다. 또한 스탠다드 모드와 감시 모드 웹 UI 유형 간에 전환하는 데 사용할 수도 있습니다.

스탠다드 모드는 스위치의 네트워크 및 시스템 요소를 관리하는 데 사용됩니다. 감시 모드는 네트워크에서 감시 및 IP 보안 장치를 모니터링하고 관리하기 위해 특별히 설계된 전용 UI입니다.

Step 1 – 웹 모드

로그인에 성공한 후, 스마트 위자드가 사용자를 D-Link 스마트 매니지드 스위치의 필수 설정을 안내합니다.

초기 페이지에서 사용자는 스위치의 스탠다드 모드와 감시 모드 중 선택할 수 있습니다.

이는 언제든지 스마트 위자드로 돌아가서 변경할 수 있습니다.

마법사를 나가려면 종료를 클릭하고 웹 인터페이스로 들어갑니다. 또한, '**Ignore the wizard next time**'를 체크하면 앞으로 웹 기반 관리 인터페이스에 로그인 할 때 스마트 마법사를 자동으로 건너뛸 수 있습니다.

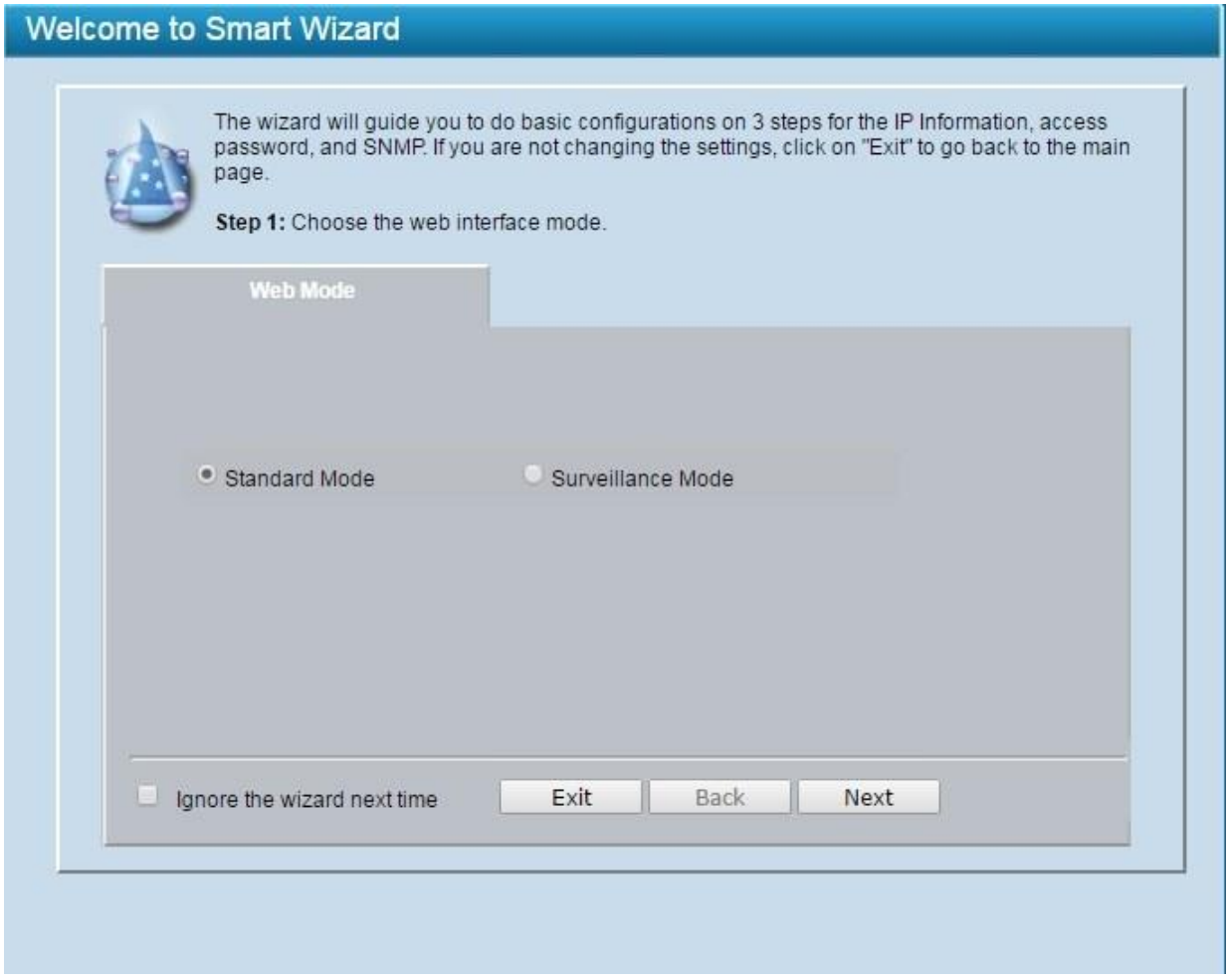


그림 4.1 - 스마트 마법사 웹 모드

구성할 수 있는 필드는 아래에 설명되어 있습니다.

항목	묘사
웹 모드	스탠다드 모드를 선택하여 다음 설정을 계속하거나 감시 모드를 선택하여 감시 모드에서 스마트 마법사를 계속합니다.

다음 구성 페이지로 이동하려면 **Next를** 클릭하세요.

2단계 – IP 정보

IP 정보 페이지를 통해 사용자는 IP 주소 할당 방법, 정적 IP 주소, 넷마스크 및 게이트웨이 주소를 구성할 수 있습니다.

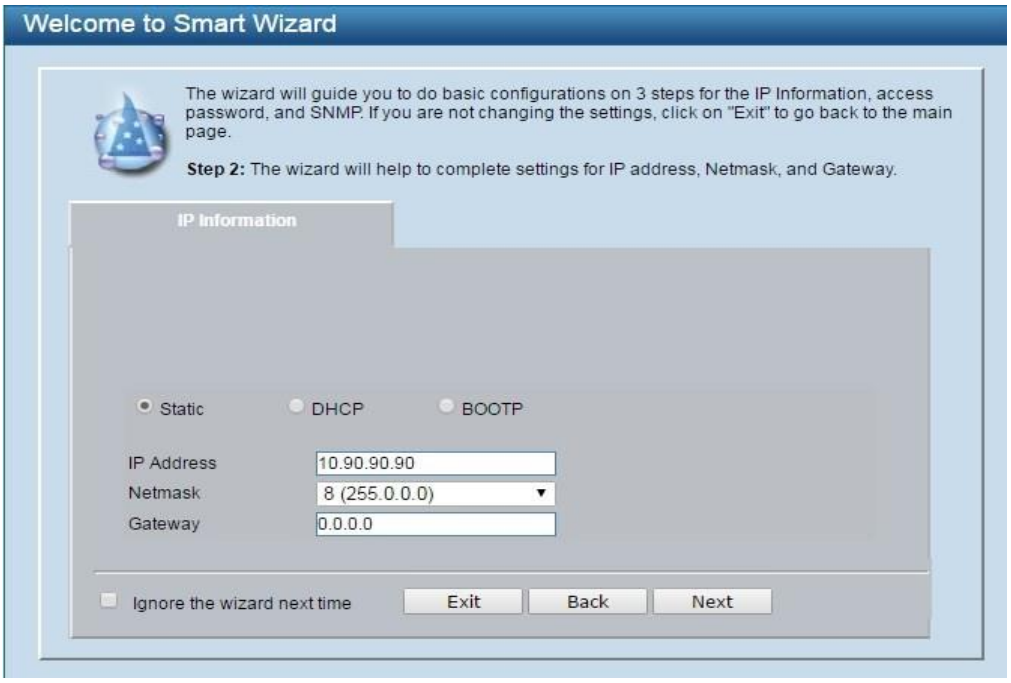


그림 4.2 - 스마트 마법사의 IP 정보

구성할 수 있는 필드는 아래에 설명되어 있습니다.

항목	묘사
정적인	IP 인터페이스의 매개 변수를 수동으로 구성하는 방법
DHCP	IP 인터페이스를 DHCP 모드로 구성하는 방법
부트	IP 인터페이스를 BOOTP 모드로 구성하는 방법
IP 주소	IP 주소 값을 입력할 필드
넷마스크	서브넷 마스크 값을 입력할 필드
게이트웨이	기본 게이트웨이 IP 주소의 값을 입력하는 필드

다음 비밀번호 설정 페이지로 이동하려면 다음을 클릭하세요.

다음 로그인 시 스마트 마법사를 건너뛰려면 **'Ignore the wizard next time'** 옵션을 체크하세요.

참고: 스마트 마법사는 IPv4 네트워크에 대한 빠른 설정을 지원합니다.

참고: 스위치는 30초마다 IP-카메라를 조사합니다. IP-카메라가 스위치와 동일한 서브넷에 없는 경우 IP-카메라가 자동으로 검색되지 않습니다. 감시 모드 웹 UI에 카메라를 자동으로 추가할 수 있도록 스위치 관리 IP를 IP-카메라와 동일한 서브넷에 배치합니다..

Step 3 – 비밀번호

원하는 새로은 패스워드를 **Password** 박스에 입력한 다음 **Confirm Password** 박스에 다시 입력하고 **Apply&Save** 버튼을 **SNMP** 설정 페이지로 이동합니다.

다음 로그인 시 스마트 마법사를 건너뛰려면 '**Ignore the wizard next time**' 옵션을 체크하세요.

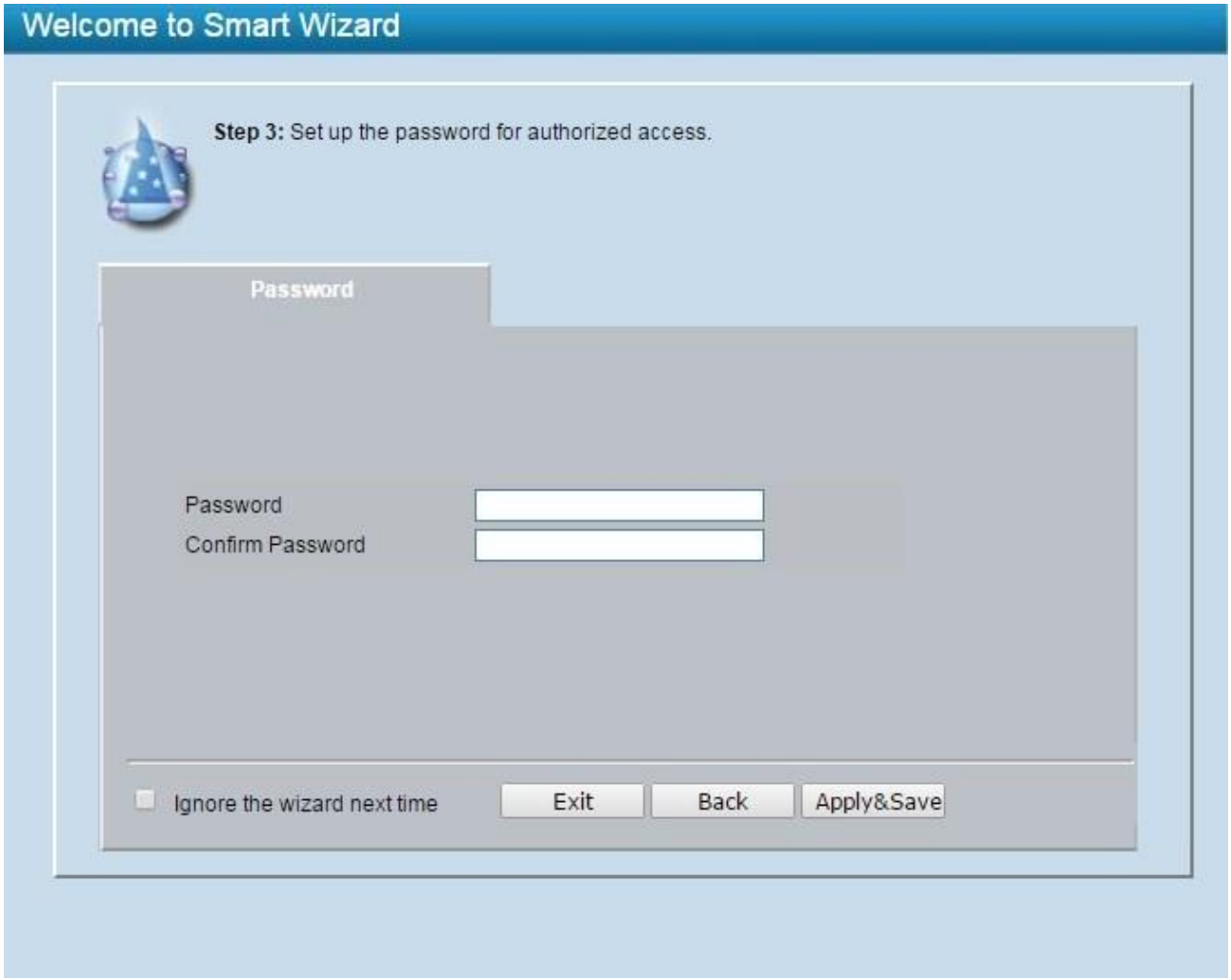


그림 4.3 - 스마트 마법사 비밀번호 설정

Step 4 – SNMP (스탠다드 모드 전용)

SNMP 설정을 통해 사용자는 SNMP 기능을 빠르게 활성화/비활성화할 수 있습니다. 기본 SNMP 설정은 비활성화되어 있습니다. 활성화를 클릭한 다음 적용을 클릭하여 적용하세요.

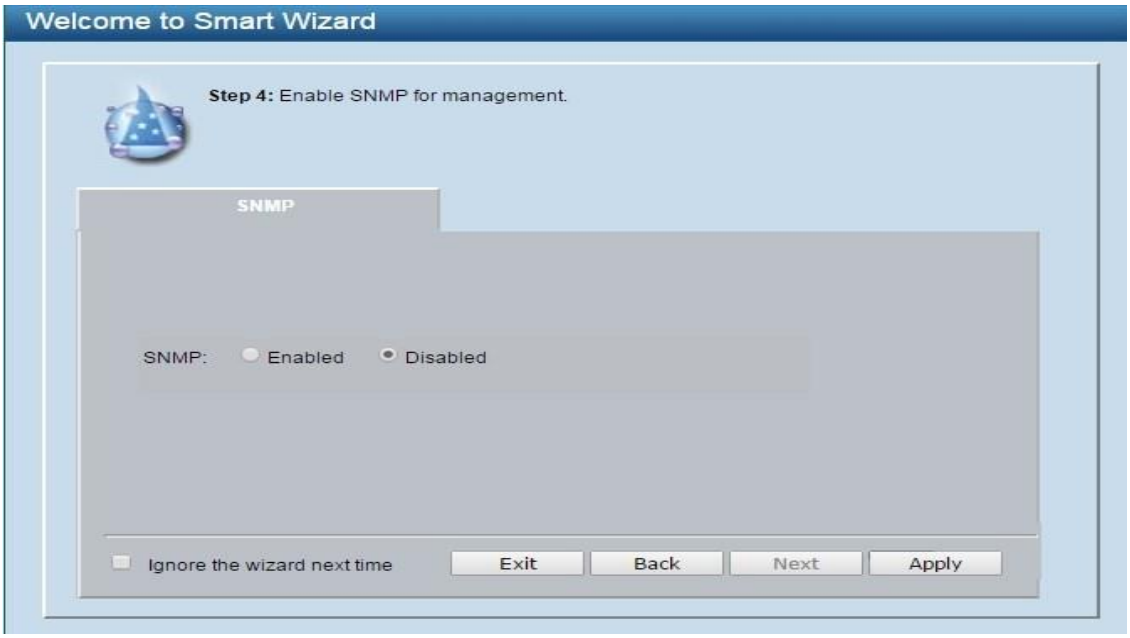


그림 4.4 – 스마트 마법사에서 SNMP

참고: 시스템 IP 주소를 변경하면 현재 관리 세션이 연결이 끊어집니다. 세션을 다시 설정하려면 웹 브라우저에 올바른 IP 주소를 다시 입력하세요. 자세한 설명은 로그인 웹 기반 관리를 참조하십시오.

참고: 표준 모드 및 감시 모드 웹 UI는 동일한 구성 파일을 공유합니다. 예를 들어, 한 인터페이스에서 활성화되는 모든 기능은 다른 인터페이스에서 사용할 수 있습니다: PoE 스케줄링, SNMP 설정 및 사용 중인 감시용 가상현실(VLAN).

변경한 IP 주소를 확인하고 **OK를** 클릭하세요.

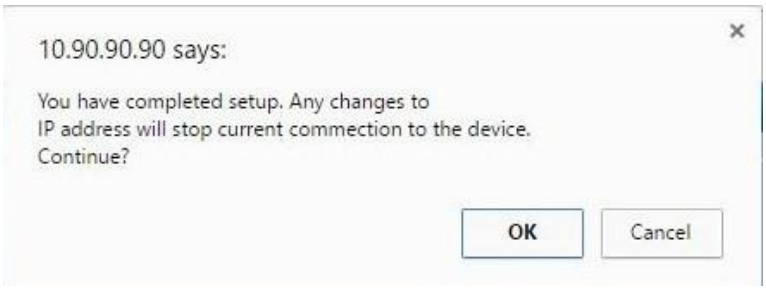


그림 4.5 - 스마트 마법사에서 IP 주소 변경 사항 확인

웹 기반 관리

스마트 마법사를 나갈 때 보이는 맨 처음 페이지:

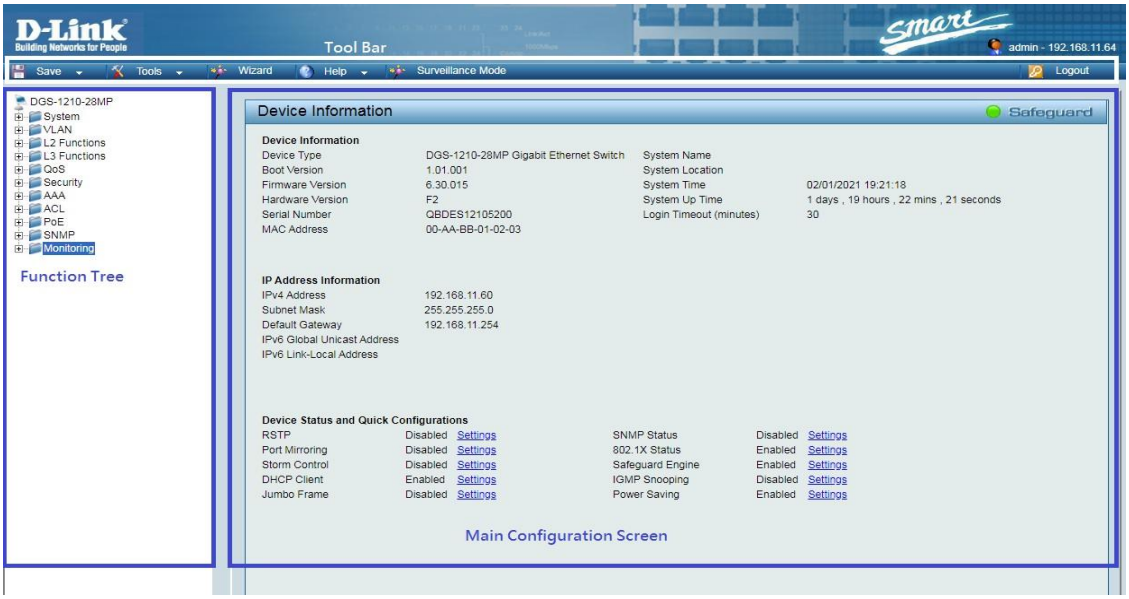


그림 4.6 – - 웹 기반 관리

위의 이미지는 웹 기반 관리 화면입니다.

상단의 **Tool Bar**, 왼쪽의 **Function Tree**, 그리고 **Main Configuration Screen** 등 3개의 구역으로 구성됩니다.

항목 영역	묘사
Tool Bar	펌웨어 및 구성 관리와 같은 필수 유틸리티 기능을 빠르고 편리하게 사용할 수 있는 방법을 제공합니다.
Function Tree	**Function Tree**에서 다양한 기능을 선택하면 **Main Configuration Screen** 에서 모든 설정을 변경할 수 있습니다.
Main Configuration Screen	**Function Tree**의 가장 위에 있는 모델명을 클릭하면 스위치의 현재 상태를 표시합니다.

화면 오른쪽 상단에는 사용자 이름과 현재 IP 주소가 표시됩니다.

사용자 이름 아래에는 **Logout** 버튼이 있습니다. 이 버튼을 클릭하여 이 세션을 종료할 수 있습니다.

참고: Logout하지 않고 웹 브라우저를 종료한 경우 비정상적인 종료로 관리 세션이 유지됩니다.

화면 좌측 상단의 D-Link 로고를 클릭하면 페이지가 지역 D-Link 웹사이트로 리디렉션 됩니다.

툴바 > 저장 메뉴

저장 메뉴는 저장 구성 및 저장 로그 기능을 제공합니다.

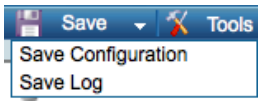


그림 4.7 - 저장 메뉴

구성 저장

사용자가 선택한 config ID로 설정 구성을 비휘발성 RAM에 저장합니다..

그림 4.8 - 저장 구성

로그 저장

로그 정보를 로컬 드라이브에 저장합니다. 대상 위치와 파일 이름은 팝업 메시지를 통해 지정할 수 있습니다.

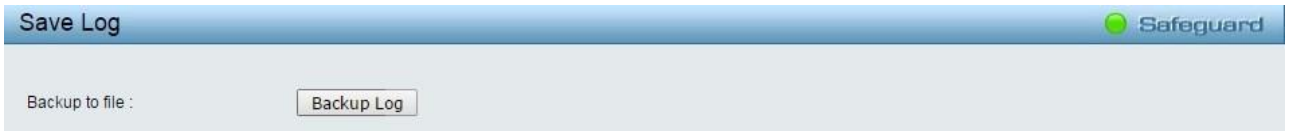


그림 4.9 - 로그 저장

툴바> 도구 메뉴

도구 메뉴는 초기화, 시스템 재설정, 장치 재부팅, 설정 백업 및 복원, 펌웨어 백업 및 업그레이드, 플래시 정보와 같은 전역 기능 제어를 제공합니다.

그림 4.10 - 도구 메뉴

재설정

리셋 메커니즘이 비휘발성 RAM에서 현재 구성 설정을 지웠습니다 (인터페이스 IP 주소 제외).

그림 4.11 - 도구 메뉴 > Reset

리셋 시스템

리셋 시스템 메커니즘은 비휘발성 RAM에 저장된 두 구성 세트를 모두 지웁니다.

장치는 재부팅 후에 공장 기본 상태로 돌아갑니다.

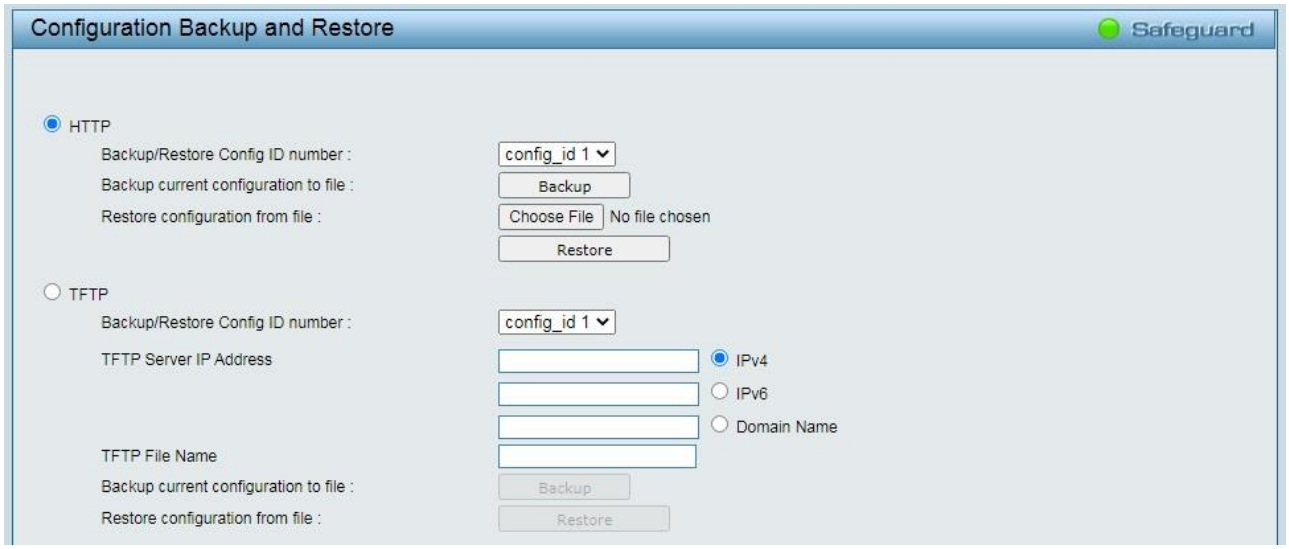
그림 4.12 - 도구 메뉴 > 리셋 시스템

장치 재부팅

재부팅하기 전 현재 설정을 저장할지 여부를 **YES** 또는 **No를 통해 선택하십시오. 그리고 Reboot**을 눌러 장치를 재부팅하십시오.

그림 4.13 - 도구 메뉴 > 장치 재부팅

구성 백업 및 복원



설정 설정을 백업하거나 복원하는 방법을 두 가지 프로토콜을 통해 제공합니다.: **HTTP** 또는 **TFTP**입니다.

그림 4.14 - 도구 메뉴 > 백업 및 복원 구성

HTTP: 로컬 드라이브로부터 구성 파일을 백업하거나 복원합니다.

Backup/Restore Config ID Number: config_id 1 또는 config_id 2를

선택하세요. 현재 설정을 로컬 드라이브에 저장하려면 백업을 클릭하세요.

Choose File을 클릭하여 백업 설정 파일을 찾습니다. 그리고 Restore을 클릭하여

복원 작업을 실행합니다.

TFTP: TFTP (Trivial File Transfer Protocol)은 파일을 전송하는 데 사용되는 파일 전송 프로토콜입니다. 최근 시스템은 TFTP 서버 주소로 구성할 수 있는 IPv4 주소, IPv6 주소 및 도메인 이름 문자열을 지원합니다.

현재 설정을 TFTP 서버에 저장하려면 **Backup을** 클릭하십시오.

복원 구성 작업을 실행하려면 **Restore을** 클릭하십시오.

참고: 복원 후 Switch가 재부팅되고 모든 현재 설정 값은 삭제됩니다.

펌웨어 백업 및 업그레이드

시스템 펌웨어를 업그레이드하거나 백업하는 방법을 두 가지 프로토콜을 통해 제공됩니다.: **HTTP** 또는 **TFTP**입니다.

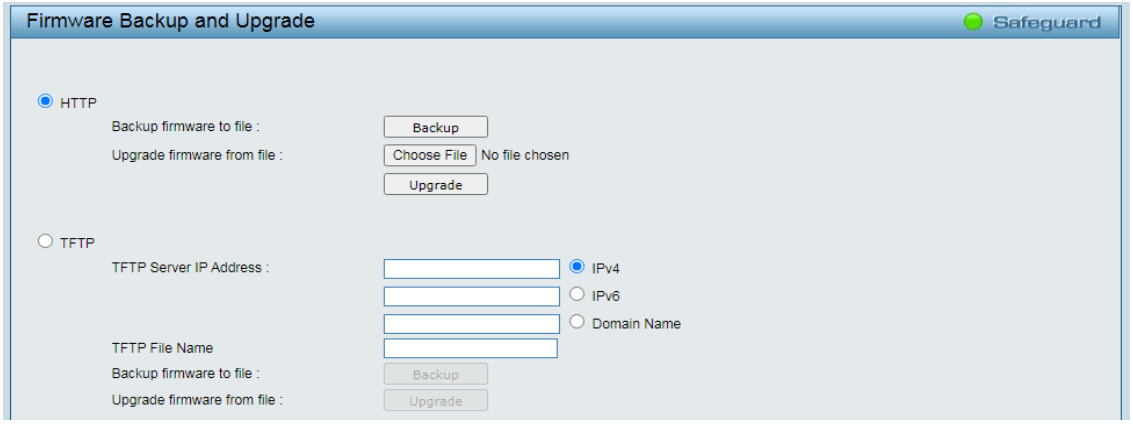


그림 4.15 - 도구 메뉴 > 펌웨어 백업 및 업로드

HTTP: HTTP 프로토콜을 통해 펌웨어를 백업하거나 업그레이드합니다.

펌웨어를 파일로 백업: 드롭다운 목록에서 image_id 1 또는 image_id 2를 선택합니다.

백업 절차를 실행하려면 백업을 클릭합니다.

파일에서 펌웨어 업그레이드: Choose File을 클릭하여 로컬 드라이브의 펌웨어 파일을 선택합니다.

Upgrade를 클릭하여 업그레이드 절차를 실행합니다.

TFTP: TFTP 프로토콜을 통해 펌웨어를 백업하거나 업그레이드합니다.

TFTP 서버 IP 주소: IPv4 주소, IPv6 주소 또는 **도메인 이름을** 통해 TFTP 서버 위치를 입력합니다.

TFTP 파일 이름: 업그레이드 또는 백업 작업에 사용되는 특정 파일 이름입니다.

펌웨어를 파일로 백업: 드롭다운 목록에서 Image_id1 또는 Image_id2를 선택합니다.

백업 절차를 실행하려면 **Backup을** 클릭합니다.

Upgrade를 클릭하여 업그레이드 절차를 실행합니다.

주의: 업그레이드가 완료될 때까지 PC의 연결을 끊거나 기기에서 전원 코드를 제거하지 마세요. 펌웨어 업그레이드가 완료되지 않으면 Switch가 손상될 수 있습니다.

Nuclias Connect 설정

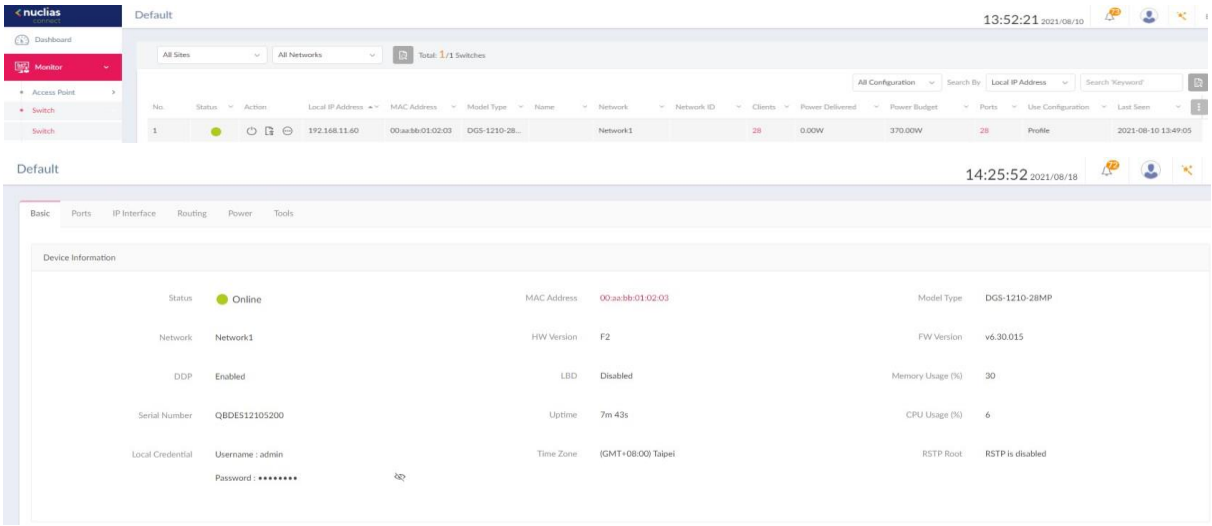
이 페이지에는 스위치의 Nuclias Connect 설정이 포함되어 있습니다.

그림 4.17 - 도구 메뉴 > Nuclias Connect 설정 (mDNS 서버 정보)

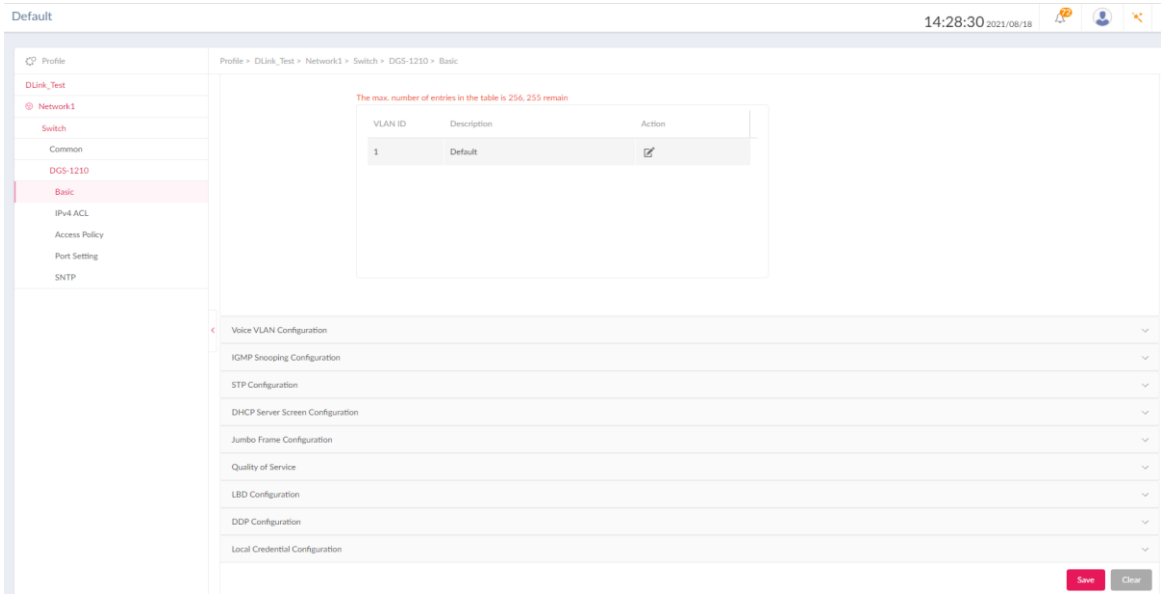
Nuclias Connect, D-Link의 중앙 집중식 관리 솔루션으로 중소기업(SMB) 네트워크를 위한 것입니다.
Nuclias Connect 커넥트를 통해 네트워크를 분석, 자동화, 구성, 최적화, 확장 및 보안하는 것이 더욱 쉬워집니다. 이는 중소기업 가격으로 엔터프라이즈급 관리 솔루션의 편의를 제공합니다.

Nuclias Connect 상태: Nuclias Connect 상태를 활성화/비활성화 할 수 있습니다.

Nuclias Connect Status: "연결 상태", "서버 IP/포트", "그룹 ID"를 포함한 Nuclias Connect 상태를 표시합니다.
DNC 서버는 mDNS 프로토콜을 지원하며, Nuclias Connect 설정 페이지에서 구성할 수 있습니다.



Nuclias Connect 에서 사용자는 장치 정보를 검색할 수 있습니다.



대부분의 기능은 Nuclias Connect를 통해 구성할 수 있습니다.

자세한 내용은 누클리아스 커넥트 웹사이트(https://www.dlink.com/en/business/nuclias/nuclias-connect)를 참조하세요.

주의: DGS-1210 시리즈는 DNC-100 버전과 호환되도록 설계되었습니다 1.2.0 이상. 사용하기 전에 DNC-100(Nuclias Connect) 버전을 확인하세요.

Nuclias Connect 파일 업로드

이 페이지에서는 이전에 저장된 Nuclias Connect 네트워크 파일을 불러올 수 있습니다.

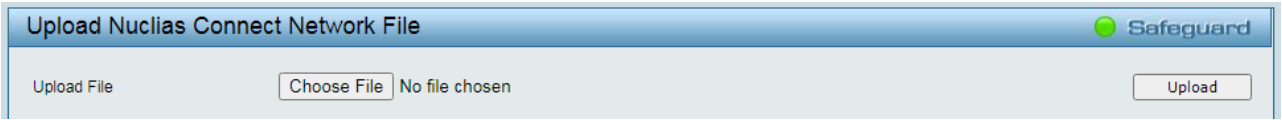
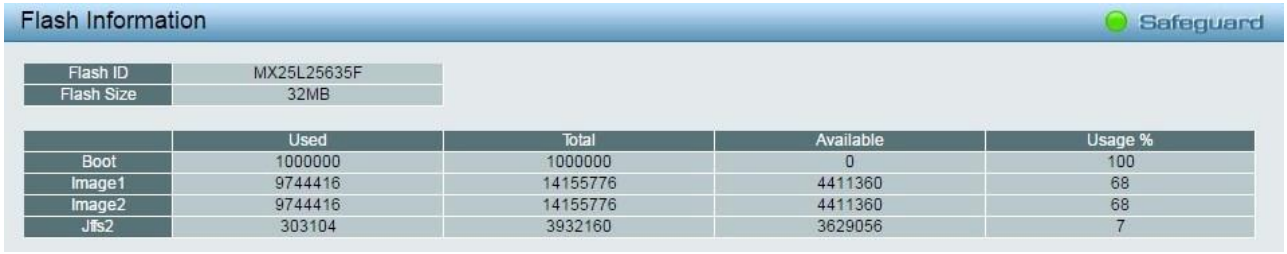


그림 4.18 - 도구 메뉴 > Nuclias Connect 파일 업로드

파일 선택: Nuclias Connect Network의 특정 DNC 파일을 선택합니다. 이 특정 유형의 파일은 장치가 DNC에 다시 가입할 수 있는 쉬운 방법을 제공하는 Nuclias Connect Network Profile을 통해 생성 및 저장되었습니다.

플래시 정보



이 페이지는 스위치의 플래시 상세 정보를 표시합니다.

그림 4.19 - 도구 메뉴 > 플래시 정보

툴바 > 마법사

사용자가 원하는 경우 마법사 버튼을 클릭하여 스마트 마법사로 돌아갈 수 있습니다.

도구 모음 > 온라인 도움말

온라인 도움말은 두 가지 온라인 지원 방법을 제공합니다: D-Link 지원 사이트는 D-Link 웹사이트로 이동하여 최신 펌웨어 이미지와 같은 온라인 자원을 찾을 수 있게 해줍니다. 사용자 가이드는 기능 정의나 구성 가이드에 대한 즉각적인 참조를 제공할 수 있습니다.

그림 4.20 - 온라인 도움말

감시 모드> 도구 모음

Surveillance Mode는 사용자가 주의를 집중하고 감시 관련 구성 및 정보를 탐색하는 데 도움이 되는 UI 디자인을 제공합니다. IP 카메라 정보, PoE 일정 또는 감시 로그와 같은 정보를 포함합니다.

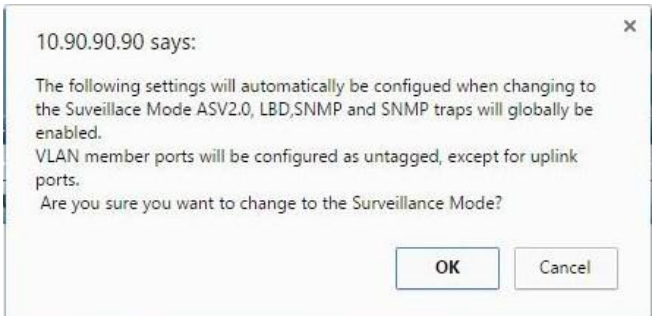


그림 4.21 - Survillance Mode 확인 메시지

위에 표시된 팝업 메시지 창은 감시 모드에 액세스할 때 구성을 변경해야 한다는 메시지를 표시합니다.

계속하려면 **OK** 버튼을 클릭하세요.

Cancel 버튼을 누르면 **Standard Mode로** 돌아갑니다.을 클릭합니다.

스위치의 웹 UI에서 감시 모드로 성공적으로 전환한 후, 다음 창이 표시됩니다.

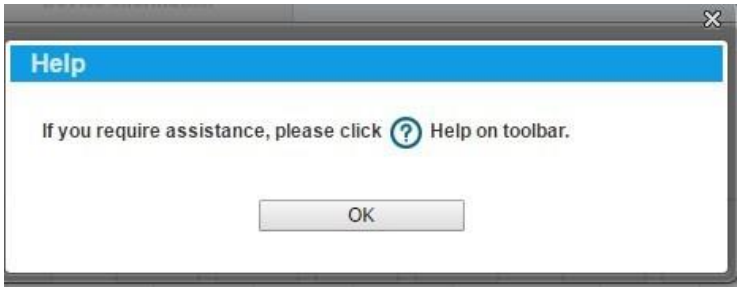


그림 4.22 - 감시 모드 도움말 메시지

계속하려면 **OK** 버튼을 클릭하십시오. 다음 페이지가 표시됩니다.

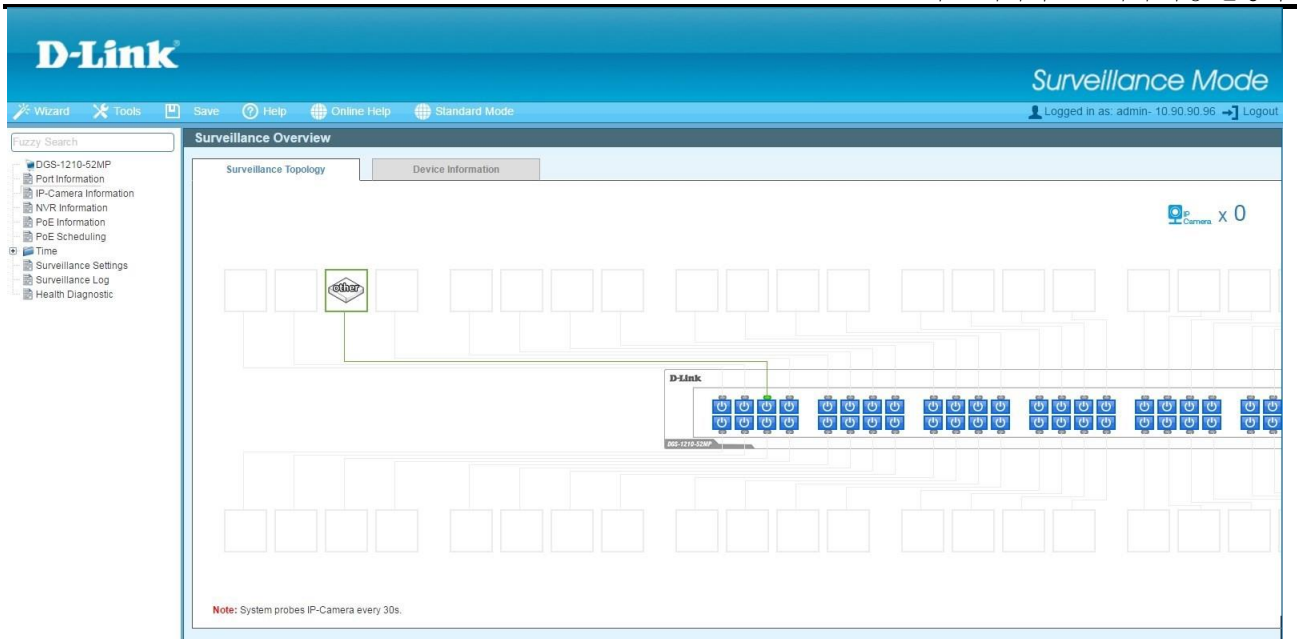


그림 4.23 - 감시 모드

페이지 하단으로 스크롤하고 확인 버튼을 클릭하여 웹 UI로 계속 이동합니다. 감시 모드에 대한 자세한 정보는 다음과 같습니다. 자세한 지침은 5장 Surveillance Mode Configuration을 참조하세요.

기능 트리

스위치의 모든 구성 옵션은 화면 왼쪽에 있는 설정 메뉴를 통해 액세스됩니다.

다음 섹션에서는 각 기능의 보다 자세한 설명을 제공합니다.

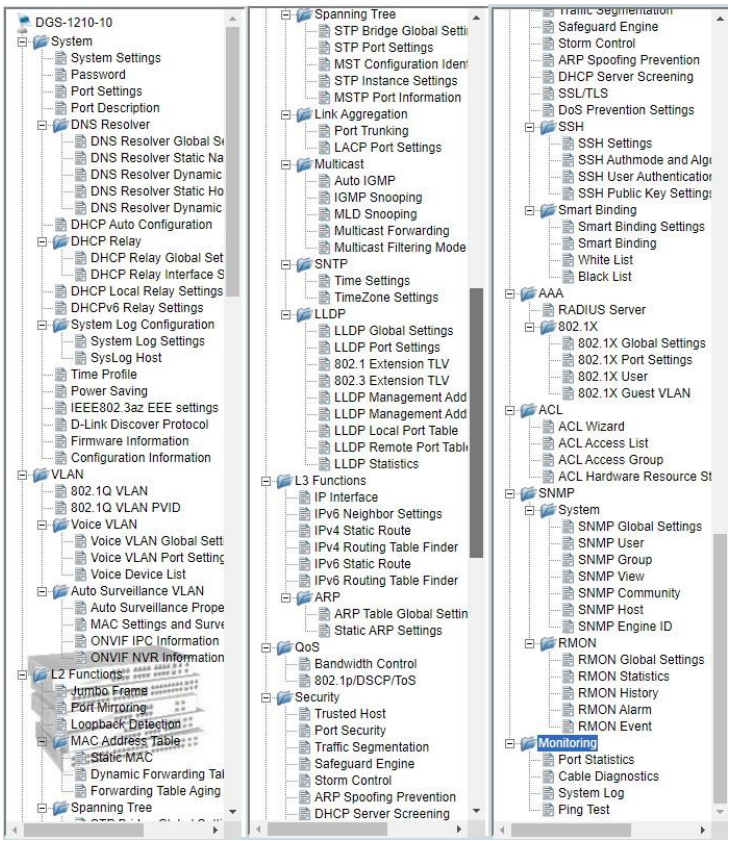


그림 4.24 –기능 트리

장치 정보

장치의 전반적인 상태를 제공합니다.

그림 4.25 - 장치 정보

RSTP: Settings을 클릭하면 L2 Functions > Spanning Tree > STP Global Settings로 연결됩니다. 기본값 : Disable

Port Mirroring: Settings을 클릭하면 L2 Functions > Port Mirroring으로 연결됩니다. 기본값 : Disable

Storm Control: Settings을 클릭하면 Security > Storm Control로 연결됩니다. 기본값 : Disable

DHCP Client: Settings을 클릭하면 System > System Settings으로 연결됩니다. 기본값 : Disable

Jumbo Frame: Settings을 클릭하면 L2 Functions > Jumbo Frame으로 연결됩니다. 기본값 : Disable

SNMP Status: Settings을 클릭하면 SNMP > SNMP > SNMP 전역 설정으로 연결됩니다. 기본값 : Disable

팔백이.일 **X Status: Settings을 클릭하면** AAA > 802.1X > 802.1X Settings으로 연결됩니다. 기본값 : Disable

Safeguard Engine: Settings을 클릭하면 Security > Safeguard Engine으로 연결됩니다. 기본값 : Enabled

IGMP Snooping: Settings을 클릭하면 L2 Functions > Multicast > IGMP Snooping으로 연결됩니다. 기본값 : Disable

Power Saving: Settings을 클릭하면 System > Power Saving으로 연결됩니다. 기본값 : Disable

시스템 > 시스템 설정

시스템 설정을 통해 사용자는 스위치의 IP 주소와 기본 시스템 정보를 구성할 수 있습니다.

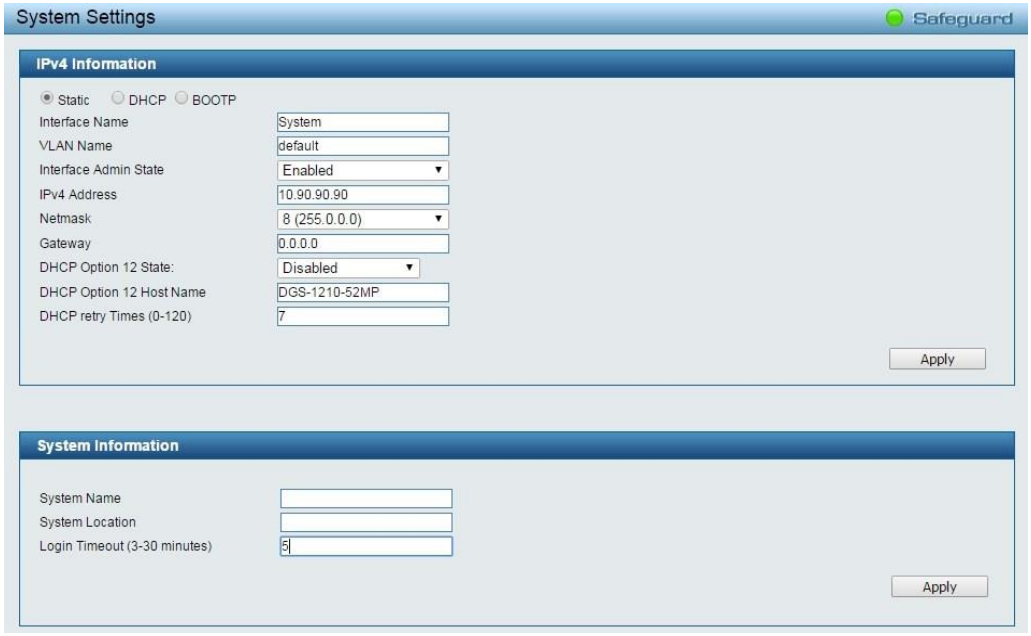


그림 4.26 - 시스템 > 시스템 설정

IPv4 정보: 스위치의 IP 주소 설정 방법은 세 가지가 있습니다: Static, DHCP, BOOTP

Static 모드를 사용할 때는 인터페이스 이름, VLAN 이름, 인터페이스 관리 상태, IPv4 주소, 넷마스크 및 게이트웨이를 수동으로 구성해야 합니다. DHCP 모드를 사용할 때는 "Apply"을 클릭하면 DHCP 절차를 시작합니다. 기본적으로 IP 설정은 IP 주소가 10.90.90.90이고 서브넷 마스크가 255.0.0.0인 Static 모드로 설정되어 있습니다.

DHCP Option 12 State: DHCP 옵션 12 상태의 활성화/비활성화를 지정합니다.

DHCP 옵션 12 Host Name: DHCP를 위한 호스트 이름을 지정합니다.

DHCP 재시도 시간: DHCP의 재시도 시간을 지정합니다.

System Information: System Name과 System Location 사용자 지정 문자열을 통해 구성할 수 있으며, 이는 장치가 스마트 콘솔 유틸리티 및 LAN 내의 다른 웹 스마트 장치에서 더 쉽게 인식될 수 있도록 도와줍니다.

Login Timeout: Login Timeout은 보안 목적을 위한 유휴 시간 제한 기간을 제어하며, 웹 기반 관리에서 특정 시간 동안 아무 작업도 없을 때 발생합니다. 현재 세션이 시간 초과되면 사용자는 다시 웹 기반 관리를 사용하기 전에 다시 로그인해야 합니다. 선택 범위는 3분부터 30분이며, 기본 설정은 5분입니다.

시스템 > 암호

비밀번호 설정은 웹 스마트 스위치를 안전하게 보호하기 위한 관리자의 중요한 도구입니다. 비밀번호 필드는 최대 20자까지 지원하며 특수 문자 (? ; " <space>)는 허용되지 않습니다.

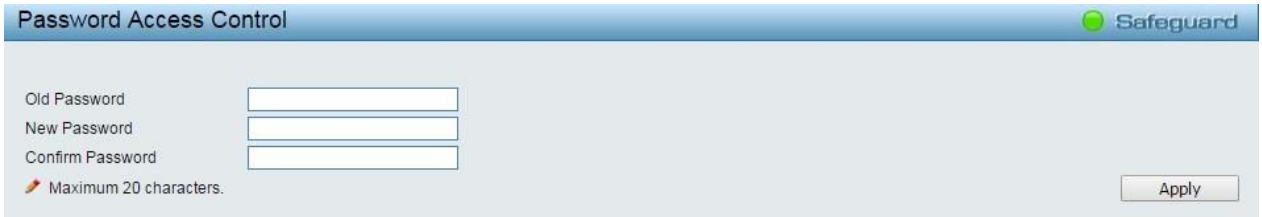
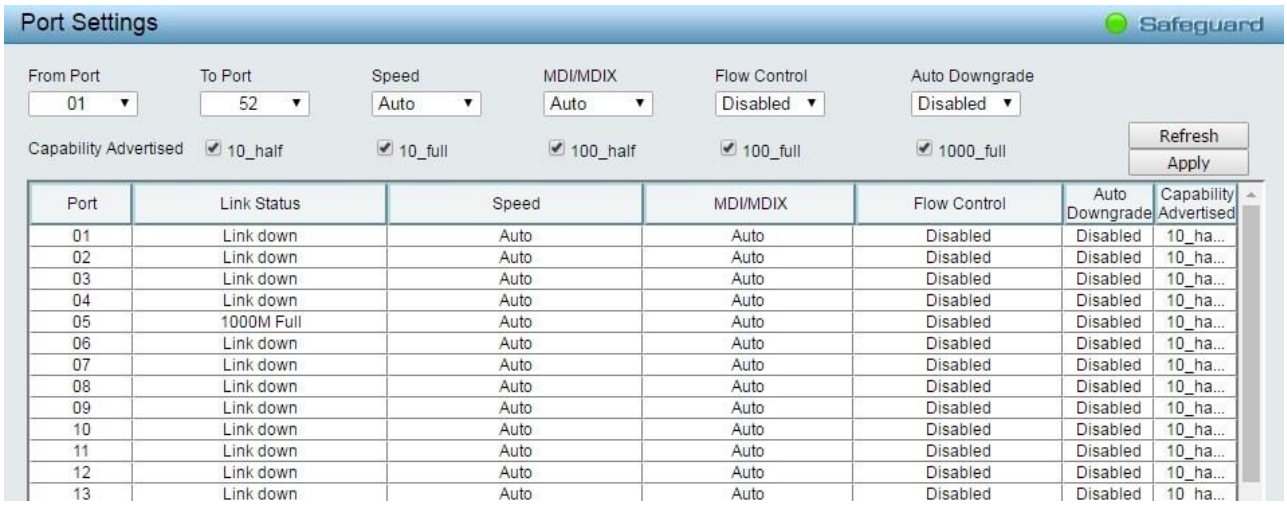


그림 4.27 - 시스템 > 비밀번호 액세스 제어

시스템 > 포트 설정

포트 설정 페이지에서 모든 포트의 상태를 모니터링하고 설정할 수 있습니다. 설정은 개별 포트 또는 포트 범위(**From Port과 To Port**)로 설정할 수 있습니다. 새로 고침 버튼을 클릭하여 최신 정보를 얻을 수 있습니다.

그림 4.28 - 시스템 > 포트 설정



Speed: 기가비트 광 연결은 1000M Auto 또는 Disabled만 지정할 수 있습니다. 구리 연결은 강제 모드(1000M Full, 100M Full, 100M Half, 10M Full, 10M Half), Auto 또는 Disabled로 설정할 수 있으며 기본 값은 **Auto입니다.**

참고: 연결된 케이블 미디어 유형을 변경한 후 포트 속도 설정을 적절히 조정해야 합니다.

참고: 속도가 1000M 강제 모드로 설정되는 경우 모든 포트가 MDI/MDI-X 기능을 지원하지 않습니다.

MDI/MDIX:

Medium Dependent Interface (**MDI**) 포트는 일반적으로 네트워크 인터페이스 카드(NIC)나 PC의 통합 NIC 포트에 사용되는 연결입니다. 스위치와 허브는 보통 **Medium dependent interface crossover (MDIX)** 인터페이스를 사용합니다. 스위치를 종단 단말에 연결할 때 사용자는 Tx/Rx 쌍이 올바르게 일치하도록 하기 위해 다이렉트 이더넷 케이블을 사용해야 합니다. 스위치를 다른 네트워킹 장치에 연결할 때는 크로스오버 케이블을 사용해야 합니다.

이 스위치는 사용자에게 설정 가능한 **MDI/MDIX을 제공합니다.** 이더넷 크로스오버 케이블 없이 다른 허브나 스위치에 연결하기 위해 스위치를 MDI 포트로 설정할 수 있습니다.

