목차

1. Introduction

이 매뉴얼의 소프트웨어 설명은 소프트웨어 릴리스 2.01 을 기준으로 작성되었습니다.
여기 나열된 기능은 DGS-1250 시리즈 스위치에서 지원되는 기능의 일부입니다.

Logging into the Web UI

웹 UI 에 접속하려면 표준 웹 브라우저를 열고 브라우저의 주소 창에 스위치의 IP 주소를 입력한 후 **ENTER** 키를 누르십시오.

알림: 스위치의 기본 IP Address 는 10.90.90.90 이고 서브넷 마스크는 255.0.0.0 입니다.

참고: 기본 사용자 이름은 *admin 이고 암호는 admin 입니다*.

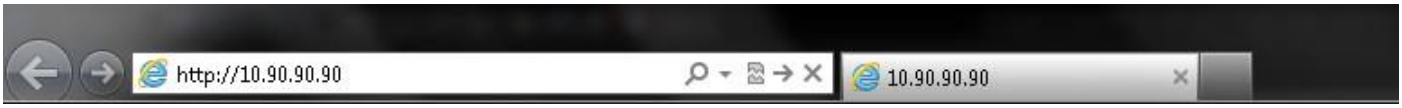

그림 2-1 Internet Explorer 에서 IP Address 입력 표시

Enter 키를 누르면 아래와 같이 다음과 같은 인증 창이 나타납니다.

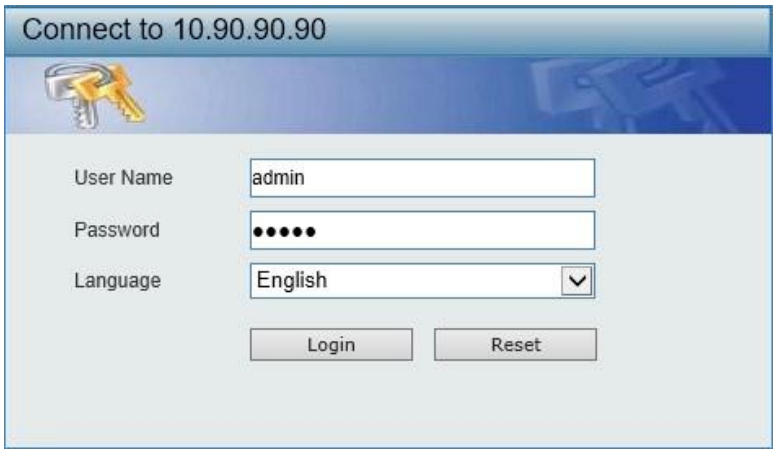

그림 2-2 웹 UI 로그인 창

해당 필드에 User Name 과 Password 를 입력하고 Login 버튼을 클릭합니다.
Login 버튼을 클릭하면 웹 UI 가 열립니다.
스위치 웹 UI 에서 사용할 수 있는 관리 기능은 아래의 장에서 설명됩니다.

참고: Switch 는 입력 값에 대해 ASCII 문자만 지원합니다.

Smart Wizard

웹 UI 에 처음 성공적으로 연결하면 내장된 Smart Wizard 웹 유틸리티가 실행됩니다.
이 마법사는 스위치에 처음 연결할 때 필요한 기본 설정 단계를 사용자에게 안내합니다.

Step 1 - Web Mode

스위치는 표준 모드와 감시 모드의 두 가지 웹 모드를 지원합니다.

- 표준 모드는 스위치에서 대부분의 소프트웨어 기능을 구성, 관리 및 모니터링하는 데 사용됩니다.
- 감시 모드는 추가 웹 스위치에서 지원하는 감시 기능을 통해 사용자를 지원하도록 특별히 설계된 모드입니다.

알림: 웹 모드는 스위치의 웹 UI 에 한 사용자 세션만 연결되어 있을 때만 변경할 수 있습니다.

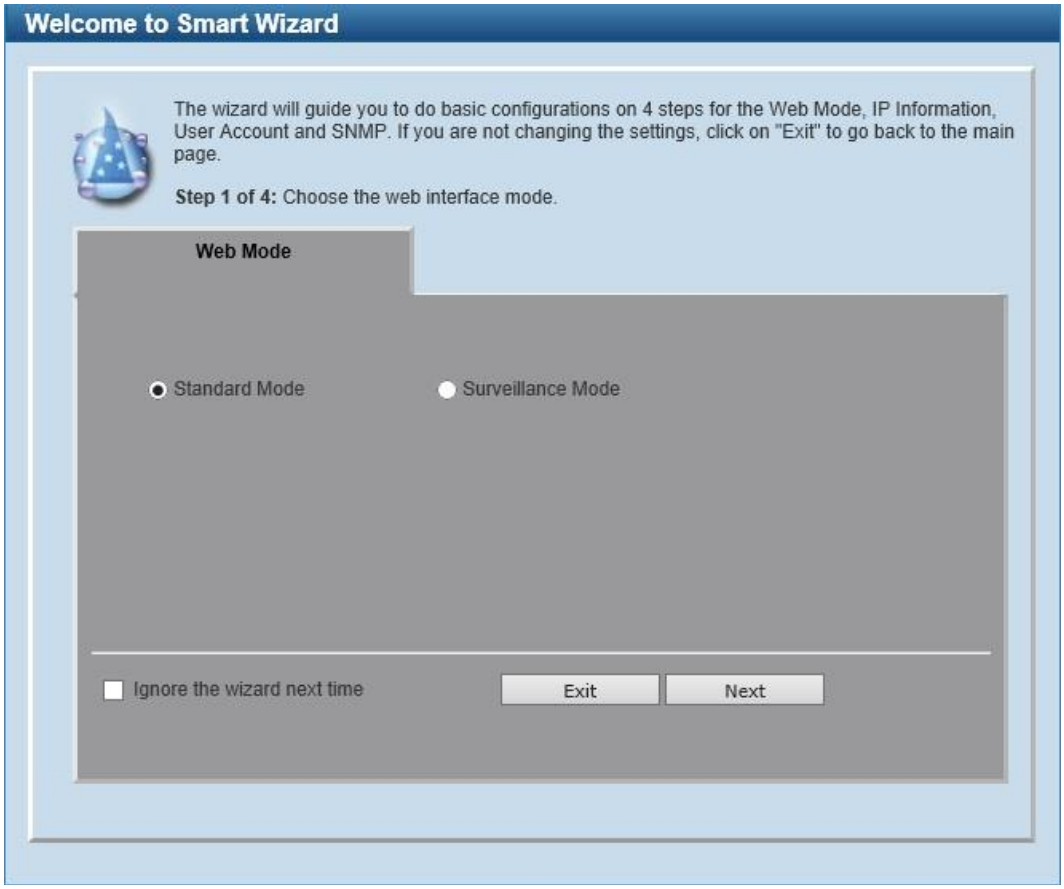

그림 2-3 웹 모드

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Standard Mode	스마트 마법사가 완료된 후 표준 모드에 액세스하려면 이 옵션을 선택합니다.
Surveillance Mode	스마트 마법사가 완료된 후 감시 모드에 액세스하려면 이 옵션을 선택합니다.

다음 로그인 시 스마트 마법사를 건너뛰려면 Ignore the wizard next time 옵션을 선택합니다.

Exit 버튼을 클릭하여 변경 사항을 취소하고 스마트 마법사를 종료한 다음 웹 UI 를 계속합니다.

Next 버튼을 클릭하여 변경 사항을 적용하고 다음 단계를 계속합니다.

Step 2 - System IP Information

이 단계에서는 시스템 IP 정보를 구성할 수 있습니다.

알림: 스위치는 30 초마다 감시 장치를 탐색합니다. 감시 장치가 스위치와 동일한 서브넷에 있지 않은 경우, 자동으로 검색되지 않습니다. ONVIF 카메라를 감시 모드 웹 UI 에 자동으로 추가하려면 스위치 관리 IP 를 감시 장치와 동일한 서브넷에 배치하십시오.

그림 2-4) 시스템 IP 정보

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Static	스위치에 대한 IP Address 설정을 수동으로 할당하고 구성하려면 이 옵션을 선택합니다.
DHCP	스위치의 DHCP 서버에서 IP Address 설정을 자동으로 가져오려면 이 옵션을 선택합니다.
IP Address	Static 옵션을 선택한 후 여기에 스위치의 IP Address 를 수동으로 입력합니다.
Netmask	정적 옵션을 선택한 후 여기에서 Netmask 옵션을 수동으로 선택합니다.
Gateway	정적 옵션을 선택한 후 여기에 기본 게이트웨이의 IP Address 를 수동으로 입력합니다.

다음 로그인 시 스마트 마법사를 건너뛰려면 Ignore the wizard next time 옵션을 선택합니다.

Exit 버튼을 클릭하여 변경 사항을 취소하고 스마트 마법사를 종료한 다음 웹 UI 를 계속합니다.

Next 버튼을 클릭하여 변경 사항을 적용하고 다음 단계를 계속합니다.

Step 3 - User Accounts Settings

이 단계에서 사용자 계정 설정을 구성할 수 있습니다.

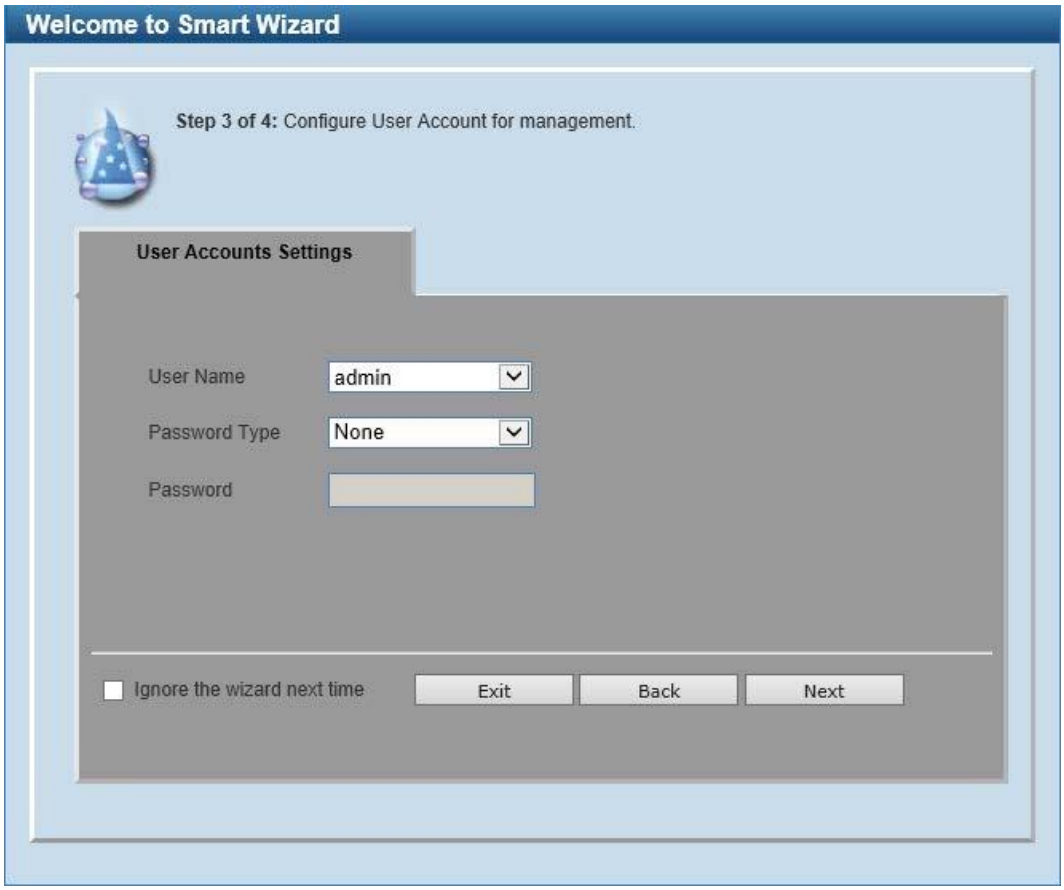

그림 2-5) 사용자 계정 설정

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
User Name	여기에서 사용자 이름을 선택합니다.
Password Type	여기에서 암호 유형을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • 없음 - 이 사용자 계정에 대해 암호를 구성하지 않도록 지정합니다. • Plain Text(일반 텍스트) - 이 사용자 계정의 암호가 일반 텍스트 형식이 되도록 지정합니다.
Password	Password Type(암호 유형)으로 Plain Text(일반 텍스트)를 선택한 후 여기에 사용자 계정의 암호를 입력합니다.

다음 로그인 시 스마트 마법사를 건너뛰려면 Ignore the wizard next time 옵션을 선택합니다.

Exit 버튼을 클릭하여 변경 사항을 취소하고 스마트 마법사를 종료한 다음 웹 UI 를 계속합니다.

Back 버튼을 클릭하여 변경 사항을 취소하고 이전 단계로 돌아갑니다.

Step 4 - SNMP Settings

이 단계에서는 SNMP 기능을 활성화 또는 비활성화 할 수 있습니다.

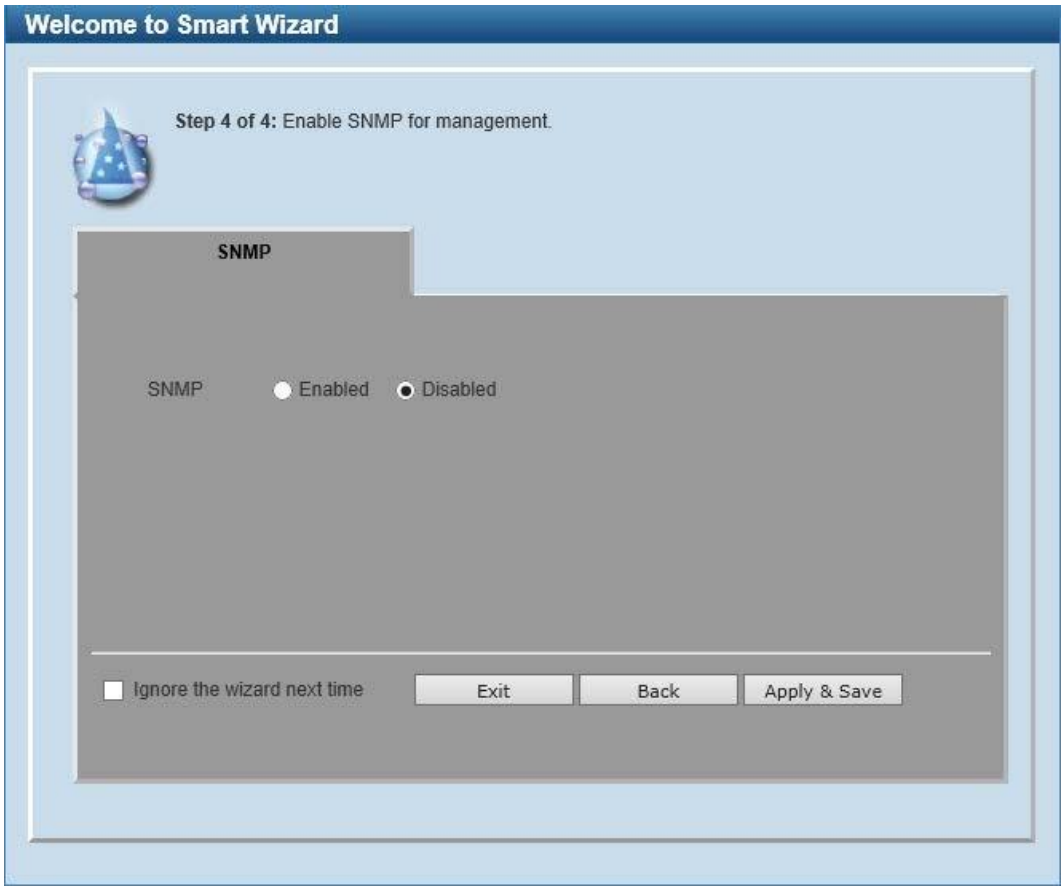

그림 2-6) SNMP 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
SNMP	여기에서 SNMP 기능을 활성화하거나 비활성화하려면 선택합니다.

다음 로그인 시 스마트 마법사를 건너뛰려면 Ignore the wizard next time 옵션을 선택합니다.

Exit 버튼을 클릭하여 변경 사항을 취소하고 스마트 마법사를 종료한 다음 웹 UI 를 계속합니다.

Back 버튼을 클릭하여 변경 사항을 취소하고 이전 단계로 돌아갑니다.

Apply & Save 버튼을 클릭하여 변경 사항을 적용하고 웹 UI 를 계속합니다.

Web User Interface (Web UI)

Areas of the User Interface

스위치의 웹 UI 는 별개의 영역으로 나눌 수 있습니다. 웹 UI 의 여러 영역은 구성 및 기능 모니터링을 단순화하기 위해 다양한 관리 효율성 옵션을 제공합니다.

Standard Mode

표준 모드에서 웹 UI 에 액세스 하면 다음이 표시됩니다.

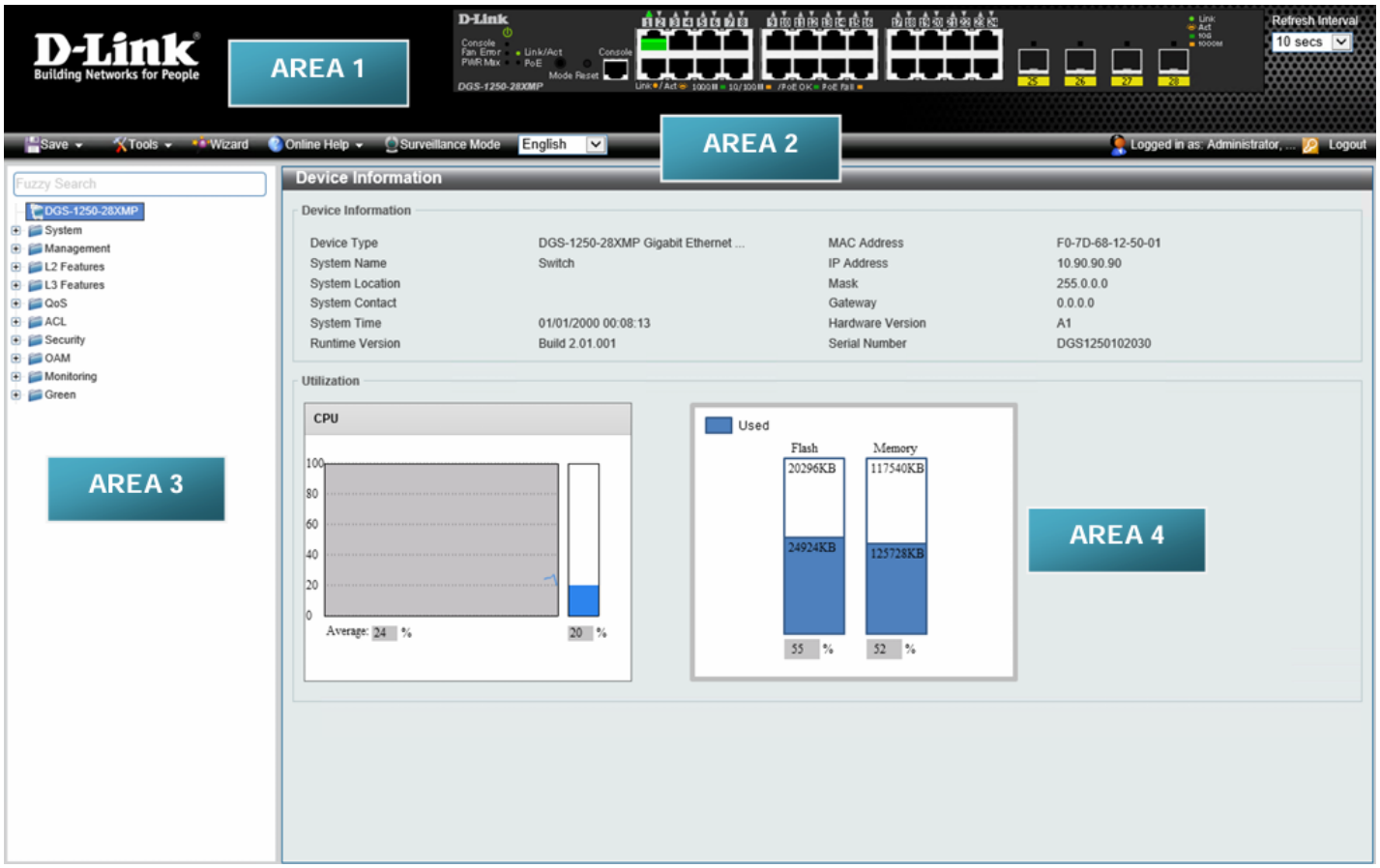

그림 2-7 Web UI(표준 모드)

Area Number	Description
AREA 1	이 영역에서는 스위치 전면 패널의 그래픽 실시간 이미지를 포트와 확장 모듈과 함께 표시합니다. 지정된 모드에 따라 포트 활동이 표시됩니다. 포트 모니터링과 같은 일부 관리 기능도 이곳에서 사용할 수 있습니다. D-Link 로고를 클릭하면 D-Link 웹사이트로 이동합니다.
AREA 2	이 영역에는 **Save**, **Tools**, **Wizard**, **Online Help**, 감시 모드에서 웹 UI 에 접근, 사용자 정의 언어 설정, **Logout** 옵션과 같은 기능에 접근할 수 있는 도구 모음이 있습니다. **Surveillance Mode** 옵션을 클릭하여 스위치 모드를 표준 모드에서 감시 모드로 변경할 수 있습니다. 현재 웹 UI 에 로그인된 사용자 계정과 IP 주소도 이 도구 모음에 표시됩니다.
AREA 3	이 영역에서는 스위치 웹 UI 에서 사용할 수 있는 소프트웨어 기능이 하이퍼링크가 포함된 폴더로 그룹화되어 있습니다. 하이퍼링크를 클릭하면 **영역 4** 에서 창 프레임이 열립니다. 또한, 이 영역에는 특정 기능 키워드를 검색하여 해당 기능 링크를 쉽게 찾을 수 있는 검색 옵션이 포함되어 있습니다.
AREA 4	이 영역에서는 **영역 3** 에서 선택한 항목에 따라 구성 및 모니터링 창이 표시됩니다.

2. System

Device Information
System information Settings
Peripheral Settings
Port Configuration
PoE
System Log
Time and SNTP
Time Range

Device Information

Device Information 섹션에서 사용자는 스위치에 대한 기본 정보 목록을 볼 수 있습니다. 스위치에 로그온하면 자동으로 나타납니다. 다른 창을 본 후 장치 정보 창으로 돌아가려면 DGS-1250-28XMP 링크를 클릭하십시오.

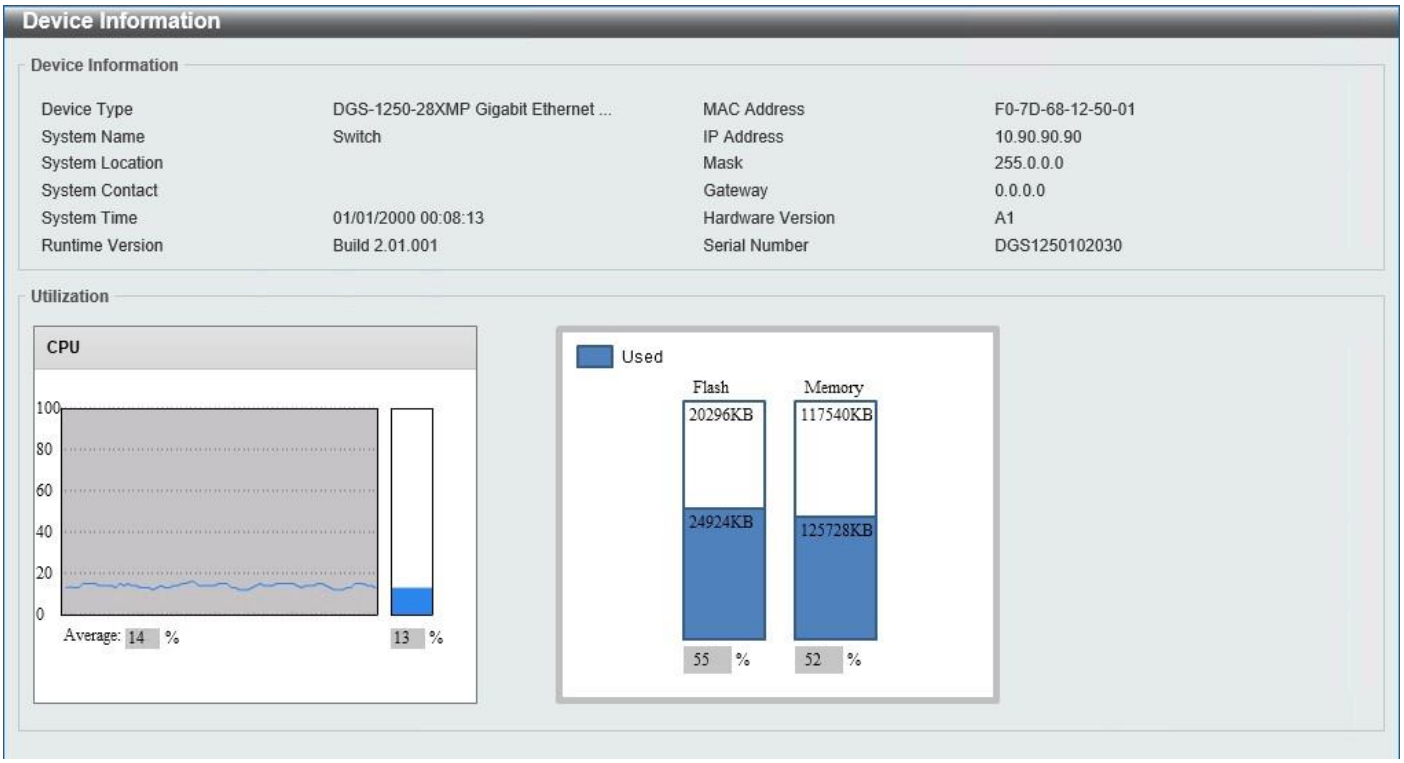

그림 3-1 장치 정보 창

System information Settings

이 창은 시스템 정보 설정 및 관리 Interface 구성 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > System Information Settings 설정을 클릭합니다.

그림 3-2) 시스템 정보 설정 창

시스템 정보 설정에서 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
System Name	여기에 스위치의 시스템 이름을 입력합니다. 이 이름은 스위치 네트워크에서 식별합니다.

System Location	여기에 스위치의 위치 설명을 입력합니다.
System Contact	여기에 스위치의 연락처 정보를 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Peripheral Settings

이 창은 환경 트랩 설정과 환경 온도 임계값 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > Peripheral Settings 를 클릭합니다.

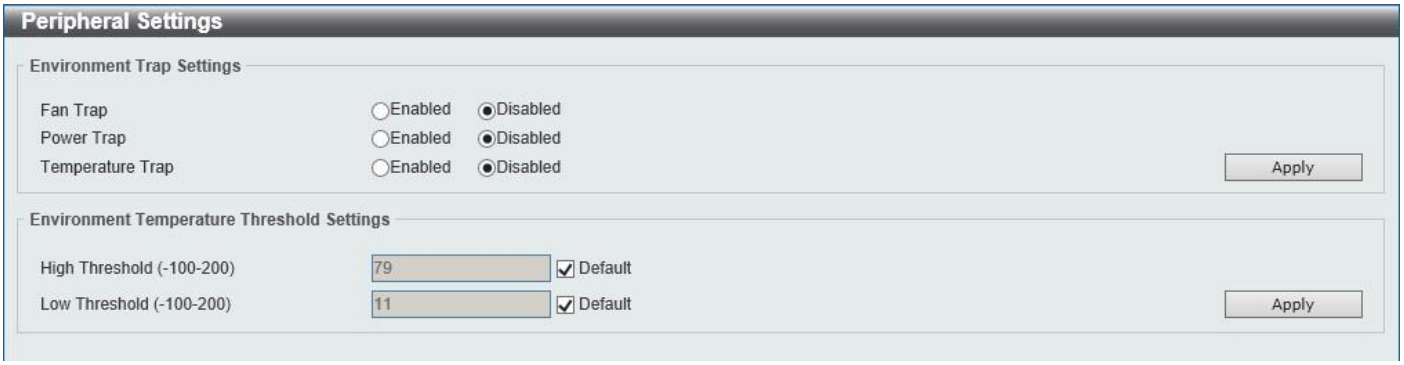

그림 3-3) 주변 장치 설정 창

Environment Trap Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Fan Trap	경고 팬 이벤트(fan failed 또는 fan recover)에 대한 팬 트랩 상태를 활성화하거나 비활성화하려면 선택합니다.
Power Trap	전원 이벤트 경고에 대한 전원 트랩 상태를 활성화하거나 비활성화하려면 선택합니다(전원 장애 또는 전원 복구).
Temperature Trap	경고 온도 이벤트(온도 임계값 초과 또는 온도 복구)에 대한 온도 트랩 상태를 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

환경 온도 임계값 설정에서 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
High Threshold	경고 온도 설정의 높은 임계값을 입력합니다. 범위는 섭씨 -100 도에서 200 도입니다. 기본값 확인란을 선택하여 기본값으로 돌아갑니다.
Low Threshold	경고 온도 설정의 하한 임계값을 입력합니다. 범위는 섭씨 -100 도에서 200 도입니다. 기본값 확인란을 선택하여 기본값으로 돌아갑니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Port Configuration

Port Settings

이 창은 스위치의 포트 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > Port Configuration > Port Settings 을 클릭합니다.

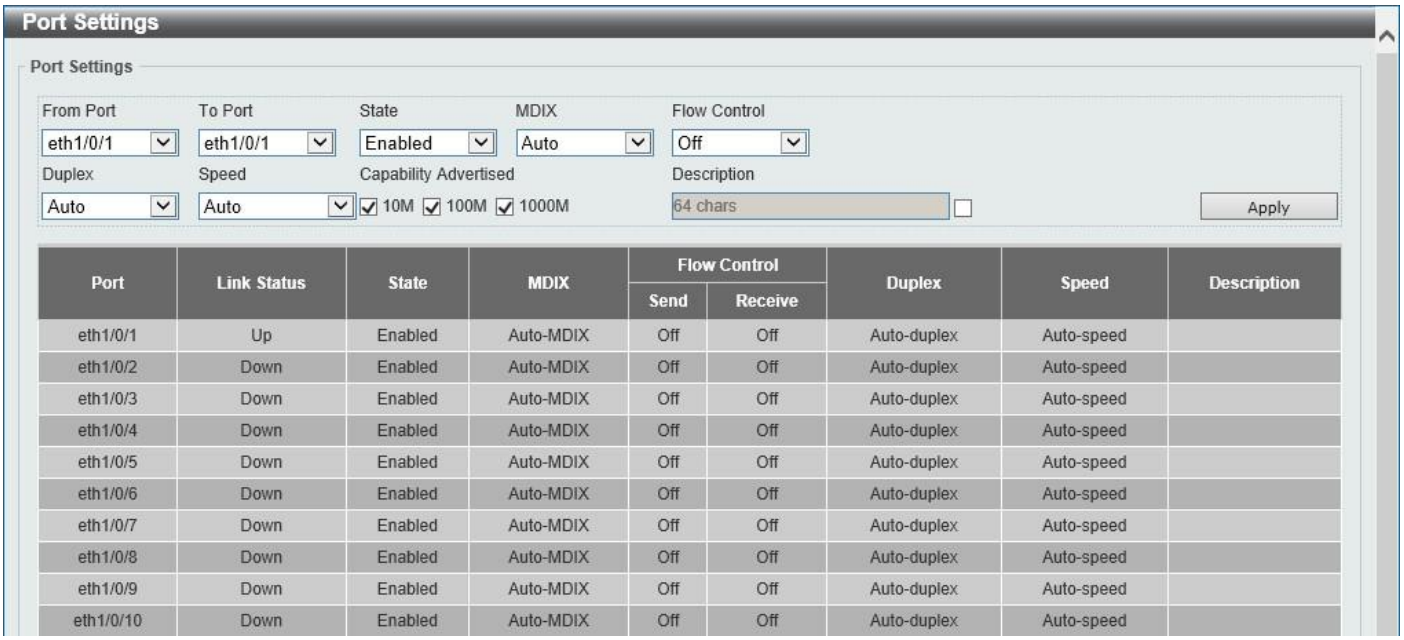

그림 3-4) 포트 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
State	여기에서 물리적 포트 상태를 활성화하거나 비활성화하려면 선택합니다.
MDIX	여기에서 MDIX(Medium Dependent Interface Crossover) 옵션을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Auto - 최적의 케이블 유형을 자동으로 감지하려면 이 옵션을 선택합니다. • Normal - 일반 케이블링에 대해 이 옵션을 선택합니다. 이 옵션을 선택하면 포트가 MDIX 모드에 있으며 직선 케이블 또는 크로스오버 케이블을 통해 다른 스위치의 포트(MDI 모드)를 사용하여 PC NIC 에 연결할 수 있습니다. • Cross - 크로스오버 케이블링에 대해 이 옵션을 선택합니다. 이 옵션을 선택하면 포트가 MDI 모드에 있으며 직선 케이블을 통해 다른 스위치의 포트(MDIX 모드)에 연결할 수 있습니다. 참고: 이 옵션은 10/100/1000Mbps RJ45 포트에서만 사용할 수 있습니다.
Flow Control	여기에서 흐름 제어를 켜거나 끄려면 선택합니다. 전이중으로 구성된 포트는 802.3x 흐름 제어를 사용하고 자동 포트는 두 개의 자동 선택을 사용합니다.
Duplex	여기에 사용된 듀플렉스 모드를 선택합니다. 선택할 수 있는 옵션은 Auto, Half 및 Full 입니다.

Speed	여기에서 포트 속도 옵션을 선택합니다. 이 옵션은 선택한 포트의 연결 속도가 지정된 속도로만 연결되도록 수동으로 강제합니다. Master 설정을 사용하면 포트에서 듀플렉스, 속도 및 물리적 레이어 유형과 관련된 기능을 광고할 수 있습니다. 마스터 설정은 연결된 두 물리 계층 간의 마스터 및 슬레이브 관계도 결정합니다. 이 관계는 두 물리적 레이어 간의 타이밍 제어를 설정하는 데 필요합니다. timing control 은 로컬 소스에 의해 마스터 물리 계층에 설정됩니다. 슬레이브 설정은 루프 타이밍을 사용하며, 타이밍은 마스터에서 수신한 데이터 스트림에서 나옵니다. 한 연결이 마스터로 설정된 경우 연결의 다른 쪽은 슬레이브로 설정되어야 합니다. 다른 컨피그레이션은 두 포트 모두에 대해 '링크 다운' 상태가 됩니다. 선택할 수 있는 옵션은 다음과 같습니다. • Auto - 구리 포트의 경우 자동 협상이 링크 파트너와 속도 및 흐름 제어 협상을 시작하도록 지정합니다. 파이버 포트의 경우 자동 협상이 링크 파트너와 클럭 및 흐름 제어를 협상하기 시작합니다. • 10M - 포트 속도를 10Mbps 로 강제 적용하도록 지정합니다. • 100M - 포트 속도를 100Mbps 로 강제 적용하도록 지정합니다. • 1000M - 포트 속도를 1Gbps 로 강제 적용하도록 지정합니다. • 1000M 마스터 - 포트 속도를 1Gbps 로 강제 적용하고 마스터로 작동하여 전송 및 수신 작업의 타이밍을 용이하게 하도록 지정합니다. • 1000M 슬레이브 - 포트 속도를 1Gbps 로 강제 적용하고 슬레이브로 작동하여 전송 및 수신 작업의 타이밍을 용이하게 하도록 지정합니다. • 10G - 포트 속도를 10Gbps 로 강제 적용하도록 지정합니다.
Capability Advertised	Speed 를 Auto 로 설정하면 자동 협상 중에 이러한 기능이 광고됩니다.
Description	확인란을 선택하고 여기에 해당 포트에 대한 설명을 입력합니다. 최대 64 자까지 입력할 수 있습니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Port Status

이 창은 스위치의 물리적 포트 상태 및 설정을 보는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > Port Configuration > Port Status 를 클릭합니다.

Port	Status	MAC Address	VLAN	Flow Control Operator		Duplex	Speed	Type
				Send	Receive			
eth1/0/1	Connected	F0-7D-68-12-50-02	1	Off	Off	Auto-Full	Auto-1000M	1000BASE-T
eth1/0/2	Not-Connected	F0-7D-68-12-50-03	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/3	Not-Connected	F0-7D-68-12-50-04	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/4	Not-Connected	F0-7D-68-12-50-05	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/5	Not-Connected	F0-7D-68-12-50-06	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/6	Not-Connected	F0-7D-68-12-50-07	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/7	Not-Connected	F0-7D-68-12-50-08	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/8	Not-Connected	F0-7D-68-12-50-09	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/9	Not-Connected	F0-7D-68-12-50-0A	1	Off	Off	Auto	Auto	1000BASE-T
eth1/0/10	Not-Connected	F0-7D-68-12-50-0B	1	Off	Off	Auto	Auto	1000BASE-T

그림 3-5) 포트 상태 창

Port Auto Negotiation

이 창은 자세한 포트 자동 협상 정보를 보는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > Port Configuration > Port Auto Negotiation 을 클릭합니다.

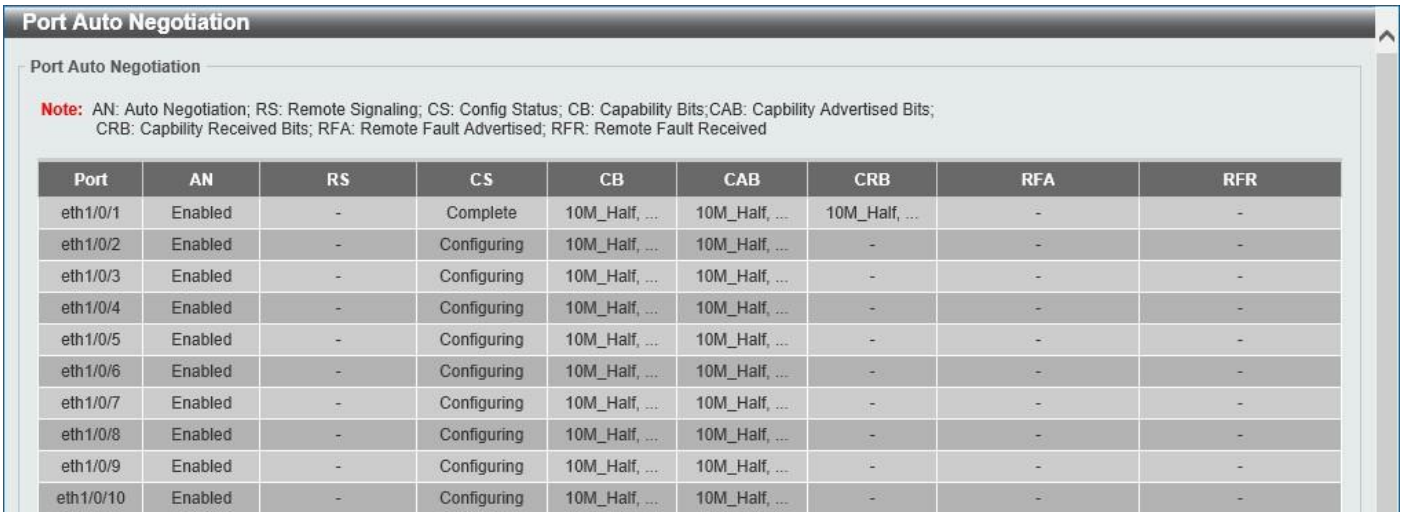

그림 3-6) 포트 자동 협상 창

Error Disable Settings

이 창은 오류 비활성화 원인으로부터 복구를 표시 및 구성하고 복구 간격을 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > Port Configuration > Error Disable Settings 을 클릭합니다.

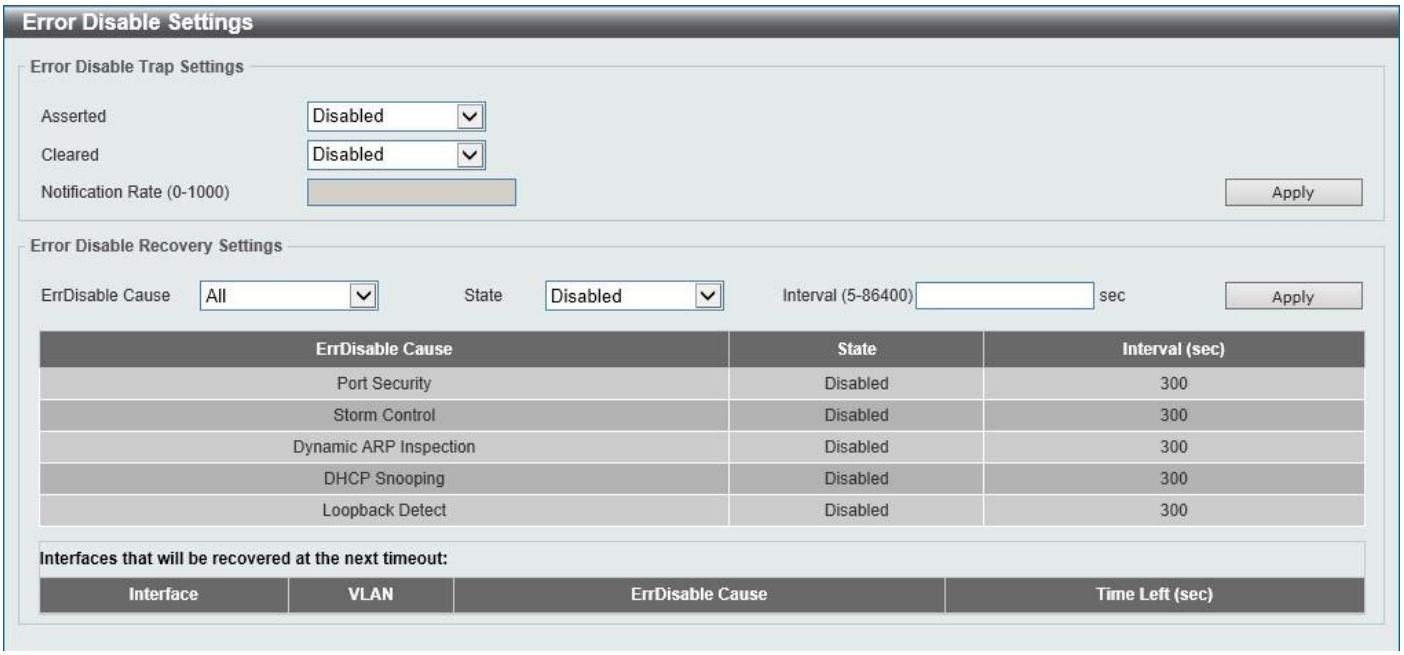

그림 3-7 오류 설정 비활성화 창

Error Disable Trap Settings 에 대해 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Asserted	오류 비활성화 상태로 전환하기 위한 알림을 사용하거나 사용하지 않도록 지정합니다.
Cleared	error-disabled 상태에서 벗어나기 위한 알림을 사용하거나 사용하지 않도록 지정합니다.

Notification Rate	여기에 알림 속도 값을 입력합니다. 분당 트랩 수를 설정합니다. 속도를 초과하는 패킷은 삭제됩니다. 범위는 0 에서 1000 사이입니다. 기본값(0)은 오류 비활성화 상태가 변경될 때마다 SNMP 트랩이 생성됨을 나타냅니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Error Disable Recovery Settings 에 대해 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
ErrDisable Cause	여기에서 오류 비활성화 원인을 선택합니다. 선택할 수 있는 옵션은 Port Security, Storm Control, Dynamic ARP Inspection, DHCP Snooping 및 Loopback Detect 입니다.
State	여기에서 오류 비활성화 복구 기능을 활성화하거나 비활성화하려면 선택합니다.
Interval	지정된 모듈로 인한 오류 상태에서 포트를 복구하는 데 걸리는 시간(초)을 입력합니다. 범위는 5 에서 86400 사이입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Jumbo Frame

이 창은 점보 프레임 크기 및 설정을 표시하고 구성하는 데 사용됩니다. 스위치는 점보 프레임을 지원합니다. 점보 프레임은 페이로드가 1,518 바이트 이상인 이더넷 프레임입니다. 스위치는 최대 프레임 크기가 최대 12,288 바이트인 점보 프레임을 지원합니다.

다음 창을 보려면 아래와 같이 System > Port Configuration > Jumbo Frame 을 클릭합니다.

그림 3-8 점보 프레임 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
최대 수신 프레임 크기	여기에 최대 수신 프레임 크기 값을 입력합니다. 이 값은 64 바이트에서 12288 바이트 사이여야 합니다. 기본적으로 이 값은 1536 바이트입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Interface Description

이 창은 스위치의 각 포트의 상태, 관리 상태 및 설명을 표시하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > Interface Description 을 클릭합니다.

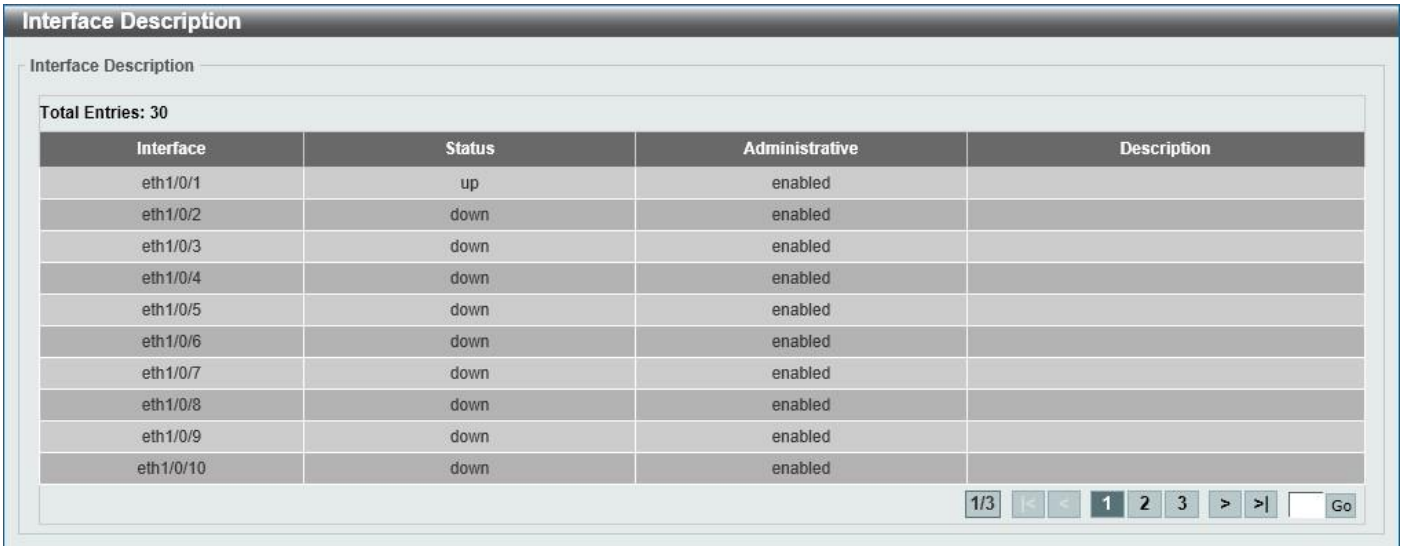

그림 3-9) Interface 설명 창

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

PoE

DGS-1250-28XMP 및 DGS-1250-52XMP 스위치는 IEEE 에서 정의한 PoE (Power over Ethernet)를 지원합니다 802.3af 및 802.3at. 모든 PoE 지원 포트는 최대 30W 의 전력을 공급할 수 있습니다. 스위치 포트는 카테고리 5 또는 카테고리 3 UTP 이더넷 케이블을 통해 PD(Powered Devices)에 약 48VDC 전원을 공급할 수 있습니다. 스위치는 표준 PSE(Power Sourcing Equipment) 핀아웃 대안 A 를 따르며, 핀 1, 2, 3 및 6 을 통해 전원이 전송됩니다. 스위치는 모든 D-Link 802.3af 지원 장치에서 작동합니다.

스위치에는 다음과 같은 PoE 기능이 포함되어 있습니다.

- 자동 검색은 PD 의 연결을 인식하고 자동으로 전원을 공급합니다.
- 자동 비활성화 기능은 다음 두 가지 조건에서 발생합니다.
  - o 총 전력 소비가 시스템 전력 제한을 초과하는 경우 o 포트당 전력 소비가 포트당 전력 제한을 초과하는 경우
- 액티브 회로 보호는 단락이 있는 경우 포트를 자동으로 비활성화합니다. 다른 포트는 활성 상태로 유지됩니다.

IEEE 802.3af/at 를 기반으로 다음 분류에 따라 전원이 수신 및 공급됩니다.

Class	PD 가 사용하는 최대 전력	스위치에서 공급하는 최대 전력
0	12.95 W	15.4 W
1	3.84 W	4 W
2	6.49 W	7 W
3	12.95 W	15.4 W
4	25.5 W	30 W

PoE System

이 창은 PoE 시스템을 구성하고 PoE 모듈에 대한 자세한 전원 정보 및 PoE 칩 매개변수를 표시하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > PoE > PoE System 을 클릭합니다.

그림 3-10 PoE 시스템 창

PoE 시스템에 대해 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Usage Threshold	사용량 임계값을 입력하여 로그를 생성하고 해당 표준 알림을 보냅니다. 범위는 1 에서 99% 사이입니다.
Policy Preempt	전력 부족 상황에서 더 높은 우선 순위로 새로 연결된 PD 에 전원을 해제하기 위해 더 낮은 우선 순위로 전원이 프로비저닝된 PD(Powered Device)의 연결 해제를 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
Trap State	PoE 트랩 알림 전송을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Show Detail 버튼을 클릭하여 창 하단에 있는 PoE 시스템 매개변수 테이블을 확인합니다.

Show Detail 버튼을 클릭하면 다음과 같은 창이 나타납니다.

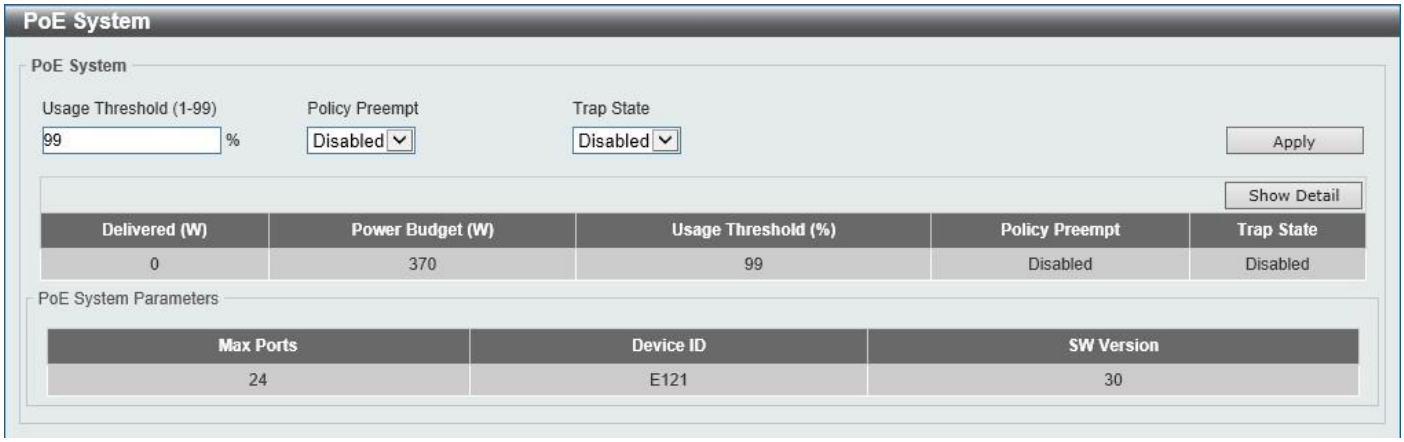

그림 3-11 PoE 시스템(세부 정보 표시) 창

PoE Status

이 창은 설명을 구성하고 각 포트의 PoE 상태를 표시하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > PoE > PoE Status 를 클릭합니다.

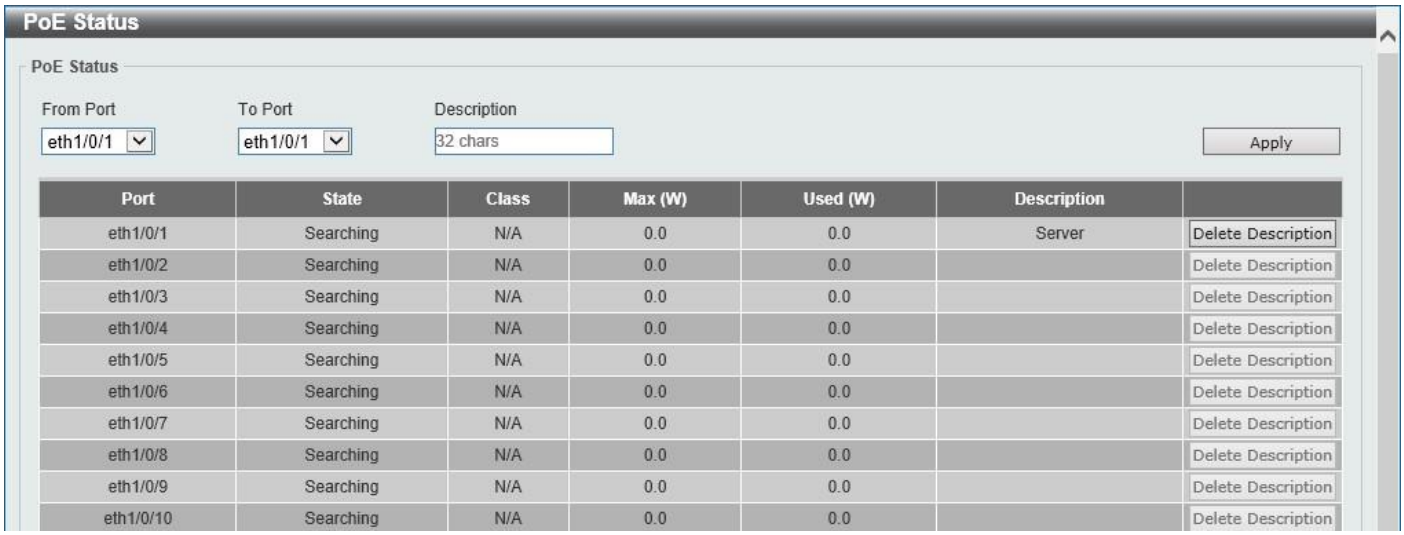

그림 3-12) PoE 상태 창

PoE 상태에 대해 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port – To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
Description	PoE Interface 에 연결된 PD 를 설명하는 텍스트를 입력합니다. 최대 길이는 32 자입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete Description(설명 삭제) 버튼을 클릭하여 항목에서 설명을 제거합니다.

PoE Configuration

이 창은 PoE 구성 설정을 표시하고 구성하는 데 사용됩니다.

참고: 스위치가 IEEE 802.3at PD 에 전원을 공급하지 못한 경우

- 포트에 연결된 PD 가 IEEE 802.3at 표준을 지원하는지 확인하십시오.
- 해당 포트에 대해 PoE 전력 제한 값을 30W 로 수동으로 구성합니다.

다음 창을 보려면 아래와 같이 System > PoE > PoE Configuration 을 클릭합니다.

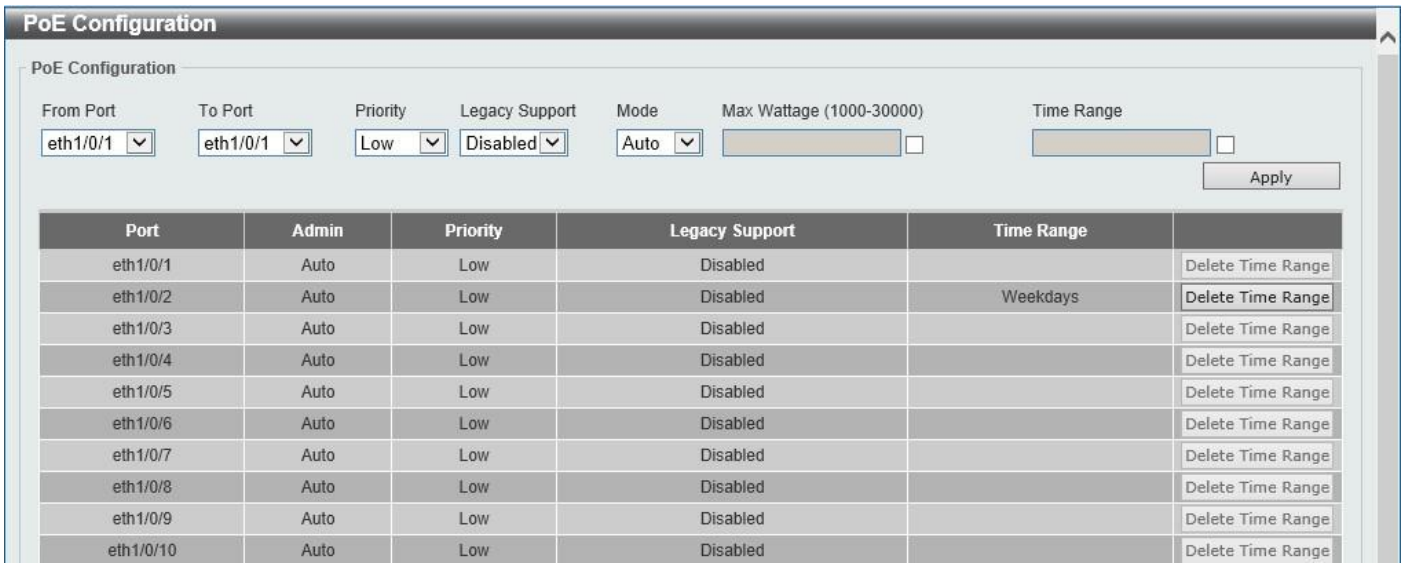

그림 3-13) PoE 구성 창

PoE Configuration 에 대해 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
Priority	포트에 전원을 프로비저닝하기 위한 우선 순위를 선택합니다. 선택할 수 있는 옵션은 Critical, High 및 Low 입니다.
Legacy Support	레거시 PD 의 지원을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
Mode	PoE 포트의 전원 관리 모드를 선택합니다. 선택할 수 있는 옵션은 Auto (자동) 및 Never(안 함)입니다.
Max Wattage	모드 드롭다운 목록에서 자동을 선택하면 이 옵션이 나타납니다. 확인란을 선택하고 자동 감지된 PD 에 프로비저닝할 수 있는 최대 전력량을 입력합니다. 값을 입력하지 않으면 PD 의 클래스가 프로비저닝할 수 있는 최대 와트를 자동으로 결정합니다. 최대 와트의 유효한 범위는 1000mW 에서 30000mW 사이입니다.
Time Range	모드 드롭다운 목록에서 자동을 선택하면 이 옵션이 나타납니다. 확인란을 선택하고 활성화 기간을 결정하기 위한 시간 범위의 이름을 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete Time Range 버튼을 클릭하여 항목에 대한 시간 범위 연결을 제거합니다.

PD Alive

이 창은 PoE 포트에 연결된 PD 에 대한 PD Alive 기능을 구성하는 데 사용됩니다. ping 기능은 PoE 포트에 연결된 PD 가 활성 상태인지 확인하는 데 사용됩니다. PD 가 비활성 상태인 것처럼 보이면 지정된 작업(재설정, 알림 또는 둘 다)이 수행됩니다.

다음 창을 보려면 아래와 같이 System > PoE > PD Alive 를 클릭합니다.

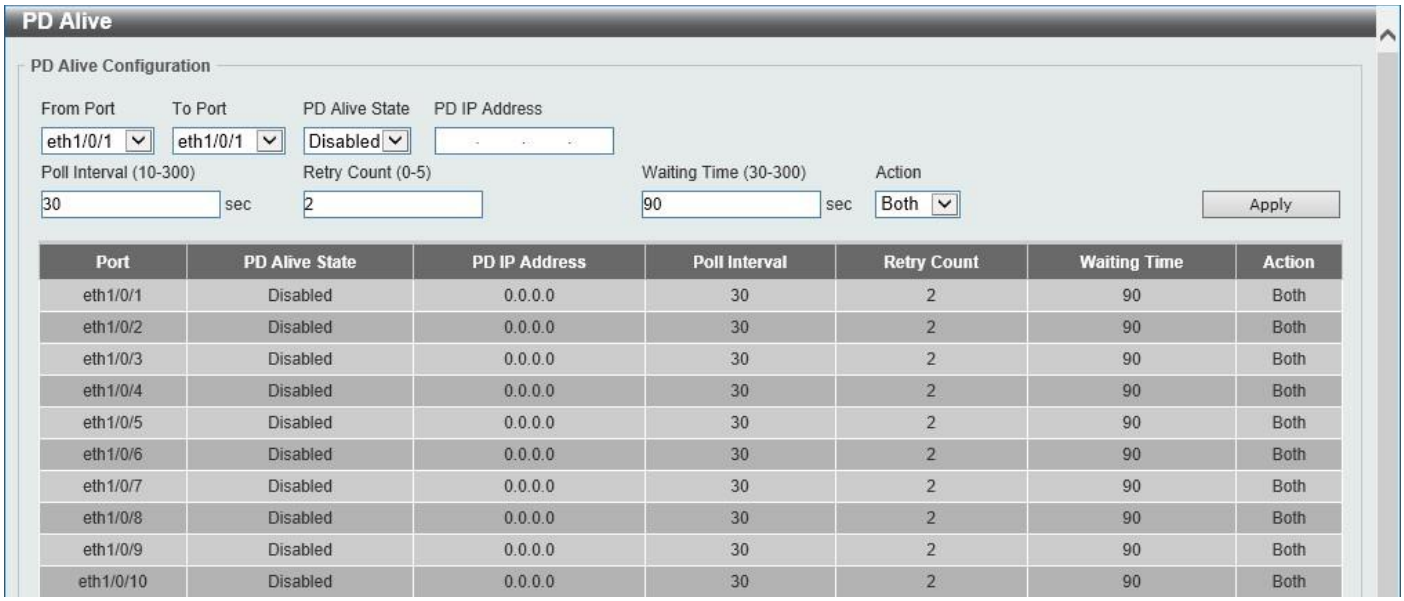

그림 3-14 PD Alive Window

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
PD Alive State	지정된 포트에서 PD Alive 기능을 활성화 또는 비활성화하려면 선택합니다.
PD IP Address	여기에 PD 의 IP Address 를 입력합니다.

Poll Interval	여기에 폴링 간격을 입력합니다. 시스템에서 PoE 포트에 연결된 PD 로 ping 메시지를 보내는 사이의 간격입니다. 기본적으로 이 값은 30 초입니다. 범위는 10 초에서 300 초 사이입니다.
Retry Count	여기에 재시도 횟수를 입력합니다. PD 가 응답하지 않을 때 (각 간격으로) 전송되는 ping 메시지의 양입니다. 기본적으로 이 값은 2 입니다. 범위는 0 에서 5 사이입니다.
Waiting Time	여기에 대기 시간을 입력합니다. 재설정 작업이 수행된 후 PoE 포트에 연결된 PD 로 ping 메시지를 보내기 전에 시스템이 대기하는 시간입니다. 기본적으로 이 값은 90 초입니다. 범위는 30 초에서 300 초 사이입니다.
Action	여기에서 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • 재설정 - PoE 포트 상태를 재설정하도록 지정합니다(PoE 끄기 및 켜기). • Notify 노티파이 - 관리자에게 알리기 위해 로그와 트랩을 보내도록 지정합니다. • 둘 다 - 로그 및 트랩을 전송하여 관리자에게 알리고 PoE 포트 상태를 재설정하도록 지정합니다(PoE 끄기 및 켜기).

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

PoE Statistics

이 창은 스위치 포트의 PoE 통계를 표시하고 지우는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > PoE > PD Alive 를 클릭합니다.

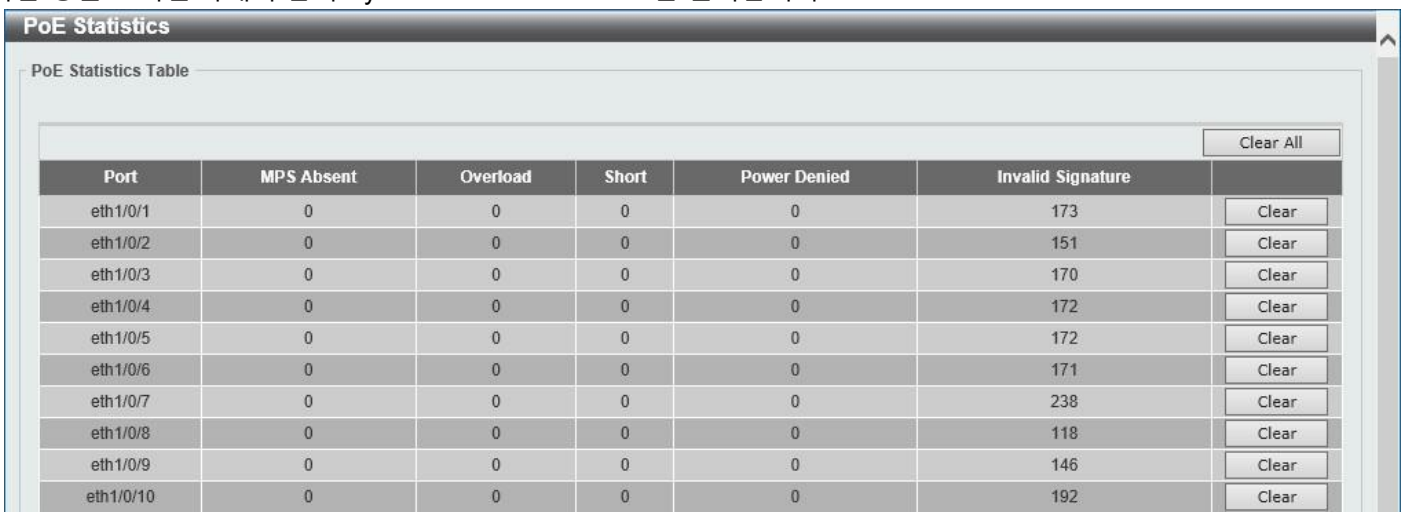

그림 3-15) PoE 통계 창

Clear All 버튼을 클릭하여 모든 포트에 대한 PoE 통계를 지웁니다.
Clear 버튼을 클릭하여 해당 포트에 대한 PoE 통계를 지웁니다.

PoE Measurement

이 창은 스위치 포트에 PoE 측정 정보를 표시하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > PoE > PoE Measurement 을 클릭합니다.

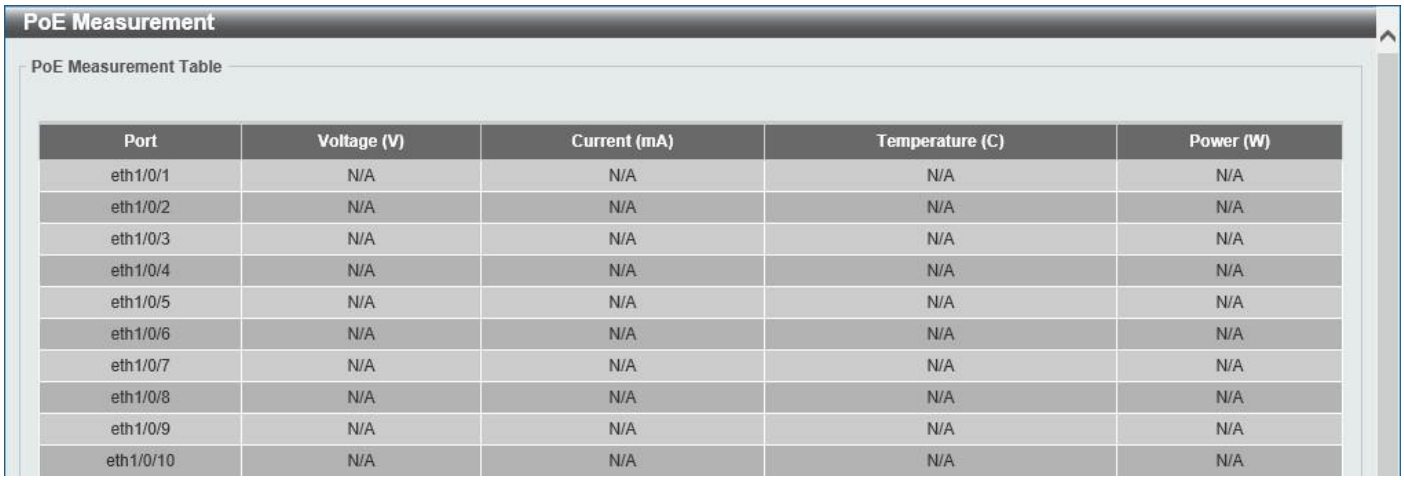

그림 3-16 PoE 측정 창

PoE LLDP Classification

이 창은 PoE LLDP(Link Layer Discovery Protocol) 분류를 표시하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > PoE > PoE LLDP Classification 을 클릭합니다.

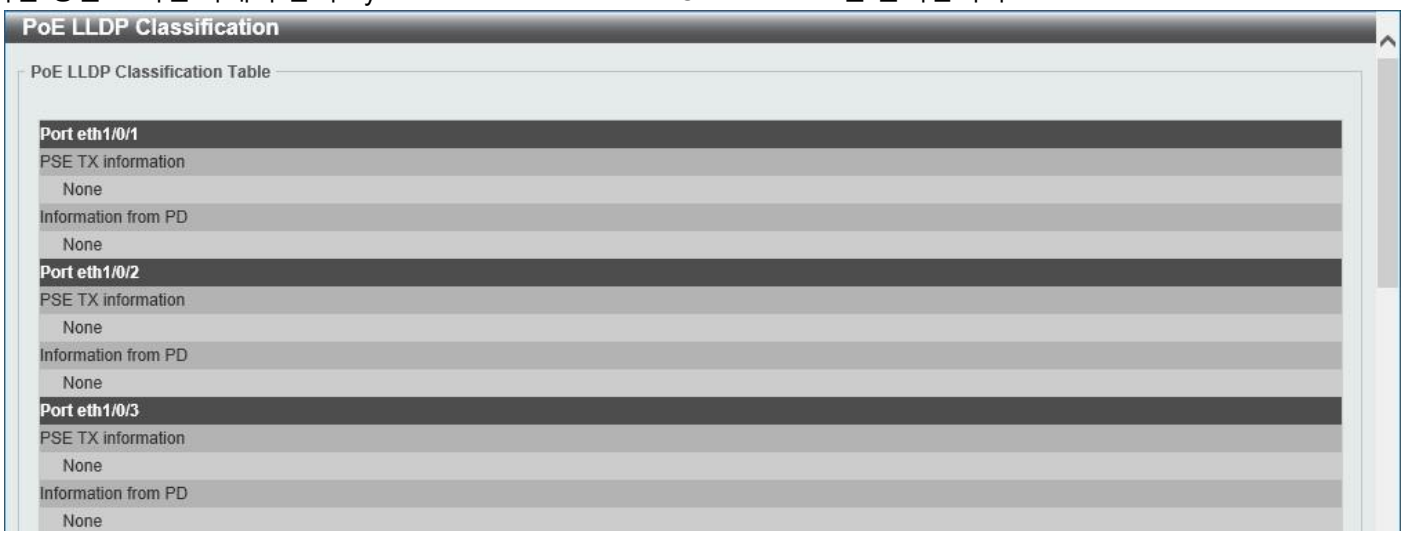

그림 3-17) PoE LLDP 분류 창

System Log

System Log Settings

이 창은 시스템 로그 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > System Log > System Log Settings 설정을 클릭합니다.

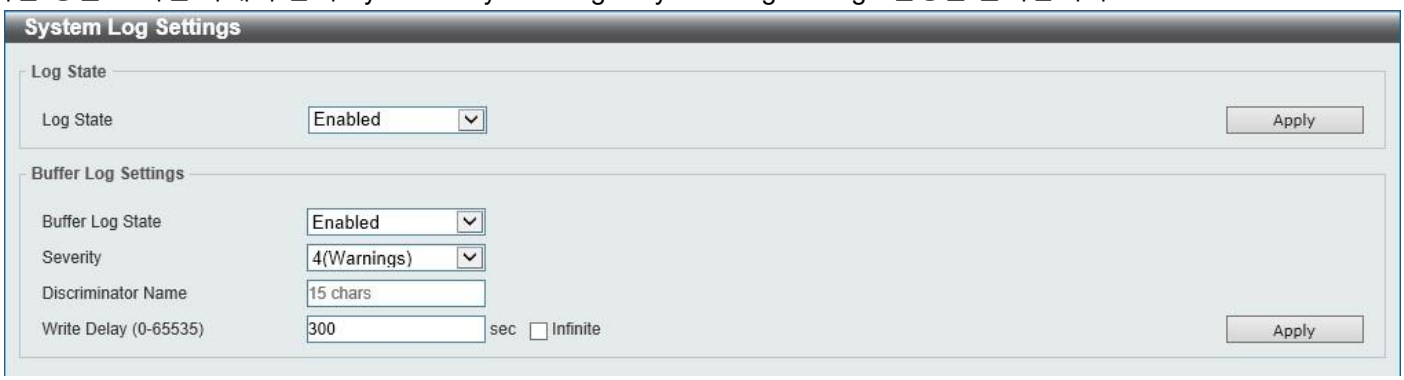

그림 3-18) 시스템 로그 설정 창

Log State 에 대해 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Log State	여기에서 전역 시스템 로그 상태 활성화 또는 비활성화를 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

버퍼 로그 설정에 대해 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Buffer Log State	여기에서 버퍼 로그 상태를 전역적으로 활성화하거나 비활성화하려면 선택합니다. 선택할 수 있는 옵션은 Enable, Disabled, Default 입니다. Default 옵션을 선택하면 전역 버퍼 로그 상태가 기본 동작을 따릅니다.
Severity	기록될 정보 유형의 Severity 값을 선택합니다. 선택할 수 있는 옵션은 0(긴급), 1(경고), 2(위험), 3(오류), 4(경고), 5(알림), 6(정보) 및 7(디버깅)입니다.
Discriminator Name	여기에 사용된 판별자 이름을 입력합니다. 이 이름은 최대 15 자까지 가능합니다. 이는 해당 프로필 내에 지정된 필터링 기준에 따라 버퍼 로그 메시지를 필터링하는 데 사용할 판별자 프로필의 이름을 지정합니다.
Write Delay	여기에 log write delay 값을 입력합니다. 이 값은 0 초에서 65535 초 사이여야 합니다. 기본적으로 이 값은 300 초입니다. Infinite 옵션을 선택하여 쓰기 지연 기능을 비활성화합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

System Log Discriminator Settings

이 창은 시스템 로그 판별자 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > System Log > System Log Discriminator Settings 클릭합니다.

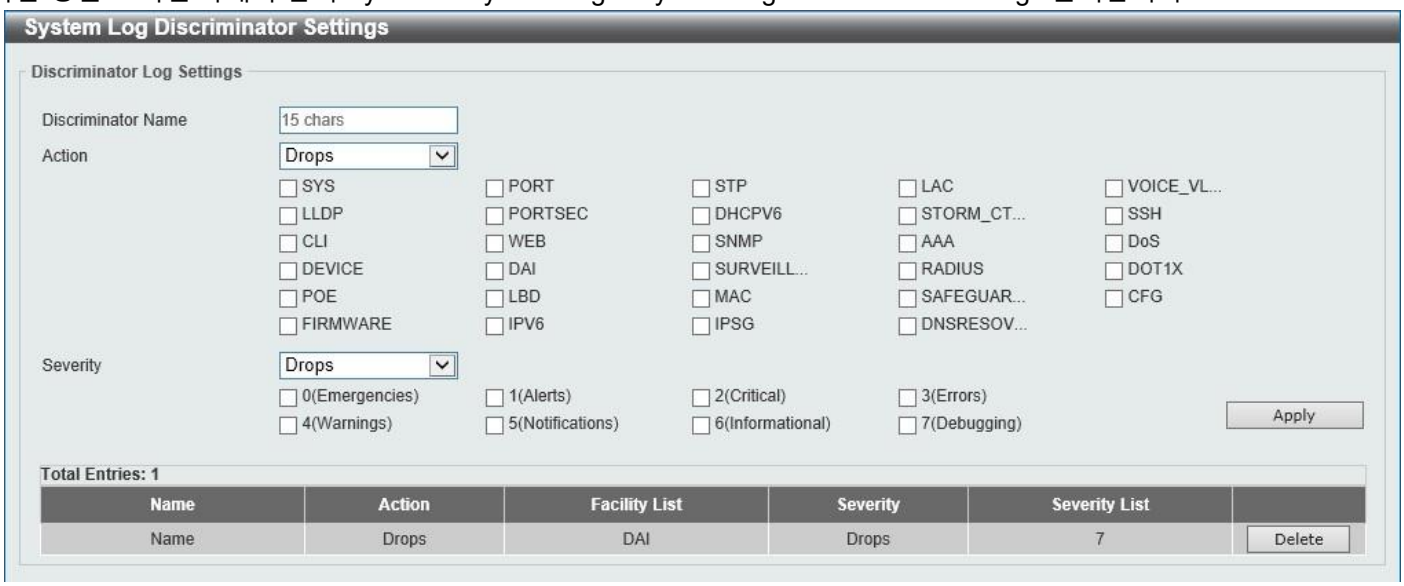

그림 3-19) 시스템 로그 판별자 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Discriminator Name	여기에 판별자 프로필의 이름을 입력합니다. 이 이름은 최대 15 자까지 가능합니다.
Action	여기에서 Facility 동작 옵션과 선택한 동작과 연결할 Facility 유형을 선택합니다. 선택할 수 있는 동작 옵션은 Drops 및 Includes 입니다.

Severity	severity behavior 옵션과 기록될 정보 유형의 값을 선택합니다. 선택할 수 있는 동작 옵션은 Drops 및 Includes 입니다. 선택할 수 있는 Severity 값 옵션은 0(긴급), 1(경고), 2(위험), 3 입니다. (오류), 4(경고), 5(알림), 6(정보) 및 7(디버깅).

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 삭제합니다.

System Log Server Settings

이 창은 시스템 로그 서버 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > System Log > System Log Server Settings 을 클릭합니다.

그림 3-20) 시스템 로그 서버 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Host IPv4 Address	여기에 시스템 로그 서버 IPv4 주소를 입력합니다.
Host IPv6 Address	여기에 시스템 로그 서버 IPv6 주소를 입력합니다.
UDP Port	여기에 시스템 로그 서버 UDP 포트 번호를 입력합니다. 이 값은 514 또는 1024 에서 65535 사이여야 합니다. 기본적으로 이 값은 514 입니다.
Severity	기록될 정보 유형의 Severity 값을 선택합니다. 선택할 수 있는 옵션은 0(긴급), 1(경고), 2(위험), 3(오류), 4(경고), 5(알림), 6(정보) 및 7(디버깅)입니다.
Facility	여기에 기록할 Facility 번호를 선택합니다. 범위는 0 에서 23 사이입니다. 각 Facility 번호는 특정 Facility 과 연결됩니다. 아래 표를 참조하십시오.

Facility Number	Facility Name	Facility Description
0	kern	Kernel messages
1	user	User-level messages
2	mail	Mail system
3	daemon	System daemons
4	auth1	Security/authorization messages
5	syslog	Messages generated internally by the SYSLOG
6	lpr	Line printer sub-system
7	news	Network news sub-system
8	uucp	UUCP sub-system
9	clock1	Clock daemon
10	auth2	Security/authorization messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	logaudit	Log audit

	14	logalert	Log alert
	15	clock2	Clock daemon
	16	local0	Local use 0 (local0)
	17	local1	Local use 1 (local1)
	18	local2	Local use 2 (local2)
	19	local3	Local use 3 (local3)
	20	local4	Local use 4 (local4)
	21	local5	Local use 5 (local5)
	22	local6	Local use 6 (local6)
	23	local7	Local use 7 (local7)
Discriminator Name	로그 서버로 전송된 메시지를 필터링하는 데 사용할 판별자의 이름을 여기에 입력합니다. 이 이름은 최대 15 자까지 가능합니다.		

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 삭제합니다.

System Log

이 창은 시스템 로그를 보고 지우는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > System Log > System Log 를 클릭합니다.

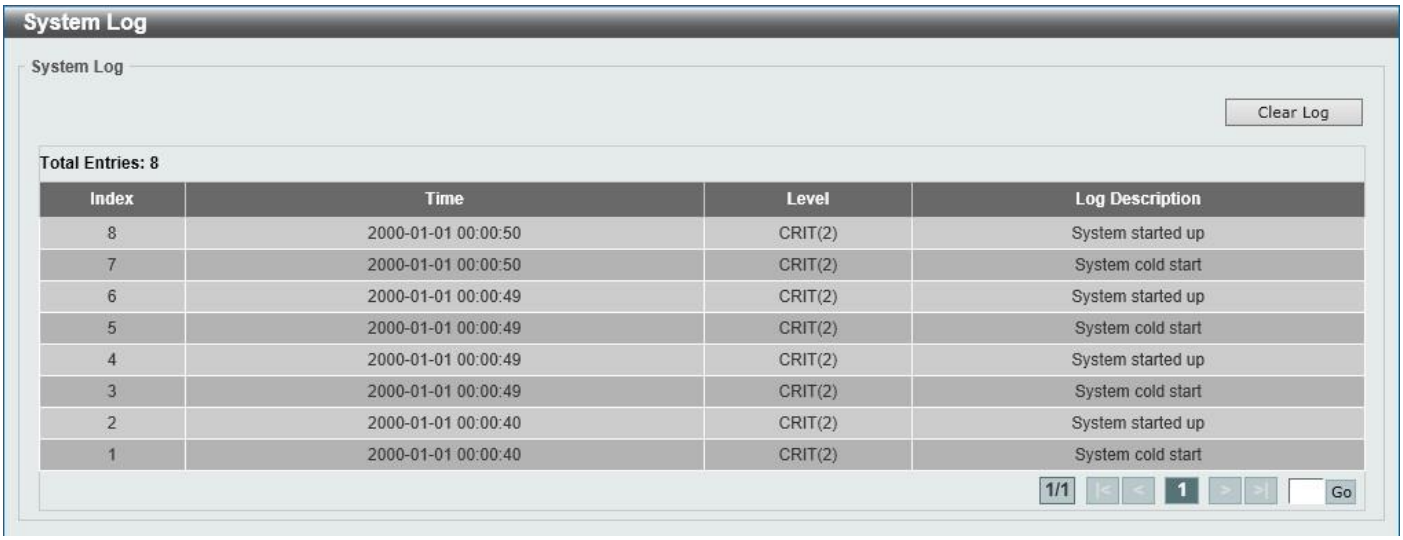

그림 3-21) 시스템 로그 창

Clear Log 버튼을 클릭하여 테이블에 표시된 시스템 로그 항목을 지웁니다.
페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

System Attack Log

이 창은 System Attack Log 를 보고 지우는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > System Log > System Attack Log 를 클릭합니다.

그림 3-22) 시스템 공격 로그 창

Clear Attack Log 버튼을 클릭하여 테이블에 표시된 시스템 공격 로그 항목을 지웁니다.

Time and SNTP

Clock Settings

이 창은 스위치의 시간 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > Time 및 SNTP > Clock Settings 를 클릭합니다.

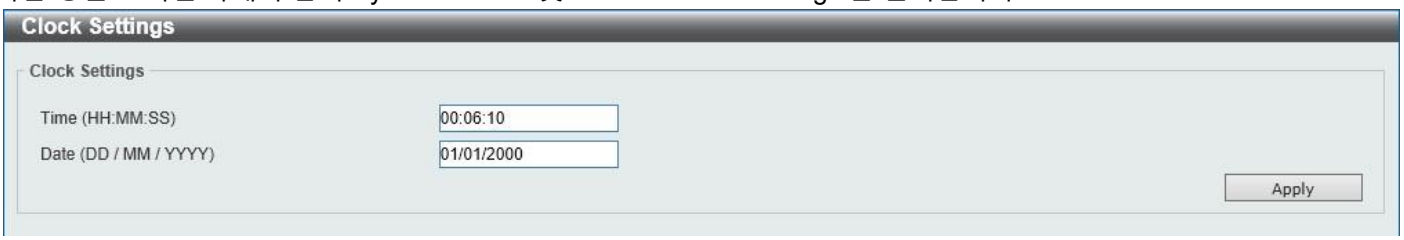

그림 3-23) 시계 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Time	여기에 현재 시간을 시(HH), 분(MM) 및 초(SS) 단위로 입력합니다. 예: 18:30:30.
Date	여기에 현재 일(DD), 월(MM) 및 연도(YYYY)를 입력합니다. 예: 30/09/2019.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Time Zone Settings

이 창은 SNTP 에 대한 표준 시간대 및 일광 절약 시간 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > Time 및 SNTP > Time Zone Settings 를 클릭합니다.

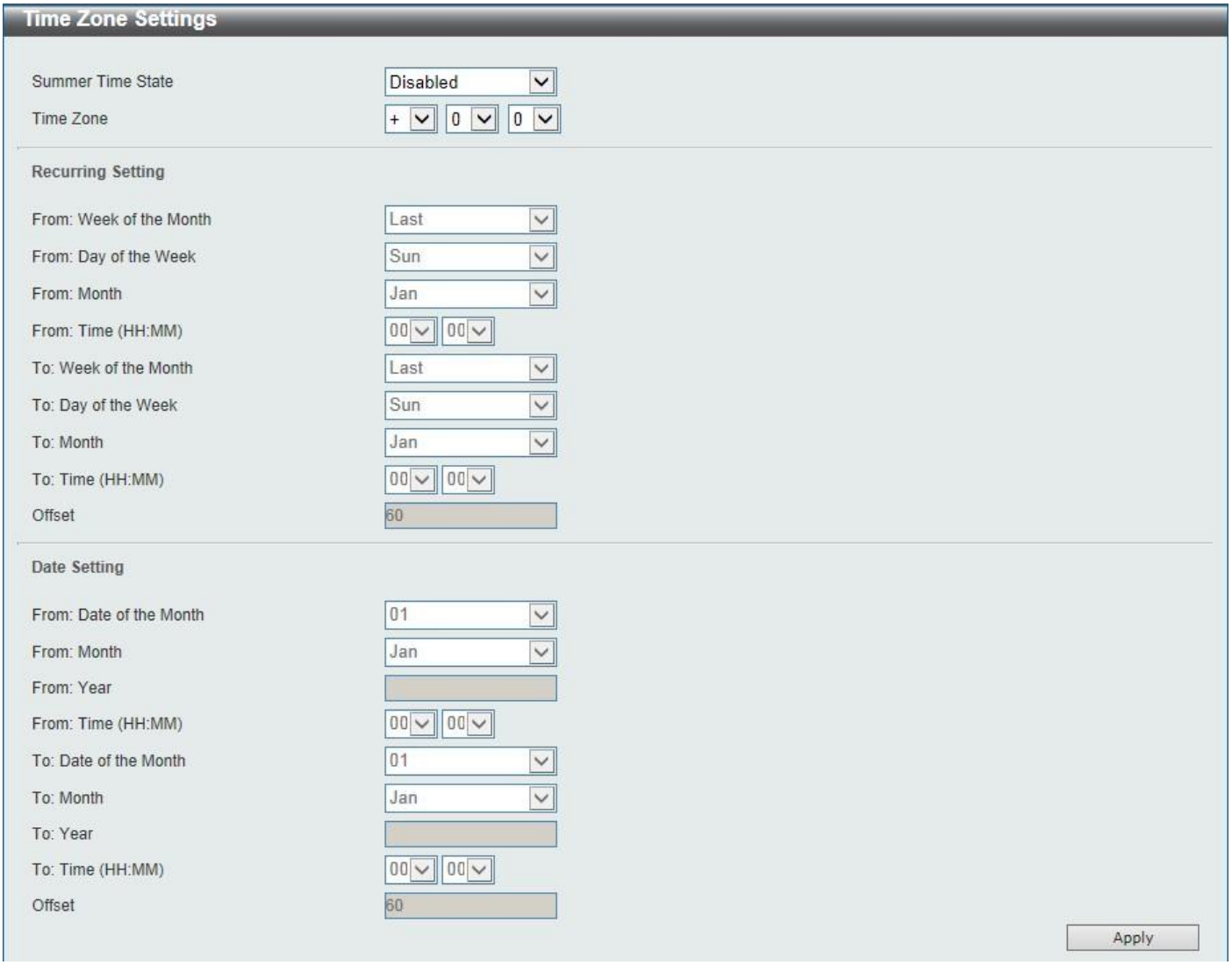

그림 3-24) 시간대 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Summer Time State	서머타임 설정을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Disabled(사용 안 함) - 서머타임 설정을 비활성화하려면 선택합니다. • 되풀이 설정(Recurring Setting) - 지정된 월의 지정된 요일에 시작하고 끝나야 하는 서머타임을 구성하려면 선택합니다. • Date Setting(날짜 설정) - 지정된 달의 지정된 날짜에 시작하고 끝나야 하는 서머타임을 구성하려면 선택합니다.

Time Zone	UTC(협정 세계시)에서 현지 표준 시간대 오프셋을 지정하려면 선택합니다.

반복 설정에서 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From: Week of the Month	서머타임이 시작되는 달의 주를 선택합니다.
From: Day of the Week	서머타임이 시작되는 요일을 선택합니다.
From: Month	서머타임이 시작되는 달을 선택합니다.
From: Time	서머타임이 시작되는 시간을 선택합니다.
To: Week of the Month	서머타임이 종료되는 달의 주를 선택합니다.
To: Day of the Week	서머타임이 종료되는 요일을 선택합니다.
To: Month	서머타임이 끝나는 달을 선택합니다.
To: Time	서머타임이 종료되는 시간을 선택합니다.
Offset	서머타임 동안 추가할 시간(분)을 입력합니다. 기본값은 60 입니다. 이 오프셋의 범위는 30, 60, 90 및 120 입니다.

날짜 설정에서 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From: Date of the Month	서머타임이 시작되는 달의 날짜를 선택합니다.
From: Month	서머타임이 시작되는 달을 선택합니다.
From: Year	서머타임이 시작되는 연도를 입력합니다.
From: Time	서머타임이 시작되는 시간을 선택합니다.
To: Date of the Month	서머타임이 종료되는 달의 날짜를 선택합니다.
To: Month	서머타임이 끝나는 달을 선택합니다.
To: Year	서머타임이 끝나는 연도를 입력합니다.
To: Time	서머타임이 종료되는 시간을 선택합니다.
Offset	서머타임 동안 추가할 시간(분)을 입력합니다. 기본값은 60 입니다. 이 오프셋의 범위는 30, 60, 90 및 120 입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

SNTP Settings

SNTP(Simple Network Time Protocol)는 인터넷을 통해 컴퓨터 시계를 동기화하기 위한 프로토콜입니다. 국가 시간 및 빈도 보급 서비스에 액세스하고, 서버 및 클라이언트의 SNTP 서브넷을 조정하고, 각 참가자의 시스템 시계를 조정할 수 있는 포괄적인 메커니즘을 제공합니다. 이 창은 스위치에 대한 SNTP 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > Time and SNTP > SNTP Settings 를 클릭합니다.

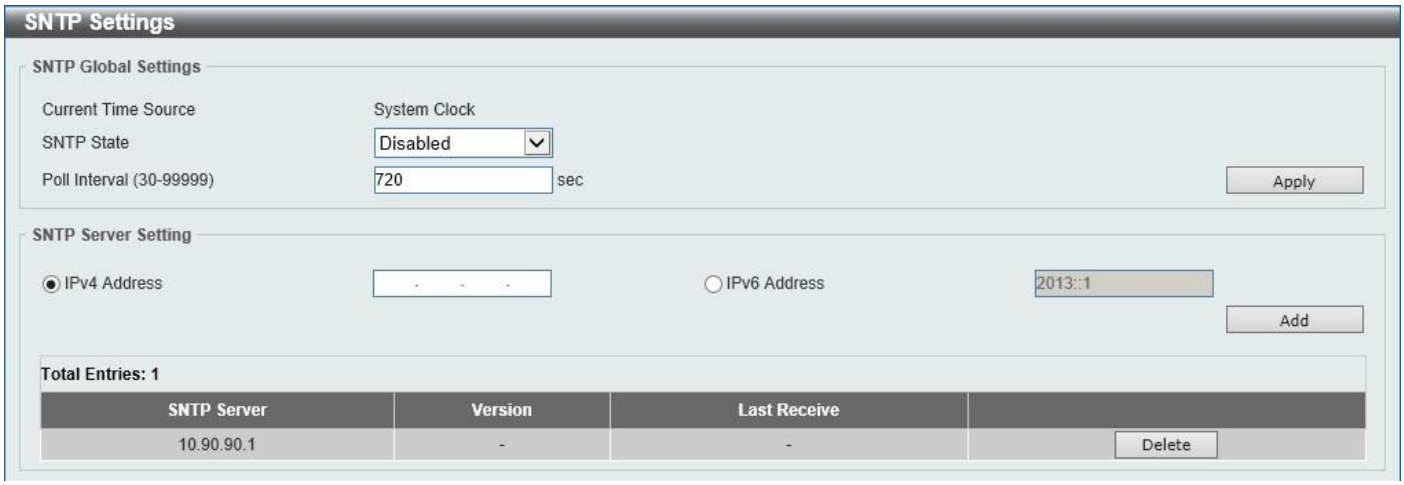

그림 3-25) SNTP 설정 창

SNTP Global Settings(SNTP Global Settings)에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
SNTP State	SNTP 를 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
Poll Interval	동기화 간격(초)을 입력합니다. 값은 30 초에서 99999 초 사이입니다. 기본 간격은 720 초입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

SNTP 서버 설정에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
IPv4 Address	SNTP 참조를 제공하는 SNTP 서버의 IPv4 주소를 입력합니다.
IPv6 Address	SNTP 참조를 제공하는 SNTP 서버의 IPv6 주소를 입력합니다.

Add 버튼을 클릭하여 SNTP 서버를 추가합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Time Range

이 창은 시간 프로필 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 System > Time Range 를 클릭합니다.

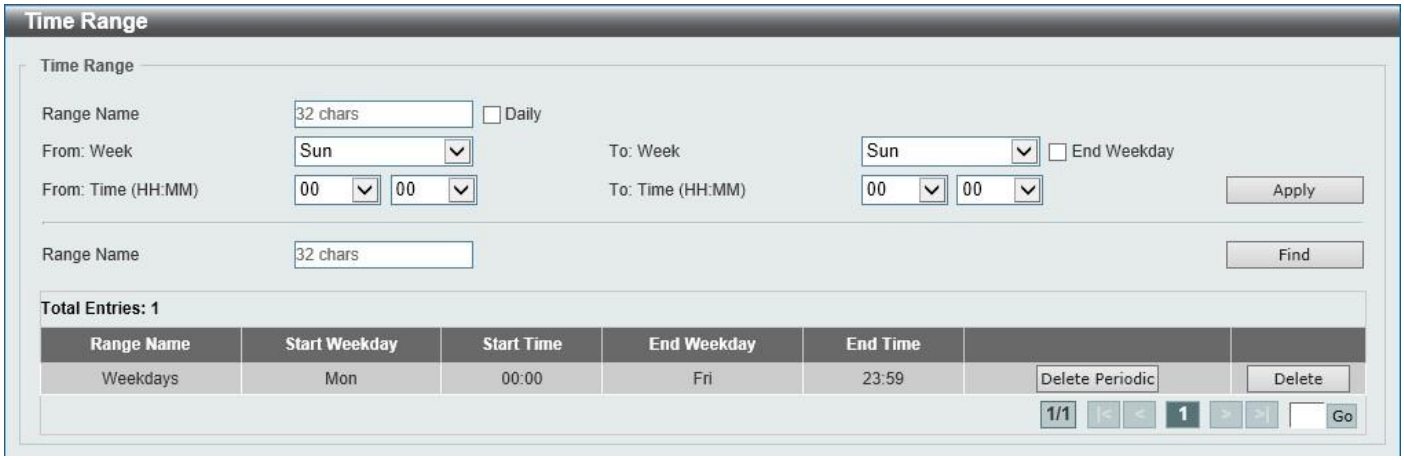

그림 3-26 시간 범위 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Range Name	여기에 시간 프로필 범위 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
From Week ~ To Week	이 시간 프로필에 사용할 주의 시작 및 종료 요일을 선택합니다. 매일 옵션을 선택하여 모든 요일에 대해 이 시간 프로필을 사용합니다. 요일 종료 옵션을 선택하면 주의 시작 요일부터 주말까지 이 시간 프로필을 사용할 수 있습니다.
From Time ~ To Time	이 시간 프로필에 사용할 하루의 시작 및 종료 시간을 선택합니다. 첫 번째 드롭다운 메뉴는 시간을 선택하고 두 번째 드롭다운 메뉴는 분을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Delete Periodic 버튼을 클릭하여 정기 항목을 삭제합니다.

Delete 버튼을 클릭하여 지정된 항목을 삭제합니다.

3. Management

User Accounts Settings
SNMP
RMON
Telnet/Web
Session Timeout
DHCP
DHCP Auto Configuration
DNS
File System
D-Link Discovery Protocol

User Accounts Settings

이 페이지에서 사용자 계정을 만들고 업데이트할 수 있습니다. 활성 사용자 계정 세션도 이 페이지에서 볼 수 있습니다.

다음 창을 보려면 아래와 Management > User Accounts Settings 을 클릭합니다.

User Management Settings 탭을 선택하면 다음 페이지가 나타납니다.

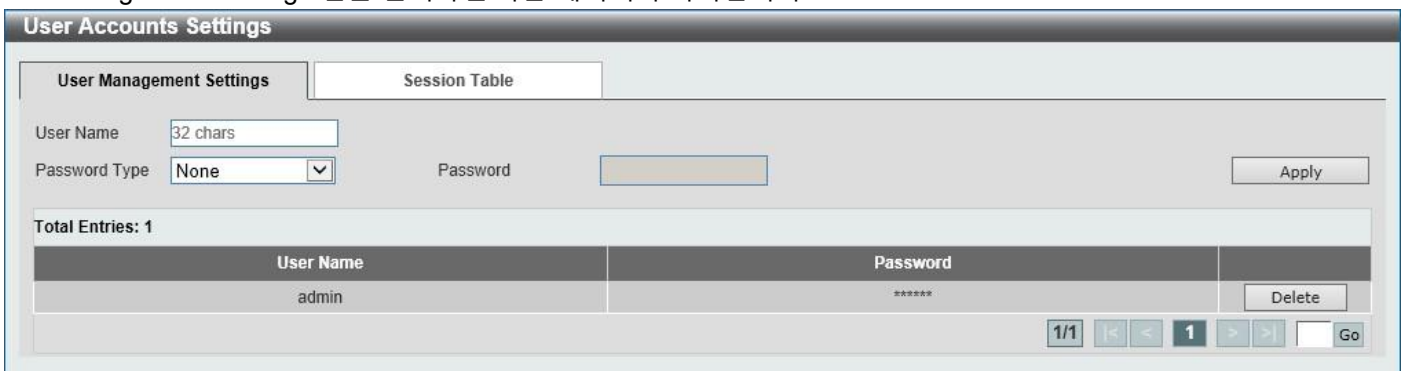

그림 4-1 사용자 계정 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
User Name	여기에 사용자 계정 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Password Type	여기에서 이 사용자 계정의 암호 유형을 선택합니다. 선택할 수 있는 옵션은 None 및 Plain Text 입니다.

Password	암호 유형으로 Plain Text(일반 텍스트)를 선택한 후 여기에 이 사용자 계정의 암호를 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.
Delete 버튼을 클릭하여 지정된 사용자 계정 항목을 삭제합니다.
페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

세션 테이블 탭을 선택하면 다음 페이지가 나타납니다.

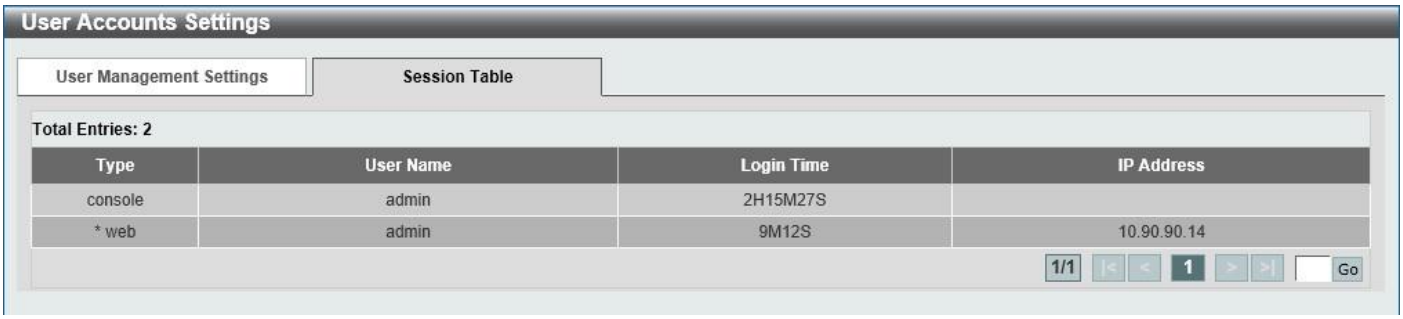

그림 4-2 세션 테이블 창

이 페이지에 활성 사용자 계정 세션 목록이 표시됩니다.
페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

SNMP

SNMP(Simple Network Management Protocol)는 네트워크 디바이스를 관리하고 모니터링하기 위해 특별히 설계된 OSI Layer 7(애플리케이션 계층)입니다. SNMP 를 사용하면 네트워크 관리 스테이션에서 게이트웨이, 라우터, 스위치 및 기타 네트워크 장치의 설정을 읽고 수정할 수 있습니다. SNMP 를 사용하여 시스템 기능을 구성하고, 성능을 모니터링하고, 스위치, 스위치 그룹 또는 네트워크에서 발생할 수 있는 문제를 감지합니다.

SNMP 를 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. SNMP 는 MIB 사양의 형식과 네트워크를 통해 이 정보에 액세스하는 데 사용되는 프로토콜을 모두 정의합니다.
스위치는 SNMP 버전 1, 2c 및 3 을 지원합니다. SNMP 의 세 가지 버전은 관리 스테이션과 네트워크 디바이스 간에 제공되는 보안 수준이 다릅니다.

SNMPv1 및 SNMPv2c 에서 사용자 인증은 암호와 같은 기능을 하는 '커뮤니티 문자열'을 사용하여 수행됩니다. 원격 사용자 SNMP 애플리케이션과 스위치 SNMP 는 동일한 커뮤니티 문자열을 사용해야 합니다. 인증되지 않은 스테이션의 SNMP 패킷은 무시(삭제)됩니다. SNMPv1 및 SNMPv2c 관리 액세스에 사용되는 스위치의 기본 커뮤니티 문자열은 다음과 같습니다.

- public - 인증된 관리 스테이션에서 MIB 개체를 검색할 수 있습니다.
- private - 인증된 관리 스테이션에서 MIB 개체를 검색하고 수정할 수 있습니다.

SNMPv3 프로토콜은 두 부분으로 구분되는 보다 정교한 인증 프로세스를 사용합니다. 첫 번째 부분에서는 SNMP 관리자 역할을 할 수 있는 사용자 및 해당 속성 목록을 유지 관리합니다. 두 번째 부분에서는 해당 목록의 각 사용자가 SNMP 관리자로서 수행할 수 있는 작업에 대해 설명합니다. 또한 SNMPv3 프로토콜은 SNMP 메시지를 암호화하는 데 사용할 수 있는 추가 보안 계층을 제공합니다.

스위치를 사용하면 사용자 그룹을 나열하고 공유 권한 집합으로 구성할 수 있습니다. SNMP 버전은 나열된 SNMP 관리자 그룹에 대해 설정할 수도 있습니다. 따라서 SNMPv1 을 사용하여 읽기 전용 정보를 보거나 트랩을 수신할 수 있는 SNMP 관리자 그룹을 생성하는 동시에 다른 그룹에 더 높은 보안 수준을 할당하고 SNMPv3 을 사용하여 읽기/쓰기 권한을 부여할 수 있습니다.

SNMPv3 를 사용하여 사용자 또는 그룹이 특정 SNMP 관리 기능을 수행하는 것을 허용하거나 금지할 수 있습니다. 이는 특정 MIB 와 연결된 OID(Object Identifier)를 사용하여 정의됩니다.

MIBs

MIB(Management Information Base)는 관리 및 카운터 정보를 저장합니다. 스위치는 표준 MIB-II Management Information Base 모듈을 사용하므로 SNMP 기반 네트워크 관리 소프트웨어를 사용하여 MIB 개체의 값을 검색할 수 있습니다. 표준 MIB-II 외에도 스위치는 확장된 관리 정보 베이스로 자체 독점 엔터프라이즈 MIB 를 지원합니다. MIB 개체 식별자를 지정하면 독점 MIB 를 검색할 수도 있습니다. MIB 값은 읽기 전용 또는 읽기-쓰기일 수 있습니다.

스위치에는 네트워크의 요구 사항과 네트워크 관리자의 기본 설정에 맞게 사용자 지정할 수 있는 유연한 SNMP 관리 시스템이 통합되어 있습니다. SNMP 의 세 가지 버전은 관리 스테이션과 네트워크 디바이스 간에 제공되는 보안 수준이 다릅니다. SNMP 설정은 웹 UI 의 SNMP 폴더에 있는 메뉴를 사용하여 구성됩니다.

Traps

트랩은 스위치에서 발생하는 이벤트를 네트워크 직원에게 알리는 메시지입니다. 이벤트는 재부팅(누군가 실수로 스위치를 끄거나 스위치를 분리함)만큼 심각할 수도 있고 포트 상태 변경과 같이 덜 심각할 수도 있습니다. 스위치는 트랩을 생성하여 트랩 수신자(또는 네트워크 관리자)에게 전송합니다. 일반적인 트랩에는 Authentication Failure, Topology Change 및 Broadcast/Multicast Storm 에 대한 트랩 메시지가 포함됩니다.

SNMP Global Settings

이 창은 전역 SNMP 및 트랩 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > SNMP > SNMP Global Settings 을 클릭합니다.

