



ES0152 / ES0152P

52-포트 GbE (PoE) Managed 스위치

사용자 매뉴얼



[www.aten.com](http://www.aten.com)

## EMC 정보

---

**미연방 통신 위원회 전파 방해 성명서:** 이 제품은 FCC 규정 15장에 의거해 Class A 디지털 기기 제한 사항 규정을 준수하도록 테스트를 받았습니다. 이러한 제한 사항은 장치가 상업 환경에서 동작할 시 유해한 간섭에 대한 합리적인 보호를 제공하기 위해 고안되었습니다. 설명서의 내용에 따라 제품 설치 및 사용하지 않을 경우 무선 통신에 유해한 전파 방해가 발생할 수 있습니다. 거주 지역에서 이 장비의 운영은 사용자가 간섭을 조정하기 위한 자기 부담금을 요하는 유해한 간섭을 일으킬 수 있습니다.

본 제품은 FCC 규정 15장에 의거하며 다음의 2가지 조건에서 동작합니다: (1)본 제품은 유해한 간섭을 일으켜서는 안되며, (2) 원하지 않는 동작을 유발하는 어떠한 간섭도 수용해야 합니다.

**FCC 경고:** 규정을 책임지는 기관으로부터 승인 받지 않은 변경 또는 수정은 본 장비를 운영하는 사용자의 권한을 무효화할 수 있습니다.

**경고:** 거주 지역 환경에서 이 제품의 작동은 전파 방해를 일으킬 수 있습니다.

**Achtung:** Der Gebrauch dieses Geräts in Wohnumgebung kann Funkstörungen verursachen.

## KCC 성명

유선 제품용 / A 급 기기 ( 업무용 방송 통신 기기 )

이 기기는 업무용 (A 급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는 것을 목적으로 합니다.

## RoHS

---

이 제품은 RoHS를 준수합니다.



## 사용자 정보

### 온라인 등록

당사의 온라인 지원 센터에 제품 등록을 하십시오:

|       |   |
|-------|---|
| 인터넷서널 | <a href="http://eservice.aten.com">http://eservice.aten.com</a> |
|-------|---|

### 전화 연결 지원

아래의 번호로 전화 연결 지원이 가능합니다:

|       |  |
|-------|--|
| 인터넷서널 | 886-2-8692-6959                          |
| 중국    | 86-400-810-0-810                         |
| 일본    | 81-3-5615-5811                           |
| 한국    | 82-2-467-6789                            |
| 북미    | 1-888-999-ATEN 내선 4988<br>1-949-428-1111 |

### 사용자 주의 사항

본 설명서에 포함된 모든 정보, 기록 그리고 사양은 제조자에 의해 사전 공지 없이 변경될 수 있습니다. 제조자는 명시적 또는 암묵적 진술 및 보증을 일체 하지 않습니다. 특히, 특정 목적을 위한 시장성과 적합성에 관한 어떠한 보증을 하지 않습니다. 본 설명서에서 설명하는 모든 제조자의 소프트웨어는 구매했거나 허가 받은 것입니다. 제품 구입에 따른 결함이 있을 경우, 바이어(제조자가 아닌 유통업자 또는 중개인)가 필요한 서비스, 수리 및 소프트웨어에 결함으로 발생한 부수적 또는 파생적 피해에 대한 모든 비용을 산정합니다.

이 시스템의 제조자는 이 장치에 인증되지 않은 수정에 의해 야기된 라디오와 TV 모두에 대한 전파 방해에 대한 책임을 지지 않습니다. 이러한 전파 방해를 조정하는 것은 사용자의 책임입니다.

제조자는 올바른 동작 전압 설정이 되어 있지 않은 경우 이 시스템의 운영에 발생하는 어떠한 손상에 대해서도 책임지지 않습니다. **사용 전 전압 설정이 올바른지 확인하십시오.**

## 구성품

---

### **ES0152**

- 1 52 포트 GbE Managed 스위치
- 1 AC 전원 코드
- 1 RJ-45 to DB-9 시리얼 콘솔 케이블
- 1 마운팅 키트
- 1 고무 패드 세트(4 pcs.)
- 1 사용자 설명서\*

---

### **ES0152P**

- 1 52 포트 GbE (PoE) Managed 스위치
- 1 AC 전원 코드
- 1 RJ-45 to DB-9 시리얼 콘솔 케이블
- 1 마운팅 키트
- 1 고무 패드 세트 (4 pcs.)
- 1 사용자 설명서\*

모든 구성품이 순서에 맞게 모두 구성되어 있는지 확인하십시오. 선적 과정에서 분실 또는 파손된 부분이 있다면 판매자에게 연락하세요.

본 설명서를 완벽히 숙지 후 설명과 동작 순서를 주의 깊게 따라 해 장치 및 장치와 연결되어 있는 기기의 파손을 방지합니다.

\* 본 설명서 인쇄 후 추가된 기능이 있을 수 있습니다. ATEN 웹사이트에서 설명서의 최신 버전을 다운로드 하십시오.

Copyright © 2020 ATEN® International Co., Ltd.

Manual Date: 2020-08-05

Altusen and the Altusen logo are registered trademarks of ATEN International Co., Ltd. All rights reserved.

All other brand names and trademarks are the registered property of their respective owners.



# 목차

|                           |      |
|---------------------------|------|
| EMC 정보.....               | ii   |
| RoHS.....                 | ii   |
| 사용자 정보.....               | iii  |
| 온라인 등록.....               | iii  |
| 전화 지원.....                | iii  |
| 사용자 주의사항.....             | iii  |
| 구성품 내용.....               | iv   |
| ES0152.....               | iv   |
| ES0152P.....              | iv   |
| 목차.....                   | v    |
| 본 설명서에 대해.....            | xii  |
| 개요.....                   | xii  |
| 규정.....                   | xiii |
| 제품 정보.....                | xiii |
| <b>1장. 소개</b>             |      |
| 개요.....                   | 1    |
| 제품특징.....                 | 3    |
| 구성.....                   | 4    |
| ES0152 앞면 보기.....         | 4    |
| ES0152P 앞면 보기.....        | 4    |
| 시스템 LED.....              | 5    |
| 포트 상태 LED.....            | 6    |
| ES0152/ES0152P 뒷면 보기..... | 8    |
| 웹 인터페이스.....              | 9    |
| 초기 설정 및 로그인 .....         | 9    |
| <b>2장. 설치</b>             |      |
| 마운팅.....                  | 13   |
| 랙 마운팅.....                | 13   |
| 데스크 마운팅.....              | 14   |
| SFP+ 모듈 설치.....           | 15   |
| 하드웨어 설치.....              | 16   |
| <b>3장. 시스템</b>            |      |
| 개요.....                   | 17   |
| 시스템 정보.....               | 18   |
| IP 주소.....                | 21   |
| 설정.....                   | 21   |
| 고급 설정.....                | 23   |
| 상태.....                   | 28   |
| IP 상태.....                | 28   |
| 라우팅 정보 기반.....            | 29   |
| 시스템 정보.....               | 33   |
| LLDP.....                 | 37   |

|                                 |     |
|---------------------------------|-----|
| LLDP 구성.....                    | 37  |
| LLDP-MED 구성.....                | 40  |
| LLDP Neighbor.....              | 51  |
| LLDP-MED Neighbor.....          | 54  |
| LLDP Neighbor PoE.....          | 59  |
| LLDP Neighbor EEE.....          | 60  |
| LLDP 통계.....                    | 63  |
| <b>4장. 포트 관리</b>                |     |
| 개요.....                         | 67  |
| 포트 관리.....                      | 68  |
| 포트 구성.....                      | 68  |
| 포트 현황.....                      | 70  |
| SFP 포트 정보.....                  | 74  |
| 에너지 효율 이더넷.....                 | 76  |
| 링크 집계.....                      | 78  |
| 정적 구성.....                      | 78  |
| LACP 구성.....                    | 80  |
| 시스템 상태.....                     | 82  |
| 내부상태.....                       | 83  |
| 인접 상태.....                      | 85  |
| 포트 상태.....                      | 87  |
| 루프 프로텍션.....                    | 90  |
| 구성.....                         | 90  |
| 상태.....                         | 92  |
| UDLD.....                       | 94  |
| UDLD 구성.....                    | 94  |
| UDLD 상태.....                    | 95  |
| <b>5장. PoE 관리 (ES0152P에 한함)</b> |     |
| 개요.....                         | 99  |
| PoE 구성.....                     | 100 |
| PoE 상태.....                     | 103 |
| PoE 전원 지연.....                  | 106 |
| PoE 자동 점검.....                  | 108 |
| PoE 일정 관리 프로파일.....             | 110 |
| <b>6장. VLAN 관리</b>              |     |
| 개요.....                         | 113 |
| VLAN 구성.....                    | 114 |
| VLAN 멤버십.....                   | 119 |
| VLAN 포트 상태.....                 | 122 |
| MAC 기반 VLAN.....                | 125 |
| 구성.....                         | 125 |
| 상태.....                         | 127 |
| 프로토콜 기반 VLAN.....               | 129 |
| 프로토콜 to 그룹.....                 | 129 |

|                                    |     |
|------------------------------------|-----|
| 그룹 to VLAN.....                    | 132 |
| IP 서브넷 기반 VLAN.....                | 134 |
| GVRP.....                          | 136 |
| 사설 VLAN.....                       | 138 |
| 포트 분리.....                         | 140 |
| 음성 VLAN.....                       | 142 |
| 구성.....                            | 142 |
| OUI.....                           | 144 |
| <b>7장. Quality of Server (QoS)</b> |     |
| 개요.....                            | 147 |
| 포트 분류.....                         | 148 |
| 포트 PCP 분류.....                     | 150 |
| 포트 폴리서.....                        | 152 |
| 포트 셰이퍼.....                        | 154 |
| 스톱 컨트롤.....                        | 157 |
| 포트 스케줄러.....                       | 160 |
| 포트 PCP 리마킹.....                    | 163 |
| DSCP.....                          | 166 |
| 포트 DSCP.....                       | 166 |
| DSCP 번역.....                       | 167 |
| DSCP 분류.....                       | 169 |
| DSCP 기반 QoS.....                   | 170 |
| QoS 제어 목록.....                     | 173 |
| 구성.....                            | 173 |
| 상태.....                            | 179 |
| QoS 통계.....                        | 182 |
| WRED.....                          | 184 |
| <b>8장. 스페닝 트리</b>                  |     |
| 개요.....                            | 187 |
| STP 구성.....                        | 189 |
| MSTI 구성.....                       | 192 |
| STP 상태.....                        | 196 |
| 포트 통계.....                         | 201 |
| <b>9장. MAC 주소 표</b>                |     |
| 개요.....                            | 203 |
| 구성.....                            | 204 |
| 정보.....                            | 207 |
| <b>10장. 멀티캐스트</b>                  |     |
| 개요.....                            | 209 |
| IGMP 스누핑.....                      | 210 |
| 기본 구성.....                         | 211 |
| VLAN 구성.....                       | 213 |
| 상태.....                            | 215 |

|                        |     |
|------------------------|-----|
| 그룹 정보.....             | 217 |
| IGMP SFM 정보.....       | 219 |
| MLD 스누핑.....           | 223 |
| 기본 구성.....             | 224 |
| VLAN 구성.....           | 226 |
| 상태.....                | 228 |
| 그룹 정보.....             | 230 |
| MLD SFM 정보.....        | 232 |
| MVR.....               | 235 |
| 기본 구성.....             | 235 |
| 상태.....                | 238 |
| MVG 그룹 정보.....         | 239 |
| MVR SFM 정보.....        | 241 |
| 멀티캐스트 필터링 프로파일.....    | 245 |
| 필터링 프로파일 테이블 .....     | 245 |
| 필터링 주소 입력.....         | 248 |
| <b>11장. DHCP</b> ..... |     |
| 개요.....                | 251 |
| 스누핑.....               | 252 |
| 구성.....                | 252 |
| 스누핑 테이블 .....          | 253 |
| 상세 통계.....             | 255 |
| 릴레이.....               | 258 |
| 구성.....                | 258 |
| 통계.....                | 260 |
| 서버.....                | 263 |
| 구성.....                | 263 |
| 상태.....                | 264 |
| <b>12장. 보안</b> .....   |     |
| 개요.....                | 267 |
| 관리.....                | 268 |
| 계정.....                | 268 |
| 권한 레벨.....             | 270 |
| 인증 방법.....             | 273 |
| 액세스 방법.....            | 276 |
| HTTPS.....             | 277 |
| 802.1X.....            | 280 |
| 구성.....                | 280 |
| 상태.....                | 291 |
| IP 소스 보호.....          | 294 |
| 구성.....                | 294 |
| 고정 테이블 .....           | 295 |
| 동적 테이블.....            | 297 |
| ARP 검사.....            | 300 |
| 구성.....                | 300 |

|                    |     |
|--------------------|-----|
| VLAN 구성.....       | 302 |
| 고정 테이블 .....       | 304 |
| 동적 테이블.....        | 306 |
| 포트 보안.....         | 309 |
| 구성.....            | 309 |
| 상태.....            | 312 |
| RADIUS.....        | 316 |
| 구성.....            | 316 |
| 상태.....            | 319 |
| TACACS+.....       | 327 |
| <b>13장. 액세스 제어</b> |     |
| 개요.....            | 331 |
| 포트 설정.....         | 332 |
| 속도 제한기.....        | 335 |
| 액세스 제어 목록.....     | 337 |
| ACL 상태.....        | 354 |
| <b>14장. SNMP</b>   |     |
| 개요.....            | 357 |
| 구성.....            | 359 |
| SNMPv3.....        | 361 |
| 커뮤니티 .....         | 361 |
| 유저 .....           | 362 |
| 그룹 .....           | 365 |
| 보기.....            | 367 |
| 액세스.....           | 369 |
| 고정.....            | 373 |
| 구성 .....           | 373 |
| 통계.....            | 374 |
| 기록.....            | 378 |
| 구성 .....           | 378 |
| 상태.....            | 379 |
| 알림.....            | 383 |
| 구성 .....           | 383 |
| 상태.....            | 389 |
| 이벤트.....           | 389 |
| 구성 .....           | 389 |
| 상태.....            | 390 |
| <b>15장. 이벤트 알림</b> |     |
| 개요.....            | 393 |
| SNMP 트랩.....       | 394 |
| 이메일.....           | 398 |
| 로그.....            | 400 |
| 시스로그 .....         | 400 |
| 로그 보기 .....        | 401 |

|   |     |
|---|-----|
| 이벤트 구성.....   | 404 |
| <b>16장. 진단</b>                                      |     |
| 개요.....   | 407 |
| Ping.....   | 408 |
| 추적 루트.....  | 410 |
| 케이블 진단 .....  | 412 |
| 미러링.....  | 414 |
| sFlow.....  | 416 |
| 구성 .....  | 416 |
| 통계 .....  | 419 |
| <b>17장. 유지보수</b>                                    |     |
| 개요.....   | 423 |
| 구성.....   | 424 |
| Startup-Config 저장.....                              | 424 |
| 백업.....   | 425 |
| 복구.....   | 426 |
| 활성화.....  | 427 |
| 삭제.....   | 428 |
| 장치 재시작.....   | 430 |
| 공장 초기값 .....  | 431 |
| 펌웨어 .....   | 432 |
| 펌웨어 업그레이드.....                                      | 432 |
| 펌웨어 선택 .....  | 432 |
| <b>18장. 장치관리 시스템(DMS: Device Management System)</b> |     |
| 개요.....   | 435 |
| 관리.....   | 437 |
| DMS 모드 .....  | 437 |
| API 키 맵.....  | 438 |
| 장치 목록.....  | 439 |
| 그래픽 모니터링 .....                                      | 441 |
| 토폴로지 뷰.....   | 441 |
| 플로어 뷰.....  | 448 |
| 지도 뷰.....   | 449 |
| 유지보수 .....  | 450 |
| 플로어 이미지.....  | 450 |
| 진단.....   | 451 |
| IP 경로 구성 .....                                      | 452 |
| <b>부록</b>   |     |
| 안전 사항.....  | 455 |
| 일반.....   | 455 |
| 랙 마운팅.....  | 457 |
| Consignes de sécurité .....                         | 459 |
| Général .....                                       | 459 |

|                        |     |
|------------------------|-----|
| Montage sur bâti ..... | 462 |
| 기술 지원 .....            | 463 |
| 국제.....                | 463 |
| 북미 지역.....             | 463 |
| 문제 해결 .....            | 464 |
| 제품 규격 .....            | 465 |
| 보증 제한 .....            | 466 |

## 본 설명서에 대해

---

본 사용자 설명서는 스위치를 동작하기 위한 웹 인터페이스 사용에 대한 정보를 제공합니다.

### 개요

**1장, 소개**,에서는 52-Port GbE (PoE) Managed 스위치를 소개합니다. 목적, 특징 및 장점을 제공하며 앞면 및 뒷면 패널 구성 설명 및 웹 인터페이스 액세스 방법에 대해 설명합니다.

**2장, 설치**에서는 스위치를 설치하기 위한 하드웨어 설명을 제공합니다.

**3-17장**,은 웹 인터페이스의 사이드 메뉴 및 관련 구성/동작에 대해 설명합니다.

**18장, 장치 관리 시스템(DMS: Device Management System)**에서는 스위치 관리를 도와줄 DMS 지능형 관리 툴 및 정보를 안내합니다.

**부록**에서는 본 설명서의 마지막에 기술 및 문제해결 정보를 제공합니다.



## 규정

본 설명서는 아래의 규정을 따릅니다.

- 고정 너비            입력해야 할 글자를 나타냅니다.
- [ ]            눌러야 할 키를 나타냅니다. 예를 들어 [Enter] **Enter** 키를 누르라는 의미입니다. 만약 키 조합이 필요하다면 같은 괄호 안에 플러스와 함께 나타냅니다: [Ctrl+Alt]
- 1.            순차적인 단계를 나타내는 번호 목록입니다.
- ◆            불릿 목록은 정보를 제공하지만 순차적인 단계를 담고 있지 않습니다.
- or>            다음에 오는 선택 사항을 나타냅니다(메뉴, 다이얼로그 박스와 같은).  
예를 들어, Start → Run 은 Start 메뉴 열고 Run 을 선택합니다.
- ⚠            주요 정보를 나타냅니다.

## 제품 정보

ATEN 제품에 대한 정보와 제한 없는 도움이 필요할 경우 ATEN 웹사이트 또는 ATEN의 인증된 판매자에 연락하십시오. 지역과 전화 번호 정보 목록에 있는 ATEN 웹사이트를 방문하세요:

|    |   |
|----|---|
| 국제 | <a href="http://www.aten.com">http://www.aten.com</a> |
|----|---|

이 페이지는 의도적으로 비워 두었습니다.

# 1 장 소개

## 개요

---

ES0152 / ES0152P는 ATEN KE 시리즈 KVM over IP 연장기 및 VE89 시리즈 비디오 over IP 연장기\*를 위한 다양한 기능의 managed 스위치입니다. KE / VE89 시리즈 제품과 조합해 사용하는 환경에 이상적이며 ES0152 / ES0152P는 사용자가 복잡한 설치에 대한 번거로움 없이 OT 인프라를 KE 시리즈와 함께 구축할 수 있도록 도와줍니다.

ES0152 / ES0152P는 설치가 빠르고 간편합니다. 플러그 앤 플레이 기능으로 추가 소프트웨어 설치 또는 장치 구성이 필요하지 않습니다. 간단하게 KE / VE89 전송기 및 수신기를 ES0152 / ES0152P에 Cat 5e/6 케이블을 이용해 연결하면 동일한 LAN 상의 모든 KE / VE89 시리즈 장치가 자동으로 탐지됩니다.

ES0152 / ES0152P 네트워크 스위치는 52 포트, 고성능 구성, 완벽한 L2 할당 기능 및 레이어 3 정적 경로, DHCP 서버 및 LLDP와 같은 고급 기능을 제공해 네트워크 동작 향상을 위한 다양한 솔루션을 제공합니다.

ES0152 및 ES0152P 모두 SFP+ (광섬유) 및 RJ45 (구리) 포트 조합을 지원해 다양한 네트워크 니즈를 충족합니다. ES0152는 4 (1G/10G) SFP+ 와 48 (10M/100M/1G) RJ45 포트, 그리고 ES0152P는 4 (1G/10G) SFP+ 및 48 (10M/100M/1G) RJ45를 PoE+ (802.3at/af 지원)와 함께 지원합니다. ES0152P는 Power over Ethernet (PoE) 기능으로 48 RJ45를 통해 최대 740 와트 전력 할당을 제공하며, 전원 아답터가 불필요 하므로 효과적으로 전원 설치 비용을 줄일 수 있습니다.

ES0152 / ES0152P 내장 DMS 기능을 제공해 장치 관리를 언제 어디서나 용이하게 할 수 있습니다. 직관적이고 사용자 친화적인 인터페이스를 이용해 IT 관리자는 네트워크와 모든 연결된 KE / VE89 장치를 손쉽게 설치 및 관리할 수 있습니다. 또한 IP 소스 보안 및 ACL과 같은 포괄적인 보안 기능을 제공해 네트워크를 인증되지 않은 액세스로부터 보호할 수 있습니다.

네트워크 환경에 대해 네트워크 효율성을 극대화할 수 있는 다양한 기능, 관리 용이성 및 신뢰성을 바탕으로 ES0152 / ES0152P는 SMB 및 대기업에 알맞는 네트워크 스위치 솔루션이며

ATEN KE 시리즈 KVM over IP 연장기 또는 VE89 시리즈 비디오 over IP 연장기를 OT 인프라에 적용하려는 환경에 특히 이상적입니다.

---

**주의:** [www.aten.com](http://www.aten.com) 을 방문해 호환 가능한 제품을 참조하십시오.

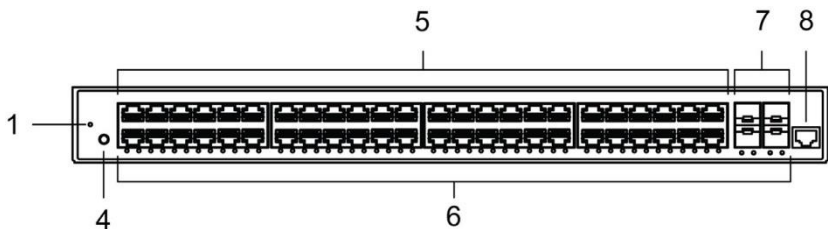
## 제품 특징

---

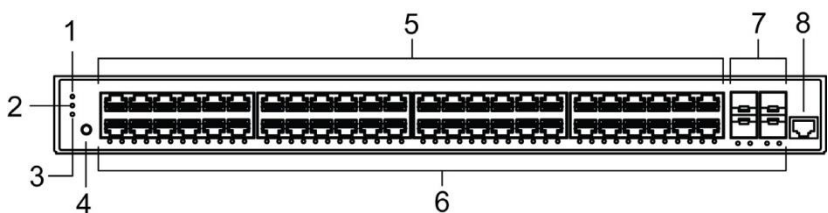
- ◆ KE/VE89 시리즈 장치 자동 탐지
- ◆ 추가 설치 없는 플러그 앤 플레이
- ◆ IGMP 스누핑 패스트 리브 지원
- ◆ 흐름 제어 지원
- ◆ IGMP v1/v2/v3 스누핑 및 IGMP v1/v2 Querier 지원
- ◆ 48 기가 비트 이더넷 포트 및 4 SFP+ 업링크 포트(10Gbps) 지원
- ◆ 176 Gbps 전환이 가능한 고성능 기가 비트 이더넷 L2 액세스 스위치 – 애플리케이션 응답 및 파일 전송 횟수 향상
- ◆ 내장 장치 관리 시스템(DMS) – 관리를 위한 모든 연결된 KE/VE89 장치 개요 제공
- ◆ IEEE 802.1w 고속 스페닝 트리 프로토콜 지원 – 링크 실패로부터 빠른 복구 및 전체 네트워크 안정성 및 신뢰성 강화
- ◆ 포괄적인 QoS – 네트워크를 통해 최대 4 트래픽 타입 마킹, 분류 및 일정 관리
- ◆ 강화된 보안 – 스위치 포트를 이용해 포트 보안은 전체 장치 수를 제한하며 MAC 플러딩 공격으로부터 보호
- ◆ IPv4/IPv6 관리
- ◆ 802.3af PoE/ 802.3at PoE+ 포트 구성 및 일정 관리 (ES0152P에 한함)

# 구성

## ES0152 앞면 보기



## ES0152P 앞면 보기



| No. | 구성                                | ES0152P  |
|-----|-----------------------------------|--|
| 1   | 시스템 LED                           | 스위치가 정상적으로 작동하는지 표시하며 문제 해결을 위한 시스템 경고가 있는지 나타냅니다.   |
| 2   | Link/Act/Spd LED<br>(ES0152P에 한함) | 이 LED에 불이 들어 오는 경우 포트 상태 LED는 링크 상태, 네트워크 동작 및 각 포트의 속도를 표시합니다. LED에 대한 관련 내용은 6페이지의 포트 상태 LED를 참조하십시오.<br>모드 버튼을 눌러 링크/동작/속도 모드 및 PoE 모드를 토글할 수 있습니다. |
| 3   | PoE LED (ES0152P에 한함)             | 이 LED에 불이 들어 오는 경우 포트 상태 LED는 각 포트의 PoE 전원 상태를 표시합니다. LED에 대한 관련 내용은 6페이지의 포트 상태 LED를 참조하십시오.<br>모드 버튼을 눌러 링크/동작/속도 모드 및 PoE 모드를 토글할 수 있습니다.           |

| No. | 구성                   | ES0152P   |
|-----|----------------------|---|
| 4   | 모드/리셋 버튼             | <p>다양한 시간대를 위해 모드/리셋 버튼을 눌러, 유저는 스위치를 리셋, 공장 초기값으로 복구하거나 포트 상태 LED 선명도를 변경할 수 있습니다. (ES0152P에 한함):</p> <ul style="list-style-type: none"> <li>♦ <b>기본값으로 복구:</b> 7-12초 동안 버튼을 누른 상태를 유지합니다.</li> <li>♦ <b>스위치 리셋:</b> 2-7초 간 버튼을 누른 상태를 유지합니다. 모든 포트 상태 LED가 꺼지며 시스템 LED가 깜빡이기 시작할 것입니다.</li> <li>♦ <b>(ES0152P에 한함) 포트 상태 LED 선명도 변경:</b> 0-2초 동안 버튼을 누른 상태를 유지합니다. 시스템 LED가 켜지며 포트 상태 LED가 페이지 6의 포트 상태 LED에 따라 다르게 변경됩니다.</li> </ul> |
| 5   | 10/100/1000 RJ-45 포트 |   |
| 6   | 포트 상태 LED            | 연결된 포트의 상태를 표시합니다. 6페이지의 포트 상태 LED에서 상세 내용을 확인하십시오.   |
| 7   | 10G SFP+ 포트          |   |
| 8   | 콘솔 포트                | CLI 동작을 위해 RJ-45를 DB-9 시리얼 콘솔 케이블에 연결합니다. CL 명령어는 <i>CLI 사용자 매뉴얼</i> 을 참조하십시오.  |

## 시스템 LED

| 색    | 상태  | 설명   |
|------|-----|--|
| 녹색   | On  | 스위치가 정상적으로 작동되고 있습니다.                      |
|      | Off | 스위치가 전원을 공급받지 못하는 상태입니다.                   |
| 빨간 색 | On  | 스위치에 동작 온도 범위 초과와 같은 정상적이지 않은 상태가 감지되었습니다. |

## 포트 상태 LED

포트 상태 LED 동작은 다음의 표와 같습니다:

| 포트         | 색상 | 상태  | 설명  |
|------------|----|-----|---|
| RJ45<br>포트 | 녹색 | On  | 포트가 활성화 되었으며 연결된 장치와 링크가<br>형성되었으며 연결 속도는 1000Mbps입니다.                                      |
|            | 녹색 | 깜빡임 | 포트가 패킷을 전송/수신 중이며 연결 속도는<br>1000Mbps입니다.  |
|            | 황색 | On  | 포트가 활성화 되었으며 연결된 장치와 링크가<br>형성되었으며 연결 속도는 10/100Mbps입니다.                                    |
|            | 황색 | 깜빡임 | 포트가 패킷을 전송/수신 중이며 연결 속도는<br>연결 속도는 10/100Mbps입니다.   |
|            | -- | Off | 포트에 네트워크 케이블 연결이 없거나 연결된<br>장치와 링크가 형성되지 않았습니다. 또는 포트가<br>스위치 유저 인터페이스를 통해 비활성화 된<br>상태입니다. |
| SFP+<br>포트 | 청색 | On  | 포트가 활성화 되었으며 연결된 장치와 링크가<br>형성되었으며 연결 속도는 10Gbps입니다.  |
|            | 청색 | 깜빡임 | 포트가 패킷을 전송/수신 중이며 연결 속도는<br>연결 속도는 10Gbps입니다.   |
|            | 녹색 | On  | 포트가 활성화 되었으며 연결된 장치와 링크가<br>형성되었으며 연결 속도는 1Gbps입니다.   |
|            | 녹색 | 깜빡임 | 포트가 패킷을 전송/수신 중이며 연결 속도는<br>연결 속도는 1Gbps입니다.  |
|            | -- | Off | 포트에 네트워크 케이블 연결이 없거나 연결된<br>장치와 링크가 형성되지 않았습니다. 또는 포트가<br>스위치 유저 인터페이스를 통해 비활성화 된<br>상태입니다. |

### ■ Link/Act/Speed LED에 불이 들어 온 경우 (ES0152P에 한함)

포트 상태 LED 동작은 위의 표와 동일합니다.



## ■ PoE LED에 불이 들어 온 경우 (ES0152P에 한함)

| 포트         | 색상 | 상태  | 설명  |
|------------|----|-----|---|
| RJ45<br>포트 | 녹색 | On  | 포트가 활성화 상태이며 연결된 장치로 전원을 공급하고 있습니다.   |
|            | 황색 | On  | 스위치에 탐지된 과부하와 같은 정상적이지 않은 상태입니다.  |
|            | -- | Off | 포트에 네트워크 케이블 연결이 없거나 PoE PD 장치와 연결되어 있지 않습니다. 또는 포트가 스위치 유저 인터페이스를 통해 비활성화 된 상태입니다. |

## **ES0152 / ES0152P 뒷면 보기**



| No. | 구성     | ES0152P  |
|-----|--------|--|
| 1   | 전원 커넥터 | 제공된 전원 코드를 이 소켓과 AC 월 전원 코드 소켓에 연결해 장치에 전원을 공급합니다. |

## 웹 인터페이스

---

스위치의 특징 및 기능은 웹 인터페이스를 통한 설정 및 관리가 가능하다는 것으로 본 설명서 3장부터 상세히 설명합니다.

### 초기 설정 및 로그인

처음으로 스위치를 켤 때 웹 인터페이스를 이용해 초기 스위치 설정을 할 수 있습니다.

초기 설정 단계를 시작하려면 PC IP 주소 및 서브넷 마스크를 재설정해 PC와 스위치 사이의 통신을 허용해야 합니다.

스위치 공장 초기값 IP 주소: 192.168.0.1

스위치의 공장 초기값 서브넷 마스크: 255.255.255.0

스위치의 공장 초기값 게이트웨이: 192.168.0.254

PC IP 주소(예: 192.168.0.250) 변경 후 스위치의 기본값 IP 주소(192.168.0.1)를 사용해 스위치의 웹 인터페이스에 액세스할 수 있습니다.

Windows® 7/8.x/10가 구동되는 PC를 위한 초기 스위치 설정 순서의 예시는 다음과 같습니다.

1. 시작 메뉴의 검색 창에 *"network and sharing"*를 입력하십시오.
2. 네트워크 및 센터 공유(Network and Sharing Center)를 선택합니다.
3. PC 화면 왼 쪽의 **아답터 설정 변경(Change adapter settings)**를 클릭합니다.

---

**주의:** WinKey+R을 눌러 1~3단계를 생략할 수 있으며 "ncpa.cpl" 명령어를 입력해 4단계로 바로 진행합니다.

---

4. 로컬 아답터의 오른 쪽을 클릭해 **속성(Properties)**을 선택합니다.
  5. **로컬 연결 속성 (Local Area Connection Properties)**창에서 **인터넷 프로토콜 버전 4(TCP/IPv4)**를 표시한 후 **속성(Properties)** 버튼을 클릭합니다.
- 

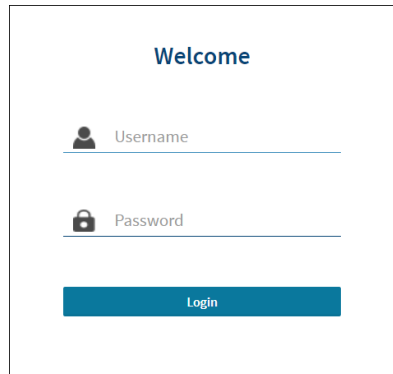
**주의:** 모든 PC의 현재 IP 설정을 기록해 차후 복구할 수 있도록 합니다.

---

6. 라디오 버튼 다음의 **IP 주소 사용 (Use the following IP address)**을 선택한 후 PC에 대한 IP(예: 모든 IP 주소가 사용되는 것이 아니며 192.168.0.2 및 192.168.0.254 사이입니다), 서브넷 마스크(예: 255.255.255.0) 그리고 네트워크 설정에 해당하는 초기값 게이트웨이를 입력합니다.

그리고 원하는 대체 DNS 서버 주소를 입력합니다.

7. **OK**를 클릭해 PC의 IP 주소를 변경하세요.
8. PC의 웹 브라우저를 열고 공장 초기값 IP 주소를 입력해 스위치의 웹 인터페이스에 액세스합니다. 로그인 페이지가 나타납니다:

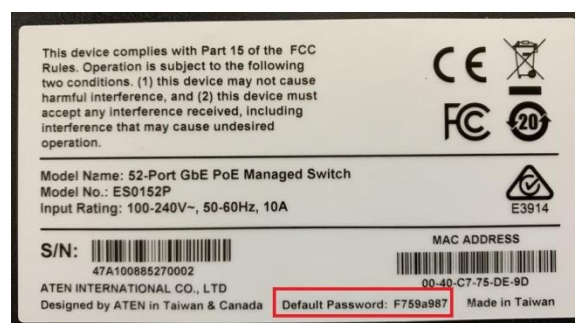


The image shows a web login interface. At the top, it says 'Welcome'. Below that are two input fields: one for 'Username' with a person icon and one for 'Password' with a lock icon. At the bottom is a blue 'Login' button.

**주의:** 위의 로그인 페이지가 보이지 않는다면 다음의 내용을 진행합니다:

1. 웹 페이지를 새로 고침 합니다.
  2. IP 충돌 문제가 없는지 확인합니다.
  3. 브라우저 쿠키 및 임시 인터넷 파일을 삭제합니다.
  4. PC 설정을 다시 확인하고 2단계를 반복합니다.
- 

9. 유저 이름과 패스워드를 입력합니다. 기본 유저이름은 admin 입니다. 각 스위치 고유의 프로그램화 된 패스워드 (하단의 빨간 색 박스 안)는 스위치의 하단 스티커에 제공됩니다. 예시는 다음과 같습니다:



10. "Login"을 클릭해 스위치에 로그인합니다.

---

**주의:** 패스워드를 변경하려면 **보안>관리>계정 (Security > Management> Account)**으로 가  
**admin**(유저 이름)을 클릭합니다. 새로운 패스워드를 입력한 후 한번 더 반복한 다음 적  
용(**Apply**)을 클릭합니다.

---

이 페이지는 의도적으로 비워 두었습니다.

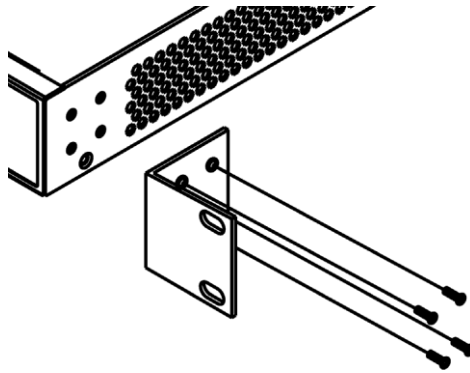
## 마운팅

---

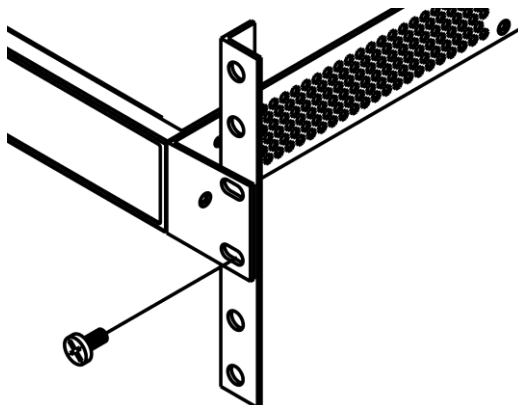
### 랙 마운팅

장치를 랙 마운팅 하려면 다음의 순서를 따라 하십시오.

1. 마운팅 브래킷을 양 쪽 새시에 부착합니다. 드라이버로 나사를 저여 브래킷을 단단히 고정합니다.



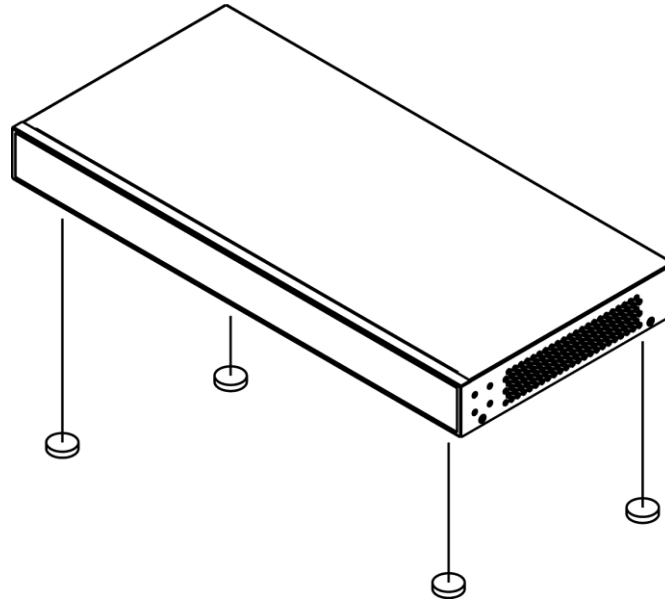
2. 스위치를 랙의 랙 선반에 놓습니다. 브래킷의 타원형 구멍과 랙 기둥의 마운팅 구멍이 일치하도록 합니다..



3. 브래킷을 기둥에 부착합니다. 나사를 조여 단단하게 고정합니다.

## **데스크 마운팅**

1. 책상/작업 공간이 장치를 장착하기에 충분히 견고한지 확인하고 올바르게 접지되어 있는지 확인할 것을 권장합니다.
2. 4개의 고무 받침을 스위치의 하단에 부착합니다.

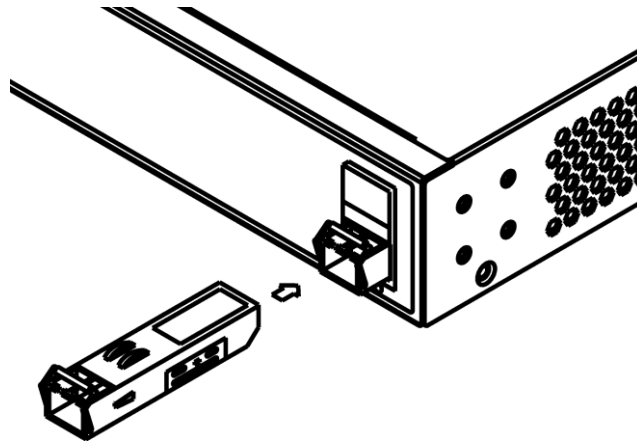




## SFP+ 모듈 설치

SFP+ 포트의 옵션 액세스리로 mini-GBIC SFP+ 모듈을 설치할 수 있습니다. SFP+ 포트의 액세스력이 최대 10Gbps이므로 최대 10Gbps 데이터 속도를 지원하는 mini-GBIC SFP+ 모듈을 선택할 수 있습니다. 스위치 작동 중에서 모듈을 설치할 수 있습니다.

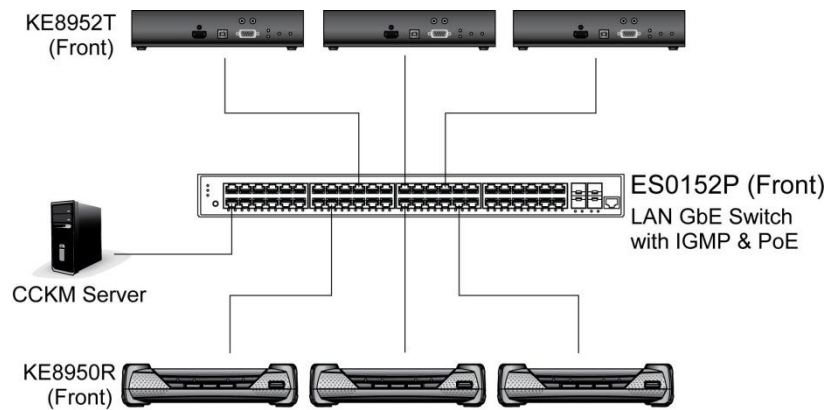
1. 모듈을 SFP+ 포트에 삽입합니다.
2. 모듈이 커넥터에 장착되도록 단단히 누릅니다.



## 하드웨어 설치

ES0152 / ES0152P의 전원 소켓과 AC 소사 사이를 전원 코드로 연결합니다. 스위치에 전원이 들어오는지 시스템 LED를 확인하십시오. 스위치의 RJ-45 포트 및 KE/VE89 시리즈 연장기의 이더넷 RS-45 포트 사이를 이더넷 LAN 케이블로 연결합니다. 포트 상태 LED가 깜빡이면 스위치는 준비가 된 것입니다.

예시는 다음과 같습니다:



## 3장 시스템

### 개요

---

이 장에서는 전체적인 기본 설정 동작을 설명합니다.

메뉴 및 하위 메뉴는 다음과 같습니다:



## 시스템 정보(System Information)

이 페이지에서 장치의 위치, 연락 및 시스템 이름을 설정할 수 있으며 시스템 정보를 확인할 수 있습니다. 이 스위치 시스템의 연락 정보 또한 이 곳에 제공됩니다.

| System Information        |                                  |
|---------------------------|----------------------------------|
| Auto-refresh              | <input type="checkbox"/> Refresh |
| Model Name                | ES0152P                          |
| System Description        | 52-Port GbE PoE Managed Switch   |
| Location                  | <input type="text"/>             |
| Contact                   | <input type="text"/>             |
| System Name               | ES0152P                          |
| System Date               | 2016-01-01T01:44:30+00:00        |
| System Uptime             | 01:44:52                         |
| Bootloader Version        | v1.2-00c98d                      |
| Firmware Version          | v8.40.981 2019-05-02             |
| Hardware Version          | v1.01                            |
| Mechanical Version        | v1.01                            |
| Serial Number             | A123119A1500001                  |
| MAC Address               | 00-40-c7-1c-e9-e8                |
| Fan Speed                 | 1463(rpm)                        |
| Temperature 1             | 37(C)                            |
| Temperature 2             | 34(C)                            |
| CPU Load (100ms, 1s, 10s) | 0%, 4%, 11%                      |

Reset Apply

### ■ 항목 설명

모델 이름 (Model Name):

식별을 위해 공장에서 지정한 모델 이름을 표시합니다.

시스템 설명 (System Description):

시스템 설명을 나타냅니다.

위치 (Location):

Configuration > System > Information > System Location에 설정된 시스템 위치입니다.

연락 (Contact):

Configuration > System > Information > System Contact 에 설정된 시스템 연락입니다.

시스템 이름 (System name):

System > System Information > Configuration > System Name에 설정된 사용자 정의 시스템 이름을 표시합니다.

시스템 날짜 (System Date):

현재(GMT)) 시스템 시간 및 날짜입니다. 시스템 시간은 스위치 상에서 동작하고 있는 타이밍 서버를 통해 정보를 제공합니다.

시스템 동작 시간 (System Uptime):

장치가 동작 가능한 시간입니다.

부트로더 버전 (Bootloader Version):

현재 부트 로더 버전 숫자를 표시합니다.

펌웨어 버전 (Firmware Version):

이 스위치의 소프트웨어 버전입니다.

하드웨어 버전 (Hardware Version):

장치의 하드웨어 버전을 표시합니다.

기계적 버전 (Mechanical Version):

장치의 기계적 버전을 표시합니다.

시리즈 번호 (Series Number):

이 스위치의 시리즈 번호입니다.

MAC 주소 (MAC Address):

이 스위치의 MAC 주소입니다.

팬 속도 (Fan Speed):

팬 속도[rpm]에 대한 정보를 표시합니다.

온도 1 (Temperature 1):

시스템 온도 1을 표시합니다.

온도 2 (Temperature 1):

시스템 온도 2를 표시합니다.

CPU 로드 (CPU Load (100ms, 1s, 10s):

시스템의 CPU 로딩 (100ms, 1s, 10s)를 표시합니다.

## ■버튼

적용 (Apply):

클릭해 변동사항을 저장합니다.

리셋 (reset):

클릭해 로컬의 변동사항을 취소하고 이전에 저장된 값으로 되돌립니다.

## IP 주소(IP Address)

### 설정

스위치의 IPv4 주소는 VLAN 1의 HDCP 서버를 통해 얻을 수 있습니다. 수동으로 주소를 설정하려면 스위치의 기본 설정을 네트워크와 호환하는 값으로 변경해야 합니다. 또한 스위치와 다른 네트워크 세그먼트 상에 존재하는 매니지먼트 스테이션 사이의 기본 게이트웨이를 구축해야 합니다.

The screenshot shows a 'Settings' window for IPv4 configuration. At the top, there's a breadcrumb trail: 'Home > System > IP Address > Settings'. The settings are as follows:

| Field                   | Value         |
|-------------------------|---------------|
| IPv4 DHCP Client Enable | off           |
| IPv4 Address            | 192.168.0.1   |
| Subnet Mask             | 255.255.255.0 |
| Gateway                 | 192.168.0.254 |
| DNS Server              | No DNS server |

An 'Apply' button is located at the bottom right of the settings area.

IP 설정을 구성하려면:

1. 시스템, IP 주소 및 설정을 클릭합니다.
2. IPv4 DHCP 클라이언트를 활성화 또는 비활성화 합니다.
3. IPv4 주소, 서브넷 마스크, 게이트웨이를 지정합니다.
4. DNS 서버를 선택합니다.
5. 적용(Apply) 버튼을 클릭합니다.

### ■항목 설명

IPv4 DHCP 클라이언트 활성화 (IPv4 DHCP Client Enable):

이 박스를 체크해 DHCP 클라이언트를 활성화 합니다. 이 옵션이 활성화 되면 시스템은 IPv4 주소 및 인터페이스 마스크를 DHCP 프로토콜을 이용해 설정할 것 입니다. DHCP 클라이언트는 호스트 이름으로 설정된 시스템 이름을 알려 DNS 검색을 제공합니다.

IPv4 주소 (IPv4 Address):

10진법으로 표기된 인터페이스의 IPv4 주소입니다.

DHCP가 활성화 되면 이 필드는 사용할 수 없습니다. 인터페이스 상의 IPv4 동작이 불필요한 경우 이 필드는 또한 공백으로 남겨 둡니다.

서브넷 마스크 (Subnet Mask):

유저 IP 서브넷 마스크 입력란입니다.

게이트웨이 (Gateway):

IP 게이트웨이의 IP 주소입니다. 유효한 포맷은 10진법으로 표시되거나 유효한 IPv6 표시법입니다.

게이트웨이와 네트워크는 같은 타입이어야 합니다.

DNS 서버 (DNS Server):

이 설정은 스위치에서 설정된 DNS 네임 해상도를 제어합니다.

설정 가능한 4가지 서버가 있으며 서버 지수는 DNS 네임 해상도 구성 시 선호도(지수가 낮을수록 높은 우선 순위)를 나타냅니다.

다음의 모드가 지원됩니다:

◆ No DNS server

DNS 서버가 사용되지 않습니다.

◆ Configured IPv4

명확하게 DNS 서버의 유효한 IPv6 유니캐스트 (링크 로컬 제외) 주소를 제공합니다.

설정된 DNS 서버가 DNS 서비스 활성화를 위해 연결이 가능한지 확인하십시오. (PING6 통해 확인)

◆ From any DHCPv4 interfaces

DHCPv4에서 DHCPv4 호환 인터페이스로 리스된 첫 번째 DNS 서버가 사용됩니다.

◆ From this DHCPv4 interface

DNS 서버에서 제공된 DHCPv4 호환 인터페이스를 선택합니다.

◆ From any DHCPv6 interfaces



DHCPv6에서 DHCPv6 호환 인터페이스로 리스된 첫 번째 DNS 서버가 사용됩니다.

◆ From this DHCPv6 interface

DNS 서버에서 제공된 DHCPv6 호환 인터페이스를 선택합니다.

## ■ 버튼

적용 (Apply):

클릭해 변동사항을 저장합니다.

## 고급 설정(Advanced Settings)

이 페이지에서 스위치-관리 IP 정보를 설정합니다.

IP 기본 설정, 제어 IP 인터페이스 및 IP 루트를 설정합니다.

지원되는 인터페이스의 최대 수는 8이며 최대 루트 수는 8입니다.

The screenshot displays the 'Advanced Settings' page. At the top, there's a breadcrumb trail: Home > System > IP Address > Advanced Settings. The main content area is divided into several sections:

- DNS Settings:** Includes fields for DNS Server 1, 2, 3, and 4, each with a dropdown menu (currently set to 'No DNS server') and an input field. There is also a checkbox for 'DNS Proxy'.
- IP Interfaces:** A table with columns for Delete, VLAN, IPv4 DHCP (Enable, Fallback, Current Lease), IPv4 (Address, Mask Length), IPv6 DHCP (Enable, Rapid Commit, Current Lease), and IPv6 (Address, Mask Length). The first row shows VLAN 1 with IPv4 address 192.168.0.1 and mask length 24.
- Add Interface:** A button to add a new interface.
- Link-Local Address binding Interface:** A dropdown menu currently set to 'VLAN 1'.
- IP Routes:** A table with columns for Delete, Network, Mask Length, Gateway, and Distance/Next Hop VLAN. It lists three routes: 0.0.0.0/0, 169.254.0.0/16, and 192.168.0.0/24.
- Add Route:** A button to add a new route.

At the bottom right, there are 'Reset' and 'Apply' buttons.

웹 인터페이스에서 고급 설정을 하려면:

1. 시스템, IP 주소 및 고급 설정을 클릭합니다.

2. 인터페이스 추가를 클릭한 후 스위치의 새로운 인터페이스를 생성할 수 있습니다.
3. 루트를 추가하고 스위치의 새로운 루트를 생성할 수 있습니다.
4. 적용(Apply)을 클릭합니다.

## ■ 항목 설명

### 기본 설정

모드(Mode):

IP 스택이 호스트 또는 라우터로 동작할지 설정합니다. 호스트 모드에서 인터페이스 간 IP 트래픽은 전달되지 않습니다. 라우터 모드에서 트래픽은 모든 인터페이스 간 전달됩니다.

DNS 서버(DNS Server):

이 설정은 스위치에서 설정된 DNS 네임 해상도를 제어합니다.

설정 가능한 4가지 서버가 있으며 서버 지수는 DNS 네임 해상도 구성 시 선호도(지수가 낮을수록 높은 우선 순위)를 나타냅니다.

다음의 모드가 지원됩니다:

◆ No DNS server

DNS 서버가 사용되지 않습니다.

◆ Configured IPv4

명확하게 DNS 서버의 유효한 IPv6 유니캐스트 (링크 로컬 제외) 주소를 제공합니다.

설정된 DNS 서버가 DNS 서비스 활성화를 위해 연결이 가능한지 확인하십시오. (PING6 통해 확인)

◆ From any DHCPv4 interfaces

DHCPv4에서 DHCPv4 호환 인터페이스로 리스된 첫 번째 DNS 서버가 사용됩니다.

◆ From this DHCPv4 interface

DNS 서버에서 제공된 DHCPv4 호환 인터페이스를 선택합니다.

◆ From any DHCPv6 interfaces

DHCPv6에서 DHCPv6 호환 인터페이스로 리스된 첫 번째 DNS 서버가 사용됩니다.

◆ From this DHCPv6 interface

DNS 서버에서 제공된 DHCPv6 호환 인터페이스를 선택합니다.

DNS 프록시 (DNS Proxy):

DNS 프록시가 활성화 되면 시스템은 현재 설정된 DNS 서버에 DNS 요청을 전달할 것 이며 DNS 확인자로서 네트워크의 클라이언트 장치에 응답할 것 입니다.

IPv4 DNS 프록시만 현재 지원됩니다.

### IP 인터페이스

삭제 (Delete):

이 옵션을 선택하면 기존 IP 인터페이스를 삭제합니다.

VLAN:

IP 인터페이스와 관련된 VLAN입니다. 이 VLAN의 포트만 IP 인터페이스에 액세스할 수 있습니다. 새 인터페이스 생성 시 이 필드는 입력만 가능합니다.

IPv4 DHCP 활성화 (IPv4 DHCP Enabled):

이 박스를 체크해 DHCP 클라이언트를 활성화 하십시오. 이 옵션이 활성화 되면 시스템은 IPv4 주소 및 인터페이스 마스크를 DHCP 프로토콜을 이용해 설정할 것 입니다. DHCP 클라이언트는 호스트 이름으로 설정된 시스템 이름을 알려 DNS 검색을 제공합니다.

IPv4 DHCP 폴백 타임아웃 (IPv4 DHCP Fallback Timeout):

DHCP 리스를 얻기 위한 초 단위 시간입니다. 이 시간이 만료되면 설정된 IPv4 주소는 IPv4 인터페이스 주소로써 사용될 것 입니다. 값이 0인 경우 DHCP는 유효한 리스를 얻을 때 까지 재시도를 하는 폴백 매커니즘을 비활성화합니다. 적합한 값은 0에서 4294967295초입니다.