Auto MDI/MDIX는 스위치에서 연결이 거꾸로 되어 있는지 자동으로 감지하도록 설계되었습니다

연결을 올바르게 일치시키려면 MDI 또는 MDIX를 선택합니다. **MDI/MDIX** 의 기본 설정 값은 "**Auto**" 입니다.

Flow Control: 이 기능은 트래픽 혼잡을 완화하는 데 사용됩니다. Full-duplex로 구성된 포트는 802.3x Flow Control을, Half-duplex로 구성된 포트는 Backpressure flow control를 사용합니다. 기본 설정은 비활성화입니다

자동 다운그레이드: 자동 속도 다운그레이드 기능을 켜거나 끕니다.을 클릭합니다. **Speed가 자동으로 설정된 경우에만** 적용됩니다.을 클릭합니다.

Capability Advertised: Speed 가 자동으로 설정되면, 이 기능들은 자동 협상 중에 전파됩니다.

시스템 > 포트 설명

포트 설명은 사용자 정의 문자열로 구성할 수 있습니다. 이 필드는 최대 32자와 특수 문자를 지원합니다.

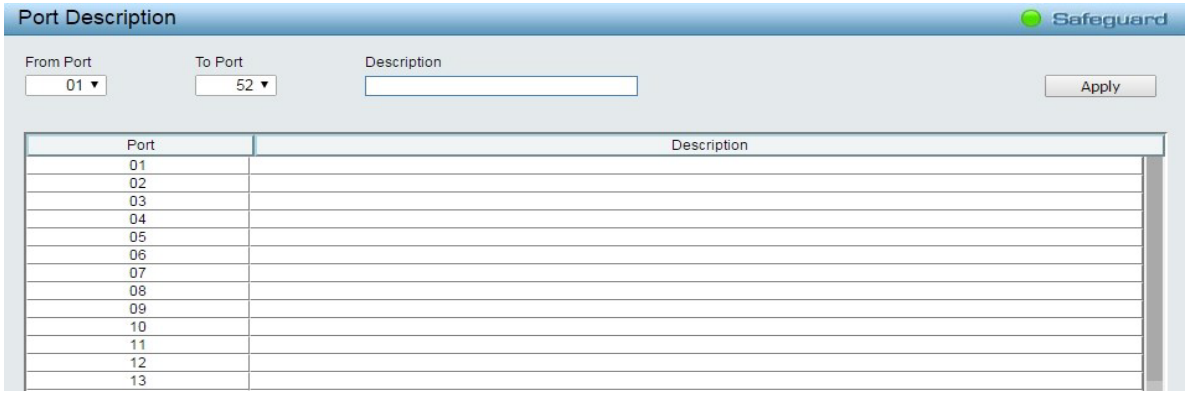


그림 4.29 - 시스템 > 포트 설명

From Port / To Port: 입력할 포트 범위를 지정

설명: 지정한 포트에 설명 입력

Apply를 클릭하여 적용

시스템 > DNS 확인자 > DNS 확인자 전역 설정

DNS resolver는 도메인 이름을 통해 IP 주소를 조회하는 데 도움을 줍니다. 이 페이지에는 DNS resolver 기능을 위한 전역 설정이 포함되어 있습니다.

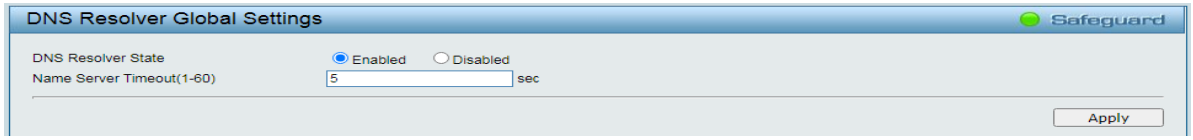


그림 4.30 - 시스템 > DNS 확인자 > DNS 확인자 전역 설정

DNS Resolver State: 드롭다운 목록에서 선택하여 전역적으로 DNS 확인자 기능을 활성화/비활성화합니다. 기본값은 활성화입니다.

Name Server Timeout: 1-60초로 설정 가능한 타임아웃 시간. 이 시간은 DNS 네임 서버로부터 응답을 기다리는 시간 범위를 의미합니다.

시스템 > DNS 확인자 > DNS 확인자 정적 이름 서버 설정

이 페이지에서 특정 DNS 이름 서버를 구성할 수 있습니다.

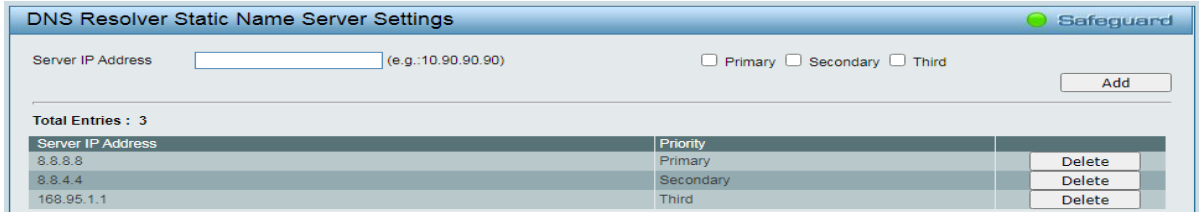


그림 4.31 - 시스템 > DNS 확인자 > DNS 확인자 정적 이름 서버 설정

서버 IP 주소: 특정 DNS 이름 서버 IP 주소는 해당 필드에서 구성할 수 있습니다. 스위치는 최대 3개의 서버 IP 주소를 지원합니다.

시스템 > DNS 확인자 > DNS 확인자 동적 이름 서버 테이블

이 페이지에는 DNS 동적 이름 서버 목록이 포함되어 있습니다.

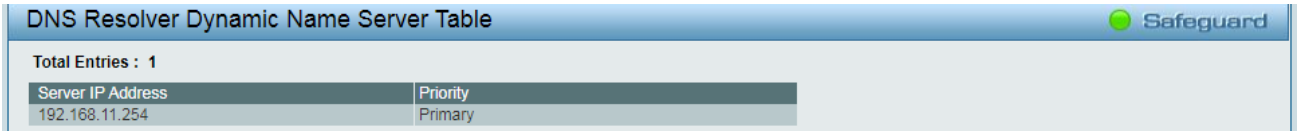


그림 4.32 - 시스템 > DNS 확인자 > DNS 확인자 동적 이름 서버 테이블

시스템 > DNS 확인자 > DNS 확인자 정적 호스트 이름 설정

정적 호스트 이름 테이블에는 사용자가 수동으로 구성한 DNS 항목이 표시됩니다. 시스템은 최대 16개의 정적 항목을 지원합니다.

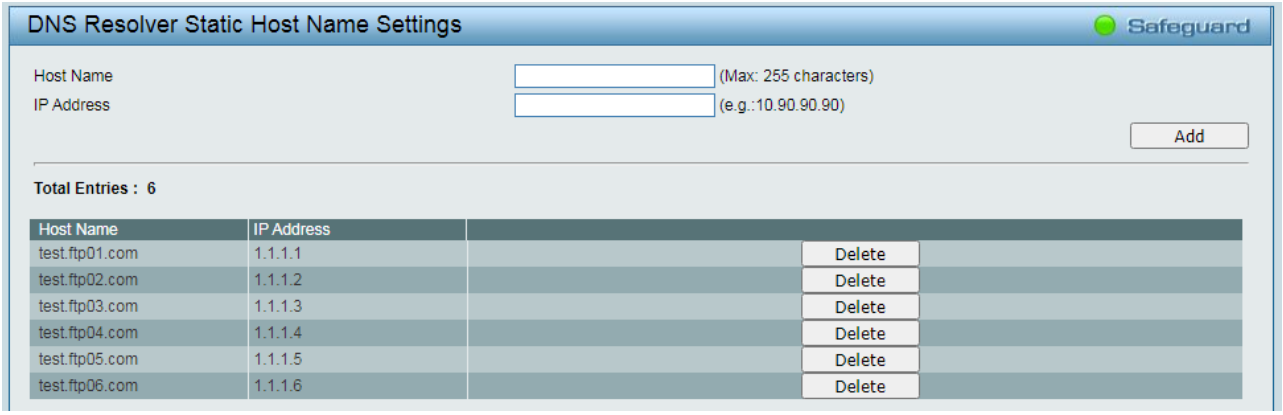


그림 4.33 - 시스템 > DNS 확인자 > DNS 확인자 정적 호스트 이름 설정

Host Name: 도메인 이름 문자열을 지정하십시오.

IP Address: 필드에 IP 주소를 지정하십시오.

시스템 > DNS 확인자 > DNS 확인자 동적 호스트 이름 테이블

DNS Resolver Dynamic Host Name Table은 동적으로 학습된 DNS 항목이 표시됩니다. 이 테이블은 최대 10개의 항목을 지원합니다.

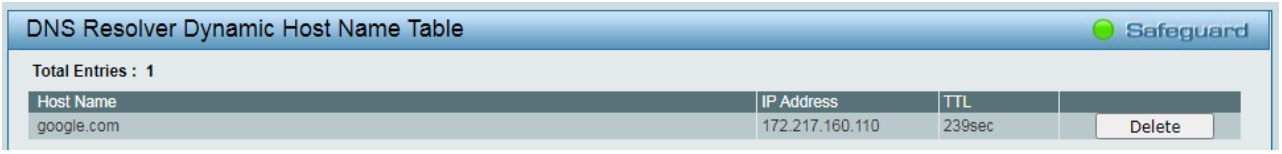


그림 4.34 - 시스템 > DHCP 릴레이 > DHCP 릴레이 전역 설정

시스템 > DHCP 자동 구성

DHCP 자동 구성은 사용자가 TFTP 프로토콜을 통해 지정된 구성 파일을 자동으로 다운로드할 수 있도록 도와주는 기능입니다. 이 기능이 활성화되면, 스위치는 DHCP 클라이언트가 되어 다음 부팅 시 TFTP 서버에서 구성 파일을 가져옵니다. 이를 위해 DHCP 서버는 DHCP 옵션에 TFTP 서버의 IP 주소와 구성 파일 이름 정보를 전달해야 합니다. TFTP 서버는 작동 중이어야 하며, 스위치의 요청이 수신될 때 필요한 구성 파일을 기본 디렉토리에 저장하고 있어야 합니다.

그림 4.35 - 시스템 > DHCP 자동 구성

시스템 > DHCP 릴레이 > DHCP 릴레이 전역 설정

DHCP 릴레이는 LAN 간에 호스트 IP를 할당하는 데 도움을 주는 기능입니다. 스위치는 이 기능이 활성화되었을 때 릴레이 에이전트 역할을 합니다.

그림 4.36 - 시스템 > DHCP 릴레이 > DHCP 릴레이 전역 설정

DHCP Relay State: 드롭다운 목록에서 선택하여 DHCP 릴레이 기능을 전역적으로 활성화/비활성화합니다. 기본값은 비활성화입니다.

DHCP Relay Hops Count Limit (1-16): 이 필드는 DHCP 메시지가 전달될 수 있는 최대 라우터 홉 수를 정의하는 1부터 16 사이의 값 입력을 허용합니다. 기본 홉 수는 4입니다.

DHCP Relay Time Threshold (0-65535): 0부터 65535초 사이의 값을 입력할 수 있으며, DHCP 패킷을 라우팅하는 최대 시간 제한을 정의합니다. 값으로 0을 입력하면 스위치는 DHCP 패킷의 **초** 필드 값을 처리하지 않습니다. 0이 아닌 값이 입력되면, 스위치는 해당 값과 홉 카운트를 사용하여 주어진 DHCP 패킷을 전달할지 여부를 결정합니다.

DHCP 릴레이 에이전트 정보 옵션 82 상태: 이 필드는 드롭다운 메뉴를 사용하여 활성화 및 비활성화 사이를 전환할 수 있습니다. 이는 스위치에서 DHCP 에이전트 정보 옵션 82를 활성화 또는 비활성화하는 데 사용됩니다. 기본 설정은 비활성화입니다.

> **Enabled –** 이 필드가 활성화로 전환되면, 릴레이 에이전트는 DHCP 서버와 클라이언트 간의 메시지에서 DHCP 릴레이 정보(옵션 82 필드)를 삽입하고 제거합니다. 릴레이 에이전트가 DHCP 요청을 수신하면, 옵션 82 정보를 추가하고 릴레이 에이전트의 IP 주소(릴레이 에이전트가 구성된 경우)를 패킷에 삽입합니다. 옵션 82 정보가 패킷에 추가되면, 이 패킷은 DHCP 서버로 전송됩니다. DHCP 서버가 패킷을 수신하면, 서버가 옵션 82를 지원하는 경우, 단일 원격 ID 또는 회로 ID에 할당할 수 있는 IP 주소의 수를 제한하는 등의 정책을 구현할 수 있습니다. 이후 DHCP 서버는 DHCP 응답에서 옵션 82 필드를 그대로 반향합니다. 요청이 릴레이 에이전트에 의해 서버로 전달된 경우, DHCP 서버는 릴레이 에이전트로 응답을 유니캐스트하여 보냅니다. 스위치는 원래 옵션 82 데이터를 삽입했는지 확인합니다. 마지막으로, 릴레이 에이전트는 옵션 82 필드를 제거하고 DHCP 요청을 보낸 DHCP 클라이언트에 연결된 스위치 포트로 패킷을 전달합니다.
>
> **Disabled -** 필드가 비활성화로 전환되면, 릴레이 에이전트는 DHCP 서버와 클라이언트 간의 메시지에서 DHCP 릴레이 정보(옵션 82 필드)를 삽입하거나 제거하지 않으며, 확인 및 정책 설정은 아무런 효과가 없습니다.

DHCP 릴레이 에이전트 정보 옵션 82 확인: 이 필드는 드롭다운 메뉴를 사용하여 활성화 또는 비활성화할 수 있습니다. 패킷의 옵션 82의 유효성을 검사하는 스위치의 기능을 활성화 또는 비활성화하는 데 사용됩니다.

> **Enabled** – 이 필드가 활성화로 전환되면, 릴레이 에이전트는 패킷의 옵션 82 필드의 유효성을 검사합니다. 스위치가 DHCP 클라이언트로부터 옵션 82 필드가 포함된 패킷을 수신하면, 해당 패킷이 유효하지 않기 때문에 스위치는 패킷을 삭제합니다. DHCP 서버로부터 수신된 패킷의 경우, 릴레이 에이전트는 유효하지 않은 메시지를 삭제합니다.
>
> **Disabled -** 필드가 비활성화로 전환되면, 릴레이 에이전트는 패킷의 옵션 82 필드의 유효성을 검사하지 않습니다.

DHCP 릴레이 에이전트 정보 옵션 82 정책: 이 필드는 드롭다운 메뉴를 사용하여 교체(Replace), 삭제(Drop), 유지(Keep)로 전환할 수 있습니다. 이는 **DHCP Agent Information Option 82 Check가** 비활성화로 설정될 때 패킷 처리에 대한 스위치의 정책을 설정하는 데 사용됩니다. 기본값은 *Replace* 입니다.

> **Replace -** DHCP 클라이언트로부터 수신된 패킷에 옵션 82 필드가 이미 존재하는 경우, 옵션 82 필드는 교체됩니다.
>
> **Drop -** DHCP 클라이언트로부터 수신된 패킷에 옵션 82 필드가 이미 존재하는 경우, 패킷이 삭제됩니다.

Keep - DHCP 클라이언트로부터 수신된 패킷에 옵션 82 필드가 이미 존재하는 경우, 옵션 82 필드는 유지됩니다.

DHCP 릴레이 에이전트 정보 옵션 82 원격 ID: 이 필드는 기본(Default)과 사용자 정의(User Define) 간에 전환할 수 있습니다.

시스템 > DHCP 릴레이 > DHCP 릴레이 인터페이스 설정

이 페이지에서는 DHCP 서버의 IP 주소를 식별할 수 있습니다. 릴레이 에이전트 인터페이스는 항상 "시스템(System)"으로 고정되어 있습니다.

그림 4.37 - 시스템 > DHCP 릴레이 > DHCP 릴레이 인터페이스 설정

인터페이스: 스위치에서 서버에 직접 연결될 IP 인터페이스입니다.

서버 IP: DHCP 서버의 IP 주소를 입력합니다. IP 인터페이스당 최대 네 개의 서버 IP를 구성할 수 있습니다. 변경 사항을 적용하려면 **Apply을 클릭하십시오**.

시스템 > DHCP 로컬 릴레이 설정

DHCP 로컬 릴레이가 활성화되면 스위치는 LAN(VLAN) 내에서 DHCP 릴레이 에이전트로 작동합니다. DHCP 브로드캐스트는 스위치에 의해 포착되어 교체됩니다. 또한 DHCP 옵션 82는 원래 DHCP 패킷에 삽입됩니다.

그림 4.38 - 시스템 > DHCP 로컬 릴레이 설정

DHCP Local Relay Status: 드롭다운 목록에서 DHCP 로컬 릴레이 기능을 전역적으로 활성화/비활성화합니다. 기본값은 비활성화입니다.

VLAN 구성 기준: 드롭다운 메뉴에서 VID 또는 VLAN 이름으로 VLAN을 구성합니다.

State: VLAN에서 DHCP 로컬 릴레이가 활성화되었는지 여부를 지정합니다.

Enabled – VLAN에서 DHCP 로컬 릴레이를 활성화합니다.

Disabled – VLAN에서 DHCP 로컬 릴레이를 비활성화합니다.

DHCP Local Relay VID List: DHCP 로컬 릴레이가 정의된 VLAN 목록을 표시합니다. 변경 사항을 적용하려면 **Apply** 버튼을 클릭하십시오.

시스템 > DHCPv6 릴레이 설정

DHCPv6 릴레이 설정 페이지에서는 사용자가 DHCPv6 설정을 구성할 수 있습니다.

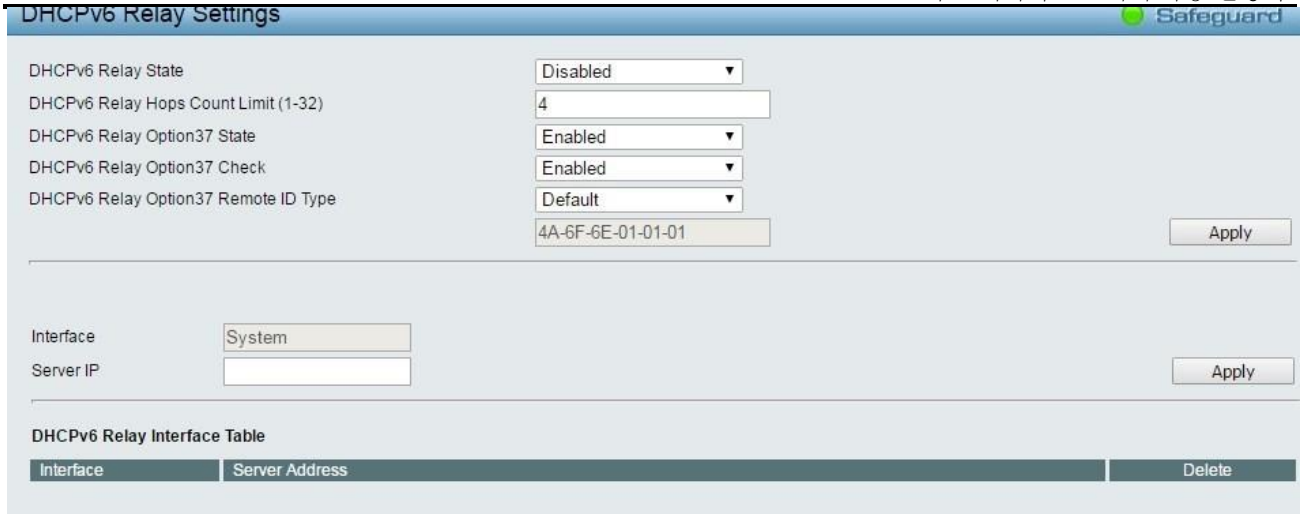


그림 4.39 - 시스템 > DHCPv6 릴레이 설정

DHCPv6 Relay Status: 드롭다운 목록에서 DHCPv6 릴레이 기능을 전역적으로 활성화/비활성화합니다. 기본값은 비활성화입니다.

DHCPv6 릴레이 홉 수 제한(1-32): DHCPv6 메시지를 전달할 수 있는 최대 라우터 홉 수를 정의하기 위해 1과 32 사이의 값을 입력합니다. 기본 홉 수는 4입니다.

DHCPv6 릴레이 옵션37 상태: DHCPv6 릴레이 옵션 37 상태를 활성화 또는 비활성화합니다.

DHCPv6 Relay Option37 Check: DHCPv6 릴레이 옵션 37 확인을 활성화 또는 비활성화합니다.

DHCPv6 Relay Option37 Remote ID Type: DHCPv6 릴레이 옵션 37 원격 ID 유형을 **CID with User Defined**, **User Defined** 또는 **Default로 지정합니다.**

인터페이스: 항상 시스템(System)으로 고정되어 있습니다.

서버 IP: 서버 IP 주소를 입력합니다.

변경 사항을 적용하려면 **Apply** 버튼을 클릭하십시오.

시스템 > 시스템 로그 구성 > 시스템 로그 설정

이 페이지에서는 이벤트 로깅 기능을 구성할 수 있습니다. 로그 메시지는 다양한 방법으로 비휘발성 RAM에 저장될 수 있습니다 .

그림 4.40 - 시스템 > 시스템 로그 구성 > 시스템 로그 설정

시스템 로그: 시스템 로그 기능을 활성화하거나 비활성화합니다.
변경 사항을 적용하려면 **Apply** 버튼을.

시스템 로그 저장 모드 설정:

Save Mode: 드롭다운 메뉴를 사용하여 로그 항목을 트리거하는 방법을 선택합니다. 요청에 따라(On Demand), 시간 간격(Time Interval), 로그 트리거(Log Trigger) 중에서 선택합니다.

On Demand – 이 방법을 선택한 사용자는 스위치에 수동으로 저장하라고 지시할 때만 로그 파일을 저장합니다.

Time Interval – 이 방법을 선택한 사용자는 스위치가 로그 파일을 저장할 시간 간격을 설정할 수 있습니다. 사용자는 1분에서 65535분 사이의 시간을 설정할 수 있습니다.

Log Trigger – 이 방법을 선택한 사용자는 스위치에서 로그 이벤트가 발생할 때마다 로그 파일이 저장됩니다.

Minutes (1-65535): 로그 항목을 작성할 시간 간격을 분 단위로 지정합니다.

변경 사항을 적용하려면 **Apply** 버튼을 클릭하십시오.스위치 로그를 스위치의 플래시 메모리에 저장하려면 **Save Log** 버튼을 클릭하십시오.

시스템 > 시스템 로그 구성 > SysLog 호스트

Syslog 호스트는 로그 수신을 처리하는 전용 호스트를 참조합니다. 메시지 심각도는 전송될 이벤트 메시지 세트를 결정합니다.

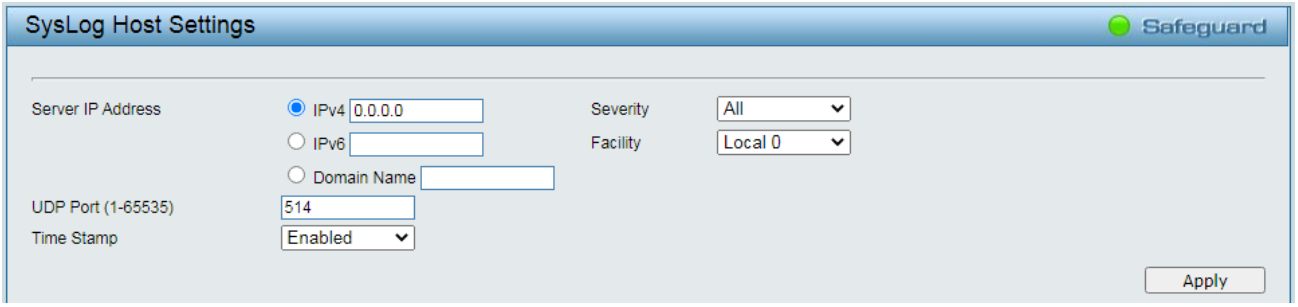


그림 4.41 - 시스템 > 시스템 로그 구성 > SysLog 호스트

서버 IP 주소: 선택 가능한 IPv4 주소, IPv6 주소 및 도메인 이름 문자열입니다.

UDP 포트: 서버 로그가 전송되는 UDP 포트를 지정합니다. 가능한 범위는 1 – 65535이며, 기본값은 514입니다.

타임스탬프: 로그 메시지에 타임 스탬프를 추가하도록 선택합니다.

Severity: 서버로 전송되는 경고 메시지의 최소 심각도를 지정합니다. 세 가지 수준이 있습니다. 심각도 수준을 선택하면 선택 위의 모든 심각도 수준이 자동으로 선택됩니다. 가능한 수준은 다음과 같습니다:

Warning - 장치 경고의 가장 낮은 수준. 장치는 정상적으로 작동하지만 운영 문제 발생.

Informational - 장치 정보를 제공.

모두 - 모든 수준의 시스템 로그를 표시합니다. 기본값.

시설: 시스템 로그가 원격 서버로 전송되는 애플리케이션을 지정합니다. 하나의 서버에 하나의 시설만 할당할 수 있습니다. 두 번째 시설 수준이 할당되면 첫 번째 시설이 덮어쓰여집니다. 최대 여덟 개의 시설(Local 0 ~ Local 7)을 할당할 수 있습니다.

시스템 > 시간 프로필

시간 프로필 페이지에서는 장치의 시간 프로필 설정을 구성할 수 있습니다.

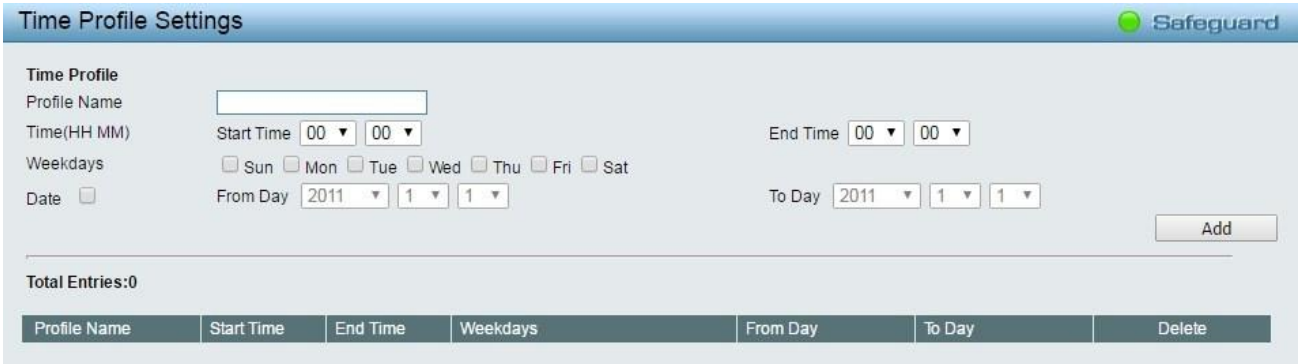


그림 4.42 - 시스템 > 시간 프로파일

Profile Name: 프로필 이름을 지정합니다.

시간(HH MM): 시작 시간과 종료 시간을 지정합니다.

평일: 작동 요일을 지정합니다.

Date: 날짜를 선택하고 시간 프로필의 시작일과 종료일을 지정합니다.

새 시간 프로필을 생성하려면 **Add를 클릭하고**, 테이블에서 시간 프로필을 삭제하려면 **Delete를 클릭하십시오**.

시스템 > 절전

전원 절약 모드 기능은 사용자가 설정한 일정에 따라 다양한 방법으로 전력 소비를 자동으로 줄이는 데 도움을 줍니다.전력 소비를 줄이면 생성되는 열이 줄어들어 제품 수명이 연장되고 운영 비용이 낮아집니다. 기본적으로 링크 상태 감지가 비활성화되어 있습니다. 변경 사항을 적용하려면 **Apply** 을 클릭하십시오.

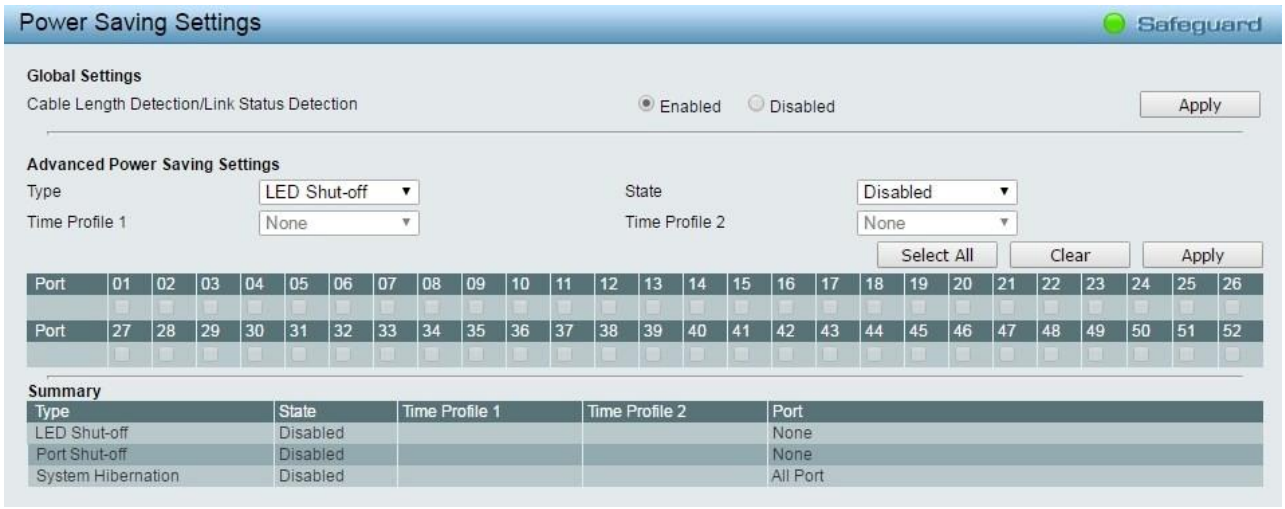


그림 4.43 - 시스템 > 절전

고급 절전 설정:

Type: 전원 절약 유형을 LED 차단(LED Shut-off), 포트 차단(Port Shut-off) 또는 시스템 휴면(System Hibernation)으로 지정합니다.

> **LED 차단 -** LED 차단이 높은 우선순위를 갖습니다. 사용자가 LED 차단을 선택하면 프로필 기능은 작동하지 않습니다. 이는 상태가 비활성화된 경우 시간 프로필 시간이 만료된 후 LED가 켜지지 않음을 의미합니다. 반대로, LED가 활성화되면 시간 프로필 기능이 작동합니다.
>
> **Port Shut-off -** 포트 차단 상태도 높은 우선순위를 가집니다(우선순위 규칙은 LED와 동일). 따라서 포트 차단 상태가 이미 비활성화된 경우, 시간 프로필 기능은 작동하지 않습니다.
>
> **System Hibernation -** 이 모드에서는 모든 포트의 주요 칩셋(MAC 및 PHY)이 비활성화되므로 스위치가 가장 많은 전력 절약 수치를 달성하며, CPU에 필요한 에너지가 최소화됩니다.

State: 전원 절약 상태를 활성화(Enabled) 또는 비활성화(Disabled)로 지정합니다.

Time Profile 1: 시간 프로필 또는 없음(None)을 지정합니다.

Time Profile 2: 시간 프로필 또는 없음(None)을 지정합니다.

포트: 전원 절약을 구성할 포트를 지정합니다.

모든 포트를 구성하려면 **Select All을 클릭하고** 모든 포트를 선택 해제하려면 **Clear를 클릭하십시오.**

그런 다음 **Apply을 클릭하여 변경 사항을 적용합니다**.

시스템 > IEEE802.3az EEE 설정

IEEE 802.3 EEE 표준은 네트워크 링크의 에너지 소비를 감소시키기 위한 메커니즘과 프로토콜을 정의합니다. 사용자가 낮은 사용량 기간 동안 인터페이스를 저전력 상태로 전환하여 네트워크 연결을 중단하지 않고도 가능하게 합니다. 전송

및 수신 측은 IEEE802.3az EEE를 준수해야 합니다. 기본적으로 스위치의 802.3az EEE 기능은 비활성화되어 있습니다. 사용자는 IEEE802.3az EEE 설정 페이지를 통해 개별 포트에서 이 기능을 활성화할 수 있습니다.

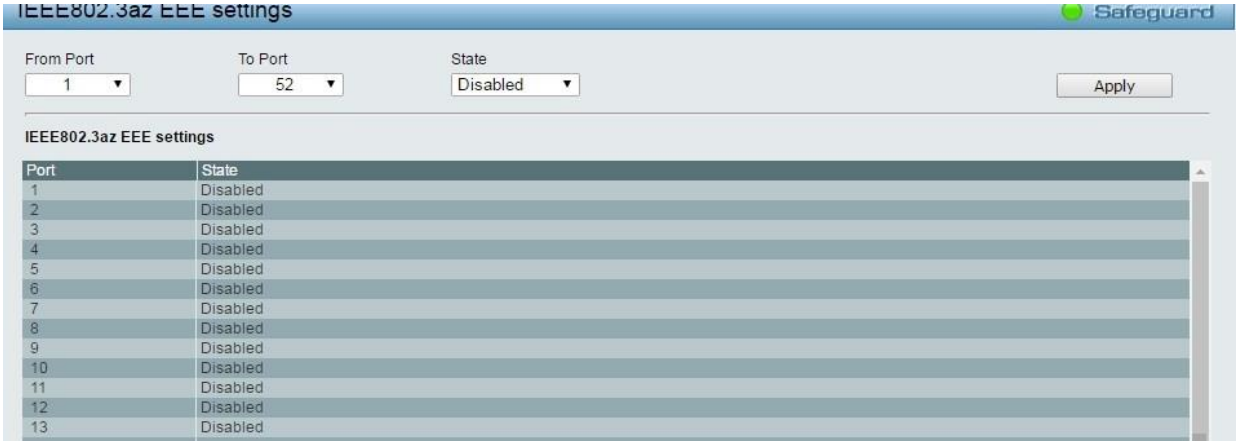


그림 4.44 - 시스템 > IEEE802.3az EEE 설정

From Port / To Port: 선택한 포트부터 시작하여 연속적인 포트 그룹을 구성할 수 있습니다.
State: 지정된 포트에 대해 IEEE802.3az EEE를 활성화 또는 비활성화합니다. 기본적으로 모든 포트는 비활성화되어 있습니다. 변경 사항을 적용하려면 **Apply** 버튼을 클릭하십시오.

연결 속도가 1000M에서 100M로 떨어지거나 첫 번째 링크가 설정되는 데 시간이 더 걸리는 경우, 아래 단계를 따르고 다시 확인하십시오:

일. 호스트 PC의 이더넷 어댑터 또는 LAN 컨트롤러의 드라이버를 업그레이드하십시오.

이. 스위치 포트에서 EEE 기능을 비활성화하십시오.

시스템 > D-Link Discover 프로토콜 설정

D-Link 전용 프로토콜인 D-Link 발견 프로토콜(DDP)은 SmartConsole 유틸리티에서 사용됩니다.

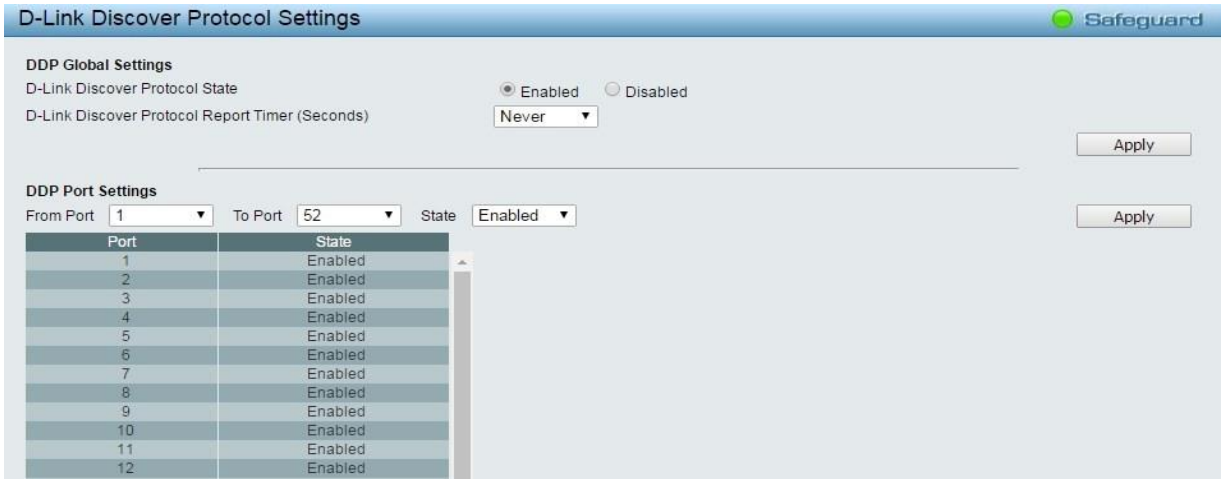


그림 4.45 - 시스템 > D-Link Discover 프로토콜 설정

D-Link Discover Protocol State: 발견 프로토콜 상태를 활성화 또는 비활성화합니다. 기본값은 활성화입니다.

D-Link Discover Protocol Report Timer (Seconds): D-Link Discover Protocol의 보고 타이머를 초 단위로 구성합니다. 값은 30, 60, 90, 120 또는 없음(Never)입니다.

변경 사항을 적용하려면 **Apply** 버튼을 클릭하십시오.

DDP 포트 설정:

From Port / To Port: 스위치의 D-Link 발견 프로토콜을 구성할 포트 범위를 지정합니다.

State: 지정된 포트에 대해 D-Link 발견 프로토콜 상태를 활성화 또는 비활성화합니다. 변경 사항을 적용하려면 **Apply** 버튼을 클릭하십시오.

시스템 > 펌웨어 정보

펌웨어 정보 페이지에서는 펌웨어 정보를 표시합니다. 사용자는 다음 시스템 부팅을 위한 이미지 ID를 선택할 수 있습니다.

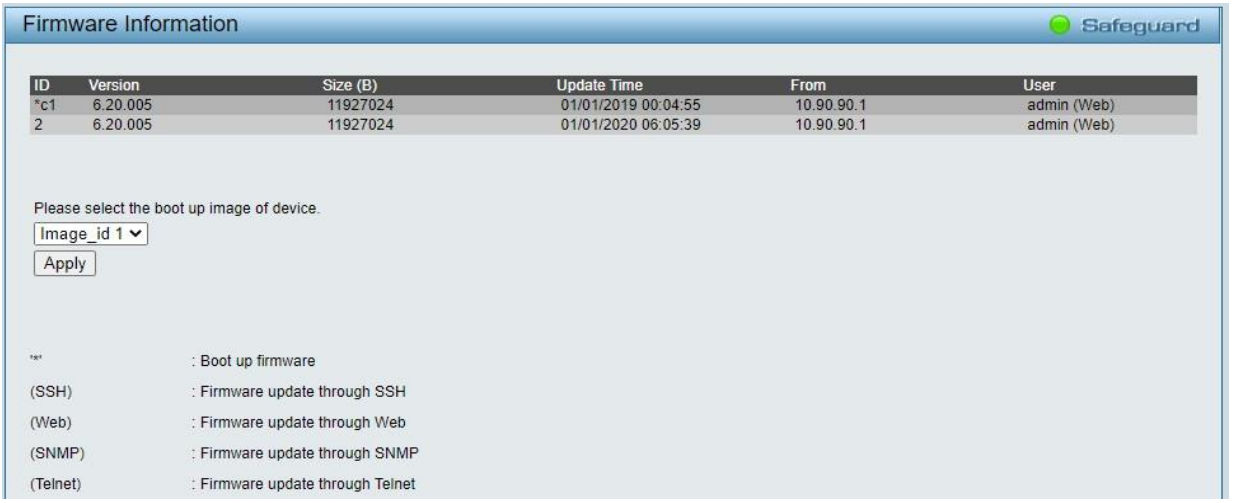


그림 4.46 - 시스템 > 펌웨어 정보

시스템 > 구성 정보

구성 정보 페이지에서는 구성 정보를 표시합니다. 사용자는 다음 시스템 부팅을 위한 구성 ID를 선택할 수 있습니다.

그림 4.47 - 시스템 > 구성 정보

VLAN > 802.1Q VLAN

VLAN은 네트워크의 어디에나 있을 수 있는 포트 그룹이지만, 마치 동일한 지역에 있는 것처럼 통신할 수 있습니다. VLAN은 부서 그룹(예: 연구개발(R&D), 마케팅), 사용 그룹(예: 이메일) 또는 멀티캐스트 그룹(비디오 회의와 같은 멀티미디어 애플리케이션)으로 쉽게 구성될 수 있으며, 따라서 물리적 연결을 변경하지 않고도 장치를 새로운 VLAN으로 이동할 수 있도록 하여 네트워크 관리의 복잡성을 줄입니다.

IEEE 802.1Q VLAN 구성 페이지는 강력한 VID 관리 기능을 제공합니다. 원래 설정은 VID가 1이며, 기본 이름이 없고 모든 포트는 "Untagged"입니다.

Rename: VLAN 그룹의 이름을 바꾸려면 클릭합니다.

Delete VID: VLAN 그룹을 삭제하려면 클릭합니다.

Add New VID: 새 VID 그룹을 만들고 포트를 01에서 28 **Untag**, **Tag** 또는 **Not Member** 로 할당합니다. 포트는 하나의 VID에서만 태그가 없을 수 있습니다. VID 그룹을 저장하려면 **Apply을 클릭합니다**.

사용자는 R&D, 마케팅, 이메일 등 원하는 그룹에 따라 이름을 변경할 수 있습니다

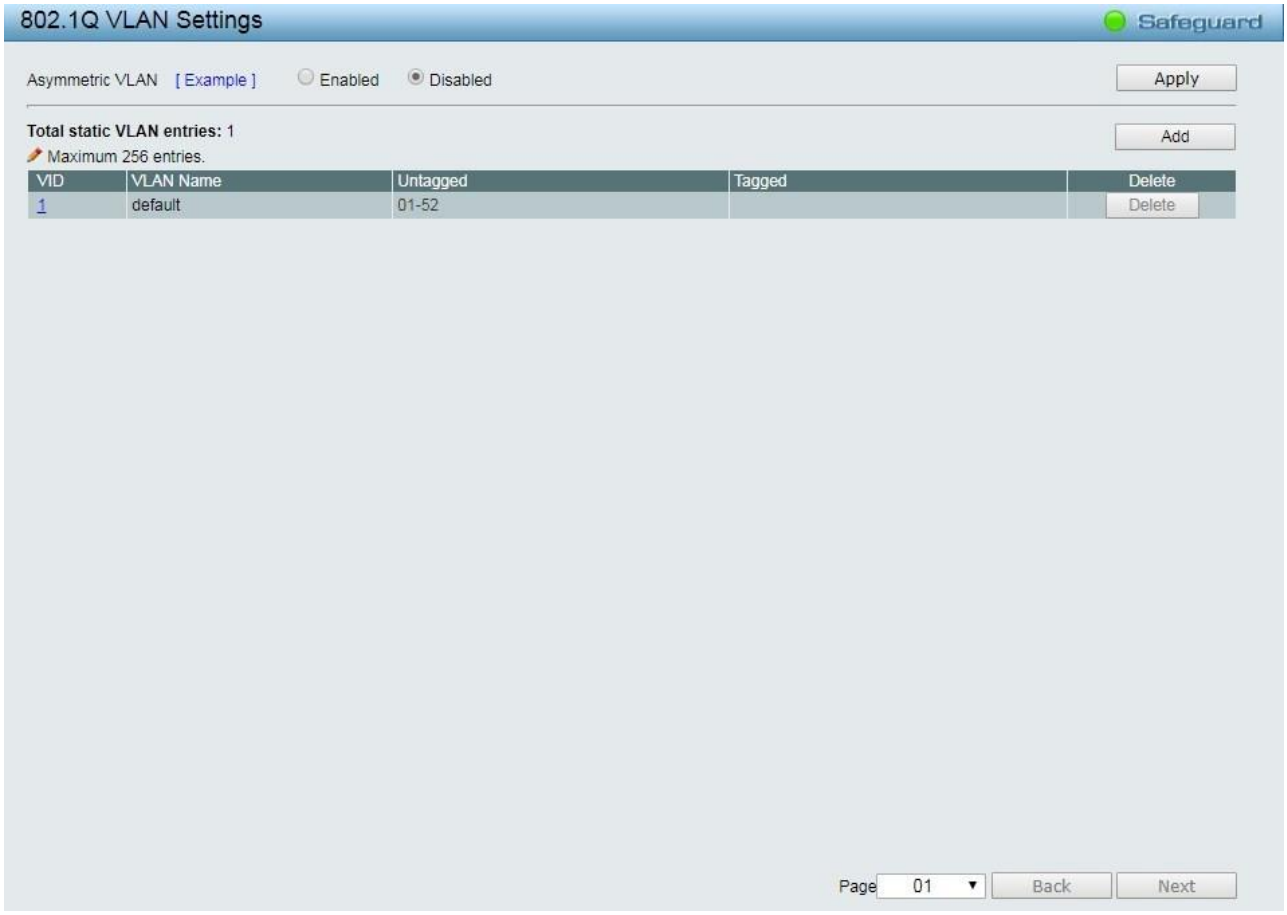


그림 4.48 - 802.1Q VLAN > 구성

새 VID 그룹을 만들려면 **Add** 를 클릭하고 VID 및 VLAN 이름을 입력한 후 01에서 52까지의 포트를 **Untag**, **Tag** 또는 **Not Member로 할당합니다. VID 그룹을 저장하려면 Apply** 을 클릭합니다 **.**

그림 4.49 - VID 추가> 802.1Q VLAN 구성 >

Apply를 클릭하면 802.1Q VLAN 구성 테이블이 업데이트된 내용을 표시합니다.

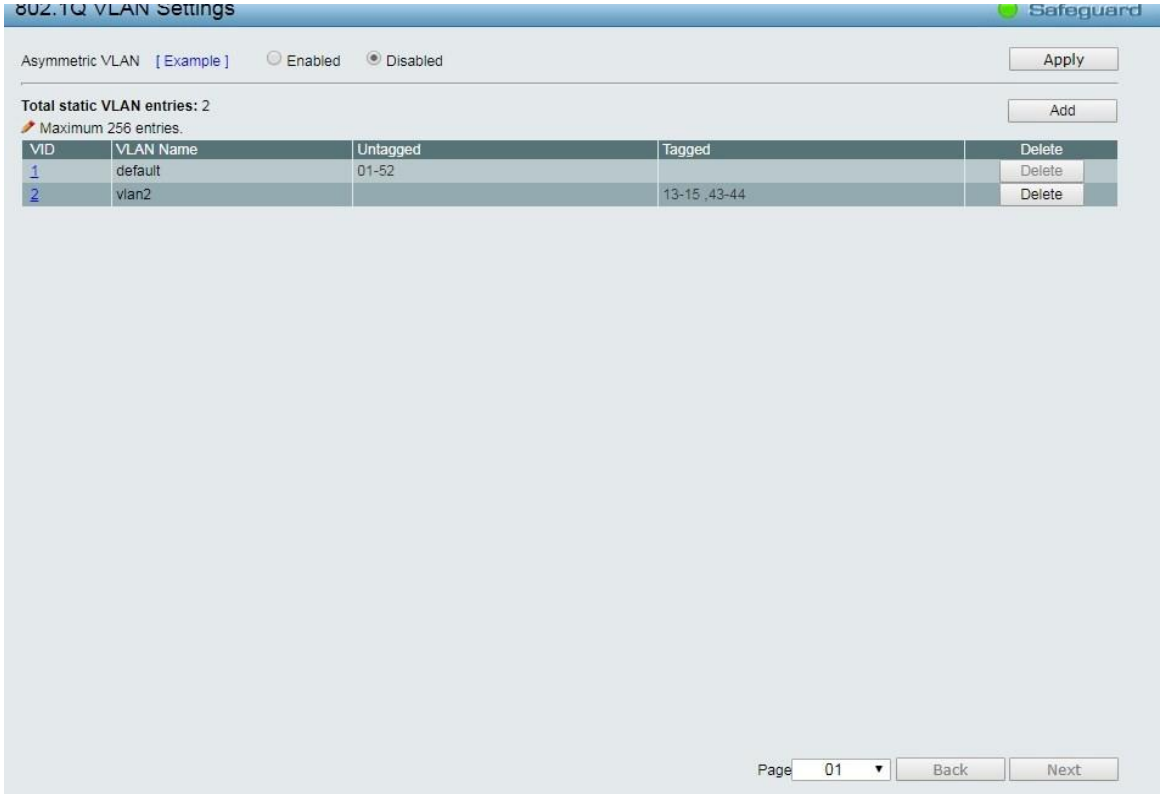


그림 4.50 - VLAN 추가 > 802.1Q VLAN 구성 >

VID 번호를 클릭하면 사용자가 선택한 VLAN 그룹의 구성이 표시됩니다.
포트 할당을 변경한 후 **Apply** 를 클릭하여 변경 사항을 적용합니다.

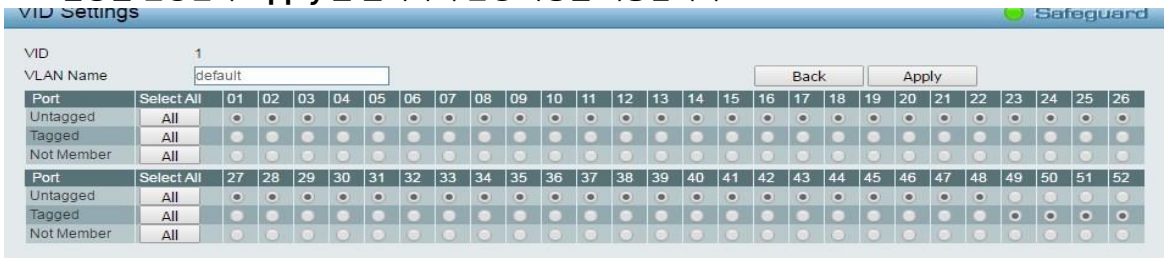


그림 4.51 - 구성 > 802.1Q VLAN > VID 할당

VLAN > 802.1Q VLAN PVID

802.1Q VLAN PVID 설정에서는 사용자에게 각 포트의 포트 VLAN ID(PVID)를 구성할 수 있는 기능을 제공합니다. 변경 사항을 적용하려면 **Apply를** 클릭합니다.

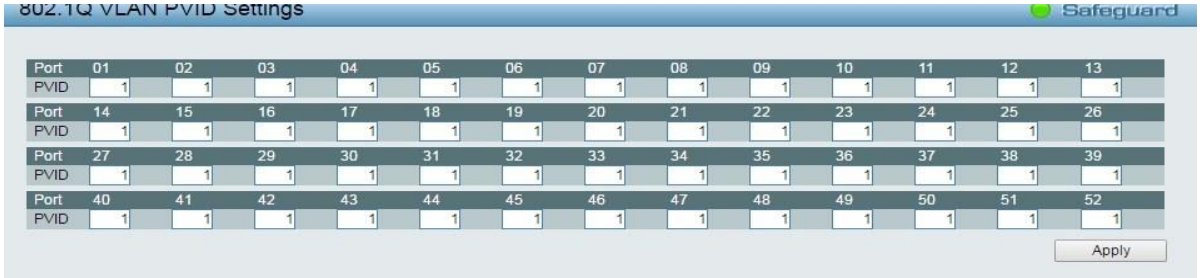


그림 4.52 - 구성 > 802.1Q VLAN PVID

VLAN > Voice VLAN > Voice VLAN 전역 설정

Vioce 트래픽은 실시간 전송에서 낮은 대기 시간(높은 우선순위)을 요구하며, 이는 음질에 심각한 영향을 미칩니다. Vioce VLAN 기능은 사용자가 자격이 있는 트래픽을 높은 우선순위로 해당 VLAN 그룹에 배치할 수 있도록 도와줍니다.

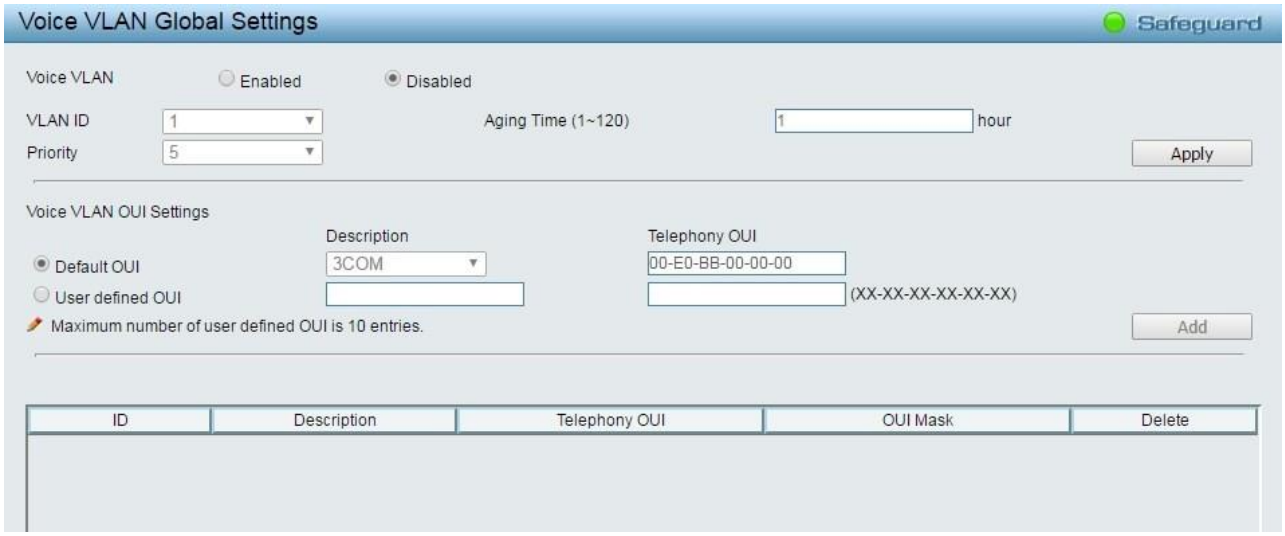


그림 4.53 - VLAN > 음성 VLAN > 음성 VLAN 전역 설정

Voice VLAN: Voice VLAN을 활성화 또는 비활성화하려면 선택합니다. 기본값은 비활성화되어 있습니다. 글로벌 상태가 활성화되면 다른 구성 가능한 매개변수가 사용 가능합니다.

VLAN ID: Vioce 트래픽을 할당할 VLAN의 ID입니다. 전용 Vioce VLAN을 할당하기 전에 802.1Q VLAN 페이지에서 먼저 VLAN을 생성해야 합니다. 802.1Q VLAN 설정 페이지에서 구성한 구성원 포트는 Voice VLAN의 정적 구성원 포트가 됩니다. Voice VLAN에 포트를 동적으로 추가하려면 **Auto Detection** 기능을 활성화해야 합니다.

Priority: Voice VLAN 트래픽에 대한 802.1p 우선 순위 수준입니다.

Aging Time (1-120): 포트가 자동 Vioce VLAN 구성원일 경우 Vioce VLAN에서 포트를 제거할 기간(시간)을 입력합니다. 마지막 Vioce 장치가 트래픽 전송을 중지하고 해당 Vioce 장치의 MAC 주소가 에이징되면 Vioce VLAN 에이징 타이머가 시작됩니다. Vioce VLAN 에이징 타이머가 만료된 후 포트는 Vioce VLAN에서 제거됩니다. 선택 가능한 범위는 1~120시간이며, 기본값은 1입니다.

변경 사항을 적용하려면 **Apply을 클릭하십시오**.

Voice VLAN OUI Settings: 사용자 정의 Vioce 트래픽의 OUI를 구성할 수 있습니다. OUI(조직 고유 식별자)는 MAC 주소의 처음 세 바이트입니다. 이 식별자는 공급업체, 제조업체 또는 기타 조직을 고유하게 식별합니다.

미리 정의된 OUI가 있으며 사용자가 개인 OUI를 구성할 때 이러한 미리 정의된 OUI를 피해야 합니다. 미리 정의된 Vioce 트래픽의 OUI는 다음과 같습니다.