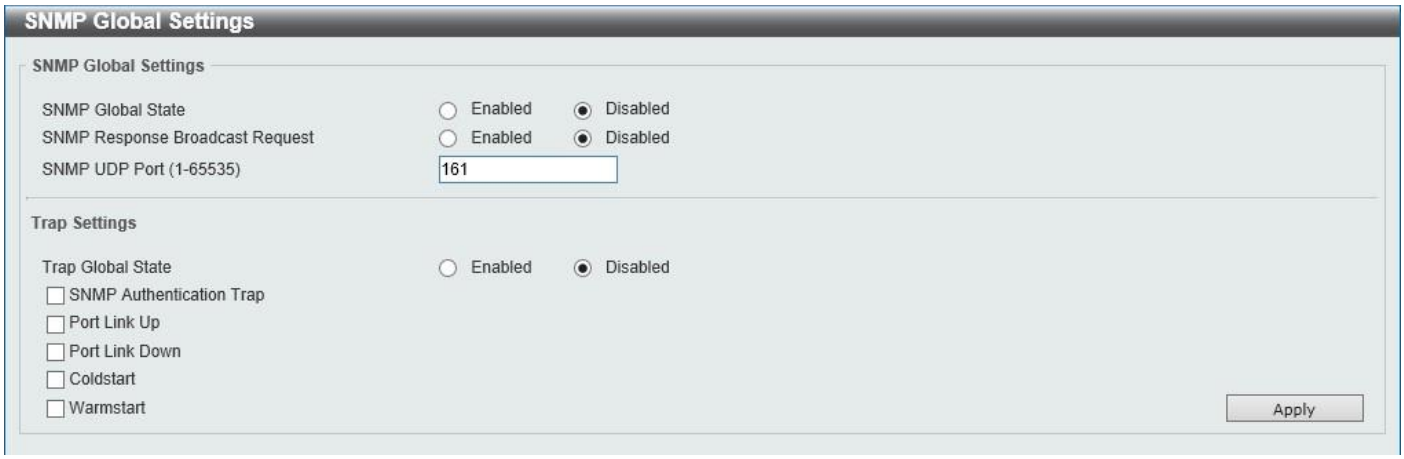

그림 4-3) SNMP Global Settings 창

NMP Global Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
SNMP Global State	SNMP 기능을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
SNMP Response Broadcast Request	브로드캐스트 SNMP GetRequest 패킷에 응답하도록 서버를 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
SNMP UDP Port	SNMP UDP 포트 번호를 입력합니다.

Trap Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Trap Global State	모든 또는 특정 SNMP 알림의 전송을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
SNMP Authentication Trap	SNMP 인증 실패 알림 전송을 제어하려면 이 옵션을 선택합니다. *authenticationFailuretrap* 트랩은 디바이스가 제대로 인증되지 않은 SNMP 메시지를 수신할 때 생성됩니다. 인증 방법은 사용 중인 SNMP 버전에 따라 다릅니다. SNMPv1 또는 SNMPv2c 의 경우 패킷이 잘못된 커뮤니티 문자열로 형성되면 인증 실패가 발생합니다.
Port Link Up	이 옵션을 선택하면 포트 링크 업 알림 전송을 제어할 수 있습니다. linkUp 트랩은 디바이스가 통신 링크 중 하나가 작동했음을 인식할 때 생성됩니다.
Port Link Down	이 옵션을 선택하면 포트 링크 다운 알림 전송을 제어할 수 있습니다. *linkDown* 트랩은 디바이스가 통신 링크 중 하나가 다운되었음을 인식할 때 생성됩니다.
Coldstart	SNMP coldStart *알림* 전송을 제어하려면 이 옵션을 선택합니다.
Warmstart	SNMP warmStart *알림* 전송을 제어하려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

SNMP Linkchange Trap Settings

이 창은 SNMP 링크 변경 트랩 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management >SNMP >SNMP Linkchange Trap Settings 를 클릭합니다.

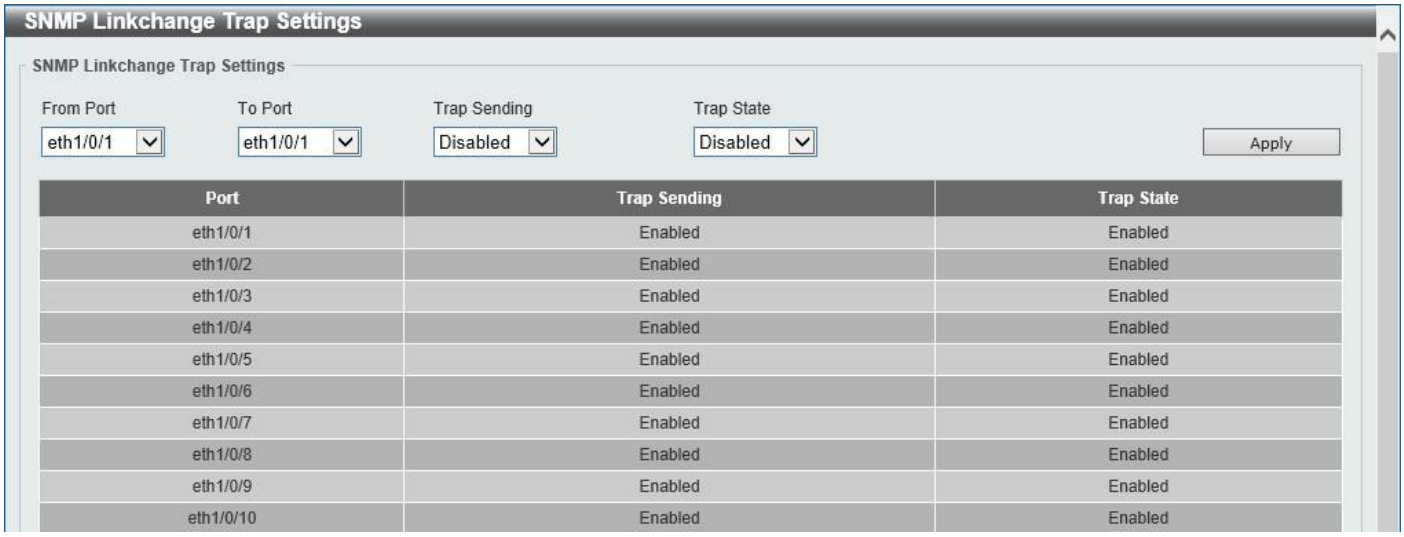

그림 4-4) SNMP 링크 변경 트랩 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
Trap Sending	시스템에서 생성된 SNMP 알림 트랩의 전송을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
Trap Sending	SNMP linkChange 트랩을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

SNMP View Table Settings

이 창은 원격 SNMP 관리자가 액세스할 수 있는 MIB 객체를 정의하는 커뮤니티 문자열에 보기를 할당하는 데 사용됩니다. 이 테이블로 생성된 SNMP 하위 트리 OID 는 SNMP 사용자를 SNMP 사용자 테이블 설정 창에서 생성된 보기에 매핑합니다.

다음 창을 보려면 아래와 같이 Management > SNMP > SNMP View Table Settings 를 클릭합니다.

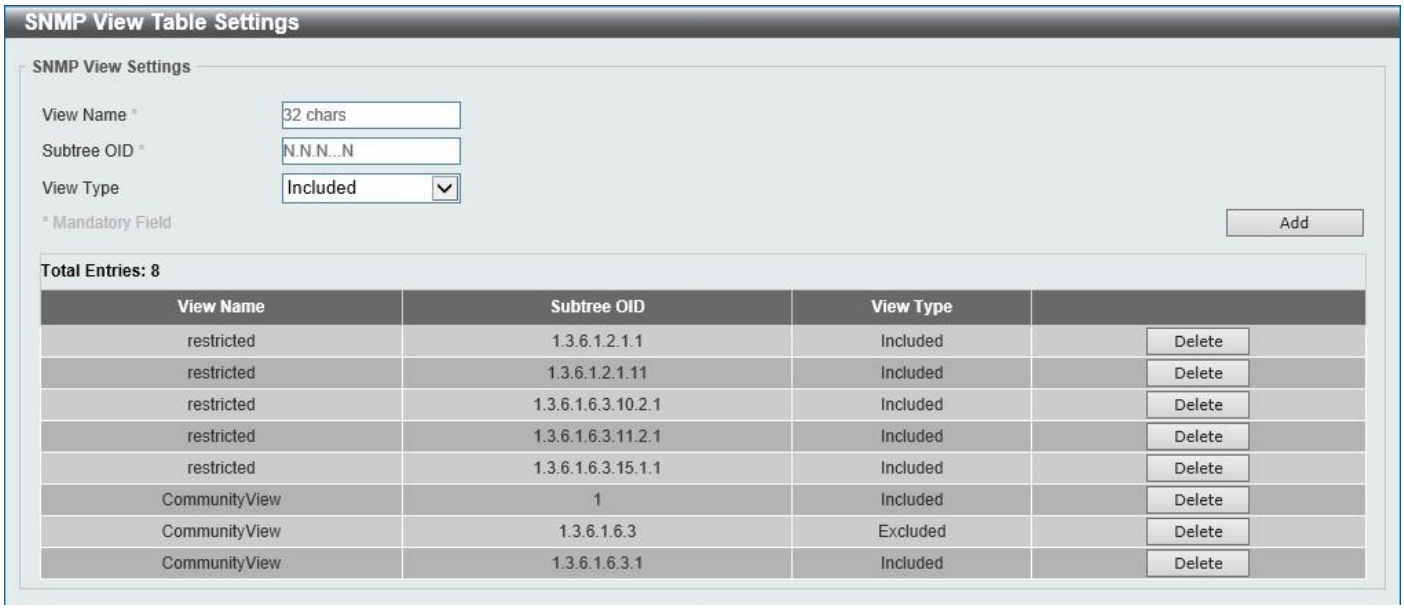

그림 4-5) SNMP 보기 테이블 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
View Name	최대 32 자의 영숫자 문자열을 입력합니다. 이는 생성되는 새 SNMP 보기를 식별하는 데 사용됩니다.
Subtree OID	뷰의 OID(개체 식별자) 하위 트리를 입력합니다. OID 는 SNMP 관리자에 의해 액세스에서 포함되거나 제외될 개체 트리(MIB 트리)를 식별합니다.
View Type	여기에서 보기 유형을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Included(포함됨) - SNMP 관리자가 액세스할 수 있는 개체 목록에 이 개체를 포함하려면 선택합니다. • Excluded(제외됨) - SNMP 관리자가 액세스할 수 있는 개체 목록에서 이 개체를 제외하려면 선택합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새 항목을 추가합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

SNMP Community Table Settings

이 창은 SNMP 관리자와 에이전트 간의 관계를 정의하기 위해 SNMP 커뮤니티 문자열을 만드는 데 사용됩니다.
커뮤니티 문자열은 스위치의 에이전트에 대한 액세스를 허용하는 암호와 같은 역할을 합니다. 다음 특성 중 하나 이상이 커뮤니티 문자열과 연관될 수 있습니다.

- 커뮤니티 문자열을 사용하여 스위치의 SNMP 에이전트에 액세스할 수 있는 SNMP 관리자의 IP Address 가 포함된 액세스 목록입니다.
- SNMP 커뮤니티에서 액세스할 수 있는 MIB 개체의 하위 집합을 정의하는 모든 MIB 보기입니다.
- SNMP 커뮤니티에서 액세스할 수 있는 MIB 개체에 대한 읽기-쓰기 또는 읽기 전용 수준 권한.

다음 창을 보려면 아래와 같이 Management > SNMP > SNMP Community Table Settings 을 클릭합니다.

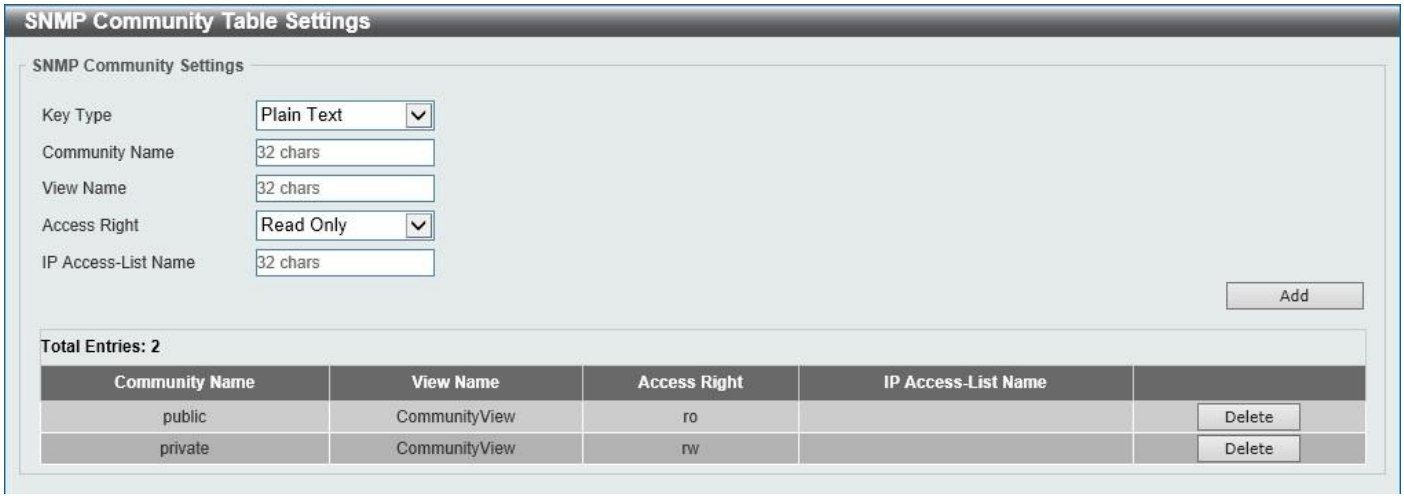

그림 4-6) SNMP 커뮤니티 테이블 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Key Type	유일하게 지원되는 키 유형은 일반 텍스트입니다.
Community Name	SNMP 커뮤니티의 구성원을 식별하는 데 사용되는 최대 32 자의 영숫자 문자열을 입력합니다. 이 문자열은 원격 SNMP 관리자에게 스위치의 SNMP 에이전트에 있는 MIB 개체에 대한 액세스 권한을 부여하기 위한 암호처럼 사용됩니다.
View Name	원격 SNMP 관리자가 스위치에서 액세스할 수 있는 MIB 개체 그룹을 식별하는 데 사용되는 최대 32 자의 영숫자 문자열을 입력합니다. 보기 이름은 SNMP 보기 테이블에 있어야 합니다.
Access Right	여기에서 바로 액세스를 선택하십시오. 선택할 수 있는 옵션은 다음과 같습니다. • Read Only- 생성된 커뮤니티 문자열을 사용하는 SNMP 커뮤니티 구성원은 스위치에서 MIB 의 내용만 읽을 수 있습니다. • Read Write- 생성된 커뮤니티 문자열을 사용하는 SNMP 커뮤니티 구성원은 스위치의 MIB 의 내용에서 읽고 쓸 수 있습니다.
IP Access-List Name	이 커뮤니티 문자열을 사용하여 SNMP 에이전트에 액세스할 수 있는 사용자를 제한하려면 표준 액세스 목록의 이름을 입력합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새 항목을 추가합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

SNMP Group Table Settings

이 테이블로 생성된 SNMP 그룹은 SNMP 사용자를 SNMP 보기 테이블 설정 창에서 생성된 보기에 매핑합니다.

다음 창을 보려면 아래와 같이 Management > SNMP > SNMP Group Table Settings 을 클릭합니다.

그림 4-7) SNMP 그룹 테이블 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Group Name	여기에 SNMP 그룹 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다. 공백은 허용되지 않습니다.
Read View Name	그룹의 사용자가 액세스할 수 있는 읽기 보기 이름을 입력합니다.
User-based Security Model	여기에서 보안 모델을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • SNMPv1 - 그룹이 SNMPv1 보안 모델을 사용할 수 있도록 하려면 선택합니다. • SNMPv2c - 그룹이 SNMPv2c 보안 모델을 사용할 수 있도록 하려면 선택합니다. • SNMPv3 - 그룹이 SNMPv3 보안 모델을 사용할 수 있도록 하려면 선택합니다.
Write View Name	그룹의 사용자가 액세스할 수 있는 쓰기 보기 이름을 입력합니다.
Security Level	User-based Security Model(사용자 기반 보안 모델) 드롭다운 목록에서 SNMPv3 를 선택하면 이 옵션을 사용할 수 있습니다. • NoAuthNoPriv - 스위치와 원격 SNMP 관리자 간에 전송되는 패킷의 권한 부여 및 암호화가 없음을 지정합니다. • AuthNoPriv - 권한 부여가 필요하지만 스위치와 원격 SNMP 관리자 간에 전송되는 패킷의 암호화는 없음을 지정합니다. • AuthPriv - 권한 부여가 필요하고 스위치와 원격 SNMP 관리자 간에 전송되는 패킷이 암호화되도록 지정합니다.
Notify View Name	그룹의 사용자가 액세스할 수 있는 알림 보기 이름을 입력합니다. 알림 보기는 트랩 패킷을 통해 그룹 사용자에게 상태를 보고할 수 있는 개체를 설명합니다.
IP Access-List Name	그룹과 연결할 표준 IP ACL(액세스 제어 목록)을 입력합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새 항목을 추가합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

SNMP Engine ID Local Settings

엔진 ID 는 스위치에서 SNMPv3 구현에 사용되는 고유 식별자입니다.

다음 창을 보려면 아래와 같이 Management > SNMP > SNMP Engine ID Local Settings 클릭합니다.

그림 4-8) SNMP 엔진 ID 로컬 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Engine ID	여기에 SNMP 엔진 ID 문자열을 입력합니다. 이 문자열은 최대 24 자까지 가능합니다.

기본값 버튼을 클릭하여 엔진 ID 를 기본값으로 되돌립니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

SNMP User Table Settings

이 창은 스위치에 현재 구성된 SNMP 사용자를 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 Management > SNMP > SNMP User Table Settings 을 클릭합니다.

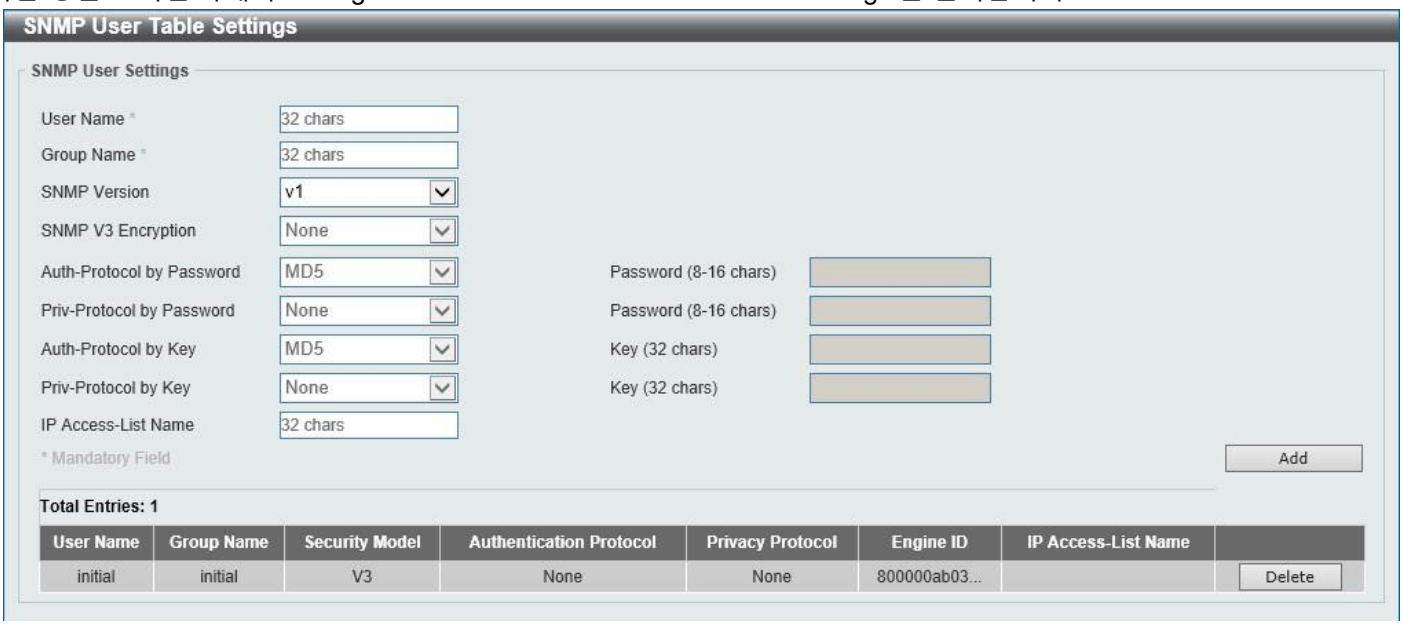

그림 4-9) SNMP 사용자 테이블 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
User Name	여기에 SNMP 사용자 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다. SNMP 사용자를 식별하는 데 사용됩니다.
Group Name	사용자가 속한 SNMP 그룹 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다. 공백은 허용되지 않습니다.
SNMP Version	SNMP 버전을 선택합니다. 선택할 수 있는 옵션은 v1, v2c 및 v3 입니다.
SNMP V3 Encryption	SNMP 버전 드롭다운 목록에서 v3 를 선택하면 이 옵션을 사용할 수 있습니다. 선택할 수 있는 옵션은 None, Password 및 Key 입니다.

Auth-Protocol by Password	SNMP 버전 드롭다운 목록에서 v3 를 선택하고 SNMP v3 암호화 드롭다운 목록에서 암호를 선택하면 이 옵션을 사용할 수 있습니다. 인증 수준을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • MD5 - HMAC-MD5-96 인증 수준을 사용하려면 선택합니다. 이 필드에서는 사용자가 암호 또는 키를 입력해야 합니다. • SHA - HMAC-SHA 인증 프로토콜이 사용되도록 지정합니다. 이 필드에서는 사용자가 암호 또는 키를 입력해야 합니다.
Password	여기에 Auth-Protocol 비밀번호를 입력합니다. MD5 의 경우 이 암호는 8 자에서 16 자 사이여야 합니다. SHA 의 경우 이 암호는 8 자에서 20 자 사이여야 합니다.
Priv-Protocol by Password	SNMP 버전 드롭다운 목록에서 v3 를 선택하고 SNMP v3 암호화 드롭다운 목록에서 암호를 선택하면 이 옵션을 사용할 수 있습니다. 개인 프로토콜을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • 없음 - 사용 중인 권한 부여 프로토콜이 없음을 지정합니다. • DES56 - CBCDES(DES-56) 표준에 따라 DES 56 비트 암호화가 사용 중임을 지정합니다. 이 필드에서는 사용자가 암호 또는 키를 입력해야 합니다.
Password	여기에 Priv-Protocol 비밀번호를 입력합니다. none 의 경우 이 필드는 비활성화됩니다. DES56 의 경우 암호는 8 자에서 16 자 사이여야 합니다.
Auth-Protocol by Key	SNMP 버전 드롭다운 목록에서 v3 를 선택하고 SNMP v3 암호화 드롭다운 목록에서 키를 선택하면 이 옵션을 사용할 수 있습니다. 인증 수준을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • MD5 - HMAC-MD5-96 인증 수준을 사용하려면 선택합니다. 이 필드에서는 사용자가 암호 또는 키를 입력해야 합니다. • SHA - HMAC-SHA 인증 프로토콜이 사용되도록 지정합니다. 이 필드에서는 사용자가 암호 또는 키를 입력해야 합니다.
Key	여기에 Auth-Protocol 키를 입력합니다. MD5 의 경우 이 키는 32 자여야 합니다. SHA 의 경우 이 키는 40 자여야 합니다.
Priv-Protocol by Key	SNMP 버전 드롭다운 목록에서 v3 를 선택하고 SNMP v3 암호화 드롭다운 목록에서 키를 선택하면 이 옵션을 사용할 수 있습니다. 개인 프로토콜을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • 없음 - 사용 중인 권한 부여 프로토콜이 없음을 지정합니다. • DES56 - CBCDES(DES-56) 표준에 따라 DES 56 비트 암호화가 사용 중임을 지정합니다. 이 필드에서는 사용자가 암호 또는 키를 입력해야 합니다.
Key	여기에 Priv-Protocol 키를 입력합니다. none 의 경우 이 필드는 비활성화됩니다. DES56 의 경우 키는 32 자여야 합니다.
IP Access-List Name	사용자와 연결할 표준 IP ACL 을 입력합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새 항목을 추가합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

SNMP Host Table Settings

이 창은 SNMP 알림의 수신자를 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > SNMP > SNMP Host Table Settings 을 클릭합니다.

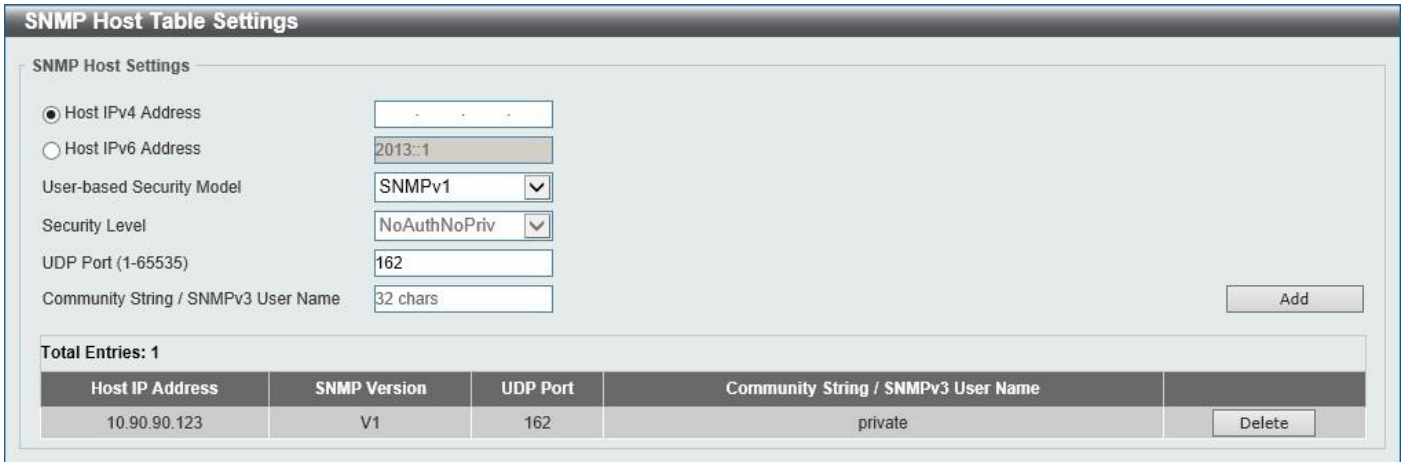

그림 4-10) SNMP 호스트 테이블 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Host IPv4 Address	SNMP 알림 호스트의 IPv4 주소를 입력합니다.
Host IPv6 Address	SNMP 알림 호스트의 IPv6 주소를 입력합니다.
User-based Security Model	여기에서 보안 모델을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • SNMPv1 - 그룹 사용자가 SNMPv1 보안 모델을 사용할 수 있도록 하려면 선택합니다. • SNMPv2c - 그룹 사용자가 SNMPv2c 보안 모델을 사용할 수 있도록 하려면 선택합니다. • SNMPv3 - 그룹 사용자가 SNMPv3 보안 모델을 사용할 수 있도록 하려면 선택합니다.
Security Level	User-based Security Model(사용자 기반 보안 모델) 드롭다운 목록에서 SNMPv3 를 선택하면 이 옵션을 사용할 수 있습니다. • NoAuthNoPriv - 스위치와 원격 SNMP 관리자 간에 전송되는 패킷의 권한 부여 및 암호화가 없음을 지정합니다. • AuthNoPriv - 권한 부여가 필요하지만 스위치와 원격 SNMP 관리자 간에 전송되는 패킷의 암호화는 없음을 지정합니다. • AuthPriv - 권한 부여가 필요하고 스위치와 원격 SNMP 관리자 간에 전송되는 패킷이 암호화되도록 지정합니다.
UDP Port	UDP 포트 번호를 입력합니다. 기본 트랩 UDP 포트 번호는 162 입니다. UDP 포트 번호의 범위는 1 에서 65535 까지입니다. 일부 포트 번호는 다른 프로토콜과 충돌할 수 있습니다.
Community String / SNMPv3 User Name	알림 패킷과 함께 전송할 커뮤니티 문자열 또는 SNMPv3 사용자 이름을 입력합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새 항목을 추가합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

RMON

RMON Global Settings

이 창은 스위치의 SNMP 기능에 대한 상승 및 하강 경보 트랩 기능에 대한 RMON 을 활성화하거나 비활성화하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > RMON > RMON Global Settings 를 클릭합니다.

그림 4-11) RMON Global Settings 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
RMON Rising Alarm Trap	RMON Rising Alarm Trap 기능을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
RMON Falling Alarm Trap	RMON Falling Alarm Trap 기능을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

RMON Statistics Settings

이 창은 지정된 포트에서 RMON 통계를 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > RMON > RMON Statistics Settings 를 클릭합니다.

그림 4-12) RMON 통계 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Port	포트를 선택하려면 선택합니다.
Index	RMON 테이블 인덱스를 입력합니다. 값은 1 에서 65535 사이입니다.
Owner	소유자 문자열을 입력합니다. 문자열은 최대 127 자까지 가능합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새 항목을 추가합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Show Detail 버튼을 클릭하여 특정 포트의 세부 정보를 확인합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Show Detail 버튼을 클릭하면 다음과 같은 창이 나타납니다.

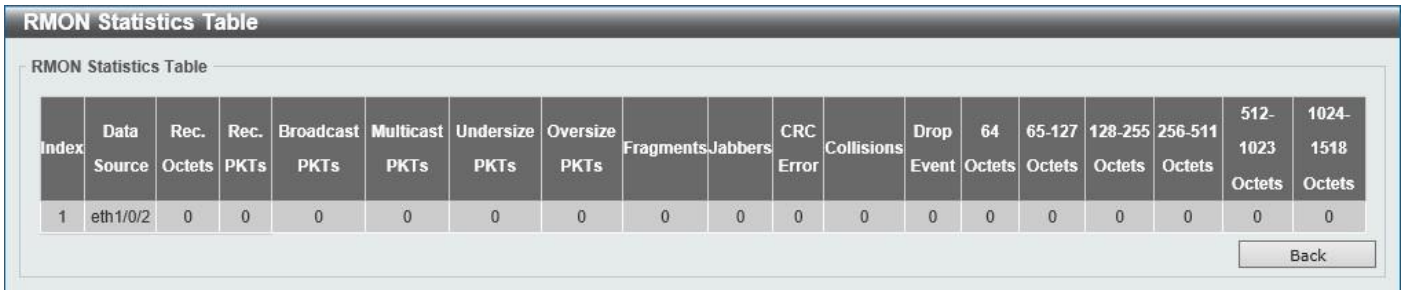

그림 4-13) RMON 통계 설정(세부 정보 표시) 창

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

RMON History Settings

이 창은 지정된 포트에서 수집된 RMON MIB 기록 통계를 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > RMON > RMON History Settings 를 클릭합니다.

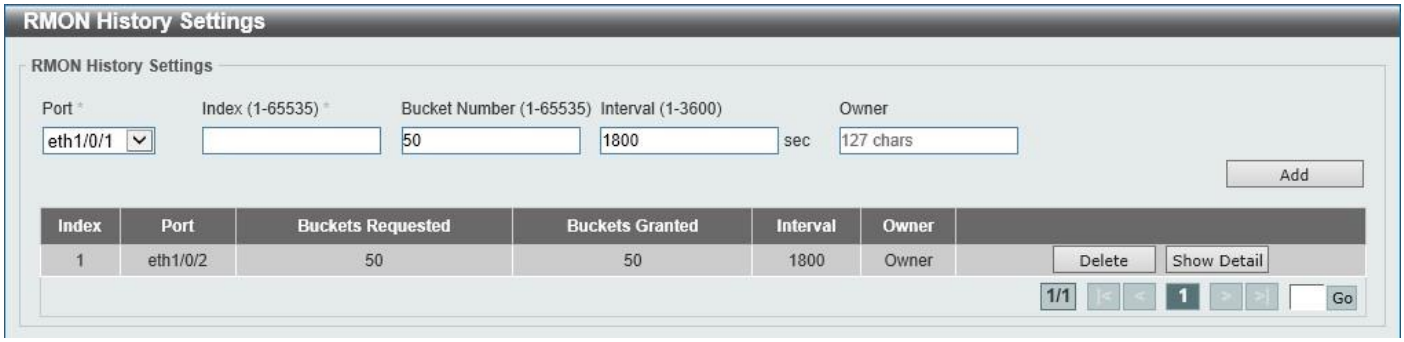

그림 4-14) RMON 기록 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Port	여기에서 사용할 포트를 선택합니다.
Index	기록 그룹 테이블 인덱스를 입력합니다. 값은 1 에서 65535 사이입니다.
Bucket Number	통계의 RMON 수집 기록 그룹에 지정된 버킷 수를 입력합니다. 범위는 1 에서 65535 사이입니다. 기본값은 50 입니다.
Interval	각 폴링 주기의 시간을 초 단위로 입력합니다. 범위는 1 에서 3600 사이입니다.
Owner	소유자 문자열을 입력합니다. 문자열은 최대 127 자까지 가능합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새 항목을 추가합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Show Detail 버튼을 클릭하여 특정 포트의 세부 정보를 확인합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Show Detail 버튼을 클릭하면 다음과 같은 창이 나타납니다.

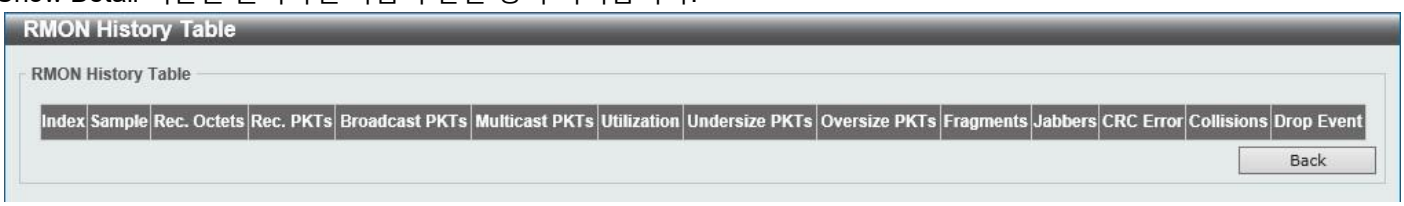

그림 4-15 RMON 기록 설정(세부 정보 표시) 창

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

RMON Alarm Settings

이 창은 Interface 를 모니터링하기 위해 경보 항목을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > RMON > RMON Alarm Settings 를 클릭합니다.

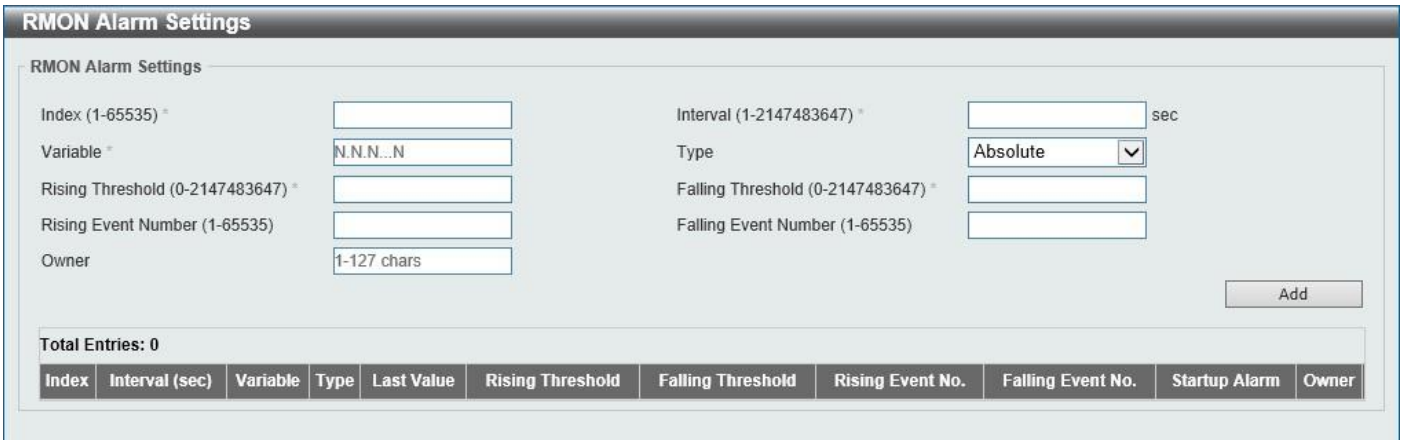

그림 4-16) RMON 알람 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Index	알람 인덱스를 입력합니다. 범위는 1 에서 65535 사이입니다.
Interval	변수를 샘플링하고 임계값을 확인하기 위한 간격(초)을 입력합니다. 유효한 범위는 1 초에서 2147483648 초 사이입니다.
Variable	샘플링할 변수의 개체 식별자를 입력합니다.
Type	모니터링 유형을 선택합니다. 선택할 수 있는 옵션은 Absolute(절대) 및 Delta(델타)입니다.
Rising Threshold	0 에서 2147483647 사이의 상승 임계값을 입력합니다.
Falling Threshold	0 에서 2147483647 사이의 하강 임계값을 입력합니다.
Rising Event Number	rising threshold crossing 이벤트를 알리는 데 사용되는 이벤트 항목의 색인을 입력합니다. 유효한 범위는 1 에서 65535 사이입니다. 지정하지 않으면 벨소리 울림 임계값을 초과하는 동안 아무 작업도 수행되지 않습니다.
Falling Event Number	떨어지는 임계값 교차 이벤트를 알리는 데 사용되는 이벤트 항목의 색인을 입력합니다. 유효한 범위는 1 에서 65535 사이입니다. 지정하지 않으면 떨어지는 임계값을 초과하는 동안 아무 작업도 수행되지 않습니다.
Owner	소유자 문자열을 최대 127 자까지 입력합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새 항목을 추가합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

RMON Event Settings

이 창은 이벤트 항목을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > RMON > RMON Event Settings 을 클릭합니다.

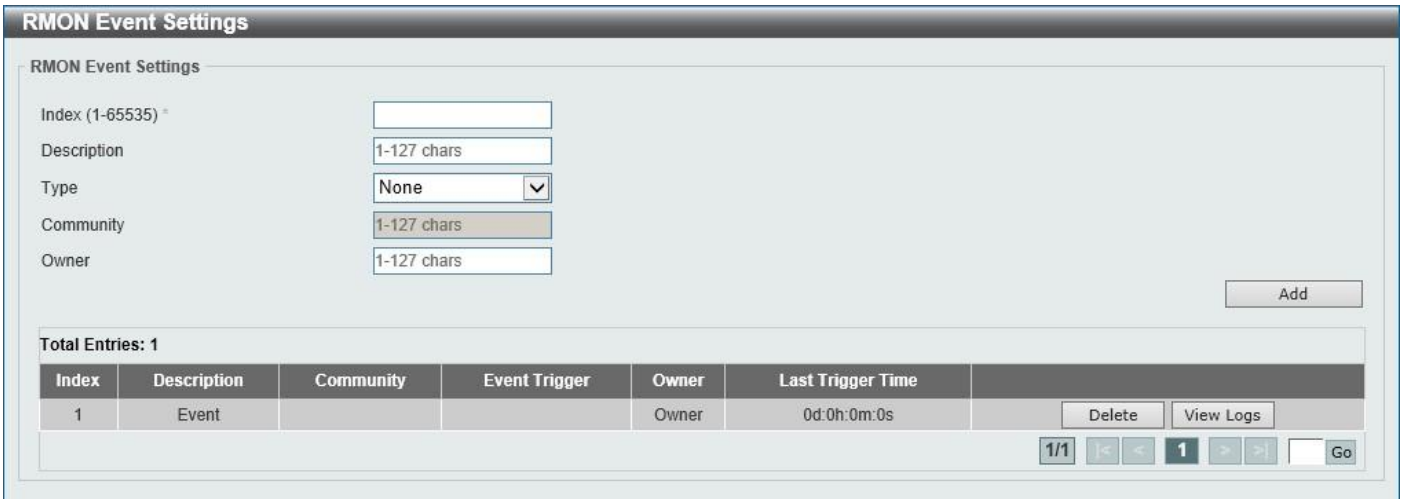

그림 4-17) RMON 이벤트 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Index	여기에 알람 항목의 인덱스 값을 입력합니다. 범위는 1 에서 65535 사이입니다.
Description	RMON 이벤트 항목에 대한 설명을 입력합니다. 문자열의 길이는 최대 127 자입니다.
Type	RMON 이벤트 항목 유형을 선택합니다. 선택할 수 있는 옵션은 None, Log, Trap 및 Log and Trap 입니다.
Community	커뮤니티 문자열을 입력합니다. 문자열은 최대 127 자까지 가능합니다.
Owner	소유자 문자열을 입력합니다. 문자열은 최대 127 자까지 가능합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새 항목을 추가합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

View Logs(로그 보기) 버튼을 클릭하여 특정 포트의 세부 정보를 확인합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

로그 보기 버튼을 클릭하면 다음과 같은 창이 나타납니다.

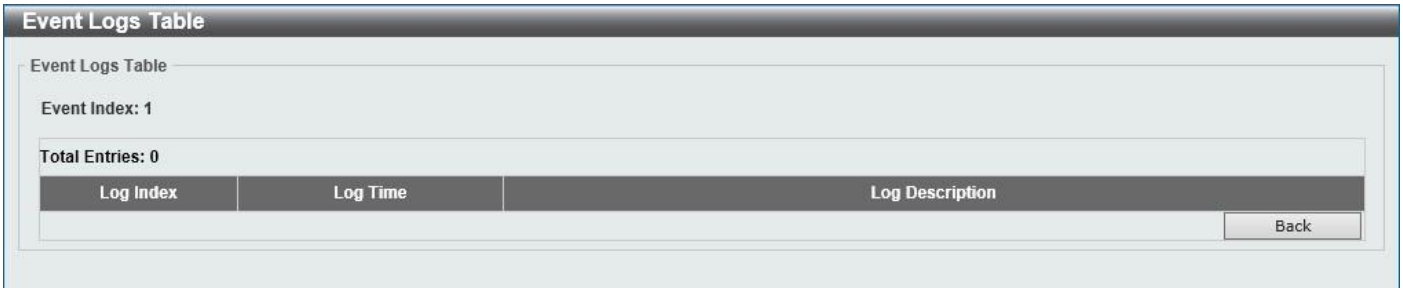

그림 4-18) RMON 이벤트 설정(로그 보기) 창

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

Telnet/Web

이 창은 스위치에서 텔넷 및 웹 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > Telnet/Web 을 클릭합니다.

그림 4-19) Telnet/Web 창

Telnet Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Telnet State	여기에서 텔넷 서버 기능을 활성화하거나 비활성화하려면 선택합니다.
Port	스위치의 텔넷 관리에 사용되는 TCP 포트 번호를 입력합니다. 텔넷 프로토콜의 잘 알려진 TCP 포트는 23 입니다. 범위는 1 에서 65535 사이입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Web Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Web State	웹을 통해 구성을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
Port	스위치의 웹 관리에 사용되는 TCP 포트 번호를 입력합니다. 웹 프로토콜의 잘 알려진 TCP 포트는 80 입니다. 범위는 1 에서 65535 사이입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Session Timeout

이 창은 세션 시간 초과 설정을 표시하고 구성하는 데 사용됩니다. 발신 세션 시간 초과 값은 스위치의 CLI 를 통해 다른 스위치의 텔넷 Interface 로 콘솔/텔넷/SSH 연결에 사용됩니다.

다음 창을 보려면 아래와 같이 Management > Session Timeout 을 클릭합니다.

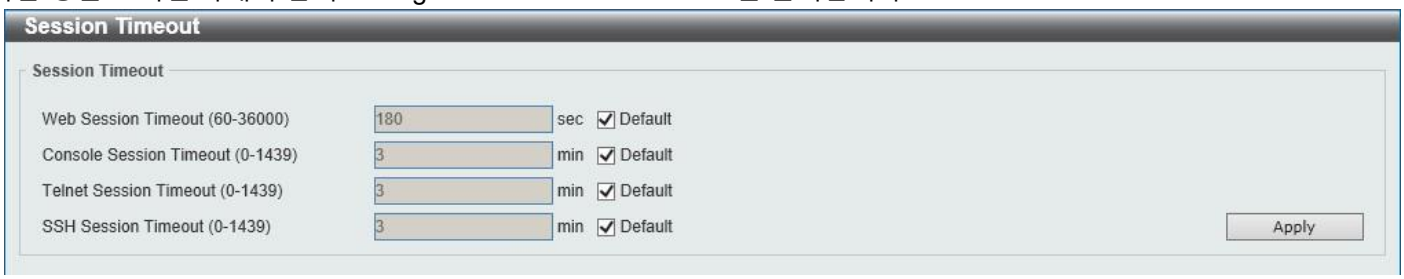

그림 4-20) 세션 시간 초과 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Web Session Timeout	여기에 웹 세션 시간 제한 값을 입력합니다. 범위는 60 초에서 36000 초 사이입니다. 기본값은 180 초입니다. 기본값을 사용하려면 기본값 옵션을 선택합니다.

Console Session Timeout	여기에 콘솔 세션 시간 제한 값을 입력합니다. 범위는 0 분에서 1439 분 사이입니다. 시간 초과를 비활성화하려면 0 을 입력합니다. 기본값은 3 분입니다. 기본값을 사용하려면 기본값 옵션을 선택합니다.
Telnet Session Timeout	여기에 Telnet 세션 시간 초과 값을 입력합니다. 범위는 0 분에서 1439 분 사이입니다. 시간 초과를 비활성화하려면 0 을 입력합니다. 기본값은 3 분입니다. 기본값을 사용하려면 기본값 옵션을 선택합니다.
SSH Session Timeout	여기에 SSH 세션 시간 제한 값을 입력합니다. 범위는 0 분에서 1439 분 사이입니다. 시간 초과를 비활성화하려면 0 을 입력합니다. 기본값은 3 분입니다. 기본값을 사용하려면 기본값 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DHCP

Service DHCP

이 창은 스위치에서 DHCP 서비스를 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > DHCP > Service DHCP 를 클릭합니다.

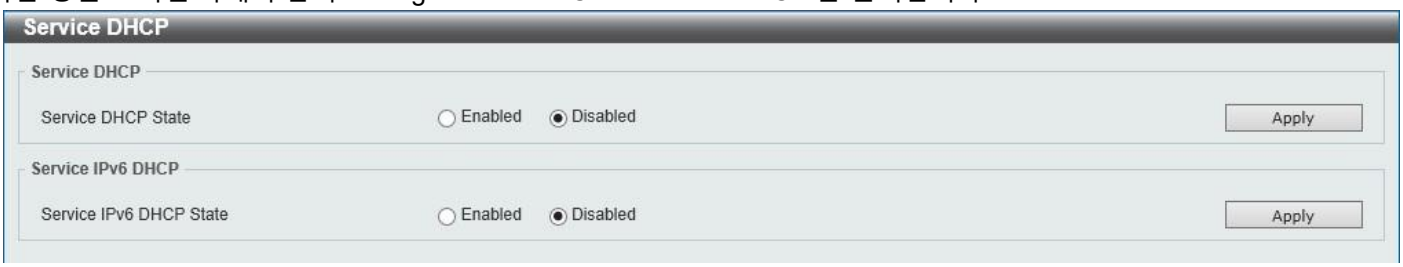

그림 4-21) 서비스 DHCP 창

서비스 DHCP 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Service DHCP State	DHCP 서비스를 활성화하거나 비활성화하려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

서비스 IPv6 DHCP 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Service IPv6 DHCP State	IPv6 DHCP 서비스를 활성화하거나 비활성화하려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DHCP Class Settings

이 창은 DHCP 클래스에 대한 DHCP 클래스 및 DHCP 옵션 일치 패턴을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > DHCP > DHCP Class Settings 를 클릭합니다.

그림 4-22) DHCP 클래스 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Class Name	DHCP 클래스 이름을 최대 32 자로 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Edit 버튼을 클릭하여 해당 DCHP 클래스에 대한 DHCP 옵션 일치 패턴을 수정합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Edit 버튼을 클릭하면 다음과 같은 창이 나타납니다.

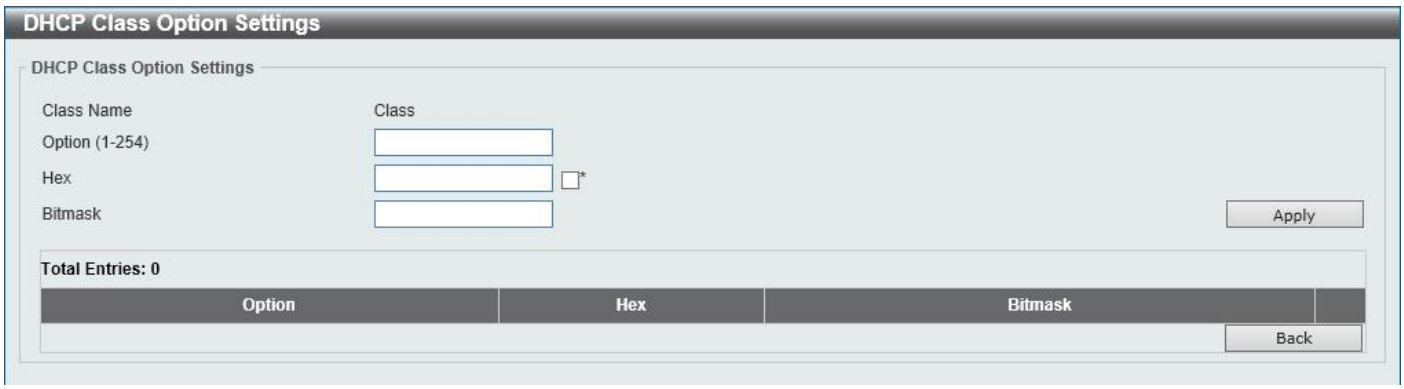

그림 4-23) DHCP 클래스 설정(편집) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Option	DHCP 옵션 번호를 입력합니다. 범위는 1 에서 254 사이입니다.
Hex	지정된 DHCP 옵션의 헥스 패턴을 입력합니다. 옵션의 나머지 비트와 일치하지 않도록 * 확인란을 선택합니다.
Bitmask	패턴 마스킹을 위해 헥스 비트 마스크를 입력합니다. 마스킹된 패턴 비트가 일치합니다. 지정하지 않으면 Hex 필드에 입력된 모든 비트가 확인됩니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

DHCP Relay

DHCP Relay Global Settings

이 창은 전역 DHCP 릴레이 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > DHCP > DHCP Relay > DHCP Relay Global Settings 를 클릭합니다.

그림 4-24) DHCP 릴레이 Global Settings 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
DHCP Smart Relay State	여기에서 DHCP 스마트 릴레이 상태를 전역적으로 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DHCP Relay Pool Settings

이 창은 DHCP 릴레이 에이전트에서 DHCP 릴레이 풀을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > DHCP > DHCP Relay > DHCP Relay Pool Settings 를 클릭합니다.

그림 4-25) DHCP 릴레이 풀 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Pool Name	주소 풀 이름을 최대 32 자로 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Edit 버튼을 클릭하여 특정 DHCP 풀의 해당 정보를 수정합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Source 에서 Edit 버튼을 클릭하면 다음과 같은 창이 나타납니다.

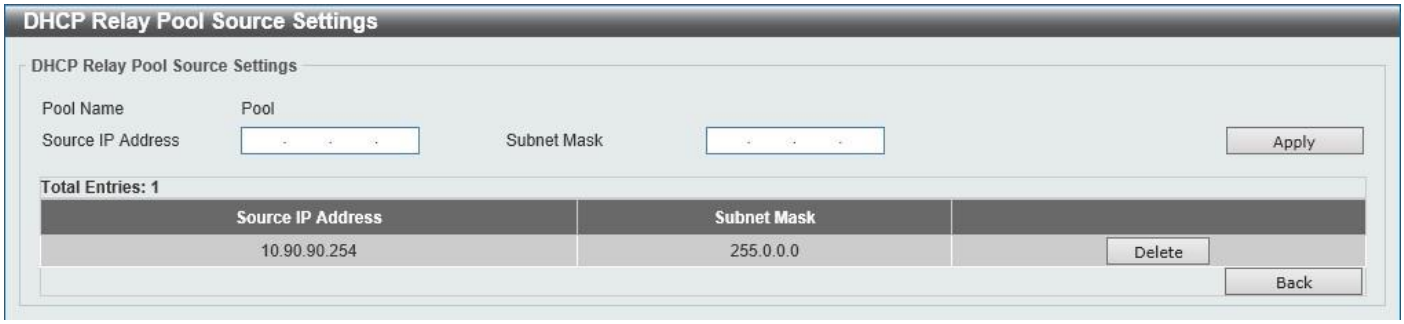

그림 4-26) DHCP 릴레이 풀 소스 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Source IP Address	클라이언트 패킷의 소스 서브넷을 입력합니다.

Subnet Mask	소스 서브넷의 네트워크 마스크를 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

Destination 에서 Edit 버튼을 클릭하면 다음과 같은 창이 나타납니다.

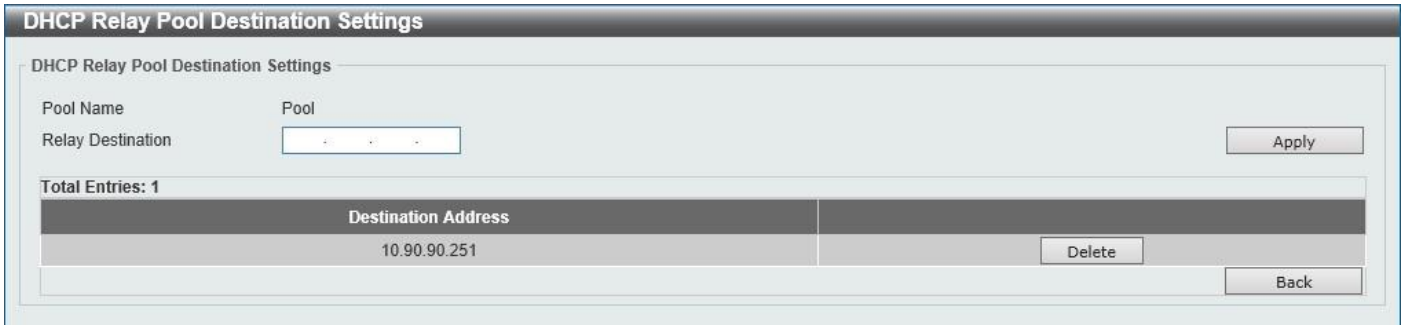

그림 4-27) DHCP 릴레이 풀 대상 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Relay Destination	릴레이 대상 DHCP 서버 IP Address 를 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

Class 에서 Edit 버튼을 클릭하면 다음과 같은 창이 나타납니다.

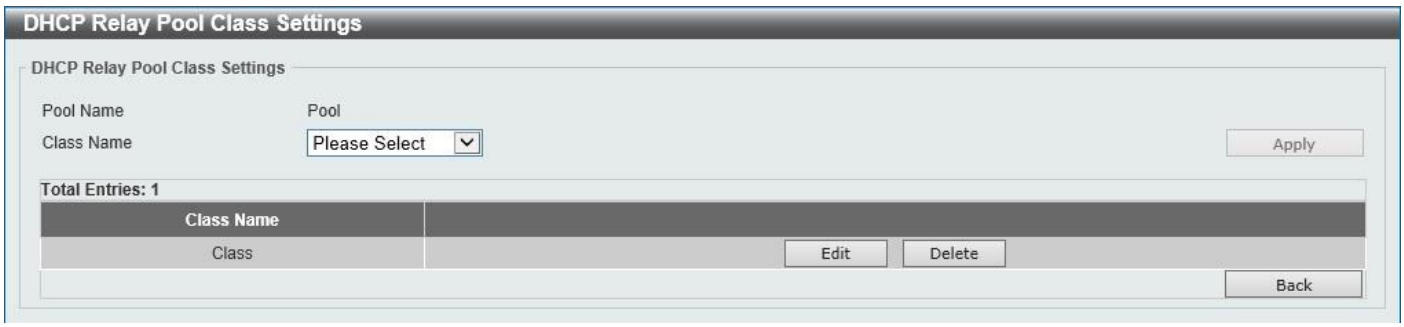

그림 4-28) DHCP 릴레이 풀 클래스 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Class Name	DHCP 클래스 이름을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Edit 버튼을 클릭하여 자세한 정보를 편집합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

Edit 버튼을 클릭하면 다음과 같은 창이 나타납니다.

그림 4-29) DHCP 릴레이 풀 클래스 편집 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Relay Target	DHCP 클래스에 정의된 옵션의 값 패턴과 일치하는 패킷을 릴레이하기 위한 DHCP 릴레이 대상을 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

DHCP Relay Information Settings

이 창은 DHCP 릴레이 정보를 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > DHCP > DHCP Relay > DHCP Relay Information Settings 을 클릭합니다.

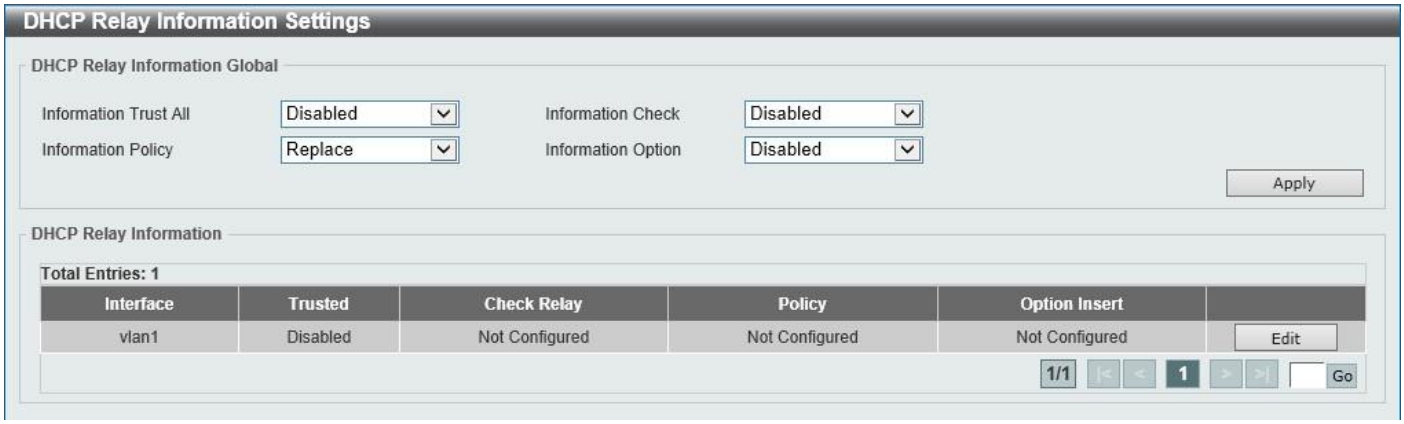

그림 4-30) DHCP 릴레이 정보 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Information Trust All	모든 Interface 에 대한 IP DHCP 릴레이 정보를 신뢰하도록 DHCP 릴레이 에이전트를 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
Information Check	수신된 DHCP 응답 패킷에서 릴레이 에이전트 정보 옵션의 유효성을 검사하고 제거하기 위해 DHCP 릴레이 에이전트를 활성화하거나 비활성화하려면 이 옵션을 선택합니다.

Information Policy	DHCP 릴레이 에이전트에 대한 Option 82 re-forwarding policy 를 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Keep(유지) - 이미 릴레이 옵션이 있는 패킷을 유지하려면 선택합니다. 패킷은 변경되지 않고 DHCP 서버로 직접 릴레이 됩니다. • Drop(삭제) - 이미 릴레이 옵션이 있는 패킷을 삭제하려면 선택합니다. • Replace(교체) - 이미 릴레이 옵션이 있는 패킷을 교체하려면 선택합니다. 패킷이 새 옵션으로 바뀝니다.
Information Option	DHCP 요청 패킷을 릴레이 하는 동안 릴레이 에이전트 정보(옵션 82)의 삽입을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Edit 버튼을 클릭하여 해당 Interface 를 수정합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

DHCP Relay Information Option Format Settings

이 창은 DHCP 정보 형식을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > DHCP > DHCP Relay > DHCP Relay Information Option Format Settings 을 클릭합니다.

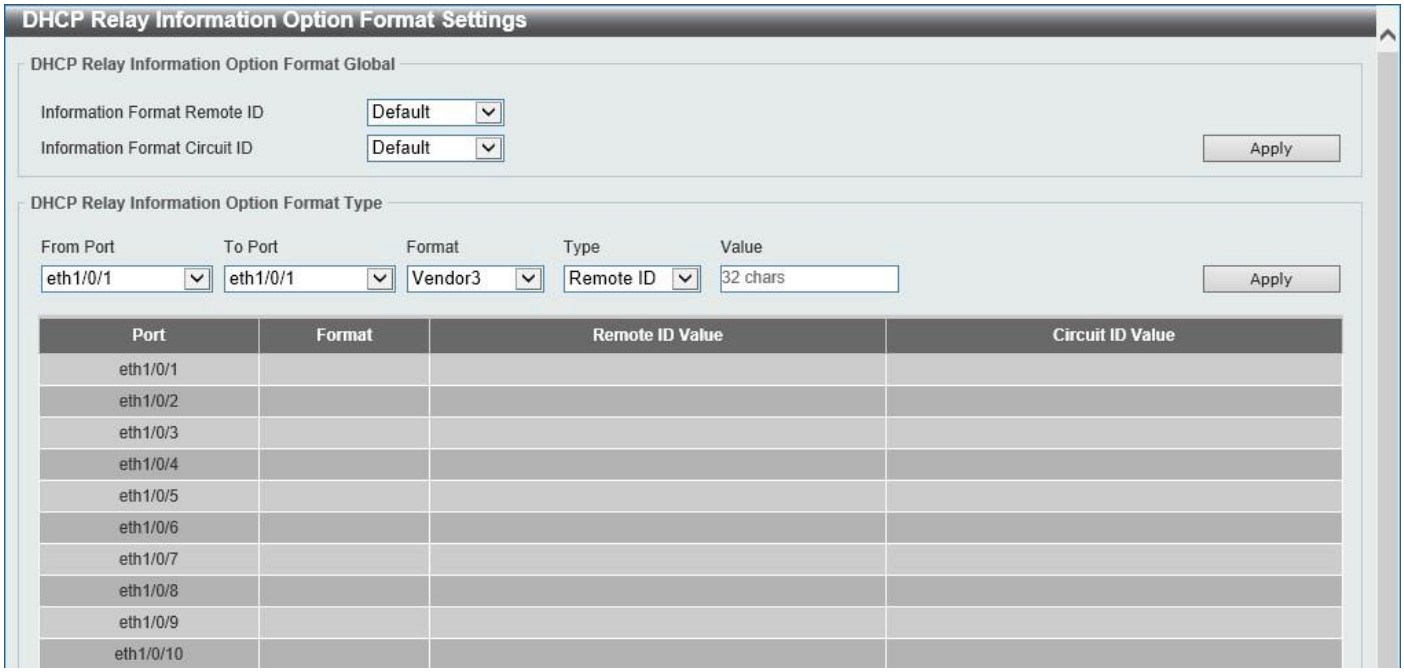

그림 4-31) DHCP 릴레이 정보 옵션 형식 설정 창

DHCP Relay Information Option Format Global 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Information Format Remote ID	DHCP 정보 원격 ID 하위 옵션을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Default(기본값) - 스위치의 시스템 MAC 주소를 원격 ID 로 사용하려면 선택합니다. • User Define(사용자 정의) - 사용자 정의 원격 ID 를 사용하려면 선택합니다. 텍스트 상자에 최대 32 자의 사용자 정의 문자열을 입력합니다. • 공급업체 2 - 공급업체 2 를 원격 ID 로 사용하려면 선택합니다.

	• 공급업체 3 - 공급업체 3 을 원격 ID 로 사용하려면 선택합니다.
Information Format Circuit ID	DHCP 정보 회로 ID 하위 옵션을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Default(기본값) - 기본 회로 ID 하위 옵션을 사용하려면 선택합니다. • User Define(사용자 정의) - 사용자 정의 회로 ID 를 사용하려면 선택합니다. 텍스트 상자에 최대 32 자의 사용자 정의 문자열을 입력합니다. • 공급업체 1 - 공급업체 1 을 회로 ID 로 사용하려면 선택합니다. • 공급업체 2 - 공급업체 2 를 회로 ID 로 사용하려면 선택합니다. • 공급업체 3 - 공급업체 3 을 회로 ID 로 사용하려면 선택합니다. • 공급업체 4 - 공급업체 4 를 회로 ID 로 사용하려면 선택합니다. • 공급업체 5 - 공급업체 5 를 회선 ID 로 사용하려면 선택합니다. • 공급업체 6 - 공급업체 6 을 회로 ID 로 사용하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DHCP Relay Information Option Format Global 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
Format	공급업체 3 형식이 사용되도록 지정합니다.
Type	여기에서 원격 ID 유형 또는 회선 ID 유형을 사용하려면 선택합니다.
Value	여기에서 remote/circuit ID 하위 옵션의 Option 82 정보에 대한 공급업체 정의 문자열을 입력합니다. 이 문자열은 최대 32 자까지 가능합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DHCP Local Relay VLAN Settings

이 창은 VLAN 또는 VLAN 그룹에서 로컬 릴레이를 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > DHCP > DHCP Relay > DHCP Local Relay VLAN Settings 를 클릭합니다.

그림 4-32) DHCP 로컬 릴레이 VLAN 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
DHCP Local Relay VID List	DHCP 로컬 릴레이의 VLAN ID 를 입력합니다. 모든 VLAN 을 선택하려면 모든 VLAN 확인란을 선택합니다.

State	특정 VLAN 에서 DHCP 로컬 릴레이를 활성화하거나 비활성화하려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

참고: DHCP 릴레이 포트의 상태가 비활성화되어 있으면 포트가 릴레이하거나 로컬로 릴레이하지 않습니다 DHCP 패킷을 수신했습니다.

DHCPv6 Relay

DHCPv6 Relay Global Settings

이 창은 DHCPv6 릴레이 원격 ID 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Global Settings 을 클릭합니다.

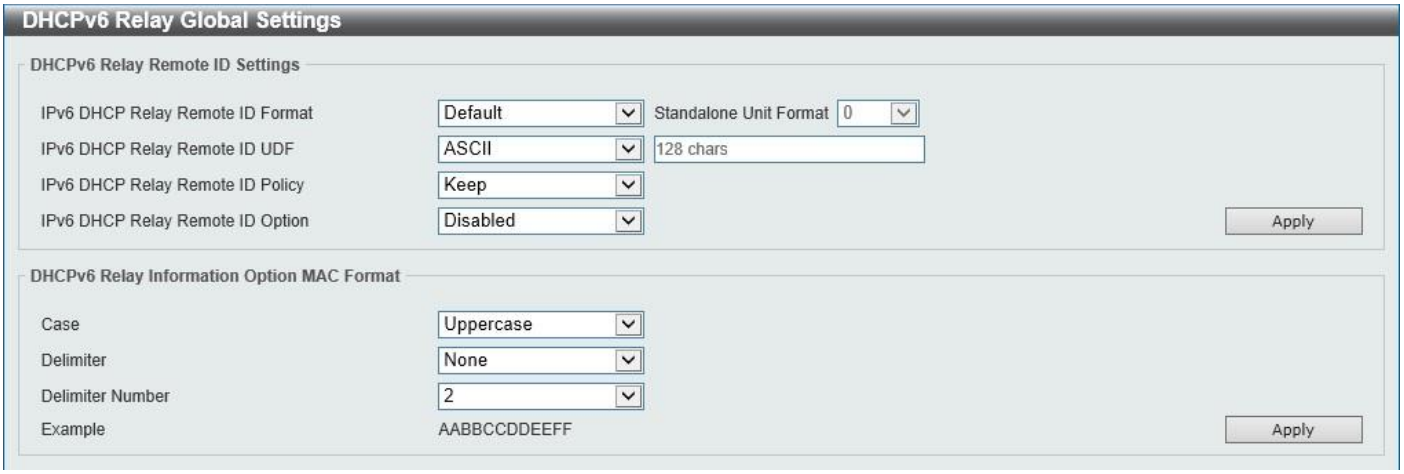

그림 4-33) DHCPv6 릴레이 Global Settings 창

DHCPv6 릴레이 원격 ID 설정에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
IPv6 DHCP Relay Remote ID Format	여기에서 사용할 IPv6 DHCP 릴레이 원격 ID 형식을 선택합니다. 선택할 수 있는 옵션은 기본값(Default), 사용자 정의가 있는 CID(CID with User Define), 사용자 정의(User Define) 및 전문가 UDF 입니다.
Standalone Unit Format	전문가 UDF 옵션을 선택한 후 여기에서 독립 실행형 단위 형식을 선택합니다. 선택할 수 있는 옵션은 0 과 1 입니다.
IPv6 DHCP Relay Remote ID UDF	원격 ID 에 대한 사용자 정의 필드(UDF)를 선택하려면 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • ASCII - 텍스트 상자에 최대 128 자의 ASCII 문자열을 입력하려면 선택합니다. • HEX - 텍스트 상자에 최대 256 자의 16 진수 문자열을 입력하려면 선택합니다.
IPv6 DHCP Relay Remote ID Policy	DHCPv6 릴레이 에이전트에 대한 옵션 37 전달 정책을 선택하려면 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Keep(유지) - 이미 릴레이 에이전트 Remote-ID 옵션이 있는 DHCPv6 요청 패킷을 변경하지 않고 DHCPv6 서버로 직접 릴레이하도록 선택합니다.

	• Drop(드롭) - 릴레이 에이전트 Remote-ID Option 37 이 이미 있는 패킷을 폐기하려면 선택합니다.
IPv6 DHCP Relay Remote ID Option	IPv6 요청 패킷에 대한 DHCP 를 릴레이하는 동안 릴레이 에이전트 원격 ID 옵션 37 의 삽입을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DHCPv6 릴레이 정보 옵션 MAC 형식에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Case	여기에서 사용할 케이스를 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • 소문자 -MAC 형식이 소문자가 되도록 지정합니다. ○ 예: aa-bb-cc-dd-ee-ff. • 대문자 -MAC 형식이 대문자가 되도록 지정합니다. ○ 예: AA-BB-CC-DD-EE-FF.
Delimiter	여기에 사용할 구분 기호를 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • 하이픈 - MAC 주소 형식에 하이픈이 포함되도록 지정합니다. 예: AA-BB-CC-DD-EE-FF. • 콜론 - MAC 주소 형식에 콜론이 포함되도록 지정합니다. 예를 들어 AA:BB:CC:DD:EE:FF 입니다. • 점 - MAC 주소 형식에 점을 포함하도록 지정합니다. 예를 들어 AA 입니다. 비비. CC.DD.EE. FF 입니다. • 없음 - MAC 주소 형식에 구분 기호가 포함되지 않도록 지정합니다. 예: AABBCCDDEEFF.
Delimiter Number	여기서 MAC 주소 형식에 사용할 구분 기호 번호를 지정합니다. 선택할 수 있는 옵션은 다음과 같습니다. • 1 - 단일 구분 기호를 사용하도록 지정합니다. 예) AABBCC.DDEEFF • 2 - 두 개의 구분 기호를 사용하도록 지정합니다. 예) AABB.CCDD.EEFF • 5 - 여러 구분 기호를 사용하도록 지정합니다. 예) AA.BB.CC.DD.EE.FF

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DHCPv6 Relay Interface Settings

이 창은 DHCPv6 릴레이 Interface 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Interface Settings 을 클릭합니다.

그림 4-34) DHCPv6 릴레이 Interface 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Interface VLAN	DHCPv6 릴레이에 사용되는 Interface VLAN ID 를 여기에 입력합니다. 범위는 1 에서 4094 사이입니다.
Destination IPv6 Address	DHCPv6 릴레이 대상 주소를 입력합니다.
Output Interface VLAN	여기에 릴레이 대상의 출력 Interface VLAN ID 를 입력합니다. 범위는 1 에서 4094 사이입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

DHCPv6 Relay Remote ID Profile Settings

이 창은 DHCPv6 릴레이 원격 ID 프로파일 설정을 표시하고 구성하는 데 사용됩니다. 이는 DHCPv6 릴레이 옵션 82 에 대한 새 프로필을 생성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Remote ID Profile Settings 을 클릭합니다.

그림 4-35) DHCPv6 릴레이 원격 ID 프로파일 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Profile Name	여기에 프로필 이름을 입력합니다. 이 문자열은 최대 32 자까지 가능합니다.
Format String	Edit 버튼을 클릭한 후 여기에 옵션 82 형식 문자열을 입력합니다. 이 문자열은 최대 251 자까지 가능합니다. 다음 규칙을 고려해야 합니다. • 이 문자열은 16 진수 값, ASCII 문자열 또는 16 진수 값과 ASCII 문자의 조합일 수 있습니다. ASCII 문자열은 "Ethernet"과 같이 따옴표("")로 묶어야 합니다. 따옴표 밖에 있는 모든 ASCII 문자는 16 진수 값으로 해석됩니다. • 형식이 지정된 키 문자열은 패킷에 캡슐화되기 전에 변환해야 하는 문자열입니다. 형식이 지정된 키 문자열은 ASCII 문자열과 16 진수 값을 모두 포함할 수 있습니다. 예를 들어 "%" +"$"+"1~32"+ "keyword"+":": ○ % - 이 문자 다음에 오는 문자열이 형식이 지정된 키 문자열임을 나타냅니다. ○ "$" 또는 "0" - (선택 사항) 채우기 표시기를 나타냅니다. 이 옵션은 길이 옵션을 충족하도록 형식화된 키 문자열을 채우는 방법을 지정합니다. 이 옵션은 "$" 또는 "0"일 수 있으며 동시에 둘 다로 지정할 수 없습니다. ▪ "$" - 선행 공백(0x20)을 채우는 것을 나타냅니다. ▪ "0" - 선행 0 을 채우는 것을 나타냅니다. 선행 0(0)을 채우는 것이 기본 설정입니다. ○ 1~32 - (선택 사항) 길이 옵션을 나타냅니다. 변환된 키 문자열이 차지해야 하는 문자 또는 바이트 수를 지정합니다. 변환된 키 문자열의 실제 길이가 길이보다 작은 경우
Parameter	Description

	이 옵션으로 지정하면 채우기 표시기가 채워집니다. 그렇지 않으면 이 길이 옵션과 채우기 표시기가 무시되고 실제 문자열이 직접 사용됩니다. ○ keyword - 키워드가 시스템의 실제 값에 따라 번역됨을 나타냅니다. 다음 키워드 정의는 알 수 없거나 지원되지 않는 키워드가 감지되는 경우 명령이 거부되도록 지정합니다. ▪ devtype - 장치의 모델 이름입니다. ASCII 문자열만 허용됩니다. ▪ sysname - 스위치의 시스템 이름을 나타냅니다. ASCII 문자열만 허용됩니다. ▪ ifdescr - *ifDescr* (IF-MIB)에서 파생됩니다. ASCII 문자열만 허용됩니다. ▪ portmac - 포트의 MAC 주소를 나타냅니다. ASCII 문자열 또는 16 진수 값일 수 있습니다. ASCII 문자열 형식인 경우 특수 CLI 명령을 사용하여 MAC 주소 형식을 사용자 지정할 수 있습니다. 16 진수 값 형식인 경우 MAC 주소는 16 진수 순서로 캡슐화됩니다. ▪ sysmac - 시스템 MAC 주소를 나타냅니다. ASCII 문자열 또는 16 진수 값일 수 있습니다. ASCII 문자열 형식에서 MAC 주소 형식은 특수 CLI 명령을 사용하여 사용자 지정할 수 있습니다. 16 진수 형식에서 MAC 주소는 16 진수 순서로 캡슐화됩니다. ▪ module - 모듈 ID 번호를 나타냅니다. ASCII 문자열 또는 16 진수 값일 수 있습니다. ▪ port - 로컬 포트 번호를 나타냅니다. ASCII 문자열 또는 16 진수 값일 수 있습니다. ▪ svlan - 외부 VLAN ID 를 나타냅니다. ASCII 문자열 또는 16 진수 값일 수 있습니다. ▪ cvlan - 내부 VLAN ID 를 나타냅니다. ASCII 문자열 또는 16 진수 값일 수 있습니다. ○ : - 포맷된 키 찌르기의 끝을 나타냅니다. 형식화된 키 문자열이 명령의 마지막 Parameter 인 경우 끝 문자(":")를 무시할 수 있습니다. " %"와 ":" 사이의 공백(0x20)은 무시됩니다. 다른 공간은 캡슐화됩니다. • ASCII 문자열은 형식화된 키 문자열과 0~9, a~z, A~Z, !@#$%^&*()_+|-=\[]{};:'"/?.,<>' 및 공백 문자의 조합일 수 있습니다. " \"는 이스케이프 문자입니다. "\" 뒤의 특수 문자는 문자 자체이며, 예를 들어 "\%"는 형식화된 키 문자열의 시작 표시기가 아니라 "%" 자체입니다. 형식화된 키 문자열에 없는 공백도 캡슐화됩니다. • 16 진수 값은 형식이 지정된 키 문자열과 0~9, A~F, a~f 및 공백 문자의 조합일 수 있습니다. 형식이 지정된 키 문자열은 16 진수 값을 지원하는 키워드만 지원합니다. 형식이 지정된 키 문자열에 없는 공백은 무시됩니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.

Delete 버튼을 클릭하여 특정 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

DHCPv6 Relay Format Type Settings

이 창은 DHCPv6 릴레이 형식 유형 설정을 표시하고 구성하는 데 사용됩니다. 이는 각 포트의 expert UDF 문자열의 DHCPv6 릴레이 옵션 37 및 옵션 18 을 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > DHCP > DHCPv6 Relay > DHCPv6 Relay Format Type Settings 을 클릭합니다.

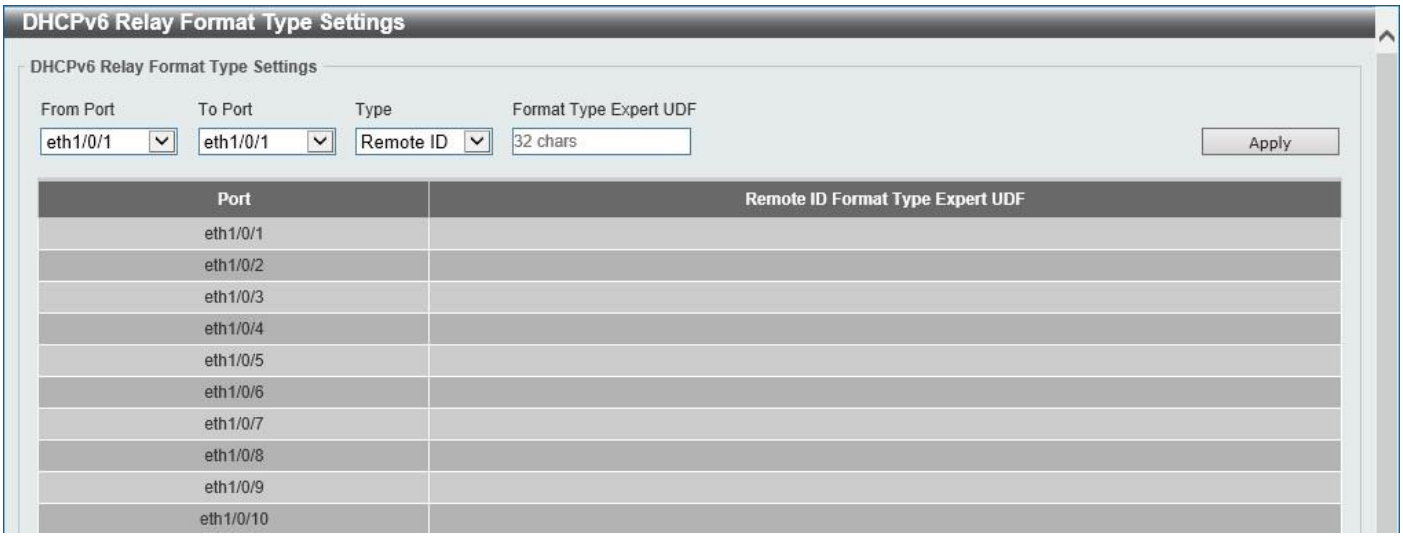

그림 4-36 DHCPv6 릴레이 형식 유형 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
Type	DHCPv6 옵션 37 에 대한 전문가 UDF 형식 유형 문자열을 구성하도록 지정합니다.
Format Type Expert UDF	지정된 포트에서 사용할 형식 유형 expert UDF 문자열을 여기에 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DHCPv6 Local Relay VLAN Settings

이 창은 DHCPv6 로컬 릴레이 VLAN 설정을 표시하고 구성하는 데 사용됩니다. DHCPv6 로컬 릴레이가 활성화되면 클라이언트의 요청 패킷에 옵션 37 및 옵션 18 이 추가됩니다. 옵션 37 의 확인 상태가 활성화된 경우 클라이언트의 요청 패킷을 확인하고 옵션 37 DHCPv6 릴레이 기능이 포함된 경우 패킷을 삭제합니다. 비활성화된 경우, 로컬 릴레이 기능은 옵션 37 의 상태가 활성화 또는 비활성화되어 있는지에 관계없이 항상 패킷을 요청하기 위해 옵션 37 을 추가합니다. DHCPv6 로컬 릴레이 기능은 서버에서 클라이언트로 패킷을 직접 전달합니다.

다음 창을 보려면 아래와 같이 Management > DHCP > DHCPv6 Relay > DHCPv6 Local Relay VLAN Settings 을 클릭합니다.

그림 4-37) DHCPv6 로컬 릴레이 VLAN 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
DHCPv6 Local Relay VID List	여기에 DHCPv6 로컬 릴레이 VLAN ID 를 입력합니다. 여기에 둘 이상의 VLAN ID 를 입력할 수 있습니다. 이 스위치에서 구성된 모든 VLAN 에 이 설정을 적용하려면 All VLANs 옵션을 선택합니다.
State	여기에서 지정된 VLAN 에서 DHCPv6 로컬 릴레이 기능을 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DHCP Auto Configuration

이 창은 DHCP 자동 구성 기능을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > DHCP Auto Configuration 을 클릭합니다.

그림 4-38) DHCP 자동 구성 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Auto Configuration State	이 옵션을 선택하면 자동 구성 기능을 활성화하거나 비활성화할 수 있습니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DNS

DNS(Domain Name System)는 사람이 읽을 수 있는 도메인 이름을 컴퓨터가 통신하는 데 사용하는 IP Address 에 매핑하는 데 사용됩니다. DNS 서버는 이름에서 주소로의 변환을 수행하며, 도메인을 주소로 변환하기 위해 여러 이름 서버에 연결해야 할 수 있습니다. 도메인 이름 서비스를 제공하는 시스템의 주소는 종종 DHCP 또는 BOOTP 서버에서 제공되거나 수동으로 입력하고 시작 시 운영 체제에 구성할 수 있습니다.

DNS Global Settings

이 창은 전역 DNS 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > DNS > DNS Global Settings 을 클릭합니다.

그림 4-39) DNS Global Settings 창

DNS Global Settings 에서 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
IP Domain Lookup	여기에서 IP 도메인 조회 상태를 활성화하거나 비활성화하려면 선택합니다.

IP Name Server Timeout	지정된 이름 서버의 응답을 기다리는 최대 시간을 입력합니다. 이 값은 1 초에서 60 초 사이입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DNS Name Server Settings

이 창은 도메인 이름 서버의 IP Address 를 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > DNS > DNS Name Server Settings 을 클릭합니다.

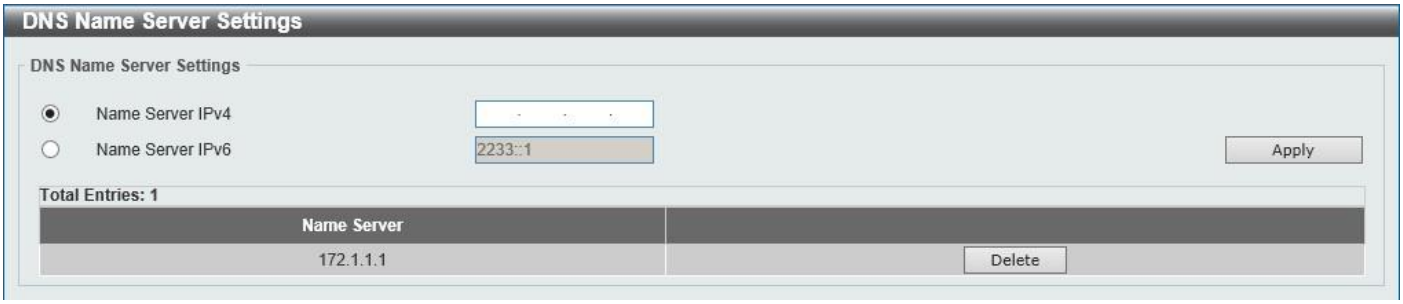

그림 4-40) DNS 이름 서버 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Name Server IPv4	DNS 서버의 IPv4 주소를 선택하여 입력합니다.
Name Server IPv6	DNS 서버의 IPv6 주소를 선택하여 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

DNS Host Settings

이 창은 호스트 테이블의 호스트 이름 및 IP Address 에 대한 정적 매핑 항목을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > DNS > DNS Host Settings 을 클릭합니다.

그림 4-41) DNS Host Settings 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Host Name	장비의 호스트 이름을 입력합니다.
IP Address	장비의 IPv4 주소를 선택하여 입력합니다.
IPv6 Address	장비의 IPv6 주소를 선택하여 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Clear All 버튼을 클릭하여 이 페이지의 모든 필드에 입력한 정보를 지웁니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

File System

이 창은 스위치 파일 시스템을 보고, 관리하고, 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > File System 을 클릭합니다.

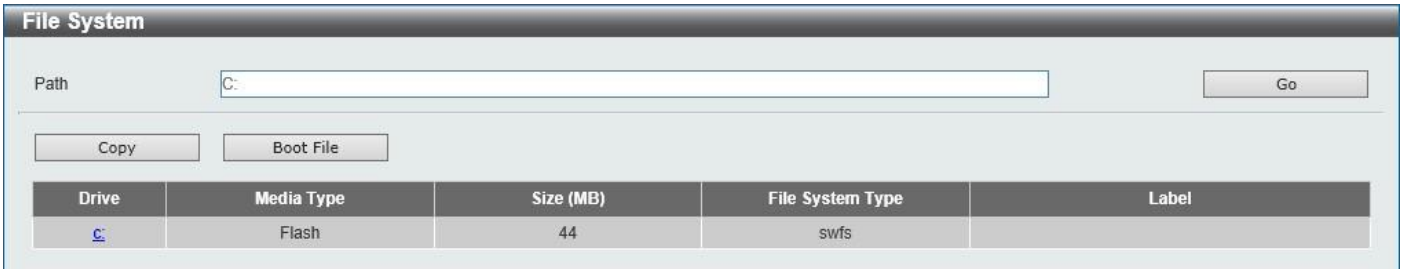

그림 4-42) 파일 시스템 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Path	경로 문자열을 입력합니다.

Go 버튼을 클릭하여 입력한 경로로 이동합니다.

Copy 버튼을 클릭하여 특정 파일을 스위치에 복사합니다.

Boot File 버튼을 클릭하여 부팅 이미지 및 구성 파일 설정을 구성합니다.

c: 하이퍼링크를 클릭하여 C: 드라이브를 탐색합니다.

c : 하이퍼링크를 클릭하면 다음 창이 나타납니다.

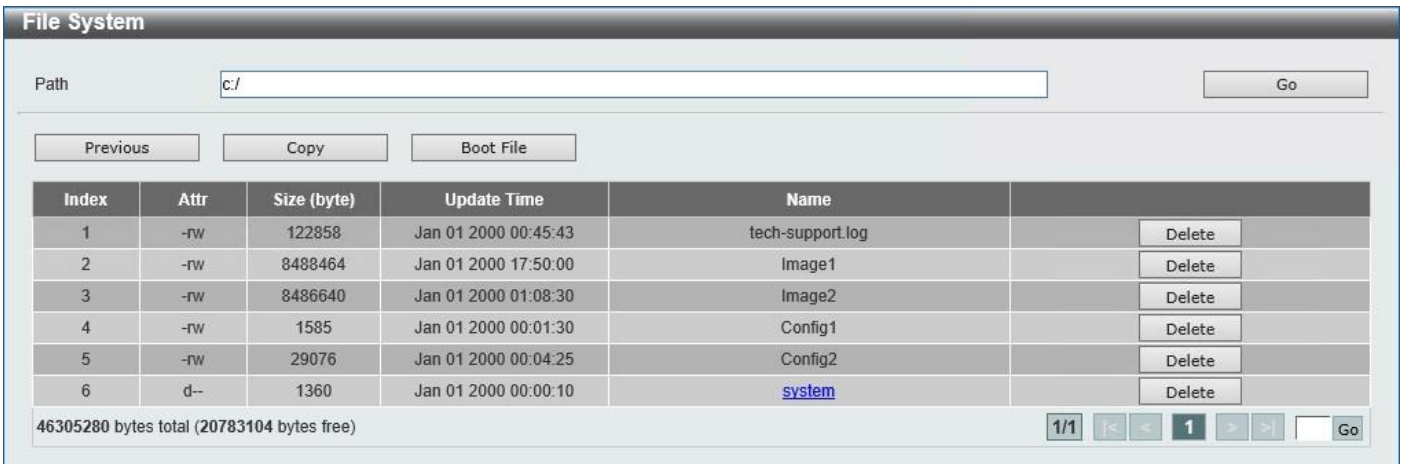

그림 4-43) File System 창

Go 버튼을 클릭하여 입력한 경로로 이동합니다.

Previous 버튼을 클릭하여 이전 창으로 돌아갑니다.

Copy 버튼을 클릭하여 특정 파일을 스위치에 복사합니다.

Boot File 버튼을 클릭하여 부팅 이미지 및 구성 파일 설정을 구성합니다.

Delete 버튼을 클릭하여 파일 시스템에서 특정 파일을 제거합니다.

참고: 부팅 구성 파일이 손상되면 스위치가 자동으로 기본 구성으로 되돌아갑니다.

참고: 부팅 이미지 파일이 손상된 경우 스위치는 다음 부팅 시 백업 이미지 파일을 자동으로 사용합니다.

Copy 버튼을 클릭하면 다음과 같은 창이 나타납니다.

그림 4-44) File System (Copy) 창

파일 복사에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Source	여기에서 복사본의 원본을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • startup-config - 시작 구성을 소스로 복사하도록 지정합니다. • Image 1 - 펌웨어 " Image 1"을 소스로 복사하도록 지정합니다. • Image 2 - 펌웨어 " Image 2"를 소스로 복사하도록 지정합니다. • Configuration 1 - " Configuration 1"을 원본으로 복사하도록 지정합니다. • Configuration 2 - " Configuration 2"를 원본으로 복사하도록 지정합니다.
Destination	여기에서 사본의 대상을 선택하십시오. 선택할 수 있는 옵션은 다음과 같습니다. • running-config - 실행 중인 구성을 소스로 덮어쓰도록 지정합니다. • startup-config - 시작 구성을 소스로 덮어쓰도록 지정합니다. • Image 1 - " Image 1"을 소스로 덮어쓰도록 지정합니다. • Image 2 - " Image 1"를 소스로 덮어쓰도록 지정합니다. • Configuration 1 - " Configuration 1"을 원본으로 덮어쓰도록 지정합니다. • Configuration 2 - " Configuration 2"를 원본으로 덮어쓰도록 지정합니다.
Replace	현재 실행 중인 구성을 표시된 구성 파일로 바꾸도록 지정합니다.

Apply 버튼을 클릭하여 복사를 시작합니다.

Cancel 버튼을 클릭하여 프로세스를 취소합니다.

Boot File 버튼을 클릭하면 다음과 같은 창이 나타납니다.

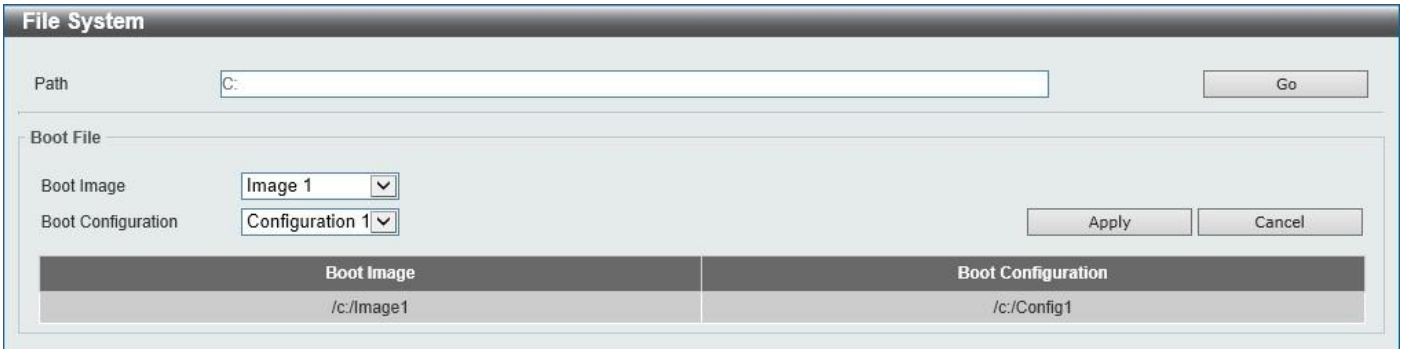

그림 4-45) 파일 시스템(부트 파일) 창

Boot File 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Boot Image	여기에서 부팅 이미지를 선택합니다. 선택할 수 있는 옵션은 Image 1 과 Image 2 입니다.
Boot Configuration	여기에서 부팅 구성을 선택합니다. 선택할 수 있는 옵션은 Configuration 1 과 Configuration 2 입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.
취소 버튼을 클릭하여 변경 사항을 취소합니다.

D-Link Discovery Protocol

이 창은 DDP(D-Link Discovery Protocol) 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Management > D-Link Discovery Protocol 을 클릭합니다.

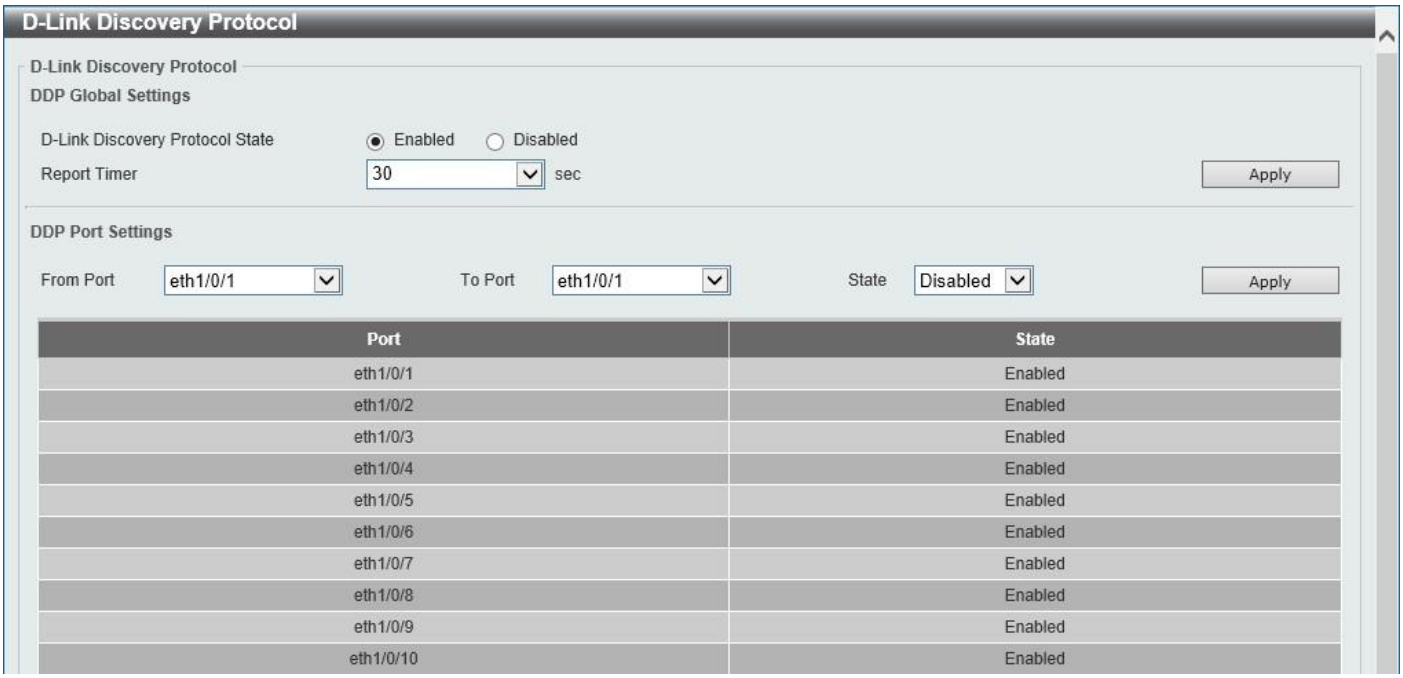

그림 4-46) D-Link Discovery Protocol 창

D-Link Discovery Protocol 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
D-Link Discovery Protocol State	여기에서 DDP 기능을 전역적으로 활성화하거나 비활성화하려면 선택합니다.
Report Timer	여기에서 보고서 타이머 값을 선택합니다. 이는 두 개의 연속 DDP 보고서 메시지 사이의 간격을 구성하는 데 사용됩니다. 선택할 수 있는 옵션은 30, 60, 90, 120 초 또는 Never 입니다. Never 를 선택하면 스위치가 보고서 메시지 전송을 중지합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DDP 포트 설정에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
State	여기에서 지정된 포트에서 DDP 기능을 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

4. Layer 2 Features

FDB
VLAN
STP
Loopback Detection
Link Aggregation
L2 Multicast Control
LLDP

FDB

Static FDB

Unicast Static FDB

이 창은 스위치에서 정적 유니캐스트 전달 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > FDB > Static FDB > Unicast Static FDB 를 클릭합니다.

그림 5-1 유니캐스트 정적 FDB 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Port/Drop	입력한 MAC 주소가 있는 포트 번호를 선택할 수 있습니다. 이 옵션은 유니캐스트 정적 FDB 에서 MAC 주소를 삭제할 수도 있습니다. 포트를 선택할 때 포트 번호를 선택하십시오.
Port Number	포트 옵션을 선택한 후 여기에 사용된 포트 번호를 선택합니다.
VID	연결된 유니캐스트 MAC 주소가 있는 VLAN ID 를 입력합니다.
MAC Address	패킷이 정적으로 전달될 MAC 주소를 입력합니다. 유니캐스트 MAC 주소여야 합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete All 버튼을 클릭하여 디스플레이 테이블에 있는 모든 항목을 삭제합니다.

Delete 버튼을 클릭하여 지정된 항목을 삭제합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

MAC Address Table Settings

이 창은 전역 MAC 주소 테이블 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > FDB > MAC Address Table Settings 을 클릭합니다.

그림 5-2) MAC 주소 테이블 설정(Global Settings) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Aging Time	여기에 MAC 주소 테이블 에이징 시간을 입력합니다. 이 값은 10 초에서 1000000 초 사이여야 합니다. 0 을 입력하면 MAC 주소 에이징이 비활성화됩니다. 기본적으로 이 값은 300 초입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

MAC 주소 학습 탭 옵션을 선택하면 페이지 상단에서 다음 페이지를 사용할 수 있습니다.

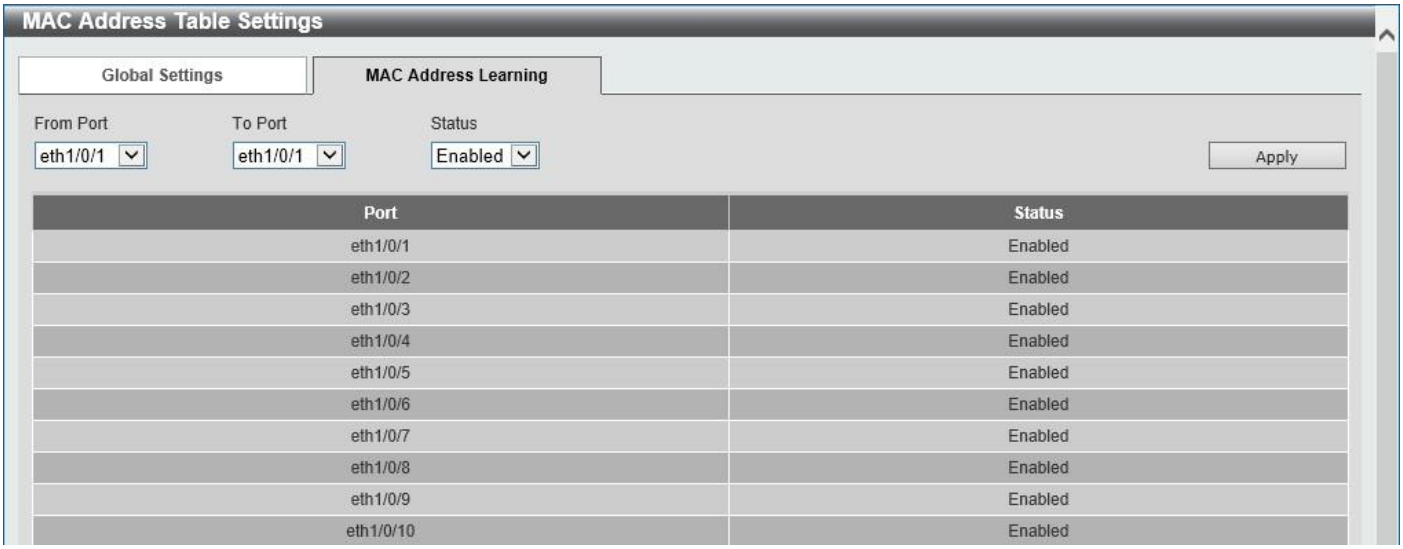

그림 5-3) MAC 주소 테이블 설정(MAC 주소 포트 학습 설정) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
Status	여기에 지정된 포트에서 MAC 주소 학습 기능을 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

MAC Address Table

이 창은 MAC 주소 테이블에 나열된 항목을 보는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > FDB > MAC Address Table 을 클릭합니다.

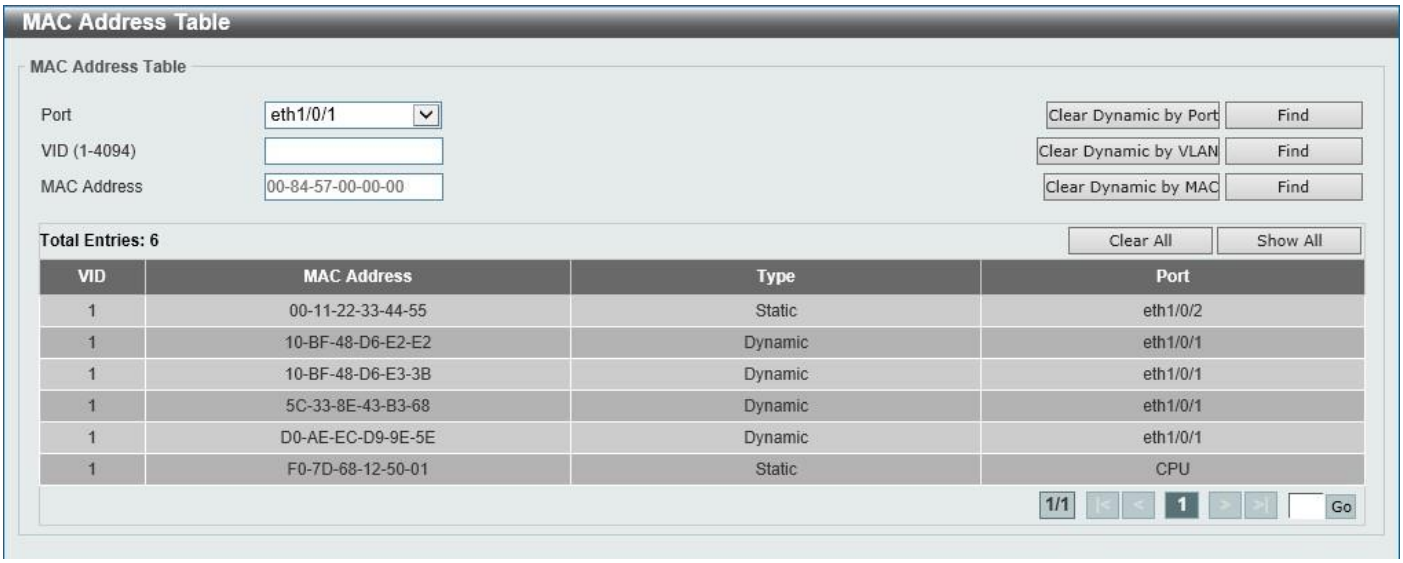

그림 5-4) MAC 주소 테이블 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Port	여기에서 사용할 포트를 선택합니다.
VID	여기에 이 컨피그레이션에 사용할 VLAN ID 를 입력합니다.
MAC Address	여기에 이 컨피그레이션에 사용할 MAC 주소를 입력합니다.

Clear Dynamic by Port 버튼을 클릭하여 해당 포트에 나열된 동적 MAC 주소를 지웁니다.

Clear Dynamic by VLAN 버튼을 클릭하여 해당 VLAN 에 나열된 동적 MAC 주소를 지웁니다.

Clear Dynamic by MAC 버튼을 클릭하여 입력한 동적 MAC 주소를 지웁니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Clear All 버튼을 클릭하여 모든 동적 MAC 주소를 지웁니다.

MAC 주소 테이블에 기록된 모든 MAC 주소를 표시하려면 Show All 버튼을 클릭합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

MAC Notification

이 창은 MAC 알림을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > FDB > MAC Notification 을 클릭합니다.