IPv4 DHCP 현재 리스 (IPv4 DHCP Current Lease):

DHCP 인터페이스와 활성 리스를 위해 이 칼럼은 DHCP 서버에 의해 제공되는 현재 인터페이스 주소를 나타냅니다.

IPv4 주소 (IPv4 Address):

10진법으로 표기된 인터페이스의 IPv4 주소입니다.

DHCP가 활성화 되면 이 필드는 사용할 수 없습니다. 인터페이스 상의 IPv4 동작이 불필요한 경우 이 필드는 또한 공백으로 남겨 둡니다.

IPv4 마스크 길이 (IPv4 Mask Length) :

비트 수(접두 길이)내의 IPv4 네트워크 마스크입니다. IPv4 주소에 대한 유효값은 0에서 30비트입니다.

DHCP가 활성화 되면 이 필드는 사용할 수 없습니다. 인터페이스 상의 IPv4 동작이 불필요한 경우 이 필드는 또한 공백으로 남겨 둡니다.

DHCPv6 활성화 (DHCPv6 Enable):

이 박스를 체크해 DHCPv6 클라이언트를 활성화 합니다. 이 옵션이 활성화 되면 시스템은 DHCPv6 프로토콜을 이용해 인터페이스의 IPv6 주소를 설정할 것 입니다.

DHCPv6 빠른 완료 (DHCPv6 Rapid Commit):

이 박스를 체크해 DHCPv6 빠른 완료 옵션을 활성화 합니다. 이 옵션이 활성화 되면 DHCPv6 클라이언트는 응답 메시지를 빠른 완료 옵션으로 수신하는 대로 대기 프로세스를 종료합니다.

이 옵션은 DHCPv6 클라이언트가 활성화 된 경우에만 관리할 수 있습니다.

DHCPv6 현재 리스 (DHCPv6 Current Lease):

DHCPv6 인터페이스와 활성 리스를 위해 이 칼럼은 DHCPv6 서버에 의해 제공되는 현재 인터페이스 주소를 나타냅니다.

IPv6 주소 (IPv6 Address):

인터페이스의 IPv6 주소입니다. IPv6 주소는 128 비트에서 각 필드를 구별하는 콜론(:)을 포함한 최대 4자리 16진수의 8 필드로 표시됩니다. 예시: fe80::215:c5ff:fe03:4dc7. :: 표시는 지속적인 0 값의 여러 16비트 그룹을 빠르게 표시하는데 사용되는 특수 구문입니다; 그러나 한번만 표시가 가능합니다. 또한 유효한 IPv4 주소를 표시할 수 있습니다. 예시: ::192.1.2.34.

인터페이스 상의 IPv6 동작이 불필요한 경우 이 필드는 또한 공백으로 남겨 둡니다.

IPv6 마스크 길이 (IPv6 Mask Length):

IPv6 네트워크 마스크 비트 수 (프리픽스 길이)입니다. IPv6 주소에 대한 유효값은 0에서 128비트입니다.

인터페이스 상의 IPv6 동작이 불필요한 경우 이 필드는 또한 공백으로 남겨 둡니다.

## IP 경로

삭제 (Delete):

기존 IP 경로를 삭제하려면 이 옵션을 선택하십시오.

네트워크 (Network):

대상 IP 네트워크 또는 이 경로의 호스트 주소입니다. 유효 형식은 10진법으로 표시되거나 유효한 IPv6 표시법입니다. 기본 경로는 0.0.0.0 또는 IPv6 :: 표시입니다.

마스크 길이(Mask Length):

대상 IP 네트워크 또는 호스트 마스크 비트 수 (프리픽스 길이)입니다. 경로의 네트워크 주소의 일치 정도를 정의합니다. 유효 값은 IPv6 경로에 각각 0에서 32비트입니다. 기본 경로만 0의 마스크 길이를 갖습니다. (모든 경로와 일치)

게이트웨이 (Gateway):

IP 게이트웨이의 IP 주소입니다. 유효 형식은 유효 형식은 10진법으로 표시되거나 유효한 IPv6 표시법입니다. 게이트웨이와 네트워크는 반드시 같은 타입이어야 합니다.

다음 홉 VLAN (Next Hop VLAN) (IPv6에 한함):

게이트웨이와 관련된 특정 IPv6 인터페이스의 VLAN ID (VID)입니다.

1~4094의 주어진 VID 범위는 해당 IPv6 인터페이스가 유효한 경우에만 적용됩니다.

IPv6 게이트웨이 주소가 링크-로컬인 경우 게이트웨이에 대한 다음 홉 VLAN을 지정해야 합니다.

IPv6 게이트웨이 주소가 링크-로컬이 아닌 경우 시스템은 게이트웨이에 대한 다음 홉 VLAN을 무시합니다.

## ■ 버튼

인터페이스 추가 (Add Interface):

새로운 IP 인터페이스를 추가하려면 클릭합니다. 최대 8개 인터페이스가 지원됩니다.

경로 추가 (Add Route):

새 IP 경로를 추가하려면 클릭합니다. 최대 8개 경로가 지원됩니다.

적용 (Apply):

클릭해 변동사항을 저장합니다.

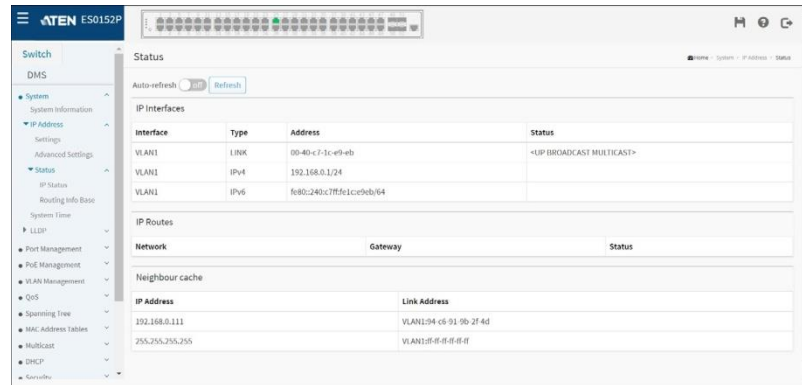
리셋 (Reset):

로컬에서의 변동 사항을 취소하고 저장된 기존 값으로 복구합니다.

## 상태 (Status)

### IP 상태 (IP Status)

이 페이지에서는 IP 프로토콜 레이어의 상태를 표시합니다. 상태는 IP 인터페이스, IP 경로 및 인접 캐시(ARP 캐시) 상태에 의해 정의됩니다.



웹 인터페이스에서 로그 설정을 표시하려면:

1. 시스템, IP 주소 및 상태를 클릭합니다.
2. IP 설정 정보를 표시합니다.

### ■ 항목 설명

인터페이스 (Interface):

인터페이스 이름을 표시합니다.

타입 (Type):

입력 주소 타입을 표시합니다. LINK 또는 IPv4입니다.

주소 (Address):

(주어진 타입의 )인터페이스의 현재 주소를 표시합니다.

상태 (Status):

인터페이스 (및/또는 주소)의 상태 플래그를 표시합니다.

IP 경로 (IP Routes)

네트워크 Network:

IP 네트워크 정의 또는 이 경로의 호스트 주소를 표시합니다.

게이트웨이 (Gateway):

이 경로의 게이트웨어 주소를 표시합니다.

상태 (Status):

경로의 상태 플래그를 표시합니다.

### 인접 캐시 (Neighbor cache)

IP 주소 (IP Address):

입력 IP 주소를 표시합니다.

링크 주소 (Link Address):

기존 IP 주소와 결합된 링크(MAC) 주소를 표시합니다.

### ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

페이지를 즉시 새로 고침 하려면 클릭합니다.

### 라우팅 정보 기반 (Routing Info Base)

라우팅 정보 기반 테이블을 탐색합니다.

각 페이지는 “페이지 당 항목” 입력 필드를 통해 선택된 최대 000 테이블 입력을 표시합니다. 처음 페이지를 열면 웹 페이지는 이 테이블의 시작 항목을 표시합니다.

“Start from ID” 입력 필드에서 유저는 이 테이블의 시작점을 변경할 수 있습니다. 새로 고침 버튼을 클릭하면 시작점부터 또는 그 다음 가까운 항목과 일치하는 표시되는 테이블을 업데이트 할 것 입니다. 추가로 이 입력 필드는 새로 고침 버튼 클릭 시 표시된 항목의 첫 번째 값을 추정하고 동일한 시작 입력 필드와 함께 지속적인 새로 고침을 허용합니다.

Routing Information Base

Auto-refresh ☐ Refresh [OK] [Cancel] [Apply]

1 - 3 of 3 entries

Start from Network / 0 Protocol Static NextHop 192.168.0.254 with 20 entries per page.

Codes: C - connected, S - static, O - OSPF, \* - selected route, D - DHCP installed route

| Protocol | Network/Prefix | NextHop       | Distance | Metric | Interface | Uptime (hh:mm:ss) | State  |
|----------|----------------|---------------|----------|--------|-----------|-------------------|--------|
| S*       | 0.0.0.0/0      | 192.168.0.254 | 1        | 0      | VLAN 1    | -                 | Active |
| C*       | 169.254.0.0/16 | -             | -        | -      | VLAN 1    | -                 | Active |
| C*       | 192.168.0.0/24 | -             | -        | -      | VLAN 1    | -                 | Active |

## 웹 인터페이스

웹 인터페이스에서 라우팅 정보를 표시하려면:

1. 시스템, IP 주소, 상태 및 라우팅 정보 기반을 클릭합니다.
2. 라우팅 정보 기반을 클릭합니다.
3. 라우팅 정보 기반을 표시합니다.

## ■ 항목 설명

DHCP:

경로는 DHCP에 의해 생성됩니다.

연결됨 (Connected):

경로 네트워크가 직접 연결됩니다.

고정 (Static):

경로가 유저에 의해 생성됩니다.

OSPF:

경로가 OSPF에 의해 생성됩니다.

네트워크/프리픽스 (Network/Prefix):

네트워크와 주어진 경로 입력 프리픽스 (예: 10.0.0.0/16)입니다.

다음 홉(NextHop):

다음 홉의 IP 주소입니다. 링크를 나타내는 값 '0.0.0.0'이 직접 연결됩니다.



거리 (Distance):

경로 거리입니다.

측정 (Metric):

경로 측정입니다.

인터페이스 (Interface):

Ip 패킷이 동작 중인 인터페이스입니다.

가동 시간 (Uptime (hh:ss:mm)):

경로가 생성되는 시간입니다 단위는 초입니다.

상태 (State):

대상 네트워크가 도달 가능한지 여부를 표시합니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

페이지를 즉시 새로 고침 하려면 클릭합니다.

|<< :

첫 번째 가능한 항목부터 테이블 항목을 업데이트 합니다. 테이블의 첫 번째 항목이 표시되면 버튼은 비활성화 됩니다.

<< :

현재 표시된 첫 번째 항목 이전 항목에서 종료된 테이블 항목을 업데이트합니다. 테이블의 첫 번째 항목이 표시되면 버튼은 비활성화 됩니다.

>> :

현재 표시된 마지막 항목의 다음 항목부터 시작하는 테이블 항목을 업데이트 합니다. 테이블의 마지막 항목이 표시되면 버튼은 비활성화 됩니다.

>>| :

마지막에 가능한 항목에서 종료된 테이블 항목을 업데이트합니다. 테이블의 마지막 항목이 표시되면 버튼은 비활성화 됩니다.

## 시스템 시간 (System Time)

스위치는 수동 및 자동으로 NTP를 이용해 시스템 시간을 설정합니다. 수동 설정은 간단합니다. "연도", "월", "일", "시간" 및 "분"을 각 항목에 표시된 유효 값 범위 내에서 입력하면 됩니다.

웹 인터페이스에서 시간을 설정하려면:

1. 시스템과 시스템 시간을 클릭합니다.
2. 시간 항목을 지정합니다.
3. 적용을 클릭합니다.

### ■ 항목 설명

#### 시간 설정

시간 소스 (Clock Source):

시간 소스 설정에는 2가지 방법이 있습니다. 로컬 시간의 시간 소스: "로컬 설정 (Local Settings)"을 선택합니다. NTP 서버의 시간 소스: "NTP 서버(NTP Server)"를 선택합니다.

시스템 날짜 (System Date):

시스템의 현재 시간을 표시합니다. 시스템 날짜의 연도는 2000에서 2037 사이로 한정되어 있습니다.

#### **시간대 설정 (Time Zone Configuration):**

시간대 (Time Zone)

다양한 시간 대의 목록을 나타냅니다. 드롭 다운 메뉴에서 적절한 시간 대를 선택해 적용 버튼을 눌러 설정하십시오.

약어 (Acronym):

시간 대의 약어를 설정할 수 있습니다. 시간대를 식별하기 위한 유저 설정 가능 약어입니다. (범위: 최대 16자)

#### **일광 절약 시간 (Daylight Saving Time Configuration)**

일광 절약 시간 (Daylight Saving Time):

이 항목은 지정된 일광 절약 시간 기간을 위해 다음과 같이 설정하기 위해 사용됩니다. '비활성화 (Disable)'을 선택해 일광 절약 시간 설정을 비활성화 합니다. '반복 (Recurring)'을 선택하고 매년 반복하는 일광 절약 시간을 설정합니다. '반복 없음 (Non-Recurring)'을 선택하고 단독 시간 설정에 대한 일광 절약 시간 기간을 설정하십시오. (기본값: 비활성화)

#### **반복 설정 (Recurring Configuration)**

시작 시간 설정(Start time settings):

Week - 시작하는 주의 숫자를 선택합니다.

Day - 시작하는 일자의 숫자를 선택합니다.

Month - 시작하는 달의 숫자를 선택합니다.

Hours - 시작하는 시간의 숫자를 선택합니다.

Minutes - 시작하는 분의 숫자를 선택합니다.

종료 시간 설정 (Day - Select the ending day)

Week - 종료하는 주의 숫자를 선택합니다.

Day - 종료하는 일자의 숫자를 선택합니다.

Month - 종료하는 달의 숫자를 선택합니다.

Hours - 종료하는 시간의 숫자를 선택합니다.

Minutes - 종료하는 분의 숫자를 선택합니다.

오프셋 설정 (Offset settings):

오프셋 - 일광 절약 시간 동안 추가하려면 분의 숫자를 입력합니다.

(범위: 1~1440)

**주의:** "시작 시간 설정" 및 "종료 시간 설정" 아래에는 설정한 "시작 시간 설정" 및 "종료 시간 설정" 필드 정보가 표시됩니다.

## ■ 버튼

적용 (Apply):

클릭해 변동사항을 저장합니다.

리셋 (Reset):

로컬에서의 변동 사항을 취소하고 저장된 기존 값으로 복구합니다.

NTP 서버 설정:

The image displays two screenshots of a system configuration interface. The top screenshot, titled 'Time Configuration', shows a 'Clock Source' dropdown menu set to 'Use NTP Server' and a 'System Date' field displaying '2018-01-01 00:36:15'. A 'Configure NTP Server' button is visible on the right. The bottom screenshot, titled 'NTP Configuration', shows a table for configuring NTP servers. The table has columns for 'NTP Time-Sync Interval' (set to 60) and five rows for 'Server 1' through 'Server 5'. At the bottom of the NTP Configuration section, there are 'Reset' and 'Apply' buttons.

시간 소스를 NTP 서버에서 선택하는 경우 NTP 서버 설정을 클릭합니다. NTP는 네트워크 시간 프로토콜이며 그리니치 표준시(GMT)를 기준으로 네트워크 시간을 동기화 할 때 사용합니다. NTP 모드를 사용하고 내장 NTP 시간 서버를 선택하거나 사용자 정의 NTP 서버 및 시간대를 수동으로 지정하는 경우, <적용> 버튼을 누르면 스위치는 빠르게 시간을 동기화 합니다.

자동으로 시간을 동기화함에도 불구하고 NTP는 사용자의 작업 없이 주기적으로 시간을 업데이트하지 않습니다.

시간대는 GMT의 오프셋 타임입니다. 시간 대를 먼저 선택한 후 NTP를 통해 시간을 동기화 하십시오. 스위치는 현지 시간을 나타내기 위해 이 시간대 오프셋과 업데이트 된 NTP 시간을 동기화 하기 때문입니다. 그렇지 않으면 올바른 시간을 표시할 수 없습니다. 스위치의 구성 가능한 시간 대는 -12 to 에서 13까지 단계 1 시간입니다.

기본 시간 대는 +8 Hrs입니다.

## ■ 항목 설명

Server 1 to 5:

이 스위치의 NTP IPv4 또는 IPv6 주소를 제공합니다. IPv6 주소는 128 비트에서 각 필드를 구별하는 콜론(:)을 포함한 최대 4자리 16진수의 8 필드로 표시됩니다. 예시: fe80::215:c5ff:fe03:4dc7. :: 표시는 지속적인 0 값의 여러 16비트 그룹을 빠르게 표시하는데 사용되는 특수 구문입니다; 그러나 한번만 표시가 가능합니다. 또한 유효한 IPv4 주소를 표시할 수 있습니다. 예시: ::192.1.2.34.

## ■ 버튼

이 버튼은 SNTP 페이지 상에 표시됩니다.

적용 (Apply):

클릭해 변동사항을 저장합니다.

리셋 (Reset):

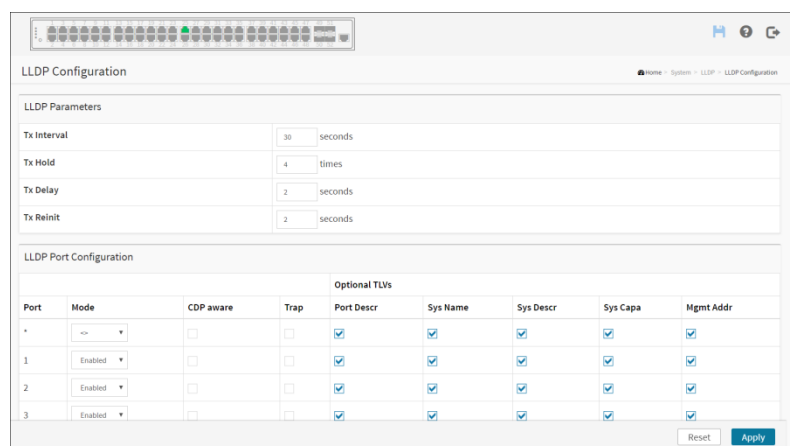
로컬에서의 변동 사항을 취소하고 저장된 기존 값으로 복구합니다.

## LLDP

스위치는 LLDP를 지원합니다. 스위치 모델의 현재 정보를 위해서 스위치가 인접한 장치에 스위치가 있음을 알리고 인접한 LLDP 장치에 대한 정보를 얻기 위한 링크 레이어 디스커버리 프로토콜 (Link Layer Discovery Protocol: LLDP)은 표준 기반의 방식을 제공합니다. 링크 레이어 디스커버리 프로토콜 (Link Layer Discovery Protocol: LLDP)은 식별 정보, 역량 그리고 IEEE 802 로컬 지역 주로 유선 이더넷의 네트워크 인접성을 알리기 위해 네트워크 장치로 사용되는 인터넷 프로토콜 슈트의 벤티-중립 링크 레이어 프로토콜입니다. 프로토콜은 공식적으로 스테이션 및 표준 문서 IEEE 802.1AB로 지정된 미디어 액세스 컨트롤 연결 디스커버리로서 IEEE로 이루어져 있습니다.

### LLDP 설정

포트 별로 LLDP 설정 및 상세 항목 구성이 가능하며 설정은 즉시 적용됩니다. 이 페이지에서는 현재 LLDP 포트 설정을 확인하고 구성할 수 있습니다.



The screenshot shows the 'LLDP Configuration' page. It has two main sections: 'LLDP Parameters' and 'LLDP Port Configuration'.

**LLDP Parameters:**

|             |    |         |
|-------------|----|---------|
| Tx Interval | 30 | seconds |
| Tx Hold     | 4  | times   |
| Tx Delay    | 2  | seconds |
| Tx Reinit   | 2  | seconds |

**LLDP Port Configuration:**

Optional TLVs

| Port | Mode    | CDP aware                | Trap                     | Port Descr                          | Sys Name                            | Sys Descr                           | Sys Capa                            | Mgmt Addr                           |
|------|---------|--------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| *    | ↕       | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1    | Enabled | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2    | Enabled | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3    | Enabled | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Buttons: Reset, Apply

### 웹 인터페이스

LLDP 설정을 하려면:

1. 시스템, LLEP 및 LLDP 설정을 클릭합니다.
2. LLDP 타이밍 항목을 조정합니다.
3. LLDP 메시지 전송 또는 수신을 위해 필요한 모드를 설정합니다.

4. 나타내는 메시지의 TLV 필드 내에 포함하도록 정보를 지정합니다.
5. 적용(Apply)을 클릭합니다.

## ■ 항목 설명

### LLDP 항목

Tx 간격 (Tx Interval):

스위치는 네트워크 발견 정보를 최신으로 하기 위해 주기적으로 주변에 LLDP 프레임을 전송합니다. 각 LLDP 프레임 간 간격은 Tx 간격 값으로 지정됩니다. 유효 값은 5 - 32768초로 제한되어 있습니다.

Tx 홀드 (Tx Hold):

각 LLDP 프레임은 LLDP 프레임의 정보가 얼마 동안 유효할지에 대한 정보를 담고 있습니다. LLDP 정보 유효 기간은 Tx 홀드를 Tx 간격 초로 곱해서 설정할 수 있습니다. 유효 값은 2 -10배로 제한됩니다.

Tx 지연 (Tx Delay):

몇몇 구성(예: IP 주소)이 변경되면 새로운 LLDP 프레임이 전송됩니다. 그러나 LLDP 프레임 간 시간은 항상 최소한 Tx 지연 초 값입니다. Tx 지연은 Tx 간격 값의 1/4보다 클 수 없습니다. 유효 값은 1 - 8192초로 제한되어 있습니다.

Tx 재입력 (Tx Reinit):

포트 비활성, LLDP 비활성 또는 스위치가 재부팅 되면 LLDP 첫다운 프레임이 가까운 장치로 전송되어 LLDP 정보가 더 이상 유효하지 않은 신호를 보냅니다. Tx 재입력은 첫다운 프레임과 새로운 LLDP 초기화 사이에서 시간(초)을 제어합니다. 유효 값은 1 -10초로 제한되어 있습니다.

### LLDP 포트 설정

페이지 머리글에 반영된 것에 따라 현재 선택된 것과 관련된 LLDP 포트입니다.

포트 (Port):

논리적인 LLDP 포트의 스위치 포트 번호입니다.

모드 (Mode):

LLDP 모드를 선택합니다.



Rx only: 스위치는 LLDP 정보를 전송하지 않지만 인접한 장치로부터의 LLDP 정보가 분석됩니다.

Tx only: 스위치는 인접한 장치에서 수신한 LLDP 정보를 누락하지만 LLDP 정보를 전송합니다.

비활성 (Disabled): 스위치는 LLDP 정보를 전송하지 않으며 인접한 장치에서 수신한 LLDP 정보를 누락합니다.

활성화 (Enabled): 스위치는 LLDP 정보를 전송하며 인접한 장치에서 수신한 LLDP 정보를 분석합니다.

CDP 인식 (CDP Aware):

CDP 인식을 선택합니다.

CDP 동작은 들어오는 CDP 프레임을 해독하는데 제한됩니다. (스위치는 CDP 프레임을 전송하지 않습니다.) CDP 프레임은 포트의 LLDP가 활성화 되었을 때만 해독할 수 있습니다.

LLDP 인접 테이블 내의 해당 필드에 발견 가능한 CDP TLV만 해독됩니다. 모든 다른 TLV는 폐기됩니다. (미인식 CDP TVL 및 폐기된 CDP 프레임은 LLDP 통계에 표시되지 않습니다.)

CDP TLV는 LLDP 인접 테이블에 다음과 같이 발견됩니다.

CDP TLV "Device ID"는 LLDP "Chassis ID" 필드에서 발견됩니다.

CDP TLV "Address"는 LLDP "Management Address" 필드에 발견됩니다.

CDP address TLV는 여러 주소를 포함할 수 있으나 첫 번째 주소만 LLDP 인접 테이블에 나타납니다.

CDP TLV "Port ID"는 LLDP "Port ID" 필드에서 발견됩니다.

CDP TLV "Version and Platform"는 LLDP "System Description" 필드에서 발견됩니다.

CDP 및 LLDP 모두 "시스템 기능"을 지원하지만 CDP 기능은 LLDP 파트가 아닌 기능을 커버합니다. 이 기능은 LLDP 인접 테이블의 "others"로 표시됩니다.

모든 포트가 CDP 인식을 하면 비활성화 된 스위치는 인접 장치에서 수신한 CDP 프레임을 전달합니다. 최소한 포트 하나가 CDP 인식을 하면 활성화 된 모든 CDP 프레임은 스위치에 의해 종료됩니다.

---

**주의:** 포트의 CDP 인식이 비활성화 되면 CDP 정보는 즉시 삭제되지 않습니다. 그러나 대기 시간이 초과되면 정보를 가져옵니다.

---

Trap:

LLDP 트래핑은 새롭게 탐지된 인접한 장치 및 링크 결함과 같은 이벤트를 알립니다.

Port Descr:

선택 가능한 TLV: 체크되면 "포트 설명 (port description)"은 전송된 LLDP 정보에 포함됩니다.

Sys Name:

선택 가능한 TLV: 체크되면 "시스템 이름(system name)"은 전송된 LLDP 정보에 포함됩니다.

Sys Descr:

선택 가능한 TLV: 체크되면 "시스템 설명(system description)"은 전송된 LLDP 정보에 포함됩니다.

Sys Capa:

선택 가능한 TLV: 체크되면 "시스템 기능(system capability)"은 전송된 LLDP 정보에 포함됩니다.

Mgmt Addr:

선택 가능한 TLV: 체크되면 "관리 주소(management address)"는 전송된 LLDP 정보에 포함됩니다.

## ■버튼

적용 (Apply):

클릭해 변동사항을 저장합니다.

리셋 (Reset):

로컬에서의 변동 사항을 취소하고 저장된 기존 값으로 복구합니다.

## **LLDP-MED 설정 (LLDP-MED Configuration)**

Media Endpoint Discovery는 LLDP이 강화된 것으로 LLDP- MED로 알려져 있으며 다음과 같은 기능이 있습니다:

플러그 앤 플레이 네트워킹이 가능한 LAN 정책 자동 탐지(VLAN, 레이어 2 우선 및 차별화된 서비스 (Diffserv) 설정)

Voice over Internet Protocol (VoIP), 강화된 911 서비스의 경우 위치 데이터베이스 생성이 가능한 장치 위치 탐지

Power over Ethernet (PoE) 종료점의 확장 가능하고 자동화된 전원 관리

네트워크 관리자가 네트워크 장치를 추적하고 특성을 정의(제조사, 소프트웨어 및 하드웨어 버전, 시리얼 또는 에셋 번호) 할 수 있는 인벤토리 관리

이 페이지에서는 LLDP-MED를 설정할 수 있습니다. 이 기능은 LLDP-MED를 지원하는 VoIP 장치에 적용됩니다.

## LLDP-MED Configuration

Home > System > LLDP > LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count

Transmit TLVs

| Port | Capabilities                        | Policies                            | Location                            | PoE                                 | Device Type  |
|------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------|
| *    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <>           |
| 1    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Connectivity |
| 2    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Connectivity |
| 3    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Connectivity |
| 4    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Connectivity |
| 5    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Connectivity |
| 49   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Connectivity |
| 50   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Connectivity |
| 51   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Connectivity |
| 52   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Connectivity |

Coordinates Location

|          |                                |        |           |                                |      |
|----------|--------------------------------|--------|-----------|--------------------------------|------|
| Latitude | <input type="text" value="0"/> | North  | Longitude | <input type="text" value="0"/> | East |
| Altitude | <input type="text" value="0"/> | Meters | Map Datum | WGS84                          |      |

Civic Address Location

|                       |                      |                          |                      |                        |                      |
|-----------------------|----------------------|--------------------------|----------------------|------------------------|----------------------|
| Country code          | <input type="text"/> | State/Province           | <input type="text"/> | County                 | <input type="text"/> |
| City                  | <input type="text"/> | City district            | <input type="text"/> | Block (Neighborhood)   | <input type="text"/> |
| Street                | <input type="text"/> | Leading street direction | <input type="text"/> | Trailing street suffix | <input type="text"/> |
| Street suffix         | <input type="text"/> | House no.                | <input type="text"/> | House no. suffix       | <input type="text"/> |
| Landmark              | <input type="text"/> | Additional location info | <input type="text"/> | Name                   | <input type="text"/> |
| Zip code              | <input type="text"/> | Building                 | <input type="text"/> | Apartment              | <input type="text"/> |
| Floor                 | <input type="text"/> | Room no.                 | <input type="text"/> | Place type             | <input type="text"/> |
| Postal community name | <input type="text"/> | P.O. Box                 | <input type="text"/> | Additional code        | <input type="text"/> |

Emergency Call Service

Emergency Call Service

Policies

| Delete             | Policy ID | Application Type | Tag | VLAN ID | L2 Priority | DSCP |
|--------------------|-----------|------------------|-----|---------|-------------|------|
| No entries present |           |                  |     |         |             |      |

Add New Policy

Reset

Apply

## 웹 인터페이스

LLDP-MED를 설정하려면:

1. 시스템, LLDP 및 LLDP-MED 설정을 클릭합니다.

2. 빠른 시작 반복 횟수 (Fast start repeat count) 항목을 조정합니다. 기본값은 4입니다.
3. TLV 전송 (Transmit TLV) 항목을 조정합니다.
4. 위치 조정 (Coordinates Location) 항목을 조정합니다.
5. 시 주소 지역 (Civic Address Location) 항목을 채웁니다.
6. 긴급 콜 서비스 (Emergency Call Service) 항목을 채웁니다.
7. 새 정책을 추가합니다.
8. 적용을 클릭하면 정책 포트 설정이 나타납니다.
9. 각 포트의 정책 ID를 선택합니다.
10. 적용을 클릭합니다.

## ■ 항목 설명

### 빠른 시작 반복 횟수 (Fast start repeat count)

종료점의 빠른 시작과 긴급 콜 서비스 지역 식별 탐지는 일반적인 VoIP 시스템의 측면에서 매우 중요합니다. 또한 네트워크 정책의 적절하지 않은 정보를 가져올 수 있는 제한된 LLDPDU 공간을 보존하고 보안 및 시스템 통합 문제를 줄이기 위해, 특정 종료점 타입(예를 들어 음성 네트워크 정책을 허용된 음성 기능 장치에만 알림)과 특별히 관련된 정보를 나타내는 것이 최우선입니다.

이를 염두에 두고 LLDP-MED는 프로토콜과 프로토콜의 위의 애플리케이션 레이어 사이의 LLDP-MED 빠른 시작 상호 작용을 정의합니다. 초기에 네트워크 연결 장치는 LLDPDU에서 LLDP TLV만 전송합니다. LLDP-MED 종료점 장치가 탐지된 이후에만 LLDP-MED 지원 네트워크 연결 장치는 관련 포트 상의 LLDPDU 발신에서 LLDP-MED TLV 알림을 시작합니다. 가능한 빨리 새 neighbor에 LLDP-MED 정보를 공유하도록 새로운 LLDP-MED neighbor가 발견되면 LLDP-MED 애플리케이션은 한시적으로 LLDPDU의 전송 속도를 단번에 올립니다.

neighbors 간 전송되는 동안 손실되는 LLDP 프레임의 위험이 있기 때문에, neighbor가 LLDP 프레임을 수신하는 가능성을 높이기 위해 빠른 시작 전송을 여러 번 반복하는 것을 추천합니다. 빠른 시작 반복 카운트로 빠른 시작 전송이 반복이 될 횟수를 지정하는 것이 가능합니다. 새 정보와 함께 LLDP 프레임이 수신될 때 1초 간격으로 4 LLDP 프레임이 전송될 것으로 고려해 권장 값은 4회입니다.

LLDP-MED 및 LLDP-MED 빠른 시작 매커니즘은 LLDP-MED 네트워크 연결 장치 및 종료점 장치 사이의 링크에서 동작하기 위한 것임을 주의해야 합니다. 따라서 네트워크 연결 장치를 포함한 LAN 인프라 요소 간 링크 및 다른 타입의 링크에는 적용되지 않습니다.

TLV 전송 (Transmit TLVs)

포트 (Port):

설정을 적용할 인터페이스 이름입니다.

기능 (Capabilities):

체크하면 스위치의 기능은 전송되는 LLDP-MED 정보에 포함됩니다.

정책 (Policies):

체크하면 인터페이스에 대해 설정된 정책은 전송되는 LLDP-MED 정보에 포함됩니다.

위치 (Location):

체크하면 스위치에 설정된 위치 정보가 전송되는 LLDP-MED 정보에 포함됩니다.

PoE:

체크하면 설정된 인터페이스에 대한 PoE (Power Over Ethernet) 정보가 전송되는 LLDP-MED 정보에 포함됩니다.

장치 타입 (Device Type):

모든 LLDP-MED 장치는 다음과 같이 정의된 네트워크 연결 장치 또는 특정 종료점 장치의 클래스 중 하나인 LLDP-MED 장치의 특정 타입으로써 동작합니다:

네트워크 연결 장치는 LLDP-MED 종료점 장치를 위해 LAN 인프라를 기반으로 한 IEEE 802에 액세스를 제공하는 LLDP-MED 장치입니다.

LLDP-MED 네트워크 연결 장치는 다음의 기술을 기반으로 한 LAN 액세스 장치입니다:

1. LAN 스위치/라우터
2. IEEE 802.1 Bridge
3. IEEE 802.3 리피터 (기록 포함)
4. IEEE 802.11 무선 액세스 포인트

5. 어떠한 방식으로든 IEEE 802 프레임을 전달하는 IEEE 802 1AB 및 MED 확장을 지원하는 장치입니다.

종료점 장치 LLDP-MED 장치는 네트워크 엣지에 있으며 IEEE 802 LAN 기술을 기반으로 하는 IP 통신 서비스의 일부를 제공합니다.

네트워크 연결 장치와 종료점 장치 사이가 다른 점은 종료점 장치가 LLDP-MED 정보 교환을 할 수 있다는 것뿐입니다.

스위치가 항상 네트워크 연결 장치이어야 함에도 불구하고, 종료점 장치처럼 동작하도록 설정할 수 있습니다. 그렇게 함으로써 LLDP-MED 정보 교환을 시작할 수 있습니다. (2개의 네트워크 연결 장치가 함께 연결된 경우)

#### 위치 조정 (Coordinates Location)

위도 (Latitude):

위도는 최대 4자리 숫자의 0-90도 이내로 지정해야 합니다.

적도 북쪽 또는 적도의 남쪽으로 방향을 지정할 수 있습니다.

경도 (Longitude):

경도는 최대 5자리 숫자의 0-180도 이내로 지정해야 합니다.

본초 자오선의 동쪽 또는 서쪽으로 방향을 지정할 수 있습니다.

고도 (Altitude):

고도는 최대 4자리 숫자의 -32767 ~ 32767내에서 지정해야 합니다.

2개의 고도 타입 (Meters or Floors) 사이에서 선택할 수 있습니다.

미터 (Meters): 지정된 수직 기준면에 의해 정의된 고도의 미터 표시

층 (Floors): 서로 다른 바닥 치수를 가진 빌딩과 관련된 형태에서 고도를 표시합니다. 고도 =0.0은 빌딩 밖에서도 의미가 있으며 지면 레벨을 표시합니다. 주어진 위도 및 경도에서의 지면 레벨을 표시합니다. 빌딩 내부에서의 0.0은 메인 출입구에서 지면 층과 관련된 층 수를 표시합니다.

기준 지형 (Map Datum):

기준 지형은 다음의 옵션을 조정하는데 사용합니다:

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327 및 Prime Meridian Name: Greenwich

NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; 관련 수직 기준면은 1988의 North American Vertical Datum (NAVD88)입니다. 이 기준 페어는 조위 근처가 아닌 지상 위치를 참조하는데 사용됩니다. (Datum = NAD83/MLLW 사용)

NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; 관련 수직 기준은 Mean Lower Low Water (MLLW)입니다. 이 기준 페어는 물/바다/해양의 지역을 참조할 때 사용됩니다.

### **지역 주소 위치 (Civic Address Location)**

Location Configuration Information (Civic Address LCI) 기반 IETF Geopriv 지역 주소

국가 코드 (Country code):

대문자 ASCII 글자의 2자 ISO 3166 국가 코드 - 예: DK, DE 또는 US

주/현(State/Province):

행정 구역 (주, 지역, 도, 현)

자치주/군 (Country):

자치주, 교구, 군 (일본), 지역

시 (City):

시, 거주구, 시(일본) - 예: 코펜하겐

도시 지구 (City district):

도시 구분, 자치구, 도시 지구, 구, 조(일반)

구역 Block (neighborhood):

지역 구역

도로 (Street):

거리 - 예: Poppelvej.

선두 거리 방향 (Leading street direction) :



선두 거리 방향 - 예: N.

Trailing street suffix:

도로 후행 접미사 - 예: SW.

Street suffix:

도로 접미사- 예: Ave, Platz.

House no.:

집 번호 - 예: 21.

House no. suffix:

집 번호 접미사- 예: A, 1/2.

Landmark:

랜드마크 또는 무의미한 주소 - 예: Columbia University.

Additional location info:

추가 지역 정보- 예: South Wing. Name:

이름 (거주 및 사무실 거주) - 예: Flemming Jahn.

Zip code:

우편 번호- 예: 2791.

Building:

빌딩 (건물) - 예: Low Library. Apartment:

유닛 (아파트, 공간) - 예: Apt 42.

Floor:

층 - 예: 4.

Room no.:

방 번호- 예: 450F.

Place type:

공간 유형- 예: Office.

Postal community name:

우편 지역 이름 - 예: Leonia.

P.O. Box:

사서함(P.O. BOX) - 예: 12345.

Additional code:

추가 코드- 예: 1320300003.

Emergency Call Service:

TIA 또는 NENA에 의해 정의된 것을 포함한 비상 콜 서비스 (예: E911 등)

비상 콜 서비스 (Emergency Call Service):

비상 콜 서비스 ELIN 식별자 데이터 포맷은 비상 콜 설정 동안 기존 CAMA 또는 ISDN trunk-based PSAP에 사용되면서 ELIN 식별자를 전송하기 위해 정의됩니다. 이 포맷은 비상 콜에 사용되는 해당 ELIN의 숫자열을 포함합니다.

### 정책 (Policies)

네트워크 정책 디스커버리로 포트의 특정한 프로토콜 애플리케이션을 요청하는 관련된 레이어 2 및 레이어 3 속성과 함께 VLAN 설정과 일치하지 않은 문제의 효과적인 탐지 및 진단이 가능합니다. 올바르게 않은 네트워크 정책 설정은 자주 음성 품질 저하 또는 서비스 손실을 초래하므로 VoIP 환경에서 매우 큰 문제입니다. 정책은 상호 작용 음성 및/또는 비디오 서비스와 같은 특정한 '실시간' 네트워크 정책 요구사항이 있는 애플리케이션과 사용하기 위한 목적으로만 사용됩니다.

알려진 네트워크 정책 특징은:

1. 레이어 2 VLAN ID (IEEE 802.1Q-2003)
2. 레이어 2 우선값(IEEE 802.1D-2004)
3. 레이어 3 Diffserv 코드 포인트(DSCP) 값 (IETF RFC 2474)

이 네트워크 정책은 주어진 포트에 지원되는 여러 애플리케이션 세트와 알려지고 연계됩니다. 애플리케이션 타입은 특히 다음과 같이 표시됩니다:

1. 음성
2. 게스트 음성
3. 스마트폰 음성

4. 비디오 컨퍼런싱
5. 스트리밍 비디오
6. 컨트롤링 / 신호 (조건부로 위의 미디어 타입을 위한 별도의 네트워크 정책을 지원합  
다.)

큰 네트워크는 전체 구성의 여러 VoIP 및 애플리케이션 타입 별로 다른 정책을 지원합니다. LLDP-MED 다양한 정책이 포트 당, 각각 해당하는 다양한 애플리케이션 타입을 알리도록 허용합니다. 같은 네트워크 연결 장치의 서로 다른 포트는 인증된 유저 식별 또는 포트 설정을 기반으로 다양한 정책을 알릴 것 입니다.

LLDP-MED는 네트워크 연결 장치 및 종료점이 아닌 링크에서 작동하는 것이 목적이 아닌 것을 주의해야 합니다. 따라서 주기적으로 LAN까지 종합 링크 내부상에서 동작하는 다수의 네트워크 정책을 알릴 필요가 없습니다.

삭제 (Delete):

체크해 정책을 삭제합니다. 다음 저장 동안 삭제될 것 입니다.

정책 ID (Policy ID):

정책 ID입니다. 이 것은 자동으로 동작하며 특정 포트에 지정된 정책 선택 시 사용됩니다.

애플리케이션 타입 (Application Type):

애플리케이션 타입의 사용 목적:

1. 음성 – 전용 IP 전화 통신 단말기 및 쌍방향 음성 서비스를 지원하는 기타 비슷한 기기로 사용하기 위한 것 입니다. 이 기기는 일반적으로 데이터 애플리케이션으로부터 분리되어 쉬운 배치 및 강화된 보안을 위해 별도의 VLAN에 지정됩니다.
2. 음성 신호 (조건부) – 음성 미디어가 아닌 음성 신호를 위한 여러 정책을 요구하는 네트워크 토폴로지에서 사용하기 위한 것 입니다. 모든 동일한 네트워크 정책이 음성 애플리케이션 정책에 적용되면 이 애플리케이션 타입은 전송되어서는 안됩니다.
3. 게스트 음성 – 게스트 유저 및 방문자를 위해 유저 및 방문자의 IP 전화 통신 단말기 및 쌍방향 음성 서비스를 지원하는 기타 비슷한 기기로 별도의 '제한된 기능-세트' 음성 서비스를 지원합니다.
4. 게스트 음성 신호 (조건부) – 게스트 음성 미디어가 아닌 게스트 음성 신호를 위한 다른 정책을 요구하는 네트워크 토폴로지를 사용하기 위한 것 입니다.

모든 동일한 네트워크 정책이 게스트 음성 애플리케이션 정책에 적용되면 이 애플리케이션 타입은 전송되어서는 안됩니다.

5. 소프트웨어 음성 – PC 또는 노트북과 같은 일반적인 데이터 중심 장치의 소프트웨어 애플리케이션으로 사용하기 위한 것 입니다. 이 종료점의 클래스는 주기적으로 멀티플 VLAN을 지원하지 않습니다. 지원이 되더라도 '태그 미지정' VLAN 또는 싱글 '태그' 데이터 지정 VLAN을 사용하기 위해 일반적으로 설정됩니다. 네트워크 정책이 '태그 미지정' VLAN (아래의 태그된 플래그 참조)과 함께 사용하기 위해 지정되면 L2 우선 필드는 무시되며 DSCP 값만 타당성을 갖습니다.
6. 비디오 컨퍼런싱 – 전용 비디오 컨퍼런싱 장비 및 실시간 쌍방향 비디오/오디오 서비스를 지원하는 기타 비슷한 기기로 사용하기 위한 것 입니다.
7. 스트리밍 비디오 – 특정 네트워크 정책 처리를 필요로 하는 비디오 콘텐츠 분배 및 스트리밍 비디오 서비스를 지원하는 기타 비슷한 애플리케이션 기반의 브로드캐스트 또는 멀티캐스트를 사용하기 위한 것 입니다. 버퍼링이 있는 TCP를 필요로 하는 비디오 애플리케이션은 이 애플리케이션 타입에 사용되지 않습니다.
8. 비디오 신호 (조건부) - 비디오 미디어가 아닌 비디오 신호에 별도의 정책을 요하는 네트워크 토폴로지를 사용하기 위한 것 입니다. 모든 동일한 네트워크 정책이 비디오 컨퍼런싱 애플리케이션 정책에 적용되면 이 애플리케이션 타입은 전송되어서는 안됩니다.

태그 (Tag):

지정된 애플리케이션 타입이 '태그 지정' 또는 '태그 미지정' VLAN을 사용하고 있는지 표시하는 태그입니다.

태그 미지정은 장치가 태그가 미지정된 포맷을 사용하고 있음을 표시하며 IEEE 802.1Q-2003에 의해 정의된 대로 태그 헤더를 포함하지 않습니다. 이 경우 VLAN ID와 레이어 2 우선 필드 모두 무시되며 DSCP 값만 타당성을 갖습니다. 태그 지정은 장치가 태그 지정된 프레임 포맷인 IEEE 802.1Q를 사용하고 있음을 표시하며 VLAN ID와 레이어 2 우선 값, 그리고 DSCP 값도 모두 사용되고 있는 것 입니다. 태그 지정된 포맷은 태그 헤더라고 하는 추가 필드를 포함합니다. 태그 지정된 프레임 포맷은 또한 IEEE 802.1Q-2003로 정의된 우선 태그 지정 프레임을 포함합니다.

VLAN ID:

IEEE 802.1Q-2003에서 정의된 포트에 대한 VLAN 식별자 (VID)입니다.

L2 우선권 (L2 Priority) :

L2 우선권은 지정된 애플리케이션 타입을 위해 사용하는 레이어 2 우선권입니다. L2 우선권은 IEEE 802.1D-2004에서 지정된 대로 8개의 우선권 레벨 (0에서 7) 중 하나를 지정합니다.

0 값은 IEEE 802.1D-2004에서 정의한 대로 기본 우선권 사용을 나타냅니다.

DSCP:

DSCP 값은 IETF RFC 2474에 정의된 대로 지정된 애플리케이션 타입에 대한 Diffserv 노드 작용을 제공하기 위해 사용됩니다. DSCP는 64 코드 포인트 값 중 하나 (0~63)입니다. 0 값은 RFC 2475에서 정의된 대로 기본값 DSCP 값을 나타냅니다.

포트 정책 구성 (Port Policies Configuration):

각 포트는 인증된 유저 식별 또는 포트 설정을 기반으로 고유의 네트워크 정책 또는 같은 네트워크 정책의 다른 특성을 나타냅니다.

포트 (Port):

설정을 적용할 포트 번호입니다.

정책 ID (Policy Id):

주어진 포트에 적용될 정책입니다. 정책은 해당 정책에 체크박스를 체크해 선택됩니다.

버튼 (Buttons)

새 정책 추가 (Adding New Policy):

클릭해 새 정책을 추가합니다. 새 정책에 대한 애플리케이션 타입, 태크, VLAN ID, L2 우선권 및 DSCP를 지정합니다. "적용(Apply)"를 클릭합니다.

적용 (Apply):

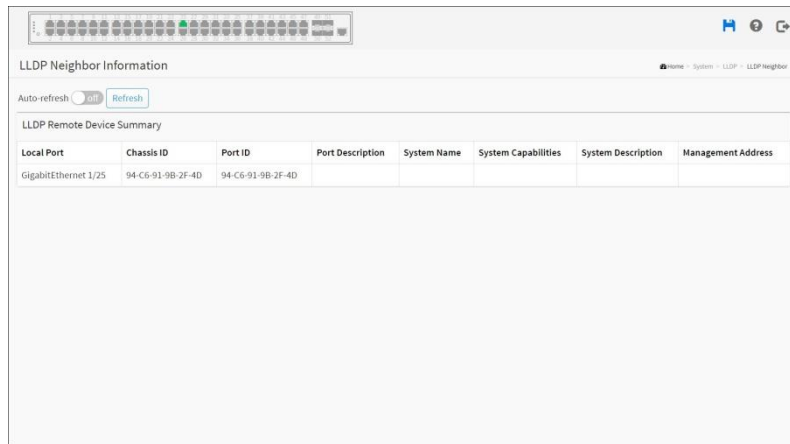
변경을 저장하려면 클릭합니다.

리셋 (Reset):

클릭해 로컬의 변동사항을 취소하고 이전에 저장된 값으로 되돌립니다.

## **LLDP Neighbor**

이 페이지에서는 모든 LLDP Neighbor에 대한 상태 개요를 제공합니다. 표시된 테이블은 LLDP Neighbor가 탐지된 각 포트에 대한 열을 제공합니다. 칼럼은 다음의 정보를 담고 있습니다:



### 웹 인터페이스 (Web Interface)

LLDP neighbors를 표시하려면:

1. 시스템, LLDP 및 LLDP neighbor를 클릭합니다.
2. 수동 업데이트 웹 화면을 위해 새로 고침을 클릭합니다.
3. 자동-업데이트 웹 화면을 위해 자동 새로 고침을 클릭합니다.

**주의:** 네트워크에 LLDP를 지원하는 장치가 없는 경우 테이블은 “No LLDP neighbor information found”를 표시합니다.

### ■ 항목 설명:

로컬 포트 (Local Port):

LLDP 프레임이 수신된 포트입니다.

캐시 ID (Chassis ID):

캐시 ID는 neighbor의 LLDP 프레임의 식별입니다.

포트 ID (Port ID):

원격 포트 ID는 neighbor 포트의 식별입니다.

포트 설명 (Port Description):

포트 설명은 neighbor 유닛에 의해 표시되는 포트 설명입니다.

시스템 이름 (System Name):

시스템 이름은 neighbor 유닛에 의해 표시되는 이름입니다.

시스템 기능 (System Capabilities):

시스템 기능은 neighbor 유닛의 기능을 설명합니다. 가능한 기능은 다음과 같습니다:

1. 기타 (Other)
2. 리피터 (Repeater)
3. 브리지 (Bridge)
4. (WLAN 액세스 포인트) WLAN Access Point
5. 라우터 (Router)
6. 전화 (Telephone)
7. DOCSIS 케이블 장치 (DOCSIS cable device)
8. 스테이션 한정 (Station only)
9. 예비 (Reserved)

(+)와 함께 기능이 활성화 됩니다. 기능이 비활성화 되면 기능은 (-)와 함께 표시됩니다.

시스템 설명 (System Description)

시스템 설명을 표시합니다.

주소 관리 (Management Address):

주소 관리는 네트워크 관리에 의한 탐지를 보조하도록 더 높은 레이어 독립체를 위해 사용되는 neighbor 유닛의 주소입니다. 예를 들어, neighbor IP 주소를 담을 수 있습니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

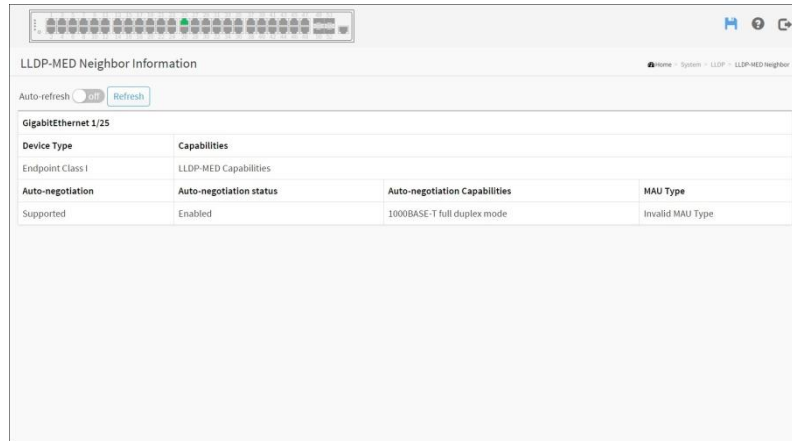
이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 즉시 새로 고칩니다.

## LLDP-MED Neighbor

이 페이지는 모든 LLDP-MED neighbor의 상태 개요를 제공합니다. 표시된 테이블은 LLDP neighbor가 탐지된 각 포트의 열을 포함합니다. 이 기능은 LLDP-MED를 지원하는 VoIP 장치에 적용됩니다. 칼럼은 다음의 정보를 담고 있습니다:



| LLDP-MED Neighbor Information                 |                         |                               |                  |
|---|-------------------------|-------------------------------|------------------|
| Auto-refresh <input type="checkbox"/> Refresh |                         |                               |                  |
| GigabitEthernet 1/25                          |                         |                               |                  |
| Device Type                                   | Capabilities            |                               |                  |
| Endpoint Class I                              | LLDP-MED Capabilities   |                               |                  |
| Auto-negotiation                              | Auto-negotiation status | Auto-negotiation Capabilities | MAU Type         |
| Supported                                     | Enabled                 | 1000BASE-T full duplex mode   | Invalid MAU Type |

### 웹 인터페이스 (Web Interface)

LLDP-MED Neighbor를 표시하려면:

1. 시스템, LLDP 및 LLDP-MED Neighbor를 클릭합니다.
2. 수동 업데이트 웹 화면을 위해 새로 고침을 클릭합니다.
3. 자동-업데이트 웹 화면을 위해 자동 새로 고침을 클릭합니다.

포트 (Port):

LLDP 프레임이 수신된 포트입니다.

장치 타입 (Device Type):

LLDP-MED 장치는 2개의 주요 장치 타입 - 네트워크 연결 장치 및 종료점 장치로 구성되어 있습니다.

- ♦ LLDP-MED 네트워크 연결 장치 정의  
TIA-1057에서 정의된 대로 LLDP-MED 네트워크 연결 장치는 LLDP-MED 종료점 장치의 LAN 인프라 기준 IEEE 802에 액세스를 제공합니다. LLDP-MED 네트워크 연결 장치는 다음의 기술을 기반으로 한 LAN 액세스 장치입니다:



1. LAN 스위치/라우터
2. IEEE 802.1 브리지
3. IEEE 802.3 리피터 (기록 포함)
4. IEEE 802.11 무선 액세스 포인트
5. TIA-1057에 의해 정의된 IEEE 802.1AB 및 MED 확장을 지원하는 장치이며 어떠한 방법으로든 IEEE802 프레임에 전달할 수 있습니다.