예	공급업체	약어명
00:E0:BB	3Com	3com
00:03:6B	Cisco	cisco
00:E0:75	Veritel	veritel
00:D0:1E	Pingtel	pingtel
00:01:E3	Siemens	siemens
00:60:B9	NEC/ Philips	nec&philips
00:0F:E2	Huawei-3COM	huawei&3com
00:09:6E	Avaya	avaya

기본 OUI: 3COM, Cisco, Veritel, Pingtel, Siemens, NEC/Philips, Huawei3COM 및 Avaya의 브랜드 이름을 포함한 미리 정의된 OUI 값입니다.

사용자 정의 OUI: 사용자는 설명과 함께 전화 통신 OUI를 수동으로 생성할 수 있습니다. 사용자 정의 OUI의 최대 수는 10입니다.

OUI를 선택하고 하단 표에 **Add** 를 눌러 자동 Voice VLAN 설정을 완료합니다.

참고: Vioce VLAN은 QoS를 포함한 다른 모든 기능보다 높은 우선순위를 갖습니다. 따라서 Vioce 트래픽은 Vioce VLAN 설정에 따라 작동하며 QoS 기능의 영향을 받지 않습니다.

참고: VoIP 트래픽의 품질을 보장하기 위해 Vioce VLAN에 가장 높은 우선 순위를 설정하는 것이 좋습니다.

VLAN > 음성 VLAN > 음성 VLAN 포트 설정

Vioce VLAN 포트 설정 페이지에서는 사용자가 IP 전화에서 Vioce 트래픽을 자동으로 할당된 VLAN에 배치하여 VoIP 서비스를 향상시킬 수 있도록 합니다. 높은 우선순위와 개별 VLAN을 통해 VoIP 트래픽의 품질과 보안을 보장합니다.

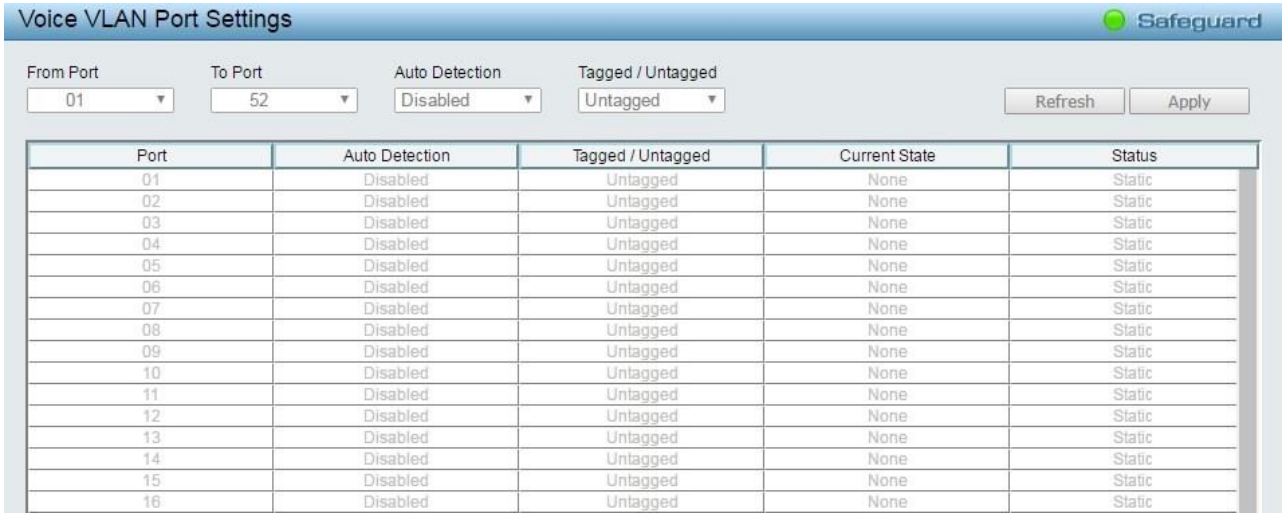


그림 4.54 - VLAN > 음성 VLAN > 음성 VLAN 포트 설정

From Port / To Port: 선택한 포트부터 시작하여 연속적인 포트 그룹을 구성할 수 있습니다.
Auto Detection: 스위치는 장치의 OUI가 Vioce VLAN OUI 설정 페이지에서 구성된 전화 통신 OUI와 일치할 경우 포트를 자동으로 Vioce VLAN에 추가합니다. 드롭다운 메뉴를 사용하여 OUI 자동 감지 기능을 활성화 또는 비활성화합니다. 기본값은 비활성화되어 있습니다.

Tagged / Untagged: 포트를 Tagged 또는 untagged로 설정합니다.

변경 사항을 적용하려면 **Apply** 을 클릭하고, Vioce VLAN 테이블을 새로 고치려면 **Refresh를** 클릭하십시오.

참고: Vioce VLAN은 QoS를 포함한 다른 모든 기능보다 높은 우선순위를 갖습니다. 따라서 Vioce 트래픽은 Vioce VLAN 설정에 따라 작동하며 QoS 기능의 영향을 받지 않습니다.

참고: VoIP 트래픽의 품질을 보장하기 위해 Vioce VLAN에 가장 높은 우선 순위를 설정하는 것이 좋습니다.

VLAN > 음성 VLAN > 음성 장치 목록

Vioce 장치 목록 페이지에서는 감지되거나 생성된 Vioce 장치의 정보를 표시합니다.

그림 4.55 - VLAN > 음성 VLAN > 음성 장치 목록

포트를 선택하거나 모든 포트를 선택한 후 **Search를** 클릭하여 테이블에 Vioce 장치 정보를 표시합니다.

VLAN > 자동 감시 VLAN > 자동 감시 속성

비디오 트래픽은 실시간 전송에서 낮은 대기 시간(높은 우선순위)을 요구하며, 이는 이미지와 소리의 품질에 심각한 영향을 미칩니다. 자동 감시 VLAN 기능은 사용자가 자격이 있는 트래픽을 높은 우선순위로 해당 VLAN 그룹에 배치할 수 있도록 도와줍니다.

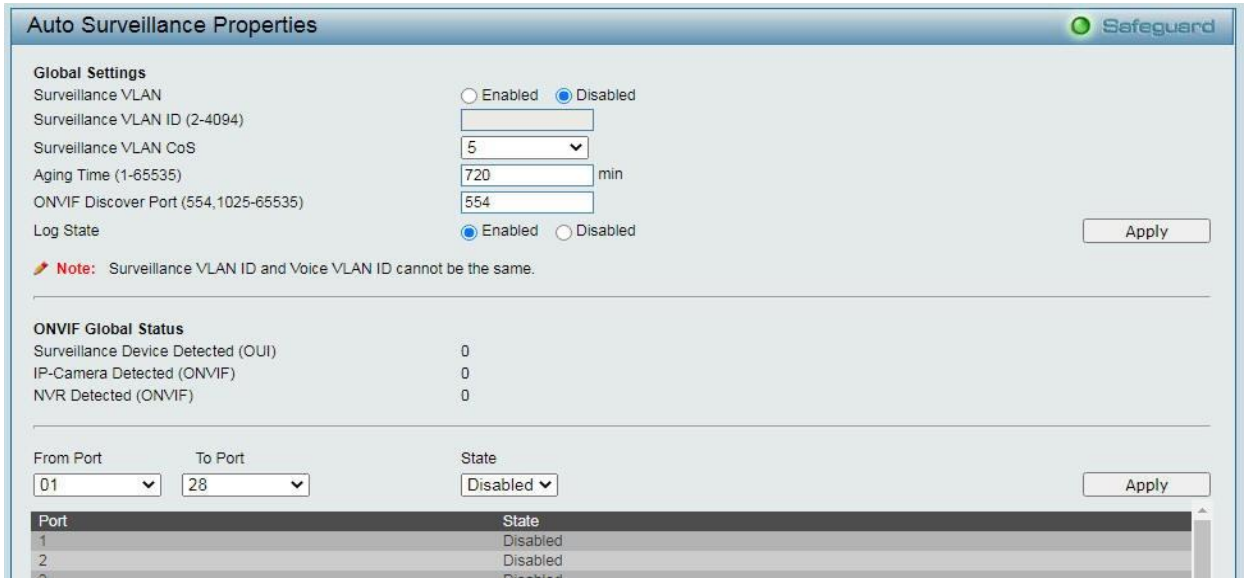


그림 4.56 - VLAN > 자동 감시 VLAN > 자동 감시 속성

전역 설정: 관련 자동 Surveillance VLAN 글로벌 설정을 구성합니다.
자동 감시 VLAN: 자동 감시 VLAN 상태를 활성화 또는 비활성화합니다.

감시 VLAN ID: 감시 VLAN ID를 지정합니다. 범위는 2에서 4094입니다.

감시 VLAN CoS: Surveillance VLAN의 우선 순위를 지정합니다. 범위는 0에서 7입니다.

Aging Time (1-65535): Surveillance VLAN의 에이징 시간을 지정합니다. 범위는 1에서 65535분이며, 기본값은 720분입니다. 에이징 시간은 포트가 자동 Surveillance VLAN 구성원일 경우 포트를 Surveillance VLAN에서 제거하는 데 사용됩니다. 마지막 감시 장치가 트래픽 전송을 중지하고 해당 감시 장치의 MAC 주소가 에이징되면 Surveillance VLAN 에이징 타이머가 시작됩니다. Surveillance VLAN 에이징 타이머가 만료된 후 포트는 Surveillance VLAN에서 제거됩니다. 감시 트래픽이 에이징 시간 동안 복구되면 에이징 타이머가 재설정되고 중단됩니다.

Discover Port (554, 1024-65535): Surveillance VLAN의 TCP/UDP 포트 번호를 지정합니다. 범위는 554 또는 1024에서 65535 사이입니다. 이는 RTSP 스트림 스누핑을 위한 TCP/UDP 포트 번호를 구성하는 데 사용됩니다. ONVIF 지원 IPC 및 ONVIF 지원 NVR은 WS-Discovery를 사용하여 다른 장치를 찾습니다. IPC가 발견되면 스위치는 RTSP, HTTP 및 HTTPS 패킷을 스누핑하여 NVR을 추가로 발견할 수 있습니다. 이러한 패킷은 TCP/UDP 포트가 RTSP 포트 번호와 같지 않으면 스누핑할 수 없습니다.

로그 상태: Surveillance VLAN의 로그 상태를 활성화 또는 비활성화합니다.
변경 사항을 적용하려면 **Apply** 버튼을 클릭하십시오.

VLAN > 자동 감시 VLAN > MAC 설정 및 감시 장치

Voice VLAN과 유사하게, 자동 Surveillance VLAN은 사용자가 D-Link IP 카메라에서 비디오 트래픽을 자동으로 할당된 VLAN으로 배치하여 IP 감시 서비스를 향상시킬 수 있도록 하는 기능입니다. 높은 우선순위와 개별 VLAN을 통해 감시 트래픽의 품질과 보안을 보장합니다. 자동 Surveillance VLAN 기능은 수신 패킷의 소스 MAC 주소/VLAN ID를 확인합니다. 지정된 MAC 주소/VLAN ID와 일치하는 경우, 패킷은 원하는 우선 순위로 스위치를 통과합니다.

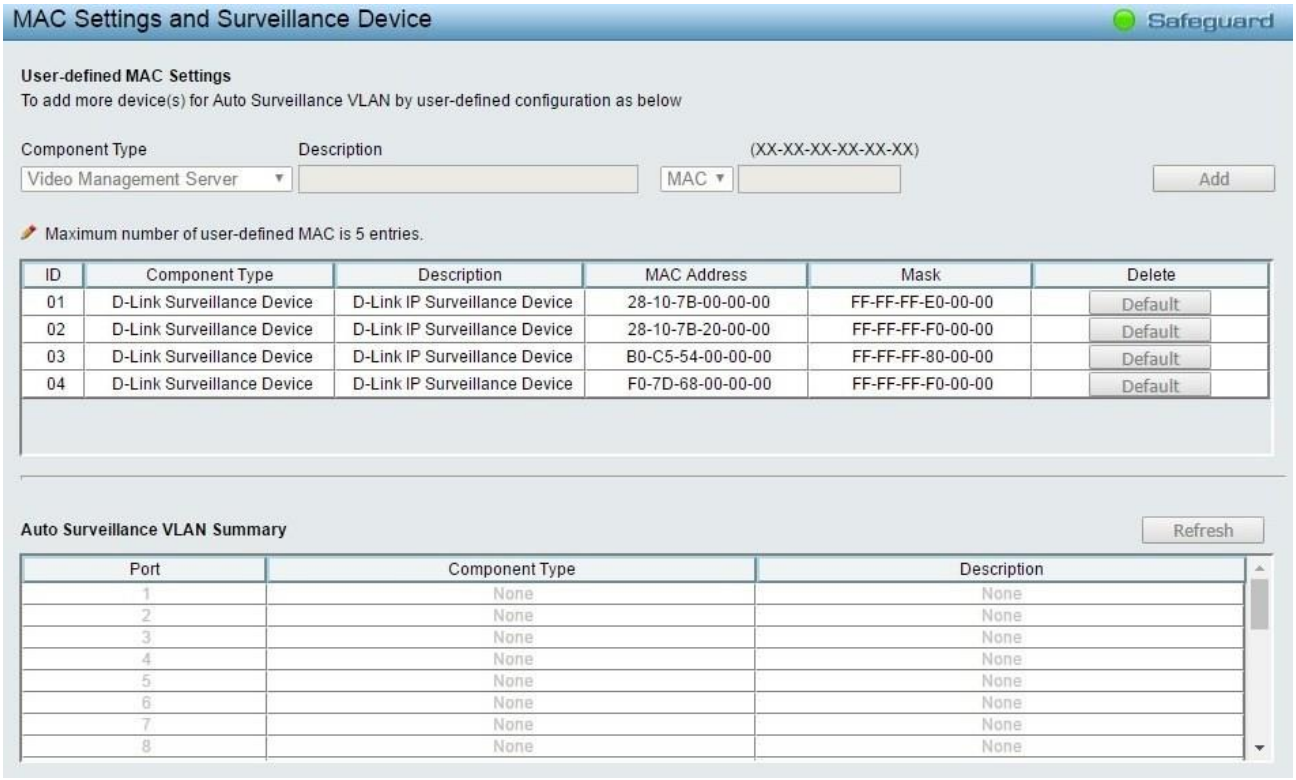


그림 4.57 - VLAN > 자동 감시 VLAN > MAC 설정 및 감시 장치

사용자 정의 MAC 설정:

구성 요소 유형: 기본적으로 자동 감시 VLAN은 D-Link 감시 장치를 자동으로 감지합니다. 자동 감지되도록 구성할 수 있는 다른 다섯 개의 감시 구성 요소가 있습니다. 이 다섯 가지 구성 요소는 비디오 관리 서버(VMS), VMS 클라이언트/원격 뷰어, 비디오 인코더, 네트워크 저장소 및 기타 IP 감시 장치입니다.

설명: 구성 요소 유형에 대한 설명을 입력합니다.

MAC 주소: 사용자는 감시 구성 요소를 위한 MAC 또는 OUI 주소를 수동으로 생성할 수 있습니다. 사용자 정의 MAC 주소의 최대 수는 5입니다.

Mask: MAC 또는 OUI에 대한 마스크 주소를 지정합니다.

새로운 감시 구성 요소를 생성하려면 **Add** 를 클릭하고, 자동 Surveillance VLAN 요약 테이블을 새로 고치려면 **Refresh** 을 클릭하십시오.

VLAN > 자동 감시 VLAN > ONVIF IPC 정보

ONVIF(Open Network Video Interface Forum) IPC 정보 페이지에서는 스위치에 연결된 각 IP 카메라에 대한 정보를 표시합니다. 정보에는 포트 번호, IP 주소, MAC 주소, 처리량 및 포트 설명 및 모델 이름과 같은 기타 정보가 포함됩니다.

그림 4.58 - VLAN > 자동 감시 VLAN > ONVIF IPC 정보

VLAN > 자동 감시 VLAN > ONVIF NVR 정보

ONVIF(Network Video Interface Forum) NVR 정보 페이지에서는 스위치에 연결된 각 NVR에 대한 정보를 표시합니다. 정보에는 포트 번호, IP 주소, MAC 주소, IP 카메라 수, 처리량 및 NVR에 연결된 카메라에 대한 설명(그룹 이름, 총 카메라 수, 각 카메라의 포트 및 IP 주소 등)이 포함됩니다.

그림 4.59 - VLAN > 자동 감시 VLAN > ONVIF NVR 정보

점보 프레임> L2 기능

D-Link 기가비트 스마트 관리 스위치는 최대 10000바이트(태그됨)의 점보 프레임(이더넷 프레임 크기인 1536바이트를 초과하는 프레임)을 지원합니다. 기본값은 비활성화되어 있습니다. **Enabled**를 선택한 다음 **Apply**를 클릭하여 점보 프레임 지원을 켭니다.

그림 4.60 - 점보 프레임> L2 기능

포트 미러링 > L2 기능

포트 미러링은 스위치의 하나의 포트에서 다른 포트로 각 수신 및/또는 송신 패킷의 복사본을 전달하여 네트워크 트래픽을 모니터링하는 방법입니다. 이를 통해 네트워크 관리자는 네트워크 성능을 보다 잘 모니터링할 수 있습니다.

그림 4.61 - 포트 미러링> L2 기능

소스 포트 선택 옵션은 다음과 같습니다:

TX (transmit) mode: 소스 포트에서 전송된 데이터를 복제하여 대상 포트로 전달합니다. 모든 포트를 포트 미러링에 포함하려면 "All"을 클릭하십시오.

RX (receive) mode: 소스 포트에서 수신된 데이터를 복제하여 대상 포트로 전달합니다. 모든 포트를 포트 미러링에 포함하려면 "All"을 클릭하십시오.

TX/RX(전송 및 수신) 모드: 소스 포트에서 전송된 데이터와 소스 포트로 전송된 데이터 모두를 복제하여 지정된 대상 포트로 전달합니다. 모든 포트를 포트 미러링에 포함하려면 "All"을 클릭하십시오.

None: 포트의 미러링을 끕니다. 모든 포트를 미러링에서 제거하려면 "모두"를 클릭하십시오.

루프백 감지를 > L2 기능

루프백 감지 기능은 다른 예방 메커니즘이 없는 포트로 생성된 루프를 감지하는 데 사용됩니다. 예를 들어, 스패닝 트리 프로토콜(STP)이 있을 수 있습니다. 일반적으로 링크 파트너가 허브 또는 관리되지 않는 스위치일 때 발생합니다. 루프백 감지 기능은 루프가 발생할 경우 포트를 자동으로 종료하고 관리자에게 로그를 보냅니다. 또한 루프 조건이 제거되면 복구 메커니즘을 제공합니다.

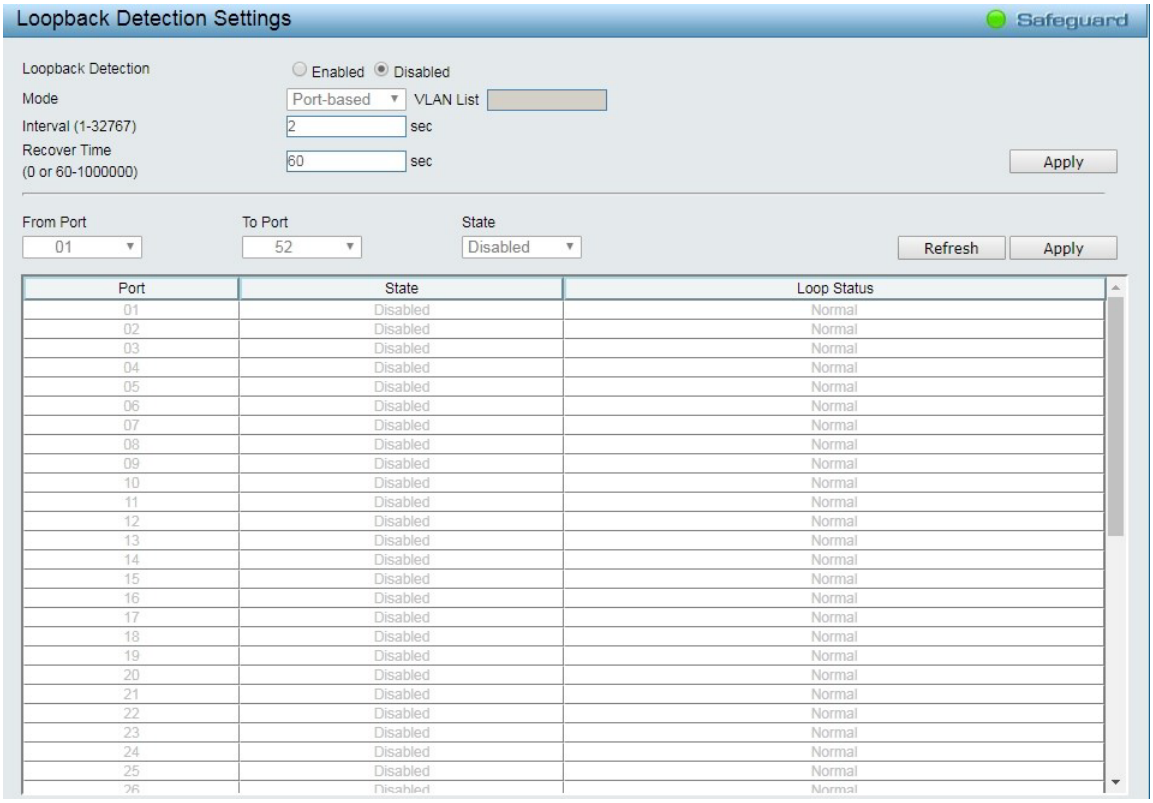


그림 4.62 - 루프백 감지> L2 기능

루프백 감지: 드롭다운 메뉴를 사용하여 루프백 감지를 활성화 또는 비활성화합니다. 기본값은 비활성화입니다 *포트 기반 또는 VLAN 기반 모드를 지정합니다. 포트 기반 모드가 선택된 경우 루프가 발생한 포트는 종료되며 모든 구성원 VLAN에 영향을 미칩니다. VLAN 기반 모드가 선택된 경우 루프가 발생한 VLAN의 구성원 포트만 종료됩니다.*

VID List: VID를 지정합니다.

Interval (1-32767): 1초에서 32767초 사이의 루프 감지 간격을 설정합니다. 기본값은 2초입니다.

복구 시간(0 또는 60-1000000): 루프백이 감지될 때 복구를 허용하는 시간(초)입니다. 루프 감지 복구 시간은 0초 또는 60초에서 1000000초로 설정할 수 있습니다. 0을 입력하면 루프 감지 복구 시간이 비활성화됩니다. 기본값은 60초입니다.

From Port: 선택한 포트부터 시작하여 연속적인 포트 그룹의 시작입니다.

To Port: 선택한 포트부터 시작하여 연속적인 포트 그룹의 종료입니다.

State: 드롭다운 메뉴를 사용하여 활성화 및 비활성화로 전환합니다. 기본값은 비활성화되어 있습니다.

변경 사항을 적용하려면 **Apply** 버튼을 클릭하고 루프백 감지 테이블을 새로 고치려면 **refresh를** 클릭하십시오.

L2 기능 > MAC 주소 테이블 > 정적 MAC

정적 MAC 주소 항목을 전달 테이블에 생성할 수 있습니다. 이 기능은 일반적으로 네트워크에서 영구적으로 사용되는 특정 장치에 연결된 포트에 사용됩니다. 예: DHCP 서버, syslog 서버, 네트워크 게이트웨이 위치 등.

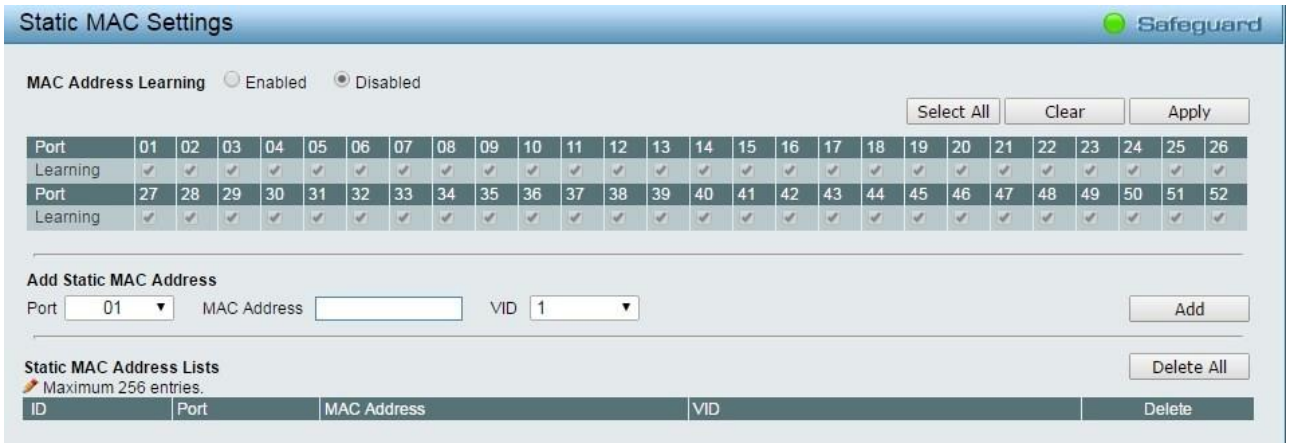


그림 4.63 - L2 기능 > MAC 주소 테이블 > 정적 MAC 주소

Static MAC Address Lists 테이블은 연결된 정적 MAC 주소와 VID를 표시합니다.

Add Static MAC Address(고정 MAC 주소 추가): 사용자는 할당된 포트 번호를 선택해야 합니다. MAC 주소와 VID를 모두 입력한 다음 **추가를 클릭합니다. 하나의 항목을 제거하려면 Delete** 를 클릭하고 모든 항목을 지우려면 **Delete all** 를 클릭합니다.

MAC 주소 자동 학습 기능을 비활성화하고 정적 MAC 주소를 지정하면 네트워크는 해커와 같은 잠재적 위협으로부터 보호됩니다. 불법 MAC 주소의 트래픽은 스위치에서 전달되지 않기 때문입니다.

L2 기능 > MAC 주소 테이블 > 동적 포워딩 테이블

각 포트에 대해 이 테이블은 스위치에서 학습한 MAC 주소를 표시합니다. 정적 MAC 주소 목록에 MAC 주소를 추가하려면 **Add** 체크박스를 클릭한 다음 식별된 주소와 관련된 **Apply을 클릭합니다**.

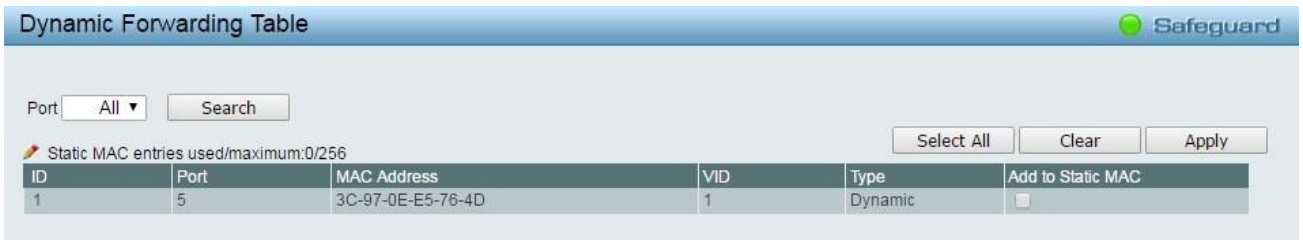


그림 4.64 - L2 기능 > MAC 주소 테이블 > 동적 전달 테이블

L2 기능 > 스패닝 트리 > STP 브리지 전역 설정

스위치는 세 가지 버전의 스패닝 트리 프로토콜을 구현합니다. IEEE 802.1w 사양에 정의된 Rapid Spanning Tree Protocol(RSTP)와 IEEE 802.1D STP 및 Multiple Spanning Tree Protocol(MSTP)에 호환되는 버전입니다. RSTP는 IEEE 802.1D를 구현하는 레거시 장비와 함께 작동할 수 있지만 RSTP를 사용함으로써 얻는 이점은 잃게 됩니다.

IEEE 802.1w Rapid Spanning Tree Protocol(RSTP)은 802.1D STP 표준에서 발전한 것입니다. RSTP는 최근 스위칭 혁신의 기능을 방해하는 STP의 일부 한계를 극복하기 위해 개발되었습니다. 기본 기능과 많은 용어는 STP와 동일합니다. STP에 대해 구성된 대부분의 설정은 RSTP에서도 사용됩니다. 이 섹션에서는 몇 가지 새로운 스패닝 트리 개념을 소개하고 두 프로토콜 간의 주요 차이점을 설명합니다.

IEEE 802.1 Multiple Spanning Tree(MSTP)는 여러 VLAN을 단일 스패닝 트리 인스턴스에 매핑하여 다양한 로드 밸런싱 시나리오를 제공합니다. 예를 들어, 포트 A가 하나의 STP 인스턴스에서 차단되는 동안, 동일한 포트는 다른 STP 인스턴스에서 전달 상태로 배치될 수 있습니다.

기본적으로 Rapid Spanning Tree는 비활성화되어 있습니다. 활성화되면 스위치는 BPDU 패킷과 해당 Hello 패킷을 수신합니다. BPDU 패킷은 BPDU 패킷을 수신하지 않아도 전송됩니다. 따라서 브리지 간의 각 링크는 링크의 상태에 민감합니다. 궁극적으로 이 차이는 실패한 링크를 더 빠르게 감지하고, 따라서 토폴로지 조정을 더 빠르게 수행하는 결과를 가져옵니다.

기본적으로 Multiple Spanning Tree는 활성화되어 있습니다. 이 기능은 BPDU 패킷을 수신 장치에 태그하고 스패닝 트리 인스턴스, 스패닝 트리 지역 및 이에 연결된 VLAN을 구별합니다.

STP를 활성화한 후 STP 전역 설정을 설정하는 데는 다음 옵션이 포함됩니다:

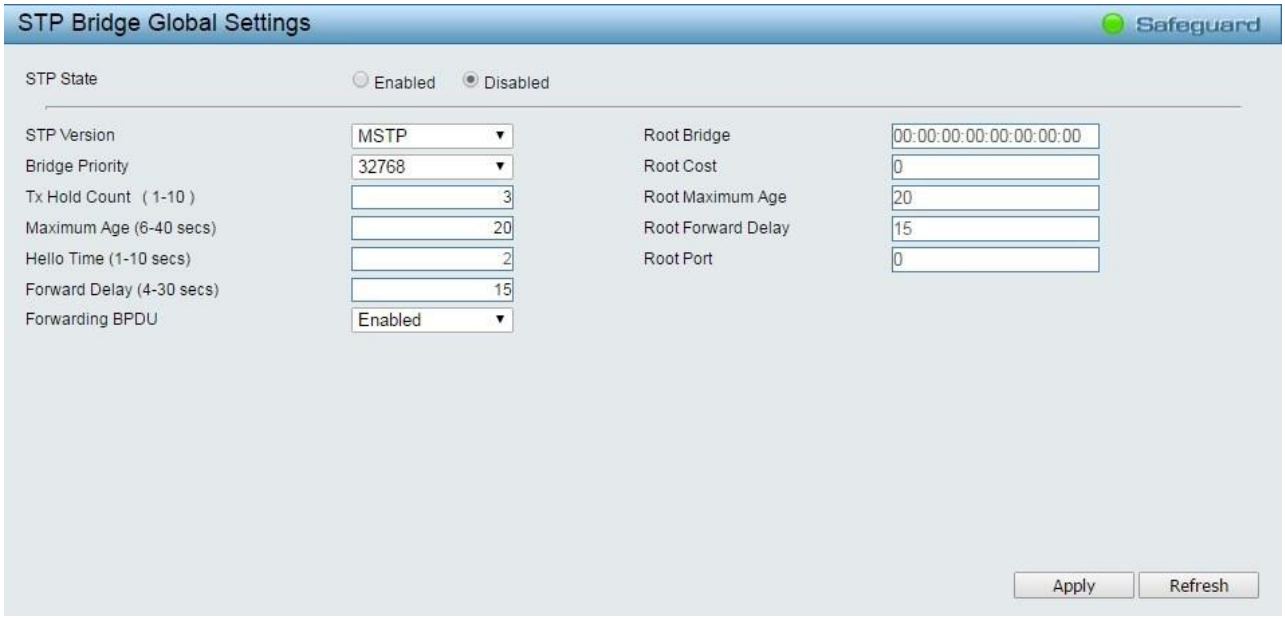


그림 4.65 - L2 기능 > 스패닝 트리 > STP 브리지 전역 설정

STP State: 스패닝 트리 프로토콜을 활성화 또는 비활성화합니다.

STP 버전: MSTP, RSTP 또는 STP 호환 모드 중에서 선택할 수 있습니다. 기본 설정은 MSTP입니다.

Bridge Priority: 0에서 61410 사이의 값으로 패킷 전송 우선 순위를 지정합니다. 값이 낮을수록 우선 순위가 높아집니다. 기본값은 32768입니다.

TX Hold Count (1-10): 간격당 전송되는 Hello 패킷의 최대 수를 설정하는 데 사용됩니다. 카운트는 1에서 10까지 지정할 수 있습니다. 기본값은 6입니다.

Maximum Age (6-40초): 이 값은 오래된 정보가 네트워크의 중복 경로를 통해 끝없이 순환하지 않도록 보장하는 데 사용됩니다. 이 값은 루트 브리지에 의해 설정되며, 스위치가 브리징된 LAN의 다른 장치와 일관된 스패닝 트리 구성 값을 결정하는 데 도움이 됩니다. 값이 만료되면 루트 브리지에서 BPDU가 수신되지 않으면 스위치는 다른 모든 스위치에 루트 브리지가 되기 위한 허가를 요청하는 자신의 BPDU를 보내기 시작합니다. 스위치가 가장 낮은 브리지 식별자를 가진 경우

루트 브리지가 됩니다. 시간 간격은 6초에서 40초 사이로 선택할 수 있습니다. 수 있습니다. 기본값은 20입니다. (최대 연령은 Hello 시간보다 커야 합니다.)

Hello Time (1-10 sec): 루트 장치에서 전송되는 구성 메시지 간의 시간 간격을 설정하여 스위치가 여전히 작동하고 있음을 알립니다. 기본값은 2초입니다.

Forward Delay (4-30초): 루트 장치가 상태를 변경하기 전에 기다릴 최대 시간을 설정합니다. 기본값은 15초입니다.

Root Bridge: 루트 브리지의 MAC 주소를 표시합니다.

Root Cost: 루트 브리지의 Cost를 표시합니다.

Root Maximum Age: 루트 브리지의 Maximum Age를 표시합니다.

Root Forward Delay: 루트 브리지의 Forward Delay를 표시합니다.

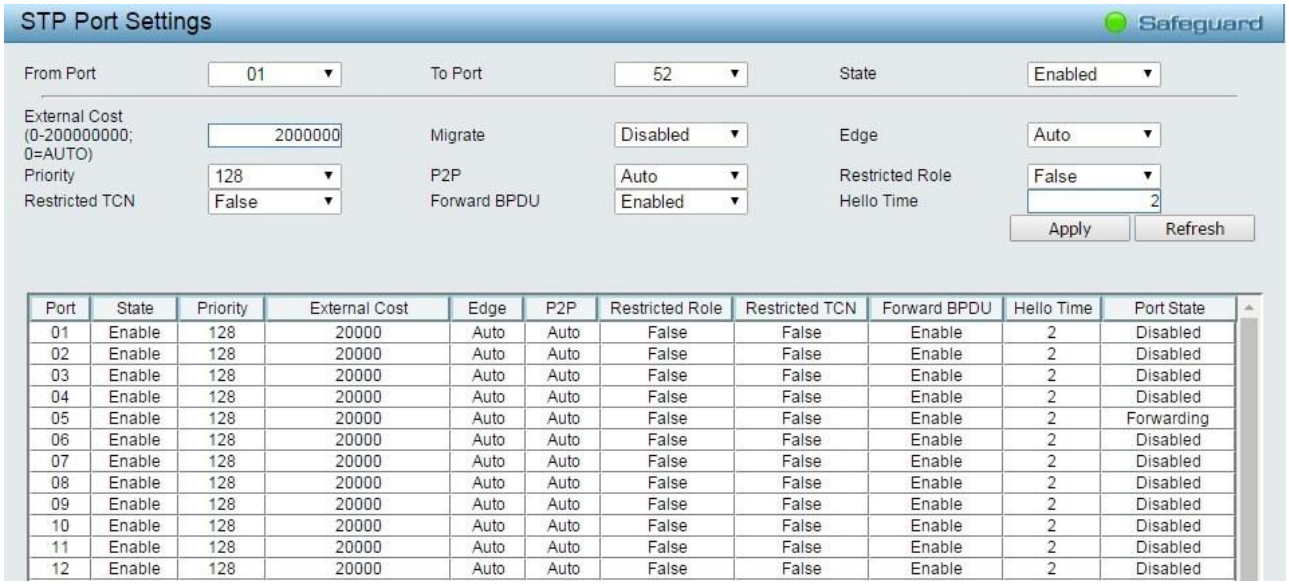
Root Port: 루트 포트를 표시합니다.

변경 사항을 적용하려면 **Apply** 버튼을 클릭하십시오.
페이지를 새로 고치려면 **Refresh를** 클릭하십시오.

L2 기능 > 스패닝 트리 > STP 포트 설정

STP는 포트별로 설정할 수 있습니다. 스위치 수준에서 스패닝 트리 매개변수를 설정하는 것 외에도 스위치는 포트 그룹의 구성을 허용하며, 각 포트 그룹은 자체 스패닝 트리를 가지고 있으며, 자체 구성 설정이 필요합니다. STP 그룹 스패닝 트리는 스위치 수준 스패닝 트리와 같은 방식으로 작동하지만 루트 브리지 개념은 루트 포트 개념으로 대체됩니다. 루트 포트는 포트 우선 순위와 포트 비용을 기준으로 네트워크에 연결되는 그룹의 포트입니다. 중복 링크는 스위치 수준에서 중복 링크가 차단되는 것처럼 차단됩니다. 스위치 수준의 STP는 스위치 간(및 유사한 네트워크 장치 간) 중복 링크를 차단합니다. 포트 수준 STP는 STP 그룹 내에서 중복 링크를 차단합니다.

VLAN 포트 그룹에 해당하는 STP 그룹을 정의하는 것이 좋습니다.



Port	State	Priority	External Cost	Edge	P2P	Restricted Role	Restricted TCN	Forward BPDU	Hello Time	Port State
01	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
02	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
03	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
04	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
05	Enable	128	20000	Auto	Auto	False	False	Enable	2	Forwarding
06	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
07	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
08	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
09	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
10	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
11	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
12	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled

그림 4.66 - 스패닝 트리 > STP 포트 설정을 > L2 기능

From Port/To Port: 선택한 포트부터 시작하여 연속적인 포트 그룹을 구성할 수 있습니다.

State: 드롭다운 메뉴를 사용하여 포트별로 STP를 활성화하거나 비활성화합니다. 글로벌 STP가 활성화된 후 선택할 수 있습니다.

External Cost: 지정된 포트 목록으로 패킷을 전달하는 상대적 비용을 나타내는 메트릭을 정의합니다. 포트 비용은 자동으로 설정하거나 메트릭 값으로 설정할 수 있습니다. 기본값은 0(Auto)입니다.

0 (auto) - 외부 비용을 0으로 설정하면 지정된 포트로 패킷을 전달하는 가장 빠른 경로를 자동으로 설정하여 최적의 효율성을 보장합니다. 기본 포트 비용: 100Mbps 포트 = 200000, 기가비트 포트 = 20000.

Value 1-200000000 - 1에서 200000000 사이의 값을 선택하여 외부 비용을 설정합니다. 숫자가 낮을수록 포트가 패킷을 전달하는 데 선택될 가능성이 높아집니다.

Migrate: 이 매개변수를 예로 설정하면 포트가 다른 브리지에 BPDU 패킷을 전송하여 STP 설정에 대한 정보를 요청합니다. 스위치가 RSTP로 구성된 경우 포트는 802.1d STP에서 802.1w RSTP로 마이그레이션할 수 있습니다. 마이그레이션은 네트워크 스테이션이나 802.1w RSTP로 업그레이드할 수 있는 세그먼트에 연결된 포트에서 예로 설정해야 합니다.

Edge: True 매개변수를 선택하면 포트를 엣지 포트로 지정합니다. 엣지 포트는 루프를 생성할 수 없지만, 토폴로지 변경으로 인해 루프 가능성이 생기면 엣지 포트 상태를 잃을 수 있습니다. 엣지 포트는 일반적으로 BPDU 패킷을 수신하지 않아야 합니다. BPDU 패킷이 수신되면 자동으로 엣지 포트 상태를 잃습니다. False 매개변수를 선택하면 포트가 엣지 포트 상태가 없음을 나타냅니다. Auto 매개변수를 선택하면 포트가 엣지 포트 상태가 있거나 없음을 자동으로 결정합니다.

Priority: 각 포트의 우선 순위를 지정합니다. 선택 가능한 범위는 0에서 240이며, 기본 설정은 128입니다. 숫자가 낮을수록 루트 포트로 선택될 가능성이 높아집니다.

P2P: True 매개변수를 선택하면 포인트 투 포인트(P2P) 공유 링크를 나타냅니다. P2P 포트는 엣지 포트와 유사하지만, P2P 포트는 전이중으로 작동해야 합니다.

엣지 포트처럼 P2P 포트는 RSTP로부터 이점을 누리기 위해 전달 상태로 빠르게 전환합니다. P2P 값이 false이면 포트는 P2P 상태를 가질 수 없음을 나타냅니다. Auto는 포트가 가능한 경우 P2P 상태를 가지도록 하고 P2P 상태가 true인 것처럼 작동합니다. 포트가 이 상태를 유지할 수 없는 경우(예: 포트가 반이중 작동으로 강제 전환된 경우) P2P 상태는 false처럼 작동하도록 변경됩니다. 이 매개변수의 기본 설정은 Auto입니다.

Restricted Role: 패킷의 제한 역할 상태를 True와 False 사이에서 전환합니다. True로 설정하면 포트가 루트 포트로 선택되지 않습니다. 기본값은 False입니다.

Restricted TCN: 패킷의 제한 TCN을 True와 False 사이에서 전환합니다. 토폴로지 변경 알림(TCN)은 브리지가 루트 포트로 보내어 토폴로지 변경을 알리는 BPDU입니다. True로 설정하면 포트가 수신한 TCN을 다른 포트로 전파하지 못하게 합니다. 기본값은 False입니다.

Forwarding BPDU: 브리지는 스패닝 트리 정보를 제공하기 위해 브리지 프로토콜 데이터 단위(BPDU)를 사용합니다. STP BPDU 필터링은 브리지가 두 지역을 상호 연결할 때 유용합니다. 각 지역은 별도의 스패닝 트리가 필요합니다. BPDU 필터링은 STP가 전역적으로 비활성화되거나 단일 인터페이스에서 비활성화될 때만 작동합니다. 가능한 필드 값은 다음과 같습니다:

Disabled – 포트에서 BPDU 필터링이 활성화됩니다.

Enabled – 포트에서 BPDU 전달이 활성화됩니다(스위치가 STP가 비활성화된 경우).

Hello Time: 루트 브리지가 다른 모든 스위치에 루트 브리지임을 나타내기 위해 전송하는 BPDU 패킷 간의 간격입니다. 기본값은 2입니다.

변경 사항을 적용하려면 **Apply** 버튼을 클릭하십시오. 페이지를 새로 고치려면 **Refresh를** 클릭하십시오.

L2 기능 > 스패닝 트리 > MST 구성 식별

MST 구성 식별 페이지를 통해 사용자는 스위치에서 MSTI 인스턴스를 구성할 수 있습니다. 이 설정은 스위치에 설정된 다중 스패닝 트리 인스턴스를 고유하게 식별합니다. 스위치는 기본적으로 하나의 CIST(공통 내부 스패닝 트리)를 소유하며, 사용자는 이 매개변수를 수정할 수 있지만 MSTI ID는 변경할 수 없으며 삭제할 수 없습니다.

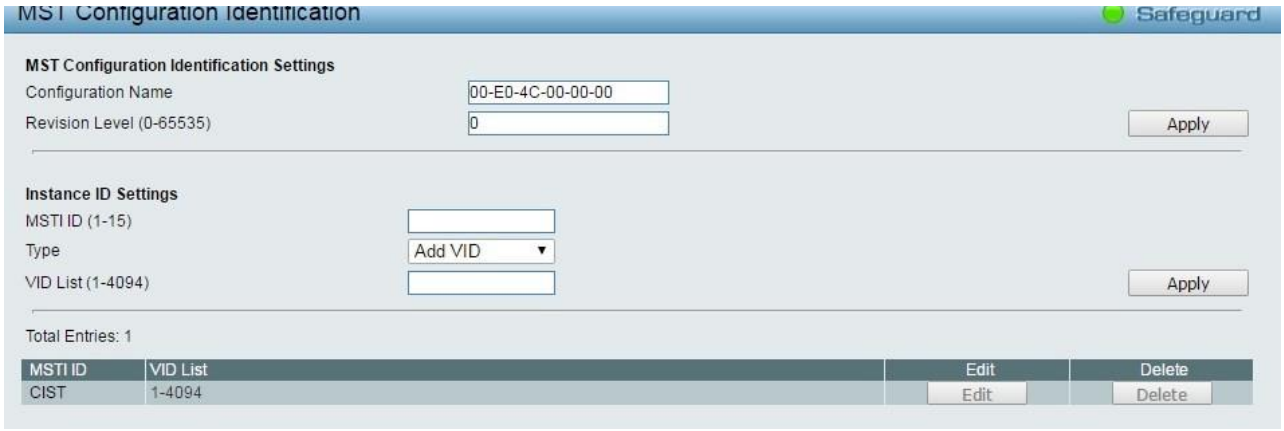


그림 4.67 - L2 기능 > 스패닝 트리 > MST 구성 식별

MST 구성 식별 설정:

Configuration Name: 스위치에서 MSTI(다중 스패닝 트리 인스턴스)를 고유하게 식별하기 위해 설정된 이름입니다. 구성 이름이 설정되지 않은 경우 이 필드는 MSTP를 실행하는 장치의 MAC 주소를 표시합니다. 이 필드는 **STP Bridge Global Set-tings** 창에서 설정할 수 있습니다.

Revision Level: 이 값은 구성 이름과 함께 스위치에 구성된 MSTP 지역을 식별합니다. 사용자는 0에서 65535 사이의 값을 선택할 수 있으며 기본 설정은 0입니다.

MSTI ID (1-15): 1에서 15 사이의 숫자를 입력하여 스위치에 새 MSTI를 설정합니다.

Type: 이 필드를 통해 사용자는 MSTI 설정을 변경할 방법을 선택할 수 있습니다.

Add VID - 이 매개변수를 선택하여 VID 목록 매개변수와 함께 MSTI ID에 VIDs를 추가합니다.

Remote VID – 이 매개변수를 선택하여 MSTI ID에서 VIDs를 제거합니다.

VID List (1-4094): 이 필드는 특정 MSTI와 연결된 VLAN ID를 표시합니다. 변경 사항을 적용하려면 **Apply**을 클릭하십시오.

L2 기능 > 스패닝 트리 > STP 인스턴스 설정

STP 인스턴스 설정 페이지는 스위치에서 현재 설정된 MSTI를 표시하고 사용자가 MSTP의 우선 순위를 변경할 수 있도록 합니다.

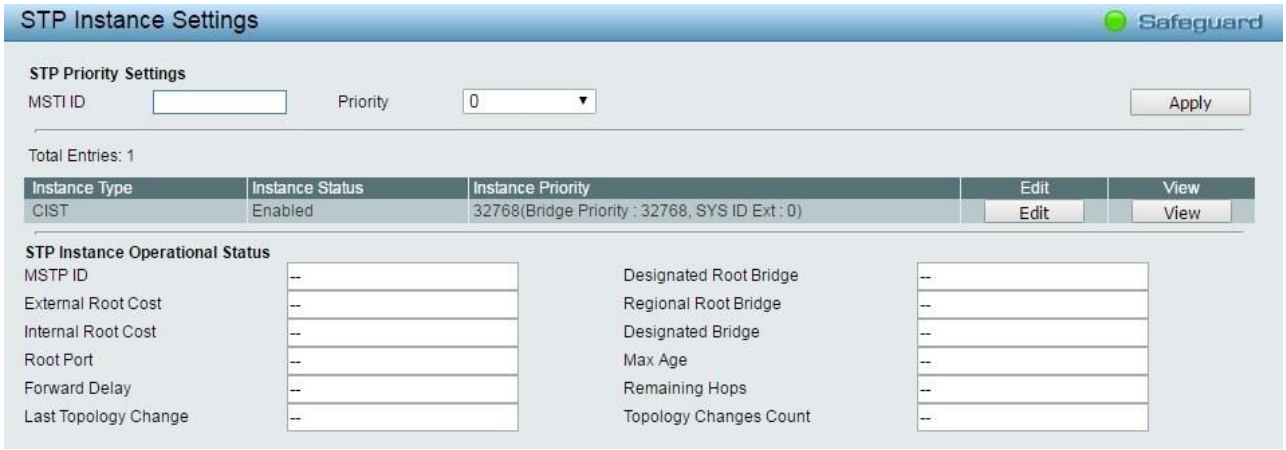


그림 4.68 - L2 기능 > 스패닝 트리 > STP 인스턴스 설정

특정 항목을 수정하려면 **Edit** 버튼을 클릭하십시오. 테이블의 항목에 대한 더 많은 정보를 보려면 창 상단의 **view** 버튼을 클릭하십시오.

위 창에는 다음 정보가 포함됩니다:

MSTI ID: 이 필드에 MSTI ID를 입력합니다. 0의 항목은 CIST(기본 MSTI)를 나타냅니다.

우선 순위: 우선 순위 필드에 새 우선 순위를 입력합니다. 사용자는 0에서 61440 사이의 우선 순위 값을 설정할 수 있습니다. 변경 사항을 적용하려면 **Apply** 버튼을 클릭하십시오.

L2 기능 > 스패닝 트리 > MSTP 포트 정보

MSTP 포트 정보 페이지는 MSTI ID의 포트 구성을 업데이트하는 데 사용될 수 있습니다. 루프가 발생하면 MSTP 기능은 포트 우선 순위를 사용하여 전달 상태로 전환할 인터페이스를 선택합니다. 인터페이스가 먼저 선택되도록 하려면 더 높은 우선 순위 값을 설정하십시오. 우선 순위 값이 동일한 경우 MSTP 기능은 가장 낮은 MAC 주소를 가진 포트를 전달 상태로 설정하고 다른 인터페이스는 차단됩니다.

특정 포트에 대한 MSTI 설정을 보려면 포트 번호를 선택하고 **Find** 버튼을 클릭하십시오. 특정 MSTI 인스턴스의 설정을 수정하려면 **Edit** 버튼을 클릭한 다음 MSTP 포트 설정을 수정하고 **Apply**를 클릭하십시오.

그림 4.69 - L2 기능 > 스패닝 트리 > MST 포트 정보

Instance ID: 구성 중인 인스턴스의 MSTI ID를 표시합니다. 이 필드에 0이 입력되면 CIST(기본 MSTI)를 나타냅니다.

Internal Path Cost (0=Auto): 이 매개 변수는 STP 인스턴스 내에서 인터페이스를 선택할 때 지정된 포트로 패킷을 전달하는 상대적 비용을 나타내도록 설정됩니다. 기본 설정은 0(자동)입니다.

0 (Auto) - 내부 비용에 대해 이 매개 변수를 선택하면 인터페이스에 가장 빠른 경로가 자동으로 최적으로 설정됩니다. 기본값은 인터페이스의 미디어 속도에서 파생됩니다.

값: 0-200000000 – 0-20000000 범위의 값으로 이 매개 변수를 선택하면 루프가 발생하는 경로가 가장 빠르게 설정됩니다. 내부 비용이 낮을수록 전송 속도가 빨라집니다.

Priority: 포트 인터페이스의 우선순위를 설정하기 위해 0부터 240 사이의 값을 입력하십시오. 높은 우선순위는 패킷을 먼저 전달할 인터페이스로 지정합니다. 낮은 숫자는 더 높은 우선순위를 나타냅니다.

L2 기능 > 링크 어그리게이션 > 포트 트렁킹

물리적 인터페이스는 포트 트렁킹 기능을 통해 논리적으로 결합할 수 있으며, 이는 효율적인 비용으로 대역폭을 증가시키는 데 도움이 됩니다. 최대 8개의 트렁크 그룹이 생성될 수 있으며, 각 그룹은 최대 8개의 포트로 구성됩니다. 함께 그룹화할 포트를 선택한 다음 **Apply**을 클릭하여 선택한 트렁킹 그룹을 활성화합니다. 지원되는 링크 집합 메커니즘에는 두 가지 유형이 있습니다::

Static - 정적 링크 집계입니다.

LACP - LACP를 사용하면 포트 트렁킹 그룹의 링크를 자동으로 감지할 수 있습니다.

Disable - 이 트렁크 그룹의 모든 구성원을 제거합니다.

그림 4.70 - L2 기능 > 링크 어그리게이션 > 포트 트렁킹

참고: 결합된 각 트렁크 포트는 동일한 VLAN 그룹 내의 장치에 연결되어야 합니다.

L2 기능 > 링크 어그리게이션 > LACP 포트 설정

LACP 포트 설정은 스위치에서 포트 트렁킹 그룹을 생성하는 데 사용됩니다. 사용자는 LACP 제어 프레임을 처리하고 전송하는 활성 및 수동 포트를 설정할 수 있습니다.

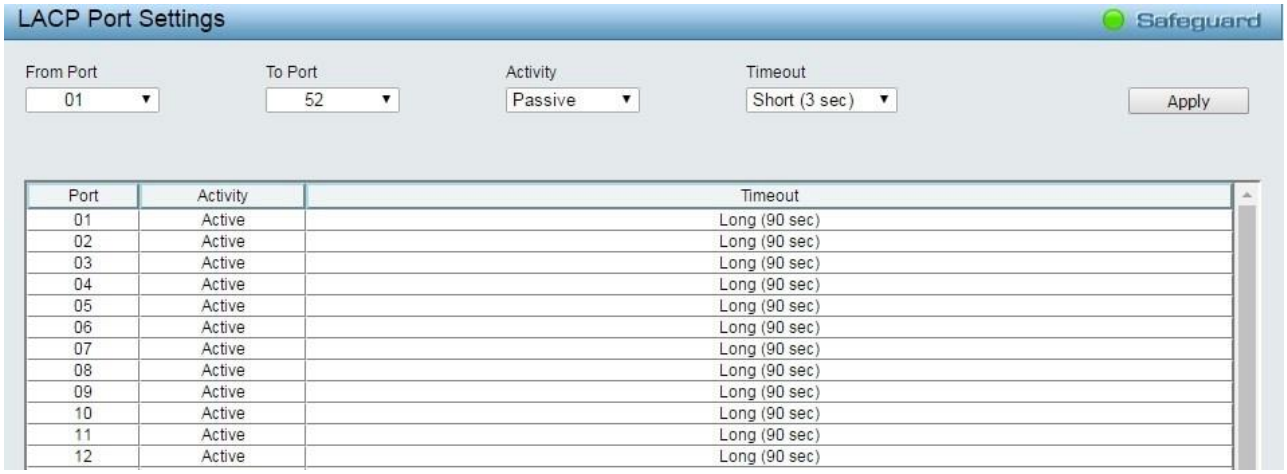


그림 4.71 - L2 기능 > 링크 어그리게이션 > LACP 포트 설정

From Port: 선택한 포트부터 시작하여 연속적인 포트 그룹을 구성할 수 있습니다.

To Port: 선택한 포트부터 시작하여 연속적인 포트 그룹의 종료입니다.

활동: LACP 포트의 두 가지 역할:

활성 - 활성 LACP 포트는 LACP 제어 프레임을 처리하고 전송할 수 있습니다. 이를 통해 LACP 호환 장치가 집계 링크를 협상할 수 있으므로 필요에 따라 그룹이 동적으로 변경될 수 있습니다. 집계 포트 그룹을 변경하는 기능을 활용하려면 참여 장치 중 하나는 LACP 포트를 Active로 설정해야 합니다. 두 장치 모두 LACP를 지원해야 합니다.