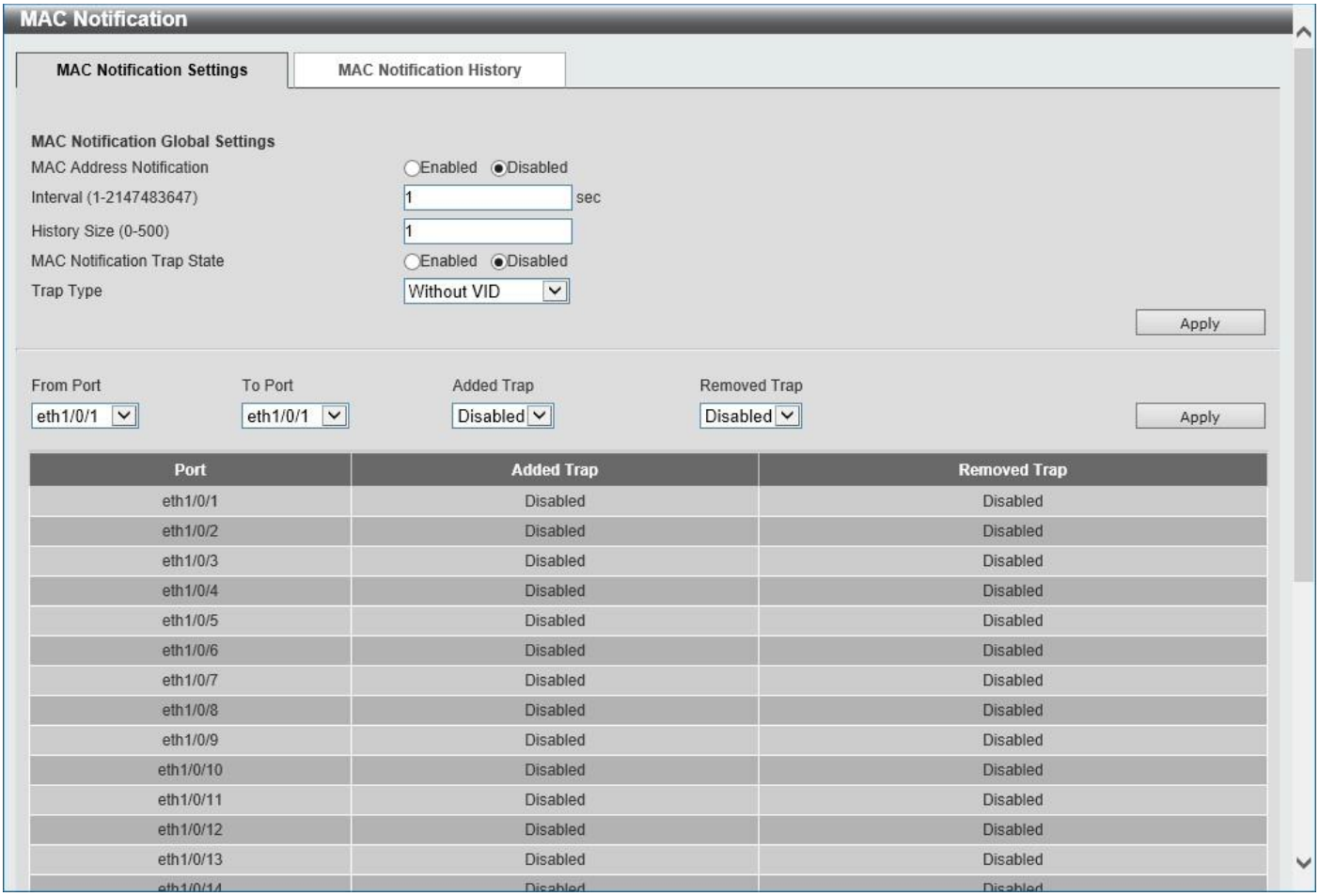

그림 5-5) MAC 알림(MAC 알림 설정) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
MAC Address Notification	MAC 알림 기능을 전체적으로 활성화하거나 비활성화하려면 선택합니다.

Interval	알림 사이의 시간 값을 입력합니다. 이 값은 1 초에서 2147483647 초 사이여야 합니다. 기본적으로 이 값은 1 초입니다.
History Size	알림에 사용되는 기록 로그에 나열된 최대 항목 수를 입력합니다. 이 값은 0 에서 500 사이여야 합니다. 기본적으로 이 값은 1 입니다.
MAC Notification Trap State	MAC 알림 트랩 상태를 활성화하거나 비활성화하려면 선택합니다.
Trap Type	트랩 유형을 지정합니다. 선택할 수 있는 옵션은 VID 없음 및 VID 포함입니다.
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
Added Trap	선택한 포트에 대해 추가된 트랩을 활성화하거나 비활성화하려면 선택합니다.
Removed Trap	선택한 포트에 대해 제거된 트랩을 활성화하거나 비활성화하려면 선택합니다.

적용(Apply) 버튼을 클릭하여 각 개별 섹션에 대한 변경 사항을 적용합니다.

MAC Notification History 탭을 선택하면 페이지 상단에서 다음 페이지를 사용할 수 있습니다.

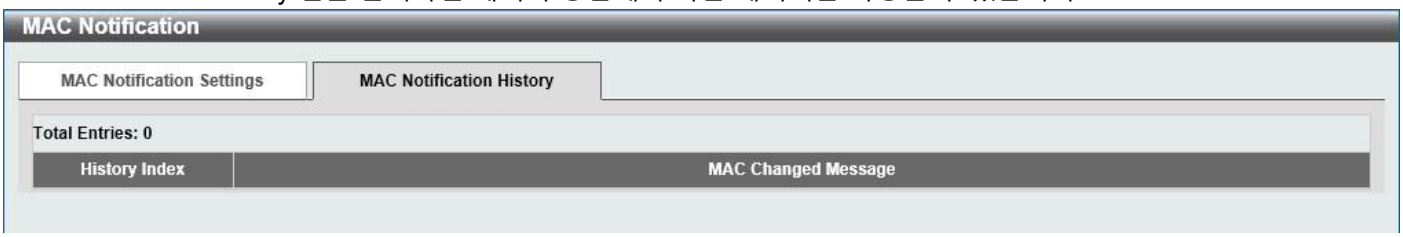

그림 5-6) MAC 알림(MAC 알림 기록) 창

이 페이지에 MAC 알림 메시지 목록이 표시됩니다.

VLAN

VLAN Configuration Wizard

이 창은 VLAN Configuration Wizard 를 시작하는 데 사용됩니다.

Create/Configure VLAN

다음 창을 보려면 아래와 같이 L2 Features > VLAN > VLAN Configuration Wizard 를 클릭합니다.

그림 5-7 VLAN Configuration Wizard (단계 1) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Create VLAN	새 VLAN 을 생성하려면 이 옵션을 선택합니다. VID - 여기에 VLAN ID 를 입력합니다. 범위는 1 에서 4094 사이입니다.
Configure VLAN	기존 VLAN 을 구성하려면 이 옵션을 선택합니다. VID - 여기에 VLAN ID 를 입력합니다. 범위는 1 에서 4094 사이입니다.

Next 버튼을 클릭하여 다음 단계를 계속합니다.

VLAN 생성

Create VLAN 옵션을 선택하고 Next 버튼을 클릭하면 다음 창이 나타납니다.

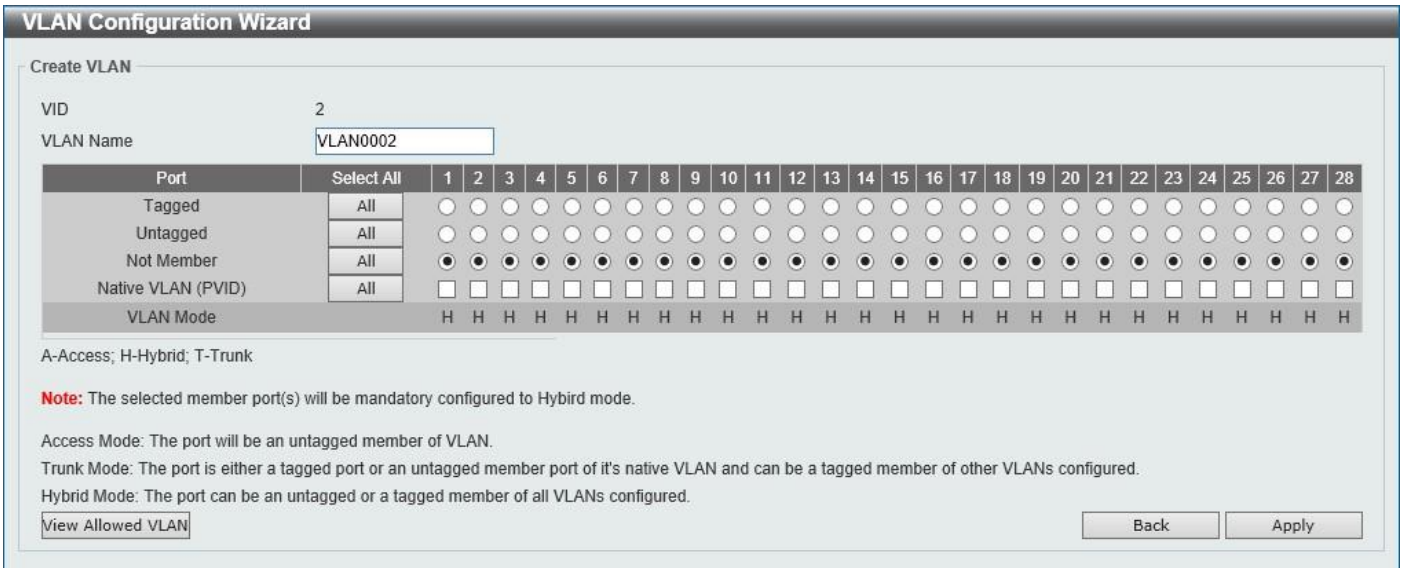

그림 5-8 VLAN Configuration Wizard (VLAN 생성) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
VLAN Name	여기에 VLAN 의 이름을 입력합니다.
Tagged	여기에서 이 VLAN 의 태그가 지정된 멤버인 스위치 포트를 선택합니다.
Untagged	여기에서 이 VLAN 의 태그가 지정되지 않은 멤버인 스위치 포트를 선택합니다.
Not Member	여기에서 이 VLAN 의 멤버가 아닌 스위치 포트를 선택합니다.
Native VLAN (PVID)	여기에서 네이티브 VLAN 을 지원하는 스위치 포트를 선택합니다.

View Allowed VLAN 버튼을 클릭하여 허용된 VLAN 설정을 확인합니다.

Back 버튼을 클릭하여 이전 단계로 돌아갑니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

View Allowed VLAN 버튼을 클릭하면 다음 창이 나타납니다.

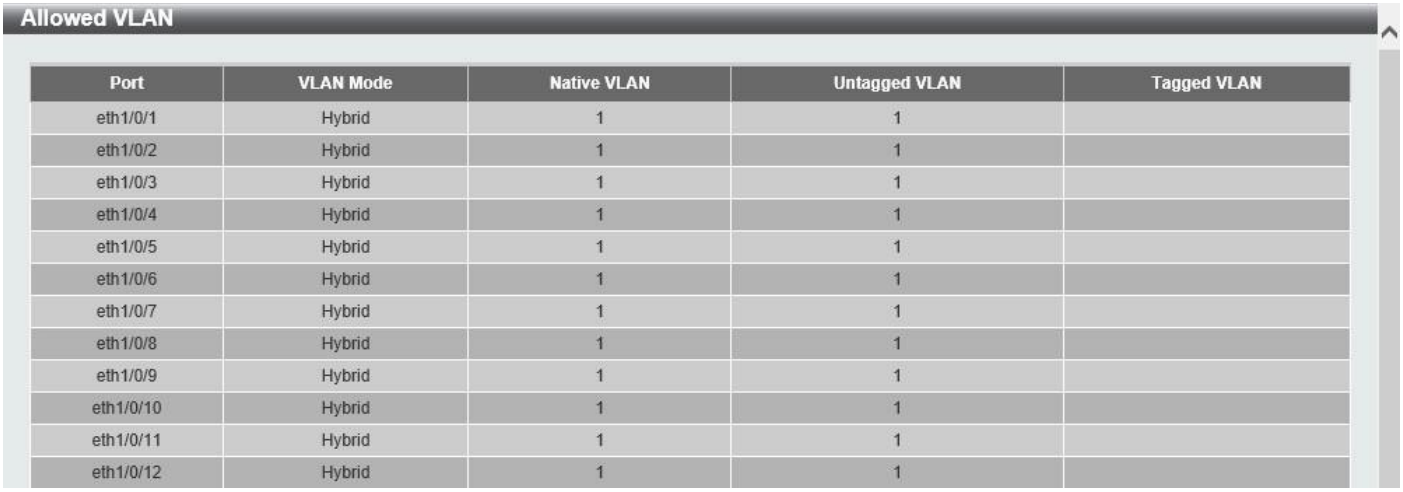

그림 5-9) 허용된 VLAN 창

Configure VLAN

Configure VLAN 옵션을 선택하고 Next 버튼을 클릭하면 다음 창이 나타납니다.

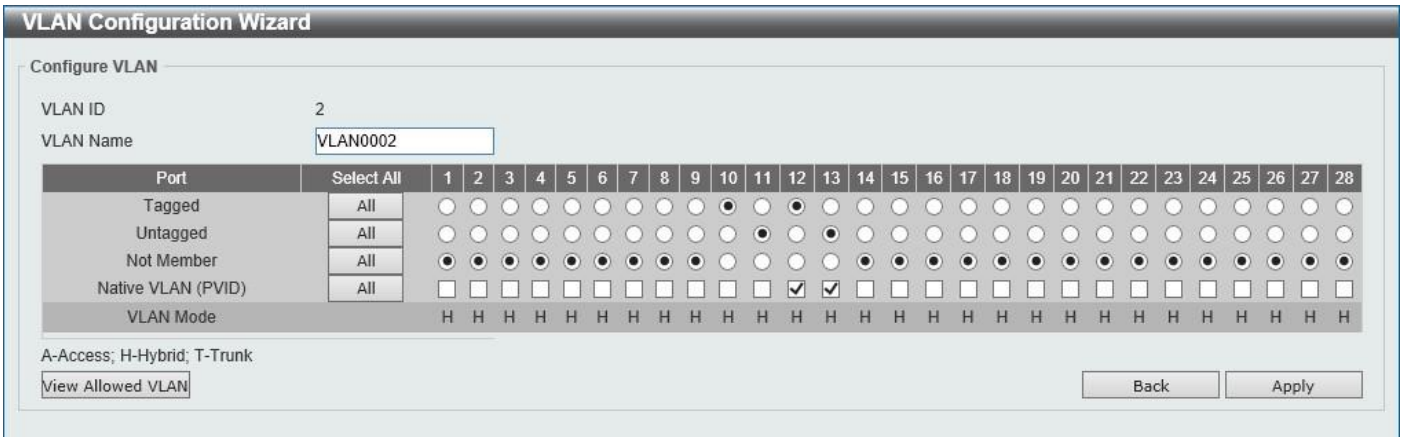

그림 5-10) VLAN Configuration Wizard (VLAN 구성) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
VLAN Name	여기에 VLAN 의 이름을 입력합니다.
Tagged	여기에서 이 VLAN 의 태그가 지정된 멤버인 스위치 포트를 선택합니다.
Untagged	여기에서 이 VLAN 의 태그가 지정되지 않은 멤버인 스위치 포트를 선택합니다.
Not Member	여기에서 이 VLAN 의 멤버가 아닌 스위치 포트를 선택합니다.
Native VLAN (PVID)	여기에서 네이티브 VLAN 을 지원하는 스위치 포트를 선택합니다.

View Allowed VLAN 버튼을 클릭하여 허용된 VLAN 설정을 확인합니다.

Back 버튼을 클릭하여 이전 단계로 돌아갑니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

View Allowed VLAN 버튼을 클릭하면 다음 창이 나타납니다.

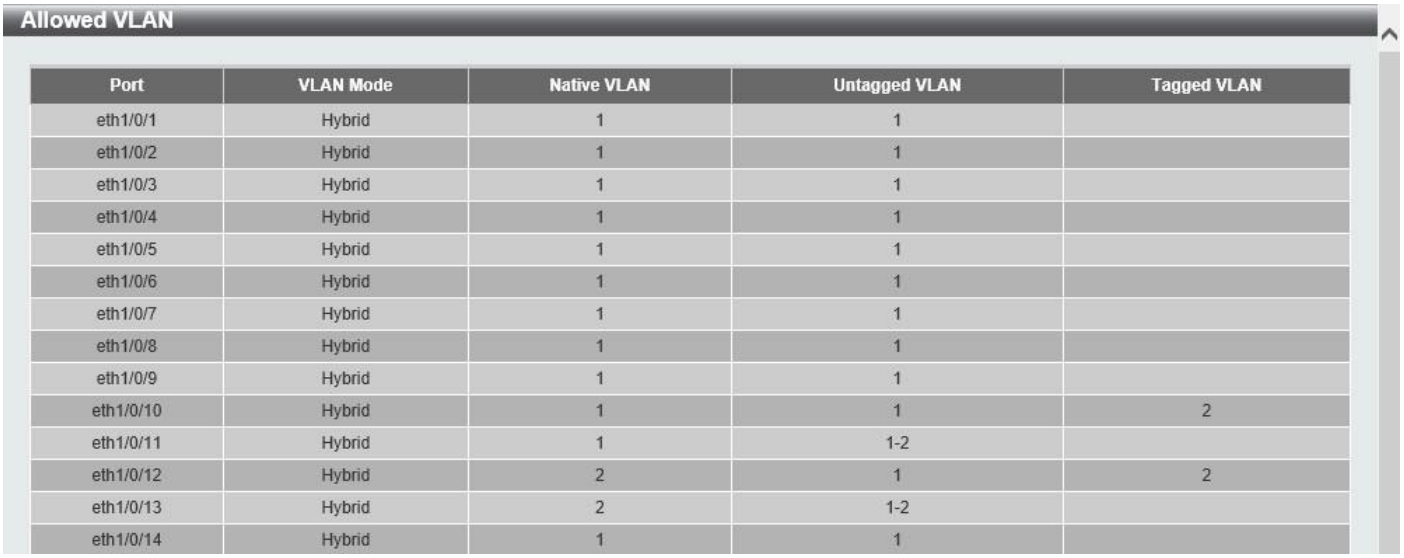

그림 5-11) 허용된 VLAN 창

802.1Q VLAN

이 창은 이 스위치의 VLAN 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > VLAN > 802.1Q VLAN 을 클릭합니다.

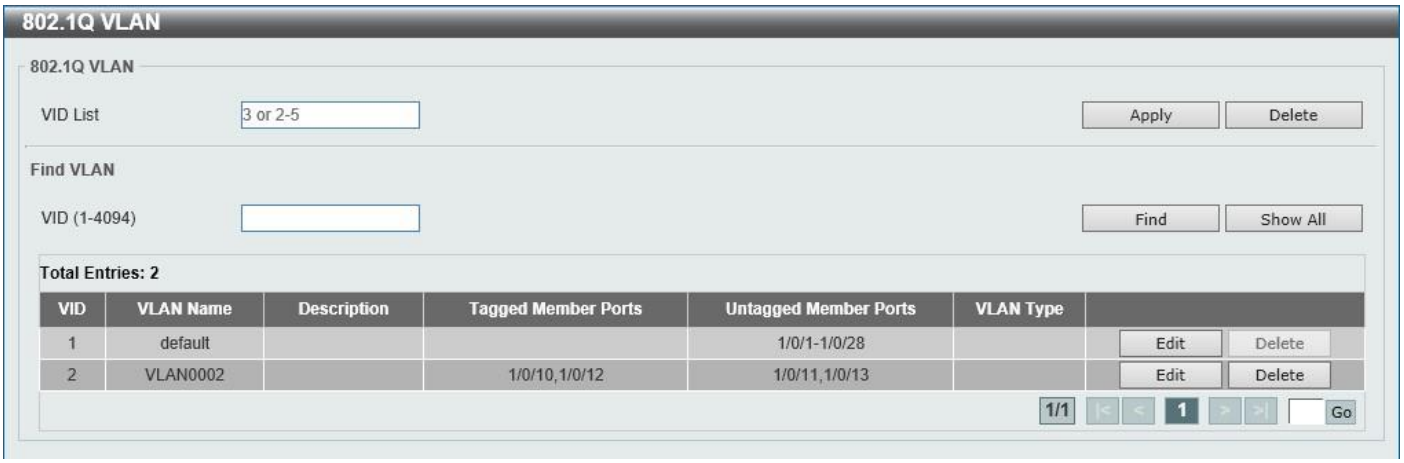

그림 5-12 802.1Q VLAN 창

802.1Q VLAN 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
VID List	여기에 생성될 VLAN ID 목록을 입력합니다.

Apply 버튼을 클릭하여 새 802.1Q VLAN 을 생성합니다.

Delete 버튼을 클릭하여 지정된 802.1Q VLAN 을 제거합니다.

VLAN 찾기에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
VID	여기에 표시될 VLAN ID 를 입력합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Show All 버튼을 클릭하여 모든 항목을 찾습니다.

Edit 버튼을 클릭하여 VLAN 이름을 수정합니다.

Delete 버튼을 클릭하여 특정 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

VLAN Interface

VLAN Interface Settings

이 창은 VLAN Interface 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > VLAN > VLAN Interface 를 클릭합니다.

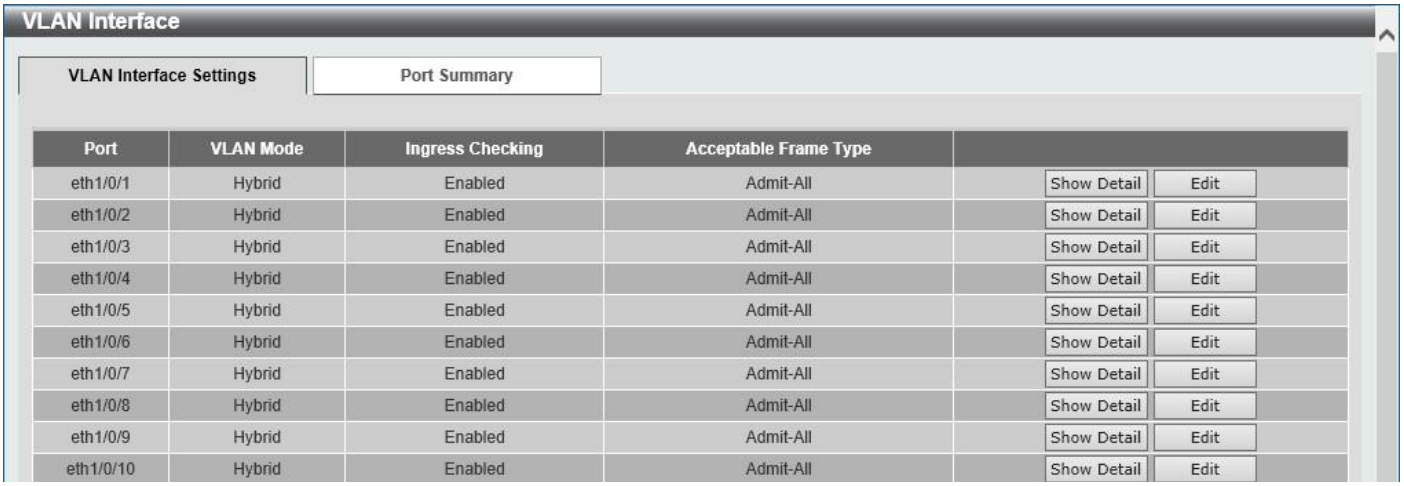

그림 5-13) VLAN Interface 창

Show Detail 버튼을 클릭하여 특정 Interface 의 VLAN 에 대한 자세한 정보를 확인합니다.

Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.

Show Detail 버튼을 클릭하면 다음 페이지가 나타납니다.

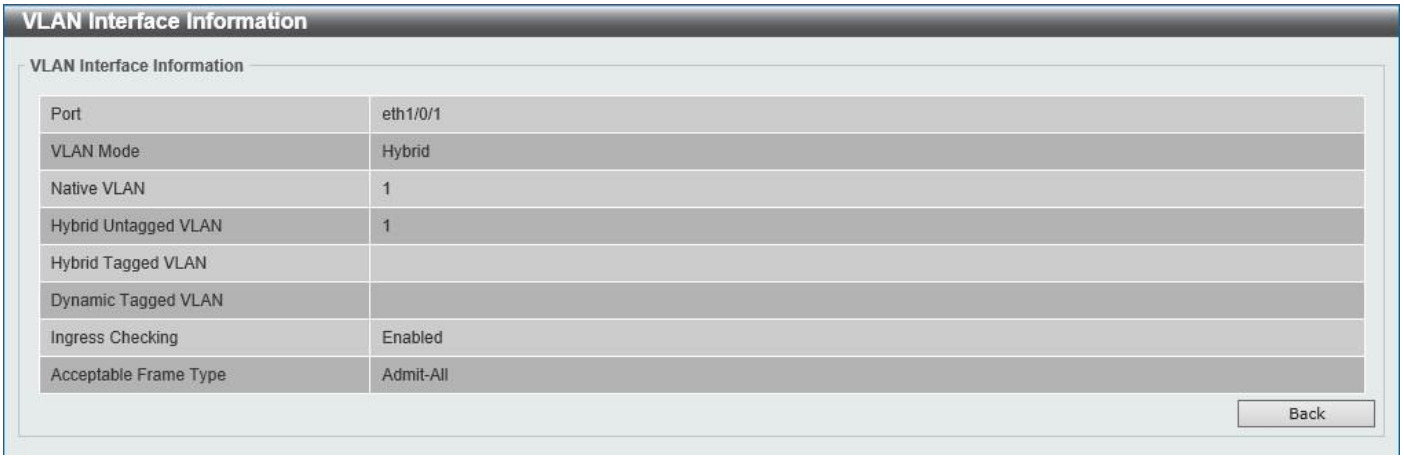

그림 5-14) VLAN Interface(VLAN 세부 정보) 창

이 페이지에는 특정 Interface 의 VLAN 에 대한 자세한 정보가 표시됩니다.
Back 버튼을 클릭하여 이전 페이지로 돌아갑니다.

Edit 버튼을 클릭하면 다음 페이지가 나타납니다.
이 페이지는 다른 VLAN 모드를 선택할 때 변경되는 동적 페이지입니다.
VLAN 모드로 Access 를 선택한 경우 다음 페이지가 나타납니다.

그림 5-15) VLAN Interface(액세스) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
VLAN Mode	여기에서 VLAN 모드 옵션을 선택합니다. 선택할 수 있는 옵션은 Access, Hybrid 및 Trunk 입니다.
Acceptable Frame	여기에서 허용 가능한 프레임 동작 옵션을 선택합니다. 선택할 수 있는 옵션은 Tagged Only(태그가 지정된 항목만), Untagged Only(태그되지 않은 항목) 및 Admit All(모두 허용)입니다.
Ingress Checking	ingress checking 기능을 활성화하거나 비활성화하려면 선택합니다.
VID	여기에 이 컨피그레이션에 사용되는 VLAN ID 를 입력합니다. 이 값은 1 에서 4094 사이여야 합니다.
Clone	이 옵션을 선택하면 복제 기능이 활성화됩니다.
From Port - To Port	여기에서 클론 기능에 사용할 포트 범위를 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.
Back 버튼을 클릭하여 변경 사항을 취소하고 이전 페이지로 돌아갑니다.

VLAN 모드를 Hybrid 로 선택한 경우 다음 페이지가 나타납니다.

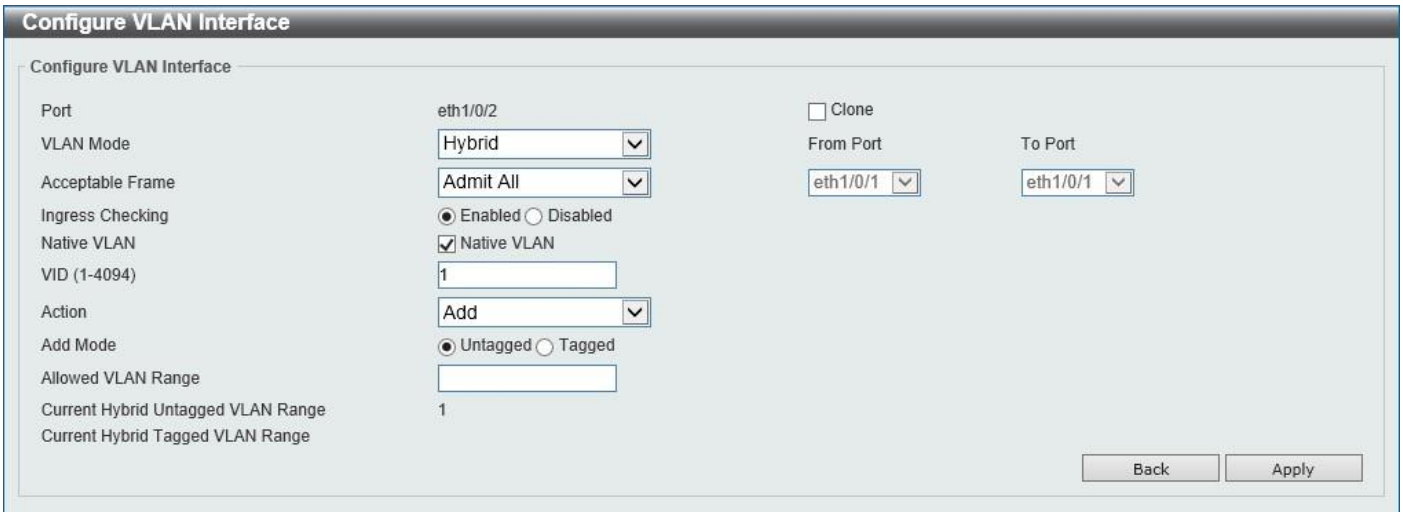

그림 5-16) VLAN Interface(하이브리드) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
VLAN Mode	여기에서 VLAN 모드 옵션을 선택합니다. 선택할 수 있는 옵션은 Access, Hybrid 및 Trunk 입니다.
Acceptable Frame	여기에서 허용 가능한 프레임 동작 옵션을 선택합니다. 선택할 수 있는 옵션은 Tagged Only(태그가 지정된 항목만), Untagged Only(태그되지 않은 항목) 및 Admit All(모두 허용)입니다.
Ingress Checking	ingress checking 기능을 활성화하거나 비활성화하려면 선택합니다.
Native VLAN	이 옵션을 선택하면 기본 VLAN 기능이 활성화됩니다.
VID	네이티브 VLAN 옵션을 선택하면 다음 매개변수를 사용할 수 있습니다. 여기에 이 컨피그레이션에 사용되는 VLAN ID 를 입력합니다. 이 값은 1 에서 4094 사이여야 합니다.
Action	여기에서 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 Add(추가), Remove(제거), Tagged(태그 지정) 및 Untagged(태그 없음)입니다.
Add Mode	Untagged(태그 없음) 또는 Tagged(태그가 지정됨) 매개변수를 추가할지 여부를 선택합니다.
Allowed VLAN Range	여기에 허용되는 VLAN 범위를 입력합니다.
Clone	이 옵션을 선택하면 복제 기능이 활성화됩니다.
From Port - To Port	여기에서 클론 기능에 사용할 포트 범위를 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Back 버튼을 클릭하여 변경 사항을 취소하고 이전 페이지로 돌아갑니다.

VLAN 모드 Trunk 로 선택한 경우 다음 페이지가 나타납니다.

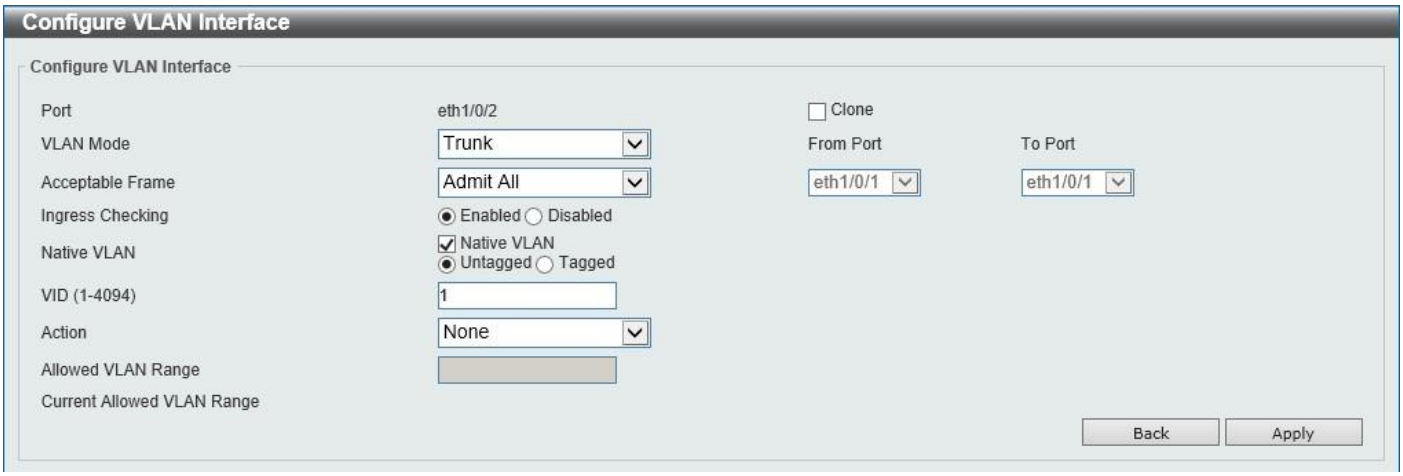

그림 5-17) VLAN Interface(트렁크) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
VLAN Mode	여기에서 VLAN 모드 옵션을 선택합니다. 선택할 수 있는 옵션은 Access, Hybrid 및 Trunk 입니다.
Acceptable Frame	여기에서 허용 가능한 프레임 동작 옵션을 선택합니다. 선택할 수 있는 옵션은 Tagged Only(태그가 지정된 항목만), Untagged Only(태그되지 않은 항목) 및 Admit All(모두 허용)입니다.
Ingress Checking	트렁크를 VLAN 모드로 선택하면 다음 Parameter 를 사용할 수 있습니다. Ingress Checking 기능을 활성화하거나 비활성화하려면 선택합니다.
Native VLAN	이 옵션을 선택하면 기본 VLAN 기능이 활성화됩니다. 또한 이 VLAN 이 태그가 지정되지 않음 또는 태그가 지정된 프레임을 지원하는지 선택합니다.
VID	네이티브 VLAN 옵션을 선택하면 다음 매개변수를 사용할 수 있습니다. 여기에 이 컨피그레이션에 사용되는 VLAN ID 를 입력합니다. 이 값은 1 에서 4094 사이여야 합니다.
Action	여기에서 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 All(모두), Add(추가), Remove(제거), Except(제외) 및 Replace(바꾸기)입니다.
Allowed VLAN Range	여기에 허용되는 VLAN 범위를 입력합니다.
Clone	이 옵션을 선택하면 복제 기능이 활성화됩니다.
From Port - To Port	여기에서 클론 기능에 사용할 포트 범위를 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Back 버튼을 클릭하여 변경 사항을 취소하고 이전 페이지로 돌아갑니다.

Port Summary

Port Summary 탭을 선택하면 다음 페이지를 사용할 수 있습니다.

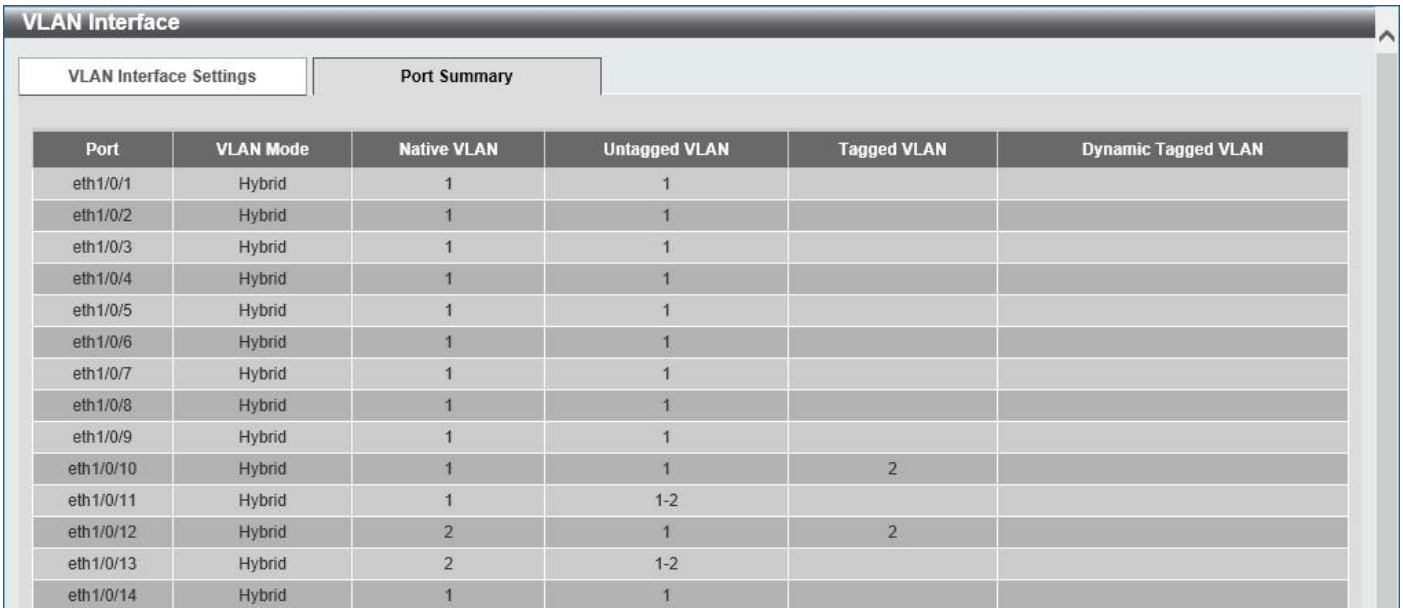

그림 5-18) VLAN Interface 포트 요약 창

Asymmetric VLAN

이 창은 비대칭 VLAN 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > VLAN > Asymmetric VLAN 을 클릭합니다.

그림 5-19) 비대칭 VLAN 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Asymmetric VLAN State	여기에서 비대칭 VLAN 기능을 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

L2VLAN Interface Description

이 창은 레이어 2 VLAN Interface 설명을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > VLAN > L2VLAN Interface Description 을 클릭합니다.

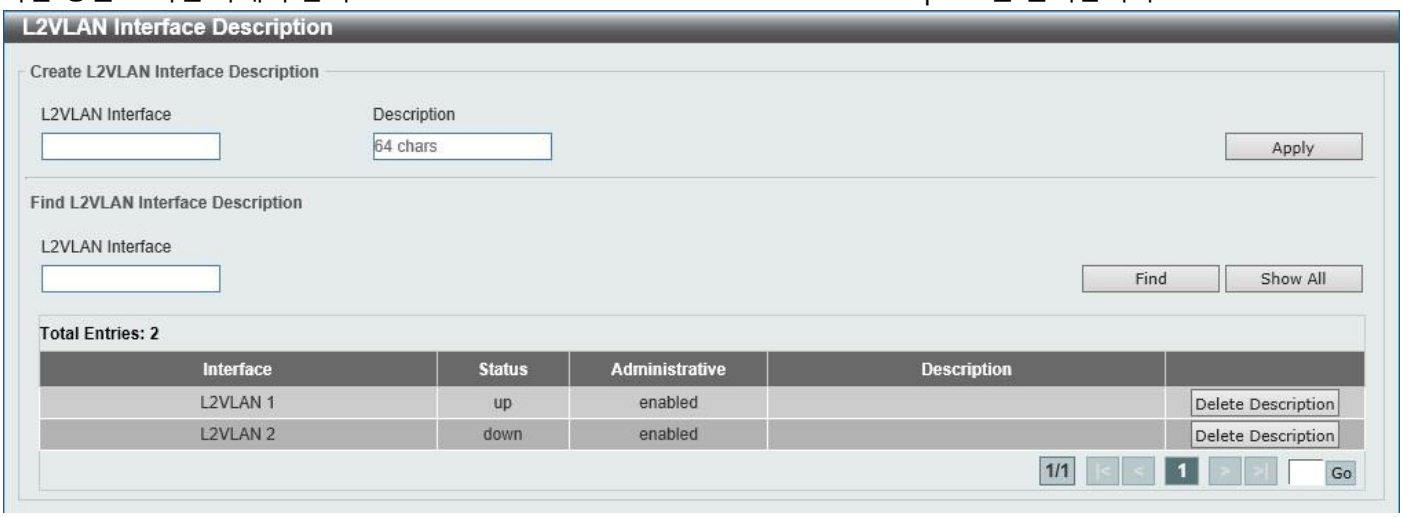

그림 5-20 L2VLAN Interface 설명 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
L2VLAN Interface	여기에 레이어 2 VLAN Interface 의 ID 를 입력합니다.
Description	여기에 레이어 2 VLAN Interface 에 대한 설명을 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 디스플레이를 생성합니다.

Show All 버튼을 클릭하여 사용 가능한 모든 항목을 표시합니다.

Delete Description 버튼을 클릭하여 지정된 레이어 2 VLAN 에서 설명을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Auto Surveillance VLAN

Auto Surveillance Properties

이 창은 자동 감시 VLAN Global Settings 을 구성하고 포트 감시 VLAN 정보를 표시하는 데 사용됩니다.

스위치는 HTTP, HTTPS 또는 RTSP 를 통해 IPC 에 연결되면 호스트를 NVR 로 간주합니다. 스위치는 이 포트에서 NVR 을 학습하고 트리거된 에이징 메커니즘이 만료되거나 LAN 케이블이 제거될 때까지 감시 VLAN 으로 이동합니다. 호스트가 IPC 에 ARP 요청을 보내면 스위치는 여전히 호스트를 NVR 로 간주하지만 임시로 감시 VLAN 으로 이동합니다. 호스트는 더 이상 NVR 로 인식되지 않는 경우 약 30 초 후에 감시 VLAN 에서 자동으로 이동됩니다.

참고: 동일한 PC 또는 스위치의 동일한 LAN 포트에 연결된 PC 는 스위치와 스위치에 연결된 IP 카메라를 동시에 관리할 수 없습니다.

다음 창을 보려면 아래와 같이 L2 Features > VLAN > Auto Surveillance VLAN > Auto Surveillance Properties 를 클릭합니다.

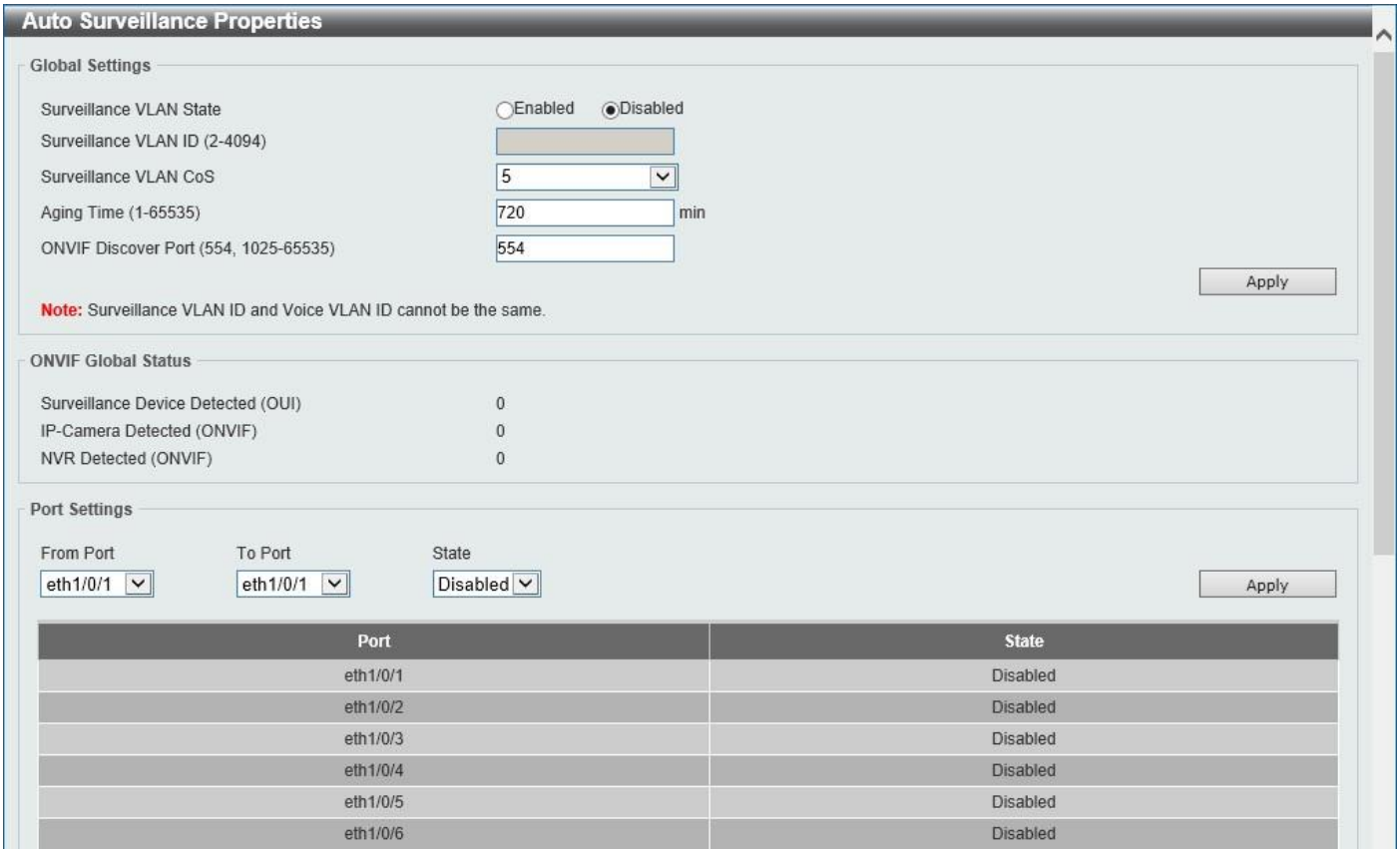

그림 5-21) 자동 감시 속성 창

Global Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Surveillance VLAN State	여기에서 감시 VLAN 기능을 활성화하거나 비활성화하려면 선택합니다.
Surveillance VLAN ID	여기에 감시 VLAN 의 VLAN ID 를 입력합니다. 범위는 2 에서 4094 사이입니다. VLAN 을 감시 VLAN 으로 할당하기 전에 일반 VLAN 을 생성해야 합니다.
Surveillance VLAN CoS	여기에 감시 VLAN 에 대한 CoS(Class of Service) 값을 입력합니다. 감시 VLAN 지원 포트에 도착하는 감시 패킷은 여기에 지정된 CoS 로 표시됩니다. CoS 를 리마킹하면 감시 VLAN 트래픽을 서비스 품질에서 데이터 트래픽과 구별할 수 있습니다. 범위는 0 에서 7 사이입니다.
Aging Time	여기에 에이징 시간 값을 입력합니다. 이는 감시 VLAN 동적 멤버 포트를 노후화하기 위한 에이징 시간을 구성하는 데 사용됩니다. 범위는 1 분에서 65535 분 사이입니다. 포트에 연결된 마지막 감시 장치가 트래픽 전송을 중지하고 이 감시 장치의 MAC 주소가 만료되면 감시 VLAN 에이징 타이머가 시작됩니다. 포트는 감시 VLAN 에이징 타이머가 만료된 후 감시 VLAN 에서 제거됩니다. 에이징 시간 동안 감시 트래픽이 재개되면 에이징 타이머가 취소됩니다.
ONVIF Discover Port	여기에 TCP/UDP 포트 번호를 입력합니다. 범위는 554 또는 1025 에서 65535 사이입니다. RTSP 스트림 Snooping 을 위한 TCP/UDP 포트 번호를 구성하는 데 사용됩니다. ONVIF 지원 IPC 및 ONVIF 지원 NVR 은 WS-Discovery 를 사용하여 다른 디바이스를 찾습니다. IPC 가 검색되면 스위치는 NVR 과 IPC 간의 RTSP, HTTP 및 HTTPS 패킷을 Snooping 하여 NVR 을 추가로 검색할 수 있습니다. TCP/UDP 포트가 RTSP 포트 번호와 같지 않으면 이러한 패킷을 Snooping 할 수 없습니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Port Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
State	여기에서 지정된 포트에서 감시 VLAN 기능을 활성화하거나 비활성화하려면 선택합니다. 포트에 대해 감시 VLAN 이 활성화되면 포트는 자동으로 태그가 지정되지 않은 감시 VLAN 멤버로 학습되고 수신된 태그가 없는 감시 패킷은 감시 VLAN 으로 전달됩니다. 수신된 패킷은 패킷의 소스 MAC 주소가 OUI(Organizationally Unique Identifier) 주소를 준수하는 경우 감시 패킷으로 결정됩니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

MAC Settings and Surveillance Device

이 창은 감시 장치 및 해당 MAC 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > VLAN > Auto Surveillance VLAN > MAC Settings and Surveillance Device 를 클릭합니다.

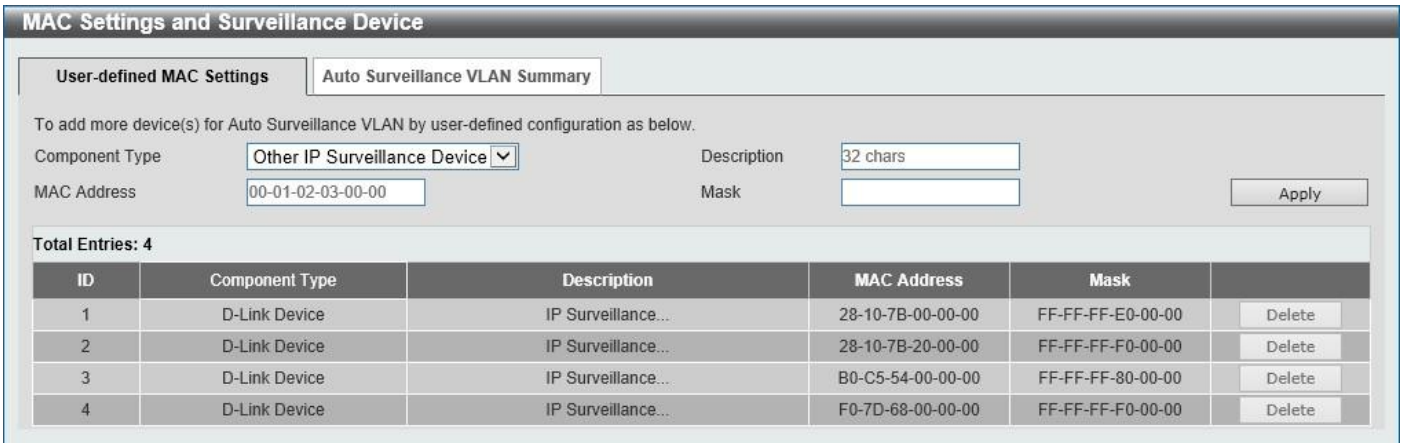

그림 5-22) MAC 설정 및 감시 장치 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Component Type	여기에서 구성 요소 유형을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • 비디오 관리 서버 - 감시 디바이스 유형을 비디오 관리 서버(VMS)로 지정합니다. • VMS Client/Remote Viewer - 감시 장치 유형을 VMS 클라이언트로 지정합니다. • 비디오 인코더 - 감시 장치 유형을 비디오 인코더로 지정합니다. 네트워크 스토리지 - 감시 장치 유형을 네트워크 스토리지로 지정합니다. • 기타 IP 감시 장치 - 감시 장치 유형을 기타 IP 감시 장치로 지정합니다.
Description	여기에 사용자 정의 OUI 에 대한 설명을 입력합니다. 이 문자열은 최대 32 자까지 가능합니다.
MAC Address	여기에 OUI MAC 주소를 입력합니다. 수신된 패킷의 소스 MAC 주소가 OUI 패턴 중 하나와 일치하면 수신된 패킷은 감시 패킷으로 결정됩니다.
Mask	여기에 OUI MAC 주소와 일치하는 비트 마스크를 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 삭제합니다.

Auto Surveillance VLAN Summary 탭 옵션을 선택하면 페이지 상단에서 다음 페이지를 사용할 수 있습니다.

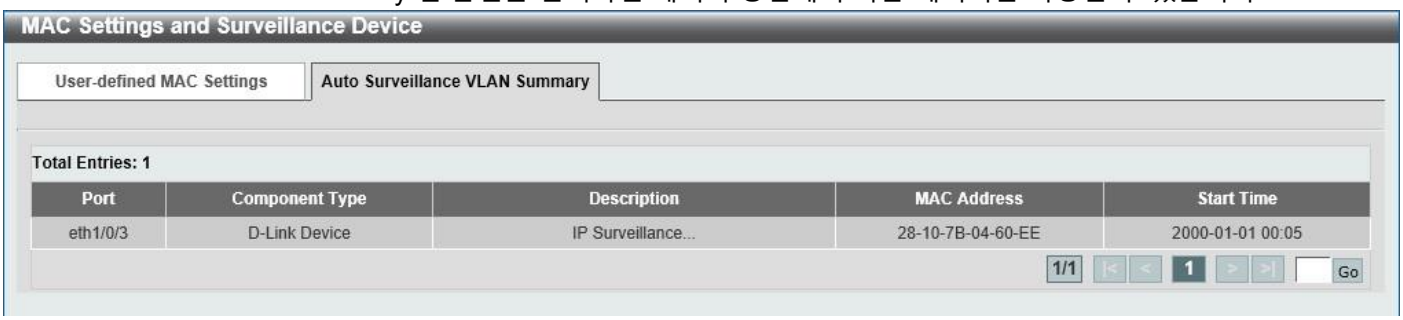

그림 5-23) MAC 설정 및 감시 장치(자동 감시 VLAN 요약) 창

ONVIF IP-Camera Information

이 창은 ONVIF IP 카메라 정보를 표시하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > VLAN > Auto Surveillance VLAN > ONVIF IP-Camera Information 을 클릭합니다.

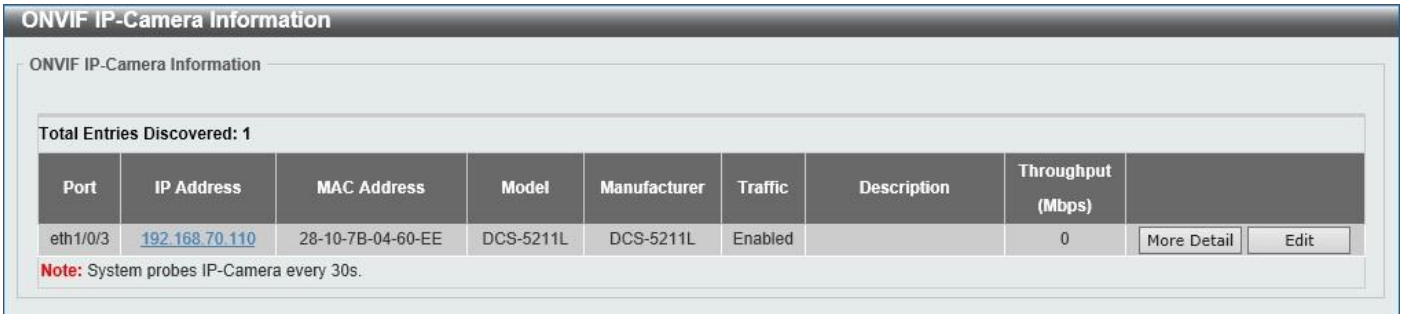

그림 5-24 ONVIF IP 카메라 정보 창

IP Address 하이퍼링크를 클릭하여 IP 카메라의 웹 Interface 에 연결합니다.
자세한 ONVIF IP 카메라 정보를 보려면 More Detail 버튼을 클릭하십시오.
Edit 버튼을 클릭하여 IP 카메라의 상태와 설명을 구성합니다.

More Detail 버튼을 클릭하면 다음과 같은 창이 나타납니다.

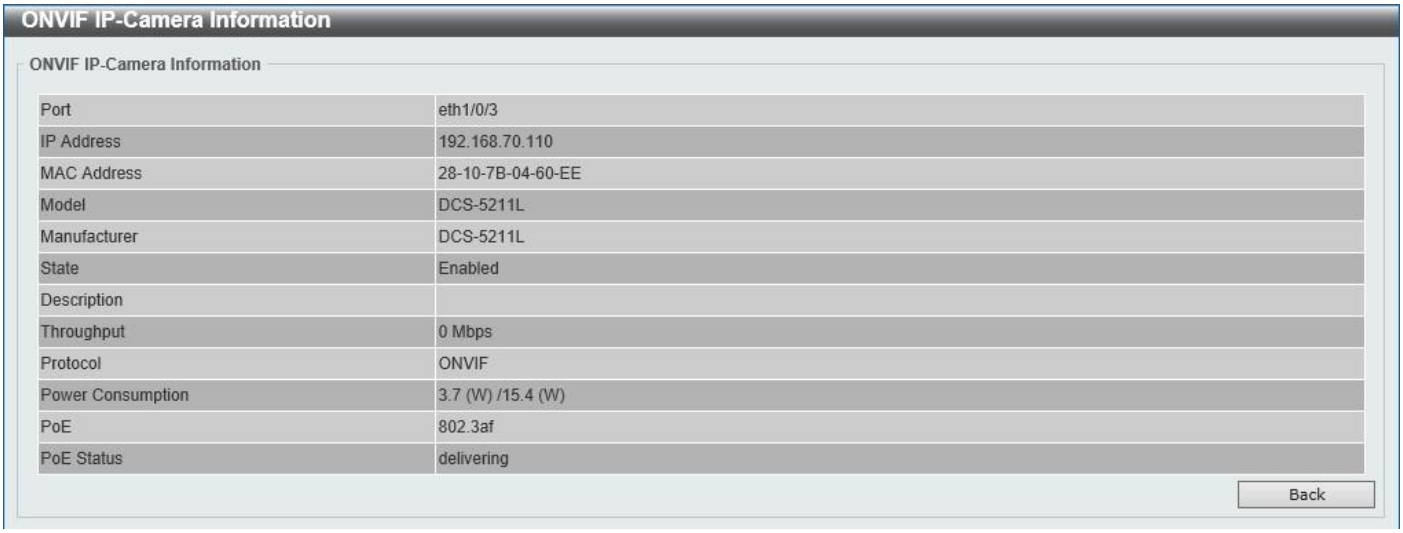

그림 5-25 ONVIF IP 카메라 정보(자세한 내용) 창

Edit 버튼을 클릭하면 다음과 같은 창이 나타납니다.

그림 5-26 ONVIF IP 카메라 정보(편집) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
IP-Camera State	여기에서 IP 카메라 상태를 활성화하거나 비활성화하려면 선택합니다.
Description	여기에 이 IP 카메라에 대한 설명을 입력합니다.

Back 버튼을 클릭하여 변경 사항을 취소하고 이전 창으로 돌아갑니다. Apply 버튼을 클릭하여 변경 사항을 적용합니다.

ONVIF NVR Information

이 창은 ONVIF NVR(Network Video Recorder) 정보를 표시하는 데 사용됩니다.

다음 창을 보려면 아래와 L2 Features > VLAN > Auto Surveillance VLAN > ONVIF NVR Information 을 클릭합니다.

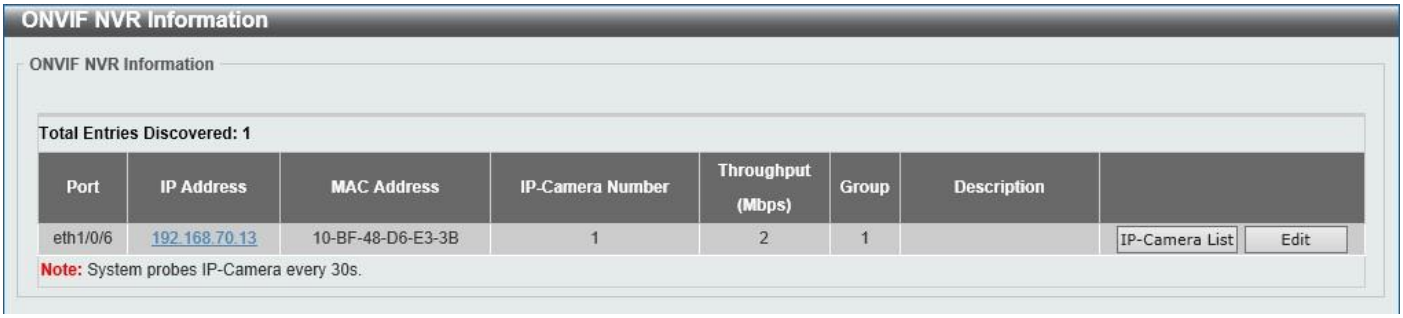

그림 5-27 ONVIF NVR 정보 창

IP Address 하이퍼링크를 클릭하여 웹 NVR 의 Interface.

IP-Camera List 버튼을 클릭하여 NVR 에 연결된 IP 카메라 목록을 확인합니다.

Edit 버튼을 클릭하여 NVR 에 대한 설명을 구성합니다.

IP-Camera List 버튼을 클릭하면 다음과 같은 창이 나타납니다.

그림 5-28 ONVIF NVR 정보(IP-카메라 목록) 창

IP Address 하이퍼링크를 클릭하여 IP 카메라의 웹 Interface 에 연결합니다.

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

Edit 버튼을 클릭하면 다음과 같은 창이 나타납니다.

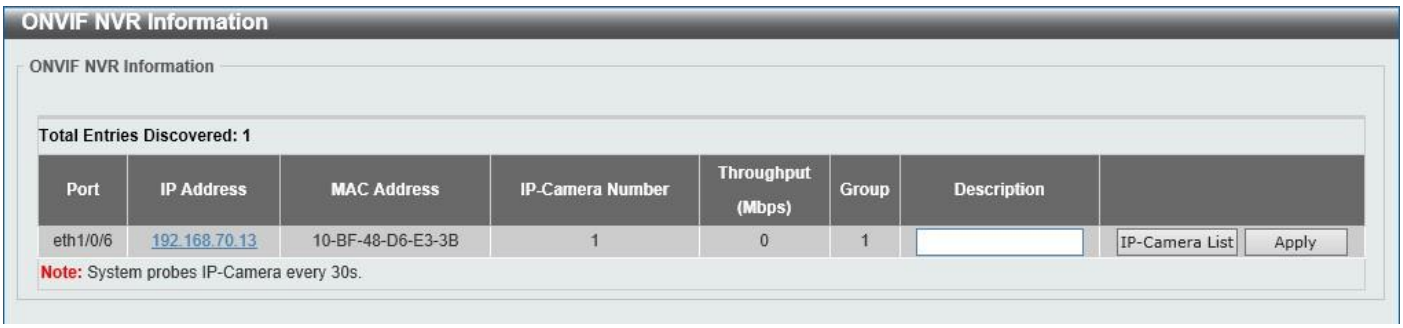

그림 5-29 ONVIF NVR 정보(편집) 창

구성할 수 있는 추가 필드는 아래에 설명되어 있습니다.

Parameter	Description
Description	여기에 이 NVR 에 대한 설명을 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Voice VLAN

Voice VLAN Global

이 창은 전역 음성 VLAN 설정을 표시하고 구성하는 데 사용됩니다. 이는 전역 음성 VLAN 기능을 활성화하고 스위치에서 음성 VLAN 을 지정하는 데 사용됩니다. 스위치에는 음성 VLAN 이 하나만 있습니다.

다음 창을 보려면 아래와 같이 L2 Features > VLAN > Voice VLAN > Voice VLAN Global 을 클릭합니다.

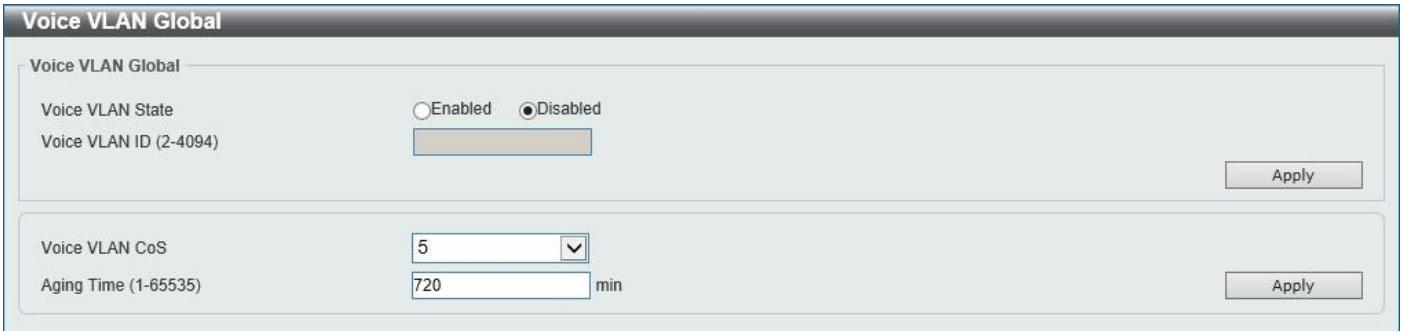

그림 5-30 Voice VLAN Global Window

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Voice VLAN State	여기에서 음성 VLAN 기능을 전역적으로 활성화하거나 비활성화하려면 선택합니다.
Voice VLAN ID	여기에 음성 VLAN 의 VLAN ID 를 입력합니다. 음성 VLAN 으로 지정할 VLAN 은 컨피그레이션 전에 미리 존재해야 합니다. 범위는 2 에서 4094 사이입니다.
Voice VLAN CoS	여기에서 음성 VLAN 의 CoS 를 선택합니다. 범위는 0 에서 7 사이입니다. 음성 VLAN 지원 포트에 도착하는 음성 패킷은 여기에 지정된 CoS 로 표시됩니다. CoS 패킷의 리마킹을 통해 음성 VLAN 트래픽을 QoS(Quality of Service)의 데이터 트래픽과 구별할 수 있습니다.
Aging Time	여기에 에이징 시간 값을 입력합니다. 이는 자동으로 학습된 음성 디바이스 및 음성 VLAN 정보를 에이징하기 위한 에이징 시간을 구성하는 데 사용됩니다. 포트에 연결된 마지막 음성 디바이스가 트래픽 전송을 중지하고 이 음성 디바이스의 MAC 주소가 FDB 에서 에이징되면 음성 VLAN 에이징 타이머가 시작됩니다. 음성 VLAN 에이징 타이머가 만료된 후 포트가 음성 VLAN 에서 제거됩니다. 에이징 시간 동안 음성 트래픽이 재개되면 에이징 타이머가 취소됩니다. 범위는 1 분에서 65535 분 사이입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Voice VLAN Port

이 창은 음성 VLAN Interface 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > VLAN > Voice VLAN > Voice VLAN Port 를 클릭합니다.

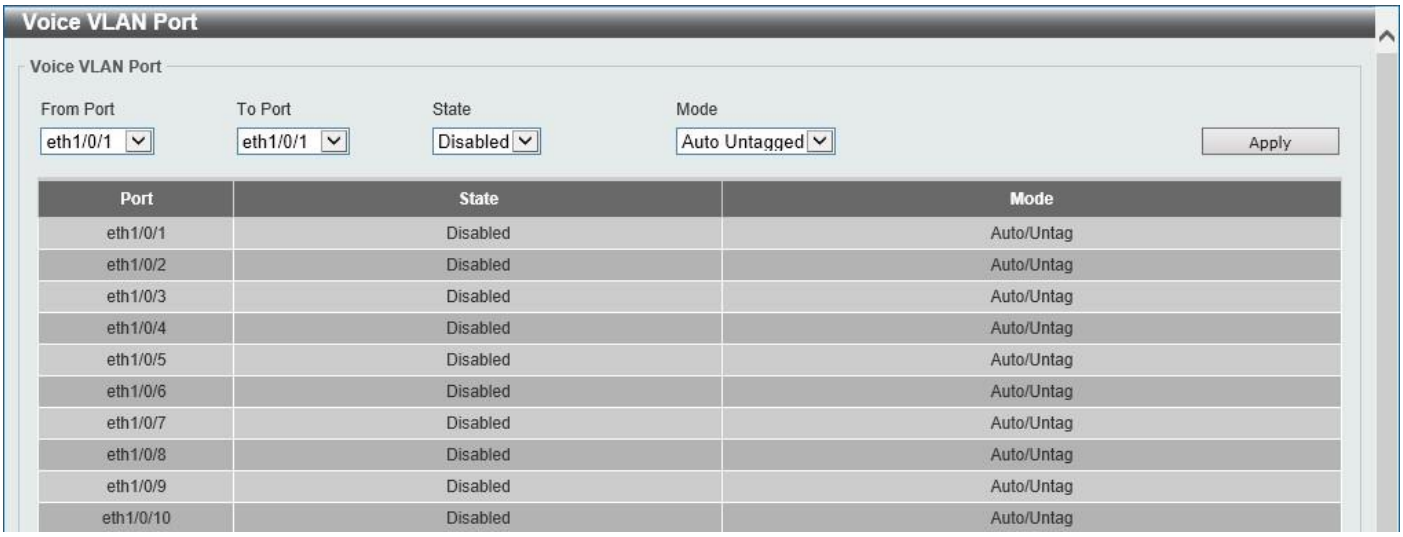

그림 5-31) Voice VLAN Port 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
State	여기에서 지정된 포트에서 음성 VLAN 기능을 활성화하거나 비활성화하려면 선택합니다. 포트에 대해 음성 VLAN 이 활성화되면 수신된 음성 패킷이 음성 VLAN 으로 전달됩니다. 패킷의 소스 MAC 주소가 OUI 주소를 준수하는 경우 수신된 패킷은 음성 패킷으로 결정됩니다.
Mode	여기에서 모드를 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Auto Untagged(자동 태그 없음) - 음성 VLAN 태그 없는 멤버십이 자동으로 학습되도록 지정합니다. • Auto Tagged(자동 태그 지정) - 음성 VLAN 태그 지정 멤버십이 자동으로 학습되도록 지정합니다. • Manual(수동) - 음성 VLAN 멤버십을 수동으로 구성하도록 지정합니다. 자동 학습이 활성화된 경우 포트는 자동으로 음성 VLAN 멤버로 학습됩니다. 이 멤버십은 자동으로 만료됩니다. 포트가 자동 태그 지정 모드에서 작동 중이고 포트가 디바이스의 OUI 를 통해 음성 디바이스를 캡처하면 음성 VLAN 에 태그 멤버로 자동으로 조인됩니다. 음성 장치가 태그가 지정된 패킷을 전송하면 스위치의 우선 순위가 변경됩니다. 음성 디바이스가 태그가 지정되지 않은 패킷을 전송하면 PVID(Port VLAN ID)로 전달합니다. 포트가 자동 태그 없음 모드에서 작동 중이고 포트가 디바이스의 OUI 를 통해 음성 디바이스를 캡처하는 경우 자동으로 태그 없는 멤버로 음성 VLAN 에 조인됩니다. 음성 장치가 태그가 지정된 패킷을 전송하면 스위치의 우선 순위가 변경됩니다. 음성 디바이스가 태그가 지정되지 않은 패킷을 전송하면 음성 VLAN 으로 전달합니다. 스위치가 LLDP-MED 패킷을 수신하면 VLAN ID, 태그 플래그 및 우선순위 플래그를 확인합니다. 스위치는 태그가 지정된 플래그 및 우선 순위 설정을 따라야 합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Voice VLAN OUI

이 창은 음성 VLAN OUI 설정을 표시하고 구성하는 데 사용됩니다. 이 창을 사용하여 음성 VLAN 에 대한 사용자 정의 OUI 를 추가합니다. 음성 VLAN 의 OUI 는 음성 VLAN 기능을 사용하여 음성 트래픽을 식별하는 데 사용됩니다. 수신된 패킷의 소스 MAC 주소가 OUI 패턴 중 하나와 일치하면 수신된 패킷은 음성 패킷으로 결정됩니다.
사용자 정의 OUI 는 기본 OUI 와 같을 수 없습니다. 기본 OUI 는 삭제할 수 없습니다.

다음 창을 보려면 아래와 같이 L2 Features > VLAN > Voice VLAN > Voice VLAN OUI 를 클릭합니다.

그림 5-32 음성 VLAN OUI 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
OUI Address	여기에 음성 VLAN OUI MAC 주소를 입력합니다.
Mask	여기에 음성 VLAN OUI MAC 주소와 일치하는 비트 마스크를 입력합니다.
Description	여기에 사용자 정의 OUI MAC 주소에 대한 설명을 입력합니다. 이 문자열은 최대 32 자까지 가능합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.
Delete 버튼을 클릭하여 지정된 항목을 삭제합니다.

Voice VLAN Device

이 창은 음성 VLAN 디바이스 테이블을 보는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > VLAN > Voice VLAN > Voice VLAN Device 를 클릭합니다.

그림 5-33) Voice VLAN Device 창

Voice VLAN LLDP-MED Device

이 창은 Voice VLAN LLDP-MED 디바이스 테이블을 보는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > VLAN > Voice VLAN > Voice VLAN LLDP-MED Devices 를 클릭합니다.

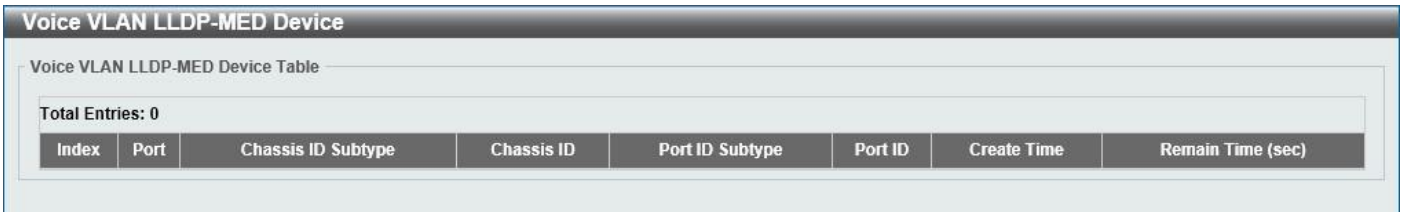

그림 5-34 Voice VLAN LLDP-MED 장치 창

STP

이 스위치는 IEEE 802.1D-1998 STP, IEEE 802.1D-2004 Rapid STP 및 IEEE 802.1Q-2005 MSTP 의 세 가지 버전의 STP(Spanning Tree Protocol)를 지원합니다. IEEE 802.1D-1998 STP 표준은 대부분의 네트워킹 전문가에게 친숙할 것입니다. 그러나 IEEE 802.1D-2004 RSTP 및 IEEE 802.1Q-2005 MSTP 가 최근 D-Link 관리 이더넷 스위치에 도입됨에 따라 아래에 기술에 대한 간략한 소개가 제공되고 IEEE 802.1D-1998 STP, IEEE 802.1D-2004 RSTP 및 IEEE 802.1Q-2005 MSTP 를 설정하는 방법에 대한 설명이 제공됩니다.

802.1Q-2005 MSTP

MSTP(Multiple Spanning Tree Protocol)는 IEEE 커뮤니티에서 정의한 표준으로, 여러 VLAN 을 단일 스패닝 트리 인스턴스에 매핑할 수 있도록 하여 네트워크 전반에 걸쳐 여러 경로를 제공합니다. 따라서 이러한 MSTP 구성은 트래픽 로드를 밸런싱하여 단일 스패닝 트리 인스턴스에 장애가 발생할 때 광범위한 중단을 방지합니다. 이렇게 하면 실패한 인스턴스에 대한 새 토폴로지를 더 빠르게 수렴할 수 있습니다.

이러한 VLAN 에 지정된 프레임은 세 가지 스패닝 트리 프로토콜(STP, RSTP 또는 MSTP) 중 하나를 사용하여 상호 연결된 브리지 전체에서 빠르고 완벽하게 처리됩니다.

MSTI(Multiple Spanning Tree Instance) ID 는 이러한 인스턴스를 분류합니다. MSTP 는 여러 스패닝 트리를 CIST(Common and Internal Spanning Tree)와 연결합니다. CIST 는 각 MSTP 영역과 가능한 최대 범위를 자동으로 결정하고 단일 스패닝 트리 인스턴스를 실행하는 하나의 가상 브리지로 표시됩니다. 서로 다른 VLAN 에 할당된 프레임은 네트워크에서 관리적으로 설정된 지역 내에서 서로 다른 데이터 경로를 따르므로 VLAN 및 해당 스패닝 트리를 정의할 때 발생하는 관리 오류에 관계없이 프레임을 간단하고 완벽하게 처리할 수 있습니다.

네트워크에서 MSTP 를 사용하는 각 스위치는 다음과 같은 세 가지 특성을 가진 단일 MSTP 컨피그레이션을 공유합니다.

- 최대 32 자의 영숫자 문자열로 정의되는 구성 이름입니다(Configuration Name 필드의 MST Configuration Identification(MST 구성 식별) 창 에 정의됨).
- 컨피그레이션 개정 번호(여기서는 Revision Level(개정 레벨)로 명명되며 MST Configuration Identification(MST 컨피그레이션 식별) 창에서 찾을 수 있음)
- 4094 요소 테이블(MST Configuration Identification 창에서 VID 목록으로 정의됨)은 지정된 인스턴스에 대해 스위치에서 지원하는 가능한 각 4094 VLAN 을 연결합니다.

스위치에서 MSTP 기능을 사용하려면 다음 세 단계를 수행해야 합니다.

- 스위치는 MSTP 설정(STP Mode 필드의 STP Global Settings(STP Global Settings) 창에 있음)으로 설정해야 합니다.
- MSTP 인스턴스에 대한 올바른 스패닝 트리 우선 순위를 입력해야 합니다(MSTI ID 설정을 구성할 때 MSTP 포트 정보 창에서 우선 순위로 정의됨).
- 공유할 VLAN 은 MSTP 인스턴스 ID 에 추가해야 합니다(MSTI ID 설정을 구성할 때 MST 구성 식별 창에서 VID 목록 으로 정의됨).

802.1D-2004 Rapid Spanning Tree

이 스위치는 IEEE 802.1Q-2005 에 정의된 MSTP(Multiple Spanning Tree Protocol), IEEE 802.1D-2004 에 의해 정의된 RSTP(Rapid Spanning Tree Protocol) 및 IEEE 802.1D-1998 과 호환되는 버전의 세 가지 버전의 스패닝 트리 프로토콜을 구현합니다. RSTP 는 IEEE 802.1D1998 을 구현하는 레거시 장비와 함께 작동할 수 있습니다. 그러나 RSTP 사용의 이점은 손실됩니다. 이 섹션에서는 몇 가지 새로운 스패닝 트리 개념을 소개하고 두 프로토콜 간의 주요 차이점을 설명합니다.

Port Transition States

세 프로토콜의 근본적인 차이점은 포트가 포워딩 상태로 전환되는 방식이며, 이러한 전환은 토폴로지에서 포트의 역할(포워딩 또는 포워딩하지 않음)과 관련이 있습니다. MSTP 및 RSTP 는 802.1D-1998 에서 사용되는 전환 상태 Disabled, Blocking 및 Listening 을 결합하고 Discarding 이라는 단일 상태를 생성합니다. 두 경우 모두 포트는 패킷을 전달하지 않습니다. STP 포트, 전환 상태 Disabled(비활성화), Blocking 또는 Listening(수신 대기) 또는 RSTP/MSTP 포트 상태 Discarding(폐기)에서 기능적 차이는 없으며 포트는 네트워크 토폴로지에서 활성화되지 않습니다. 아래 표 7-3 은 포트 상태 전환과 관련하여 세 가지 프로토콜이 어떻게 다른지 비교합니다.

세 가지 프로토콜 모두 동일한 방식으로 안정적인 토폴로지를 계산합니다. 모든 세그먼트에는 루트 브리지에 대한 단일 경로가 있습니다. 모든 브리지는 BPDU 패킷을 수신합니다. 그러나 BPDU 패킷은 모든 Hello 패킷과 함께 더 자주 전송됩니다. BPDU 패킷이 수신되지 않은 경우에도 BPDU 패킷이 전송됩니다. 따라서 브리지 간의 각 링크는 링크의 상태에 민감합니다. 궁극적으로 이러한 차이로 인해 장애가 발생한 링크를 더 빠르게 탐지할 수 있으므로 토폴로지 조정 속도가 빨라집니다. IEEE 802.1D-1998 의 단점은 인접 브리지에서 즉각적인 피드백이 없다는 것입니다.

802.1Q-2005 MSTP	802.1D-2004 RSTP	802.1D-1998 STP	Forwarding	Learning
Disabled	Disabled	Disabled	No	No
Discarding	*Discarding*	*Blocking*	No	No
Discarding	*Discarding*	*청취*	No	No
Learning	*Learning*	*Learning*	No	**Yes**
Forwarding	**Forwarding**	**Forwarding**	**Yes**	**Yes**

RSTP 는 포워딩 상태로 보다 신속하게 전환할 수 있습니다. RSTP 는 더 이상 타이머 구성에 의존하지 않으며 RSTP 호환 브리지는 다른 RSTP 호환 브리지 링크의 피드백에 민감합니다. 포트는 포워딩 상태로 전환하기 전에 토폴로지가 안정화될 때까지 기다릴 필요가 없습니다. 이러한 빠른 전환을 허용하기 위해 프로토콜은 에지 포트와 P2P(Point-to-Point) 포트라는 두 가지 새로운 변수를 도입합니다.

Edge Port

포트는 루프를 생성할 수 없는 세그먼트에 직접 연결된 경우 Edge Port(에지 포트)로 구성할 수 있습니다. 예를 들어 단일 워크스테이션에 직접 연결된 포트가 있습니다. 에지 포트로 지정된 포트는 Listening 및 Learning 상태를 거치지 않고 즉시 전달 상태로 전환됩니다. 에지 포트는 BPDU 패킷을 수신하면 상태를 잃게 되며, 그 후에는 즉시 일반 스패닝 트리 포트가 됩니다.

P2P Port

P2P 포트는 또한 빠른 전환이 가능합니다. P2P 포트를 사용하여 다른 브리지에 연결할 수 있습니다. RSTP/MSTP 에서 전이중 모드에서 작동하는 모든 포트는 컨피그레이션을 통해 수동으로 재정의하지 않는 한 P2P 포트로 간주됩니다.

802.1D-1998/802.1D-2004/802.1Q-2005 Compatibility

MSTP 또는 RSTP 는 레거시 장비와 상호 운용할 수 있으며 필요한 경우 BPDU 패킷을 802.1D-1998 형식으로 자동 조정할 수 있습니다. 그러나 802.1D-1998 STP 를 사용하는 모든 세그먼트는 MSTP 또는 RSTP 의 빠른 전환 및 신속한 토폴로지 변경 탐지의 이점을 누릴 수 없습니다. 이 프로토콜에는 세그먼트의 레거시 장비가 RSTP 또는 MSTP 를 사용하도록 업데이트되는 경우 마이그레이션에 사용되는 변수도 포함되어 있습니다.

STP(Spanning Tree Protocol)는 두 가지 레벨에서 작동합니다.

- 스위치 수준에서는 설정이 전역적으로 구현됩니다.
- 포트 수준에서 설정은 사용자 정의 포트 그룹에 구현됩니다.

STP Global Settings

이 창은 전역 STP 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > STP > STP Global Settings 을 클릭합니다.

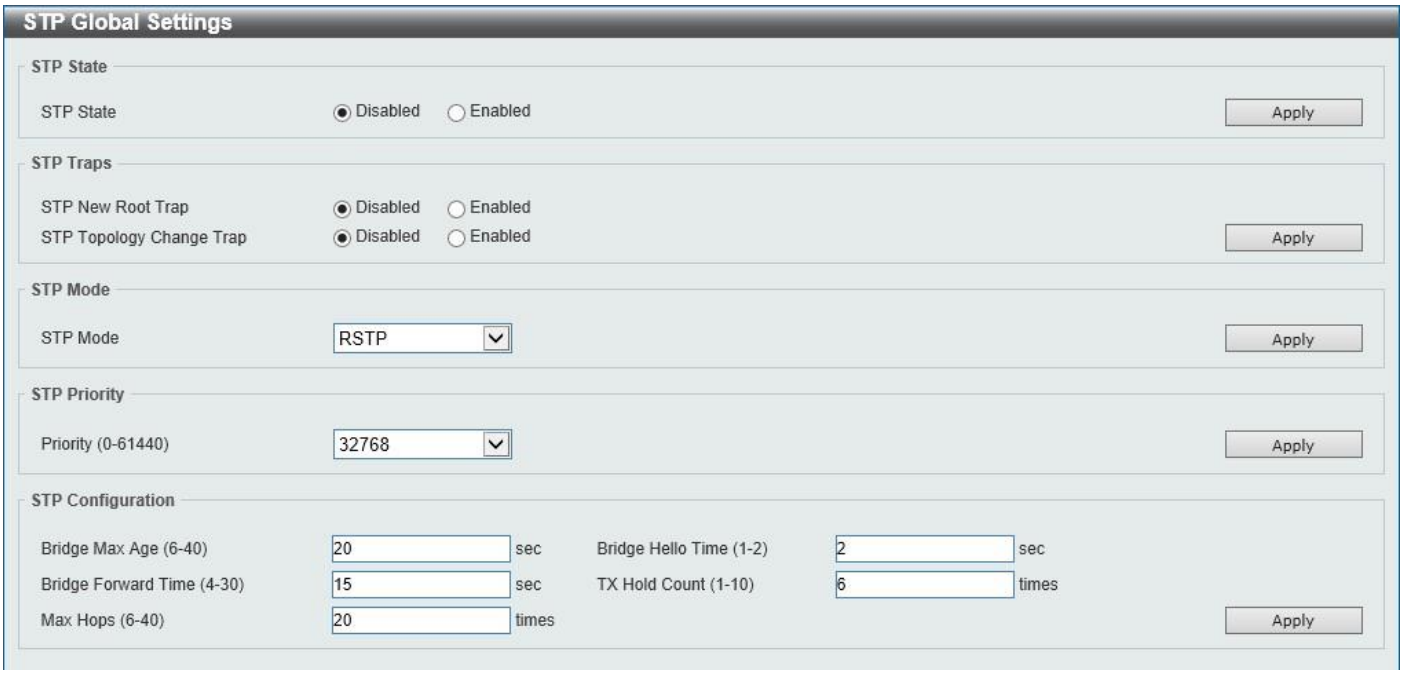

그림 5-35) STP Global Settings 창

STP State 에 대해 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
STP State	여기에서 전역 STP 상태를 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

STP Traps 에 대해 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
STP New Root Trap	여기에서 STP New Root Trap(STP 새 루트 트랩) 옵션을 활성화하거나 비활성화하려면 선택합니다.
STP Topology Change Trap	여기에서 STP Topology Change Trap(STP 토폴로지 변경 트랩) 옵션을 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

STP 모드에 대해 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
STP Mode	여기에 사용된 STP 모드를 선택합니다. 선택할 수 있는 옵션은 MSTP, RSTP 및 STP 입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

STP Priority(STP 우선 순위)에 대해 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description

Priority	여기에서 STP 우선순위 값을 선택합니다. 이 값은 0 에서 61440 사이입니다. 기본적으로 이 값은 32768 입니다. 값이 낮을수록 우선 순위가 높습니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

STP Configuration 에 대해 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Bridge Max Age	여기에 bridge Maximum Age(브리지 최대 사용 기간) 값을 입력합니다. 이 값은 6 초에서 40 초 사이여야 합니다. 기본적으로 이 값은 20 초입니다. Maximum Age 값은 이전 정보가 네트워크의 중복 경로를 통해 끝없이 순환하지 않도록 설정하여 새 정보의 효과적인 전파를 방해하지 않도록 할 수 있습니다. 루트 브리지에 의해 설정되는 이 값은 스위치에 브리지 LAN 의 다른 디바이스와 일치하는 스패닝 트리 컨피그레이션 값이 있는지 확인하는 데 도움이 됩니다.
Bridge Hello Time	스패닝 트리 모드로 RSTP/STP 를 선택하면 이 매개변수를 사용할 수 있습니다. 여기에 bridge Hello Time 값을 입력합니다. 이 값은 1 초에서 2 초 사이여야 합니다. 기본적으로 이 값은 2 초입니다. 이는 루트 브리지에서 보낸 BPDU 패킷의 두 전송 사이의 간격으로, 다른 모든 스위치에 실제로 루트 브리지임을 알립니다. 이 필드는 STP 버전에 대해 STP 또는 RSTP 를 선택한 경우에만 여기에 나타납니다. MSTP 의 경우 Hello Time 은 포트별로 설정해야 합니다.
Bridge Forward Time	여기에 브리지 전달 시간 값을 입력합니다. 이 값은 4 초에서 30 초 사이여야 합니다. 기본적으로 이 값은 15 초입니다. 스위치의 모든 포트는 이번에는 Blocking 상태에서 Forwarding 상태로 이동하는 동안 Listening 상태입니다.
TX Hold Count	여기에 Transmit Hold Count 값을 입력합니다. 이 값은 1 에서 10 배 사이여야 합니다. 기본적으로 이 값은 6 배입니다. 이 값은 간격당 전송되는 Hello 패킷의 최대 수를 설정하는 데 사용됩니다.
Max Hops	허용되는 최대 홉 수를 입력합니다. 이 값은 6 에서 40 홉 사이여야 합니다. 기본적으로 이 값은 20 홉입니다. 이 값은 스위치에서 보낸 BPDU(Bridge Protocol Data Unit) 패킷이 폐기되기 전에 스패닝 트리 영역의 디바이스 간 홉 수를 설정하는 데 사용됩니다. hop count 의 각 Switch 는 값이 0 이 될 때까지 hop count 를 1 씩 줄입니다. 그런 다음 스위치는 BDPU 패킷을 버리고 포트에 대해 보유된 정보가 만료됩니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

STP Port Settings

이 창은 STP 포트 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > STP > STP Port Settings 를 클릭합니다.

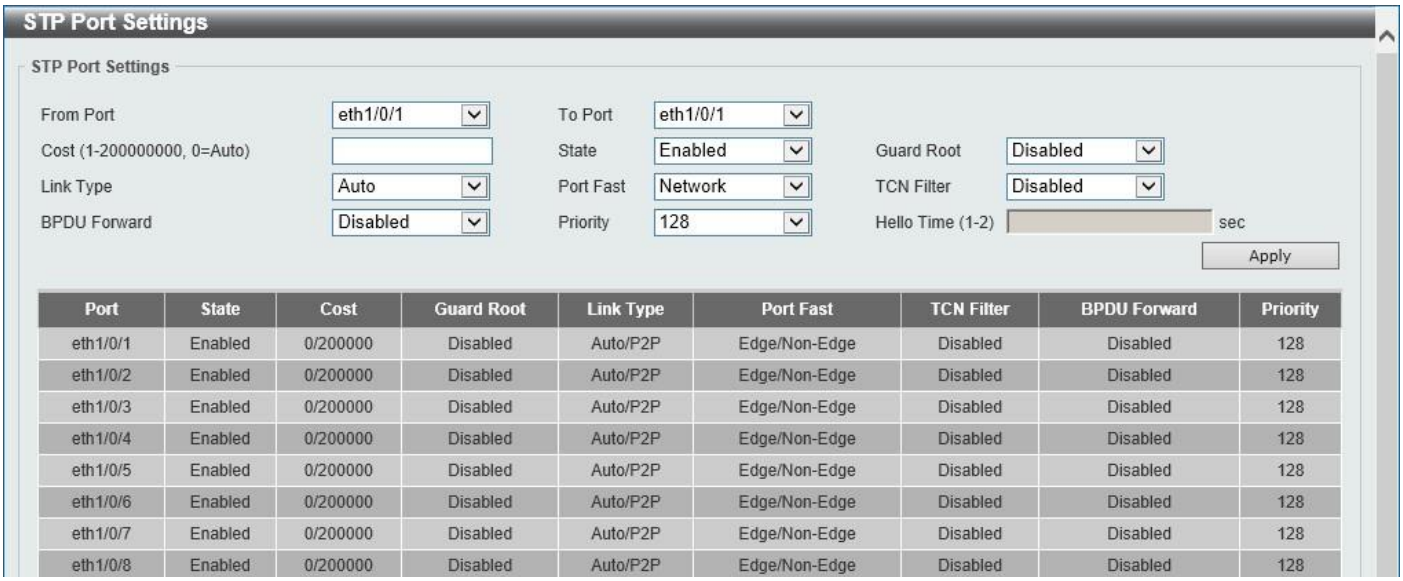

그림 5-36) STP 포트 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
Cost	여기에 비용 값을 입력합니다. 이 값은 1 에서 200000000 사이여야 합니다. 이 값은 지정된 포트 목록으로 패킷을 전달하는 상대적 비용을 나타내는 메트릭을 정의합니다. 포트 비용은 자동으로 또는 메트릭 값으로 설정할 수 있습니다. 기본값은 0 (자동)입니다. 외부 비용을 0 으로 설정하면 최적의 효율성을 위해 목록의 지정된 포트로 패킷을 전달하는 속도가 자동으로 설정됩니다. 100Mbps 포트의 기본 포트 비용은 200000, 기가비트 포트는 20000, 10 기가비트 포트는 2000 입니다. 숫자가 낮을수록 패킷을 전달하기 위해 포트가 선택될 확률이 커집니다.
State	STP 포트 상태를 활성화하거나 비활성화하려면 선택합니다.
Guard Root	Guard Root 기능을 활성화하거나 비활성화하려면 선택합니다.
Link Type	여기에서 링크 유형을 선택합니다. 선택할 수 있는 옵션은 자동, P2P 및 공유입니다. 전이중 포트는 P2P(Point-to-Point) 연결이 있는 것으로 간주됩니다. 포트는 링크 유형을 Shared(공유)로 설정하여 전달 상태로 빠르게 전송할 수 없습니다. 기본적으로 이 옵션은 자동입니다.
Port Fast	여기에서 Port Fast(빠른 포트) 옵션을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • 네트워크 모드에서 포트는 3 초 동안 비포트 고속 상태로 유지됩니다. BPDU 가 수신되지 않고 포워딩 상태로 변경되면 포트가 포트 고속 상태로 변경됩니다. 포트가 나중에 BPDU 를 수신하면 비포트 고속 상태로 변경됩니다. • 비활성화 모드에서 포트는 항상 비포트 고속 상태입니다. 전달 시간 지연이 전달 상태로 변경될 때까지 항상 대기합니다. • Edge 모드에서는 forward-time delay 를 기다리지 않고 link-up 이 발생하면 포트가 스패닝 트리 전달 상태로 직접 변경됩니다. Interface 가 나중에 BPDU 를 수신하면 해당 작업 상태가 비포트 고속 상태로 변경됩니다.

	기본적으로 이 옵션은 네트워크입니다.
TCN Filter	TCN 필터 옵션을 활성화하거나 비활성화하려면 선택합니다. 포트가 TCN 필터 모드로 설정되면 포트에서 수신한 TC 이벤트는 무시됩니다. 기본적으로 이 옵션은 사용 안 함입니다.
BPDU Forward	BPDU 전달을 활성화하거나 비활성화하려면 선택합니다. 활성화된 경우 수신된 STP BPDU 는 태그가 지정되지 않은 형식으로 모든 VLAN 멤버 포트로 전달됩니다. 기본적으로 이 옵션은 사용 안 함입니다.
Priority	여기에서 우선 순위 값을 선택합니다. 선택할 수 있는 옵션은 0 에서 240 사이입니다. 기본적으로 이 옵션은 0 입니다. 값이 낮을수록 우선 순위가 높습니다.
Hello Time	여기에 hello 시간 값을 입력합니다. 이 값은 1 초에서 2 초 사이여야 합니다. 이 값은 지정된 포트가 각 구성 메시지의 주기적 전송 사이에 대기하는 간격을 지정합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

MST Configuration Identification

이 창은 MST 컨피그레이션 식별 설정을 표시하고 구성하는 데 사용됩니다. 이러한 설정은 스위치에 구성된 MSTI 를 고유하게 식별합니다. 스위치는 처음에 사용자가 매개변수를 수정할 수 있지만 MSTI ID 를 변경하거나 삭제할 수 없는 하나의 CIST(Common Internal Spanning Tree)를 소유합니다.

다음 창을 보려면 아래와 같이 L2 Features > STP > MST Configuration Identification 을 클릭합니다.

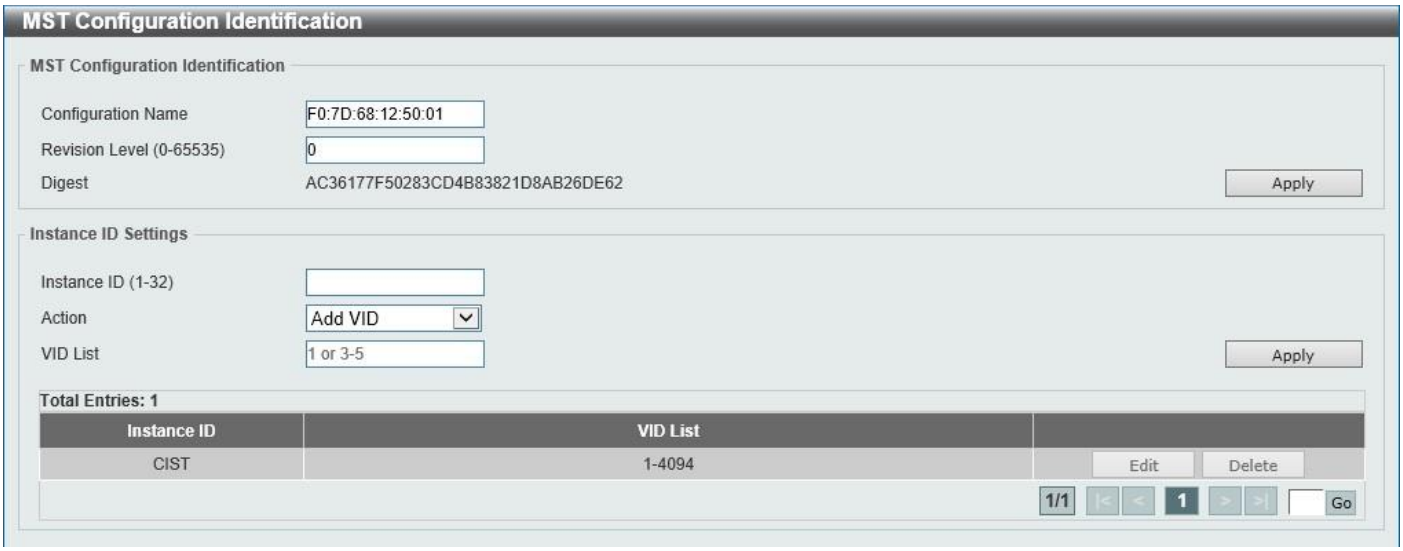

그림 5-37) MST 구성 식별 창

MST Configuration Identification 에 대해 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description

Configuration Name	MST 를 입력합니다. 이 이름은 MSTI(Multiple Spanning Tree Instance)를 고유하게 식별합니다. 구성 이름이 설정되지 않은 경우 이 필드에는 MSTP 를 실행하는 디바이스에 대한 MAC 주소가 표시됩니다.
Revision Level	여기에 리비전 레벨 값을 입력합니다. 이 값은 0 에서 65535 사이여야 합니다. 기본적으로 이 값은 0 입니다. 이 값은 Configuration Name(컨피그레이션 이름)과 함께 스위치에 구성된 MSTP 영역을 식별합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

인스턴스 ID 설정에 대해 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Instance ID	여기에 인스턴스 ID 를 입력합니다. 이 값은 1 에서 32 사이여야 합니다.
Action	여기에서 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 VID 추가 및 VID 제거입니다.
VID List	여기에 VID 목록 값을 입력합니다. 이 필드는 스위치에 설정된 구성된 VLAN 의 VID 범위를 지정하는 데 사용됩니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.

Delete 버튼을 클릭하여 특정 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

STP Instance

이 창은 STP 인스턴스 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > STP > STP Instance 를 클릭합니다.

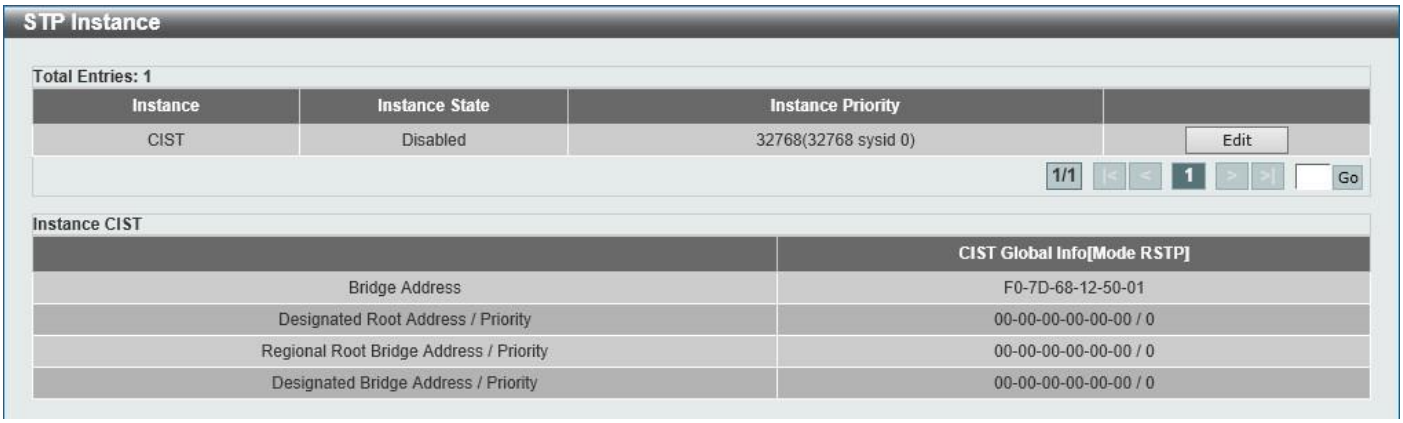

그림 5-38) STP 인스턴스 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Instance Priority	Edit 버튼을 클릭한 후 여기에 Instance Priority(인스턴스 우선 순위) 값을 입력합니다. 범위는 0 에서 61440 사이입니다.

Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다. Apply 버튼을 클릭하여 변경 사항을 적용합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

MSTP Port Information

이 창은 MSTP 포트 정보 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > STP > MSTP Port Information 을 클릭합니다.

그림 5-39) MSTP 포트 정보 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Port	여기에서 지울 포트 번호를 선택합니다.
Cost	Edit 버튼을 클릭한 후 여기에 비용 값을 입력합니다. 이 값은 1 에서 200000000 사이여야 합니다.
Priority	Edit 버튼을 클릭한 후 여기에서 우선 순위 값을 선택합니다. 선택할 수 있는 옵션은 0 에서 240 사이입니다. 기본적으로 이 옵션은 0 입니다. 값이 낮을수록 우선 순위가 높습니다.

Clear Detected Protocol 버튼을 클릭하여 선택한 포트에 대한 감지된 프로토콜 설정을 지웁니다.
Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.
Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.
페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Loopback Detection

LBD(Loopback Detection) 기능은 특정 포트에서 생성된 루프를 감지하는 데 사용됩니다. 이 기능은 CTP(Configuration Testing Protocol) 패킷이 스위치로 다시 루프된 경우 스위치의 포트를 임시로 종료하는 데 사용됩니다. 스위치가 포트 또는 VLAN 에서 수신된 CTP 패킷을 탐지하면 네트워크의 루프를 의미합니다. 스위치는 자동으로 포트 또는 VLAN 을 차단하고 관리자에게 경고를 보냅니다. 이
루프백 탐지 복구 시간이 초과되면 루프백 탐지 포트가 다시 시작(정상 상태로 변경)됩니다.
루프백 감지 기능은 한 번에 여러 포트에서 구현할 수 있습니다. 사용자는 드롭다운 메뉴를 사용하여 이 기능을 활성화하거나 비활성화할 수 있습니다.

다음 창을 보려면 아래와 같이 L2 Features > Loopback Detection 을 클릭합니다.

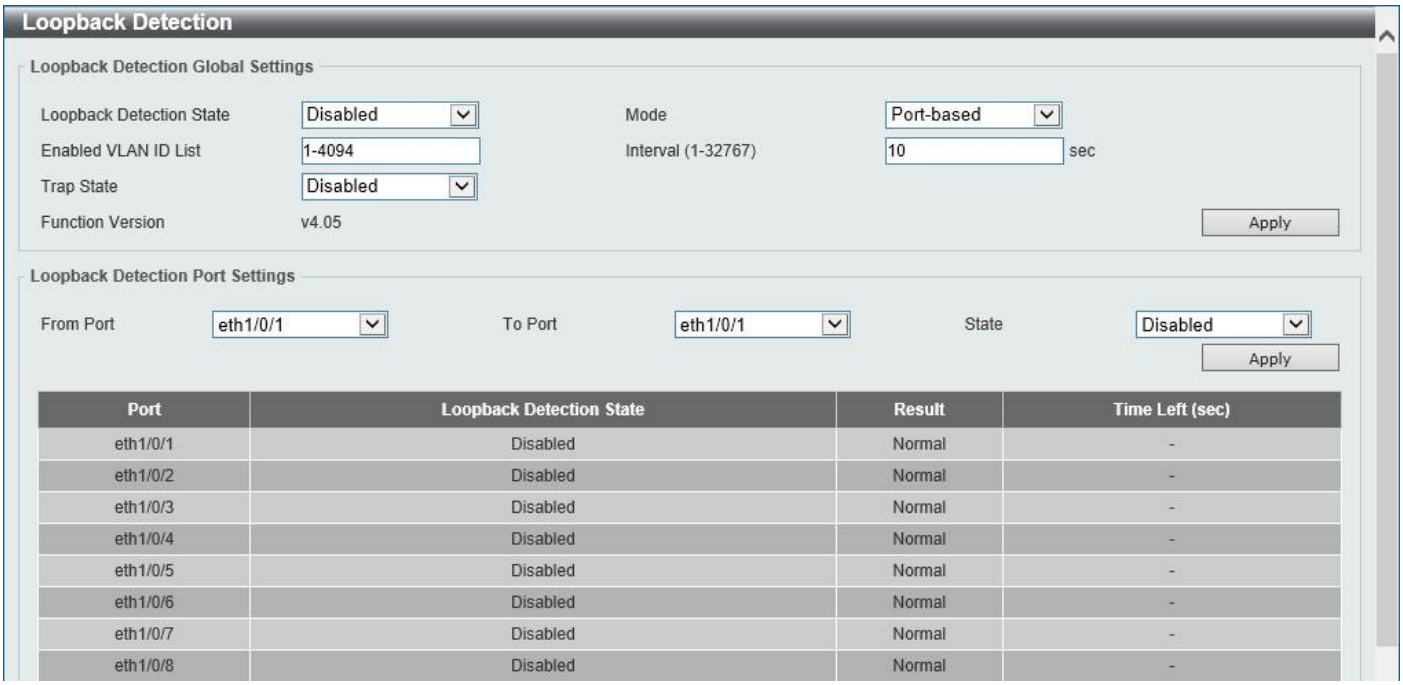

그림 5-40) 루프백 감지 창

Loopback Detection Global Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Loopback Detection State	루프백 감지를 활성화하거나 비활성화하려면 선택합니다. 기본값은 사용 안 함입니다.
Mode	루프백 감지 모드를 선택합니다. 선택할 수 있는 옵션은 포트 기반 및 VLAN 기반입니다.
Enabled VLAN ID List	루프 감지를 위한 VLAN ID 를 입력합니다. 이는 모드 드롭다운 목록에서 VLAN 기반을 선택한 경우에만 적용됩니다.
Interval	디바이스가 루프백 이벤트를 감지하기 위해 CTP(Configuration Test Protocol) 패킷을 전송하는 데 사용할 간격(초)을 입력합니다. 유효한 범위는 1 초에서 32767 초 사이입니다. 기본 설정은 10 초입니다.
Trap State	루프백 탐지 트랩 상태를 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Loopback Detection Port Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
State	이 옵션을 선택하면 포트의 상태를 활성화하거나 비활성화할 수 있습니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Link Aggregation

포트 트렁크 그룹 이해

포트 트렁크 그룹은 여러 포트를 결합하여 단일 고대역폭 데이터 파이프라인을 만드는 데 사용됩니다.