◆ LLDP-MED 종료점 장치 정의

TIA-1057로 정의된 대로 LLDP-MED 종료점 장치는 IEEE 802 LAN 네트워크 edge에 위치하며 LLDP-MED 체계를 이용해 IP 통신 서비스와 연계합니다.

LLDP-MED 종료점 장치 카테고리 내에서 LLDP-MED 배열은 다음에서 정의된 대로 더 많은 종료점 장치 캐시로 나뉘어 집니다.

각 LLDP-MED 종료점 장치 클래스는 이전 종료점 장치 클래스를 위해 정의된 기능을 생성하기 위해 정의된 것입니다.

예를 들어, 미디어 종료점(Class II)으로 규정 이행을 요하는 LLDP-MED 종료점 장치는 또한 일반 종료점(Class I)이 적용되는 TIA-1057 모든 항목을 지원합니다. 그리고 통신 장치(Class III)로 규정 이행을 요하는 LLDP-MED 종료점 장치는 또한 미디어 종료점 Endpoints(Class II) 및 일반 종료점 (Class I)에 적용되는 TIA-1057 모든 항목을 지원합니다.

◆ LLDP-MED 일반 종료점 (Class I):

LLDP-MED 일반 종료점 (Class I) 정의는 TIA-1057에서 정의된 기본 LLDP 탐지 서비스를 필요로 하는 모든 종료점 제품에 적용됩니다. 그러나 IP 미디어를 지원하지 않거나 유저 통신 설비로써 동작합니다. 이러한 장치는 IP 통신 컨트롤러, 서버 관련 기타 통신 또는 TIA-1057로 정의된 기본 서비스를 포함(제한 없음)합니다.

이 클래스에 정의된 탐지 서비스는 LAN 설정, 장치 위치, 네트워크 정책, 전원 관리 및 인벤토리 관리를 포함합니다.

◆ LLDP-MED 미디어 종료점 (Class II):

LLDP-MED 미디어 종료점 (Class II) 정의는 특정 최종 유저와 관련 여부와 상관 없이 IP 미디어 기능을 가진 모든 종료점 제품에 적용됩니다. 기능은 이전 일반 포인트 클래스(Class I)에 대해 정의된 모든 기능을 포함하며 미디어 스트리밍에 관련된 항목을 포함하도록 확장됩니다.

이 클래스에 부착하는 것으로 예상되는 예시 제품 카테고리는 음성 / 미디어 게이트웨이, 컨퍼런스 브리지, 미디어 서버 등을 포함합니다. (제한되지 않음)

이 클래스에 정의된 탐지 서비스는 미디어-타입-특정 네트워크 레이어 정책 탐지를 포함합니다.

♦ LLDP-MED 통신 종료점 (Class III):

LLDP-MED 통신 종료점 (Class III) 정의는 IP 미디어를 지원하는 최종 유저 통신 기기로서 동작하는 모든 종료점 제품에 적용됩니다. 기능은 이전 일반 종료점 (Class I) 및 미디어 종료점 (Class II) 클래스에 대해 정의된 모든 기능을 포함하며 최종 유저기와 관련된 항목을 포함하도록 확장됩니다. 이 클래스에 부착하는 것으로 예상되는 예시 제품 카테고리는 IP 전화, PC 기반 소프트폰 또는 직접적으로 최종 유저를 지원하는 기타 통신 기기와 같은 최종 유저 통신 기기를 포함합니다. (제한되지 않음)

이 클래스에 정의된 탐지 서비스는 위치 식별자 공급 (ECS / E911 정보), 내장된 L2 스위치 지원, 인벤토리 관리를 포함합니다.

LLDP-MED 기능 (LLDP-MED Capabilities):

LLDP-MED 기능은 인접한 유닛의 LLDP-MED 기능을 설명합니다. 가능한 기능은 다음과 같습니다:

1. LLDP-MED 기능
2. 네트워크 정책
3. 위치 식별
4. MDI – PS0E를 통한 확장된 전원
5. MDI – PD를 통한 확장된 전원
6. 인벤토리
7. 예비

애플리케이션 타입 (Application Type):

이 네트워크 정책에 정의된 애플리케이션의 주요 기능을 표시하는 애플리케이션 타입입니다.

종료점 또는 네트워크 연결 장치에 의해 나타냅니다. 가능한 애플리케이션 타입은 다음과 같이 표시됩니다.

1. 음성 - 전용 IP 전화 통신 단말기 및 쌍방향 음성 서비스를 지원하는 기타 비슷한 기기로서 사용하기 위한 것 입니다. 이 기기는 일반적으로

데이터 애플리케이션으로부터 분리되어 쉬운 배치 및 강화된 보안을 위해 별도의 VLAN에 지정됩니다.

2. 음성 신호 - 음성 미디어가 아닌 음성 신호를 위한 여러 정책을 요구하는 네트워크 토폴로지에서 사용하기 위한 것 입니다.
3. 게스트 음성 - 게스트 유저 및 방문자를 위해 유저 및 방문자의 IP 전화 통신 단말기 및 쌍방향 음성 서비스를 지원하는 기타 비슷한 기기로 별도의 제한된 기능-세트 음성 서비스를 지원합니다.
4. 게스트 음성 신호- 게스트 음성 미디어가 아닌 게스트 음성 신호를 위한 다른 정책을 요구하는 네트워크 토폴로지를 사용하기 위한 것 입니다.
5. 스마트폰 음성 - PC 또는 노트북과 같은 일반적인 데이터 중심 장치의 스마트폰 애플리케이션으로 사용하기 위한 것 입니다.
6. 비디오 컨퍼런싱 - 전용 비디오 컨퍼런싱 장비 및 실시간 쌍방향 비디오/오디오 서비스를 지원하는 기타 비슷한 기기로 사용하기 위한 것 입니다.
7. 스트리밍 비디오 - 특정 네트워크 정책 처리를 필요로 하는 비디오 콘텐츠 분배 및 스트리밍 비디오 서비스를 지원하는 기타 비슷한 애플리케이션 기반의 브로드캐스트 또는 멀티캐스트를 사용하기 위한 것 입니다.
8. 비디오 신호 - 비디오 미디어가 아닌 비디오 신호에 별도의 정책을 요하는 네트워크 토폴로지를 사용하기 위한 것 입니다.

정책 (Policy):

정책은 종료점 장치는 분명하게 정책이 장치에 의해 요청되는 것을 알리길 원하는 것을 표시합니다. 지정됨 또는 미확인입니다.

미확인: 지정된 애플리케이션 타입의 네트워크 정책이 현재 미확인입니다.

지정됨: 네트워크 정책이 정의되었습니다.

태그 (TAG):

태그는 지정된 애플리케이션 타입이 태그 지정인지 태그 미지정 VLAN을 사용하는지 식별합니다. 태그 지정 또는 태그 미지정입니다.

태그 미지정: 장치는 미지정 태그 프레임 형식을 사용하고 있으며 IEEE 802.1Q-2003로 정의된 대로 태그 헤더를 포함하지 않습니다.

태그 지정: 장치는 태그 지정된 프레임 포맷인 IEEE 802.1Q을 사용하고 있습니다.

**VLAN ID:**

IEEE 802.1Q-2003에서 정의된 포트에 대한 VLAN 식별자 (VID)입니다. 1에서 4094의 값은 유효한 VLAN ID를 정의하기 위해 사용됩니다. 장치가 우선 태그 프레임을 사용하고 있는 경우 IEEE 802.1Q-2003으로 정의된 대로 0 값 (우선 태그됨)이 사용됩니다. IEEE 802.1D 우선권 레벨만이 의미가 있으며 내부포트의 기본값 PVID가 대신 사용됩니다.

**우선권 (Priority):**

우선권은 레이어 2 우선권으로 지정된 애플리케이션 타입을 위해 사용됩니다. 8개 우선권 레벨 중 하나입니다. (0에서 7)

**DSCP:**

DSCP는 IETF RFC 2474에 정의된 대로 지정된 애플리케이션 타입에 대한 Diffserv 노드 작용을 제공하기 위해 사용되는 DSCP 값입니다. 64 코드 포인트 값 중 하나 (0~63)입니다.

**자동 탐색 (Auto-negotiation):**

자동 탐색은 MAC/PHY 자동-탐색이 링크 파트너에 의해 지원되는지 식별합니다.

**자동 탐색 상태 (Auto-negotiation status):**

자동 탐색이 현재 링크 파트너에서 활성화 되어 있는지 자동 탐색 상태를 식별합니다. 자동 탐색이 지원되며 자동 탐색 상태가 비활성화라면 802.3 PMD 동작 모드는 자동 탐색이 아닌 운영상의 MAU 타입 필드 값으로 지정됩니다.

## ■ 버튼

**자동 새로 고침 (Auto-refresh):**

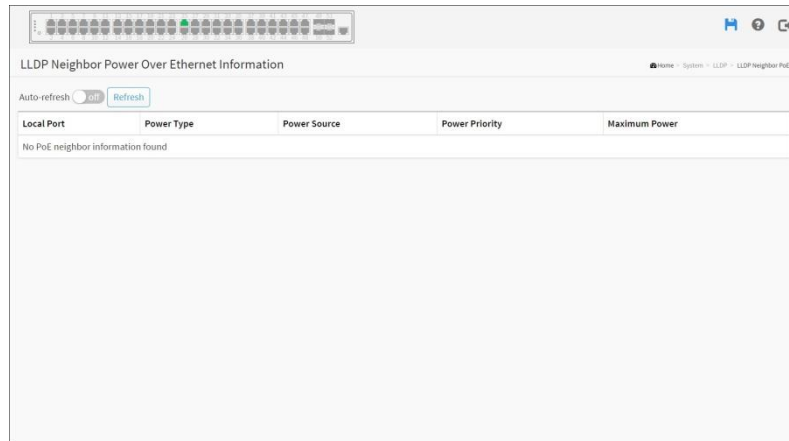
이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

**새로 고침 (Refresh):**

페이지를 즉시 새로 고침 하려면 클릭합니다.

## LLDP Neighbor PoE

이 페이지는 모든 LLDP PoE neighbors에 대한 상태 개요를 제공합니다. 표시된 테이블은 어느 LLDP PoE neighbor가 탐지되었는지에 대한 각 인터페이스의 열을 포함합니다. 칼럼은 다음의 정보를 담고 있습니다:



| Local Port                        | Power Type | Power Source | Power Priority | Maximum Power |
|-----------------------------------|------------|--------------|----------------|---------------|
| No PoE neighbor information found |            |              |                |               |

### 웹 인터페이스

LLDP Neighbor PoE를 표시하려면:

1. 시스템, LLDP 및 LLDP-MED Neighbor PoE를 클릭합니다.
2. 수동 업데이트 웹 화면을 위해 새로 고침을 클릭합니다.
3. 자동-업데이트 웹 화면을 위해 자동 새로 고침을 클릭합니다.

### ■ 항목 설명:

로컬 포트 (Local Port):

LLDP 프레임이 수신된 이 스위치에 대한 인터페이스입니다.

전원 타입 (Power Type):

전원 타입은 장치가 전력 소싱 개체 (PSE) 또는 전력 장치 (PD)인지 나타냅니다.

전원 타입이 미확인 되면 "Reserved"로 표시됩니다.

전력 소스 (Power Source):

전력 소스는 PSE 또는 PD 장치에 의해 사용되는 전력 소스를 나타냅니다.

장치가 PSE 장치인 경우 주요 전원 소스 또는 백업 전원 소스 중 하나에서 동작합니다. PSE 장치가 주요 전원 소스 또는 백업 전원 소스로 사용되고 있는지 미확인인 경우 “미확인”으로 식별됩니다.

장치가 PD 장치인 경우 로컬 전원 공급에서 동작 가능하거나 또는 전원 소스로 PSE가 사용 가능합니다. 또한 로컬 전원 공급과 PSE 모두 사용 가능합니다.

PD 장치가 사용 중인 전원 공급이 무엇인지 미확인인 경우 “미확인”으로 식별됩니다.

전력 우선권 (Power Priority):

전력 우선권은 PD 장치의 우선권 또는 전력을 소싱하는 PSE 타입 장치의 인터페이스와 관련된 전력 우선권을 나타냅니다. 전력 우선권의 3단계가 있습니다. 3단계는 중요, 높은 및 낮음입니다. 전력 우선권이 미확인인 경우 “미확인”으로 표시됩니다.

최대 전력 (Maximum Power):

최대 전력 값은 PSE 장치에서 PD 장치에 의해 요구되는 와트 최대 전력 또는 현재 설정을 기반으로 PSE 장치가 최대 길이 케이블을 통해 소싱 가능한 최소 전력 나타내는 수치 값을 포함합니다.

허용된 최대 수치는 102.3 W입니다. 장치가 102.3 W보다 더 높은 값을 표시하면 “reserved”가 나타납니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

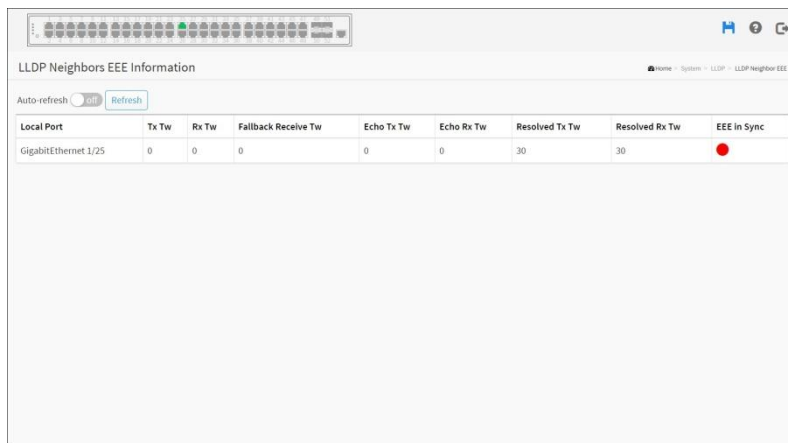
페이지를 즉시 새로 고침 하려면 클릭합니다.

## LLDP Neighbor EEE

EEE 전원 절약은 트래픽 지연 경비를 낮출 수 있습니다. 이 지연은 링크를 통해 트래픽 전송 전 전원을 절약하기 위해 EEE를 끈 서킷, 부팅을 위해 필요한 시간 때문에 발생합니다.

이 시간을 “wakeup time” 이라고 부릅니다. 최소한의 지연 시간을 위해서 장치는 필요한 최소한의 wakeup time을 설정한대로 각각의 tx와 rx “wakeuptime”에 대한 정보를 교환하는 LLDP를 사용할 수 있어야 합니다.

이 페이지는 LLDP에 의해 교환된 EEE 정보의 개요를 제공합니다.



| Local Port           | Tx Tw | Rx Tw | Fallback Receive Tw | Echo Tx Tw | Echo Rx Tw | Resolved Tx Tw | Resolved Rx Tw | EEE In Sync                        |
|----------------------|-------|-------|---------------------|------------|------------|----------------|----------------|------------------------------------|
| GigabitEthernet 1/25 | 0     | 0     | 0                   | 0          | 0          | 30             | 30             | <span style="color: red;">●</span> |

## 웹 인터페이스

LLDP Neighbor EEE를 표시하려면:

1. 시스템, LLDP 및 LLDP-MED Neighbor EEE를 클릭합니다.
2. 수동 업데이트 웹 화면을 위해 새로 고침을 클릭합니다.
3. 자동-업데이트 웹 화면을 위해 자동 새로 고침을 클릭합니다.

## ■ 항목 설명:

로컬 포트 (Local Port):

LLDP 프레임이 수신 또는 전송된 곳의 인터페이스입니다.

Tx Tw:

LPI의 불이행 후 경로를 전송하는 링크 파트너의 최대 시간은 데이터 전송을 미룰 수 있습니다.

Rx Tw:

수신기는 전송기가 수신기에 대한 휴지 시간을 해제하도록 허용하는 시간을 미루고자 하는 링크 파트너의 시간입니다.

폴백 수신 Tw (Fallback Receive Tw):

링크 파트너의 폴백 수신 Tx.

수신 링크 파트너는 필요한 선택 가능한 Tw\_sys\_tx의 전송기를 알릴 수 있습니다. 수신 링크 파트너는 절약 개별 수치를 가질 가능성이 있으므로 이 것은 더욱 효율적인 할당을 위해 사용할 수 있는 추가 정보의 전송기를 제공합니다. 이 옵션을 실행할 수 없는 시스템은 수신 Tw\_sys\_tx와 동일한 기본값이 됩니다.

Echo Tx Tw:

링크 파트너의 Echo Tx Tw 값:

각 에코 값은 원격 링크 파트너 각 값의 로컬 링크 파트너 반응(에코)으로써 정의됩니다. 로컬 링크 파트너가 원격 링크 파트너로부터 반복되는 값을 수신하면 원격 링크 파트너가 가장 최근 값을 수신, 등록, 처리 여부를 정의할 수 있습니다. 예를 들어, 로컬 링크 파트너가 로컬 MIB의 값과 일치하지 않는 반복되는 변수를 수신하면, 로컬 링크 파트너는 원격 링크 파트너 요청이 오랜 정보를 기반으로 한 것을 뜻합니다.

Echo Rx Tw:

링크 파트너의 Echo Rx Tw 값입니다.

Resolved Tx Tw:

이 링크의 예비 Tx Tw입니다. 주의: 링크 파트너 아님

이 링크(LLDP를 통해 교환된 EEE 정보 기반)에 사용된 실제 "tx wakeup time "인 예비 값입니다.

Resolved Rx Tw:

이 링크의 예비 Rx Tw입니다. 주의: 링크 파트너 아님

이 링크(LLDP를 통해 교환된 EEE 정보 기반)에 사용된 실제 "tx wakeup time "인 예비 값입니다.

EEE 동기화 (EEE in Sync):

스위치 및 링크 파트너가 wakeup-time에 대한 동의 여부를 표시합니다.

적색 - 스위치 및 링크 파트너가 wakeup-time에 대해 동의하지 않았습니다.

녹색 - 스위치 및 링크 파트너가 wakeup-time에 대해 동의했습니다.

## ■ 버튼





자동 새로 고침 (Auto-refresh):

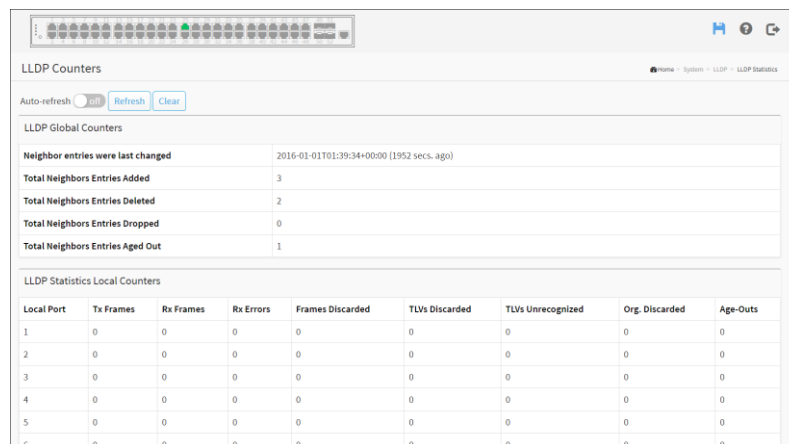
이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

페이지를 즉시 새로 고침 하려면 클릭합니다.

## LLDP 통계 (LLDP Statistics)

카운터의 2가지 타입이 표시됩니다. 로컬 카운터가 현재 스위치의 포트 당 카운터를 참조하는 반면 글로벌 카운터는 전체 스위치를 참조합니다.



LLDP Counters

Auto-refresh ☐ Refresh Clear

LLDP Global Counters

|                                    |  |
|------------------------------------|--|
| Neighbor entries were last changed | 2016-01-01T01:39:34+00:00 (1952 secs. ago) |
| Total Neighbors Entries Added      | 3  |
| Total Neighbors Entries Deleted    | 2  |
| Total Neighbors Entries Dropped    | 0  |
| Total Neighbors Entries Aged Out   | 1  |

LLDP Statistics Local Counters

| Local Port | Tx Frames | Rx Frames | Rx Errors | Frames Discarded | TLVs Discarded | TLVs Unrecognized | Org. Discarded | Age-Outs |
|------------|-----------|-----------|-----------|------------------|----------------|-------------------|----------------|----------|
| 1          | 0         | 0         | 0         | 0                | 0              | 0                 | 0              | 0        |
| 2          | 0         | 0         | 0         | 0                | 0              | 0                 | 0              | 0        |
| 3          | 0         | 0         | 0         | 0                | 0              | 0                 | 0              | 0        |
| 4          | 0         | 0         | 0         | 0                | 0              | 0                 | 0              | 0        |
| 5          | 0         | 0         | 0         | 0                | 0              | 0                 | 0              | 0        |
| 6          | 0         | 0         | 0         | 0                | 0              | 0                 | 0              | 0        |

웹 인터페이스

LLDP 및 LLDP 통계를 표시하려면:

1. 시스템, LLDP 및 LLDP 통계를 클릭합니다.
2. 수동 업데이트 웹 화면을 위해 새로 고침을 클릭합니다.
3. 자동-업데이트 웹 화면을 위해 자동 새로 고침을 클릭합니다.
4. 모든 카운터를 삭제하려면 삭제(Clear)를 클릭합니다.

### ■ 항목 설명:

#### 글로벌 카운터 (Global Counters)

마지막으로 변경된 Neighbor 엔트리:

또한 마지막 엔트리가 삭제 또는 추가된 시간을 표시합니다. 그리고 마지막 변경이 탐지된 후 경과 시간을 나타냅니다.

추가된 전체 neighbor 엔트리 (Total neighbors Entries Added):

스위치를 재부팅한 이후 추가된 새 엔트리의 번호를 나타냅니다.

삭제된 전체 neighbor 엔트리 (Total neighbors Entries Deleted):

스위치를 재부팅한 이후 삭제된 새 엔트리의 번호를 나타냅니다.

감소한 전체 neighbor 엔트리 (Total neighbors Entries Dropped):

엔트리 표가 가득 차 삭제한 LLDP 프레임의 수를 나타냅니다.

오래 된 전체 neighbor 엔트리 (Total neighbors Entries Aged Out):

Time-To-Live 만료로 인해 삭제된 엔트리의 수를 나타냅니다.

### **로컬 카운터 (Local Counters)**

표시된 테이블은 각 포트의 열을 포함합니다. 칼럼은 다음 정보를 담고 있습니다:

로컬 포트 (Local Port):

LLDP 프레임이 수신 또는 전송된 곳의 인터페이스입니다.

Tx 프레임 (Tx Frames):

포트에 전송된 LLDP 프레임의 수 입니다.

Rx 프레임 (Rx Frames):

포트에 수신된 LLDP 프레임의 수 입니다.

Rx 에러 (Rx Errors):

일부 문제를 포함한 수신된 LLDP 프레임의 수입니다.

폐기된 프레임 (Frames Discarded):

LLDP 프레임이 포트에 수신되고 스위치의 내부테이블이 완전 동작하면, LLDP 프레임은 카운트를 하고 폐기됩니다. 이 상황은 LLDP 표준에서 "너무 많은 neighbors(Too Many neighbors)"로 알려져 있습니다. 캐시 ID 또는 원격 포트 ID는 이미 테이블 내에 포함되어 있지 않다면 LLDP 프레임은 테이블에서 새로운 엔트리를 요합니다. 주어진 포트의 링크가 다운되고 LLDP 첫다운 프레임이 수신되거나 엔트리가 오래 되면 엔트리는 테이블에서 삭제됩니다.

폐기된 TLV (TLVs Discarded):

각 LLDP 프레임은 TLV로 알려진 (TLV는 "Type Length Value(입력 길이 값)"의 줄임말 입니다.) 다양한 정보를 담을 수 있습니다. TLV가 기형인 경우 카운트가 되며 폐기됩니다.

미인식 되는 TLV (TLVs Unrecogniz):

올바르게 형성된 TLV의 수, 그러나 미확인 된 타입 값입니다.

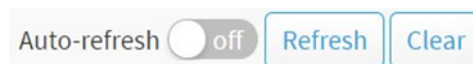
폐기된 Org (Org. Discarded):

유기적으로 수신된 TLV의 수입니다.

만료 (Age-Outs):

각 LLDP 프레임은 LLDP 정보가 유효한 기간(만료 시간)에 대한 정보를 포함합니다. 새로운 LLDP 프레임이 만료 시간 안에 수신되지 않으면 LLDP 정보는 삭제되면 시간 만료 카운터가 증가됩니다.

## ■버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

페이지를 즉시 새로 고침 하려면 클릭합니다.

삭제(Clear):

선택된 포트에 대한 카운터를 삭제합니다.

이 페이지는 의도적으로 비워 두었습니다.

## 4장

# 포트 관리

### 개요

이 섹션은 스위치의 포트 상세 항목을 설정하기 위한 설명입니다. 사용할 수 있는 그 외 항목은 포트를 스위치의 포트 활성화 또는 비활성화 하도록 설정합니다. 기능의 포트 콘텐츠 또는 상태를 모니터링 합니다.

메뉴 및 하위 메뉴는 다음과 같습니다:



## 포트 관리

이 섹션은 스위치의 포트 상세 항목을 설정하기 위한 설명입니다. 사용할 수 있는 그 외 항목은 포트를 스위치의 포트 활성화 또는 비활성화 하도록 설정합니다. 기능의 포트 콘텐츠 또는 상태를 모니터링 합니다.

### 포트 설정

이 페이지는 현재 포트 설정을 표시합니다. 포트는 또한 여기에서 구성할 수 있습니다.

| Port | Description | Speed |        |      | Flow Control |           |      | Maximum Frame Size |
|------|-------------|-------|--------|------|--------------|-----------|------|--------------------|
|      |             | Link  | Status | Mode | Rx Status    | Tx Status | Mode |                    |
| *    |             |       |        | Auto |              |           | off  | 9000               |
| 1    |             | Down  | Down   | Auto | off          | off       | off  | 9000               |
| 2    |             | Down  | Down   | Auto | off          | off       | off  | 9000               |
| 3    |             | Down  | Down   | Auto | off          | off       | off  | 9000               |
| 4    |             | Down  | Down   | Auto | off          | off       | off  | 9000               |
| 5    |             | Down  | Down   | Auto | off          | off       | off  | 9000               |
| 6    |             | Down  | Down   | Auto | off          | off       | off  | 9000               |
| 7    |             | Down  | Down   | Auto | off          | off       | off  | 9000               |

웹 인터페이스:

웹 인터페이스에서 현재 포트 설정을 구성하려면:

1. 포트 관리 및 포트 설정을 클릭합니다.
2. 상세 포트 대체 이름 또는 전체 이름과 시스템의 하드웨어 타입, 소프트웨어 버전 및 네트워크 애플리케이션에 대한 버전 식별을 설명하는 글자와 숫자 열을 지정합니다.
3. 설정 속도, 흐름 제어, 최대 프레임 크기를 지정합니다.
4. 적용을 클릭합니다.

### ■ 항목 설명:

포트 (Port):

이 열에 대한 논리적 포트 번호입니다.

설명 (Description):

최대 63자의 이 포트 식별을 위한 기술적인 이름을 입력합니다.

링크 (Link):

현재 링크 상태는 상세히 표시됩니다. 녹색은 링크가 동작 중임을 나타내며 적색은 링크가 꺼져 있음을 의미합니다.

현재 링크 속도 상태 (Current Link Speed Status):

포트의 현재 링크 속도를 제공합니다.

설정된 링크 속도 (Configured Link Speed):

주어진 스위치 포트의 가능한 링크 속도를 선택합니다. 지정된 포트에 의해 지원되는 속도만 표시합니다. 가능한 속도는 다음과 같습니다:

Disabled – 스위치 포트 동작이 비활성화 됩니다.

Auto – 링크 파트너와 포트 속도 조정 및 링크 파트너와 호환 가능한 가장 높은 속도를 선택합니다.

10Mbps HDX - 10Mbps half duplex 모드에서 cu 포트를 선택합니다.

10Mbps FDX - 10Mbps full duplex 모드에서 cu 포트를 선택합니다.

100Mbps HDX - 100Mbps half duplex 모드에서 cu 포트를 선택합니다.

100Mbps FDX - 100Mbps full duplex 모드에서 cu 포트를 선택합니다.

1Gbps FDX - 1Gbps full duplexFlow 컨트롤에서 포트를 선택합니다.

포트의 자동 속도가 선택되면 이 섹션은 링크 파트너에 전송되는 흐름 제어 기능을 식별합니다.

고정 속도 설정이 선택되면 선택된 것으로 사용됩니다. 현재 Rx 칼럼은 포트의 중지 프레임 준수 여부를 식별하며 현재 Tx 칼럼은 포트의 중지 프레임 전송 여부를 식별합니다. Rx 및 Tx 설정은 마지막 자동-조정 결과에 따라 정의됩니다.

설정된 칼럼을 체크해 흐름 제어를 사용합니다. 이 설정은 설정된 링크 속도에 대한 설정과 관련이 있습니다.

최대 프레임 크기 (Maximum Frame Size)

FCS를 포함한 스위치 포트에 허용되는 최대 프레임을 입력합니다. 범위는 1518-10240 바이트입니다.

## ■ 버튼

새로 고침 (Refresh):

페이지를 즉시 새로 고침 하려면 클릭합니다.

적용 (Apply):

클릭해 변동사항을 저장합니다.

리셋 (Reset):

로컬에서의 변동 사항을 취소하고 저장된 기존 값으로 복구합니다.

## 포트 현황 (Port Statistics)

이 섹션은 포트 현황 정보를 설명하며 모든 스위치 포트에 대한 일반적인 트래픽 현황을 제공합니다.

| Port | Packets  |             | Bytes    |             | Errors   |             | Drops    |             | Filtered |
|------|----------|-------------|----------|-------------|----------|-------------|----------|-------------|----------|
|      | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received |
| 1    | 0        | 0           | 0        | 0           | 0        | 0           | 0        | 0           | 0        |
| 2    | 0        | 0           | 0        | 0           | 0        | 0           | 0        | 0           | 0        |
| 3    | 0        | 0           | 0        | 0           | 0        | 0           | 0        | 0           | 0        |
| 4    | 0        | 0           | 0        | 0           | 0        | 0           | 0        | 0           | 0        |
| 5    | 0        | 0           | 0        | 0           | 0        | 0           | 0        | 0           | 0        |
| 6    | 0        | 0           | 0        | 0           | 0        | 0           | 0        | 0           | 0        |
| 7    | 0        | 0           | 0        | 0           | 0        | 0           | 0        | 0           | 0        |
| 8    | 0        | 0           | 0        | 0           | 0        | 0           | 0        | 0           | 0        |
| 9    | 0        | 0           | 0        | 0           | 0        | 0           | 0        | 0           | 0        |
| 10   | 0        | 0           | 0        | 0           | 0        | 0           | 0        | 0           | 0        |
| 11   | 0        | 0           | 0        | 0           | 0        | 0           | 0        | 0           | 0        |

### 웹 인터페이스

포트 현황 개요를 웹 인터페이스에 표시하려면:

1. 포트 관리 및 포트 현황을 클릭합니다.
2. 자동 새로 고침을 하고자 하면 "자동 새로 고침(Auto-refresh)"를 사용합니다.
3. "Refresh"를 클릭해 포트 현황을 새로 고침 하거나 "Clear"를 클릭해 모든 정보를 지웁니다.
4. 포트 현황의 상세 내용을 보고자 하는 경우 해당 포트를 클릭합니다.

### 항목 설명:

포트 (Port):

같은 열에 포함하는 설정을 위한 논리적 포트입니다.

패킷 (Packets):

포트 당 수신 및 전송된 패킷 수 입니다.

바이트 (Bytes):

포트 당 수신 및 전송된 바이트 수 입니다.



에러 (Errors):

에러에 대해 수신한 프레임의 수 및 포트 당 불완전환 전송 수 입니다.

삭제 (Drops):

내부 또는 출입 혼잡으로 인해 폐기된 프레임 수 입니다.

필터 (Filtered):

포워딩 프로세스로 여과된 수신 프레임의 수 입니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

페이지를 즉시 새로 고침 하려면 클릭합니다.

삭제(Clear):

선택된 포트에 대한 카운터를 삭제합니다.

포트 현황의 상세 내용을 보고자 하는 경우 해당 포트를 클릭합니다. 표시된 카운터는 전체 수신 및 전송, 수신 및 전송 사이즈 카운터, 그리고 수신 및 전송의 에러 카운터입니다.

| Detailed Port Statistics Port 26                            |         |                         |          |
|---|---------|-------------------------|----------|
| Auto-refresh <input type="checkbox"/> Refresh Clear Port 26 |         |                         |          |
| Receive Total   |         | Transmit Total          |          |
| Rx Packets  | 10753   | Tx Packets              | 163345   |
| Rx Octets   | 1673896 | Tx Octets               | 13699853 |
| Rx Unicast  | 5945    | Tx Unicast              | 6756     |
| Rx Multicast  | 3430    | Tx Multicast            | 5075     |
| Rx Broadcast  | 1378    | Tx Broadcast            | 151514   |
| Rx Pause  | 0       | Tx Pause                | 0        |
| Receive Size Counters                                       |         | Transmit Size Counters  |          |
| Rx 64 Bytes   | 4397    | Tx 64 Bytes             | 148340   |
| Rx 65-127 Bytes   | 3452    | Tx 65-127 Bytes         | 11290    |
| Rx 128-255 Bytes  | 1468    | Tx 128-255 Bytes        | 333      |
| Rx 256-511 Bytes  | 101     | Tx 256-511 Bytes        | 1408     |
| Rx 512-1023 Bytes   | 1335    | Tx 512-1023 Bytes       | 83       |
| Rx 1024-1526 Bytes  | 0       | Tx 1024-1526 Bytes      | 1891     |
| Rx 1527- Bytes  | 0       | Tx 1527- Bytes          | 0        |
| Receive Queue Counters                                      |         | Transmit Queue Counters |          |
| Rx Q0   | 10753   | Tx Q0                   | 15072    |
| Rx Q1   | 0       | Tx Q1                   | 0        |
| Rx Q2   | 0       | Tx Q2                   | 0        |
| Rx Q3   | 0       | Tx Q3                   | 0        |
| Rx Q4   | 0       | Tx Q4                   | 0        |
| Rx Q5   | 0       | Tx Q5                   | 0        |
| Rx Q6   | 0       | Tx Q6                   | 0        |
| Rx Q7   | 0       | Tx Q7                   | 148273   |
| Receive Error Counters                                      |         | Transmit Error Counters |          |
| Rx Drops  | 0       | Tx Drops                | 0        |
| Rx CRC/Alignment  | 0       | Tx Late/Exc. Coll.      | 0        |
| Rx Undersize  | 0       |                         |          |
| Rx Oversize   | 0       |                         |          |
| Rx Fragments  | 0       |                         |          |
| Rx Jabber   | 0       |                         |          |
| Rx Filtered   | 3174    |                         |          |

## ■ 항목 설명:

상단 좌측 스크롤바:

포트 현황을 "Port-1", "Port-2", ... 같이 표시할 포트를 스크롤 합니다.

### 수신 합계 및 전송 합계

Rx 및 Tx 패킷 (Rx and Tx Packets):

수신 및 전송 (좋은 및 나쁨) 패킷을 수 입니다.

Rx 및 Tx 바이트 수 (Rx and Tx Octets):

수신 및 전송 (좋은 및 나쁨) 바이트 수 입니다. FCS를 포함하지만 프레임링 비트는 제외합니다.

Rx 및 Tx 유니캐스트 (Rx and Tx Unicast):

수신 및 전송 (좋은 및 나쁨) 유니캐스트 패킷 수 입니다.

Rx 및 Tx 멀티캐스트 (Rx and Tx Multicast):

수신 및 전송 (좋은 및 나쁨) 멀티캐스트 패킷 수 입니다.

Rx 및 Tx 브로드캐스트 (Rx and Tx Broadcast):

수신 및 전송 (좋은 및 나쁨) 브로드캐스트 패킷 수 입니다.

Rx 및 Tx 중지 (Rx and Tx Pause):

중지 동작을 표시하는 연산 코드가 있는 이 포트에 대한 수신 또는 전송된 MAC 컨트롤 프레임 수 입니다.

#### **크기 카운터 수신 및 전송 (Receive and Transmit Size Counters)**

수신 및 전송 (좋은 및 나쁨) 패킷 수는 각각의 프레임 크기를 기반으로 카테고리를 분리합니다.

#### **에러 카운터 수신 (Receive Error Counters):**

Rx 삭제 (Rx Drops):

버퍼 또는 출력 혼잡 수신 부족으로 인해 삭제된 프레임 수 입니다.

Rx CRC/정렬 (Rx CRC/Alignment):

CRC 또는 정렬 에러를 수신하는 프레임 수 입니다.

Rx 크기 축소 (Rx Undersize):

유효한 CRC를 수신하는 짧은 1 프레임의 수 입니다.

Rx 크기 확대 (Rx Oversize):

유효한 CRC를 수신하는 긴 2 프레임의 수 입니다.

Rx 프래그먼트 (Rx Fragments):

유효하지 않은 CRC를 수신하는 짧은 1 프레임의 수 입니다.

Rx Jabber:

유효하지 않은 CRC를 수신하는 긴 2 프레임의 수 입니다.

#### **에러 카운터 전송**

Tx Drops:

출력 버퍼 혼잡으로 인해 삭제된 프레임 수 입니다.

Tx Late/Exc. Coll.:

과도하거나 늦은 충돌로 인해 삭제된 프레임 수 입니다.

Tx 크기 확대 (Tx Oversize):

프레임 크기 확대로 인해 삭제된 프레임의 수 입니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

페이지를 즉시 새로 고침 하려면 클릭합니다.

삭제(Clear):

선택된 포트에 대한 카운터를 삭제합니다.

## SFP 포트 정보 (SFP Port Info)

이 섹션은 스위치가 스위치에 연결하는 SFP 모듈의 상세 정보 표시하는 것을 설정합니다. 정보는 다음을 포함합니다: 커넥터 타입, 광섬유 타입, 파장, 비트 속도 및 벤더 OUT 등

|                       |      |
|-----------------------|------|
| Connector Type        | none |
| Fiber Type            | none |
| Tx Central Wavelength | none |
| Bit Rate              | none |
| Vendor OUI            | none |
| Vendor Name           | none |
| Vendor P/N            | none |
| Vendor Revision       | none |
| Vendor Serial Number  | none |
| Data Code             | none |
| Temperature           | none |
| Vcc                   | none |
| Mon1 (Bias)           | none |
| Mon2 (TX PWR)         | none |
| Mon3 (RX PWR)         | none |

## ■ 항목 설명:

상단 좌측 스크롤바:

어느 포트의 포트 현황을 표시할지 포트 현황을 스크롤 합니다.

커넥터 타입 (Connector Type)::

커넥터 타입, 예를 들어, UTP, SC, ST, LC 등을 표시합니다.

광섬유 타입 (Fiber Type):

멀티-모드, 싱글-모드와 같은 광섬유 모드를 표시합니다.

Tx 중앙 파장 (Tx Central Wavelength):

중앙 파장, 예를 들어 850nm, 1310nm, 1550nm 등을 전송하고 있는 광섬유를 표시합니다.

비트 속도 (Bit Rate):

트랜스미버의 명목상 비트 속도를 표시합니다.

벤더 OUI (Vendor OUI):

EEED에 의해 할당된 제조자의 OUI 코드를 표시합니다.

벤더 이름 (Vendor Name):

모듈 제조자의 회사 이름을 표시합니다.

벤더 P/N (Vendor P/N):

모듈 제조자에 의해 생성된 제품 이름을 표시합니다.

벤더 수정 (Vendor Rev (Revision)):

모듈 수정을 표시합니다.

벤더 SN (Vendor SN (시리얼 번호)):

제조자에 의해 지정된 시리얼 번호를 표시합니다.

날짜 코드 (Date Code):

이 SFP 모듈이 생성된 날짜를 표시합니다.

온도 (Temperature):

SFP 모듈의 현재 온도를 표시합니다.

Vcc:

SFP 모듈의 동작 중인 DC 전압을 표시합니다.

Mon1(Bias) mA:

SFP 모듈의 Bias 전류를 표시합니다.

Mon2(TX PWR):

SFP 모듈의 전송 전력을 표시합니다.

Mon3(RX PWR):

SFP 모듈의 수신기 전원을 표시합니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

페이지를 즉시 새로 고침 하려면 클릭합니다.

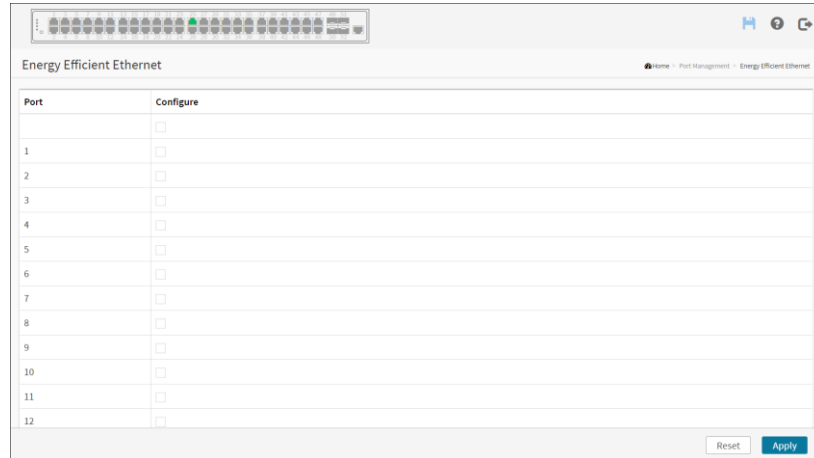
## 에너지 효율 이더넷 (Energy Efficient Ethernet)

EEE는 IEEE 802.3az에서 정의한 에너지 효율 이더넷의 축약형입니다.

이 페이지에서 유저는 현재 EEE 포트 설정을 감시하고 설정할 수 있습니다.

매우 낮은 트래픽 사용 (또는 트래픽 없음)이 있는 경우 EEE는 전력 사용을 줄이는 전력 절감 옵션입니다.

트래픽이 없을 때 EEE는 서킷의 전력을 저하시키며 동작합니다. 포트가 전송되는 데이터를 얻 으면 모든 서킷에 전력이 동작합니다. 서킷에 전력을 작동하는데 걸리는 시간은 wakeup-time 이라고 합니다. 기본 wakeup-time 시간은 1Gbit 링크에 17 us 및 다른 링크 속도에 30 us입니 다. 트래픽 전송 시 수신 및 전송 장치가 전원이 켜진 모든 서킷을 가지고 있는지 확인하기 위 해 EEE 장치가 wakeup-time 값에 동의해야 합니다. 장치는 LLDP 프로토콜을 사용하는 장치 wakeup-time에 대한 정보를 교환할 수 있습니다.



### 웹 인터페이스

웹 인터페이스에서 에너지 효율 이더넷을 설정하려면:

1. 포트 관리 및 에너지 효율 이더넷을 클릭합니다.
2. 에너지 효율 이더넷을 포트에 활성화 또는 비활성화 합니다.
3. 설정을 저장하려면 적용을 클릭합니다.
4. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아갑니다.

### ■ 항목 설명:

포트 (Port):

논리적인 EEE 포트의 스위치 포트 번호입니다.

설정 (Configure):

이 스위치 포트의 EEE가 활성화 되도록 제어합니다.

버튼 (Buttons)

적용 (Apply):

변경을 저장하려면 클릭합니다.

리셋 (Reset):

클릭해 로컬의 변동사항을 취소하고 이전에 저장된 값으로 되돌립니다.

## 링크 집계 (Link Aggregation)

### 정적 구성

이 페이지는 집계 해시 모드 및 집계 그룹을 설정하도록 사용됩니다.

### 웹 인터페이스

웹 인터페이스에서 집계 해시 모드 및 집계 그룹을 설정하려면:

1. 포트 관리, 링크 집계 및 정적 설정을 클릭합니다.
2. 집계 모드 기능을 활성화 및 비활성화 합니다.
3. 집계 그룹 ID 및 포트 번호를 호출합니다.
4. 적용을 클릭해 설정을 저장합니다.
5. 설정을 취소하려면 리셋 버튼을 클릭 합니다. 이전에 저장된 값으로 되돌아갑니다.

### ■ 항목 설명:

#### 해시 코드 제공자 (Hash Code Contributors)

소스 MAC 주소 (Source MAC Address):

소스 MAC 주소는 프레임의 대상 포트를 측정하기 위해 사용할 수 있습니다. 체크해 소스 MAC 주소 사용을 활성화 하거나 체크를 해제해 비활성화 합니다. 기본값은 소스 MAC 주소는 활성화 입니다.



대상 MAC 주소 (Destination MAC Address):

대상 MAC 주소는 프레임의 대상 포트를 측정하기 위해 사용할 수 있습니다. 체크해 소스 MAC 주소 사용을 활성화 하거나 체크를 해제해 비활성화 합니다. 기본값은 소스 MAC 주소는 활성화 입니다.

IP 주소 (IP Address):

IP 주소는 프레임의 대상 포트를 측정하기 위해 사용할 수 있습니다. 체크해 IP 주소 사용을 활성화 하거나 체크를 해제해 비활성화 합니다. 기본값은 IP 주소 활성화입니다.

TCP/UDP 포트 번호 (TCP/UDP Port Number):

TCP/UDP 포트 번호는 대상 포트를 측정하기 위해 사용할 수 있습니다. 체크해 TCP/UDP 포트 번호 사용을 활성화 하거나 체크를 해제해 비활성화 합니다. 기본값은 TCP/UDP 포트 번호 활성화 입니다.

### 집계 그룹 설정 (Aggregation Group Configuration)

그룹 ID (Group ID):

동일한 열에 포함된 설정에 대한 그룹 ID를 식별합니다. 그룹 ID "Normal"은 집합체가 아님을 표시합니다. 그룹 ID만이 포트 별로 유효합니다.

포트 멤버 (Port Members):

각 스위치 포트는 각 그룹 ID에 대한 목록입니다. 집계의 포트를 포함하기 위한 라디오 버튼을 선택합니다. 또는 집계에서 포트를 삭제하기 위해 라디오 버튼을 삭제합니다. 기본값으로 모든 집계 그룹에 속한 포트는 없습니다. 전체 듀플렉스 포트만 집계에 속할 수 있으며 포트는 각 그룹에 동일한 속도로 설정되어야 합니다.

### ■ 버튼 (Buttons)

적용 (Apply):

변경을 저장하려면 클릭합니다.

리셋 (Reset):

클릭해 로컬의 변동사항을 취소하고 이전에 저장된 값으로 되돌립니다.

## LACP 설정 (LACP Configuration)

이 페이지에서 유저는 현재 LACP 포트 설정을 검사 및 변경이 가능합니다.

| Port | LACP Enabled             | Key | Role   | Timeout | Prio  |
|------|--------------------------|-----|--------|---------|-------|
| *    | <input type="checkbox"/> |     |        |         | 32768 |
| 1    | <input type="checkbox"/> |     | Active | Fast    | 32768 |
| 2    | <input type="checkbox"/> |     | Active | Fast    | 32768 |
| 3    | <input type="checkbox"/> |     | Active | Fast    | 32768 |
| 4    | <input type="checkbox"/> |     | Active | Fast    | 32768 |
| 5    | <input type="checkbox"/> |     | Active | Fast    | 32768 |
| 6    | <input type="checkbox"/> |     | Active | Fast    | 32768 |
| 7    | <input type="checkbox"/> |     | Active | Fast    | 32768 |
| 8    | <input type="checkbox"/> |     | Active | Fast    | 32768 |
| 9    | <input type="checkbox"/> |     | Active | Fast    | 32768 |
| 10   | <input type="checkbox"/> |     | Active | Fast    | 32768 |

### 웹 인터페이스

웹 인터페이스에서 LACP 포트 설정을 하려면:

1. 포트 관리, 링크 집계 및 LACP 설정을 클릭합니다.
2. 스위치 포트의 LACP를 활성화 또는 비활성화 합니다.
3. 키 항목을 자동 또는 지정으로 스크롤 합니다. 기본값은 자동입니다.
4. Active 또는 Passive로 기능을 스크롤 합니다. 기본값은 동적입니다.
5. 적용을 클릭해 설정을 저장합니다.
6. 설정을 취소하려면 리셋 버튼을 클릭 합니다. 이전에 저장된 값으로 되돌아갑니다.

### ■ 항목 설명:

포트 (Port):

스위치 포트 번호입니다.

LACP 활성화 (LACP Enabled):

LACP가 이 스위치 포트에서 활성화 상태인지 제어합니다. 2 이상의 포트가 동일한 파트너에 연결된 경우 LACP는 집합체를 구성합니다.

키 (Key):

포트에 의해 발생된 키 값은 1-65535입니다. 자동 설정은 물리적 링크 속도 10Mb = 1, 100Mb = 2, 1Gb = 3로 올바른 키를 설정합니다. 특정 설정을 사용해 유저 정의 값을 입력할 수 있습니다. 동일한 키 값의 포트는 같은 집계 그룹에 속할 수 있으며 다른 키의 포트는 할 수 없습니다.

기능 (Role):

기능은 LACP 동작 상태를 표시합니다. Active는 매 초 LACP 패킷을 전송합니다. 반면 Passive는 파트너로부터 LACP 패킷을 기다립니다.

타임아웃 (Timeout):

타임아웃은 BPDU 전송 사이의 시간을 제어합니다. Fast는 매 초 LACP 패킷을 전송하며 Slow는 LACP 패킷 전송 전에 30초를 기다립니다.

Prio:

Prio는 포트의 우선권을 제어합니다. LACP 파트너가 본래보다 이 장치에 의해 더 큰 그룹을 형성하고자 하면, 이 항목은 동작할 포트와 백업 기능에 속할 포트를 선택합니다. 낮은 번호일수록 더 큰 우선권을 의미합니다.

## ■ 버튼 (Buttons)

적용 (Apply):

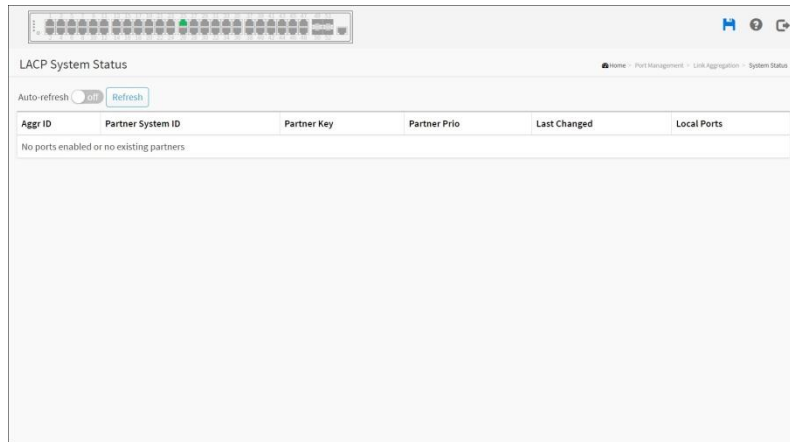
변경을 저장하려면 클릭합니다.

리셋 (Reset):

클릭해 로컬의 변동사항을 취소하고 이전에 저장된 값으로 되돌립니다.

## 시스템 상태 (System Status)

이 섹션은 스위치의 LACP 기능을 설정을 완료 모든 LACP 경우의 현황 개요 제공을 표시합니다.



웹 인터페이스

웹 인터페이스에서 LCAP 시스템 상태를 표시하려면:

1. 포트 관리, 링크 집계 및 시스템 상태를 클릭합니다.
2. "자동 새로 고침"을 체크합니다.
3. "새로 고침"을 클릭해 포트 상세 현황을 새로 고칩니다.

### ■ 항목 설명:

Aggr ID:

이 집계 사계와 관련된 집계 ID입니다. 'isid: aggr-id'로 표시되는 LLAG의 경우 id는 'isid: aggr-id'로 GLAG는 'aggr-id'입니다.

파트너 시스템 (Partner System ID):

집계 파트너의 시스템 ID (MAC 주소)입니다.

파트너 키 (Partner Key):

이 집계 ID에 할당된 파트너 키입니다.

파트너 Prio (Partner Prio):

이 집계 ID에 할당된 파트너 우선권입니다.

마지막 변경 (Last changed):

이 집계가 변경된 이후 시간입니다.

로컬 포트 (Local Ports):

포트가 이 스위치의 집계인지를 표시합니다. 포맷은 다음과 같습니다:

"Switch ID:Port".

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

페이지를 즉시 새로 고침 하려면 클릭합니다.

## 내부상태 (Internal Status)

이 페이지는 모든 포트에 대한 LACPinternal(즉, 로컬 시스템) 상태의 상태 개요를 제공합니다. LACP 그룹의 일부인 포트만 표시됩니다. 표시된 항목의 상세 내용은 IEEE 801.AX-2014를 참조하십시오.

| Port                  | State | Key | Priority | Activity | Timeout | Aggregation | Synchronization | Collecting | Distributing | Defaulted | Expired |
|-----------------------|-------|-----|----------|----------|---------|-------------|-----------------|------------|--------------|-----------|---------|
| No LACP ports enabled |       |     |          |          |         |             |                 |            |              |           |         |

웹 인터페이스

웹 인터페이스의 LACP 내부시스템 상태를 표시하려면:

1. 포트 관리, 링크 집계 및 내부상태를 클릭합니다.
2. "자동 새로 고침"을 체크합니다.

3. “새로 고침”을 클릭해 포트 상세 현황을 새로 고침 합니다.

## ■ 항목 설명:

포트 (Port):

스위치 포트 번호입니다.

상태 (State):

현재 포트 상태 (The current port state):

Down: 포트가 동작하지 않습니다.

Active: 포트가 동작 상태입니다.

Standby: 포트가 대기 상태입니다.

Key: 이 포트에 할당된 키입니다. 동일한 키의 포트만 함께 결합합니다.

우선권 (Priority):

이 집계 그룹에 할당된 우선권입니다.

동작 (Activity):

그룹의 LACP 모드입니다. (Fast 또는 Slow)

집합체 (Aggregation):

시스템이 이 링크가 “aggregateable”가 되도록 고려할지 나타냅니다. 즉, 집합체의 가능한 후보입니다.