Passive - 수동으로 설정된 LACP 포트는 처음에 LACP 제어 프레임을 전송할 수 없습니다. 연결된 포트 그룹이 협상 조정을 허용하려면 연결의 한 쪽이 "Acitve" LACP 포트를 가져야 합니다.

Timeout: 관리 LACP 시간 초과를 지정합니다. 가능한 필드 값은 다음과 같습니다:

Short (3 Sec) - LACP 시간 초과를 3초로 정의합니다.

Long (90 Sec) - LACP 시간 초과를 90초로 정의합니다. 기본값입니다.

변경 사항을 적용하려면 **Apply** 버튼을 클릭하십시오.

L2 기능 > 멀티캐스트 > 자동 IGMP

Auto IGMP 는 특정 VLAN 그룹에 대한 IGMP 스누핑 관련 매개변수를 위한 두 단계 구성 기능을 제공합니다. 매개변수에는 IGMP 스누핑 상태, IGMP 스누핑 쿼리 상태, 빠른 퇴장 상태 및 IGMP 스누핑 필터 모드가 포함됩니다.

자동 IGMP의 설정은 다음과 같습니다.

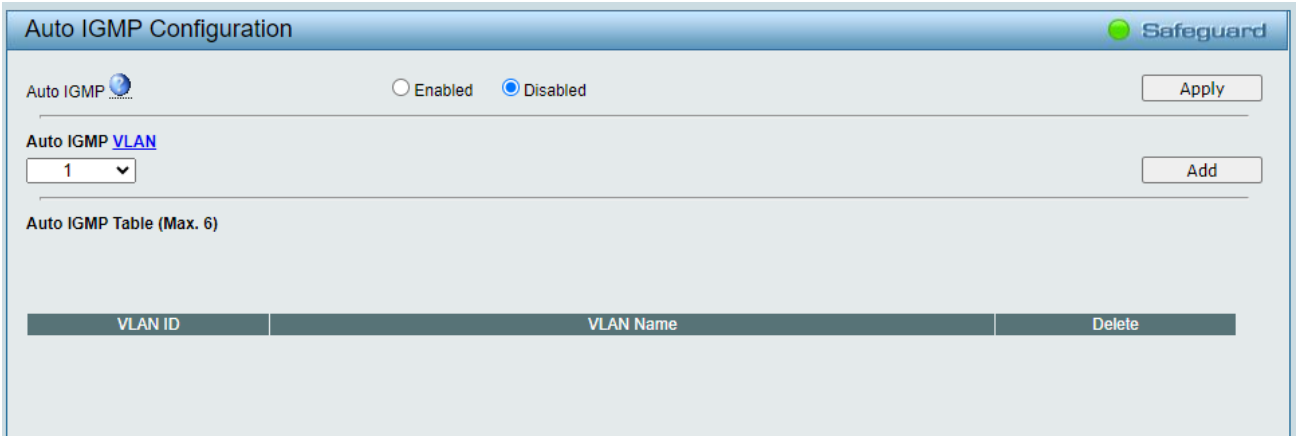


그림 4.72 - 멀티캐스트 > 자동 IGMP> L2 기능

기본적으로 **Auto IGMP**는 **Disabled** 되어 있습니다.
Enabled하면 **IGMP** 스누핑 글로벌 상태가 활성화로 변경됩니다.

Auto IGMP VLAN은 Auto IGMP 그룹 테이블에 추가될 특정 VLAN 그룹을 참조합니다.
VLAN 그룹을 Auto IGMP에 추가하면 다음 매개변수가 변경됩니다:

- IGMP 스누핑 활성화(IGMP 스누핑은 비활성화 모드인 경우 활성화 모드로 변경됨)
- IGMP Snooping Querier 활성화
- IGMP Snooping Fast Leave 활성화
- 모든 인터페이스에 대한 Multicast Filter 모드를 필터링으로 변경

IGMP 테이블에서 특정 VLAN 그룹을 **Delete**하면 다음과 같은 작업이 수행됩니다:

- IGMP Snooping Querier가 기본 설정으로 복원
- IGMP Snooping Fast Leave 가 기본 설정으로 복원

참고: 개별 VLAN과 연결된 "Delete" 버튼은 해당 VLAN에서 자동 IGMP 기능을 제거하는 작업을 나타냅니다. 이렇게 하면 해당 VLAN에 대한 모든 IGMP 스누핑 기능이 기본 설정으로 복원됩니다. VLAN 자체는 삭제되지 않습니다.

L2 기능 > 멀티캐스트 > IGMP 스누핑

인터넷 그룹 관리 프로토콜(IGMP) 스누핑을 사용하면 스마트 관리 스위치는 각 프레임의 레이어 2 MAC 헤더의 내용을 검사하여 지능적인 멀티캐스트 전달 결정을 내릴 수 있습니다. IGMP 스누핑은 LAN에서 혼잡한 트래픽을 줄이는 데 도움이 될 수 있습니다. IGMP 스누핑이 전역적으로 활성화되면 스마트 관리 스위치는 그룹 구성원이 연결된 포트로만 멀티캐스트 트래픽을 전달합니다..

기본 IGMP 스누핑 버전은 v3이며, 이는 IGMP v1 및 v2와 호환됩니다. DGS-1210 시리즈는 IGMP v1/v2/v3 인식 기능을 지원합니다. IGMP v3 인식은 IGMP v3 스누핑을 지원함을 의미하며, 즉 스위치는 IGMP 제어 패킷을 읽고 이해할 수 있습니다. 스위치는 여전히 보고서/퇴장 패킷을 기반으로 올바른 동작을 수행할 수 있습니다. 그러나 RFC 관점에서 보면, 완전한 IGMP v3는 소스 필터링을 지원해야 하며 이는 L2 스위치에서 지원하는 것이 불가능합니다.

IGMP 스누핑의 설정은 각 VLAN별로 설정됩니다.

그림 4.73 - 멀티캐스트 > IGMP 스누핑> L2 기능

기본적으로 IGMP는 비활성화되어 있습니다. 활성화되면 IGMP 글로벌 설정을 입력해야 합니다.

Host Timeout (130-153025 sec): 학습된 호스트 포트 항목이 제거되는 간격입니다. 학습된 각 호스트 포트에 대해 '포트 제거 타이머'가 '호스트 포트 제거 간격' 동안 실행됩니다. 이 타이머는 해당 포트에서 호스트로부터 보고서 메시지를 수신할 때마다 재시작됩니다. '호스트 포트 제거 간격' 시간 동안 보고서 메시지가 수신되지 않으면 학습된 호스트 항목이 멀티캐스트 그룹에서 제거됩니다. 기본값은 260초입니다.

견고성 변수(2-255초): 내구성 변수는 서브넷에서 예상되는 패킷 손실을 조정할 수 있게 해줍니다. 서브넷에서 손실이 예상되는 경우 내구성 변수를 증가시켜야 할 수 있습니다. 내구성 변수는 0으로 설정할 수 없으며, 0으로 설정해서는 안 됩니다. 기본값은 2입니다.

Query Interval (60-600 sec): 일반 쿼리가 전송되는 간격입니다. 쿼리 간격을 조정하면 IGMP 메시지 수를 늘리거나 줄일 수 있습니다. 값이 클수록 IGMP 쿼리가 덜 자주 전송됩니다. 기본값은 125초입니다.

라우터 시간 초과(60-600초): 학습된 라우터 포트 항목이 제거되는 간격입니다. 학습된 각 라우터 포트에 대해 '라우터 포트 제거 타이머'가 '라우터 포트 제거 간격' 동안 실행됩니다. 이 타이머는 해당 포트에서 쿼리 제어 메시지를 수신할 때마다 재시작됩니다. '라우터 포트 제거 간격' 시간 동안 쿼리 제어 메시지가 수신되지 않으면 학습된 라우터 포트 항목이 제거됩니다. 기본값은 260초입니다.

Last Member Query Interval (1-25 sec): 마지막 구성원 쿼리 간격은 그룹 특정 쿼리에 삽입된 최대 응답 시간입니다. 이 값은 마지막 구성원의 손실을 감지하는 시간을 줄입니다. 기본값은 1초입니다.

최대 응답 시간(10-25초): 최대 응답 시간은 응답 보고서 메시지를 보내기 전에 허용되는 최대 시간입니다. 이 설정을 조정하면 IGMP 트래픽의 빈도를 조절할 수 있습니다. 기본값은 10초입니다.

특정 VLAN에 대해 IGMP 스누핑을 활성화하려면 활성화를 선택하고 **Apply** 버튼을 클릭하십시오. 그런 다음 **VLAN ID** 번호를 눌러 IGMP 스누핑을 위한 라우터 포트로 할당할 포트를 선택하고 변경 사항을 적용하려면 **Apply**를 누르십시오. 수동으로 구성된 라우터 포트는 **Static Router Port**이며, 쿼리 제어 메시지가 수신될 때 스위치에 의해 동적으로 구성된 **Dynamic Router Port**입니다.

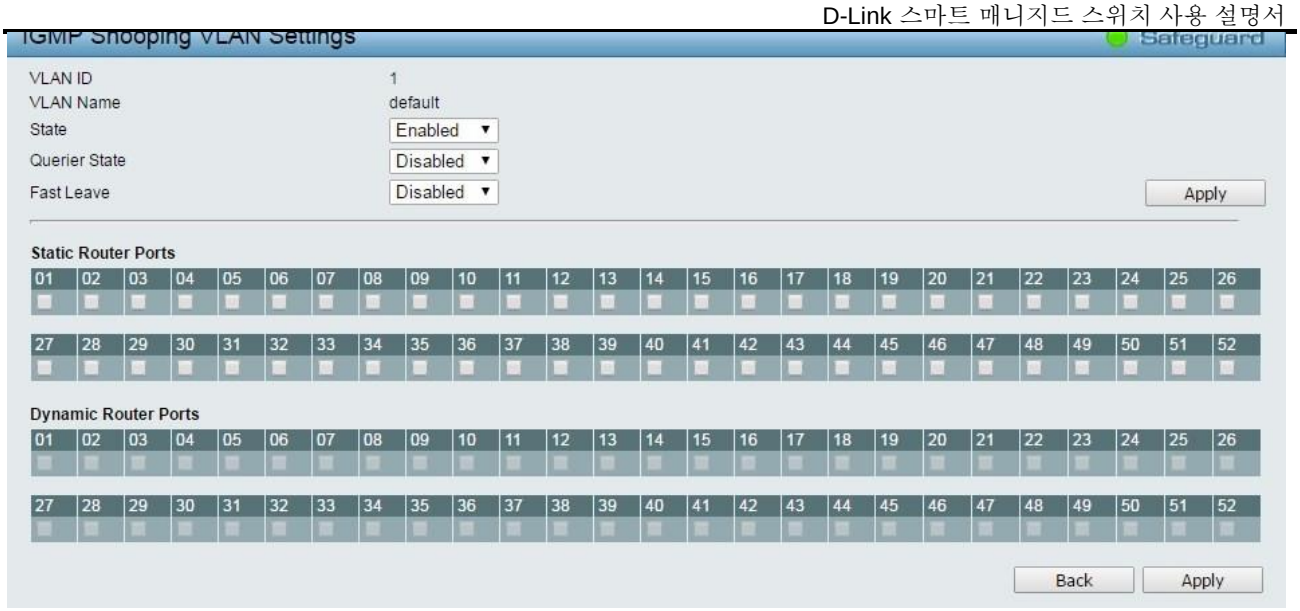


그림 4.74 - L2 기능 > 멀티캐스트 > IGMP 스누핑 VLAN 설정

상태: IGMP 스누핑 VLAN을 활성화 또는 비활성화합니다.

쿼리 발생기 상태: D-Link 스마트 스위치는 IGMP 쿼리를 전송하여 멀티캐스트 클라이언트의 상태를 확인할 수 있습니다. 기본값은 비활성화되어 있습니다.

Fast Leave: 기능을 활성화 또는 비활성화합니다.

지정된 VLAN에 대한 멀티캐스트 항목 테이블을 보려면 **View** 버튼을 누르십시오.

그림 4.75 - L2 기능 > 멀티 캐스트 > IGMP 멀티 캐스트 항목 테이블

특정 항목을 삭제하려면 **Delete** 를 클릭하고 모든 항목을 삭제하려면 **Delete All** 클릭합니다.

L2 기능 > 멀티캐스트 > MLD 스누핑

멀티캐스트 리스너 발견(MLD) 스누핑은 IGMP 스누핑과 유사하게 IPv6에서 사용되는 기능입니다. 이는 VLAN에서 멀티캐스트 데이터를 요청하는 포트를 발견하는 데 사용됩니다. 선택된 VLAN의 모든 포트에 멀티캐스트 트래픽을 플러딩하는 대신 MLD 스누핑은 요청하는 포트에서 생성된 쿼리 및 보고서를 통해 이 데이터를 수신하고자 하는 포트로만 멀티캐스트 데이터를 전달합니다.

MLD 스누핑은 엔드 노드와 MLD 라우터 간에 전송되는 MLD 제어 패킷의 레이어 3 부분을 검사하여 수행됩니다. 스위치가 이 경로에서 멀티캐스트 트래픽을 요청하는 것을 발견하면, 스위치는 해당 포트를 올바른 IPv6 멀티캐스트 테이블에 추가하고 멀티캐스트 트래픽을 해당 포트로 전달하기 시작합니다. 멀티캐스트 라우팅 테이블의 이 항목은 포트, VLAN ID 및 연결된 멀티캐스트 IPv6 멀티캐스트 그룹 주소를 기록하며, 이 포트를 활성 리스닝 포트로 간주합니다. 활성 리스닝 포트만이 멀티캐스트 그룹 데이터를 수신합니다.

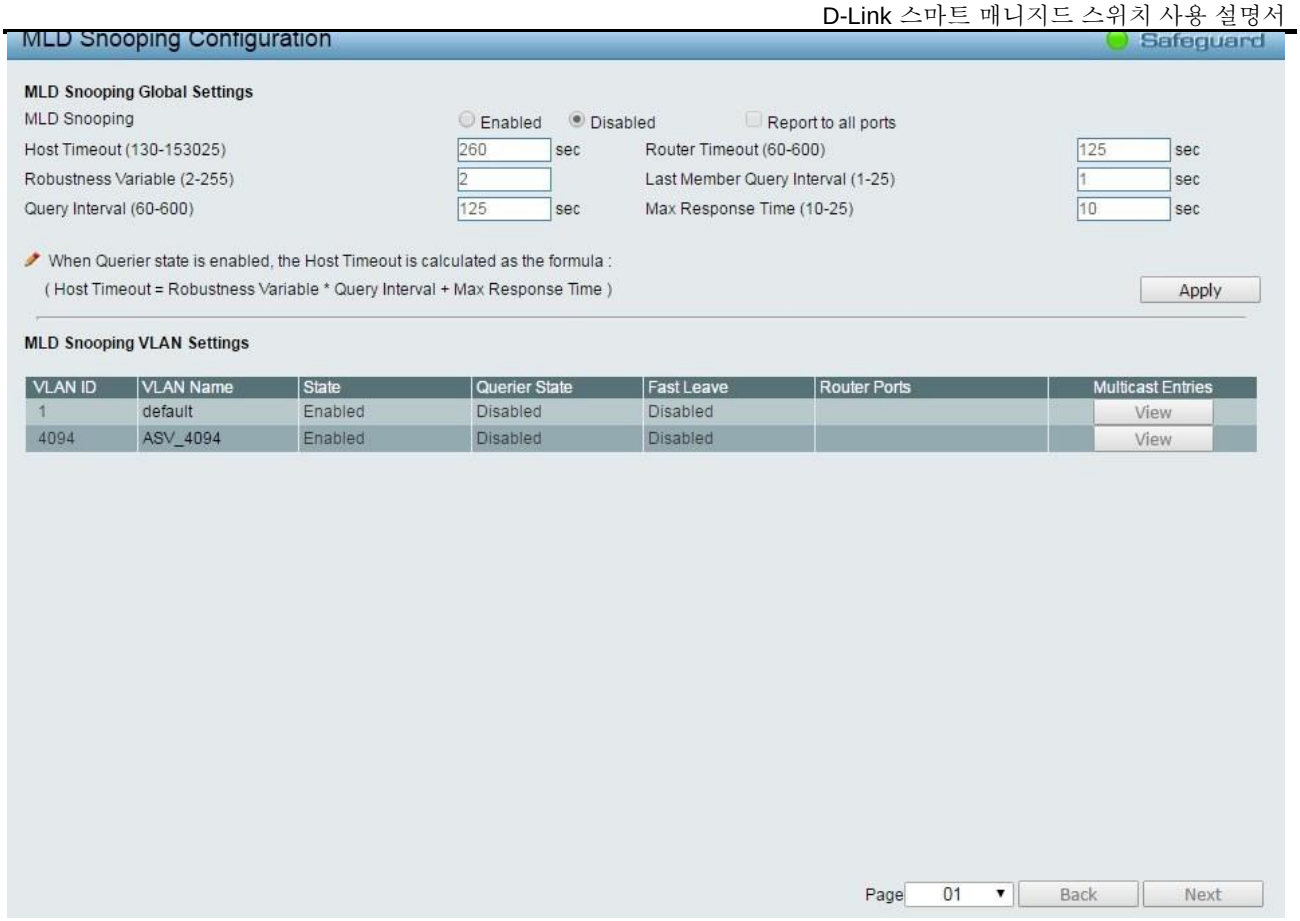


그림 4.76 - 멀티캐스트 > MLD 스누핑> L2 기능

MLD 전역 설정:

MLD Snooping: MLD 스누핑을 활성화 또는 비활성화합니다.

Host Timeout (130-153025 sec): 멀티캐스트 그룹에서 포트를 제거하는 초 단위 시간 간격입니다. 멀티캐스트 그룹 MLD 보고서가 멀티캐스트 포트에서 정의된 호스트 시간 초과 기간 내에 수신되지 않으면 포트가 제거됩니다. 가능한 필드 범위는 130 - 153025초입니다. 기본 시간 초과는 260초입니다.

Router Timeout (60-600): 메시지를 수신하기 위해 멀티캐스트 라우터가 대기하는 시간 간격입니다. 가능한 필드 범위는 60 - 600초입니다. 기본 시간 초과는 125초입니다.

견고성 변수(2-255): 내구성 변수는 서브넷에서 예상되는 패킷 손실을 조정할 수 있게 해줍니다. 서브넷에서 손실이 예상되는 경우 내구성 변수를 증가시켜야 할 수 있습니다. 내구성 변수는 0으로 설정할 수 없으며, 0으로 설정해서는 안 됩니다. 기본값은 2입니다.

Last Member Query Interval (1-25 sec): 마지막 구성원 쿼리 간격은 Leave Group 메시지에 대한 응답으로 전송된 그룹 특정 쿼리에 삽입된 최대 응답 시간입니다. 이 값은 네트워크의 "퇴장 지연"을 수정하는 데 조정할 수 있습니다. 기본값은 1초입니다.

Query Interval (60-600 sec): 일반 쿼리가 전송되는 간격입니다. 쿼리 간격을 조정하면 MLD 메시지 수를 늘리거나 줄일 수 있습니다. 기본값은 125초입니다.

Max Response Time (10-25초): 멀티캐스트 멤버십 그룹에서 포트를 제거하는 시간 간격을 지정합니다. 포트가 멀티캐스트 그룹을 떠나도록 요청할 때 Done 메시지를 전송하면 포트가 멀티캐스트 멤버십에서 제거됩니다. 필드 범위는 10-25초입니다. 기본 시간 초과는 10초입니다.

변경 사항을 적용하려면 **Apply** 버튼을 클릭하십시오.

MLD 스누핑 VLAN 설정 목록:

VLAN ID 번호를 클릭하여 설정을 수정합니다:

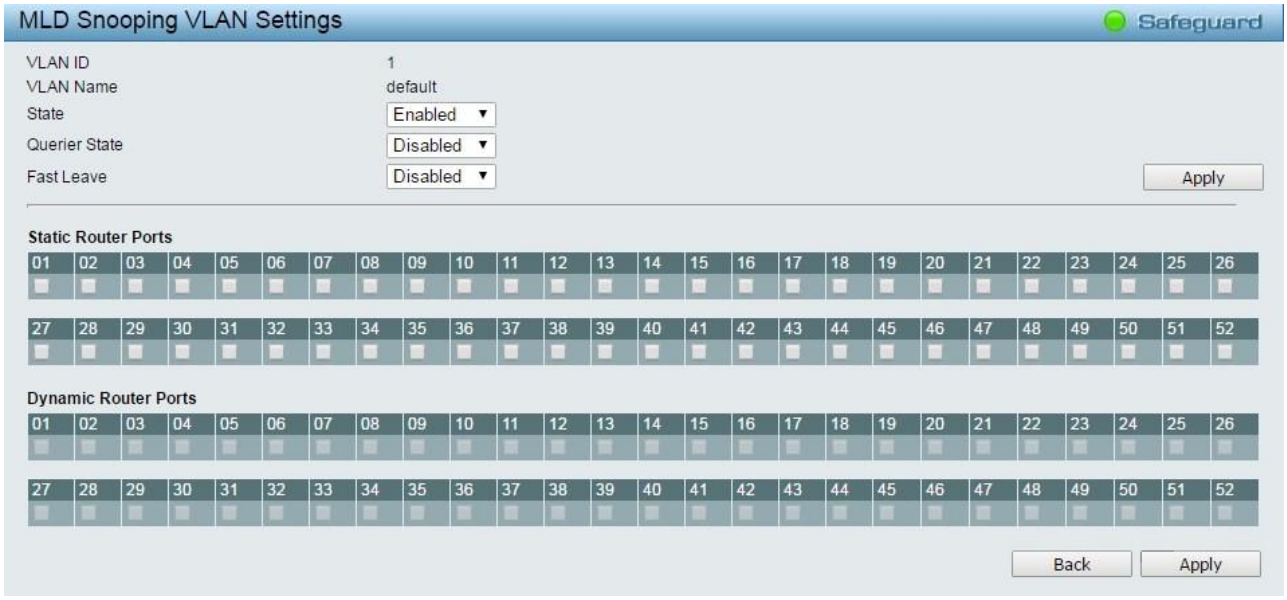


그림 4.76 - 멀티캐스트 > 멀티캐스트 포워딩> L2 기능

상태: MLD 스누핑 VLAN의 상태를 활성화 또는 비활성화합니다.

Querier State: 쿼리 상태를 활성화 또는 비활성화합니다.

Fast Leave: Fast leave 기능을 활성화 또는 비활성화합니다.

변경 사항을 적용하려면 **Apply** 버튼을 클릭하십시오.

Static Router Ports: 정적 라우터 포트로 할당할 포트를 선택합니다.

Dynamic Router Ports: 동적 라우터 포트로 할당할 포트를 선택합니다.

변경 사항을 적용하려면 **Apply** 버튼을 클릭하십시오.

L2 기능 > 멀티캐스트 > 멀티캐스트 포워딩

멀티캐스트 전달 기능은 사용자에게 특정 멀티캐스트 패킷을 지정된 포트 인터페이스로 정적 전달 규칙을 생성할 수 있게 해줍니다.

그림 4.77 - 멀티캐스트 > 멀티캐스트 포워딩> L2 기능

VID: VLAN에 해당하는 MAC 주소가 속한 VLAN의 VLAN ID입니다.

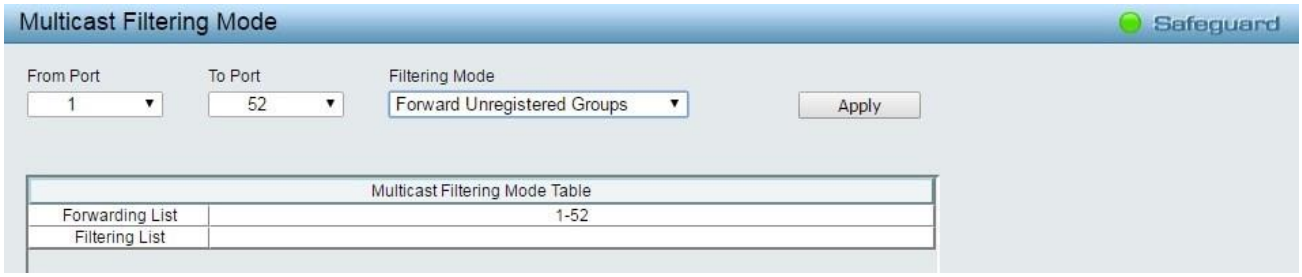
Multicast MAC Address: 정적 멀티캐스트 패킷의 출처가 되는 MAC 주소입니다. 이 주소는 멀티캐스트 MAC 주소여야 합니다.

Port Settings(포트 설정): 정적 멀티캐스트 그룹의 구성원이 될 포트와 동적으로 조인할 수 없거나 GMRP를 사용하여 동적으로 멀티캐스트 그룹에 조인할 수 있는 포트를 선택할 수 있습니다.

Member - 포트는 멀티캐스트 그룹의 정적 멤버입니다.

None - 멀티캐스트 그룹에 동적으로 조인하는 포트에 대한 제한이 없습니다. **None**을 선택하면 포트가 Static Multicast Group(고정 멀티캐스트 그룹)의 멤버가 되지 않습니다.

L2 기능 > 멀티캐스트 > 멀티캐스트 필터링 모드



Multicast Filtering Mode 기능은 포트 인터페이스를 기준으로 멀티캐스트 패킷을 특별히 필터링합니다.

그림 4.78 - 멀티캐스트 > 필터링 모드> L2 기능

VLAN ID: VLAN ID 를 지정합니다.

Filtering Mode:

Forward Unregistered Group: 멀티캐스트 스트림은 등록된 그룹의 등록 테이블을 기반으로 전달되지만 등록되지 않은 그룹의 VLAN의 모든 포트로 플러딩됩니다.

Filter Unregistered Groups: 등록된 그룹은 등록 테이블을 기반으로 전달되고 등록되지 않은 그룹은 필터링됩니다.

Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

L2 기능 > SNTP > 시간 설정

SNTP(Simple Network Time Protocol)는 스위치에서 컴퓨터의 시계를 동기화하는 데 사용됩니다. SNTP 설정 폴더에는 시간 설정과 시간대 설정이라는 두 개의 창이 있습니다. 사용자는 스위치에 대한 시간 설정을 구성할 수 있으며 다음 매개변수를 설정하거나 시간 설정 페이지에 표시할 수 있습니다.

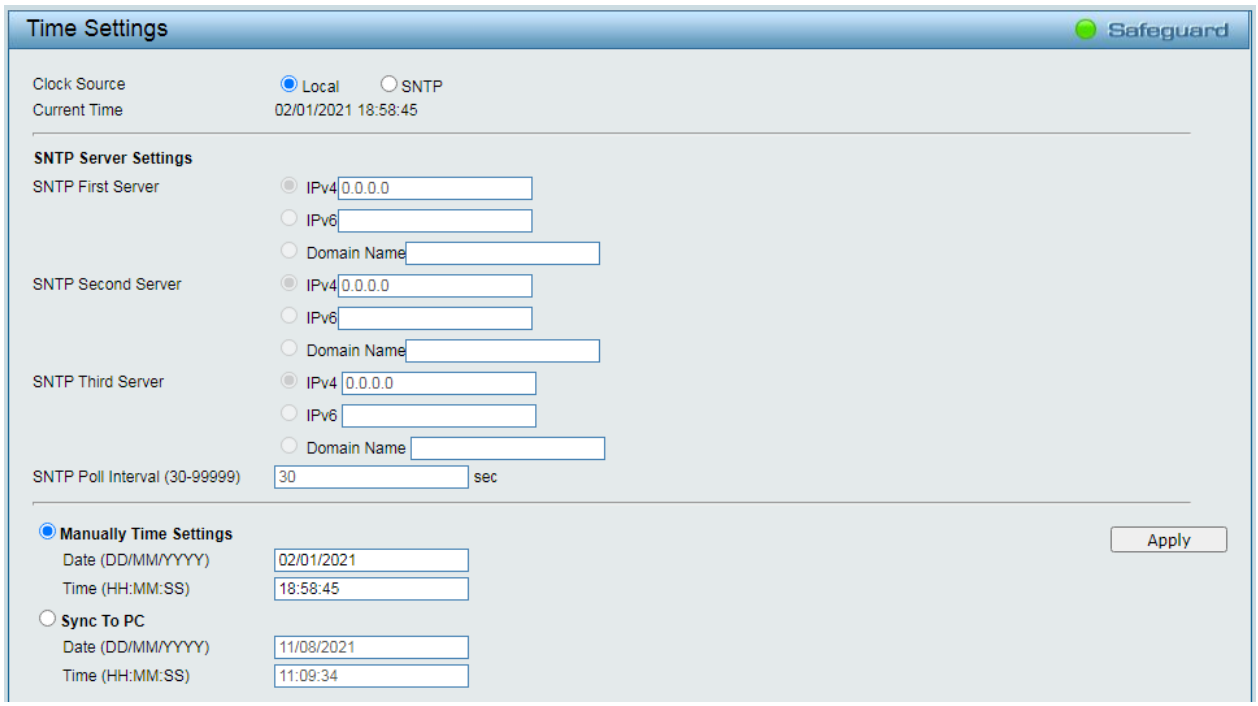


그림 4.79 - L2 기능 > SNTP > 시간 설정

Clock Source: 시스템 시간이 설정되는 클럭 소스를 지정합니다. 가능한 옵션은 다음과 같습니다.

Local(로컬) - 시스템 시간이 장치에 의해 로컬로 설정됨을 나타냅니다.

SNTP - 시스템 시간이 SNTP 서버에서 검색됨을 나타냅니다.

Current Time: 스위치의 현재 날짜와 시간을 표시합니다.

Clock Source에 대해 SNTP 를 선택하는 경우 다음 매개변수를 사용할 수 있습니다.

SNTP First Server: 선택 가능한 IPv4 주소, IPv6 주소 또는 도메인 이름.

SNTP Second Server: 선택 가능한 IPv4 주소, IPv6 주소 또는 도메인 이름.

SNTP Third Server: 선택 가능한 IPv4 주소, IPv6 주소 또는 도메인 이름.

SNTP Poll Interval in Seconds (30-99999): SNTP 서버가 유니캐스트 정보를 폴링하는 간격(초)을 정의합니다. 폴링 간격 기본값은 30초입니다.

Apply(**적용**)를 클릭하여 변경 사항을 적용합니다.

Clock Source에 대해 Local을 선택할 때 사용자는 다음 두 가지 옵션 중 하나를 선택할 수 있습니다.

Manually Time Settings: 사용자가 시스템 시간을 수동으로 입력합니다.

Sync to PC: 시스템 시간이 로컬 컴퓨터에서 동기화됩니다.

L2 기능 > SNTP > 시간대 설정

TimeZone 설정 페이지는 SNTP에 대한 표준 시간대 및 일광 절약 시간 설정을 구성하는 데 사용됩니다.

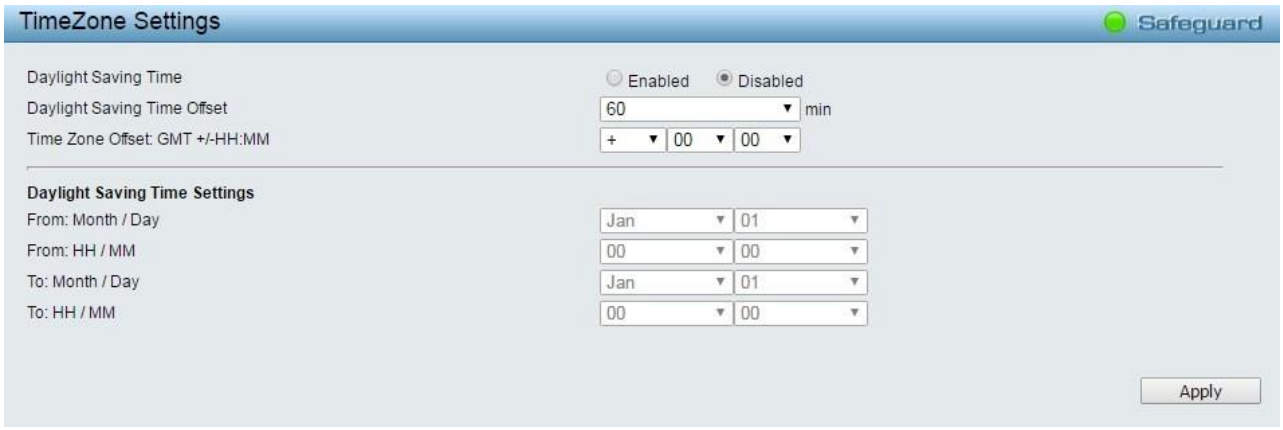


그림 4.80 - L2 기능 > SNTP > 시간대 설정

Daylight Saving Time State: DST 설정을 사용하거나 사용하지 않도록 설정합니다.

Daylight Saving Time Offset: 이 드롭다운 메뉴를 사용하여 DST가 발생했을 때 조정된 시간을 지정합니다. 선택 가능한 값: *30*분, *60분*, *90*분 또는 *120*분.

Time Zone Offset GMT +/- HH:MM: 이 드롭다운 메뉴를 사용하여 그리니치 표준시(GMT)에서 현지 시간대의 오프셋을 지정합니다.

Daylight Saving Time Settings:

From: Month / Day: 매년 DST가 시작되는 월과 날짜를 입력합니다.

From: HH:MM: 매년 DST가 시작되는 시간을 입력합니다.

To: Month / Day: 매년 DST가 종료되는 월과 날짜를 입력합니다.

To: HH:MM: 매년 DST가 종료되는 시간을 입력합니다.

Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

LLDP > 전역 설정 > L2 기능

LLDP(Link Layer Discovery Protocol) 는 스위치가 인접 디바이스에 자신을 광고하고 인접 LLDP 디바이스에 대해 학습할 수 있는 IEEE 802.1AB 표준 기반 방법을 제공합니다. SNMP 유틸리티는 각 LLDP 디바이스에서 MIB 정보를 가져와서 네트워크 토폴로지를 학습할 수 있습니다. LLDP 기능은 기본적으로 활성화되어 있습니다.

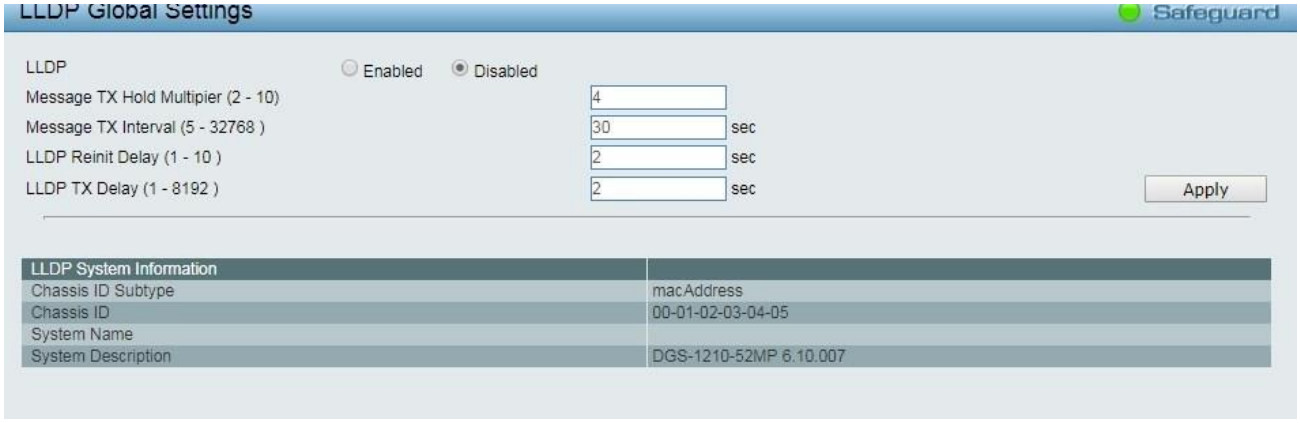


그림 4.81 - LLDP > 전역 설정을 > L2 기능

LLDP: 이 기능이 *활성화*되면 스위치가 LLDP 패킷의 전송, 수신 및 처리를 시작할 수 있습니다. LLDP 패킷의 광고를 위해 스위치는 포트를 통해 이웃에게 정보를 알립니다. LLDP 패킷을 수신하기 위해 스위치는 네이버 테이블의 네이버에서 광고된 LLDP 패킷에서 정보를 학습합니다. **적용**을 클릭하여 변경 사항을 적용합니다.

Message TX Hold Multiplier (2-10): 이 매개변수는 LLDPDU에서 사용되는 실제 TTL 값을 결정하는 승수입니다. 기본값은 **4입니다**.

Message TX Interval (5-32768): 이 매개변수는 이 LLDP 에이전트를 대신하여 LLDP 프레임이 전송되는 간격을 나타냅니다. 기본값은 **30** 초입니다.

LLDP ReInit Delay(1-10): 이 매개변수는 adminStatus가 "disabled" 상태가 된 후 다시 초기화를 시도할 때까지의 지연 시간을 나타냅니다. 기본값은 **2** 초입니다.

LLDP TX Delay(1-8192): 이 매개변수는 LLDP 로컬 시스템 MIB의 값 또는 상태 변경에 의해 시작된 연속 LLDP 프레임 전송 간의 지연을 나타냅니다. txDelay의 값은 1 < txDelay <(0.25 °— msgTxInterval) 범위 수식으로 설정됩니다. 기본값은 **2** 초입니다.

LLDP > LLDP-MED 설정 > L2 기능

LLDP-MED(Link Layer Discovery Protocol-Media Endpoint Discovery)는 LLDP의 향상된 기능입니다. IP 전화 및 AP와 같은 엔드포인트 디바이스 간의 LLDP 작업을 개선합니다. LLDP-MED는 LAN 정책 자동 검색 및 디바이스 위치 검색과 같은 기능을 지원합니다.

이 페이지에서는 사용자가 802.3at 포트의 **Power PSE TLV**(Type-length-value) 상태를 구성할 수 있습니다. **From Port/ To Port(포트/To Port)**를 선택하고 **Enable/Disable(활성화/비활성화)**을 선택한 다음 Apply(**적용)를 클릭하여** Power PSE TLV **전송**을 켜거나 끕니다.

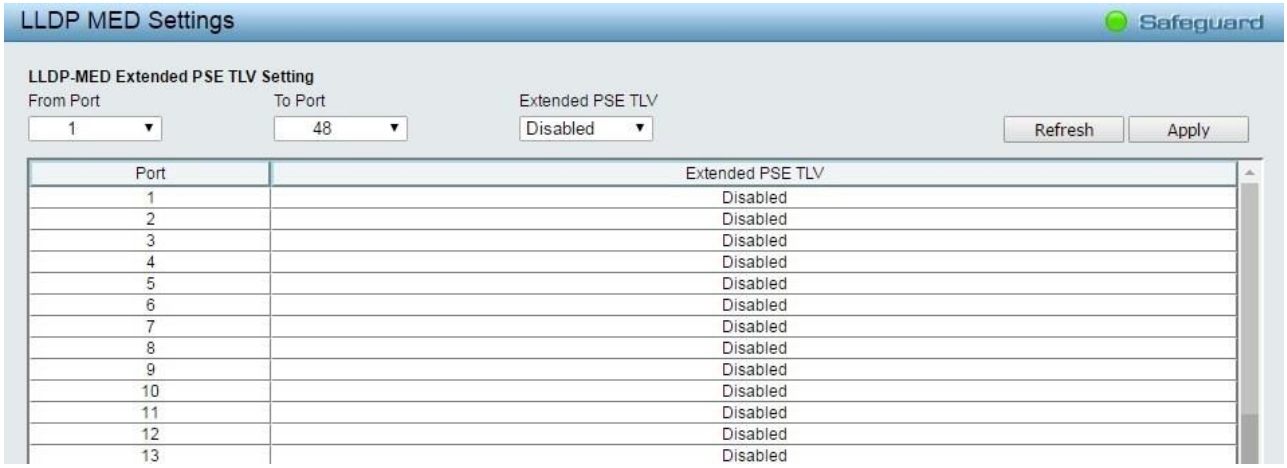


그림 4.82 - LLDP > LLDP–MED 설정을 > L2 기능

LLDP > LLDP 포트 설정 > L2 기능

Basic LLDP Port Settings(기본 LLDP 포트 설정) 페이지에는 LLDP 포트 정보가 표시되며 LLDP 포트 설정을 구성하기 위한 매개변수가 포함되어 있습니다.

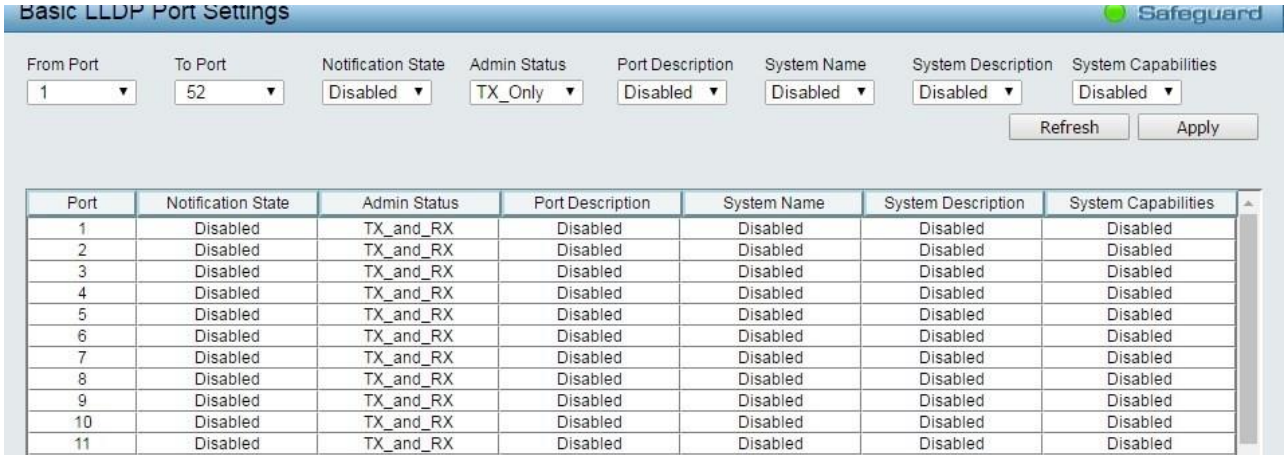


그림 4.83 - LLDP > LLDP 포트 설정을 > L2 기능

From Port/ To Port: 선택한 포트부터 시작하여 연속된 포트 그룹을 구성할 수 있습니다.

Notification State(알림 상태): 포트에서 LLDP 토폴로지 변경이 발생할 때 알림을 보낼지 여부를 지정합니다. 가능한 필드 값은 다음과 같습니다.

Enabled(활성화됨) - 포트에서 LLDP 알림을 활성화합니다.

Disabled(비활성화됨) - 포트에서 LLDP 알림을 비활성화합니다. 이 값은 기본값입니다.

Admin Status(관리 상태): 포트의 LLDP 전송 모드를 지정합니다. 가능한 필드 값은 다음과 같습니다.

TX_Only – LLDP 패킷만 전송할 수 있습니다.

RX_Only - LLDP 패킷만 수신할 수 있습니다.

TX_and_RX - LLDP 패킷을 송수신할 수 있습니다. 이것이 기본값입니다.

Disabled(비활성화됨) - 포트에서 LLDP를 비활성화합니다.

Port Description: 포트에서 포트 설명 TLV를 사용할 수 있는지 여부를 지정합니다. 가능한 필드 값은 다음과 같습니다.

Enabled(활성화됨) - 포트에서 포트 설명 TLV를 활성화합니다.

Disabled(비활성화됨) - 포트에서 포트 설명 TLV를 비활성화합니다.

System Name : 포트에서 시스템 이름 TLV를 사용할 수 있는지 여부를 지정합니다. 가능한 필드 값은 다음과 같습니다.

Enabled(활성화됨) - 포트에서 시스템 이름 TLV를 활성화합니다.

Disabled(비활성화) - 포트에서 시스템 이름 TLV를 비활성화합니다.

System Description: 포트에서 시스템 설명 TLV가 활성화되어 있는지 여부를 지정합니다. 가능한 필드 값은 다음과 같습니다.

Enabled(활성화됨) - 포트에서 시스템 설명 TLV를 활성화합니다.

Disabled(비활성화됨) - 포트에서 시스템 설명 TLV를 비활성화합니다.

System Capabilities: 포트에서 시스템 기능 TLV가 활성화되어 있는지 여부를 지정합니다. 가능한 필드 값은 다음과 같습니다.

Enabled(활성화됨) - 포트에서 시스템 기능 TLV를 활성화합니다.

Disabled(비활성화됨) - 포트에서 시스템 기능 TLV를 비활성화합니다.

이러한 매개 변수 필드를 정의합니다. **Apply(적용)** 버튼을 클릭하여 변경 사항을 구현하고 **Refresh(새로 고침)**를 클릭하여 테이블 정보를 새로 고칩니다.

LLDP > 802.1 확장 TLV> L2 기능

이 802.1 확장 TLV 페이지는 LLDP 포트 설정을 구성하는 데 사용됩니다.

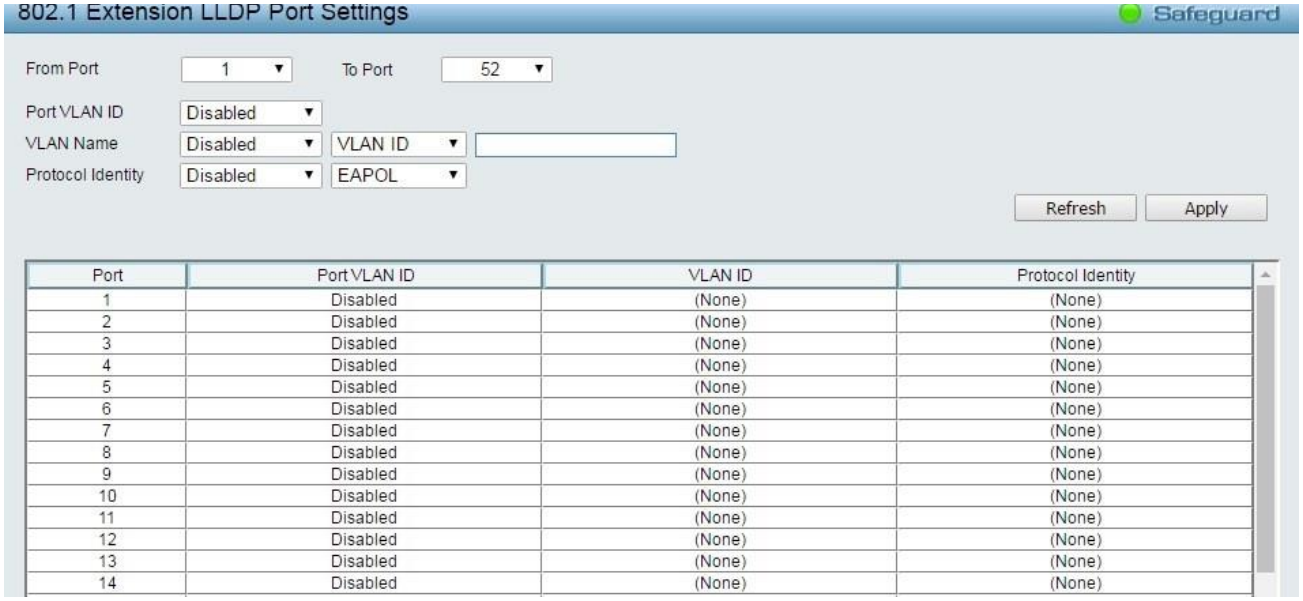


그림 4.84 - LLDP > 802.1 확장 TLV 포트 설정을 > L2 기능

From Port / To Port: 선택한 포트부터 시작하여 연속된 포트 그룹을 구성할 수 있습니다.

Port VLAN ID: 활성화 또는 비활성화할 포트 VLAN ID를 지정합니다.

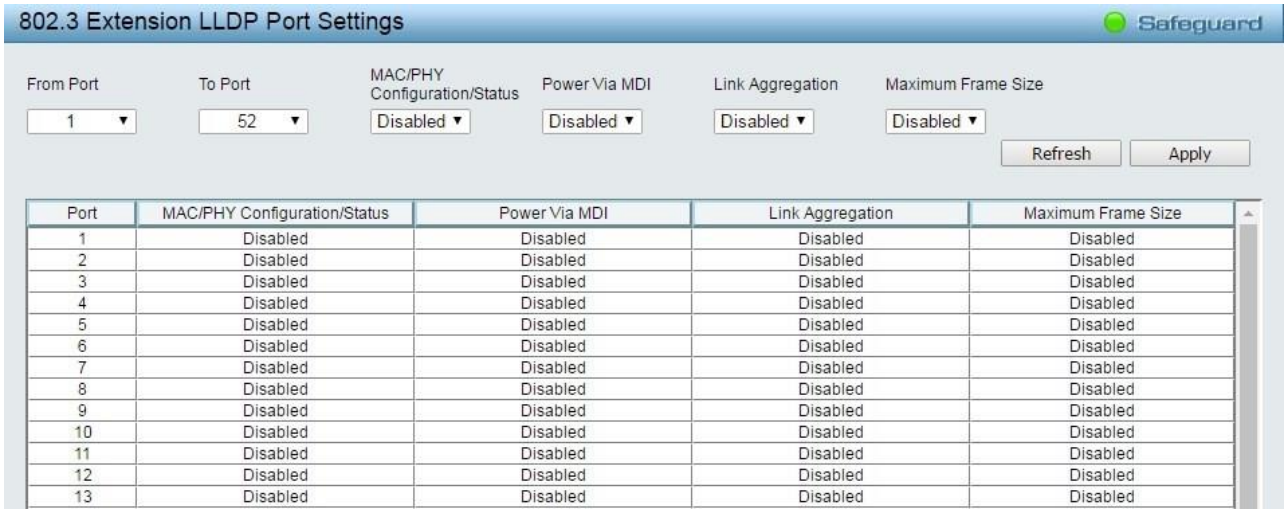
VLAN Name: LLDP 포트에서 활성화 또는 비활성화할 VLAN 이름을 지정합니다. Enabled(활성화됨)를 선택하면 사용자는 VLAN ID 또는 VLAN Name(VLAN 이름) 또는 all의 내용을 지정할 수 있습니다.

Protocol Identity: LLDP 포트에서 활성화하거나 비활성화할 프로토콜 ID를 지정합니다. 사용을 선택하면 사용자가 EAPOL, LACP, GVRP, STP 또는 ALL을 지정할 수 있습니다.

Apply(**적용**) 버튼을 클릭하여 변경 사항을 구현하고 **Refresh(새로 고침)**를 클릭하여 테이블 정보를 새로 고칩니다.

LLDP > 802.3 확장 TLV> L2 기능

802.3 확장 LLDP 포트 설정 페이지에는 802.3 확장 LLDP 포트 정보가 표시되며 802.3 확장 LLDP 포트 설정을 구성하기



위한 매개 변수가 포함되어 있습니다.

그림 4.85 - LLDP > 802.3 확장 TLV> L2 기능

From Port / To Port: 선택한 포트부터 시작하여 연속된 포트 그룹을 구성할 수 있습니다.

MAC/PHY Configuration/Status: 포트에서 MAC/PHY 구성 상태가 활성화되어 있는지 여부를 지정합니다. 가능한 필드 값은 다음과 같습니다.

Enabled(활성화됨) - 포트에서 MAC/PHY 컨피그레이션 상태를 활성화합니다.

Disabled(비활성화됨) - 포트에서 MAC/PHY 컨피그레이션 상태를 비활성화합니다.

Power via MDI: 포트에서 지원하는 Power via MDI 구현을 광고합니다. 가능한 필드 값은 다음과 같습니다.

Enabled(활성화됨) - 포트에 구성된 MDI를 통한 전원을 활성화합니다.

Disabled(비활성화됨) - 포트에 구성된 MDI를 통한 전원을 비활성화합니다.

Link Aggregation: 포트에서 Link Aggregation을 사용할 수 있는지 여부를 지정합니다. 가능한 필드 값은 다음과 같습니다.

Enabled(활성화됨) - 포트에 구성된 링크 집계를 활성화합니다.

Disabled(비활성화됨) - 포트에 구성된 링크 집계를 비활성화합니다.

Maximum Frame Size(최대 프레임 크기): 포트에서 Maximum Frame Size(최대 프레임 크기)를 사용할 수 있는지 여부를 지정합니다. 가능한 필드 값은 다음과 같습니다.

Enabled(활성화됨) - 포트에 구성된 최대 프레임 크기를 활성화합니다.

Disabled(비활성화됨) - 포트에 구성된 Maximum Frame Size(최대 프레임 크기)를 비활성화합니다.

이러한 매개 변수 필드를 정의합니다.

Apply(적용) 버튼을 클릭하여 변경 사항을 적용하거나 **Refresh(새로 고침)**를 클릭하여 테이블 정보를 새로 고칩니다.

LLDP > LLDP 관리 주소 설정 > L2 기능

LLDP 관리 주소 설정을 사용하면 전송되는 LLDP 정보에 포함되는 관리 주소를 설정할 수 있습니다.

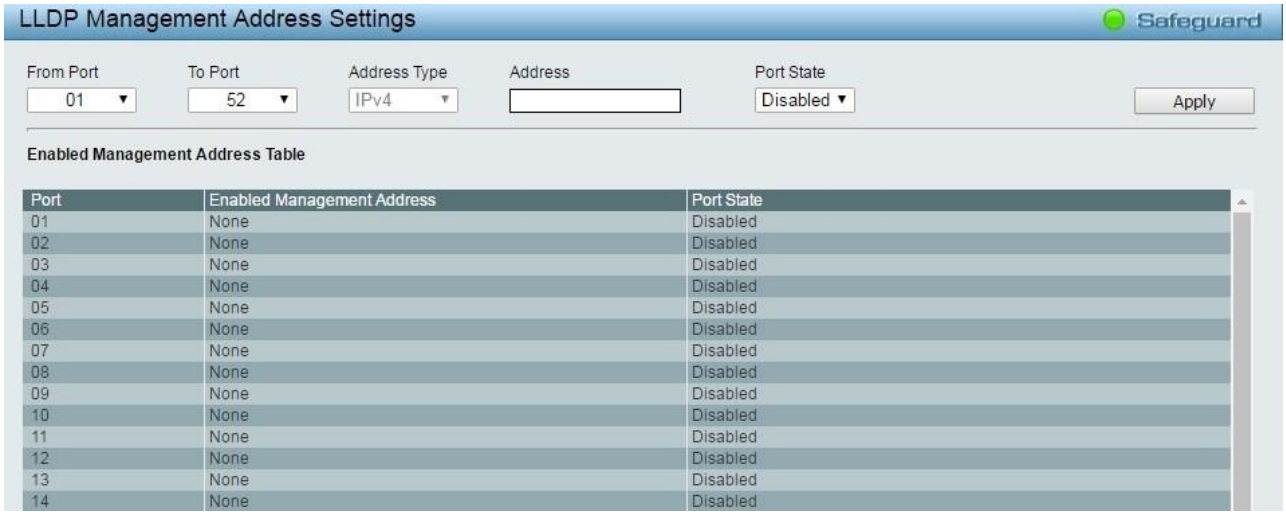


그림 4.86 - LLDP > 관리 주소 설정을 > L2 기능

From Port / To Port: 선택한 포트부터 시작하여 연속된 포트 그룹을 구성할 수 있습니다.

Address Type: 포트의 LLDP 주소 유형을 지정합니다. 값은 항상 IPv4입니다.

Address: 주소를 지정합니다.

Port State: 포트 상태가 포트에서 활성화되어 있는지 여부를 지정합니다. 가능한 필드 값은 다음과 같습니다.

Enabled(활성화됨) - 포트에 구성된 포트 상태를 활성화합니다.

Disabled(비활성화됨) - 포트에 구성된 포트 상태를 비활성화합니다.

Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

LLDP > LLDP 관리 주소 테이블 > L2 기능

LLDP Management Address Table 페이지에는 항목에 대한 자세한 관리 주소 정보가 표시됩니다.

그림 4.87 - LLDP > LLDP 관리 주소 테이블 > L2 기능

Management Address: IPv4 또는 IPv6 주소를 선택하고 IP 주소를 입력합니다.
Search를 클릭하면 테이블이 업데이트되고 필요한 값이 표시됩니다.

Subtype: 관리되는 주소 하위 유형을 표시합니다. 예를 들어 MAC 주소 또는 IPv4 주소입니다.