스위치는 각 그룹에 최대 8 개의 포트가 있는 최대 8 개의 포트 트렁크 그룹을 지원합니다.

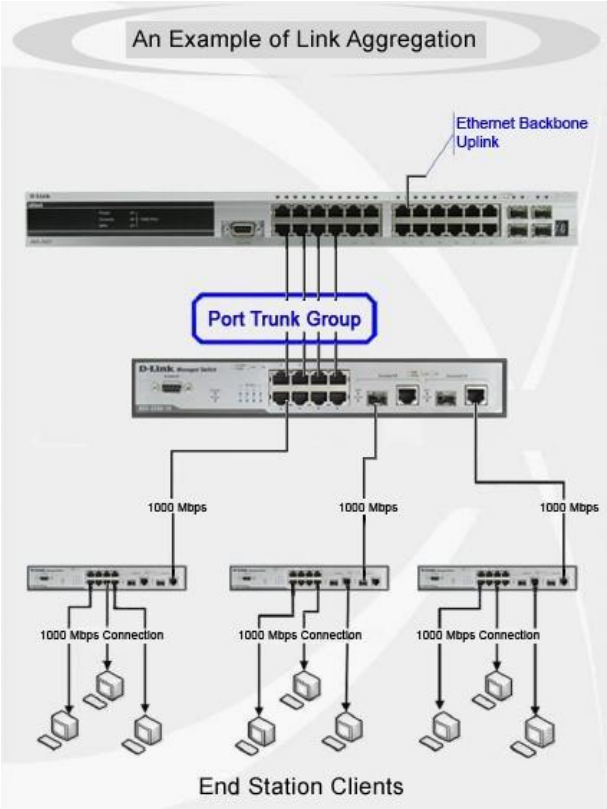

그림 5-41) 포트 트렁크 그룹의 예

스위치는 트렁크 그룹의 모든 포트를 단일 포트로 취급합니다. 특정 호스트(대상 주소)로 전송되는 데이터는 항상 트렁크 그룹의 동일한 포트를 통해 전송됩니다. 이렇게 하면 데이터 스트림의 패킷이 전송된 순서와 동일한 순서로 도착할 수 있습니다.

링크 어그리게이션을 사용하면 여러 포트를 함께 그룹화하고 단일 링크로 작동할 수 있습니다. 그 결과 대역폭이 단일 링크 대역폭의 배수가 됩니다.

링크 집계는 서버와 같이 대역폭을 많이 사용하는 네트워크 장치를 네트워크 백본에 연결하는 데 가장 일반적으로 사용됩니다.

스위치를 사용하면 최대 8 개의 링크 집계 그룹을 생성할 수 있으며, 각 그룹은 최대 8 개의 링크(포트)로 구성됩니다. 각 포트는 단일 링크 집계 그룹에만 속할 수 있습니다.

로드 밸런싱은 집계된 그룹의 포트에 자동으로 적용되며, 그룹 내의 링크 장애로 인해 네트워크 트래픽이 그룹의 나머지 링크로 전달됩니다.

스패닝 트리 프로토콜은 링크 집계 그룹을 단일 링크로 취급합니다. 스위치에 두 개의 이중화 링크 어그리게이션 그룹이 구성된 경우 STP 는 하나의 전체 그룹을 차단합니다. 같은 방식으로 STP 는 이중화 링크가 있는 단일 포트를 차단합니다.

메모: 트렁크 그룹 내의 포트 연결이 끊어지면 연결이 끊긴 포트로 향하는 패킷은 링크 어그리게이션의 다른 연결된 포트 간에 로드 공유됩니다 그룹.

이 창은 링크 집계 설정을 표시하고 구성하는 데 사용됩니다. 다음 창을 보려면 아래와 같이 L2 Features > Link Aggregation 을 클릭합니다.

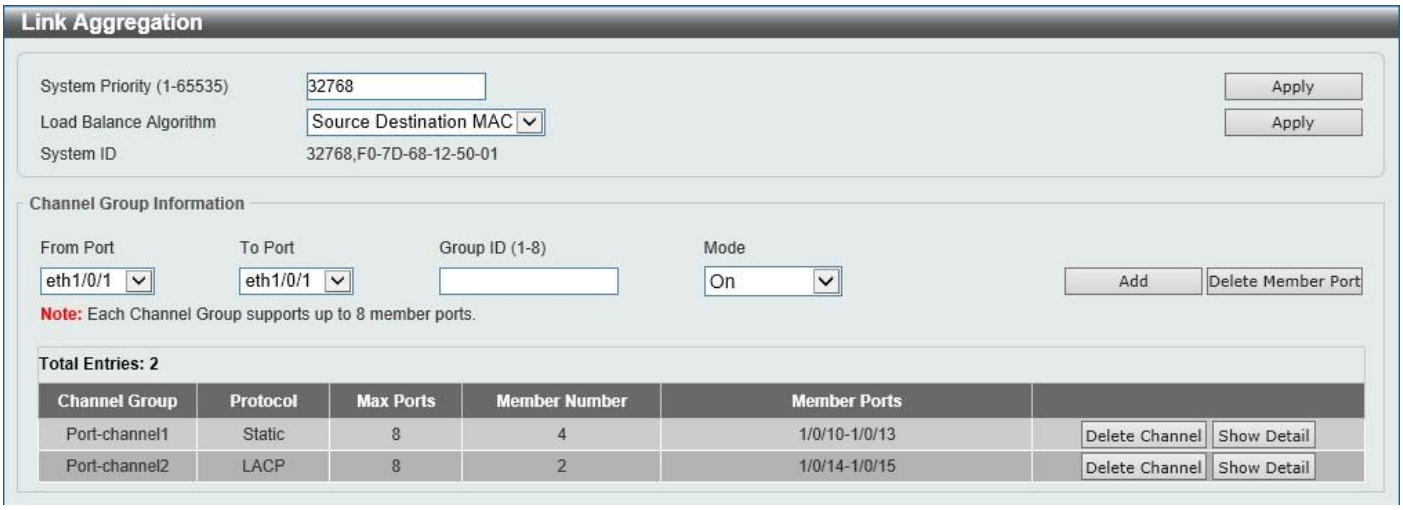

그림 5-42) Link Aggregation 창

Link Aggregation 에 대해 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
System Priority	여기에 사용된 시스템 우선 순위 값을 입력합니다. 이 값은 1 에서 65535 사이여야 합니다. 기본적으로 이 값은 32768 입니다. 시스템 우선 순위는 포트 채널에 조인할 수 있는 포트와 독립형 모드에 배치되는 포트를 결정합니다. 값이 낮을수록 우선 순위가 높습니다. 두 개 이상의 포트가 동일한 우선 순위를 갖는 경우 포트 번호에 따라 우선 순위가 결정됩니다.
Load Balance Algorithm	여기에서 사용할 부하 분산 알고리즘을 선택합니다. 선택할 수 있는 옵션은 소스 MAC, 대상 MAC, 소스 대상 MAC, 소스 IP, 대상 IP 및 소스 대상 IP 입니다. 기본적으로 이 옵션은 Source Destination MAC 입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Channel Group Information 에 대해 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성과 연결할 포트 목록을 선택합니다.
Group ID	여기에 채널 그룹 번호를 입력합니다. 이 값은 1 에서 8 사이여야 합니다. 시스템은 물리적 포트가 채널 그룹에 처음 가입할 때 포트 채널을 자동으로 생성합니다. Interface 는 하나의 채널 그룹에만 가입할 수 있습니다.
Mode	여기에서 모드 옵션을 선택합니다. 선택할 수 있는 옵션은 On(켜기), Active(활성) 및 지속 효과. On 모드 가 지정된 경우 채널 그룹 유형은 정적입니다. 액티브 또는 패시브 모드 가 지정된 경우 채널 그룹 유형은 LACP 입니다. 채널 그룹은 정적 멤버 또는 LACP 멤버로만 구성될 수 있습니다. 채널 그룹 유형이 결정되면 다른 유형의 Interface 는 채널 그룹에 가입할 수 없습니다.

Add 버튼을 클릭하여 새 채널 그룹을 추가합니다.

Delete Member Port 버튼을 클릭하여 그룹에서 지정된 멤버 포트를 삭제합니다.

Delete Channel 버튼을 클릭하여 지정된 채널 그룹을 삭제합니다.

Show Detail 버튼을 클릭하면 채널에 대한 자세한 정보를 볼 수 있습니다.

Static Protocol 을 사용하는 항목에서 *Show Detail* 버튼을 클릭하면 다음 페이지를 사용할 수 있습니다.

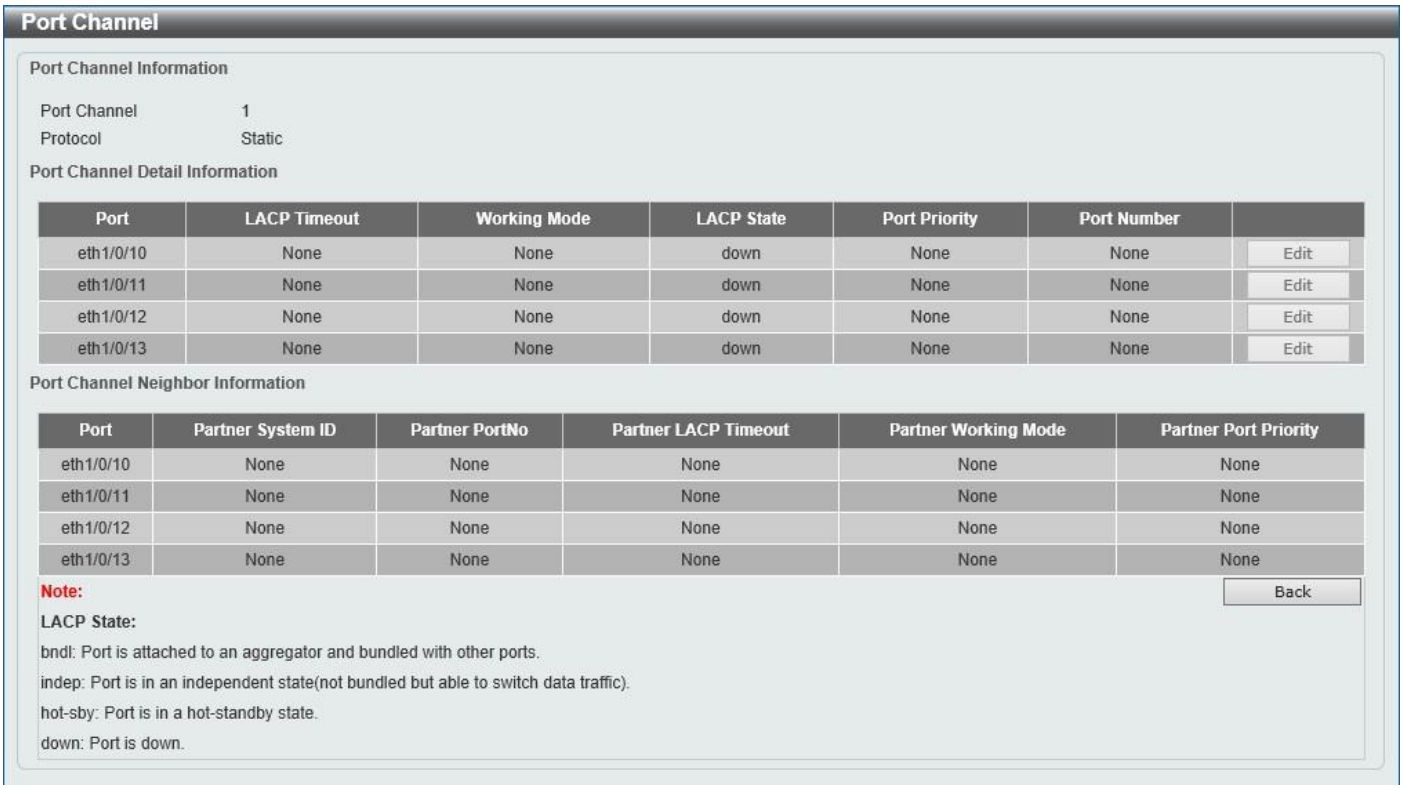

그림 5-43) Link Aggregation (Channel 1 Detail) 창

Back 버튼을 클릭하여 이전 페이지로 돌아갑니다.

LACP 프로토콜을 사용하는 항목에서 *Show Detail* 버튼을 클릭하면 다음 페이지를 사용할 수 있습니다.

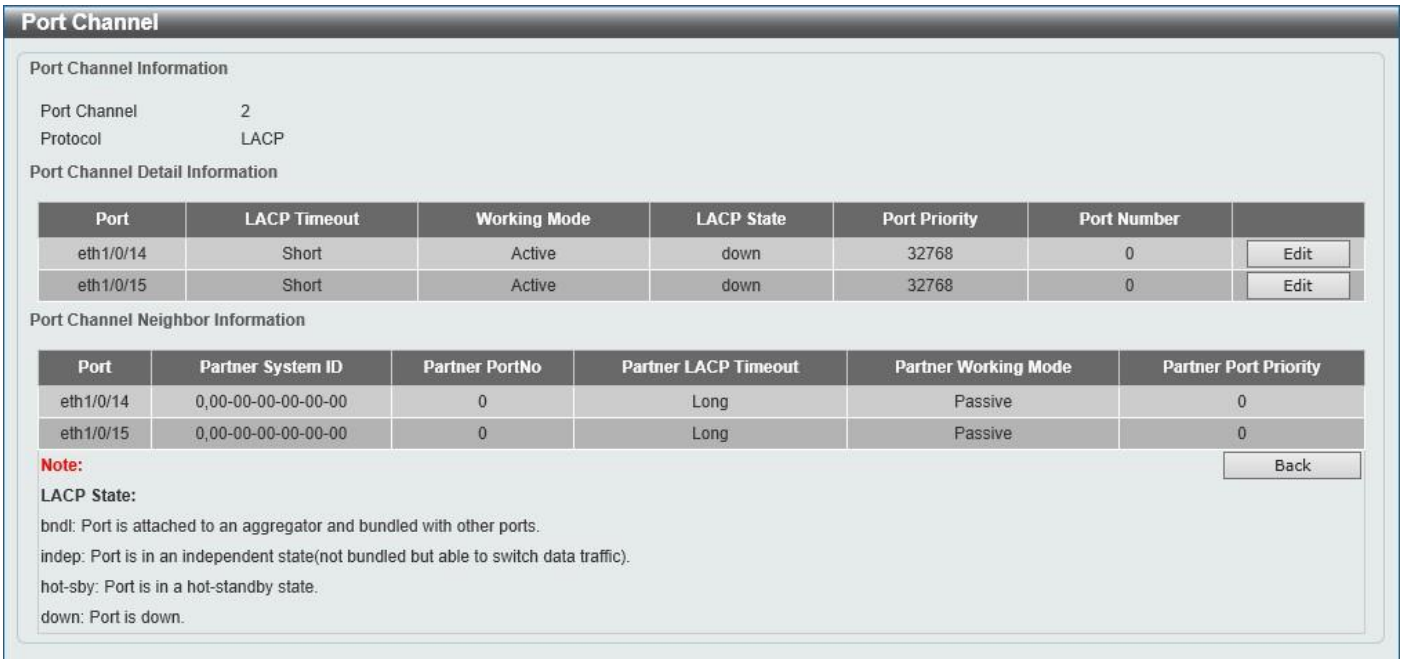

그림 5-44) Link Aggregation (Channel 2 Detail) 창

Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.
Back 버튼을 클릭하여 이전 페이지로 돌아갑니다.
Edit 버튼을 클릭하면 다음 페이지를 사용할 수 있습니다.

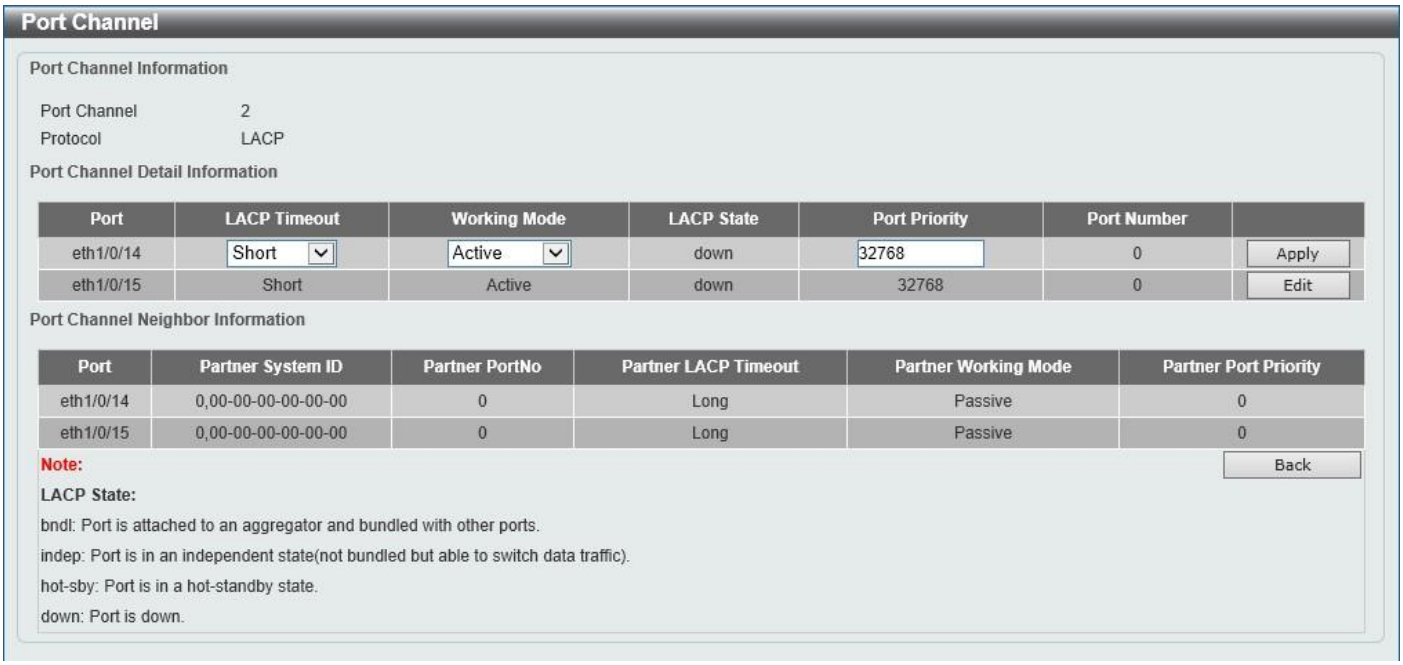

그림 5-45) Link Aggregation (Channel 2 Detail, Edit) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
LACP Timeout	여기에서 LACP 타임아웃 옵션을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Short - 수신된 LACPDU 정보가 유효하지 않은 것으로 선언되기까지 3 초가 남았음을 지정합니다. 파트너가 수신된 PDU 의 정보를 인식하면 LACP PDU 의 주기적인 전송이 Interface 에서 1 초 간격으로 전송됩니다. 이것이 기본 옵션입니다. • Long - 수신된 LACPDU 정보가 유효하지 않은 것으로 선언되기까지 90 초가 남았음을 지정합니다. 파트너가 수신된 PDU 의 정보를 인식하면 LACP PDU 의 주기적인 전송이 Interface 에서 30 초 간격으로 전송됩니다.
Working Mode	여기에서 작업 모드를 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Passive(패시브) - LACP 패시브 모드에서 작동하도록 지정합니다. • Active(활성) - LACP 활성 모드에서 작동하도록 지정합니다.
Port Priority	여기에 포트 우선 순위 값을 입력합니다. 이는 portchannel 에 조인할 수 있는 포트와 독립형 모드에서 작동하는 포트를 결정합니다. 값이 낮을수록 우선 순위가 높습니다. 범위는 1 에서 65535 사이입니다. 기본적으로 이 값은 32768 입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.

Back 버튼을 클릭하여 이전 페이지로 돌아갑니다.

L2 Multicast Control

IGMP Snooping

IGMP(Internet Group Management Protocol) Snooping 을 통해 스위치는 네트워크 스테이션 또는 장치와 IGMP 호스트 간에 전송된 IGMP 쿼리 및 보고서를 인식할 수 있습니다.

IGMP Snooping Settings

IGMP Snooping 을 사용하려면 먼저 창 상단의 IGMP Global Settings(IGMP Global Settings)에서 전체 스위치에 대해 활성화해야 합니다. 그런 다음 해당 Edit 버튼을 클릭하여 각 VLAN 에 대한 설정을 미세 조정할 수 있습니다. IGMP Snooping 을 위해 활성화된 경우, 스위치는 장비에서 IGMP 호스트로 또는 그 반대로 전송된 IGMP 메시지를 기반으로 특정 멀티캐스트 그룹 멤버에 대한 포트를 열거나 닫을 수 있습니다. 스위치는 IGMP 메시지를 모니터링하고 더 이상 계속을 요청하는 호스트가 없을 때 멀티캐스트 패킷 전달을 중단합니다.

다음 창을 보려면 아래와 같이 L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings 을 클릭합니다.

그림 5-46) IGMP Snooping 설정 창

Global Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Global State	여기에서 IGMP Snooping 을 전역적으로 활성화하거나 비활성화하려면 선택합니다. 기본적으로 이 기능은 비활성화되어 있습니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

VLAN Status Settings(VLAN 상태 설정)에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
VID	여기에 VLAN ID 를 입력합니다. 범위는 1 에서 4094 사이입니다. VLAN 에서 IGMP Snooping 을 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

IGMP Snooping Table 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
VID	1 에서 4094 까지 VLAN ID 를 입력합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Show All 버튼을 눌러 모든 항목을 봅니다.

Show Detail 버튼을 클릭하여 특정 VLAN 의 세부 정보를 확인합니다.

Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Show Detail 버튼을 클릭하면 다음과 같은 창이 나타납니다.

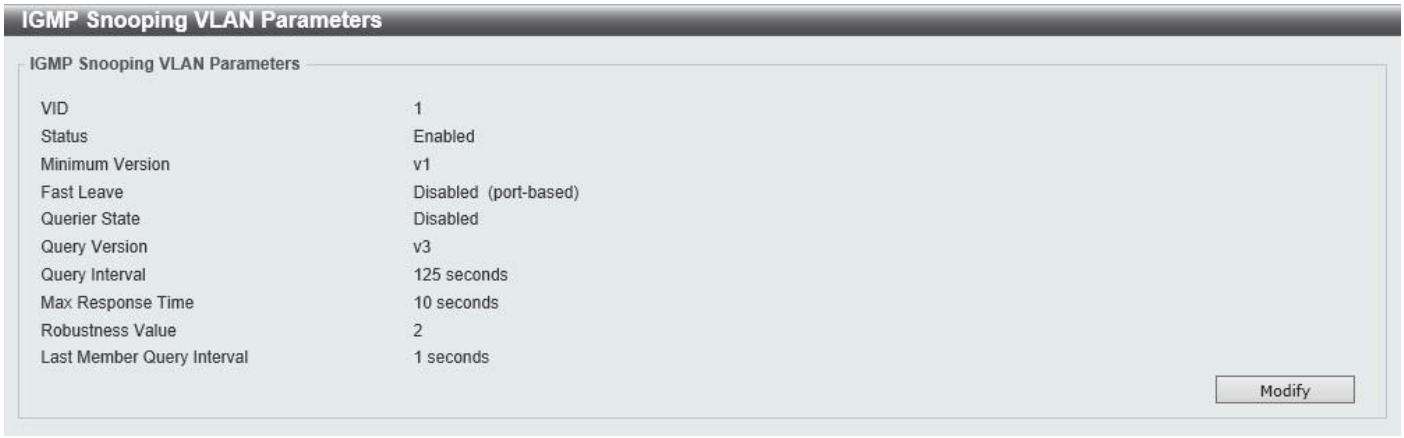

그림 5-47) IGMP Snooping 설정(세부 정보 표시) 창

이 창에는 IGMP Snooping VLAN 에 대한 세부 정보가 표시됩니다.
Modify 버튼을 클릭하여 다음 창에서 정보를 편집합니다.

IGMP Snooping Settings 창에서 Modify 또는 Edit 버튼을 클릭하면 다음 창이 나타납니다.

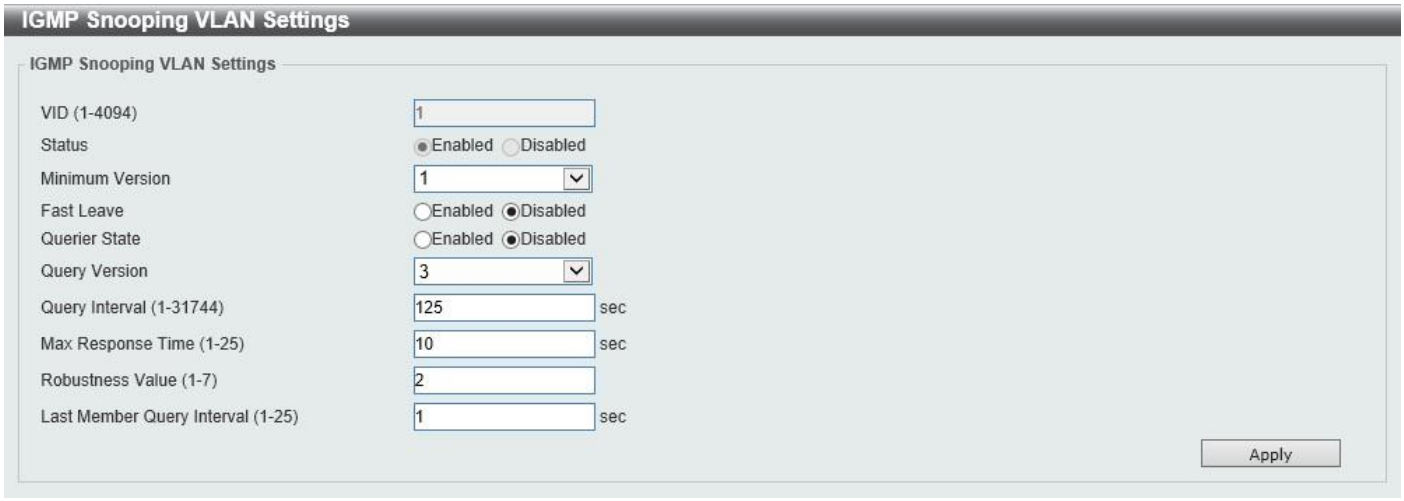

그림 5-48) IGMP Snooping 설정(Modify, Edit) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Minimum Version	VLAN 에서 허용되는 최소 IGMP 호스트 버전을 선택합니다. 선택할 수 있는 옵션은 1, 2 및 3 입니다.
Fast Leave	IGMP Snooping Fast Leave 기능을 활성화하거나 비활성화하려면 이 옵션을 선택합니다. 활성화된 경우, 시스템이 마지막 멤버로부터 IGMP done 메시지를 수신할 때 멤버십이 즉시 제거됩니다. 빠른 휴가가 활성화되면 스위치는 특정 쿼리를 생성하지 않습니다. 빠른 휴가가 비활성화되면 스위치는 특정 쿼리를 생성합니다.
Querier State	쿼리 발생기 상태를 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
Query Version	IGMP Snooping 쿼리 발생기에서 보낸 일반 쿼리 패킷 버전을 선택합니다. 선택할 수 있는 옵션은 1, 2 및 3 입니다.
Query Interval	IGMP Snooping 쿼리 발생기가 IGMP 일반 쿼리 메시지를 주기적으로 전송하는 간격을 입력합니다. 범위는 1 에서 31744 사이입니다.

Max Response Time	IGMP Snooping 쿼리에 광고되는 최대 응답 시간(초)을 입력합니다. 범위는 1 에서 25 사이입니다.
Robustness Value	IGMP Snooping 에 사용되는 견고성 변수를 입력합니다. 범위는 1 에서 7 사이입니다.
Last Member Query Interval	IGMP Snooping 쿼리 발생기가 IGMP 그룹별 또는 그룹 소스별(채널) 쿼리 메시지를 보내는 간격을 입력합니다. 범위는 1 에서 25 사이입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

IGMP Snooping Groups Settings

이 창은 IGMP Snooping 정적 그룹을 표시 및 구성하고 IGMP Snooping 그룹을 보는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings 을 클릭합니다.

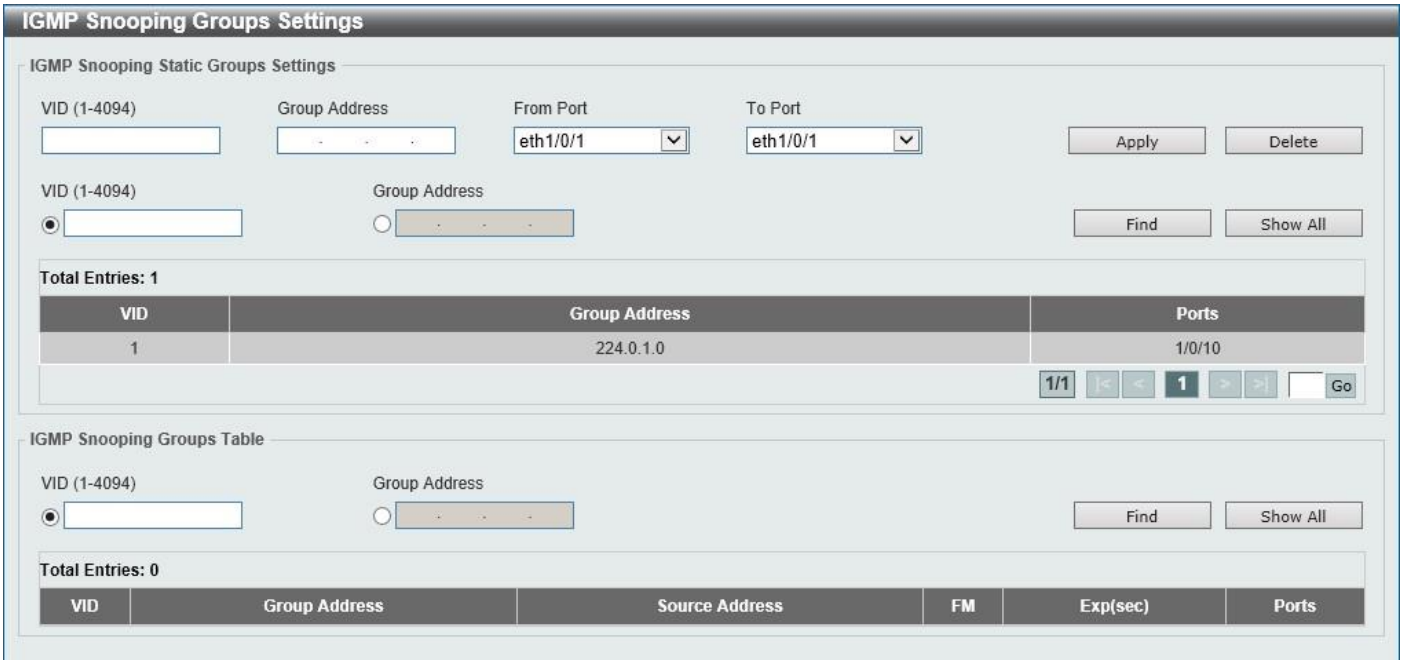

그림 5-49) IGMP Snooping 그룹 설정 창

IGMP Snooping Static Groups Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
VID	멀티캐스트 그룹의 VLAN ID 를 입력합니다. 범위는 1 에서 4094 사이입니다.
Group Address	IP 멀티캐스트 그룹 주소를 입력합니다.
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
VID	라디오 버튼을 클릭하고 멀티캐스트 그룹의 VLAN ID 를 입력합니다. 범위는 1 에서 4094 사이입니다.
Group Address	라디오 버튼을 클릭하고 IP 멀티캐스트 그룹 주소를 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Find 버튼을 사용하여 입력된 정보를 기반으로 특정 항목을 찾습니다.

Show All 버튼을 눌러 모든 항목을 봅니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

IGMP Snooping 그룹 테이블에 대해 구성하거나 표시할 수 있는 필드는 다음과 같습니다.

Parameter	Description
VID	라디오 버튼을 클릭하고 멀티캐스트 그룹의 VLAN ID 를 입력합니다. 범위는 1 에서 4094 사이입니다.
Group Address	라디오 버튼을 클릭하고 IP 멀티캐스트 그룹 주소를 입력합니다.
FM	필터 모드를 표시합니다. 다음이 표시될 수 있습니다. • EX (제외) - 필터 모드는 제외입니다. • IN (포함) - 필터 모드는 포함입니다.
Exp (sec)	항목이 만료되기까지 남은 시간(초)을 표시합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Show All 버튼을 클릭하여 모든 항목을 봅니다.

IGMP Snooping Mrouter Settings

이 창은 IGMP Snooping Mrouter 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings 를 클릭합니다.

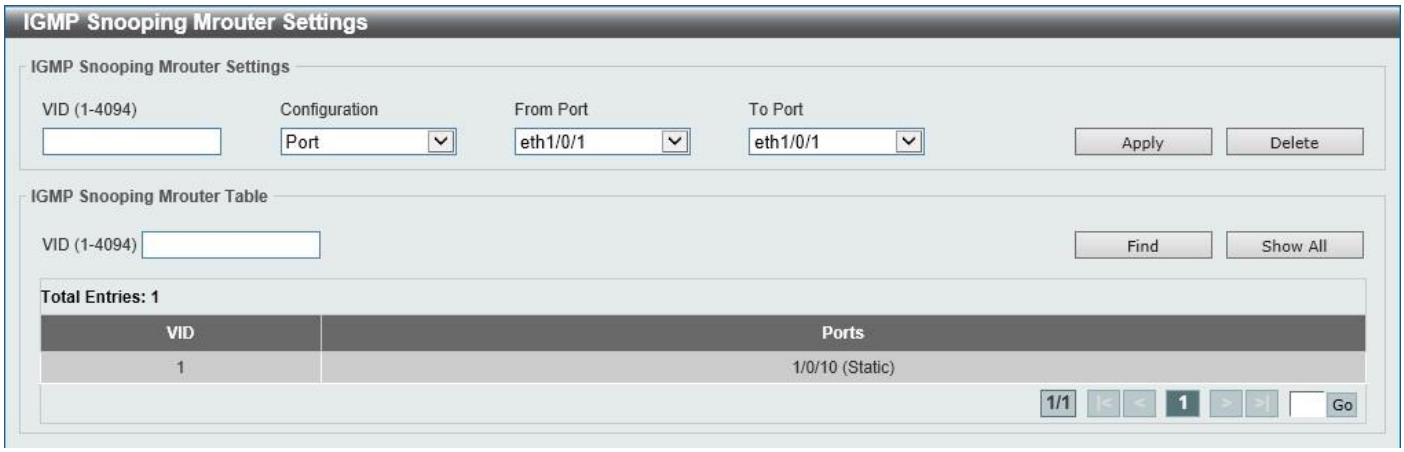

그림 5-50 IGMP Snooping Mrouter 설정 창

IGMP Snooping Mrouter Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
VID	여기에 사용된 VLAN ID 를 입력합니다. 범위는 1 에서 4094 사이입니다.
Configuration	포트 구성을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Port(포트) - 구성된 포트를 고정 멀티캐스트 라우터 포트로 설정하려면 선택합니다. • Forbidden Port(금지된 포트) - 구성된 포트가 멀티캐스트 라우터 포트가 되지 않도록 하려면 선택합니다.
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

IGMP Snooping Mrouter Table 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
VID	여기에 사용된 VLAN ID 를 입력합니다. 범위는 1 에서 4094 사이입니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.
Show All 버튼을 클릭하여 모든 항목을 봅니다.
페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

IGMP Snooping Statistics Settings

이 창은 IGMP snooping 관련 통계를 보고 지우는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings 을 클릭합니다.

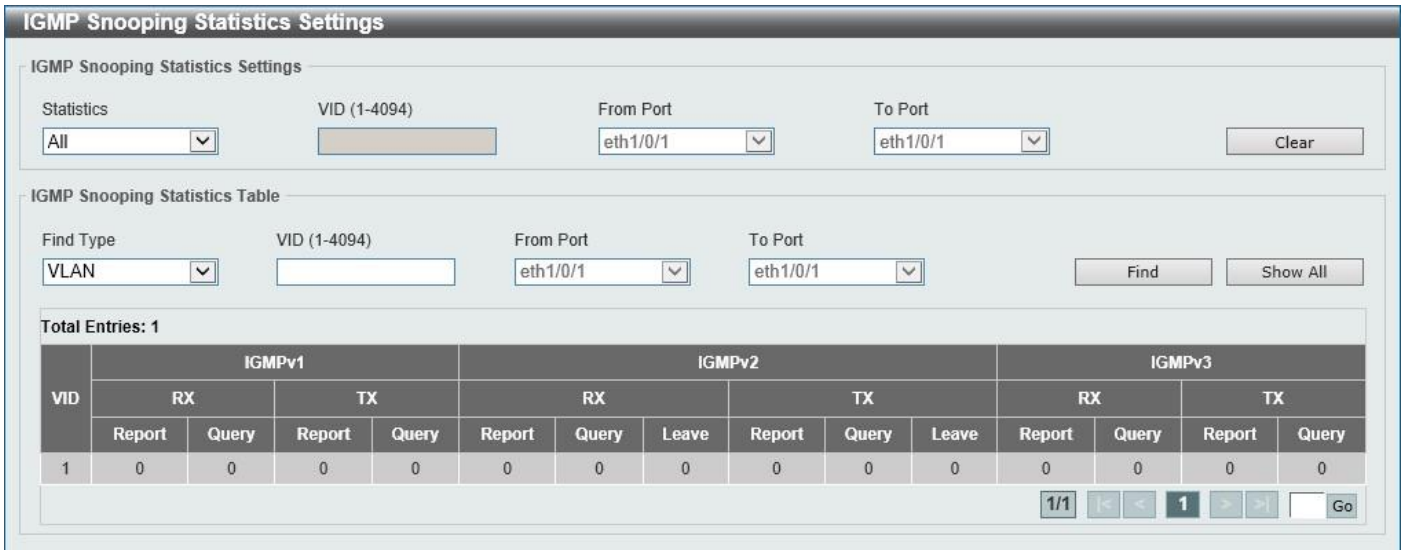

그림 5-51) IGMP Snooping 통계 설정 창

IGMP Snooping 통계 설정에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Statistics	여기에서 Interface 를 선택합니다. 선택할 수 있는 옵션은 모두, VLAN 및 포트입니다.
VID	1 에서 4094 사이의 VLAN ID 를 입력합니다. Statistics(통계) 드롭다운 목록에서 VLAN 을 선택한 경우 사용할 수 있습니다.
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다. Statistics(통계) 드롭다운 목록에서 Port(포트)를 선택한 경우 사용할 수 있습니다.

Clear 버튼을 클릭하여 IGMP Snooping 관련 통계를 지웁니다.

IGMP Snooping Statistics Table 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
유형 찾기	Interface 유형을 선택합니다. 선택할 수 있는 옵션은 VLAN 및 포트입니다.
VID	1 에서 4094 사이의 VLAN ID 를 입력합니다. Find Type(찾기 유형) 드롭다운 목록에서 VLAN 을 선택한 경우 사용할 수 있습니다.
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다. Find Type(찾기 유형) 드롭다운 목록에서 Port(포트)를 선택한 경우 이 옵션을 사용할 수 있습니다.

Find 버튼을 사용하여 입력된 정보를 기반으로 특정 항목을 찾습니다.
Show All 버튼을 눌러 모든 항목을 봅니다.
페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

MLD Snooping

MLD(Multicast Listener Discovery) Snooping 은 IPv4 의 IGMP Snooping 과 유사하게 사용되는 IPv6 기능입니다. 멀티캐스트 데이터를 요청하는 VLAN 에서 포트를 검색하는 데 사용됩니다. 선택한 VLAN 의 모든 포트를 멀티캐스트 트래픽으로 플러딩하는 대신, MLD Snooping 은 요청 포트와 멀티캐스트 트래픽의 소스에서 생성된 쿼리 및 보고서를 사용하여 이 데이터를 수신하려는 포트로만 멀티캐스트 데이터를 전달합니다.

MLD Snooping 은 엔드 노드와 MLD 라우터 간에 전송되는 MLD 제어 패킷의 레이어 3 부분을 검사하여 수행됩니다. 스위치가 이 경로가 멀티캐스트 트래픽을 요청하고 있음을 발견하면 직접 연결된 포트를 올바른 IPv6 멀티캐스트 테이블에 추가하고 해당 포트로 멀티캐스트 트래픽을 전달하는 프로세스를 시작합니다. 멀티캐스트 라우팅 테이블의 이 항목은 포트, VLAN ID 및 관련 멀티캐스트 IPv6 멀티캐스트 그룹 주소를 기록한 다음 이 포트를 활성 수신 포트로 간주합니다. 활성 수신 포트는 멀티캐스트 그룹 데이터를 수신하는 유일한 포트입니다.

MLD Control Messages

이러한 유형의 메시지는 MLD Snooping 을 사용하여 디바이스 간에 전송됩니다. 이러한 메시지는 모두 130, 131, 132 및 143 으로 표시된 4 개의 ICMPv6 패킷 헤더로 정의됩니다.

- Multicast Listener Query- IPv4 용 IGMPv2 Host Membership Query 와 유사하며 ICMPv6 패킷 헤더에 130 으로 레이블이 지정된 이 메시지는 라우터에서 전송하여 링크가 멀티캐스트 데이터를 요청하는지 묻습니다. 라우터에서 내보내는 MLD 쿼리 메시지에는 두 가지 유형이 있습니다. 모든 수신 포트로 멀티캐스트 데이터를 보낼 준비가 된 모든 멀티캐스트 주소를 광고하는 데 사용되는 General Query 와 준비된 특정 멀티캐스트 주소를 광고하는 데 사용되는 Multicast Specific query. 이 두 가지 유형의 메시지는 IPv6 헤더에 있는 멀티캐스트 대상 주소와 Multicast Listener Query Message 의 멀티캐스트 주소로 구분됩니다.
- Multicast Listener Report, Version 1 - IGMPv2 의 Host Membership Report 와 유사하고 ICMP 패킷 헤더에 131 로 레이블이 지정된 이 메시지는 수신 포트에서 Multicast Listener Query 메시지에 대한 응답으로 멀티캐스트 주소에서 멀티캐스트 데이터를 수신하는 데 관심이 있음을 나타내는 스위치로 전송됩니다.
- Multicast Listener Done - IGMPv2 의 Leave Group Message 와 유사하며 ICMPv6 패킷 헤더에서 132 로 레이블이 지정된 이 메시지는 특정 멀티캐스트 그룹 주소에서 멀티캐스트 데이터를 수신하는 데 더 이상 관심이 없음을 나타내는 멀티캐스트 수신 포트에서 전송되므로 이 주소의 멀티캐스트 데이터에 대해 "완료"되었음을 나타냅니다. 스위치에서 이 메시지를 수신하면 더 이상 특정 멀티캐스트 그룹 주소에서 이 수신 포트로 멀티캐스트 트래픽을 전달하지 않습니다.
- Multicast Listener Report, Version 2 - IGMPv3 의 Host Membership Report 와 유사하며 ICMP 패킷 헤더에 143 으로 레이블이 지정된 이 메시지는 수신 포트에서 Multicast Listener Query 메시지에 대한 응답으로 멀티캐스트 주소에서 멀티캐스트 데이터를 수신하는 데 관심이 있음을 나타내는 스위치로 전송됩니다.

MLD Snooping Settings

이 창은 MLD Snooping 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Settings 을 클릭합니다.

그림 5-52) MLD Snooping 설정 창

Global Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Global State	Global MLD Snooping 상태를 활성화하거나 비활성화하려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

VLAN Status Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
VID	1 에서 4094 까지의 VLAN ID 를 입력하고 VLAN 에서 MLD Snooping 을 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

MLD Snooping Table 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
VID	1 에서 4094 사이의 VLAN ID 를 입력합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Show All 버튼을 클릭하여 모든 항목을 봅니다.

Show Detail 버튼을 클릭하여 특정 VLAN 의 세부 정보를 확인합니다.

Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Show Detail 버튼을 클릭하면 다음과 같은 창이 나타납니다.

그림 5-53 MLD Snooping 설정(세부 정보 표시) 창

이 창에는 MLD Snooping VLAN 에 대한 세부 정보가 표시됩니다.
Modify 버튼을 클릭하여 다음 창에서 정보를 편집합니다.

MLD Snooping Settings 창에서 Modify 또는 Edit 버튼을 클릭하면 다음과 같은 창이 나타납니다.

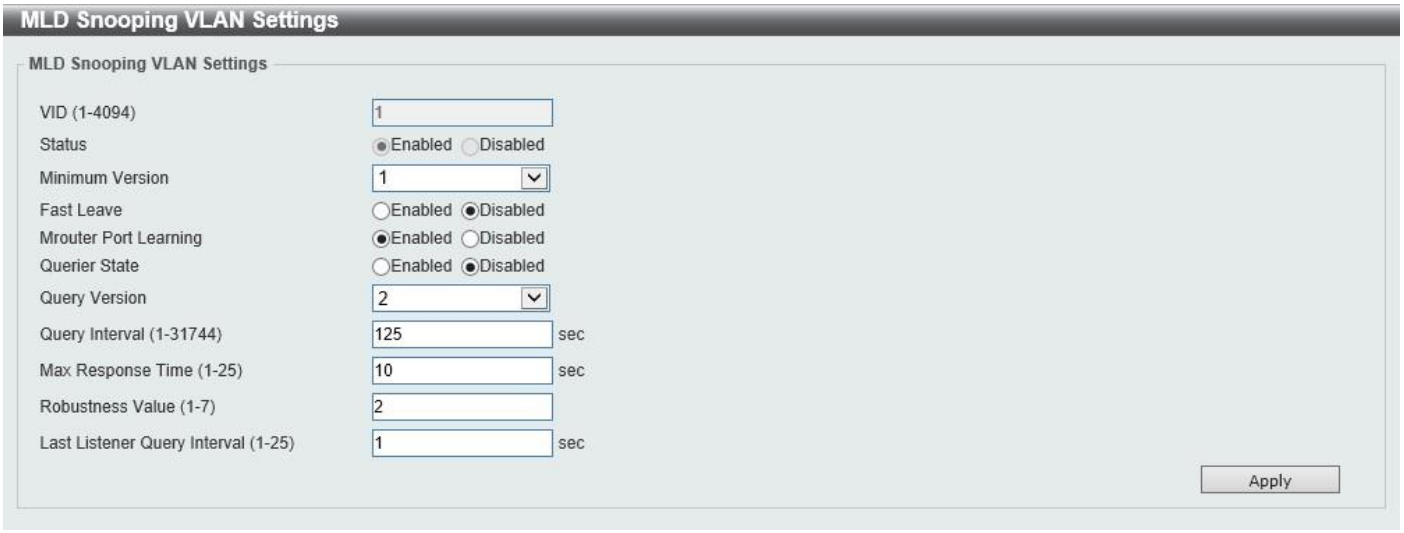

그림 5-54) MLD Snooping 설정(Modify, Edit) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Minimum Version	VLAN 에서 허용되는 MLD 호스트의 최소 버전을 선택합니다. 선택할 수 있는 옵션은 1 과 2 입니다.
Fast Leave	MLD Snooping Fast Leave 기능을 활성화하거나 비활성화하려면 이 옵션을 선택합니다. 활성화된 경우, 시스템이 마지막 멤버로부터 MLD done 메시지를 수신하면 멤버십이 즉시 제거됩니다.
Mrouter Port Learning	Mrouter 포트 학습을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
Querier State	쿼리 발생기 상태를 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
Query Version	MLD Snooping 쿼리 발생기에서 보낸 일반 쿼리 패킷 버전을 선택합니다. 선택할 수 있는 옵션은 1 과 2 입니다.
Query Interval	MLD Snooping 쿼리 발생기가 MLD 일반 쿼리 메시지를 주기적으로 전송하는 간격을 입력합니다. 범위는 1 에서 31744 사이입니다.
Max Response Time	MLD Snooping 쿼리에 광고된 최대 응답 시간(초)을 입력합니다. 범위는 1 에서 25 사이입니다.
Robustness Value	MLD Snooping 에 사용되는 견고성 변수를 입력합니다. 범위는 1 에서 7 사이입니다.
Last Listener Query Interval	MLD Snooping 쿼리 발생기가 MLD 그룹별 또는 그룹 소스별(채널) 쿼리 메시지를 보내는 간격을 입력합니다. 범위는 1 에서 25 사이입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

MLD Snooping Groups Settings

이 창은 MLD Snooping 정적 그룹을 표시 및 구성하고 MLD Snooping 그룹을 보는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Groups Settings 을 클릭합니다.

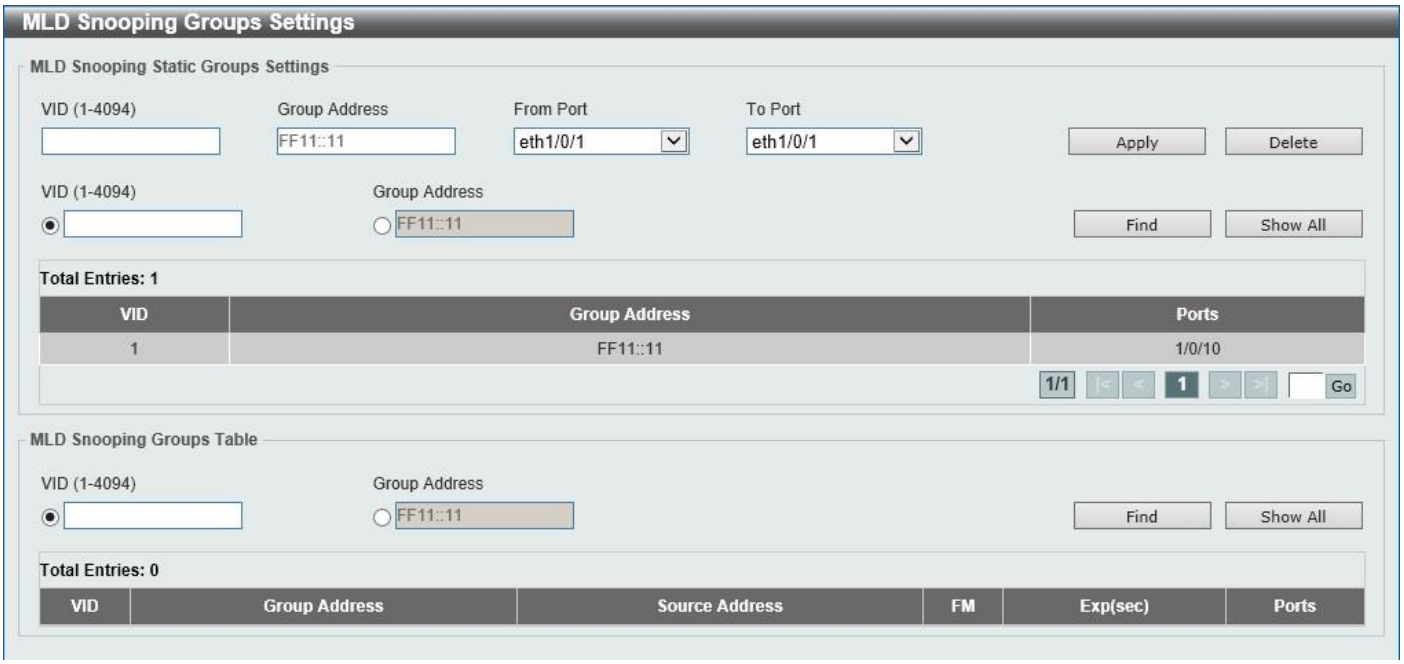

그림 5-55 MLD Snooping 그룹 설정 창

MLD Snooping Static Groups Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
VID	여기에 멀티캐스트 그룹의 VLAN ID 를 입력합니다. 범위는 1 에서 4094 사이입니다.
Group Address	여기에 IPv6 멀티캐스트 그룹 주소를 입력합니다.
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
VID	라디오 버튼을 클릭하고 멀티캐스트 그룹의 VLAN ID 를 입력합니다. 범위는 1 에서 4094 사이입니다.
Group Address	라디오 버튼을 클릭하고 IPv6 멀티캐스트 그룹 주소를 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Show All 버튼을 클릭하여 모든 항목을 봅니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

MLD Snooping 그룹 테이블에 대해 구성하거나 표시할 수 있는 필드는 다음과 같습니다.

Parameter	Description
VID	라디오 버튼을 클릭하고 멀티캐스트 그룹의 VLAN ID 를 입력합니다. 범위는 1 에서 4094 사이입니다.
그룹 주소	라디오 버튼을 클릭하고 IPv6 멀티캐스트 그룹 주소를 입력합니다.
에프엠	필터 모드를 표시합니다. 다음이 표시될 수 있습니다. • EX (제외) - 필터 모드는 제외입니다. • IN (포함) - 필터 모드는 포함입니다.
경험치 (초)	항목이 만료되기까지 남은 시간(초)을 표시합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다. Show All 버튼을 클릭하여 모든 항목을 봅니다.

MLD Snooping Mrouter Settings

이 창은 지정된 Interface 를 라우터 포트로 표시하고 구성하는 데 사용되거나 스위치의 VLAN Interface 에서 IPv6 멀티캐스트 라우터 포트로 금지됩니다.

다음 창을 보려면 아래와 같이 L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings 를 클릭합니다.

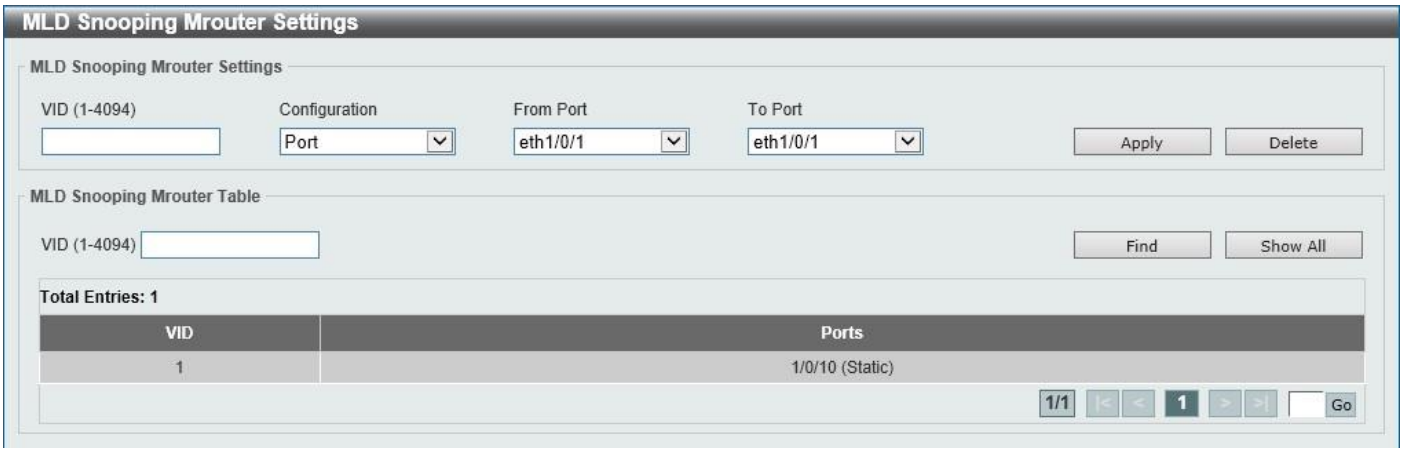

그림 5-56 MLD Snooping 라우터 설정 창

MLD Snooping Mrouter Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
VID	1 에서 4094 사이의 VLAN ID 를 입력합니다.
Configuration	포트 구성을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Port(포트) - 구성된 포트가 멀티캐스트 지원 라우터에 연결되도록 하려면 선택합니다. • Forbidden Port(금지된 포트) - 구성된 포트가 멀티캐스트 지원 라우터에 연결되지 않도록 하려면 선택합니다. • Learn pimv6 - 멀티캐스트 라우터 포트의 동적 학습을 활성화하려면 선택합니다.
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

MLD Snooping Mrouter Table 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
VID	1 에서 4094 사이의 VLAN ID 를 입력합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Show All 버튼을 클릭하여 모든 항목을 봅니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

MLD Snooping Statistics Settings

이 창은 MLD Snooping 관련 통계를 보고 지우는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings 을 클릭합니다.

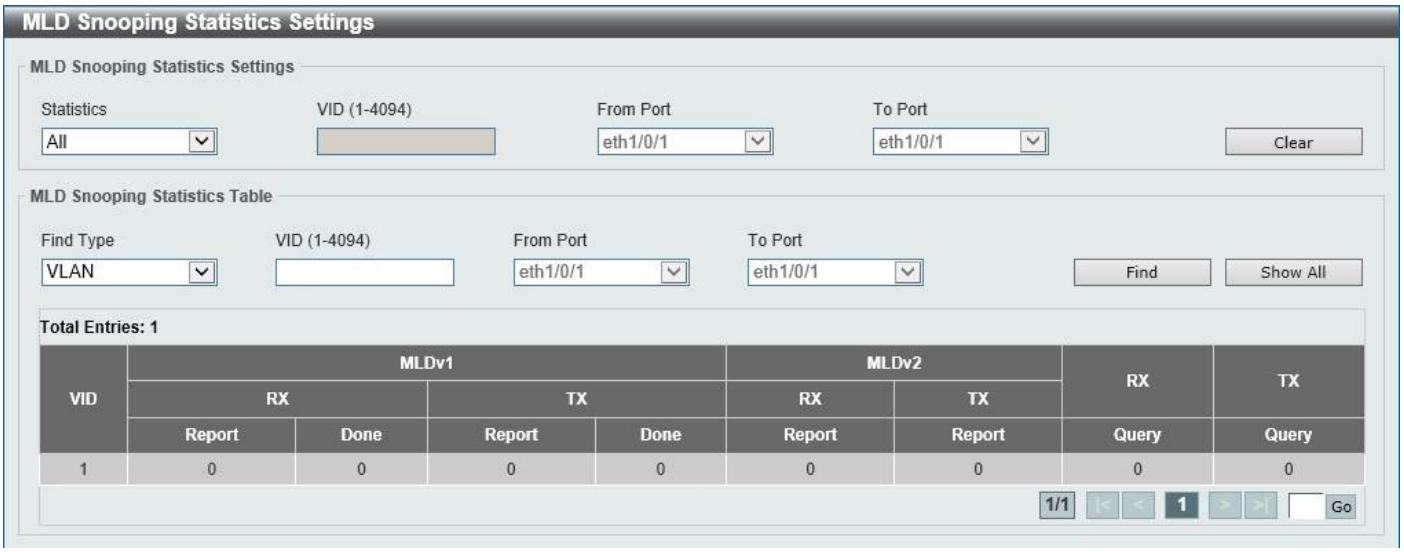

그림 5-57) MLD Snooping 통계 설정 창

MLD Snooping 통계 설정에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Statistics	여기에서 Interface 를 선택합니다. 선택할 수 있는 옵션은 모두, VLAN 및 포트입니다.
VID	1 에서 4094 사이의 VLAN ID 를 입력합니다. Statistics(통계) 드롭다운 목록에서 VLAN 을 선택한 경우 사용할 수 있습니다.
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다. Statistics(통계) 드롭다운 목록에서 Port(포트)를 선택한 경우 사용할 수 있습니다.

Clear 버튼을 클릭하여 MLD Snooping 관련 통계를 지웁니다.

MLD Snooping 통계 테이블에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
유형 찾기	Interface 유형을 선택합니다. 선택할 수 있는 옵션은 VLAN 및 포트입니다.
VID	1 에서 4094 사이의 VLAN ID 를 입력합니다. Find Type(찾기 유형) 드롭다운 목록에서 VLAN 을 선택한 경우 사용할 수 있습니다.
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다. Find Type(찾기 유형) 드롭다운 목록에서 Port(포트)를 선택한 경우 이 옵션을 사용할 수 있습니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Show All 버튼을 클릭하여 모든 항목을 봅니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Multicast Filtering Mode

이 창은 레이어 2 멀티캐스트 필터링 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > L2 Multicast Control > Multicast Filtering Mode 를 클릭합니다.

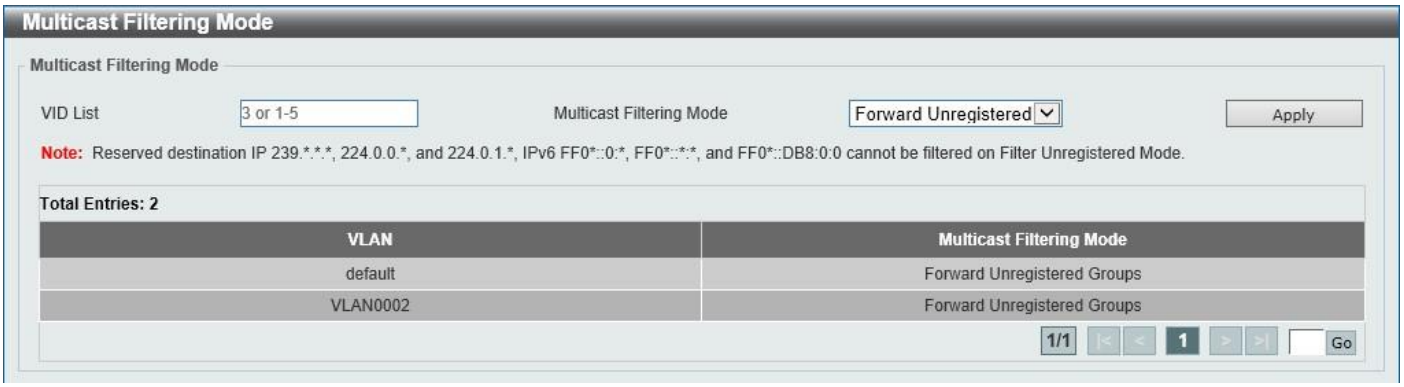

그림 5-58) Multicast Filtering Mode 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
VID List	여기에 이 컨피그레이션에 사용할 VLAN ID 목록을 입력합니다.
Multicast Filter Mode	여기에서 멀티캐스트 필터 모드를 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Forward Unregistered - 등록된 멀티캐스트 패킷이 전달 테이블을 기반으로 전달되고 등록되지 않은 모든 멀티캐스트 패킷이 VLAN 도메인을 기반으로 플러딩되도록 지정합니다. • Forward All(모두 전달) - 모든 멀티캐스트 패킷이 VLAN 도메인을 기반으로 플러딩되도록 지정합니다. • Filter Unregistered(등록되지 않은 필터) - 등록된 패킷이 전달 테이블을 기반으로 전달되고 등록되지 않은 모든 멀티캐스트 패킷이 필터링되도록 지정합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

LLDP

LLDP Global Settings

이 창은 global LLDP 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > LLDP > LLDP Global Settings 를 클릭합니다.

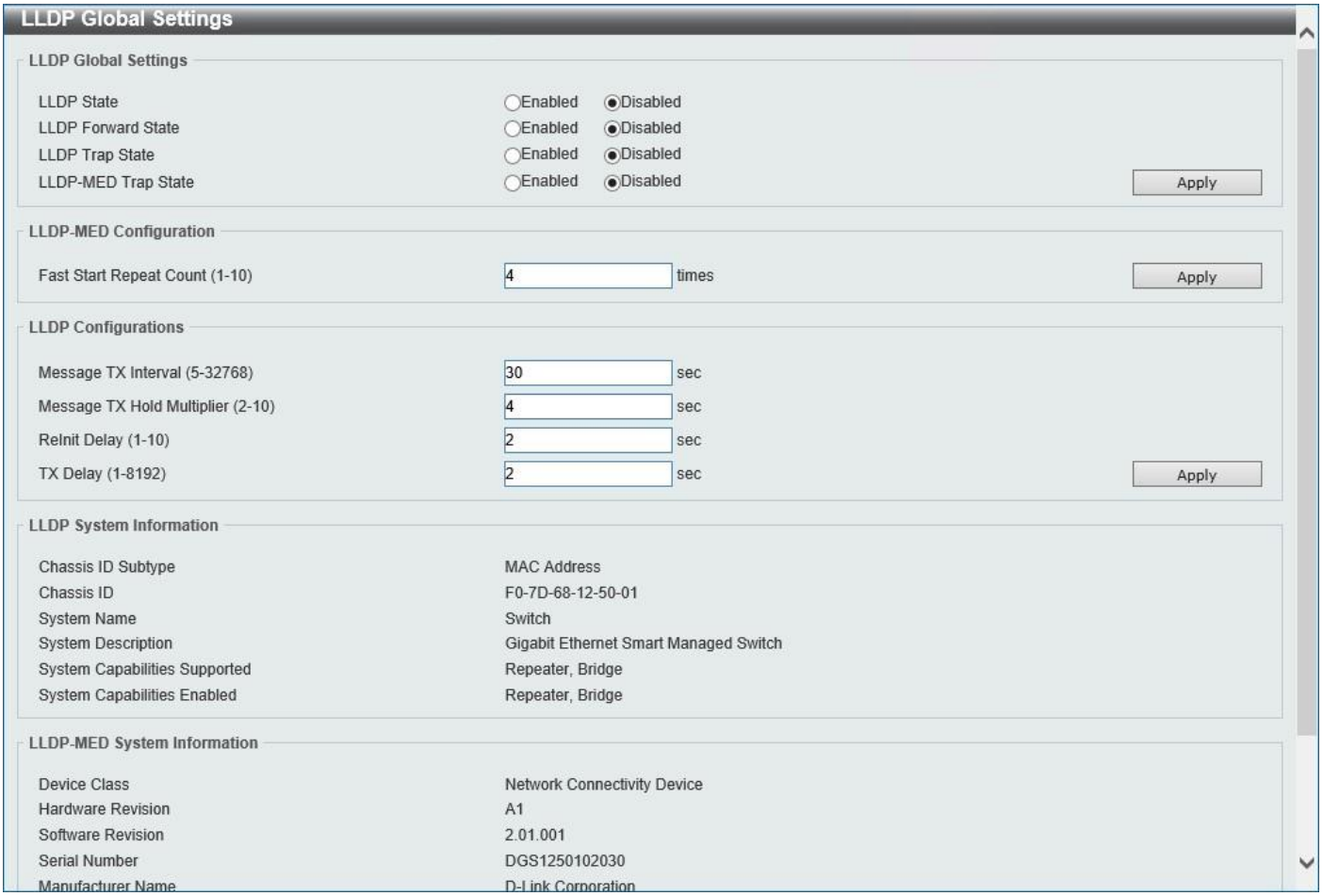

그림 5-59) LLDP Global Settings 창

LLDP Global Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
LLDP State	LLDP 기능을 활성화하거나 비활성화하려면 이 옵션을 선택합니다. 기본적으로 이 기능은 비활성화되어 있습니다.
LLDP Forward State	LLDP 전달 상태를 활성화하거나 비활성화하려면 이 옵션을 선택합니다. LLDP State(LLDP 상태)가 비활성화되고 LLDP Forward Sate(LLDP 전달 상태)가 활성화된 경우 수신된 LLDPDU 패킷이 전달됩니다.
LLDP Trap State	LLDP 트랩 상태를 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
LLDP-MED Trap State	LLDP-MED 트랩 상태를 활성화하거나 비활성화하려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

LLDP-MED 설정에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Fast Start Repeat Count	LLDP-MED 빠른 시작 반복 횟수 값을 입력합니다. 이 값은 1 에서 10 사이여야 합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

LLDP Configurations 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Message TX Interval	각 물리적 Interface 에서 LLDP 광고의 연속 전송 사이의 간격을 입력합니다. 범위는 5 초에서 32768 초 사이입니다.
Message TX Hold Multiplier	LLDPDU 의 TTL 값을 계산하는 데 사용된 LLDPDUs 전송 간격의 승수를 입력합니다. 이 값은 2 에서 10 사이여야 합니다.
ReInit Delay	Interface 에서 LLDP 초기화를 위한 지연 값을 입력합니다. 이 값은 1 초에서 10 초 사이여야 합니다.
TX Delay	Interface 에서 연속적인 LLDPDU 를 전송하기 위한 지연 값을 입력합니다. 유효한 값은 1 초에서 8192 초 사이이며 전송 간격 타이머의 1/4 보다 크지 않아야 합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

LLDP Port Settings

이 창은 LLDP 포트 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > LLDP > LLDP Port Settings 을 클릭합니다.

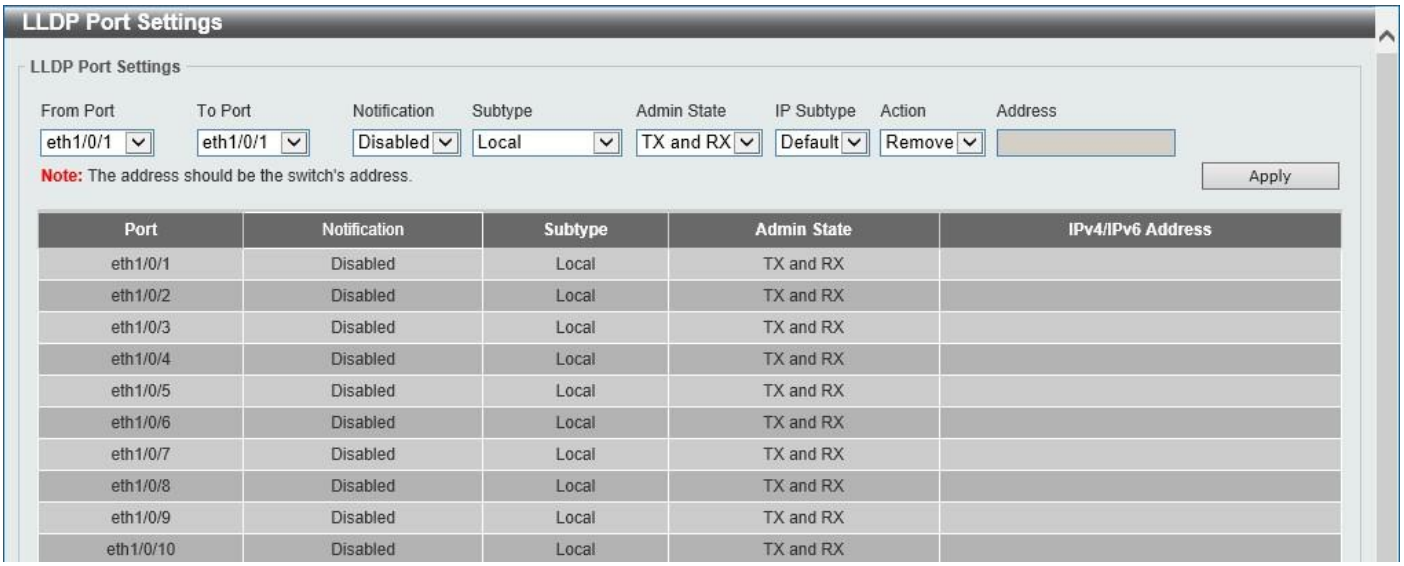

그림 5-60 LLDP 포트 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
Notification	여기에서 알림 기능을 활성화하거나 비활성화하려면 선택합니다.
Subtype	LLDP TLV 의 하위 유형을 선택합니다. 선택할 수 있는 옵션은 MAC 주소 및 로컬입니다.
Admin State	로컬 LLDP 에이전트를 선택하고 포트에서 LLDP 프레임을 보내고 받을 수 있도록 허용합니다. 선택할 수 있는 옵션은 다음과 같습니다. • TX - 로컬 LLDP 에이전트는 LLDP 프레임만 전송할 수 있습니다. • RX - 로컬 LLDP 에이전트는 LLDP 프레임만 수신할 수 있습니다. • TX 및 RX - 로컬 LLDP 에이전트는 LLDP 프레임을 전송하고 수신할 수 있습니다. 이것이 기본 옵션입니다.

	Disabled(비활성화됨) - 로컬 LLDP 에이전트는 LLDP 프레임을 전송하거나 수신할 수 없습니다.
IP Subtype	전송할 IP Address 정보의 유형을 선택합니다. 선택할 수 있는 옵션은 기본, IPv4 및 IPv6 입니다.
Action	여기에서 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 제거 및 추가입니다.
Address	전송할 IP Address 를 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

참고: 여기에 입력한 IPv4 또는 IPv6 주소는 기존 LLDP 관리 IP Address 여야 합니다.

LLDP Management Address List

이 창은 LLDP 관리 주소 목록을 보는 데 사용됩니다.

다음 창을 보려면 아래와 L2 Features > LLDP > LLDP Management Address List 를 클릭합니다.

그림 5-61) LLDP 관리 주소 목록 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Subtype	하위 유형을 선택합니다. 선택할 수 있는 옵션은 모두, IPv4 및 IPv6 입니다. IPv4 옵션을 선택한 후 제공된 공간에 IPv4 주소를 입력합니다. IPv6 옵션을 선택한 후 제공된 공간에 IPv6 주소를 입력합니다.

Find 버튼을 클릭하여 선택한 항목에 따라 특정 항목을 찾습니다.

LLDP Basic TLVs Settings

TLV(Type-Length-Value) 필드를 사용하면 LLDP 패킷 내에서 특정 정보를 전송할 수 있습니다. 이 창은 기본 TLV 설정을 구성하는 데 사용됩니다. 스위치의 활성 LLDP 포트에는 항상 아웃바운드 광고에 필수 데이터가 포함됩니다. 아웃바운드 LLDP 알림에서 이러한 데이터 유형 중 하나 이상을 제외하도록 구성할 수 있는 4 가지 선택적 데이터 유형이 있습니다. 필수 데이터 유형에는 LLDPDU TLV 끝, 섀시 ID TLV, 포트 ID TLV 및 TTL TLV 의 4 가지 기본 TLV 가 포함됩니다. 필수 데이터 형식은 비활성화할 수 없습니다. 선택적으로 선택할 수 있는 4 가지 데이터 유형도 있습니다. 여기에는 Port Description(포트 설명), System Name(시스템 이름), System Description(시스템 설명) 및 System Capability(시스템 기능)가 포함됩니다.

다음 창을 보려면 아래와 같이 L2 Features > LLDP > LLDP Basic TLVs Settings 을 클릭합니다.

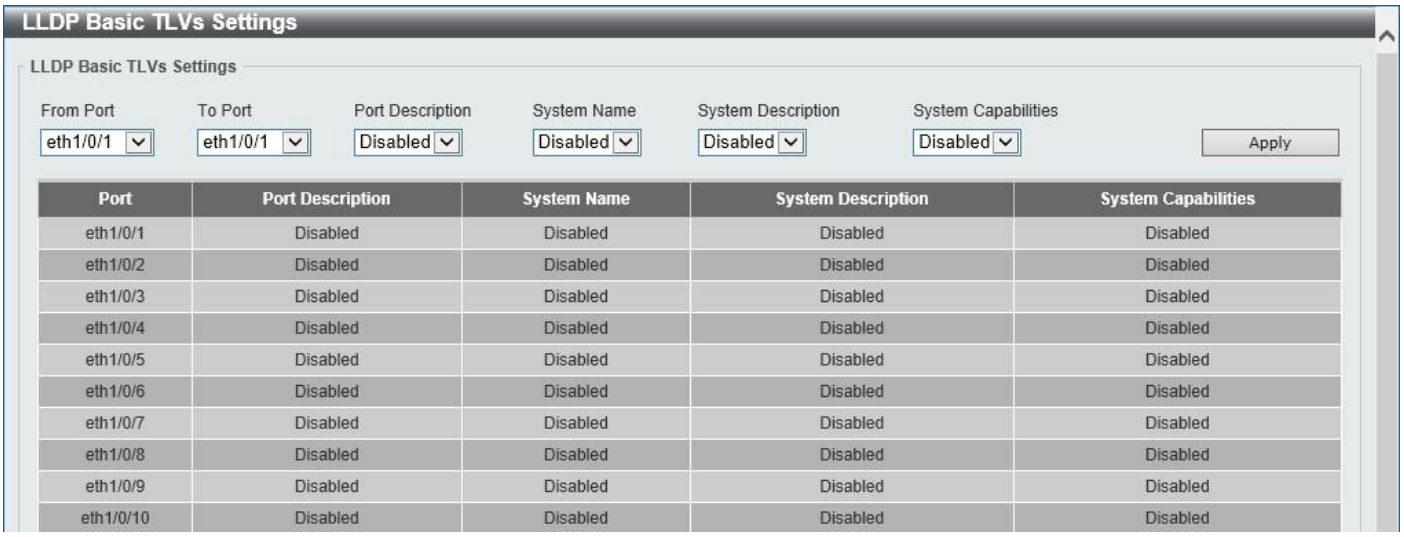

그림 5-62) LLDP 기본 TLV 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
Port Description	Port Description(포트 설명) 옵션을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
System Name	시스템 이름 옵션을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
System Description	시스템 설명 옵션을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
System Capabilities	시스템 기능 옵션을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

LLDP Dot1 TLVs Settings

LLDP Dot1 TLVs Settings 페이지는 IEEE 802.1 조직적으로 고유한 포트 VLAN ID TLV 에 대한 아웃바운드 LLDP 광고를 활성화하거나 비활성화하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > LLDP > LLDP Dot1 TLVs Settings 을 클릭합니다.

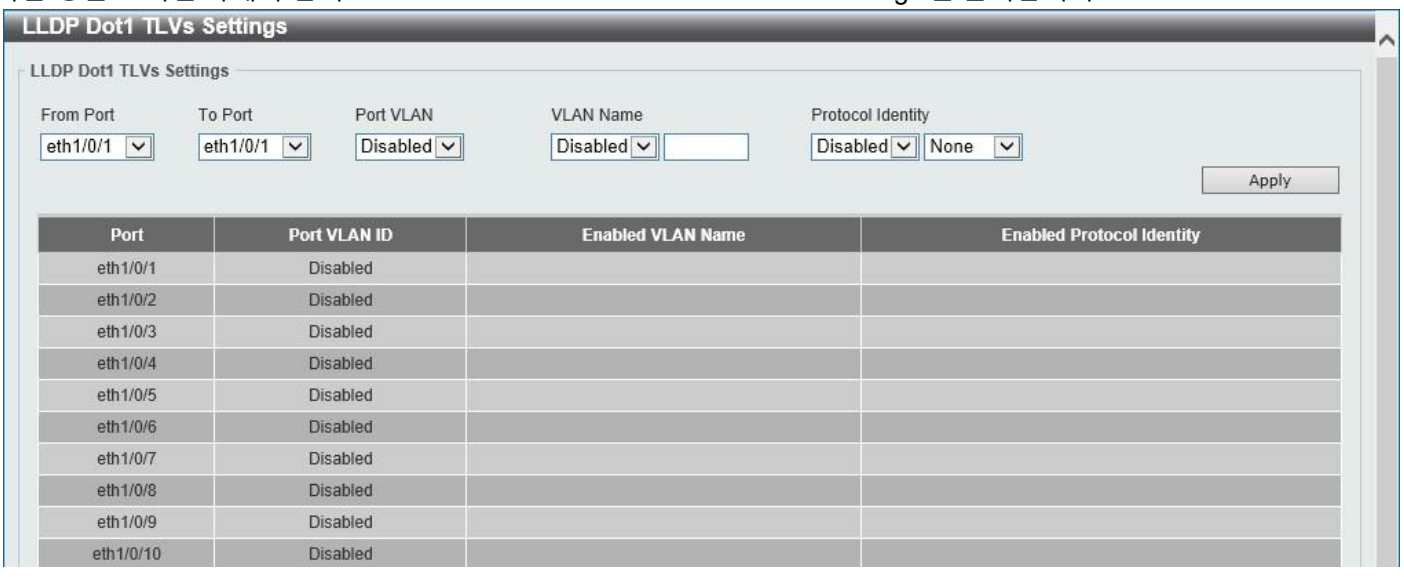

그림 5-63 LLDP Dot1 TLV 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
Port VLAN	포트 VLAN ID TLV 전송을 활성화하거나 비활성화하려면 이 옵션을 선택합니다. 포트 VLAN ID TLV 는 VLAN 브리지 포트가 태그가 지정되지 않은 프레임 또는 우선순위 태그가 지정된 프레임과 연결될 포트 VLAN ID(PVID)를 광고할 수 있도록 하는 선택적 고정 길이 TLV 입니다.
VLAN Name	VLAN 이름 TLV 전송을 활성화하거나 비활성화하려면 이 옵션을 선택합니다. VLAN 이름 TLV 에 VLAN 의 ID 를 입력합니다.
Protocol Identity	프로토콜 ID TLV 및 프로토콜 이름 전송을 활성화하거나 비활성화하려면 이 옵션을 선택합니다. 선택할 수 있는 프로토콜 이름 옵션은 None, EAPOL, LACP, STP 및 All 입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

LLDP Dot3 TLVs Settings

LLDP Dot3 TLVs Settings(LLDP Dot3 TLV 설정) 페이지는 IEEE 802.3 조직적으로 고유한 TLV 에 대한 아웃바운드 LLDP 광고를 활성화하거나 비활성화하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > LLDP > LLDP Dot3 TLVs Settings 을 클릭합니다.

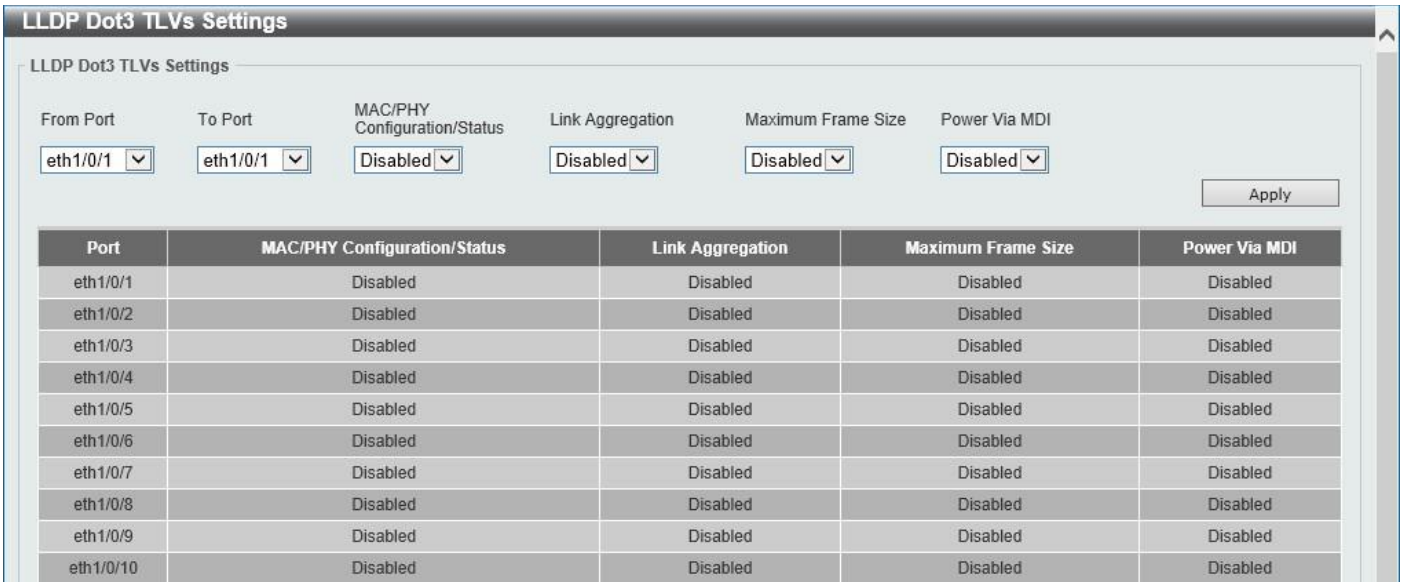

그림 5-64 LLDP Dot3 TLV 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
MAC/PHY Configuration/Status	전송할 MAC/PHY 구성/상태 TLV 를 활성화하거나 비활성화하려면 이 옵션을 선택합니다. MAC/PHY 구성/상태 TLV 는 (1) 전송 IEEE 802.3 LAN 노드의 이중 및 비트 전송률 기능과 (2) 전송 IEEE 802.3 LAN 노드의 현재 이중 및 비트 전송률 설정을 식별하는 선택적 TLV 입니다.
Link Aggregation	전송할 Link Aggregation TLV 를 활성화하거나 비활성화하려면 이 옵션을 선택합니다. 링크 어그리게이션 TLV 는 다음과 같은 정보를 포함하고 있습니다. 링크를 집계할 수 있는지 여부, 링크가 현재 어그리게이션에 있는지 여부, 포트의 집계된 포트 채널 ID 입니다. 포트가 집계되지 않은 경우 ID 는 0 입니다.

Maximum Frame Size	전송할 최대 프레임 크기 TLV 를 활성화하거나 비활성화하려면 이 옵션을 선택합니다. Maximum Frame Size TLV 는 구현된 MAC 및 PHY 의 최대 프레임 크기 기능을 나타냅니다.
Power Via MDI	MDI TLV 를 통해 전송할 전원을 활성화하거나 비활성화하려면 이 옵션을 선택합니다. IEEE 802.3 PMD 구현을 사용하면 연결된 전원이 공급되지 않는 시스템에 대한 링크를 통해 전원을 공급할 수 있습니다. Power Via MDI TLV 를 사용하면 네트워크 관리에서 송신 IEEE 802.3 LAN 스테이션의 MDI 전원 지원 기능을 광고하고 검색할 수 있습니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

LLDP-MED Port Settings

LLDP-MED Port Settings 페이지는 LLDP-MED TLV 에 대한 아웃바운드 LLDP 광고를 활성화하거나 비활성화하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > LLDP > LLDP-MED Port Settings 을 클릭합니다.

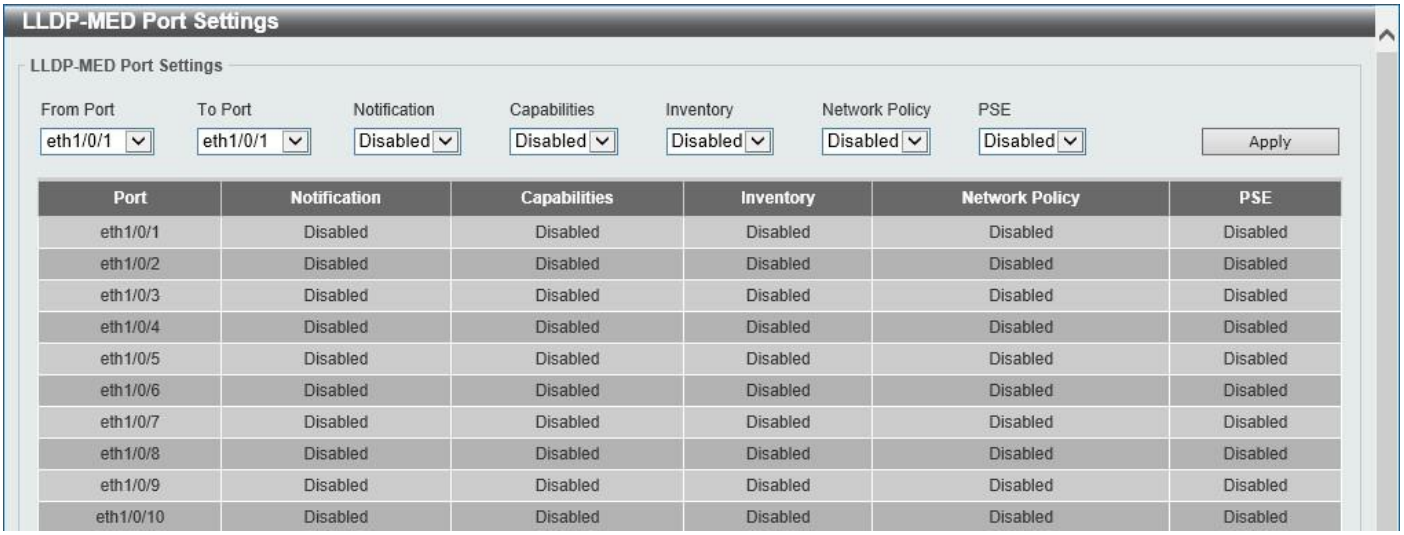

그림 5-65) LLDP-MED 포트 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
Notification	LLDP-MED 알림 TLV 전송을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
Capabilities	LLDP-MED 기능 TLV 전송을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
Inventory	LLDP-MED 인벤토리 관리 TLV 전송을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
Network Policy	LLDP-MED 네트워크 정책 TLV 전송을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.
PSE	로컬 디바이스가 PSE 디바이스 또는 PD 디바이스인 경우 MDI TLV 를 통해 LLDP-MED 확장 전력 전송을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

LLDP Statistics Information

이 창은 인접 디바이스 탐지 활동, LLDP 통계 및 스위치의 개별 포트에 대한 설정을 보는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > LLDP > LLDP Statistics Information 을 클릭합니다.

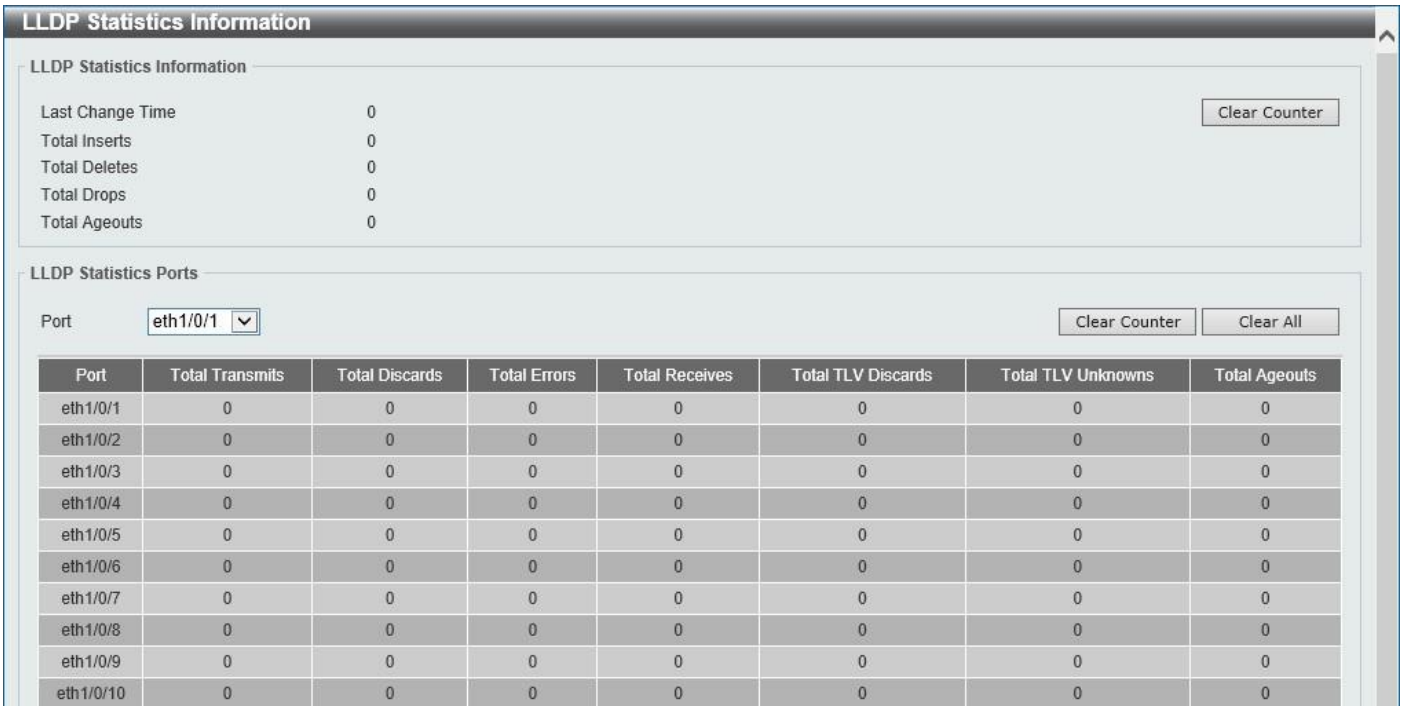

그림 5-66) LLDP 통계 정보 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Port	여기에서 사용할 포트 번호를 선택합니다.

Clear Counter 버튼을 클릭하여 표시된 통계에 대한 카운터 정보를 지웁니다.

Clear All 버튼을 클릭하여 표시된 모든 카운터 정보를 지웁니다.

LLDP Local Port Information

이 창은 아웃바운드 LLDP 광고를 채우는 데 현재 사용할 수 있는 정보를 표시하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L2 Features > LLDP > LLDP Local Port Information 을 클릭합니다.

그림 5-67) LLDP 로컬 포트 정보 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Port	표시될 포트 번호를 선택합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Show Detail 버튼을 클릭하면 특정 포트의 자세한 정보를 볼 수 있습니다.

Show Detail 버튼을 클릭하면 다음과 같은 창이 나타납니다.

그림 5-68 LLDP 로컬 포트 정보(세부 정보 표시) 창

MAC/PHY 구성/상태 등에 대한 자세한 내용을 보려면 Show Detail 하이퍼링크를 클릭합니다.

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

Show Detail 하이퍼링크를 클릭하면 창 아래쪽에 새 섹션이 나타납니다.

그림 5-69 LLDP Local Port Information (Show Detail) 창

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

LLDP Neighbor Port Information

이 창은 인접 스위치에서 학습한 LLDP 정보를 표시하는 데 사용됩니다. 스위치는 원격 스테이션에서 패킷을 수신하지만 정보를 로컬에 저장할 수 있습니다.

다음 창을 보려면 아래와 같이 L2 Features > LLDP > LLDP Neighbor Port Information 을 클릭합니다.

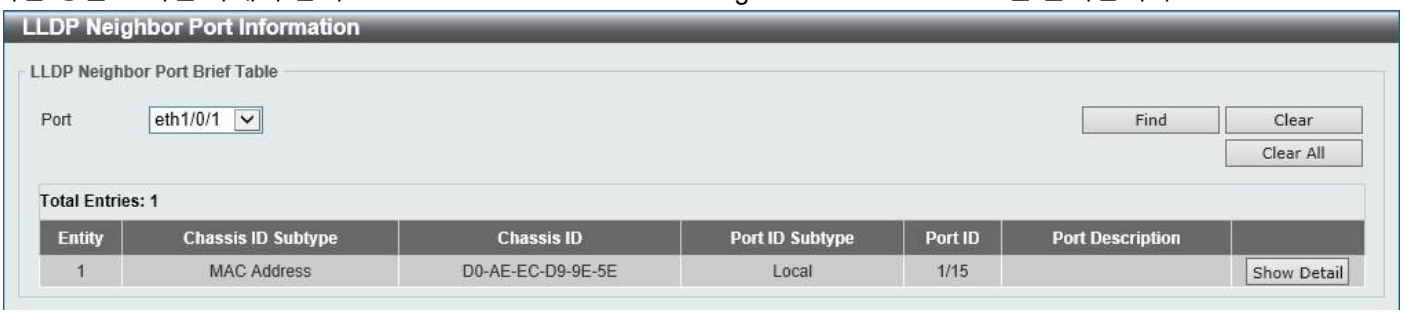

그림 5-70 LLDP Neighbor Port Information 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Port	표시될 포트 번호를 선택합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Clear 버튼을 클릭하여 특정 포트 정보를 지웁니다.

Clear All 버튼을 클릭하여 표시된 모든 포트 정보를 지웁니다.

Show Detail 버튼을 클릭하면 특정 포트의 자세한 정보를 볼 수 있습니다.

Show Detail 버튼을 클릭하면 다음과 같은 창이 나타납니다.

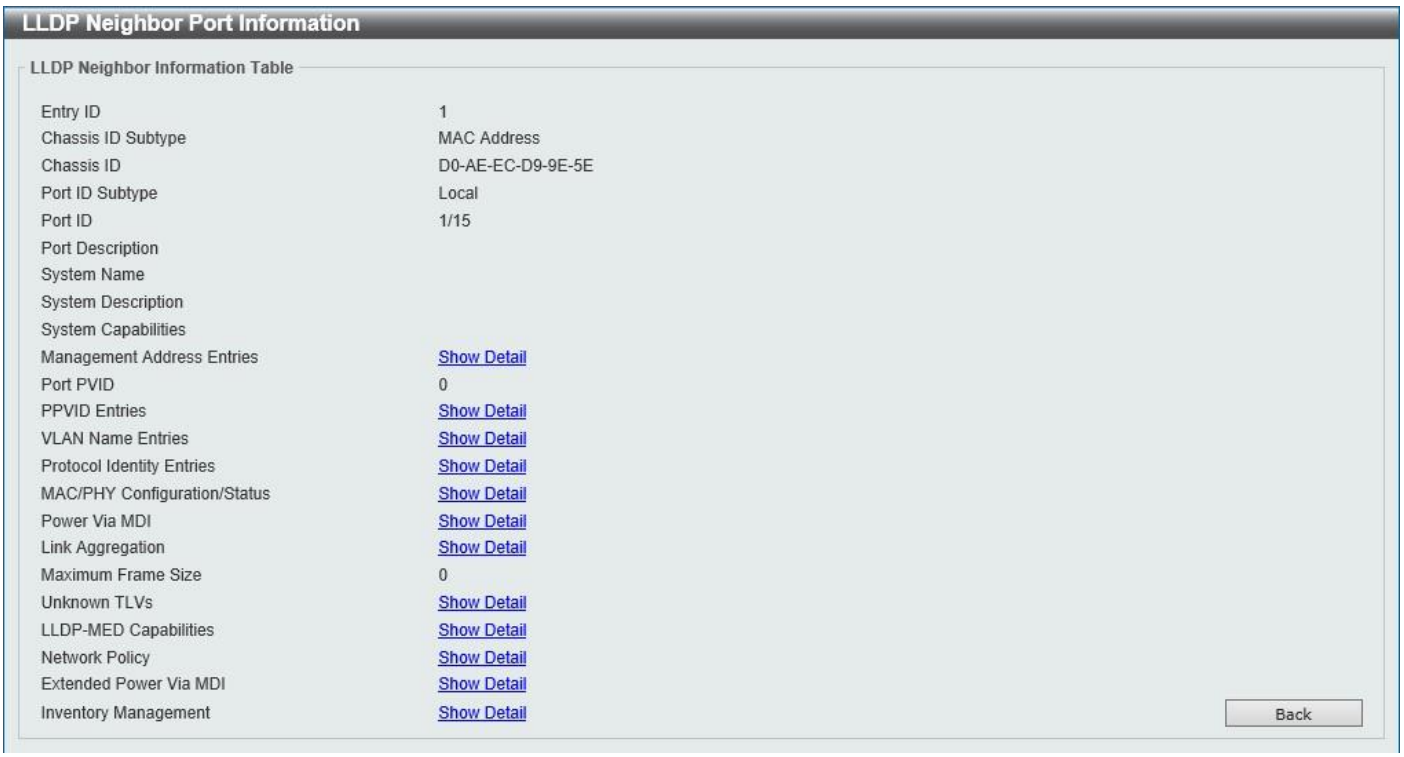

그림 5-71 LLDP Neighbor Port Information (Show Detail) 창

MAC/PHY 구성/상태 등에 대한 자세한 내용을 보려면 Show Detail 하이퍼링크를 클릭합니다.

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

Show Detail 하이퍼링크를 클릭하면 창 아래쪽에 새 섹션이 나타납니다.

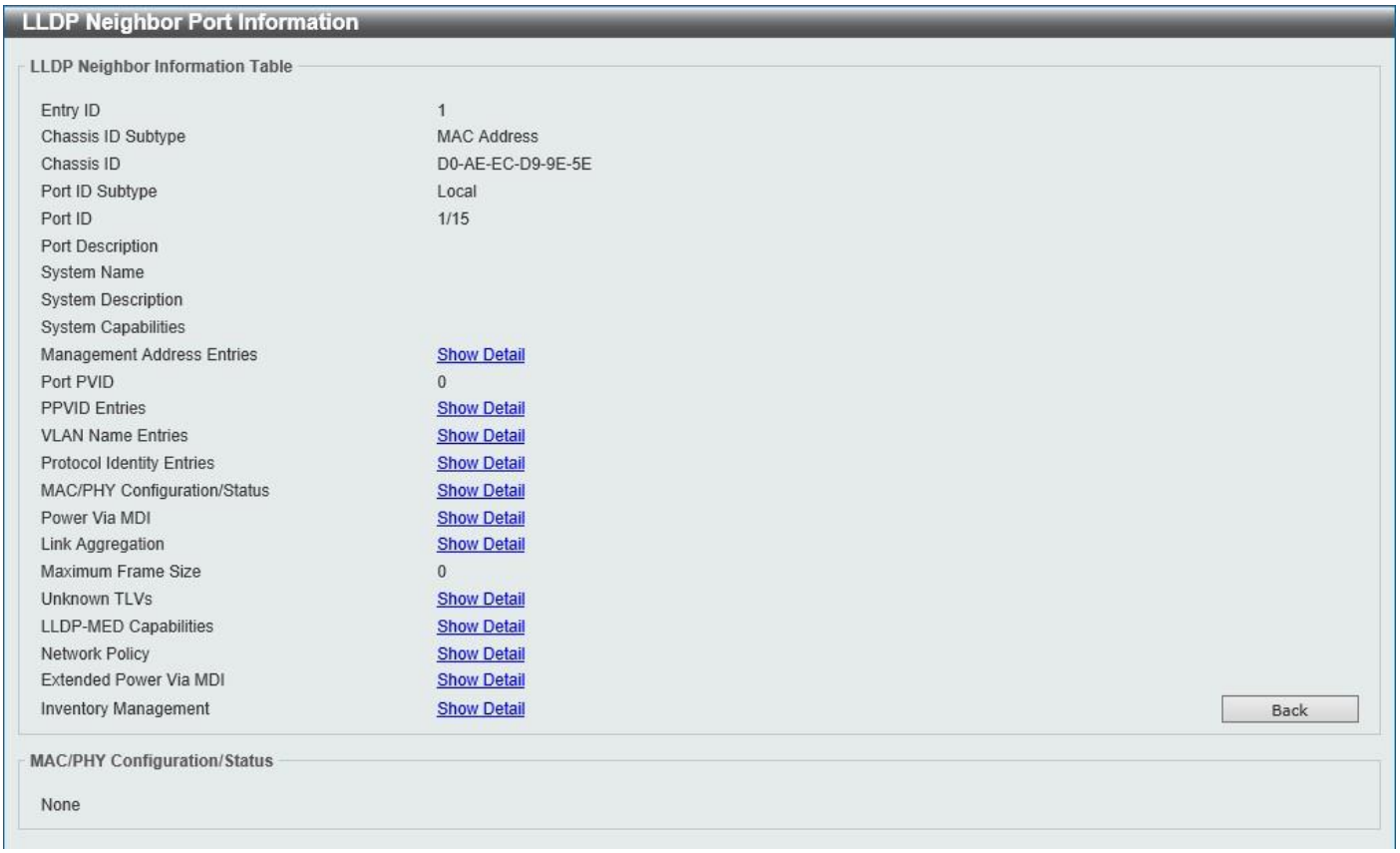

그림 5-72 LLDP Neighbor Port Information (Show Detail) 창

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

5. Layer 3 Features

ARP
Gratuitous ARP
IPv6 Neighbor
Interface
IPv4 Static/Default Route
IPv4 Route Table
IPv6 Static/Default Route
IPv6 Route Table
IP Multicast Routing Protocol

ARP

ARP Aging Time

이 창은 ARP aging time 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L3 Features > ARP > ARP Aging Time 을 클릭합니다.

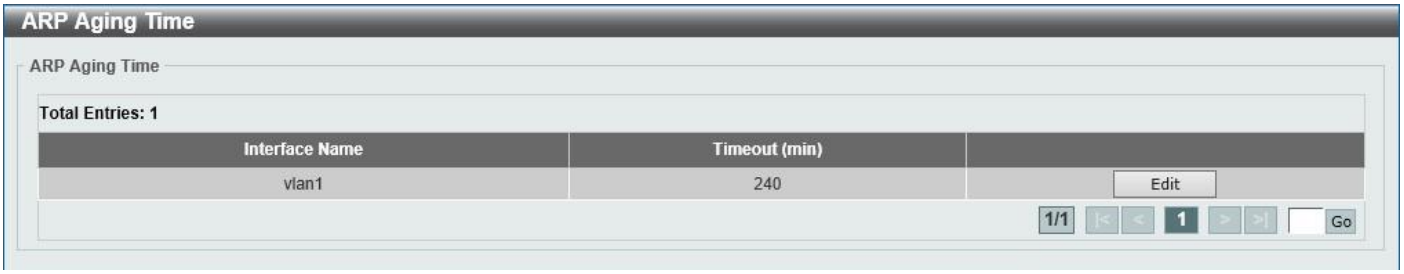

그림 6-1 ARP 에이징 시간 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Timeout	Edit 버튼을 클릭한 후 여기에 ARP 에이징 타임아웃 값을 입력합니다. 범위는 0 에서 65535 사이입니다. 이 값이 0 이면 항목이 시간 초과되지 않습니다.

Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Static ARP

이 창은 정적 ARP 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L3 Features > ARP > Static ARP 를 클릭합니다.

그림 6-2 정적 ARP 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
IP Address	여기에 MAC 주소와 연결할 IP Address 를 입력합니다.
Hardware Address	여기에 IP Address 와 연결할 MAC 주소를 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.
Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.
Delete 버튼을 클릭하여 특정 항목을 제거합니다.
페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

ARP Table

이 창은 ARP Table 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L3 Features > ARP > ARP Table 을 클릭합니다.