동기화 (Synchronization):

시스템이 이 링크가 “IN\_SYNC”가 되도록 고려할지 나타냅니다; 즉 맞는 LAG에 할당되어 있습니다. 그룹은 compatiXBFe Aggregator와 관련되어 있습니다. 또한 LAG 식별은 시스템 ID와 전송된 동작 키 정보와 일치합니다.

수집 (Collecting):

이 링크의 입력 프레임 수집이 활성화 상태임을 나타냅니다.

분배 (Distributing):

이 링크의 출력 프레임 분배가 활성화 상태임을 나타냅니다.

초기화 됨 (Defaulted):

Actor's Receive 기계가 초기화 된 동작상 파트너 정보를 사용하는지 표시합니다.

만료 (Expired):

Actor's Receive 기계가 만료 상태인지 나타냅니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

페이지를 즉시 새로 고침 하려면 클릭합니다.

## Neighbor 상태 (Neighbor Status)

이 페이지는 모든 포트의 LACP Neighbor 상태에 대한 상태 개요를 제공합니다. LACP 그룹의 부분인 포트만 표시됩니다. 표시된 항목에 대한 상세 내용은 IEEE 801.AX-2014를 참조하십시오.

<

## 웹 인터페이스

웹 인터페이스에서 LCAP Neighbor 포트 상태를 표시하려면:

1. 포트 관리, 링크 집합체 및 Neighbor 상태를 클릭합니다.

2. "자동 새로 고침"을 체크합니다.
3. "새로 고침"을 클릭해 포트 상세 현황을 새로 고침 합니다.

## ■ 항목 설명:

Aggr ID:

포트가 할당된 집합체 그룹입니다.

포트 (Port):

스위치 포트 번호 입니다.

상태 (State):

현재 포트 상태입니다.

Down: 포트가 동작하지 않습니다.

Active: 포트가 동작 상태입니다.

Standby: 포트가 대기 상태입니다.

파트너 키 (Partner Key): 파트너에 의해 이 포트에 할당된 키입니다.

파트너 포트 (Partner Port): 이 링크에 관련된 파트너 포트 번호입니다.

파트너 포트 우선권 (Partner Port Priority): 이 파트너 포트에 할당된 우선권입니다.

동작 (Activity): 그룹의 LACP 모드입니다. (Active 또는 Passive)

타임아웃 (Timeout):

포트에 설정된 타임아웃 모드입니다. (Fast 또는 Slow)

집합체 (Aggregation):

시스템이 이 링크가 "aggregateable"가 되도록 고려할지 나타냅니다. 즉, 집합체의 가능한 후보입니다.

동기화 (Synchronization):

시스템이 이 링크가 "IN\_SYNC"가 되도록 고려할지 나타냅니다; 즉 맞는 LAG에 할당되어 있습니다. 그룹은 compatiXBFe Aggregator와 관련되어 있습니다. 또한 LAG 식별은 시스템 ID와 전송된 동작 키 정보와 일치합니다.



수집 (Collecting):

이 링크의 입력 프레임 수집이 활성화 상태임을 나타냅니다.

분배 (Distributing):

이 링크의 출력 프레임 분배가 활성화 상태임을 나타냅니다.

초기화 됨 (Defaulted):

Actor's Receive 기계가 초기화 된 동작상 파트너 정보를 사용하는지 표시합니다.

만료 (Expired):

Actor's Receive 기계가 만료 상태인지 나타냅니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

페이지를 즉시 새로 고침 하려면 클릭합니다.

## 포트 상태 (Port Status)

이 섹션은 스위치의 LACP 기능을 완료할 때 모든 LACP 경우에 대한 포트 상태 개요를 제공하는 것에 대한 내용을 설명합니다.

LACP Status

Auto-refresh ☐ Refresh

| Port | LACP | Key | Aggr ID | Partner System ID | Partner Port | Partner Prio |
|------|------|-----|---------|-------------------|--------------|--------------|
| 1    | No   | -   | -       | -                 | -            | -            |
| 2    | No   | -   | -       | -                 | -            | -            |
| 3    | No   | -   | -       | -                 | -            | -            |
| 4    | No   | -   | -       | -                 | -            | -            |
| 5    | No   | -   | -       | -                 | -            | -            |
| 6    | No   | -   | -       | -                 | -            | -            |
| 7    | No   | -   | -       | -                 | -            | -            |
| 8    | No   | -   | -       | -                 | -            | -            |
| 9    | No   | -   | -       | -                 | -            | -            |
| 10   | No   | -   | -       | -                 | -            | -            |
| 11   | No   | -   | -       | -                 | -            | -            |
| 12   | No   | -   | -       | -                 | -            | -            |
| 13   | No   | -   | -       | -                 | -            | -            |
| 14   | No   | -   | -       | -                 | -            | -            |

## 웹 인터페이스

웹 인터페이스에서 LACP 포트 상태를 표시하려면:

1. 포트 관리, 링크 집합체 및 포트 상태를 클릭합니다.
2. 정보를 자동 새로 고침 하려면 "자동 새로 고침"을 사용합니다.
3. "새로 고침"을 클릭해 LACP 포트 상태를 새로 고침 합니다.

## ■ 항목 설명:

포트 (Port):

스위치 포트 번호입니다.

LACP:

'Yes'는 LACP가 활성화 되었으며 포트 링크가 Up 상태임을 뜻합니다. 'No'는 LACP가 활성화 되어 있지 않거나 링크가 down 상태임을 뜻합니다. 'Backup'은 포트가 집합체 그룹에 속하지 못함을 뜻하지만 다른 포트가 그룹에서 나가면 속하게 됩니다. LACP 상태는 비활성화 입니다.

키 (Key):

이 포트에 할당된 키입니다. 동일한 키의 포트만이 함께 집합체가 될 수 있습니다.

Aggr ID:

이 집합체 그룹에 할당된 집합체 ID입니다. ID 1과 2는 GLAG이며 ID 3-14는 LLAG입니다.

파트너 시스템 ID (Partner System ID):

파트너 시스템 ID입니다. (MAC 주소)

파트너 포트 (Partner Port):

이 포트에 연결된 파트너의 포트 번호입니다.

파트너 Prio (Partner Prio):

파트너의 포트 우선권입니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

페이지를 즉시 새로 고침 하려면 클릭합니다.

## 루프 프로텍션 (Loop Protection)

### 설정

루프 프로텍션은 트래픽을 탐지하는데 사용됩니다. 스위치가 포트와 동일한 패킷의(루핑 탐지 프레임) MAC 주소를 수신하는 경우 루프 프로텍션이 동작하는 것을 나타냅니다. 포트는 루핑 프로텍션 프레임을 수신할 때 잠기게 됩니다. 잠긴 포트를 다시 사용하려면 루핑 경로를 찾고 루핑 경로에서 벗어난 후 잠긴 포트 재개를 선택합니다. 그리고 "Resume"을 클릭해 잠긴 포트를 켵니다.

| Port | Enable                              | Action        | Tx Mode |
|------|-------------------------------------|---------------|---------|
| *    | <input checked="" type="checkbox"/> | <>            | <>      |
| 1    | <input checked="" type="checkbox"/> | Shutdown Port | Enable  |
| 2    | <input checked="" type="checkbox"/> | Shutdown Port | Enable  |
| 3    | <input checked="" type="checkbox"/> | Shutdown Port | Enable  |
| 4    | <input checked="" type="checkbox"/> | Shutdown Port | Enable  |

### 웹 인터페이스

웹 인터페이스에서 루프 프로텍션 항목을 설정하려면:

1. 포트 관리, 루프 프로텍션 및 설정
2. 포트 루프 프로텍션 활성화 또는 비활성화를 선택합니다.
3. 적용을 클릭해 설정을 저장하십시오.
4. 설정을 취소하려면 리셋 버튼을 클릭 합니다. 이전에 저장된 값으로 되돌아갑니다.

### ■ 항목 설명:

#### 글로벌 설정 (Global Configuration)

루프 프로텍션 활성화 (Enable Loop Protection):

루프 프로텍션 활성화 여부를 제어합니다. (전체)

전송 시간 (Transmission Time):

각 포트상에 전송된 각 루프 프로텍션 PDU 사이의 간격입니다. 유효 값은 1에서 10초입니다.

셴다운 시간 (Shutdown Time):

루프가 탐지될 때 포트가 비활성화를 유지하는 기간입니다. (초 단위) 유효 값은 10 ~ 604800초입니다. (7일)

### **포트 설정 (Port Configuration)**

포트 (Port):

포트의 스위치 포트 번호입니다.

활성화 (Enable):

루프 프로텍션이 이 스위치 포트에서 활성화 되는지 여부를 제어합니다.

동작 (Action):

루프가 포트 상에서 탐지되면 실행된 동작을 설정합니다. 유효 값은 셴다운 포트, 셴다운 포트 및 로그 또는 로그만 입니다.

Tx 모드 (Tx Mode) :

포트가 능동적으로 루프 프로텍션 PUD 실행 중 인지 또는 수동적으로 루프 PDU를 찾고 있는지를 제어 합니다.

### **■버튼**

적용 (Apply):

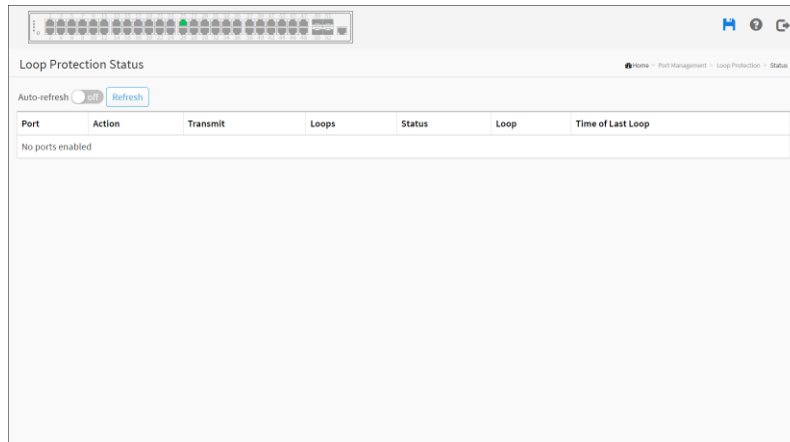
클릭해 설정을 저장합니다.

리셋 (Reset):

로컬에서의 변동 사항을 취소하고 저장된 기존 값으로 복구합니다.

## 상태 Status

이 섹션은 현재 선택된 스위치의 포트의 루프 프로텍션 포트 상태를 표시합니다.



웹 인터페이스

웹 인터페이스의 루프 프로텍션 상태를 표시하려면:

1. 포트 관리, 루프 프로텍션 및 상태를 클릭합니다.
2. 정보를 자동 새로 고침 하려면 "자동 새로 고침"을 사용합니다.
3. "새로 고침"을 클릭해 루프 프로텍션 상태를 새로 고침 합니다.

### ■ 항목 설명:

포트 (Port):

논리적 포트의 스위치 포트 번호입니다.

동작 (Action):

현재 설정된 포트 동작입니다.

전송 (Transmit):

현재 설정된 포트 전송 모드입니다.

루프 개수 (Loops):

이 포트에 탐지된 루프의 수 입니다.

상태 (Status):

포트의 현재 루프 프로텍션 상태입니다.

루프 (Loop):

포트에 루프 탐지 여부입니다.

마지막 루프 시간 (Time of Last Loop):

마지막 루프 이벤트가 탐지된 시간입니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

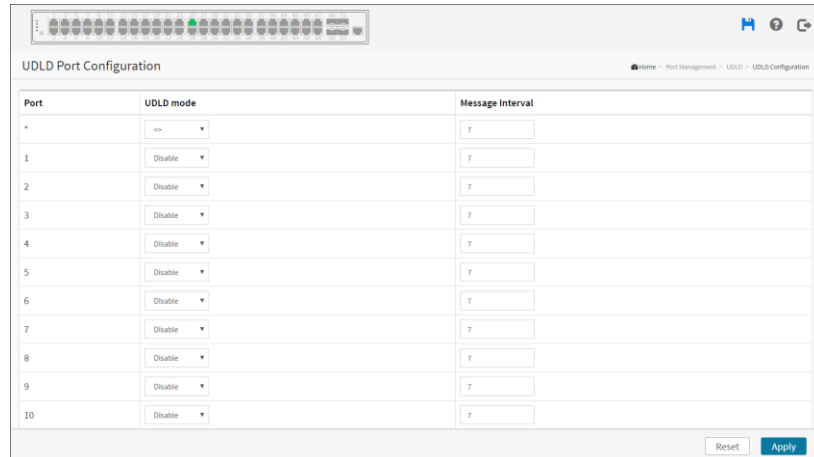
새로 고침 (Refresh):

페이지를 즉시 새로 고침 하려면 클릭합니다.

# UDLD

## UDLD 설정 (UDLD Configuration)

이 페이지에서 유저는 현재 UDLD 설정을 검사하고 변경이 가능합니다.



The screenshot shows the 'UDLD Port Configuration' web interface. At the top, there is a breadcrumb trail: 'Home > Port Management > UDLD > UDLD Configuration'. Below this is a table with three columns: 'Port', 'UDLD mode', and 'Message interval'. The 'Port' column lists ports from 1 to 10. The 'UDLD mode' column has a dropdown menu for each port, currently set to 'Disable'. The 'Message interval' column has a text input field for each port, currently set to '7'. At the bottom right of the table, there are 'Reset' and 'Apply' buttons.

| Port | UDLD mode | Message interval |
|------|-----------|------------------|
| *    | <>        | 7                |
| 1    | Disable   | 7                |
| 2    | Disable   | 7                |
| 3    | Disable   | 7                |
| 4    | Disable   | 7                |
| 5    | Disable   | 7                |
| 6    | Disable   | 7                |
| 7    | Disable   | 7                |
| 8    | Disable   | 7                |
| 9    | Disable   | 7                |
| 10   | Disable   | 7                |

### 웹 인터페이스

웹 인터페이스에서 UDLD 항목을 설정하려면:

1. 포트 관리, UDLD 및 UDLD 설정을 클릭합니다.
2. 포트 UDLD를 활성화 또는 비활성화 합니다.
3. 메시지 간격을 지정합니다.
4. 설정을 저장하려면 적용을 클릭하세요.
5. 설정을 취소하려면 리셋 버튼을 클릭 합니다. 이전에 저장된 값으로 되돌아갑니다.

### ■ 항목 설명:

포트 (Port):

스위치 포트 번호입니다.

UDLD 모드 (UDLD Mode):

포트의 UDLD 모드를 설정합니다. 유효 값은 Disable, Normal 그리고 Aggressive 입니다. 기본 모드는 Disable 입니다.



Disable” 비활성화 모드에서 UDLD 기능은 포트에 존재하지 않습니다.

Normal: 정상 모드에서는 포트의 링크 상태가 단방향으로 지정되었다면 포트 상태에 영향을 미치지 않습니다.

Aggressive: 단방향으로 탐지된 포트는 셧다운 됩니다. 포트를 다시 동작하려면 해당 포트의 UDLD를 비활성화 합니다.

메시지 간격 (Message Interval):

알림 단계에 있으며 양방향으로 지정된 포트의 UDLD 탐색 메시지 간 시간을 설정합니다. 범위는 7에서 90초입니다. (기본값은 7초입니다.) (RFC 5171의 상세 정보 부족으로 인해 현재 기본 시간 간격이 지원됩니다.)

## ■ 버튼

적용 (Apply):

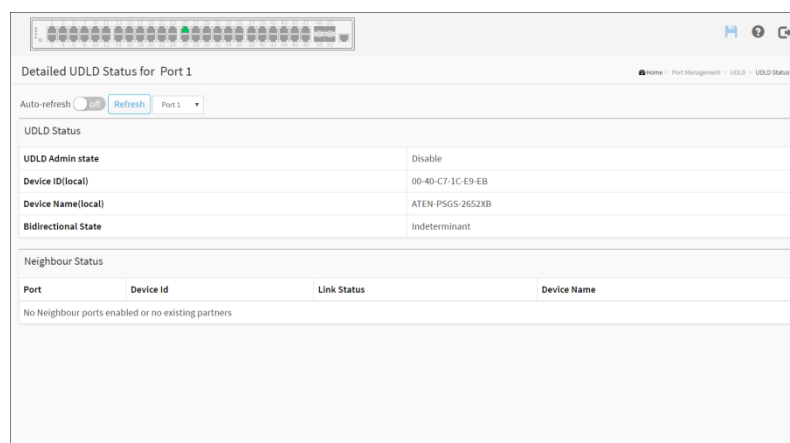
클릭해 설정을 저장합니다.

리셋 (Reset):

로컬에서의 변동 사항을 취소하고 저장된 기존 값으로 복구합니다.

UDLD 상태 (UDLD Status)

이 페이지는 포트의 UDLD 상태를 표시합니다.



웹 인터페이스

웹 인터페이스에서 루프 프로텍션을 표시하려면:

1. 포트 관리, UDLD 및 UDLD 상태를 클릭합니다.

2. UDLD 상태를 표시하고자 하는 포트를 선택합니다.
3. 정보를 자동 새로 고침 하려면 "자동 새로 고침"을 사용합니다.
4. "새로 고침"을 클릭해 루프 프로텍션 상태를 새로 고침 합니다.

## ■ 항목 설명:

UDLD 포트 상태 (UDLD port status)

UDLD 관리자 상태 (UDLD Admin State):

물리적 포트의 현재 포트 상태입니다. Normal 또는 Aggressive 상태가 활성화 되면 활성화 된 것 입니다.

장치 ID (로컬) Device ID(local): 장치의 ID 입니다.

장치 이름 (로컬) Device Name(local): 장치의 이름입니다.

양방향 상태 (Bidirectional State): 포트의 현재 상태입니다.

## Neighbor 상태 (Neighbor Status)

포트 (Port):

Neighbor 장치의 현재 포트입니다.

장치 ID (Device ID):

Neighbor 장치의 현재 ID 입니다.

링크 상태 (Link Status):

Neighbor 포트의 현재 링크 상태입니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

페이지를 즉시 새로 고침 하려면 클릭합니다.

포트 1 (Port 1):

DHCP 상세 현황을 표시하고자 하는 포트를 클릭합니다.

이 페이지는 의도적으로 비워 두었습니다.

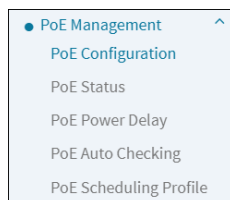
# PoE 매니지먼트 (ES0152P에 한함)

## 개요

---

PoE는 Power over Ethernet의 줄임말입니다. Power over Ethernet은 전력을 표준 이더넷 케이블을 통해 원격 장치에 전송하는데 사용됩니다. 예를 들어, 메인 전원 공급에 장비를 연결하기 어렵거나 비용이 많이 드는 IP 전화, 무선 LAN 액세스 포인트 및 기타 장치에 전원을 공급합니다.

메뉴는 다음과 같습니다:



## PoE 설정

이 페이지에서 유저는 현재 PoE 포트 설정을 검사 및 구성하고 모든 PoE Supply W를 표시합니다.

PoE Configuration

Reserved Power determined by: ☐ Class ☒ Allocation ☐ LLDP-Med

Power Management Mode: ☒ Actual Consumption ☐ Reserved Power

Capacitor Detection: ☐

PoE Power Supply Configuration

PoE Firmware Version: 012-001

Primary Power Supply [W]: 740

PoE Port Configuration

| Port | PoE Mode | PoE Schedule | Priority | Maximum Power [W] | Delay Mode | Delay Time(0-300 sec) |
|------|----------|--------------|----------|-------------------|------------|-----------------------|
| *    | <>       | <>           | <>       | 30                | <>         | 0                     |
| 1    | Enabled  | Disabled     | Low      | 30                | Disabled   | 0                     |
| 2    | Enabled  | Disabled     | Low      | 30                | Disabled   | 0                     |

Reset Apply

### 웹 인터페이스

웹 인터페이스에서 Power over Ethernet을 설정하려면:

1. PoE 관리 및 PoE 설정을 클릭합니다.
2. 정의된 예비 전력을 지정합니다.
3. PoE 또는 PoE+ 모드 스케줄, 우선권, 최대 전력(W), 지연 모드 및 지연 시간을 지정합니다.
4. 적용을 클릭해 설정을 저장합니다.
5. 설정을 취소하려면 리셋 버튼을 클릭 합니다. 이전에 저장된 값으로 되돌아갑니다.

### ■ 항목 설명:

#### Power Over Ethernet 설정 (Power Over Ethernet Configuration)

정의된 예비 전력 (Reserved Power determined by):

포트/PD 예비 전력 설정 방법에는 3가지 모드가 있습니다.

1. Allocated mode: 이 모드에서 유저는 각 포트가 비축하고 있는 전력을 할당합니다. 각 포트 /PD에 대한 할당된/비축된 전력은 최대 전력 필드에서 지정됩니다.

2. Class mode: 이 모드에서 각 포트는 연결된 PD에 따라 얼마나 많은 전력을 비축할지 자동으로 정의해 그에 따라 전력을 비축합니다. 4개의 다른 포트 클래스가 존재하며 1/4, 7, 15.4 또는 30와트 입니다.

이 모드에서 최대 전력 필드는 적용되지 않습니다.

3. LLDP-MED mode: 이 모드는 Class 모드와 비슷하며, LLDP 프로토콜을 사용한 PoE 정보를 교환함으로써 각 포트는 비축하는 전력량을 지정하며 그에 맞추어 전력을 비축합니다. LLDP 정보가 포트에 가능하지 않은 경우 포트는 class 모드를 사용해 전원을 비축합니다.

이 모드에서 최대 전력 필드는 적용되지 않습니다.

For all modes: 포트가 비축된 전력보다 더 많은 전력을 사용하는 경우 포트는 셧다운 됩니다.

전원 관리 모드 (Power Management Mode):

포트 셧다운 시 설정 가능한 2가지 모드가 있습니다:

1. 실제 전력 소비 (Actual Consumption): 이 모드에서 전력 공급이 전송 가능한 모든 포트에 대한 실제 전력 소비를 전력량을 초과하거나, 주어진 포트에 대한 실제 전력 소비가 해당 포트에 비축된 전력을 초과하면 포트는 셧다운 됩니다. 포트는 포트 우선권에 따라 셧다운 됩니다. 2개의 포트가 동일한 우선권이 있는 경우, 가장 높은 포트 번호가 셧다운 됩니다.
2. 예비 전력 (Reserved Power): 이 모드에서 전체 비축된 전력이 전송 가능한 전력 공급량을 초과하면 포트는 셧다운 됩니다. 이 모드에서 PD가 포트가 전력 공급에서 가능한 것 보다 더 많은 전력을 필요로 하는 경우 전원은 동작하지 않습니다.

### PoE 전력 공급 설정 (PoE Power Supply Configuration)

주요 전력 공급 [W] (Primary Power Supply [W]):

주요 전력 공급 와트를 표시합니다.

PoE 포트 설정 (PoE Port Configuration)

포트 (Port):

이 열의 논리적 포트 번호입니다.

PoE 모드 (PoE Mode):

PoE 모드는 포트에 대한 PoE 동작 모드입니다. PoE를 활성화 또는 비활성화 합니다.

PoE 일정 관리 (PoE Schedule):

PoE 일정 관리 프로파일을 비활성화 또는 선택합니다.

우선권 (Priority):

우선권은 포트의 우선권을 나타냅니다. Low, High 그리고 Critical 이라고 하는 전원 우선권의 3단계가 있습니다.

우선권은 원격 장치가 공급 가능한 것 보다 더 많은 전력을 필요로 하는 경우 사용합니다. 이 경우 가장 낮은 우선권을 가진 포트가 꺼지면 가장 높은 포트 번호를 가진 포트에서 시작합니다.

최대 전력 [W] (Maximum Power [W]):

최대 전력 값은 원격 장치에 전송 가능한 최대 전력을 와트로 표시하는 숫자 값을 포함합니다.

최대 가능 값은 30W입니다.

지연 모드 (Delay Mode):

전력 지연 기능을 켜고 끕니다.

**Enabled:** POE 전력 지연을 활성화 합니다.

**Disabled:** POE 전력 지연을 비활성화 합니다.

지연 시간 (Delay Time) (0~300sec):

재부팅 시 지연 시간을 초과하면 PoE 포트는 전력을 PD에 제공하기 시작할 것 입니다.

기본값: 0, 범위: 0-300초

## ■ 버튼

적용 (Apply):

클릭해 설정을 저장합니다.

리셋 (Reset):

로컬에서의 변동 사항을 취소하고 저장된 기존 값으로 복구합니다.



## PoE 상태

이 페이지에서 유저는 모든 PoE 포트에 대해 현재 상태를 검사할 수 있습니다.

| Local Port | PD class | Power Requested | Power Allocated | Power Used | Current Used | Priority | Port Status    |
|------------|----------|-----------------|-----------------|------------|--------------|----------|----------------|
| 1          | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | No PD detected |
| 2          | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | No PD detected |
| 3          | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | No PD detected |
| 4          | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | No PD detected |
| 5          | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | No PD detected |
| 6          | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | No PD detected |
| 7          | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | No PD detected |
| 8          | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | No PD detected |
| 9          | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | No PD detected |
| 10         | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | No PD detected |
| 11         | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | No PD detected |
| 12         | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | No PD detected |
| 13         | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | No PD detected |
| 14         | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | No PD detected |

### 웹 인터페이스

웹 인터페이스에서 PoE 상태를 표시하려면:

1. PoE 관리 및 PoE 상태를 클릭합니다.
2. "자동 새로 고침"을 On/Off로 스크롤 합니다.
3. "새로 고침"을 클릭해 포트 상세 현황을 새로 고침 합니다.

### ■ 항목 설명:

로컬 포트 (Local Port):

이 열의 논리적 포트 번호입니다.

PD 클래스 (PD Class):

각 PD는 PD가 사용할 최대 파워를 지정하는 클래스에 따라 분리됩니다. PD 클래스는 여러 클래스를 표시합니다.

5개 클래스가 정의됩니다:

Class 0: 최대 전력 15.4 W

Class 1: 최대 전력 4.0 W

Class 2: 최대 전력 7.0 W

Class 3: 최대 전력 15.4 W

Class 4: 최대 전력 30.0 W

전력 요구 (Power Requested):

전력 요구는 비축하고자 하는 PD 전력의 필요한 양을 표시합니다.

전력 할당 (Power Allocated):

전력 할당은 스위치가 PD에 할당한 전력량을 표시합니다.

전력 사용 (Power Used):

전력 사용은 PD가 현재 사용 중인 전력량을 표시합니다.

전류 사용 (Current Used):

전류 사용은 PD가 현재 사용 중인 전류량을 표시합니다.

우선권 (Priority):

우선권은 유저에 의해 설정된 포트의 우선권을 표시합니다.

포트 상태 (Port Status):

포트 상태는 포트의 상태를 표시합니다. 상태는 다음의 값 중 하나입니다:

PoE not available - PoE 칩이 발견되지 않습니다. – 포트를 위한 PoE 가 지원되지 않습니다.

PoE turned OFF - PoE 비활성화 : PoE가 유저에 의해 비활성화 되었습니다.

PoE turned OFF – 전력 예산이 초과되었습니다 – PD가 전력 공급을 할 수 있는 최대 전력을 초과 함으로써 필요한 총량 또는 사용된 전력이며 가장 낮은 우선권은 전원이 꺼집니다.

No PD detected – 포트의 PD를 탐지할 수 없습니다.

PoE turned OFF – PD 과부하 –포트가 전송할 수 있는 것 보다 더 많은 PD가 필요하거나 사용되며 전원이 꺼집니다.

PoE turned OFF – PD가 off 상태입니다.

Invalid PD – PD가 탐지되었지만 올바르게 작동하지 않습니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

페이지를 새로 고침 하려면 클릭합니다.

## PoE 전원 지연

이 페이지에서 유저는 장치 재부팅 후 제공되는 전원 지연 시간을 설정할 수 있습니다.

| Port | Delay Mode | Delay Time(0-300 sec) |
|------|------------|-----------------------|
| *    | ↔          | 0                     |
| 1    | Disabled   | 0                     |
| 2    | Disabled   | 0                     |
| 3    | Disabled   | 0                     |
| 4    | Disabled   | 0                     |
| 5    | Disabled   | 0                     |
| 6    | Disabled   | 0                     |
| 7    | Disabled   | 0                     |
| 8    | Disabled   | 0                     |
| 9    | Disabled   | 0                     |
| 10   | Disabled   | 0                     |

Reset Apply

### 웹 인터페이스

웹 인터페이스에서 Power over Ethernet 상태를 표시하려면:

1. PoE 관리와 PoE 전원 지연을 클릭합니다.
2. 전원 장치의 포트를 활성화합니다.
3. 재부팅 시 전원 공급 지연 시간을 설정합니다.
4. 적용을 클릭해 변경 사항을 저장합니다.

### ■ 항목 설명:

포트 (Port):

이 열의 논리적 포트 번호입니다.

지연 모드 (Delay Mode):

전원 지연 기능을 On/Off 합니다.

Enabled: Enable POE 전원 지연을 활성화 합니다.

Disabled: Enable POE 전원 지연을 비활성화 합니다.

지연 시간 (Delay Time) (0~300sec):

재부팅 시, PoE 포트는 지연 시간 초과 시 전력을 PD에 제공하기 시작합니다.

초기값:0, 범위: 0-300 초

## ■버튼

적용 (Apply):

클릭해 설정을 저장합니다.

리셋 (Reset):

로컬에서의 변동 사항을 취소하고 저장된 기존 값으로 복구합니다.

## PoE 자동 확인

이 페이지에서 유저는 PoE 포트 및 PD 사이의 연결 상태를 확인하기 위해 자동 탐지 변수를 지정할 수 있습니다. 연결 실패가 발견되면 원격 PD를 자동으로 재부팅 합니다.

| Port | Ping IP Address | Startup Time | Interval Time(sec) | Retry Time | Failure Log      | Failure Action | Reboot Time(sec) |
|------|-----------------|--------------|--------------------|------------|------------------|----------------|------------------|
| 1    | 0.0.0.0         | 60           | 30                 | 3          | error=0, total=0 | Nothing        | 15               |
| 2    | 0.0.0.0         | 60           | 30                 | 3          | error=0, total=0 | Nothing        | 15               |
| 3    | 0.0.0.0         | 60           | 30                 | 3          | error=0, total=0 | Nothing        | 15               |
| 4    | 0.0.0.0         | 60           | 30                 | 3          | error=0, total=0 | Nothing        | 15               |
| 5    | 0.0.0.0         | 60           | 30                 | 3          | error=0, total=0 | Nothing        | 15               |
| 6    | 0.0.0.0         | 60           | 30                 | 3          | error=0, total=0 | Nothing        | 15               |
| 7    | 0.0.0.0         | 60           | 30                 | 3          | error=0, total=0 | Nothing        | 15               |
| 8    | 0.0.0.0         | 60           | 30                 | 3          | error=0, total=0 | Nothing        | 15               |
| 9    | 0.0.0.0         | 60           | 30                 | 3          | error=0, total=0 | Nothing        | 15               |

### 웹 인터페이스

Power over Ethernet 자동 확인을 웹 인터페이스 설정하려면:

1. PoE 관리와 PoE 자동 확인을 클릭합니다.
2. Ping 확인 기능을 활성화 합니다.
3. PD의 IP 주소, 시작 시간, 시간 간격, 재시도 시간, 실패 시 동작 및 재부팅 시간을 지정합니다.
4. 적용을 클릭해 변경사항을 저장합니다.

### ■ 항목 설명:

Ping 확인 (Ping Check):

Ping 확인 기능 활성화는 PoE 포트 및 전원 장치 사이의 연결을 탐지합니다. 비활성화 하면 탐지 기능을 끄게 됩니다.

포트 (Port):

이 열의 논리적 포트 번호입니다.

Ping IP 주소 (Ping IP Address):

시스템이 Ping 해야 하는 PD의 IP 주소입니다.

시작 시간 (Startup Time):

시작 시간 후 장치는 자동 확인을 활성화 합니다. 초기값: 30, 범위: 30-60 초

시간 간격 (초) (Interval Time)(sec):

장치는 확인 메시지를 PD로 각 시간 간격에 따라 보냅니다. 초기값: 30, 범위: 10-120 초

재시도 (Retry Time):

PoE 포트가 PD를 ping 할 수 없을 때 다시 탐지하도록 재시도 합니다. 3번째 재시도의 경우 실패 시 동작을 실행합니다. 초기값: 3, 범위: 1-5 초

실패 로그 (Failure Log):

실패 로그인 카운터입니다.

실패 시 동작 (Failure Action):

3번째 탐지 실패 시 동작입니다.

Nothing: 원격 PD를 계속 Ping하지만 탐지할 수 없습니다.

Reboot: PoE 포트의 전원을 중단하고 PD를 재부팅 합니다.

재부팅 시간(초) (Reboot time) (sec):

PD가 재부팅되면 PoE 포트는 지정된 시간 후에 전원을 복구합니다. 초기값: 15, 범위: 3-120 초

## ■ 버튼

적용 (Apply):

클릭해 설정을 저장합니다.

리셋 (Reset):

로컬에서의 변동 사항을 취소하고 저장된 기존 값으로 복구합니다.

## PoE 일정 관리 프로파일

이 페이지에서 유저는 PoE 일정 관리에 대한 프로파일을 설정할 수 있습니다.

| Week Day  | Start Time |    | End Time |    |
|-----------|------------|----|----------|----|
|           | HH         | MM | HH       | MM |
| *         | 0          | 0  | 0        | 0  |
| Monday    | 0          | 0  | 0        | 0  |
| Tuesday   | 0          | 0  | 0        | 0  |
| Wednesday | 0          | 0  | 0        | 0  |
| Thursday  | 0          | 0  | 0        | 0  |
| Friday    | 0          | 0  | 0        | 0  |
| Saturday  | 0          | 0  | 0        | 0  |
| Sunday    | 0          | 0  | 0        | 0  |

### 웹 인터페이스

웹 인터페이스에서 PoE 일정 관리 프로파일을 설정하려면:

1. PoE 관리 및 PoE 일정 관리 프로파일을 클릭합니다.
2. 프로파일 번호를 선택하고 프로파일 이름을 지정합니다.
3. 요일을 선택하고 시간 시간, 종료 시간을 설정합니다.
4. 적용을 클릭해 변경 사항을 저장합니다.

### ■ 항목 설명:

프로파일 (Profile):

프로파일 인덱스 입니다. 설정에 16개 프로파일이 있습니다.

이름 (Name):

프로파일 이름입니다. 초기 이름은 "Profile #"입니다. 유저는 프로파일 식별을 위해 이름을 지정할 수 있습니다.

요일 (Week Day):

PoE 일정 관리를 위한 요일입니다.

시작 시간 (Start Time):

PoE 시작 시간입니다. 시간 00:00는 이 요일의 첫 번째 초입니다.



종료 시간 (End Time):

PoE 종료 시간입니다. 시간 00:00는 이 요일의 마지막 초입니다.

## ■ 버튼

적용 (Apply):

클릭해 설정을 저장합니다.

리셋 (Reset):

로컬에서의 변동 사항을 취소하고 저장된 기존 값으로 복구합니다.

이 페이지는 의도적으로 비워 두었습니다.

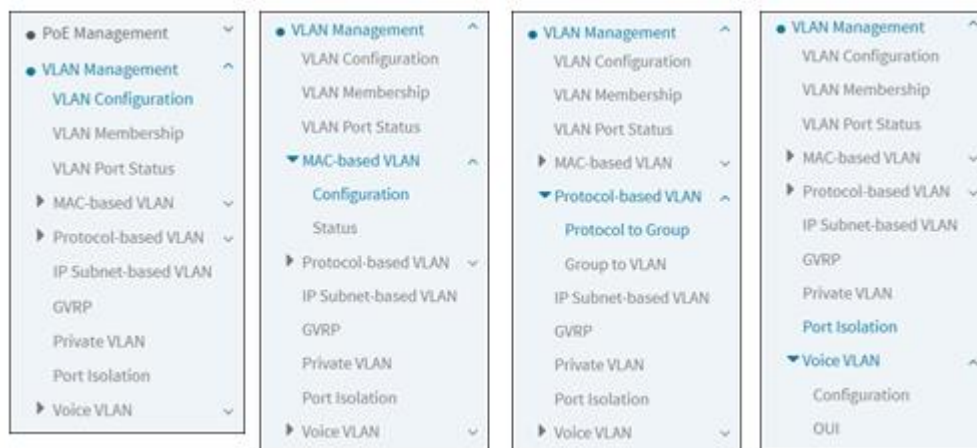
## VLAN 매니지먼트

## 개요

관리 목적으로 특정 VLAN을 할당하기 위한 것 입니다. 매니지먼트 VLAN은 VLAN에서 포트로 연결된 워크스테이션에서 스위치까지 IP 연결을 구축하기 위해 사용됩니다. 이 연결은 VSM, SNMP 및 텔넷 세션을 지원합니다. 기본적으로 동적 매니지먼트 VLAN은 VLAN 1입니다. 그러나 매니지먼트 VLAN 창을 통한 매니지먼트 VLAN에 따라 VLAN을 지정할 수 있습니다. 하나의 매니지먼트 VLAN만 한 번에 동작 가능합니다.

새로운 매니지먼트 VLAN 지정 시 , 이전의 매니지먼트 VLAN의 HTTP 연결은 없어집니다. 이러한 이유로 새 매니지먼트 VLAN에서 매니지먼트 스테이션과 포트 사이의 연결을 구축하거나 멀티 VLAN 경로를 통해 새 매니지먼트 VLAN에 연결해야 합니다.

메뉴 및 하위 메뉴는 다음과 같습니다:



## VLAN 설정

### 웹 인터페이스

웹 인터페이스에서 VLAN 멤버십 설정을 구성하려면:

1. VLAN 매니지먼트 및 VLAN 설정을 클릭합니다.
2. 글로벌 VLAN 설정 항목을 수정합니다.
3. 모드, 포트 VLAN, 포트 타입을 스크롤 해 포트 VLAN 설정 항목을 활성화 합니다.
4. 적용을 클릭해 설정을 저장하세요.
5. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아 갑니다.

### ■ 항목 설명:

#### 글로벌 VLAN 설정 (Global VLAN Configuration)

액세스 허용된 VLAN (Allowed Access VLANs):

이 필드는 스위치에 생성된 VLAN을 보여줍니다.

기본값으로 VLAN 1 만 존재합니다. 더 많은 VLAN은 콤마로 분리되는 각각의 요소를 포함한 구문 리스트를 이용해 생성할 수 있습니다. 범위는 상한과 하한을 구별하는 대쉬로 지정할 수 있습니다.

다음의 예시는 VLAN 1, 10, 11, 12, 13, 200 및 300을 생성하는 것 입니다:

1,10-13,200,300. 구분 사이에 공백이 들어갈 수 있습니다.

전용 S-포트를 위한 Ethertype (Ethertype for Custom S-ports):

이 필드는 전용 S-포트를 위해 사용되는 ethertype/TPID (16진수 지정)를 지정합니다. 설정은 포트 타입이 S-전용-포트로 설정되는 모든 포트에 실행 중입니다.

### 포트 VLAN 설정 (Port VLAN Configuration)

포트 (Port):

이 열의 논리적 포트 번호입니다.

모드 (Mode):

포트 모드 (기본값은 Access)는 문제가 되는 포트의 기본 동작을 지정합니다. 포트는 다음에 설명된 대로 3가지 모드 중 하나입니다. 특정 모드가 선택될 때마다 그 열의 남은 필드는 문제가 되는 모드에 따라 흐려지거나 변경이 가능합니다. 흐려진 필드는 모드가 적용되는 포트가 얻는 값을 표시합니다.

Access:

Access 포트는 종료 스테이션에 연결하기 위해 정상적으로 사용됩니다. Dynamic은 음성 VLAN이 포트를 뒤에서 더 많은 VLAN에 추가하는 것과 같은 기능을 합니다. Access 포트는 다음의 특징이 있습니다:

- 정확히 하나의 VLAN의 멤버, 기본값 1 포트 VLAN (즉, Access VLAN)
- 태그 미지정 프레임 및 C-태그 지정 프레임 허용
- Access VLAN에 분류되지 않은 모든 프레임 폐기
- 모든 프레임이 전송되는 태그 미지정 된 외부

Trunk:

Trunk 포트는 멀티플 VLAN에서 동시에 트래픽을 전송할 수 있으며 일반적으로 다른 스위치를 연결하기 위해 사용됩니다. Trunk 포트는 다음의 특징이 있습니다:

- 초기값으로 Trunk 포트는 모든 기존 VLAN의 멤버입니다. 허용된 VLAN의 사용으로 인해 제한될 수 있습니다.
- VLAN Trunking이 포트 상에서 활성화 되지 않는 이상, 멤버가 아닌 포트 VLAN에 분류된 프레임은 폐기될 것 입니다.
- 초기값으로, 모든 프레임, 그러나 포트 VLAN (즉, Native VLAN)에 분류된 프레임은 외부 상에 태그됩니다. 포트 VLAN에 분류된 프레임은 외부에 C-태그 지정을 갖지 않습니다.
- 태그 지정된 외부는 모든 프레임을 태그하기 위해 변경 가능합니다.
- 태그된 프레임만 입구 상에서 허용됩니다.
- VLAN Trunking이 활성화 될 수 있습니다.

Hybrid:

하이브리드 포트는 trunk 포트여 많은 면에서 비슷하지만, 추가 포트 설정 기능을 추가합니다.

Trunk 포트에 설명된 특징에 더해 하이브리드 포트에는 다음의 기능이 있습니다:

- VLAN 태그 미인식, C-태그 인식, S-태그 인식 또는 S-전용-태그 인식이 되기 위해 설정할 수 있습니다.
- 내부 필터링 제어가 가능합니다.
- 프레임의 내부 허용 및 태그되는 외부 설정을 독립적으로 할 수 있습니다.

포트 VLAN (Port VLAN):

하드브리드 모드의 포트는 포트 타입 변경을 허용합니다. 즉, 프레임의 VLAN 태그가 내부프레임을 특정 VLAN으로 분류하는데 사용될지 여부, 이 경우 반응할 TPID를 정합니다. 마찬가지로 외부에서 포트 타입은 태그가 필요한 경우 태그의 TPID를 지정합니다.

미인식 (Unaware):

내부에서 VLAN 태그를 실행하거나 하지 않거나 모든 프레임은 포트 VLAN으로 분류되며 가능한 태그는 외부에서 삭제되지 않습니다.

C-Port:

내부에서, TPID = 0x8100의 VLAN 태그와 프레임은 태그에 내장된 VLAN ID로 분류됩니다. 프레임이 태그 되지 않거나 우선권이 있는 태그인 경우 프레임은 포트 VLAN에 분류됩니다. 프레임은 외부에서 태그되어야 하며 C-태그와 함께 태그될 것 입니다.

S-Port:

내부에서, TPID = 0x8100 or 0x88A8의 VLAN 태그와 프레임은 태그에 내장된 VLAN ID로 분류됩니다. 프레임이 태그 되지 않거나 우선권이 있는 태그인 경우 프레임은 포트 VLAN에 분류됩니다. 프레임은 외부에서 태그되어야 하며 S-태그와 함께 태그될 것 입니다.

S-전용-포트 (S-Custom-Port):

내부에서, TPID = 0x8100의 VLAN 태그와 프레임 또는 전용-S 포트로 설정된 Ethertype에 동일한 프레임이 태그에 내장된 VLAN ID로 분류됩니다. 프레임이 태그 되지 않거나 우선권이 있는 태그인 경우 프레임은 포트 VLAN에 분류됩니다. 프레임은 외부에서 태그되어야 하며 전용 S-태그와 함께 태그될 것입니다.

내부필터링 (Ingress Filtering):

하이브리드 포트는 내부필터링 변경을 허용합니다. Access 및 Trunk 포트는 활성화된 내부필터링을 가집니다.

내부 필터링이 활성화되면 (체크 박스 클릭) 멤버가 아닌 포트 VLAN으로 분류된 프레임은 폐기됩니다.

멤버가 아닌 포트의 VLAN이 폐기됩니다.

내부 필터링이 비활성화 되면 멤버가 아닌 포트 VLAN으로 분류된 프레임이 허용되며 스위치 엔진으로 전달됩니다. 그러나 포트는 멤버가 아닌 VLAN에 분류된 프레임을 전송하지 않습니다.

내부 허용 (Ingress Acceptance):

하이브리드 포트는 내부에 허용된 프레임 타입을 변경합니다.

태그 지정 및 태그 미지정 (Tagged and untagged)

태그 지정 및 태그 미지정 프레임 모두 허용됩니다.

태그 지정만 (Tagged Only)

태그 지정된 프레임만 내부에 허용됩니다. 태그 미지정 프레임은 폐기됩니다.

태그 미지정만 (Untagged Only)

태그 미지정 프레임만 내부에 허용됩니다. 태그 지정 프레임은 폐기됩니다.

외부 태그 (Egress Tagging):

Trunk와 하이브리드 모드에서 포트는 외부에서 프레임 태그를 제어할 수 있습니다.

태그 미지정 포트 VLAN (Untag Port VLAN)

포트 VLAN에 분류된 프레임은 태그 미지정 되어 전송됩니다. 다른 프레임은 관련 태그와 함께 전송됩니다.

전체 태그 (Tag All)

포트 VLAN에 분류 여부와 관계없이 모든 프레임은 태그된 채로 전송됩니다.

전체 태그 미지정 (Untag All)

포트 VLAN에 분류 여부와 관계없이 모든 프레임은 태그되지 않은 채로 전송됩니다.

이 옵션은 하이브리드 모드에서만 가능합니다.

허용되는 VLAN (Allowed VLANs):

Trunk 및 하이브리드 모드에서 포트는 어느 VLAN이 멤버가 될지 제어합니다. 액세스 포트는 하나의 VLAN, 액세스 VLAN의 멤버만 될 수 있습니다.

필드 구문은 기존 VLAN 필드에 사용된 구문과 동일합니다. 초기값으로 포트는 모든 가능한 VLAN의 멤버가 될 수 있으므로 1-4095로 설정됩니다.

필드는 빈 상태일 것 입니다. 포트가 기존 VLAN의 멤버가 아니라는 것을 의미합니다. 그러나 VLAN Trunking에 설정되면 모든 미확인 VLAN을 전송할 수 있습니다.

금지된 VLAN (Forbidden VLANs):

포트는 하나 이상의 VLAN에 절대 멤버가 될 수 없도록 설정할 수 있습니다. 이 것은 MVRP와 GVRP 같은 동적 VLAN 프로토콜을 동적으로 VLAN에 포트에 추가하는 것을 방지하기에 특히 유용합니다.

이 트릭은 문제가 되는 포트에 금지된 VLAN이라고 표시합니다. 구문은 활성화 된 VLAN 필드에 사용된 구문과 동일합니다.

기본값으로 필드는 공백이며 포트가 모든 가능한 VLAN의 멤버가 될 수 있다는 뜻 입니다.

## ■버튼

적용 (Apply):

클릭해 설정을 저장합니다.

리셋 (Reset):

로컬에서의 변동 사항을 취소하고 저장된 기존 값으로 복구합니다.



## VLAN 멤버십

이 페이지는 VLAN 유저 멤버십 상태의 개요를 제공합니다.

포트는 페이지 헤더에 반영된 것 처럼 현재 선택된 여러 유닛에 속합니다.

| VLAN ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 |
|---------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1       | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  |

웹 인터페이스

웹 인터페이스에서 VLAN 멤버십 설정을 하려면:

1. VLAN 매니지먼트 및 VLAN 멤버십을 클릭합니다.
2. 바를 스크롤 해 표시할 VLAN 을 선택합니다.
3. 새로 고침을 클릭해 상태를 업데이트 합니다.

### ■ 항목 설명:

VLAN 유저 (VLAN USER):

여러 내부소프트웨어 모듈은 상황에 따라 VLAN 멤버십을 설정하기 위해 VLAN 서비스를 사용할 수 있습니다.

오른 쪽의 드롭 다운 목록은 관리자(Admin) 또는 내부소프트웨어 모듈 중 하나로 설정된 VLAN 멤버십을 선택할 수 있습니다.

“Combined” 엔트리는 관리자와 내부소프트웨어 모듈 설정 조합을 나타내며 기본적으로 하드웨어에 실제로 설정된 것을 반영합니다.

VLAN 유저 모듈은 VLAN 매니지먼트 기능의 서비스를 사용해 PVID 및 UVID 와 같은 VLAN 멤버십과 VLAN 포트 설정을 할 수 있습니다. 현재 다음의 VLAN 유저 타입을 지원합니다:

NAS: NAS 는 신청자, 인증자 및 인증 서버 사이의 통신을 포함하는 포트 기반 인증을 제공합니다.

GVRP: 가까운 VLAN-인식 장치는 Generic VLAN Registration Protocol (GVRP)를 사용해 VLAN 정보를 서로 교환하며 VLAN 정보를 브리지 된 네트워크를 통해 전파합니다.

MVR: MVR 은 각 VLAN 에 이용자를 위해 멀티캐스트 트래픽을 복제할 필요성을 제거하는데 사용됩니다. 모든 채널의 멀티캐스트 트래픽은 싱글 (멀티캐스트) VLAN 상에서만 전송됩니다.

Voice VLAN: Voice VLAN 은 일반적으로 IP 전화에서 동작하는 음성 트래픽을 위해 특별히 설정되는 VLAN 입니다.

MSTP: 802.1s Multiple Spanning Tree protocol (MSTP)은 VLAN 을 사용해 네트워크에 여러 스패닝 트리를 생성합니다. 이로 인해 루프-프리 환경을 유지 보수하는 동안 네트워크 리소스 사용을 매우 향상시킬 수 있습니다.

DMS: DMS VLAN 멤버십 상태를 표시합니다.

VCL: 다양한 MAC 기반 VLAN 유저에 의해 설정되는 MAC 기반 VLAN 엔트리를 표시합니다.

VLAN ID:

포트 번호가 표시되는 VLAN ID 입니다.

포트 멤버 (Port Members):

각 포트에 대한 체크 박스 열이 각각의 VLAN ID 를 위해 표시됩니다.

포트가 VLAN 에서 포함되면 이미지가 표시될 것 입니다. 외부 필터링 프레임 상태가 태그 지정 또는 미지정인지 표시합니다. 포트 VLAN 에 분류된 프레임은 태그 지정 또는 미지정 상태로 전송됩니다.

VLAN 멤버십 (VLAN Membership):

VLAN 멤버십 상태 페이지는 선택된 VLAN 유저의 의해 설정된 모든 VLAN 의 현재 VLAN 포트 멤버를 표시합니다. 기본적으로 모든 VLAN 유저를 위해 정보를 표시합니다. VLAN 멤버십에서 VLAN ID 에 분류된 프레임은 각각의 VLAN 멤버 포트에 전달 가능합니다.

엔트리 표시 (Show entries):

표시하기를 원하는 만큼의 항목을 선택할 수 있습니다.

Admin ▼ :

Vlan 유저를 선택할 수 있습니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

페이지를 새로 고침 하려면 클릭합니다.

첫 페이지 (First Page):

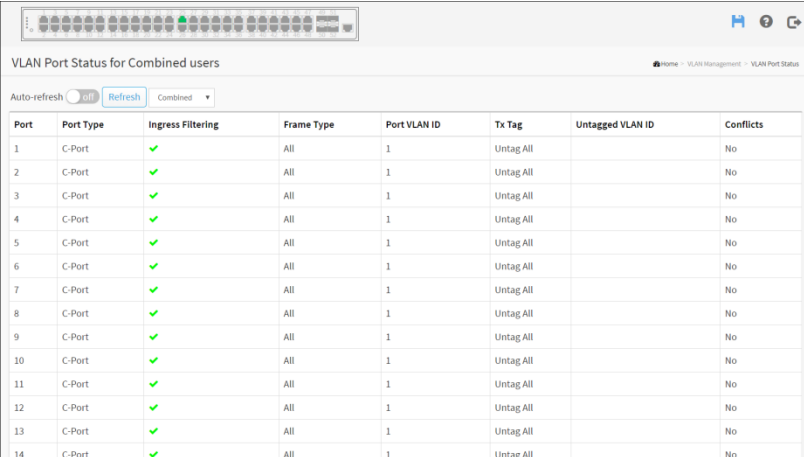
시스템 로그 엔트리를 업데이트하고 첫 번째 페이지로 이동합니다.

다음 페이지 (Next Page):

시스템 로그 엔트리를 업데이트하고 다음 페이지로 이동합니다.

## VLAN 포트 상태

포트 상태 기능은 모든 VLAN 상태의 정보를 모으며 Combined, Admin, NAS, GVRP, MVR, Voice VLAN, MSTP, DMS, VCL 순서로 기록합니다.



| Port | Port Type | Ingress Filtering | Frame Type | Port VLAN ID | Tx Tag    | Untagged VLAN ID | Conflicts |
|------|-----------|-------------------|------------|--------------|-----------|------------------|-----------|
| 1    | C-Port    | ✓                 | All        | 1            | Untag All |                  | No        |
| 2    | C-Port    | ✓                 | All        | 1            | Untag All |                  | No        |
| 3    | C-Port    | ✓                 | All        | 1            | Untag All |                  | No        |
| 4    | C-Port    | ✓                 | All        | 1            | Untag All |                  | No        |
| 5    | C-Port    | ✓                 | All        | 1            | Untag All |                  | No        |
| 6    | C-Port    | ✓                 | All        | 1            | Untag All |                  | No        |
| 7    | C-Port    | ✓                 | All        | 1            | Untag All |                  | No        |
| 8    | C-Port    | ✓                 | All        | 1            | Untag All |                  | No        |
| 9    | C-Port    | ✓                 | All        | 1            | Untag All |                  | No        |
| 10   | C-Port    | ✓                 | All        | 1            | Untag All |                  | No        |
| 11   | C-Port    | ✓                 | All        | 1            | Untag All |                  | No        |
| 12   | C-Port    | ✓                 | All        | 1            | Untag All |                  | No        |
| 13   | C-Port    | ✓                 | All        | 1            | Untag All |                  | No        |
| 14   | C-Port    | ✓                 | All        | 1            | Untag All |                  | No        |

### 웹 인터페이스

웹 인터페이스에서 VLAN 포트 상태를 표시하려면:

1. VLAN 매니지먼트와 VLAN 포트 상태를 클릭합니다.
2. Combined, Admin, NAS, GVRP, MVR, Voice VLAN, MSTP, DMS, VCL, RMirror 를 지정합니다.
3. 포트 상태 정보를 표시합니다.