Management Address: IP 주소를 표시합니다.

IF Type: IF 타입을 표시합니다.

OID: SNMP OID (알림)

Advertising Ports: 광고 포트를 표시합니다.

LLDP > LLDP 로컬 포트 테이블 > L2 기능

LLDP Local Port Table(LLDP 로컬 포트 테이블) 페이지에는 LLDP 로컬 포트 정보가 표시됩니다.

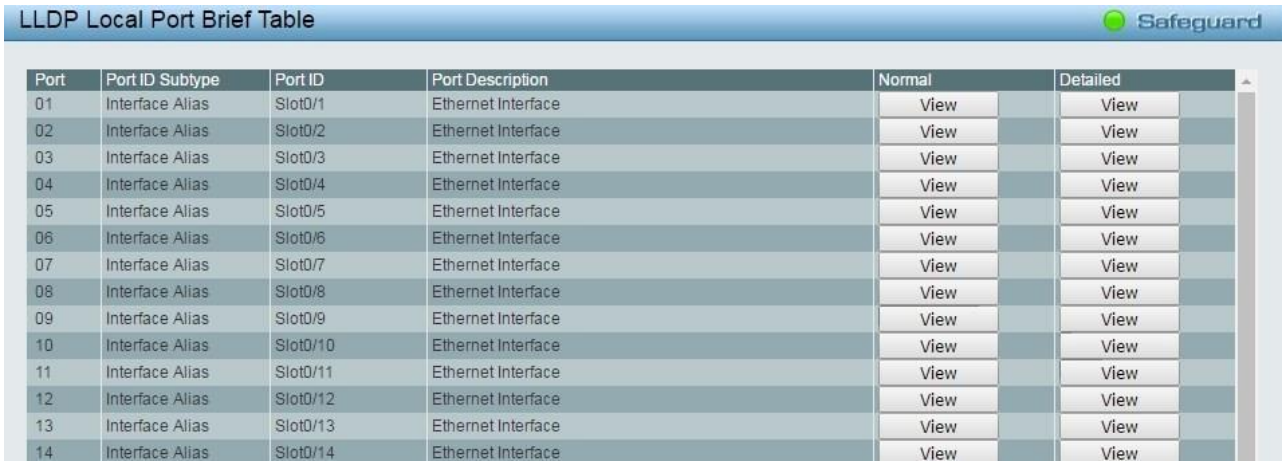


그림 4.88 - LLDP > LLDP 로컬 포트 테이블의 L2 기능 >

Port: 포트 번호를 표시합니다.

Port ID Subtype: 포트 ID 하위 유형을 표시합니다.

Port ID: 포트 ID(장치 번호/포트 번호)를 표시합니다.

Port Description: 포트 설명을 표시합니다.

Normal 열의 **View**를 클릭하면 자세한 정보를 표시됩니다.

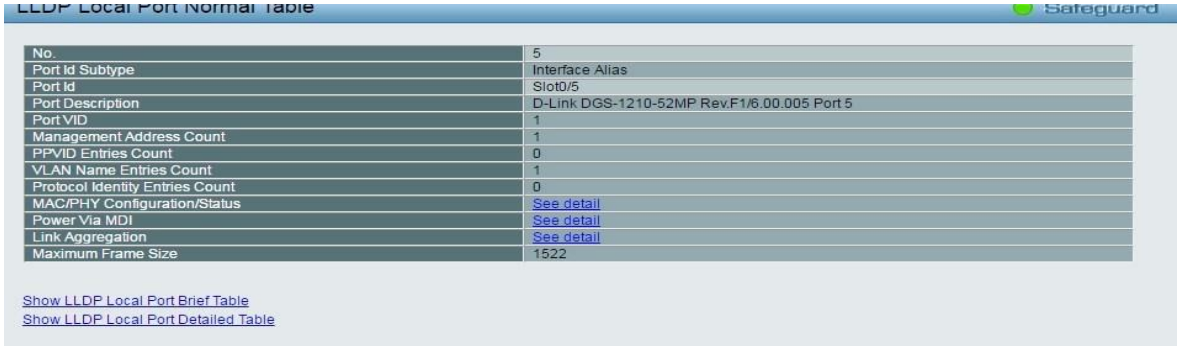


그림 4.89 - LLDP > LLDP 로컬 포트 일반 테이블 > L2 기능

Detailed 열의 **View**를 클릭하여 자세한 정보를 표시됩니다.

그림 4.90 - LLDP > LLDP 로컬 포트> L2 기능 상세 표

LLDP > LLDP 원격 포트 테이블 > L2 기능

이 LLDP Remote Port Table 페이지는 LLDP Remote Port Brief Table을 표시하는 데 사용됩니다. 포트 번호를 선택하고 **Search**를 클릭하여 추가 정보를 표시합니다.

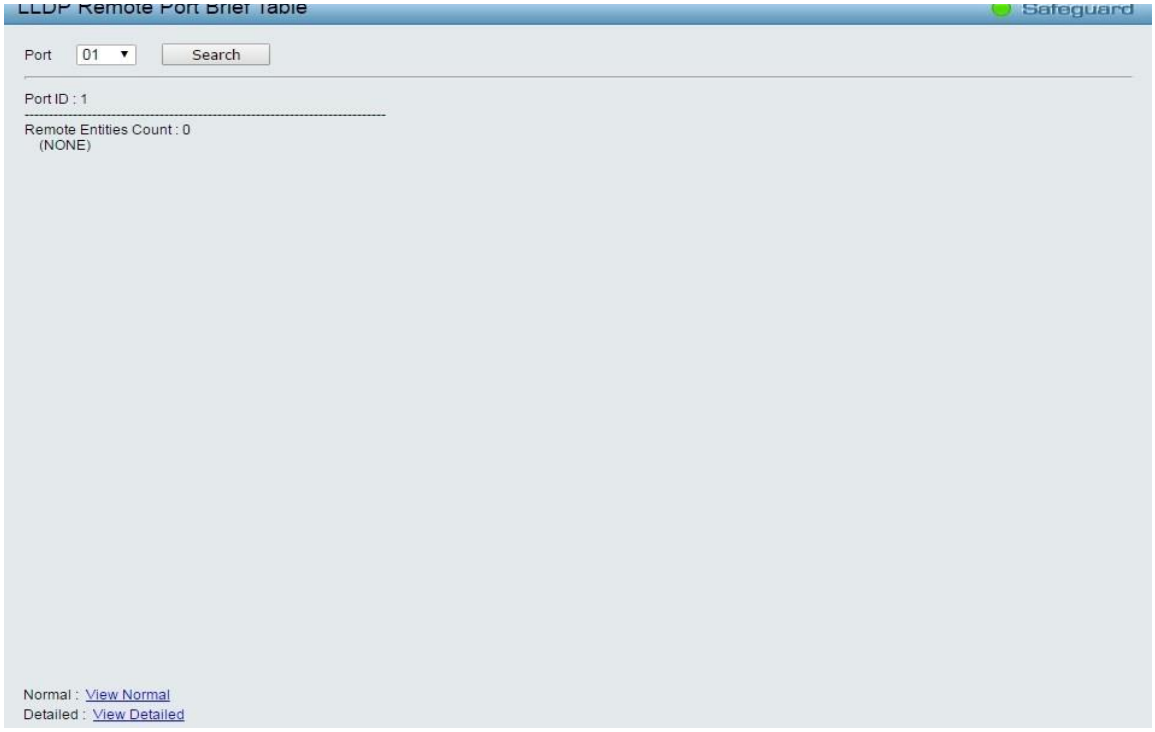


그림 4.91 - LLDP > LLDP 원격 포트 테이블의 L2 기능 >

원격 포트에 대한 설정을 보려면 **View Normal**을 클릭하면 다음 페이지가 표시됩니다.

그림 4.92 - LLDP > LLDP 원격 포트 일반 테이블 > L2 기능

원격 포트에 대한 세부 설정을 보려면 **View Detail**을 클릭하면 다음 페이지가 표시됩니다.

그림 4.93 - LLDP > LLDP 원격 포트 상세 표 > L2 기능

LLDP > 통계 > L2 기능

LLDP Statistics(LLDP 통계) 페이지에는 모든 LLDP 트래픽에 대한 개요가 표시됩니다.

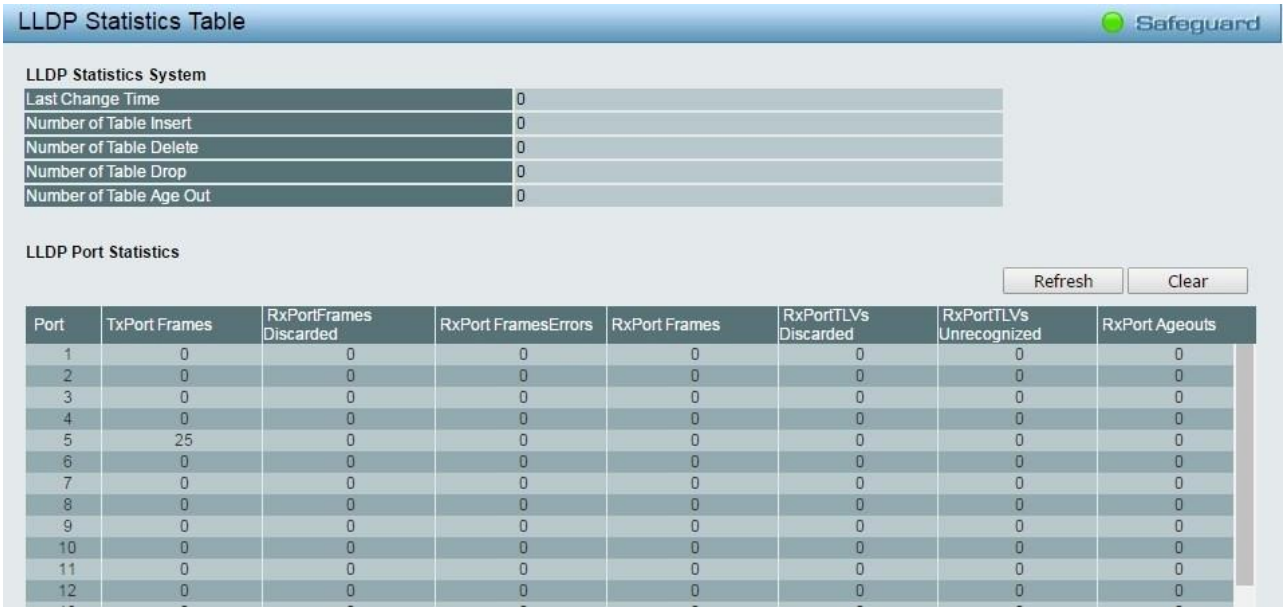


그림 4.94 - LLDP > 통계> L2 기능

다음 정보를 볼 수 있습니다.

LLDP Statistics System: 전체 스위치를 참조하는 카운터를 표시합니다.

Last Change Time – 마지막 변경 항목이 마지막으로 삭제되거나 추가된 시간을 표시합니다. 또한 마지막 변경 사항이 감지된 이후 경과된 시간도 표시됩니다.

Number of Table Insert(테이블 삽입 수) - 스위치 재부팅 이후 삽입된 새 항목의 수를 표시합니다.

Number of Table Delete(테이블 삭제 수) - 스위치 재부팅 이후 삭제된 새 항목 수를 표시합니다.

Number of Table Drop(테이블 삭제 수) - 테이블이 꽉 찼기 때문에 삭제된 LLDP 프레임 수를 표시합니다.

Number of Table Age Out(테이블 사용 시간 초과) – TTL(Time-To-Live) 만료로 인해 삭제된 항목 수를 표시합니다.

LLDP Port Statistics(LLDP 포트 통계): 포트를 참조하는 카운터를 표시합니다.

TxPort FramesTotal - 포트에서 전송된 총 LLDP 프레임 수를 표시합니다.

RxPort FramesDiscarded - 포트에서 수신된 LLDP 프레임의 폐기된 총 프레임 수를 표시합니다.

RxPort FramesErrors - 포트에서 수신된 LLDP 프레임의 오류 프레임 번호를 표시합니다.

RxPort Frames(RxPort 프레임) - 포트에서 수신된 총 LLDP 프레임 수를 표시합니다.

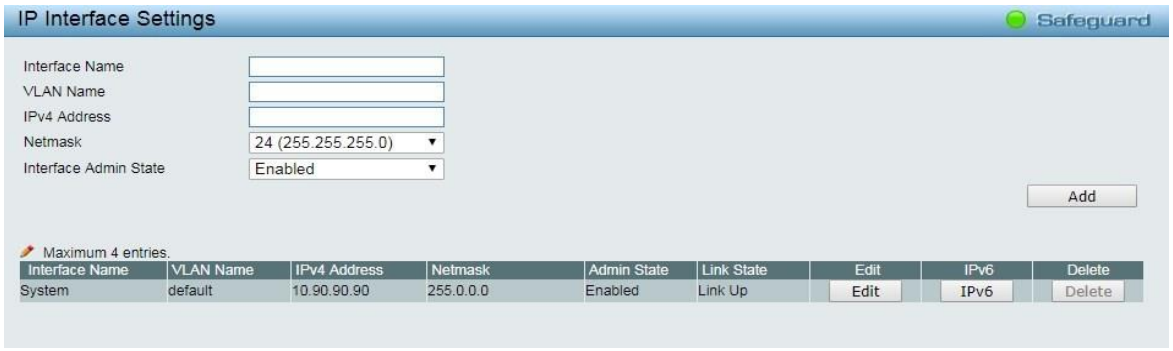
RxPortTLVsDiscarded - 각 LLDP 프레임에는 TLV라고 하는 여러 정보가 포함될 수 있습니다. TLV의 형식이 잘못되면 계산되고 폐기됩니다.

RxPortTLVsUnrecognized – 올바른 형식의 TLV 수를 표시하지만 알려진 유형 값을 사용합니다.

RxPort Ageouts - 각 LLDP 프레임에는 LLDP 정보가 유효한 기간에 대한 정보가 포함되어 있습니다. 에이지아웃 시간 내에 새 LLDP 프레임이 수신되지 않으면 LLDP 정보가 제거되고 에이지아웃 카운터가 증가합니다.

Refresh(새로 고침)를 클릭하여 페이지를 갱신하고 Clear(**지우기**)를 클릭하여 모든 통계를 지웁니다.

L3 기능 > IP 인터페이스



IP Interface(IP 인터페이스) 페이지에서는 사용자가 관리 IP 인터페이스를 구성할 수 있습니다.

그림 4.95 - IP 인터페이스> L3 기능

Interface Name: IP 인터페이스의 이름을 지정합니다.

VLAN Name: IP 인터페이스의 VLAN 이름을 지정합니다.

IPv4 Address: 인터페이스의 IPv4 주소를 지정합니다.

Netmask: IP 주소의 넷마스크를 선택합니다.

Interface Admin State(인터페이스 관리 상태): 인터페이스 관리 상태를 활성화하거나 비활성화합니다. Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

Edit(**편집**) 버튼을 클릭하여 IP 설정을 수정합니다.

그림 4.96 - L3 기능 > IPv6 인터페이스 설정 - 편집

IPv4 Address: 인터페이스의 IPv4 주소를 지정합니다.

Netmask: IP 주소의 넷마스크를 선택합니다.

Admin State(관리 상태): 인터페이스 관리 상태를 활성화하거나 비활성화합니다. Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

IPv6 버튼을 클릭하여 IPv6 인터페이스 설정을 구성합니다.

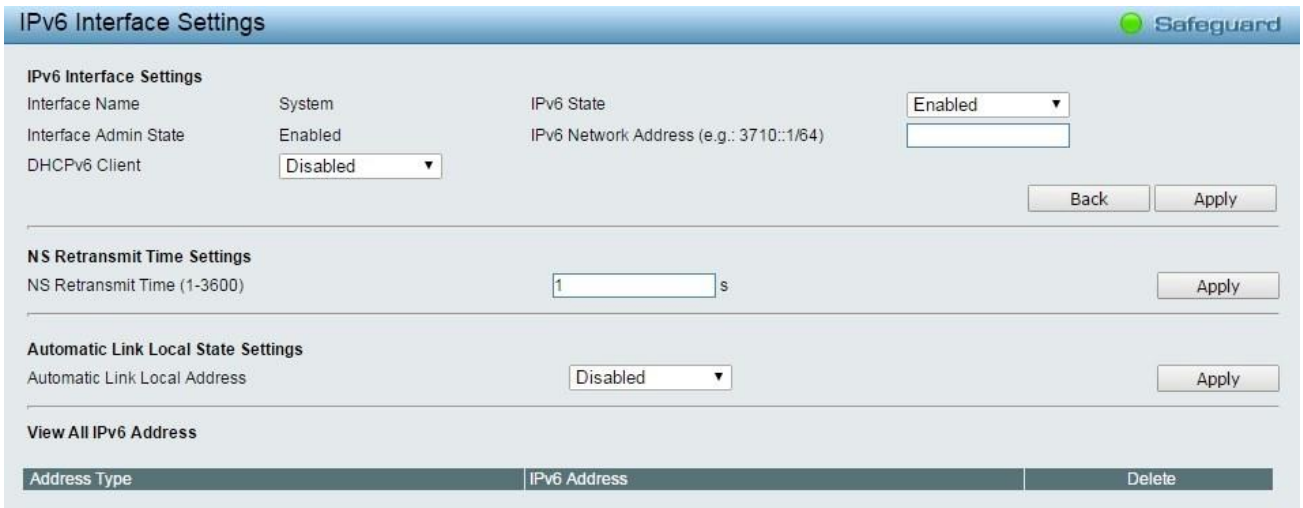


그림 4.97 - L3 기능 > IPv6 인터페이스 설정 – IPv6

IPv6 System Settings:

Interface Name: IPv6의 인터페이스 이름을 표시합니다.

IPv6 State: 사용하거나 사용하지 않도록 설정할 IPv6을 지정합니다.

Interface Admin State: 인터페이스 관리자 상태를 표시합니다.

DHCPv6 Client: 활성화 또는 비활성화할 DHCPv6 클라이언트를 지정합니다.

IPv6 Network Address: IPv6 네트워크 주소를 지정합니다.

NS Retransmit Time Settings:

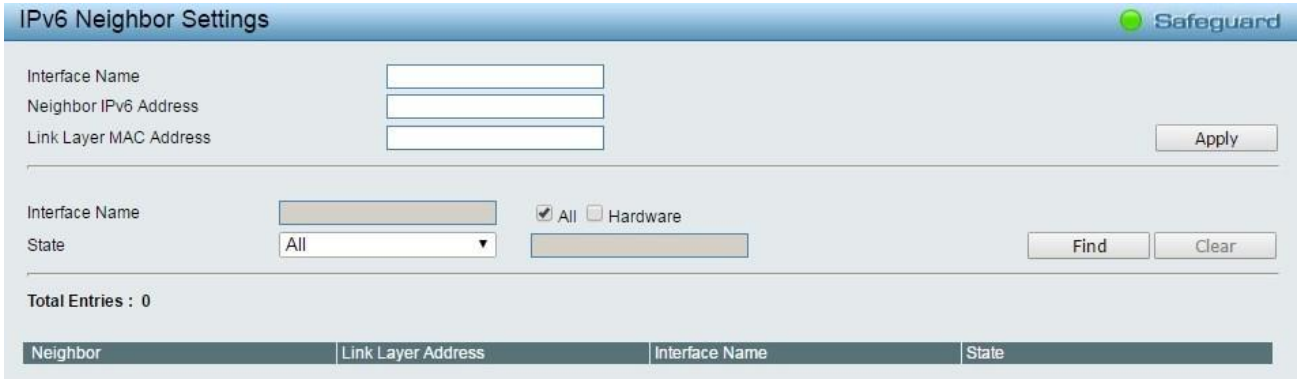
NS Retransmit Time (1-3600): 여기에 네이버 요청의 재전송 타이머를 두 번째로 입력합니다. IPv6에 대한 NS 재전송 시간을 지정합니다. 필드 범위는 1-3600이고 기본값은 1초입니다.

Automatic Link Local State Settings:

Automatic Link Local Address: 자동 링크를 사용하거나 사용하지 않도록 지정합니다.
Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

L3 기능 > IPv6 네이버 설정

사용자는 스위치의 IPv6 네이버 설정을 구성할 수 있습니다. 스위치의 현재 IPv6 네이버 설정이 이 창 하단의 표에



표시됩니다.

그림 4.98 - L3 기능 > IPv6 네이버 설정

Interface Name: IPv6 인접 디바이스의 인터페이스 이름을 입력합니다.
Neighbor IPv6 Address: 인접 IPv6 주소를 지정합니다.
Link Layer MAC Address: 링크 레이어 MAC 주소를 지정합니다.

Apply(**적용**)를 클릭하여 변경 사항을 적용합니다.

Interface Name: IPv6 인접 디바이스의 인터페이스 이름을 지정합니다. 스위치에서 현재 인터페이스를 모두 검색하려면 창 중간에 있는 두 번째 Interface Name(인터페이스 이름) 필드로 이동하여 All(모두) 확인란을 선택합니다. Hardware(하드웨어) 옵션을 선택하여 하드웨어 테이블에 기록된 모든 인접 캐시 항목을 표시합니다.

State(상태): 드롭다운 메뉴를 사용하여 All(모두), Address(주소), Static(정적) 또는 Dynamic(동적)을 선택합니다. 사용자가 드롭다운 메뉴에서 주소를 선택하면 상태 옵션 옆에 제공된 공간에 IP 주소를 입력할 수 있습니다.

Find를 클릭하여 입력한 정보를 기반으로 특정 항목을 찾습니다.
Clear를 클릭하여 필드에 입력한 모든 정보를 지웁니다.

L3 기능 > IPv4 고정 경로

스위치는 IPv4 형식의 주소 지정에 대한 정적 라우팅을 지원합니다. 사용자는 IPv4에 대해 최대 124개의 고정 경로 항목을 생성할 수 있습니다. IPv4 고정 경로의 경우 고정 경로가 설정되면 스위치는 사용자가 설정한 다음 hop 라우터로 ARP 요청 패킷을 보냅니다. 다음 홉에서 스위치에 의해 ARP 응답이 검색되면 경로가 활성화됩니다. 그러나 ARP 항목이 이미 있는 경우 ARP 요청이 전송되지 않습니다.

또한 스위치는 부동 고정 경로를 지원하며, 이는 사용자가 다른 다음 홉에 대한 대체 고정 경로를 생성할 수 있음을 의미합니다. 이 보조 next hop 디바이스 경로는 기본 정적 경로가 다운된 경우 백업 정적 경로로 간주됩니다. 기본 경로가 손실되면 백업 경로가 업링크되고 해당 상태가 활성이 됩니다. 스위치의 포워딩 테이블에 대한 입력은 IP 주소, 서브넷 마스크 및 게이트웨이를 모두 사용하여 만들 수 있습니다.

IPv4 Static Route(IPv4 고정 경로) 페이지에서는 사용자가 IPv4 경로 설정을 활성화하고 구성할 수 있습니다.

그림 4.99 - L3 기능 > IPv4 고정 경로

IPv4 Static Route(IPv4 고정 경로): 스위치에서 IPv4 고정 경로 기능을 활성화하거나 비활성화하도록 지정합니다. Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

IPv4 Address: 고정 경로에 할당할 IPv4 주소를 지정합니다.

Netmask: IPv4 주소의 해당 서브넷 마스크에 적용할 서브넷 마스크를 지정합니다.

Gateway: 다음 홉 게이트웨이 주소에 해당하는 IPv4 주소(IPv4 형식)입니다.

Metric: 테이블에 입력된 IP 인터페이스의 메트릭 값을 나타냅니다. 이 필드는 1에서 65535 사이의 숫자를 읽을 수 있습니다.

Backup State: 사용자는 기본과 백업 중에서 선택할 수 있습니다. 기본 고정 경로가 실패하면 백업 경로가 항목을 지원합니다. 기본 항목과 백업 항목은 동일한 게이트웨이를 가질 수 없다는 점을 유의하십시오.

Add(**추가**)를 클릭하여 고정 경로를 생성합니다.

예를 들어 새 IPv4 고정 경로 항목을 생성하려면 아래에 표시된 구성을 입력한 다음 Add(추가)를 클릭합니다.

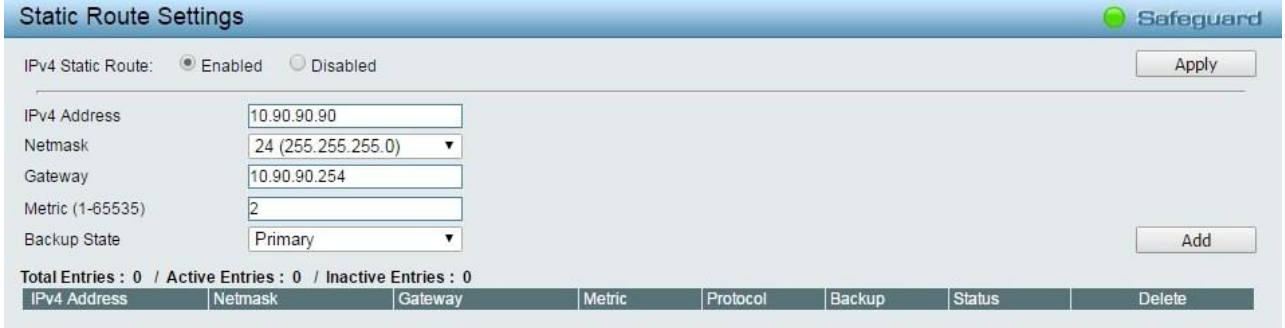


그림 4.100 - L3 기능 > IPv4 고정 경로 – 추가

새 항목이 IPv4 고정 경로 테이블에 표시됩니다.

그림 4.101 - L3 기능 > IPv4 정적 경로 – 정적 경로 테이블

Delete 버튼을 클릭하여 항목을 제거합니다.

L3 기능 > IPv4 라우팅 테이블 파인더

IPv4 Routing Table Finder 페이지에는 스위치의 현재 IPv4 라우팅 테이블이 표시됩니다. 특정 IPv4 경로를 찾으려면 **Network Address** 필드에 IPv4 주소를 입력하고 **Search** 버튼을 클릭합니다.

그림 4.102 - IPv4 라우팅 테이블 파인더> L3 기능

IPv6 고정 경로 > L3 기능

IPv6 고정 경로 페이지에서는 사용자가 IPv6 경로 설정을 활성화하고 구성할 수 있습니다.

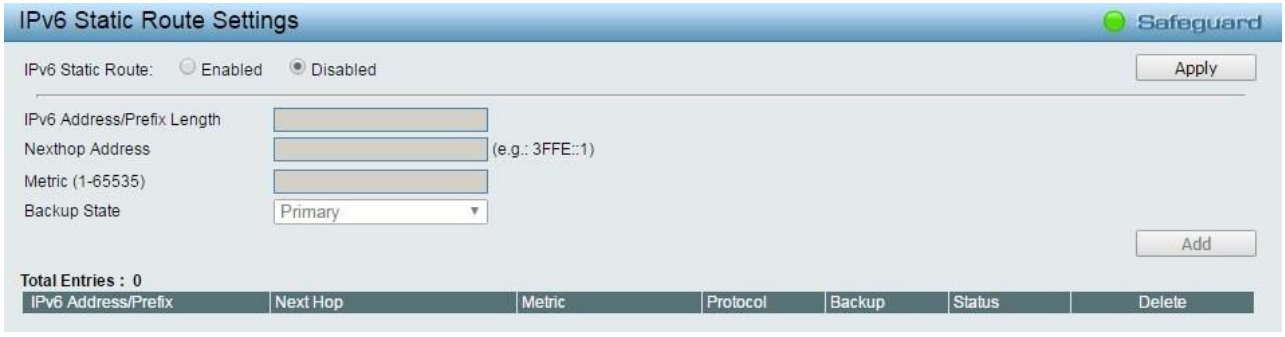


그림 4.103 - IPv6 고정 경로> L3 기능

IPv6 Static Route(IPv6 고정 경로): 스위치에서 IPv6 고정 경로 기능을 활성화하거나 비활성화하도록 지정합니다. Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

IPv6 Address/Prefix Length: 해당 주소와 일치하는 패킷이 변환되도록 지정합니다.

Nexthop Address: 다음 홉 게이트웨이 주소에 해당하는 IPv6 주소를 IPv6 형식으로 지정합니다.

Metric (1-65535): 스위치와 위의 IPv6 주소 사이의 라우터 수를 나타내는 테이블에 IPv6 인터페이스의 메트릭을 지정합니다. 값의 범위는 1에서 65535 사이입니다.

Backup State: 각 IP 주소에는 하나의 기본 경로만 있을 수 있지만 다른 경로는 백업 상태에 할당해야 합니다. 기본 경로에 장애가 발생하면 스위치는 경로가 성공할 때까지 라우팅 테이블에서 학습한 순서에 따라 백업 경로를 시도합니다. 이 필드는 Static 및 Default Route가 구성된 백업 상태를 나타냅니다.

Add를 클릭하여 새 IPv6 고정 경로를 만듭니다.

L3 기능 > IPv6 라우팅 테이블 파인더

IPv6 Routing Table Finder 페이지에는 스위치의 현재 Ipv6 라우팅 테이블이 표시됩니다. 특정 Ipv6 경로를 찾으려면 **IPv6 Network Address** 필드에 및 IPv6 주소를 입력하고 **Search**를 클릭합니다.

그림 4.104 - IPv6 라우팅 테이블 찾기> L3 기능

IPv6 Network Address: IPv6 주소를 지정합니다.

참고: Ipv4 / IPv6의 고정 경로 설정 및 라우팅 테이블 파인더는 다른 설정 페이지로 구성해야 합니다.

L3 기능 > ARP > ARP 테이블 전역 설정

ARP Table Global Settings(ARP 테이블 전역 설정) 페이지에는 스위치의 현재 ARP 항목이 표시됩니다. 이 테이블을 통해 네트워크 관리자는 특정 장치에 대한 ARP 정보를 보고, 정의하고, 수정하고, 삭제할 수 있습니다. 정적 항목은 ARP 테이블에서 정의할 수 있습니다. 정적 항목이 정의되면 영구 항목이 입력되고 IP 주소를 MAC 주소로 변환하는 데 사용됩니다.

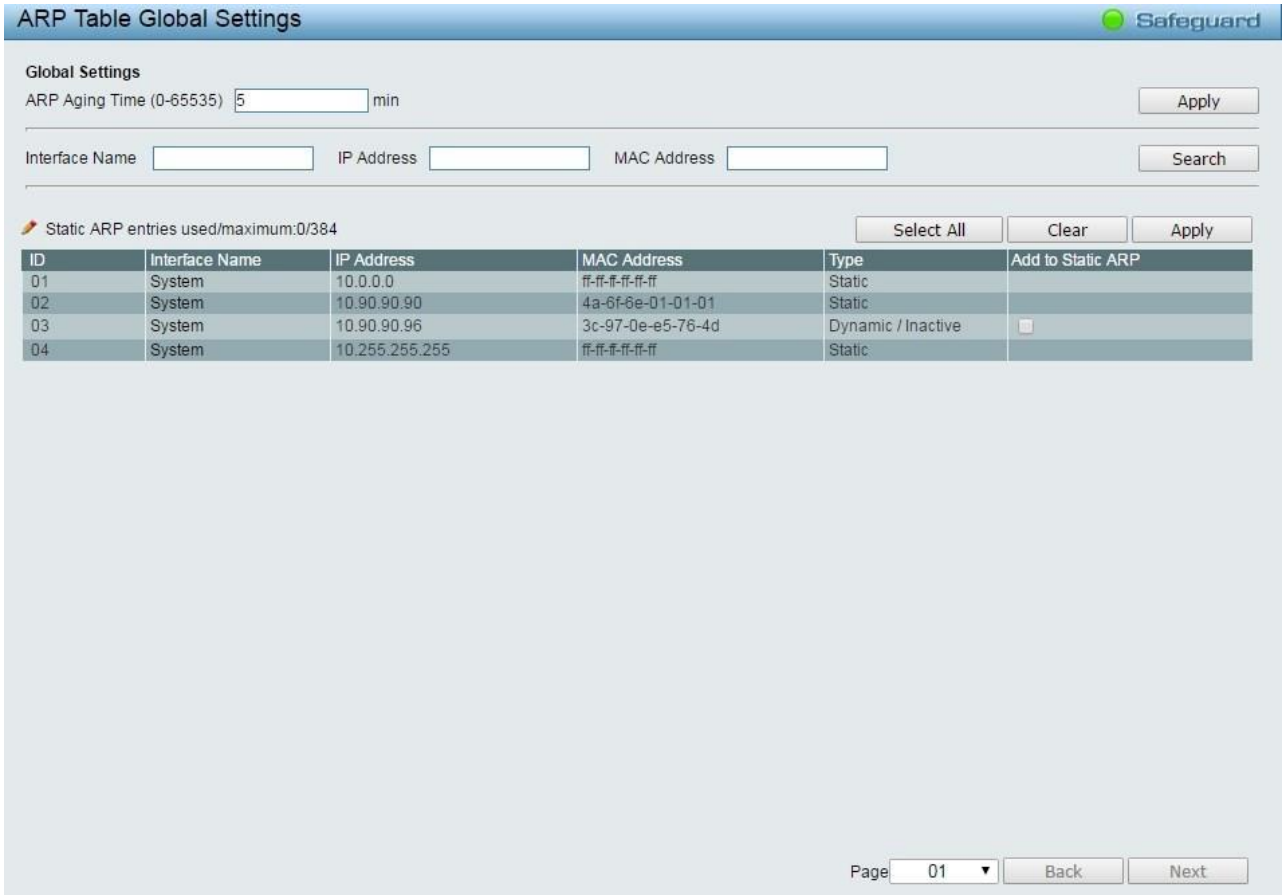


그림 4.105 - L3 기능 > ARP > ARP 테이블 전역 설정

전역 설정:

ARP Aging Time (0-65535): ARP 항목 에이징 아웃 시간(분)을 지정합니다. 기본값은 5분입니다.

Interface Name: 사용된 인터페이스 이름을 입력하거나 봅니다.

IP Address: 사용된 IP 주소를 입력하거나 봅니다.

MAC Address: 사용된 MAC 주소를 입력하거나 봅니다.

Search(**검색**) 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Select All 버튼을 클릭하고 **Clear** 버튼을 클릭하여 테이블에 나열된 항목을 제거합니다.

L3 기능 > ARP > 정적 ARP 설정

주소 확인 프로토콜은 IP 주소를 실제 주소로 변환하는 TCP/IP 프로토콜입니다. 이 테이블을 통해 네트워크 관리자는 특정 장치에 대한 ARP 정보를 보고, 정의하고, 수정하고, 삭제할 수 있습니다. 정적 항목은 ARP 테이블에서 정의할 수 있습니다. 정적 항목이 정의되면 영구 항목이 입력되고 IP 주소를 MAC 주소로 변환하는 데 사용됩니다.

그림 4.106 - L3 기능 > ARP > 정적 ARP 설정

IP Address: IP 주소를 지정합니다.

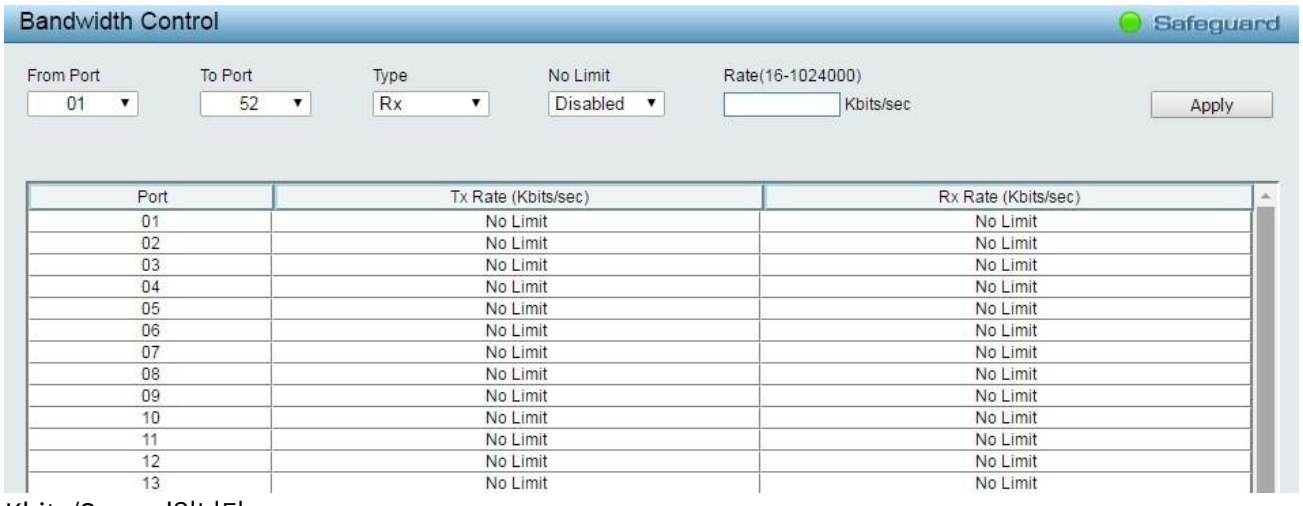
MAC Address: MAC 주소를 지정합니다.

Add(**추가**) 버튼을 클릭하여 정적 ARP 항목을 생성합니다.

Delete All(모두 삭제**)** 버튼을 클릭하여 나열된 모든 항목을 제거하고, Delete(**삭제**) 버튼을 클릭하여 특정 항목을 제거합니다.

QoS > 대역폭 제어

Bandwidth Control(대역폭 제어)은 특정 포트 인터페이스의 속도 속도를 제한하는 데 사용됩니다. 측정 단위는



Kbits/Second입니다.

그림 4.107 - QoS > 대역폭 제어

From Port / To Port: 선택한 포트부터 시작하여 연속된 포트 그룹을 구성할 수 있습니다.

Type: 드롭다운 목록에서 "Tx", "Rx" 및 "Both" 유형을 선택할 수 있습니다.

Tx: 송신 패킷에 특정 Rx: 수신
패킷에 특정 둘 다: Tx/Rx 모드가
포함됩니다.

No Limit: 이 드롭다운 메뉴를 사용하면 선택한 포트에 대역폭 제한이 없도록 지정할 수 있습니다.

Enabled(사용) 는 제한을 비활성화합니다.

Rate (64-1024000): 이 필드를 사용하면 사용자가 선택한 포트에 대한 제한이 되는 초당 Kbits 단위의 데이터 속도를 입력할 수 있습니다. 값은 64에서 1024000 사이입니다.

Apply(적용)를 클릭하여 선택한 포트에 대한 대역폭 제어를 설정합니다.

QoS > 802.1p/DSCP/ToS

QoS는 IEEE 802.1p 표준의 구현으로, 네트워크 관리자가 더 큰 대역폭이 필요하거나 VoIP(Voice-over Internet Protocol), 웹 브라우징 응용 프로그램, 파일 서버 응용 프로그램 또는 화상 회의와 같이 더 높은 우선 순위를 가질 수 있는 중요한 기능에 대한 대역폭을 예약할 수 있도록 합니다. 따라서 대역폭이 클수록 덜 중요한 트래픽이 제한되므로 과도한 대역폭을 절약할 수 있습니다.

다음 그림은 각 포트의 Quality of Service 우선 순위 수준 상태를 표시하며, 우선 순위가 높을수록 이 포트의 트래픽이 스위치에서 먼저 처리됨을 의미합니다. 태그가 지정되지 않은 패킷의 경우 스위치는 컨피그레이션에 따라 우선 순위를 할당합니다.

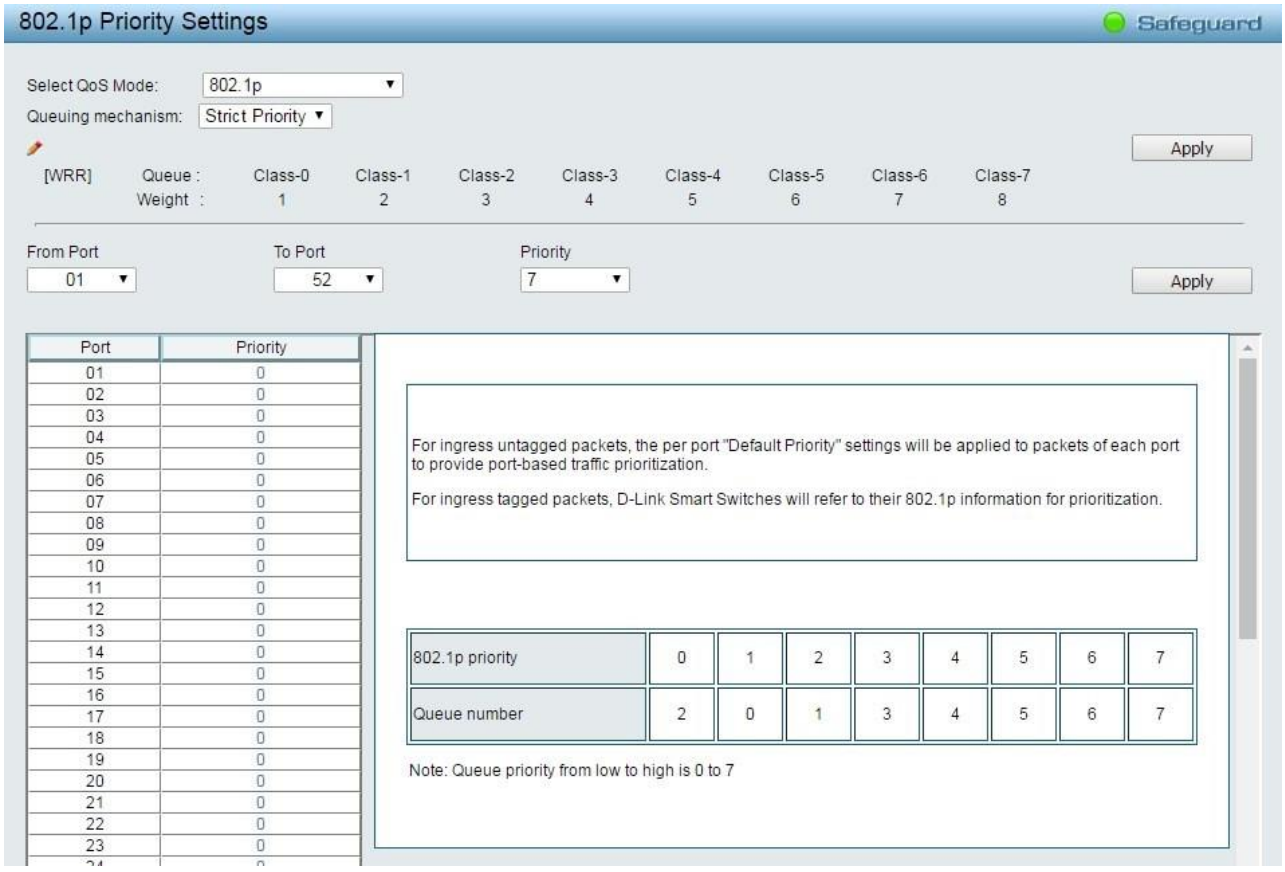


그림 4.108 - QoS > 802.1p/DSCP/ToS

Select QoS Mode: QoS 모드를 802.1p, DSCP 또는 ToS로 지정합니다.

Queuing Mechanism:

Strict Priority: 엄격한 스케줄링을 나타내면 가장 높은 대기열이 먼저 비워지도록 설정하고 다른 대기열은 가중치 기반 라운드 로빈 스케줄링 체계를 따릅니다.

WRR: WRR(Weighted Round-Robin) 알고리즘을 사용하여 우선 순위 서비스 클래스에서 균등하게 배포된

패킷을 처리합니다.

설정을 적용하려면 **Apply(**적용)를 클릭합니다.

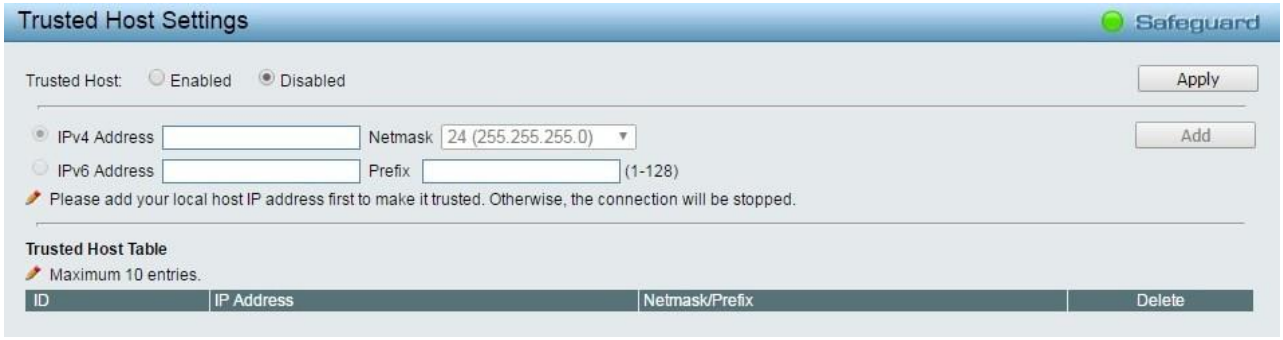
From Port / To Port: 포트 패킷 우선 순위가 정의되는 포트 범위를 정의합니다.

Priority: 포트에 할당된 우선 순위를 정의합니다. 우선 순위 범위는 0에서 7 사이이며 0은 가장 낮은 우선 순위에 할당되고 7은 가장 높은 우선 순위에 할당됩니다.

Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

신뢰할 수 있는 호스트> 보안

신뢰할 수 있는 호스트 기능을 사용하면 사용자가 최대 10개의 지정된 관리 호스트 항목을 지정할 수 있습니다. 항목은 CIDR(Classless Inter-Domain Routing) 주소 형식을 지원하여 사용자가 보다 유연하게 구성할 수 있는 방법을



제공합니다.

그림 4.109 신뢰할 수 있는 호스트 > 보안

신뢰할 수 있는 호스트: 사용하거나 사용하지 않도록 설정할 신뢰할 수 있는 호스트를 지정합니다. 기본값은 비활성화되어 있습니다.

관리 스테이션 IP 설정을 정의하려면 **추가** 버튼을 클릭하고 IP 주소 및 서브넷 마스크를 입력합니다. Apply(**적용**) 버튼을 클릭하여 설정을 저장합니다. CIRD 주소 형식은 다음 표에 표시된 예와 같이 지원됩니다.

IP 주소	서브넷 마스크	허용된 IP
192.168.0.1	255.255.255.0	192.168.0.1~192.168.0.255
172.17.5.215	255.0.0.0	172.0.0.1~172.255.255.255

IP 주소를 삭제하려면 **삭제** 버튼을 클릭하고 원치 않는 주소를 확인한 다음 **Apply**를 클릭하세요.

보안 > 포트 보안

포트 보안은 자동 학습 처리가 네트워크에 액세스하는 것을 중지하기 전에 스위치에 알려지지 않은 인증되지 않은 컴퓨터(소스 MAC 주소 포함)를 방지하는 보안 기능입니다.

포트 잠금이 활성화되면 MAC 주소 전달 테이블에 입력된 현재 소스 MAC 주소를 변경할 수 없도록 지정된 포트(또는 포트 범위)의 동적 MAC 주소 학습을 중지할 수 있습니다. 드롭다운 메뉴를 사용하여 **Admin State(관리 상태)**를 Enabled(활성화)로 변경하고 Max Learning Address(최대 학습 주소)를 입력한 다음 Apply(적용)를 클릭합니다.

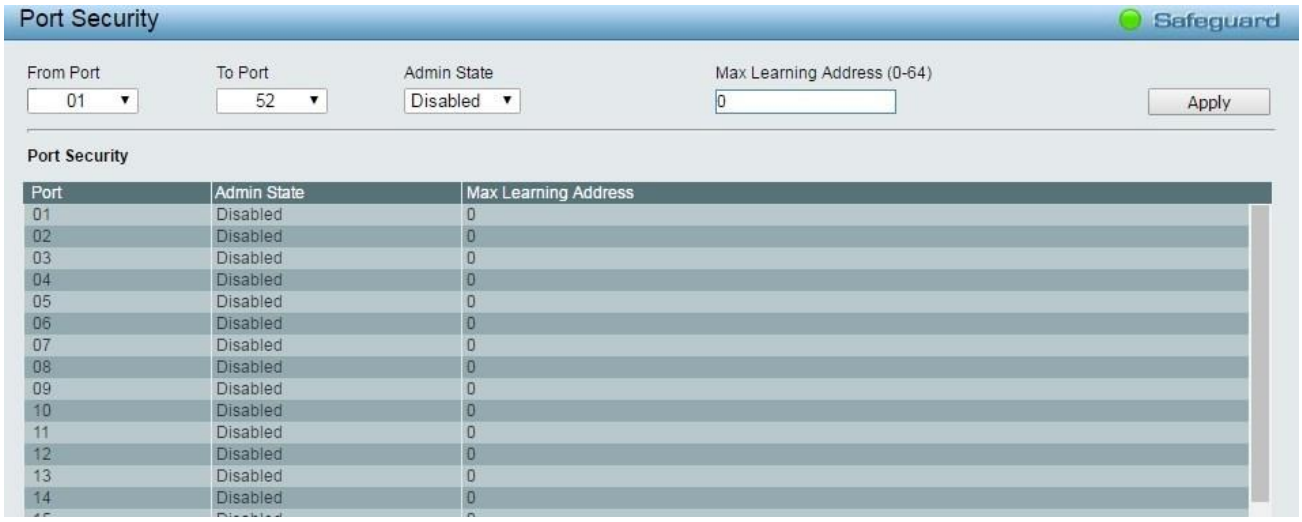


그림 4.110 - 보안 > 포트 보안

보안 > 트래픽 세분화

이 기능을 통해 관리자는 레이어 2 메커니즘의 세그먼트 내에서 트래픽 흐름을 제한할 수 있습니다. 그러나 세그먼트는 VLAN 그룹 장벽을 허물 수 없습니다.

그림 4.111 - 보안 > 트래픽 세분화

Forwarding Port Settings(전달 포트 설정): Enabled(활성화) 또는 Disabled(비활성화)를 선택하고 **Apply(적용)**를 클릭하여 이 기능을 구성합니다.

From Port: 드롭다운 메뉴를 사용하여 해당 스위치에서 포트 또는 모든 포트를 선택합니다. 패킷을 전송할 포트입니다.

To Port: 포트 상자를 클릭하면 패킷을 전달할 수 있습니다. 이러한 포트는 위에서 지정한 포트에서 패킷을 수신할 수 있습니다.

Apply(적용)를 클릭하여 스위치의 **Traffic Segmentation(트래픽 세그멘테이션)** 테이블에 설정을 입력합니다. **Select All** 버튼을 클릭하여 모든 포트를 확인하거나 **Clear** 버튼을 클릭하여 모든 포트를 선택 취소합니다.

보안 > 세이프가드 엔진

D-Link의 **Safeguard Engine** 은 스위치 자체로 들어오는 패킷 플러딩의 영향을 자동으로 제한하는 강력하고 혁신적인 기술입니다. 이 기능은 Web-Smart Switch가 악성 바이러스나 웜 공격에 의해 중단되지 않도록 보호합니다. 이 옵션은

기본적으로 활성화되어 있습니다.

그림 4.112 - 보안 > Safeguard Engine

보안 > 스톰 컨트롤

Storm Control 기능은 브로드캐스트, 멀티캐스트 및 알 수 없는 유니캐스트 패킷의 수신 속도를 제어할 수 있는 기능을 제공합니다. 패킷 스톰이 감지되면 스위치는 스톰이 가라앉을 때까지 스위치로 들어오는 패킷을 드롭합니다.

그림 4.113 - 보안 > 스톰 컨트롤

Storm Control Type: 사용자는 브로드캐스트 전용, 멀티캐스트 및 브로드캐스트, 멀티캐스트 및 브로드캐스트 및 알 수 없는 유니캐스트 중에서 다른 스톰 유형을 선택할 수 있습니다.

Threshold (16Kbps * N): 스톰 제어가 활성화된 경우(기본값은 비활성화되어 있습니다.), 임계값은 초당 16 ~ 1,024,000Kbit이며 단계(N)는 16Kbps입니다. N은 1에서 64000까지일 수 있습니다.

Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

보안 > ARP 스푸핑 방지

ARP 포이즈닝이라고도 하는 ARP 스푸핑은 공격자가 LAN에서 데이터 프레임을 스니핑하거나, 트래픽을 수정하거나, 트래픽을 중지할 수 있도록 하여 이더넷 네트워크를 공격하는 방법입니다(서비스 거부 – DoS 공격이라고 함). ARP 스푸핑의 주요 개념은 가짜 또는 스푸핑된 ARP 메시지를 이더넷 네트워크로 보내는 것입니다. 공격자 또는 임의의 MAC 주소를 기본 게이트웨이와 같은 다른 노드의 IP 주소와 연결합니다. 해당 IP 주소를 대상으로 하는 모든 트래픽은 공격자가 지정한 노드로 실수로 리디렉션됩니다.

오늘날 일반적인 DoS 공격은 존재하지 않거나 지정된 MAC 주소를 네트워크 기본 게이트웨이의 IP 주소에 연결하여 수행할 수 있습니다. 악의적인 공격자는 게이트웨이라고 주장하는 네트워크에 하나의 무상 ARP만 브로드캐스트하면 되므로 인터넷에 대한 모든 패킷이 잘못된 노드로 전달되므로 전체 네트워크 작업이 중단됩니다.

ARP 스푸핑 방지 기능은 불필요한 ARP 패킷을 확인하고 불법 IP 또는 MAC 주소로 필터링하여 네트워크에서 ARP 스푸핑 공격을 폐기할 수 있습니다.

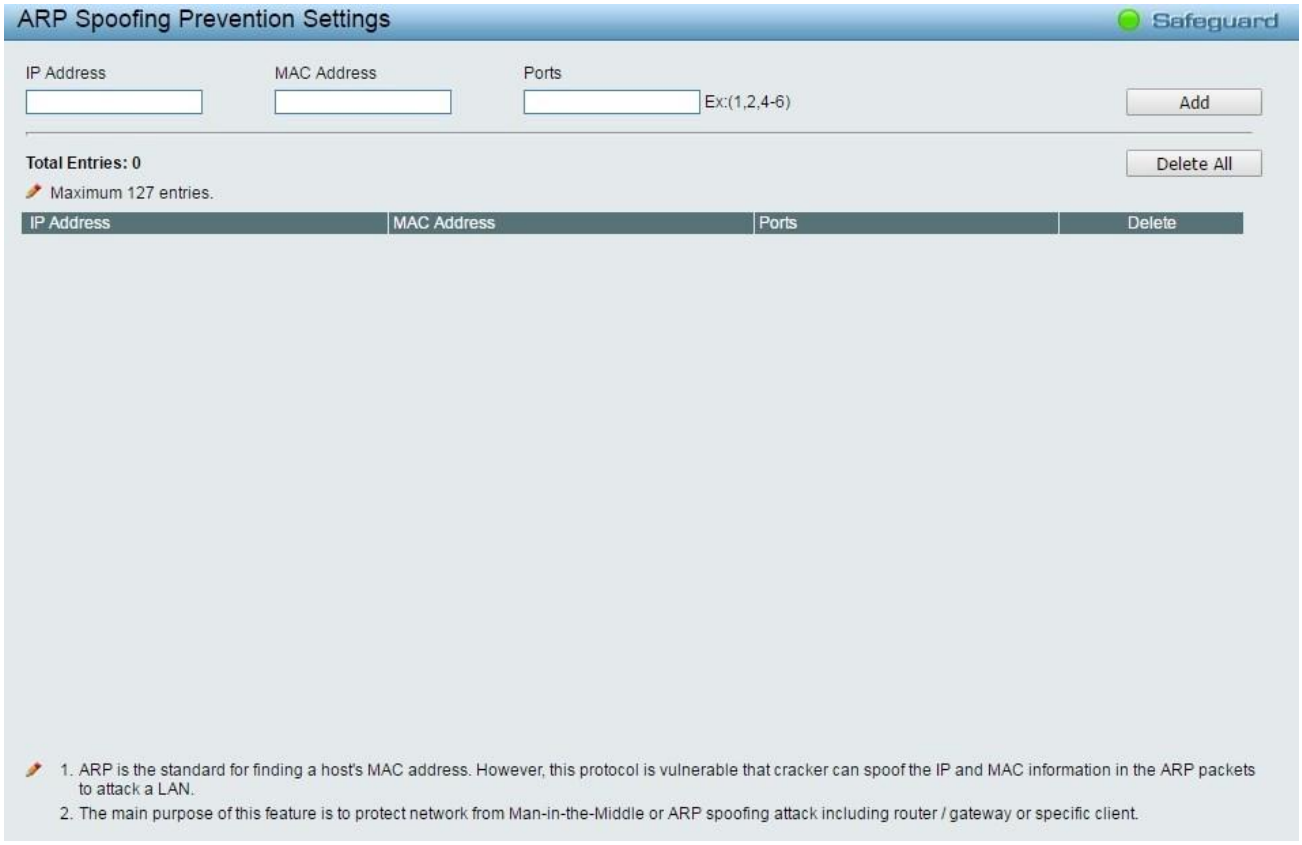


그림 4.114 - 보안 > ARP 스푸핑 방지

IP Address(IP 주소**),** MAC Address(MAC 주소**),** Ports(포트)를 입력한 다음 **Add(추가)**를 클릭하여 확인/필터링 규칙을 생성합니다. 클릭
Delete (삭제)를 선택하여 기존 규칙을 제거하거나 **Delete All(모두 삭제**)을 선택하여 모든 항목을 지웁니다.