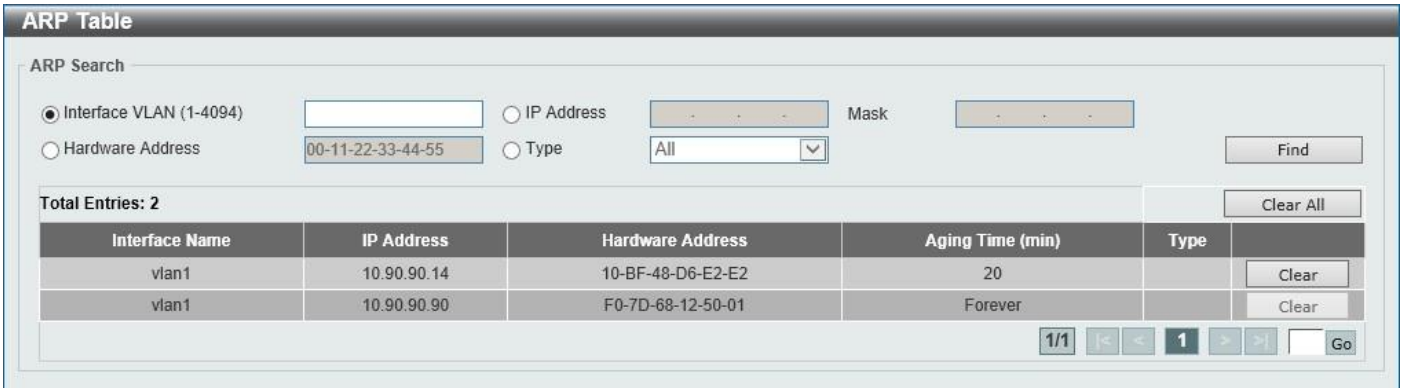

그림 6-3 ARP 테이블 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Interface VLAN	여기에 사용된 Interface VLAN ID 를 입력합니다. 이 값은 1 에서 4094 사이여야 합니다.
IP Address	여기에 표시할 IP Address 를 선택하고 입력합니다.
Mask	IP Address 옵션을 선택한 후 여기에 IP Address 의 마스크 주소를 입력합니다.
Hardware Address	여기에 표시할 MAC 주소를 선택하고 입력합니다.
Type	여기에서 유형 옵션을 선택합니다. 선택할 수 있는 옵션은 All (모두) 및 Dynamic(동적)입니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.
Clear All 버튼을 클릭하여 모든 동적 ARP 캐시를 지웁니다.
Clear 버튼을 클릭하여 특정 항목과 연결된 동적 ARP 캐시를 지웁니다.
페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Gratuitous ARP

이 창은 무상 ARP 설정을 표시하고 구성하는 데 사용됩니다. 무상 ARP 요청 패킷은 소스 및 대상 IP Address 가 모두 전송 디바이스의 IP Address 로 설정되고 대상 MAC 주소가 브로드캐스트 주소인 ARP 요청 패킷입니다.
일반적으로 디바이스는 무상 ARP 요청 패킷을 사용하여 IP Address 가 다른 호스트에 의해 중복되는지 여부를 검색하거나 Interface 에 연결된 호스트의 ARP 캐시 엔트리를 미리 로드하거나 재구성합니다.

다음 창을 보려면 아래와 같이 L3 Features > Gratuitous ARP 를 클릭합니다.

그림 6-4) 무상 ARP 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Gratuitous ARP Trap State	여기에서 무상 ARP 기능 트랩 상태를 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

IPv6 Neighbor

이 창은 IPv6 Neighbor 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L3 Features > IPv6 Neighbor 를 클릭합니다.

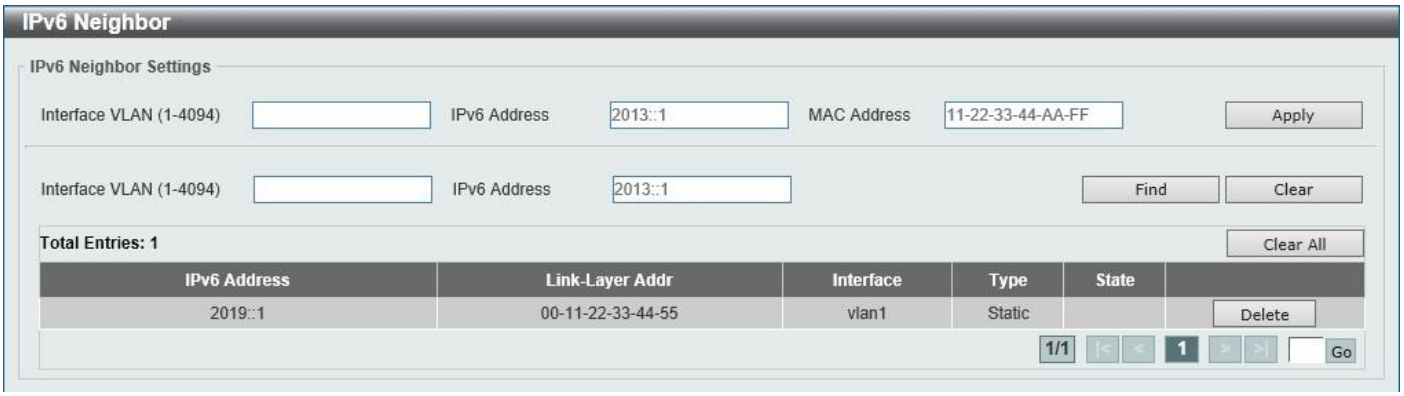

그림 6-5 IPv6 Neighbor 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Interface VLAN	여기에 VLAN Interface ID 를 입력합니다.
IPv6 Address	IPv6 주소를 입력합니다.
MAC Address	MAC 주소를 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Clear 버튼을 클릭하여 특정 Interface 에 대한 모든 동적 정보를 지웁니다.

Clear All 버튼을 클릭하여 이 테이블의 모든 동적 IPv6 네이버 정보를 지웁니다.

Delete 버튼을 클릭하여 특정 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Interface

IPv4 Interface

이 창은 IPv4 Interface 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L3 Features > Interface > IPv4 Interface 를 클릭합니다.

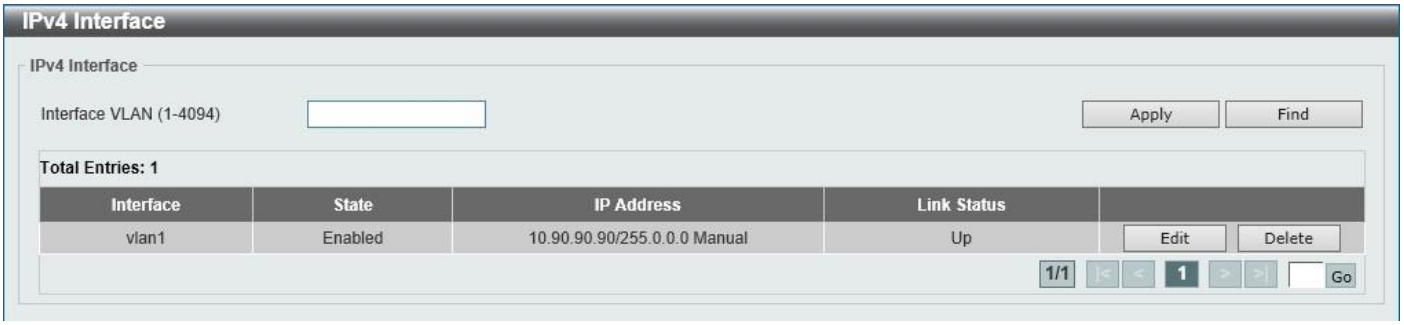

그림 6-6 IPv4 Interface 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Interface VLAN	여기에 Interface VLAN ID 를 입력합니다. 이 값은 1 에서 4094 사이여야 합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.

Delete 버튼을 클릭하여 특정 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Edit 버튼을 클릭하면 다음 페이지를 사용할 수 있습니다.

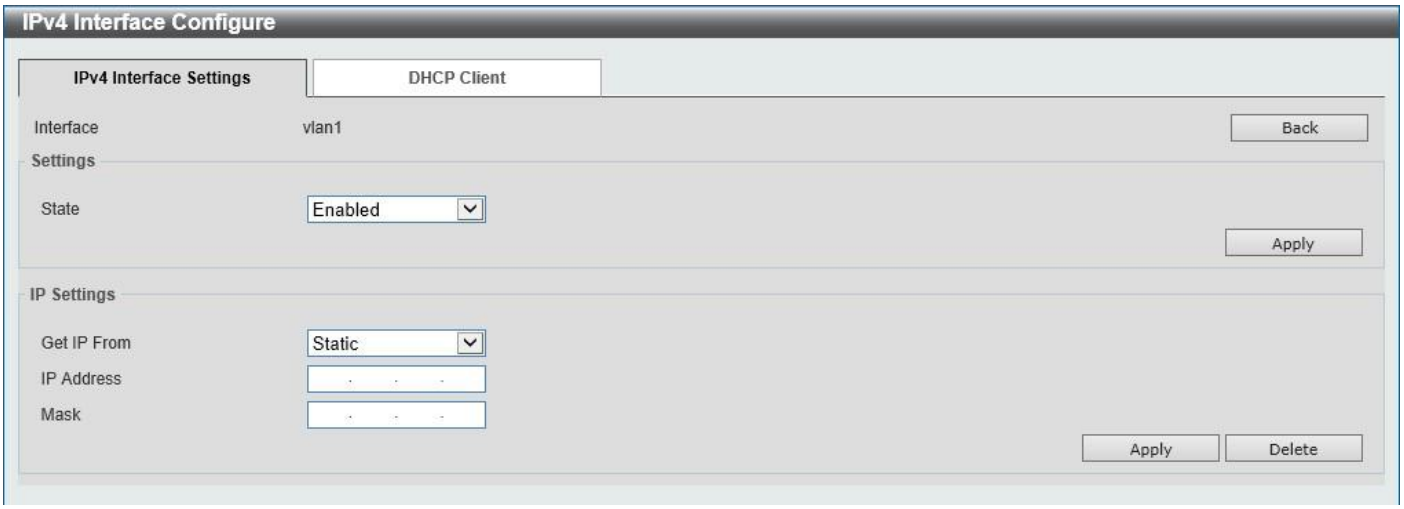

그림 6-7 IPv4 Interface(편집) 창

Settings 섹션에서 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
State	IPv4 Interface 전역 상태를 활성화하거나 비활성화하려면 선택합니다.

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Primary IP Settings 섹션에서 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Get IP From	여기에서 IP 가져오기 옵션을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Static(정적) 옵션을 선택하면 사용자는 제공된 필드에 이 Interface 의 IPv4 주소를 수동으로 입력할 수 있습니다. • DHCP 옵션을 선택하면 이 Interface 는 로컬 네트워크에 있는 DHCP 서버에서 자동으로 IPv4 정보를 가져옵니다.
IP Address	여기에 이 Interface 의 기본 IPv4 주소를 입력합니다.
Mask	여기에 이 Interface 의 기본 IPv4 서브넷 마스크를 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 특정 항목을 제거합니다.

DHCP 클라이언트 탭을 선택하면 다음 페이지가 나타납니다.

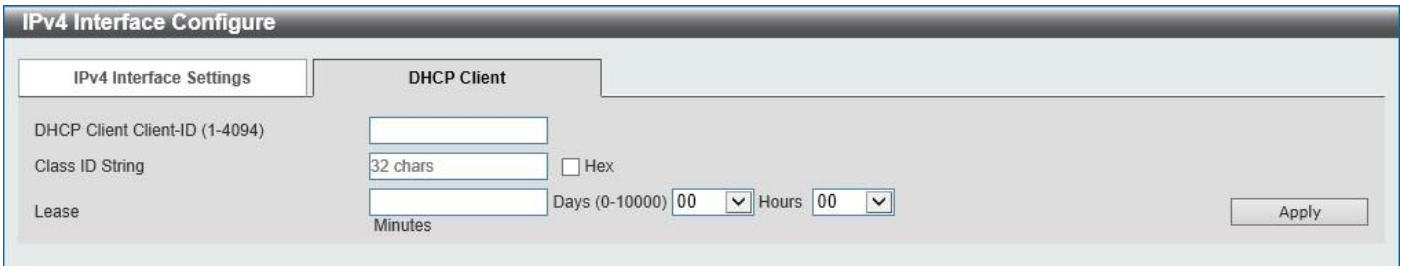

그림 6-8 IPv4 Interface(Edit, DHCP Client) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
DHCP Client Client-ID	여기에 DHCP 클라이언트 ID 를 입력합니다. 범위는 1 에서 4094 사이입니다. 이 매개변수는 16 진수 MAC 주소가 discover 메시지와 함께 전송된 클라이언트 ID 로 사용되는 VLAN Interface 를 지정하는 데 사용됩니다.
Class ID String	여기에 클래스 ID 문자열을 입력합니다. 이 문자열은 최대 32 자까지 가능합니다. Hex 옵션을 선택하여 클래스 ID 문자열을 16 진수 형식으로 입력합니다. 이 문자열은 최대 64 자까지 가능합니다. 이 매개변수는 DHCP 검색 메시지에서 옵션 60 의 값으로 사용되는 공급업체 클래스 식별자를 지정하는 데 사용됩니다.
Lease	여기에 DHCP 클라이언트 임대 시간을 입력하고 선택적으로 선택합니다. 텍스트 상자에 임대 시간(일)을 입력할 수 있습니다. 범위는 0 일에서 10000 일 사이입니다. 시간과 분을 선택적으로 선택할 수도 있습니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

IPv6 Interface

이 창은 IPv6 Interface 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L3 Features > Interface > IPv6 Interface 를 클릭합니다.

그림 6-9) IPv6 Interface 창

IPv6 Interface 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Interface VLAN	IPv6 항목과 연결할 VLAN Interface ID 를 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Show Detail 버튼을 클릭하여 IPv6 Interface 항목에 대한 세부 설정을 보고 구성합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Show Detail 버튼을 클릭하면 다음 페이지를 사용할 수 있습니다.

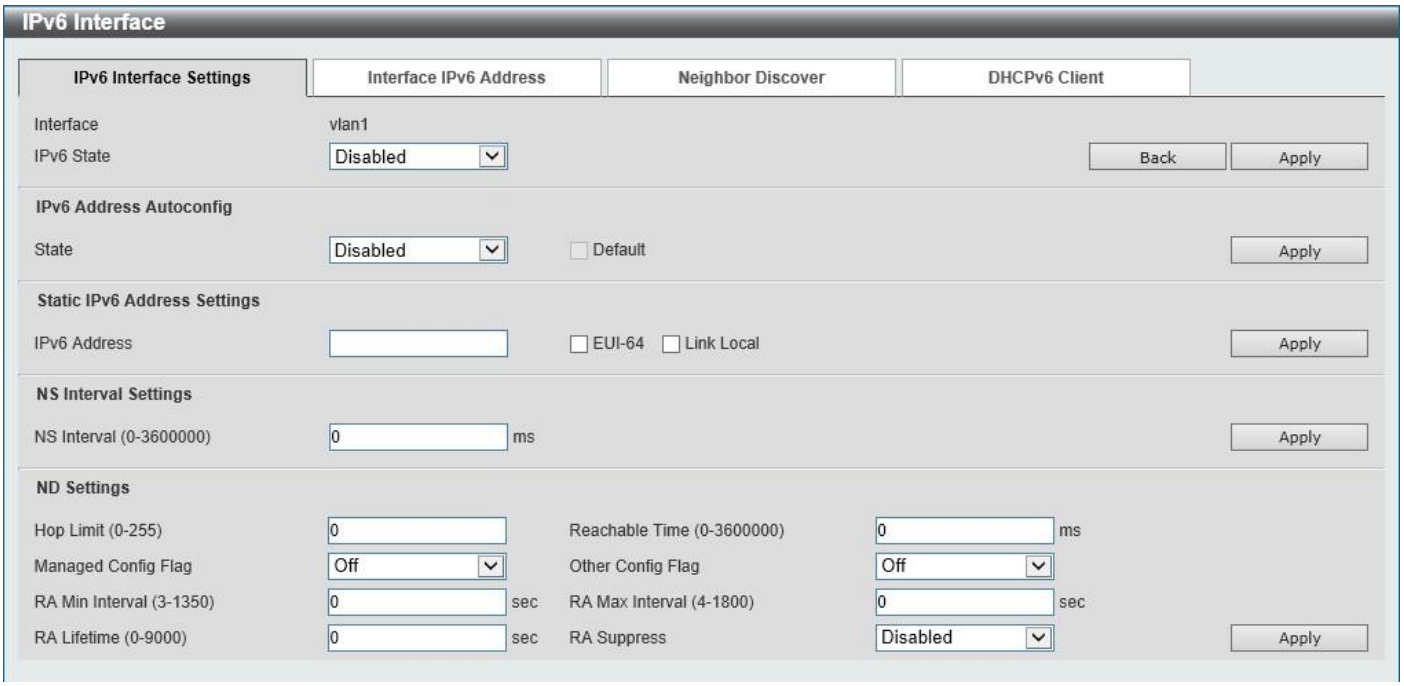

그림 6-10) IPv6 Interface(상세, IPv6 Interface 설정) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
IPv6 State	여기에서 IPv6 Interface 전역 상태를 활성화하거나 비활성화하려면 선택합니다.

Back 버튼을 클릭하여 변경 사항을 취소하고 이전 페이지로 돌아갑니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

IPv6 Address Autoconfig 에 대해 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
State	여기에서 상태 비저장 자동 구성을 사용하여 IPv6 주소의 자동 구성을 활성화하거나 비활성화하려면 선택합니다. 수신된 라우터 알림에 따라 IPv6 라우팅 테이블에 기본 경로를 삽입하려면 기본 옵션을 선택합니다. 기본 경로의 유형은 SLAAC 입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

정적 IPv6 주소 설정에 대해 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
IPv6 Address	여기에 이 IPv6 Interface 의 IPv6 주소를 입력합니다. EUI-64 Interface ID 를 사용하여 Interface 에서 IPv6 주소를 구성하려면 EUI-64 옵션을 선택합니다. Link Local 옵션을 선택하여 IPv6 Interface 에 대한 링크-로컬 주소를 구성합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

NS 간격 설정에 대해 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
NS Interval	여기에 이웃 요청(NS) 간격 값을 입력합니다. 범위는 0 ~ 3600000 밀리초(1000 의 배수)입니다. 지정된 시간이 0 인 경우 라우터는 인터페이스에서 1 초를 사용하고 라우터 광고(RA) 메시지에 0(지정되지 않음)을 광고합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

ND 설정에 대해 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Hop Limit	여기에 hop limit 값을 입력합니다. 범위는 0 에서 255 사이입니다. 시스템에서 시작된 IPv6 패킷도 이 값을 초기 홉 제한으로 사용합니다.
Reachable Time	여기에 도달 가능한 시간을 입력합니다. 범위는 0 에서 3600000 밀리초 사이입니다. 지정된 시간이 0 인 경우 라우터는 Interface 에서 1200 초를 사용하고 RA 메시지에서 0(지정되지 않음)을 광고합니다. Reachable Time(도달 가능 시간)은 IPv6 노드가 인접 노드의 도달 가능성을 결정하는 데 사용됩니다.
Managed Config Flag T	여기에서 Managed Config Flag 옵션을 켜 거나 끕니다. 인접 호스트 호스트가 플래그가 설정된 RA 를 수신하면 호스트는 상태 저장 구성 프로토콜을 사용하여 IPv6 주소를 가져와야 합니다.
RA Min Interval	여기에서 Other Config Flag 옵션을 켜 거나 끕니다. 다른 구성 플래그를 on 으로 설정하면 라우터는 연결된 호스트에 상태 저장 구성 프로토콜을 사용하여 IPv6 주소 이외의 자동 구성 정보를 얻도록 지시합니다.
RA Min Interval	여기에 최소 RA 간격 시간 값을 입력합니다. 범위는 3 초에서 1350 초 사이입니다. 이 값은 최대값의 0.75 배보다 작아야 합니다.
RA Max Interval	여기에 최대 RA 간격 시간 값을 입력합니다. 범위는 4 초에서 1800 초 사이입니다.
RA Lifetime	여기에 RA 수명 값을 입력합니다. 범위는 0 초에서 9000 초 사이입니다. RA 의 수명 값은 수신된 호스트에 라우터를 기본 라우터로 사용하기 위한 수명 값을 지시합니다.
RA Suppress	여기에서 RA 억제 기능을 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Interface IPv6 주소 탭 옵션을 선택하면 페이지 상단에서 다음 페이지를 사용할 수 있습니다.

그림 6-11 IPv6 Interface(상세, Interface IPv6 주소) 창

Delete 버튼을 클릭하여 지정된 항목을 삭제합니다.

Neighbor Discover 탭 옵션을 선택하면 페이지 상단에서 다음 페이지를 사용할 수 있습니다.

그림 6-12) IPv6 Interface(Detail, Neighbor Discover) 창

Edit 버튼을 클릭하여 다음 매개변수를 구성합니다.

그림 6-13 IPv6 Interface(Detail, Neighbor Discover, Edit) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Preferred Life Time	여기에 선호하는 평생 가치를 입력하세요. 범위는 0 초에서 4294967295 초 사이입니다. 기본값은 604800 초(7 일)입니다.
Valid Life Time	여기에 유효한 생애 가치를 입력합니다. 범위는 0 초에서 4294967295 초 사이입니다. 기본값은 2592000 초(30 일)입니다.
Link Flag	여기에서 on-link 플래그를 활성화하거나 비활성화하려면 선택합니다. 기본 옵션은 Enabled 입니다.
Autoconfig Flag	여기에서 자동 구성 플래그를 활성화하거나 비활성화하려면 선택합니다. 기본 옵션은 Enabled 입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DHCPv6 클라이언트 탭 옵션을 선택하면 페이지 상단에서 다음 페이지를 사용할 수 있습니다.

그림 6-14 IPv6 Interface(세부 정보, DHCPv6 클라이언트) 창

Restart 버튼을 클릭하여 DHCPv6 클라이언트 서비스를 다시 시작합니다.

DHCPv6 클라이언트 설정에 대해 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Client State	여기에서 DHCPv6 클라이언트 서비스를 활성화하거나 비활성화하려면 선택합니다. Rapid Commit 옵션을 선택하여 주소 위임을 위한 두 메시지 교환을 진행합니다. 이 rapid-commit 옵션은 twomessage 핸드셰이크를 요청하기 위해 Solicit 메시지에 포함됩니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

IPv4 Static/Default Route

이 창은 IPv4 정적 및 기본 경로 설정을 표시하고 구성하는 데 사용됩니다. 스위치는 IPv4 형식의 주소 지정에 대한 정적 라우팅을 지원합니다. 사용자는 IPv4 에 대해 최대 124 개의 정적 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.

스위치는 또한 부동 고정 경로를 지원하며, 이는 사용자가 다른 다음 홉으로 대체 고정 경로를 생성할 수 있음을 의미합니다. 이 보조 next hop 디바이스 경로는 기본 정적 경로가 다운될 때 백업 정적 경로로 간주됩니다. 기본 경로가 손실되면 백업 경로가 활성화되고 트래픽 전달을 시작합니다. 스위치의 포워딩 테이블에 대한 입력은 IP Address, 서브넷 마스크 및 게이트웨이를 사용하여 만들 수 있습니다.

다음 창을 보려면 아래와 같이 L3 Features > IPv4 Static/Default Route 를 클릭합니다.

그림 6-15 IPv4 Static/Default Route 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
IP Address	여기에 이 경로의 IPv4 주소를 입력합니다. 기본 경로를 IPv4 주소로 사용하려면 기본 경로 옵션을 선택합니다.
Mask	여기에 이 경로에 대한 IPv4 네트워크 마스크를 입력합니다.
Gateway	여기에 이 경로에 대한 게이트웨이 주소를 입력합니다.
Backup State	여기에서 백업 상태 옵션을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Primary - 대상에 대한 기본 경로로 경로를 지정합니다. • Backup - 대상에 대한 백업 경로로 경로를 지정합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 특정 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

IPv4 Route Table

이 창은 IPv4 route table 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L3 Features > IPv4 Route Table 을 클릭합니다.

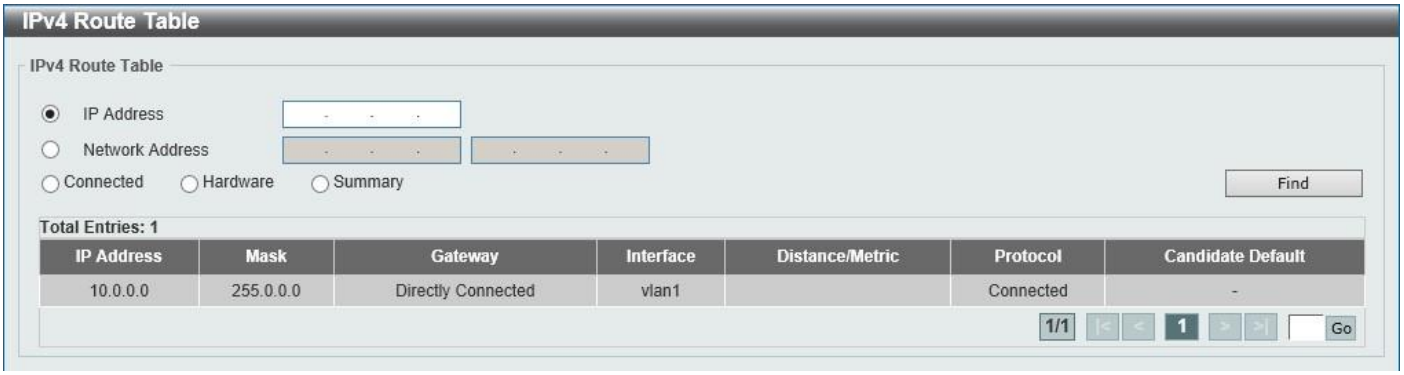

그림 6-16) IPv4 경로 테이블 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
IP Address	여기에서 단일 IPv4 주소를 선택하여 입력합니다.
Network Address	여기에서 IPv4 네트워크 주소를 선택하여 입력합니다. 첫 번째 공간에는 네트워크 접두사를 입력하고 두 번째 공간에는 네트워크 마스크를 입력합니다.
Connected	이 옵션을 선택하면 연결된 경로만 표시됩니다.
Hardware	하드웨어 경로만 표시하려면 이 옵션을 선택합니다. 하드웨어 경로는 하드웨어 칩에 기록된 경로입니다.
Summary	이 스위치에 구성된 경로 소스의 요약 및 수를 표시하려면 이 옵션을 선택합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

IPv6 Static/Default Route

이 창은 IPv6 정적 또는 기본 경로를 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L3 Features > IPv6 Static/Default Route 를 클릭합니다.

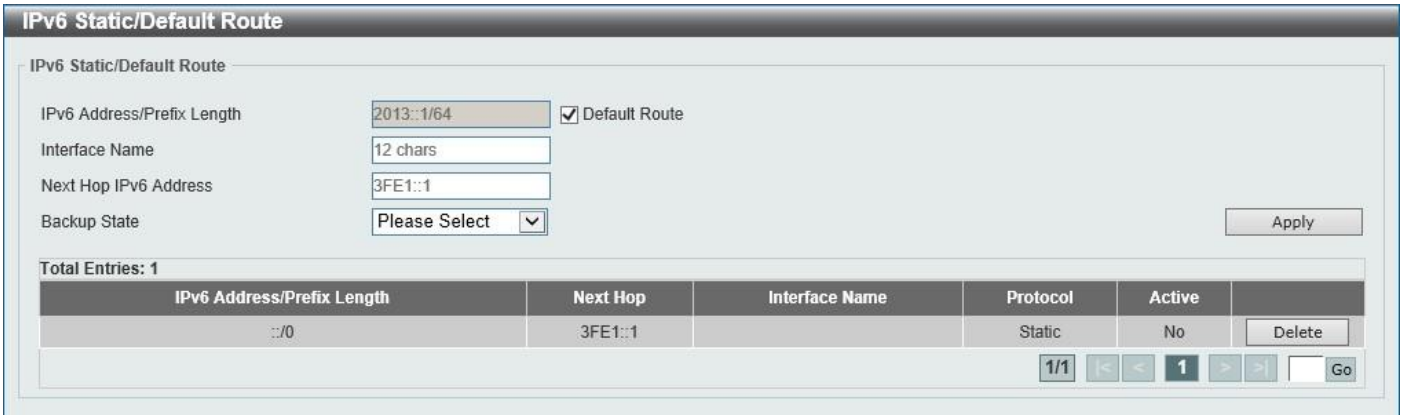

그림 6-17 IPv6 정적/기본 경로 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
IPv6 Address/Prefix Length	여기에 이 경로의 IPv6 주소 및 접두사 길이를 입력합니다. 이 경로를 기본 경로로 사용하려면 기본 경로 옵션을 선택합니다.
Interface Name	여기에 이 경로와 연결할 Interface 의 이름을 입력합니다.
Next Hop IPv6 Address	여기에 다음 홉 IPv6 주소를 입력합니다.
Backup State	여기에서 백업 상태 옵션을 선택합니다. 선택할 수 있는 옵션은 Primary 및 Backup 입니다. Primary 옵션을 선택하면 경로가 대상에 대한 기본 경로로 지정됩니다. Backup 옵션을 선택하면 경로가 대상에 대한 백업 경로로 지정됩니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 특정 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

IPv6 Route Table

이 창은 IPv6 경로 테이블을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L3 Features > IPv6 Route Table 을 클릭합니다.

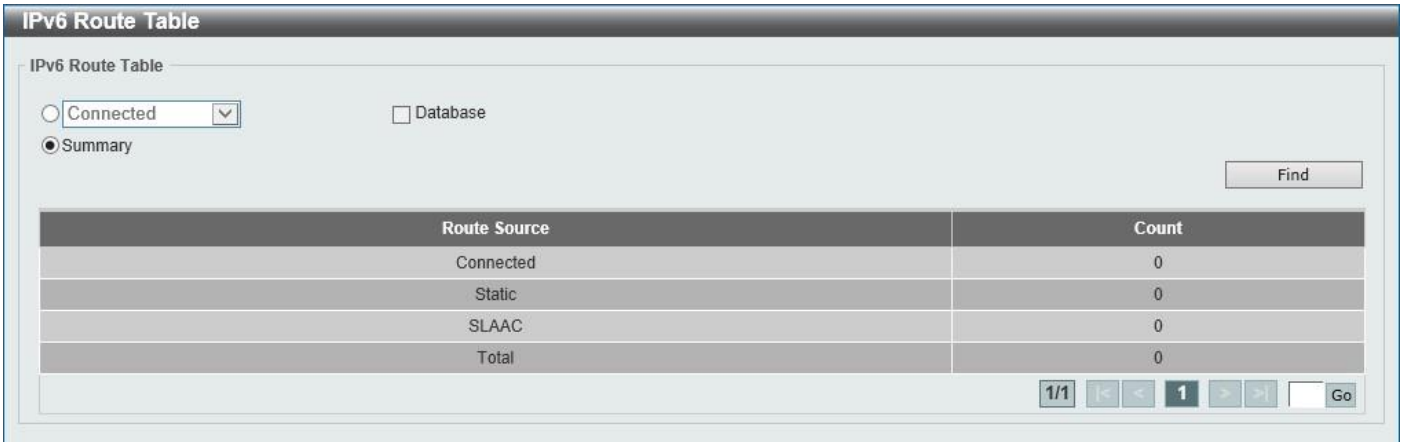

그림 6-18 IPv6 경로 테이블 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Connected	이 옵션을 선택하면 연결된 경로만 표시됩니다.
Database	이 옵션을 선택하면 최적 경로 대신 라우팅 데이터베이스의 모든 관련 항목이 표시됩니다.
Summary	이 스위치에 구성된 경로 소스의 요약 및 수를 표시하려면 이 옵션을 선택합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

IP Multicast Routing Protocol

IPMC

IP Multicast Routing Forwarding Cache Table

이 창은 IP 멀티캐스트 라우팅 전달 캐시 데이터베이스의 내용을 표시하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L3 Features > IP Multicast Routing Protocol > IPMC > IP Multicast Routing Forwarding Cache Table 을 클릭합니다.

그림 6-19) IP 멀티캐스트 라우팅 전달 캐시 테이블 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Group Address	여기에 멀티캐스트 그룹 IP Address 를 입력합니다.
Source Address	여기에 소스 IP Address 를 입력합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Show All 버튼을 클릭하여 모든 항목을 표시합니다.

IPv6MC

IPv6 Multicast Routing Forwarding Cache Table

이 창은 IPv6 멀티캐스트 라우팅 전달 캐시 데이터베이스의 내용을 표시하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 L3 Features > IP Multicast Routing Protocol > IPv6MC > IPv6 Multicast Routing Forwarding Cache Table 을 클릭합니다.

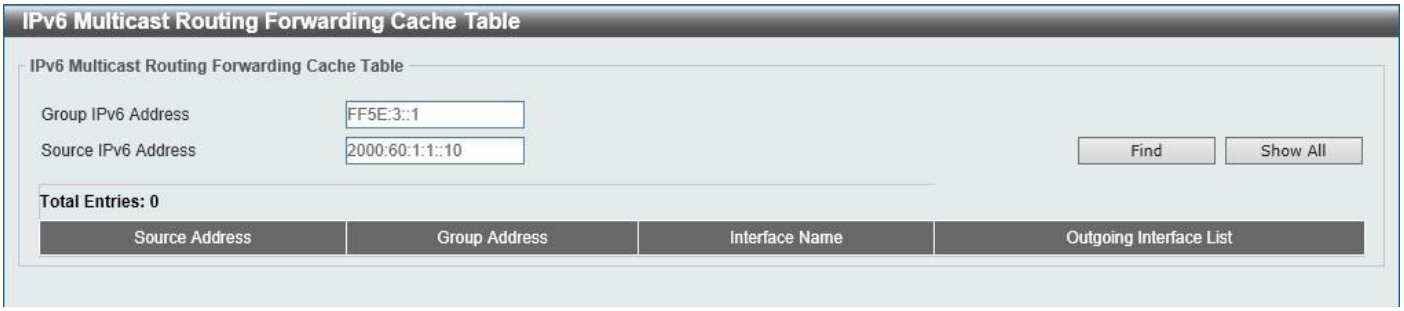

그림 6-20 IPv6 멀티캐스트 라우팅 전달 캐시 테이블 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Group IPv6 Address	여기에 멀티캐스트 그룹 IPv6 주소를 입력합니다.
Source IPv6 Address	여기에 소스 IPv6 주소를 입력합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Show All 버튼을 클릭하여 모든 항목을 표시합니다.

6. Quality of Service (QoS)

Basic Settings
Advanced Settings

Basic Settings

Port Default CoS

이 창은 Port Default CoS 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 QoS > Basic Settings > Port Default CoS 를 클릭합니다.

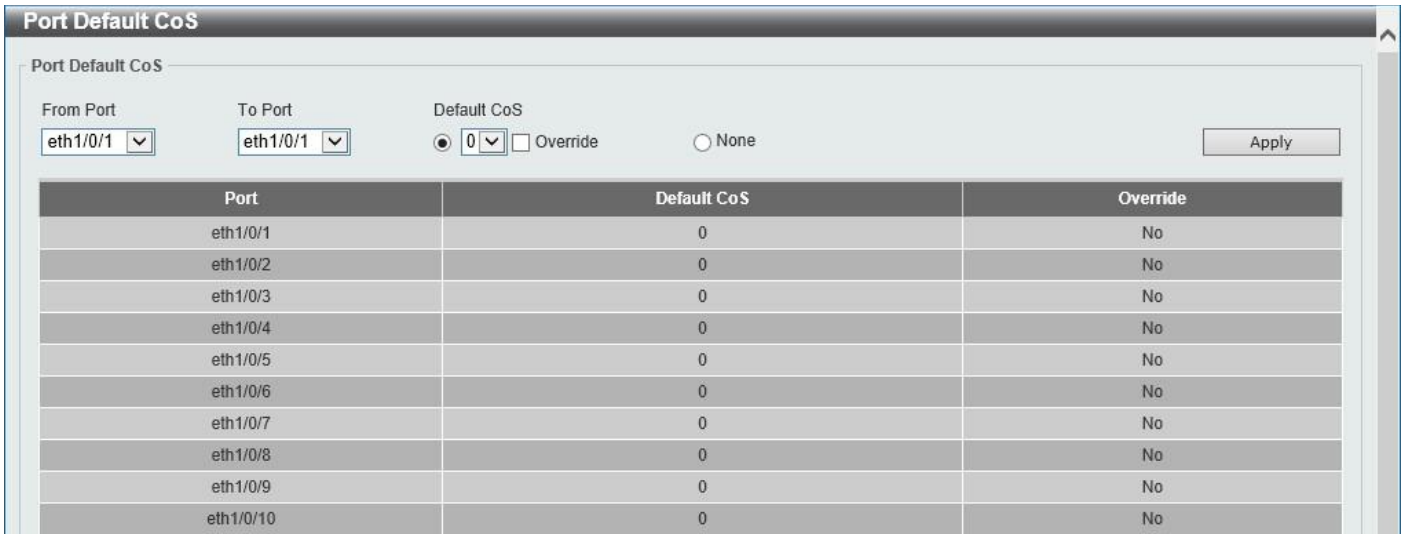

그림 7-1 포트 기본 CoS 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
Default CoS	여기에 지정된 포트에 대한 기본 CoS 옵션을 선택합니다. 선택할 수 있는 옵션은 0 에서 7 사이입니다. Override(재정의) 옵션을 선택하여 패킷의 CoS 를 재정의합니다. 기본 CoS 는 포트에서 수신한 모든 수신 패킷(태그 지정 또는 태그 없음)에 적용됩니다. None 옵션을 선택하여 패킷에 태그가 지정된 경우 패킷의 CoS 가 패킷의 CoS 가 되고 패킷에 태그가 지정되지 않은 경우 포트 기본 CoS 가 되도록 지정합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Port Scheduler Method

이 창은 Port Scheduler Method 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 QoS > Basic Settings > Port Scheduler Method 를 클릭합니다.

그림 7-2 포트 스케줄러 방법 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
Scheduler Method	지정된 포트에 적용할 스케줄러 방법을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • SP (Strict Priority) - 모든 큐가 엄격한 우선 순위 스케줄링을 사용하도록 지정합니다. 가장 높은 CoS 대기열에서 가장 낮은 대기열까지 대기열에 대한 엄격한 우선 순위 액세스를 제공합니다. • RR (라운드 로빈) - 모든 큐가 라운드 로빈 스케줄링을 사용하도록 지정합니다. 다음 대기열로 이동하기 전에 각 대기열에서 단일 패킷을 서비스할 수 있는 공정한 액세스를 제공합니다. • WRR (Weighted Round-Robin) - 허용된 패킷을 라운드 로빈 순서로 전송 대기열로 전송하도록 지정합니다. 처음에 각 대기열은 가중치를 구성 가능한 가중치로 설정합니다. 우선 순위가 더 높은 CoS 대기열의 패킷이 전송될 때마다 해당 가중치에 1 이 차감되고 다음으로 낮은 CoS 대기열의 패킷이 서비스됩니다. CoS 대기열의 가중치가 0 에 도달하면 가중치가 보충될 때까지 대기열이 서비스되지 않습니다. 모든 CoS 대기열의 가중치가 0 에 도달하면 가중치가 한 번에 보충됩니다. 이것이 기본 옵션입니다. • WDRR (Weighted Deficit Round-Robin) - 전송 대기열에서 누적된 백로그된 크레딧 집합을 라운드 로빈 순서로 제공하도록 지정합니다. 처음에 각 대기열은 크레딧 카운터를 구성 가능한 양자 값으로 설정합니다. CoS 대기열의 패킷이 전송될 때마다 패킷의 크기가 해당 크레딧 카운터에서 차감되고 서비스 권한이 다음으로 낮은 CoS 대기열로 넘겨집니다. 크레딧 카운터가 0 아래로 떨어지면 크레딧이 보충될 때까지 대기열이 더 이상 서비스되지 않습니다. 모든 CoS 대기열의 크레딧 카운터가 0 에 도달하면 해당 시점에 크레딧 카운터가 보충됩니다. 모든 패킷은 크레딧 카운터가 0 또는 음수가 되고 마지막 패킷이 완전히 전송될 때까지 서비스됩니다. 이 조건이 발생하면 크레딧이 보충됩니다. 크레딧이 보충되면 각 CoS 대기열 크레딧 카운터에 퀀텀 크레딧이 추가됩니다. 각 CoS 대기열에 대한 퀀텀은 사용자 구성에 따라 다를 수 있습니다.

	SP 모드에서 CoS 대기열을 설정하려면 우선 순위가 더 높은 CoS 대기열도 엄격한 우선 순위 모드에 있어야 합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Queue Settings

이 창은 대기열 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 QoS > Basic Settings > Queue Settings 을 클릭합니다.

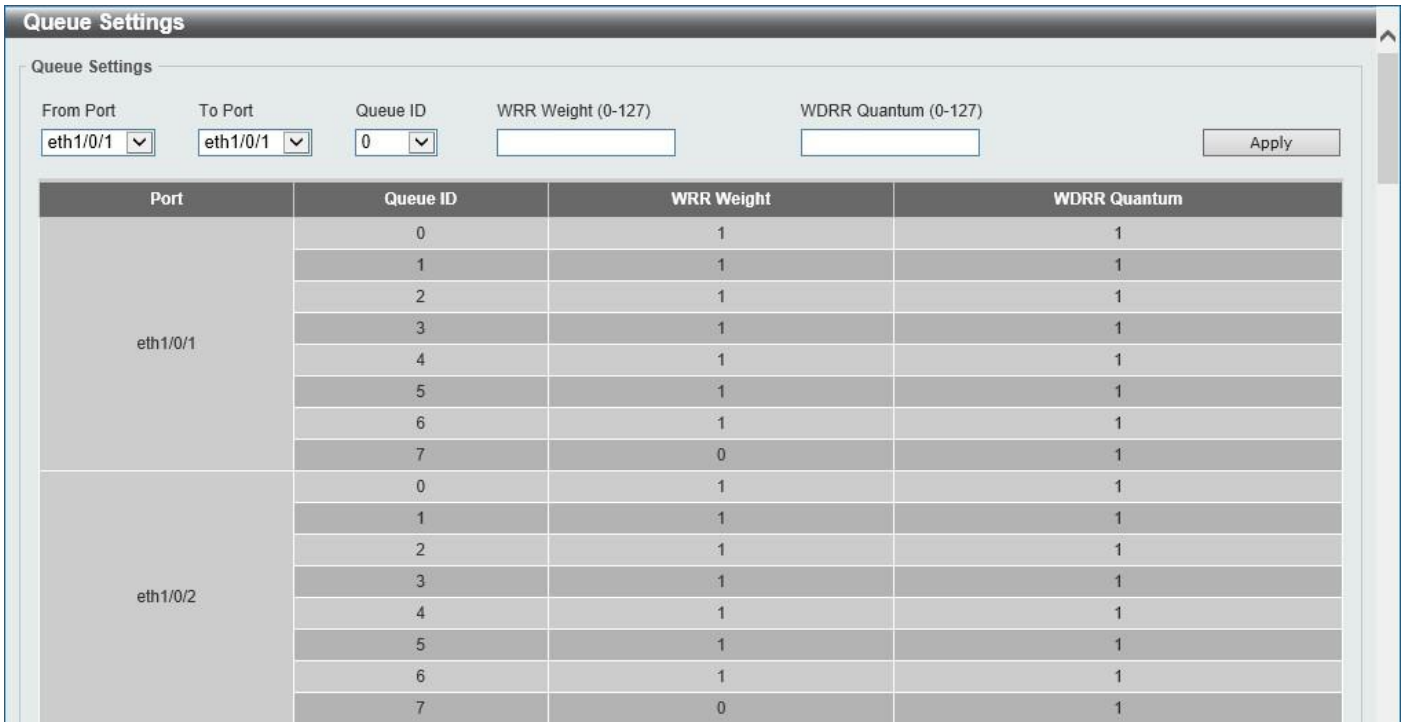

그림 7-3) 대기열 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
Queue ID	여기에 대기열 ID 값을 입력합니다. 이 값은 0 에서 7 사이여야 합니다.
WRR Weight	여기에 WRR 가중치 값을 입력합니다. 이 값은 0 에서 127 사이여야 합니다. EF(Expedited Forwarding)의 동작 요구 사항을 충족하기 위해 가장 높은 큐는 항상 PHB(Per-hop Behavior) EF 에 의해 선택되며 이 큐의 일정 모드는 엄격한 우선 순위 스케줄링이어야 합니다. 따라서 Differentiate 서비스가 지원되는 동안 마지막 큐의 가중치는 0 이어야 합니다.
WDRR Quantum	여기에 WDRR 양자 값을 입력합니다. 이 값은 0 에서 127 사이여야 합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

CoS to Queue Mapping

이 창은 CoS-to-Queue mapping 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 QoS > Basic Settings > CoS to Queue Mapping 을 클릭합니다.

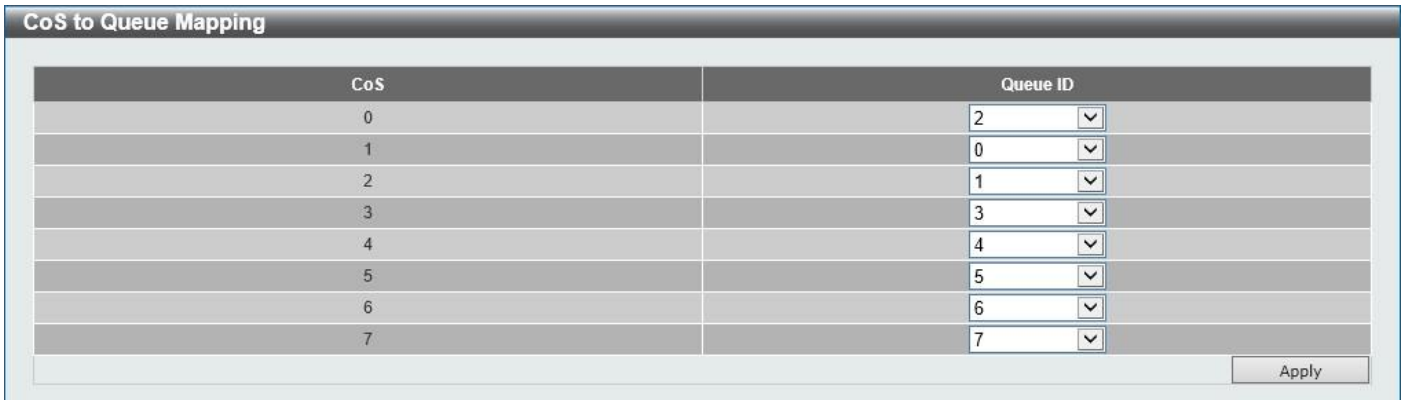

그림 7-4 CoS-Queue 매핑 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Queue ID	해당 CoS 값에 매핑할 대기열 ID 를 선택합니다. 선택할 수 있는 옵션은 0 에서 7 사이입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Port Rate Limiting

이 창은 포트 속도 제한 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 QoS > Basic Settings > Port Rate Limiting 을 클릭합니다.

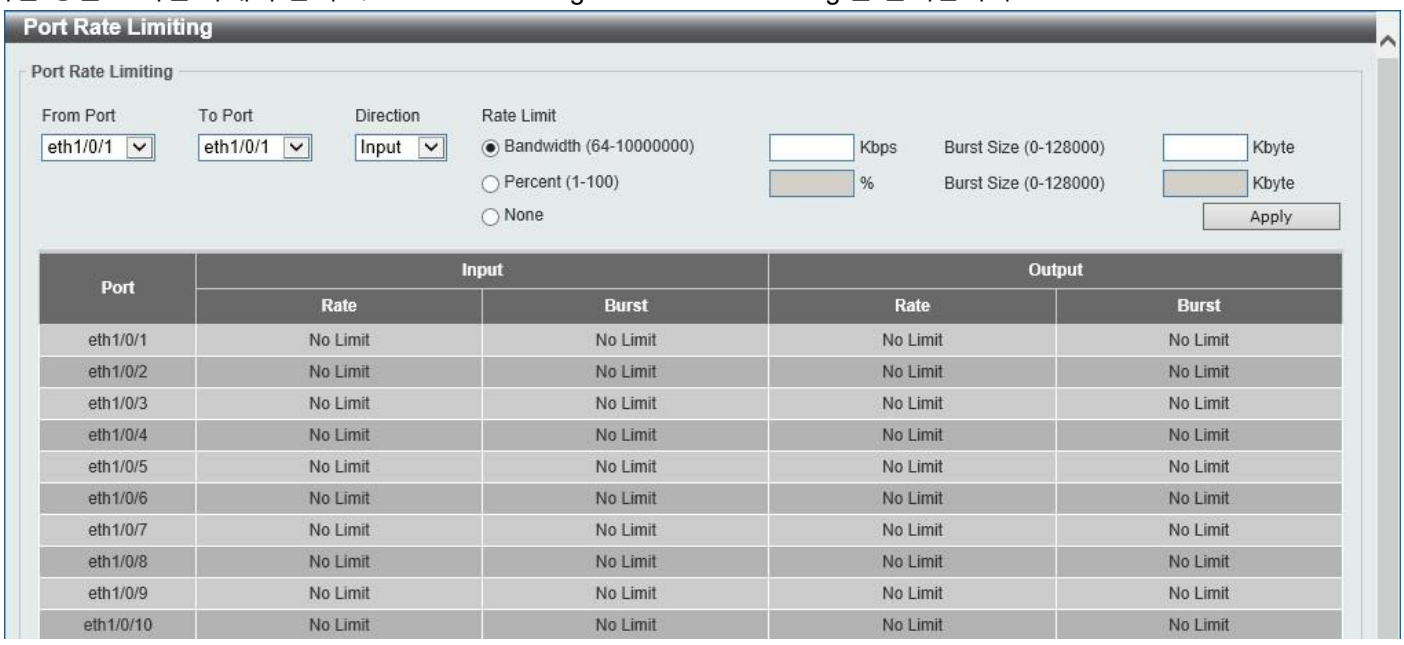

그림 7-5 Port Rate Limiting 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
Direction	여기에서 방향 옵션을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Input - 인그레스 패킷에 대한 속도 제한이 구성됩니다. • Output - 이그레스 패킷에 대한 속도 제한이 구성됩니다.

Rate Limit	여기에 속도 제한 값을 선택하고 입력합니다. • Bandwidth(대역폭)를 선택한 경우 제공된 공간에 사용된 입력/출력 대역폭 값을 입력합니다. 이 값은 64kbps 에서 10000000kbps 사이여야 합니다. 또한 제공된 공간에 Burst Size 값을 입력합니다. 이 값은 0 에서 128000KB 사이여야 합니다. • Percent(백분율)를 선택한 경우 제공된 공간에 사용된 입력/출력 대역폭 백분율 값을 입력합니다. 이 값은 1 에서 100%(%) 사이여야 합니다. 또한 제공된 공간에 Burst Size 값을 입력합니다. 이 값은 0 에서 128000KB 사이여야 합니다. • None(없음) 옵션을 선택하여 지정된 포트의 속도 제한을 제거합니다. 지정된 제한은 지정된 Interface 의 최대 속도를 초과할 수 없습니다. ingress 대역폭 제한의 경우, ingress 는 수신된 트래픽이 제한을 초과할 때 일시 중지 프레임 또는 흐름 제어 프레임을 전송합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Queue Rate Limiting

이 창은 queue rate limiting 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 QoS > Basic Settings > Queue Rate Limiting 을 클릭합니다.

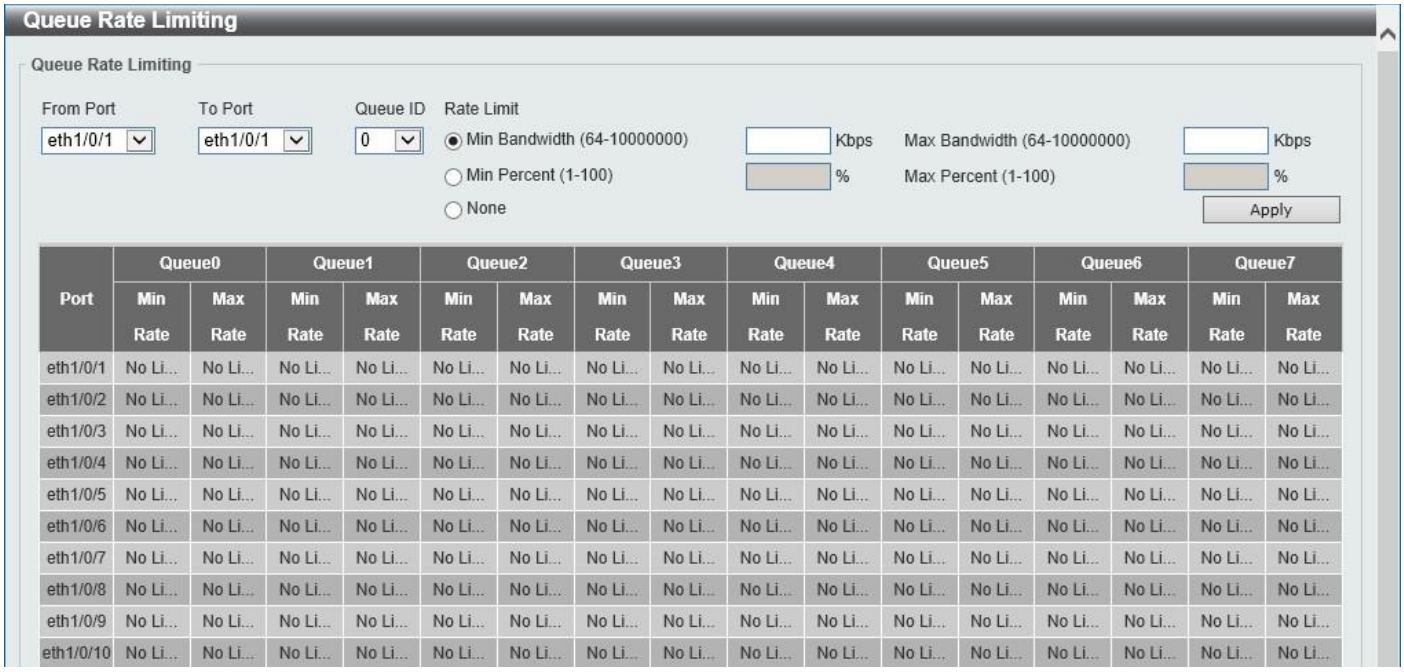

그림 7-6) 대기열 속도 제한 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
Queue ID	여기에서 구성할 대기열 ID 를 선택합니다. 선택할 수 있는 옵션은 0 에서 7 사이입니다.

Rate Limit	여기에서 대기열 속도 제한 설정을 선택하고 입력합니다. • Min Bandwidth(최소 대역폭) 옵션을 선택한 경우 제공된 공간에 최소 대역폭 속도 제한 값을 입력합니다. 이 값은 64kbps 에서 10000000kbps 사이여야 합니다. 또한 제공된 공간에 최대 대역폭(최대 대역폭) 속도 제한을 입력합니다. 이 값은 64kbps 에서 10000000kbps 사이여야 합니다. 최소 대역폭이 구성되면 대기열에서 전송되는 패킷을 보장할 수 있습니다. 최대 대역폭이 구성되면 대역폭을 사용할 수 있더라도 큐에서 전송된 패킷은 최대 대역폭을 초과할 수 없습니다. 최소 대역폭을 구성할 때 구성된 최소 대역폭의 집계는 구성된 최소 대역폭을 보장할 수 있도록 Interface 대역폭의 75% 미만이어야 합니다. 가장 엄격한 우선 순위 대기열에 대해 최소 보장 대역폭을 설정할 필요가 없습니다. 이는 모든 대기열의 최소 대역폭이 충족되는 경우 이 대기열의 트래픽이 먼저 서비스되기 때문입니다. 이 명령의 컨피그레이션은 물리적 포트에만 연결할 수 있으며 포트 채널에는 연결할 수 없습니다. 즉, 물리적 포트에서 사용할 수 없는 하나의 CoS 의 최소 보장 대역폭입니다. • Min Percent(최소 백분율) 옵션을 선택한 경우 제공된 공간에 최소 대역폭 백분율 값을 입력합니다. 이 값은 1 에서 100%(%) 사이여야 합니다. 또한 제공된 공간에 최대 백분율 값(Max Percent)을 입력합니다. 이 값은 1 에서 100%(%) 사이여야 합니다. • None(없음) 옵션을 선택하여 지정된 포트의 속도 제한을 제거합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Advanced Settings

DSCP Mutation Map

이 창은 DSCP(Differentiated Services Code Point) 변형 맵 설정을 표시하고 구성하는 데 사용됩니다. DSCP 변형 맵을 기반으로 Interface 에서 패킷을 수신하면 QoS 작업 직전에 수신 DSCP 를 다른 DSCP 로 변경할 수 있습니다. DSCP 변형은 DSCP 할당이 다른 도메인을 통합하는 데 유용합니다. DSCP-CoS 맵은 여전히 패킷의 원래 DSCP 를 기반으로 합니다. 모든 후속 작업은 변경된 DSCP 를 기반으로 합니다.

다음 창을 보려면 아래와 같이 QoS > Advanced Settings > DSCP Mutation Map(DSCP 변형 맵)을 클릭합니다.

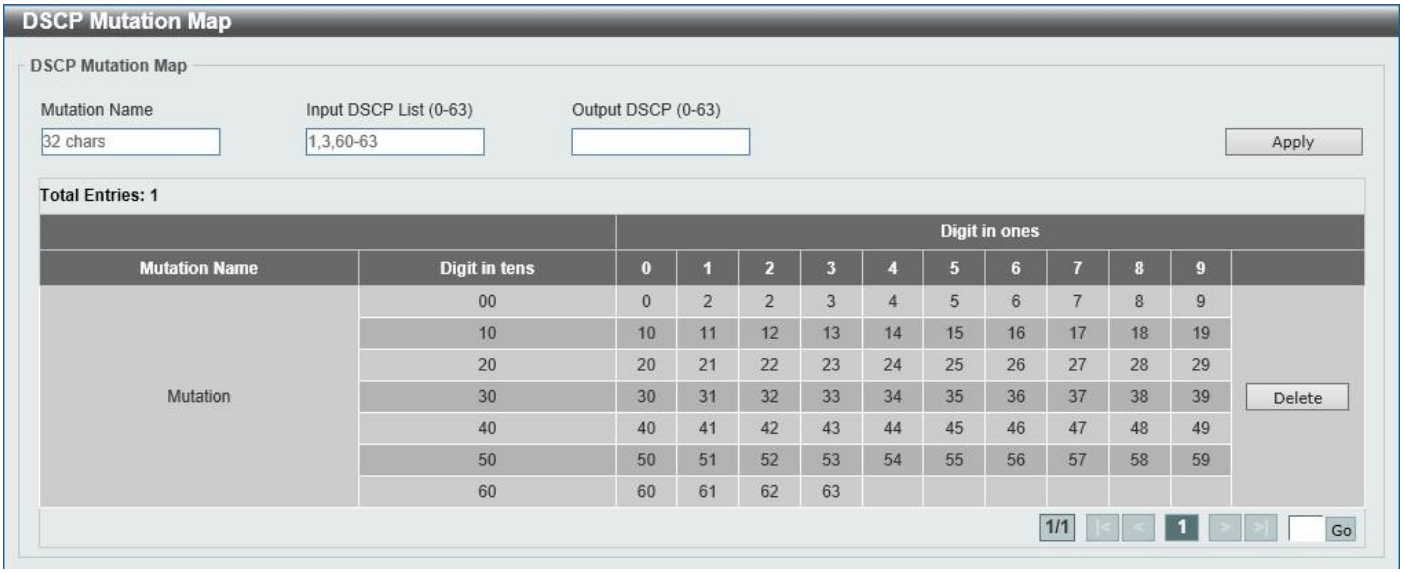

그림 7-7 DSCP Mutation Map 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Mutation Name	여기에 DSCP 변형 맵 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Input DSCP List	여기에 입력 DSCP 목록 값을 입력합니다. 이 값은 0 에서 63 사이여야 합니다.
Output DSCP List	여기에 출력 DSCP 목록 값을 입력합니다. 이 값은 0 에서 63 사이여야 합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 특정 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Port Trust State and Mutation Binding

이 창은 Port Trust State and Mutation Binding 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 QoS > Advanced Settings > Port Trust State and Mutation Binding 을 클릭합니다.

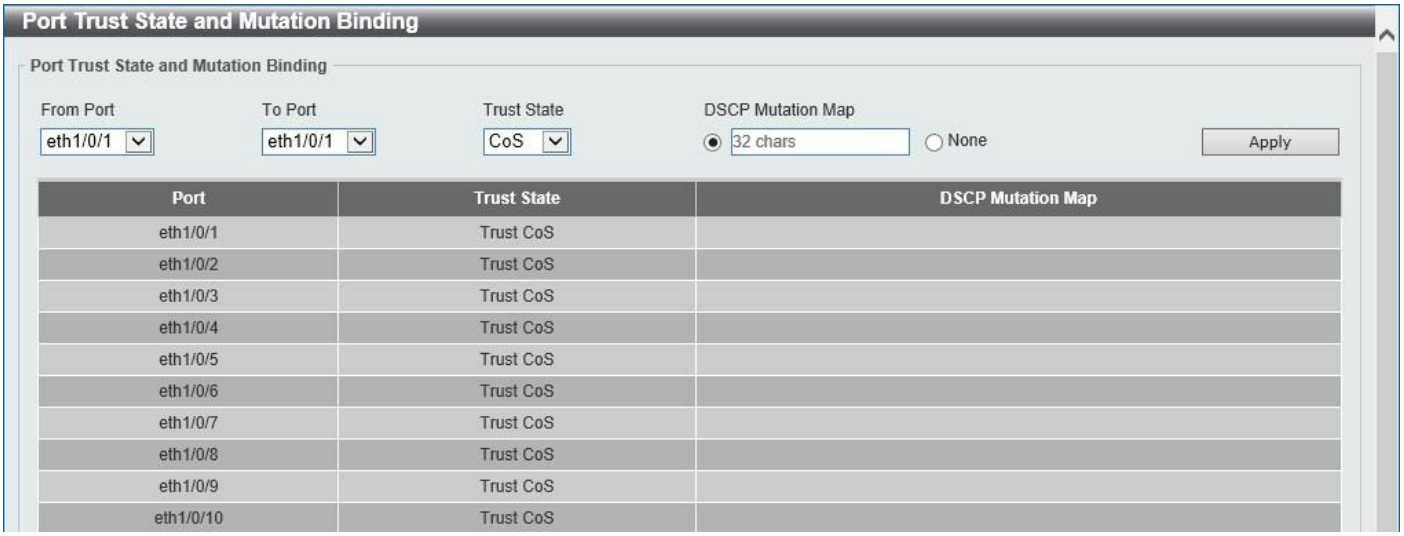

그림 7-8 Port Trust State 및 Mutation Binding 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
Trust State	여기에서 포트 신뢰 상태 옵션을 선택합니다. 선택할 수 있는 옵션은 CoS 및 DSCP 입니다.
DSCP Mutation Map	여기에 사용된 DSCP 변형 맵 이름을 선택하고 입력합니다. 이 이름은 최대 32 자까지 가능합니다. DSCP 변형 맵을 포트에 할당하지 않으 려면 None 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DSCP CoS Mapping

이 창은 DSCP CoS Mapping 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 QoS > Advanced Settings > DSCP CoS Mapping 을 클릭합니다.

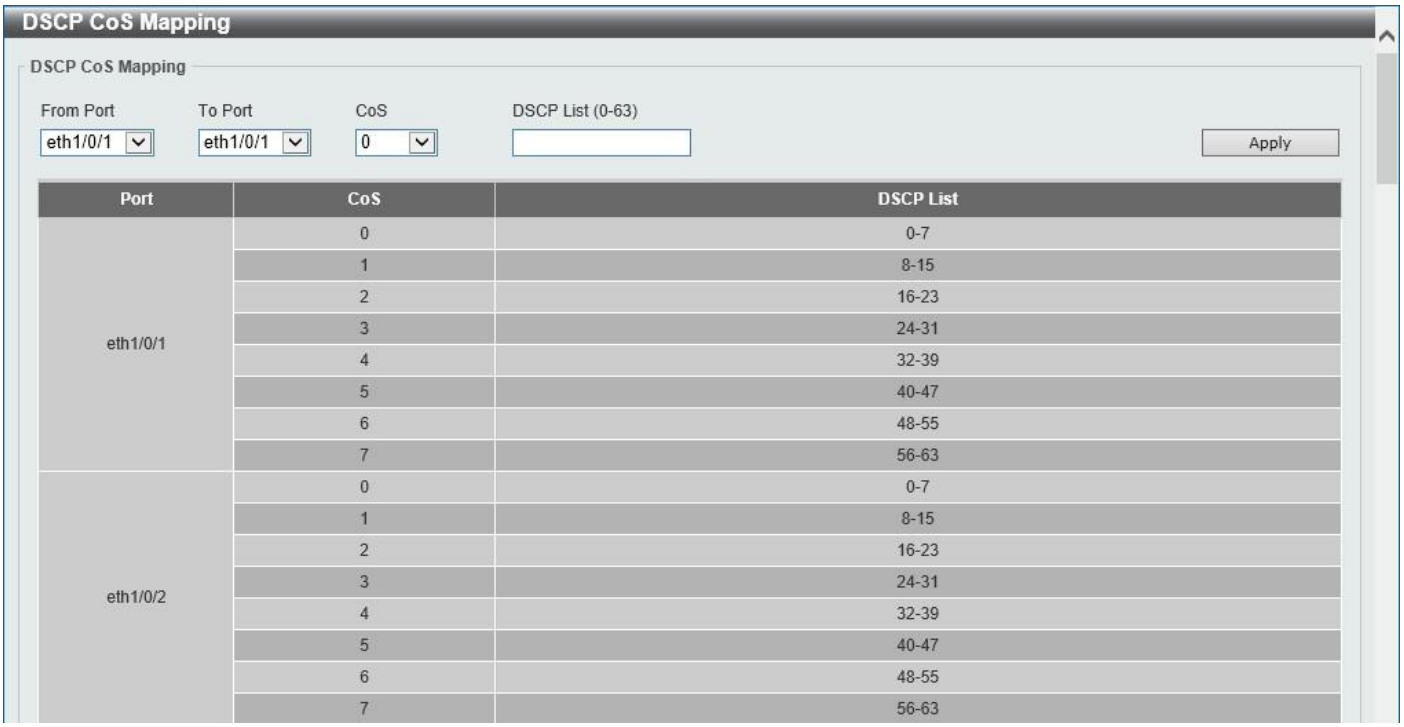

그림 7-9 DSCP CoS 매핑 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
CoS	DSCP 목록에 매핑할 CoS 값을 선택합니다. 선택할 수 있는 옵션은 0 에서 7 사이입니다.
DSCP List	여기에 CoS 값에 매핑할 DSCP 목록 값을 입력합니다. 이 값은 0 에서 63 사이여야 합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Class Map

이 창은 Class Map 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 QoS > Advanced Settings > Class Map 을 클릭합니다.

그림 7-10 클래스 맵 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Class Map Name	여기에 클래스 맵 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Multiple Match Criteria	여기에서 여러 일치 기준 옵션을 선택합니다. 선택할 수 있는 옵션은 Match All(모두 일치) 및 Match Any(모두 일치)입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.
Match 버튼을 클릭하여 특정 항목을 구성합니다.
Delete 버튼을 클릭하여 특정 항목을 제거합니다.
페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

일치 버튼을 클릭하면 다음 페이지를 사용할 수 있습니다.

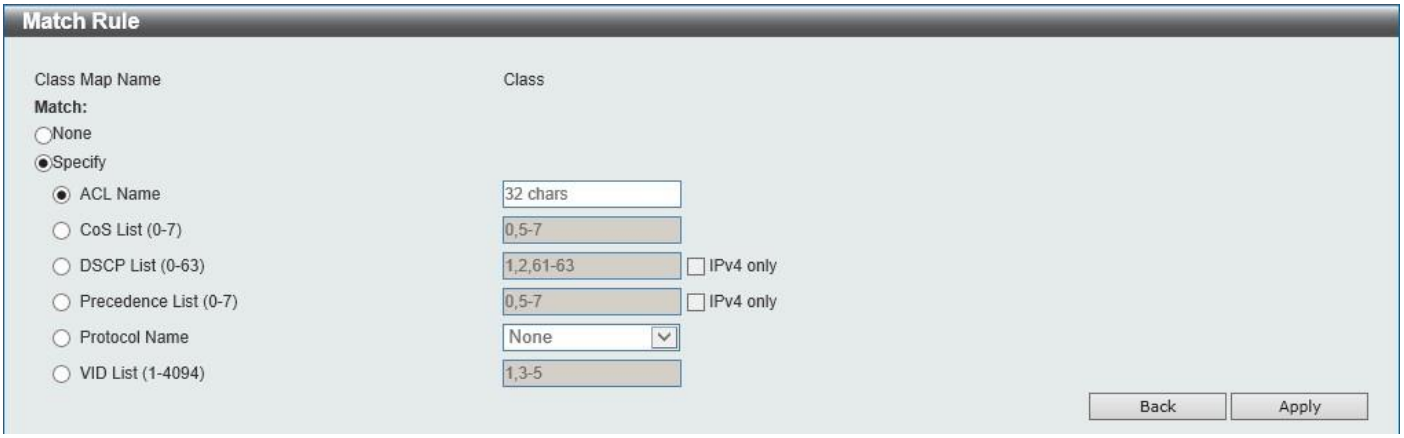

그림 7-11 클래스 맵(일치) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
None	이 클래스 맵과 아무 것도 일치시키지 않으려면 이 옵션을 선택합니다.
Specify	이 클래스 맵에 항목을 일치시키는 옵션을 선택합니다.
ACL Name	여기에서 이 클래스 맵과 일치시킬 액세스 목록 이름을 선택하고 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
CoS List	여기에서 이 클래스 맵과 일치시킬 CoS 목록 값을 선택하고 입력합니다. 이 값은 0 에서 7 사이여야 합니다.
DSCP List	여기에서 이 클래스 맵과 일치시킬 DSCP 목록 값을 선택하고 입력합니다. 이 값은 0 에서 63 사이여야 합니다. IPv4 패킷 만 일치시키려면 IPv4 전용 옵션을 선택합니다. 지정하지 않으면 IPv4 및 IPv6 패킷 모두에 대해 일치합니다.
Precedence List	여기에서 이 클래스 맵과 일치시킬 우선 순위 목록 값을 선택하고 입력합니다. 이 값은 0 에서 7 사이여야 합니다. IPv4 패킷 만 일치시키려면 IPv4 전용 옵션을 선택합니다. 지정하지 않으면 IPv4 및 IPv6 패킷 모두에 대해 일치합니다. IPv6 패킷의 경우 우선 순위는 IPv6 헤더의 트래픽 클래스의 가장 중요한 3 비트입니다.
Protocol Name	여기에서 클래스 맵과 일치시킬 프로토콜 이름을 선택합니다. 선택할 수 있는 옵션은 ARP, BGP, DHCP, DNS, EGP, FTP, IPv4, IPv6, NetBIOS, NFS, NTP, OSPF, PPPOE, RIP, RTSP, SSH, Telnet 입니다.및 TFTP 가 있습니다.
VLAN List	여기에서 클래스 맵과 일치시킬 VLAN 목록 값을 선택하고 입력합니다. 이 값은 1 에서 4094 사이여야 합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.
Back 버튼을 클릭하여 변경 사항을 취소하고 이전 페이지로 돌아갑니다.

Policy Map

이 창은 정책 맵 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 QoS > Advanced Settings > Policy Map 을 클릭합니다.

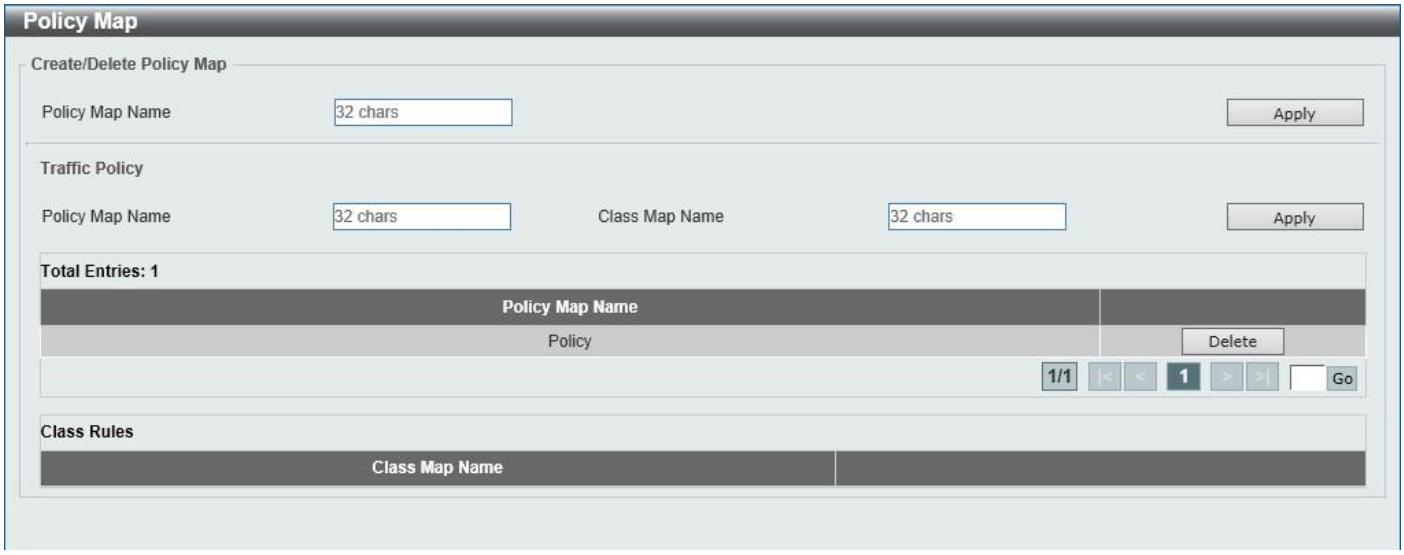

그림 7-12) 정책 맵 창

Create/Delete Policy Map 에 대해 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Policy Map Name	여기에 생성할 정책 맵의 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Traffic Policy 에 대해 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Policy Map Name	여기에 정책 맵 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Class Map Name	여기에 클래스 맵 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 특정 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

정책에 할당된 Class Rules 를 보려면 Policy Map 테이블에서 Policy Map 항목을 선택합니다. 정책에 할당된 클래스 규칙은 아래와 같이 클래스 규칙 테이블에 표시됩니다.

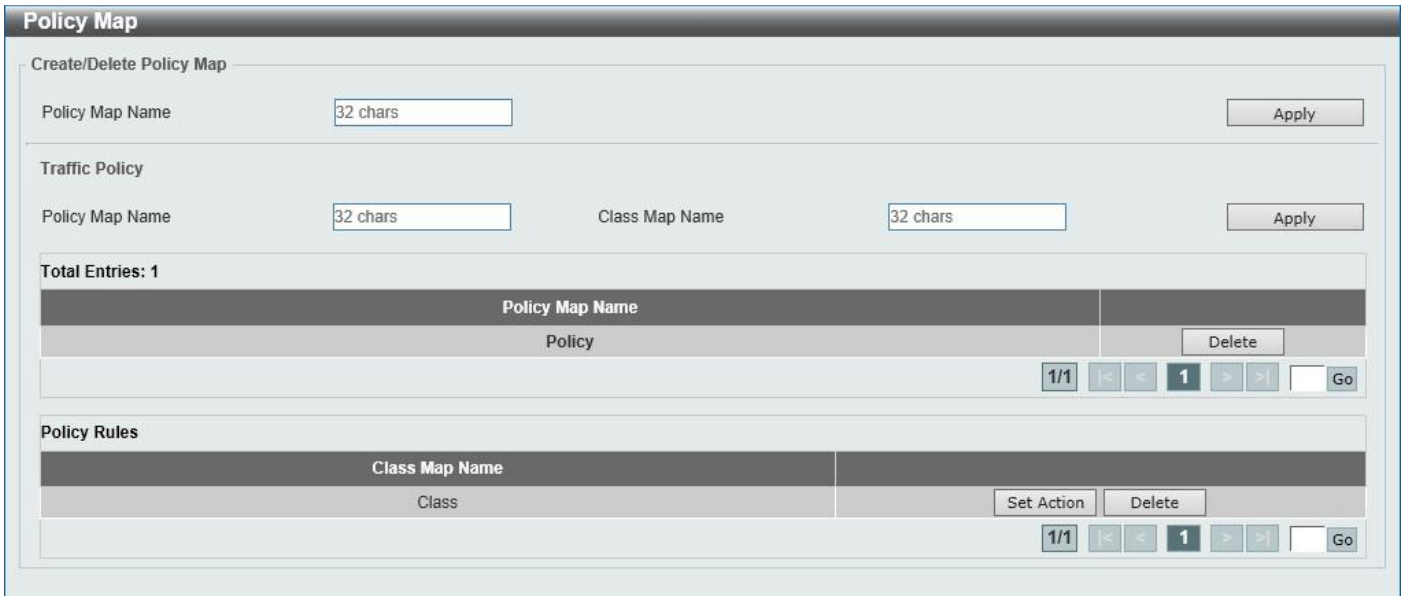

그림 7-13) 정책 맵(클래스 규칙) 창

Set Action 버튼을 클릭하여 지정된 항목에 대한 설정 Action 설정을 구성합니다.
Delete 버튼을 클릭하여 특정 항목을 제거합니다.
페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Set Action 버튼을 클릭하면 다음 페이지가 나타납니다.

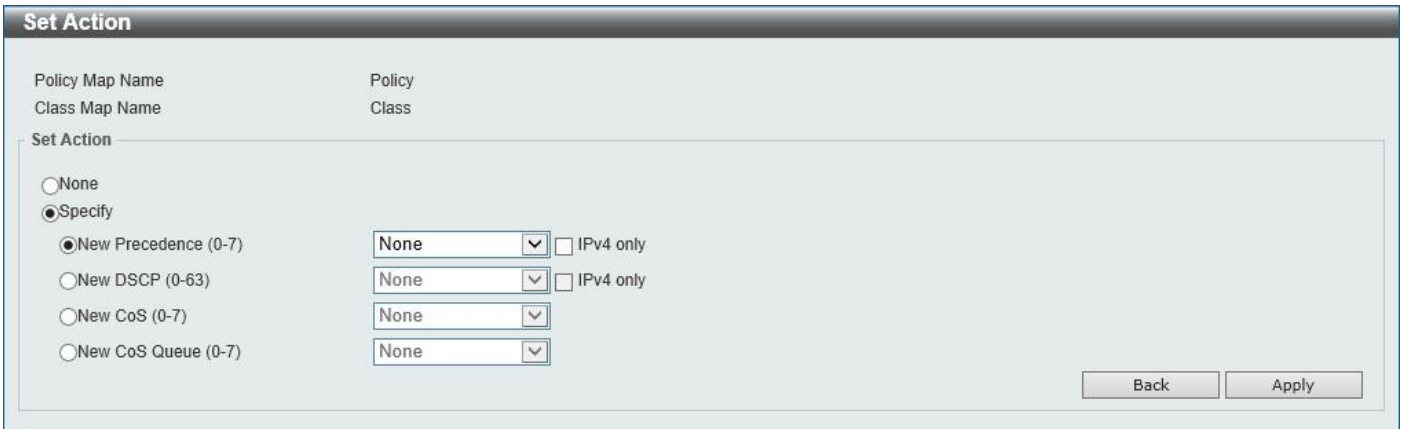

그림 7-14) 정책 맵(Set Action) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
None	아무 작업도 수행하지 않도록 지정하려면 이 옵션을 선택합니다.
Specify	이 옵션을 선택하면 수행된 구성에 따라 작업이 수행되도록 지정할 수 있습니다.
New Precedence	여기에서 패킷에 대한 새 우선 순위 값을 선택합니다. 범위는 0 에서 7 사이입니다. IPv4 전용 옵션을 선택하여 IPv4 우선 순위만 표시되도록 지정합니다. 선택하지 않으면 IPv4 및 IPv6 우선 순위가 모두 표시됩니다. IPv6 패킷의 경우 우선 순위는 IPv6 헤더의 트래픽 클래스에서 가장 중요한 3 비트입니다. 우선 순위를 설정해도 CoS 대기열 선택에는 영향을 주지 않습니다.
New DSCP	여기에서 패킷의 새 DSCP 값을 선택합니다. 범위는 0 에서 63 까지입니다. IPv4 전용 옵션을 선택하여 IPv4 DSCP 만 표시되도록 지정합니다. 이 옵션을 선택하지 않으면 IPv4 및 IPv6 DSCP 가 모두 표시됩니다. DSCP 를 설정해도 CoS 큐 선택에 영향을 미치지 않습니다.
새로운 CoS	여기에서 패킷에 대한 새 CoS 값을 선택합니다. 범위는 0 에서 7 사이입니다. CoS 설정은 CoS 대기열 선택에 영향을 주지 않습니다. CoS 만 표시됩니다.
새 Cos 대기열	여기에서 패킷에 대한 새 CoS 대기열 값을 선택합니다. 이렇게 하면 원래 CoS 대기열 선택을 덮어씁니다. CoS 대기열 설정은 정책 맵이 Interface 에 적용되는 경우 적용됩니다.

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.
Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Policy Binding

이 창은 정책 바인딩 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 QoS > Advanced Settings > Policy Binding 을 클릭합니다.

그림 7-15) 정책 바인딩 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
Direction	여기에서 방향 옵션을 선택합니다. 입력은 수신 트래픽을 지정합니다.
Policy Map Name	여기에 정책 맵 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다. 정책 맵을 이 항목에 연결하지 않으려면 None 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

7. Access Control List (ACL)

ACL Configuration Wizard
ACL Access List
ACL Interface *Access Group*

ACL Configuration Wizard

이 창은 사용자가 새 ACL 액세스 목록을 생성하거나 기존 ACL 액세스 목록을 구성하도록 안내하는 데 사용됩니다.

Step 1 - Create/Update

다음 창을 보려면 아래와 같이 ACL > ACL Configuration Wizard 를 클릭합니다.

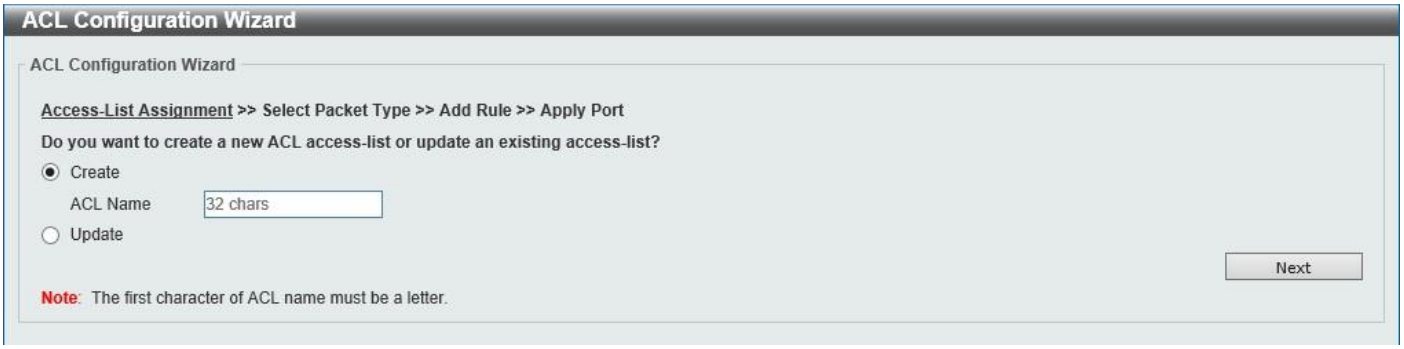

그림 8-1 ACL Configuration Wizard (Create) 창

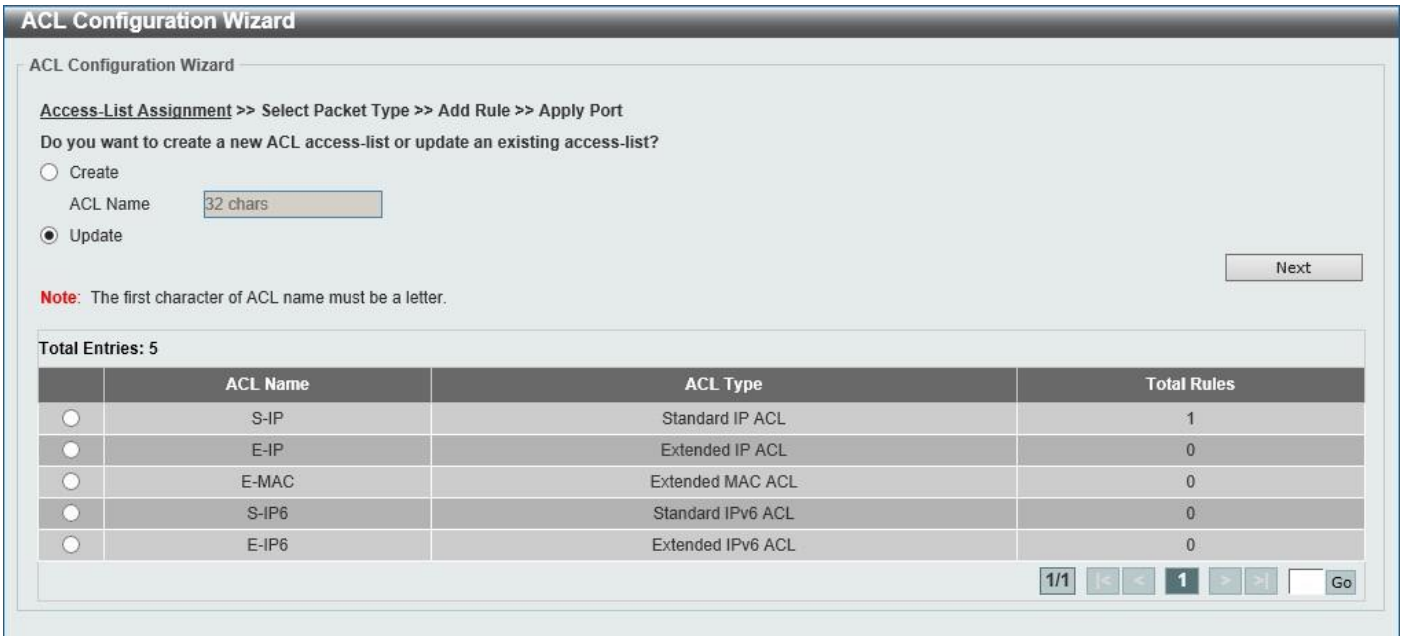

그림 8-2 ACL Configuration Wizard (업데이트) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Create	Configuration Wizard 를 사용하여 새 ACL 액세스 목록을 만들려면 이 옵션을 선택합니다.
ACL Name	여기에 새 ACL 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Update	기존 ACL 액세스 목록을 업데이트하려면 이 옵션을 선택합니다. 업데이트와 함께 처리할 테이블의 기존 ACL 을 선택합니다.

Next 버튼을 클릭하여 다음 단계를 계속합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Step 2- Select Packet Type

Next 버튼을 클릭하면 다음과 같은 창이 나타납니다.

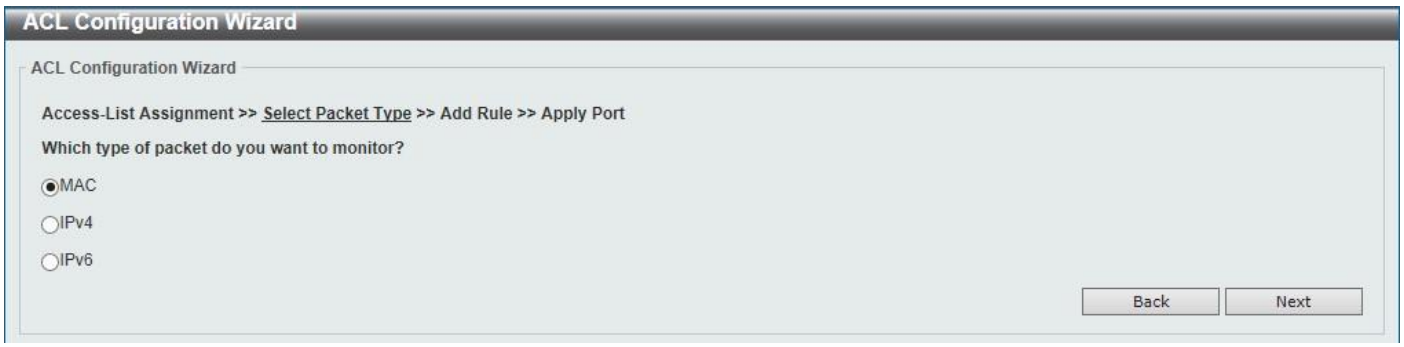

그림 8-3 ACL Configuration Wizard (Create, Packet Type) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
MAC	MAC ACL 을 생성/업데이트하려면 선택합니다.
IPv4	IPv4 ACL 을 생성/업데이트하려면 선택합니다.
IPv6	IPv6 ACL 을 생성/업데이트하려면 선택합니다.

Back 버튼을 클릭하여 이전 단계로 돌아갑니다.

Next 버튼을 클릭하여 다음 단계를 계속합니다.

Step 3 - Add Rule

MAC

MAC 라디오 버튼과 Next 버튼을 클릭하면 다음 창이 나타납니다.

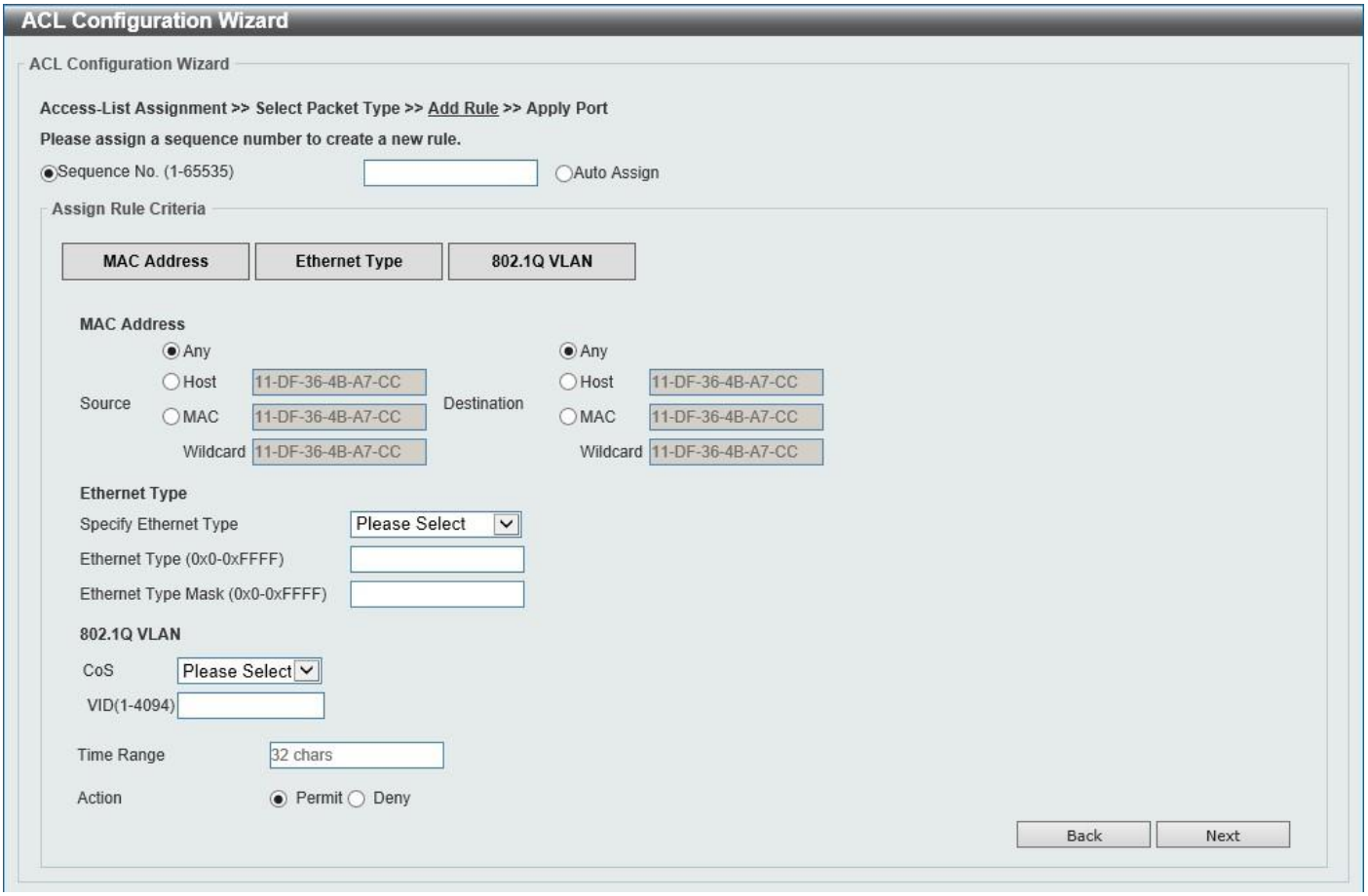

그림 8-4 ACL Configuration Wizard (Create, Packet Type, MAC) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Sequence No.	여기에 ACL 규칙 번호를 입력합니다. 이 값은 1 에서 65535 사이여야 합니다. Auto Assign(자동 할당)을 선택하여 이 항목에 대한 ACL 규칙 번호를 자동으로 생성합니다.
Source	여기에서 소스 MAC 주소 정보를 선택하여 입력합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Any- 이 옵션을 선택하면 모든 소스 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host - 이 옵션을 선택한 경우 여기에 소스 호스트 MAC 주소를 입력합니다. • MAC - 이 옵션을 선택하면 와일드카드 옵션도 사용할 수 있습니다. 제공된 공간에 소스 MAC 주소와 와일드카드 값을 입력합니다.

Destination	여기에서 대상 MAC 주소 정보를 선택하여 입력합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Any- 이 옵션을 선택하면 모든 대상 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host - 이 옵션을 선택한 경우 여기에 대상 호스트 MAC 주소를 입력합니다. • MAC - 이 옵션을 선택하면 와일드카드 옵션도 사용할 수 있습니다. 제공된 공간에 대상 MAC 주소와 와일드카드 값을 입력합니다.
Specify Ethernet Type	여기에서 이더넷 유형 옵션을 선택합니다. 선택할 수 있는 옵션은 AARP, AppleTalk, Decent-IV, EType-6000, ETYPE-8042, LAT, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp 및 arp 입니다.
Ethernet Type	여기에 Ethernet type hexadecimal 값을 입력합니다. 이 값은 0x0 에서 0xFFFF 사이여야 합니다. Ethernet 유형 지정 드롭다운 목록에서 이더넷 유형 프로필을 선택하면 적절한 16 진수 값이 자동으로 입력됩니다.
Ethernet Type Mask	여기에 Ethernet type mask hexadecimal 값을 입력합니다. 이 값은 0x0 에서 0xFFFF 사이여야 합니다. Ethernet 유형 지정 드롭다운 목록에서 이더넷 유형 프로필을 선택하면 적절한 16 진수 값이 자동으로 입력됩니다.
CoS	여기에서 사용할 CoS 값을 선택합니다. 범위는 0 에서 7 사이입니다.
VID	여기에 이 ACL 규칙과 연결할 VLAN ID 를 입력합니다. 범위는 1 에서 4094 사이입니다.
Time Range	이 ACL 규칙에 사용할 시간 범위 프로필의 이름을 여기에 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Action	여기에서 이 규칙이 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 Permit 및 Deny 입니다.

Back 버튼을 클릭하여 이전 단계로 돌아갑니다.

Next 버튼을 클릭하여 다음 단계를 계속합니다.

IPv4

IPv4 라디오 버튼과 Next 버튼을 클릭하면 다음 창이 나타납니다.

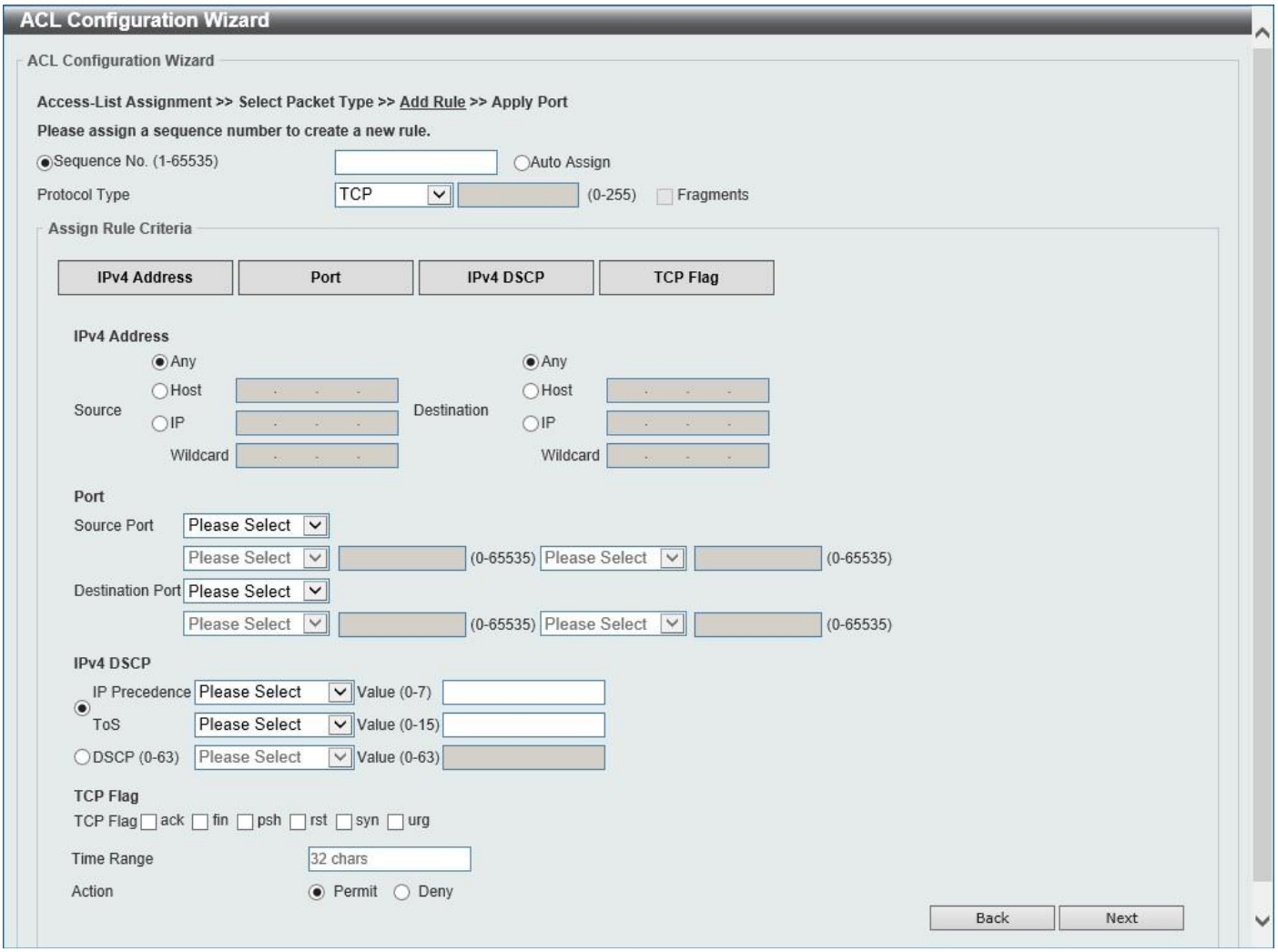

그림 8-5 ACL Configuration Wizard (Create, Packet Type, IPv4) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Sequence No.	여기에 ACL 규칙 번호를 입력합니다. 이 값은 1 에서 65535 사이여야 합니다. Auto Assign(자동 할당)을 선택하여 이 항목에 대한 ACL 규칙 번호를 자동으로 생성합니다.
Protocol Type	여기에서 프로토콜 유형 옵션을 선택합니다. 선택할 수 있는 옵션은 TCP, UDP, ICMP, EIGRP(88), ESP(50), GRE(47), IGMP(2), OSPF(89), PIM(103), VRRP(112), IP-in-IP(94), PCP(108), 프로토콜 ID 및 없음입니다. • 값 - 프로토콜 ID 를 여기에 수동으로 입력할 수도 있습니다. 범위는 0 에서 255 사이입니다. • Fragments - 패킷 프래그먼트 필터링을 포함하려면 이 옵션을 선택합니다.

Assign rule criteria 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Source	여기에서 소스 정보를 선택하고 입력합니다. 선택할 수 있는 옵션은 Any, Host 및 IP 입니다. • Any 옵션을 선택하면 모든 소스 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host 옵션을 선택한 경우 여기에 소스 호스트 IP 주소를 입력합니다. • IP 옵션을 선택하면 와일드카드 옵션도 사용할 수 있습니다. 와일드카드 비트맵을 사용하여 원본 IP 주소 그룹을 입력합니다. 비트 값 1 에 해당하는 비트는 무시됩니다. 비트 값 0 에 해당하는 비트가 확인됩니다.
Destination	여기에서 목적지 정보를 선택하고 입력합니다. 선택할 수 있는 옵션은 Any, Host 및 IP 입니다. • Any 옵션을 선택하면 모든 대상 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host 옵션을 선택한 경우 여기에 대상 호스트 IP Address 를 입력합니다. • IP 옵션을 선택하면 와일드카드 옵션도 사용할 수 있습니다. 와일드카드 비트맵을 사용하여 대상 IP Address 그룹을 입력합니다. 비트 값 1 에 해당하는 비트는 무시됩니다. 비트 값 0 에 해당하는 비트가 확인됩니다.
Source Port	여기에 소스 포트 값을 선택하고 입력합니다. 선택할 수 있는 옵션은 =, >, <, ≠ 및 Range 입니다. • = 옵션을 선택하면 선택한 특정 포트 번호가 사용됩니다. • > 옵션을 선택하면 선택한 포트보다 큰 모든 포트가 사용됩니다. • < 옵션을 선택하면 선택한 포트보다 작은 모든 포트가 사용됩니다. • ≠ 옵션을 선택하면 선택한 포트를 제외한 모든 포트가 사용됩니다. • 범위 옵션을 선택하면 선택한 범위의 시작 포트 번호와 끝 포트 번호가 사용됩니다. 또는 포트 번호를 드롭다운 목록에서 사용할 수 없는 경우 제공된 공간에 포트 번호를 수동으로 입력할 수 있습니다. 이 매개변수는 프로토콜 유형 TCP 및 UDP 에서만 사용할 수 있습니다.
Destination Port	여기에 대상 포트 값을 선택하고 입력합니다. 선택할 수 있는 옵션은 =, >, <, ≠ 및 Range 입니다. • = 옵션을 선택하면 선택한 특정 포트 번호가 사용됩니다. • > 옵션을 선택하면 선택한 포트보다 큰 모든 포트가 사용됩니다. • < 옵션을 선택하면 선택한 포트보다 작은 모든 포트가 사용됩니다. • ≠ 옵션을 선택하면 선택한 포트를 제외한 모든 포트가 사용됩니다. • 범위 옵션을 선택하면 선택한 범위의 시작 포트 번호와 끝 포트 번호가 사용됩니다. 또는 포트 번호를 드롭다운 목록에서 사용할 수 없는 경우 제공된 공간에 포트 번호를 수동으로 입력할 수 있습니다. 이 매개변수는 프로토콜 유형 TCP 및 UDP 에서만 사용할 수 있습니다.
Specify ICMP Message Type	여기에 사용된 ICMP 메시지 유형을 선택합니다. 이 매개변수는 프로토콜 유형 ICMP 에서만 사용할 수 있습니다.

ICMP Message Type	ICMP Message Type(ICMP 메시지 유형)을 선택하지 않은 경우 여기에 사용된 ICMP Message Type(ICMP 메시지 유형) 숫자 값을 입력합니다. 범위는 0 에서 255 사이입니다. ICMP 메시지 유형을 선택하면 이 숫자 값이 자동으로 입력됩니다. 이 매개변수는 프로토콜 유형 ICMP 에서만 사용할 수 있습니다.
Message Code	ICMP Message Type(ICMP 메시지 유형)을 선택하지 않은 경우 여기에 사용된 Message Code(메시지 코드) 숫자 값을 입력합니다. 범위는 0 에서 255 사이입니다. ICMP 메시지 유형을 선택하면 이 숫자 값이 자동으로 입력됩니다. 이 매개변수는 프로토콜 유형 ICMP 에서만 사용할 수 있습니다.
IP Precedence	여기에서 사용되는 IP 우선 순위 값을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다 (0), 우선순위(1), 즉시(2), 플래시(3), 플래시 override(4), 중요(5), 인터넷 (6), 및 네트워크(7) • Value - IP 우선 순위 값은 여기에 수동으로 입력할 수도 있습니다. 범위는 0 ~ 7 입니다.
ToS	여기에서 사용할 ToS(Type-of-Service) 값을 선택합니다. 선택할 수 있는 옵션은 normal(0), min-monetary-cost(1), max-reliability(2), maxthroughput(4) 및 min-delay(8) 중에서 선택할 수 있습니다. • Value - ToS 값을 여기에 수동으로 입력할 수도 있습니다. 범위는 0 에서 15 사이입니다.
DSCP	여기에서 사용할 DSCP 값을 선택합니다. 선택할 수 있는 옵션은 기본값입니다 (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), AF33 (30), AF41 (34), AF42 (36), AF43 (38), CS1 (8), CS2 (16), CS3 (24), CS4 (32), CS5 (40), CS6 (48), CS7 (56) 및 EF (46). • Value - DSCP 값을 여기에 수동으로 입력할 수도 있습니다. 범위는 0 에서 63 사이입니다.
TCP 플래그	이 규칙에 플래그를 포함하려면 적절한 TCP 플래그 옵션을 선택합니다. 선택할 수 있는 옵션은 ack, fin, psh, rst, syn 및 urg 입니다. 이 매개변수는 프로토콜 유형 TCP 에서만 사용할 수 있습니다.
시간 범위	이 ACL 규칙에 사용할 시간 범위 프로필의 이름을 여기에 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Action	여기에서 이 규칙이 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 Permit 및 Deny 입니다.

Back 버튼을 클릭하여 이전 단계로 돌아갑니다.

Next 버튼을 클릭하여 다음 단계를 계속합니다.

IPv6

IPv6 라디오 버튼과 Next 버튼을 클릭하면 다음 창이 나타납니다.