### ■ 항목 설명:

VLAN 유저 (VLAN USER):

VLAN 유저 모듈은 VLAN 매니지먼트 기능의 서비스를 사용해 PVID 및 UVID 와 같은 VLAN 멤버십과 VLAN 포트 설정을 할 수 있습니다. 현재 다음의 VLAN 유저 타입을 지원합니다:

NAS: NAS 는 신청자, 인증자 및 인증 서버 사이의 통신을 포함하는 포트 기반 인증을 제공합니다.

GVRP:

가까운 VLAN-인식 장치는 Generic VLAN Registration Protocol (GVRP)를 사용해 VLAN 정보를 서로 교환하며 VLAN 정보를 브리지 된 네트워크를 통해 전파합니다.

MVR: MVR 은 각 VLAN 에 이용자를 위해 멀티캐스트 트래픽을 복제할 필요성을 제거하는데 사용됩니다. 모든 채널의 멀티캐스트 트래픽은 싱글 (멀티캐스트) VLAN 상에서만 전송됩니다.

Voice VLAN: Voice VLAN 은 일반적으로 IP 전화에서 동작하는 음성 트래픽을 위해 특별히 설정되는 VLAN 입니다.

MSTP: 802.1s Multiple Spanning Tree protocol (MSTP)은 VLAN 을 사용해 네트워크에 여러 스패닝 트리를 생성합니다. 이로 인해 루프-프리 환경을 유지 보수하는 동안 네트워크 리소스 사용을 매우 향상시킬 수 있습니다.

DMS: DMS VLAN 멤버십 상태를 표시합니다.

VCL: 다양한 MAC 기반 VLAN 유저에 의해 설정되는 MAC 기반 VLAN 엔트리를 표시합니다.

포트 (Port):

동일한 열에 포함된 설정을 위한 논리적 포트입니다.

포트 타입 (Port Type):

포트 타입을 표시합니다. 포트 타입은 Unaware, C-port, S-port, Custom S-port 가 가능합니다.

포트 타입이 Unaware인 경우 모든 프레임은 포트 VLAN으로 분류되며 가능한 태그는 삭제되지 않습니다. , C-port는 고객 포트입니다. S- port는 서비스 포트입니다. Custom S-port는 전용 TPID 를 가진 S- port입니다.

내부필터링 (Ingress Filtering):

포트의 내부필터링을 표시합니다. 이 항목은 VLAN 내부 프로세스에 영향을 미칩니다. 내부필터링 이 활성화 되고 내부포트가 분류된 VLAN의 멤버가 아닌 경우 프레임은 폐기됩니다.

프레임 타입 (Frame Type):

포트가 모든 프레임 또는 태그 된 프레임만 허용할 지 표시합니다. 이 항목은 VLAN 내부 프로세스에 영향을 미칩니다. 포트가 태그 된 프레임만 허용하면, 포트에 수신한 태그 미지정 프레임은 폐기됩니다.

포트 VLAN ID (Port VLAN ID):

지정된 유저 포트에 지정하고 싶은 포트 VLAN ID (PVID)를 표시합니다.

선택된 유저에 의해 중단되지 않으면 필드는 공백입니다.

Tx 태그 (Tx Tag):

외부 필터링 프레임 태그 여부를 표시합니다.

태그 미지정 VLAN ID (Untagged VLAN ID):

Tx 태그는 선택된 유저에 의해 중단되고 태그 지정 또는 태그 미지정 UVID로 설정되면 이 필드는 유저가 외부에 태그 지정 또는 미지정 하고자 하는 VLAN ID를 표시합니다.

충돌 (Conflicts):

2명의 유저는 포트 설정의 요구사항을 충돌할 수 있습니다. 예를 들어, 한 명의 유저는 모든 프레임이 외부에 태그 지정이 되길 원하는 반면 다른 유저는 모든 프레임이 외부에 태그 지정이 않길 원할 수 있습니다.

양 쪽 유저 모두 충족할 수 없으므로 충돌이 커지므로 우선 순위에 따라 문제를 해결합니다. 관리자는 최소한의 우선권을 가집니다. 다른 소프트웨어 모듈은 드롭 다운 목록의 위치에 따라 우선 순위가 매겨집니다: 목록에서 높을수록 높은 우선권입니다.

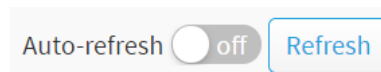
충돌이 있는 경우 "Combined" 유저와 문제가 되는 소프트웨어 모듈을 위해 "Yes"로 표시됩니다.

"Combined" 유저는 하드웨어에 실제로 설정된 것을 반영합니다.

:

Vlan 유저를 선택할 수 있습니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

페이지를 새로 고침 하려면 클릭합니다.

## MAC 기반 VLAN

### 설정

VLAN ID 매핑의 MAC 주소는 여기에서 설정할 수 있습니다. 이 페이지에서 MAC 기반 VLAN 분류 목록 엔트리를 추가 및 삭제할 수 있으며 다른 포트에 엔트리를 할당합니다.

MAC-based VLAN Membership Configuration

Auto-refresh: ☐ Refresh First Page Next Page

| Delete                       | MAC Address | VLAN ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 |
|------------------------------|-------------|---------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Currently no entries present |             |         |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |

Add New Entry

Reset Apply

### 웹 인터페이스

웹 인터페이스에서 MAC 주소 기반 VLAN 설정을 하려면:

1. VLAN 매니지먼트, MAC 기반 VLAN 및 설정을 클릭합니다.
2. "새 엔트리 추가 (Add New Entry)"를 클릭합니다.

MAC-based VLAN Membership Configuration

Auto-refresh: ☐ Refresh First Page Next Page

| Delete | MAC Address       | VLAN ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 |
|--------|-------------------|---------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|        | 00:00:00:00:00:00 | 1       |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |

Add New Entry

Reset Apply

3. MAC 주소 및 VLAN ID를 지정합니다.
4. 적용을 클릭합니다.

**■ 항목 설명:**

MAC 주소 (MAC Address):

MAC 주소를 표시합니다.

VLAN ID:

VLAN ID를 표시합니다.

포트 멤버 (Port Members):

각 포트의 체크 박스 열은 각 MAC to VLAN ID 매핑 엔트리를 나타냅니다. 매핑에 포트를 포함하려면 박스를 체크하십시오. 매핑에서 포트를 제거 또는 제외하려면 박스가 해제되어 있는 것을 확인하십시오. 기본적으로 모든 포트가 멤버가 아니며 모든 박스는 체크 해제되어 있습니다.

**■ 버튼**

새 엔트리 추가 (Adding New Entry):

새로운 MAC 기반 VLAN 엔트리를 추가하려면 클릭합니다. 빈 열은 테이블에 추가되며 MAC 기반 VLAN 엔트리는 필요한대로 설정 가능합니다. 유니캐스트 MAC 주소는 MAC 기반 VLAN 엔트리를 위해 설정 가능합니다. 허용되는 브로드캐스트 또는 멀티캐스트 MAC 주소가 없습니다.

VLAN ID에 대한 합법적인 값은 1에서 4095입니다.

삭제 (Delete):

MAC 기반 VLAN 엔트리를 삭제하려면 이 박스를 체크하고 적용을 누릅니다. 엔트리는 선택된 스위치에서 삭제될 것입니다.

적용 (Apply):

클릭해 설정을 저장합니다.

리셋 (Reset):

로컬에서의 변동 사항을 취소하고 저장된 기존 값으로 복구합니다.

버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):



페이지를 새로 고침 하려면 클릭합니다.

첫 페이지 (First Page):

시스템 로그 엔트리를 업데이트하고 첫 번째 페이지로 이동합니다.

다음 페이지 (Next Page):

시스템 로그 엔트리를 업데이트하고 다음 페이지로 이동합니다.

## 상태

MAC 기반 VLAN 상태를 표시합니다.



웹 인터페이스

MAC 기반 주소 VLAN 설정을 웹 인터페이스에서 표시하려면:

1. VLAN 관리, MAC-기반 VLAN 및 상태를 클릭합니다.
2. 정보를 새로 고침 하려면 "자동 새로 그림"을 사용합니다.
3. "새로 고침"을 클릭해 MAC 기반 VLAN 멤버십 상태를 새로 고칩니다.

## ■ 항목 설명:

MAC 주소 (MAC Address):

MAC 주소를 표시합니다.

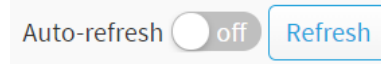
VLAN ID:

VLAN ID를 표시합니다.

포트 멤버 (Port Members):

MAC 기반 VLAN 엔트리의 포트 멤버입니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh)

페이지를 새로 고침 하려면 클릭합니다.

## 프로토콜 기반 VLAN

---

이 섹션은 프로토콜 기반 VLAN을 설명합니다. 스위치는 이더넷 LLC SNAP 프로토콜을 포함하는 프로토콜을 지원합니다.

### LLC

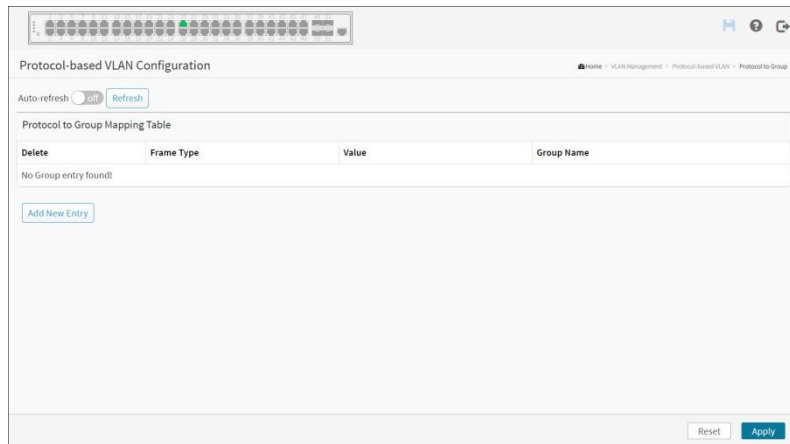
Logical Link Control (LLC) 데이터 통신 프로토콜 레이어는 7-레이어 OSI 참조 모델에서 데이터 링크 레이어의 상단 하위 레이어 (그 자체가 레이어 2, 물리적 레이어 위)입니다. 멀티포인트 네트워크 내에서 공존 및 동일한 네트워크 미디어를 통해 전송하기 위해 여러 네트워크 프로토콜 (IP, IPX, Decnet 및 Appletalk)을 가능하게 하는 다중 매커니즘을 제공합니다. 그리고 흐름 제어 및 자동 반복 요청 (ARQ) 에러 매니지먼트 매커니즘을 제공합니다.

### SNAP

Subnetwork Access Protocol (SNAP)는 IEEE 802.2 LLC를 사용하는 8-bit 802.2 Service Access Point (SAP) 필드에 의해 구분이 가능한 네트워크 상의 다중화 매커니즘입니다. SNAP는 이더넷 타입 필드 값으로 프로토콜 식별을 지원합니다. 또한 판매업자간 식별자 공간을 지원합니다. IEEE 802.3, IEEE 802.4, IEEE 802.5, IEEE 802.11 및 기타 IEEE 802 물리적 네트워크 레이어 그리고 802.2 LLC를 사용하는 FDDI와 같은 비IEEE 802 물리적 네트워크와 사용됩니다.

### 프로토콜 to 그룹 (Protocol to Group)

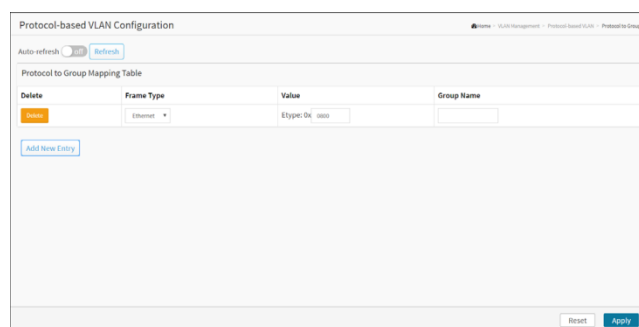
이 페이지는 새로운 프로토콜을 그룹 이름(각 그룹 고유) 매핑 엔트리에 추가할 수 있습니다. 또한 선택된 스택 스위치 유닛 스위치에 대해 이미 매핑된 엔트리를 보거나 삭제할 수 있습니다.



## 웹 인터페이스

웹 인터페이스에서 프로토콜 기반 VLAN 설정을 구성하려면:

1. VLAN 관리, 프로토콜 기반 VLAN 및 프로토콜 to 그룹을 클릭합니다.
2. "새 엔트리 추가"를 클릭합니다.



3. 프레임 타입, 값 그리고 그룹 이름을 지정합니다.
4. 적용을 클릭합니다.

## ■ 항목 설명:

프레임 타입 (Frame Type):

프레임 타입은 다음의 값 중 하나를 갖습니다:

1. 이더넷
2. LLC

### 3. SNAP

**주의:** 프레임 타입 필드, 다음의 텍스트 필드의 유효 값은 사용자가 선택한 새로운 프레임 타입에 따라 다릅니다.

값 (Value):

이 텍스트 필드에 입력 가능한 유효 값은 진행하는 프레임 타입 선택 메뉴에서 선택된 옵션에 따라 다릅니다.

다음은 3가지 다른 프레임 타입에 대한 기준입니다:

1. 이더넷: 이더넷이 프레임 타입으로 선택된 경우 텍스트 필드의 값은 etype 로 불립니다. Etype 의 유효 값은 0x0600-0xffff 범위입니다.
2. LLC: 이 경우 유효 값은 2개의 다른 하위 값으로 구성되어 있습니다.
  - a. DSAP: 1-바이트 긴 문자열 (0x00-0xff)
  - b. SSAP: 1-바이트 긴 문자열 (0x00-0xff)
3. SNAP: 이 경우 유효 값은 2개의 다른 하위 값으로 구성되어 있습니다.
  - a. OUI: OUI (Organizationally Unique Identifier)는 문자열의 각 페어 (xx)가 0x00-0xff 범위의 16진수 값인 xx-xx-xx 형식의 값입니다.
  - b. PID: OUI가 16진수 000000인 경우 프로토콜 ID는 SNAP 상에서 동작 중인 프로토콜에 대한 이더넷 타입 (EtherType) 필드 값입니다. OUI는 특정 기간을 위한 OUI입니다. 프로토콜 ID는 SNAP 상에서 동작 중인 프로토콜에 관련된 기관에 의해 할당된 값입니다.

그룹 이름 (Group Name):

유효한 그룹 이름은 고유한 16자의 긴 문자열입니다. 빈 열이 테이블에 추가됩니다. 프레임 타입, 값 그리고 그룹 이름을 필요한대로 설정할 수 있습니다.

버튼은 새 엔트리 추가를 취소하는데 사용할 수 있습니다.

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.



4. 적용을 클릭합니다.

## ■ 항목 설명:

그룹 이름 (Group Name):

유효한 그룹 이름은 대체로 16자의 문자열입니다.

VLAN ID:

매핑 될 그룹에 ID를 표시합니다. 유효 VLAN ID는 1-4095의 범위입니다.

포트 멤버 (Port Members):

각 포트의 체크 박스 열이 각 그룹 이름을 VLAN ID 매핑에 대해 표시됩니다. 매핑에서 포트를 포함하려면 박스를 체크합니다. 매핑에서 포트를 제거하거나 제외하려면 박스가 체크되어 있지 않는 것을 확인하세요. 초기값으로 모든 포트는 멤버가 아니며 모든 박스는 체크되어 있지 않습니다.

## ■ 버튼

삭제 (Delete):

그룹 이름 to 프로토콜 맵 엔트리를 삭제하려면 이 박스를 체크하세요. 엔트리는 다음 저장 동안 스위치에 상에서 삭제됩니다.

새 엔트리 추가 (Add New Entry):

매핑 테이블의 새 엔트리를 추가하려면 클릭하세요. 빈 열이 테이블에 추가되며 그룹 이름, VLAN ID 및 포트 멤버는 필요한대로 설정할 수 있습니다. VLAN ID에 대한 합법적인 값은 1에서 4095입니다. 버튼은 새 엔트리 추가를 취소하는데 사용됩니다.

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh)

페이지를 새로 고침 하려면 클릭합니다.

## IP 서브넷 기반 VLAN

IP 서브넷 기반 VLAN 엔트리를 이 곳에서 설정 가능합니다. 이 페이지에서 IP 서브넷 기반 VLAN 엔트리를 추가, 업데이트 및 삭제할 수 있습니다.

IP Subnet-based VLAN Configuration

Port Members

| Delete                       | IP Address | Mask Length | VLAN ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 |
|------------------------------|------------|-------------|---------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Currently no entries present |            |             |         |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |

Add New Entry

Reset Apply

### 웹 인터페이스

웹 인터페이스에서 설정된 IP 서브넷 기반 VLAN 멤버십을 구성하려면:

1. VLAN 매니지먼트 및 IP 서브넷 기반 VLAN을 클릭합니다.
2. "새 엔트리 추가"를 클릭합니다.

IP Subnet-based VLAN Configuration

Port Members

| Delete | IP Address | Mask Length | VLAN ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |  |  |  |  |
|--------|------------|-------------|---------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--|--|--|--|
|        | 0.0.0.0    | 24          | 1       |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |  |  |  |

Add New Entry

Reset Apply

3. IP 주소, 마스크 길이, VLAN ID를 지정합니다.
4. 적용을 클릭합니다.



**■ 항목 설명:**

IP 주소 (IP Address):

IP 주소를 표시합니다.

마스크 길이 (Mask Length):

네트워크 마스크 길이를 표시합니다.

VLAN ID:

VLAN ID를 나타냅니다. VLAN ID는 기존 엔트리를 변경할 수 있습니다.

포트 멤버 (Port Members):

각 포트에 대한 체크 박스 열이 각각의 VLAN ID 매핑 엔트리의 IP 서브넷을 위해 표시됩니다.

매핑에서 포트를 추가하려면 간단히 박스를 체크합니다. 매핑에서 포트를 제거 또는 제외하려면 박스가 체크되어 있지 않는 것을 확인하십시오. 초기값으로 모든 포트는 멤버가 아니며 모든 박스는 체크되어 있지 않습니다.

**■ 버튼**

삭제 (Delete):

IP 서브넷 기반 VLAN 엔트리를 삭제하려면 이 박스를 체크하세요. 엔트리는 스택에서 선택된 스위치 상에서 삭제될 것입니다.

새 엔트리 추가 (Add New Entry):

IP 서브넷 기반 VLAN 새 엔트리를 추가하려면 클릭하세요. 빈 열이 테이블에 추가되며 IP 서브넷 기반 VLAN 엔트리를 필요한대로 설정할 수 있습니다. VLAN ID에 대한 합법적인 값은 1에서 4095입니다.

“저장”을 클릭하면 IP 서브넷 기반 VLAN 엔트리는 선택된 스택 스위치 유닛 상에서 활성화 됩니다. “삭제” 버튼은 새 IP 서브넷 기반 VLAN 추가를 취소할 수 있습니다. 최대 가능한 IP 서브넷 기반 VLAN 엔트리는 128에 제한됩니다.

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## GVRP

Generic Attribute Registration Protocol (GARP)는 브리지 된 LAN 즉, 종료 스테이션 및 스위치, 에서 장치가 VLAN 식별자와 같은 속성 값을 서로 등록 또는 등록 취소할 수 있는 일반적인 체계를 제공합니다. 그렇게 해서 속성은 브리지 된 LAN의 장치에 전파되며 이러한 장치는 액티브 토폴로지의 일부인 도달 가능한 트리를 형성합니다. GARP는 구조, 동작 규칙, 상태 시스템 및 속성 값의 등록 및 취소 변수를 정의합니다.

스위치 또는 종료 스테이션의 GARP 참여는 GARP 애플리케이션 및 각 포트 또는 스위치와 관련된 GARP Information Declaration (GID) 구성을 포함합니다. 브리지의 같은 애플리케이션에 대한 GARP 참여자 사이의 정보 전파는 GARP Information Propagation (GIP) 구성에 의해 전송됩니다. 프로토콜은 교환은 GARP 애플리케이션으로 정의된 그룹 MAC 주소 및 PDU 포맷을 사용하는 LLC Type 1 서비스에 의해 GARP 참여자 사이에 발생합니다.

| Parameter      | Value            |
|----------------|------------------|
| Join-time:     | 20 (1-20)        |
| Leave-time:    | 60 (60-300)      |
| LeaveAll-time: | 1000 (1000-5000) |
| Max VLANs:     | 20               |

| Port | Mode     |
|------|----------|
| 1    | Disabled |
| 2    | Disabled |

### 웹 인터페이스

웹 인터페이스에서 GVRP를 설정하려면:

1. VLAN 매니지먼트 그리고 GVRP를 클릭합니다.
2. GVRP를 활성화 또는 비활성화 합니다.
3. Join-time, Leave-time, Leave All-time, Max VLANs를 지정합니다.
4. 모드를 활성화 또는 비활성화 합니다.

5. 적용을 클릭해 설정을 저장합니다.
6. 설정을 취소하고자 하는 경우 리셋 버튼을 이전 저장 값으로 되돌아 갑니다.

### ■ 항목 설명:

GVRP 전반적 활성화 (Enable GVRP globally):

GVRP 기능은 활성화 GVRP 체크박스에 체크 마크 설정으로 활성화 됩니다.

GVRP 프로토콜 타이머 (GVRP protocol timers):

Join-time은 100분의 1초 단위의 1-20 범위의 값입니다. 기본값은 20입니다.

Leave-time은 100분의 1초 단위의 60-300입니다. 기본값은 60입니다.

Leave All-time은 100분의 1초 단위의 1000-5000입니다. 기본값은 1000입니다.

최대 VLAN (Max VLANs):

GVRP 지정으로 GVRP는 VLAN의 최대 수가 활성화 됩니다. 기본값으로 이 번호는 20입니다. 이 번호는 GVRP가 꺼진 경우에만 변경이 가능합니다.

포트 (Port):

포트 칼럼은 포트 목록을 표시합니다.

모드 (Mode):

이 설정은 특정 포트 상에서 GVRP 모드를 로컬에서 활성화/비활성화 합니다.

Disable: 이 포트의 GVRP 모드를 비활성화 합니다.

GVRP Enable: 이 포트의 GVRP 모드를 활성화 합니다.

### ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## 사설 VLAN

스위치의 사설 VLAN 멤버십 설정을 이 곳에서 모니터링 및 수정 가능합니다. 사설 VLAN을 이 곳에서 추가 또는 삭제할 수 있습니다. 각 사설 VLAN의 포트 멤버를 이 곳에서 추가 또는 삭제할 수 있습니다.

사설 VLAN은 소스 포트 마스크를 기반으로 하며 VLAN으로의 연결은 없습니다. 이 것은 VLAN ID와 사설 VLAN ID가 동일할 수 있다는 것을 의미합니다.

포트는 패킷 전송을 위해 VLAN과 사설 VLAN 모두의 멤버여야 합니다. 기본적으로 모든 포트는 VLAN 미인식 및 VLAN 1과 사설 VLAN 1의 멤버입니다.

VLAN 미인식 포트는 한 개의 VLAN 멤버만 될 수 있으나, 여러 사설 VLAN의 멤버가 될 수 있습니다.

VLAN 우선권 (VLAN Priority): 음성 VLAN>MAC 기반 VLAN>프로토콜 기반 VLAN>태그 기반 VLAN

The screenshot shows the 'Private VLAN Membership Configuration' page. At the top, there's a breadcrumb trail: Home > VLAN Management > Private VLAN. Below the title, there's an 'Auto-refresh' toggle set to 'Off' and a 'Refresh' button. The main section is titled 'Private VLAN Membership Configuration' and contains a table labeled 'Port Members'. The table has columns for 'Delete', 'PVID', and 35 ports (1-35). The first row shows PVID 1, and all 35 ports have checkmarks in the 'Delete' column, indicating they are members of this Private VLAN. Below the table is an 'Add New Private VLAN' button. At the bottom right, there are 'Reset' and 'Apply' buttons.

### 웹 인터페이스

웹 인터페이스에서 포트 분리 설정을 하려면:

1. VLAN 매니지먼트 및 사설 VLAN을 클릭합니다.
2. 스위치에 대한 사설 VLAN 멤버십 설정을 구성합니다.
3. 적용을 클릭합니다.

**■ 항목 설명:**

삭제 (Delete):

사설 VLAN 엔트리를 삭제하려면 이 박스를 체크합니다. 다음 적용 동안 엔트리가 삭제됩니다.

사설 VLAN ID (Private VLAN ID):

이 특정 사설 VLAN ID를 식별합니다.

포트 멤버 (Port Members):

각 포트에 대한 체크 박스 열은 각 사설 VLAN ID를 표시합니다. 사설 VLAN에서 포트를 포함하려면 박스를 체크합니다. 사설 VLAN의 포트를 제거 또는 제외하려면 박스가 체크 해제됩니다. 기본적으로 모든 포트는 멤버가 아니며 모든 박스는 체크 해제되어 있습니다.

새 사설 VLAN 추가 (Add New Private VLAN):

클릭해 새 사설 VLAN ID를 추가합니다. 비어 있는 열은 표에 추가되며 사설 VLAN을 필요한 대로 설정 가능합니다. 사설 VLAN ID 허용 범위는 스위치 포트 번호 범위와 동일합니다. 외부의 어떠한 값도 허용되지 않으며 경고 메시지가 나타납니다. "OK"를 클릭해 올바르지 않은 엔트리를 삭제하고 "취소"를 클릭해 편집으로 되돌아가 수정합니다.

"적용"을 클릭하면 사설 VLAN은 활성화 됩니다.

버튼은 새 사설 VLAN 추가를 취소할 때 사용합니다.

**■ 버튼**

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## 포트 분리

포트 분리는 동일한 VLAN 상의 레이어 2 스위치의 포트를 분리하기 위한 장치 및 방법을 제공해 트래픽 흐름을 제한합니다. 장치는 많은 수의 포트, 보호된 포트 또는 비보호 된 포트에 설정된 각 포트에 할당되는 스위치로 구성됩니다. 주소 테이블 메모리는 대상 주소 및 포트 번호가 서로 일치하는 주소 테이블을 저장합니다. 포워딩 맵 생성기는 대응할 데이터 패킷의 대상 주소 포워딩 맵을 생성합니다. 레이어 2 스위치의 포트 분리 방법은 보호된 포트 또는 비보호 된 포트로서 레이어 2 스위치의 각 포트 설정으로 구성되어 있습니다. 데이터 패킷에 대한 대상 주소는 레이어 2 스위치의 물리적 주소와 일치하며, 포워딩 맵은 데이터 패킷의 대상 주소를 기반으로 데이터 패킷을 생성합니다. 데이터 패킷은 내부포트가 보호 또는 비보호 포트에 설정될지를 기준으로 생성된 포워딩 맵에 따라 많은 포트에 전송됩니다.

이 페이지에서 사설 VLAN에서 포트의 포트 분리를 활성화 또는 비활성화 합니다. VLAN의 포트 번호는 동일한 VLAN 및 사설 VLAN 상의 다른 분리된 포트에 분리 가능합니다.



### 웹 인터페이스

웹 인터페이스에서 포트 분리 설정을 하려면:

1. VLAN 관리 및 포트 분리를 클릭합니다.
2. 포트 분리를 활성화 할 포트를 선택합니다.
3. 적용을 클릭합니다.

**■ 항목 설명:**

포트 번호 (Port Numbers):

사설 VLAN의 각 포트 별로 체크 박스가 제공됩니다. 체크되면 포트 분리가 포트 상에서 활성화 됩니다. 체크 해제되면 포트 분리가 포트 상에서 비활성화 됩니다. 기본값으로 포트 분리는 모든 포트에서 비활성화 입니다.

**■ 버튼**

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## 음성 VLAN

음성 VLAN은 음성 트래픽을 위해 특별히 설정된 VLAN입니다. 음성 VLAN을 지원하는 음성 장치와 포트를 추가해 음성 데이터에 대한 QoS-관련 설정을 할 수 있어 음성 트래픽 전송 우선권 및 음성 품질을 지원합니다.

### 설정

음성 VLAN 기능을 이용해 음성 VLAN에서 음성 트래픽 포워딩을 지원하며, 스위치는 네트워크 트래픽을 분류하고 일정 관리를 정할 수 있습니다. 포트에 2개 VLAN – 하나는 음성, 나머지 하나는 데이터 – 을 권장합니다. 스위치에 IP 장치를 연결하기 전에, IP 전화는 음성 VLAN ID를 맞게 설정합니다. 자체 GUI를 통해 설정될 것 입니다.

The screenshot displays the 'Voice VLAN Configuration' web interface. It is divided into two main sections: 'Voice VLAN Configuration' and 'Port Configuration'.

**Voice VLAN Configuration:**

- Mode:** A toggle switch set to 'On'.
- VLAN ID:** A text input field containing '1000'.
- Aging Time:** A text input field containing '86400' with the unit 'seconds'.
- Traffic:** A dropdown menu set to '7 (High)'.

**Port Configuration:**

| Port | Mode     | Security | Discovery Protocol |
|------|----------|----------|--------------------|
| *    | Disabled | <>       | <>                 |
| 1    | Disabled | Disabled | Out                |
| 2    | Disabled | Disabled | Out                |
| 3    | Disabled | Disabled | Out                |

At the bottom right, there are 'Reset' and 'Apply' buttons.

### 웹 인터페이스

웹 인터페이스에서 음성 VLAN을 설정하려면:

1. VLAN 매니지먼트, 음성 VLAN 및 설정을 클릭합니다.
2. 음성 VLAN 설정에서 "on"를 선택합니다.
3. VLAN ID, 에이징 타임 및 트래픽 클래스를 지정합니다.
4. 음성 VLAN 설정에서 포트 멤버를 선택합니다.
5. 포트 설정에서 (모드, 보안, 디스커버리 프로토콜)을 지정합니다.
6. 적용을 클릭해 설정을 저장합니다.



7. 설정을 취소하고자 하는 경우 리셋 버튼을 이전 저장 값으로 되돌아 갑니다.

## ■ 항목 설명:

모드 (Mode):

음성 VLAN 모드 동작을 표시합니다. 음성 VLAN을 활성화 하기 전 MSTP 기능을 비활성 해야 합니다. 내부필터링 충돌을 피할 수 있습니다.

On: 음성 VLAN 모드 동작을 활성화 합니다.

Off: 음성 VLAN 모드 동작을 비활성화 합니다.

VLAN ID:

음성 VLAN ID를 표시합니다. 시스템에 고유의 VLAN ID가 있어야 하며 각 포트 PVID는 동일해서는 안됩니다. 값이 관리 VID, MVR VID, PVID 등과 동일한 경우 설정 충돌입니다. 허용 범위는 1~4095입니다.

에이징 타임 (Aging Time):

음성 VLAN 보안 러닝 에이징 타임을 표시합니다. 허용 범위는 10~10000000초입니다. 보안 모드 또는 자동 탐지 모드 활성화 시 사용됩니다. 다른 경우는 하드웨어 에이징 타임을 기반입니다. 실제 에이징 타임은 [age\_time; 2 \* age\_time] 간격 사이를 고려할 것 입니다.

트래픽 (Traffic):

음성 VLAN 트래픽 클래스를 표시합니다. 음성 VLAN에 대한 모든 트래픽은 이 클래스에 적용될 것 입니다.

포트 (Port):

음성 VLAN 포트의 스위치 포트 번호 입니다.

포트 모드 (Port Mode):

음성 VLAN 포트 모드를 표시합니다. 가능한 포트 모드는:

Disabled: 음성 VLAN에서 분리합니다.

Auto: 자동 탐지 모드를 활성화 합니다. 특정 포트에 지원되는 VoIP 전화를 탐지하며 음성 VLAN 멤버를 자동으로 설정합니다.

Forced: 음성 VLAN에 강제 참여합니다.

이 필드는 SPF 기능이 활성화 될 때만 읽을 수 있습니다. STP 포트 모드는 이 필드가 활성화가 아닌 모드에 설정되었을 때만 읽을 수 있습니다.

#### 포트 보안 (Port Security):

음성 VLAN 포트 보안 모드를 표시합니다. 기능이 활성화 되면, 음성 VLAN의 모든 비전화 MAC 주소는 10초간 차단됩니다. 가능한 포트 모드는 다음과 같습니다:

Enabled: 음성 VLAN 보안 모드 동작을 활성화 합니다.

Disabled: 음성 VLAN 보안 모드 동작을 비활성화 합니다.

#### 포트 디스커버리 프로토콜 (Port Discovery Protocol)

음성 VLAN 포트 디스커버리 프로토콜을 표시합니다. 자동 탐지 모드가 활성화 된 경우만 동작합니다. 디스커버리 프로토콜을 "LLDP" 또는 "Both"로 설정하기 전에 LLDP 기능을 활성화 해야 합니다. 디스커버리 프로토콜을 "OUI" 또는 "LLDP"로 변경하면 자동 탐지 프로세스를 재시작합니다. 가능한 디스커버리 프로토콜은 다음과 같습니다:

OUI: OUI 주소로 전화 장치를 탐지합니다.

LLDP: LLDP로 전화 장치를 탐지합니다.

Both: OUI와 LLDP입니다.

## ■버튼

적용 (Apply):

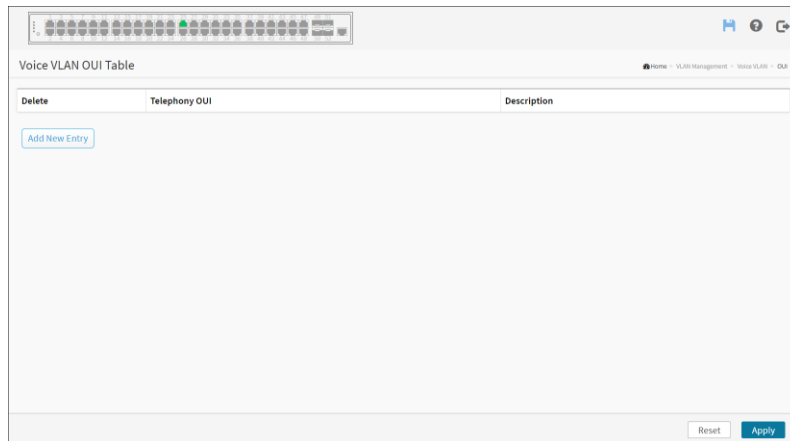
변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## OUI

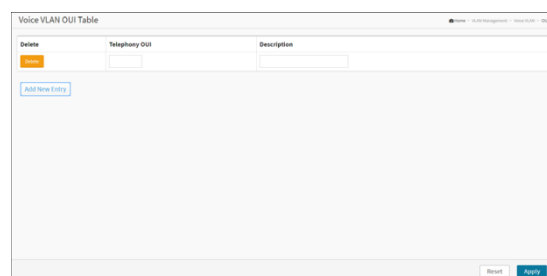
이 섹션은 VOICE VLAN OUI 테이블 설정을 설명합니다. 최대 입력 수는 16입니다. OUI 테이블을 수정하면 OUI 프로세스 자동 탐지가 재시작 될 것 입니다.



### 웹 인터페이스

웹 인터페이스에서 음성 VLAN OUI 테이블을 설정하려면:

1. VLAN 관리, 음성 VLAN 및 OUI를 클릭합니다.
2. 음성 VLAN OUI 테이블에서 "새 엔트리 추가", "삭제"를 선택합니다.



3. 전화 OUI, 설명을 지정합니다.
4. 적용을 클릭합니다.

### ■ 항목 설명:

삭제 (Delete):

엔트리 삭제를 클릭합니다. 다음 저장 동안 삭제될 것 입니다.

전화 OUI (Telephony OUI):

전화 OUI 주소는 IEEE에 의한 벤더에 할당된 전세계적인 고유 식별자입니다. 6자 길이이며 입력 형식은 "xx-xx-xx" (x는 16진수 숫자입니다.)

설명 (Description):

OUI 주소 설명입니다. 일반적으로 어느 벤더 전화 장치가 속한 것인지에 대한 설명입니다. 허용 문자열 길이는 0~32입니다.

새 엔트리 추가 (Add New entry):

클릭해 음성 VLAN OUI 테이블에 새 엔트리를 추가합니다. 빈 열이 테이블, 전화 OUI, 설명에 추가됩니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## Quality of Server (QoS)

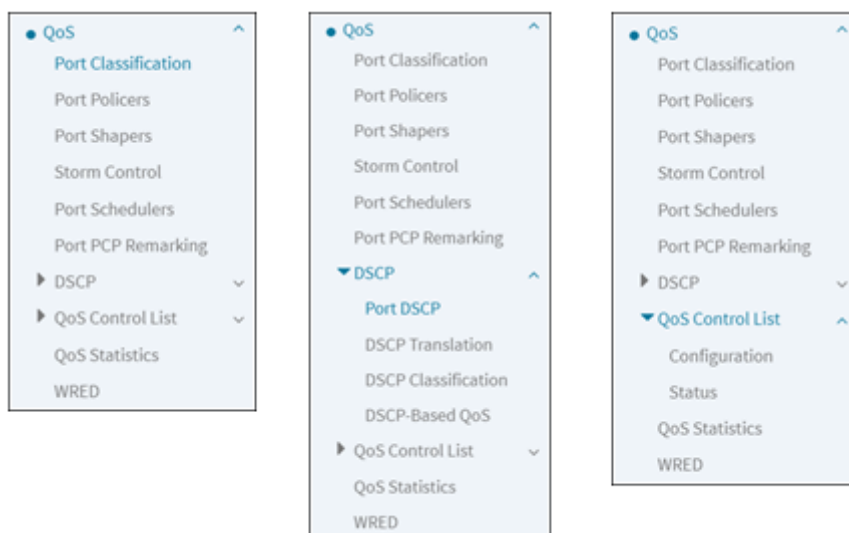
### 개요

스위치는 엄격하거나 편중된 대기열 일정 관리와 함께 포트 당 4개의 QoS 대기열을 지원합니다. 고급 프로그래밍 가능한 QoS 분류를 위한 IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP 및 UDP/TCP 포트와 범위를 기반으로 하는 QoS Control Lists (QCL)를 지원합니다.

QoS 클래스에 입력되는 프레임 분류에서 우수한 유연성을 제공합니다. QoS 분류는 IPv4 및 IPv6 DSCP, IPv4 TCP/UDP 포트 번호 및 태그된 프레임의 유저 우선권 포함한 최대 레이어 4 정보를 찾습니다. 이 프레임에 할당된 QoS 클래스는 특정 QoS 클래스에 설정에 따라 프레임의 대기열, 일정 관리 및 혼잡 제어 보장을 제공하기 위한 장치 전체에 사용됩니다.

스위치는 점보 프레임을 포함해 어떠한 트래픽 시나리오에서도 모든 QoS 클래스의 우수한 기능을 제공하는 강화된 메모리 제어 메커니즘을 지원합니다. 조율 시 지정된 메모리와 엄격한 가장 높은 순위와 함께 우선 순위를 정합니다. 모든 QoS 클래스 대기열이 혼잡한 경우 CPU에 전송 수신 및 대기하도록 내부 우선 순위 대기열은 CPU 트래픽으로 인식되는 트래픽을 허용합니다.

메뉴 및 하위 메뉴는 다음과 같습니다:



## 포트 분류

이 섹션은 사용자가 모든 스위치 포트에 대한 기본 QoS 내부 분류 설정할 수 있습니다.

| Port | Queue Priority<br>(7 is the highest priority) | DPL | PCP | DEI | PCP Classification | DSCP Based               | WRED Group |
|------|---|-----|-----|-----|--------------------|--------------------------|------------|
| *    | 0 ▼   | 0 ▼ | 0 ▼ | 0 ▼ | Disabled           | <input type="checkbox"/> | 1 ▼        |
| 1    | 0 ▼   | 0 ▼ | 0 ▼ | 0 ▼ | Disabled           | <input type="checkbox"/> | 1 ▼        |
| 2    | 0 ▼   | 0 ▼ | 0 ▼ | 0 ▼ | Disabled           | <input type="checkbox"/> | 1 ▼        |
| 3    | 0 ▼   | 0 ▼ | 0 ▼ | 0 ▼ | Disabled           | <input type="checkbox"/> | 1 ▼        |
| 4    | 0 ▼   | 0 ▼ | 0 ▼ | 0 ▼ | Disabled           | <input type="checkbox"/> | 1 ▼        |
| 5    | 0 ▼   | 0 ▼ | 0 ▼ | 0 ▼ | Disabled           | <input type="checkbox"/> | 1 ▼        |
| 6    | 0 ▼   | 0 ▼ | 0 ▼ | 0 ▼ | Disabled           | <input type="checkbox"/> | 1 ▼        |
| 7    | 0 ▼   | 0 ▼ | 0 ▼ | 0 ▼ | Disabled           | <input type="checkbox"/> | 1 ▼        |
| 8    | 0 ▼   | 0 ▼ | 0 ▼ | 0 ▼ | Disabled           | <input type="checkbox"/> | 1 ▼        |
| 9    | 0 ▼   | 0 ▼ | 0 ▼ | 0 ▼ | Disabled           | <input type="checkbox"/> | 1 ▼        |
| 10   | 0 ▼   | 0 ▼ | 0 ▼ | 0 ▼ | Disabled           | <input type="checkbox"/> | 1 ▼        |

### 웹 인터페이스

웹 인터페이스에서 QoS 내부포트 분류 항목을 설정하려면:

1. 서비스 품질 및 포트 분류를 클릭합니다.
2. 스크롤 해 QoS 내부포트 항목을 선택합니다.
3. 적용을 클릭해 설정을 저장합니다.
4. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아갑니다.
5. "PCP 분류"를 클릭해 "포트 PCP 분류"로 이동합니다.

### ■ 항목 설명:

포트 (Port):

다음 적용을 설정할 포트 번호입니다.

대기열 우선권 (Queue Priority):

모든 프레임은 CoS로 분류됩니다. CoS, 대기열 및 우선권 사이에서 하나를 매핑합니다. 0 값의 CoS는 가장 낮은 순위입니다.

포트가 VLAN 인식인 경우 프레임은 태그되고 태그 클래스가 활성화 되면 프레임은 프레임은 태그의 PCP와 DEI 값에서 매핑되는 CoS로 분류됩니다. 그렇지 않으면 프레임은 초기값 CoS로 분류됩니다.

분류된 CoS는 QCL 엔트리에 의해 무효화 될 수 있습니다.

주의: 초기값 CoS이 동적으로 변경된 경우, 설정된 초기값 CoS 이후 실제 초기값 CoS는 괄호 안에 나타납니다.

DPL:

초기값 삭제 우선 레벨을 제어합니다.

모든 프레임은 삭제 우선 레벨로 분류됩니다.

포트가 VLAN 인식인 경우 프레임은 태그되고 태그 클래스가 활성화 되면 프레임은 프레임은 태그의 PCP와 DEI 값에서 매핑되는 DPL로 분류됩니다. 그렇지 않으면 프레임은 초기값 DPL로 분류됩니다.

분류된 DPL은 QCL 엔트리에 의해 무효화 될 수 있습니다.

PCP

초기값 PCP 값을 제어합니다.

모든 프레임은 PCP 값으로 분류됩니다.

포트가 VLAN 인식인 경우 프레임은 태그되고 태그 클래스가 활성화 되면 프레임은 프레임은 태그의 PCP 값으로 분류됩니다. 그렇지 않으면 프레임은 초기값 PCP 값으로 분류됩니다.

DEI:

초기값 DEI 값을 제어합니다.

모든 프레임은 DEI 값으로 분류됩니다.

포트가 VLAN 인식인 경우 프레임은 태그되고 태그 클래스가 활성화 되면 프레임은 프레임은 태그의 DEI 값으로 분류됩니다. 그렇지 않으면 프레임은 초기값 DEI 값으로 분류됩니다.

DSCP 기반 (DSCP Based):

DSCP 기반 QoS 내부포트 분류를 활성화 하려면 클릭합니다.

WRED 그룹 (WRED Group):

WRED 그룹 멤버십을 제어합니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

PCP 분류 (PCP Classification):

이 포트의 태그된 프레임을 위한 분류 모드를 표시합니다.

Disabled: 태그된 프레임에 초기값 CoS 및 DPL을 사용합니다.

Enabled: 태그된 프레임에 PCP 및 DEI 매핑된 버전을 사용합니다.

모드 및/또는 매핑을 설정하기 위해 모드를 클릭합니다.

주의: 포트는 VLAN 미인식이면 이 설정을 적용되지 않습니다. VLAN 미인식 포트에 수신된 태그된 프레임은 항상 초기값 CoS와 DPL에 분류됩니다.

## 포트 PCP 분류

Ingress Port PCP Classification Port 26

Port 26 ▼

Tagged Frames Settings

PCP Classification Disabled ▼

(PCP, DEI) to (Queue Priority, DP level) Mapping

| PCP | DEI | Queue Priority | DP level |
|-----|-----|----------------|----------|
| *   | *   | <> ▼           | <> ▼     |
| 0   | 0   | 1 ▼            | 0 ▼      |
| 0   | 1   | 1 ▼            | 1 ▼      |
| 1   | 0   | 0 ▼            | 0 ▼      |
| 1   | 1   | 0 ▼            | 1 ▼      |
| 2   | 0   | 2 ▼            | 0 ▼      |
| 2   | 1   | 2 ▼            | 1 ▼      |
| 3   | 0   | 3 ▼            | 0 ▼      |
| 3   | 1   | 3 ▼            | 1 ▼      |
| 4   | 0   | 4 ▼            | 0 ▼      |
| 4   | 1   | 4 ▼            | 1 ▼      |
| 5   | 0   | 5 ▼            | 0 ▼      |
| 5   | 1   | 5 ▼            | 1 ▼      |
| 6   | 0   | 6 ▼            | 0 ▼      |
| 6   | 1   | 6 ▼            | 1 ▼      |
| 7   | 0   | 7 ▼            | 0 ▼      |
| 7   | 1   | 7 ▼            | 1 ▼      |

Cancel Reset Apply



**■ 항목 설명:**

PCP 분류

PCP 분류 (PCP Classification):

이 포트의 태그된 프레임을 위한 분류 모드를 제어합니다.

Disabled: 태그된 프레임에 초기값 CoS 및 DPL을 사용합니다.

Enabled: 태그된 프레임에 PCP 및 DEI 매핑된 버전을 사용합니다.

(PCP, DEI)에서 (대기열 우선권, DPL 레벨) 매핑

태그 분류가 활성화 되면 분류된 (PCP, DEI)에서 (대기열 우선권, DPL 레벨) 값의 매핑을 제어합니다.

**■ 버튼**

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

취소 (Cancel):

클릭해 로컬의 변동사항을 취소하고 이전에 저장된 값으로 되돌립니다.

## 포트 폴리서

이 섹션은 모든 스위치 포트에 대한 QoS 내부포트 폴리서의 개요를 제공합니다. 포트 폴리싱은 특정 속도 이상의 트래픽 흐름 제어 및 프레임 마킹에 효과적입니다. 음성 및 비디오는 일반적으로 안정적인 트래픽 속도에서 유지보수 되므로 폴리싱은 데이터 흐름 및 음성 또는 비디오 흐름에 매우 유용합니다.

| Port | Enable                   | Rate | Unit | Flow Control             |
|------|--------------------------|------|------|--------------------------|
| *    | <input type="checkbox"/> | 500  | <-   | <input type="checkbox"/> |
| 1    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| 2    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| 3    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| 4    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| 5    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| 6    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| 7    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| 8    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| 9    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| 10   | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |

### 웹 인터페이스

웹 인터페이스에서 QoS 포트 폴리서를 설정하려면:

1. Quality of Service 및 포트 폴리서를 클릭합니다.
2. QoS 내부포트 폴리서를 활성화에 필요한 포트를 클릭합니다. 그리고 속도 제한 상태를 설정합니다.
3. 스크롤 해 속도 및 유닛 칼럼을 선택하세요.
4. 적용을 클릭해 설정을 저장합니다.
5. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아갑니다.

### ■ 항목 설명:

포트 (Port):

동일한 열에 포함된 설정의 논리적 포트입니다. 스케줄러를 설정하려면 포트 번호를 클릭합니다.

활성화 (Enabled):

QoS 내부포트 폴리서 기능 활성화에 필요한 포트를 사용합니다.

속도 (Rate):

이 포트에 대한 속도 제한 값을 설정하려면 기본값은 1000000입니다.

유닛 (Unit):

포트 폴리서 속도 측정 유닛을 kbps, Mbps, fps 또는 kfps로 제어합니다.

흐름 제어 (Flow Control):

흐름 제어 활성화되며 포트가 흐름 제어 모드가 되면, 정지 프레임이 폐기된 프레임 대신 전송됩니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## 포트 셰이퍼

이 섹션은 모든 스위치 포트에 대한 QoS 외부 포트 셰이퍼의 개요를 제공합니다. 다른 유저는 페이지 헤더에 반영된 대로 현재 선택된 스택 유닛에 속한 포트의 모든 상세 정보를 얻을 수 있습니다.

QoS Egress Port Shapers

Port: Port 1

| Queue | Enable                   | Rate | Unit |
|-------|--------------------------|------|------|
| 0     | <input type="checkbox"/> | 500  | kbps |
| 1     | <input type="checkbox"/> | 500  | kbps |
| 2     | <input type="checkbox"/> | 500  | kbps |
| 3     | <input type="checkbox"/> | 500  | kbps |
| 4     | <input type="checkbox"/> | 500  | kbps |
| 5     | <input type="checkbox"/> | 500  | kbps |
| 6     | <input type="checkbox"/> | 500  | kbps |
| 7     | <input type="checkbox"/> | 500  | kbps |

Port Shaper

| Enable                   | Rate (kbps) | Rate-type |
|--------------------------|-------------|-----------|
| <input type="checkbox"/> | 500         | Line      |

Reset Apply

### 웹 인터페이스

웹 인터페이스에서 QoS 포트 셰이퍼를 설정하려면:

1. Quality of Service 및 포트 셰이퍼를 클릭합니다.
2. 포트를 클릭하고 QoS 외부 포트 셰이퍼를 표시합니다.
3. 포트 및 스케줄러 모드를 스크롤 해 대기열 셰이퍼 항목을 지정합니다.
4. 적용을 클릭하고 설정을 저장합니다.
5. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아갑니다.

### ■ 항목 설명:

포트 (Port):

동일한 열에 포함된 설정의 논리적 포트입니다.

셰이퍼를 설정하기 위한 포트 번호를 클릭합니다.

Shapers – Qn:

비활성 또는 실제 대기열 셰이퍼 속도를 표시합니다. - 예: "800 Mbps".

Shapers – Port:

비활성 또는 실제 포트 셰이퍼 속도를 표시합니다. - e.g. "800 Mbps".

스케줄러 모드 (Scheduler Mode):

엄격하게 관리되는 대기열 수 일정 및 이 스위치 포트에 편중되어 관리되는 수를 제어합니다.

대기열 셰이퍼 활성화 (Queue Shaper Enable):

이 스위치 포트의 대기열에 대기열 셰이퍼 활성화 여부를 제어합니다.

대기열 셰이퍼 속도 (Queue Shaper Rate):

대기열 셰이퍼 속도를 제어합니다. "유닛"이 kbps인 경우 이 값은 100- 13107100로 제한됩니다.

그리고 "유닛"이 Mbps인 경우 1-13107입니다. 속도는 내부에서 대기열 셰이퍼에 의해 지원되는 가장 가까운 값을 모읍니다.

대기열 셰이퍼 유닛 (Queue Shaper Unit):

kbps 또는 Mbps로 대기열 셰이퍼 속도의 측정 유닛을 제어합니다.

대기열 셰이퍼 속도 타입 (Queue Shaper Rate-type):

대기열 셰이퍼의 속도 유형입니다. 허용되는 값은 다음과 같습니다:

Line: 셰이퍼가 라인 속도에서 동작하는 것을 지정합니다.

Data: 셰이퍼가 데이터 속도에서 동작하는 것을 지정합니다.

대기열 스케줄러 가중치 (Queue Scheduler Weight):

이 대기열의 무게를 제어합니다. 값은 1-100 사이입니다. 이 항목은 "스케줄러 모드"가

"Weighted"로 설정된 경우에만 표시됩니다.

대기열 스케줄러 퍼센트 (Queue Scheduler Percent):

이 대기열의 가중치 퍼센트를 표시합니다. 이 항목은 "스케줄러 모드"가 "Weighted"로 설정된 경우에만 표시됩니다.

포트 셰이퍼 활성화 (Port Shaper Enable):

포트 셰이퍼가 이 스위치 포트를 활성화하는지 여부를 제어합니다.

포트 셰이퍼 속도 (Port Shaper Rate):

포트 셰이퍼 속도를 제어합니다. 이 값은 "유닛"이 kbps인 경우 100- 13107100로 제한됩니다. 속도는 내부에서 포트 셰이퍼에 의해 지원되는 가장 가까운 값을 모읍니다.

포트 셰이퍼 유닛 (Port Shaper Unit):

kbps 또는 Mbps로 포트 셰이퍼 속도 측정 유닛을 제어합니다.

포트 셰이퍼 속도 타입 (Port Shaper Rate-type):

대기열 셰이퍼의 속도 유형입니다. 허용되는 값은 다음과 같습니다:

Line: 셰이퍼가 라인 속도에서 동작하는 것을 지정합니다.