보안 > DHCP 서버 스크리닝

DHCP 서버 스크리닝 기능을 사용하면 신뢰할 수 없는 포트에서 DHCP 서비스를 삭제하여 불법 DHCP 서버를 필터링할 수 있습니다. 신뢰할 수 있는 상태로 표시되는 확인된 포트 ID입니다.

그림 4.115 - 보안 > DHCP 서버 스크리닝

Trusted DHCP Server IP Settings: IPv4 및 IPv6 주소는 DHCP 서버 IP로 지원됩니다. 기본적으로 포트는 모두 신뢰할 수 있는 DHCP 서버에서 활성화됩니다.

Add(**추가**)를 클릭하여 신뢰할 수 있는 DHCP 서버를 추가합니다.

SSL/TLS> 보안

SSL(Secure Sockets Layer)은 웹 서버와 액세스 클라이언트 간의 보안 통신 방법을 제공하는 보안 기능입니다. ciphersuite는 인증 세션에 사용할 암호화 매개변수, 암호화 알고리즘 및 키 크기를 결정하는 보안 문자열로, 키 교환, 암호화 및 알고리즘의 세 가지 수준으로 구성됩니다.

DGS-1210 시리즈는 업계의 보안 요구 사항을 대부분 충족하는 최신 TLS 1.3 버전을 지원합니다. 이 페이지에서는 사용자가 SSL 전역 상태 및 Ciphersuite 설정을 구성할 수 있습니다. **Enable(활성화**) 또는 **Disable(비활성화**)을 선택한 다음 **Apply**(적용)를 클릭하여 스위치의 SSL 상태 또는 Ciphersuite 설정을 변경합니다. SSL 상태는 기본적으로 **Disabled**입니다.

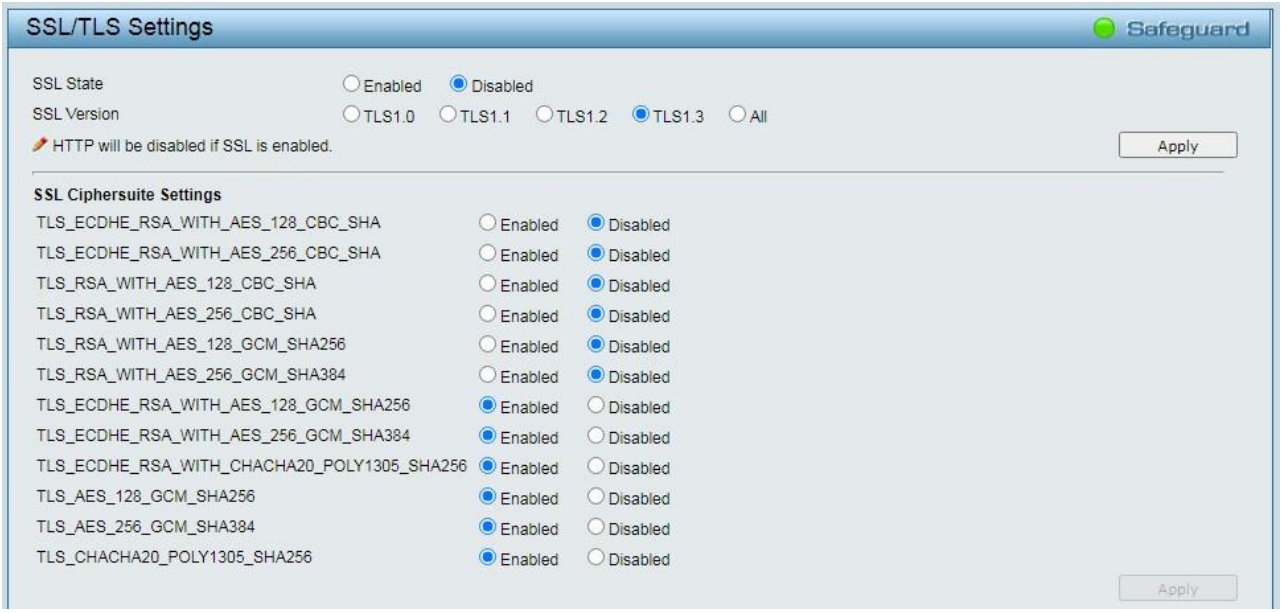


그림 4.116 - SSL/TLS > 보안

참고: SSL이 활성화되면 암호화로 인해 웹 페이지를 여는 데 시간이 더 오래 걸리고 HTTP가 비활성화됩니다.

아래에 나열된 SSL 프로토콜의 버전:

버전	묘사
SSL 버전 2.0	구현이 존재하는 첫 번째 SSL 프로토콜입니다.
SSL 버전 3.0	특정 보안 공격을 방지하기 위한 수정 버전에는 RSA가 아닌 암호가 추가되고 인증서 체인에 대한 지원이 추가됩니다.
TLS 버전 1.0	SSL 3.0 개정으로 MAC 계층을 HMAC로 업데이트하고, 블록 암호에 대한 블록 패딩을 추가하고, 메시지 순서 표준화 및 더 많은 경고 메시지를 추가합니다.
TLS 버전 1.1	CBC(Cipher Block Changing) 공격에 대한 보호 메커니즘입니다.
TLS 버전 1.2	TLS 1.2의 주요 목표 중 하나는 MD5 및 SHA-1 다이제스트 알고리즘에 대한 종속성을 제거하는 것이었습니다.
TLS 버전 1.3	더 빠른 TLS 핸드셰이크와 더 안전한 암호 그룹.

참고: DGS-1210 시리즈는 TLS 1.3, 1.2, 1.1을 지원하며 SSL v3.0을 지원하지 않습니다.

SSL(Secure Sockets Layer)은 대부분의 인터넷 커뮤니티에서 선택하는 보안 통신 프로토콜입니다. SSL은 TCP를 통한 모든 전송을 보호할 수 있기 때문에 SSL의 많은 응용 프로그램이 존재합니다.

TLS(전송 계층 보안)는 SSL의 후속 제품이며 거의 동일한 기능을 제공합니다. 통신하는 응용 프로그램과 인터넷 사용자 간의 개인 정보를 보장합니다. 서버와 클라이언트가 통신할 때 TLS는 제3자가 메시지를 도청하거나 변조할 수 없도록 합니다.

HTTPS(Hyper Text Transfer Protocol Secure)는 기밀 정보를 보호하고 암호화 및 인증을 강화하며 SSL/TLS를 기반으로 실행되는 데 자주 사용되는 HTTP의 보안 버전입니다. HTTPS는 브라우저와 웹 서버 간의 웹 브라우징 서비스를 보호하는 데 사용됩니다.

고도의 암호화 및 인증을 통해 HTTPS를 통해 웹을 탐색하려면 **Enabled**를 선택하고 Apply(적용)를 클릭합니다 버튼을 눌러 SSL 상태를 활성화하고 HTTP가 비활성화됩니다.

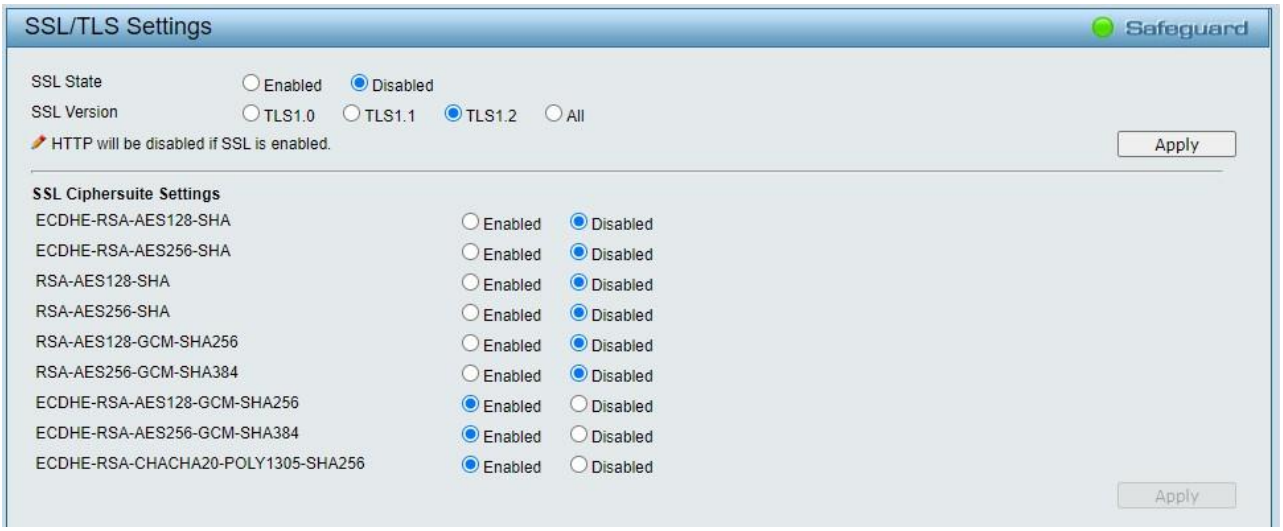
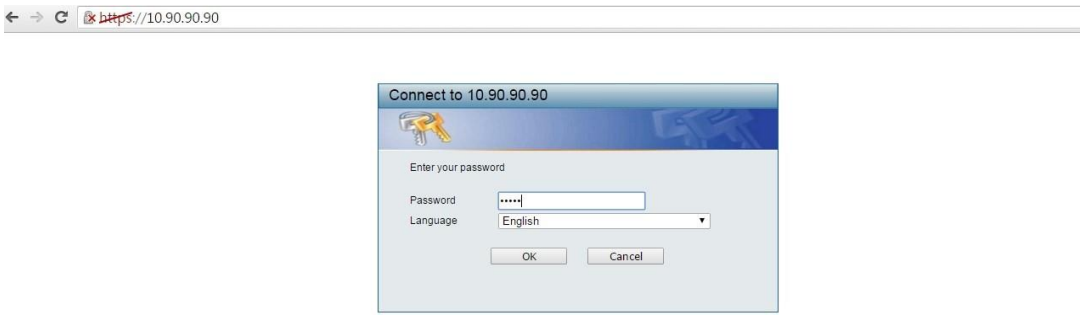


그림 4.117 - 보안 > SSL 설정 - 활성화

SSL 암호 그룹:

사이퍼슈트	키 교환/인증	암호화	비트 길이
ECDHE-RSA-AES128-샤	증권 시세 표시기/RSA	AES (에이에스)	128
ECDHE-RSA-AES256-샤	증권 시세 표시기/RSA	AES (에이에스)	256
RSA-AES128-샤	증권 시세 표시기	AES (에이에스)	128
RSA-AES256-SHA를 참조하십시오.	증권 시세 표시기	AES (에이에스)	256
RSA-AES128-GCM-SHA256	증권 시세 표시기	AES (에이에스)	128
RSA-AES256-GCM-SHA384	증권 시세 표시기	AES (에이에스)	256
ECDHE-RSA-AES128-GCM-SHA256	증권 시세 표시기/RSA	AES (에이에스)	128
ECDHE-RSA-AES256-GCM-SHA384	증권 시세 표시기/RSA	AES (에이에스)	256
ECDHE-RSA-CHACHA20-POLY1305-SHA256	증권 시세 표시기/RSA	ChaCha 스트림 암호 및 Poly1305 인증자	256



https://10.90.90.90 입력하여 웹 관리 페이지에 다시 로그인합니다.

그림 4.118 - 보안 > SSL 설정 - HTTPS 활성화

보안 > DoS 방지 설정

사용자는 각 DoS 공격의 방지를 활성화하거나 비활성화할 수 있습니다. 사용자가 DoS 방지를 활성화하는 한, 스위치는 아래 표에 나열된 DoS Attachk 방지 유형과 일치하는 패킷을 중지할 수 있습니다. 패킷 매칭은 하드웨어에 의해 수행됩니다.

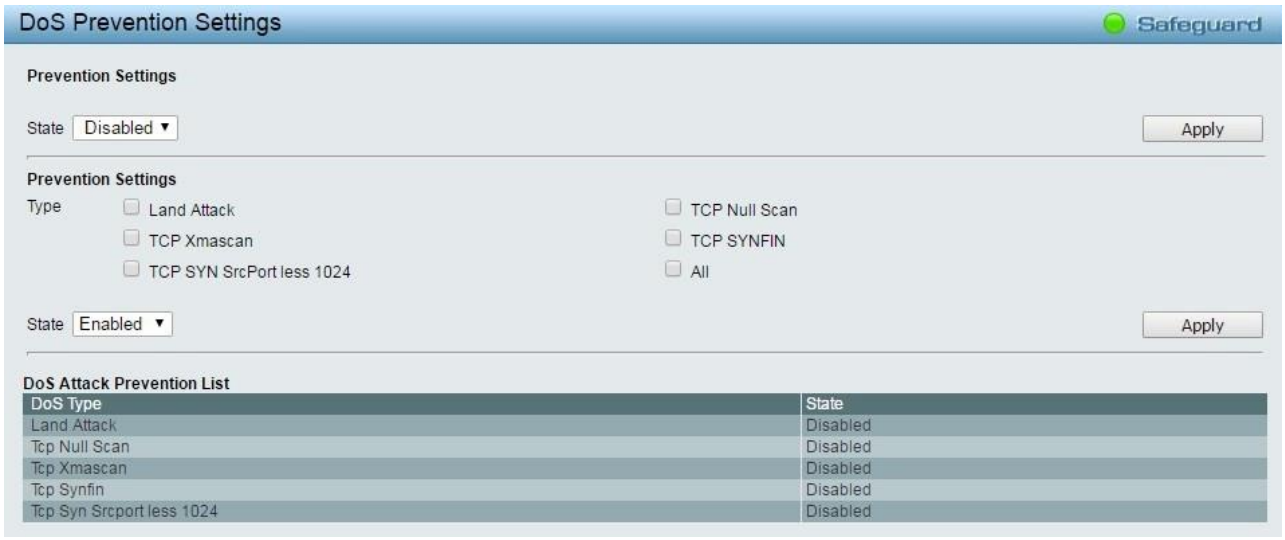


그림 4.119 - DoS 방지 설정 > 보안

State: 사용하거나 사용하지 않도록 설정할 상태를 지정합니다. **Apply(적용)**를 클릭하여 변경 사항을 적용합니다.

Prevention Settings:

Type: 차단할 공격 유형을 선택합니다. 유형은 *Land Attack, TCP Null Scan, TCP Xmascan, TCP SYNFIN, TCP SYN, SrcPortless 1024* 또는 *All*입니다.

State: 사용하거나 사용하지 않도록 설정할 상태를 지정합니다. Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

SSH > SSH 설정을 > 보안

SSH는 Secure Shell의 약자로, 엔드포인트 호스트 간에 보안 및 암호화된 연결을 설정할 수 있습니다. SSH는 네트워크 관리자에게 더 높은 수준의 보안을 제공하는 일반 텍스트 전송(텔넷)보다 안전한 방법입니다.

그림 4.120 - 보안 > SSH > SSH 설정

스위치에서 SSH 서버를 구성하려면 다음 매개변수를 수정하고 Apply(적용)를 클릭합니다 .

SSH State: 스위치에서 SSH 활성화 또는 비활성화. 기본값은 비활성화되어 있습니다..

Max Session (1 - 4): 1 에서 4 *사이의 값을 입력하여* 동시에 스위치에 액세스할 수 있는 사용자 수를 설정합니다. 기본 설정은 *1입니다*.

Connection Timeout (120 - 600): 사용자가 연결 시간 제한을 설정할 수 있습니다. 사용은 *120* 초에서 *600* 초 사이의 시간을 설정할 수 있습니다. 기본 설정은 *120*초입니다.

Authfail Attempts (2 - 20): 관리자가 SSH 인증을 사용하여 SSH 서버에 로그온을 시도할 수 있는 최대 시도 횟수를 설정할 수 있습니다. 최대 시도 횟수를 초과하면 스위치의 연결이 끊어지고 사용자는 다른 로그인을 시도하려면 스위치에 다시 연결해야 합니다. 최대 시도 횟수는 *2 에서*20 사이로 설정할 수 *있습니다*. 기본 설정은 *2입니다*.

Rekey Timeout (키 키 시간 초과): 풀다운 메뉴를 사용하면 이 필드를 사용하여 스위치가 보안 셸 암호화를 변경하는 기간을 설정합니다. 사용 가능한 옵션은 *사용 안 함*, *10분*, *30분* 및 *60분입니다.* 기본 설정은 *60분입니다.*

Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

보안 > SSH > SSH 인증 모드 및 알고리즘 설정

SSH Authentication and Algorithm Settings(SSH 인증 및 알고리즘 설정) 페이지에서는 인증 암호화에 사용되는 원하는 유형의 SSH 알고리즘을 구성할 수 있습니다.

그림 4.121 - 보안 > SSH > SSH 설정

SSH Authentication Mode Settings:

Password(비밀번호): 사용자가 스위치에서 인증을 위해 로컬로 구성된 비밀번호를 사용할 수 있습니다.

Public Key: 관리자가 스위치에서 인증을 위해 SSH 서버에 설정된 공개 키 구성을 사용하려는 경우 이 매개변수를 활성화할 수 있습니다.

Host Based(호스트 기반): 관리자가 인증을 위해 호스트 컴퓨터를 사용하려는 경우 이 매개 변수를 사용하도록 설정할 수 있습니다. 이 매개변수는 SSH 인증 기술이 필요한 Linux 사용자를 위한 것이며 호스트 컴퓨터는 이전에 SSH 프로그램이 설치된 Linux 운영 체제를 실행하고 있습니다.

암호화 알고리즘:

3DES-CBC: 이 확인란을 사용하여 Cipher Block Chaining을 사용하는 Triple Data Encryption Standard 암호화 알고리즘을 활성화하거나 비활성화합니다. 기본값은 사용입니다.

Data Integrity Algorithm:

HMAC-MD5: 메시지 인증 코드(HMAC) MD5 메시지 다이제스트(MD5) 메커니즘에 대한 해시 지원을 활성화하려면 확인란을 사용합니다.

HMAC-SHA1: 메시지 인증 코드(HMAC) 보안 해시 알고리즘(SHA) 메커니즘에 대한 해시 지원을 활성화하려면 확인란을 사용합니다.

Public Key Algorithm:

HMAC-RSA: RSA 암호화 알고리즘을 사용하여 HMAC(Hash for Message Authentication Code) 메커니즘을 지원하도록 설정하려면 확인란을 사용합니다.

Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

보안 > SSH > SSH 사용자 인증 목록

SSH User Authentication Lists(SSH 사용자 인증 목록) 페이지는 SSH를 통해 스위치에 액세스하려는 사용자에 대한 매개변수를 구성하는 데 사용됩니다.

그림 4.122 - 보안 > SSH > SSH 사용자 인증 목록

사용자는 다음 매개 변수를 볼 수 있습니다.

User Name: SSH 사용자를 식별하기 위한 15자 이하의 이름입니다. 이 사용자 이름은 스위치에서 이전에 구성한 사용자 계정이어야 합니다.

Auth. Mode: 관리자는 다음 중 하나를 선택하여 스위치에 액세스하려는 사용자에 대한 권한을 설정할 수 있습니다.

> **Host Based(호스트 기반)** - 관리자가 인증 목적으로 원격 SSH 서버를 사용하려는 경우 이 매개변수를 선택해야 합니다.
>
> **Password(비밀번호)** – 관리자가 인증에 관리자가 정의한 비밀번호를 사용하려는 경우 이 매개변수를 선택해야 합니다. 이 매개변수를 입력하면 스위치는 관리자에게 암호를 묻는 메시지를 표시한 다음 확인을 위해 암호를 다시 입력하라는 메시지를 표시합니다.
>
> **Public Key** – 관리자가 인증을 위해 SSH 서버의 공개 키를 사용하려는 경우 이 매개 변수를 선택해야 합니다.

Host Name: 원격 SSH 사용자를 식별하기 위해 32 자 *이하의 영숫자 문자열을 입력합니다*. 이 매개변수는 *Auth. Mode 필드의* Host Based 선택과 함께만 사용됩니다.

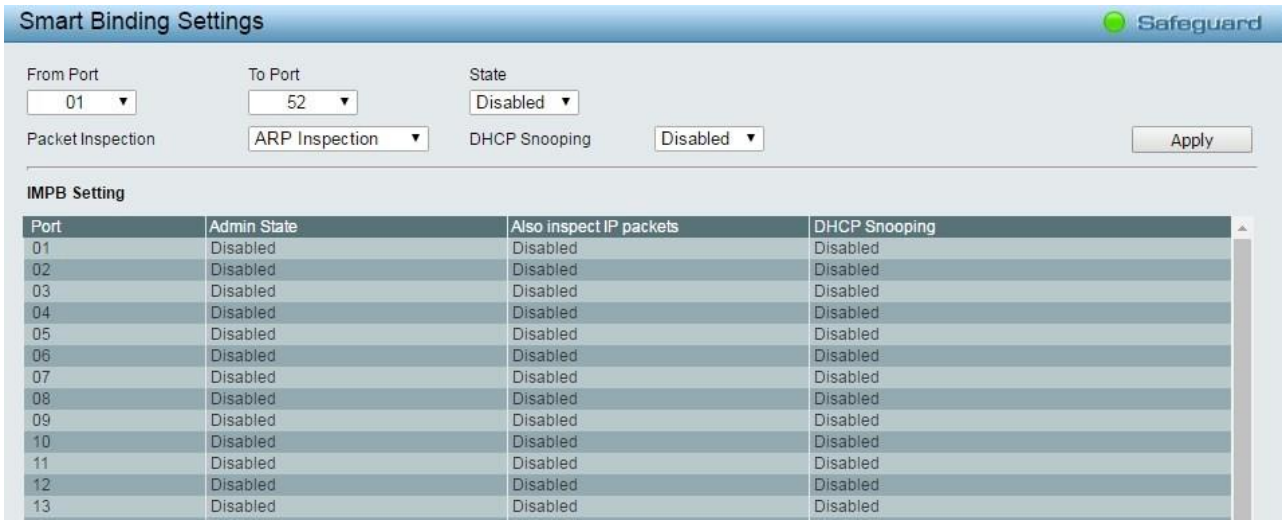
Host IPv4: SSH 사용자의 해당 IPv4 주소를 입력합니다. 이 매개변수는 *Auth. Mode 필드의* Host Based 선택과 함께만 사용됩니다.

Host IPv6: SSH 사용자의 해당 IPv6 주소를 입력합니다. 이 매개변수는 *Auth. Mode 필드의* Host Based 선택과 함께만 사용됩니다.

보안 > 스마트 바인딩 > 스마트 바인딩 설정

스마트 바인딩의 주요 목적은 관리자가 스위치를 통해 네트워크에 액세스할 수 있는 클라이언트 MAC 및 IP 주소 쌍을 구성할 수 있도록 하여 스위치에 대한 클라이언트 액세스를 제한하는 것입니다.

Smart Binding 기능은 포트 기반이므로 사용자가 개별 포트에서 기능을 활성화하거나 비활성화할 수 있습니다. 스위치 포트에서 스마트 바인딩이 활성화되면 스위치는 "IMPB 화이트 리스트"라고도 하는 사전 구성된 데이터베이스로 IP-MAC 주소 쌍을 확인하여 클라이언트 액세스를 제한하거나 허용합니다.



사용자는 스위치에서 **검사 패킷** 및 **DHCP 스누핑**을 활성화하거나 비활성화할 수 있습니다.

그림 4.123 - 보안 > 스마트 바인딩 > 스마트 바인딩 설정

Smart Binding Settings 페이지에는 다음 필드가 있습니다.

From Port/ To Port: IP-MAC-포트 바인딩을 위해 설정할 포트 범위를 선택합니다.

State: 드롭다운 메뉴를 사용하여 스마트 바인딩에 대해 이러한 포트를 활성화하거나 비활성화합니다.

Enabled(활성화) – 포트에 대한 관련 구성을 사용하여 Smart Binding을 활성화합니다.

Disabled(비활성화됨) – 스마트 바인딩을 비활성화합니다.

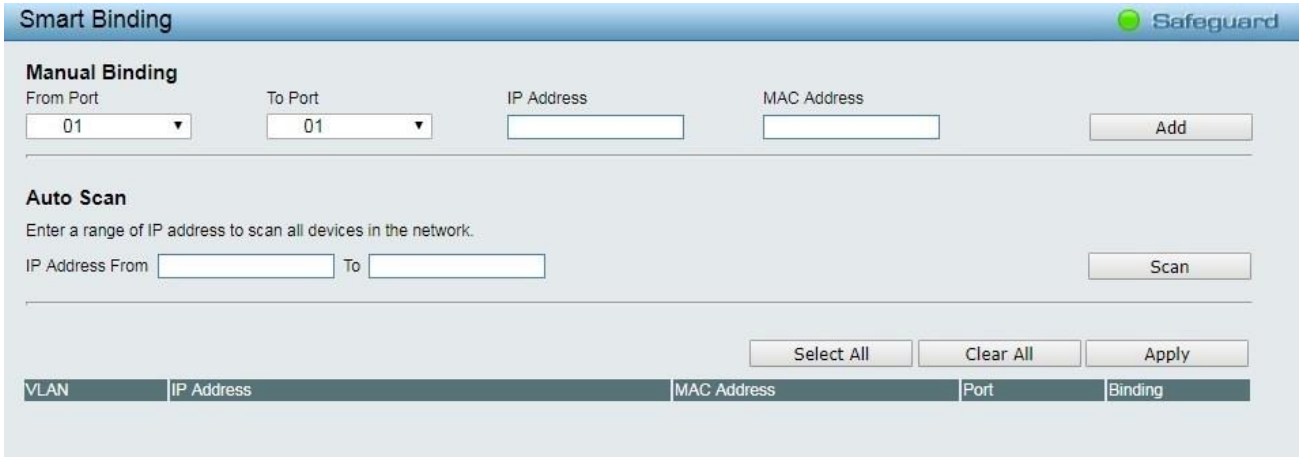
Packet Inspection: IP 패킷에 대한 *ARP 검사* 또는 *IP+ARP 검사를* 지정합니다. ARP 검사를 선택한 경우 스위치는 수신 ARP 패킷을 검사하고 이를 스위치의 스마트 바인딩 화이트 목록 항목과 비교합니다. ARP 패킷의 IP-MAC 쌍이 화이트리스트에서 발견되지 않으면 스위치는 MAC 주소를 차단합니다. 느슨한 상태의 주요 이점은 CPU 리소스를 덜 사용한다는 것입니다. 그러나 유니캐스트 IP 패킷만 보내는 악의적인 사용자는 차단할 수 없습니다. 예를 들어 악의적인 사용자는 PC에서 ARP 테이블을 정적으로 구성하여 DoS 공격을 수행할 수 있습니다. 이 경우 PC는 ARP 패킷을 전송하지 않으므로 스위치는 이러한 공격을 차단할 수 없습니다. **ARP+ IP 검사** 모드를 선택한 경우 스위치는 모든 수신 ARP 및 IP 패킷을 검사하고 IMPB 화이트리스트와 비교합니다. IP-MAC 쌍의 경우 화이트리스트에서 일치하는 항목을 찾으면 해당 MAC 주소의 패킷이 차단 해제됩니다. 그렇지 않은 경우 MAC 주소는 차단된 상태로 유지됩니다. 이 모드는 모든 인그레스 ARP 및 IP 패킷을 검사하지만 더 나은 보안을 적용합니다.

DHCP Snooping: DHCP 스누핑을 활성화하면 스위치가 DHCP 서버 및 클라이언트에서 보낸 패킷을 스누핑하고 정보를 화이트리스트에 업데이트합니다. 여기에는 DHCPv6 스누핑이 포함됩니다.

Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

보안 > 스마트 바인딩 > 스마트 바인딩

스마트 바인딩 설정 페이지에서는 사용자가 필요한 정보를 수동으로 입력하거나 연결된 모든 장치를 스캔하고 바인딩을



클릭하여 IP-MAC-포트 바인딩 항목을 설정할 수 있습니다.

그림 4.124 - 보안 > 스마트 바인딩 > 스마트 바인딩

Manual Binding Settings에는 다음 필드가 포함되어 있습니다.

From Port / To Port: 이 IP-MAC 바인딩 항목(IP 주소 + MAC 주소)을 구성할 스위치 포트 범위를 지정합니다.

IP Address: 아래에 설정된 MAC 주소에 바인딩할 IP 주소를 지정합니다. **MAC 주소:**
위에서 설정한 IP 주소에 바인딩할 MAC 주소를 지정합니다. **추가** 를 클릭하여 새 항목을
추가합니다.

Auto Scan: 자동 스캔 설정은 연결된 장치를 나열하고 바인딩을 쉽게 선택할 수 있습니다. 여기에는 다음 필드가 포함되어 있습니다.

IP Address From/To: 원하는 장치를 찾기 위한 IP 주소 범위를 지정하거나 연결된 모든 장치를 보려면 필드를 비워 둡니다.

Scan을 클릭하면 검색 결과가 아래 표와 같이 나열됩니다.

Binding: 확인란을 선택하여 원하는 바인딩 장치를 선택합니다.
Apply: 적용을 클릭하여 IP-MAC-포트 바인딩 항목을 설정합니다."
Select All(모두 선택): 검색된 모든 장치에 대한 바인딩 상자를
선택합니다.

Clear All: 바인딩 상자를 취소합니다.

보안 > 스마트 바인딩 > 화이트리스트

"IP + ARP 검사" 모드를 선택하면 화이트 목록 페이지에 스마트 바인딩 페이지에서 완료된 IP-MAC-포트 바인딩 항목이 표시됩니다. 일치하는 IP-MAC-Port 정보를 전달하는 IP 패킷 또는 ARP 패킷만 스위치에 액세스할 수 있습니다. 필요한 경우 화이트리스트 항목을 삭제할 수 있습니다.

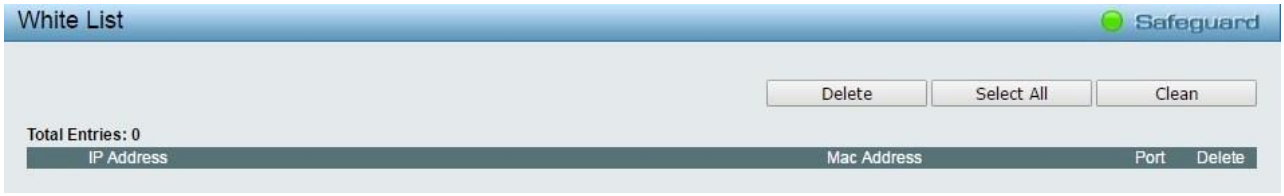


그림 4.125 - 보안 > 스마트 바인딩 > 화이트리스트

항목의 확인란을 선택한 다음 **Delete**를 클릭하여 제거합니다.

모두 선택(Select All)을 클릭하여 테이블의 모든 항목을 선택하거나 정리(**Clean**)를 클릭하여 항목을 선택하지 않습니다. 하나 이상의 관리 호스트를 화이트 리스트에 유지하십시오.

보안 > 스마트 바인딩 > 블랙리스트

블랙 리스트 페이지에는 무단 액세스가 표시됩니다. ARP Inspection(ARP 검사)을 선택하고 디바이스가 일치하지 않는 IP-MAC-Port 정보가 포함된 ARP 패킷을 전송하면 디바이스가 금지되고 여기에 나열됩니다.

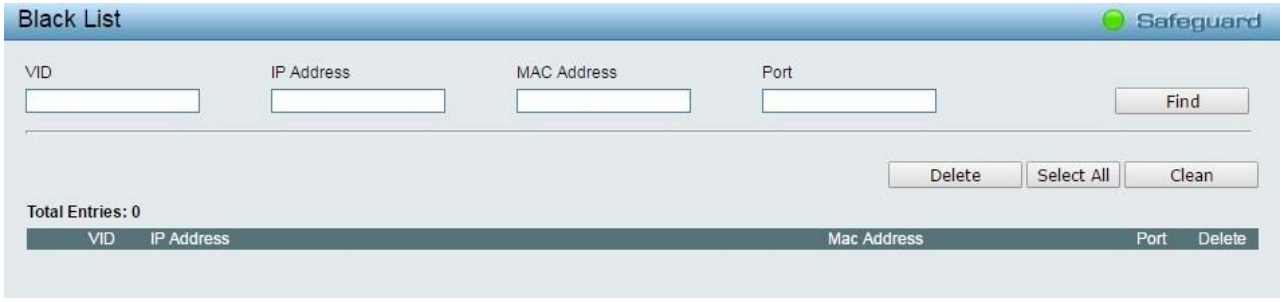


그림 4.126 - 보안 > 스마트 바인딩 > 블랙리스트

조건을 제공하면 아래에서 원하는 장치 정보를 선별한 다음 찾기를 클릭하여 항목 목록을 검색할 수 있습니다.

VID: 장치의 VLAN ID 번호를 입력합니다.

IP Address: 장치의 IP 주소를 입력합니다.

MAC Address: 장치의 MAC 주소를 입력합니다.

Port: 장치가 연결되는 포트 번호를 입력합니다.

Delete column(삭제 열) 상자를 선택하여 금지된 목록에서 항목을 해제한 다음 **Apply(적용**)를 클릭하여 목록에서 항목을 삭제합니다.

Select All(모두 선택)을 클릭하여 모든 항목을 선택하거나 **Clean(정리**)을 클릭하여 항목을 선택하지 않습니다

AAA > RADIUS 서버

스위치의 RUAIUS 서버를 통해 사용자는 중앙 집중식 사용자 관리를 용이하게 할 수 있을 뿐만 아니라 스니핑하는 활성 해커에 대한 보호를 제공할 수 있습니다.

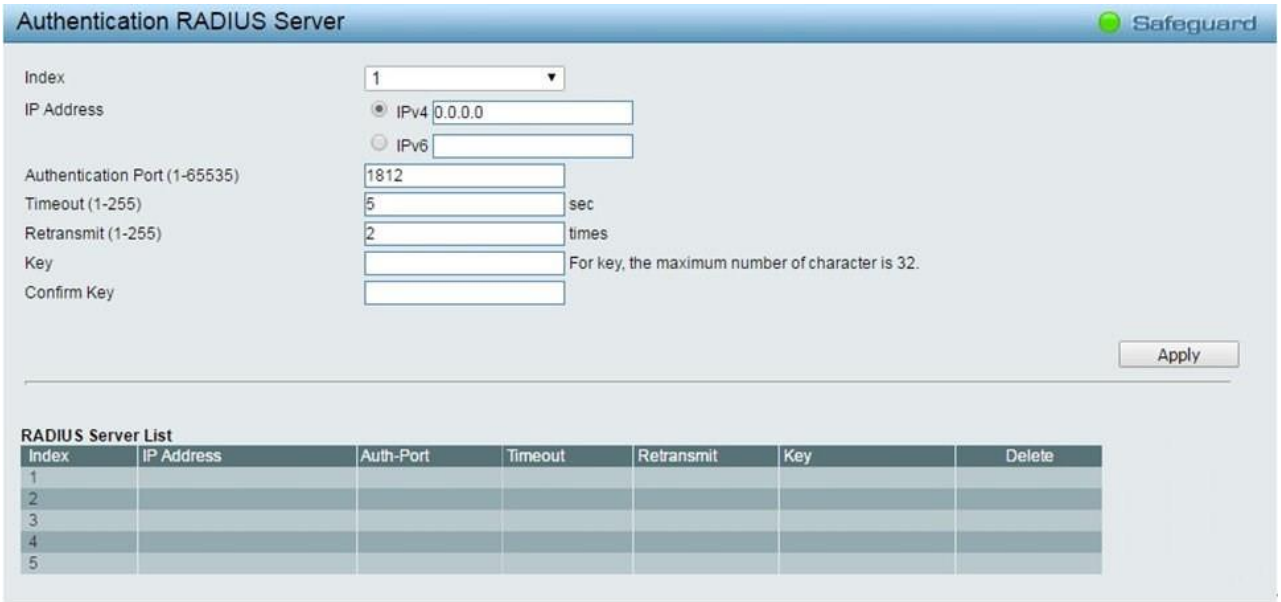


그림 4.127 - AAA > RADIUS 서버

Index: 구성할 RADIUS 서버(1, 2 또는 3)를 선택합니다. 사용자는 최대 5개의 RADIUS 서버를 생성할 수 있습니다.

IP Address: IPv4 또는 IPv6을 선택하고 IP 주소를 입력합니다.

Authentication Port (1 - 65535): RADIUS 인증 서버 UDP 포트를 설정합니다. 기본 포트는 1812입니다.

Timeout (1 – 255초): 이 필드는 스위치가 사용자의 인증 응답을 기다리는 시간을 설정합니다. 사용자는 *1* 초에서 *255* 초 사이의 시간을 설정할 수 있습니다. 기본 설정은 *5*초입니다.

Retransmit (1 – 255회): 이 명령은 스위치가 인증 시도를 수락하는 최대 횟수를 구성합니다. 설정된 시도 횟수 후에 인증에 실패한 사용자는 스위치에 대한 액세스가 거부되고 추가 인증 시도가 잠깁니다. 명령줄 인터페이스 사용자는 다른 인증을 시도하기 전에 60초 동안 기다려야 합니다. 텔넷 및 웹 사용자는 스위치에서 연결이 끊어집니다. 사용자는 1 에서 *255*까지 시도 횟수를 설정할 수 있습니다. 기본 설정은 *2입니다*.

Key: RADIUS 서버의 키와 동일하게 키를 설정합니다.

Confirm Key(키 확인): 공유 키가 RADIUS 서버의 키와 동일한지 확인합니다.
Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

AAA > 802.1X > 802.1X 전역 설정

네트워크 스위치는 클라이언트 PC를 연결하기만 하면 리소스에 대한 쉽고 개방적인 액세스를 제공합니다. 불행히도 이 자동 구성을 사용하면 권한이 없는 사람이 민감한 데이터에 쉽게 침입하여 액세스할 수 있습니다.

IEEE-802.1X는 특히 Wi-Fi 무선 네트워크에서 네트워크 액세스 제어를 위한 보안 표준을 제공합니다. 802.1X는 인증이 완료될 때까지 네트워크 포트를 끊은 상태로 유지합니다. 스위치는 EAPOL(Extensible Authentication Protocol over LANs)을 사용하여 인증 프로토콜 클라이언트 ID(예: 사용자 이름)를 클라이언트와 교환하고 다른 원격 RADIUS 인증 서버로 전달하여 액세스 권한을 확인합니다. RADIUS 서버의 EAP 패킷에는 사용할 인증 방법도 포함되어 있습니다. 클라이언트는 클라이언트 소프트웨어 및 RADIUS 서버의 구성에 따라 인증 방법을 거부하고 다른 방법을 요청할 수 있습니다. 인증된 결과에 따라 사용자가 포트를 사용할 수 있게 되거나 사용자가 네트워크에 대한 액세스를 거부합니다.

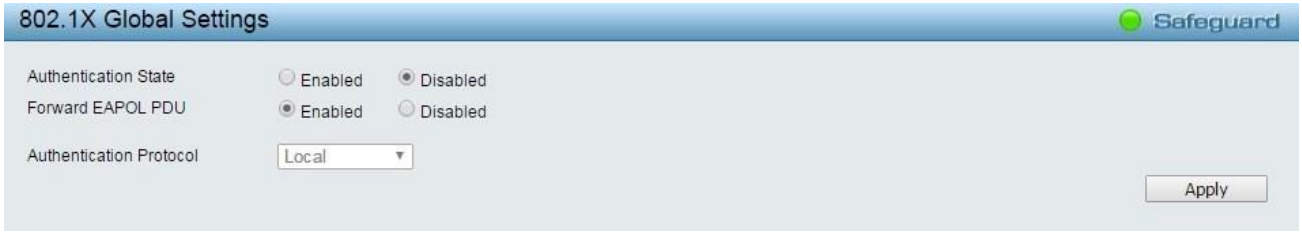


그림 4.128 - AAA > 802.1X 전역 설정

Authentication State: 802.1X 기능을 활성화하거나 비활성화하도록 지정합니다.

Forward EAPOL PDU: EAPOL PDU 의 전달을 제어하는 전역 설정입니다. 802.1X 기능이 전역적으로 또는 포트에 대해 비활성화되고 802.1X 전달 PDU가 전역 및 포트에 대해 모두 활성화된 경우, 포트에서 수신된 EAPOL 패킷은 동일한 VLAN에서 802.1X 전달 PDU가 활성화되고 802.1X가 비활성화된 포트(전역적으로 또는 포트에만 해당)로 플러딩됩니다. 기본 상태는 disabled입니다.

Authentication Protocol: 장치에서 802.1X 프로토콜을 나타냅니다. 가능한 필드 값은 로컬 및 RADIUS입니다.

Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

AAA > 802.1X > 802.1X 포트 설정

보안을 위해 EAP를 사용하려면 Radius 서버에 대한 802.1X 포트 설정 및 해당 인증 정보를 설정합니다.

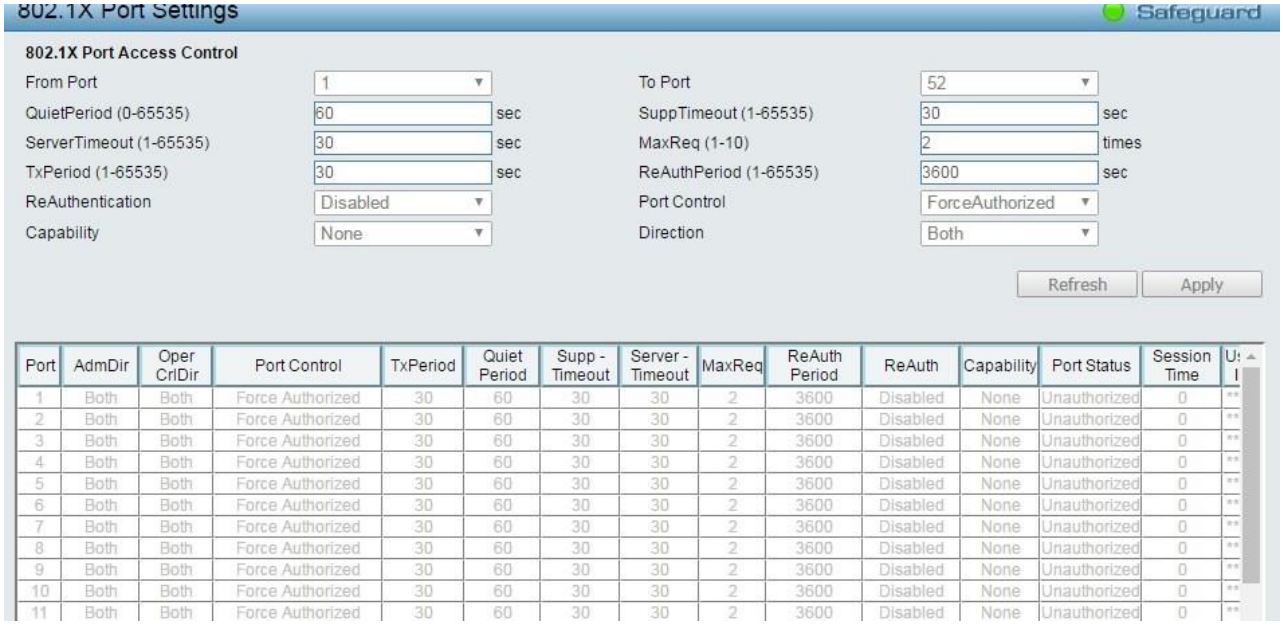


그림 4.129 - AAA > 802.1X > 802.1X 포트 설정

From Port/To Port: 설정할 포트를 입력합니다.

QuietPeriod(0 – 65535초): 클라이언트와의 인증 교환에 실패한 후 스위치가 조용한 상태로 유지되는 시간(초)을 설정합니다. 기본값은 *60* 초입니다.

ServerTimeout(1 – 65535초): 스위치가 인증 서버에 응답을 다시 보내기 전에 클라이언트의 응답을 기다리는 시간을 설정합니다. 기본값은 *30* 초입니다.

TxPeriod(1 – 65535초): 인증자 PAE 상태 시스템의 TxPeriod를 설정합니다. 이 값은 클라이언트로 전송되는 EAP 요청/ID 패킷의 기간을 결정합니다. 기본값은 *30* 초입니다.

ReAuthentication: 이 포트에서 정기적인 재인증이 수행되는지 여부를 결정합니다. 기본 설정은 *사용 안 함입니다*.

Capability: 802.1X의 기능을 나타냅니다. 가능한 필드 값은 다음과 같습니다.

Authenticator(인증자) – 포트별로 적용할 Authenticator 설정을 지정합니다. **없음 –** 포트에서 802.1X 기능을 비활성화합니다.

SuppTimeout(1 – 65535초): 이 값은 인증자와 클라이언트 간의 교환에서 시간 초과 조건을 결정합니다. 기본값은 *30* 초입니다.

MaxReq(1 – 10): 이 매개변수는 인증 세션이 시간 초과되기 전에 스위치가 EAP 요청(md-5challnege)을 클라이언트로 재전송하는 최대 횟수를 지정합니다. 기본값은 *2* 회입니다.

ReAuthPeriod(1 – 65535초): 클라이언트의 주기적 재인증 사이의 0이 아닌 시간(초)을 정의하는 상수입니다. 기본 설정은 *3600* 초입니다.

Port Control: 이를 통해 사용자는 포트 권한 부여 상태를 제어할 수 있습니다.

ForceAuthorized 를 선택하여 802.1X를 비활성화하고 인증 교환 없이 포트가 인증된 상태로 전환되도록 합니다. 즉, 포트는 클라이언트의 802.1X 기반 인증 없이 일반 트래픽을 전송하고 수신합니다.

ForceUnauthorized 를 선택하면 포트가 무단 상태로 유지되어 클라이언트의 모든 인증 시도를 무시합니다. 스위치는 인터페이스를 통해 클라이언트에 인증 서비스를 제공할 수 없습니다.

Auto(자동)를 선택하면 802.1X가 활성화되고 포트가 무단 상태로 시작되어 EAPOL 프레임만 포트를 통해 보내고 받을 수 있습니다. 인증 프로세스는 포트의 링크 상태가 다운에서 업으로 전환되거나 EAPOL-start 프레임이 수신될 때 시작됩니다. 그런 다음 스위치는 클라이언트의 ID를 요청하고 클라이언트와 인증 서버 간에 인증 메시지를 릴레이하기 시작합니다.

기본 설정은 *자동입니다*.

Direction: 포트에서 관리 제어 방향을 설정합니다. 가능한 필드 값은 다음과 같습니다.

Both – 첫 번째 필드에서 선택한 제어된 포트를 통해 들어오는 트래픽과 나가는 트래픽 모두에 대해 제어가 수행되도록 지정합니다.

In – 현재 펌웨어 릴리스에서 지원을 비활성화합니다.

Apply (적용) 버튼을 클릭하여 변경 사항을 적용합니다.

AAA > 802.1X > 802.1X 사용자

802.1X User 페이지에서는 사용자가 스위치에서 다른 로컬 사용자를 설정할 수 있습니다. **802.1X User** 이름을 입력합니다.

Password(비밀번호) 및 **Confirm Password(비밀번호 확인)**를 클릭합니다. 올바르게 구성된 로컬 사용자가 테이블에 표시됩니다.

그림 4.130 - AAA > 802.1X > 802.1X 사용자

Add를 클릭하여 새 802.1X 사용자를 추가합니다.

AAA > 802.1X > 802.1X 게스트 VLAN

802.1X Guest VLAN 은 802.1X를 통해 인증에 실패한 포트를 게스트 VLAN 그룹에 할당합니다. 사용자는 이 페이지에서 802.1X 게스트 VLAN을 켤 포트를 지정할 수 있습니다.

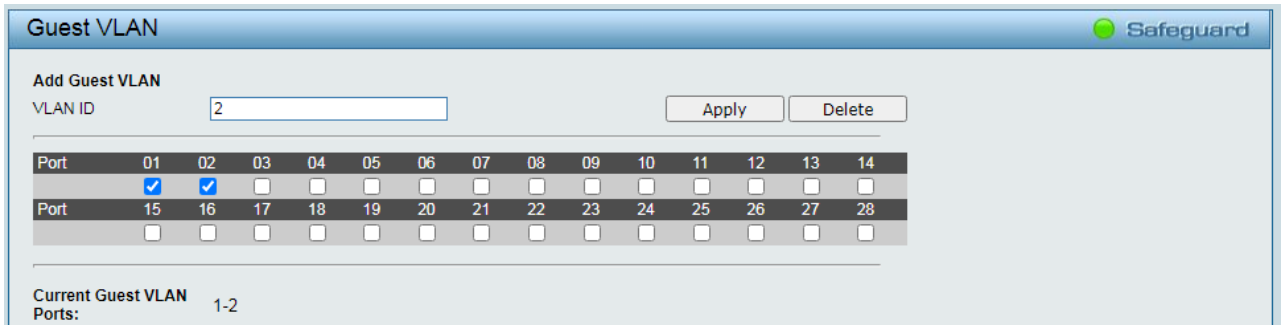


그림 4.131 - AAA > 802.1X > 802.1X 사용자

Add**(추가)를 클릭하여 특정 포트에서 802.1X 게스트 VLAN 기능을 켭니다.**

ACL > ACL 마법사

ACL(Access Control List)을 사용하면 각 패킷의 헤더에 포함된 정보를 기반으로 스위치가 패킷을 전달할지 여부를 결정하는 기준을 설정할 수 있습니다. 이 기준은 MAC 주소 또는 IP 주소를 기준으로 지정할 수 있습니다.

ACL Configuration Wizard는 액세스 프로파일 및 ACL 규칙을 생성하는 데 도움이 됩니다. ACL 마법사는 액세스 규칙 및 프로필을 자동으로 만듭니다. 사용 가능한 최대 프로필은 50개이며 스위치에 대해 총 200개의 규칙이 있습니다.

새 액세스 규칙을 만들려면 **Create(생성)**를 선택하고 **Access-List Name(액세스 목록 이름)**을 입력한 후 **Next(다음)** 버튼을 클릭합니다.

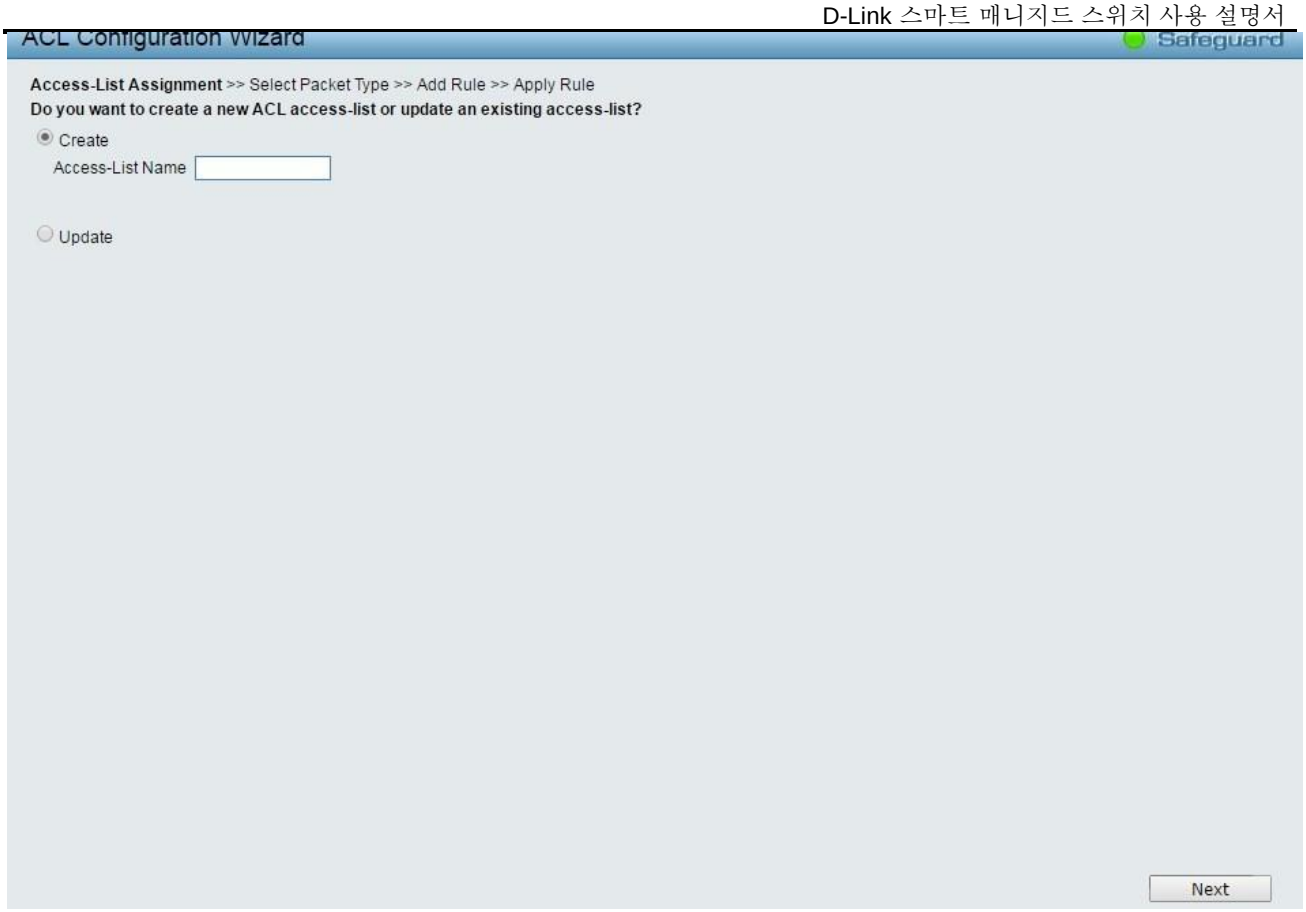


그림 4.132 - ACL > ACL 마법사 – 액세스 목록 만들기

액세스 프로필을 추가하는 단계는 아래에 설명되어 있습니다.

1. 패킷 유형(MAC, IPv4 **또는** IPv6)을 선택합니다.