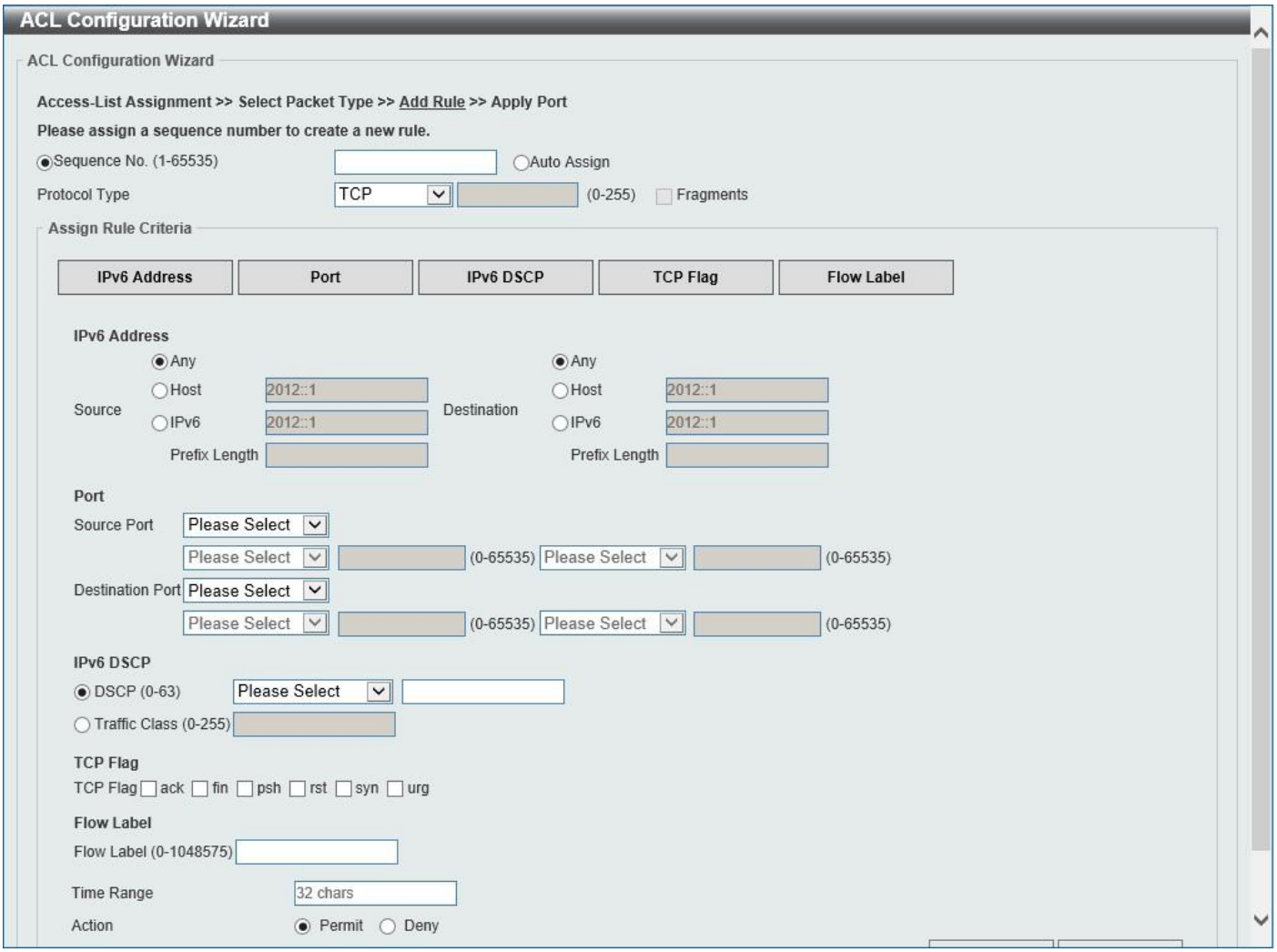

그림 8-6) ACL Configuration Wizard (Create, Packet Type, IPv6) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Sequence No.	여기에 ACL 규칙 번호를 입력합니다. 이 값은 1 에서 65535 사이여야 합니다. Auto Assign(자동 할당)을 선택하여 이 항목에 대한 ACL 규칙 번호를 자동으로 생성합니다.
Protocol Type	여기에서 프로토콜 유형 옵션을 선택합니다. 선택할 수 있는 옵션은 TCP, UDP, ICMP, 프로토콜 ID, ESP(50), PCP(108), SCTP(132) 및 없음입니다. • Value - 프로토콜 ID 를 여기에 수동으로 입력할 수도 있습니다. 범위는 0 에서 255 사이입니다. • Fragments - 패킷 프래그먼트 필터링을 포함하려면 이 옵션을 선택합니다.

Assign rule criteria(규칙 기준 할당)에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Source	여기에서 소스 정보를 선택하고 입력합니다. 선택할 수 있는 옵션은 Any, Host 및 IPv6 입니다. • Any 옵션을 선택하면 모든 소스 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host 옵션을 선택한 경우 여기에 소스 호스트 IPv6 주소를 입력합니다. • IPv6 옵션을 선택하면 접두사 길이 옵션도 사용할 수 있습니다. 제공된 공간에 소스 IPv6 주소 및 접두사 길이 값을 입력합니다.
Destination	여기에서 목적지 정보를 선택하고 입력합니다. 선택할 수 있는 옵션은 Any, Host 및 IPv6 입니다. • Any 옵션을 선택하면 모든 대상 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host 옵션을 선택한 경우 여기에 대상 호스트 IPv6 주소를 입력합니다. • IPv6 옵션을 선택하면 접두사 길이 옵션도 사용할 수 있습니다. 제공된 공간에 대상 IPv6 주소 및 접두사 길이 값을 입력합니다.
Source Port	여기에 소스 포트 값을 선택하고 입력합니다. 선택할 수 있는 옵션은 =, >, <, ≠ 및 Range 입니다. • = 옵션을 선택하면 선택한 특정 포트 번호가 사용됩니다. • > 옵션을 선택하면 선택한 포트보다 큰 모든 포트가 사용됩니다. • < 옵션을 선택하면 선택한 포트보다 작은 모든 포트가 사용됩니다. • ≠ 옵션을 선택하면 선택한 포트를 제외한 모든 포트가 사용됩니다. • 범위 옵션을 선택하면 선택한 범위의 시작 포트 번호와 끝 포트 번호가 사용됩니다. 또는 포트 번호를 드롭다운 목록에서 사용할 수 없는 경우 제공된 공간에 포트 번호를 수동으로 입력할 수 있습니다. 이 매개변수는 프로토콜 유형 TCP 및 UDP 에서만 사용할 수 있습니다.
Destination Port	여기에 대상 포트 값을 선택하고 입력합니다. 선택할 수 있는 옵션은 =, >, <, ≠ 및 Range 입니다. • = 옵션을 선택하면 선택한 특정 포트 번호가 사용됩니다. • > 옵션을 선택하면 선택한 포트보다 큰 모든 포트가 사용됩니다. • < 옵션을 선택하면 선택한 포트보다 작은 모든 포트가 사용됩니다. • ≠ 옵션을 선택하면 선택한 포트를 제외한 모든 포트가 사용됩니다. • 범위 옵션을 선택하면 선택한 범위의 시작 포트 번호와 끝 포트 번호가 사용됩니다. 또는 포트 번호를 드롭다운 목록에서 사용할 수 없는 경우 제공된 공간에 포트 번호를 수동으로 입력할 수 있습니다. 이 매개변수는 프로토콜 유형 TCP 및 UDP 에서만 사용할 수 있습니다.
Specify ICMP Message Type	여기에 사용된 ICMP 메시지 유형을 선택합니다. 이 매개변수는 프로토콜 유형 ICMP 에서만 사용할 수 있습니다.
ICMP Message Type	ICMP Message Type(ICMP 메시지 유형)을 선택하지 않은 경우 여기에 사용된 ICMP Message Type(ICMP 메시지 유형) 숫자 값을 입력합니다. 범위는 0 에서 255 사이입니다. ICMP 메시지 유형을 선택하면 이 숫자 값이 자동으로 입력됩니다. 이 매개변수는 프로토콜 유형 ICMP 에서만 사용할 수 있습니다.

Message Code	ICMP Message Type 을 선택하지 않은 경우 여기에 사용된 Message Code 숫자 값을 입력합니다. 범위는 0 에서 255 사이입니다. ICMP 메시지 유형을 선택하면 이 숫자 값이 자동으로 입력됩니다. 이 매개변수는 프로토콜 유형 ICMP 에서만 사용할 수 있습니다.
DSCP	여기에서 사용할 DSCP 값을 선택합니다. 선택할 수 있는 옵션은 기본값입니다 (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), AF33 (30), AF41 (34), AF42 (36), AF43 (38), CS1 (8), CS2 (16), CS3 (24), CS4 (32), CS5 (40), CS6 (48), CS7 (56) 및 EF (46). • Value - DSCP 값을 여기에 수동으로 입력할 수도 있습니다. 범위는 0 에서 63 사이입니다.
Traffic Class	여기에서 트래픽 클래스 값을 선택하고 입력합니다. 범위는 0 에서 255 사이입니다.
TCP Flag	이 규칙에 플래그를 포함하려면 적절한 TCP 플래그 옵션을 선택합니다. 선택할 수 있는 옵션은 ack, fin, psh, rst, syn 및 urg 입니다. 이 매개변수는 프로토콜 유형 TCP 에서만 사용할 수 있습니다.
Flow Label	여기에 흐름 레이블 값을 입력합니다. 이 값은 0 에서 1048575 사이여야 합니다.
Time Range	이 ACL 규칙에 사용할 시간 범위 프로필의 이름을 여기에 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Action	여기에서 이 규칙이 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 Permit 및 Deny 입니다.

Back 버튼을 클릭하여 이전 단계로 돌아갑니다.

Next 버튼을 클릭하여 다음 단계를 계속합니다.

Step 4 - Apply Port

Next 버튼을 클릭하면 다음과 같은 창이 나타납니다.

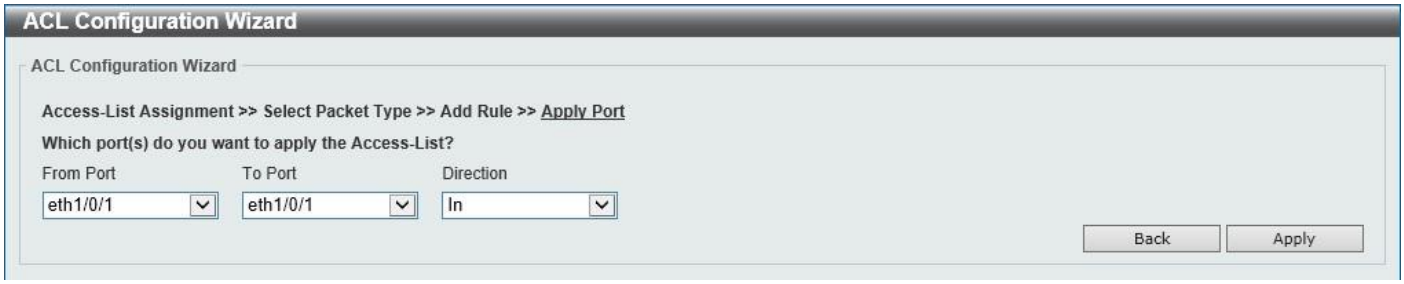

그림 8-7 ACL Configuration Wizard (Create, Port) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
Direction	In 방향이 사용되도록 지정합니다.

Back 버튼을 클릭하여 이전 단계로 돌아갑니다.

Apply 버튼을 클릭하여 변경 사항을 적용하고 기본 ACL Wizard 창으로 돌아갑니다.

ACL Access List

이 창은 ACL, ACL 규칙 및 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 ACL > ACL Access List 를 클릭합니다.

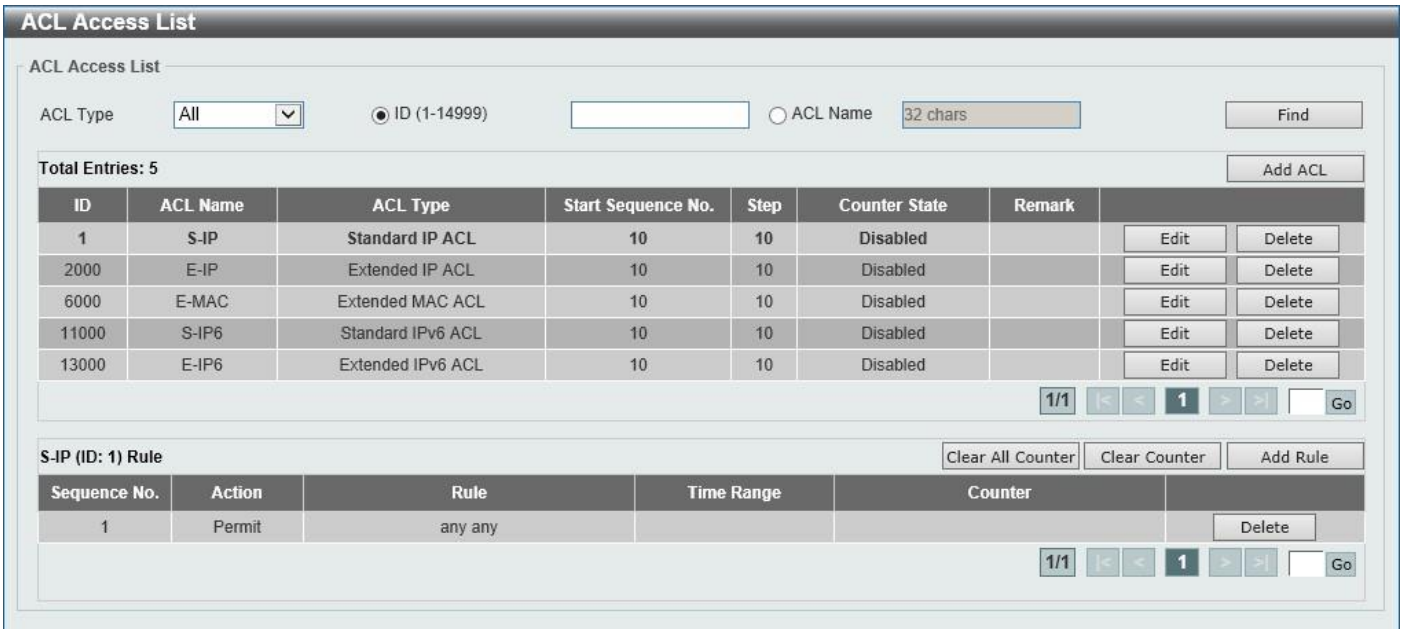

그림 8-8) ACL 액세스 목록 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
ACL Type	여기에서 찾을 ACL 유형을 선택합니다. 선택할 수 있는 옵션은 모두, IP ACL, IPv6 ACL 및 MAC ACL 입니다.
ID	여기에서 액세스 목록 ID 를 선택하고 입력합니다. 범위는 1 에서 14999 사이입니다.
ACL Name	여기에서 액세스 목록 이름을 선택하고 입력합니다. 이 이름은 최대 32 자까지 가능합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Add ACL 버튼을 클릭하여 새 ACL 을 생성합니다.

Edit 버튼을 클릭하여 특정 ACL 을 재구성합니다.

ACL 옆에 있는 Delete 버튼을 클릭하여 특정 ACL 을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Clear All Counter 버튼을 클릭하여 표시된 모든 카운터 정보를 지웁니다.

Clear Counter 버튼을 클릭하여 표시된 규칙에 대한 카운터 정보를 지웁니다.

Add Rule 버튼을 클릭하여 선택한 ACL 에 대한 ACL 규칙을 생성합니다.

ACL 규칙 옆에 있는 Delete 버튼을 클릭하여 특정 ACL 규칙을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Edit 버튼을 클릭하면 다음 페이지가 나타납니다.

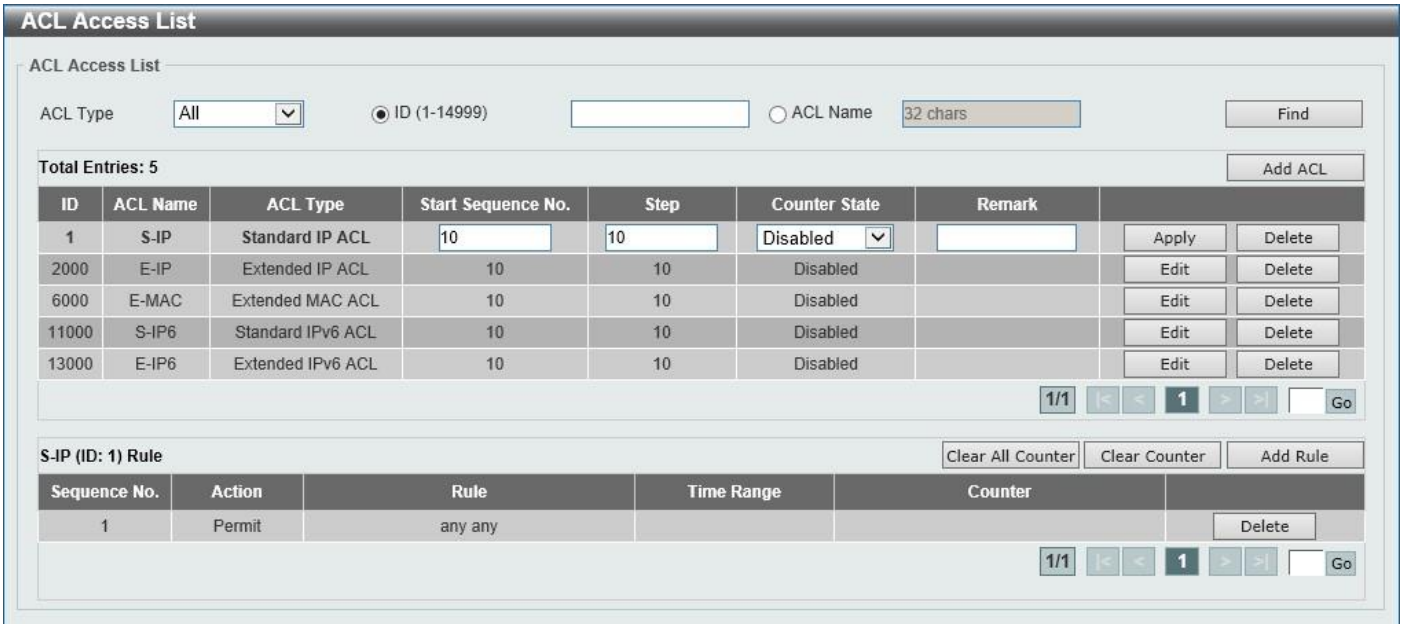

그림 8-9) ACL 액세스 목록(편집) 창

Edit 버튼을 클릭하면 구성할 수 있는 필드가 아래에 설명되어 있습니다.

Parameter	Description
Start Sequence No.	여기에 시작 Sequence No.를 입력합니다.
Step	여기에 Sequence No. 단계를 입력합니다. 단계 범위는 1 에서 32 까지입니다. Sequence No.가 단계별로 표시되는 번호를 지정합니다. 기본값은 10 입니다. 예를 들어, 증분(단계) 값이 5 이고 시작 Sequence No.가 20 인 경우 후속 Sequence No.는 25, 30, 35, 40 등입니다.
Counter State	여기에서 카운터 상태 옵션을 활성화하거나 비활성화하려면 선택합니다.
Remark	여기에 이 ACL 과 연결할 선택적 설명을 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Add ACL 버튼을 클릭하면 다음 페이지가 나타납니다.

그림 8-10) ACL 액세스 목록(ACL 추가) 창

Add ACL 버튼을 클릭한 후 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
ACL Type	여기에서 생성할 ACL 유형을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다 표준 IP ACL, 확장 IP ACL, 표준 IPv6 ACL, 확장 IPv6 ACL 및 확장 MAC ACL.
ID	여기에 ACL 의 ID 를 입력합니다. • 표준 IP ACL 의 경우 범위는 1 에서 1999 까지입니다. • 확장 IP ACL 의 경우 범위는 2000 에서 3999 사이입니다.

	• 표준 IPv6 ACL 의 경우 범위는 11000 에서 12999 사이입니다. • 확장 IPv6 ACL 의 경우 범위는 13000 에서 14999 까지입니다. • 확장 MAC ACL 의 경우 범위는 6000 에서 7999 사이입니다.
ACL Name	여기에 ACL 의 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Standard IP ACL

표준 IP ACL 을 선택하고 Add Rule 버튼을 클릭하면 다음 페이지가 나타납니다.

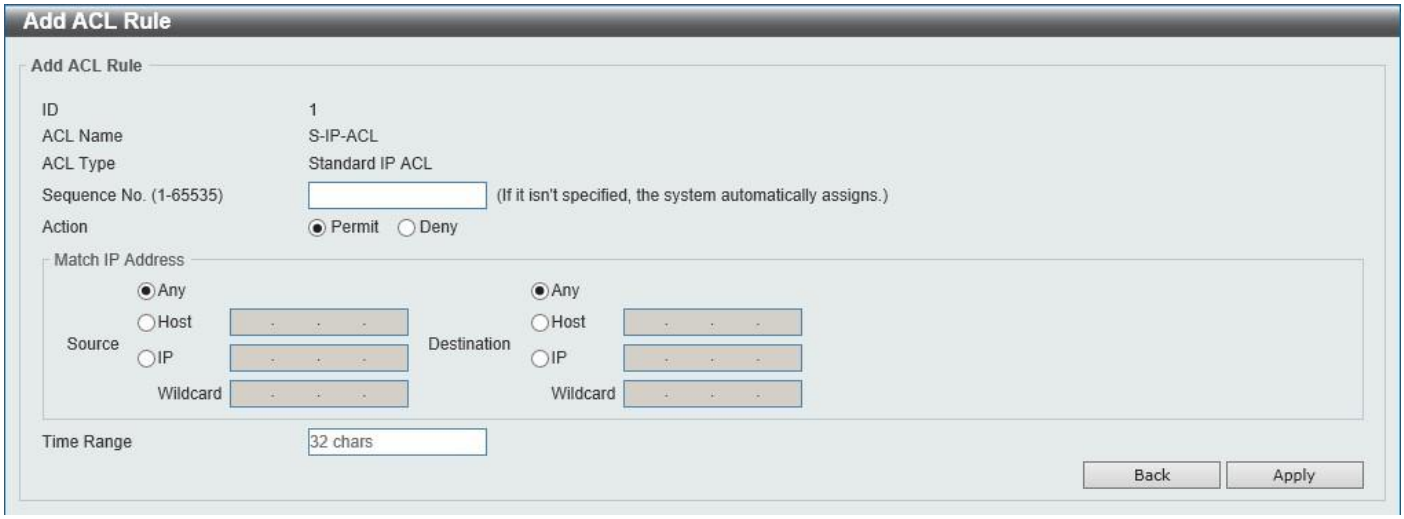

그림 8-11) 표준 IP ACL(규칙 추가) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Sequence No.	여기에 이 ACL 규칙의 Sequence No.를 입력합니다. 범위는 1 에서 65535 사이입니다. 이 값을 지정하지 않으면 시스템은 이 항목에 대한 ACL 규칙 번호를 자동으로 생성합니다.
Action	여기에서 이 규칙이 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 Permit(허용) 및 Deny(거부)입니다.
Source	여기에서 소스 정보를 선택하고 입력합니다. 선택할 수 있는 옵션은 Any, Host, IP 및 Wildcard 입니다. • Any 옵션을 선택하면 모든 소스 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host 옵션을 선택한 경우 여기에 소스 호스트 IP Address 를 입력합니다. • IP 옵션을 선택하면 와일드카드 옵션도 사용할 수 있습니다. 와일드카드 비트맵을 사용하여 원본 IP Address 그룹을 입력합니다. 비트 값 1 에 해당하는 비트는 무시됩니다. 비트 값 0 에 해당하는 비트가 확인됩니다.
Destination	여기에서 목적지 정보를 선택하고 입력합니다. 선택할 수 있는 옵션은 Any, Host, IP 및 Wildcard 입니다. • Any 옵션을 선택하면 모든 대상 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host 옵션을 선택한 경우 여기에 대상 호스트 IP Address 를 입력합니다. • IP 옵션을 선택하면 와일드카드 옵션도 사용할 수 있습니다.

	와일드카드 비트맵을 사용하여 대상 IP Address 그룹을 입력합니다. 비트 값 1 에 해당하는 비트는 무시됩니다. 비트 값 0 에 해당하는 비트가 확인됩니다.
시간 범위	이 ACL 규칙에 사용할 시간 범위 프로필의 이름을 여기에 입력합니다. 이 이름은 최대 32 자까지 가능합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Back 버튼을 클릭하여 변경 사항을 취소하고 이전 페이지로 돌아갑니다.

Extended IP ACL

Extended IP ACL 을 선택하고 Add Rule 버튼을 클릭하면 다음 페이지가 나타납니다.

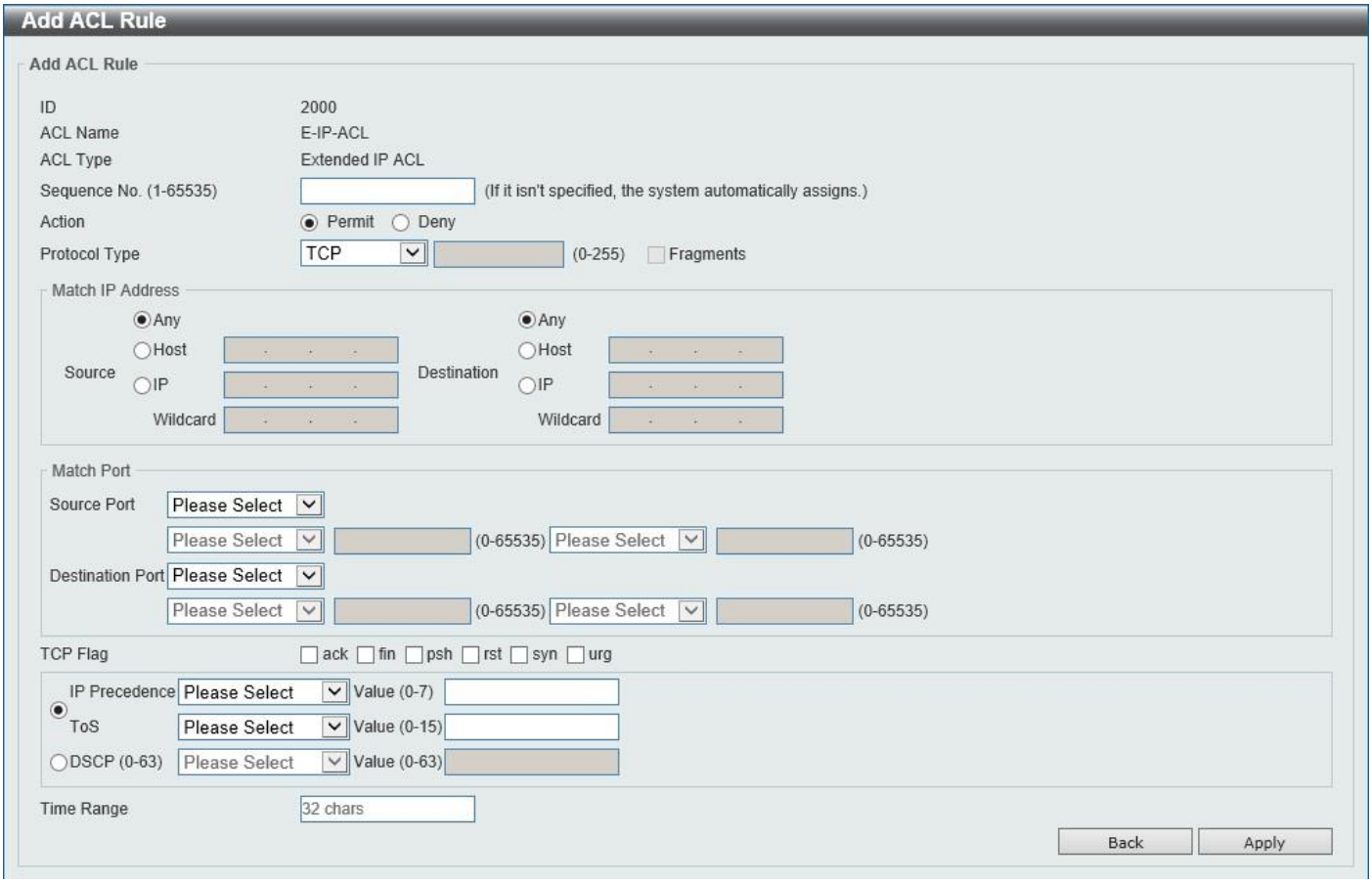

그림 8-12) 확장 IP ACL(규칙 추가) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Sequence No.	여기에 이 ACL 규칙의 Sequence No.를 입력합니다. 범위는 1 에서 65535 사이입니다. 이 값을 지정하지 않으면 시스템은 이 항목에 대한 ACL 규칙 번호를 자동으로 생성합니다.

Action	여기에서 이 규칙이 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 Permit(허용) 및 Deny(거부)입니다.
Protocol Type	여기에서 프로토콜 유형 옵션을 선택합니다. 선택할 수 있는 옵션은 TCP, UDP, ICMP, EIGRP(88), ESP(50), GRE(47), IGMP(2), OSPF(89), PIM(103), VRRP(112), IP-in-IP(94), PCP(108), 프로토콜 ID 및 없음입니다. • 값 - 프로토콜 ID 를 여기에 수동으로 입력할 수도 있습니다. 범위는 0 에서 255 사이입니다. • Fragments(프래그먼트) - 패킷 프래그먼트 필터링을 포함하려면 이 옵션을 선택합니다.
Source	여기에서 소스 IP 정보를 선택하여 입력합니다. 선택할 수 있는 옵션은 Any, Host 및 IP 입니다. • Any 옵션을 선택하면 모든 소스 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host 옵션을 선택한 경우 여기에 소스 호스트 IP Address 를 입력합니다. • IP 옵션을 선택하면 와일드카드 옵션도 사용할 수 있습니다. 와일드카드 비트맵을 사용하여 원본 IP Address 그룹을 입력합니다. 비트 값 1 에 해당하는 비트는 무시됩니다. 비트 값 0 에 해당하는 비트가 확인됩니다.
Destination	여기에서 대상 IP 정보를 선택하여 입력합니다. 선택할 수 있는 옵션은 Any, Host 및 IP 입니다. • Any 옵션을 선택하면 모든 대상 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host 옵션을 선택한 경우 여기에 대상 호스트 IP Address 를 입력합니다. • IP 옵션을 선택하면 와일드카드 옵션도 사용할 수 있습니다. 와일드카드 비트맵을 사용하여 대상 IP Address 그룹을 입력합니다. 비트 값 1 에 해당하는 비트는 무시됩니다. 비트 값 0 에 해당하는 비트가 확인됩니다.
Source Port	여기에 소스 포트 값을 선택하고 입력합니다. 선택할 수 있는 옵션은 =, >, <, ≠ 및 Range 입니다. • = 옵션을 선택하면 선택한 특정 포트 번호가 사용됩니다. • > 옵션을 선택하면 선택한 포트보다 큰 모든 포트가 사용됩니다. • < 옵션을 선택하면 선택한 포트보다 작은 모든 포트가 사용됩니다. • ≠ 옵션을 선택하면 선택한 포트를 제외한 모든 포트가 사용됩니다. • 범위 옵션을 선택하면 선택한 범위의 시작 포트 번호와 끝 포트 번호가 사용됩니다. 또는 포트 번호를 드롭다운 목록에서 사용할 수 없는 경우 제공된 공간에 포트 번호를 수동으로 입력할 수 있습니다. 이 매개변수는 프로토콜 유형 TCP 및 UDP 에서만 사용할 수 있습니다.

Destination Port	여기에 대상 포트 값을 선택하고 입력합니다. 선택할 수 있는 옵션은 =, >, <, ≠ 및 Range 입니다. • = 옵션을 선택하면 선택한 특정 포트 번호가 사용됩니다. • > 옵션을 선택하면 선택한 포트보다 큰 모든 포트가 사용됩니다. • < 옵션을 선택하면 선택한 포트보다 작은 모든 포트가 사용됩니다. • ≠ 옵션을 선택하면 선택한 포트를 제외한 모든 포트가 사용됩니다. • 범위 옵션을 선택하면 선택한 범위의 시작 포트 번호와 끝 포트 번호가 사용됩니다. 또는 포트 번호를 드롭다운 목록에서 사용할 수 없는 경우 제공된 공간에 포트 번호를 수동으로 입력할 수 있습니다. 이 매개변수는 프로토콜 유형 TCP 및 UDP 에서만 사용할 수 있습니다.
Specify ICMP Message Type	여기에 사용된 ICMP 메시지 유형을 선택합니다. 이 매개변수는 프로토콜 유형 ICMP 에서만 사용할 수 있습니다.
ICMP Message Type	ICMP Message Type(ICMP 메시지 유형)을 선택하지 않은 경우 여기에 사용된 ICMP Message Type(ICMP 메시지 유형) 숫자 값을 입력합니다. 범위는 0 에서 255 사이입니다. ICMP 메시지 유형을 선택하면 이 숫자 값이 자동으로 입력됩니다. 이 매개변수는 프로토콜 유형 ICMP 에서만 사용할 수 있습니다.
Message Code	ICMP Message Type(ICMP 메시지 유형)을 선택하지 않은 경우 여기에 사용된 Message Code(메시지 코드) 숫자 값을 입력합니다. 범위는 0 에서 255 사이입니다. ICMP 메시지 유형을 선택하면 이 숫자 값이 자동으로 입력됩니다. 이 매개변수는 프로토콜 유형 ICMP 에서만 사용할 수 있습니다.
TCP Flag	이 규칙에 플래그를 포함하려면 적절한 TCP 플래그 옵션을 선택합니다. 선택할 수 있는 옵션은 ack, fin, psh, rst, syn 및 urg 입니다. 이 매개변수는 프로토콜 유형 TCP 에서만 사용할 수 있습니다.
IP Precedence	여기에 사용된 IP 우선 순위 값을 선택합니다. 선택할 수 있는 옵션은 루틴(0), 우선 순위(1), 즉시(2), 플래시(3), 플래시 오버라이드(4), 중요(5), 인터넷입니다 (6) 및 네트워크 (7). • Value - IP 우선 순위 값을 여기에 수동으로 입력할 수도 있습니다. 범위는 0 에서 7 사이입니다.
ToS	여기에서 사용할 ToS(Type-of-Service) 값을 선택합니다. 선택할 수 있는 옵션은 normal(0), min-monetary-cost(1), max-reliability(2), maxthroughput(4) 및 min-delay(8) 중에서 선택할 수 있습니다. • Value - ToS 값을 여기에 수동으로 입력할 수도 있습니다. 범위는 0 에서 15 사이입니다.
DSCP	여기에서 사용할 DSCP 값을 선택합니다. 선택할 수 있는 옵션은 기본값입니다 (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), AF33 (30), AF41 (34), AF42 (36), AF43 (38), CS1 (8), CS2 (16), CS3 (24), CS4 (32), CS5 (40), CS6 (48), CS7 (56) 및 EF (46). 값 - DSCP 값을 여기에 수동으로 입력할 수도 있습니다. 범위는 0 에서 63 사이입니다.
Time Range	이 ACL 규칙에 사용할 시간 범위 프로필의 이름을 여기에 입력합니다. 이 이름은 최대 32 자까지 가능합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Back 버튼을 클릭하여 변경 사항을 취소하고 이전 페이지로 돌아갑니다.

Standard IPv6 ACL

Standard IPv6 ACL 을 선택하고 Add Rule 버튼을 클릭하면 다음 페이지가 나타납니다.

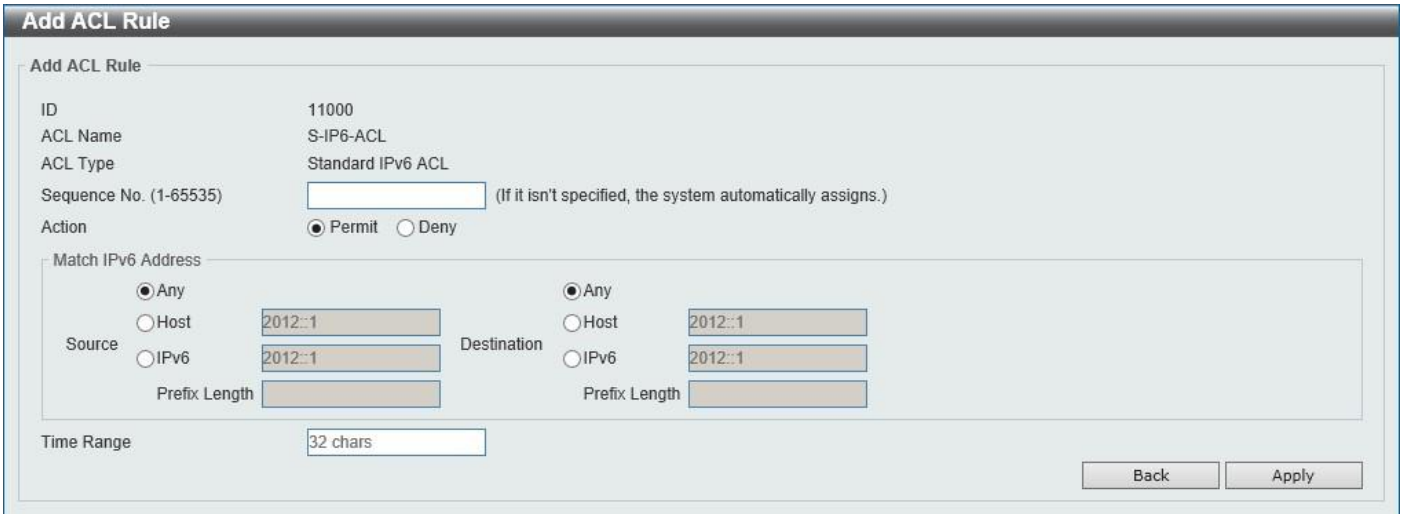

그림 8-13) 표준 IPv6 ACL(규칙 추가) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Sequence No.	여기에 이 ACL 규칙의 Sequence No.를 입력합니다. 범위는 1 에서 65535 사이입니다. 이 값을 지정하지 않으면 시스템은 이 항목에 대한 ACL 규칙 번호를 자동으로 생성합니다.
Action	여기에서 이 규칙이 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 Permit(허용) 및 Deny(거부)입니다.
Source	여기에서 소스 IPv6 정보를 선택하여 입력합니다. 선택할 수 있는 옵션은 Any, Host, IPv6(IPv6) 및 Prefix Length(접두사 길이)입니다. • Any 옵션을 선택하면 모든 소스 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host 옵션을 선택한 경우 여기에 소스 호스트 IPv6 주소를 입력합니다. • IPv6 옵션을 선택하면 접두사 길이 옵션도 사용할 수 있습니다. 제공된 공간에 소스 IPv6 주소 및 접두사 길이 값을 입력합니다.
Destination	여기에서 대상 IPv6 정보를 선택하여 입력합니다. 선택할 수 있는 옵션은 Any, Host, IPv6(IPv6) 및 Prefix Length(접두사 길이)입니다. • Any 옵션을 선택하면 모든 대상 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host 옵션을 선택한 경우 여기에 대상 호스트 IPv6 주소를 입력합니다. • IPv6 옵션을 선택하면 접두사 길이 옵션도 사용할 수 있습니다. 제공된 공간에 대상 IPv6 주소 및 접두사 길이 값을 입력합니다.
Time Range	이 ACL 규칙에 사용할 시간 범위 프로필의 이름을 여기에 입력합니다. 이 이름은 최대 32 자까지 가능합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Back 버튼을 클릭하여 변경 사항을 취소하고 이전 페이지로 돌아갑니다.

Extended IPv6 ACL

Extended IPv6 ACL 을 선택하고 Add Rule 버튼을 클릭하면 다음 페이지가 나타납니다.

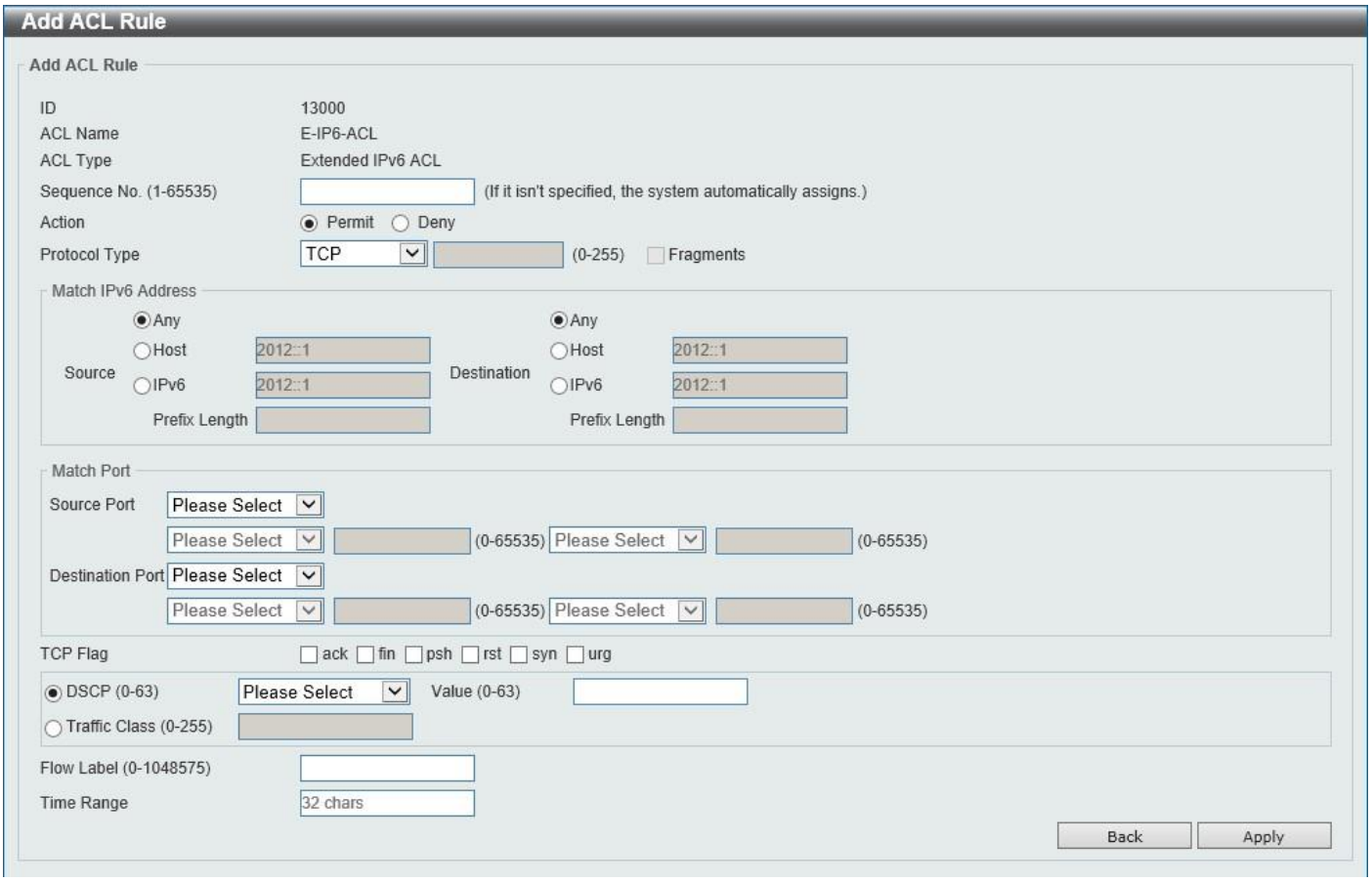

그림 8-14) 확장 IPv6 ACL(규칙 추가) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Sequence No.	여기에 이 ACL 규칙의 Sequence No.를 입력합니다. 범위는 1 에서 65535 사이입니다. 이 값을 지정하지 않으면 시스템은 이 항목에 대한 ACL 규칙 번호를 자동으로 생성합니다.
Action	여기에서 이 규칙이 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 Permit(허용) 및 Deny(거부)입니다.
Protocol Type	여기에서 프로토콜 유형 옵션을 선택합니다. 선택할 수 있는 옵션은 TCP, UDP, ICMP, 프로토콜 ID, ESP(50), PCP(108), SCTP(132) 및 없음입니다. • 값 - 프로토콜 ID 를 여기에 수동으로 입력할 수도 있습니다. 범위는 0 에서 255 사이입니다. • Fragments(프래그먼트) - 패킷 프래그먼트 필터링을 포함하려면 이 옵션을 선택합니다.
Source	여기에서 소스 IPv6 정보를 선택하여 입력합니다. 선택할 수 있는 옵션은 Any, Host 및 IPv6 입니다. • Any 옵션을 선택하면 모든 소스 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host 옵션을 선택한 경우 여기에 소스 호스트 IPv6 주소를 입력합니다. • IPv6 옵션을 선택하면 접두사 길이 옵션도 사용할 수 있습니다. 제공된 공간에 소스 IPv6 주소 및 접두사 길이 값을 입력합니다.

목적지	여기에서 대상 IPv6 정보를 선택하여 입력합니다. 선택할 수 있는 옵션은 Any, Host 및 IPv6 입니다. • Any 옵션을 선택하면 모든 대상 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host 옵션을 선택한 경우 여기에 대상 호스트 IPv6 주소를 입력합니다. • IPv6 옵션을 선택하면 접두사 길이 옵션도 사용할 수 있습니다. 제공된 공간에 대상 IPv6 주소 및 접두사 길이 값을 입력합니다.
Source Port(소스 포트)	여기에 소스 포트 값을 선택하고 입력합니다. 선택할 수 있는 옵션은 =, >, <, ≠ 및 Range 입니다. • = 옵션을 선택하면 선택한 특정 포트 번호가 사용됩니다. • > 옵션을 선택하면 선택한 포트보다 큰 모든 포트가 사용됩니다. • < 옵션을 선택하면 선택한 포트보다 작은 모든 포트가 사용됩니다. • ≠ 옵션을 선택하면 선택한 포트를 제외한 모든 포트가 사용됩니다. • 범위 옵션을 선택하면 선택한 범위의 시작 포트 번호와 끝 포트 번호가 사용됩니다. 또는 포트 번호를 드롭다운 목록에서 사용할 수 없는 경우 제공된 공간에 포트 번호를 수동으로 입력할 수 있습니다. 이 매개변수는 프로토콜 유형 TCP 및 UDP 에서만 사용할 수 있습니다.
대상 포트	여기에 대상 포트 값을 선택하고 입력합니다. 선택할 수 있는 옵션은 =, >, <, ≠ 및 Range 입니다. • = 옵션을 선택하면 선택한 특정 포트 번호가 사용됩니다. • > 옵션을 선택하면 선택한 포트보다 큰 모든 포트가 사용됩니다. • < 옵션을 선택하면 선택한 포트보다 작은 모든 포트가 사용됩니다. • ≠ 옵션을 선택하면 선택한 포트를 제외한 모든 포트가 사용됩니다. • 범위 옵션을 선택하면 선택한 범위의 시작 포트 번호와 끝 포트 번호가 사용됩니다. 또는 포트 번호를 드롭다운 목록에서 사용할 수 없는 경우 제공된 공간에 포트 번호를 수동으로 입력할 수 있습니다. 이 매개변수는 프로토콜 유형 TCP 및 UDP 에서만 사용할 수 있습니다.
Parameter	**Description**
TCP 플래그	이 규칙에 플래그를 포함하려면 적절한 TCP 플래그 옵션을 선택합니다. 선택할 수 있는 옵션은 ack, fin, psh, rst, syn 및 urg 입니다. 이 매개변수는 프로토콜 유형 TCP 에서만 사용할 수 있습니다.
ICMP 메시지 유형 지정	여기에 사용된 ICMP 메시지 유형을 선택합니다. 이 매개변수는 프로토콜 유형 ICMP 에서만 사용할 수 있습니다.
ICMP 메시지 유형	ICMP Message Type(ICMP 메시지 유형)을 선택하지 않은 경우 여기에 사용된 ICMP Message Type(ICMP 메시지 유형) 숫자 값을 입력합니다. 범위는 0 에서 255 사이입니다. ICMP 메시지 유형을 선택하면 이 숫자 값이 자동으로 입력됩니다. 이 매개변수는 프로토콜 유형 ICMP 에서만 사용할 수 있습니다.
메시지 코드	ICMP Message Type(ICMP 메시지 유형)을 선택하지 않은 경우 여기에 사용된 Message Code(메시지 코드) 숫자 값을 입력합니다. 범위는 0 에서 255 사이입니다. ICMP 메시지 유형을 선택하면 이 숫자 값이 자동으로 입력됩니다. 이 매개변수는 프로토콜 유형 ICMP 에서만 사용할 수 있습니다.

DSCP (주)디에스피	여기에서 사용할 DSCP 값을 선택합니다. 선택할 수 있는 옵션은 기본값 입니다 (0), af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), AF33 (30), AF41 (34), AF42 (36), AF43 (38), CS1 (8), CS2 (16), CS3 (24), CS4 (32), CS5 (40), CS6 (48), CS7 (56) 및 EF (46). • Value - DSCP 값을 여기에 수동으로 입력할 수도 있습니다. 범위는 0 에서 63 사이입니다.
트래픽 클래스	여기에서 트래픽 클래스 값을 선택하고 입력합니다. 범위는 0 에서 255 사이입니다.
플로우 레이블	여기에 흐름 레이블 값을 입력합니다. 이 값은 0 에서 1048575 사이여야 합니다.
시간 범위	이 ACL 규칙에 사용할 시간 범위 프로필의 이름을 여기에 입력합니다. 이 이름은 최대 32 자까지 가능합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Back 버튼을 클릭하여 변경 사항을 취소하고 이전 페이지로 돌아갑니다.

Extended MAC ACL

Extended MAC ACL 을 선택하고 Add Rule 버튼을 클릭하면 다음 페이지가 나타납니다.

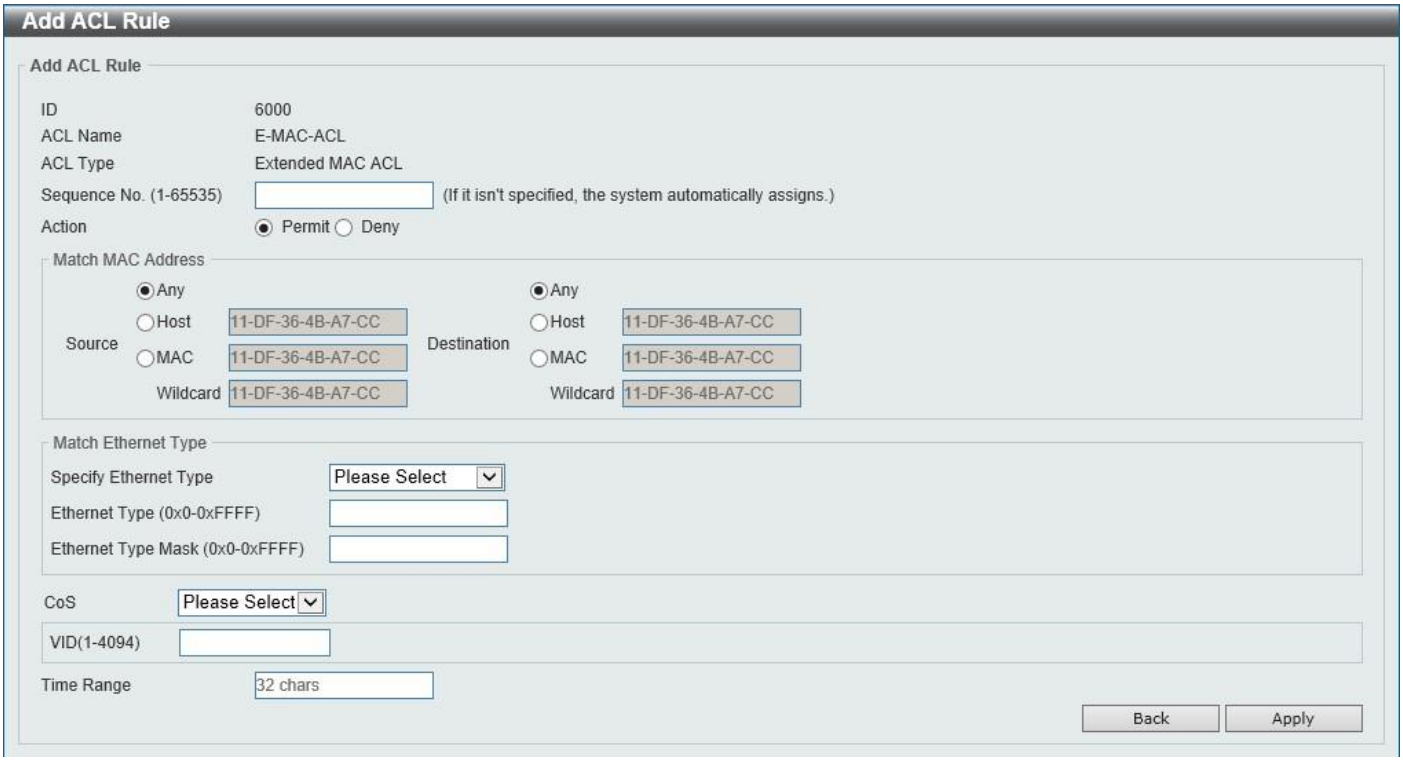

그림 8-15) 확장 MAC ACL(규칙 추가) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Sequence No.	여기에 이 ACL 규칙의 Sequence No.를 입력합니다. 범위는 1 에서 65535 사이입니다. 이 값을 지정하지 않으면 시스템은 이 항목에 대한 ACL 규칙 번호를 자동으로 생성합니다.
Action	여기에서 이 규칙이 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 Permit(허용) 및 Deny(거부)입니다.

Source	여기에서 소스 MAC 주소 정보를 선택하여 입력합니다. 선택할 수 있는 옵션은 Any, Host, MAC 및 Wildcard 입니다. • Any 옵션을 선택하면 모든 소스 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host 옵션을 선택한 경우 여기에 소스 호스트 MAC 주소를 입력합니다. • MAC 옵션을 선택하면 와일드카드 옵션도 사용할 수 있습니다. 제공된 공간에 소스 MAC 주소와 와일드카드 값을 입력합니다.
Destination	여기에서 대상 MAC 주소 정보를 선택하여 입력합니다. 선택할 수 있는 옵션은 Any, Host, MAC 및 Wildcard 입니다. • Any 옵션을 선택하면 모든 대상 트래픽이 이 규칙의 조건에 따라 평가됩니다. • Host 옵션을 선택한 경우 여기에 대상 호스트 MAC 주소를 입력합니다. • MAC 옵션을 선택하면 와일드카드 옵션도 사용할 수 있습니다. 제공된 공간에 대상 MAC 주소와 와일드카드 값을 입력합니다.
Specify Ethernet Type	여기에서 이더넷 유형 옵션을 선택합니다. 선택할 수 있는 옵션은 AARP, AppleTalk, Decent-IV, EType-6000, ETYPE-8042, LAT, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp 및 arp 입니다.
Ethernet Type	여기에 Ethernet type hexadecimal 값을 입력합니다. 이 값은 0x0 에서 0xFFFF 사이여야 합니다. 이더넷 유형 프로필을 선택하면 위에서 적절한 16 진수 값이 자동으로 입력됩니다.
Ethernet Type Mask	여기에 Ethernet type mask hexadecimal 값을 입력합니다. 이 값은 0x0 에서 0xFFFF 사이여야 합니다. 이더넷 유형 프로필을 선택하면 위에서 적절한 16 진수 값이 자동으로 입력됩니다.
CoS	여기에서 사용할 CoS 값을 선택합니다. 범위는 0 에서 7 사이입니다.
VID	여기에 이 ACL 규칙과 연결할 VLAN ID 를 입력합니다. 범위는 1 에서 4094 사이입니다.
Time Range	이 ACL 규칙에 사용할 시간 범위 프로필의 이름을 여기에 입력합니다. 이 이름은 최대 32 자까지 가능합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Back 버튼을 클릭하여 변경 사항을 취소하고 이전 페이지로 돌아갑니다.

ACL Interface Access Group

이 창은 ACL Interface Access Group 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 ACL > ACL Interface Access Group 을 클릭합니다.

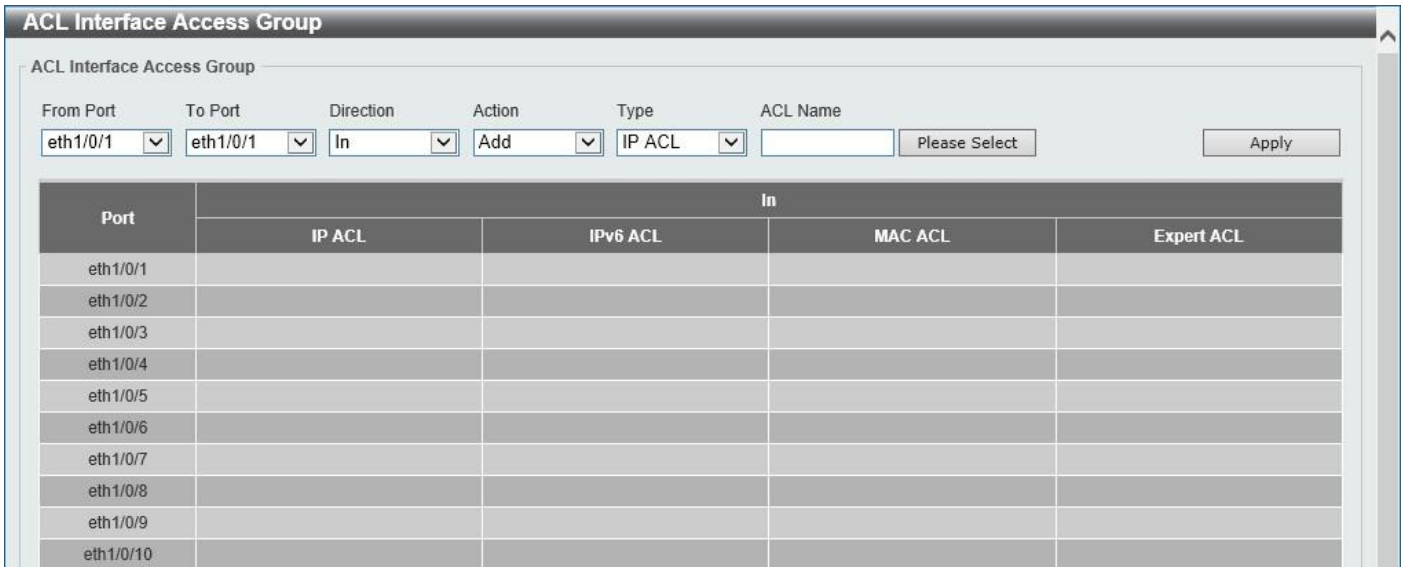

그림 8-16) ACL Interface 액세스 그룹 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 이 구성에 사용할 포트 범위를 선택합니다.
Direction	IN 방향이 사용되도록 지정합니다.
Action	여기에서 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 Add 및 Delete 입니다.
Type	여기에서 ACL 유형을 선택합니다. 선택할 수 있는 옵션은 IP ACL, IPv6 ACL 및 MAC ACL 입니다.
ACL Name	여기에 ACL 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다. Please Select 버튼을 클릭하여 목록에서 기존 ACL 을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Please Select 버튼을 클릭하면 다음 창이 나타납니다.

그림 8-17 ACL Interface 액세스 그룹(선택하십시오) 창

컨피그레이션에서 해당 ACL 을 사용하려면 항목 옆에 있는 라디오 버튼을 선택합니다.
페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다. 확인 버튼을 클릭하여 선택 사항을 수락합니다.

8. Security

Port Security
802.1X
AAA
RADIUS
IMPB
DHCP Server Screening
ARP Spoofing Prevention
Network Access Authentication
Safeguard Engine
Trusted Host
Traffic Segmentation Settings
Storm Control Settings
DoS Attack Prevention Settings
SSH
SSL
Network Protocol Port Protect Settings

Port Security

Port Security Global Settings

이 창은 전역 포트 보안 설정을 표시하고 구성하는 데 사용됩니다. 포트 보안은 포트를 잠그기 전에 스위치에 알려지지 않은 인증되지 않은 컴퓨터(소스 MAC 주소 포함)가 스위치의 잠긴 포트에 연결하고 네트워크에 액세스하는 것을 방지하는 보안 기능입니다.

다음 창을 보려면 아래와 같이 Security > Port Security > Port Security Global Settings 을 클릭합니다.

그림 9-1) Port Security Global Settings(포트 보안 Global Settings) 창

Port Security Trap Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Trap State	스위치에서 포트 보안 트랩을 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Port Security Trap Rate Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Trap Rate	초당 트랩 수를 입력합니다. 범위는 0 에서 1000 사이입니다. 기본값 0 은 모든 보안 위반에 대해 생성될 SNMP 트랩을 나타냅니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Port Security System Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description

System Maximum Address	허용되는 보안 MAC 주소의 최대 수를 입력합니다. 지정하지 않으면 기본값은 No Limit 입니다. 유효한 범위는 1 에서 3328 사이입니다. 보안 MAC 주소의 최대 수를 허용하려면 제한 없음 확인란을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Port Security Port Settings

이 창은 포트 보안 포트 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > Port Security > Port Security Port Settings 을 클릭합니다.

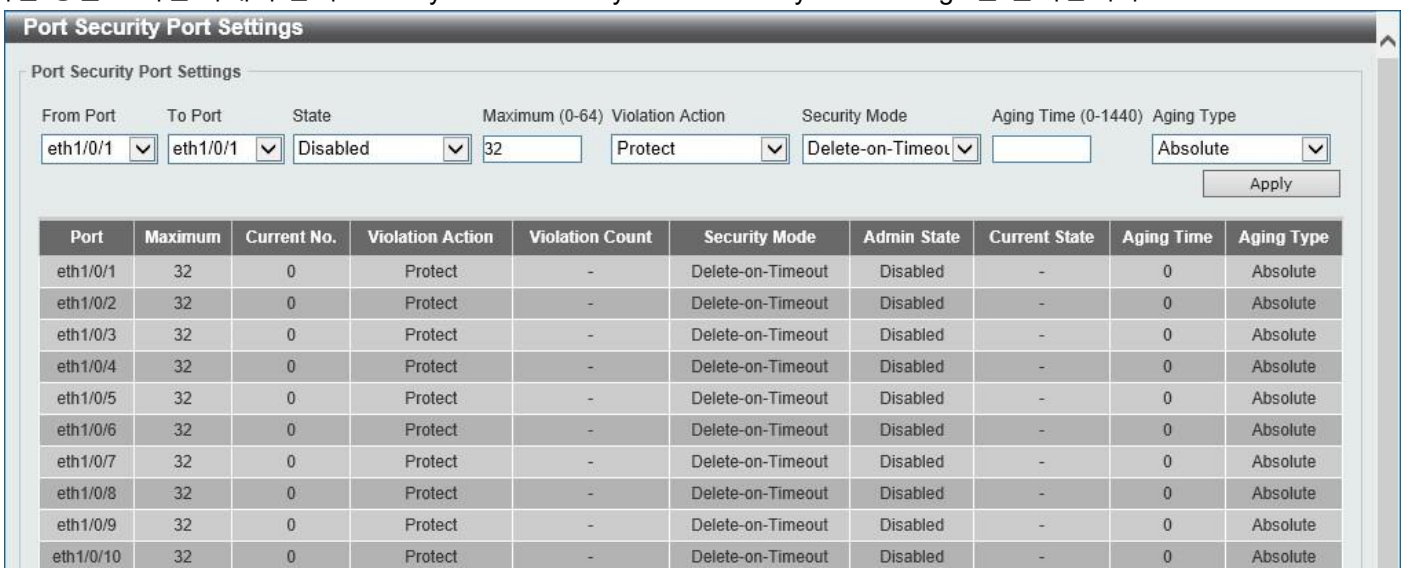

그림 9-2 포트 보안 포트 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
State	지정된 포트에서 포트 보안 기능을 활성화하거나 비활성화하려면 선택합니다.
Maximum	지정된 포트에서 허용되는 보안 MAC 주소의 최대 수를 입력합니다. 이 값은 0 에서 64 사이여야 합니다. 기본적으로 이 값은 32 입니다.
Violation Action	여기에서 수행할 위반 작업을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Protect - portsecurity 프로세스 레벨에서 비보안 호스트의 모든 패킷을 삭제하도록 지정하지만 보안 위반 횟수는 증가시키지 않습니다. • Restrict - portsecurity 프로세스 레벨에서 비보안 호스트의 모든 패킷을 삭제하도록 지정하고 보안 위반 횟수를 증가시키고 시스템 로그를 기록합니다. • Shutdown - 보안 위반이 있는 경우 포트를 종료하고 시스템 로그를 기록하도록 지정합니다.
Security Mode	여기에서 보안 모드 옵션을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Permanent -이 모드에서 사용자가 해당 항목을 수동으로 삭제하지 않는 한 학습된 모든 MAC 주소가 제거되지 않도록 지정합니다. • Delete-on-Timeout -이 모드에서 항목이 오래되거나 사용자가 이러한 항목을 수동으로 삭제할 때 학습된 모든 MAC 주소가 제거되도록 지정합니다.
Aging Time	지정된 포트에서 자동 학습된 동적 보안 주소에 사용되는 에이징 시간 값을 여기에 입력합니다. 이 값은 0 분에서 1440 분 사이여야 합니다.

Aging Type	Absolute 가 사용되도록 지정합니다. 이 포트의 모든 보안 주소는 지정된 시간 후에 정확히 만료되고 보안 주소 목록에서 제거됩니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Port Security Address Entries

이 창은 포트 보안 주소 항목을 보고, 지우고, 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > Port Security > Port Security Address Entries 를 클릭합니다.

그림 9-3 Port Security Address Entries 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
MAC Address	여기에 MAC 주소를 입력합니다. 영구 옵션을 선택하여 사용자가 해당 항목을 수동으로 삭제하지 않는 한 학습된 모든 MAC 주소가 제거되지 않도록 지정합니다.
VID	여기에 VLAN ID 를 입력합니다. 이 값은 1 에서 4094 사이여야 합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새 항목을 추가합니다.

Delete 버튼을 클릭하여 입력한 정보에 따라 새 항목을 제거합니다.

Clear by Port 버튼을 클릭하여 선택한 포트에 따라 정보를 지웁니다.

Clear by MAC 버튼을 클릭하여 입력한 MAC 주소를 기반으로 정보를 지웁니다.

Clear All 버튼을 클릭하여 이 테이블의 모든 정보를 지웁니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

802.1X

802.1X (Port-based and Host-based Access Control)

IEEE 802.1X 표준은 클라이언트 및 서버 기반 액세스 제어 모델을 사용하여 지정된 LAN(Local Area Network)의 다양한 유선 또는 무선 장치에 액세스할 수 있도록 사용자에게 권한을 부여하고 인증하기 위한 보안 조치입니다. 이 작업은 RADIUS 서버를 사용하여 클라이언트와 서버 간에 EAPOL(Extensible Authentication Protocol over LAN) 패킷을 릴레이하여 네트워크에 액세스하려는 사용자를 인증함으로써 수행됩니다.

다음 그림은 기본 EAPOL 패킷을 나타냅니다.

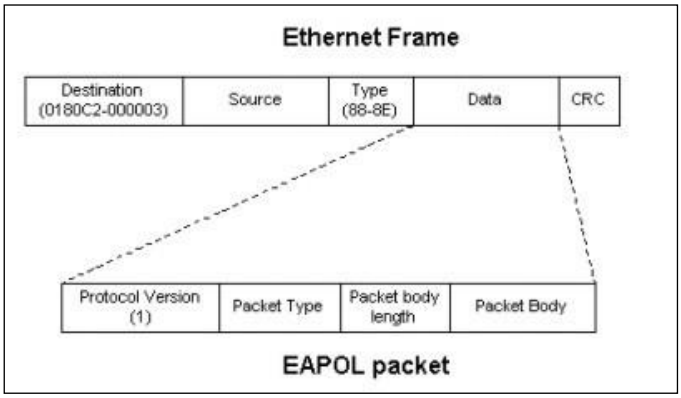

그림 9-4 EAPOL 패킷

이 방법을 사용하면 권한이 없는 장치가 사용자가 연결된 포트를 통해 LAN 에 연결하는 것이 제한됩니다. EAPOL 패킷은 권한 부여가 부여될 때까지 특정 포트를 통해 전송할 수 있는 유일한 트래픽입니다. 802.1X 액세스 제어 방법에는 세 가지 역할이 있으며, 각 역할은 안정적이고 작동하는 액세스 제어 보안 방법을 만들고 유지하는 데 중요합니다.

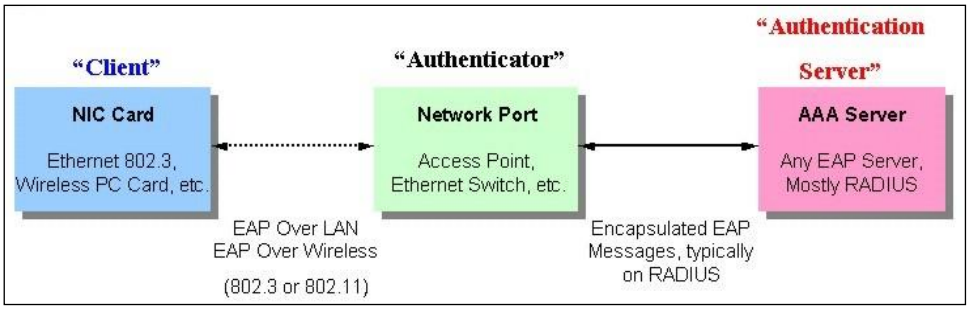

그림 9-5 802.1X 의 세 가지 역할

다음 섹션에서는 Client, Authenticator 및 Authentication Server 의 세 가지 역할에 대해 자세히 설명합니다.

Authentication Server

인증 서버는 클라이언트 및 인증자와 동일한 네트워크에 연결된 원격 디바이스이며, RADIUS 서버 프로그램을 실행해야 하며 인증자(스위치)에서 올바르게 구성되어야 합니다. 스위치의 포트에 연결된 클라이언트는 LAN 의 스위치에서 제공하는 서비스를 얻기 전에 인증 서버(RADIUS)에 의해 인증되어야 합니다. 인증 서버의 역할은 EAPOL 패킷을 통해 RADIUS 서버와 클라이언트 간에 보안 정보를 교환하여 네트워크에 액세스하려는 클라이언트의 ID 를 인증하고, 클라이언트에게 LAN 및/또는 스위치 서비스에 대한 액세스 권한이 부여되었는지 여부를 스위치에 알리는 것입니다.

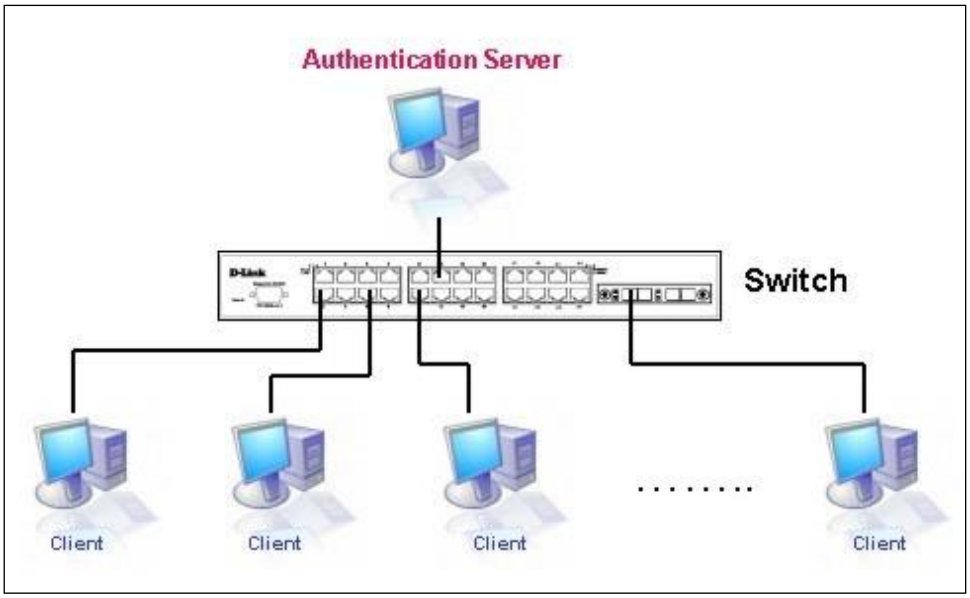

그림 9-6) 인증 서버

Authenticator

Authenticator(스위치)는 인증 서버와 클라이언트 간의 중개자입니다. 인증자는 802.1X 기능을 사용할 때 두 가지 용도로 사용됩니다. 첫 번째 목적은 클라이언트에 액세스 권한이 부여되기 전에 인증자를 통과할 수 있는 유일한 정보인 EAPOL 패킷을 통해 클라이언트로부터 인증 정보를 요청하는 것입니다. 인증자의 두 번째 목적은 인증 서버를 사용하여 클라이언트에서 수집된 정보를 확인한 다음 해당 정보를 다시 클라이언트로 릴레이하는 것입니다.

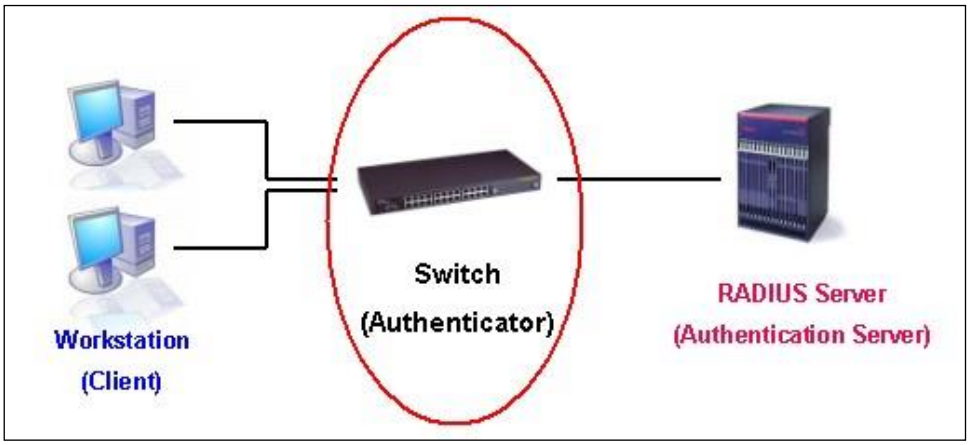

그림 9-7 인증자

Authenticator 를 올바르게 구성하려면 스위치에서 세 단계를 구현해야 합니다.

- 802.1X 상태는 활성화되어야 합니다. (보안 > 802.1X > 802.1X Global Settings)
- 802.1X 설정은 포트별로 구현해야 합니다(보안 > 802.1X > 802.1X 포트 설정).
- 스위치에서 RADIUS 서버를 구성해야 합니다. (보안 > RADIUS > RADIUS 서버 설정)

Client

클라이언트는 LAN 또는 스위치 서비스에 액세스하려는 엔드 스테이션입니다. 모든 엔드 스테이션은 802.1X 프로토콜과 호환되는 소프트웨어를 실행해야 합니다. Windows XP 및 Windows Vista 를 실행하는 사용자의 경우 해당 소프트웨어가 운영 체제에 포함되어 있습니다. 다른 모든 사용자는 외부 소스에서 802.1X 클라이언트 소프트웨어를 구해야 합니다. 클라이언트는 EAPOL 패킷을 통해 LAN 및/또는 스위치에 대한 액세스를 요청하고 스위치의 요청에 응답합니다.

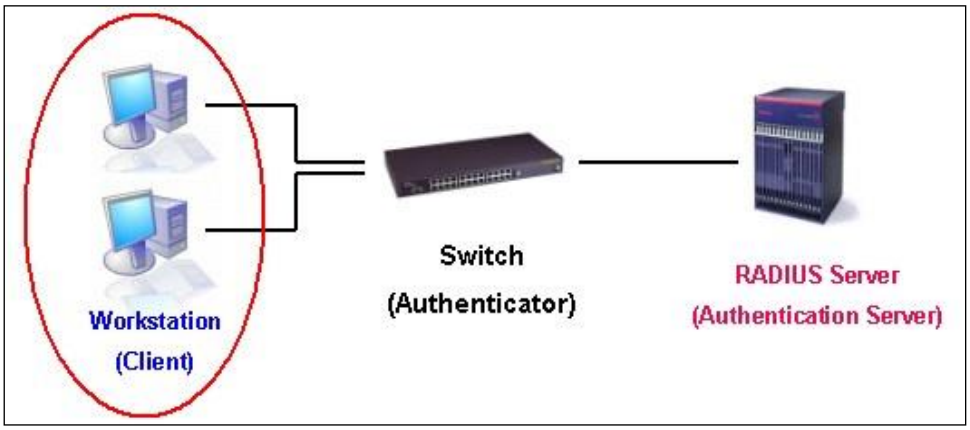

그림 9-8) 클라이언트

Authentication Process

위에서 언급한 세 가지 역할을 활용하는 802.1X 프로토콜은 네트워크에 액세스하려는 사용자에게 안정적이고 안전한 권한을 부여하고 인증하는 방법을 제공합니다. 인증이 성공적으로 이루어지기 전에 EAPOL 트래픽만 지정된 포트를 통과할 수 있습니다. 이 포트는 올바른 사용자 이름과 비밀번호(MAC 주소로 802.1X 가 활성화된 경우 MAC 주소)를 가진 클라이언트에 액세스 권한이 부여되어 포트가 성공적으로 "잠금 해제"될 때까지 "잠겨 있습니다". 포트가 잠금

해제되면 일반 트래픽이 포트를 통과할 수 있습니다. 다음 그림에서는 위에서 설명한 세 가지 역할 간에 인증 프로세스가 완료되는 방법에 대한 자세한 설명을 표시합니다.

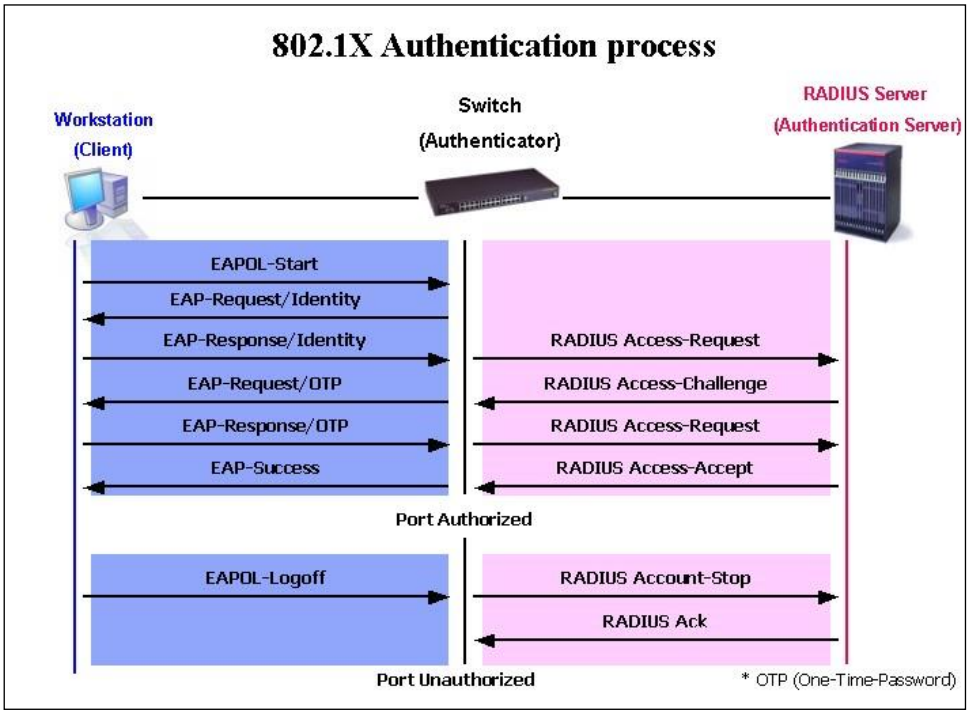

그림 9-9 802.1X 인증 프로세스

802.1X 의 D-Link 구현을 통해 네트워크 관리자는 스위치에서 사용되는 두 가지 유형의 액세스 제어 중에서 선택할 수 있습니다.

- 포트 기반 액세스 제어 - 이 방법을 사용하면 원격 RADIUS 서버에서 포트당 한 명의 사용자만 인증하여 동일한 포트의 나머지 사용자가 네트워크에 액세스할 수 있도록 합니다.
- 호스트 기반 액세스 제어 - 이 방법을 사용하면 스위치가 포트별로 최대 1,000 개의 MAC 주소를 자동으로 학습하고 목록에 설정합니다. 각 MAC 주소는 네트워크에 대한 액세스를 허용하기 전에 원격 RADIUS 서버를 사용하여 스위치에 의해 인증되어야 합니다.

Understanding 802.1X Port-based and Host-based Network Access Contro

802.1X 개발의 원래 목적은 LAN 에서 포인트-투-포인트(point-to-point)의 특성을 활용하는 것이었습니다. 이러한 인프라의 단일 LAN 세그먼트에는 두 개 이상의 장치가 연결되어 있지 않으며 그 중 하나는 브리지 포트입니다. Bridge Port 는 링크의 원격 끝에 활성 장치가 연결되어 있거나 활성 장치가 비활성화되고 있음을 나타내는 이벤트를 탐지합니다. 이러한 이벤트는 포트의 권한 부여 상태를 제어하고 포트가 인증되지 않은 경우 연결된 디바이스를 인증하는 프로세스를 시작하는 데 사용할 수 있습니다. 포트 기반 네트워크 액세스 제어입니다.

Port-based Network Access Control

연결된 디바이스가 성공적으로 인증되면 Port 는 Authorized(인증됨) 상태가 되며, Port(포트)를 Unauthorized(권한 없음) 상태로 만드는 이벤트가 발생할 때까지 포트의 모든 후속 트래픽은 액세스 제어 제한의 적용을 받지 않습니다. 따라서 포트가 실제로 두 개 이상의 연결된 장치가 있는 공유 미디어 LAN 세그먼트에 연결된 경우 연결된 장치 중 하나를 성공적으로 인증하면 공유 세그먼트의 모든 장치에 대해 LAN 에 액세스할 수 있습니다. 분명히 이러한 상황에서 제공되는 보안은 공격에 노출되어 있습니다.

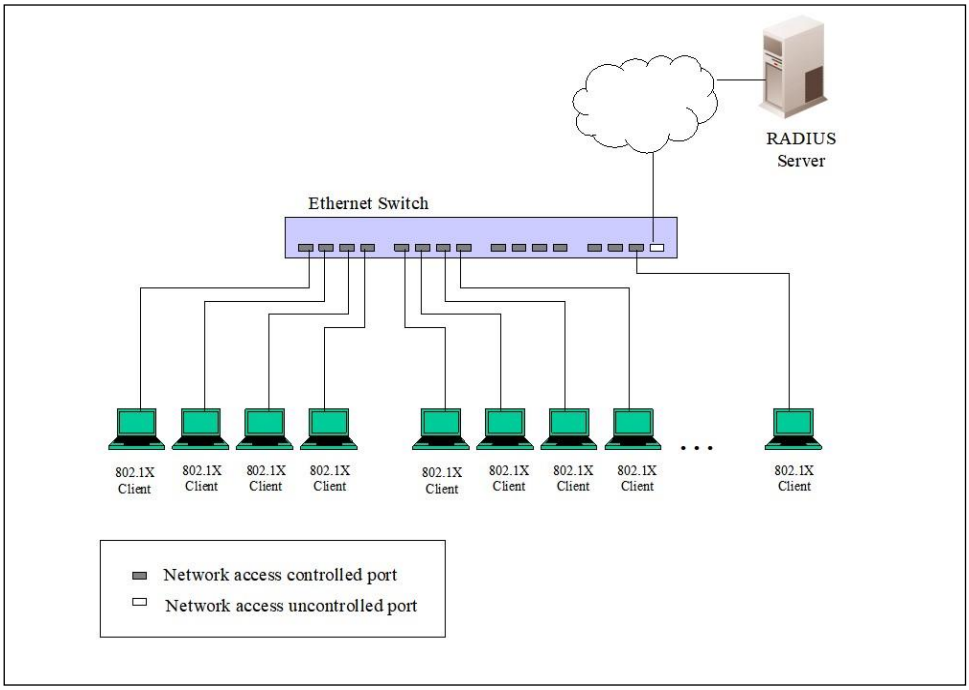

그림 9-10 일반적인 포트 기반 구성의 예

Host-based Network Access Control

공유 미디어 LAN 세그먼트에서 802.1X 를 성공적으로 사용하려면 LAN 에 액세스해야 하는 각 연결된 장치에 대해 하나씩 "논리적" 포트를 만들어야 합니다. 스위치는 공유 미디어 세그먼트에 연결하는 단일 물리적 포트를 여러 개의 고유한 논리적 포트로 구성된 것으로 간주하며, 각 논리적 포트는 EAPOL 교환 및 권한 부여 상태의 관점에서 독립적으로 제어됩니다. 스위치는 연결된 각 디바이스의 개별 MAC 주소를 학습하고 연결된 디바이스가 스위치를 통해 LAN 과 통신하는 데 사용할 수 있는 논리적 포트를 효과적으로 생성합니다.

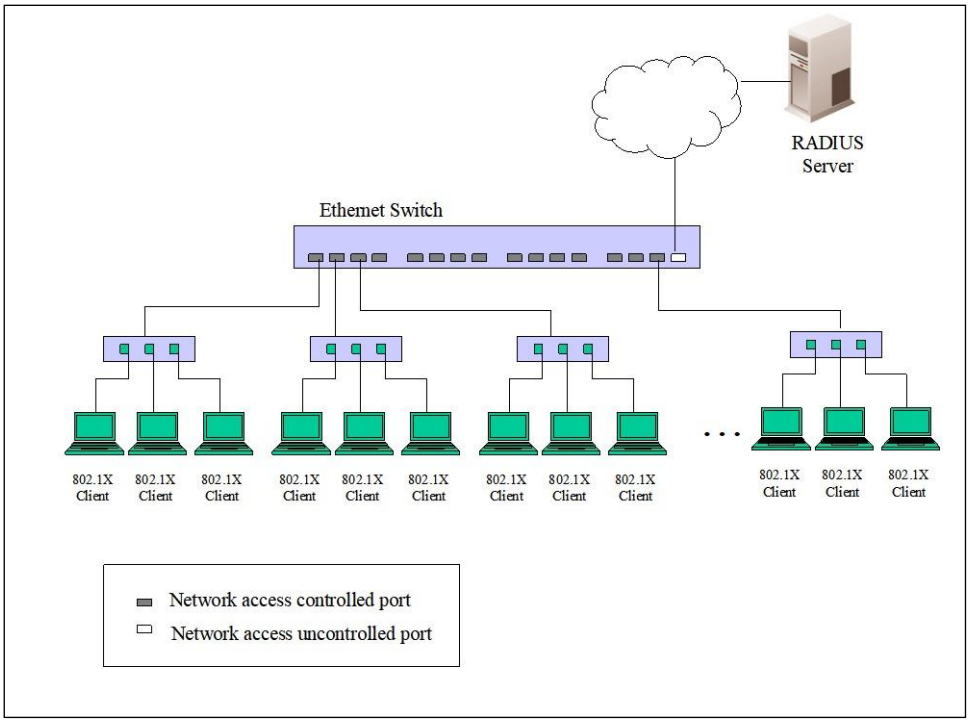

그림 9-11) 일반적인 호스트 기반 구성의 예

802.1X Global Settings

이 창은 전역 802.1X 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > 802.1X > 802.1X Global Settings 을 클릭하십시오.

그림 9-12 802.1X Global Settings 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
802.1X State	여기에서 전역 802.1X 상태를 활성화하거나 비활성화하려면 선택합니다.
802.1X Trap State	여기에서 802.1X 트랩 상태를 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

802.1X Port Settings

이 창은 802.1X 포트 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > 802.1X > 802.1X Port Settings 을 클릭합니다.

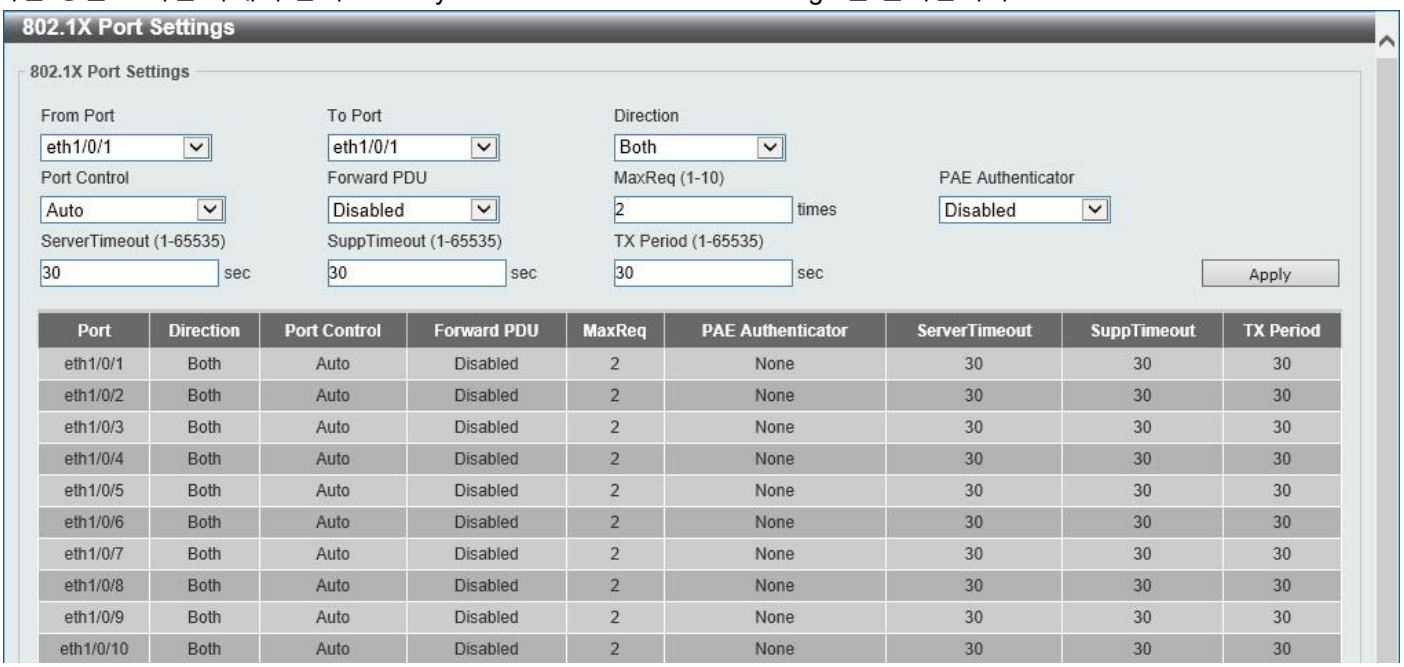

그림 9-13 802.1X 포트 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
Direction	여기에서 방향을 선택합니다. 선택할 수 있는 옵션은 Both 및 In 입니다. 이 옵션은 제어된 포트의 트래픽 방향을 단방향(In) 또는 양방향(Both)으로 구성합니다. In control 방향은 Network Access Authentication Port Settings(네트워크 액세스 인증 포트 설정) 창에서 Host Mode(호스트 모드)가 Multi Host(다중 호스트)*로 구성된 경우에만 유효합니다.*

Port Control	여기에서 포트 제어 옵션을 선택합니다. 선택할 수 있는 옵션은 ForceAuthorized, Auto 및 ForceUnauthorized 입니다. 포트 제어가 force-authorized 로 설정된 경우 포트는 양방향으로 제어되지 않습니다. 포트 제어가 자동으로 설정된 경우 제어된 방향에 대한 포트에 대한 액세스를 인증해야 합니다. 포트 제어가 force-unauthorized 로 설정된 경우 제어된 방향에 대한 포트에 대한 액세스가 차단됩니다.
Forward PDU	여기에서 전달 PDU 옵션을 활성화하거나 비활성화하려면 선택합니다.
MaxReq	여기에 필요한 최대 시간 값을 입력합니다. 이 값은 1 에서 10 사이여야 합니다. 기본적으로 이 값은 2 입니다. 이 옵션은 백엔드 인증 상태 시스템이 인증 프로세스를 다시 시작하기 전에 EAP(Extensible Authentication Protocol) 요청 프레임을 서플리컨트로 재전송하는 최대 횟수를 구성합니다.
PAE Authenticator	여기에서 PAE 인증자 옵션을 사용하거나 사용하지 않도록 설정하려면 선택합니다. 이 옵션은 특정 포트를 IEEE 802.1X PAE(Port Access Entity) 인증자로 구성합니다.
Server Timeout	여기에 서버 시간 제한 값을 입력합니다. 이 값은 1 초에서 65535 초 사이여야 합니다. 기본적으로 이 값은 30 초입니다.
SuppTimeout	여기에 supplicant timeout 값을 입력합니다. 이 값은 1 초에서 65535 초 사이여야 합니다. 기본적으로 이 값은 30 초입니다.
TX Period	여기에 전송 기간 값을 입력합니다. 이 값은 1 초에서 65535 초 사이여야 합니다. 기본적으로 이 값은 30 초입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Authentication Sessions Information

이 창은 인증 세션 정보를 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > 802.1X > Authentication Sessions Information 를 클릭합니다.

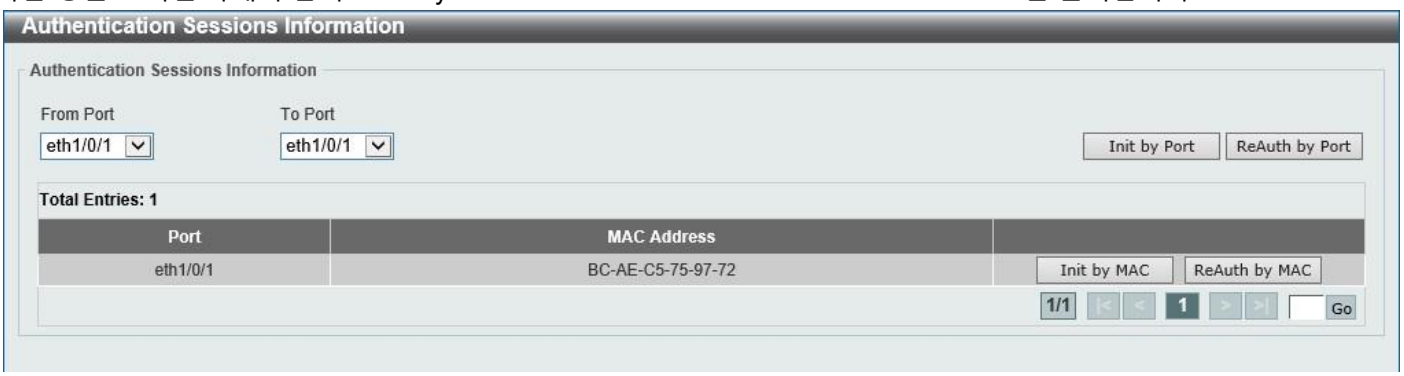

그림 9-14) Authentication Sessions Information 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.

Init by Port 버튼을 클릭하여 선택한 포트에 따라 세션 정보를 시작합니다.

ReAuth by Port 버튼을 클릭하여 선택한 포트에 따라 세션 정보를 다시 인증합니다.

Init by MAC 버튼을 클릭하여 MAC 주소를 기반으로 세션 정보를 시작합니다.

ReAuth by MAC 버튼을 클릭하여 MAC 주소를 기반으로 세션 정보를 다시 인증합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Authenticator Statistics

이 창은 Authenticator Statistics 를 보고 지우는 데 사용됩니다.

다음 창을 보려면 아래와 Security > 802.1X > Authenticator Statistics 를 클릭합니다.

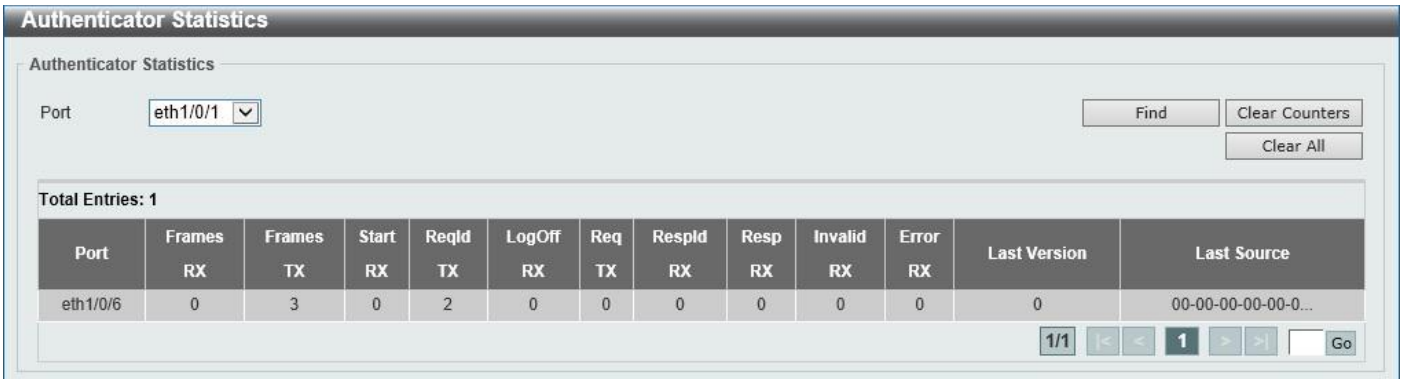

그림 9-15) Authenticator Statistics 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Port	여기에서 쿼리에 사용되는 적절한 포트를 선택합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Clear Counters 버튼을 클릭하여 선택한 항목에 따라 카운터 정보를 지웁니다.

Clear All 버튼을 클릭하여 이 테이블의 모든 정보를 지웁니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Authenticator Session Statistics

이 창은 인증자 세션 통계를 보고 지우는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > 802.1X > Authenticator Session Statistics 를 클릭합니다.

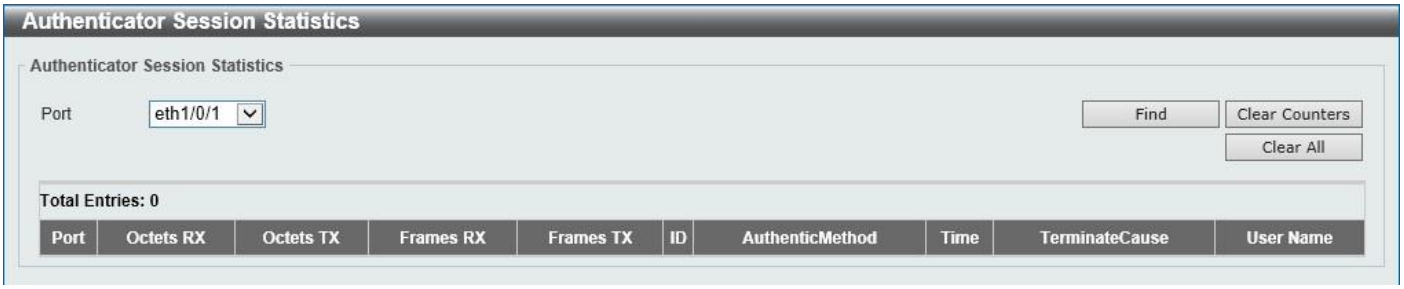

그림 9-16) Authenticator Session Statistics 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Port	여기에서 쿼리에 사용되는 적절한 포트를 선택합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Clear Counters 버튼을 클릭하여 선택한 항목에 따라 카운터 정보를 지웁니다.

Clear All 버튼을 클릭하여 이 테이블의 모든 정보를 지웁니다.

Authenticator Diagnostics

이 창은 인증자 진단 정보를 보고 지우는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > 802.1X > Authenticator Diagnostics 를 클릭합니다.

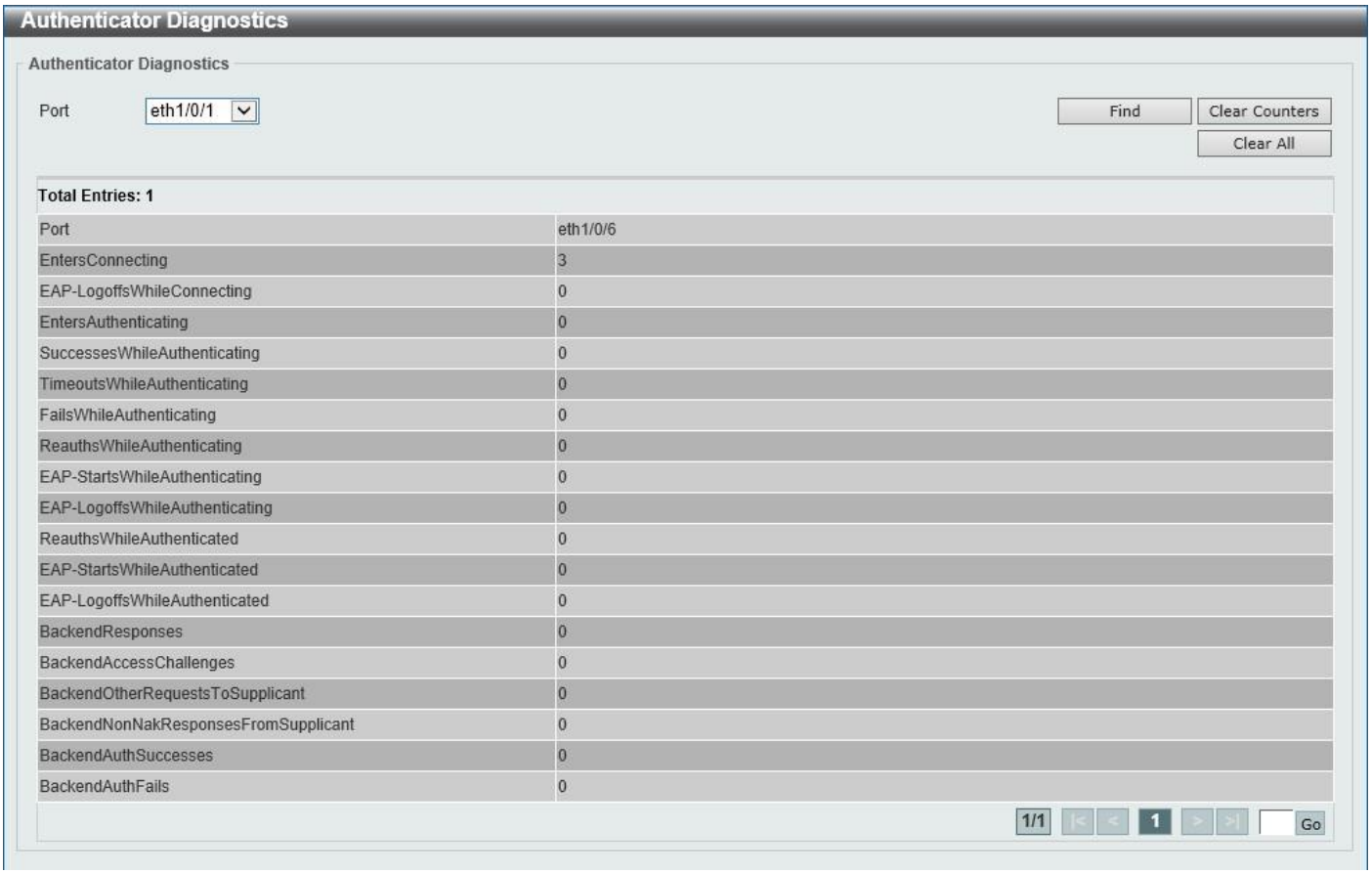

그림 9-17) Authenticator Diagnostics 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Port	여기에서 쿼리에 사용되는 적절한 포트를 선택합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Clear Counters 버튼을 클릭하여 선택한 항목에 따라 카운터 정보를 지웁니다.

Clear All 버튼을 클릭하여 이 테이블의 모든 정보를 지웁니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

AAA

AAA Global Settings

이 창은 전역 AAA(Authentication, Authorization, and Accounting) 상태를 활성화하거나 비활성화하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > AAA > AAA Global Settings 를 클릭합니다.

그림 9-18) AAA Global Settings 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description

AAA State	전역 AAA(Authentication, Authorization, and Accounting) 상태를 활성화하거나 비활성화하려면 선택합니다. 기본적으로 이 기능은 비활성화되어 있습니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Authentication Settings

이 창은 AAA 네트워크 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > AAA > Authentication Settings 를 클릭합니다.

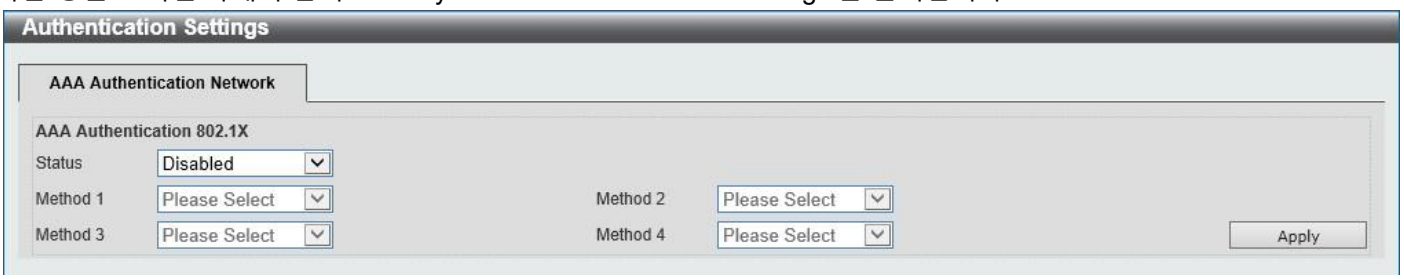

그림 9-19) 인증 설정 창

AAA Authentication 802.1X 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Status	여기에서 AAA 802.1X 인증 상태를 활성화하거나 비활성화하려면 선택합니다.
Method 1 ~ Method 4	여기에서 이 구성에 사용할 방법 목록을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • none - 일반적으로 메서드가 마지막 메서드로 나열됩니다. 사용자는 이전 방법 인증에 의해 거부되지 않은 경우 인증을 통과합니다. • local - 인증에 로컬 데이터베이스를 사용하도록 지정합니다. • group - AAA 그룹 서버에서 정의한 서버 그룹을 사용하도록 지정합니다. 제공된 공간에 AAA 그룹 서버 이름을 입력합니다. 이 문자열은 최대 32 자까지 가능합니다. • radius - RADIUS 서버 호스트 명령으로 정의된 서버를 사용하도록 지정합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

RADIUS

RADIUS Global Settings

이 창은 전역 RADIUS 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > RADIUS > RADIUS Global Settings 을 클릭합니다.