Data: 셰이퍼가 데이터 속도에서 동작하는 것을 지정합니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## 스톰 컨트롤

이 섹션에서 유저는 스위치의 스톰 컨트롤을 설정할 수 있습니다. 대상 검색 실패 스톰 속도 컨트롤, 멀티캐스트 스톰 속도 컨트롤 및 브로드캐스트 스톰 속도 컨트롤이 있습니다. 이는 쇠도한 프레임, 즉 (VLAN ID, DMAC)과 페어인 프레임에만 영향을 주며 MAC 주소 테이블에 표시하지 않습니다. 설정은 스위치를 통해 유니캐스트, 멀티캐스트 또는 브로드캐스트 트래픽의 허용된 패킷 속도를 표시합니다.

| Global Storm Policer Configuration |                          |      |      |
|------------------------------------|--------------------------|------|------|
| Frame Type                         | Enable                   | Rate | Unit |
| Unicast                            | <input type="checkbox"/> | 10   | pps  |
| Multicast                          | <input type="checkbox"/> | 10   | pps  |
| Broadcast                          | <input type="checkbox"/> | 10   | pps  |

| Port Storm Policer Configuration |                          |      |      |                          |      |      |                          |      |      |
|----------------------------------|--------------------------|------|------|--------------------------|------|------|--------------------------|------|------|
| Port                             | Unicast Frames           |      |      | Broadcast Frames         |      |      | Unknown Frames           |      |      |
|                                  | Enable                   | Rate | Unit | Enable                   | Rate | Unit | Enable                   | Rate | Unit |
| *                                | <input type="checkbox"/> | 500  | pps  | <input type="checkbox"/> | 500  | pps  | <input type="checkbox"/> | 500  | pps  |
| 1                                | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> | 500  | kbps |
| 2                                | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> | 500  | kbps |
| 3                                | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> | 500  | kbps |

### 웹 인터페이스

웹 인터페이스에서 스톰 컨트롤 구성 항목을 설정하려면:

1. Quality of Service와 스톰 컨트롤을 클릭합니다.
2. 스톰 컨트롤을 활성화 하려면 프레임 타입을 선택합니다.
3. 속도 항목 및 유닛을 설정하려면 스크롤 합니다.
4. 활성화 하기 위해 필요한 포트를 클릭하고 속도 제한 상태를 설정합니다.
5. 적용을 클릭해 설정을 저장합니다.
6. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아갑니다.

### ■ 항목 설명:

#### 글로벌 스톰 폴리서 설정 (Global Storm Policer Configuration)

스위치의 글로벌 스톰 폴리서를 이 페이지에서 설정합니다.

유니캐스트 스톱 폴리서, 멀티캐스트 스톱 폴리서 및 브로드캐스트 스톱 폴리서가 있습니다.

이는 채도한 프레임, 즉 (VLAN ID, DMAC)과 페어인 프레임에만 영향을 주며 MAC 주소 테이블에 표시하지 않습니다.

프레임 타입 (Frame Type):

다음의 설정 프레임 타입을 적용합니다.

활성화 (Enable):

주어진 프레임 타입의 글로벌 스톱 폴리서를 활성화 또는 비활성화 합니다.

속도 (Rate):

글로벌 스톱 폴리서 속도를 제어합니다. "유닛"이 fps 또는 kbps인 경우 이 값은 10- 13128147로 제한됩니다. "유닛"이 kfps 또는 Mbps인 경우 1-13128입니다. 속도는 내부에서 글로벌 스톱 폴리서에 의해 지원되는 가장 가까운 값을 모읍니다. 지원되는 비율은 10 fps 또는 25 kbps로 나눌 수 있습니다.

유닛 (Unit):

포트 스톱 폴리서 속도 측정 유닛을 fps, kfps, kbps 또는 Mbps로 제어합니다.



## ■ 버튼

적용 (Apply):

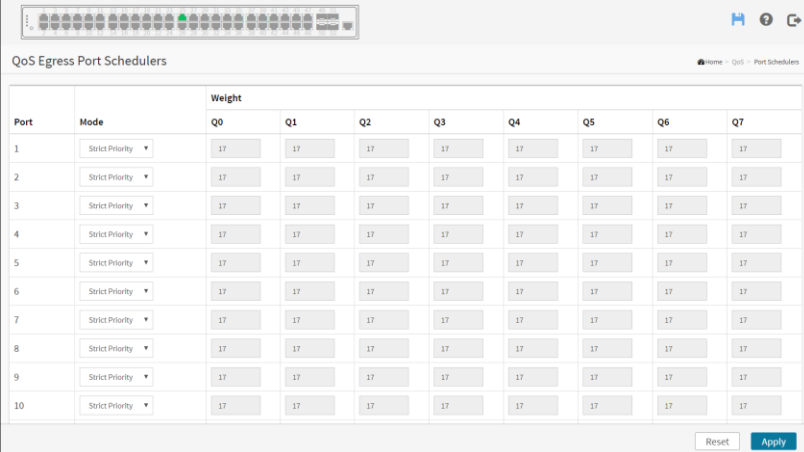
변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## 포트 스케줄러

이 섹션에서는 모든 스위치 포트의 QoS 외부 포트 스케줄러의 개요를 제공합니다. 그리고 페이지 헤더에 반영된 대로 포트는 현재 선택된 스택 유닛에 속합니다.



| Port | Mode              | Weight |    |    |    |    |    |    |    |
|------|-------------------|--------|----|----|----|----|----|----|----|
|      |                   | Q0     | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 |
| 1    | Strict Priority ▼ | 17     | 17 | 17 | 17 | 17 | 17 | 17 | 17 |
| 2    | Strict Priority ▼ | 17     | 17 | 17 | 17 | 17 | 17 | 17 | 17 |
| 3    | Strict Priority ▼ | 17     | 17 | 17 | 17 | 17 | 17 | 17 | 17 |
| 4    | Strict Priority ▼ | 17     | 17 | 17 | 17 | 17 | 17 | 17 | 17 |
| 5    | Strict Priority ▼ | 17     | 17 | 17 | 17 | 17 | 17 | 17 | 17 |
| 6    | Strict Priority ▼ | 17     | 17 | 17 | 17 | 17 | 17 | 17 | 17 |
| 7    | Strict Priority ▼ | 17     | 17 | 17 | 17 | 17 | 17 | 17 | 17 |
| 8    | Strict Priority ▼ | 17     | 17 | 17 | 17 | 17 | 17 | 17 | 17 |
| 9    | Strict Priority ▼ | 17     | 17 | 17 | 17 | 17 | 17 | 17 | 17 |
| 10   | Strict Priority ▼ | 17     | 17 | 17 | 17 | 17 | 17 | 17 | 17 |

### 웹 인터페이스

웹 인터페이스에서 QoS 포트 스케줄러를 설정하려면:

1. Quality of Service와 포트 스케줄러를 클릭합니다.
2. 포트와 QoS 외부 포트 스케줄러를 클릭합니다.
3. 포트와 스케줄러 모드를 스크롤 하고 대기열 셰이퍼 항목을 지정합니다.
4. 적용을 클릭하고 설정을 저장합니다.
5. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아갑니다.

### ■ 항목 설명:

포트 (Port):

동일한 열에 포함된 설정의 논리적 포트입니다.

모드 (Mode):

이 포트의 스케줄링 모드를 표시합니다.

Qn:

이 대기열과 포트의 가중치를 표시합니다.

스케줄러 모드 (Scheduler Mode):

엄격하게 관리되는 대기열 수 일정 및 이 스위치 포트에 편중되어 관리되는 수를 제어합니다.

대기열 셰이퍼 활성화 (Queue Shaper Enable):

이 스위치 포트의 대기열에 대기열 셰이퍼 활성화 여부를 제어합니다.

대기열 셰이퍼 속도 (Queue Shaper Rate):

대기열 셰이퍼 속도를 제어합니다. "유닛"이 kbps인 경우 이 값은 100- 13107100로 제한됩니다.

그리고 "유닛"이 Mbps인 경우 1-13107입니다. 속도는 내부에서 대기열 셰이퍼에 의해 지원되는 가장 가까운 값을 모읍니다.

대기열 셰이퍼 유닛 (Queue Shaper Unit):

kbps 또는 Mbps로 대기열 셰이퍼 속도의 측정 유닛을 제어합니다.

대기열 셰이퍼 속도 타입 (Queue Shaper Rate-type):

대기열 셰이퍼의 속도 유형입니다. 허용되는 값은 다음과 같습니다:

Line: 셰이퍼가 라인 속도에서 동작하는 것을 지정합니다.

Data: 셰이퍼가 데이터 속도에서 동작하는 것을 지정합니다.

대기열 스케줄러 가중치 (Queue Scheduler Weight):

이 대기열의 무게를 제어합니다. 값은 1-100 사이입니다. 이 항목은 "스케줄러 모드"가 "Weighted"로 설정된 경우에만 표시됩니다.

대기열 스케줄러 퍼센트 (Queue Scheduler Percent):

이 대기열의 가중치 퍼센트를 표시합니다. 이 항목은 "스케줄러 모드"가 "Weighted"로 설정된 경우에만 표시됩니다.

포트 셰이퍼 활성화 (Port Shaper Enable):

포트 셰이퍼가 이 스위치 포트를 활성화하는지 여부를 제어합니다.

포트 셰이퍼 속도 (Port Shaper Rate):

포트 셰이퍼 속도를 제어합니다. 이 값은 "유닛"이 kbps인 경우 100- 13107100로 제한됩니다. 속도는 내부에서 포트 셰이퍼에 의해 지원되는 가장 가까운 값을 모읍니다.

포트 셰이퍼 유닛 (Port Shaper Unit):

kbps 또는 Mbps로 포트 셰이퍼 속도 측정 유닛을 제어합니다.

포트 셰이퍼 속도 타입 (Port Shaper Rate-type):

대기열 셰이퍼의 속도 유형입니다. 허용되는 값은 다음과 같습니다:

Line: 셰이퍼가 라인 속도에서 동작하는 것을 지정합니다.

Data: 셰이퍼가 데이터 속도에서 동작하는 것을 지정합니다.

## ■ 버튼

적용 (Apply):

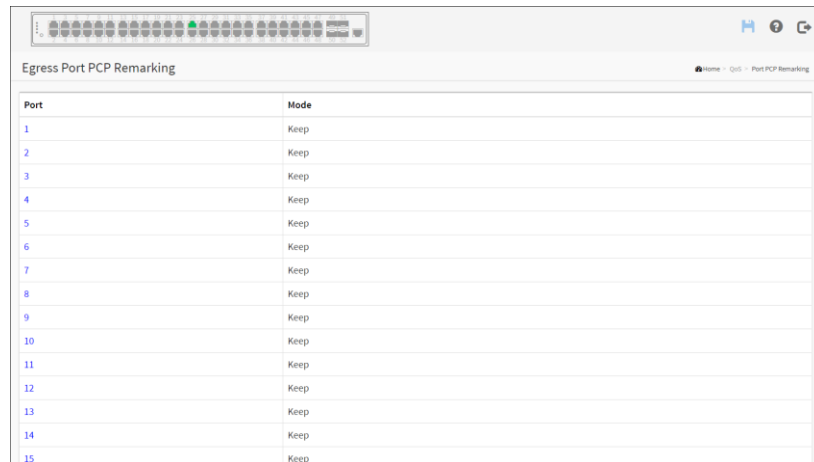
변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## 포트 PCP 리마킹

이 섹션에서는 모든 스위치 포트의 QoS 외부 포트 PCP 리마킹의 개요를 제공합니다. 그리고 페이지 헤더에 반영된 대로 다른 포트는 현재 선택된 스택 유닛에 속합니다.

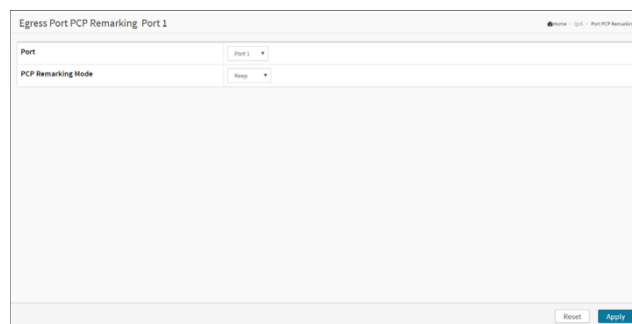


| Port | Mode |
|------|------|
| 1    | Keep |
| 2    | Keep |
| 3    | Keep |
| 4    | Keep |
| 5    | Keep |
| 6    | Keep |
| 7    | Keep |
| 8    | Keep |
| 9    | Keep |
| 10   | Keep |
| 11   | Keep |
| 12   | Keep |
| 13   | Keep |
| 14   | Keep |
| 15   | Keep |

### 웹 인터페이스

웹 인터페이스에서 QoS 포트 PCP 리마킹을 설정하려면:

1. Quality of Service와 포트 PCP 리마킹을 클릭합니다.
2. 포트를 클릭하고 QoS 포트 PCP 리마킹을 표시합니다.



3. 포트와 PCP 리마킹 모드를 스크롤 하고 대기열 셰이퍼 항목을 지정합니다.
4. 적용을 클릭해 설정을 저장합니다.

5. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아갑니다.

## ■ 항목 설명:

포트 (Port):

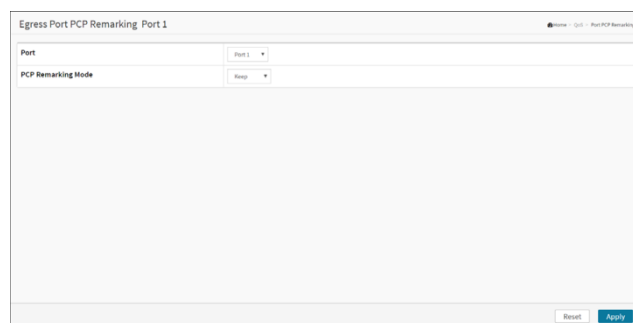
동일한 열에 포함된 설정의 논리적 포트입니다.

PCP 리마킹을 설정하려면 포트 번호를 클릭합니다.

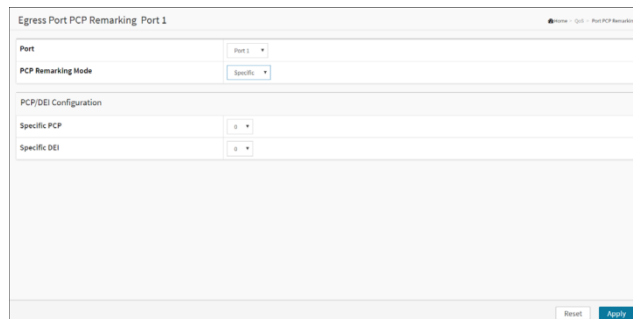
모드 (Mode):

이 포트의 PCP 리마킹 모드를 표시합니다.

Keep: 분류된 PCP/DEI 값을 사용합니다.



Specific: 초기값 PCP/DEI 값을 사용합니다.



Mapped: 매핑된 CoS와 DPL 버전을 사용합니다.

| Queue Priority | DP level | PCP | DEI |
|----------------|----------|-----|-----|
| 0              | 0        | 0   | 0   |
| 0              | 1        | 1   | 1   |
| 1              | 0        | 0   | 0   |
| 1              | 1        | 1   | 1   |
| 2              | 0        | 0   | 0   |
| 2              | 1        | 1   | 1   |
| 3              | 0        | 0   | 0   |
| 3              | 1        | 1   | 1   |
| 4              | 0        | 0   | 0   |
| 4              | 1        | 1   | 1   |
| 5              | 0        | 0   | 0   |
| 5              | 1        | 1   | 1   |
| 6              | 0        | 0   | 0   |
| 6              | 1        | 1   | 1   |
| 7              | 0        | 0   | 0   |
| 7              | 1        | 1   | 1   |

PCP/DEI 설정 (PCP/DEI Configuration):

모드가 기본값으로 설정되면 기본값 PCP 및 DEI 값을 제어합니다.

(QoS class, DP level) to (PCP, DEI) 매핑:

모드가 Mapped로 설정되는 경우 분류된 (QoS class, DP level) to (PCP, DEI) 값의 매핑을 제어합니다.

■버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## DSCP

### 포트 DSCP

이 섹션은 모든 스위치 포트에 대한 기본 QoS 포트 DSCP 구성 설정을 허용한 QoS 포트 DSCP 구성 설정 방법을 유저에게 제공합니다. 페이지 헤더에 의해 반영된 다른 설정은 현재 선택된 스택 유닛과 관련되어 있습니다.

| Port | Ingress                  |         | Classify | Egress Rewrite |
|------|--------------------------|---------|----------|----------------|
|      | Translate                |         |          |                |
| *    | <input type="checkbox"/> | <>      | <>       |                |
| 1    | <input type="checkbox"/> | Disable | Disable  |                |
| 2    | <input type="checkbox"/> | Disable | Disable  |                |
| 3    | <input type="checkbox"/> | Disable | Disable  |                |
| 4    | <input type="checkbox"/> | Disable | Disable  |                |
| 5    | <input type="checkbox"/> | Disable | Disable  |                |
| 6    | <input type="checkbox"/> | Disable | Disable  |                |
| 7    | <input type="checkbox"/> | Disable | Disable  |                |
| 8    | <input type="checkbox"/> | Disable | Disable  |                |
| 9    | <input type="checkbox"/> | Disable | Disable  |                |

#### 웹 인터페이스

웹 인터페이스에서 QoS 포트 DSCP 항목을 설정하려면:

1. Quality of Service, DSCP 및 포트 DSCP를 클릭합니다.
2. 내부 변환을 활성화 또는 비활성화 하고 분류한 항목을 스크롤 합니다.
3. Egress Rewrite 항목을 선택하려면 스크롤 합니다.
4. 적용을 클릭해 설정을 저장합니다.
5. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아갑니다.

#### ■ 항목 설명:

포트 (Port):

포트 칼럼은 dscp 내부 및 외부 설정을 구성할 수 있는 포트 목록을 표시합니다.



내부 (Ingress):

내부 설정에서 각 포트에 대한 내부 변경과 분류 설정이 가능합니다.

내부에서 가능한 2가지 설정 항목이 있습니다.

Translate: 내부 변경을 활성화 하려면 체크 박스를 클릭하세요.

Classify: 포트 분류는 4개의 다른 값이 있습니다.

Disable: 내부 DSCP 분류가 없습니다.

DSCP=0: 들어오는 (또는 활성화 시 변경된) DSCP가 0인 경우 분류합니다.

Selected: 특정 DSCP에 대한 DSCP 변경 창에 지정된 대로 분류가 활성화 된 선택된 DSCP만 분류합니다.

All: 모든 DSCP를 분류합니다.

외부 (Egress):

포트 외부 수정은 다음 항목 중 하나입니다.

Disable: 외부 수정이 없습니다.

Enable: 재매핑 없이 수정을 활성화 합니다.

Remap: 분석기에서 DSCP는 재매핑 되며 프레임은 리매핑 된 DSCP 값과 리마크됩니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## **DSCP 변경 (DSCP Translation)**

이 섹션은 스위치가 모든 스위치의 기본 QoS DSCP 변경 설정을 설정을 허용합니다. DSCP 변경은 내부 또는 외부에서 완료할 수 있습니다.

| DSCP    | Ingress   |                          | Egress  |
|---------|-----------|--------------------------|---------|
|         | Translate | Classify                 | Remap   |
| *       | <>        | <input type="checkbox"/> | <>      |
| 0 (BE)  | 0 (BE)    | <input type="checkbox"/> | 0 (BE)  |
| 1       | 1         | <input type="checkbox"/> | 1       |
| 2       | 2         | <input type="checkbox"/> | 2       |
| 3       | 3         | <input type="checkbox"/> | 3       |
| 4       | 4         | <input type="checkbox"/> | 4       |
| 5       | 5         | <input type="checkbox"/> | 5       |
| 6       | 6         | <input type="checkbox"/> | 6       |
| 7       | 7         | <input type="checkbox"/> | 7       |
| 8 (CS1) | 8 (CS1)   | <input type="checkbox"/> | 8 (CS1) |

Reset Apply

## 웹 인터페이스

웹 인터페이스에서 DSCP 변경 항목을 설정하려면:

1. Quality of Service, DSCP 및 DSCP 변경을 클릭합니다.
2. 내부 변경과 외부 리맵 항목을 설정하려면 스크롤 합니다.
3. 분류를 활성화 또는 비활성화 하려면 클릭합니다.
4. 적용을 클릭해 설정을 저장합니다.
5. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아갑니다.

## ■ 항목 설명:

DSCP:

선택된 DSCP 값의 최대 수는 64이며 유효 DSCP 값 범위는 0에서 63입니다.

내부 (Ingress):

QoS 클래스와 DPL 맵의 DSCP를 사용하기 전에 내부 쪽 DSCP는 새로운 DSCP로 처음 변경될 수 있습니다.

DSCP 변경에 대한 설정 항목은 2가지가 있습니다 –

Translate: 내부 쪽 DSCP가 (0-63) DSCP 값으로 변경 가능합니다.

Classify: 내부 쪽 분류를 활성화 하려면 클릭합니다.

외부 (Egress):

리맵하고 싶은 선택 메뉴에서 DSCP 값을 선택합니다. DSCP 값은 0에서 63입니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## DSCP 분류

이 섹션은 DSCP 값을 QoS 클래스와 DPL 값에 매핑하고 설정하는 방법을 유저에게 제공합니다.

페이지 헤더에 의해 반영된 다른 설정은 현재 선택된 스택 유닛과 관련되어 있습니다.

| Queue Priority | DSCP DP0 | DSCP DP1 | DSCP DP2 | DSCP DP3 |
|----------------|----------|----------|----------|----------|
| 0              | 0 (BE)   | 0 (BE)   | 0 (BE)   | 0 (BE)   |
| 1              | 0 (BE)   | 0 (BE)   | 0 (BE)   | 0 (BE)   |
| 2              | 0 (BE)   | 0 (BE)   | 0 (BE)   | 0 (BE)   |
| 3              | 0 (BE)   | 0 (BE)   | 0 (BE)   | 0 (BE)   |
| 4              | 0 (BE)   | 0 (BE)   | 0 (BE)   | 0 (BE)   |
| 5              | 0 (BE)   | 0 (BE)   | 0 (BE)   | 0 (BE)   |
| 6              | 0 (BE)   | 0 (BE)   | 0 (BE)   | 0 (BE)   |
| 7              | 0 (BE)   | 0 (BE)   | 0 (BE)   | 0 (BE)   |

웹 인터페이스

웹 인터페이스에서 DSCP 분류 항목을 설정하려면:

1. Quality of Service, DSCP 및 DSCP 변경을 클릭합니다.
2. DSCP 항목을 설정하려면 스크롤 합니다.
3. 적용을 클릭해 설정을 저장합니다.
4. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아갑니다.

## ■ 항목 설명:

대기열 우선권 (Queue Priority):

서비스 실제 클래스입니다.

DSCP DP0:

삭제 우선 레벨 0에 대한 분류된 DSCP 값 (0-63)을 선택합니다.

DSCP DP1:

삭제 우선 레벨 1에 대한 분류된 DSCP 값 (0-63)을 선택합니다.

DSCP DP2:

삭제 우선 레벨 2에 대한 분류된 DSCP 값 (0-63)을 선택합니다.

DSCP DP3:

삭제 우선 레벨 3에 대한 분류된 DSCP 값 (0-63)을 선택합니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## DSCP 기반 QoS

이 섹션은 유저에게 DSCP 기반 QoS 모드 설정 방법을 제공합니다. 이 페이지에서 모든 스위치에 대한 기본 QoS DSCP 기반 QoS 내부 분류 설정을 허용합니다.

| DSCP    | Trust                    | Queue Priority       | DPL                  |
|---------|--------------------------|----------------------|----------------------|
| *       | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> |
| 0 (BE)  | <input type="checkbox"/> | 0 ▼                  | 0 ▼                  |
| 1       | <input type="checkbox"/> | 0 ▼                  | 0 ▼                  |
| 2       | <input type="checkbox"/> | 0 ▼                  | 0 ▼                  |
| 3       | <input type="checkbox"/> | 0 ▼                  | 0 ▼                  |
| 4       | <input type="checkbox"/> | 0 ▼                  | 0 ▼                  |
| 5       | <input type="checkbox"/> | 0 ▼                  | 0 ▼                  |
| 6       | <input type="checkbox"/> | 0 ▼                  | 0 ▼                  |
| 7       | <input type="checkbox"/> | 0 ▼                  | 0 ▼                  |
| 8 (CS1) | <input type="checkbox"/> | 0 ▼                  | 0 ▼                  |
| 9       | <input type="checkbox"/> | 0 ▼                  | 0 ▼                  |

Reset Apply

## 웹 인터페이스

웹 인터페이스에서 DSCP-기반 QoS 내부 분류 항목을 설정하려면:

1. Quality of Service, DSCP 및 DSCP-기반 QoS를 클릭합니다.
2. 신뢰를 위해 DSCP를 활성화 또는 비활성화 합니다.
3. 스크롤 해 대기열 우선권과 DPL 항목을 선택합니다.
4. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아갑니다.

## ■ 항목 설명:

DSCP:

최대 지원되는 DSCP 값은 64입니다.

Trust:

DSCP 값이 신뢰 가능하면 체크를 클릭합니다.

대기열 우선권 (Queue Priority):

대기열 우선권은 0에서 7 사이입니다. 7이 가장 높습니다.

DPL:

삭제 우선 레벨 (0-3)

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

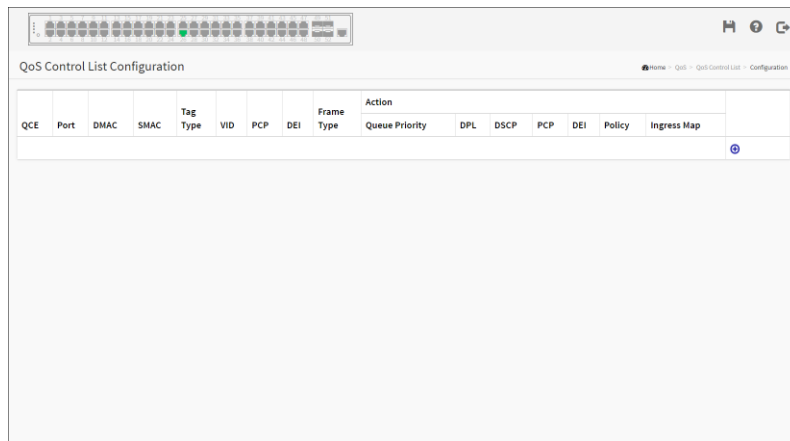
리셋 (Reset):

로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## QoS 제어 목록

### 설정


이 섹션은 QCE 구성인 QoS 제어 목록 (QCL)을 표시합니다. 각 열은 정의된 QCE를 설명합니다. 각 스위치의 QCE의 최대 수는 256입니다. 가장 아래의 플러스 사인을 클릭해 새로운 QCE를 목록에 추가합니다.



| QCE | Port | DMAC | SMAC | Tag Type | VID | PCP | DEI | Frame Type | Action         |     |      |     |     |        |             |
|-----|------|------|------|----------|-----|-----|-----|------------|----------------|-----|------|-----|-----|--------|-------------|
|     |      |      |      |          |     |     |     |            | Queue Priority | DPL | DSCP | PCP | DEI | Policy | Ingress Map |
| +   |      |      |      |          |     |     |     |            |                |     |      |     |     |        |             |

### 웹 인터페이스

웹 인터페이스에서 QoS 제어 목록 항목을 구성하려면:

1. Quality of Service, QoS 목록 및 구성을 클릭하세요.
2. 를 클릭해 새로운 QoS 제어 목록에 추가합니다.

The image shows the 'QCE Configuration' window. At the top, there's a breadcrumb trail: 'Home > QCE > QCE Control List > Configuration'. Below this is a 'Port Members' section with a table of 36 ports. Each port has a 'Member' checkbox, all of which are checked. Below the table is a scrollable list of configuration options, each with a dropdown menu set to 'Any': DMAC, SMAC, Tag, VID, PCP, DEI, Inner Tag, Inner VID, Inner PCP, Inner DEI, and Frame Type. Below this is an 'Action' section with several settings: Queue (0), Priority (0), DPL (Default), DSCP (Default), PCP (Default), DEI (Default), Policy (checkbox), and Ingress Map ID (checkbox). At the bottom right are three buttons: 'Cancel', 'Reset', and 'Apply'.

3. 모든 항목을 스크롤하고 포트 멤버를 선택해 QCE 룰에 연결합니다.
4. 적용을 클릭해 설정을 저장합니다.
5. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아갑니다.

## ■ 항목 설명:

QCE:

QCE 인덱스를 표시합니다.

포트 (Port):

QCE와 설정된 포트 목록을 표시합니다.

DMAC:

대상 MAC 주소를 표시합니다. 가능한 값은 다음과 같습니다:

Any: 어떠한 DMAC와도 일치합니다.

Unicast: 유니캐스트 DMAC와 일치합니다.



Multicast: 멀티캐스트 DMAC와 일치합니다.

Broadcast: 브로드캐스트 DMAC와 일치합니다.

<MAC>: 특정 DMAC와 일치합니다.

기본값은 'Any'입니다.

SMAC:

특정 소스 MAC 주소 또는 'Any'와 일치합니다.

포트가 DMAC/DIP에서 일치되도록 설정되면, 이 필드는 DMAC를 표시합니다.

태그 타입 (Tag Type):

태그 타입을 표시합니다. 가능한 값은 다음과 같습니다:

Any: 태그 지정 및 태그 미지정 프레임에 일치합니다.

Untagged: 태그 미지정 프레임에 일치합니다.

Tagged: 태그 지정 프레임에 일치합니다.

C-Tagged: C-태그된 프레임에 일치합니다.

S-Tagged: S-태그된 프레임에 일치합니다.

기본값은 'Any'입니다.

VID:

(VLAN ID), 특정 VID 또는 VID 범위 중 하나를 표시합니다. VID는 1-4095 범위 또는 'Any'입니다.

PCP:

우선권 코드 포인트: PCP 유효한 값은 (0, 1, 2, 3, 4, 5, 6, 7) 또는 범위(0-1, 2-3, 4-5, 6-7, 0-3, 4-7)

또는 'Any'로 특정됩니다.

DEI:

삭제 조건 표시자: DEI 유효 값은 0, 1 또는 'Any'입니다.

프레임 타입 (Frame Type):

수신하는 프레임을 찾기 위한 프레임 타입을 표시합니다. 가능한 프레임 타입은 다음과 같습니다:

Any: QCE는 모든 프레임 타입에 일치합니다.

Ethernet: 이더넷 프레임 타입(Ether Type 0x600-0Xffff과 함께)만 허용됩니다.

LLC: (LLC) 프레임만 허용됩니다.

SNAP: (SNAP) 프레임만 허용됩니다.

IPv4: QCE는 IPV4 프레임에만 일치합니다.

IPv6: QCE가 IPV6 프레임에만 일치합니다.

동작 (Action):

설정된 항목이 프레임의 콘텐츠와 일치하면 내부 프레임에서 실행된 분류 동작을 표시합니다.

가능한 동작은 다음과 같습니다:

CoS: 서비스 클래스를 분류합니다.

DPL: 삭제 우선 레벨을 분류합니다.

DSCP: DSCP 값을 분류합니다.

PCP: PCP 값을 분류합니다.

DEI: DEI 값을 분류합니다.

Policy: ACL 정책 번호를 분류합니다.

수정 버튼:

다음 버튼을 이용해 테이블에서 각 QCE (QoS Control Entry)를 수정할 수 있습니다.



: 현재 열 전에 새로운 QCE를 삽입합니다.



: QCE를 편집합니다.



: QCE를 목록 위로 올립니다.



: QCE를 목록 아래로 올립니다.



: QCE를 삭제합니다.



: 가장 낮은 플러스 사인은 QCE 목록 가장 아래에 새 엔트리를 추가합니다.

포트 멤버 (Port Members):

체크 박스 버튼을 체크해 QCL 엔트리의 포트를 포함합니다. 기본값으로 모든 포트는 포함됩니다.

키 항목 (Key Parameters):

키 설정은 다음과 같습니다:

DMAC Destination MAC address: 가능한 값은 'Unicast', 'Multicast', 'Broadcast', 'Specific' (xx-xx-xx-xx-xx-xx) 또는 'Any'입니다.

SMAC Source MAC address: xx-xx-xx-xx-xx-xx 또는 'Any' 입니다.

태그 필드의 태그 값은 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' 또는 'Any' 입니다.

VLAN ID의 VID 유효 값은 1-4095 또는 'Any' 입니다; 유저는 특정 값 또는 VID 범위 중 하나를 입력할 수 있습니다.

PCP 유효 값 PCP는 특정 (0, 1, 2, 3, 4, 5, 6, 7) 또는 범위 range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) 또는 'Any'입니다.

DEI의 DEI 유효 값은 '0', '1' 또는 'Any'입니다.

내부태그 필드의 내부태그 값은 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' 또는 'Any' 입니다.

내부VLAN ID의 내부VID 유효 값은 1-4095 범위 또는 'Any'의 값이 될 수 있습니다; 유저는 특정 값 또는 VID 범위 중 하나를 입력할 수 있습니다.

내부PCP의 내부PCP 유효 값은 특정 (0, 1, 2, 3, 4, 5, 6, 7) 또는 범위 (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) 또는 'Any' 입니다.

내부DEI의 내부DEI 유효 값은 '0', '1' 또는 'Any'입니다.

프레임 타입은 다음의 값 중 하나입니다:

Any

EtherType

LLC

SNAP

IPv4

IPv6

주의: 모든 프레임 타입은 아래에 설명됩니다.

Any:

프레임의 모든 타입을 허용합니다.

EtherType:

유효 Ether Type은 0x800(IPv4) 및 0x86DD(IPv6) 또는 'Any'를 제외한 0x600-0xFFFF입니다.

LLC:

DSAP 주소 유효 DSAP (Destination Service Access Point)는 0x00 에서 0xFF 또는 'Any'에 따라 달라질 수 있습니다.

SSAP 주소 유효 SSAP (Source Service Access Point)는 0x00 에서 0xFF 또는 'Any'에 따라 달라질 수 있습니다.

컨트롤 유효 제어 필드는 0x00 에서 0xFF 또는 'Any'에 따라 달라질 수 있습니다.

SNAP:

PID 유효 PID (즉, Ether Type)는 0x0000-0Xffff 또는 'Any'에 따라 달라질 수 있습니다.

IPv4:

프로토콜 IP 프로토콜 번호: (0-255, 'TCP' or 'UDP') 또는 'Any' 입니다.

값/마스크 포맷 또는 'Any'에서 소스 IP 지정 소스 IP 주소입니다. IP 및 마스크는 x, y, z 및 w 0에서 255 사이의 10진수를 갖는 x.y.z.w 포맷입니다. 마스크가 32 비트 2진수로 변환되고 왼 쪽에서 오른 쪽으로 읽을 때 다음의 첫 번째 0인 모든 비트 또는 0이 되어야 합니다.

대상 IP 특정 대상 IP 주소는 값/마스크 포맷 또는 'Any'입니다.

IP 프래그먼트 IPv4 프레임 프래그먼트 옵션: 'Yes', 'No' 또는 'Any'

DSCP Diffserv Code Point value (DSCP): 특정 값, 범위의 값 또는 'Any'가 될 수 있습니다. DSCP 값은 BE, CS1-CS7, EF 또는 AF11-AF43을 포함한 0-63입니다.

스포츠 소스 TCP/UDP 포트: (0-65535) 또는 'Any'입니다, IP 프로토콜 UDP/TCP에 적용 가능한 특정 또는 포트 범위입니다.

IPv6:

프로토콜 IP 프로토콜 번호: (0-255, 'TCP' or 'UDP') 또는 'Any' 입니다.

값/마스크 포맷 또는 'Any'의 IPv6 소스 주소의 소스 IP 32 LS 비트입니다.

대상 IP 특정 대상 IP 주소는 값/마스크 포맷 또는 'Any'입니다.

DSCP Diffserv Code Point value (DSCP): 특정 값, 범위의 값 또는 'Any'가 될 수 있습니다. DSCP 값은 BE, CS1-CS7, EF 또는 AF11-AF43을 포함한 0-63입니다.

스포츠 소스 TCP/UDP 포트: (0-65535) 또는 'Any'입니다, IP 프로토콜 UDP/TCP에 적용 가능한 특정 또는 포트 범위입니다.

Dport Destination TCP/UDP 포트: (0-65535) 또는 'Any'입니다, IP 프로토콜 UDP/TCP에 적용 가능한 특정 또는 포트 범위입니다.

동작 항목 (Action Parameters):

CoS Class of Service: (0-7) 또는 'Default'

DPL Drop Precedence Level: (0-3) 또는 'Default'.

DSCP DSCP: (0-63, BE, CS1-CS7, EF 또는 AF11-AF43) 또는 'Default'.

PCP PCP: (0-7) 또는 'Default'. 주의: PCP 및 DEI는 독립적으로 설정할 수 없습니다.

DEI DEI: (0-1) 또는 'Default'.

Policy ACL Policy number: (0-127) 또는 'Default' (공백 필드).

'Default'는 초기값으로 분류된 값이 QCE로 수정되지 않는다는 뜻 입니다.

## ■버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다.

리셋 (Reset):

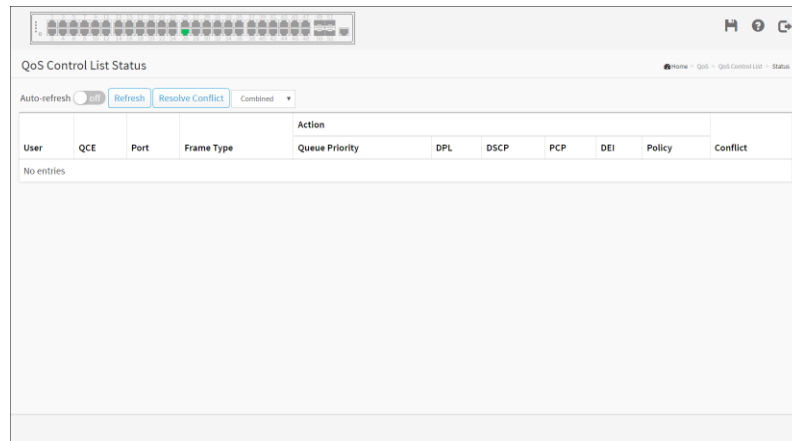
로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

취소 (Cancel):

설정 변경을 저장하지 않고 이전 페이지로 되돌아 갑니다.

## 상태

이 섹션에서 여러 QCL 유저가 QCL 상태를 설정하고 표시하는 방법을 설명합니다. 각 열은 정의된 QCE를 설명합니다. 하드웨어 제한으로 인해 특정 QCE가 하드웨어에 적용되지 않으면 충돌이 일어납니다. 최대 QCE 번호는 각 스위치의 256입니다.



### 웹 인터페이스

웹 인터페이스에서 QoS 컨트롤 목록 상태를 표시하려면:

1. Quality of Service, QoS 컨트롤 목록 및 상태를 클릭합니다.
2. 정보를 새로 고침 하려면 "자동 새로 고침"을 클릭합니다.
3. combined, static, Voice VLAN 및 conflict를 선택하려면 스크롤 하세요.
4. "새로 고침"을 클릭해 MVR 현황 정보 엔트리를 새로 고침 합니다.

### ■ 항목 설명:

유저 (User):

QCL 유저를 나타냅니다.

QCE:

QCE 인덱스를 나타냅니다.

포트 (Port)

QCE로 설정된 포트 목록을 나타냅니다.

프레임 타입 (Frame Type):

프레임 타입을 표시합니다. 가능한 값은 다음과 같습니다:

Any: 모든 프레임 타입에 일치합니다.

Ethernet: EtherType 프레임 타입에 일치합니다.

LLC: (LLC) 프레임 타입에 일치합니다.

SNAP: (SNAP) 프레임 타입에 일치합니다.

IPv4: IPv4 프레임 타입에 일치합니다.

IPv6: IPv6 프레임 타입에 일치합니다.

동작 (Action):

설정된 항목이 프레임 콘텐츠와 일치하는 경우 내부 프레임 상에 분류된 동작을 표시합니다.

가능한 값은 다음과 같습니다:

CoS: Class of Service를 분류합니다.

DPL: Drop Precedence Level을 분류합니다.

DSCP: DSCP 를 분류합니다.

PCP: PCP 값을 분류합니다.

DEI: DEI 값을 분류합니다.

Policy: ACL Policy 번호를 분류합니다.

Ingress Map: Ingress Map ID를 분류합니다.

충돌 (Conflict):

QCL 엔트리의 충돌 상태를 표시합니다. QCE를 추가하는데 필요한 리소스가 가능하지 않을 수 있습니다. 이러한 경우 충돌 상태를 'Yes'로 표시하며, 그렇지 않은 경우 항상 'No'입니다. '(충돌 해결)Resolve Conflict' 버튼을 눌러 충돌이 QCL 엔트리 추가에 필요한 H/W 리소스를 해제함으로써 해결될 수 있음을 참조하십시오.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 즉시 새로 고칩니다.

Combined:

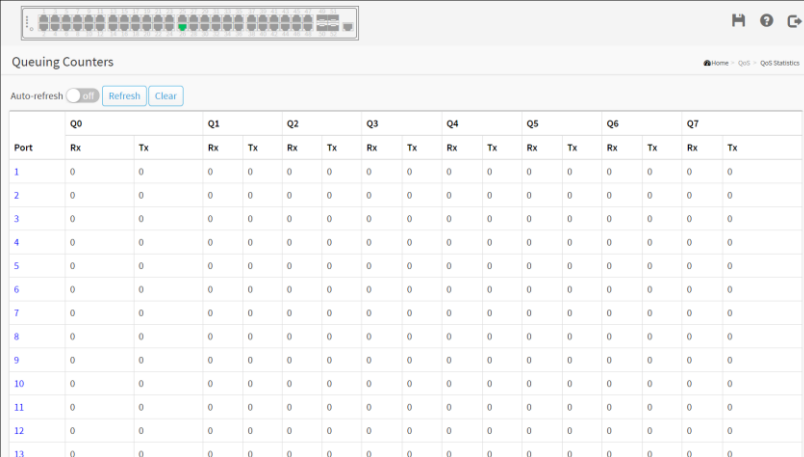
드롭 다운 목록에서 QCL 상태를 선택합니다.

충돌 해결 (Resolve Conflict):

QCL 엔트리 충돌 상태가 'yes'인 경우 클릭해서 QCL 엔트리 추가에 필요한 리소스를 해제하십시오.

## QoS 현황

이 페이지는 모든 스위치 포트에 대한 여러 대기열 현황을 제공합니다.



Queuing Counters

Auto-refresh: ☐ Refresh Clear

| Port | Q0 |    | Q1 |    | Q2 |    | Q3 |    | Q4 |    | Q5 |    | Q6 |    | Q7 |    |
|------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|      | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx |
| 1    | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 2    | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 3    | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 4    | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 5    | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 6    | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 7    | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 8    | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 9    | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 10   | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 11   | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 12   | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |
| 13   | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  | 0  |

### 웹 인터페이스

웹 인터페이스에서 대기열 카운터를 표시하려면:

1. Quality of Service와 QoS 현황을 클릭합니다.
2. 정보를 자동으로 새로 고침 하려면 "자동 새로 고침"을 클릭합니다.
3. 대기열 카운터를 새로 고침 하려면 "새로 고침"을 클릭하세요. 또는 모든 정보를 삭제하려면 "삭제 (Clear)"를 클릭합니다.

### ■ 항목 설명:

포트 (Port):

동일한 열에 포함된 설정을 위한 논리적 포트입니다.

Qn:

뽀은 대기열 번호입니다. 포트당 8 QoS 대기열이 있습니다. Q0은 가장 낮은 순위의 대기열입니다.

Rx/Tx:

대기열 당 수신 및 전송된 패킷의 수입니다.



## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고칩니다.

삭제 (Clear)

클릭해 페이지를 삭제합니다.

## WRED

이 페이지에서 Random Early Detection (RED) 설정을 구성할 수 있습니다. 대기열의 다양한 RED 설정을 통해 대기열 간 Weighted Random Early Detection (WRED) 동작이 가능합니다. 설정은 스위치의 모든 포트에 전체적으로 적용됩니다.

| Group | Queue | DPL | Enable                   | Min | Max | Max Unit           |
|-------|-------|-----|--------------------------|-----|-----|--------------------|
| 1     | 0     | 1   | <input type="checkbox"/> | 0   | 50  | Drop Probability ▼ |
| 1     | 0     | 2   | <input type="checkbox"/> | 0   | 50  | Drop Probability ▼ |
| 1     | 0     | 3   | <input type="checkbox"/> | 0   | 50  | Drop Probability ▼ |
| 1     | 1     | 1   | <input type="checkbox"/> | 0   | 50  | Drop Probability ▼ |
| 1     | 1     | 2   | <input type="checkbox"/> | 0   | 50  | Drop Probability ▼ |
| 1     | 1     | 3   | <input type="checkbox"/> | 0   | 50  | Drop Probability ▼ |
| 1     | 2     | 1   | <input type="checkbox"/> | 0   | 50  | Drop Probability ▼ |
| 1     | 2     | 2   | <input type="checkbox"/> | 0   | 50  | Drop Probability ▼ |
| 1     | 2     | 3   | <input type="checkbox"/> | 0   | 50  | Drop Probability ▼ |
| 1     | 3     | 1   | <input type="checkbox"/> | 0   | 50  | Drop Probability ▼ |
| 1     | 3     | 2   | <input type="checkbox"/> | 0   | 50  | Drop Probability ▼ |

Reset Apply

### 웹 인터페이스

웹 인터페이스에서 Random Early Detection을 구성하고 표시하려면:

1. Quality of Service와 WRED를 클릭합니다.
2. 모든 항목을 스크롤하고 Weighted Random Early Detection (WRED) 설정을 선택합니다.
3. 적용을 클릭해 설정을 저장합니다.
4. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아갑니다.

### ■ 항목 설명:

포트 (Port):

동일한 열에 포함된 설정을 위한 논리적 포트입니다.

그룹 (Group):

다음 설정을 적용하는 WRED 그룹 번호입니다.

대기열 (Queue):

다음 설정을 적용하는 대기열 번호 (CoS)입니다.

DPL:

다음 설정을 적용하는 Drop Precedence Level입니다.

Enable:

이 엔트리의 RED 활성화 여부를 제어합니다.

Min:

더 낮은 RED 채움 레벨 한계점을 제어합니다. 대기열 채움 레벨이 이 한계점 아래인 경우 삭제 우선 순위는 0입니다. 이 값은 0-100%로 제한됩니다.

Max:

삭제 우선 레벨 > 0 (노란색 프레임)이 표시된 프레임의 상단 RED 삭제 순위 또는 채움 레벨 한계점을 제어합니다. 이 값은 0-100%로 제한됩니다.

Max Unit:

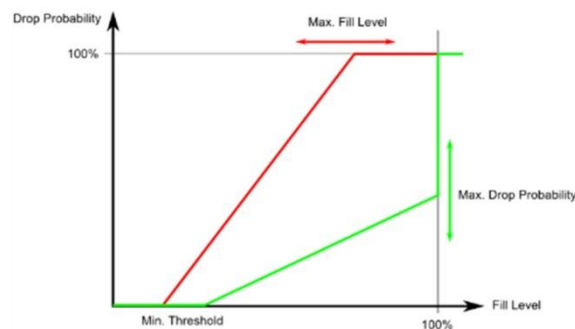
Max 유닛을 선택합니다. 가능한 값은 다음과 같습니다:

삭제 순위: Max는 삭제 순위를 100% 채움 레벨 바로 아래로 제어합니다.

채움 레벨: Max는 삭제 순위가 100%에 도달하는 채움 레벨을 제어합니다.

### RED 삭제 우선 순위 기능

다음의 그림은 삭제 우선 순위(drop probability) 대 채움 레벨(fill level) 기능을 관련 변수와 함께 표시합니다.



Min은 대기열이 무작위로 삭제 우선 레벨 > 0 (노란색 프레임)이 표시된 프레임을 삭제하기 시작하는 채움 레벨입니다.

Max 유닛이 '삭제 우선 순위' (녹색 선)인 경우, 채움 레벨이 100% 바로 아래이면 Max는 삭제 순위를 제어합니다.

Max 유닛이 '채움 레벨 (적색 선)'인 경우, Max는 삭제 순위가 100%에 도달하는 채움 레벨을 제어합니다.

이 설정으로 인해 우선 순위 레벨 0 (녹색 선)으로 표시된 프레임에 대해 독점적으로 대기열의 일정 부분을 유보할 수 있습니다. 유보 부분은  $(100 - \text{Max}) \%$ 로 계산됩니다. 우선 순위 레벨 0 (녹색 선)으로 표시된 프레임은 절대 삭제되지 않습니다.

프레임의 삭제 우선 순위는 0에서 (Min 평균 대기열 채움 레벨에서) 연속적으로 최대 삭제 우선 순위 또는 채움 레벨로 증가합니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다

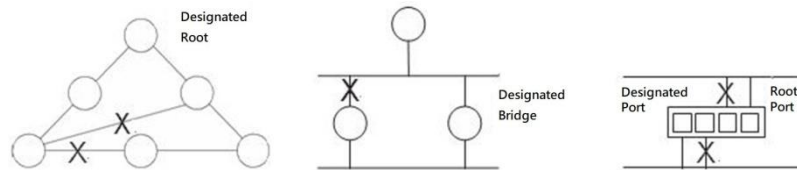
새로 고침 (Refresh):

클릭해 페이지를 새로 고침합니다.

## 개요

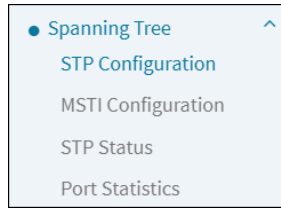
스패닝 트리 프로토콜 (Spanning Tree Protocol: STP)은 네트워크 루프를 탐지하고 비활성 하는데 사용할 수 있으며 스위치, 브리지 또는 라우터 간 백업 링크를 제공합니다. 스위치는 네트워크 통신에서 다른 브리지 장치 (STP 호환 스위치, 브리지 또는 라우터)와 상호 작용이 가능하며 네트워크 상의 두 개의 스테이션 사이에 하나의 루트만이 존재하도록 합니다. 또한 주 링크가 작동하지 않을 때 자동으로 백업 링크를 제공합니다.

**STP** -STP는 스패닝 트리 네트워크의 루트로써 브리지 장치(STP 호환 스위치, 브리지 또는 라우터)를 선택하기 위해 분산된 알고리즘을 사용합니다. 이는 장치에서 각 브리지 장치 (루트 장치 제외)의 루트 포트를 선택하며 루트 장치로 패킷 전송 시 가장 낮은 경로 비용을 발생시킵니다. 그리고 각 LAN에서 지정된 브리지 장치를 선택하며 LAN에서 루트 장치로 패킷 전송 시 가장 낮은 비용을 발생시킵니다. 지정된 브리지 장치에 연결된 모든 포트는 지정된 포트로 할당됩니다. 가장 낮은 비용 스패닝 트리를 지정한 후 모든 루트 포트와 지정 포트를 허용하며 모든 다른 포트는 비활성 합니다. 따라서 네트워크 패킷은 루트 포트와 지정 포트 사이에만 전송 가능하며 가능한 네트워크 루프를 제거합니다.



일단 안정적인 네트워크 토폴로지가 생성되면 모든 브리지에서 루트 브리지에서 전송된 Hello BPDUs (Bridge Protocol Data Units) 소리를 들을 수 있습니다. 사전 설정된 간격 (최대 기간)브리지에서 Hello BPDUs 소리가 확인되지 않으면, 브리지는 루트 브리지로의 링크가 작동하지 않는 것으로 추정합니다. 따라서 이 브리지는 다른 브리지로 네트워크 재설정을 위한 조정을 시작해 유효한 네트워크 토폴로지를 재생성합니다.

메뉴는 다음과 같습니다:



## STP 설정

이 섹션에서는 스페닝 트리 프로토콜 활성화 여부를 선택할 수 있으며 원하는 프로토콜 버전을 선택할 수 있다는 것을 설명합니다.

STP Bridge Configuration

Basic Settings

Protocol Version: MSTP

Bridge Priority: 32768

Hello Time: 2

Forward Delay: 15

Max Age: 20

Maximum Hop Count: 20

Transmit Hold Count: 6

Advanced Settings

Edge Port BPDU Filtering: ☐

Edge Port BPDU Guard: ☐

Port Error Recovery: ☐

Port Error Recovery Timeout:

Root Guard

| Port | Root Guard               |
|------|--------------------------|
| 0    | <input type="checkbox"/> |
| 1    | <input type="checkbox"/> |
| 2    | <input type="checkbox"/> |
| 3    | <input type="checkbox"/> |
| 4    | <input type="checkbox"/> |

Reset Apply

### 웹 인터페이스

웹 인터페이스에서 스페닝 트리 프로토콜 버전을 설정하려면:

1. 스페닝 트리 및 STP 설정을 클릭합니다.
2. 스크롤 해 항목을 선택하고 기본 설정의 비어 있는 필드에 가능한 항목 값을 입력합니다.
3. 항목을 활성화 또는 비활성화 하며 고급 설정의 비어 있는 필드에 가능한 항목 값을 입력합니다.
4. 적용을 클릭해 설정을 저장합니다.
5. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아갑니다.

## ■ 항목 설명:

### 기본 설정 (Basic Settings)

프로토콜 버전 (Protocol Version):

MSTP / RSTP / STP 프로토콜 버전 설정입니다. 유효 값은 STP, RSTP 및 MSTP입니다.

브리지 우선권 (Bridge Priority):

브리지 우선권을 제어합니다. 낮은 숫자 값일수록 우선 순위가 더 높습니다. 브리지 우선권에 더해 스위치의 6-바이트 MAC 주소와 연결된 STI 인스턴스 숫자는 브리지 식별자를 형성합니다.

MSTP 동작의 경우는 CIST의 우선 순위입니다. 그렇지 않으면 STP/RSTP 브리지의 우선 순위입니다.