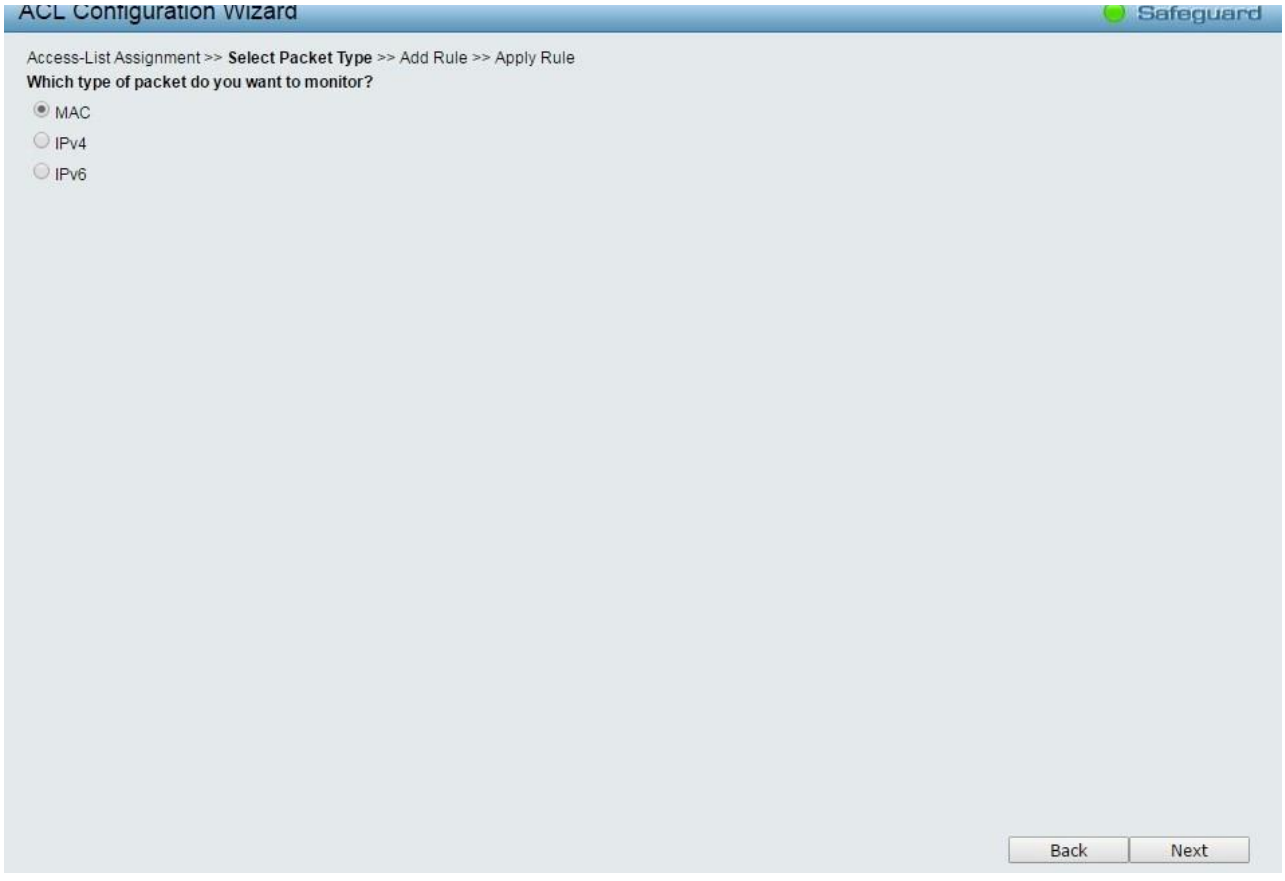


그림 4.133 - ACL > ACL 마법사 – 패킷 유형 선택

MAC 주소, IPv4 주소, IPv6 주소 또는 패킷 내용에 따라 패킷 유형을 선택합니다. 이렇게 하면 프로필 유형에 대한 요구 사항에 따라 창이 변경됩니다.

MAC: ACL 프로파일 레이어 2 프로토콜을 정의합니다. MAC을 선택하여 각 패킷의 MAC 주소를 모니터링합니다.

IPv4: IPv4 ACL 프로필 프로토콜을 정의합니다. 각 패킷의 IPv4 주소를 모니터링하려면 IPv4를 선택합니다.

IPv6: IPv6 ACL 프로필 프로토콜을 정의합니다. 각 패킷의 IPv6 주소를 모니터링하려면 IPv6을 선택합니다.

참고: ACL(Access Control List) 규칙은 시스템 MAC/IP 주소로/나가는 트래픽에 적용되지 않습니다. DGS-1210 시리즈는 CPU ACL 기능을 지원하지 않습니다.

- **MAC ACL 규칙을 정의**하려면 다음을 선택합니다. **MAC** 을 선택하고 **다음** 버튼을 클릭합니다. 업데이트를 통해 다음과 같은 내용이 표시됩니다.

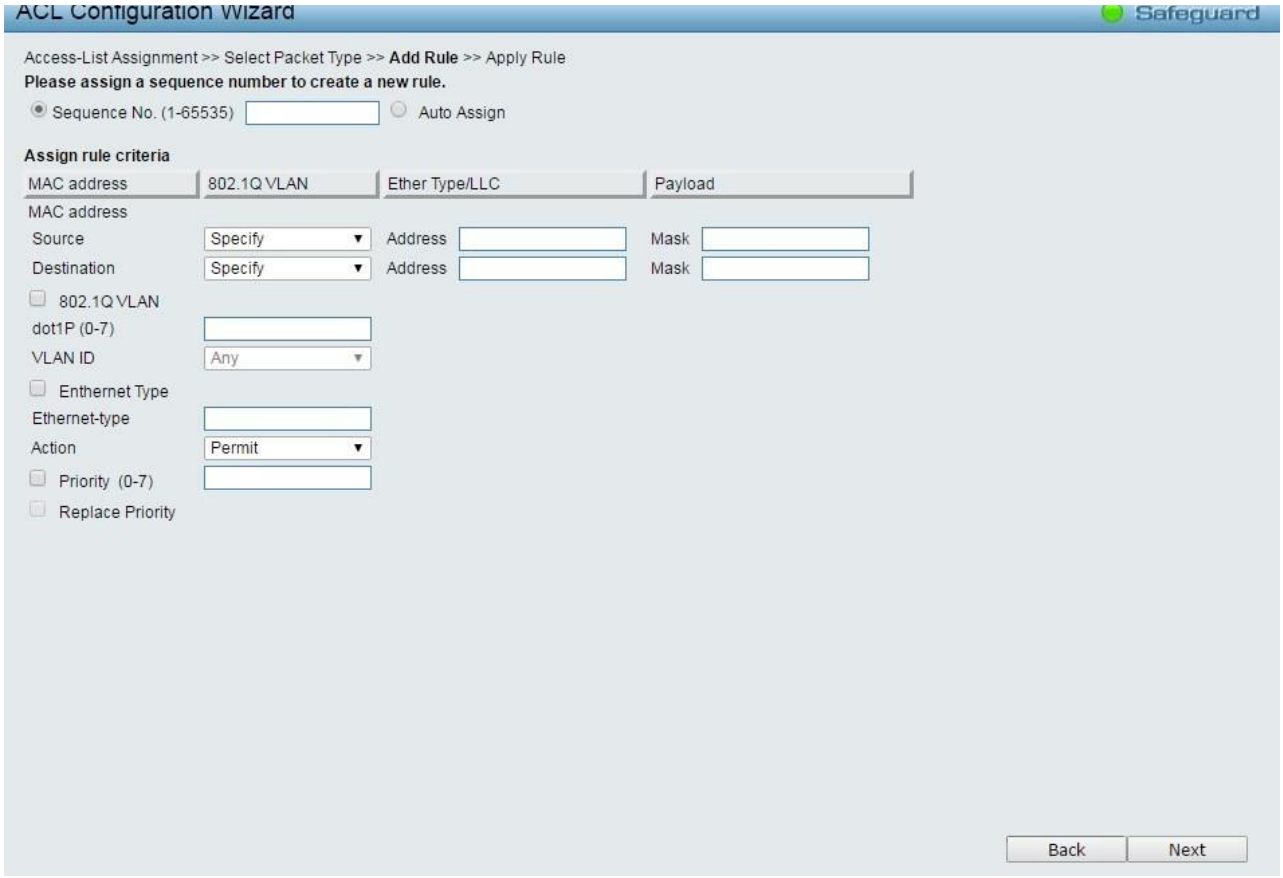


그림 4.134 - 액세스 규칙 추가 - MAC

Assign sequence number:

Sequence No (1-65535): 시퀀스 번호를 지정합니다. 값은 1에서 65535 사이입니다.

Auto Assign: 새 규칙의 시퀀스 번호를 자동으로 할당합니다.

Assign Rule Criteria: MAC 주소 설정을 지정합니다.

Source: 지정할 소스 MAC 또는 모두를 선택합니다. 소스 MAC 주소와 소스 MAC 마스크를 입력하고,
예: FF-FF-FF-FF-FF-FF.

Destination: 지정할 대상 MAC 또는 모두를 선택합니다. 대상 MAC 주소 및 대상 MAC 마스크(예: FF-FF-FF-FF-FF-FF-FF)를 입력합니다.

사용자가 **802.1Q VLAN** 상자를 선택하는 경우 **dot1p** 및 **VLAN ID**를 지정해야 합니다.
Dot1p(0-7): dot1p 우선 순위를 지정합니다.
VLAN ID: 이 옵션을 선택하면 스위치가 각 패킷 헤더의 802.1p 우선 순위 값을 검사하고 이를 전달 기준의 일부로 사용하도록 지시합니다.

사용자가 **이더넷 유형** 상자를 선택하는 경우 **이더넷 유형**을 지정하고 **작업**을 선택해야 합니다.

Ethernet Type(이더넷 유형): 이 옵션을 선택하면 스위치가 각 프레임의 헤더에서 이더넷 유형 값을 검사하도록 지시합니다.

Action: 규칙 조건과 일치하는 ACL 전달 작업을 지정합니다. 다른 모든 ACL 기준이 충족되는 경우 패킷 전달을 허용합니다.**Deny(거부)**는 다른 모든 ACL 기준이 충족되는 경우 패킷을 삭제합니다.

Priority (0-7): 값이 0-7인 MAC ACL 우선 순위를 지정합니다.
Replace Priority(우선 순위 교체): 확인란을 선택하여 Replace Priority 기능을 활성화합니다. Next(**다음**) 버튼을 클릭하면 ACL 프로파일이 추가됩니다.

- **IPv4 ACL ICMP 규칙을 정의하려면** : IPv4를 선택하고 다음 버튼을 클릭합니다. 프로토콜 유형을 ICMP로 선택하면 업데이트에 다음이 표시됩니다.

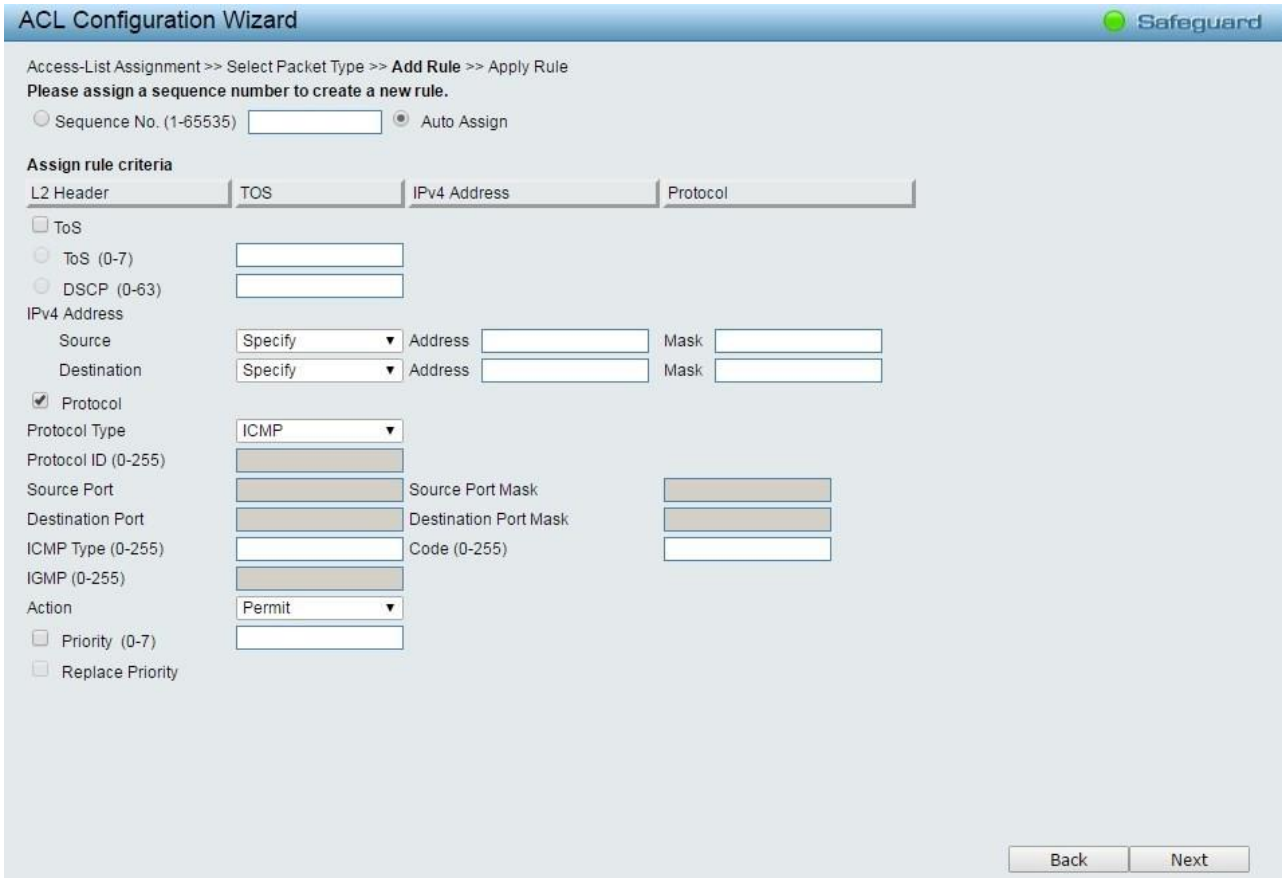


그림 4.135 - 액세스 규칙 추가 – IPv4 ICMP

Assign sequence number:

Sequence No. (1-65535): 시퀀스 번호를 지정합니다. 값은 1에서 65535 사이입니다.

Auto Assign: 새 규칙의 시퀀스 번호를 자동으로 할당합니다.

Assign Rule Criteria: IPv4 ACL 설정을 지정합니다.

ToS: 확인란을 선택하여 ToS 우선 순위 및 DSCP 값을 지정합니다.

ToS(0-7): ToS 값을 지정합니다.

DSCP(0-63): DSCP 값을 지정합니다. 값은 0에서 63 사이입니다.

IPv4 Address: IPv4 소스 및 대상 주소를 지정합니다.

Source: 지정할 소스 IP 또는 ACL 규칙과 관련된 Any를 선택합니다. 소스 IP 주소 및 소스 IP 마스크를 입력합니다. 예를 들어 176.212.XX.XX를 설정하려면 마스크 255.255.0.0을 사용합니다.

Destination: 지정할 대상 IP 또는 ACL 규칙과 관련된 모든 IP를 선택합니다. 대상 IP 주소와 대상 IP 마스크를 입력합니다. 예를 들어 176.212.XX.XX를 설정하려면 마스크 255.255.0.0을 사용합니다.

Protocol: 프로토콜을 **선택하여** 관련 설정을 구성합니다.

Protocol Type: IPv4에 대한 프로토콜 유형을 선택합니다. 가능한 필드는 **ICMP, IGMP, TCP, UDP** 및 **프로토콜 ID**입니다.

ICMP Type (0-255): ICMP 유형 필드를 일치시킬 필수 필드로 설정합니다.

Code (0-255): ICMP 코드 필드를 일치시킬 필수 필드로 설정합니다.

Access-List에 추가된 포트를 선택하고 Next(다음) 버튼을 클릭하면 ACL 프로필이 추가됩니다.

- IPv4 ACL IGMP 규칙을 정의하려면 : IPv4 ACL을 선택하고 다음 버튼을 클릭합니다. IGMP에 대한 프로토콜 유형을 선택하면 업데이트에 다음이 표시됩니다.

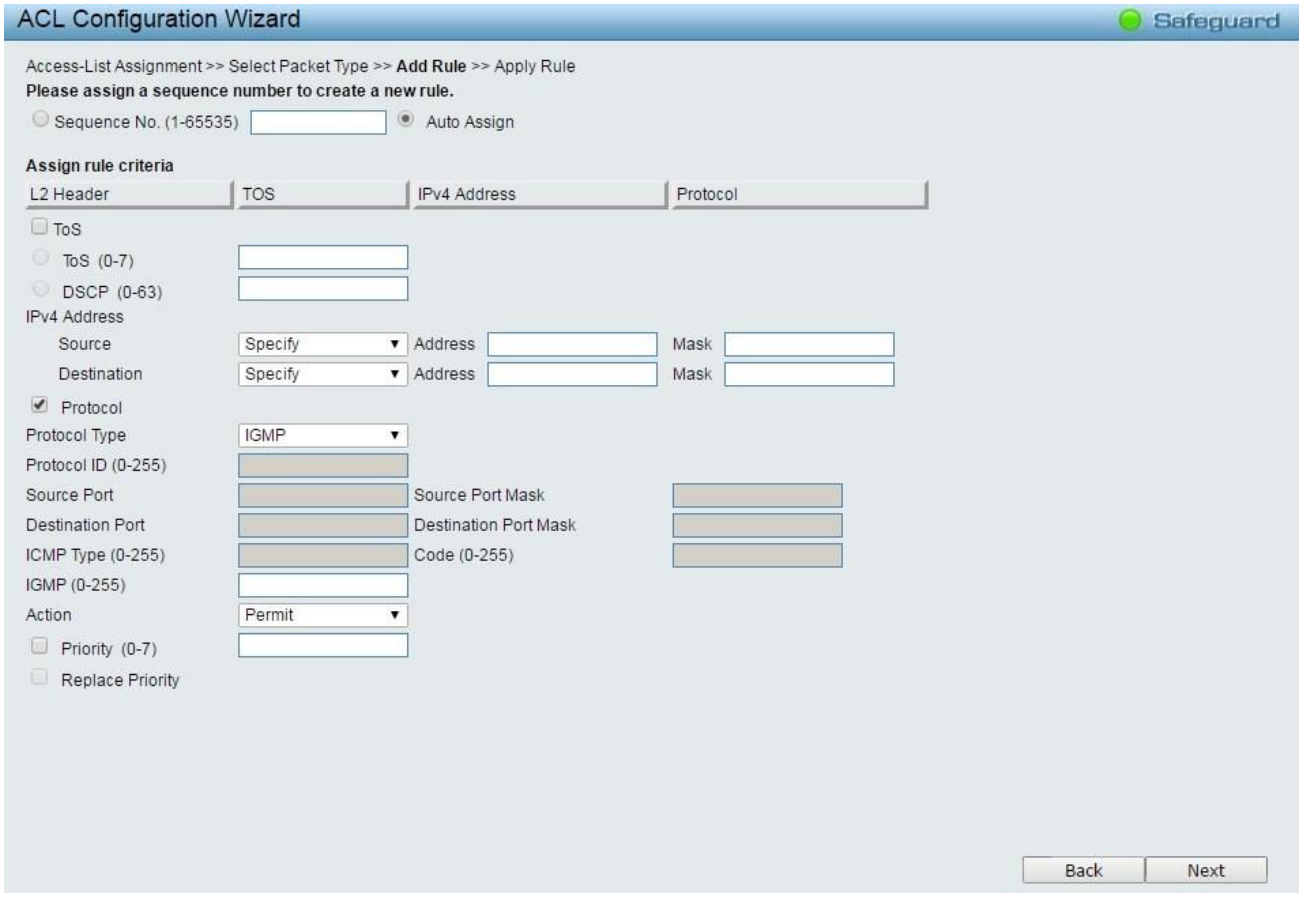


그림 4.136 - 액세스 규칙 추가 – IPv4 IGMP

IGMP Type (0-255): IGMP 유형 필드를 일치시킬 필수 필드로 설정합니다.
Next(**다음**) 버튼을 클릭하면 ACL 프로파일이 추가됩니다.

IPv4 ACL TCP 규칙을 정의하려면: IPv4 ACL을 선택하고 다음 버튼을 클릭합니다. TCP에 대한 프로토콜 유형을 선택하면 업데이트에 다음이 표시됩니다:

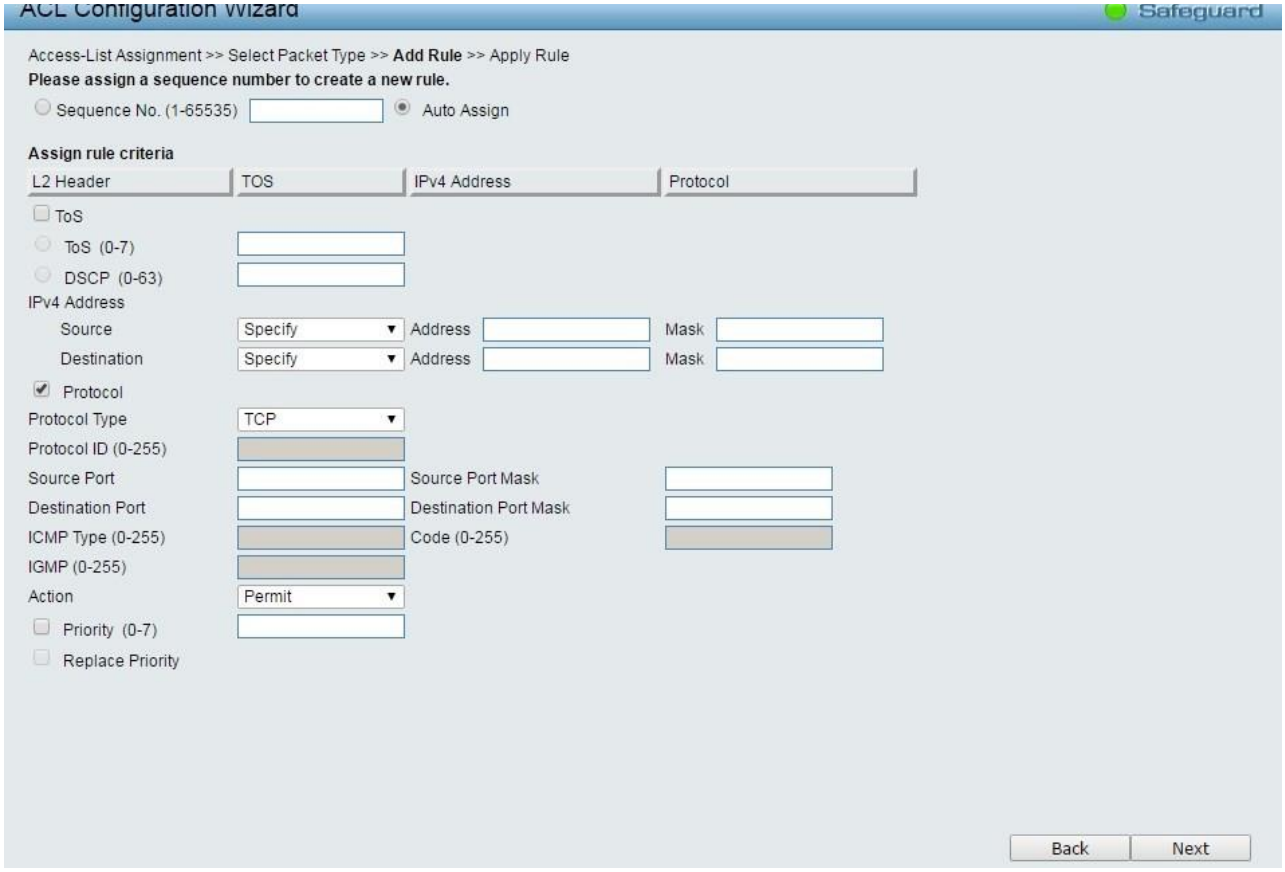


그림 4.137 - 액세스 규칙 추가 – IPv4 TCP

IPv4 주소: ACL 규칙과 관련된 소스 포트의 범위를 정의합니다.

Source: ACL 규칙과 관련된 소스 포트의 범위를 정의합니다. 예를 들어, 0 – 15를 설정하려면 FFF0의 마스크를 설정합니다.

Destination: ACL 규칙과 관련된 대상 IP 주소의 범위를 정의합니다. 예를 들어, 0 – 15를 설정하려면 FFF0의 마스크를 설정합니다.

Next(**다음**) 버튼을 클릭하면 ACL 프로파일이 추가됩니다.

IPv4 ACL UDP 규칙을 정의하려면: IPv4 ACL을 선택하고 다음 버튼을 클릭합니다. UDP에 대한 프로토콜 유형을 선택하면 업데이트에 다음이 표시됩니다.

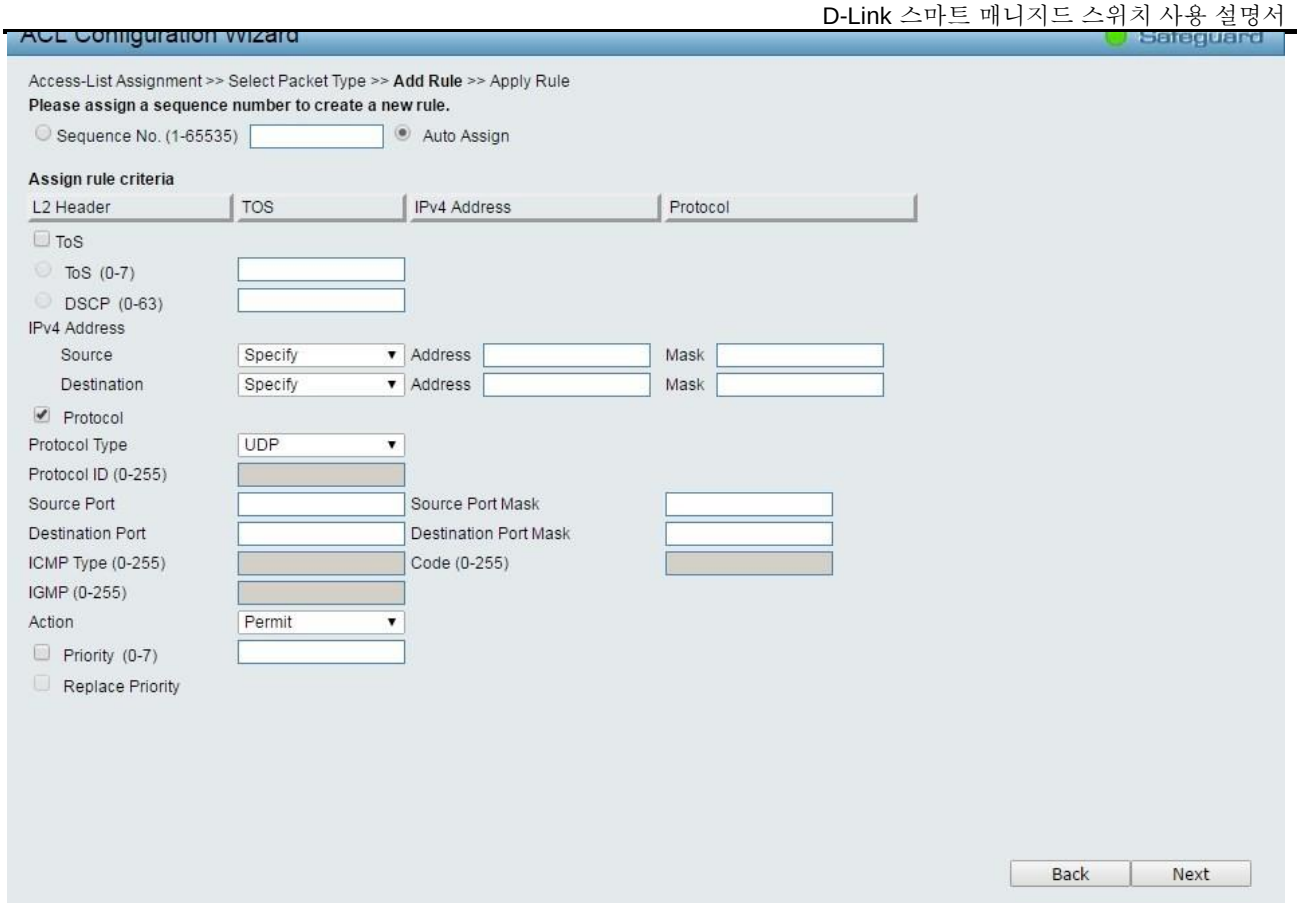


그림 4.138 - 액세스 규칙 추가 – IPv4 UDP

IPv4 Address: ACL 규칙과 관련된 소스 포트의 범위를 정의합니다.

Source: ACL 규칙과 관련된 소스 포트의 범위를 정의합니다. 예를 들어, 0 – 15를 설정하려면 FFF0의 마스크를 설정합니다.

Destination: ACL 규칙과 관련된 대상 IP 주소의 범위를 정의합니다. 예를 들어, 0 – 15를 설정하려면 FFF0의 마스크를 설정합니다.

Next(**다음**) 버튼을 클릭하면 ACL 프로파일이 추가됩니다.

IPv4 ACL 프로토콜 ID 규칙을 정의하려면 : IPv4 ACL을 선택하고 다음 버튼을 클릭합니다. 프로토콜 ID에 대한 프로토콜 유형을 선택하면 업데이트에 다음이 표시됩니다.

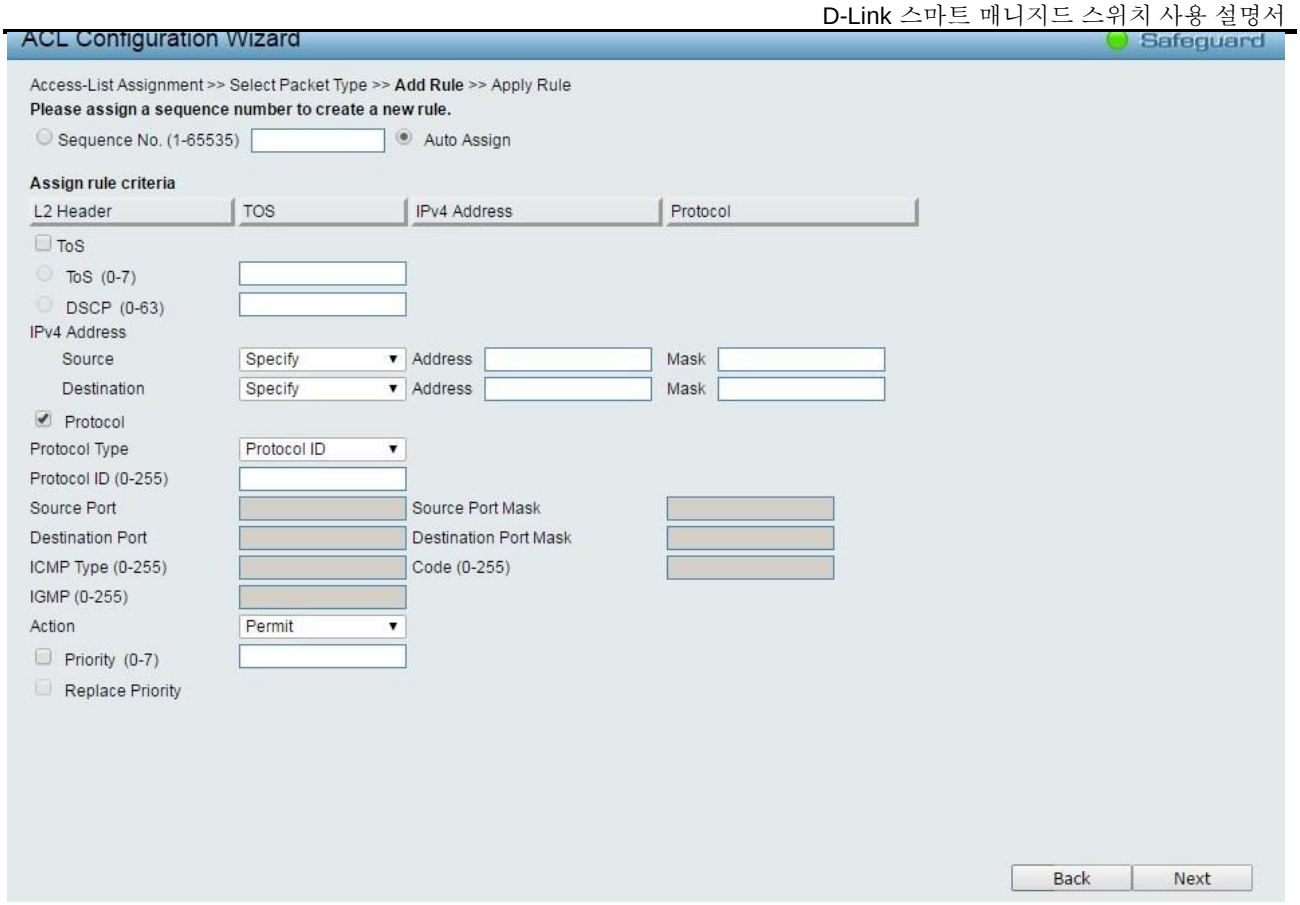


그림 4.139 - 액세스 규칙 추가 – IPv4 프로토콜 ID

IPv4 Address: ACL 규칙과 관련된 소스 포트의 범위를 정의합니다.

Source: ACL 규칙과 관련된 소스 포트의 범위를 정의합니다. 예를 들어, 0 – 15를 설정하려면 FFF0의 마스크를 설정합니다.

Destination: ACL 규칙과 관련된 대상 IP 주소의 범위를 정의합니다. 예를 들어, 0 – 15를 설정하려면 FFF0의 마스크를 설정합니다.

Protocol ID(0-255) - 구성할 프로토콜 ID를 지정합니다. Next(**다음**)
버튼을 클릭하면 ACL 프로파일이 추가됩니다.

참고: 하나 또는 여러 필터링 마스크의 조합을 동시에 선택할 수 있습니다. 페이지가 관련 필드로 업데이트됩니다.

IPv6 ACL ICMP 규칙을 정의하려면: 프로토콜 유형의 ICMP가 있는 IPv6 ACL을 선택하고 다음 버튼을 클릭합니다. 업데이트에 다음이 표시됩니다.

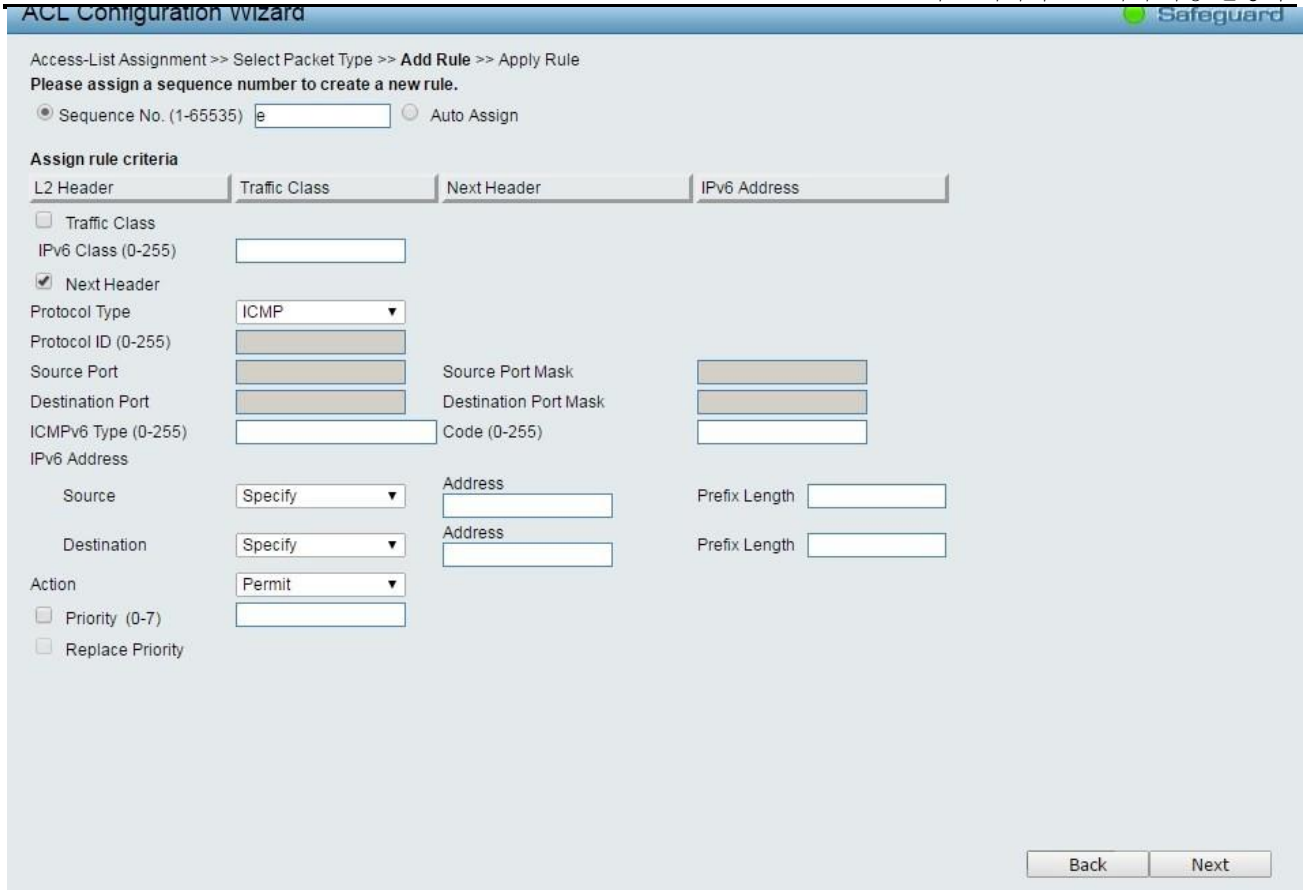


그림 4.140 - 액세스 규칙 추가 – IPv6 ICMP

IPv6 Class (0-255): 액세스 규칙의 클래스를 지정합니다. 필드 범위는 0에서 255 사이입니다.

ICMPv6 Type: ICMP 유형 필드를 일치시킬 필수 필드로 설정합니다. 코드(0-255): ICMP 코드 필드를 일치시킬 필수 필드로 설정합니다.

Source IPv6 Address: ACL 규칙과 관련된 소스 IP 주소의 범위를 정의합니다. 예를 들어 2002:0:0:0:0:0:b0d4:0을 설정하려면 마스크 128을 사용합니다.

Destination IPv6 Address: ACL 규칙과 관련된 대상 IP 주소의 범위를 정의합니다. 예를 들어 2002:0:0:0:0:0:bfd4:0을 설정하려면 마스크 128을 사용합니다.

Action: 규칙 조건과 일치하는 ACL 전달 작업을 지정합니다. 다른 모든 ACL 기준이 충족되는 경우 패킷 전달을 허용합니다. **Deny(거부)**는 다른 모든 ACL 기준이 충족되는 경우 패킷을 삭제합니다.

Next(**다음**) 버튼을 클릭하면 ACL 프로파일이 추가됩니다.

IPv6 ACL TCP 프로필을 정의하려면: 프로토콜 유형의 TCP가 포함된 IPv6 ACL을 선택하고 다음 버튼을 클릭합니다. 업데이트에 다음이 표시됩니다.

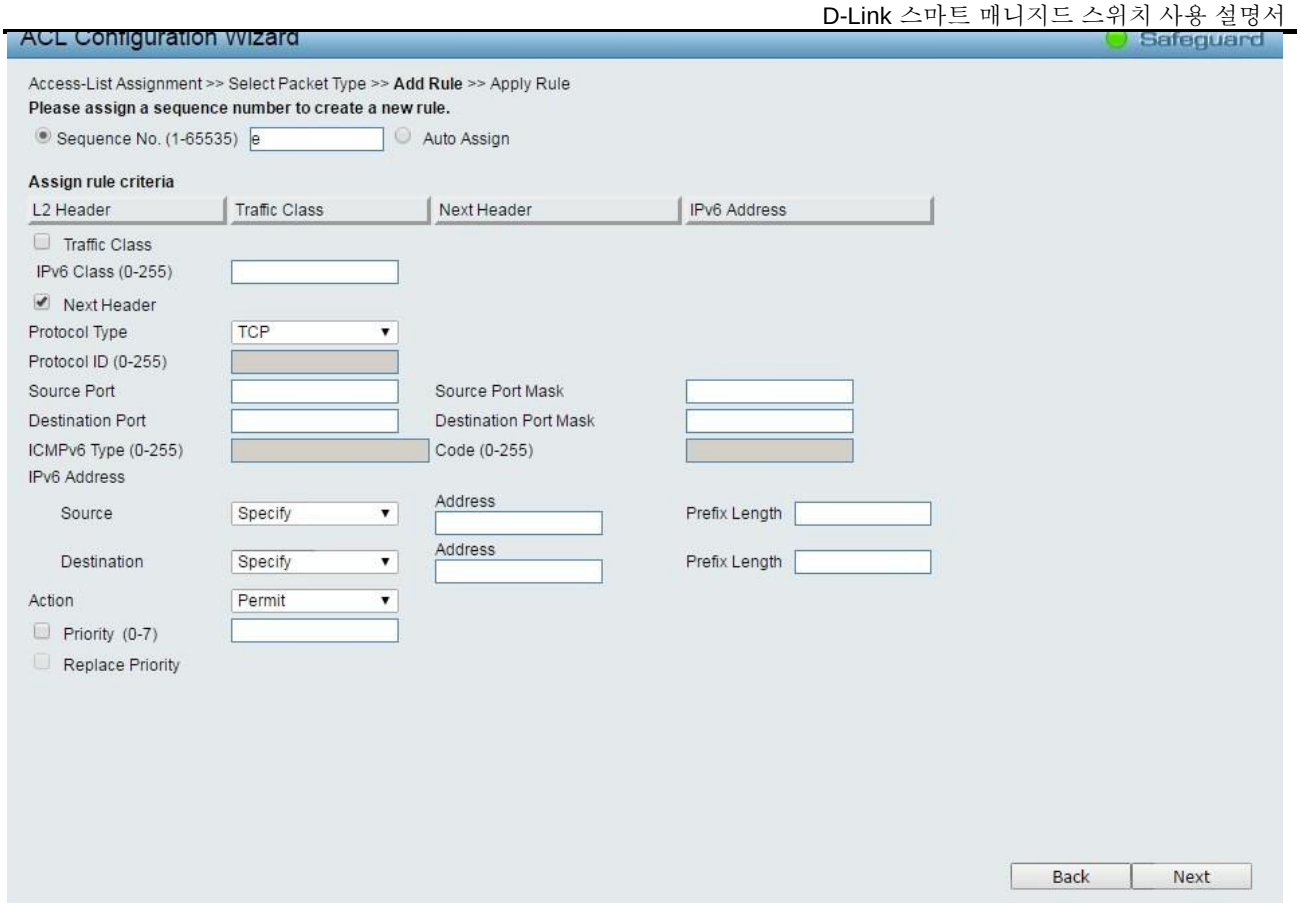


그림 4.141 - 액세스 규칙 추가 – IPv6 TCP

Source Port: 소스 포트를 지정합니다.

Source Port Mask(소스 포트 마스크): ACL 규칙과 관련된 소스 IP 주소의 범위를 정의합니다. 예를 들어, 0 – 15를 설정하려면 FFF0의 마스크를 설정합니다.

Destination Port: 대상 포트를 지정합니다.

Destination Port Mask: ACL 규칙과 관련된 대상 IP 주소의 범위를 정의합니다. 예를 들어, 0 – 15를 설정하려면 FFF0의 마스크를 설정합니다.

Next(**다음**) 버튼을 클릭하면 ACL 프로파일이 추가됩니다.

IPv6 IPv6 ACL UDP 프로필을 정의하려면: 프로토콜 유형의 UDP가 있는 IPv6 ACL을 선택하고 다음 버튼을 클릭합니다. 업데이트에 다음이 표시됩니다

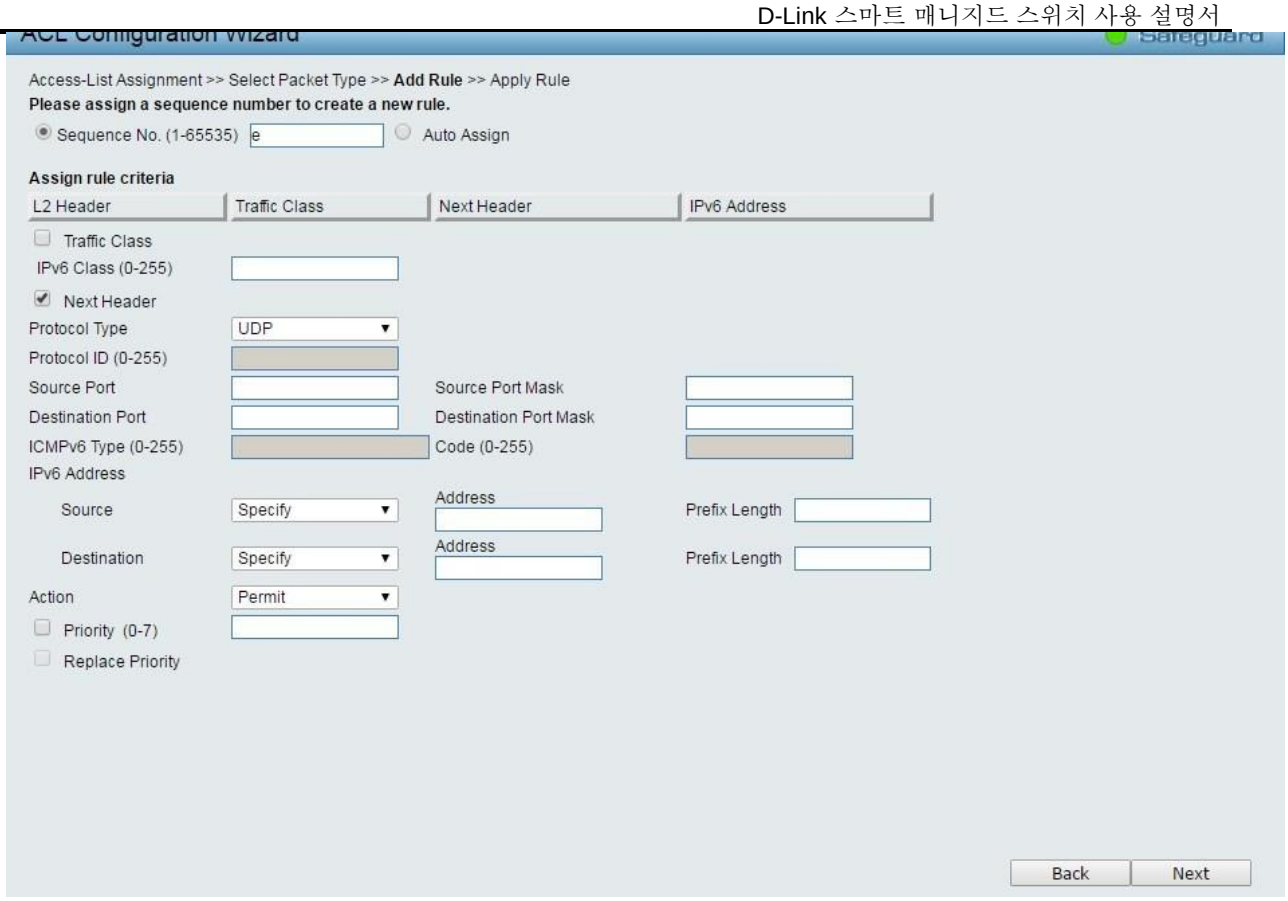


그림 4.142 - 액세스 규칙 추가 – IPv6 UDP

Source Port: 소스 포트를 지정합니다.

Source Port Mask(소스 포트 마스크): ACL 규칙과 관련된 소스 IP 주소의 범위를 정의합니다. 예를 들어, 0 – 15를 설정하려면 FFF0의 마스크를 설정합니다.

Destination Port: 대상 포트를 지정합니다.

Destination Port Mask: ACL 규칙과 관련된 대상 IP 주소의 범위를 정의합니다. 예를 들어, 0 – 15를 설정하려면 FFF0의 마스크를 설정합니다.

Next(**다음**) 버튼을 클릭하면 ACL 프로파일이 추가됩니다.

IPv6 ACL 프로토콜 ID 프로필을 정의하려면: 프로토콜 유형의 프로토콜 ID가 있는 IPv6 ACL을 선택하고 다음 버튼을 클릭합니다. 업데이트에 다음이 표시됩니다.

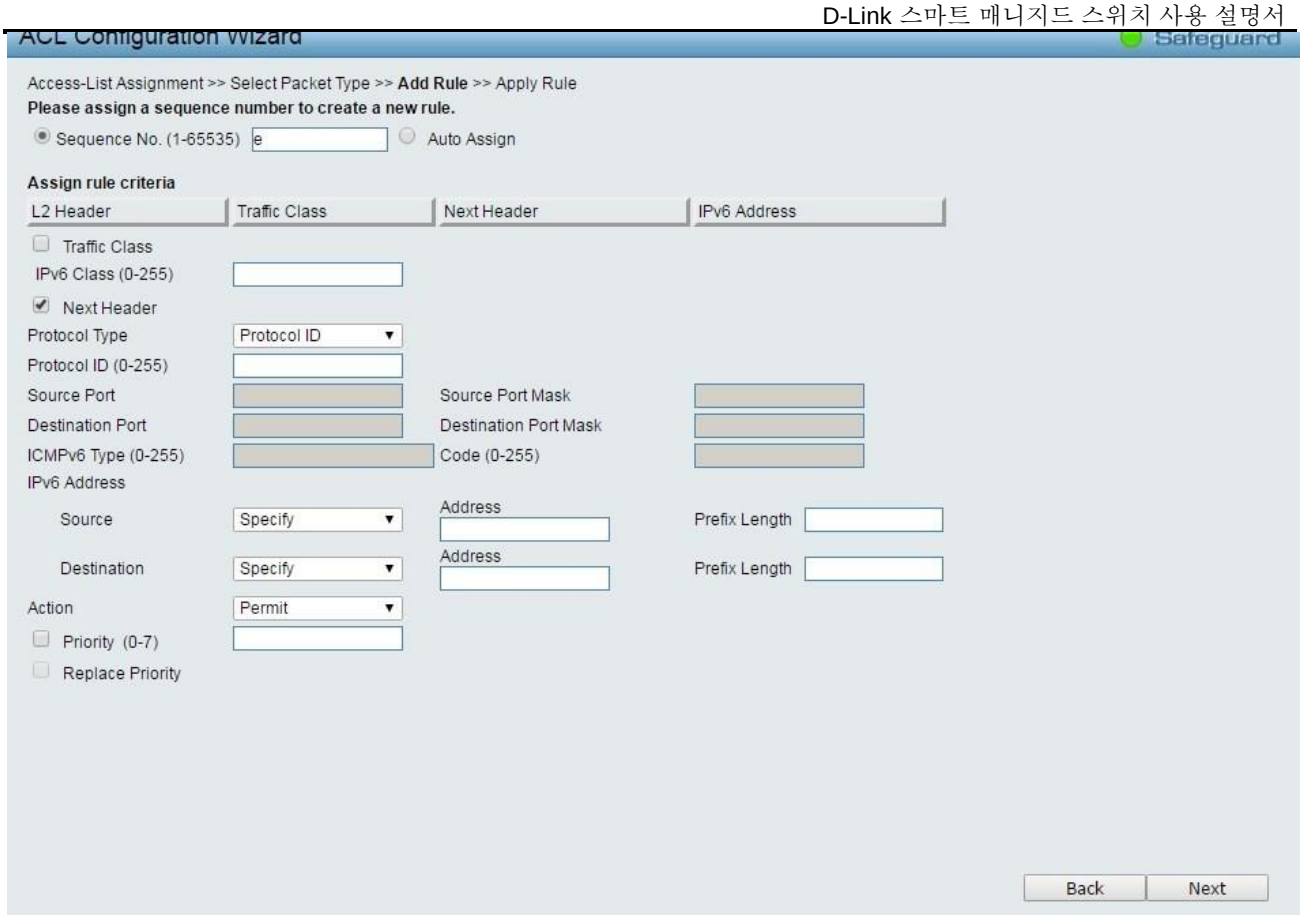


그림 4.143 - 액세스 규칙 추가 – IPv6 프로토콜 ID

Source Port: 소스 포트를 지정합니다.

Source Port Mask: ACL 규칙과 관련된 소스 IP 주소의 범위를 정의합니다. 예를 들어, 0 – 15를 설정하려면 FFF0의 마스크를 설정합니다.

Destination Port: 대상 포트를 지정합니다.

Destination Port Mask: ACL 규칙과 관련된 대상 IP 주소의 범위를 정의합니다. 예를 들어, 0 – 15를 설정하려면 FFF0의 마스크를 설정합니다.

Source IPv6 Address: ACL 규칙과 관련된 소스 IP 주소의 범위를 정의합니다. 예를 들어 2002:0:0:0:0:0:b0d4:0을 설정하려면 마스크 128을 사용합니다.

Destination IPv6 주소: ACL 규칙과 관련된 대상 IP 주소의 범위를 정의합니다. 예를 들어 2002:0:0:0:0:0:bfd4:0을 설정하려면 마스크 128을 사용합니다.

Action: 규칙 조건과 일치하는 ACL 전달 작업을 지정합니다. **다른 모든 ACL 기준이 충족되는 경우 패킷 전달** 을 허용합니다.**Deny(거부**)는 다른 모든 ACL 기준이 충족되는 경우 패킷을 삭제합니다.

Next(**다음**) 버튼을 클릭하면 ACL 프로파일이 추가됩니다.

참고: 하나 또는 여러 필터링 마스크의 조합을 동시에 선택할 수 있습니다. 페이지가 관련 필드로 업데이트됩니다.

2. 관심 필드를 선택하면 다음을 보여주는 다음 페이지가 표시됩니다.

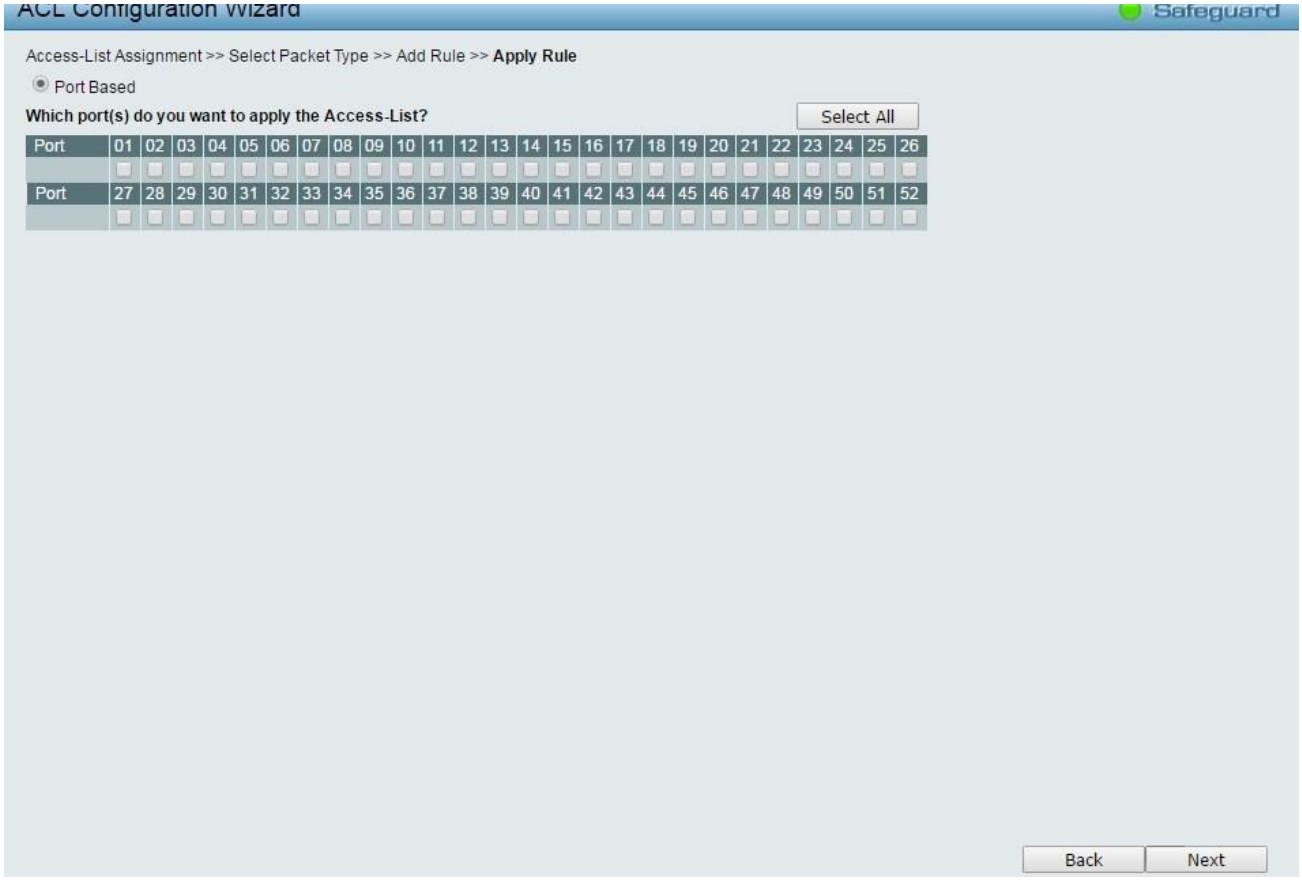


그림 4.144 - Add Access Rule – 포트

Next(**다음**) 버튼을 클릭하면 ACL 프로파일이 추가됩니다.