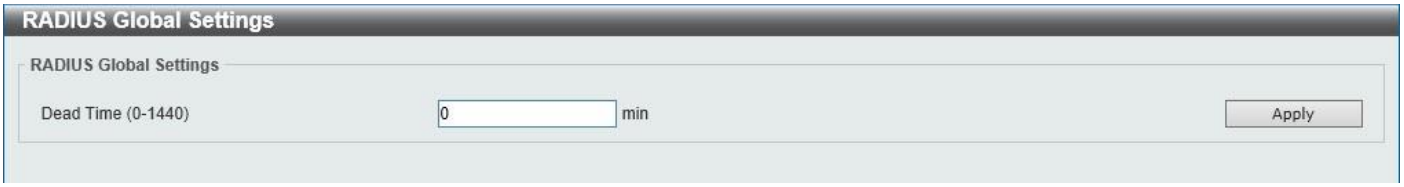

그림 9-20) RADIUS Global Settings 창

RADIUS Global Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description

Dead Time	여기에 데드 타임 값을 입력합니다. 이 값은 0 분에서 1440 분 사이여야 합니다. 기본적으로 이 값은 0 분입니다. 이 옵션이 0 이면 응답하지 않는 서버가 비활성으로 표시되지 않습니다. 이 설정을 사용하여 다음을 개선할 수 있습니다. 응답하지 않는 서버 호스트 항목을 건너뛰기 위해 데드 시간을 설정하여 인증 처리 시간. 시스템은 인증 서버로 인증을 수행할 때 한 번에 하나의 서버를 시도합니다. 시도한 서버가 응답하지 않으면 시스템은 다음 서버를 시도합니다. 시스템이 서버가 응답하지 않는 것을 발견하면 서버를 다운으로 표시하고, 데드 타임 타이머를 시작하고, 데드 타임이 만료될 때까지 다음 요청의 인증에서 이를 건너뜁니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

RADIUS Server Settings

이 창은 RADIUS 서버 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > RADIUS > RADIUS Server Settings 을 클릭합니다.

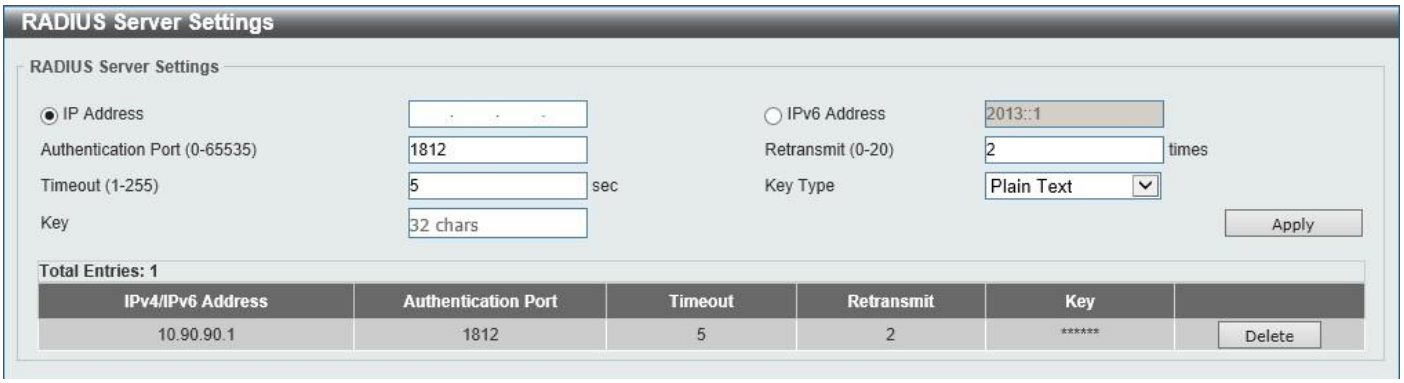

그림 9-21) RADIUS 서버 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
IP Address	여기에 RADIUS 서버 IPv4 주소를 입력합니다.
IPv6 Address	여기에 RADIUS 서버 IPv6 주소를 입력합니다.
Authentication Port	여기에 사용된 인증 포트 번호를 입력합니다. 이 값은 0 에서 65535 사이여야 합니다. 기본적으로 이 값은 1812 입니다. 인증을 사용하지 않는 경우 값 0 을 사용합니다.
Retransmit	여기에 사용된 재전송 값을 입력합니다. 이 값은 0 에서 20 사이여야 합니다. 기본적으로 이 값은 2 입니다. 이 옵션을 비활성화하려면 값 0 을 입력합니다.
Timeout	여기에 사용된 시간 제한 값을 입력합니다. 이 값은 1 초에서 255 초 사이여야 합니다. 기본적으로 이 값은 5 초입니다.
Key Type	일반 텍스트 키 유형이 사용되도록 지정합니다.
Key	RADIUS 서버와 통신하는 데 사용되는 키를 여기에 입력합니다. 이 키는 최대 32 자까지 가능합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

RADIUS Group Server Settings

이 창은 RADIUS 그룹 서버 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > RADIUS > RADIUS Group Server Settings 을 클릭합니다.

그림 9-22) RADIUS 그룹 서버 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Group Server Name	여기에 RADIUS 그룹 서버 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
IP Address	여기에 그룹 서버 IPv4 주소를 입력합니다.
IPv6 Address	여기에 그룹 서버 IPv6 주소를 입력합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새 항목을 추가합니다.

Show Detail 버튼을 클릭하여 RADIUS 그룹 서버에 대한 자세한 설정을 보고 구성합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Show Detail 버튼을 클릭하면 다음 페이지를 사용할 수 있습니다.

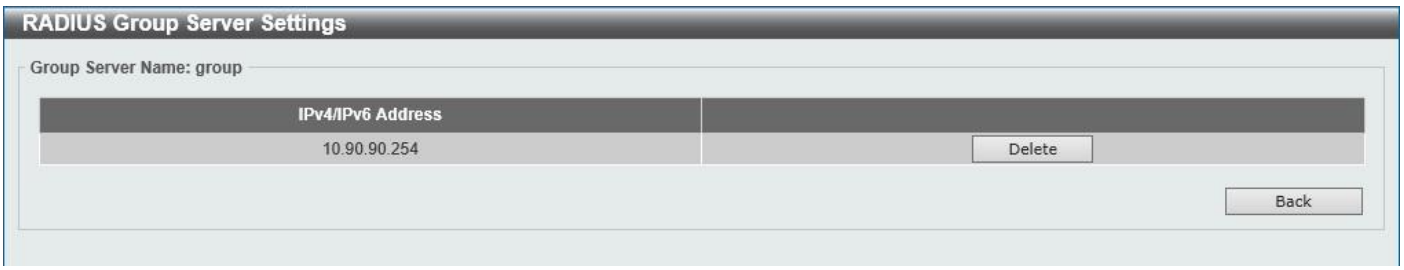

그림 9-23) RADIUS 그룹 서버 설정(상세) 창

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

RADIUS Statistic

이 창은 RADIUS 통계 정보를 보고 지우는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > RADIUS > RADIUS Statistic 을 클릭합니다.

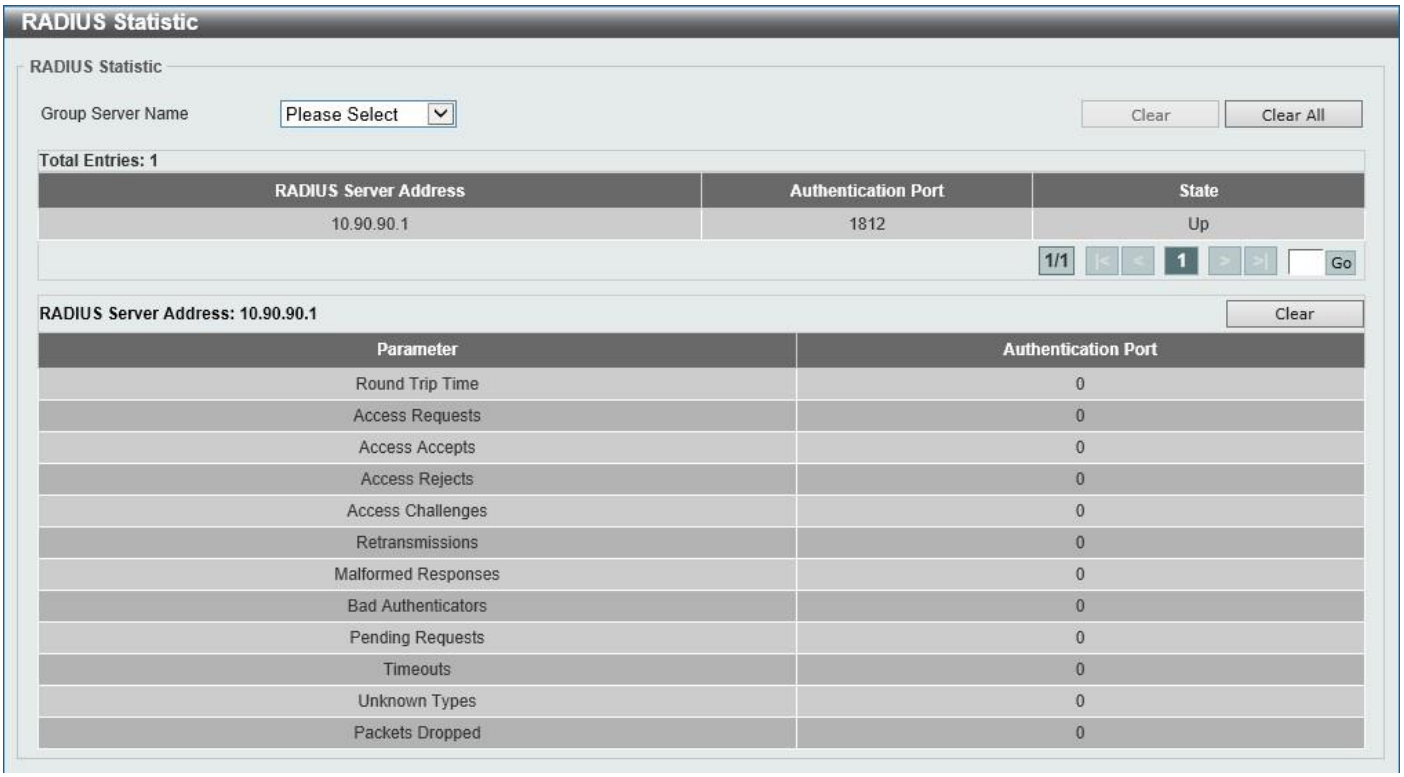

그림 9-24) RADIUS Statistic 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Group Server Name	여기에서 이 목록에서 RADIUS 그룹 서버 이름을 선택합니다.

Clear 버튼을 클릭하여 선택한 항목에 따라 정보를 지웁니다.

Clear All 버튼을 클릭하여 이 테이블의 모든 정보를 지웁니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

IMPB

IP 네트워크 계층은 4 바이트 주소를 사용합니다. 이더넷 링크 레이어는 6 비트 MAC 주소를 사용합니다. 이 두 주소 유형을 함께 바인딩하면 레이어 간에 데이터를 전송할 수 있습니다. IMPB(IP-MAC-Port Binding)의 주요 목적은 스위치에 대한 액세스를 권한이 있는 여러 사용자로 제한하는 것입니다. 인증된 클라이언트는 사전 구성된 데이터베이스로 IP-MAC 주소 쌍을 확인하거나 DHCP Snooping 이 활성화된 경우 스위치가 DHCP 패킷을 Snooping 하고 IMPB 화이트리스트에 저장하여 IP/MAC 쌍을 자동으로 학습하여 스위치의 포트에 액세스할 수 있습니다. 권한이 없는 사용자가 IP-MAC 바인딩이 활성화된 포트에 액세스하려고 하면 시스템은 해당 패킷을 삭제하여 액세스를 차단합니다. 활성 항목과 비활성 항목은 동일한 데이터베이스를 사용합니다. 이 기능은 포트 기반이므로 사용자가 개별 포트에서 기능을 활성화하거나 비활성화할 수 있습니다.

IPv4(IPv4)

DHCPv4 Snooping

DHCP Snooping Global Settings

이 창은 전역 DHCP Snooping 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings 을 클릭합니다.

그림 9-25) DHCP Snooping Global Settings 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
DHCP Snooping	전역 DHCP Snooping 상태를 활성화하거나 비활성화하려면 선택합니다.
Information Option Allow Untrusted	신뢰할 수 없는 Interface 에서 릴레이 옵션 82 를 사용하여 DHCP 패킷을 전역적으로 허용하는 옵션을 활성화하거나 비활성화하려면 선택합니다.
Source MAC Verification	DHCP 패킷의 소스 MAC 주소가 클라이언트 하드웨어 주소와 일치하는지 확인을 활성화하거나 비활성화하려면 선택합니다.
Station Move Deny	DHCP Snooping 스테이션 이동 상태를 활성화하거나 비활성화하려면 선택합니다. DHCP Snooping 스테이션 이동이 활성화되면 특정 포트에서 동일한 VLAN ID 및 MAC 주소를 가진 동적 DHCP Snooping 바인딩 엔트리가 새 DHCP 프로세스가 동일한 VLAN ID 및 MAC 주소에 속한다는 것을 감지하면 다른 포트로 이동할 수 있습니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DHCP Snooping Port Settings

이 창은 DHCP Snooping 포트 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Port Settings 설정을 클릭합니다.

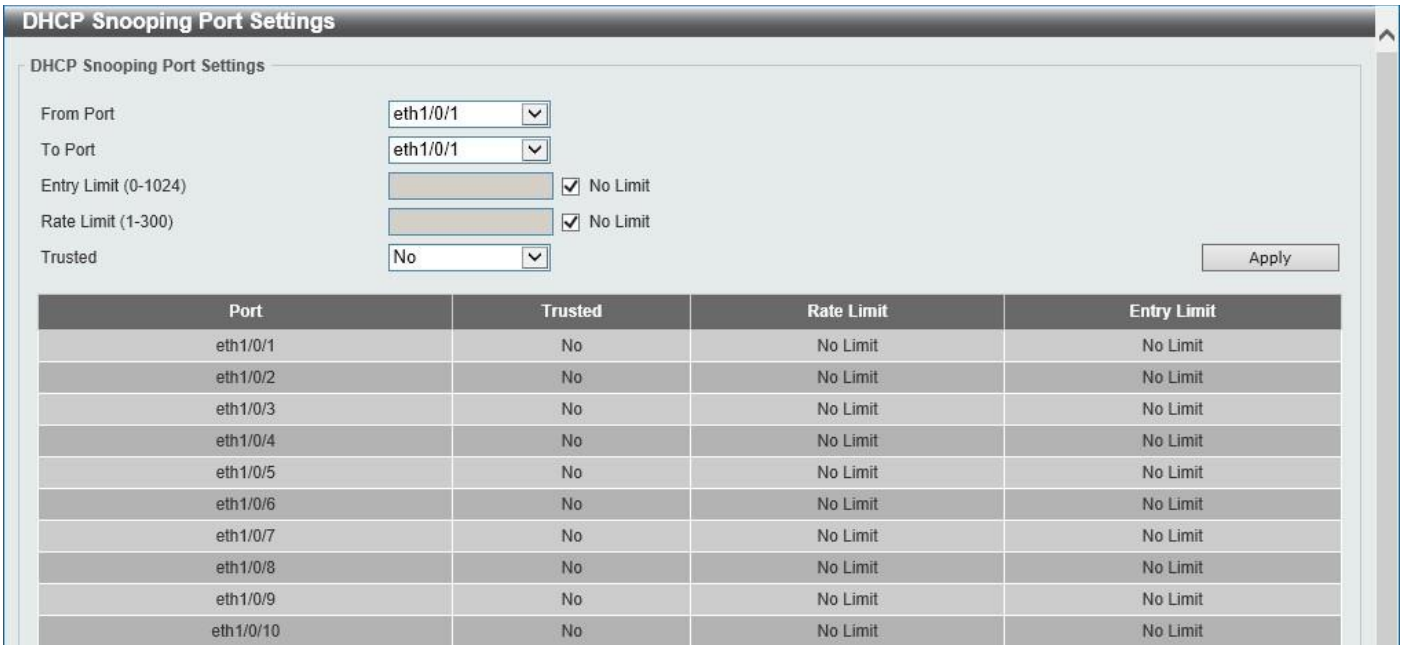

그림 9-26) DHCP Snooping 포트 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description

From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
Entry Limit	여기에 입장 제한 값을 입력합니다. 이 값은 0 에서 1024 사이여야 합니다. 체크 제한 없음 기능을 비활성화하는 옵션.
Rate Limit	여기에 속도 제한 값을 입력합니다. 이 값은 1 에서 300 사이여야 합니다. 체크 제한 없음 기능을 비활성화하는 옵션.
Trusted	여기에서 신뢰할 수 있는 옵션을 선택합니다. 선택할 수 있는 옵션은 아니요 와 예입니다. DHCP 서버 또는 다른 스위치에 연결된 포트는 신뢰할 수 있는 Interface 로 구성해야 합니다. DHCP 클라이언트에 연결된 포트는 신뢰할 수 없는 Interface 로 구성해야 합니다. DHCP Snooping 은 신뢰할 수 없는 Interface 와 DHCP 서버 간의 방화벽 역할을 합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DHCP Snooping VLAN Settings

이 창은 DHCP Snooping VLAN 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings 설정을 클릭합니다.

그림 9-27) DHCP Snooping VLAN 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
VID List	여기에 사용된 VLAN ID 목록을 입력합니다.
State	여기에서 DHCP Snooping VLAN 설정을 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DHCP Snooping Database

이 창은 DHCP Snooping 데이터베이스 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Database 를 클릭합니다.

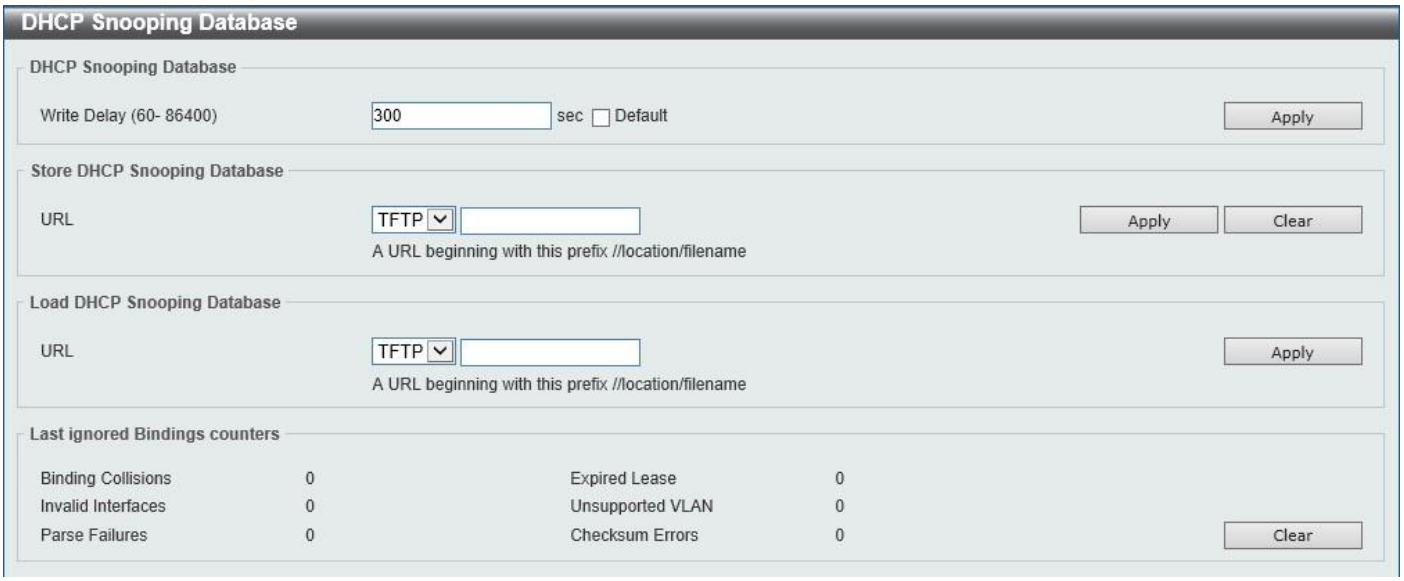

그림 9-28) DHCP Snooping 데이터베이스 창

DHCP Snooping 데이터베이스에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Write Delay	여기에 쓰기 지연 시간 값을 입력합니다. 이 값은 60 초에서 86400 초 사이여야 합니다. 기본적으로 이 값은 300 초입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Store DHCP Snooping Database 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
URL	DHCP Snooping 데이터베이스를 TFTP 서버에 저장하도록 지정합니다. 제공된 공간에 URL 을 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Load DHCP Snooping Database 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
URL	TFTP 서버에서 DHCP Snooping 데이터베이스를 로드하도록 지정합니다. 제공된 공간에 URL 을 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.
Clear 버튼을 클릭하여 모든 카운터 정보를 지웁니다.

DHCP Snooping Binding Entry

이 창은 DHCP Snooping 바인딩 엔트리를 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Binding Entry 항목을 클릭합니다.

그림 9-29) DHCP Snooping 바인딩 항목 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
MAC Address	여기에 DHCP Snooping 바인딩 엔트리의 MAC 주소를 입력합니다.
VID	여기에 DHCP Snooping 바인딩 엔트리의 VLAN ID 를 입력합니다. 이 값은 1 에서 4094 사이여야 합니다.
IP Address	여기에 DHCP Snooping 바인딩 엔트리의 IP Address 를 입력합니다.
Port	여기에서 컨피그레이션에 사용되는 적절한 포트를 선택합니다.
Expiry	여기에 사용된 만료 시간 값을 입력합니다. 이 값은 60 초에서 4294967295 초 사이여야 합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새 항목을 추가합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Dynamic ARP Inspection

ARP Access List

이 창은 동적 ARP 검사 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Access List 를 클릭합니다.

그림 9-30) ARP 액세스 목록 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
ARP Access List Name	여기에 사용된 ARP 액세스 목록 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새 항목을 추가합니다.

Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.
Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Edit 버튼을 클릭하면 다음과 같은 창이 나타납니다.

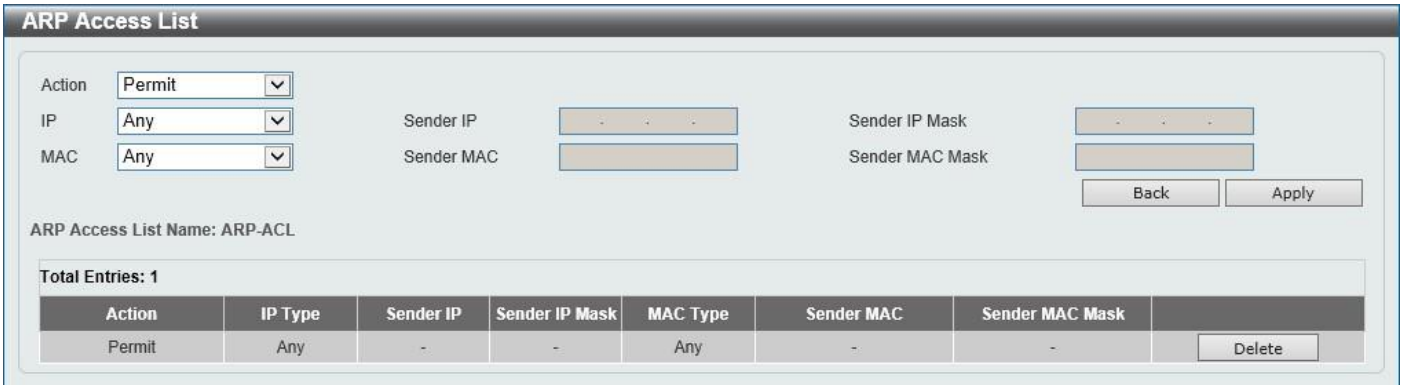

그림 9-31) ARP 액세스 목록(편집) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Action	여기에서 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 Permit 및 Deny 입니다.
IP	여기에서 사용할 보낸 사람 IP Address 유형을 선택합니다. 선택할 수 있는 옵션은 Any, Host 및 IP with Mask 입니다.
Sender IP	IP 유형으로 호스트 또는 마스크가 있는 IP 옵션을 선택한 후 여기에 사용된 발신자 IP Address 를 입력합니다.
Sender IP Mask	IP 유형으로 마스크가 있는 IP 옵션을 선택한 후 여기에 사용된 발신자 IP 마스크를 입력합니다.
MAC	여기에서 사용할 발신자 MAC 주소 유형을 선택합니다. 선택할 수 있는 옵션은 Any, Host 및 MAC with Mask 입니다.
Sender MAC	MAC 유형으로 Host 또는 MAC with Mask 옵션을 선택한 후 여기에 사용된 발신자 MAC 주소를 입력합니다.
Sender MAC Mask	MAC 유형으로 MAC with Mask 옵션을 선택한 후 여기에 사용된 발신자 MAC 마스크를 입력합니다.

Back 버튼을 클릭하여 이전 페이지로 돌아갑니다.
Apply 버튼을 클릭하여 변경 사항을 적용합니다.
Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

ARP Inspection Settings

이 창은 ARP 검사 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Settings 를 클릭합니다.

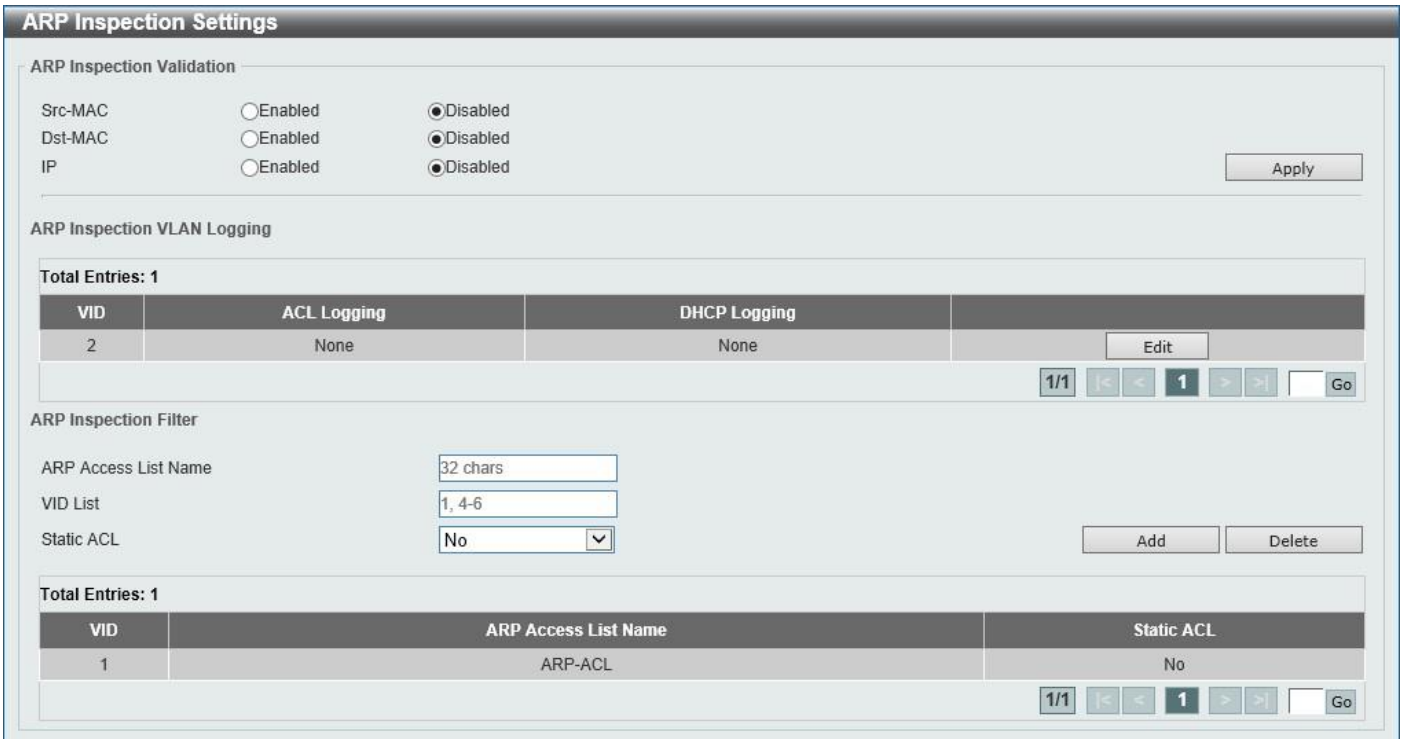

그림 9-32) ARP 검사 설정 창

ARP Inspection Validation(ARP 검사 검증)에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Src-MAC	여기에서 소스 MAC 옵션을 활성화하거나 비활성화하려면 선택합니다. 이 옵션은 ARP 요청 및 응답 패킷과 ARP 페이로드의 발신자 MAC 주소에 대한 이더넷 헤더의 소스 MAC 주소의 일관성을 확인하도록 지정합니다.
Dst-MAC	여기에서 대상 MAC 옵션을 활성화하거나 비활성화하려면 선택합니다. 이 옵션은 ARP 응답 패킷과 ARP 페이로드의 대상 MAC 주소에 대한 이더넷 헤더의 대상 MAC 주소의 일관성을 확인하도록 지정합니다.
IP	여기에서 IP 옵션을 활성화하거나 비활성화하려면 선택합니다. 이 옵션은 ARP 본문에서 유효하지 않은 IP Address 와 예기치 않은 Address S 를 확인하도록 지정합니다. 또한 ARP 페이로드에서 IP Address 의 유효성을 확인하도록 지정합니다. ARP 요청 및 응답의 발신자 IP 와 ARP 응답의 대상 IP 가 검증됩니다. IP Address 0.0.0.0, 255.255.255.255 및 모든 IP 멀티캐스트 주소로 향하는 패킷은 삭제됩니다. 보낸 사람 IP Address 는 모든 ARP 요청 및 응답에서 확인되고 대상 IP Address 는 ARP 응답에서만 확인됩니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Edit 버튼을 클릭하여 ARP 검사 VLAN 로깅 설정을 구성합니다.

Edit 버튼을 클릭한 후 다음 필드를 구성할 수 있습니다.

Parameter	Description

ACL Logging	여기에서 ACL 로깅 작업을 선택합니다. ACL 일치에 따라 삭제되거나 허용되는 패킷에 대한 로깅 기준을 지정합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Deny - 구성된 ACL 에 의해 거부된 경우 로깅을 지정합니다. • Permit - 구성된 ACL 에서 허용하는 경우 로깅을 지정합니다. • All - 구성된 ACL 에서 허용하거나 거부하는 경우 로깅을 지정합니다. • None - ACL 일치 패킷이 기록되지 않도록 지정합니다.
DHCP Logging	여기에서 DHCP 로깅 작업을 선택합니다. 이는 DHCP 바인딩에 대한 일치를 기반으로 삭제되거나 허용되는 패킷에 대한 로깅 기준을 지정합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Deny - DHCP 바인딩에 의해 거부된 경우 로깅을 지정합니다. • Permit - DHCP 바인딩에서 허용하는 경우 로깅을 지정합니다. • All - DHCP 바인딩에 의해 허용되거나 거부되는 경우 로깅을 지정합니다. • None - DHCP 바인딩에 의해 허용되거나 거부된 모든 패킷의 로깅을 방지하도록 지정합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

ARP Inspection Filter 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
ARP Access List Name	여기에 사용된 ARP 액세스 목록 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
VID List	여기에 사용된 VLAN ID 목록을 입력합니다.
Static ACL	여기에서 예 또는 아니요를 선택하여 정적 ACL 을 사용할지 여부를 선택합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새 항목을 추가합니다.

Delete 버튼을 클릭하여 입력한 정보에 따라 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

ARP Inspection Port Settings

이 창은 ARP 검사 포트 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Port Settings 를 클릭합니다.

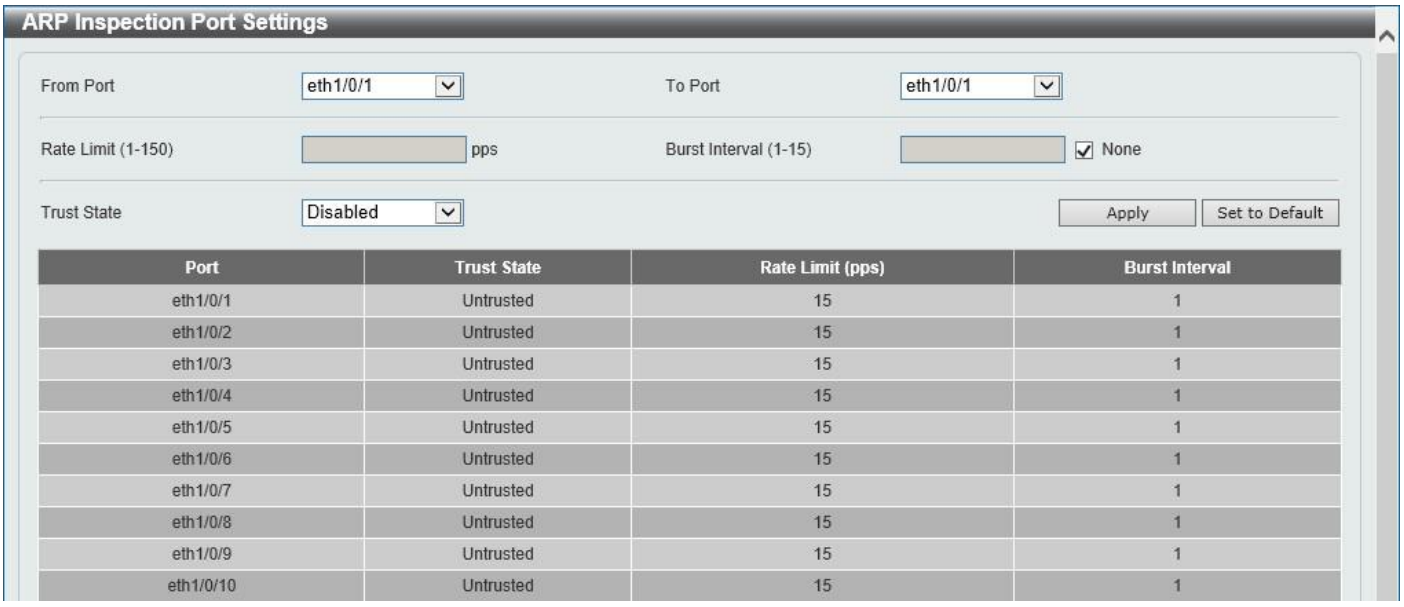

그림 9-33) ARP 검사 포트 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
Rate Limit 제한	여기에 속도 제한 값을 입력합니다. 이 값은 초당 1 에서 150 패킷 사이여야 합니다.
Burst Interval	여기에 버스트 간격 값을 입력합니다. 이 값은 1 에서 15 사이여야 합니다. 이 옵션을 활성화하려면 None 옵션을 체크 해제합니다.
Trust State	여기에서 신뢰 상태를 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Set to Default 버튼을 클릭하여 정보를 기본값으로 변경합니다.

ARP Inspection VLAN

이 창은 ARP Inspection VLAN 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection VLAN 을 클릭합니다.

그림 9-34 ARP 검사 VLAN 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
VID List	여기에 사용된 VLAN ID 목록을 입력합니다.
State	여기에서 지정된 VLAN 에 대한 ARP 검사 옵션의 상태를 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

ARP Inspection Statistics

이 창은 ARP 검사 통계 정보를 보고 지우는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Statistics 를 클릭합니다.

그림 9-35) ARP 검사 통계 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description

VID List	여기에 사용된 VLAN ID 목록을 입력합니다.

Clear by VLAN 버튼을 클릭하여 입력한 VLAN ID 에 따라 정보를 지웁니다.

Clear All 버튼을 클릭하여 이 테이블의 모든 정보를 지웁니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

ARP Inspection Log

이 창은 ARP 검사 로그 정보를 보고, 구성하고, 지우는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv4 > Dynamic ARP Inspection > ARP Inspection Log 를 클릭합니다.

그림 9-36) ARP 검사 로그 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Log Buffer	여기에 사용된 로그 버퍼 값을 입력합니다. 이 값은 1 에서 1024 사이여야 합니다. 기본적으로 이 값은 32 입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Clear Log 버튼을 클릭하여 로그를 지웁니다.

IP Source Guard

IP Source Guard Port Settings

이 창은 IPSG(IP Source Guard) 포트 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Port Settings 를 클릭합니다.

그림 9-37) IP Source Guard Port 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
State	여기에서 지정된 포트에 대한 IPSG 의 상태를 활성화하거나 비활성화하려면 선택합니다.

Validation	여기에 사용된 유효성 검사 방법을 선택합니다. 선택할 수 있는 옵션은 IP 및 IPMAC 입니다. IP 를 선택하면 수신된 패킷의 IP Address 가 확인됩니다. IP-MAC 을 선택하면 수신된 패킷의 IP Address 와 MAC 주소가 확인됩니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

IP Source Guard Binding

이 창은 IPSG 바인딩 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Binding 을 클릭합니다.

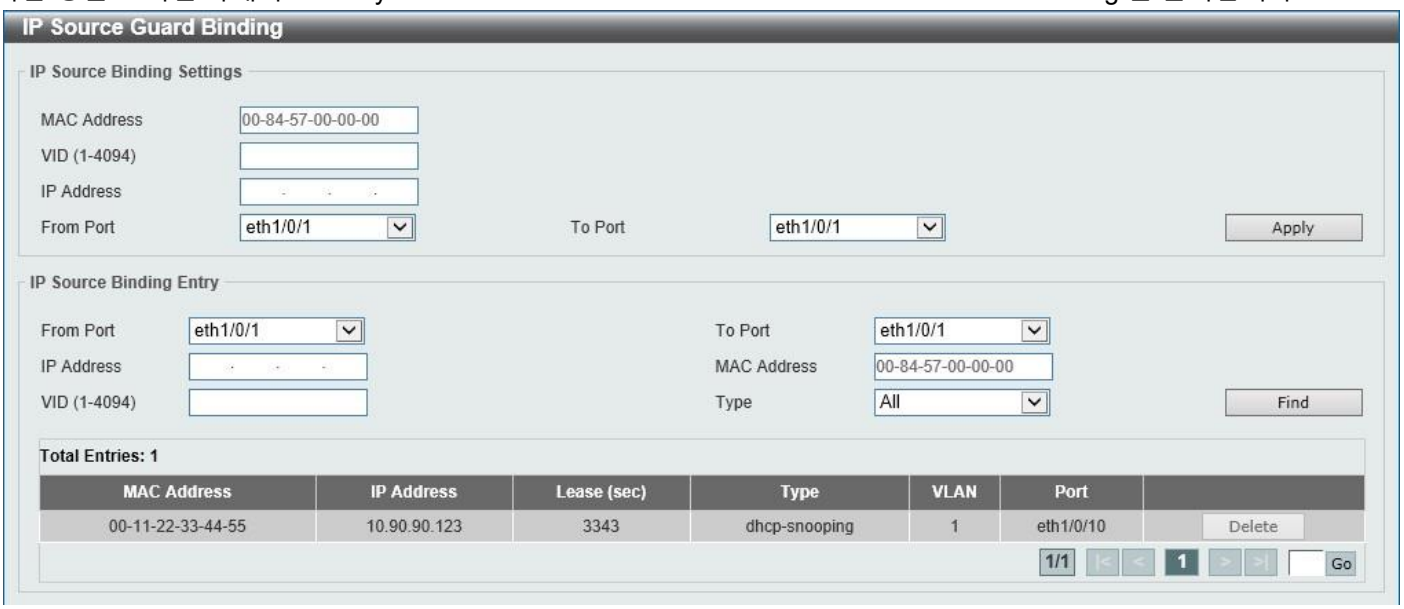

그림 9-38) IP Source Guard 바인딩 창

IP Source Binding Settings(IP 소스 바인딩 설정)에서 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
MAC Address	여기에 바인딩 항목의 MAC 주소를 입력합니다.
VID	여기에 바인딩 항목의 VLAN ID 를 입력합니다.
IP Address	여기에 바인딩 항목의 IP Address 를 입력합니다.
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

IP Source Binding Entry 에서 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 쿼리에 사용되는 적절한 포트 범위를 선택합니다.
IP Address	여기에 바인딩 항목의 IP Address 를 입력합니다.
MAC Address	여기에 바인딩 항목의 MAC 주소를 입력합니다.
VID	여기에 바인딩 항목의 VLAN ID 를 입력합니다.
Type	여기에서 찾을 바인딩 항목의 유형을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • All - 모든 DHCP 바인딩 항목이 표시되도록 지정합니다. • DHCP Snooping - DHCP 바인딩 Snooping 에 의해 학습된 IP 소스 가드 바인딩 항목을 표시하도록 지정합니다.

	• Static - 수동으로 구성된 IP-source guard 바인딩 항목을 표시하도록 지정합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

IP Source Guard HW Entry

이 창은 IPSG 하드웨어 항목을 보는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv4 > IP Source Guard > IP Source Guard HW Entry 를 클릭합니다.

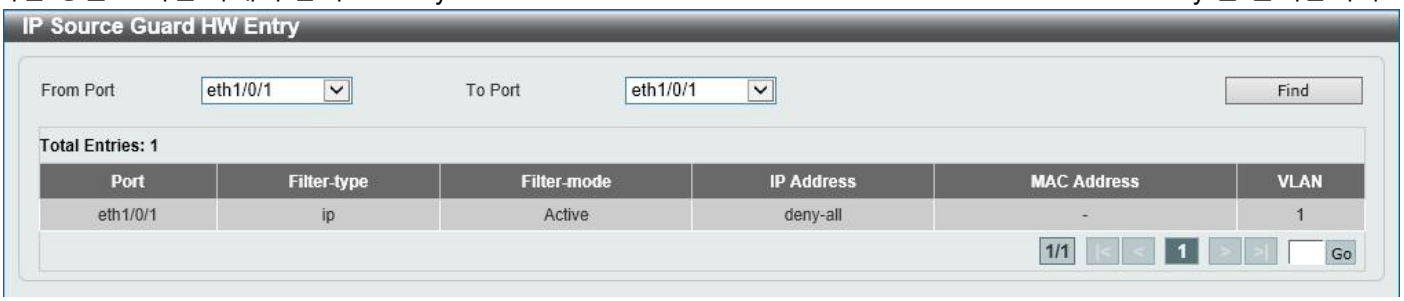

그림 9-39) IP Source Guard HW 입력 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 쿼리에 사용되는 적절한 포트 범위를 선택합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Advanced Settings

IP-MAC-Port Binding Settings

이 창은 IP-MAC-Port Binding Settings 을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Settings 설정을 클릭합니다.

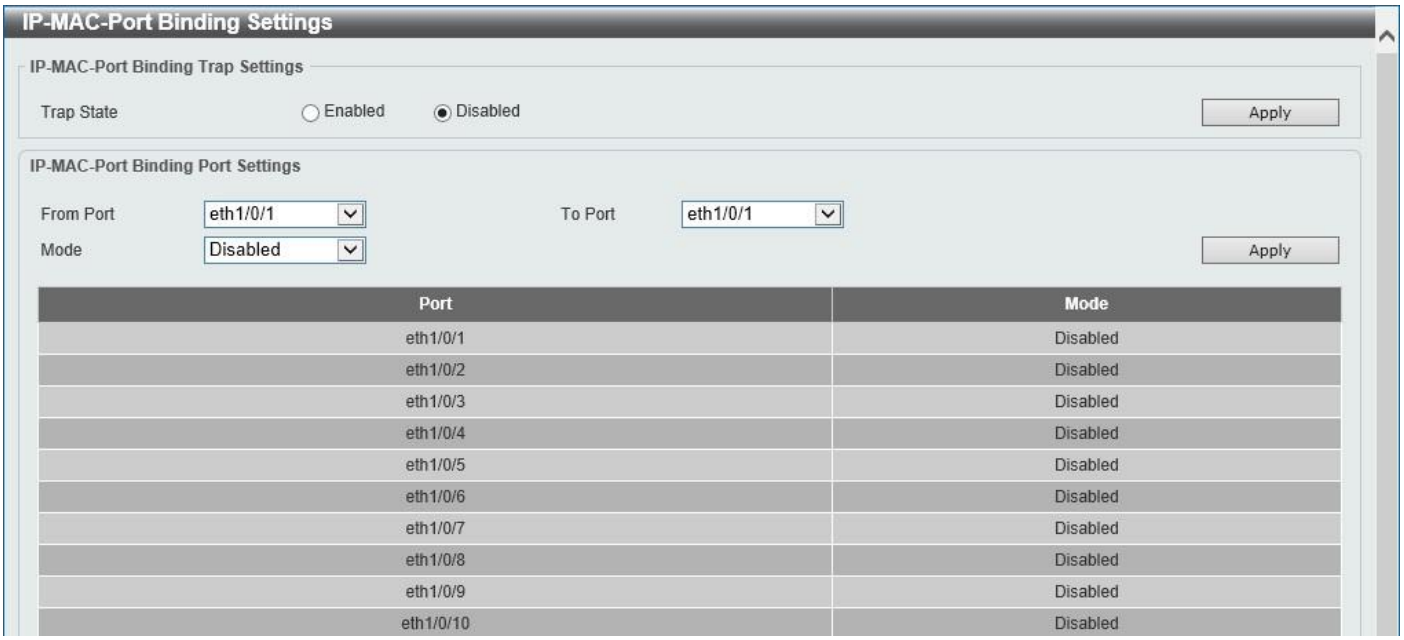

그림 9-40) IP-MAC-Port 바인딩 설정 창

IP-MAC-Port Binding Trap Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Trap State	IP-MAC-Port 바인딩 옵션의 트랩 상태를 활성화 또는 비활성화합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

IP-MAC-Port 바인딩 포트 설정에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
Mode	여기에서 사용할 액세스 제어 모드를 선택합니다. 선택할 수 있는 옵션은 Disabled, Strict 및 Loose 입니다. 포트가 IMPB 엄격 모드 액세스 제어를 사용하도록 설정된 경우 호스트는 ARP 또는 IP 패킷을 보내고 호스트에서 보낸 ARP 패킷 또는 IP 패킷이 바인딩 검사를 통과한 후에만 포트에 액세스할 수 있습니다. 바인딩 검사를 통과하려면 소스 IP Address, 소스 MAC 주소, VLAN ID 및 도착 포트 번호가 IPSG 정적 바인딩 항목 또는 DHCP Snooping 학습 동적 바인딩 항목으로 정의된 엔트리 중 하나와 일치해야 합니다. 포트가 IMPB 느슨한 모드 액세스 제어를 사용하도록 설정된 경우 호스트가 ARP 또는 IP 패킷을 보내고 호스트에서 보낸 ARP 패킷 또는 IP 패킷이 바인딩 검사를 통과하지 못한 후 호스트가 포트에 액세스할 수 없습니다. 바인딩 검사를 통과하려면 소스 IP Address, 소스 MAC 주소, VLAN ID 및 도착 포트가 IPSG 정적 바인딩 엔트리 또는 DHCP Snooping 학습 동적 바인딩 엔트리에 의해 정의된 엔트리 중 하나와 일치해야 합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

IP-MAC-Port Binding Blocked Entry

이 창은 IP-MAC-Port Binding Blocked Entry 테이블을 보고 지우는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Blocked Entry 을 클릭합니다.

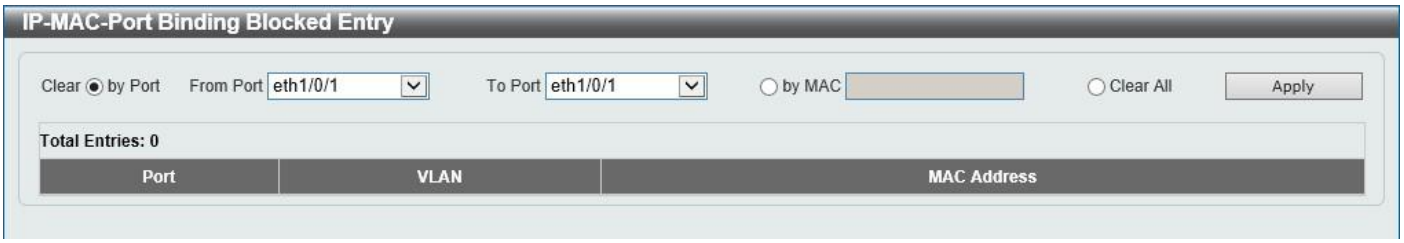

그림 9-41 IP-MAC-Port 바인딩 차단된 진입 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Clear by Port	선택한 포트에 따라 항목 테이블을 지우려면 이 옵션을 선택합니다.
From Port - To Port	여기에서 지울 적절한 포트 범위를 선택합니다.
Clear by MAC	입력한 MAC 주소를 기준으로 입력 테이블을 지우려면 이 옵션을 선택합니다. 제공된 공간에 지워질 MAC 주소를 입력합니다.
Clear All	MAC 주소가 포함된 모든 항목을 지우려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

IPv6

IPv6 Snooping

이 창은 IPv6 Snooping 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv6 > IPv6 Snooping 을 클릭합니다.

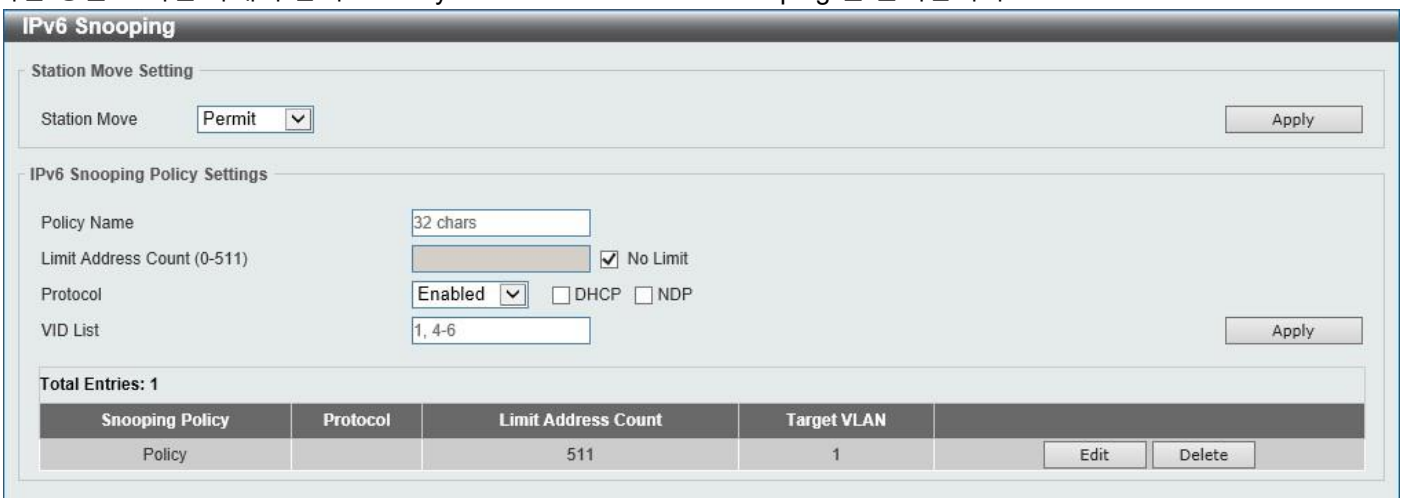

그림 9-42 IPv6 Snooping 창

Station Move Setting 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Station Move	여기에서 스테이션 이동 옵션을 선택합니다. 선택할 수 있는 옵션은 Permit 및 Deny 입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

IPv6 Snooping 정책 설정에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Policy Name	여기에 사용된 IPv6 Snooping 정책 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.

Limit Address Count	여기에 사용된 주소 수 제한 값을 입력합니다. 이 값은 0 에서 511 사이여야 합니다. 이 옵션을 비활성화하려면 No Limit 옵션을 선택하십시오.
Protocol	여기에서 프로토콜 상태를 선택합니다. 선택할 수 있는 옵션은 Enabled (활성화됨) 및 Disabled(비활성화됨)입니다. • DHCP - DHCPv6 패킷에서 주소를 Snooping 하도록 지정합니다. • NDP - NDP 패킷에서 주소를 Snooping 하도록 지정합니다. DHCPv6 Snooping 은 주소 할당 절차에서 DHCPv6 클라이언트와 서버 간에 전송되는 DHCPv6 패킷을 스니핑합니다. DHCPv6 클라이언트가 유효한 IPv6 주소를 성공적으로 얻으면 DHCPv6 Snooping 이 바인딩 데이터베이스를 생성합니다. ND Snooping 은 상태 비저장 자동 구성에 할당된 IPv6 주소 및 수동으로 구성된 IPv6 주소를 위해 설계되었습니다. IPv6 주소를 할당하기 전에 호스트는 먼저 중복 주소 감지를 수행해야 합니다. ND Snooping 은 DAD 메시지(DAD NS(Neighbor Solicitation) 및 DAD NA(Neighbor Advertisement))를 감지하여 바인딩 데이터베이스를 구축합니다. NDP 패킷(NS 및 NA)은 호스트에 여전히 연결할 수 있는지 여부를 감지하고 바인딩을 삭제할지 여부를 결정하는 데도 사용됩니다.
VID List	여기에 사용된 VLAN ID 목록을 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

IPv6 ND Inspection

이 창은 IPv6 ND Inspection 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv6 > IPv6 ND Inspection 을 클릭합니다.

그림 9-43 IPv6 ND 검사 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Policy Name	여기에 사용된 정책 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
장치 Device Role	여기에서 디바이스 역할을 선택합니다. 선택할 수 있는 옵션은 Host 와 Router 입니다. 기본적으로 디바이스의 역할은 호스트로 설정되고 NS 및 NA 메시지에 대한 검사가 수행됩니다. 디바이스 역할이 라우터로 설정된 경우 NS 및 NA 검사가 수행되지 않습니다. NS/NA 검사를 수행할 때 ND 프로토콜 또는 DHCP 에서 학습한 동적 바인딩 테이블에 대해 메시지를 확인합니다.

Validate Source-MAC	여기에서 소스 MAC 주소 옵션의 검증을 활성화하거나 비활성화하려면 선택합니다. 스위치가 링크 레이어 주소가 포함된 ND 메시지를 수신하면 소스 MAC 주소가 링크 레이어 주소에 대해 확인됩니다. 링크 레이어 주소와 MAC 주소가 서로 다른 경우 패킷이 삭제됩니다.
Target Port	이 옵션을 선택하여 대상 포트를 지정합니다.
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

IPv6 RA Guard

이 창은 IPv6 RA Guard 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv6 > IPv6 RA Guard 를 클릭합니다.

그림 9-44 IPv6 RA Guard 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Policy Name	여기에 정책 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Device Role	여기에서 디바이스 역할을 선택합니다. 선택할 수 있는 옵션은 Host 와 Router 입니다. 기본적으로 디바이스의 역할은 Host 이며, 모든 RA 패킷을 차단합니다. 장치의 역할이 라우터인 경우 RA 패킷은 포트의 바인딩된 ACL 에 따라 전달됩니다.
Match IPv6 Access List	여기에 일치시킬 IPv6 액세스 목록을 입력하거나 선택합니다. Please Select 버튼을 클릭하여 목록에서 기존 ACL 을 선택합니다.
Target Port	이 옵션을 선택하여 대상 포트를 지정합니다.
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Please Select 버튼을 클릭하면 다음 창이 나타납니다.

그림 9-45) ACL Access List 창

컨피그레이션에서 해당 ACL 을 사용하려면 항목 옆에 있는 라디오 버튼을 선택합니다.
페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.
OK 버튼을 클릭하여 선택 사항을 수락합니다.

IPv6 DHCP Guard

이 창은 IPv6 DHCP Guard 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv6 > IPv6 DHCP Guard 를 클릭합니다.

그림 9-46 IPv6 DHCP Guard 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Policy Name	여기에 정책 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Device Role	여기에서 디바이스 역할을 선택합니다. 선택할 수 있는 옵션은 Client(클라이언트)와 Server(서버)입니다. 기본적으로 장치의 역할은 클라이언트로 설정되며, 이 경우 DHCPv6 서버의 모든 DHCPv6 패킷이 차단됩니다. 장치의 역할이 서버로 설정된 경우 DHCPv6 서버 패킷은 포트의 바인딩된 ACL 에 따라 전달됩니다.
Match IPv6 Access List	여기에 일치시킬 IPv6 액세스 목록을 입력하거나 선택합니다. Please Select(선택하십시오) 버튼을 클릭하여 목록에서 기존 ACL 을 선택합니다.
Target Port	이 옵션을 선택하여 대상 포트를 지정합니다.
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.
Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.
Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Please Select 버튼을 클릭하면 다음 창이 나타납니다.

그림 9-47) ACL Access List 창

컨피그레이션에서 해당 ACL 을 사용하려면 항목 옆에 있는 라디오 버튼을 선택합니다.
페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.
OK 버튼을 클릭하여 선택 사항을 수락합니다.

IPv6 Source Guard

IPv6 Source Guard Settings

이 창은 IPv6 소스 가드 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Source Guard Settings 을 클릭합니다.

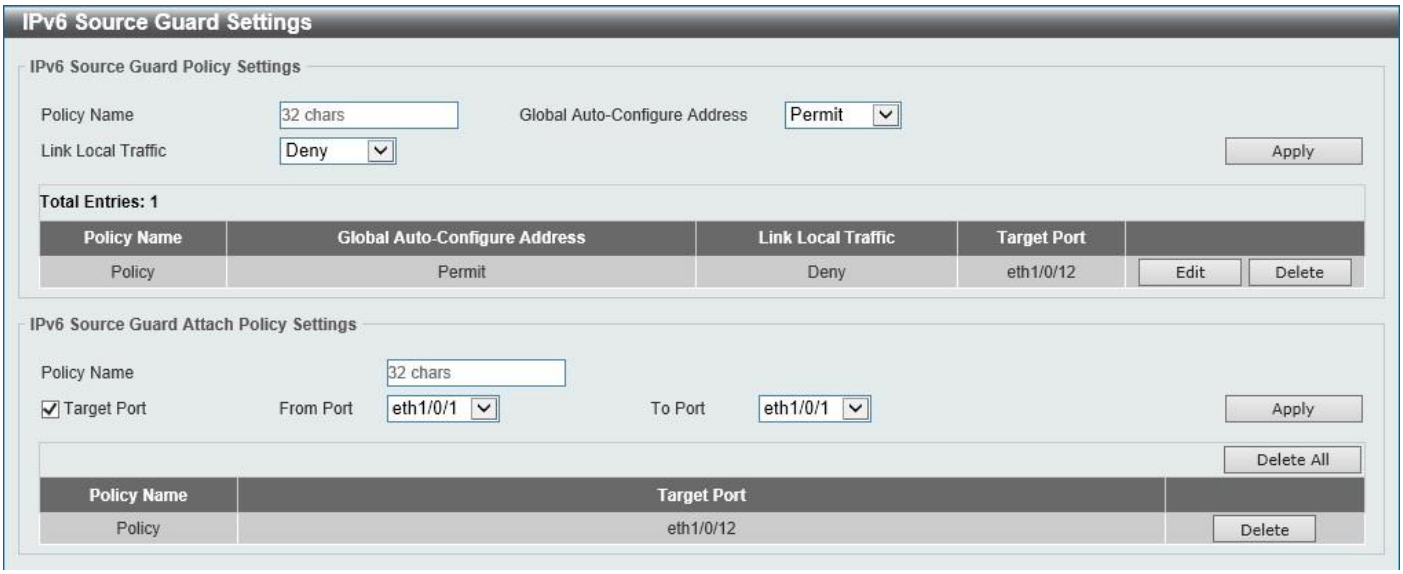

그림 9-48 IPv6 Source Guard 설정 창

IPv6 Source Guard 정책 설정에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Policy Name	여기에 정책 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Global Auto-Configure Address	자동 구성된 전역 주소에서 데이터 트래픽 거부를 허용하려면 선택합니다. 링크의 모든 전역 주소가 DHCP 및 자체 구성된 주소를 가진 호스트가 트래픽을 전송하지 못하도록 차단하려는 관리자에 의해 할당되는 경우에 유용합니다. 기본적으로 Permit 이 사용됩니다.
Link Local Traffic	링크-로컬 주소로 보내는 하드웨어 허용 데이터 트래픽 거부를 허용하려면 선택합니다. 기본적으로 Deny 가 사용됩니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.
Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.
Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

IPv6 Source Guard Attach Policy Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Policy Name	여기에 정책 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Target Port	대상 포트를 지정하려면 이 옵션을 선택합니다.
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete All 버튼을 클릭하여 모든 항목을 제거합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

IPv6 Neighbor Binding

이 창은 IPv6 Neighbor Binding 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Neighbor Binding 을 클릭합니다.

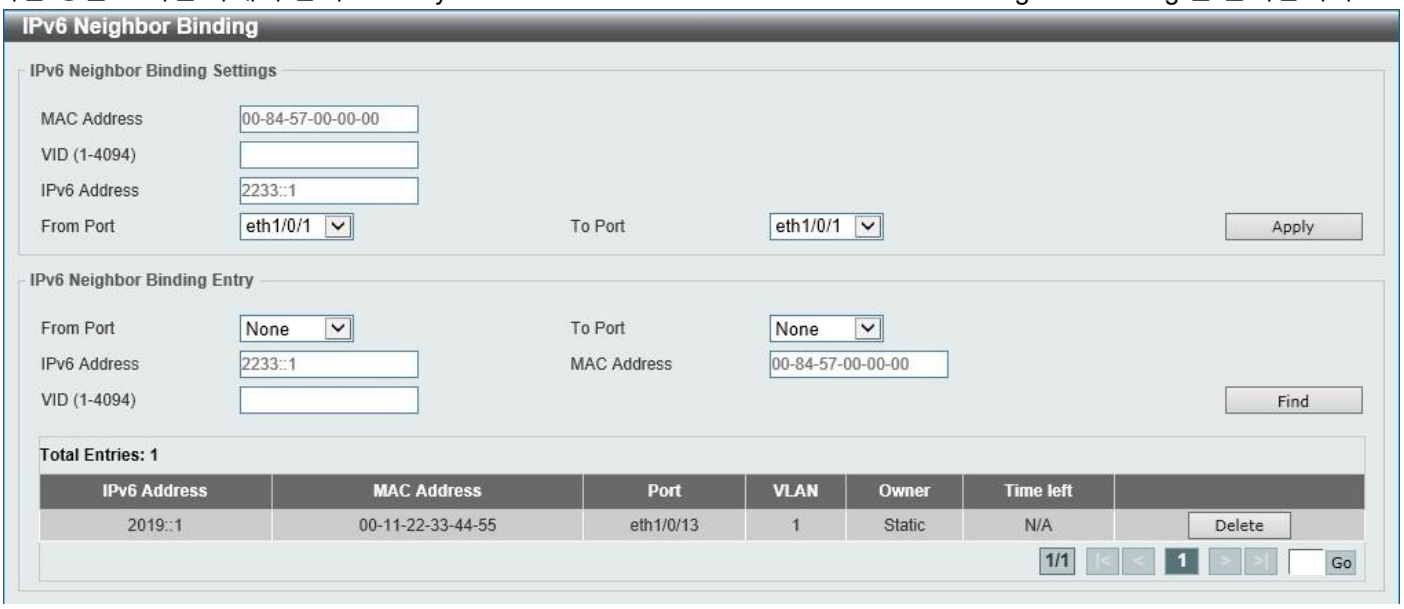

그림 9-49) IPv6 Neighbor Binding 창

IPv6 Neighbor Binding Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
MAC Address	여기에 사용된 MAC 주소를 입력합니다.
VID	여기에 사용된 VLAN ID 를 입력합니다. 이 값은 1 에서 4094 사이여야 합니다.
IPv6 Address	여기에 사용된 IPv6 주소를 입력합니다.
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

IPv6 Neighbor Binding Entry 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
From Port - To Port	여기에서 검색에 사용되는 적절한 포트 범위를 선택합니다.
IPv6 Address	여기에서 찾을 IPv6 주소를 입력합니다.
MAC Address	여기에서 찾을 MAC 주소를 입력합니다.

VID	여기에서 찾을 VLAN ID 를 입력합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

DHCP Server Screening

이 기능을 사용하면 모든 DHCP 서버 패킷을 제한할 수 있을 뿐만 아니라 지정된 DHCP 클라이언트에서 지정된 DHCP 서버 패킷을 받을 수도 있습니다. 네트워크에 하나 이상의 DHCP 서버가 있고 둘 다 서로 다른 클라이언트 그룹에 DHCP 서비스를 제공하는 경우에 유용합니다.

포트에서 DHCP 서버 스크리닝 기능이 활성화되면 이 포트에서 수신된 모든 DHCP 서버 패킷은 소프트웨어 기반 검사를 위해 CPU 로 리디렉션됩니다. 합법적인 DHCP 서버 패킷은 전달되고 잘못된 DHCP 서버 패킷은 삭제됩니다.

DHCP 서버 스크리닝 기능이 활성화되면 모든 DHCP 서버 패킷이 특정 포트에서 필터링됩니다.

DHCP Server Screening Global Settings

이 창은 전역 DHCP 서버 차단 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > DHCP Server Screening > DHCP Server Screening Global Settings 을 클릭합니다.

그림 9-50) DHCP Server Screening Global Settings 창

Trap Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Trap State	여기에서 DHCP 서버 스크리닝 트랩을 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

프로필 설정에서 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Profile Name	여기에 DHCP 서버 차단 프로파일 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.

만들기 버튼을 클릭하여 새 프로필을 만듭니다.

Binding 버튼을 클릭하여 프로파일에서 클라이언트 MAC 주소를 구성합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.
Profile Delete 버튼을 클릭하여 지정된 프로필을 제거합니다.

Log Information 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Log Buffer Entries	여기에 기록된 버퍼 항목 값을 입력합니다. 이 값은 10 에서 1024 사이여야 합니다. 기본적으로 이 값은 32 입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.
Clear Log 버튼을 클릭하여 로그를 지웁니다.

Binding 버튼을 클릭하면 다음 창이 나타납니다.

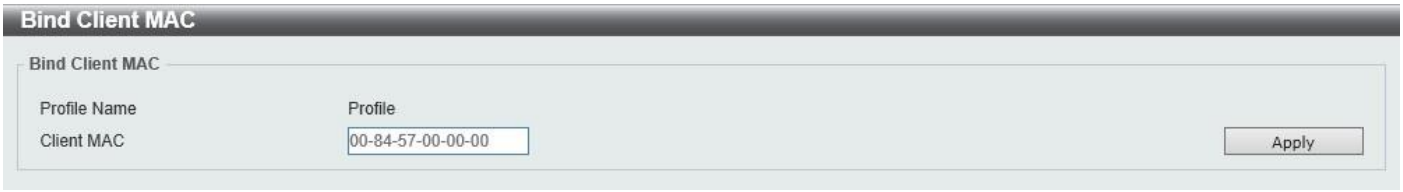

그림 9-51) Bind Client MAC 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Client MAC	여기에 사용된 MAC 주소를 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DHCP Server Screening Port Settings

이 창은 DHCP Server Screening Port 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > DHCP Server Screening > DHCP Server Screening Port Settings 을 클릭합니다.

그림 9-52) DHCP 서버 스크리닝 포트 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.

State	지정된 포트에서 DHCP 서버 차단 기능을 활성화하거나 비활성화하려면 선택합니다.
서버 IP	여기에 DHCP 서버 IP Address 를 입력합니다.
프로필 이름	여기에 지정된 포트에 사용할 DHCP 서버 차단 프로필을 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

ARP Spoofing Prevention

이 창은 ARP 스푸핑 방지 설정을 표시하고 구성하는 데 사용됩니다. 엔트리가 생성되면 송신자 IP Address 가 엔트리의 게이트웨이 IP Address 와 일치하지만 송신자 MAC 주소 필드가 엔트리의 게이트웨이 MAC 주소와 일치하지 않는 ARP 패킷이 시스템에 의해 삭제됩니다. ASP 는 발신자 IP Address 가 구성된 게이트웨이 IP Address 와 일치하지 않는 ARP 패킷을 우회합니다.

ARP 주소가 구성된 게이트웨이의 IP Address, MAC 주소 및 포트 목록과 일치하는 경우 수신 포트가 ARP 를 신뢰할 수 있는지 여부에 관계없이 DAI(Dynamic ARP Inspection) 검사를 우회합니다.

다음 창을 보려면 아래와 같이 Security > ARP Spoofing Prevention 을 클릭합니다.

그림 9-53) ARP 스푸핑 방지 창

ARP 스푸핑 방지에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
Gateway IP	여기에 사용된 게이트웨이 IP Address 를 입력합니다.
Gateway MAC	여기에 사용된 게이트웨이 MAC 주소를 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Network Access Authentication

Guest VLAN

이 창은 네트워크 액세스 인증 Guest VLAN 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > Network Access Authentication > Guest VLAN 을 클릭합니다.

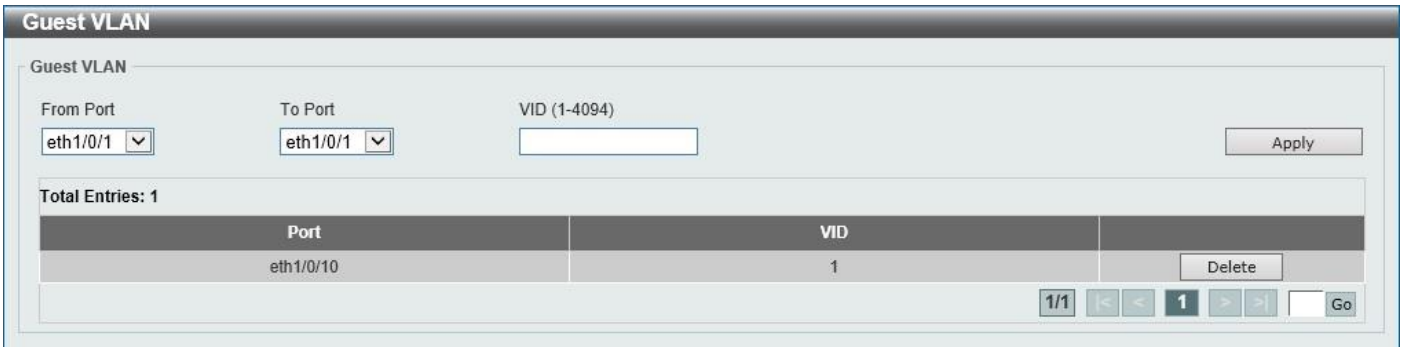

그림 9-54) 게스트 VLAN 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
VID	여기에 사용된 VLAN ID 를 입력합니다. 이 값은 1 에서 4094 사이여야 합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

Network Access Authentication Global Settings

이 창은 전역 네트워크 액세스 인증 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > Network Access Authentication > Network Access Authentication Global Settings 을 클릭합니다.

그림 9-55) 네트워크 액세스 인증 Global Settings 창

일반 설정에 대해 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Max Users	여기에 허용되는 최대 사용자 수를 입력합니다. 이 값은 1 에서 1000 사이여야 합니다. 기본값은 1000 입니다.
Authorization State	여기에서 인증된 상태를 활성화하거나 비활성화하려면 선택합니다. 이 옵션은 권한이 부여된 구성의 수락을 활성화하거나 비활성화하는 데 사용됩니다. 인증에 대해 권한 부여가 활성화되면 권한 부여 상태가 활성화된 경우 RADIUS 서버에서 할당한 권한 부여 속성(예: VLAN)이 수락됩니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

사용자 정보에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
User Name	여기에 사용된 사용자 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
VID	여기에 사용된 VLAN ID 를 입력합니다.
Password Type	암호 유형을 Plain Text 로 지정합니다.
Password	여기에 사용된 비밀번호를 입력합니다. 최대 32 자까지 입력할 수 있습니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Network Access Authentication Port Settings

이 창은 네트워크 액세스 인증 포트 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > Network Access Authentication > Network Access Authentication Port Settings 을 클릭합니다.

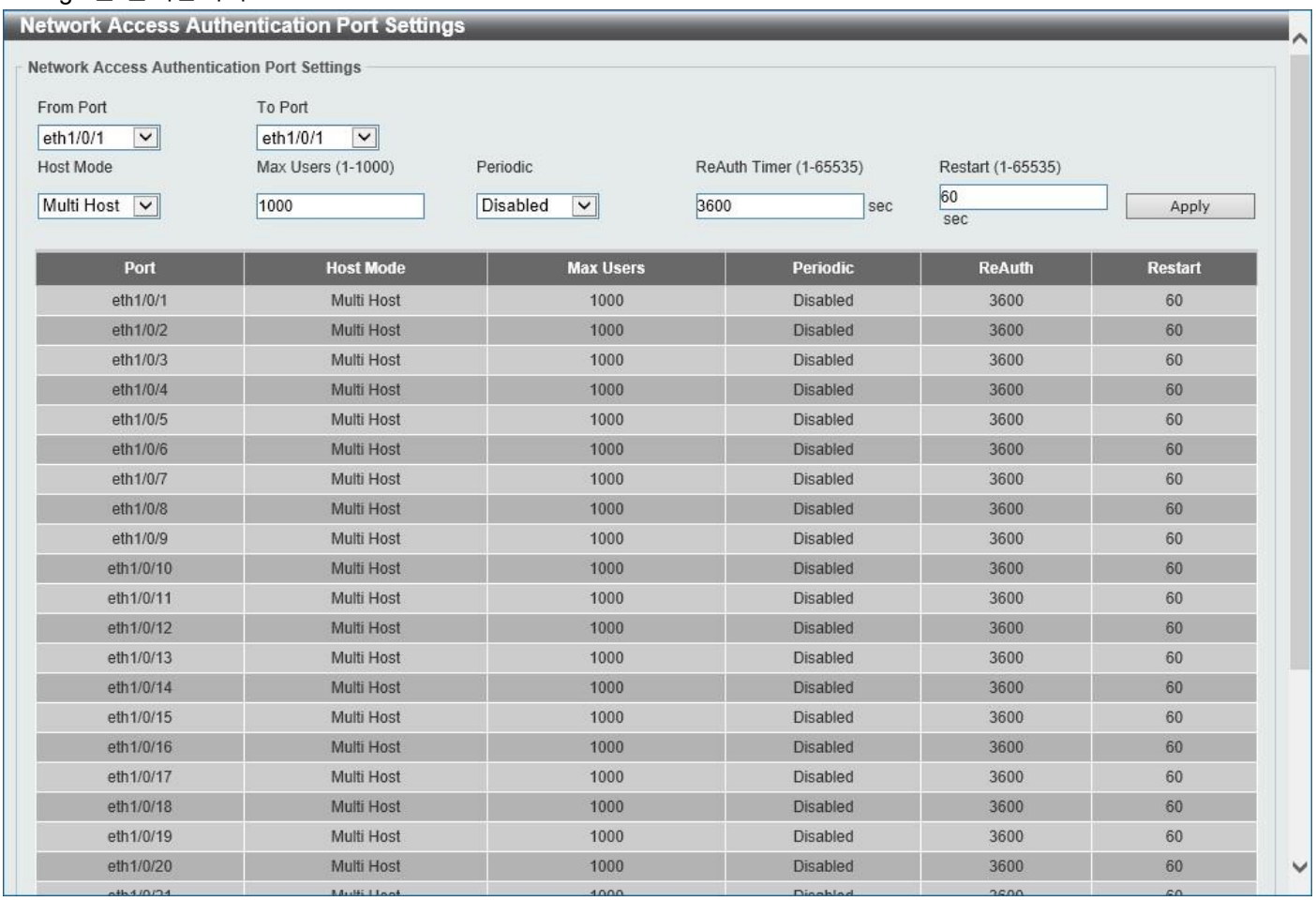

그림 9-56) 네트워크 액세스 인증 포트 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 구성에 대한 포트를 선택합니다.
Host Mode	여기에서 선택한 포트와 연결할 호스트 모드 옵션을 선택합니다. 선택할 수 있는 옵션은 Multi Host 및 Multi Auth 입니다. 포트가 다중 호스트 모드에서 작동하고 호스트 중 하나가 인증된 경우 다른 모든 호스트가 포트에 액세스할 수 있습니다. 802.1X 인증에 따라 재인증에 실패하거나 인증된 사용자가 로그오프하면 포트가 조용한 기간 동안 차단됩니다. 포트는 조용한 기간 후에 EAPOL 패킷의 처리를 복원합니다. 포트가 Multi Auth 모드에서 작동하는 경우 포트에 액세스하려면 각 호스트를 개별적으로 인증해야 합니다. 호스트는 MAC 주소로 표시됩니다. 인증된 호스트만 액세스할 수 있습니다.
Max Users	여기에 사용된 최대 사용자 값을 입력합니다. 이 값은 1 에서 1000 사이여야 합니다.
Periodic	여기에서 선택한 포트에 대한 주기적 재인증을 활성화하거나 비활성화하려면 선택합니다. 이 매개변수는 802.1X 프로토콜에만 영향을 줍니다.

ReAuth Timer	여기에 재인증 타이머 값을 입력합니다. 범위는 1 초에서 65535 초 사이입니다. 기본적으로 이 값은 3600 초입니다.
Restart	여기에 사용된 재시작 시간 값을 입력합니다. 범위는 1 초에서 65535 초 사이입니다. 기본적으로 이 값은 60 초입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Network Access Authentication Sessions Information

이 창은 네트워크 액세스 인증 세션 정보를 보고 지우는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > Network Access Authentication > Network Access Authentication Sessions Information 을 클릭합니다.

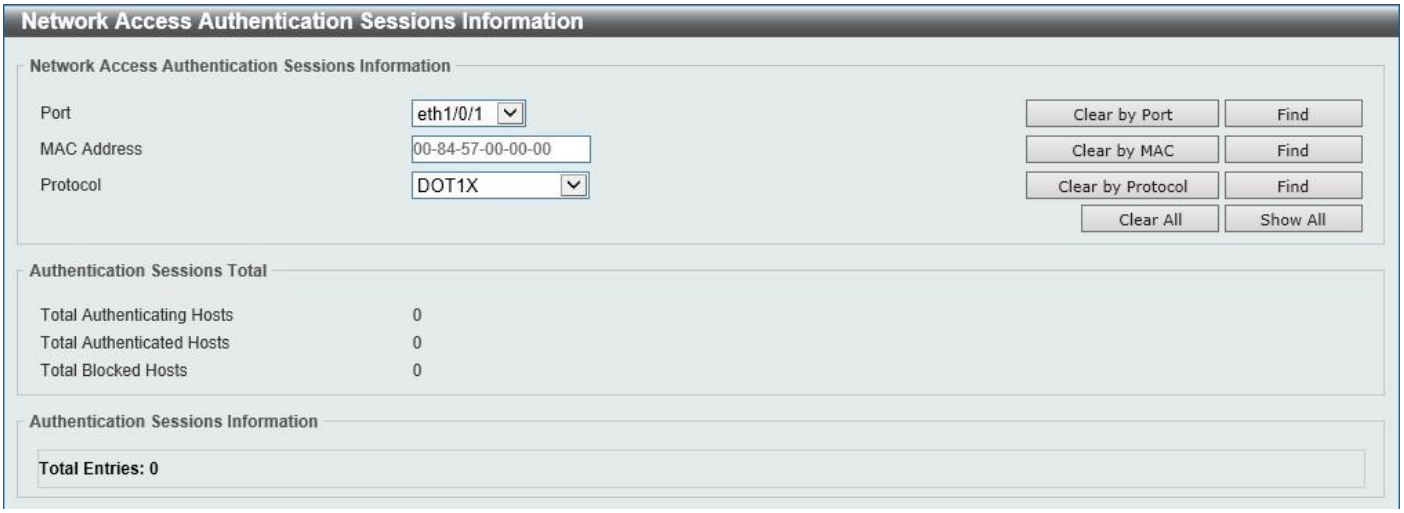

그림 9-57) 네트워크 액세스 인증 세션 정보 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Port	여기에서 쿼리에 대한 포트를 선택합니다.
MAC Address	여기에 사용된 MAC 주소를 입력합니다.
Protocol	프로토콜이 DOT1X(IEEE 802.1X) 임을 지정합니다.

Clear by Port 버튼을 클릭하여 선택한 포트에 따라 정보를 지웁니다.

MAC 으로 Clear 버튼을 클릭하여 입력한 MAC 주소를 기반으로 정보를 지웁니다.

Clear by Protocol 버튼을 클릭하여 선택한 프로토콜에 따라 정보를 지웁니다.

Clear All 버튼을 클릭하여 이 테이블의 모든 정보를 지웁니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Show All 버튼을 클릭하여 모든 항목을 찾아 표시합니다.

Safeguard Engine

네트워크의 악의적인 호스트가 주기적으로 패킷 플러딩(ARP 스톰) 또는 기타 방법을 사용하여 스위치를 공격할 수 있습니다. 이러한 공격은 스위치의 CPU 부하를 과도하게 증가시킬 수 있습니다. 이 문제를 완화하기 위해 Safeguard Engine 기능이 스위치 소프트웨어에 추가되었습니다.

Safeguard Engine 은 공격이 진행 중일 때 스위치의 작업량을 최소화하여 제한된 대역폭 내에서 필수 패킷을 네트워크에 전달할 수 있도록 함으로써 스위치의 전체 운영 능력을 향상시킵니다.

CPU 부하가 상승 임계값을 초과하면 Safeguard Engine 기능이 활성화되며, 스위치는 'Exhausted 모드'로 진입합니다. Exhausted 모드에서는 ARP 및 브로드캐스트 IP 패킷에 사용할 수 있는 대역폭이 제한됩니다. CPU 부하가 하락 임계값 이하로 떨어지면 Safeguard Engine 이 비활성화되며 스위치는 Exhausted 모드를 종료하고 정상 모드로 전환됩니다.
CPU 로 전송되는 패킷은 세 가지 그룹으로 분류할 수 있습니다. 이 그룹들은 '서브 인터페이스'라고도 불리며, CPU 가 특정 유형의 트래픽을 식별하는 데 사용하는 논리적 인터페이스입니다. 이 세 가지 그룹은 Protocol, Manage, Route 입니다.
일반적으로, 스위치의 CPU 가 수신 패킷을 처리할 때 Protocol 그룹은 가장 높은 우선순위를 부여받아야 하며, Route 그룹은 일반적으로 라우팅 패킷의 처리가 필요하지 않으므로 가장 낮은 우선순위를 부여받습니다. Protocol 그룹에는 라우터에서 식별된 프로토콜 제어 패킷이 포함됩니다. Manage 그룹에는 Telnet 과 SSH 와 같은 대화형 액세스 프로토콜을 통해 라우터 또는 시스템 네트워크 관리 인터페이스로 전송되는 패킷이 포함됩니다. Route 그룹에는 일반적으로 라우터 CPU 에 의해 처리되는 라우팅 패킷으로 식별된 패킷이 포함됩니다.

다음 표에는 지원되는 프로토콜 목록이 해당 하위 Interface(그룹)와 함께 표시됩니다.

Protocol Name	Sub-interface (Group)	Description
802.1X	Protocol	Port-based Network Access Control
ARP	Protocol	Address resolution Protocol
DHCP	Protocol	Dynamic Host Configuration Protocol
DNS	Protocol	Domain Name System
ICMPv4	Protocol	Internet Control Message Protocol
ICMPv6 Neighbor	Protocol	IPv6 Internet Control Message Protocol Neighbor Discovery Protocol (NS/NA/RS/RA)
ICMPv6-Other	Protocol	IPv6 Internet Control Message Protocol except Neighbor Discovery Protocol (NS/NA/RS/RA)
IGMP	Protocol	Internet Group Management Protocol
LACP	Protocol	Link Aggregation Control Protocol
SNMP	Manage	Simple Network Management Protocol
SSH	Manage	Secure Shell
STP	Protocol	Spanning Tree Protocol
Telnet	Manage	Telnet
TFTP	Manage	Trivial File Transfer Protocol
Web	Manage	HTTP(Hypertext Transfer Protocol) 및 HTTPS(Hypertext Transfer Protocol Secure)

사용자 지정 속도 제한(초당 패킷 수)은 Safeguard Engine 의 하위 Interface 전체 또는 관리 Interface 에서 사용자가 지정한 개별 프로토콜에 할당할 수 있습니다. 이 기능을 사용하여 개별 프로토콜에 대한 속도 제한을 사용자 지정할 때 부적절한 속도 제한으로 인해 스위치가 패킷을 비정상적으로 처리할 수 있으므로 주의하십시오.

참고: Safeguard Engine 이 활성화되면, 스위치는 FFP(Fast Filter Processor) 미터링 테이블을 사용하여 ARP 와 IP 같은 다양한 트래픽 흐름에 대역폭을 할당하여 CPU 사용량을 제어하고 트래픽을 제한합니다. 이로 인해 네트워크에서 라우팅 트래픽의 속도가 제한될 수 있습니다.

Safeguard Engine Settings

이 창은 세이프가드 엔진 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > Safeguard Engine > Safeguard Engine Settings 설정을 클릭합니다.

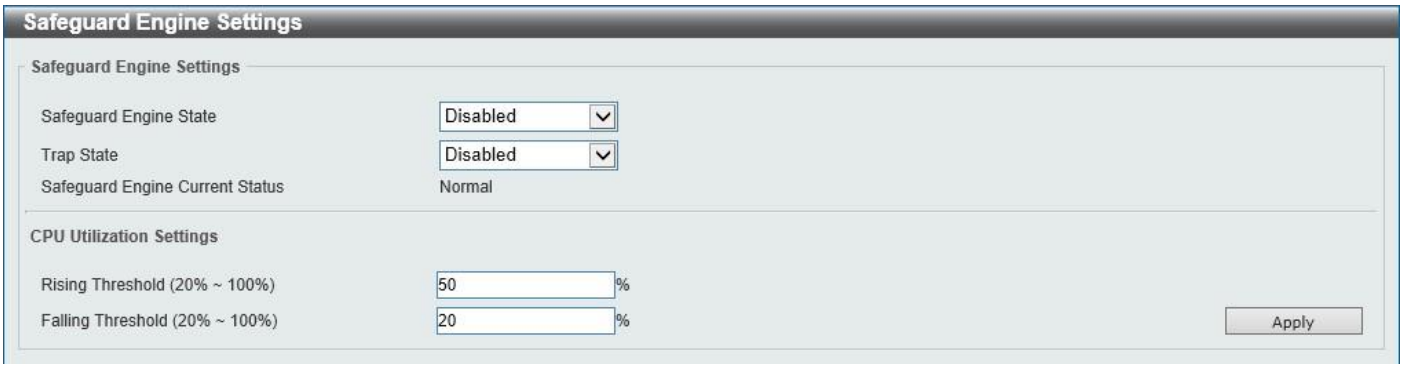

그림 9-58) Safeguard Engine 설정 창

Safeguard Engine Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Safeguard Engine State	여기에서 보호 엔진 기능을 활성화하거나 비활성화하려면 선택합니다.
Trap State	여기에서 세이프가드 엔진 트랩 상태를 활성화하거나 비활성화하려면 선택합니다.

CPU 사용률 설정에서 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Rising Threshold	여기에 상승 임계값을 입력합니다. 이 값은 20%에서 100% 사이여야 합니다. 이 값은 Safeguard Engine 메커니즘이 활성화되기 전에 허용 가능한 CPU 사용률 수준을 구성하는 데 사용됩니다. CPU 사용률이 이 백분율 수준에 도달하면 스위치는 이 창에 제공된 매개변수에 따라 소진 모드로 전환됩니다.
Falling Threshold	여기에 떨어지는 임계값을 입력합니다. 이 값은 20%에서 100% 사이여야 합니다. 이 값은 허용 가능한 CPU 사용률 수준을 백분율로 구성하는 데 사용되며, 여기서 스위치는 Safeguard Engine 상태를 벗어나 일반 모드로 돌아갑니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

CPU Protect Counters

이 창은 CPU Protect Counters 정보를 보고 지우는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > Safeguard Engine > CPU Protect Counters 를 클릭합니다.

그림 9-59) CPU Protect Counters 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description

Sub Interface	여기에서 하위 Interface 옵션을 선택합니다. 선택할 수 있는 옵션은 Manage, Protocol, Route 및 All 입니다. 이 옵션은 하위 Interface 의 CPU 보호 관련 카운터를 지우도록 지정합니다.
Protocol Name	여기에서 프로토콜 이름 옵션을 선택합니다.

Clear 버튼을 클릭하여 선택한 항목에 따라 정보를 지웁니다.

Clear All 버튼을 클릭하여 이 테이블의 모든 정보를 지웁니다.

CPU Protect Sub-Interface

이 창은 CPU Protect Sub-Interface 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > Safeguard Engine > CPU Protect Sub-Interface 를 클릭합니다.

그림 9-60 CPU Protect Sub-Interface 창

CPU Protect Sub-Interface 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Sub-Interface	여기에서 하위 Interface 옵션을 선택합니다. 선택할 수 있는 옵션은 Manage(관리), Protocol(프로토콜) 및 Route(경로)입니다.
Rate Limit	여기에 사용된 속도 제한 값을 입력합니다. 이 값은 초당 0 에서 1024 패킷 사이여야 합니다. 속도 제한을 비활성화하려면 No Limit 옵션을 선택하십시오.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Sub-Interface Information 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Sub-Interface	여기에서 하위 Interface 옵션을 선택합니다. 선택할 수 있는 옵션은 Manage, Protocol 및 Route 입니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

CPU Protect Type

이 창은 CPU Protect Type 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > Safeguard Engine > CPU Protect Type 을 클릭합니다.

그림 9-61) CPU 보호 유형 창

CPU Protect Type 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Protocol Name	여기에서 프로토콜 이름 옵션을 선택합니다.
Rate Limit	여기에 사용된 속도 제한 값을 입력합니다. 이 값은 초당 0 에서 1024 패킷 사이여야 합니다. 속도 제한을 비활성화하려면 No Limit 옵션을 선택하십시오.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Protect Type Information 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Type	여기에서 프로토콜 유형을 선택합니다. 프로토콜 유형을 선택하면 프로토콜 유형에 할당된 Rate Limit 가 표시됩니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Trusted Host

이 창은 신뢰할 수 있는 호스트 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > Trusted Host 를 클릭합니다.

그림 9-62) Trusted Host 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
ACL Name	여기에 액세스 클래스의 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Type	여기에서 신뢰할 수 있는 호스트 유형을 선택합니다. 선택할 수 있는 옵션은 Telnet, SSH, Ping, HTTP 및 HTTPS 입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 특정 항목을 제거합니다.

Traffic Segmentation Settings

이 창은 트래픽 세분화 설정을 표시하고 구성하는 데 사용됩니다. 트래픽 세분화 전달 도메인이 지정되면, 포트가 수신한 패킷은 해당 도메인 내 인터페이스로의 Layer 2 패킷 전달이 제한됩니다. 포트의 전달 도메인이 비어 있는 경우, 포트가 수신한 패킷의 Layer 2 전달에는 제한이 없습니다.

트래픽 세분화 멤버 목록은 포트와 포트 채널 같은 다양한 인터페이스 유형으로 구성될 수 있으며, 동일한 전달 도메인 내에 있을 수 있습니다. 명령어로 지정된 인터페이스에 포트 채널이 포함된 경우, 해당 포트 채널의 모든 멤버 포트가 전달 도메인에 포함됩니다.

인터페이스의 전달 도메인이 비어 있으면, 포트가 수신한 패킷의 Layer 2 전달에는 제한이 없습니다.

다음 창을 보려면 아래와 같이 Security > Traffic Segmentation Settings 을 클릭합니다.

그림 9-63) Traffic Segmentation Settings 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 구성에 사용되는 수신 포트 범위를 선택합니다.
From Forward Port ~ To Forward Port	여기에서 컨피그레이션에 사용되는 전달 포트 범위를 선택합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새 항목을 추가합니다.

Delete 버튼을 클릭하여 입력한 정보에 따라 항목을 제거합니다.

Storm Control Settings

이 창은 Storm Control Settings 을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > Storm Control Settings 를 클릭합니다.

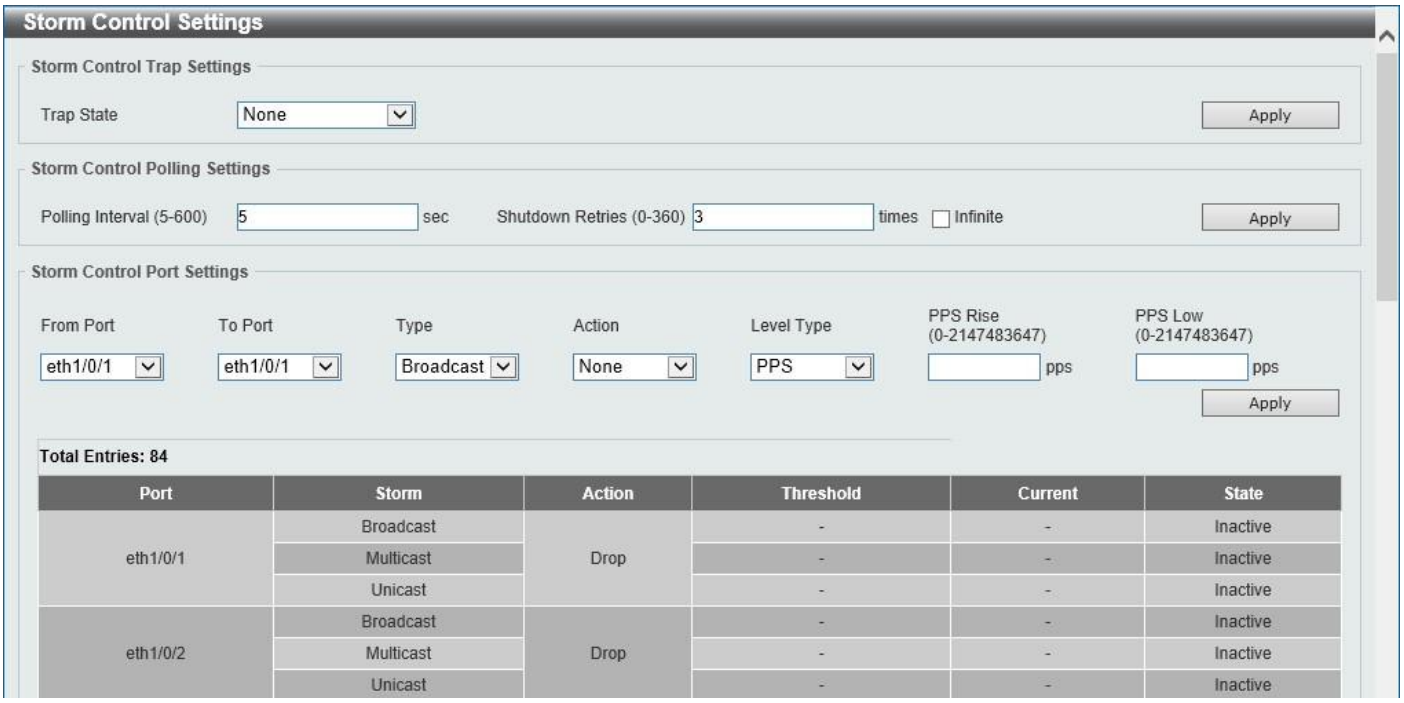

그림 9-64) Storm Control 설정 창

Storm Control Trap Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Trap State	여기에서 폭풍 통제 트랩 옵션을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • None - 트랩이 전송되지 않도록 지정합니다. • Storm Occurs - 스톰 이벤트가 감지될 때 트랩 알림이 전송되도록 지정합니다. • Storm Clear - 스톰 이벤트가 지워질 때 트랩 알림이 전송되도록 지정합니다. • Both - 스톰 이벤트가 감지 및/또는 지워질 때 트랩 알림이 전송되도록 지정합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Storm Control Polling Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Polling Interval	여기에 사용된 간격 값을 입력합니다. 이 값은 5 초에서 600 초 사이여야 합니다. 기본적으로 이 값은 5 초입니다.
Shutdown Retries	여기에 사용된 종료 재시도 값을 입력합니다. 이 값은 0 에서 360 사이여야 합니다. 기본적으로 이 값은 3 입니다. 이 기능을 비활성화하려면 무한 옵션을 선택하십시오.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Storm Control Port Settings 에서 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.

Type	여기에서 제어할 폭풍 공격 유형을 선택합니다. 선택할 수 있는 옵션은 브로드캐스트, 멀티캐스트 및 유니캐스트입니다. 작업이 종료 모드로 구성되면 유니캐스트는 알려진 유니캐스트 패킷과 알 수 없는 유니캐스트 패킷을 모두 참조합니다. 즉, 알려진 유니캐스트 패킷과 알 수 없는 유니캐스트 패킷이 지정된 임계값에 도달하면 포트가 종료됩니다. 그렇지 않으면 유니캐스트는 알 수 없는 유니캐스트 패킷을 참조합니다.
Action	여기에서 수행할 작업을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • None - 폭풍 패킷을 필터링하지 않도록 지정합니다. • Shutdown - rise threshold 에 지정된 값에 도달할 때 포트를 종료하도록 지정합니다. • Drop - 상승된 임계값을 초과하는 패킷을 삭제하도록 지정합니다.
Level Type	여기에서 레벨 유형 옵션을 선택합니다. 선택할 수 있는 옵션은 PPS, Kbps 및 레벨입니다.
PPS Rise	여기에 rise packets per second 값을 입력합니다. 이 옵션은 상승 임계값을 packets count per second 로 지정합니다. 이 값은 초당 0 에서 2147483647 패킷 사이여야 합니다. 낮은 PPS 값을 지정하지 않으면 기본값은 지정된 상승 PPS 의 80%입니다.
PPS Low	여기에 low packets per second 값을 입력합니다. 이 옵션은 초당 패킷 수에서 낮은 임계값을 지정합니다. 이 값은 초당 0 에서 2147483647 패킷 사이여야 합니다. 낮은 PPS 값을 지정하지 않으면 기본값은 지정된 상승 PPS 의 80%입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Kbps 옵션을 Level Type 으로 선택한 후 사용할 수 있는 매개변수는 다음과 같습니다.

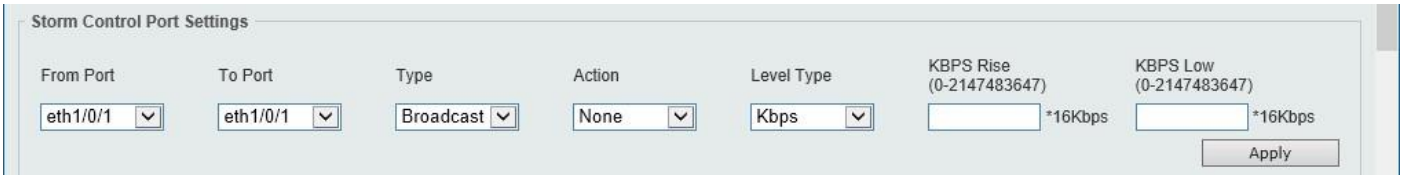

그림 9-65 Storm Control 설정(Level Type - Kbps) 창

Storm Control Port Settings 에서 구성할 수 있는 추가 필드는 다음과 같습니다.

Parameter	Description
KBPS Rise	여기에 사용된 상승 KBPS 값을 입력합니다. 이 옵션은 상승 임계값을 포트에서 트래픽이 수신되는 초당 킬로비트의 속도로 지정합니다. 이 값은 0 에서 2147483647 Kbps 사이여야 합니다.
KBPS Low	여기에 사용된 낮은 KBPS 값을 입력합니다. 이 옵션은 낮은 임계값을 포트에서 트래픽이 수신되는 초당 킬로비트 속도로 지정합니다. 이 값은 0 에서 2147483647 Kbps 사이여야 합니다. 낮은 KBPS 를 지정하지 않으면 기본값은 지정된 상승 KBPS 의 80%입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Level 옵션을 Level Type 으로 선택한 후 사용할 수 있는 매개변수는 다음과 같습니다.

그림 9-66 Storm Control 설정(Level Type - Level) 창

Storm Control Port Settings 에서 구성할 수 있는 추가 필드는 다음과 같습니다.

Parameter	Description
KBPS Rise	여기에 사용된 상승 레벨 값을 입력합니다. 이 옵션은 포트에서 트래픽이 수신되는 포트당 총 대역폭의 백분율로 상승 임계값을 지정합니다. 이 값은 0%에서 100% 사이여야 합니다.
KBPS Low	여기에 사용된 낮은 수준 값을 입력합니다. 이 옵션은 포트에서 트래픽이 수신되는 포트당 총 대역폭의 백분율로 낮은 임계값을 지정합니다. 이 값은 0%에서 100% 사이여야 합니다. 낮은 수준을 지정하지 않으면 기본값은 지정된 상승 수준의 80%입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DoS Attack Prevention Settings

이 창은 DoS(Denial-of-Service) 공격 방지 설정을 표시하고 구성하는 데 사용됩니다. 다음은 대부분의 스위치에서 탐지할 수 있는 잘 알려진 DoS 공격 유형입니다.

- Land Attack: 소스와 대상 주소가 타겟 장치의 주소로 설정된 IP 패킷을 사용하는 공격입니다. 타겟 장치가 자신에게 지속적으로 응답하게 만들 수 있습니다.
- Blat Attack: TCP/UDP 소스 포트가 타겟 장치의 대상 포트와 동일한 패킷을 보내는 공격입니다. 타겟 장치가 자신에게 응답하게 할 수 있습니다.
- TCP-Null: 시퀀스 번호가 0 이고 플래그가 없는 특정 패킷을 사용한 포트 스캐닝 공격입니다.
- TCP-Xmas: 시퀀스 번호가 0 이며 URG(Urgent), PSH(Push), FIN 플래그를 가진 특정 패킷을 사용한 포트 스캐닝 공격입니다.
- TCP SYN-FIN: SYN 및 FIN 플래그를 포함하는 특정 패킷을 사용한 포트 스캐닝 공격입니다.
- TCP SYN SrcPort Less 1024: 소스 포트가 0 에서 1023 사이이고 SYN 플래그를 포함하는 특정 패킷을 사용한 포트 스캐닝 공격입니다.
- Ping of Death Attack: 비정상적이거나 악의적인 핑 패킷을 보내는 공격입니다. 핑은 보통 64 바이트이지만, 65535 바이트를 초과하는 큰 핑 패킷을 보내면 타겟 컴퓨터가 충돌할 수 있습니다. 이 크기의 패킷은 조각화하여 전송할 수 있으며, 타겟 컴퓨터가 재조립하는 과정에서 버퍼 오버플로가 발생하여 시스템 충돌을 유발할 수 있습니다.
- TCP Tiny Fragment Attack: IP 단편화를 사용해 매우 작은 조각을 만들어 TCP 헤더 정보를 별도의 패킷 조각으로 나누어 라우터의 검사를 통과한 후 공격을 시도하는 공격입니다.
- Smurf Attack: Smurf 는 DDoS.Smurf 악성 코드를 활성화하고 실행하는 DDoS 공격입니다. 많은 ICMP Echo 요청 패킷을 보내는 핑 플러드 공격과 유사하지만, 브로드캐스트 네트워크의 특성을 악용하여 공격을 증폭시키는 공격 벡터입니다.
- TCP Flag SYN RST: TCP SYN/RESET 플러드는 정상적인 TCP 3 방향 핸드셰이크를 악용해 타겟의 자원을 소모시켜 응답하지 못하게 만드는 DDoS 공격입니다. TCP 연결 요청이 타겟이 처리할 수 있는 속도보다 빠르게 전송되어 네트워크 트래픽이 포화 상태가 될 수 있습니다.
- All Types: 위의 모든 유형을 포함합니다.

다음 창을 보려면 아래와 같이 Security > DoS Attack Prevention Settings 을 클릭합니다.

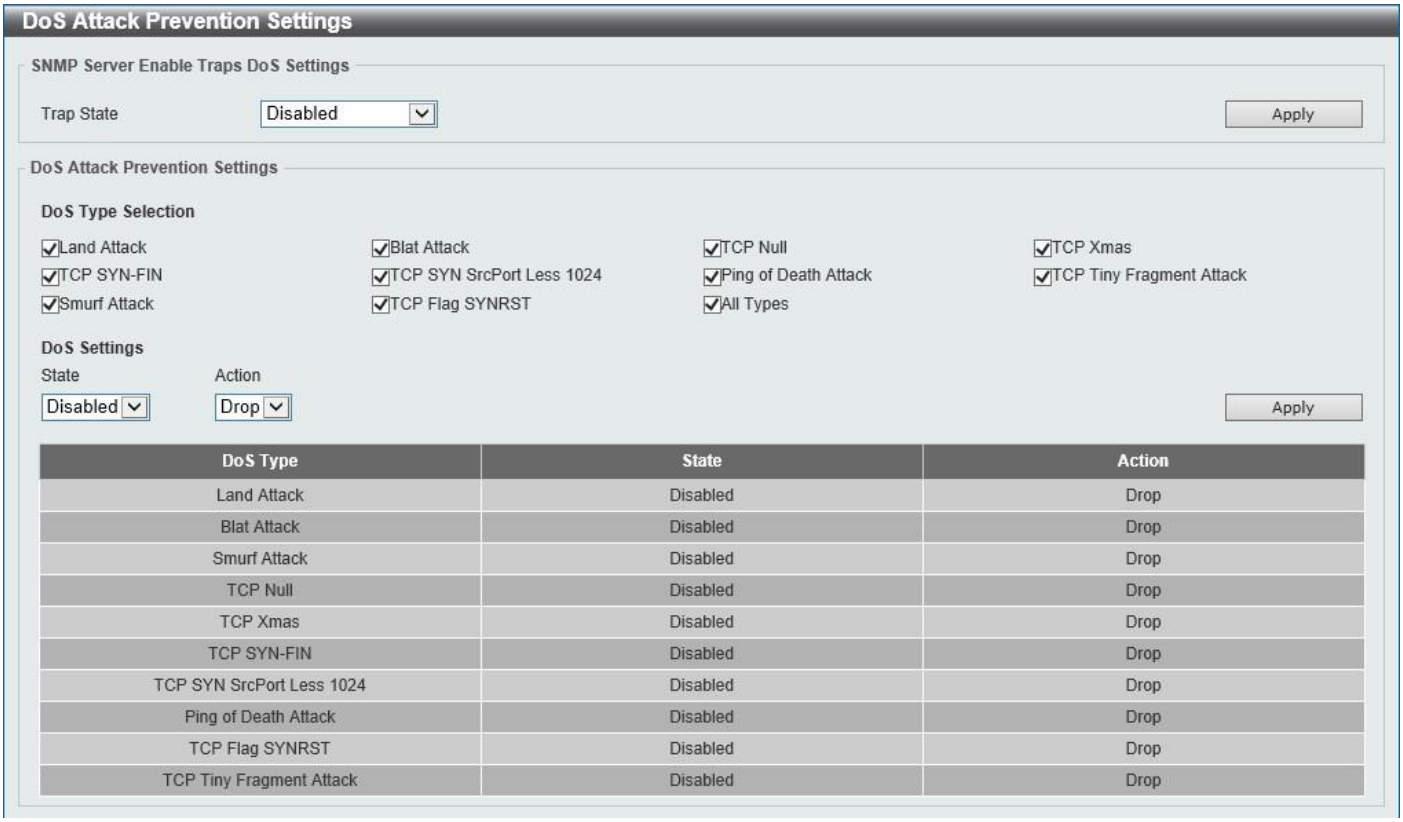

그림 9-67 DoS 공격 차단 설정 창

SNMP Server Enable Traps DoS Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Trap State	여기에서 DoS 공격 방지 트랩 상태를 활성화하거나 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

DoS Attack Prevention Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
DoS Type Selection	여기에서 방지할 DoS 유형 옵션을 선택합니다.
State	여기에서 전역 DoS 공격 방지 상태를 활성화하거나 비활성화하려면 선택합니다.
Action	여기에서 DoS 공격이 탐지되었을 때 수행할 작업을 선택합니다. 여기서 선택할 수 있는 유일한 옵션은 드롭입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

SSH

SSH(Secure Shell)는 안전하지 않은 네트워크에서 안전한 원격 로그인 및 네트워크 서비스를 제공하는 프로그램입니다. 이를 통해 원격 호스트 컴퓨터에 안전하게 로그인하고 원격 엔드 노드에서 명령을 안전하게 실행할 수 있으며, 신뢰할 수 없는 두 호스트 간에 암호화되고 인증된 통신을 제공합니다. SSH 는 오늘날의 네트워킹 환경에서 필수적인 도구로, 네트워크 통신을 위협하는 다양한 보안 위험에 대해 강력한 방어 수단입니다.