Hello Time:

STP BPDU 전송 간 간격입니다. 유효 값은 1에서 10 초입니다. 기본값은 2초입니다.

주의: 기본값에서 이 항목을 변경하는 것은 권장하지 않습니다. 사용자의 네트워크에 악영향을 끼칠 수 있습니다.

포워딩 지연 (Forward Delay):

(STP 호환 모드에서 사용된) 포워딩에 루트와 지정 포트를 전송하기 위해 STP 브리지로 사용된 지연입니다. 유효 값 범위는 4에서 30초입니다.

최대 시간 (Max Age):

루트 브리지 시 브리지로 전송된 정보의 최대 시간입니다. 유효 값은 6에서 40초이며 최대 시간은  $(\text{FwdDelay}-1)*2$ 입니다.

최대 홉 수 (Maximum Hop Count):

MSTI 부분의 경계에서 동작한 MSTI 정보에 대한 남은 홉의 초기 값입니다. 이는 루트 브리지가 BPDU 정보를 분산할 수 있는 브리지 수를 정의합니다. 유효 값은 6에서 40홉입니다.

전송 보류 수 (Transmit Hold Count):

브리지 포트가 초당 전송할 수 있는 BPDU의 수입니다. 초과 시 다음 BPDU 전송이 지연될 것입니다. 유효 값은 초당 1에서 10 BPDU입니다.



**고급 설정 (Advanced Settings)**

에지 포트 BPDU 필터링 (Edge Port BPDU Filtering):

에지로 설정된 포트가 BPDU를 전송 및 수신할지 여부를 제어합니다.

에지 포트 BPDU 가드 (Edge Port BPDU Guard):

에지로 설정된 포트가 BPDU를 받자마자 자체 비활성화 할지 여부를 제어합니다. 포트는 에러-비활성 상태이며 액티브 토폴로지에서 삭제됩니다.

포트 에러 복구 (Port Error Recovery):

시정 시간 후에 에러-비활성 상태의 포트를 자동으로 활성화 하도록 제어합니다. 복구가 활성화 되지 않으며 포트는 비활성화 되고 일반 STP 동작에서 다시 활성화 해야 합니다. 조건은 시스템 재부팅에 의해 정해집니다.

포트 에러 회복 타임아웃 (Port Error Recovery Timeout)

에러-비활성화 상태의 포트가 활성화 되기 전 경과하는 시간입니다. 유효 값은 30에서 86400초입니다. (24시간)

**■버튼**

적용 (Apply):

변경 사항을 저장하려면 클릭합니다

리셋 (Reset):

클릭하면 로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## MSTI 설정

브릿지 인스턴스 스위치의 스페닝 트리 프로토콜 실행 전, 정확하게 매핑되지 않은 VLAN을 수신하므로 CIST는 정확한 매핑이 불가능합니다. 따라서 MSTI에 매핑된 VLAN 목록을 설정해야 합니다. VLAN은 콤마 및/또는 공백으로 분리되어야 합니다. VLAN은 하나의 MSTI만 매핑 가능합니다. 사용되지 않는 MSTI는 공백으로 남겨둡니다. (즉, MSIT에 매핑된 VLAN이 없습니다.)

이 섹션에서 유저는 현재 STP MSTI 브릿지 인스턴스 우선권 설정과 검사하며 변경할 수 있습니다.

| Instance | VLANs Mapped                          | MSTI Priority | MSTI Port            |
|----------|---------------------------------------|---------------|----------------------|
| CIST     | Unmapped VLANs are mapped to the CIST | 32768 ▼       | <a href="#">Edit</a> |
| MSTI1    | Example: 2,3-5,11,13,20-40            | 32768 ▼       | <a href="#">Edit</a> |
| MSTI2    | Example: 2,3-5,11,13,20-40            | 32768 ▼       | <a href="#">Edit</a> |
| MSTI3    | Example: 2,3-5,11,13,20-40            | 32768 ▼       | <a href="#">Edit</a> |
| MSTI4    | Example: 2,3-5,11,13,20-40            | 32768 ▼       | <a href="#">Edit</a> |

### 웹 인터페이스

웹 인터페이스에서 스페닝 트리 MSTI를 설정하려면:

1. 스페닝 트리 및 MSTI 설정을 클릭합니다.
2. 필드의 설정 식별 항목을 지정합니다. 빈 필드에 매핑된 VLAN을 지정합니다.
3. 적용을 클릭해 설정을 저장합니다.
4. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아갑니다.
5. 편집을 클릭해 STP CIST 포트 설정을 구성합니다.

## ■ 항목 설명:

### 설정 식별 (Configuration Identification)

설정 이름 (Configuration Name):

VLAN to MSTI 매핑 식별 이름입니다. 브릿지는 이름과 변경 (하단 참조) 및 MSTI(내부위치) 의 스페닝 트리 공유를 위해 VLAN-to-MSTI 매핑 설정을 공유해야 합니다. 이름은 최대 32자입니다.

설정 변경 (Configuration Revision):

위에서 설정한 이름의 MSTI 설정 변경입니다. 정수 0에서 65535이어야 합니다.

### MSTI 매핑 (MSTI Mapping)

인스턴스 (Instance):

브릿지 인스턴스입니다. 정확하게 매핑되지 않은 VLAN을 수신하므로 CIST는 정확한 매핑이 불가능합니다.

매핑된 VLAN (VLANs Mapped):

MSTI에 매핑된 VLAN 목록입니다. VLAN은 싱글 (1에서 4094 사이의 xx,xx) VLAN 또는 범위(xx-yy)로 주어지며, 이는 콤마 및/또는 공백으로 구별되어야 합니다. VLAN은 MSTI에만 매핑 가능합니다. 사용되지 않는 MSTI는 공백으로 남겨둡니다. (즉, MSIT에 매핑된 VLAN이 없습니다.) 예시: 2,5,20-40.

MSTI 우선권 (MSTI Priority):

브릿지 우선 순위를 제어합니다. 낮은 숫자일수록 더 높은 우선권을 갖습니다. 브릿지 우선권에 더해 스위치의 6-바이트 MAC 주소와 서로 연결된 MSTI 인스턴스 번호는 브릿지 식별자를 형성합니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다

리셋 (Reset):

클릭하면 로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

MSTI 포트 (MSTI Port):

STP CIST 포트 구성을 설정하려면 클릭하십시오.

STP CIST Port Configuration Home > Spanning Tree > MSTI Configuration

---

CIST Aggregated Port Configuration

| Port | STP Enabled                         | Path Cost | Priority | Admin Edge | Auto Edge                           | Restricted               |                          |                          | Point-to-point |
|------|-------------------------------------|-----------|----------|------------|-------------------------------------|--------------------------|--------------------------|--------------------------|----------------|
|      |                                     |           |          |            |                                     | Role                     | TCN                      | BPDU Guard               |                |
| -    | <input checked="" type="checkbox"/> | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Forced True    |

---

CIST Normal Port Configuration

| Port | STP Enabled                         | Path Cost | Priority | Admin Edge | Auto Edge                           | Restricted               |                          |                          | Point-to-point |
|------|-------------------------------------|-----------|----------|------------|-------------------------------------|--------------------------|--------------------------|--------------------------|----------------|
|      |                                     |           |          |            |                                     | Role                     | TCN                      | BPDU Guard               |                |
| *    | <input checked="" type="checkbox"/> | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto           |
| 1    | <input checked="" type="checkbox"/> | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto           |
| 2    | <input checked="" type="checkbox"/> | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto           |
| 3    | <input checked="" type="checkbox"/> | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto           |
| 4    | <input checked="" type="checkbox"/> | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto           |

[Back to MSTI Configuration](#)
[Reset](#)
[Apply](#)

## ■ 항목 설명:

포트 (Port):

논리적 STP 포트의 스위치 포트 번호입니다.

STP 활성화 (STP Enabled):

스위치 포트 상에서 STP 활성화 여부를 제어합니다. 이 필드는 음성 VLAN 기능이 활성화 된 경우에만 읽힙니다. 음성 VLAN 포트 모드는 이 필드가 활성화 상태일 때만 읽힙니다.

경로 비용 (Path Cost):

포트에 의해 발생하는 경로 비용을 제어합니다. 자동 설정은 802.1D 권장 값을 이용한 물리적 링크 속도에 의해 적절하게 경로 비용을 설정합니다. 특정 설정을 이용해 유저 정의 값이 입력됩니다. 경로 비용은 네트워크 액티브 토폴로지 구축 시 사용됩니다. 더 높은 경로 비용 포트를 위해 포트를 포워딩 함으로써 더 낮은 경로 비용 포트가 선택됩니다. 유효 값은 1에서 200000000의 범위입니다.

우선권 (Priority):

포트 우선권을 제어합니다. 동일한 포트 비용 (상단 참조)을 갖는 포트의 우선권을 제어하는데 사용됩니다.

AdminEdge:

OperEdge 플래그가 설정 또는 삭제로 시작될지에 대해 제어합니다. (포트 초기화 시 초기 OperEdge 상태)

AutoEdge:

브리지 포트에서 브리지가 자동 에지 탐지 활성화 여부를 제어합니다. 포트 상에서 BPDU 수신 여부에서 operEdge를 얻습니다.

제한된 기능 (Restricted Role):

활성화 되면 최고의 스페닝 트리 우선권 벡터일지라도 CIST 또는 MSTI 루트 포트로서 선택되지 않기 위한 포트를 가져 옵니다. 루트 포트가 선택되면 이러한 포트는 대안 포트로서 선택됩니다. 설정하면 스페닝 트리 연결 부족을 야기할 수 있습니다. 스페닝 트리 액티브 토폴로지에 영향을 미치는 네트워크의 핵심 부분에 외부 브리지를 방지하기 위해 네트워크 관리자로 설정될 수 있습니다. 이러한 브리지는 관리자의 완벽한 제어 아래에 있지 않기 때문입니다. 이 기능은 또한 루트 가드로 알려져 있습니다.

제한된 TCN (Restricted TCN):

활성화 되면 수신된 토폴로지 변경 알림과 다른 포트에 토폴로지 변경이 누적되지 않도록 포트를 가져옵니다. 설정하면 지속적인 부정확한 러닝 스테이션 위치 정보의 결과로써 스페닝 트리의 액티브 토폴로지 변경 후에 일시적인 연결 손실을 초래할 수 있습니다. 해당 부분에 주소 플러싱을 야기하는 네트워크의 핵심 부분에 외부 브리지를 방지하기 위해 네트워크 관리자로 설정될 수 있습니다. 이러한 브리지는 관리자의 완벽한 제어 아래에 있지 않거나 연결된 LAN의 물리적 링크 상태를 주기적으로 전송합니다.

BPDU 가드 (BPDU Guard):

활성화 되면 유효 BPDU를 수신하는 대로 비활성화 하는 포트를 가져 옵니다. 유사 브리지 설정과 반대로 포트 에지 상태는 이 설정에 영향을 미치지 않습니다. 이 설정으로 인해 에러-비활성 상태 포트는 브리지 포트 에러 복구 설정 대상이기도 합니다.

포인트 to 포인트 (Point to Point):

포트가 공유 매체가 아닌 포인트 to 포인트 LAN으로 연결하는지 여부를 제어합니다. 이 것은 자동으로 지정되거나 true 또는 false 중 하나가 됩니다. 포워딩 상태로 전송은 공유 미디어 보다 포인트 to 포인트에서 더 빠릅니다.

## ■버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다

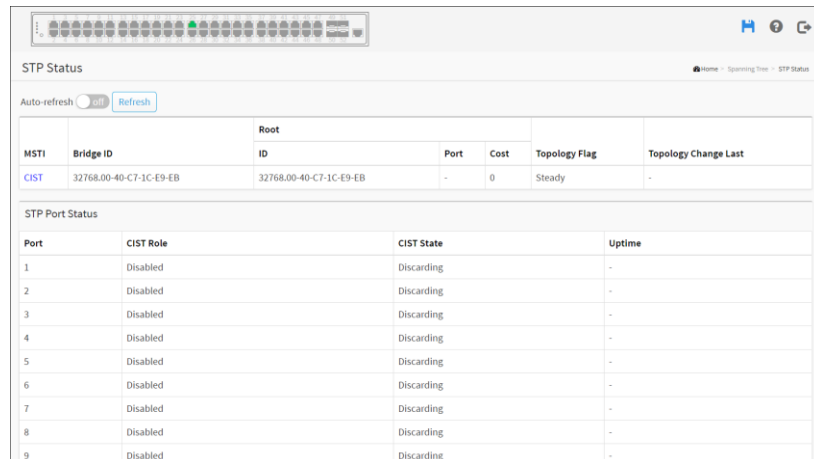
리셋 (Reset):

클릭하면 로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## STP 상태

이 페이지는 모든 STP 브리지 인스턴스의 상태 개요를 제공합니다.

아래의 테이블은 각 STP 브리지 인스턴스에 대한 열과 관련 정보를 표시하는 칼럼을 포함합니다.



| MSTI | Bridge ID               | Root ID                 | Port | Cost | Topology Flag | Topology Change Last |
|------|-------------------------|-------------------------|------|------|---------------|----------------------|
| CIST | 32768.00-40-C7-1C-E9-EB | 32768.00-40-C7-1C-E9-EB | -    | 0    | Steady        | -                    |

| Port | CIST Role | CIST State | Uptime |
|------|-----------|------------|--------|
| 1    | Disabled  | Discarding | -      |
| 2    | Disabled  | Discarding | -      |
| 3    | Disabled  | Discarding | -      |
| 4    | Disabled  | Discarding | -      |
| 5    | Disabled  | Discarding | -      |
| 6    | Disabled  | Discarding | -      |
| 7    | Disabled  | Discarding | -      |
| 8    | Disabled  | Discarding | -      |
| 9    | Disabled  | Discarding | -      |

### 웹 인터페이스

웹 인터페이스에서 STP 브리지 상태를 표시하려면:

1. 스페닝 트리와 STP 상태를 클릭합니다.
2. 정보를 자동 새로 고침 하려면 "자동 새로 고침"을 사용합니다.
3. "새로 고침"을 클릭해 STP 브리지를 새로 고침 합니다.
4. "CIST"를 클릭해 "STP 상세 브리지 상태"로 이동합니다.

### ■ 항목 설명:

MSTI:

브리지 인스턴스입니다. STP 상세 브리지 상태와 연결되는 링크입니다.

브리지 ID (Bridge ID):

이 브리지 인스턴스의 브리지 ID입니다.

루트 ID (Root ID):

현재 선택된 루트 브리지의 브리지 ID입니다.

루트 포트 (Root Port):

현재 루트 포트 기능에 할당된 스위치 포트입니다.

루트 비용 (Root Cost):

루트 경로 비용입니다. 루트 브리지의 경우 0입니다. 다른 모든 브리지의 경우, 루트 브리지로의 최소 비용 경로에서 포트 경로 비용의 총액입니다.

토폴로지 플래그 (Topology Flag):

이 브리지 인스턴스 토폴로지 변경 플래그의 현재 상태입니다.

마지막 토폴로지 변경(Topology Change Last):

마지막 토폴로지 변경 발생 이후의 시간입니다.

STP 포트 상태 (STP Port Status):

포트:

논리적 STP 포트의 스위치 포트 번호입니다.

CIST 기능 (CIST Role):

CIST 포트의 현재 STP 포트 기능입니다. 포트 기능은 다음의 값 중 하나입니다: AlternatePort, Backup Port, RootPort, DesignatedPort Disabled.

CIST 상태 (CIST State):

CIST 포트의 현재 STP 포트 상태입니다. 포트 상태는 다음의 값 중 하나입니다: Blocking Learning Forwarding.

가동 시간 (Uptime):

브리지 포트가 마지막으로 초기화된 이후의 시간입니다.

## ■버튼

Auto-refresh ☐ off [Refresh](#)

자동 새로고침:

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고칩니다.

CIST:

“CIST”를 클릭해 “STP 상세 브리지 상태”로 이동합니다.

| STP Detailed Bridge Status                    |                         |                |            |           |      |                |             |
|---|-------------------------|----------------|------------|-----------|------|----------------|-------------|
| Auto-refresh <input type="checkbox"/> Refresh |                         |                |            |           |      |                |             |
| STP Bridge Status                             |                         |                |            |           |      |                |             |
| Bridge Instance                               | CIST                    |                |            |           |      |                |             |
| Bridge ID                                     | 32768.00-40-C7-1C-E9-EB |                |            |           |      |                |             |
| Root ID                                       | 32768.00-40-C7-1C-E9-EB |                |            |           |      |                |             |
| Root Cost                                     | 0                       |                |            |           |      |                |             |
| Root Port                                     | -                       |                |            |           |      |                |             |
| Regional Root                                 | 32768.00-40-C7-1C-E9-EB |                |            |           |      |                |             |
| Internal Root Cost                            | 0                       |                |            |           |      |                |             |
| Topology Flag                                 | Steady                  |                |            |           |      |                |             |
| Topology Change Count                         | 0                       |                |            |           |      |                |             |
| Topology Change Last                          | -                       |                |            |           |      |                |             |
| CIST Ports & Aggregations State               |                         |                |            |           |      |                |             |
| Port  | Port ID                 | Role           | State      | Path Cost | Edge | Point-to-Point | Uptime      |
| 26  | 12801a                  | DesignatedPort | Forwarding | 20000     | Yes  | Yes            | 0d 07:37:19 |

## ■ 항목 설명:

### STP 브리지 상태 (STP Bridge Status)

브리지 인스턴스 (Bridge Instance):

브리지 인스턴스 - CIST, MST1, ...

브리지 ID

이 브리지 인스턴스의 브리지 ID입니다.

루트 ID (Root ID):

현재 선택된 루트 브리지의 브리지 ID입니다.

루트 비용 (Root Cost):

루트 경로 비용입니다. 루트 브리지의 경우 0입니다. 다른 모든 브리지의 경우, 루트 브리지로의 최소 비용 경로에서 포트 경로 비용의 총액입니다.

루트 포트 (Root Port):

현재 루트 포트 기능에 할당된 스위치 포트입니다.

국지적 루트 (Regional Root):

이 브리지의 내부MSTP 부분인 국지적 루트 브리지의 브리지 ID 입니다.

내부루트 비용 (Internal Root Cost):

국지적 루트 경로 비용입니다. 국제적 루트 브리지의 경우 0입니다. 동일한 MSTP 상에서 다른 모든 CIST 인스턴스의 경우, 내부루트 브리지로의 최소 비용 경로의 내부포트 경로 비용의 합계입니다. (CIST 인스턴스의 경우에 한함)



토폴로지 플래그

이 브리지 인스턴스 토폴로지 변경 플래그의 현재 상태입니다.

토폴로지 변경 카운트 (Topology Change Count):

토폴로지 변경 플래그가 설정된 횟수입니다. (1초 간격 동안)

마지막 토폴로지 변경 (Topology Change Last)

토폴로지 플래그가 마지막으로 설정된 이후 경과 시간입니다.

### **CIST 포트 & 집계 상태 (CIST Ports & Aggregations State)**

포트 (Port):

논리적 STP 포트의 스위치 포트 번호입니다.

포트 ID (Port ID):

STP 프로토콜로 사용되는 포트 ID입니다. 이 것은 브리지 포트의 우선 순위 부분 및 논리적 포트 인덱스입니다.

기능 (Role):

현재 STP 포트 기능입니다. 포트 기능은 다음의 값 중 하나입니다: AlternatePort BackupPort RootPortDesignatedPort.

상태 (State):

현재 ATP 포트 상태입니다. 포트 상태는 다음의 값 중 하나입니다: Discarding Learning Forwarding.

경로 비용 (Path Cost):

현재 STP 포트 경로 비용입니다. 이 것은 자동 설정 또는 기타 명확하게 설정된 값에서 계산된 값입니다.

에지 (Edge):

현재 STP 포트(옵션) 에지 플래그입니다. 에지 포트는 브리지가 연결되지 않은 스위치 포트입니다. 플래그는 자동으로 계산되거나 명확하게 설정됩니다. 루프에 연동할 가능성이 없으므로 각 에지 포트는 포워딩 포트 상태에 직접 전송됩니다.

Point-to-Point

현재 STP 포트 point-to-point 플래그입니다. point-to-point 포트는 공유되지 않는 LAN 미디어에 연결합니다. 플래그는 자동으로 계산되거나 설정됩니다. 포트의 point-to-point 속성은 STP 상태로의 전송 속도에 영향을 미칩니다.

가동 시간 (Uptime):

브리지 포트가 마지막으로 초기화된 이후의 시간입니다.

## ■ 버튼



자동 새로고침:

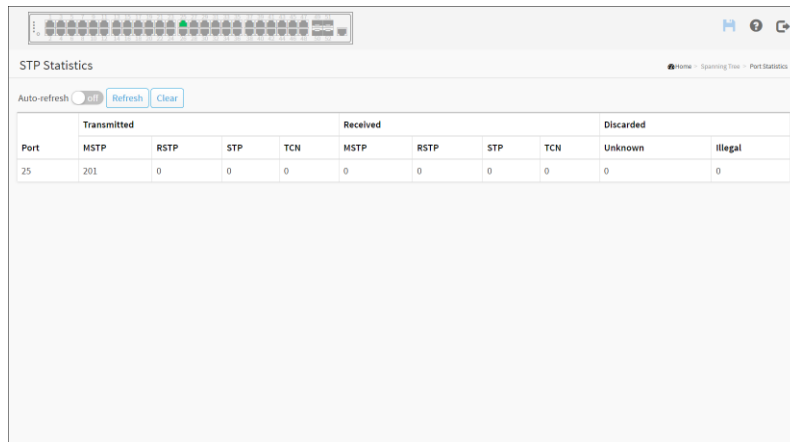
이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고칩니다.

## 포트 현황

이 페이지는 스위치에서 브리지 포트의 STP 포트 현황 수를 나타냅니다.



STP Statistics

Auto-refresh ☐ Refresh Clear

| Port | Transmitted |      |     |     | Received |      |     |     | Discarded |         |
|------|-------------|------|-----|-----|----------|------|-----|-----|-----------|---------|
|      | MSTP        | RSTP | STP | TCN | MSTP     | RSTP | STP | TCN | Unknown   | Illegal |
| 25   | 201         | 0    | 0   | 0   | 0        | 0    | 0   | 0   | 0         | 0       |

웹 인터페이스

웹 인터페이스에서 STP 포트 현황을 표시하려면:

1. 스페닝 트리 및 포트 현황을 클릭합니다.
2. 정보를 자동 새로 고침 하려면 "자동 새로 고침"을 사용합니다.
3. "새로 고침"을 클릭해 STP 브리지를 새로 고침 합니다.

### ■ 항목 설명:

포트 (Port):

논리적 STP 포트의 스위치 포트 번호입니다.

MSTP:

포트 상에 수신/전송된 BPDU의 MSTP 설정 수입입니다.

RSTP:

포트 상에 수신/전송된 BPDU의 RSTP 설정 수입입니다.

STP:

포트 상에 수신/전송된 BPDU의 STP 설정 수입입니다.

TCN:

포트 상에 수신/전송된 BPDU의 (기존) 토폴로지 변경 알림 수 있습니다.

미확인 삭제 (Discarded Unknown):

포트 상에 수신된 (그리고 삭제된) BPDU의 미확인 스페닝 트리 수 있습니다.

음성적 삭제 (Discarded Illegal):

포트 상에 수신된 (그리고 삭제된) BPDU의 음성적 스페닝 트리 수 있습니다.

## ■ 버튼

Auto-refresh ☐ off [Refresh](#)

자동 새로고침:

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고칩니다.

## MAC 주소 테이블

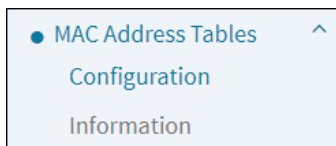
## 개요

---

프레임 전환은 프레임에 포함된 DMAC 주소를 기반으로 합니다. 스위치는 프레임이 이동할 포트(프레임의 DMAC 주소 기반)를 인식하기 위한 스위치 포트에 MAC 주소를 매핑하는 테이블을 구축합니다. 이 테이블은 정적, 동적 엔트리를 모두 포함합니다. 관리자가 DMAC 주소 및 스위치 포트 사이의 고정 매핑을 원하는 경우 정적 엔트리는 네트워크 관리자에 의해 구성됩니다.

프레임은 또한 MAC 주소(SMAC 주소)를 포함해 프레임을 전송하는 장비의 MAC 주소를 표시합니다. SMAC 주소는 스위치에 의해 자동으로 MAC 테이블을 동적 MAC 주소와 업데이트 하기 위해 사용됩니다. 설정 가능한 시간 이후 프레임에 해당 표시되는 SMAC 주소 반응이 없는 경우 동적 엔트리는 MAC 테이블에서 제거됩니다.

메뉴는 다음과 같습니다:



## 설정

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging ☐

Aging Time  seconds

MAC Table Learning

| Port Members |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |    |    |
|--------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|----|----|
|              | 1                                   | 2                                   | 3                                   | 4                                   | 5                                   | 6                                   | 7                                   | 8                                   | 9                                   | 10                                  | 11                                  | 12                                  | 13                                  | 14                                  | 15                                  | 16                                  | 17                                  | 18                                  | 19                                  | 20                                  | 21                                  | 22                                  | 23                                  | 24                                  | 25                                  | 26                                  | 27                                  | 28                                  | 29                                  | 30                                  | 31                                  | 32                                  | 33                                  | 34                                  | 35 | 36 |
| Auto         | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |    |    |
| Disable      | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |    |    |
| Secure       | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |    |    |

VLAN Learning Configuration

Learning-disabled VLANs

Static MAC Table Configuration

| Port Members             |                                |  |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |    |
|--------------------------|--------------------------------|--|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|----|
| Delete                   | VLAN ID                        | MAC Address                                    | 1                        | 2                        | 3                        | 4                        | 5                        | 6                        | 7                        | 8                        | 9                        | 10                       | 11                       | 12                       | 13                       | 14                       | 15                       | 16                       | 17                       | 18                       | 19                       | 20                       | 21                       | 22                       | 23                       | 24                       | 25                       | 26                       | 27                       | 28                       | 29                       | 30                       | 31                       | 32                       | 33                       | 34                       | 35                       | 36 |
| <input type="checkbox"/> | <input type="text" value="1"/> | <input type="text" value="00-00-00-00-00-00"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |    |

Add New Static Entry

Reset Apply

### 웹 인터페이스

웹 인터페이스에서 MAC 주소 테이블을 설정하려면:

1. MAC 주소 테이블 및 설정을 클릭합니다.
2. 자동 에이징 및 에이징 시간 비활성화를 지정합니다.
3. 포트 멤버 (Auto, Disable, Secure)를 지정합니다.
4. 러닝-비활성화 VLAN을 지정합니다.
5. 새 정적 엔트리를 입력하고, VLAN ID와 MAC 주소, 포트 멤버를 지정합니다.

Static MAC Table Configuration

| Port Members                        |         |                   |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |                          |
|-------------------------------------|---------|-------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Delete                              | VLAN ID | MAC Address       | 1                        | 2                        | 3                        | 4                        | 5                        | 6                        | 7                        | 8                        | 9                        | 10                       | 11                       | 12                       | 13                       | 14                       | 15                       | 16                       | 17                       | 18                       | 19                       | 20                       | 21                       | 22                       | 23                       | 24                       | 25                       | 26                       | 27                       | 28                       | 29                       |                          |                          |                          |                          |
| <input checked="" type="checkbox"/> | 1       | 00-00-00-00-00-00 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

6. 적용을 클릭합니다.

**■ 항목 설명:**

에이징 설정 (Aging Configuration):

기본값으로, 동적 엔트리는 300초 후에 MAC 테이블에서 제거됩니다. 이 삭제를 또한 에이징이라고 부릅니다.

초 단위로 이 곳에 값을 입력해 에이징 시간을 설정합니다; 예를 들어, 에이징 시간은 초 입니다. 허용 범위는 10에서 1000000초 입니다.

☒ Disable 자동 에이징을 체크해 동적 엔트리의 자동 에이징을 비활성화 합니다.

MAC 테이블 러닝 (MAC Table Learning):

주어진 포트의 러닝 모드가 흐려지면, 유저에 의해 변경되지 못하도록 다른 모듈이 모드 제어 상태입니다. 이런 모듈의 예시는 802.1X 아래의 MAC-기반 인증입니다. 각 포트는 다음의 설정을 기반으로 러닝을 할 수 있습니다:

Auto:

미확인 SMAC의 프레임이 수신 되자마자 자동으로 러닝이 완료됩니다.

Disable:

완료되는 러닝이 없습니다.

Secure:

정적 MAC 엔트리가 러닝 상태인 경우만 다른 모든 프레임이 제거됩니다.

---

**주의:** 러닝 모드 보안을 위해 변경 전 스위치 관리를 위해 사용된 링크가 정적 MAC 테이블에 추가되어 있는지 확인하십시오. 그렇지 않으면 매니지먼트 링크가 삭제되며 다른 비보안 포트를 이용하거나 시리얼 인터페이스를 통한 스위치에 연결을 통해서만 복구 가능합니다.

---

**VLAN 러닝 설정 (VLAN Learning Configuration)**

러닝-비활성 VLAN (Learning-disabled VLANs):

이 필드는 러닝-비활성 VLAN입니다. NEW MAC이 러닝-비활성 VLAN에 전송되면 MAC은 러닝을 실행하지 않습니다. 기본값으로 필드는 공백입니다. 더 많은 VLAN이 각각의 요소가 콤마로 구별되는 목록 구문을 이용해 생성될 것 입니다. 범위는 하한선 및 상한선을 구별하는 대시로 지정됩니다.

다음 예시는 VLAN 1, 10, 11, 12, 13, 200 그리고 300: 1,10-13,200,300을 생성합니다: 공백은 구분 기호 사이에서 허용됩니다.

정적 MAC 테이블 설정 (Static MAC Table Configuration)

MAC 테이블의 정적 엔트리가 이 테이블에 표시됩니다. 정적 MAC 테이블은 128 엔트리를 포함합니다. 최대 128 엔트리는 전체 스택을 위한 것이며 스위치 별로 아닙니다.

VLAN ID:

엔트리의 VLAN ID 입니다.

MAC 주소 (MAC Address):

엔트리의 MAC 주소입니다.

포트 멤버 (Port Members):

체크마크는 어느 포트가 엔트리 멤버인지를 표시합니다. 엔트리를 수정을 하려면 원하는 대로 체크 또는 체크를 해제하십시오.

## ■ 버튼

새 정적 엔트리 추가 (Add a New Static Entry):

새 엔트리를 정적 MAC 테이블에 추가하려면 클릭하십시오. 새 엔트리의 VLAN ID, MAC 주소 및 포트 번호를 지정합니다. "적용"을 클릭합니다.

삭제 (Delete):

엔트리를 삭제하려면 클릭합니다. 다음 저장 동안 삭제될 것 입니다.

적용 (Apply):

변경 사항을 저장하려면 클릭합니다

리셋 (Reset):

클릭하면 로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.



## 정보

MAC 테이블의 엔트리를 이 페이지에 표시합니다. MAC 테이블은 최대 8192 엔트리를 포함하며 VLAN ID로 먼저 정렬된 다음 MAC 주소로 정렬됩니다.

MAC Address Table

Auto-refresh

Off

Refresh

Clear

First Page

Next Page

Start from VLAN 

1

 and MAC address: 

00-00-00-00-00-00

 , 

20

 entries per page.

Port Members

| Type    | VLAN | MAC Address       | CPU | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |   |
|---------|------|-------------------|-----|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|
| Static  | 1    | 33-33-00-00-00-01 | ✓   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓ |
| Static  | 1    | 33-33-FF-1C-E9-EB | ✓   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓ |
| Dynamic | 1    | 94-C6-91-9B-2F-4D |     |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    | ✓  |    |    |   |
| Static  | 1    | FF-FF-FF-FF-FF-FF | ✓   | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓ |

<

웹 인터페이스

웹 인터페이스의 MAC 주소 테이블을 표시하려면:

1. MAC 주소 테이블과 정보를 클릭합니다.
2. 정보를 자동-새로 고침 하려면 "자동-새로 고침"을 사용합니다.
3. MAC 주소 테이블을 새로 고침 하려면 "새로 고침" 을 클릭합니다.

### ■ 항목 설명:

MAC 테이블 탐색

각 페이지는 MAC 테이블에서 999 엔트리에 나타납니다. 기본값은 "페이지당 엔트리" 입력 필드를 통해 선택된 10입니다. 첫 방문 시 웹 페이지는 MAC 테이블 처음에 먼저 10 엔트리를 표시합니다. 첫 번째 표시되는 것은 MAC 테이블에서 발견된 가장 낮은 VLAN ID와 가장 낮은 MAC 주소입니다.

타입 (Type):

엔트리가 정적인지 동적 802.1x, DMS 인지를 표시합니다.

VLAN:

엔트리의 VLAN ID 입니다.

MAC 주소 (MAC address):

엔트리의 MAC 주소입니다.

포트 멤버 (Port Members):

엔트리 멤버인 포트입니다.

## ■ 버튼



자동 새로고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고칩니다.

첫 번째 페이지:

시스템 로그 엔트리를 업데이트하고 첫 번째 페이지로 이동합니다.

다음 페이지:

시스템 로그 엔트리를 업데이트하고 다음 페이지로 이동합니다.

**주의:** 00-40-C7-73-01-29: 사용자 스위치 MAC 주소 (IPv4용)

: 대상 MAC (IPv6 라우터 알림) (IPv6 RA.JPG 참조)

: 대상 MAC (IPv6 라우터 요청) (IPv6 RS.JPG 참조)

33-33-FF-73-01-29 : 대상 MAC (IPv6 네이버 요청) (IPv6 DAD.JPG 참조)

33-33-FF-A8-01-01 : 사용자 스위치 MAC 주소 (IPv6 글로벌 IP)

FF-FF-FF-FF-FF-FF: 브로드캐스트 용

---

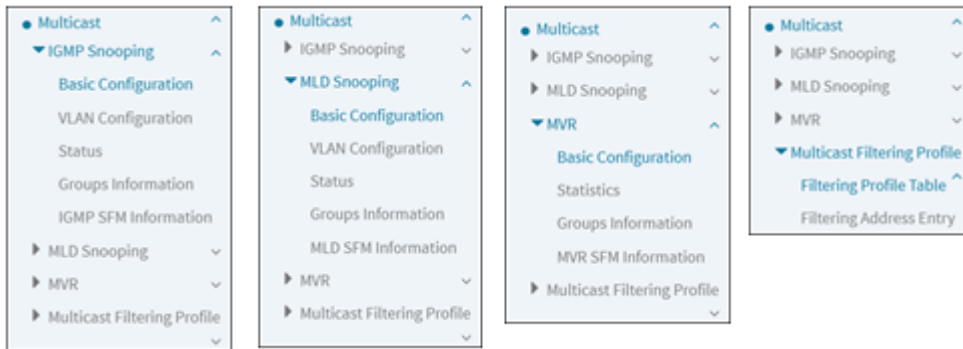
# 10장

## 멀티캐스트

### 개요

---

메뉴와 하위 메뉴는 다음과 같습니다:



## IGMP 스누핑

---

IP 멀티캐스트 패킷이 네트워크 상에서 동작하는 동안, 멀티캐스트 패킷을 멤버 포트에 전송하기 위한 멀티캐스트 그룹을 생성과 사실상 대역폭 낭비를 막는 기능입니다. 이 것은 IGMP 또는 IGMP 스누핑을 지원하지 않는 스위치가 브로드캐스트 패킷에서 멀티캐스트 패킷을 알릴 수 없기 때문입니다. 따라서 모두 브로드캐스트 패킷으로 처리할 수 있습니다. IGMP 스누핑 없이 멀티캐스트 패킷 포워딩 기능은 기본이며 브로드캐스트 패킷과 다르지 않습니다.

쿼리, 리포트 및 중지 기능을 내장한 IGMP 스누핑을 지원하는 스위치이며, 멤버 (포트)가 IP 멀티캐스트 대상 주소에 참여하거나 나갈 때 IP 멀티캐스트 라우터/스위치 및 IP 멀티캐스트 호스트 사이를 교환하는 패킷 타입은 멀티캐스트 테이블 정보를 업데이트할 수 있습니다. 이 기능으로 스위치가 일단 IP 멀티캐스트 패킷을 수신하면, 전에 지정된 IP 멀티캐스트 그룹에 참여한 멤버에게 패킷을 전송합니다.

유저가 멀티캐스트 패킷을 미리 생성되지 않은 멀티 캐스트 그룹에 전송하면 패킷은 IGMP 스누핑에 의해 삭제될 것 입니다. IGMP 모드는 스위치에서 IGMP 프록시 또는 스누핑을 활성화 하는 IGMP 기능을 실행하기 위해 스위치를 활성화 하며, 라우터 클로저를 트리의 루트에 연결할 수 있습니다. 이 인터페이스는 업스트림 인터페이스 입니다. 업스트림 인터페이스의 라우터는 IGMP 를 작동해야 합니다. 이 페이지에서 유저는 현재 PoE 포트 검사 및 설정을 할 수 있고 모든 PoE Supply W를 표시할 수 있습니다.

## 기본 설정

이 섹션은 라우터 클로저를 트리의 루트에 연결하는 스위치에서 기본 IGMP 스누핑을 설정하는 방법을 설명합니다. 인터페이스는 업스트림 인터페이스입니다. 업스트림 인터페이스의 라우터는 IGMP를 작동해야 합니다.

| Port | Router Port              | Fast Leave                          | Throttling | Filtering Profile |
|------|--------------------------|-------------------------------------|------------|-------------------|
| *    | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <=         | <=                |
| 1    | <input type="checkbox"/> | <input checked="" type="checkbox"/> | unlimited  | - Preview         |
| 2    | <input type="checkbox"/> | <input checked="" type="checkbox"/> | unlimited  | - Preview         |
| 3    | <input type="checkbox"/> | <input checked="" type="checkbox"/> | unlimited  | - Preview         |

### 웹 인터페이스

웹 인터페이스에서 Power over Ethernet을 설정하려면:

1. 멀티캐스트, IGMP 스누핑 및 기본 설정을 클릭합니다.
2. 글로벌 설정의 활성화 또는 비활성화를 선택합니다.
3. 라우터 포트가 될 포트를 선택하고 패스트 리브 (Fast Leave) 기능을 활성화 비활성화 합니다.
4. 스크롤 해 제한 및 프로파일을 설정합니다.
5. 적용을 클릭하고 설정을 저장합니다.
6. 설정을 취소하려면 리셋 버튼을 클릭하세요. 이전 저장 값으로 되돌아 갈 것 입니다.

## ■ 항목 설명:

### 글로벌 설정

스누핑 활성화 (Snooping Enabled):

글로벌 IGMP 스누핑을 활성화 합니다.

등록되지 않은 IPMCv4 활성화 (Unregistered IPMCv4 Flooding enabled):

등록되지 않은 IPMCv4 트래픽 플러딩을 활성화 합니다. 비활성화 된 IPMCv4 트래픽은 미확인 멀티캐스트라고도 불립니다.

선택 후 미등록 된 멀티캐스트 스트림은 정상 패킷처럼 전송됩니다. 선택 해제하면 이 스트림은 삭제됩니다.

IGMP SSM 범위 (IGMP SSM Range):

SSM (Source-Specific Multicast) 범위는 SSM-인식 호스트를 허용하며 라우터는 주소 범위 내에서 그룹에 대한 SSM 서비스 모델을 작동합니다. 포맷: (IP 주소/서브 마스크)

Leave 프록시 활성화 (Leave Proxy Enabled):

IGMP Leave 프록시를 활성화 합니다. 이 기능은 라우터 쪽에 불필요한 메시지 남김 전송을 피하는데 사용할 수 있습니다.

프록시 활성화 (Proxy Enabled):

IGMP 프록시를 활성화 합니다. 이 기능은 라우터 쪽에 불필요한 참여와 메시지 남김 전달을 피하는데 사용할 수 있습니다.

### **포트 관련 설정**

포트 (Port):

스위치의 물리적 포트 인덱스를 표시합니다.

라우터 포트 (Port):

라우터 포트로서 동작할 포트를 지정합니다. 라우터 포트는 레이어 3 멀티캐스트 장치 또는 IGMP querier로 연결되는 이더넷 스위치의 포트입니다.

그룹 멤버 포트가 라우터 포트로 선택되면 전체 그룹은 라우터 포트로서 동작합니다.

패스트 리브 (Fast Leave):

포트의 패스트 리브를 활성화 합니다.

제한 (Throttling):

스위치 포트가 속할 수 있는 멀티캐스트 그룹 수를 제한합니다.

프로파일 (Profile):

이 포트의 프로파일을 선택합니다. 선택된 프로파일과 관련된 규칙이 나열된 페이지를 미기 보기 합니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다

리셋 (Reset):

클릭하면 로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## VLAN 설정

이 섹션은 IGMP 스누핑 기능과 통합된 VLAN 구성 설정 프로세스를 설명합니다. 각 설정 페이지는 VLAN 테이블에서 99엔트리를 나타냅니다. 초기값은 20이며, “페이지 당 엔트리”입력 필드를 통해 선택됩니다. 첫 방문 시, 웹 페이지는 VLAN 테이블 시작부터 처음 20 엔트리를 표시합니다. 표시된 첫 번째는 VLAN 테이블에서 발견된 가장 낮은 VLAN ID입니다. “VLAN” 입력 필드에서 유저는 VLAN 테이블에서 시작 포인트를 선택할 수 있습니다. 버튼을 클릭하면 표시된 테이블을 업데이트 해 VLAN 테이블 또는 다음 가장 가까운 VLAN 테이블과 일치하는 것부터 시작합니다.

| VLAN ID | Snooping Enabled                    | Querier Election                    | Querier Address | Compatibility | PRI | RV | QI (sec) | QRI (0.1 sec) | LLQI (0.1 sec) | URI (sec) |
|---------|-------------------------------------|-------------------------------------|-----------------|---------------|-----|----|----------|---------------|----------------|-----------|
| 1       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 0.0.0.0         | IGMP-Auto     | 0   | 3  | 125      | 100           | 100            | 1         |

## 웹 인터페이스

웹 인터페이스에서 IGMP 스누핑 VLAN 설정을 구성하려면:

1. 멀티캐스트, IGMP 스누핑 및 VLAN 설정을 클릭합니다.
2. 새 IGMP VLAN을 추가하려면 클릭하세요.
3. 적용을 클릭해 설정을 저장합니다.

4. 설정을 취소하려면 리셋 버튼을 클릭하세요. 이전 저장 값으로 되돌아 갈 것 입니다.

#### ■ 항목 설명:

VLAN에서 시작(Start from Vlan):

"VLAN"입력 필드부터 표시된 테이블을 새로 고침 시작합니다.

삭제 (Delete):

엔트리를 삭제합니다. 지정 엔트리는 다음 저장 동안 삭제될 것 입니다.

VLAN ID:

엔트리의 VLAN ID를 표시합니다.

스누핑 활성화 (Snooping Enabled):

per-VLAN IGMP Snooping을 활성화 합니다. 최대 32 VLAN만 선택 가능합니다.

IGMP Querier:

VLAN에서 IGMP Querier 선택 참여를 활성화 합니다. 비활성화 하면 IGMP Non-Querier로써 동작 합니다.

호환성 (Compatibility):

호환성은 네트워크에서 호스트와 라우터의 IGMP 동작 버전에 따라 다르게 적절한 동작을 실행하는 호스트와 라우터에 의해 유지 보수됩니다. 허용되는 선택은 IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3입니다. 기본 호환성 값은 IGMP-Auto입니다.

Rv:

강인성 변수 (Robustness Variable)입니다. 강인성 변수는 네트워크 상의 기대 패킷 손실로 변경되는 것을 허용합니다. 허용 범위는 1에서 255입니다; 기본 강인성 변수 값은 2입니다.

QI(sec):

쿼리 간격 (Query Interval)입니다. 쿼리 간격은 Querier에 의해 전송된 일반 쿼리 사이의 간격입니다. 허용 범위는 1에서 31744초입니다; 기본 쿼리 간격은 125초입니다.

QRI(0.1 sec):

쿼리 응답 간격(Query Response Interval)입니다. 주기적인 일반 쿼리에 삽입되는 Max Resp Code를 계산하기 위해 사용되는 최대 응답 시간입니다.



허용되는 범위는 0.1초단위의 0에서 31744입니다; 기본 쿼리 응답 간격은 0.1초의 100입니다. (10초)

LLQI (0.1 sec):

마지막 멤버 쿼리 간격(Last Member Query Interval)입니다. 마지막 멤버 쿼리 시간은 마지막 멤버 쿼리 간격에 마지막 멤버 쿼리 수를 곱해 나타내는 시간 값입니다. 허용 범위는 0.1초단위의 0에서 31744입니다; 기본 마지막 쿼리 간격은 0.1초의 10입니다. (1초)

URI(sec):

임의 리포트 간격 (Unsolicited Report Interval)입니다. 임의 리포트 간격은 그룹 내 멤버십의 호스트의 초기 리포트 반복 사이의 시간입니다. 허용 범위는 0에서 31744입니다. 기본 임의 리포트 간격은 1초입니다.

## ■ 버튼

적용 (Apply):

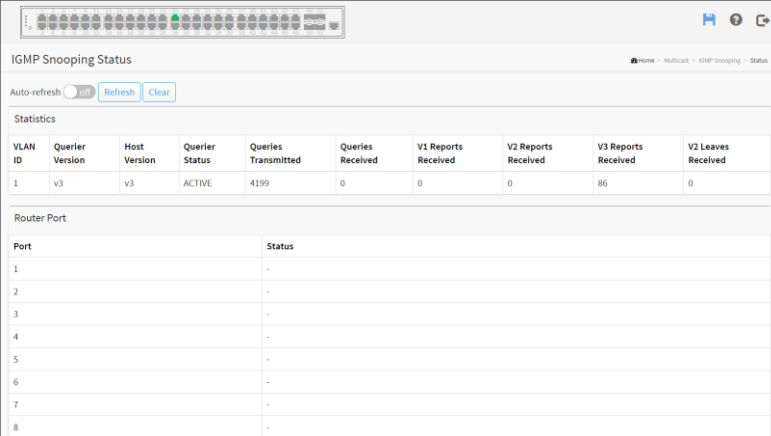
변경 사항을 저장하려면 클릭합니다

리셋 (Reset):

클릭하면 로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## 상태

IGMP 스누핑 설정 완료 후, 스위치가 IGMP 스누핑 상태를 표시하도록 합니다. 이 섹션에서는 스위치가 IGMP 스누핑 상세 상태를 표시하도록 설정할 수 있습니다.



The screenshot shows the 'IGMP Snooping Status' configuration page. At the top, there is a status bar with a green indicator. Below it, the title 'IGMP Snooping Status' is displayed. There are buttons for 'Auto-refresh', 'Refresh', and 'Clear'. The main content area is divided into two sections: 'Statistics' and 'Router Port'.

| VLAN ID | Querier Version | Host Version | Querier Status | Queries Transmitted | Queries Received | V1 Reports Received | V2 Reports Received | V3 Reports Received | V2 Leaves Received |
|---------|-----------------|--------------|----------------|---------------------|------------------|---------------------|---------------------|---------------------|--------------------|
| 1       | v3              | v3           | ACTIVE         | 4199                | 0                | 0                   | 0                   | 86                  | 0                  |

| Port | Status |
|------|--------|
| 1    | -      |
| 2    | -      |
| 3    | -      |
| 4    | -      |
| 5    | -      |
| 6    | -      |
| 7    | -      |
| 8    | -      |

## 웹 인터페이스

웹 인터페이스에서 IGMP 스누핑 상태를 표시하려면:

1. 멀티캐스트, IGMP 스누핑 및 상태를 클릭합니다.
2. 정보를 자동 새로 고침 하려면 "자동-새로 고침"을 클릭합니다.
3. "새로 고침"을 클릭해 IGMP 스누핑 상태를 새로 고침 합니다.

## ■ 항목 설명:

### 현황 (Statistic)

VLAN ID:

엔트리의 VLAN ID입니다.

Querier 버전 (Querier Version):

현재 동작 중인 Querier 버전입니다.

호스트 버전 (Host Version):

현재 동작 중인 호스트 버전입니다.

Querier 상태 (Querier Status):

Querier 상태 "ACTIVE" 또는 "IDLE"를 표시합니다.

"DISABLE"은 특정 인터페이스가 관리 상 비활성화 입니다.

쿼리 전송 (Queries Transmitted):

전송된 쿼리의 수입니다.

쿼리 수신 (Queries Received):

수신된 쿼리의 수입니다.

V1 리포트 수신 (V1 Reports Received):

V1 리포트 수신 수입니다.

V2 리포트 수신 (V2 Reports Received):

V2 리포트 수신 수입니다.

V3 리포트 수신 (V3 Reports Received):

V3 리포트 수신 수입니다.

V2 Leaves 수신:

수신된 V2 Leaves 수입니다.

**라우터 포트 (Router Port)**

라우터 포트는 동작할 포트를 표시합니다. 라우터 포트는 레이어 3 멀티캐스트 장치 또는 IGMP querier로 연결하는 이더넷 스위치의 포트입니다. Static은 특정 포트가 라우터 포트가 되도록 설정한다는 의미입니다. Dynamic은 특정 포트가 라우터 포트가 되도록 기억합니다. Both는 특정 포트가 라우터 포트가 되도록 설정 또는 기억하는 것을 뜻합니다.

포트 (Port):

스위치 포트 번호입니다.

상태 (Status):

특정 포트가 라우터 포트인지 아닌지 표시합니다.

**■ 버튼**

자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

삭제 (Clear):

클릭해 페이지의 내용을 삭제합니다.

**그룹 정보**

IGMP 스누핑 기능 설정 완료 후, 스위치가 IGMP 스누핑 그룹 정보를 표시하도록 할 수 있습니다. IGMP 그룹 테이블의 엔트리가 이 페이지에 표시됩니다. IGMP 그룹 테이블은 VLAN ID로 먼저 정렬된 후 그룹으로 정렬됩니다. 다음 페이지는 다음 검색의 기준으로 현재 표시된 테이블의 마지막 엔트리를 사용합니다. 마지막이 되면 "No more entries" 문구가 표시된 테이블에 나타납니다. 다시 시작하려면 버튼을 사용합니다.

IGMP Snooping Group Information

Auto-refresh: ☐ Refresh First Page Next Page

Start from VLAN: 1 and group address: 239.0.0.0 entries per page: 20

| VLAN ID | Groups          | Port Members   |
|---------|-----------------|--|
|         |                 | 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 |
| 1       | 239.255.255.250 | ✓  |

## 웹 인터페이스

웹 인터페이스에서 IGMP 스누핑 그룹 정보를 표시하려면:

1. 멀티캐스트, IGMP 스누핑 및 그룹 정보를 클릭합니다.
2. 한 페이지에 얼마나 많은 엔트리를 표시할지 지정합니다.
3. 정보를 자동 새로 고침 하고자 하면 "자동-새로 고침"을 선택합니다.
4. "새로 고침"을 클릭해 IGMP 스누핑 그룹 정보 엔트리를 새로 고침 합니다.
5. 첫 번째/다음 페이지를 클릭해 페이지를 변경합니다.

## ■ 항목 설명:

### IGMP 그룹 테이블 탐색 (Navigating the IGMP Group Table)

각 페이지는 IGMP 그룹 테이블에서 99엔트리를 표시합니다. 기본값은 20이며 "페이지 당 엔트리" 입력 필드를 통해 선택됩니다. 첫 번째 방문 시, 웹 페이지는 IGMP 그룹 테이블 시작에서 처음 20 엔트리를 표시합니다.

"VLAN에서 시작" 및 "그룹" 입력 필드에서 유저는 IGMP 그룹 테이블에서 시작 포인트를 선택할 수 있습니다. 새로 고침 버튼을 클릭하면 표시된 테이블을 업데이트 하며 IGMP 그룹 테이블 또는 가장 가까운 다음의 일치하는 IGMP 그룹 테이블에서 시작합니다. 추가로, 2개 입력 필드는 - 새로 고침 버튼 클릭 - 처음 표시된 엔트리 값으로 추정하며, 동일한 시작 주소의 지속적인 새로 고침을 허용합니다.

다음 페이지는 다음 검색의 기준으로 현재 표시된 테이블의 마지막 엔트리를 사용합니다. 마지막 이 되면 “No more entries” 문구가 표시된 테이블에 나타납니다. 다시 시작하려면 버튼을 사용합니다.

엔트리 표시 (Show entries):

표시하고 싶은 하는 항목 수를 선택합니다.

VLAN ID:

그룹 VLAN ID입니다.

그룹 (Groups):

표시된 그룹의 그룹 주소입니다.

포트 멤버 (Port Members):

이 그룹 내의 포트입니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

첫 페이지 (First Page):

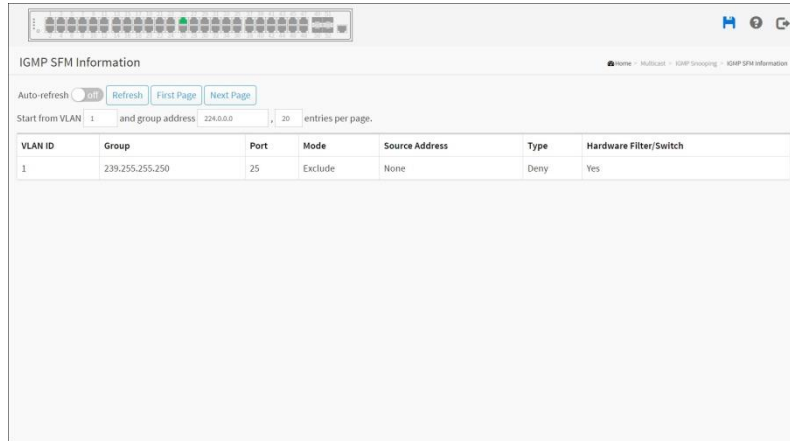
시스템 로그 엔트리를 업데이트하고 첫 페이지로 이동합니다.

다음 페이지 (Next Page):

그룹 정보 엔트리를 업데이트 하고 다음 페이지로 이동합니다.