3. 기존 규칙을 수정하려면 **업데이트** 및 **Access-List Name** 하이퍼링크를 선택하고 Next(다음)를 클릭하십시오 단추.

그림 4.145 - ACL > ACL 마법사 – ACL 목록 업데이트

ACL > ACL 액세스 목록

ACL Access List 페이지는 ACL 액세스를 수동으로 구성하기 위한 정보를 제공합니다. **Edit Rules** 버튼을 클릭하여 액세스 프로필을 수정하거나 **Delete** 버튼을 클릭하여 ACL 프로필을 제거합니다.

그림 4.146 - ACL > ACL 액세스 목록

새 프로필을 추가하려면 **Add** 버튼을 클릭합니다. 업데이트를 통해 다음과 같은 내용이 표시됩니다.

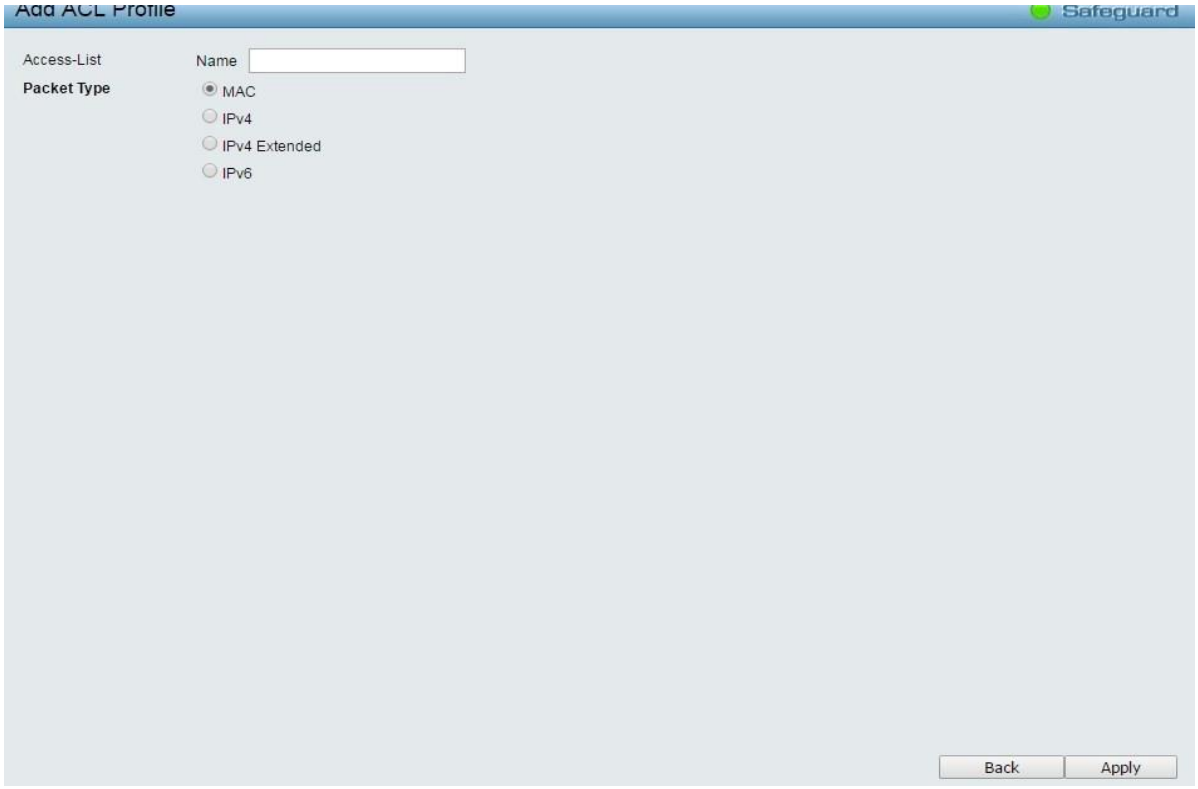


그림 4.147 - ACL > ACL 액세스 목록 - ACL 프로필 추가

Access-List: 추가할 ACL 프로필의 액세스 목록 이름을 지정합니다.

Packet Type: 패킷 유형을 **MAC, IPv4**, **IPv4 확장** 또는 **IPv6**로 지정한 다음 **Apply** 버튼을 클릭합니다.

기존 규칙을 수정하기 위해 **Edit Rules** 버튼을 클릭하면 ACL Access list 테이블이 표시됩니다.
시퀀스 번호를 클릭하십시오.

그림 4.148 - ACL > ACL 액세스 목록 – ACL 프로필 업데이트

ACL > ACL 액세스 그룹

ACL Access Group(ACL 액세스 그룹) 페이지에서는 사용자가 ACL 액세스 그룹 설정을 구성할 수 있습니다.

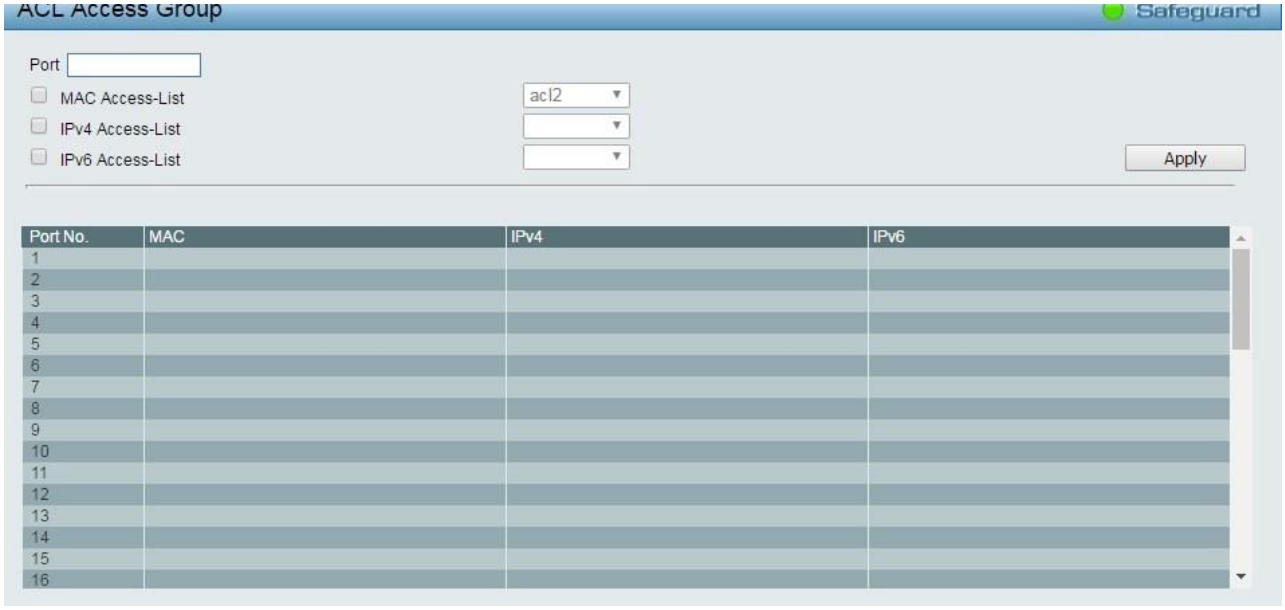


그림 4.149 - ACL > ACL 액세스 그룹

Port: 액세스 목록 그룹에 추가할 포트를 지정합니다.

MAC Access-List: MAC 액세스 목록 그룹에 지정된 포트를 추가합니다.

IPv4 Access-List: IPv4 액세스 목록 그룹에 지정된 포트를 추가합니다.

IPv6 Access-List: IPv6 액세스 목록 그룹에 지정된 포트를 추가합니다.

Apply(**적용**) 버튼을 클릭하여 변경 사항을 구현합니다.

ACL > ACL 하드웨어 리소스 상태

ACL 하드웨어 리소스 상태 페이지에는 ACL 하드웨어 리소스 상태 정보가 표시됩니다.

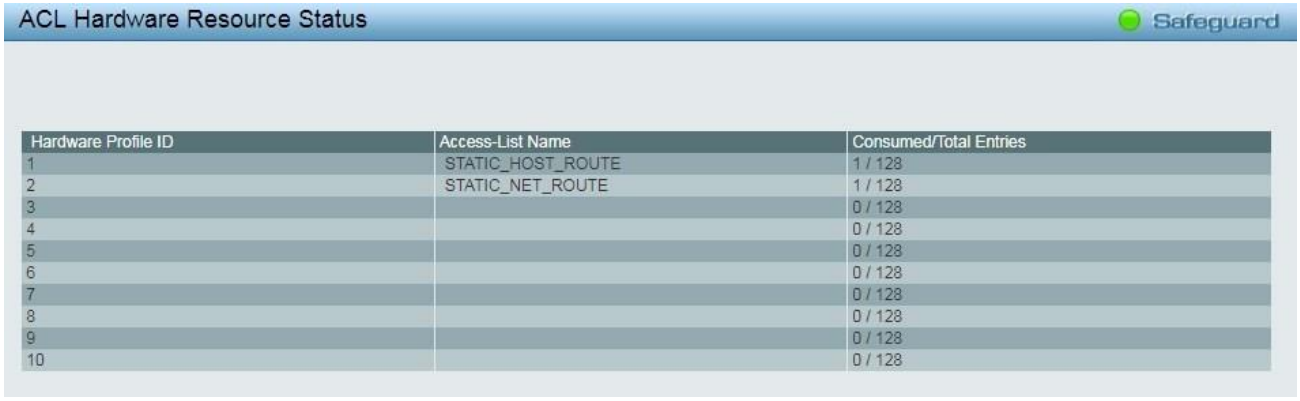


그림 4.150 - ACL > ACL 하드웨어 리소스 상태

PoE > PoE 전역 설정(DGS-1210-10P/10MP/28P/28MP/52MP에만 해당)

이 페이지에는 시스템 예산 전력, 지원 총 전력, 잔여 전력 및 시스템 전원 공급 장치 비율을 포함한 PoE 상태가 표시됩니다.

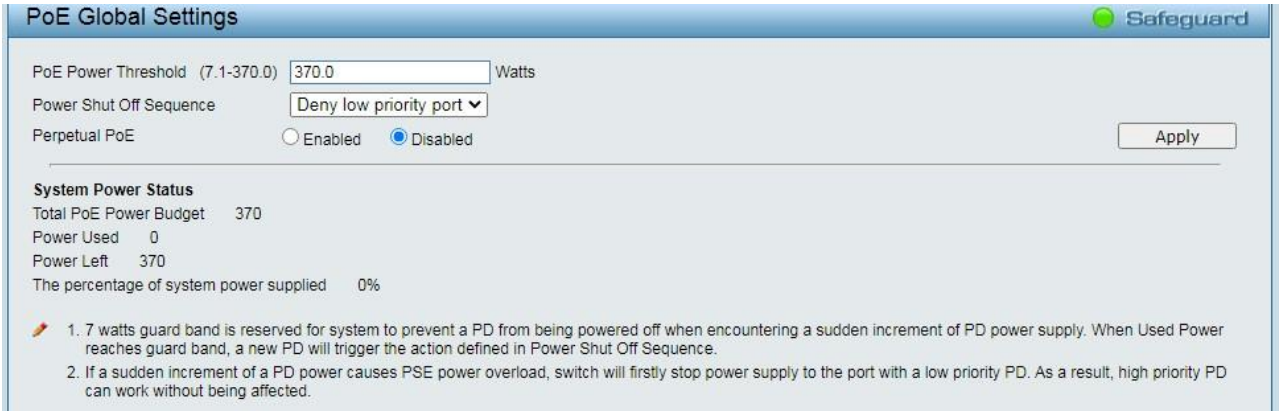


그림 4.151 - PoE > PoE 전역 설정

시스템 전력 임계값: 시스템 전력 예산을 수동으로 구성합니다.

Power Shut Off Sequence(전원 차단 시퀀스): 임계값에 도달하면 포트에 대한 전원을 거부하는 데 사용되는 방법을 정의합니다. 가능한 필드는 다음과 같습니다.

Deny next port: 사용된 총 전력이 전력 예산에 도달하면 포트 우선 순위에 관계없이 전원을 켜려는 다음 포트가 거부됩니다.

Deny low priority port: 우선 순위가 낮은 포트가 종료되어 우선 순위가 높은 포트의 전원을 켤 수 있습니다.

Perpetual PoE: 스위치는 부팅 중인 스위치에도 PD에 무정전 전원을 제공합니다.
Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.
System Power Status: 장치의 시스템 전원 상태를 표시합니다.

Total PoE Power Budget: 이 스위치의 총 PoE 전력 예산을 표시합니다.

Power Used: 스위치의 현재 사용 전력을 표시합니다.

Power Left: 스위치의 예비 전원을 표시합니다.

The percentage of system power supplied: 스위치에 공급된 시스템 전력의 백분율을 표시합니다.

PoE > PoE 포트 설정 (DGS-1210-10P / 10MP / 28P / 28MP / 52MP 만 해당)

DGS-1210 시리즈는 IEEE 사양에 정의된 대로 PoE(Power over Ethernet)를 지원합니다.

PoE 포트 사양은 아래 표에 나열되어 있습니다.

모델명	PoE 지원 포트	전력 예산
DGS-1210-10P	포트 1 ~ 포트 8: 최대 PoE 출력 30W	65 W
DGS-1210-10MP	포트 1 ~ 포트 8: 최대 PoE 출력 30W	130 W
DGS-1210-28P	포트 1 ~ 포트 24: 최대 PoE 출력 30W	193 W
DGS-1210-28MP	포트 1 ~ 포트 24: 최대 PoE 출력 30W	370 W
DGS-1210-52MP	포트 1 ~ 포트 48: 최대 PoE 출력 30W	370 W

DGS-1210 시리즈는 모든 D-Link 802.3af 또는 802.3at 지원 장치에서 작동합니다. 스위치는 또한 PoE 분배기 DWL-P802.3을 통해 모든 비 802af 지원 D-Link AP, IP Cam 및 IP 전화 장비와 함께 PoE 모드에서 작동합니다.

IEEE 802.3at는 다음 분류에 따라 PSE가 전력을 제공한다고 정의했습니다.

클래스	사용법	PSE에 의한 출력 전력 제한
0	기본값	15.4W
1	선택적	4.0W
2	선택적	7.0W
3	선택적	15.4W
4	선택적	30W

PoE 포트 테이블에는 포트 활성화, 전력 제한, 전력(W), 전압(V), 전류(mA), 분류, 포트 상태를 포함한 PoE 상태가 표시됩니다. 사용자는 **From Port** / **To Port** 를 선택하여 포트의 PoE 기능을 제어할 수 있습니다. DGS-1210 시리즈는 포트 전류가 802.3af 모드에서 375mA 이상이거나 802.3at 이전 모드에서 625mA 이상인 경우 포트를 자동으로 비활성화합니다.

참고: Power current, Power Voltage, Current의 PoE Status 정보는 연결된 PD의 전력 사용량 정보입니다. 정보를 갱신하려면 "Refresh"를 누르십시오.

참고: Power Limit 설정에서 User Define을 선택한 경우 Power(W)의 허용 오차는 10%일 수 있습니다.

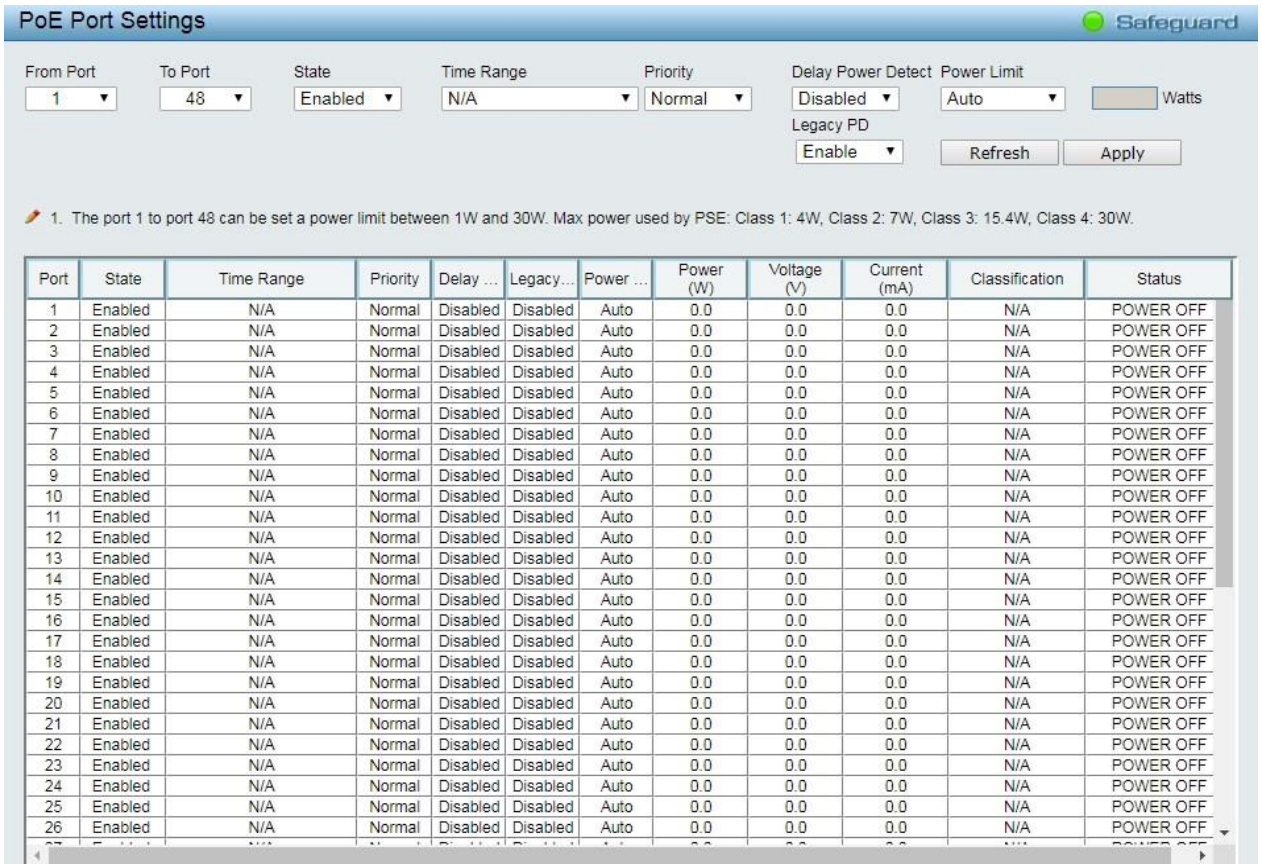


그림 4.152 - PoE > PoE 포트 설정

From Port / To Port: 포트의 PoE 기능을 지정합니다.

State: "Enabled" 또는 "Disabled"를 선택하여 지정된 포트에 대한 PoE 기능을 구성합니다. 기본값은 **사용입니다**.

Time Range: PoE 시간 프로를 선택합니다.file 시간 기반 PoE > 시간 범위 설정에서 구성되어 지정된 포트에서 시간 기반 PoE 기능을 활성화합니다. 기본 설정은 **N/A입니다**.

Priority: 지정된 포트에서 전원 공급 장치 우선 순위를 "낮음", "보통" 또는 "높음"으로 구성합니다. 기본값은 보통.

Delay Power Detect(지연 전력 감지): 지연 전력 감지를 구성합니다. 기본값은 비활성화되어 있습니다..

Power Limit: 이 기능을 사용하면 사용자가 PD에 제공할 포트 전력 전류 제한을 수동으로 설정할 수 있습니다. DGS-1210 PoE 시리즈 및 연결된 장치를 보호하기 위해 전력 제한 기능은 전원이 과부하 될 때 포트의 PoE 기능을 비활성화합니다. **전력 제한은 "**Class 1**", "**Class 2**", "**Class 3**",** Class 4" **및 "**Auto" 중에서 선택합니다.

자동"은 802.3at 표준을 기반으로 PD 전력 전류의 분류를 협상하고 따릅니다.

User Define: 확인란을 선택하고 전력 예산(1에서 30W까지)을 입력하여 지정된 포트에서 포트 전력 예산의 상한을 수동으로 할당합니다.

Legacy PD: 레거시 PD 신호 감지를 활성화하거나 비활성화하도록 지정합니다.

Apply(**적용**)를 클릭하여 구성을 적용하거나 **Refresh(새로 고침)**를 클릭하여 테이블을 다시 표시합니다.

참고: PoE 포트 설정 표의 경우 분류가 "레거시 PD"로 표시된 경우 비 AF PD 또는 레거시 PD로 분류됩니다.

참고: 이 스위치는 IEEE 802.3af 및 802.3at 표준을 준수합니다. IEEE PoE 표준은 400ms 시간 간격 내에 전력 소모량이 10mA 미만인 경우 스위치가 포트의 전원을 차단하도록 요구합니다. 더 오래 걸릴 수 있는 일부 비표준 디바이스를 지원하기 위해 이 기능은 시간 간격을 500ms로 연장하는 데 도움이 됩니다. PD의 전원이 여전히 켜지지 않으면 PD 장치의 기술 지원에 문의하십시오.

PoE > PD Alive (DGS-1210-10P / 10MP / 28P / 28MP / 52MP 전용)

PD Alive 기능은 핑 동작을 통해 항상 PoE PD 장치를 확인합니다. PD 장치가 응답을 멈추면 DGS-1210 시리즈는 PoE 포트 전원을 재활용하거나 네트워크 관리자에게 알립니다.

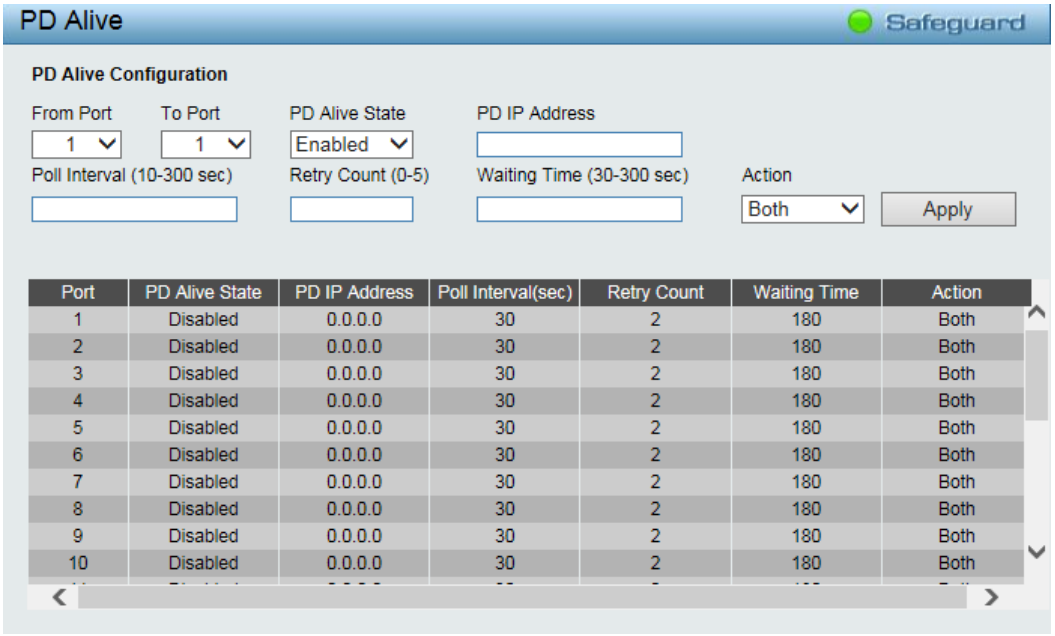


그림 4.153 - PoE > PoE 포트 설정

PD Alive State: PD Alive 기능을 활성화/비활성화합니다.

PD IP Address: PD의 IP 주소를 지정합니다.

Poll Interval: ping 패킷을 통해 PD IP 주소를 확인할 시간 간격을 지정합니다.

Retry Count: PD가 ping에 응답하지 않는 재시도 시간을 지정합니다.

Waiting Time: 각 재시도 사이의 대기 시간을 지정합니다.

Action: PD가 응답하지 않을 때 작업 선택: **Reboot**, **Notify** (syslog) 또는 **Both**

SNMP > SNMP > SNMP 전역 설정

SNMP(Simple Network Management Protocol)는 네트워크 디바이스를 관리하고 모니터링하기 위해 특별히 설계된 OSI Layer 7(Application Layer) 프로토콜입니다. SNMP를 사용하면 네트워크 관리 스테이션에서 게이트웨이, 라우터, 스위치 및 기타 네트워크 장치의 설정을 읽고 수정할 수 있습니다. SNMP를 사용하여 적절한 작동을 위한 시스템 기능을 구성하고, 성능을 모니터링하고, 스위치 또는 LAN의 잠재적인 문제를 감지합니다.

SNMP를 지원하는 매니지드 디바이스에는 디바이스에서 로컬로 실행되는 소프트웨어(에이전트라고 함)가 포함됩니다. 정의된 변수 집합(관리 개체)은 SNMP 에이전트에 의해 유지 관리되며 디바이스를 관리하는 데 사용됩니다. 이러한 객체는 MIB(Management Information Base)에 정의되어 있으며, 이는 온보드 SNMP 에이전트에 의해 제어되는 정보의 표준 표시를 제공합니다. SNMP는 MIB 사양의 형식과 네트워크를 통해 이 정보에 액세스하는 데 사용되는 프로토콜을 모두 정의합니다.

기본 SNMP 전역 상태는 비활성화되어 있습니다. Enable(활성화)을 선택하고 **Apply** (적용)를 클릭하여 SNMP 기능을 활성화합니다.

그림 4.154 - SNMP > SNMP > SNMP 전역 설정

Trap Settings: 장치가 SNMP 알림을 보낼 수 있는지 여부를 지정합니다.

SNMP 인증 트랩: 인증 실패 알림을 보낼 장치를 지정합니다.

Device Bootup: 시스템 부팅 정보입니다.

Illegal Login: 잘못된 비밀번호 로그인 이벤트로, 원래 PC의 IP를 기록합니다.

Port Link Up / Link Down: 구리 포트 연결 정보입니다.

RSTP Port State Change: RSTP 포트 상태 변경의 이벤트입니다.

Firmware Upgrade State: 펌웨어 업그레이드 정보 - 성공 또는 실패.

PoE power On / Off: 포트별 전원 상태입니다.

PoE Power Error: 4가지 트랩 이벤트는 부하 초과, 단락, 과열 시 전원 차단 및 전원 거부입니다.

PoE over max power budget: 시스템이 PD에 전원을 공급하고 최대 PoE 전력 예산에 도달하면 시스템에서 이 트랩 메시지를 보냅니다.

Loopback Detection occurring / recovery: 루프백 탐지 발생 및 복구 시 SNMP 트랩을 보낼 장치를 지정합니다.

SNMP > SNMP > SNMP 사용자

이 페이지는 SNMPv3 사용을 위한 SNMP 사용자 테이블을 유지 관리하는 데 사용됩니다. SNMPv3는 MIB OID를 사용하여 사용자를 허용하거나 제한하고 사용자와 스위치 간에 전송되는 SNMP 메시지도 암호화합니다.

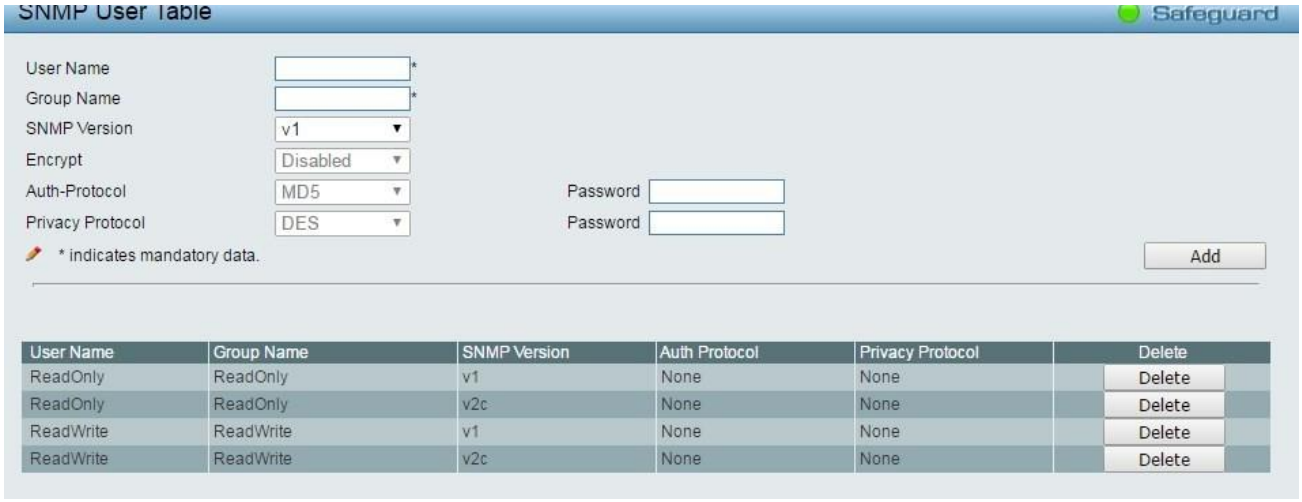


그림 4.155 - SNMP > SNMP > SNMP 사용자 테이블

User Name: 최대 32자의 SNMP 사용자 이름을 입력합니다.

Group Name: SNMP 사용자의 SNMP 그룹을 지정합니다.

SNMP Version: 사용자의 SNMP 버전을 지정합니다. SNMPv3만 메시지를 암호화합니다.

Encrypt: SNMP 버전이 V3인 경우 암호화를 사용하거나 사용하지 않도록 지정합니다.

Auth-Protocol/Password: HMAC-MD5-96 또는 HMAC-SHA를 인증 프로토콜로 지정합니다. 오른쪽 열에 SNMPv3 암호화를 위한 비밀번호를 입력합니다.

Priv-Protocol/Password: 권한 부여 안 함 또는 DES 56비트 암호화를 지정한 다음 오른쪽 열에 SNMPv3 암호화를 위한 암호를 입력합니다.

Add(**추가**)를 클릭하여 새 SNMP 사용자 계정을 만들고 **Delete**(삭제)를 클릭하여 기존 데이터를 제거합니다.

SNMP > SNMP > SNMP 그룹 테이블

이 페이지는 SNMP 사용자 테이블의 사용자와 연결된 SNMP 그룹 테이블을 유지 관리하는 데 사용됩니다. SNMPv3는 사용자 그룹에 대한 MIB 액세스 정책, 보안 정책을 직접 제어할 수 있습니다.

Group Name: 최대 32자의 SNMP 사용자 그룹을 지정합니다.

Read View Name: 스위치의 SNMP 에이전트에 대한 SNMP 읽기 권한이 허용되는 사용자의 SNMP 그룹 이름을 지정합니다.

Write View Name: 스위치의 SNMP 에이전트에 대한 SNMP 쓰기 권한이 허용되는 사용자의 SNMP 그룹 이름을 지정합니다.

Security Model: SNMP 보안 모델을 선택합니다.

SNMPv1 - SNMPv1은 보안 기능을 지원하지 않습니다.

SNMPv2 - SNMPv2는 중앙 집중식 및 분산 네트워크 관리 전략을 모두 지원합니다. 여기에는 SMI(관리 정보 구조)의 개선 사항이 포함되어 있으며 몇 가지 보안 기능이 추가되었습니다.

SNMPv3 - SNMPv3는 네트워크를 통한 인증 및 패킷 암호화의 조합을 통해 디바이스에 대한 보안 액세스를 제공합니다.

Security Level: 이 기능은 SNMPv3 보안 수준을 선택한 경우에만 사용할 수 있습니다.

NoAuthNoPriv - 스위치와 SNMP 관리자 간에 전송된 패킷에 대한 권한 부여 및 암호화가 없습니다.

AuthNoPriv - 권한 부여가 필요하지만 스위치와 SNMP 관리자 간에 전송되는 패킷에 대한 암호화는 필요하지 않습니다.

AuthPriv – 스위치와 SNMP 관리자 간에 전송되는 패킷에는 권한 부여와 암호화가 모두 필요합니다.

Notify View Name(알림 보기 이름): 스위치의 SNMP 에이전트에서 생성된 SNMP 트랩 메시지를 받을 수 있는 사용자의 SNMP 그룹 이름을 지정합니다.

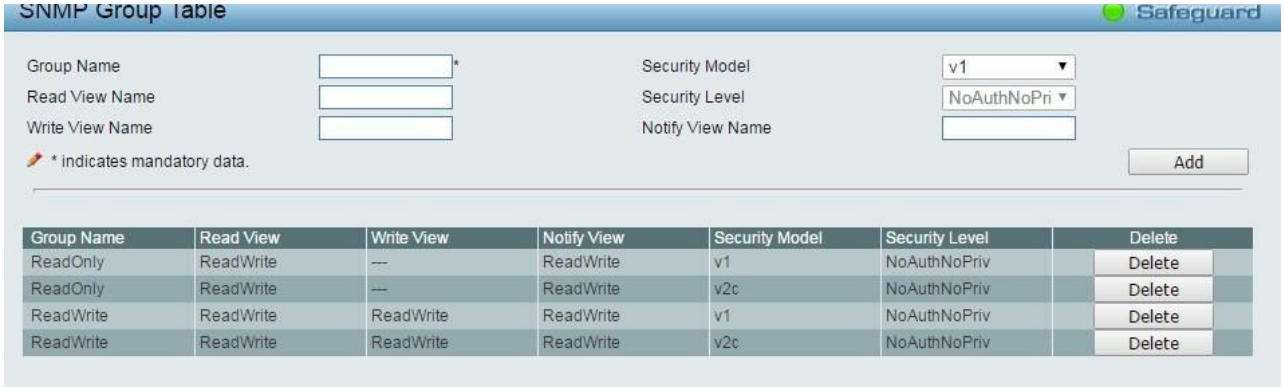


그림 4.156 - SNMP > SNMP > SNMP 그룹 테이블

SNMP > SNMP > SNMP 보기

이 페이지에서는 원격 SNMP 관리자가 액세스할 수 있는 MIB 객체를 정의하는 커뮤니티 문자열에 대한 SNMP 보기를 유지할 수 있습니다.

그림 4.157 - SNMP > SNMP > SNMP 보기

View Name: 보기의 이름(최대 32자)입니다.

Subtree OID: 뷰의 OID(개체 식별자) 하위 트리입니다. OID는 SNMP 관리자에 의해 액세스에서 포함되거나 제외될 개체 트리(MIB 트리)를 식별합니다.

OID Mask: 하위 트리 OID의 마스크입니다. 1은 이 개체 번호가 관련되어 있음을 의미하고, 0은 관련이 없음을 의미합니다. 예를 들어 마스크 1.1.1.1.1.1.1.0이 있는 1.3.6.1.2.1.1은 1.3.6.1.2.1.X를 의미합니다.

View Type: SNMP 관리자가 액세스할 수 있는 구성된 OID를 포함 또는 제외로 지정합니다.

Add(**추가**)를 클릭하여 새 보기를 만들고, **Delete(삭제**)를 클릭하여 기존 보기를 제거합니다.

SNMP > SNMP > SNMP 커뮤니티

이 페이지는 동일한 커뮤니티 문자열을 사용하는 SNMP 관리자의 SNMP 커뮤니티 문자열을 유지 관리하는 데 사용되며, 스위치의 SNMP 에이전트에 대한 액세스 권한을 얻을 수 있습니다.

Community Name: 커뮤니티 이름

User Name (View Policy): SNMP 커뮤니티에서 액세스할 수 있는 MIB 개체에 대한 읽기/쓰기 또는 읽기 전용 수준 권한을 지정합니다.

그림 4.158 – SNMP > SNMP > SNMP 커뮤니티

Add(**추가**)를 클릭하여 새 SNMP 커뮤니티를 생성하고, **Delete(삭제**)를 클릭하여 기존 커뮤니티를 제거합니다.

SNMP > SNMP > SNMP 호스트

이 SNMP 호스트 페이지는 SNMP 트랩 수신자를 구성하기 위한 것입니다.

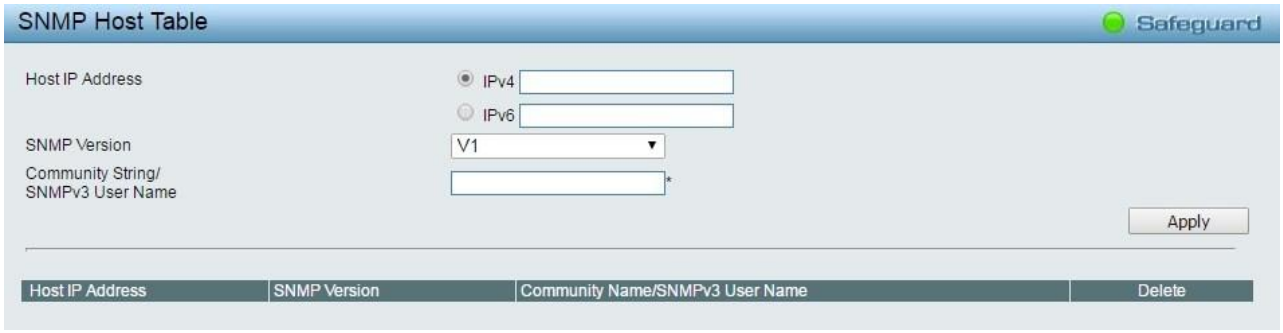


그림 4.159 - SNMP > SNMP > SNMP 호스트

Host IP Address: IPv4 또는 IPv6을 선택하고 SNMP 관리 호스트의 IP 주소를 지정합니다.

SNMP Version: 관리 호스트에 사용할 SNMP 버전을 지정합니다.

Community String/SNMPv3 User Name: 관리 호스트의 커뮤니티 문자열 또는 SNMPv3 사용자 이름을 지정합니다.

Apply(적용)**를 클릭하여** 새 SNMP 호스트를 생성하고, **Delete(삭제**)를 클릭하여 기존 호스트를 제거합니다.

SNMP > SNMP > SNMP 엔진 ID

엔진 ID는 스위치에서 SNMPv3 엔진을 식별하는 데 사용되는 고유 식별자입니다.

엔진 ID를 입력한 다음 Apply(**적용**)를 클릭하여 변경 사항을 적용하고 **Default(기본값**)를 클릭하여 기본값으로 재설정합니다.

그림 4.160 - SNMP > SNMP > SNMP 엔진 ID

SNMP > RMON > RMON 전역 설정

사용자는 스위치의 SNMP 기능에 대한 RMON(Remote Monitoring) 상태를 활성화 및 비활성화할 수 있습니다. 또한 RMON Rising and Falling Alarm Traps를 활성화 및 비활성화할 수 있습니다. **적용** 을 클릭하여 효과를 만듭니다.

그림 4.161 - SNMP > RMON > RMON 전역 설정

SNMP > RMON > RMON 통계

RMON Statistics Configuration 페이지에는 RMON 이더넷 통계 정보가 표시되며 사용자가 설정을 구성할 수 있습니다.

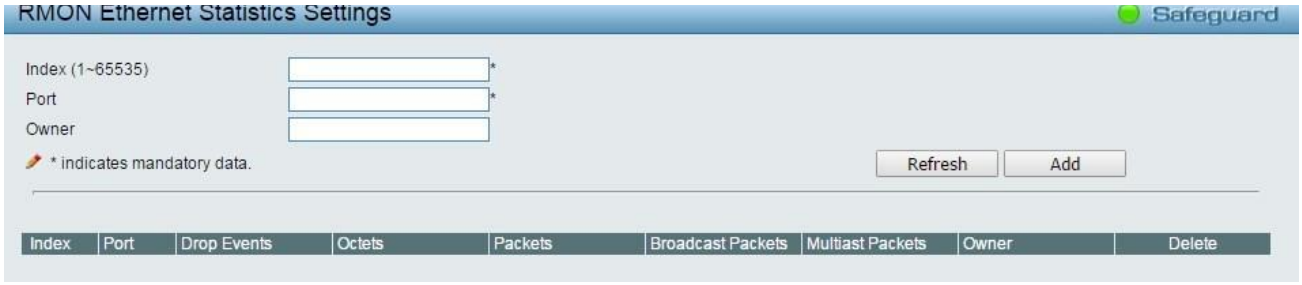


그림 4.162 - SNMP > RMON > RMON 이더넷 통계 구성

RMON 이더넷 통계 구성에는 다음 필드가 포함되어 있습니다.

Index (1 - 65535): RMON 이더넷 통계 항목 번호를 나타냅니다.

Port: RMON 정보를 가져온 포트를 지정합니다.

Owner: RMON 정보를 요청한 RMON 스테이션 또는 사용자를 표시합니다.

Add(**추가**)를 클릭하여 구성을 적용하고 **Refresh(새로 고침**)를 클릭하여 테이블 정보를 다시 표시합니다.

SNMP > RMON > RMON 기록

RMON History Control Configuration 페이지에는 포트에서 가져온 데이터 샘플에 대한 정보가 포함되어 있습니다. 예를 들어, 샘플에는 인터페이스 정의 또는 폴링 기간이 포함될 수 있습니다.

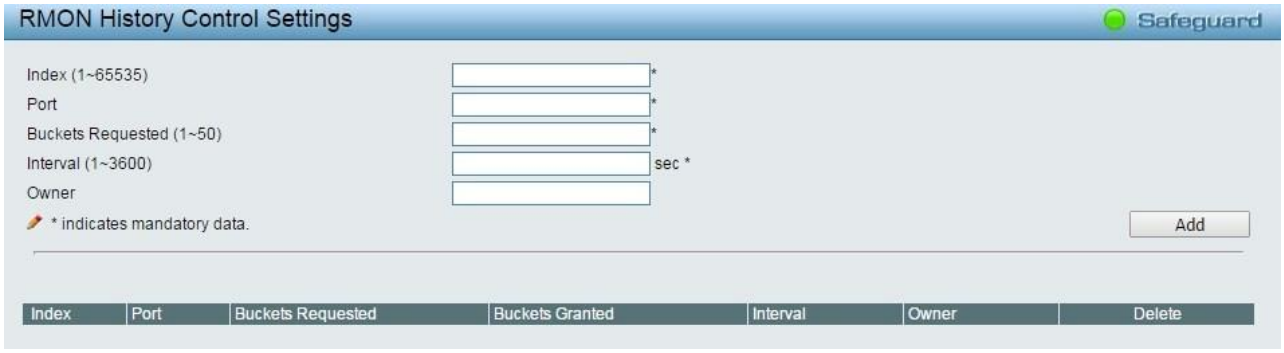


그림 4.163 - SNMP > RMON > RMON 기록 제어 설정

History Control Configuration(기록 제어 구성)에는 다음 필드가 포함되어 있습니다.

Index (1 - 65535): 히스토리 컨트롤 항목 번호를 나타냅니다.

Port: RMON 정보를 가져온 포트를 지정합니다.

Buckets Requested (1 ~ 50): 장치가 저장하는 버킷의 수를 지정합니다.

Interval (1 ~ 3600): 포트에서 샘플링을 가져오는 시간(초)을 나타냅니다. 필드 범위는 *1-3600*입니다. 기본값은 *1800*초(30분과 같음)입니다.

Owner: RMON 정보를 요청한 RMON 스테이션 또는 사용자를 표시합니다. Apply(**적용**) 버튼을 클릭하여 변경 사항을 적용합니다.

SNMP > RMON > RMON 경보

RMON Alarm Settings(RMON 경보 설정) 페이지에서는 사용자가 네트워크 경보를 구성할 수 있습니다. 네트워크 경보는 네트워크 문제 또는 이벤트가 감지될 때 발생합니다.

그림 4.164 - SNMP > RMON > RMON 경보 설정

구성에는 다음 필드가 포함되어 있습니다.

Index (1 - 65535): 특정 알람을 나타냅니다.

Variable: 선택한 MIB 변수 값을 지정합니다.

Rising Threshold (0 ~ 2^31-1): 상승 임계값 알람을 트리거하는 상승 카운터 값을 표시합니다.

Rising Event Index (1 ~ 65535): 특정 알람을 트리거하는 이벤트를 표시합니다. 가능한 필드 값은 사용자 정의 RMON 이벤트입니다.

Owner: 알람을 정의한 장치 또는 사용자를 표시합니다.

Interval (1 ~ 2^31-1): 알람 간격 시간을 초 단위로 정의합니다.

Sample type: 선택한 변수에 대한 샘플링 방법을 정의하고 값을 임계값과 비교합니다. 가능한 필드 값은 다음과 같습니다.

Delta value – 현재 값에서 마지막으로 샘플링된 값을 뺍니다. 값의 차이는 임계값과 비교됩니다.

Absolute value(절대값) – 샘플링 간격이 끝날 때의 임계값과 값을 직접 비교합니다.

Falling Threshold (0 ~ 2^31-1): 하강 임계값 알람을 트리거하는 하강 카운터 값을 표시합니다.

Falling Event Index (1 ~ 65535): 특정 알람을 트리거하는 이벤트를 표시합니다. 가능한 필드 값은 사용자 정의 RMON 이벤트입니다.

Add(**추가**)를 클릭하여 구성을 적용합니다.

SNMP > RMON > RMON 이벤트

RMON Event(RMON 이벤트) 페이지에는 RMON 이벤트 통계를 정의, 수정 및 보기 위한 필드가 포함되어 있습니다.

그림 4.165 - SNMP > RMON > RMON 이벤트 설정

RMON 이벤트 페이지에는 다음 필드가 있습니다.

Index (1~ 65535): 이벤트를 표시합니다.

Description: 사용자 정의 이벤트 설명을 지정합니다.

Type: 이벤트 유형을 지정합니다. 가능한 값은 다음과 같습니다.

None – 이벤트가 발생하지 않았음을 나타냅니다.

Log – 이벤트가 로그 항목임을 나타냅니다.

SNMP Trap - 이벤트가 트랩임을 나타냅니다.

Log and Trap(로그 및 트랩) – 이벤트가 로그 항목이자 트랩임을 나타냅니다.

Community: 이벤트가 속한 커뮤니티를 지정합니다.

Owner: 이벤트가 발생한 시간을 지정합니다.

Add(**추가)**를 클릭하여 새 RMON 이벤트를 추가합니다.

Monitoring > Port Statistics

Port Statistics(포트 통계) 화면에는 각 포트 패킷 수의 상태가 표시됩니다.

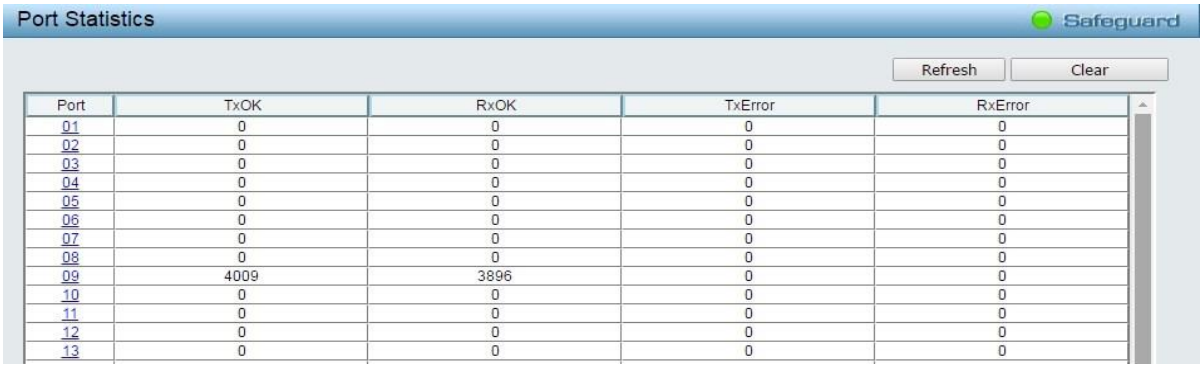


그림 4.166 - > 포트 통계 모니터링

Refresh: 수집 및 표시되는 세부 정보를 갱신합니다.

Clear: 표시된 세부 정보를 재설정합니다.

TxOK: 성공적으로 전송된 패킷 수입니다.

RxOK: 성공적으로 수신된 패킷 수입니다.

TxError: 오류를 일으킨 전송된 패킷 수입니다.

RxError: 오류를 일으킨 수신된 패킷 수입니다.

개별 포트의 통계를 보려면 연결된 포트 번호 중 하나를 클릭하여 자세한 내용을 확인하십시오.

그림 4.167 - 모니터링 > 포트 통계

Back: 통계 기본 페이지로 돌아갑니다.

Refresh: 수집 및 표시된 세부 정보를 갱신합니다.

Clear: 표시된 세부 정보를 재설정합니다.

모니터링 > 케이블 진단

케이블 진단은 주로 관리자와 고객 서비스 담당자가 구리 케이블 품질을 검사할 수 있도록 설계되었습니다. 케이블에서 발생한 케이블 오류의 유형을 신속하게 파악합니다.
포트를 선택한 다음 **Test Now(지금 테스트**) 버튼을 클릭하여 진단을 시작합니다.

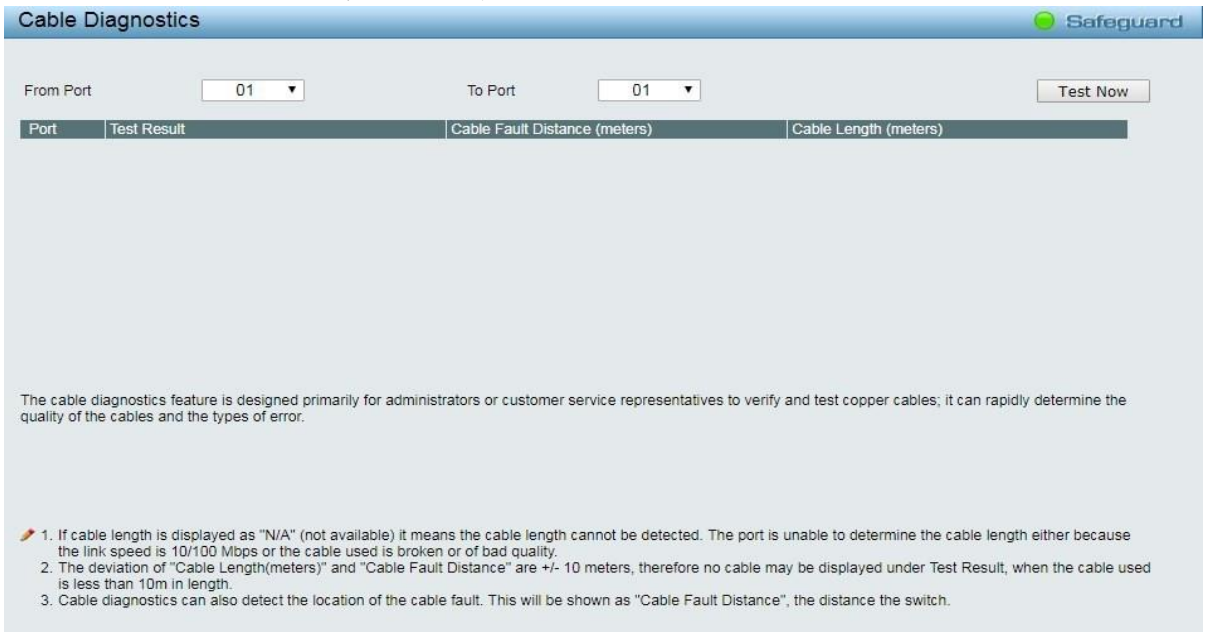


그림 4.168 - 모니터링 > 케이블 진단

Test Result(테스트 결과): 케이블 진단 결과에 대한 설명입니다.

- **OK** 은 케이블이 연결에 적합함을 의미합니다.
- **Short in Cable**은 RJ45 케이블의 전선이 어딘가에 접촉되어 있을 수 있음을 의미합니다.
- **Open in Cable**은 RJ45 케이블의 전선이 끊어졌거나 케이블의 다른 쪽 끝이 단순히 분리되었을 수 있음을 의미합니다.
- **Mismatched**는 케이블 진단 중에 다른 오류가 발생했음을 의미합니다. 동일한 포트를 선택하고 다시 테스트하십시오.
- **Line Driver:** 고임피던스가 감지됩니다. 출력 시나리오는 전원 끄기 링크 파트너에 대한 케이블 플러그입니다.

Cable Fault Distance (meters): 스위치 포트에서 케이블 결함까지의 거리를 나타내며 케이블이 2미터 미만인 경우 "케이블 없음"이 표시됩니다.

Cable Length (meter): 테스트 결과가 정상으로 표시되면 케이블의 총 길이에 대해 케이블 길이가 표시됩니다. 케이블 길이는 <50미터, 50~80미터, 80~100미터, 100~140미터, >140미터의 네 가지 유형으로 분류됩니다.

참고: 케이블 길이 감지는 기가비트 포트에서만 유효합니다.

참고: Cable Diagnostics 기능을 활성화하기 전에 Power Saving 기능이 비활성화되어 있는지 확인하십시오.

참고: "케이블 길이(미터)" 및 "케이블 결함 거리"의 편차는 +/- 10미터이므로 사용된 케이블의 길이가 10m 미만인 경우 테스트 결과에 케이블이 표시되지 않을 수 있습니다.

모니터링 > 시스템 로그

시스템 로그 페이지는 디바이스가 부팅된 시간, 포트 작동 방식, 사용자가 로그인한 시간, 세션 시간이 초과된 시간 및 기타 시스템 정보를 포함하여 시스템 로그에 대한 정보를 제공합니다.

그림 4.169 - > 시스템 로그 모니터링

ID: 시스템 로그 항목의 증가된 카운터를 표시합니다. 최대 항목은 500개입니다.

Time: 로그가 입력된 일, 시간, 분 단위로 표시합니다.

Log Description: 기록된 설명 이벤트를 표시합니다.

Severity: 기록된 이벤트의 심각도 수준을 표시합니다.

Refresh(새로 고침)를 클릭하여 페이지를 갱신하고 Clear(**지우기**)를 클릭하여 모든 로그 항목을 지웁니다.

참고: 시스템 로그는 재설정되며 스위치가 재부팅된 후에는 저장되지 않습니다.

모니터링 > 핑 테스트

"Ping"은 지정된 목적지에 필요한 최소 시간을 측정하는 방법입니다.

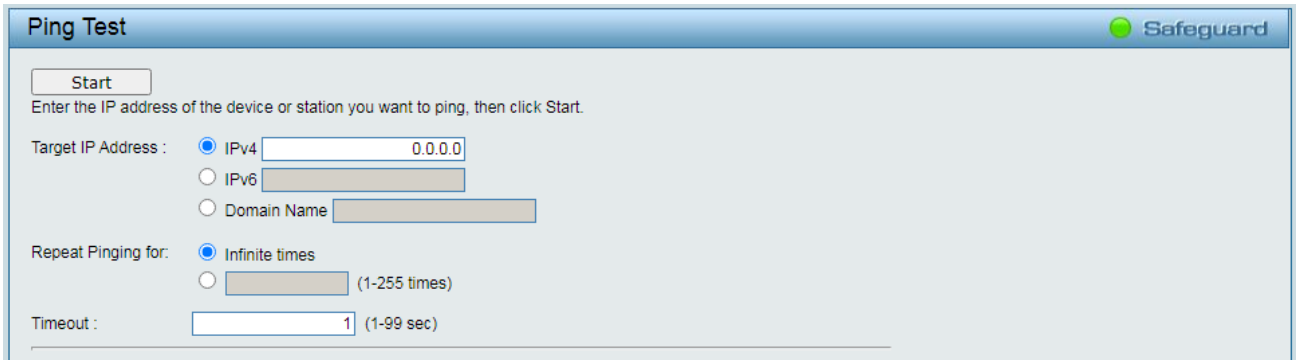


그림 4.166 - 모니터링 > Ping 테스트

Target IP Address: IPv4, IPv6 **또는** 도메인 이름 **중에서 선택할 수 있는 주소 모드**.
Repeat Pinging for: 1-255회 **또는** 무한 횟**수에서 구성 가능한 값**.
Timeout: 1-99초**에서 구성 가능한 시간 제한 값**입니다.


D-Link
Building Networks for People