원격 PC(SSH 클라이언트)와 스위치(SSH 서버) 간의 안전한 통신을 위해 SSH 프로토콜을 사용하는 단계는 다음과 같습니다:

- 관리자 수준 사용자 계정 생성: User Accounts 창을 사용하여 관리자 수준 액세스를 가진 사용자 계정을 생성합니다. 이 작업은 스위치에 다른 관리자 수준의 사용자 계정을 생성하는 것과 동일하며, 비밀번호 지정이

포함됩니다. 이 비밀번호는 SSH 프로토콜을 사용하여 안전한 통신 경로가 설정된 후 스위치에 로그인하는 데 사용됩니다.

- 사용자 계정의 인증 방법 구성: SSH User Authentication Mode 창을 사용하여 스위치와 SSH 연결을 설정할 수 있는 사용자를 식별하기 위해 지정된 인증 방법을 설정합니다. SSH 가 사용자를 인증하는 방법에는 호스트 기반, 비밀번호, 공개 키의 세 가지가 있습니다.
- 암호화 알고리즘 구성: SSH Authentication Method and Algorithm Settings 창을 사용하여 SSH 클라이언트와 SSH 서버 간에 전송되는 메시지를 암호화하고 해독할 암호화 알고리즘을 설정합니다.
- SSH 활성화: SSH Configuration 창을 사용하여 스위치에서 SSH 를 활성화합니다.

이러한 단계를 완료하면 원격 PC 의 SSH 클라이언트를 사용하여 스위치를 안전한 인밴드 연결로 관리할 수 있습니다.

SSH Global Settings

이 창은 전역 SSH 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > SSH > SSH Global Settings 을 클릭합니다.

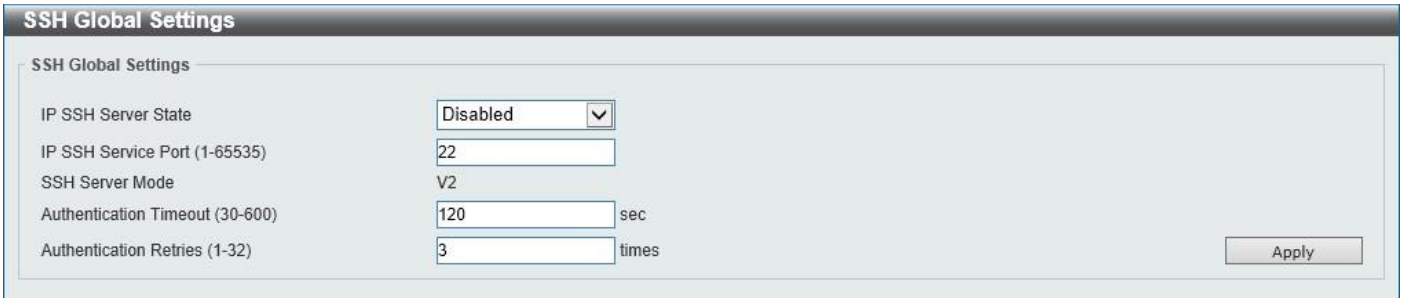

그림 9-68) SSH Global Settings 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
IP SSH Server State	전역 SSH 서버 상태를 활성화하거나 비활성화하려면 선택합니다.
IP SSH Service Port	여기에 사용된 SSH 서비스 포트 번호를 입력합니다. 이 값은 1 에서 65535 사이여야 합니다. 기본적으로 이 숫자는 22 입니다.
Authentication Timeout	여기에 인증 시간 제한 값을 입력합니다. 이 값은 30 초에서 600 초 사이여야 합니다. 기본적으로 이 값은 120 초입니다.
Authentication Retries	여기에 인증 재시도 값을 입력합니다. 이 값은 1 에서 32 사이여야 합니다. 기본적으로 이 값은 3 입니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Host Key

이 창은 SSH Host Key 를 확인하고 생성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > SSH > Host Key 를 클릭합니다.

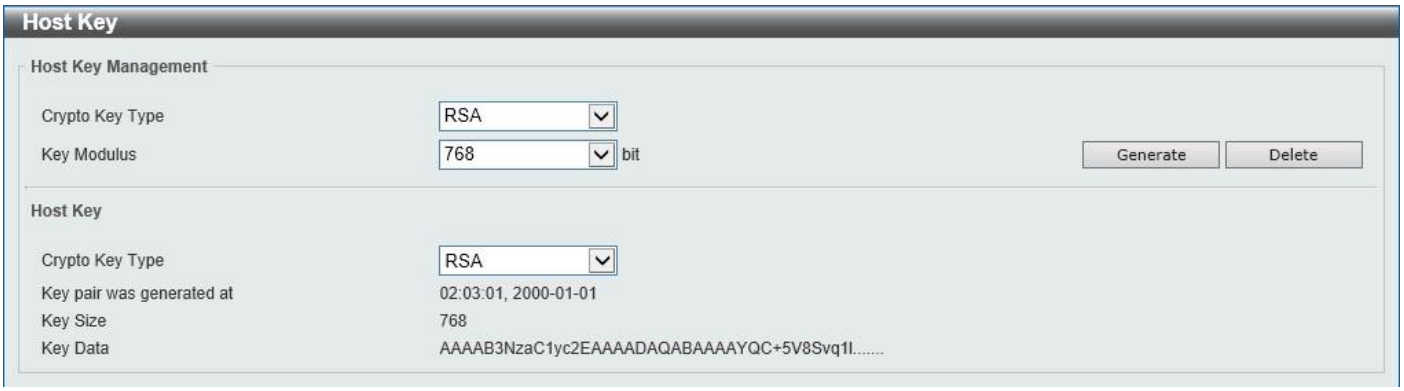

그림 9-69) Host Key 창

Host Key Management 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Crypto Key Type	여기에 사용된 암호화 키 유형을 선택합니다. RSA(Rivest Shamir Adleman) 키 유형과 DSA(Digital Signature Algorithm) 키 유형 중에서 선택할 수 있습니다.
Key Modulus	여기에서 키 모듈러스 값을 선택합니다. 360, 512, 768, 1024 및 2048 비트 중에서 선택할 수 있습니다.

Generate 버튼을 클릭하여 선택한 항목에 따라 호스트 키를 생성합니다.
Delete 버튼을 클릭하여 선택한 항목에 따라 호스트 키를 제거합니다.

Host Key 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Crypto Key Type	여기에 사용된 암호화 키 유형을 선택합니다. RSA(Rivest Shamir Adleman) 키 유형과 DSA(Digital Signature Algorithm) 키 유형 중에서 선택할 수 있습니다.

생성 버튼을 클릭하면 다음 창이 나타납니다.

그림 9-70 Host Key (Generating) 창

키가 성공적으로 생성되면 다음 창이 나타납니다.

그림 9-71 Host Key (Generating, Success) 창

SSH Server Connection

이 창은 SSH Server Connection 테이블을 보는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > SSH > SSH Server Connection 을 클릭합니다.

그림 9-72 SSH 서버 연결 창

SSH User Settings

이 창은 SSH User Settings 을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > SSH > SSH User Settings 을 클릭합니다.

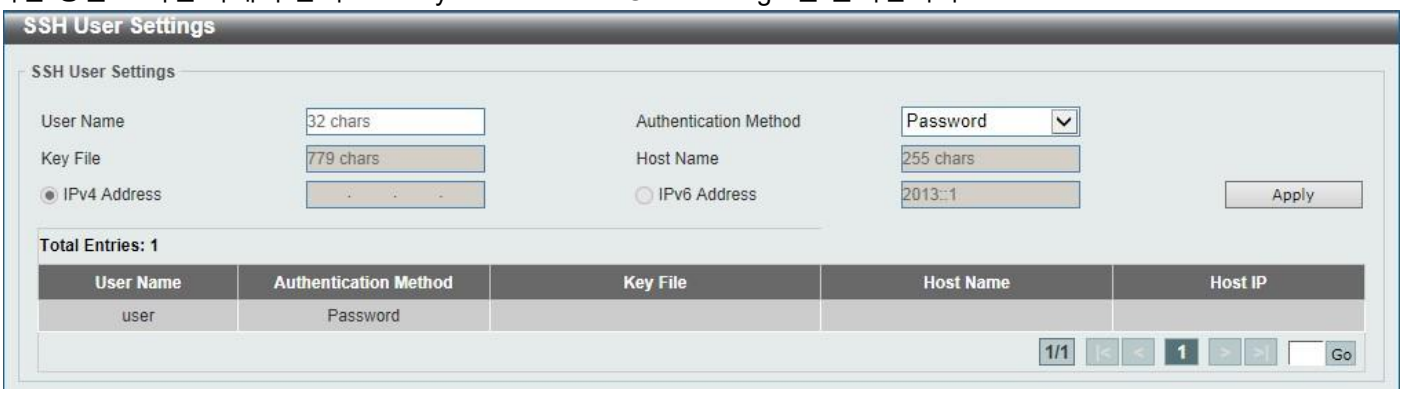

그림 9-73 SSH 사용자 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
User Name	여기에 사용된 SSH 사용자의 사용자 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Authentication Method	여기에 사용된 인증 방법을 선택합니다. 선택할 수 있는 옵션은 Password, Public Key 및 Host-based 입니다.
Key File	인증 방법으로 공개 키 또는 호스트 기반 옵션을 선택한 후 여기에 공개 키를 입력합니다.
Host Name	Authentication Method 로 Host-based 옵션을 선택한 후 여기에 호스트 이름을 입력합니다.
IPv4 Address	Authentication Method 로 Host-based 옵션을 선택한 후 여기에 IPv4 주소를 선택하고 입력합니다.
IPv6 Address	Authentication Method 로 Host-based 옵션을 선택한 후 여기에 IPv6 주소를 선택하고 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

페이지 번호를 입력하고 Go 버튼을 클릭하여 여러 페이지가 있는 경우 특정 페이지로 이동합니다.

SSL

SSL(Secure Sockets Layer)은 인증, 디지털 서명, 암호화를 통해 서버와 클라이언트 간에 안전한 통신 경로를 제공하는 보안 기능입니다. 이 보안 기능은 암호화 세트(Cipher Suite)를 통해 구현되며, 이는 인증 세션에 사용할 정확한 암호화 매개 변수, 특정 암호화 알고리즘 및 키 크기를 결정하는 보안 문자열로 세 가지 레벨로 구성됩니다:

- 키 교환(Key Exchange): 암호화 세트의 첫 번째 부분은 사용할 공개 키 알고리즘을 지정합니다. 이 스위치는 Rivest Shamir Adleman(RSA) 공개 키 알고리즘과 디지털 서명 알고리즘(DSA), 그리고 DHE DSS Diffie-

Hellman(DHE) 공개 키 알고리즘을 사용합니다. 이것은 클라이언트와 서버 간의 첫 번째 인증 과정으로, "키 교환"을 통해 일치하는 키를 찾고 인증을 승인하여 다음 단계에서 암호화 협상을 진행합니다.

- 암호화(Encryption): 암호화 세트의 두 번째 부분으로, 클라이언트와 호스트 간에 전송되는 메시지를 암호화하기 위해 사용됩니다. 스위치는 두 가지 암호화 알고리즘을 지원합니다:
    - 스트림 암호(Stream Ciphers): 스위치에는 40 비트 키와 128 비트 키를 사용하는 두 가지 유형의 RC4 스트림 암호가 있습니다. 이 키는 메시지 암호화에 사용되며, 최적의 사용을 위해 클라이언트와 호스트 간에 일관성을 유지해야 합니다.
    - CBC 블록 암호(CBC Block Ciphers): CBC(Cipher Block Chaining)는 이전에 암호화된 텍스트의 일부를 현재 블록의 암호화에 사용하는 방식입니다. 스위치는 데이터 암호화 표준(DES)과 고급 암호화 표준(AES)으로 정의된 3DES EDE 암호화를 지원합니다.
- 해시 알고리즘(Hash Algorithm): 암호화 세트의 마지막 부분으로, 메시지 인증 코드를 결정할 메시지 다이제스트 함수를 선택할 수 있습니다. 이 메시지 인증 코드는 전송된 메시지와 함께 암호화되어 무결성을 제공하고 재전송 공격을 방지합니다. 스위치는 세 가지 해시 알고리즘, MD5(Message Digest 5), SHA(Secure Hash Algorithm), SHA256 을 지원합니다.

이 세 가지 매개 변수는 네 가지 선택 옵션으로 조합되어 서버와 클라이언트 간의 안전한 통신을 위한 3 단계 암호화 코드를 생성합니다. 사용자는 사용할 수 있는 암호화 세트 중 하나 또는 여러 개를 구현할 수 있지만, 다른 암호화 세트는 보안 수준과 연결 성능에 영향을 미칠 수 있습니다. 암호화 세트에 포함된 정보는 스위치에 포함되지 않으며, 인증서 파일 형태로 외부에서 다운로드해야 합니다. 이 기능은 인증서 파일이 있어야 실행할 수 있으며, TFTP 서버 또는 스위치 파일 시스템을 통해 스위치에 다운로드할 수 있습니다. 스위치는 TLS 1.0, TLS 1.1 및 TLS 1.2 를 지원합니다. 다른 SSL 버전은 이 스위치와 호환되지 않을 수 있으며, 인증 및 클라이언트와 서버 간 메시지 전송에 문제가 발생할 수 있습니다.

SSL 기능을 활성화하면 웹은 비활성화됩니다. SSL 기능을 사용하면서 웹 기반 관리로 스위치를 관리하려면 웹 브라우저가 SSL 암호화를 지원하고 URL 의 헤더가 https://(예: https://xx.xx.xx.xx)로 시작해야 합니다. 다른 방법으로 접속하면 오류가 발생하고 웹 기반 관리 접근이 허용되지 않습니다.

사용자는 TFTP 서버에서 SSL 기능을 위한 인증서 파일을 스위치에 다운로드할 수 있습니다. 인증서 파일은 네트워크의 장치를 인증하는 데 사용되는 데이터 기록으로, 소유자 정보와 인증 및 디지털 서명 키가 포함되어 있습니다. 최적의 SSL 기능을 위해 서버와 클라이언트는 일관된 인증서 파일을 가져야 합니다. 현재 스위치는 사전 로드된 인증서를 포함하고 있지만, 사용자는 상황에 따라 더 많은 인증서를 다운로드해야 할 수 있습니다.

SSL Global Settings

이 창은 전역 SSL 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > SSL > SSL Global Settings 을 클릭하십시오.

그림 9-74) SSL Global Settings 창

SSL Global Settings 에서 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
SSL Status	여기에서 전역 SSL 상태를 활성화하거나 비활성화하려면 선택합니다.
Service Policy	여기에 서비스 정책 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Import File 에서 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
File Select	여기에 로드할 파일 형식을 선택합니다. 선택할 수 있는 옵션은 인증서와 개인 키입니다. 파일 형식을 선택한 후 Browse 버튼을 눌러 로컬 컴퓨터에 있는 해당 파일로 이동합니다.
Destination File Name	여기에 사용된 대상 파일 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

SSL-Self-signed Certificate 섹션에서 Generate 버튼을 클릭하여 기본 제공 자체 서명 인증서가 있는지 여부에 관계없이 새 자체 서명 인증서를 생성합니다. 생성된 인증서는 사용자가 다운로드한 인증서에 영향을 주지 않습니다.

참고: SSL 자체 서명 인증서는 키 길이가 2048 비트인 자체 서명 RSA 인증서만 지원합니다.

Crypto PKI Trustpoint

이 창은 Crypto PKI Trustpoint 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > SSL > Crypto PKI Trustpoint 를 클릭합니다.

그림 9-75) Crypto PKI Trustpoint 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Trustpoint	가져온 인증서 및 키 쌍과 연결된 신뢰 지점의 이름을 여기에 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
File System Path	여기에 인증서 및 키 쌍의 파일 시스템 경로를 입력합니다.
Password	개인 키를 여기에서 가져올 때 암호화를 실행 취소하는 데 사용되는 암호화된 암호 구문을 입력합니다. 암호 구문은 최대 64 자의 문자열입니다. 암호 구문을 지정하지 않으면 NULL 문자열이 사용됩니다.
TFTP Server Path	여기에 TFTP 서버 경로를 입력합니다.
Type	여기에서 가져올 인증서 유형을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Both - CA 인증서, 로컬 인증서 및 키 쌍을 가져오도록 지정합니다. • CA - CA 인증서만 가져오도록 지정합니다. • Local - 로컬 인증서와 키 쌍만 가져오도록 지정합니다.
Primary	Primary 확인란을 선택하여 기본 신뢰 지점(여러 항목이 있는 경우)을 지정합니다. 확인란을 선택하면 '성공' 확인 창이 나타납니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

SSL Service Policy

이 창은 SSL Service Policy 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > SSL > SSL Service Policy 을 클릭합니다.

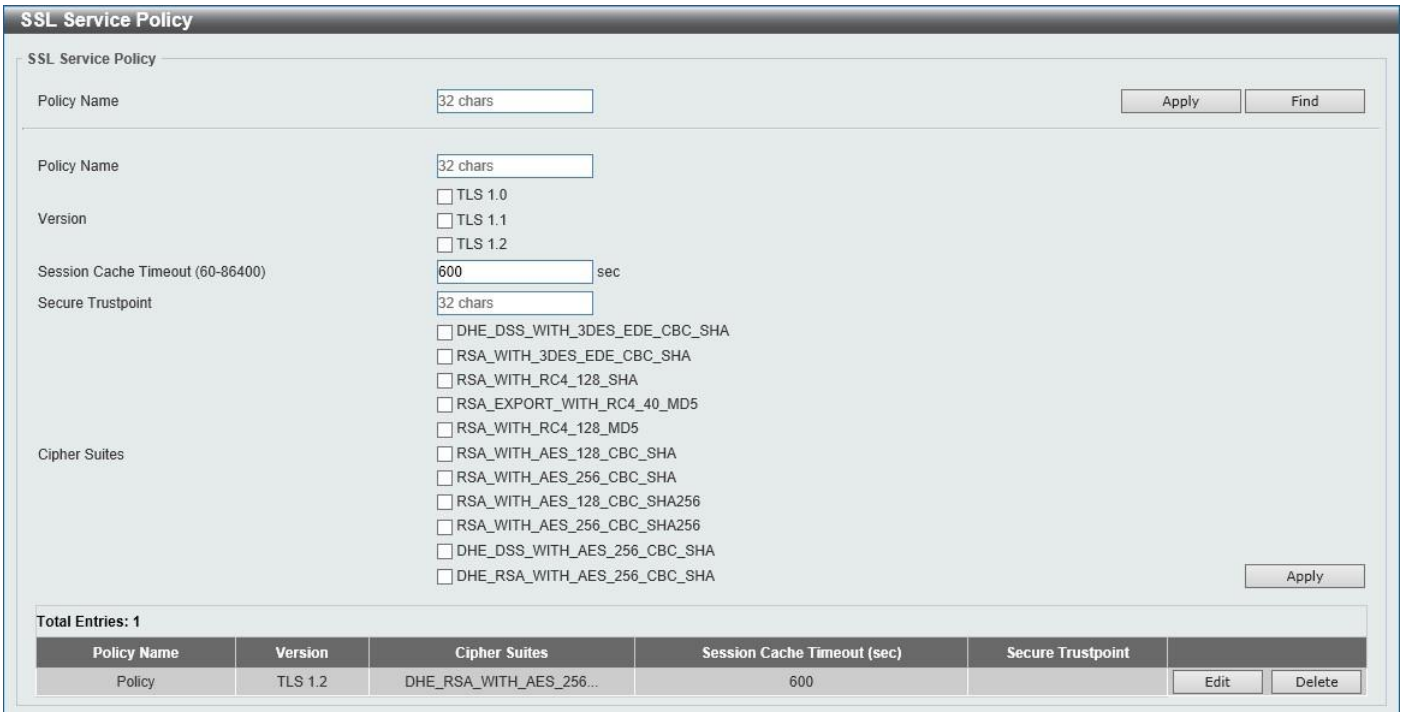

그림 9-76) SSL 서비스 정책 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Policy Name	여기에 SSL 서비스 정책 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Version	여기에서 TLS(전송 계층 보안) 버전을 선택합니다. 선택할 수 있는 옵션은 TLS 1.0, TLS 1.1 및 TLS 1.2 입니다.
Session Cache Timeout	여기에 사용된 세션 캐시 시간 제한 값을 입력합니다. 이 값은 60 초에서 86400 초 사이여야 합니다. 기본적으로 이 값은 600 초입니다.
Secure Trustpoint	여기에 보안 신뢰 지점 이름을 입력합니다. 이 이름은 최대 32 자까지 가능합니다.
Cipher Suites	여기에서 이 프로필과 연결할 암호 그룹을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Find 버튼을 클릭하여 입력한 정보에 따라 특정 항목을 찾습니다.

Edit 버튼을 클릭하여 특정 항목을 다시 구성합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Network Protocol Port Protect Settings

이 창은 Network Protocol Port Protect Settings 을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Security > Network Protocol Port Protect Settings 을 클릭합니다.

그림 9-77) 네트워크 프로토콜 포트 보호 설정 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
TCP Port Protect State	여기에서 TCP 포트 네트워크 프로토콜 보호 기능을 활성화 또는 비활성화하려면 선택합니다.
UDP Port Protect State	여기에서 UDP 포트 네트워크 프로토콜 보호 기능을 활성화 또는 비활성화하려면 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

9. OAM

Cable Diagnostics

Cable Diagnostics

케이블 진단 기능은 주로 관리자 또는 고객 서비스 담당자가 구리 케이블을 확인하고 테스트할 수 있도록 설계되었습니다. 케이블의 품질과 오류 유형을 신속하게 확인할 수 있습니다.

다음 창을 보려면 아래와 같이 OAM > Cable Diagnostics 를 클릭합니다.

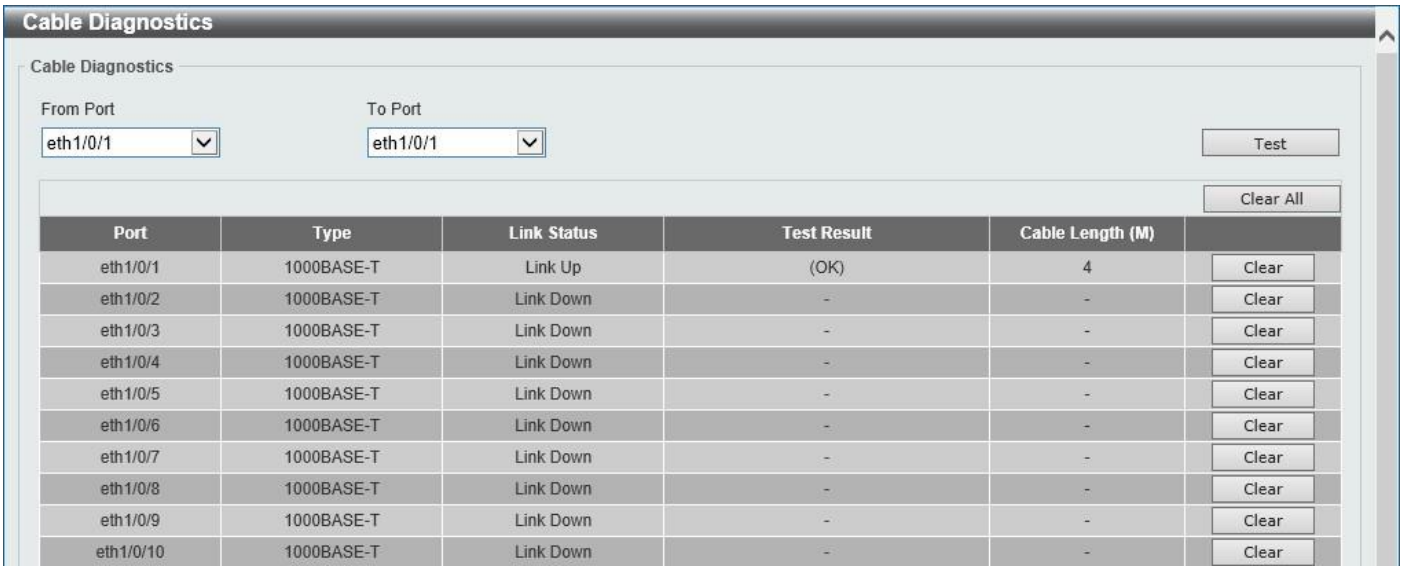

그림 10-1 케이블 진단 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.

Test 버튼을 클릭하여 특정 포트를 테스트합니다.

Clear 버튼을 클릭하여 특정 포트에 대한 모든 정보를 지웁니다.

Clear All 버튼을 클릭하여 이 테이블의 모든 정보를 지웁니다.

알림: 이 테스트의 경우 지원되는 케이블 길이는 10 미터에서 130 미터이고 와이어 속도는 100/1000Mbps 입니다. 10Mbps 테스트는 지원되지 않습니다.

참고: 100/1000Mbps 포트에서 케이블 길이 감지의 거리 편차는 다음과 같습니다.

- 40 미터 이하의 케이블에는 25 미터를 ±.
- 40 미터에서 100 미터 사이의 케이블에서 20 미터를 ±.

참고: 링크 다운 감지의 거리 편차는 다음과 같습니다.

- ± 30 미터 이하의 케이블에는 15 미터가 있습니다.
- 30 미터에서 110 미터 사이의 케이블에서 7 미터를 ±합니다.
- 110 미터에서 130 미터 사이의 케이블에서 ± 15 미터.

참고: 보다 정확한 테스트 결과를 얻으려면 RJ45 커넥터에서 TIA/EIA-568B 핀 할당을 사용하십시오.

오류 메시지:

- Open - 이 쌍은 연결되지 않았습니다.
- Short - 이 쌍의 두 선이 쇼트되었습니다.

- CrossTalk - 이 쌍의 선이 다른 쌍의 선과 쇼트되었습니다.
- Unknown - 진단이 케이블 상태를 확인하지 못했습니다. 다시 시도해 주세요.
- NA - 케이블이 발견되지 않았습니다. 진단 사양을 벗어났거나 케이블 품질이 너무 나쁠 수 있습니다.

10. Monitoring

Utilization
Statistics
Mirror Settings
Device Environment

Utilization

Port Utilization

이 창은 포트 사용률 테이블을 보는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Monitoring > Utilization > Port Utilization 을 클릭합니다.

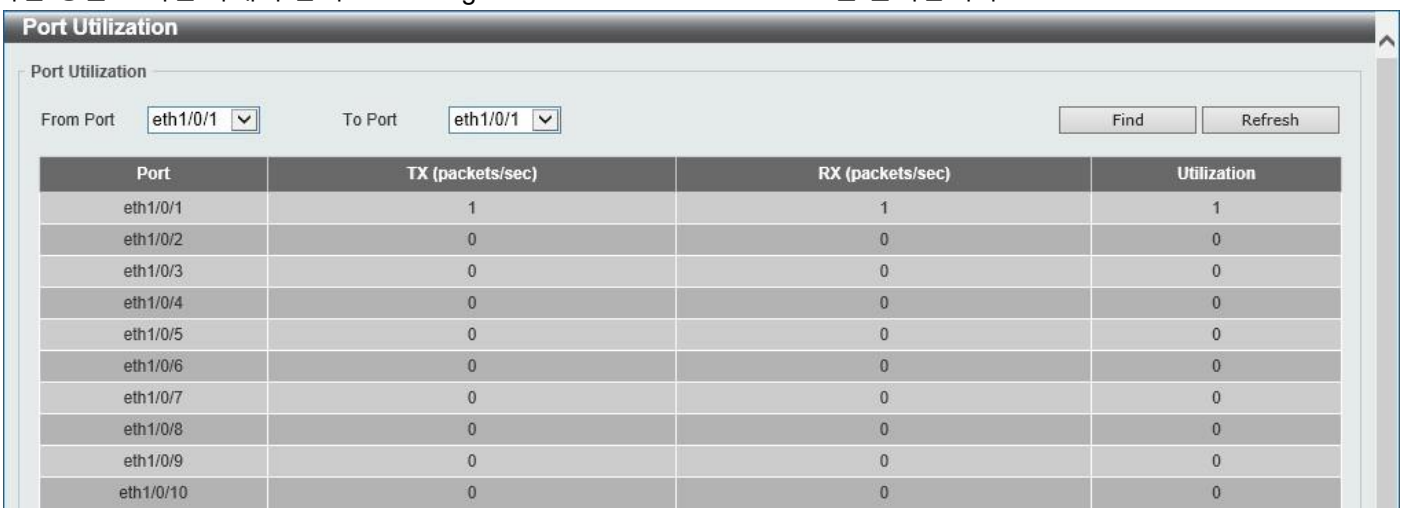

그림 11-1 Port Utilization 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 사용할 포트 범위를 선택합니다.

Find 버튼을 클릭하여 입력/선택한 정보에 따라 테이블의 항목을 표시합니다.

Refresh 버튼을 눌러 테이블에 표시된 정보를 새로 고칩니다.

Statistics

Port

이 창은 포트 통계 정보를 보는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Monitoring > Statistics > Port 를 클릭합니다.

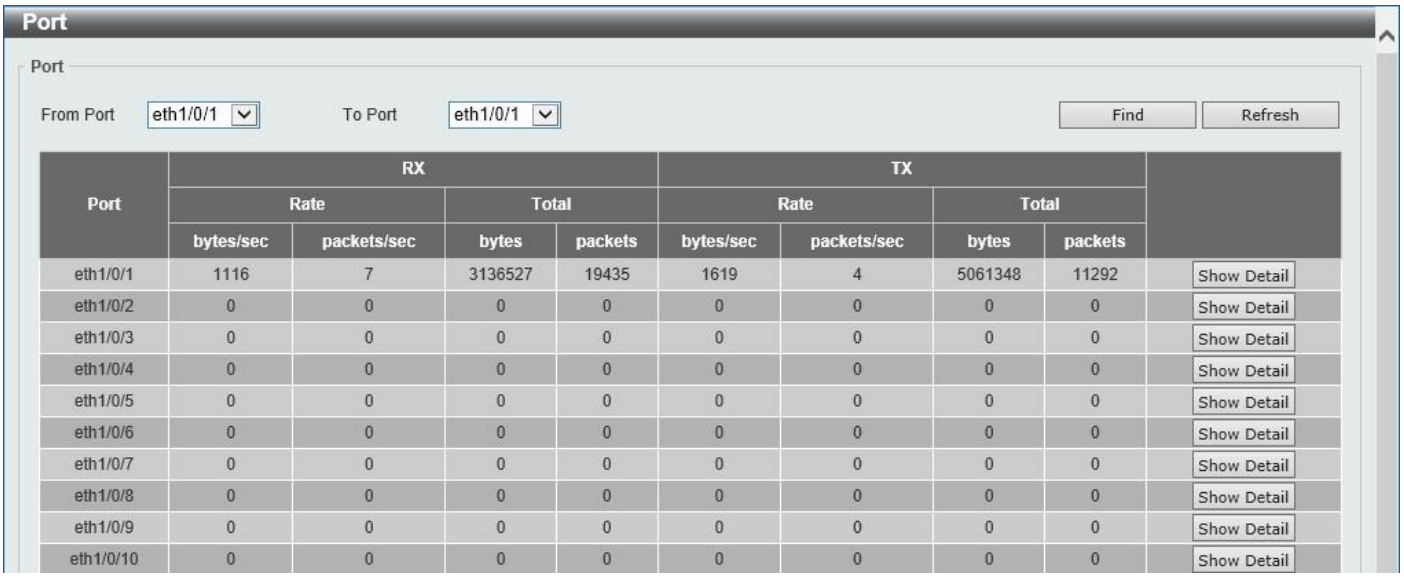

그림 11-2 포트 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 이 디스플레이에 사용할 포트 범위를 선택합니다.

Find 버튼을 클릭하여 선택한 정보에 따라 테이블의 항목을 표시합니다.

Refresh 버튼을 눌러 테이블에 표시된 정보를 새로 고칩니다.

Show Detail 버튼을 클릭하면 지정된 포트에 대한 자세한 통계 정보를 볼 수 있습니다.

Show Detail 버튼을 클릭하면 다음 창이 나타납니다.

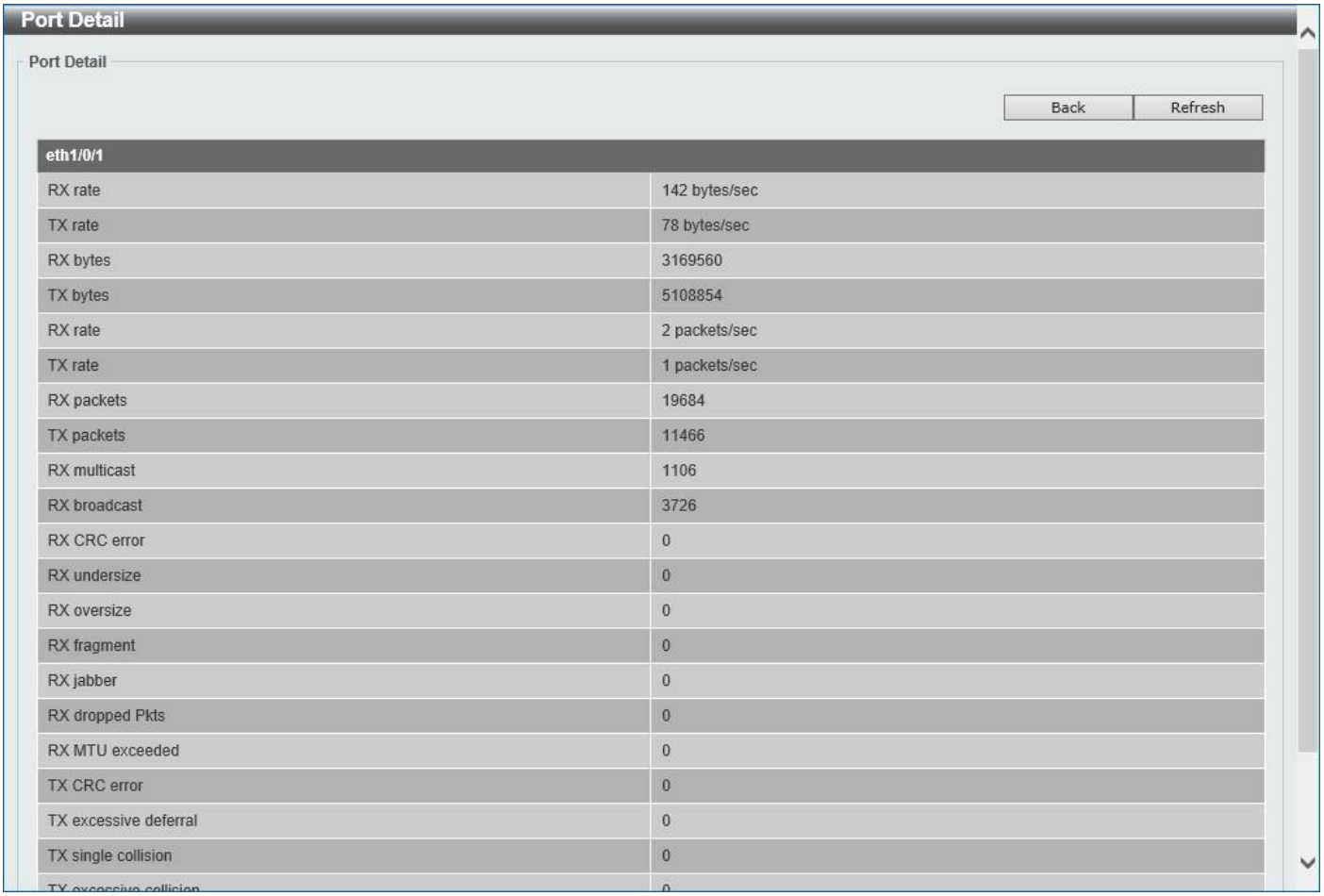

그림 11-3 Port(Show Detail) 창

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

Refresh 버튼을 눌러 테이블에 표시된 정보를 새로 고칩니다.

Interface Counters

이 창은 Interface Counters 정보를 보는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Monitoring > Statistics > Interface Counters 를 클릭합니다.

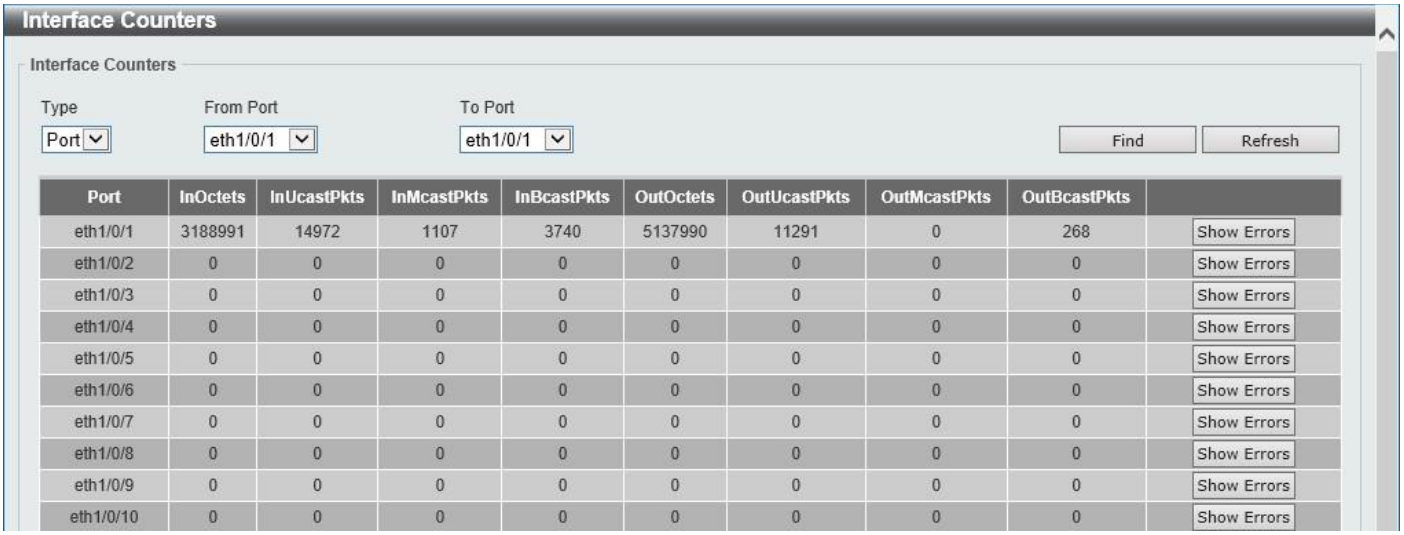

그림 11-4) Interface 카운터(포트) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Type	유형이 Port 임을 지정합니다.
From Port - To Port	여기에서 이 디스플레이에 사용할 포트 범위를 선택합니다.

Find 버튼을 클릭하여 선택한 정보에 따라 테이블의 항목을 표시합니다.

Refresh 버튼을 눌러 테이블에 표시된 정보를 새로 고칩니다.

Show Errors 버튼을 클릭하여 지정된 포트에 대한 자세한 오류 정보를 확인합니다.

Show Errors 버튼을 클릭하면 다음 창이 나타납니다.

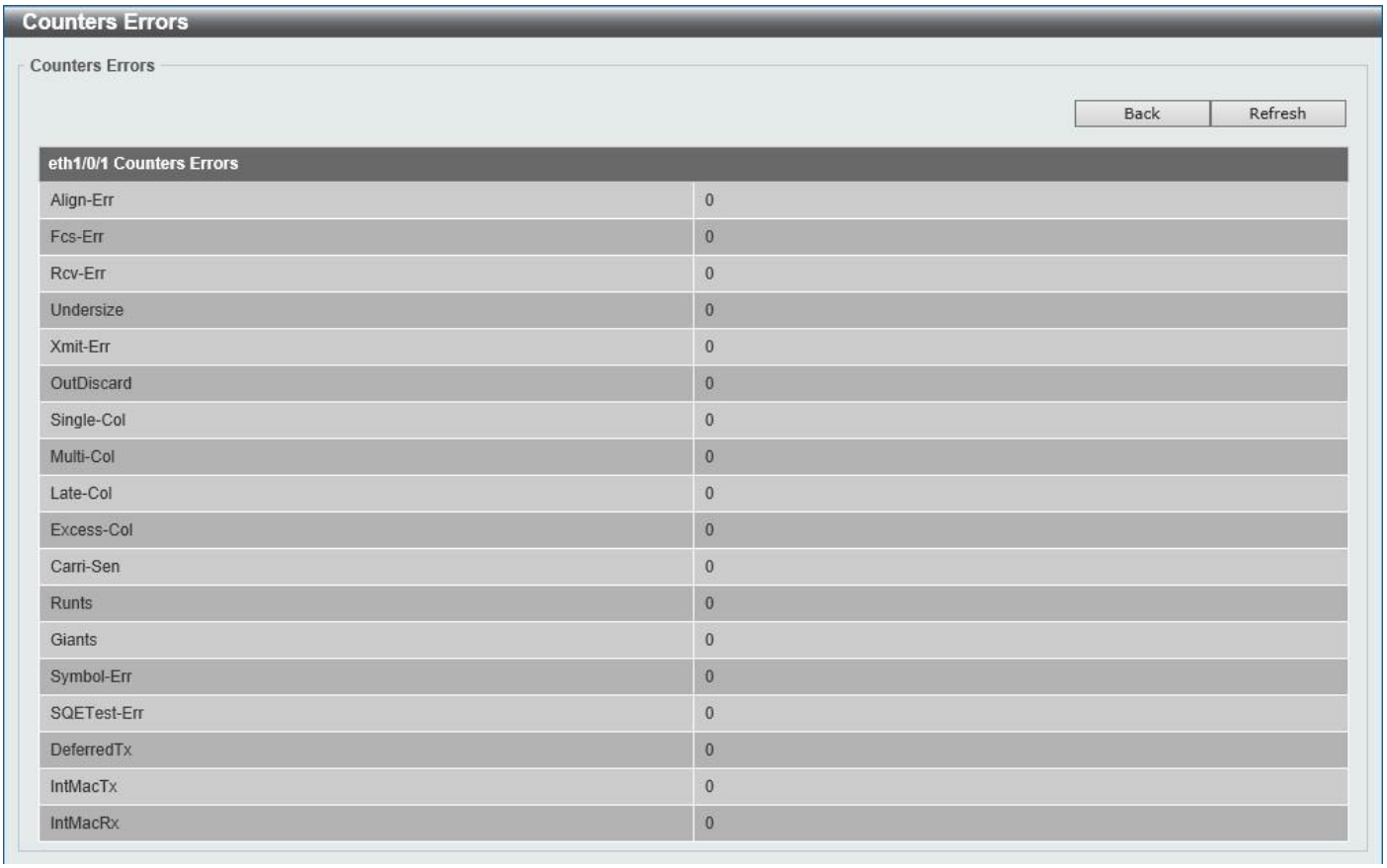

그림 11-5 Interface 카운터(오류 표시) 창

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

Refresh 버튼을 눌러 테이블에 표시된 정보를 새로 고칩니다.

Counters

이 창은 Counters 정보를 보고 지우는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Monitoring > Statistics > Counters 를 클릭합니다.

그림 11-6 카운터(포트) 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Type	유형이 Port 임을 지정합니다.

From Port - To Port	여기에서 이 디스플레이에 사용할 포트 범위를 선택합니다.

Find 버튼을 클릭하여 선택한 정보에 따라 테이블의 항목을 표시합니다.

Refresh 버튼을 클릭하여 테이블에 표시된 카운터 정보를 새로 고칩니다.

Clear 버튼을 클릭하면 선택한 정보에 따라 테이블에 표시된 카운터 정보가 지워집니다.

Clear All 버튼을 클릭하여 테이블에 표시된 모든 카운터 정보를 지웁니다.

Show Detail 버튼을 클릭하여 지정된 포트에 대한 자세한 카운터 정보를 확인합니다.

Show Detail 버튼을 클릭하면 다음 창이 나타납니다.

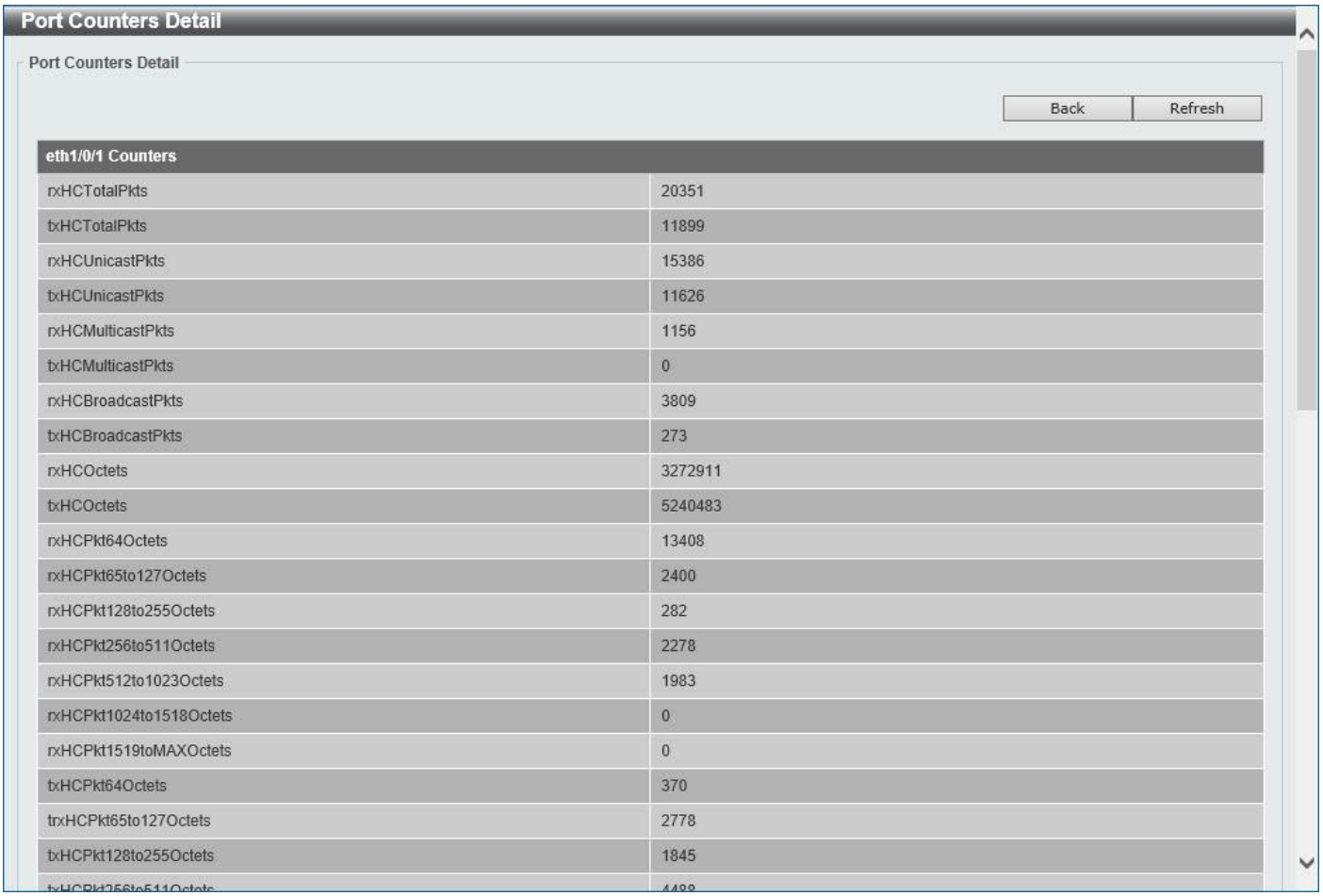

그림 11-7 카운터(세부 정보 표시) 창

Back 버튼을 클릭하여 이전 창으로 돌아갑니다.

Refresh 버튼을 눌러 테이블에 표시된 정보를 새로 고칩니다.

Mirror Settings

이 창은 미러링 기능의 설정을 표시하고 구성하는 데 사용됩니다. 스위치는 특정 포트에서 전송 및 수신되는 프레임을 복사하여 다른 포트로 리디렉션할 수 있습니다. 미러링 포트에 스니퍼 또는 RMON 프로브와 같은 모니터링 장치를 연결하여 첫 번째 포트를 통과하는 패킷의 세부 정보를 확인할 수 있습니다. 이는 네트워크 모니터링 및 문제 해결에 유용합니다.

다음 창을 보려면 아래와 같이 Monitoring > Mirror Settings 을 클릭합니다.

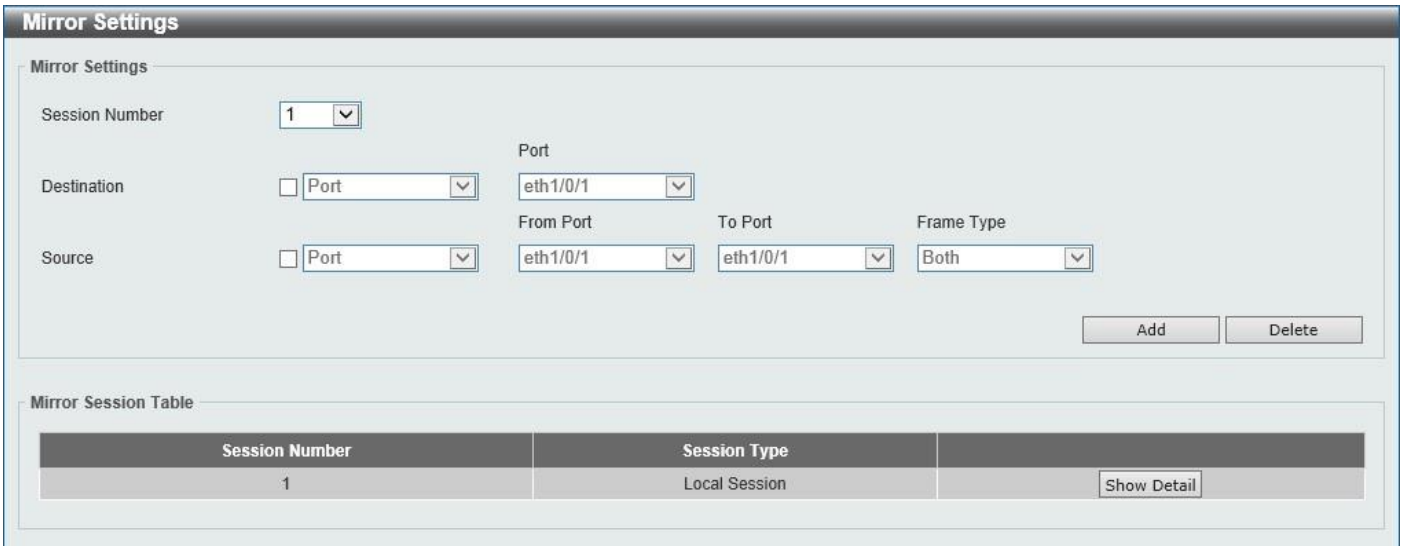

그림 11-8 미러 설정 창

미러 설정에 대해 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Session Number	여기에서 이 항목에 대한 미러 세션 번호를 선택합니다.
Destination	확인란을 선택하고 여기에서 대상 포트 번호를 선택합니다.
Source	확인란을 선택하고 이 포트 미러 항목의 소스를 선택합니다. 첫 번째 드롭다운 메뉴에서 소스 유형 옵션을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Port - 이 옵션을 선택한 후 드롭다운 메뉴에서 From Port 및 To Port 번호를 선택합니다. 마지막으로 마지막 드롭다운 메뉴에서 프레임 유형 옵션을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. ○ Both - 들어오는 방향과 나가는 방향 모두의 트래픽이 미러링되도록 지정합니다. ○ RX - 들어오는 방향의 트래픽만 미러링되도록 지정합니다. ○ TX - 나가는 방향의 트래픽만 미러링되도록 지정합니다.

Add 버튼을 클릭하여 입력한 정보에 따라 새로 구성된 미러 항목을 추가합니다.

Delete 버튼을 클릭하여 입력한 정보에 따라 기존 미러 항목을 삭제합니다.

Show Detail 버튼을 클릭하여 미러 세션에 대한 자세한 정보를 봅니다.

Show Detail 버튼을 클릭하면 다음 창이 나타납니다.

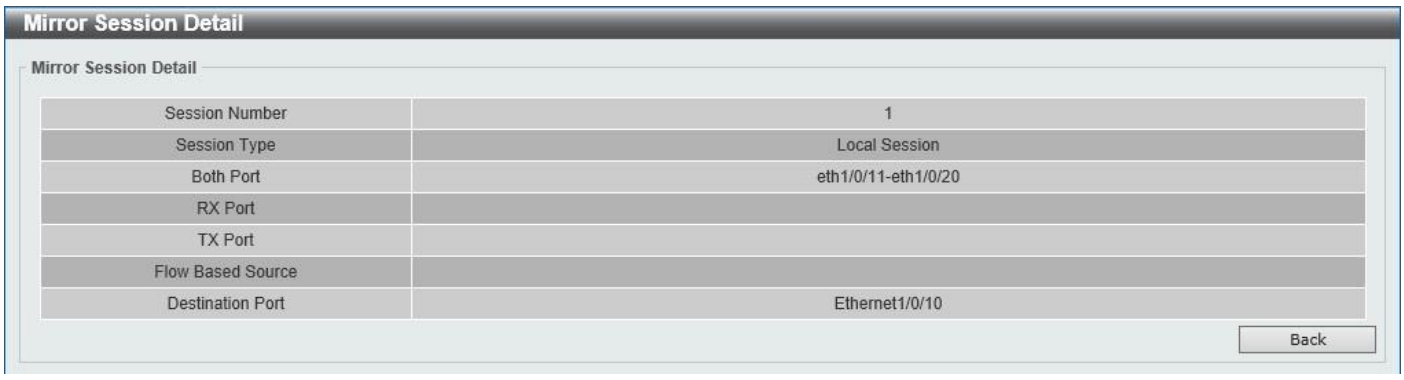

그림 11-9 미러 설정(세부 정보 표시) 창

Back 버튼을 클릭하여 이전 페이지로 돌아갑니다.

Device Environment

장치 환경 기능은 스위치 내부 온도 상태를 표시합니다.

다음 창을 보려면 아래와 같이 Monitoring > Device Environment 를 클릭합니다.

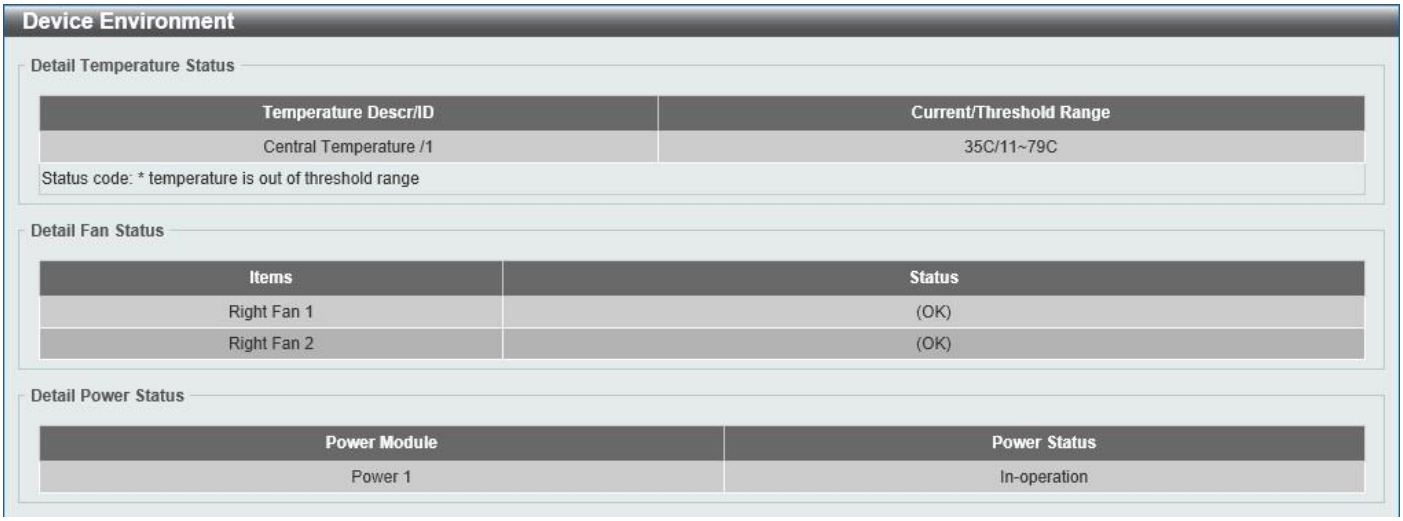

그림 11-10) 장치 환경 창

11. Green

Power Saving
EEE

Power Saving

이 창은 스위치의 절전 설정을 표시하고 구성하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Green > Power Saving 을 클릭합니다.

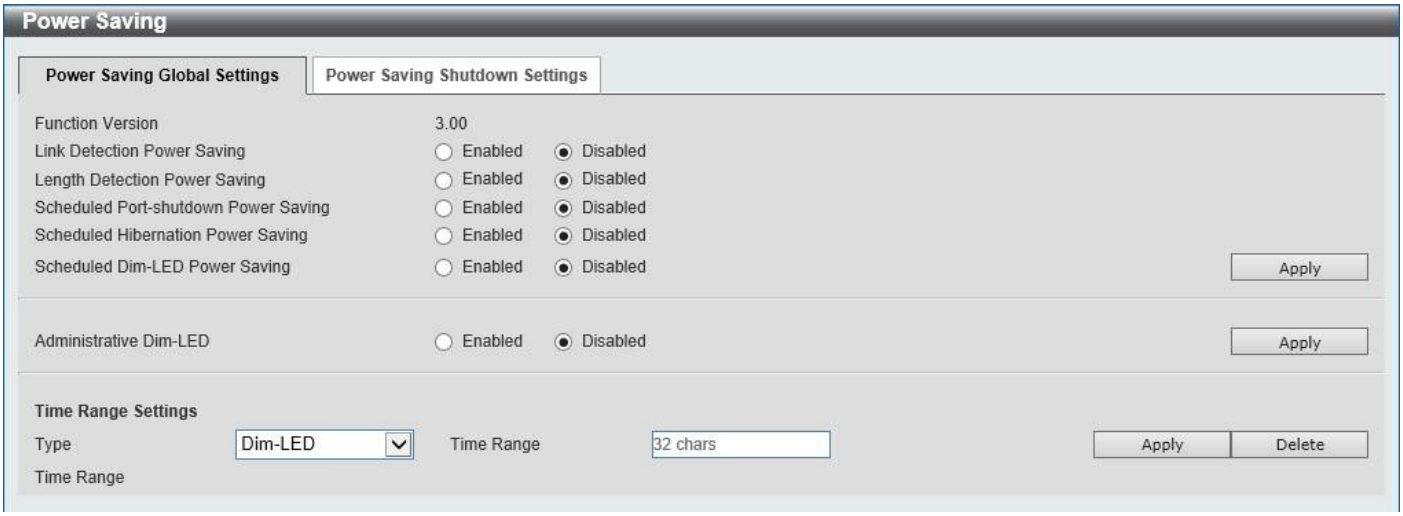

그림 12-1 Power Saving Global Settings 창

Power Saving Global Settings 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Link Detection Power Saving	여기에서 링크 감지 절전 기능을 활성화하거나 비활성화하려면 선택합니다. 활성화하면 링크 다운 상태의 포트가 꺼져 스위치의 전원을 절약합니다. 이는 포트 상태가 link up 일 때 포트의 기능에 영향을 주지 않습니다.

Length Detection Power Saving	여기에서 케이블 길이 감지 절전 기능을 활성화하거나 비활성화하려면 선택합니다. 이 기능을 사용하면 스위치가 포트에 연결된 케이블 길이를 자동으로 감지하고 그에 따라 이 포트에 필요한 전력을 늘리거나 줄여 전원을 절약할 수 있습니다.
Scheduled Port-shutdown Power Saving	여기에서 예약된 포트 종료 절전 기능을 활성화하거나 비활성화하려면 선택합니다.
Scheduled Hibernation Power Saving	여기에서 예약된 최대 절전 기능을 활성화하거나 비활성화하려면 선택합니다.
Scheduled Dim-LED Power Saving	여기에서 전원 기능을 절약하기 위해 LED 의 예약된 디밍을 활성화하거나 비활성화하려면 선택합니다.
Administrative Dim-LED	포트 LED 기능을 활성화하거나 비활성화하려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

시간 범위 설정에서 구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Type	여기에서 절전 유형을 선택하십시오. 선택할 수 있는 옵션은 다음과 같습니다. • Dim-LED -희미한 LED 일정에 대한 시간 범위 프로필을 추가하거나 삭제하도록 지정합니다. 일정이 끝나면 모든 포트 LED 가 꺼집니다. • Hibernation -시스템 최대 절전 모드 일정에 대한 시간 범위 프로필을 추가하거나 삭제하도록 지정합니다. 시스템이 최대 절전 모드에 들어가면 스위치는 저전력 상태로 전환되고 유휴 상태가 됩니다. 모든 포트와 LED 가 종료되고 모든 네트워크 기능이 비활성화되며 콘솔 연결만 RS232 포트를 통해 작동합니다. 스위치가 엔드포인트 PSE 인 경우 포트를 통해 전원이 제공되지 않습니다.
Time Range	절전 유형과 연결할 시간 범위의 이름을 입력합니다.

Apply 버튼을 클릭하여 각 개별 섹션에 대한 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

Power Saving Shutdown Settings 탭을 클릭하면 다음 페이지가 나타납니다.

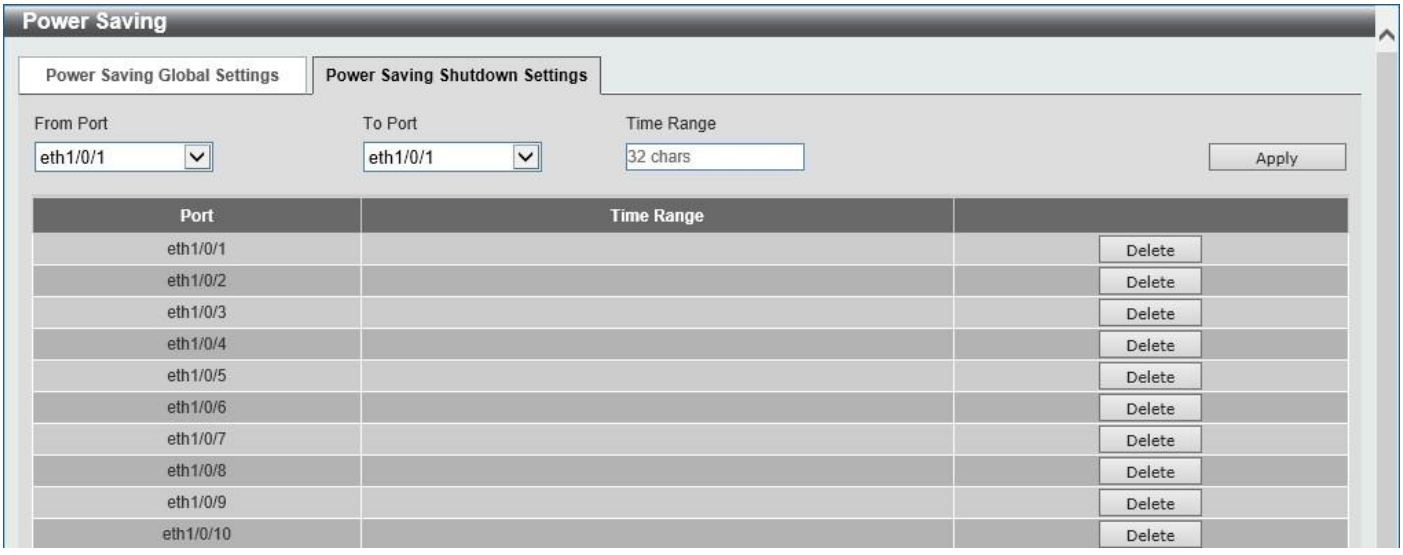

그림 12-2 Power Saving Shutdown Settings 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description

From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
시간 Time Range	포트와 연결할 시간 범위의 이름을 입력합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

Delete 버튼을 클릭하여 지정된 항목을 제거합니다.

EEE

EEE(Energy Efficient Ethernet)는 IEEE 802.3az 에 정의되어 있습니다. 패킷이 전송되지 않을 때 링크의 에너지 소비를 줄이도록 설계되었습니다.

다음 창을 보려면 아래와 같이 Green > EEE 를 클릭합니다.

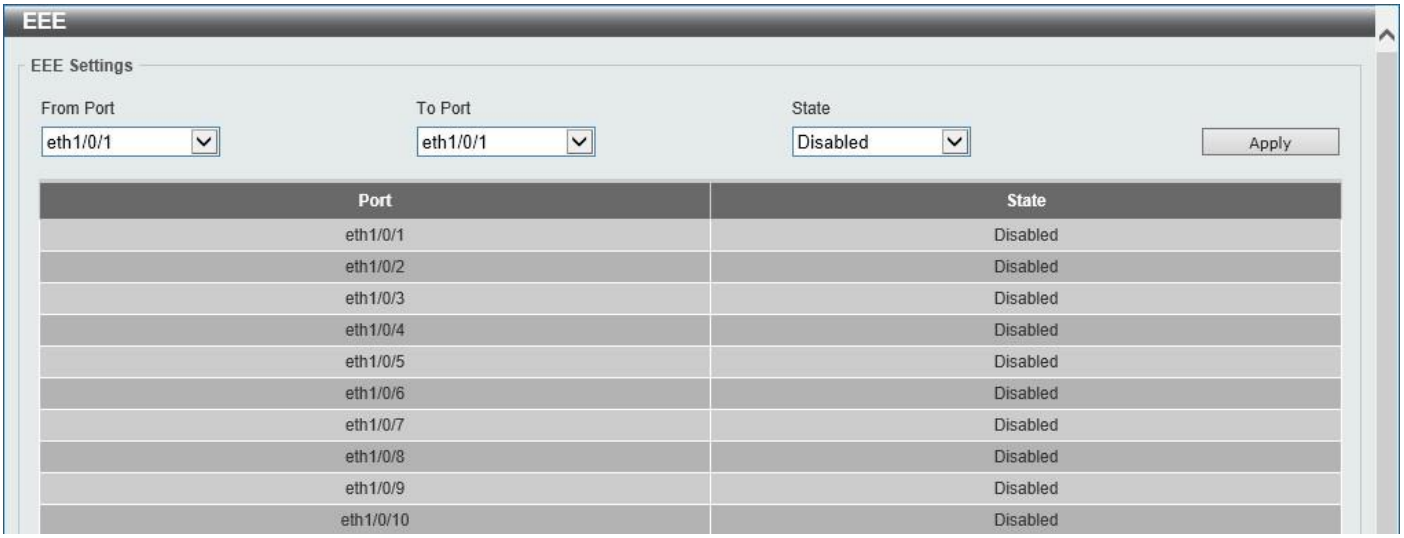

그림 12-3 EEE 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
From Port - To Port	여기에서 컨피그레이션에 사용되는 적절한 포트 범위를 선택합니다.
State	여기에서 이 기능의 상태를 활성화하거나 비활성화하려면 이 옵션을 선택합니다.

Apply 버튼을 클릭하여 변경 사항을 적용합니다.

12. Toolbar

Save
Tools
Wizard
Online Help
Surveillance Mode
Logout

Save

Save Configuration

이 창은 실행 중인 구성을 시작 구성에 저장하는 데 사용됩니다. 이는 전원 장애 시 구성이 손실되는 것을 방지하기 위한 것입니다.

다음 창을 보려면 아래와 같이 Save > Save Configuration 을 클릭합니다.

그림 13-1 Save Configuration 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
File Path	여기에서 구성을 저장할 대상을 선택합니다. 선택할 수 있는 옵션은 startup-config, Configuration 1 및 Configuration 2 입니다.

Apply 버튼을 클릭하여 구성을 저장합니다.

Tools

Firmware Upgrade & Backup

Firmware Upgrade from HTTP

이 창은 HTTP 를 사용하여 로컬 PC 에서 펌웨어 업그레이드를 시작하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP 를 클릭하십시오.

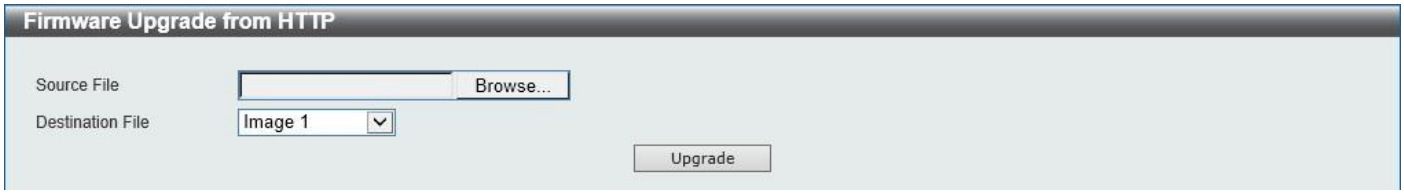

그림 13-2 HTTP 창에서 펌웨어 업그레이드

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Source File	Browse 버튼을 클릭하고 여기에서 로컬 PC 의 펌웨어 파일로 이동합니다. 이 파일은 스위치에 업로드됩니다.
Destination File	여기에서 스위치에서 펌웨어 파일을 저장할 대상을 선택하십시오. 선택할 수 있는 옵션은 Image 1 과 Image 2 입니다.

Upgrade 버튼을 클릭하여 펌웨어 업그레이드를 시작합니다.

Firmware Upgrade from TFTP

이 창은 TFTP 서버에서 펌웨어 업그레이드를 시작하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Tools > Firmware Upgrade & Backup > Firmware Upgrade from TFTP 를 클릭합니다.

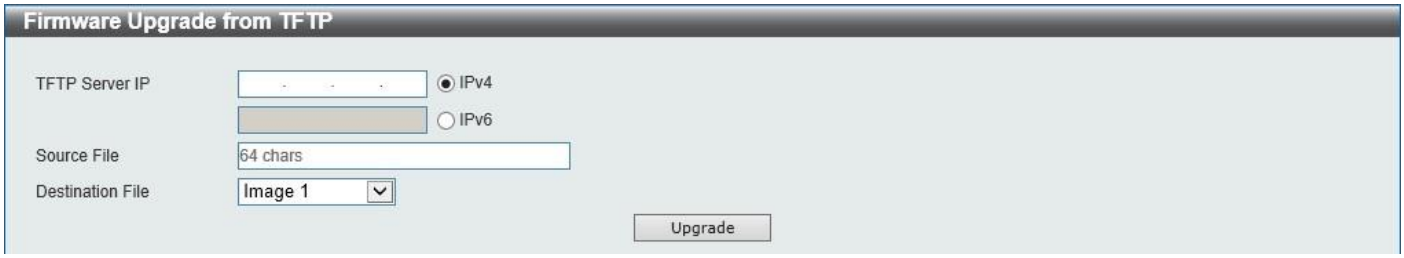

그림 13-3 TFTP 창에서 펌웨어 업그레이드

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description

TFTP Server IP	여기에 TFTP 서버의 IP Address 를 선택하여 입력합니다. • IPv4 - TFTP 서버의 IPv4 주소를 선택하고 입력하도록 지정합니다. • IPv6 - TFTP 서버의 IPv6 주소를 선택하고 입력하도록 지정합니다.
Source File	여기에 TFTP 서버에 있는 펌웨어 파일의 파일 이름과 경로를 입력합니다. 이것은 스위치에 업로드됩니다. 이 필드는 최대 64 자까지 입력할 수 있습니다.
Destination File	여기에서 스위치에서 펌웨어 파일을 저장할 대상을 선택하십시오. 선택할 수 있는 옵션은 Image 1 과 Image 2 입니다.

Upgrade 버튼을 클릭하여 펌웨어 업그레이드를 시작합니다.

Firmware Backup to HTTP

이 창은 HTTP 를 사용하여 로컬 PC 에 펌웨어 백업을 시작하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP 를 클릭하십시오.

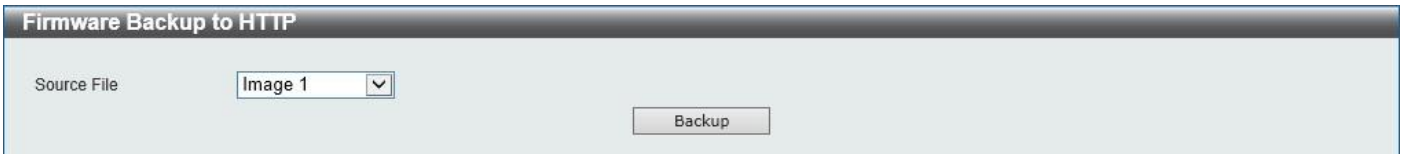

그림 13-4 HTTP 창에 펌웨어 백업

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Source File	여기에서 로컬 PC 에 백업할 스위치의 펌웨어를 선택합니다. 선택할 수 있는 옵션은 Image 1 과 Image 2 입니다.

Backup 버튼을 클릭하여 펌웨어 백업을 시작합니다.

Firmware Backup to TFTP

이 창은 TFTP 서버에 대한 펌웨어 백업을 시작하는 데 사용됩니다.

다음 창을 보려면 아래와 Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP 를 클릭합니다.

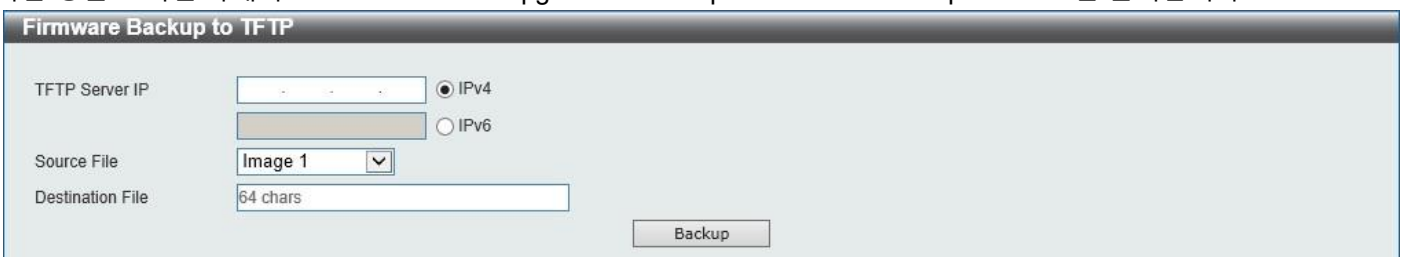

그림 13-5 TFTP 창에 펌웨어 백업

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
TFTP Server IP	여기에 TFTP 서버의 IP Address 를 선택하여 입력합니다. • IPv4 - TFTP 서버의 IPv4 주소를 선택하고 입력하도록 지정합니다. • IPv6 - TFTP 서버의 IPv6 주소를 선택하고 입력하도록 지정합니다.
Source File	여기에서 TFTP 서버에 백업할 스위치의 펌웨어 파일을 선택합니다. 선택할 수 있는 옵션은 Image 1 과 Image 2 입니다.
Destination File	TFTP 서버에 저장할 펌웨어 파일의 파일 이름과 경로를 여기에 입력합니다. 이 필드는 최대 64 자까지 입력할 수 있습니다.

Backup 버튼을 클릭하여 펌웨어 백업을 시작합니다.

Configuration Restore & Backup

Configuration Restore from HTTP

이 창은 HTTP 를 사용하여 로컬 PC 에서 구성 복원을 시작하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Tools > Configuration Restore & Backup > Configuration Restore from HTTP 를 클릭하십시오.

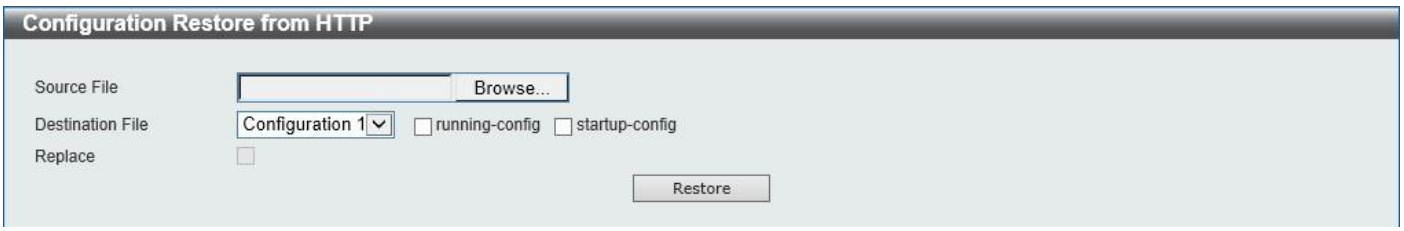

그림 13-6) HTTP 창에서 구성 복원

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Source File	Browse(찾아보기) 버튼을 클릭하고 여기에서 로컬 PC 의 구성 파일로 이동합니다. 이 파일은 스위치에 업로드됩니다.
Destination File	여기에서 스위치의 컨피그레이션 파일의 대상을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Configuration 1 - 구성 1 을 대상으로 사용하려면 이 옵션을 선택합니다. • Configuration 2 - 구성 2 를 대상으로 사용하려면 이 옵션을 선택합니다. • running-config - 실행 중인 구성을 대상으로 사용하려면 이 옵션을 선택합니다. • startup-config - 시작 구성을 대상으로 사용하려면 이 옵션을 선택합니다.
Replace	스위치에서 실행 중인 컨피그레이션을 이 컨피그레이션으로 바꾸려면 이 옵션을 선택합니다.

Restore 버튼을 클릭하여 구성 복원을 시작합니다.

Configuration Restore from TFTP

이 창은 TFTP 서버에서 컨피그레이션 복원을 시작하는 데 사용됩니다.

다음 창을 보려면 아래와 Tools > Configuration Restore & Backup > Configuration Restore from TFTP 를 클릭합니다.

그림 13-7 TFTP 창에서 구성 복원

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description

TFTP Server IP	여기에 TFTP 서버의 IP Address 를 선택하여 입력합니다. • IPv4 - TFTP 서버의 IPv4 주소를 선택하고 입력하도록 지정합니다. • IPv6 - TFTP 서버의 IPv6 주소를 선택하고 입력하도록 지정합니다.
Source File	여기에 TFTP 서버에 있는 컨피그레이션 파일의 파일 이름과 경로를 입력합니다. 이것은 스위치에 업로드됩니다. 이 필드는 최대 64 자까지 입력할 수 있습니다.
Destination File	여기에서 스위치의 컨피그레이션 파일의 대상을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Configuration 1 - 구성 1 을 대상으로 사용하려면 이 옵션을 선택합니다. • Configuration 2 - 구성 2 를 대상으로 사용하려면 이 옵션을 선택합니다. • running-config - 실행 중인 구성을 대상으로 사용하려면 이 옵션을 선택합니다. • startup-config - 시작 구성을 대상으로 사용하려면 이 옵션을 선택합니다.
Replace	스위치에서 실행 중인 컨피그레이션을 이 컨피그레이션으로 바꾸려면 이 옵션을 선택합니다.

Restore 버튼을 클릭하여 구성 복원을 시작합니다.

Configuration Backup to HTTP

이 창은 HTTP 를 사용하여 로컬 PC 에 구성 파일 백업을 시작하는 데 사용됩니다.

다음 창을 보려면 아래와 Tools > Configuration Restore & Backup > Configuration Backup to HTTP 를 클릭하십시오.

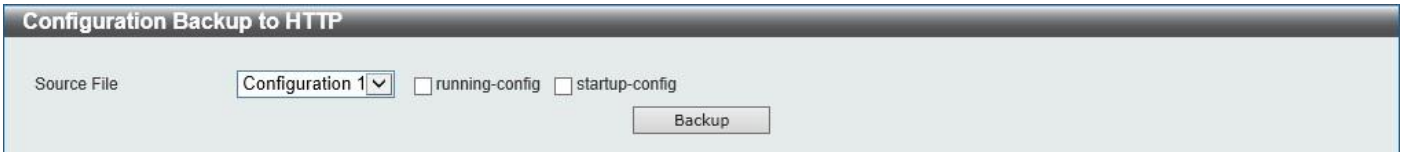

그림 13-8) HTTP 창에 구성 백업

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Source File	여기에서 로컬 PC 에 백업할 스위치의 구성을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Configuration 1 - 구성 1 을 백업하려면 이 옵션을 선택합니다. • Configuration 2 - 구성 2 를 백업하려면 이 옵션을 선택합니다. • running-config - 실행 중인 컨피그레이션을 백업하려면 이 옵션을 선택합니다. • startup-config - 시작 구성을 백업하려면 이 옵션을 선택합니다.

Backup 버튼을 클릭하여 구성 파일 백업을 시작합니다.

Configuration Backup to TFTP

이 창은 TFTP 서버에 대한 컨피그레이션 파일 백업을 시작하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Tools > Configuration Restore & Backup > Configuration Backup to TFTP 를 클릭합니다.

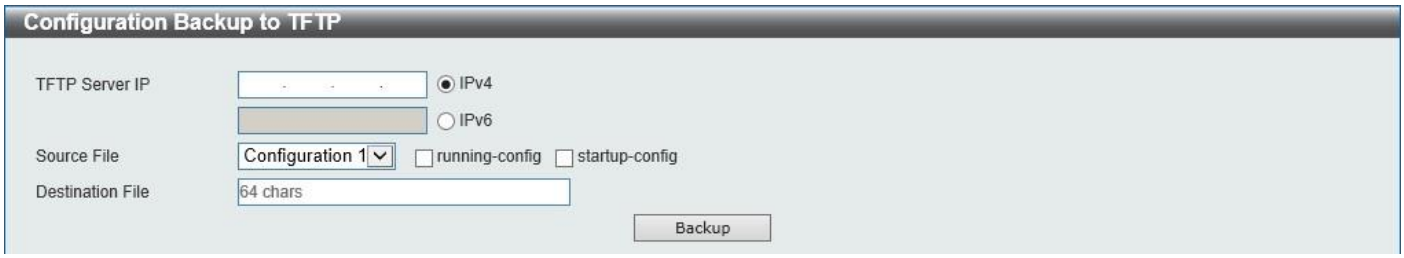

그림 13-9) TFTP 창에 구성 백업

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
TFTP Server IP	여기에 TFTP 서버의 IP Address 를 선택하여 입력합니다. • IPv4 - TFTP 서버의 IPv4 주소를 선택하고 입력하도록 지정합니다. • IPv6 - TFTP 서버의 IPv6 주소를 선택하고 입력하도록 지정합니다.
Source File	여기에서 TFTP 서버에 백업할 스위치의 컨피그레이션을 선택합니다. 선택할 수 있는 옵션은 다음과 같습니다. • Configuration 1 - 구성 1 을 백업하려면 이 옵션을 선택합니다. • Configuration 2 - 구성 2 를 백업하려면 이 옵션을 선택합니다. • running-config - 실행 중인 컨피그레이션을 백업하려면 이 옵션을 선택합니다. • startup-config - 시작 구성을 백업하려면 이 옵션을 선택합니다.
Destination File	여기에 TFTP 서버에 저장할 컨피그레이션 파일의 파일 이름과 경로를 입력합니다. 이 필드는 최대 64 자까지 입력할 수 있습니다.

Backup 버튼을 클릭하여 구성 파일 백업을 시작합니다.

Certificate & Key Restore & Backup

Certificate & Key Restore from HTTP

이 창은 HTTP 를 사용하여 로컬 PC 에서 인증서 및 키 복원을 시작하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from HTTP 를 클릭하십시오.

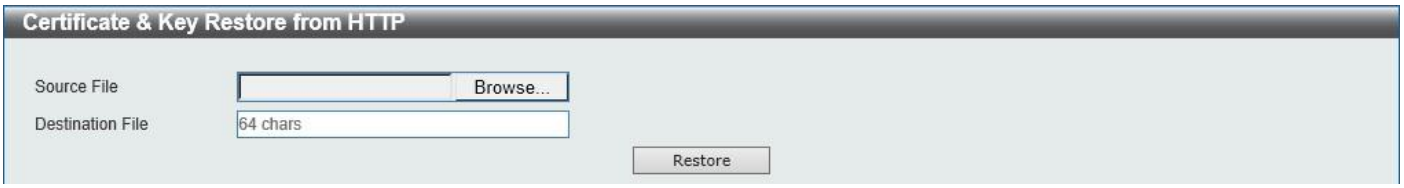

그림 13-10 HTTP 창에서 인증서 및 키 복원

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Source File	Browse 버튼을 클릭하고 여기에서 로컬 PC 의 인증서 및 키 파일로 이동합니다. 이것은 스위치에 업로드 됩니다.
Destination File	Switch 에 저장할 인증서 및 키 파일의 파일 이름과 경로를 여기에 입력합니다. 이 필드는 최대 64 자까지 입력할 수 있습니다.

Restore 버튼을 클릭하여 인증서 및 키 복원을 시작합니다.

Certificate & Key Restore from TFTP

이 창은 TFTP 서버에서 인증서 및 키 복원을 시작하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Tools > Certificate & Key Restore & Backup > Certificate & Key Restore from TFTP 를 클릭하십시오.

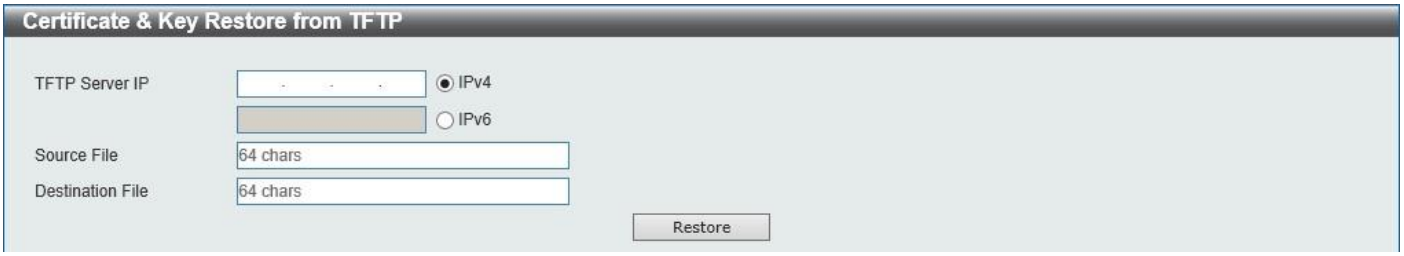

그림 13-11) TFTP 창에서 인증서 및 키 복원

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
TFTP Server IP	여기에 TFTP 서버의 IP Address 를 선택하여 입력합니다. • IPv4 - TFTP 서버의 IPv4 주소를 선택하고 입력하도록 지정합니다. • IPv6 - TFTP 서버의 IPv6 주소를 선택하고 입력하도록 지정합니다.
Source File	여기에 TFTP 서버에 있는 인증서 및 키 파일의 파일 이름과 경로를 입력합니다. 이것은 스위치에 업로드 됩니다. 이 필드는 최대 64 자까지 입력할 수 있습니다.
Destination File	Switch 에 저장할 인증서 및 키 파일의 파일 이름과 경로를 여기에 입력합니다. 이 필드는 최대 64 자까지 입력할 수 있습니다.

복원 버튼을 클릭하여 인증서 및 키 복원을 시작합니다.

Public Key Backup to HTTP

이 창은 HTTP 를 사용하여 로컬 PC 에 인증서 및 키 백업을 시작하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Tools > Certificate & Key Upgrade & Backup > Public Key Backup to HTTP 를 클릭하십시오.

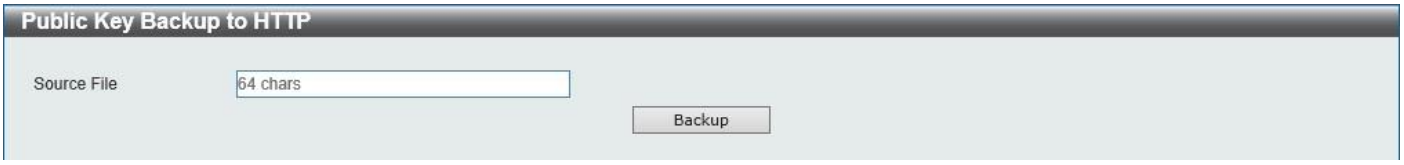

그림 13-12) HTTP 창에 공개 키 백업

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Source File	스위치에 있는 인증서 및 키 파일의 파일 이름과 경로를 여기에 입력합니다. HTTP 를 사용하여 로컬 PC 에 다운로드 됩니다. 이 필드는 최대 64 자까지 입력할 수 있습니다.

Backup 버튼을 클릭하여 인증서 및 키 백업을 시작합니다.

Public Key Backup to TFTP

이 창은 TFTP 서버에 대한 인증서 및 키 백업을 시작하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Tools > Certificate & Key Upgrade & Backup > Public Key Backup to TFTP 를 클릭하십시오.

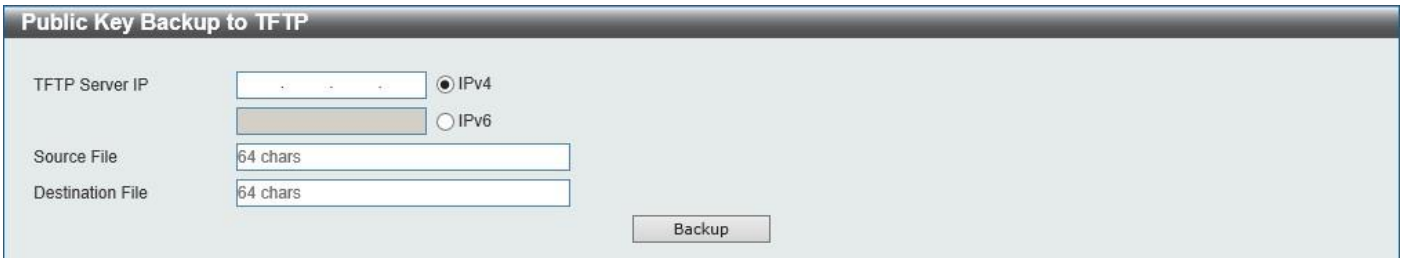

그림 13-13) TFTP 창에 공개 키 백업

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
TFTP Server IP	여기에 TFTP 서버의 IP Address 를 선택하여 입력합니다. • IPv4 - TFTP 서버의 IPv4 주소를 선택하고 입력하도록 지정합니다. • IPv6 - TFTP 서버의 IPv6 주소를 선택하고 입력하도록 지정합니다.
Source File	스위치에 있는 인증서 및 키 파일의 파일 이름과 경로를 여기에 입력합니다. 그러면 TFTP 서버에 다운로드됩니다. 이 필드는 최대 64 자까지 입력할 수 있습니다.
Destination File	TFTP 서버에 저장할 인증서 및 키 파일의 파일 이름과 경로를 여기에 입력합니다. 이 필드는 최대 64 자까지 입력할 수 있습니다.

Backup 버튼을 클릭하여 인증서 및 키 백업을 시작합니다.

Log Backup

Log Backup to HTTP

이 창은 HTTP 를 사용하여 로컬 PC 에 시스템 로그 백업을 시작하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Tools > Log Backup > Log Backup to HTTP 을 클릭합니다.

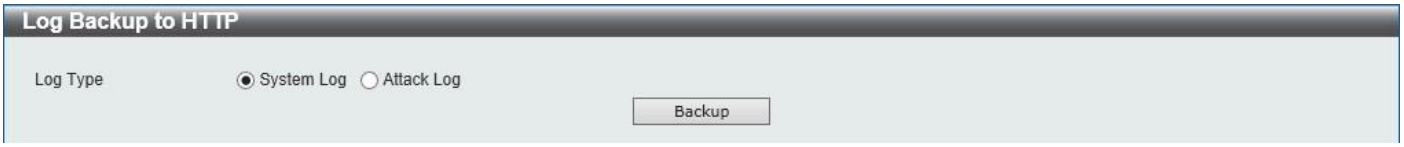

그림 13-14) HTTP 창에 로그 백업

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Log Type	여기에서 로컬 PC 에 백업할 스위치의 로그 유형을 선택합니다. 선택할 수 있는 옵션은 시스템 로그와 공격 로그입니다.

Backup 버튼을 클릭하여 시스템 로그 백업을 시작합니다.

Log Backup to TFTP

이 창은 TFTP 서버에 대한 시스템 로그 백업을 시작하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Tools > Log Backup > Log Backup to TFTP 를 클릭합니다.

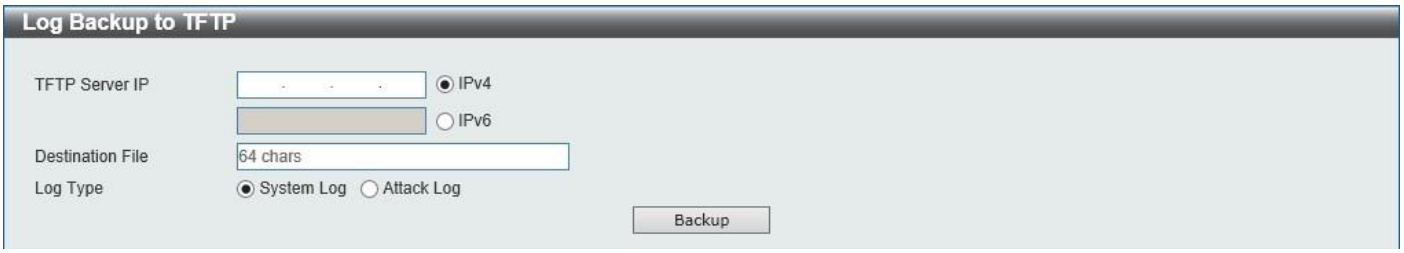

그림 13-15) TFTP 창에 로그 백업

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
TFTP Server IP	여기에 TFTP 서버의 IP Address 를 선택하여 입력합니다. • IPv4 - TFTP 서버의 IPv4 주소를 선택하고 입력하도록 지정합니다. • IPv6 - TFTP 서버의 IPv6 주소를 선택하고 입력하도록 지정합니다.
Destination File	TFTP 서버에 저장할 로그 파일의 파일 이름과 경로를 여기에 입력합니다. 이 필드는 최대 64 자까지 입력할 수 있습니다.
Log Type	여기에서 TFTP 서버에 백업할 스위치의 로그 유형을 선택합니다. 선택할 수 있는 옵션은 System Log 와 Attack Log 입니다.

백업 버튼을 클릭하여 시스템 로그 백업을 시작합니다.

Ping

Ping 은 지정한 IP Address 로 ICMP Echo 패킷을 전송하는 작은 프로그램입니다. 그런 다음 대상 노드는 스위치에서 전송된 패킷에 응답하거나 "에코"합니다. 이는 스위치와 네트워크의 다른 노드 간의 연결을 확인하는 데 매우 유용합니다.

다음 창을 보려면 아래와 같이 Tools > Ping 을 클릭합니다.

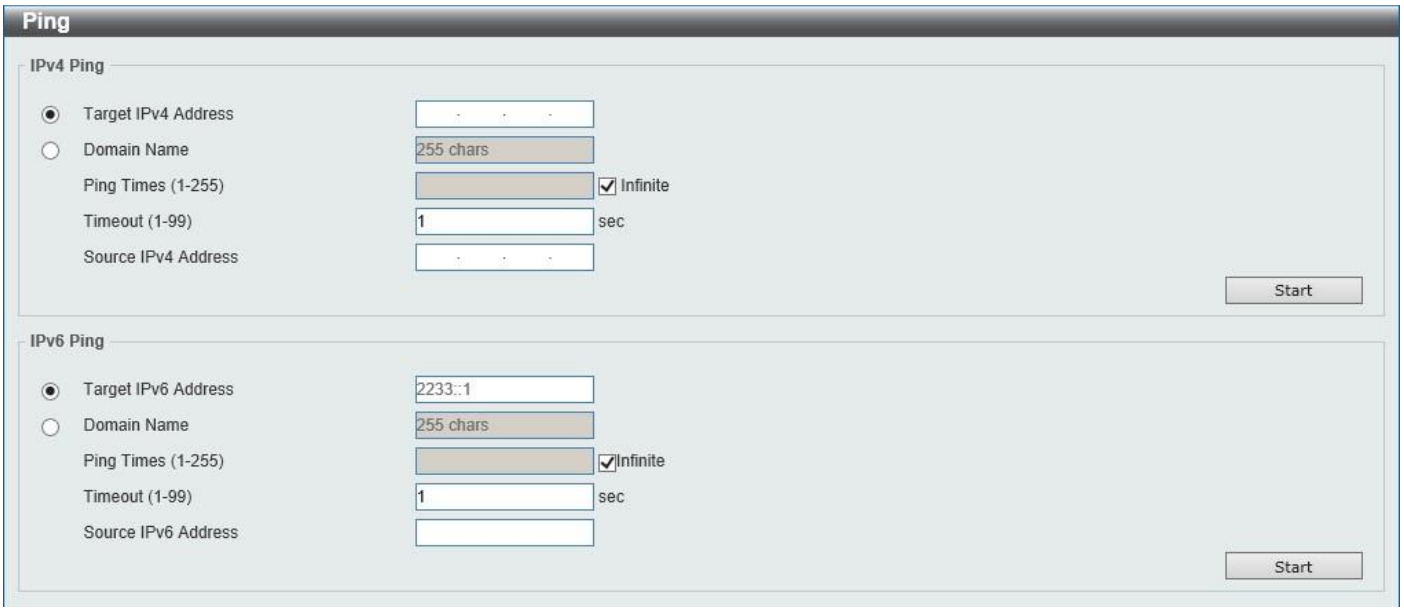

그림 13-16) Ping 창

IPv4 Ping 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Target IPv4 Address	ping 할 IP Address 를 선택하고 입력합니다.
Domain Name	검색할 시스템의 도메인 이름을 선택하고 입력합니다.

Ping Times	이 창에 구성된 IPv4 주소에 대해 Ping 을 시도할 횟수를 입력합니다. 사용자는 1 에서 255 사이의 횟수를 입력할 수 있습니다. 프로그램이 중지될 때까지 지정된 IP Address 로 ICMP Echo 패킷을 계속 보내려면 무한 확인란을 선택합니다.
Timeout	이 Ping 메시지가 대상에 도달하는 데 걸리는 시간 초과 기간을 1 초에서 99 초 사이로 선택합니다. 패킷이 이 지정된 시간 내에 IP Address 를 찾지 못하면 Ping 패킷이 삭제됩니다.
Source IPv4 Address	소스 IPv4 주소를 입력하세요. 현재 스위치에 둘 이상의 IP 주소가 있는 경우, 이 필드에 그중 하나를 입력할 수 있습니다. 입력된 IPv4 주소는 원격 호스트로 전송되는 패킷의 소스 IP 주소로 사용되거나 기본 IP 주소로 설정됩니다.

Start 버튼을 클릭하여 각 개별 섹션에 대한 Ping 테스트를 시작합니다.

IPv6 Ping 에서 구성할 수 있는 필드는 다음과 같습니다.

Parameter	Description
Target IPv6 Address	Ping 을 보낸 IPv6 주소를 입력합니다.
Domain Name	검색할 시스템의 도메인 이름을 선택하고 입력합니다.
Ping Times	이 창에 구성된 IPv6 주소에 대해 Ping 을 시도할 횟수를 입력합니다. 사용자는 1 에서 255 사이의 횟수를 입력할 수 있습니다. 프로그램이 중지될 때까지 지정된 IPv6 주소로 ICMPv6 Echo 패킷을 계속 보내려면 Infinite 확인란을 선택합니다.
Timeout	이 Ping 메시지가 대상에 도달하는 데 걸리는 시간 초과 기간을 1 초에서 99 초 사이로 선택합니다. 패킷이 이 지정된 시간 내에 IPv6 주소를 찾지 못하면 Ping 패킷이 삭제됩니다.
Source IPv6 Address	소스 IPv6 주소를 입력합니다. 현재 스위치에 둘 이상의 IPv6 주소가 있는 경우 이 필드에 그 중 하나를 입력할 수 있습니다. 이 IPv6 주소를 입력하면 원격 호스트로 전송되는 패킷의 소스 IPv6 주소 또는 기본 IPv6 주소로 사용됩니다.

시작 버튼을 클릭하여 각 개별 섹션에 대한 Ping 테스트를 시작합니다.

IPv4 Ping 섹션에서 시작 버튼을 클릭하면 다음 IPv4 Ping 결과 섹션이 나타납니다.

그림 13-17 Ping(시작) 창

Stop 버튼을 클릭하여 Ping 테스트를 중지합니다.
Back 버튼을 클릭하여 IPv4 Ping 섹션으로 돌아갑니다.

Language Management

이 창은 스위치에 언어 파일을 설치하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Tools > Language Management 를 클릭합니다.

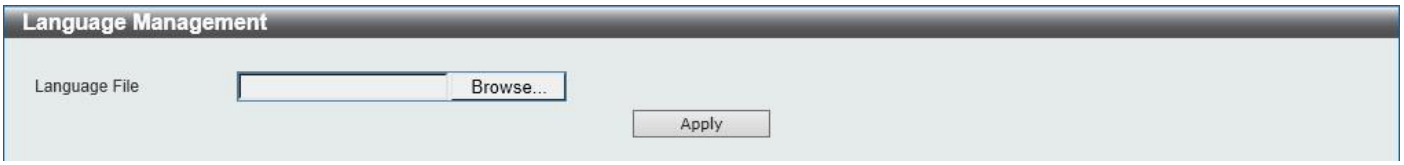

그림 13-18) 언어 관리 창

구성할 수 있는 필드는 아래에 설명되어 있습니다.

Parameter	Description
Language File	찾아보기 버튼을 클릭하고 여기에서 로컬 PC 의 언어 팩 파일로 이동합니다. 이 파일은 스위치에 업로드 됩니다.

Apply 버튼을 클릭하여 언어 팩 업로드 및 설치를 시작합니다.

Reset

이 창은 스위치의 구성을 공장 기본 설정으로 재설정하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Tools > Reset 을 클릭합니다.

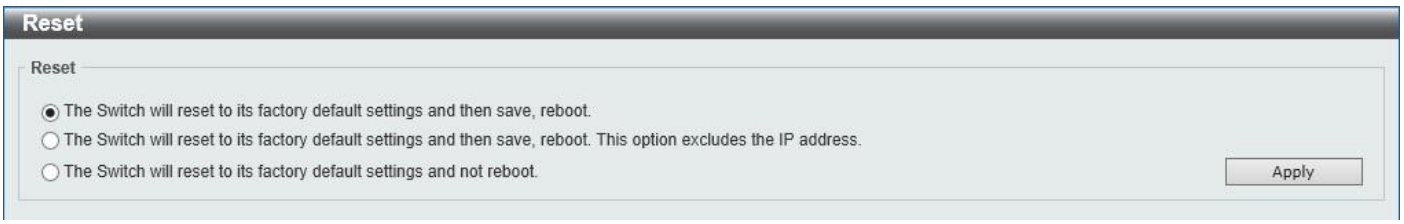

그림 13-19) 리셋 창

다음 옵션 중 하나를 선택합니다.

- 스위치는 공장 기본 설정으로 재설정된 다음 저장하고 재부팅 합니다.
- 스위치는 공장 기본 설정으로 재설정된 다음 저장하고 재부팅 합니다. 이 옵션은 IP Address 를 제외합니다.
- 스위치는 공장 기본 설정으로 재설정되고 재부팅되지 않습니다.

Apply 버튼을 클릭하여 재설정을 시작합니다.

Reboot System

이 창은 스위치를 재부팅하고 수행하기 전에 컨피그레이션을 저장하는 데 사용됩니다.

다음 창을 보려면 아래와 같이 Tools > Reboot System 을 클릭합니다.

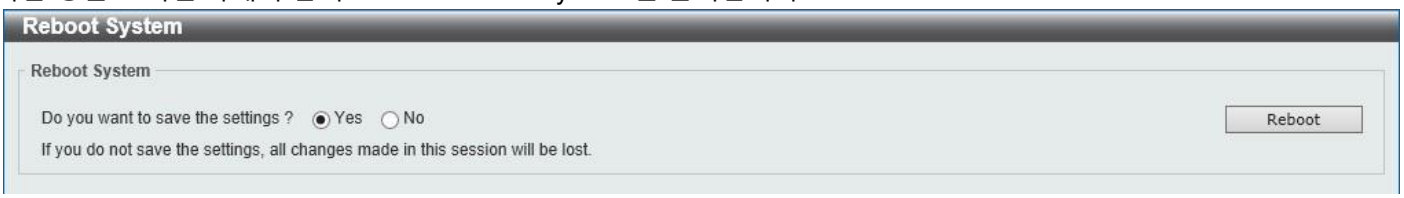

그림 13-20 Reboot System 창

스위치를 재부팅 할 때 설정을 저장할지 묻는 질문에서 Yes 옵션을 선택하지 않으면, 이번 세션 동안 수행된 모든 설정 변경 사항이 손실됩니다.

Reboot 버튼을 클릭하여 설정을 저장하고 스위치를 재부팅 합니다.

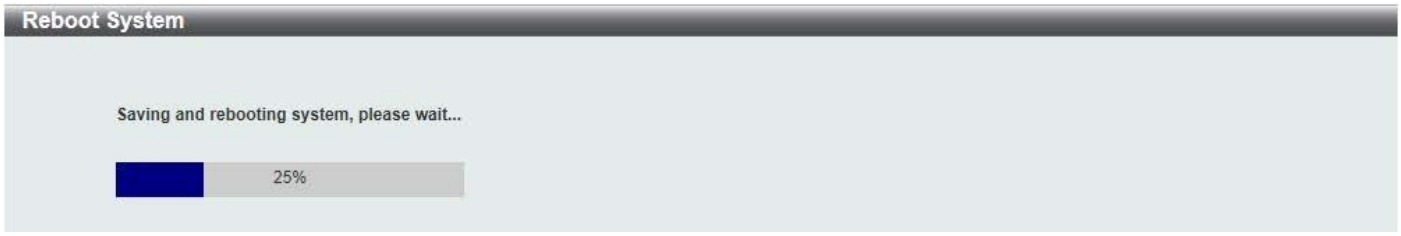

그림 13-21) Reboot System (Rebooting) 창