## IGMP SFM 정보

IGMP SFM 정보 테이블의 엔트리가 이 페이지가 표시됩니다. IGMP SFM (Source-Filtered Multicast) 정보 테이블은 또한 SSM (Source-Specific Multicast) 정보를 포함합니다. 이 테이블은 VLAN ID로 처음 정렬되고, 그 다음 포트로 정렬됩니다. 동일한 그룹에 속한 여러 소스 주소는 싱글 엔트리로 처리됩니다.



IGMP SFM Information

Auto-refresh ☐ Refresh First Page Next Page

Start from VLAN: 1 and group address: 224.0.0.0, 20 entries per page.

| VLAN ID | Group           | Port | Mode    | Source Address | Type | Hardware Filter/Switch |
|---------|-----------------|------|---------|----------------|------|------------------------|
| 1       | 239.255.255.250 | 25   | Exclude | None           | Deny | Yes                    |

## 웹 인터페이스

웹 인터페이스에서 IGMP SFM 정보를 표시하려면:

1. 멀티캐스트, IGMP 스누핑 및 IGMP SFM 정보를 클릭합니다.
2. 정보를 자동 새로 고침 하려면 "자동-새로 고침"을 선택합니다.
3. "새로 고침"을 클릭해 IGMP 스누핑 그룹 정보 엔트리를 새로 고칩니다.
4. 첫/다음 페이지를 클릭해 페이지를 변경합니다.

## ■ 항목 설명:

### IGMP 그룹 테이블 탐색 (Navigating the IGMP Group Table)

각 페이지는 IGMP SFM 정보 테이블에서 99엔트리를 표시합니다. 기본값은 20이며 "페이지 당 엔트리" 입력 필드를 통해 선택됩니다. 첫 번째 방문 시, 웹 페이지는 IGMP SFM 정보 테이블 시작에서 처음 20 엔트리를 표시합니다.

"VLAN에서 시작" 및 "그룹" 입력 필드에서 유저는 IGMP SFM 정보 테이블에서 시작 포인트를 선택할 수 있습니다. 새로 고침 버튼을 클릭하면 표시된 테이블을 업데이트 하며 IGMP SFM 정보 테이블 또는 가장 가까운 다음의 일치하는 IGMP SFM 정보 테이블에서 시작합니다. 추가로, 2개 입력 필드는 - 새로 고침 버튼 클릭 - 처음 표시된 엔트리 값으로 추정하며, 동일한 시작 주소의 지속적인 새로 고침을 허용합니다.

다음 페이지는 다음 검색의 기준으로 현재 표시된 테이블의 마지막 엔트리를 사용합니다. 마지막 이 되면 “No more entries” 문구가 표시된 테이블에 나타납니다. 다시 시작하려면 버튼을 사용합니다.

엔트리 표시 (Show entries):

표시하고 싶은 하는 항목 수를 선택합니다.

VLAN ID:

그룹 VLAN ID입니다.

그룹 (Groups):

표시된 그룹의 그룹 주소입니다.

포트 (Port):

스위치 포트 번호입니다.

모드 (Mode):

(VLAN ID, 포트 번호, 그룹 주소) 당 유지보수 된 필터링 모드를 표시합니다. Include(포함) 또는 Exclude(제외)입니다.

소스 주소 (Source Address):

소스 IP 주소입니다. 현재 시스템은 128 필터링으로 IP 소스 주소의 전체 수를 제한합니다.

타입 (Type):

타입을 식별합니다. Allow(허용) 또는 Deny(거부)입니다.

하드웨어 필터/스위치 (Hardware Filter/Switch):

소스 IPv4 주소에서 특정 그룹 주소로 지정된 데이터 플레인 이 칩으로 처리되는지 여부를 표시합니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

첫 페이지 (First Page):

시스템 로그 엔트리를 업데이트하고 첫 페이지로 이동합니다.

다음 페이지 (Next Page):

그룹 정보 엔트리를 업데이트 하고 다음 페이지로 이동합니다.

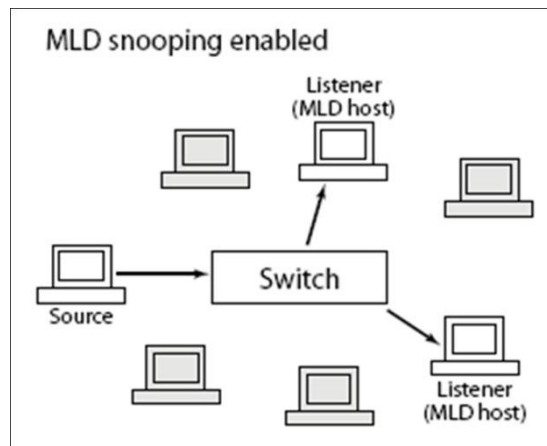


## MLD 스누핑

IPv6 멀티캐스트 트래픽 소스로서 동작하는 네트워크 노드가 MLD 스누핑에 간접적으로만 참여합니다 – 멀티캐스트 트래픽을 제공하며 MLD는 함께 상호작용하지 않습니다. (그러나 데스크탑 컨퍼런싱 같은 애플리케이션에서, 네트워크 노드는 소스와 MLD 호스트로 동작하는 것을 주의하십시오; 하지만 MLD는 자체 기능의 노드만 MLD 호스트로써 교류합니다.)

소스 노드는 멀티캐스트 주소로 패킷을 전송해 멀티캐스트 트래픽을 생성합니다. IPv6에서 처음 8비트 설정의 주소 (주소의 첫 2자가 "FF")는 멀티캐스트 주소이며, 그 주소를 따르는 노드가 주소로 전송된 트래픽을 수신합니다. 소스에 동작하는 애플리케이션 소프트웨어와 대상 시스템은 사용할 멀티캐스트 주소를 지정하는데 도움을 줍니다. (MLD가 아닌 애플리케이션 소프트웨어 기능을 주의하십시오.)

MLD 스누핑이 VLAN 상에서 활성화되면 스위치는 불필요한 멀티캐스트 트래픽을 최소화 하도록 동작합니다. 스위치가 주어진 멀티캐스트 주소로 지정된 멀티캐스트 트래픽을 수신하면, 이 주소의 MLD 호스트를 가진 VLAN 상의 포트에만 트래픽을 전송합니다. MLD 호스트가 없는 VLAN 상의 포트에 대한 트래픽을 삭제합니다.



## 기본 설정

이 섹션에서 MLD 스누핑 기본 설정 및 항목 구성 방법을 설명합니다.

| Port | Router Port              | Fast Leave               | Throttling | Filtering Profile         |
|------|--------------------------|--------------------------|------------|---------------------------|
| *    | <input type="checkbox"/> | <input type="checkbox"/> | <>         | <>                        |
| 1    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  | - <a href="#">Preview</a> |
| 2    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  | - <a href="#">Preview</a> |
| 3    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  | - <a href="#">Preview</a> |

### 웹 인터페이스

웹 인터페이스에서 MLD 스누핑 설정을 구성하려면:

1. 멀티캐스트, MLD 스누핑 및 기본 설정을 클릭합니다.
2. 글로벌 설정 항목을 On/Off 합니다.
3. 라우터 포트와 패스트 리브 사용하려면 포트를 선택합니다.
4. 스크롤 해 무제한 또는 1에서 10의 제한 (Throttling) 모드를 선택합니다.
5. 스크롤 해 프로파일을 설정합니다.
6. 적용을 클릭하면 설정을 저장합니다.
7. 설정을 취소하려면 리셋 버튼을 클릭합니다. 이전 저장 값으로 되돌아 갑니다.

### ■ 항목 설명:

#### 글로벌 설정

스누핑 활성화 (Snooping Enabled):

글로벌 MLD 스누핑을 활성화 합니다.

등록되지 않은 IPMCv6 활성화 (Unregistered IPMCv6 Flooding enabled):

등록되지 않은 IPMCv6 트래픽 플러딩을 활성화 합니다.

MLD 스누핑 활성화 시에만 플러딩 컨트롤이 동작합니다.

MLD 스누핑이 비활성화 되면, 이 설정에도 불구하고 미등록 된 IPMCv6 트래픽 플러딩은 계속 동작합니다.

MLD SSM 범위 (MLD SSM Range):

SSM (Source-Specific Multicast) 범위는 SSM-인식 호스트를 허용하며 라우터는 주소 (IPv6 주소 사용) 범위 내에서 그룹에 대한 SSM 서비스 모델을 작동합니다.

Leave 프록시 활성화 (Leave Proxy Enabled):

MLD Leave 프록시를 활성화 합니다. 이 기능은 라우터 쪽에 불필요한 메시지 남김 전송을 피하는데 사용할 수 있습니다.

프록시 활성화 (Proxy Enabled):

MLD 프록시를 활성화 합니다. 이 기능은 라우터 쪽에 불필요한 참여와 메시지 남김 전달을 피하는데 사용할 수 있습니다.

### 포트 관련 설정

포트 (Port):

스위치의 물리적 포트 인덱스를 표시합니다.

라우터 포트 (Port):

라우터 포트로서 동작할 포트를 지정합니다. 라우터 포트는 레이어 3 멀티캐스트 장치 또는 MLD querier 로 연결되는 이더넷 스위치의 포트입니다.

그룹 멤버 포트가 라우터 포트로 선택되면 전체 그룹은 라우터 포트로서 동작합니다.

패스트 리브 (Fast Leave):

포트의 패스트 리브를 활성화 합니다.

제한 (Throttling):

스위치 포트가 속할 수 있는 멀티캐스트 그룹 수를 제한합니다.

프로파일 필터링 (Filtering Profile):

멀티캐스트 프로파일 필터링에서 편집 시 프로파일을 선택할 수 있습니다.

## ■버튼

적용 (Apply):

변경 사항을 저장하려면 클릭합니다

리셋 (Reset):

클릭하면 로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## VLAN 설정

MLD 스누핑이 VLAN에서 활성화 되면 스위치는 불필요한 멀티캐스트 트래픽을 최소화 하도록 동작합니다. 스위치가 주어진 멀티캐스트 주소로 지정된 멀티캐스트 트래픽을 수신하면, 이 주소의 MLD 호스트를 가진 VLAN 상의 포트에만 트래픽을 전송합니다. MLD 호스트가 없는 VLAN 상의 포트에 대한 트래픽을 삭제합니다.

다음 페이지는 다음 검색의 기준으로 현재 표시된 테이블의 마지막 엔트리를 사용합니다. 마지막 이 되면 “No more entries” 문구가 표시된 테이블에 나타납니다. 다시 시작하려면 버튼을 사용합니다.

| VLAN ID | Snooping Enabled         | Querier Election                    | Compatibility | PRI | RV | QI (sec) | QRI (0.1 sec) | LLQI (0.1 sec) | URI (sec) |
|---------|--------------------------|-------------------------------------|---------------|-----|----|----------|---------------|----------------|-----------|
| 1       | <input type="checkbox"/> | <input checked="" type="checkbox"/> | MLD-Auto      | 0   | 2  | 125      | 100           | 10             | 1         |

### 웹 인터페이스

웹 인터페이스에서 MLD 스누핑 VLAN 설정을 구성하려면

1. 멀티캐스트, MLD 스누핑 및 VLAN 구성을 클릭합니다.
2. 새로운 MLD VLAN 추가를 클릭합니다.
3. VLAN ID를 페이지 별 엔트리와 함께 지정합니다.

### ■ 항목 설명:

삭제 (Delete):

엔트리를 삭제하려면 클릭하십시오. 지정 엔트리는 다음 저장 동안 삭제됩니다.

VLAN ID:

엔트리의 VLAN ID를 표시합니다.

스누핑 활성화 (Snooping Enabled):

per-VLAN IGMP 스누핑을 활성화 합니다. 최대 32 VLAN만 선택 가능합니다.

MLD Querier:

VLAN에서 IGMP Querier 선택 참여를 활성화 합니다. 비활성화 하면 IGMP Non-Querier로써 동작을 비활성화 합니다.

호환성 (Compatibility):

호환성은 네트워크에서 호스트와 라우터의 IGMP 동작 버전에 따라 다르게 적절한 동작을 실행하는 호스트와 라우터에 의해 유지 보수됩니다. 허용되는 선택은 IGMP-Auto, Forced IGMPv1, Forced IGMPv2입니다. 기본 호환성 값은 IGMP-Auto입니다.

Rv:

강인성 변수 (Robustness Variable)입니다. 강인성 변수는 네트워크 상의 기대 패킷 손실로 변경되는 것을 허용합니다. 허용 범위는 1에서 255입니다; 기본 강인성 변수 값은 2입니다.

QI(sec):

쿼리 간격 (Query Interval)입니다. 쿼리 간격은 Querier에 의해 전송된 일반 쿼리 사이의 간격입니다. 허용 범위는 1에서 31744초입니다; 기본 쿼리 간격은 125초입니다.

QRI(0.1 sec):

쿼리 응답 간격(Query Response Interval)입니다. 주기적인 일반 쿼리에 삽입되는 Max Resp Code를 계산하기 위해 사용되는 최대 응답 시간입니다. 허용 범위는 0.1초 단위의 0에서 31744입니다. 기본 쿼리 응답 간격은 0.1초의 100입니다. (10초)

LLQI (LMQI for IGMP):

마지막 멤버 쿼리 간격(Last Member Query Interval)입니다. 마지막 멤버 쿼리 시간은 마지막 멤버 쿼리 간격에 마지막 멤버 쿼리 수를 곱해 나타내는 시간 값입니다. 허용 범위는 0.1초단위의 0에서 31744입니다; 기본 마지막 쿼리 간격은 0.1초의 10입니다. (1초)

URI(sec):

임의 리포트 간격 (Unsolicited Report Interval)입니다. 임의 리포트 간격은 그룹 내 멤버십의 호스트의 초기 리포트 반복 사이의 시간입니다. 허용 범위는 0에서 31744입니다. 기본 임의 리포트 간격은 1초입니다.

## ■ 버튼

적용 (Apply):

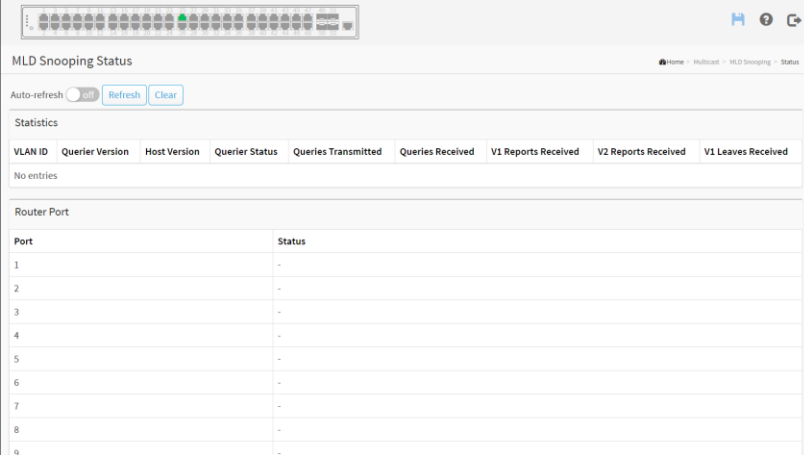
변경 사항을 저장하려면 클릭합니다

리셋 (Reset):

클릭하면 로컬의 변경 사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## 상태

이 섹션은 언제 MLD 스누핑을 설정하고 어떻게 MLD 스누핑 상태 및 상세 정보 표시 방법을 설명합니다. MLD 스누핑 상태의 상세 정보를 참조하는데 도움이 될 것 입니다.



MLD Snooping Status

Auto-refresh: ☐ Refresh Clear

Statistics

| VLAN ID    | Querier Version | Host Version | Querier Status | Queries Transmitted | Queries Received | V1 Reports Received | V2 Reports Received | V1 Leaves Received |
|------------|-----------------|--------------|----------------|---------------------|------------------|---------------------|---------------------|--------------------|
| No entries |                 |              |                |                     |                  |                     |                     |                    |

Router Port

| Port | Status |
|------|--------|
| 1    | -      |
| 2    | -      |
| 3    | -      |
| 4    | -      |
| 5    | -      |
| 6    | -      |
| 7    | -      |
| 8    | -      |
| 9    | -      |

웹 인터페이스

웹 인터페이스에서 MLD 스누핑 상태를 표시하려면:

1. 멀티캐스트, MLD 스누핑 및 상태를 클릭합니다.
2. 정보를 자동 새로 고침 하려면 "자동-새로 고침"을 선택합니다.
3. MLD 스누핑 상태 정보 엔트리를 새로 고침 하려면 "새로 고침"을 클릭합니다.

## ■ 항목 설명:

VLAN ID:

엔트리의 VLAN ID입니다.

Querier 버전 (Querier Version):

현재 동작 중인 Querier 버전입니다.

호스트 버전 (Host Version):

현재 동작 중인 호스트 버전입니다.

Querier 상태 (Querier Status):

Querier 상태가 "ACTIVE" 또는 "IDLE"입니다.

"DISABLE"는 특정 인터페이스가 관리상 비활성화임을 의미합니다.

쿼리 전송 (Queries Transmitted):

전송된 쿼리의 수입니다.

쿼리 수신 (Queries Received):

수신된 쿼리의 수입니다.

V1 리포트 수신 (V1 Reports Received):

V1 리포트 수신 수입니다.

V2 리포트 수신 (V2 Reports Received):

V2 리포트 수신 수입니다.

V1 Leaves 수신:

수신된 V1 Leaves 수입니다.

라우터 포트 (Port):

라우터 포트로서 동작할 포트를 표시합니다. 라우터 포트는 레이어 3 멀티캐스트 장치 또는 MLD querier 로 연결되는 이더넷 스위치의 포트입니다.

Static은 특정 포트가 라우터 포트가 되도록 설정한다는 의미입니다. Dynamic은 특정 포트가 라우터 포트가 되도록 기억합니다. Both는 특정 포트가 라우터 포트가 되도록 설정 또는 기억하는 것을 뜻합니다.

포트 (Port):

스위치 포트 번호입니다.

상태 (Status):

특정 포트가 라우터 포트인지 아닌지 표시합니다.

## ■버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

삭제 (Clear):

클릭해 페이지의 내용을 삭제합니다.

## 그룹 정보

MLD 그룹 테이블의 엔트리가 이 페이지에 표시됩니다. MLD 그룹 테이블은 먼저 VLAN ID로 그리고 그 다음은 그룹으로 정렬됩니다.

MLD Snooping Group Information

Auto-refresh ☐ Refresh First Page Next Page

Start from VLAN 1 and group address 20 entries per page.

| VLAN ID         | Groups |
|-----------------|--------|
| No more entries |        |

## 웹 인터페이스

웹 인터페이스에서 MLD 스누핑 그룹 정보를 표시하려면:

1. 멀티캐스트, MLD 스누핑 및 그룹 정보를 클릭합니다.
2. 정보를 자동 새로 고침 하려면 "자동-새로 고침"을 선택합니다.
3. MLD 스누핑 상태 정보 엔트리를 새로 고침 하려면 "새로 고침"을 클릭합니다.
4. 첫/다음 페이지를 클릭해 페이지를 변경합니다.



## ■ 항목 설명:

### MLD 그룹 테이블 탐색 (Navigating the MLD Group Table)

각 페이지는 MLD 그룹 테이블에서 99엔트리를 표시합니다. 기본값은 20이며 “페이지 당 엔트리” 입력 필드를 통해 선택됩니다. 첫 번째 방문 시, 웹 페이지는 MLD 그룹 테이블 시작에서 처음 20 엔트리를 표시합니다.

“VLAN에서 시작” 및 “그룹” 입력 필드에서 유저는 MLD 그룹 테이블에서 시작 포인트를 선택할 수 있습니다. 새로 고침 버튼을 클릭하면 표시된 테이블을 업데이트 하며 MLD 그룹 테이블 또는 가장 가까운 다음의 일치하는 MLD 그룹 테이블에서 시작합니다. 추가로, 2개 입력 필드는 – 새로 고침 버튼 클릭 – 처음 표시된 엔트리 값으로 추정하며, 동일한 시작 주소의 지속적인 새로 고침을 허용합니다.

다음 페이지는 다음 검색의 기준으로 현재 표시된 테이블의 마지막 엔트리를 사용합니다. 마지막 이 되면 “No more entries” 문구가 표시된 테이블에 나타납니다. 다시 시작하려면 버튼을 사용합니다.

VLAN ID:

그룹 VLAN ID입니다.

그룹 (Groups):

표시된 그룹의 그룹 주소입니다.

포트 멤버 (Port Members):

이 그룹 내의 포트입니다.

엔트리 표시 (Show entries):

표시하고 싶은 항목 개수를 선택합니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

첫 페이지 (First Page):

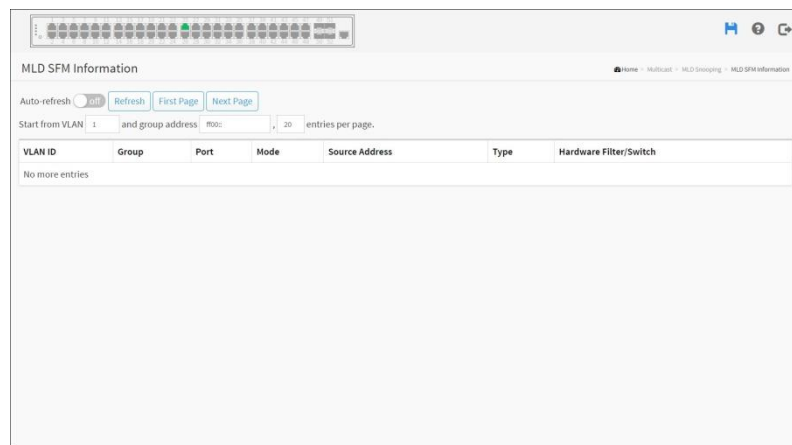
시스템 로그 엔트리를 업데이트 하고 첫 페이지로 이동합니다.

다음 페이지 (Next Page):

그룹 정보 엔트리를 업데이트 하면 다음 페이지로 이동합니다.

## MLD SFM 정보

MLD SFM 정보 테이블의 엔트리가 이 페이지가 표시됩니다. MLD SFM (Source-Filtered Multicast) 정보 테이블은 또한 SSM (Source-Specific Multicast) 정보를 포함합니다. 이 테이블은 VLAN ID로 처음 정렬되고, 그 다음 포트로 정렬됩니다. 동일한 그룹에 속한 여러 소스 주소는 싱글 엔트리로 처리됩니다.



### 웹 인터페이스

웹 인터페이스에서 MLD SFM 정보를 표시하려면:

1. 멀티캐스트, MLD 스누핑 및 MLD SFM 정보를 클릭합니다.
2. 정보를 자동 새로 고침 하려면 "자동-새로 고침"을 선택합니다.
3. MLD SFM 정보 엔트리를 새로 고침 하려면 "새로 고침"을 클릭합니다.
4. 첫/다음 페이지를 클릭해 페이지를 변경합니다.

### ■ 항목 설명:

#### MLD SFM 정보 테이블 탐색 (Navigating the MLD SFM Information Table)

각 페이지는 MLD SFM 정보 테이블에서 99엔트리를 표시합니다. 기본값은 20이며 "페이지 당 엔트리" 입력 필드를 통해 선택됩니다.

첫 번째 방문 시, 웹 페이지는 MLD SFM 정보 테이블 시작에서 처음 20 엔트리를 표시합니다.

“VLAN에서 시작” 및 “그룹” 입력 필드에서 유저는 MLD SFM 정보 테이블에서 시작 포인트를 선택할 수 있습니다. 새로 고침 버튼을 클릭하면 표시된 테이블을 업데이트 하며 MLD SFM 정보 테이블 또는 가장 가까운 다음의 일치하는 MLD SFM 정보 테이블에서 시작합니다. 추가로, 2개 입력 필드는 – 새로 고침 버튼 클릭 – 처음 표시된 엔트리 값으로 추정하며, 동일한 시작 주소의 지속적인 새로 고침을 허용합니다.

다음 페이지는 다음 검색의 기준으로 현재 표시된 테이블의 마지막 엔트리를 사용합니다. 마지막 이 되면 “No more entries” 문구가 표시된 테이블에 나타납니다. 다시 시작하려면 버튼을 사용합니다.

VLAN ID:

그룹 VLAN ID입니다.

그룹 (Groups):

IP 멀티캐스트 그룹 주소입니다.

포트 (Port):

스위치 포트 번호입니다.

모드 (Mode):

(VLAN ID, 포트 번호, 그룹 주소) 기반 별로 유지 보수된 필터링 모드를 표시합니다. 포함 (Include) 또는 제외 (Exclude) 중 하나입니다.

소스 주소 (Source Address):

소스 IP 주소입니다. 현재 시스템은 128 필터링으로 IP 소스 주소의 전체 수를 제한합니다.

타입 (Type):

타입을 식별합니다. Allow(허용) 또는 Deny(거부)입니다.

하드웨어 필터/스위치 (Hardware Filter/Switch):

소스 IPv6 주소에서 특정 그룹 주소로 지정된 데이터 플레인이 칩으로 처리되는지 여부를 표시합니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

첫 페이지 (First Page):

시스템 로그 엔트리를 업데이트 하고 첫 페이지로 이동합니다.

다음 페이지 (Next Page):

그룹 정보 엔트리를 업데이트 하면 다음 페이지로 이동합니다.

## MVR

MVR 기능은 멀티캐스트 VLAN의 멀티캐스트 포워딩을 활성화 합니다. 멀티캐스트 텔레비전 애플리케이션에서 PC 또는 셋톱 박스가 있는 텔레비전은 멀티캐스트 스트림을 수신합니다. 여러 셋톱 박스 또는 PC는 MVR 수신기 포트에 설정된 스위치 포트인 구독자 포트에 연결 가능합니다. 구독자가 채널, 셋톱 박스를 선택하거나 PC는 적절한 멀티캐스트에 참여하도록 IGMP 조인 메시지를 스위치 A에 보냅니다. 멀티캐스트 VLAN에서 멀티캐스트 데이터를 전송 및 수신하는 업링크 포트는 MVR 소스 포트를 호출합니다.

### 기본 정보

#### 웹 인터페이스

웹 인터페이스에서 MVR 설정을 구성하려면:

1. 멀티캐스트, MVR 및 기본 설정을 클릭합니다.
2. MVR 모드를 스크롤 해 활성화 또는 비활성화 하며 모든 항목을 설정하려면 스크롤 하세요.
3. "새 MVR VLAN 추가"를 클릭합니다.
4. MVR VID, MVR 이름, IGMP 주소, 모드, 태깅, 우선권, LLQI, 인터페이스 채널 프로파일을 지정합니다.
5. Immediate Leave를 클릭할 포트를 선택합니다.
6. 적용을 클릭해 설정을 저장합니다.

7. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아 갑니다.

### ■ 항목 설명:

MVR 모드 (MVR Mode):

글로벌 MVR 활성화/비활성화 입니다.

미등록 플러딩 컨트롤은 IGMP/MLD 스누핑의 현재 설정에 따라 다릅니다. MVR 그룹 테이블이 가득 차면 미등록 플러딩 컨트롤 활성화를 권장합니다.

MVR VID:

멀티캐스트 VLAN ID를 지정합니다.

주의: MVR 소스 포트는 매니지먼트 VLAN 포트와 중복되는 것을 권장하지 않습니다.

MVR 이름 (MVR Name):

MVR 이름은 특정 MVR VLAN의 이름을 식별하는데 선택적으로 사용합니다. MVR VLAN 이름 문자열의 최대 길이는 32입니다. MVR VLAN 이름은 알파벳 또는 번호만 가능합니다. MVR VLAN 이름은 기존 MVR VLAN 엔트리를 편집하거나 새 엔트리를 추가할 수 있습니다.

IGMP 주소 (IGMP Address):

IGMP 컨트롤 프레임에 대한 IP 헤더에서 사용된 소스 주소로 IPv4 주소를 정의합니다.

기본 IGMP 주소는 (0.0.0.0)으로 설정되지 않습니다.

IGMP 주소가 설정되지 않으면, 시스템은 이 VLAN과 관련된 IP 인터페이스의 IPv4 매니지먼트 주소를 사용합니다.

IPv4 매니지먼트 주소가 설정되지 않으면, 시스템은 먼저 가능한 IPv4 매니지먼트 주소를 사용합니다.

그렇지 않으면, 시스템은 미리 정의된 값을 사용합니다. 기본값으로 이 값은 192.0.2.1입니다.

모드 (Mode):

동작 MVR 모드를 지정합니다. 동적 모드에서, MVR은 소스 포트에서 동적 MVR 멤버십 리포트를 허용합니다. 호환 가능 모드에서, MVR 멤버십 리포트는 소스 포트에서 금지됩니다. 기본값은 동적 모드입니다.

태깅 (Tagging):

가로지르는 IGMP/MLD 컨트롤 프레임이 MVR VID와 태그 미지정 또는 태그 지정 상태로 전송될 지를 정합니다. 기본값은 태그 지정입니다.

우선권 (Priority):

가로지르는 IGMP/MLD 컨트롤 프레임이 우선 순위로 어떻게 전송될 지 정합니다. 기본 우선권은 0입니다.

LLQ:

멀티캐스트 그룹 멤버십에서 포트를 제거하기 전 수신기 포트의 IGMP/MLD 리포트 멤버십의 대기 최대 시간을 정합니다. 값은 0.1초 단위입니다. 범위는 0에서 31744입니다. 기본값 LLQ는 5/10 또는 1/2 초입니다.

인터페이스 채널 프로파일 (Interface Channel Profile):

MVR VLAN이 생성되면 프로파일을 선택해 특정 MVR VLAN에 대한 해당 멀티캐스트 채널 설정을 확장합니다. 파일은 필터링 프로파일 테이블에 생성되었습니다.

포트 (Port):

설정을 위한 논리적 포트입니다.

포트 기능 (Port Role):

지정된 MVR VLAN의 MVR 포트를 다음 기능 중 하나로 구성합니다.

Inactive: 지정된 포트가 MVR 동작에 참여하지 않습니다.

Source: 멀티캐스트 데이터를 소스 포트로서 수신 및 전송하는 업링크 포트를 설정합니다. 구독자는 소스 포트에 직접 연결되지 못합니다.

Receiver: 구독자 포트이며 멀티캐스트 데이터만 수신한다면, 수신기 포트로 포트를 구성합니다.

IGMP/ML 메시지를 발행해 멀티캐스트 그룹의 멤버가 되지 않는 이상 데이터를 수신하지 않습니다.

Be Caution: MVR 소스 포트는 매니지먼트 VLAN 포트와 중복되는 것을 권장하지 않습니다. 포트 기능을 기능 심볼을 클릭해 선택하면 설정을 전환합니다. I는 Inactive, S는 Source, R은 Receiver를 의미합니다. 기본 설정은 Inactive입니다.

Immediate Leave:

포트의 패스트 리브를 활성화 합니다.

## ■버튼

새로운 MVR VLAN 추가 (Add New MVR VLAN) :

클릭해 새로운 MVR VLAN을 추가합니다. MVR VID, MVR 이름, IGMP 주소, 모드, 태깅, 우선권, LLQI, 인터페이스 채널 프로파일을 지정합니다. "적용"을 클릭합니다.

삭제 (Delete):

엔트리를 삭제하려면 체크하세요. 지정된 엔트리는 다음 저장 동안 삭제됩니다.

적용 (Apply):

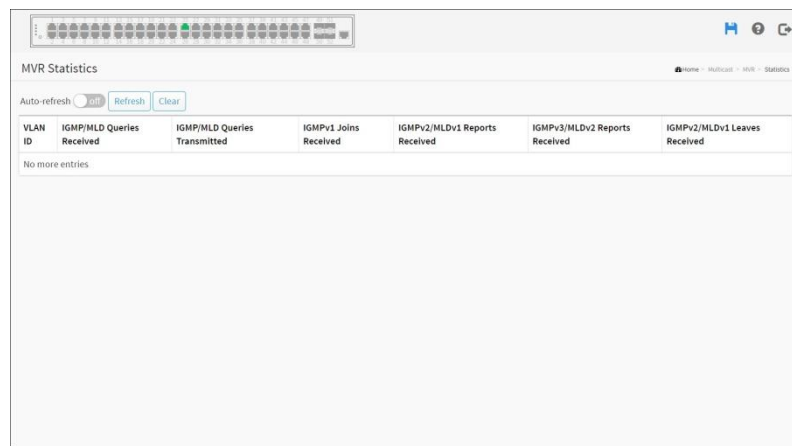
클릭하면 변경사항을 저장합니다.

리셋 (Reset):

클릭해 로컬에서 변경사항을 취소하고 이전에 저장된 값으로 되돌아 갑니다.

## 현황

이 섹션에서 스위치의 MVR 설정 후 스위치는 MVR 상세 현황을 표시합니다. 상세한 MVR 상태 정보를 제공합니다.



| VLAN ID         | IGMP/MLD Queries Received | IGMP/MLD Queries Transmitted | IGMPv1 Joins Received | IGMPv2/MLDv1 Reports Received | IGMPv3/MLDv2 Reports Received | IGMPv2/MLDv1 Leaves Received |
|-----------------|---------------------------|------------------------------|-----------------------|-------------------------------|-------------------------------|------------------------------|
| No more entries |                           |                              |                       |                               |                               |                              |

## 웹 인터페이스

웹 인터페이스에서 MVR 현황 정보를 표시하려면:

1. 멀티캐스트, MVR 및 현황을 클릭합니다.
2. 정보를 자동 새로 고침 하려면 "자동-새로 고침"을 선택합니다.
3. "새로 고침"을 클릭해 MVR 현황 정보 엔트리를 새로 고칩니다.



**■ 항목 설명:**

VLAN ID:

멀티캐스트 VLAN ID입니다.

IGMP/MLD 쿼리 수신 (IGMP/MLD Queries Received):

IGMP와 MLD에 각각 수신된 쿼리 수입입니다.

IGMP/MLD 쿼리 전송 (IGMP/MLD Queries Transmitted):

IGMP와 MLD에 각각 전송된 쿼리 수입입니다.

IGMPv1 Join 수신 (IGMPv1 Joins Received):

IGMPv1 Join에 수신된 수 수입입니다.

IGMPv2/MLDv1 리포트 수신 (IGMPv2/MLDv1 Report's Received):

IGMPv2 Join과 MLDv1 리포트에 각각 수신된 수입입니다.

IGMPv3/MLDv2 리포트 수신 (IGMPv3/MLDv2 Report's Received):

IGMPv3 Join 및 MLDv2 리포트에 각각 수신된 수입입니다.

IGMPv2/MLDv1 Leave 수신 (IGMPv2/MLDv1 Leave's Received):

IGMPv2 Leave 및 MLDv1 완료에 각각 수신된 수입입니다.

**■ 버튼**

자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

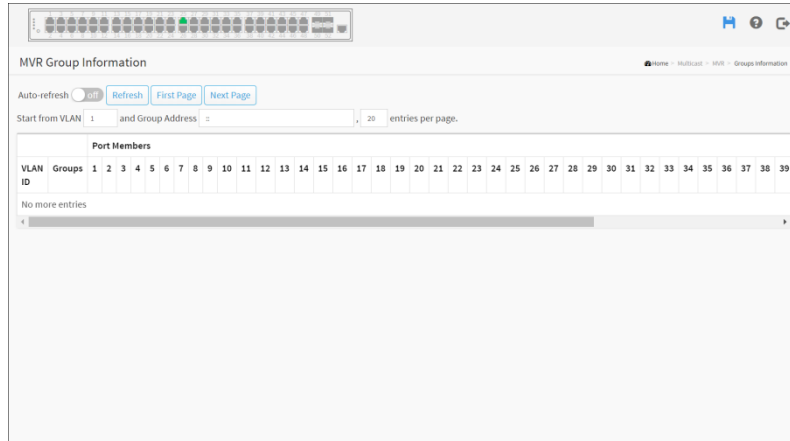
클릭해 페이지를 새로 고침 합니다.

삭제 (Clear):

클릭하면 모든 현황 카운터를 지웁니다.

**MVR 그룹 정보**

이 섹션에서 유저는 스위치의 MVR 그룹 상세 정보를 표시할 수 있습니다. MVR 그룹 테이블의 엔트리가 이 페이지에 나타납니다. MVR 그룹 테이블은 VLAN ID, 그리고 그룹 순으로 정렬됩니다.



## 웹 인터페이스

웹 인터페이스에서 MVR 그룹 정보를 표시하려면:

1. 멀티캐스트, MVR 및 그룹 정보를 클릭합니다.
2. 정보를 자동 새로 고침 하려면 “자동-새로 고침”을 선택합니다.
3. “새로 고침”을 클릭해 MVR 현황 정보 엔트리를 새로 고칩니다.
4. 첫/다음 페이지를 클릭하면 페이지를 변경합니다.

## ■ 항목 설명:

### MVR 채널 (그룹)정보 테이블 탐색

각 페이지는 MVR 그룹 테이블에서 99 엔트리를 보여줍니다. 기본 값은 20이며 “페이지 당 엔트리” 입력 필드를 통해 선택됩니다. 처음 방문하면 웹 페이지는 MVR 채널(그룹) 정보 테이블의 시작부터 20 엔트리를 먼저 표시합니다.

“VLAN부터 시작” 그리고 “그룹 주소” 입력 필드에서 유저는 MVR 채널 (그룹) 정보 테이블에서 시작 포인트를 선택할 수 있습니다. 새로 고침 버튼을 클릭하면 표시된 테이블을 MVR 채널 (그룹) 정보 테이블과 일치하는 것 또는 가장 가까운 것부터 업데이트합니다. 또한 2개 입력 필드는 – 새로 고침 버튼을 클릭하면 – 처음 표시된 엔트리 값을 추정하며, 동일한 시작 주소를 지속적으로 새로 고침 하는 것을 허용합니다.

다음 페이지는 다음 검색의 기준으로 현재 표시된 테이블의 마지막 엔트리를 사용합니다. 마지막 이 되면 “No more entries” 문구가 표시된 테이블에 나타납니다. 다시 시작하려면 버튼을 사용합니다.

### MVR 채널 (그룹) 정보 테이블 항목

엔트리 표시 (Show entries):

표시하고자 하는 항목의 수를 선택할 수 있습니다.

VLAN ID:

그룹의 VLAN ID입니다.

그룹 (Group):

표시된 그룹의 그룹 ID입니다.

포트 멤버 (Port Members):

이 그룹 내의 포트입니다.

### ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

첫 페이지 (First Page):

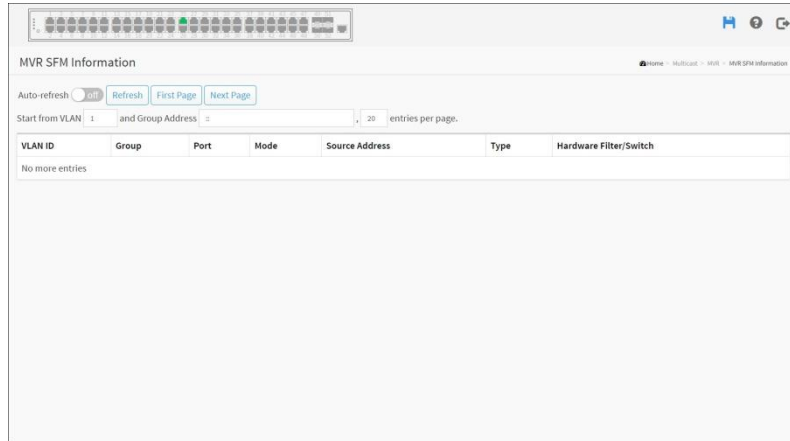
시스템 로그 엔트리를 업데이트 하고 첫 페이지로 이동합니다.

다음 페이지 (Next Page):

그룹 정보 엔트리를 업데이트 하면 다음 페이지로 이동합니다.

### MVR SFM 정보

MVR SFM(Source-Filtered Multicast) 정보 테이블은 또한 SSM (Source-Specific Multicast) 정보를 포함합니다. 이 테이블은 먼저 VLAN ID로, 그 다음은 그룹별로 정렬됩니다. 동일한 그룹에 속한 다른 소스 주소는 싱글 엔트리로 처리됩니다.



## 웹 인터페이스

웹 인터페이스에서 MVR SFM 정보를 표시하려면:

1. 멀티캐스트, MVR 및 MVR SFM 정보를 클릭합니다.
2. 정보를 자동 새로 고침 하려면 "자동-새로 고침"을 선택합니다.
3. "새로 고침"을 클릭해 MVR 현황 그룹 정보 엔트리를 새로 고칩니다.
4. 첫/다음 페이지를 클릭하면 페이지를 변경합니다.

## ■ 항목 설명:

### MVR SFM 정보 테이블 탐색

각 페이지는 MVR SFM 정보 테이블에서 99 엔트리를 보여줍니다. 기본 값은 20이며 "페이지 당 엔트리" 입력 필드를 통해 선택됩니다. 처음 방문하면 웹 페이지는 MVR SFM 정보 테이블의 시작 부터 20 엔트리를 먼저 표시합니다.

"VLAN부터 시작" 그리고 "그룹 주소" 입력 필드에서 유저는 MVR SFM 정보 테이블에서 시작 포인트를 선택할 수 있습니다. 새로 고침 버튼을 클릭하면 표시된 테이블을 MVR SFM 정보 테이블 과 일치하는 것 또는 가장 가까운 것부터 업데이트합니다. 또한 2개 입력 필드는 - 새로 고침 버튼을 클릭하면 - 처음 표시된 엔트리 값을 추정하며, 동일한 시작 주소를 지속적으로 새로 고침 하는 것을 허용합니다.

다음 페이지는 다음 검색의 기준으로 현재 표시된 테이블의 마지막 엔트리를 사용합니다. 마지막 이 되면 "No more entries" 문구가 표시된 테이블에 나타납니다. 다시 시작하려면 버튼을 사용합니다.

**MVR SFM 정보 테이블 항목**

엔트리 표시 (Show entries):

표시하고자 하는 항목의 수를 선택할 수 있습니다.

VLAN ID:

그룹의 VLAN ID입니다.

그룹 (Group):

IP 멀티캐스트 그룹 주소입니다.

포트 (Port):

스위치 포트 번호입니다.

모드 (Mode):

(VLAN ID, 포트 번호, 그룹 주소)별 기준으로 유지 보수된 필터링 모드를 표시합니다. 포함 (Include) 또는 제외(Exclude) 중 하나가 될 수 있습니다.

소스 주소 (Source Address):

소스의 IP 주소입니다. 현재 시스템은 128이 되도록 필터링에 대한 IP 소스 주소의 전체 수를 제한합니다. 소스 필터링 주소가 없으면 "None" 글자가 소스 주소 필드에 표시됩니다.

타입 (Type):

타입을 표시합니다. 허용(Allow) 또는 거부(Deny) 중 하나입니다.

하드웨어 필터/스위치 (Hardware Filter/Switch):

소스 IPv4/IPv6 주소에서 특정 그룹 주소로 지정된 데이터 플레인 이 칩으로 처리되는지 여부를 표시합니다.

**■ 버튼**

자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

첫 페이지 (First Page):

시스템 로그 엔트리를 업데이트하고 첫 페이지로 이동합니다.

다음 페이지 (Next Page):

그룹 정보 엔트리를 업데이트 하고 다음 페이지로 이동합니다.

## 멀티캐스트 필터링 프로파일

### 프로파일 테이블 필터링

IPMC 프로파일은 IP 멀티캐스트 스트림 상의 액세스 제어를 배치하는데 사용됩니다. 최대 64 프로파일을 각각 128개의 해당 규칙과 함께 생성할 수 있습니다.

웹 인터페이스

웹 인터페이스에서 IPMC 프로파일 설정을 구성하려면:

1. 멀티캐스트, 멀티캐스트 필터링 프로파일 및 프로파일 테이블 필터링을 클릭합니다.
2. 멀티캐스트 필터링 프로파일 모드를 스크롤 해 활성화 또는 비활성화 합니다.
3. “새 필터링 프로파일 추가”를 클릭합니다.

4. 프로파일 이름, 프로파일 설명 및 규칙을 제어합니다.
5. 적용을 클릭해 설정을 저장합니다.
6. 설정을 취소하고자 하면 리셋 버튼을 클릭합니다. 이전 저장된 값으로 돌아갑니다.

## ■ 항목 설명:

멀티캐스트 필터링 프로파일 모드 (Multicast Filtering Profile Mode):

멀티캐스트 필터링 프로파일을 활성화/비활성화 합니다.

글로벌 프로파일 모드가 활성화인 경우에만 시스템은 프로파일 설정을 기준으로 필터링을 시작합니다.

프로파일 이름 (Profile Name):

프로파일 테이블 색인 지정에 사용하는 이름입니다.

각 엔트리는 최대 16 알파벳과 숫자로 이루어진 고유의 이름이 있습니다.

프로파일 설명 (Profile Description):

프로파일에 대한 최대 64 알파벳과 숫자로 이루어진 추가 설명입니다.

설명에는 공백 또는 띄어쓰기를 허용하지 않습니다. "\_" 또는 "-"를 사용해 구분하십시오.

규칙 (Rule):

프로파일 생성 시, 지정된 프로파일의 규칙 설정 페이지를 입력하려면 편집 버튼을 클릭하십시오.

지정된 프로파일에 대한 요약은 보기 버튼을 클릭해 볼 수 있습니다. 다음의 버튼을 사용해 지정된 프로파일의 규칙을 관리 또는 검사하십시오:

Preview: 지정된 프로파일과 관련된 규칙을 미리 보기 합니다.

Edit: 지정된 프로파일과 관련된 규칙을 수정합니다.

| Profile Name & Index | Entry Name | Address Range | Action | Log |
|----------------------|------------|---------------|--------|-----|
|----------------------|------------|---------------|--------|-----|

Back to Configuration   Reset   Commit   Add Last Rule

프로파일 이름 & 인덱스 (Profile Name & Index):

관련된 지정된 프로파일 이름입니다. 이 필드는 편집할 수 없습니다.

엔트리 이름 (Entry Name):

이 규칙에 사용된 주소 범위를 지정하는데 사용된 이름입니다.

기존 프로파일 주소 엔트리만 선택된 박스에 내에서 선택 가능합니다. 이 필드는 규칙 설정 테이블이 실행 중 일 때 없음("-")으로 선택 불가능합니다.



주소 범위 (Address Range):

선택된 프로파일 엔트리의 해당 주소 범위입니다. 이 필드는 편집 불가능하며 선택 프로파일 엔트리에 따라 자동으로 조정됩니다.

동작 (Action):

규칙 주소 범위와 일치하는 그룹 주소를 갖는 Join/Report 프레임 수신 시 러닝 동작을 식별합니다.

허용(Permit): 특정 규칙 내의 범위와 일치하는 그룹 주소를 알립니다.

거부(Deny): 특정 규칙 내의 범위와 일치하는 그룹 주소를 삭제합니다.

로그 (Log):





규칙 주소 범위와 일치하는 그룹 주소를 갖는 Join/Report 프레임 수신 시 로깅 환경 설정을 식별합니다.

Enable: 특정 규칙 내의 범위와 일치하는 해당 그룹 주소의 정보가 기록됩니다.

Disable: 특정 규칙 내의 범위와 일치하는 해당 그룹 주소의 정보가 기록되지 않습니다.

규칙 관리 버튼 (Rule Management Buttons):

다음의 버튼을 이용해 규칙과 관련 우선 순위를 관리합니다:

- : 현재 규칙의 엔트리 전 새 규칙을 삽입합니다.
- : 현재 규칙의 엔트리를 삭제합니다.
- : 목록의 현재 규칙 엔트리를 위로 이동합니다.
- : 목록의 현재 규칙 엔트리를 아래로 이동합니다.

## ■ 버튼

새 필터링 프로파일 추가 (Add New Filtering Profile):

새로운 IPMC 프로파일을 추가하려면 클릭하세요. 이름을 지정하고 새 엔트리를 구성합니다.

“저장”을 클릭합니다.

삭제 (Delete):

클릭해서 엔트리를 삭제합니다.

다음 저장 동안 지정된 엔트리를 삭제합니다.

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

마지막 규칙 추가 (Add Last Rule):

특정 프로파일 규칙 목록의 마지막에 새로운 규칙을 추가하려면 클릭하세요. 주소 엔트리를 지정하고 새 엔트리를 설정합니다. “적용”을 클릭합니다.

## 주소 엔트리 필터링

IPMC 프로파일에 사용된 주소 범위 설정을 제공합니다.

주소 엔트리는 IPMC 프로파일과 관련되는 주소 범위를 지정하는데 사용됩니다. 시스템에서 최대 128 주소 엔트리 생성을 허용합니다.

웹 인터페이스

웹 인터페이스에서 IPMC 프로파일 주소 설정을 구성하려면:

1. 멀티캐스트, 멀티캐스트 필터링 프로파일 및 주소 엔트리 필터링을 클릭합니다.
2. “새 주소 (범위) 엔트리 추가”를 클릭합니다.

3. 엔트리 이름, 시작 주소 및 종료 주소를 지정합니다.
4. 적용을 클릭해 설정을 저장합니다.
5. 설정을 취소하고자 하면 리셋 버튼을 클릭합니다. 이전 저장된 값으로 돌아갑니다.
6. "새로 고침"을 클릭해 MLD 스누핑 그룹 정보를 새로 고침 하십시오.
7. 처음 엔트리/다음 엔트리를 클릭해 엔트리를 변경합니다.

### ■ 항목 설명:

엔트리 이름 (Entry Name):

주소 엔트리 테이블 색인 지정에 사용되는 이름입니다.

각 엔트리는 최대 16자 알파벳과 숫자로 이루어진 고유의 이름을 갖습니다.

시작 주소 (Start Address):

주소 범위로 사용될 시작 IPv4/IPv6 멀티캐스트 그룹 주소입니다.

종료 주소 (End Address):

주소 범위로 사용될 종료 IPv4/IPv6 멀티캐스트 그룹 주소입니다.

### ■ 버튼

새 주소(범위) 엔트리 추가 (Add New Address (Range) Entry):

새로운 주소 범위를 추가하려면 클릭하세요. 이름을 지정하고 주소를 설정합니다.

"적용"을 클릭합니다.

삭제 (Delete):

클릭해서 엔트리를 삭제합니다.

다음 저장 동안 지정된 엔트리를 삭제합니다.

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

첫 엔트리 (First Entry):

IPMC 프로파일 주소 설정에서 첫 엔트리에서 시작하는 테이블을 업데이트합니다.

다음 엔트리 (Next Entry):

현재 표시된 마지막 엔트리 후의 엔트리와 시작하는 테이블을 업데이트 합니다.

# 11장

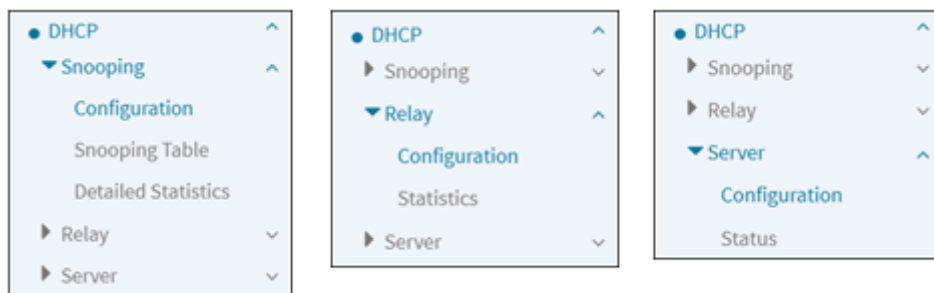
## DHCP

### 개요

---

이 섹션에서 스위치의 DHCP 스누핑 항목을 설정하고 표시하는 방법을 설명합니다. DHCP 스누핑은 네트워크에 자체 DHCP 서버를 추가해 외부 공격을 방지할 수 있습니다.

메뉴와 하위 메뉴는 다음과 같습니다:



## 스누핑

### 설정

DHCP 스누핑은 침입자가 DHCP 클라이언트와 서버 간 적절한 통신에 가짜 DHCP 응답 패킷을 삽입해 방해하는 경우, 스위치 장치의 신뢰성 없는 포트 상의 침입자를 차단하기 위해 사용됩니다.

이 섹션에서는 스위치의 DHCP 스누핑 항목 설정을 설명합니다. DHCP 스누핑은 침입자가 HDCP 서버를 네트워크에 추가하려는 것을 방지합니다.

| Port | Mode    |
|------|---------|
| *    | off     |
| 1    | Trusted |
| 2    | Trusted |
| 3    | Trusted |
| 4    | Trusted |
| 5    | Trusted |
| 6    | Trusted |
| 7    | Trusted |

### 웹 인터페이스

웹 인터페이스에서 DHCP 스누핑을 설정하려면:

1. DHCP, 스누핑 및 설정을 클릭합니다.
2. DHCP 스누핑 설정 모드에서 "on"을 선택합니다.
3. 포트 모드 설정의 모드에서 특정 포트의 "Trusted" 를 선택합니다.
4. 적용을 클릭합니다.

### ■ 항목 설명:

스누핑 모드 (Snooping Mode):

DHCP 스누핑 모드 동작을 표시합니다. 가능한 모드는 다음과 같습니다:

on: DHCP 스누핑 모드 동작을 활성화 합니다. DHCP 스누핑 모드 동작이 활성화 되면, DHCP 요청 메시지가 신뢰성 있는 포트에 전송되어 신뢰성 있는 포트로부터 패킷 응답을 허용합니다.

off: DHCP 스누핑 모드 동작을 비활성화 합니다.

포트 모드 설정 (Port Mode Configuration):

DHCP 스누핑 포트 모드를 표시합니다. 가능한 포트는 다음과 같습니다:

Trusted: DHCP 메시지의 신뢰성 있는 소스로써 포트를 설정합니다. 신뢰성 있는 포트는 DHCP 패킷을 정상적으로 전송할 수 있습니다.

Untrusted: DHCP 메시지의 신뢰성 없는 소스로써 포트를 설정합니다. 신뢰성 없는 포트는 DHCP 패킷을 수신할 때 패킷을 삭제합니다.

## ■ 버튼

적용 (Apply):

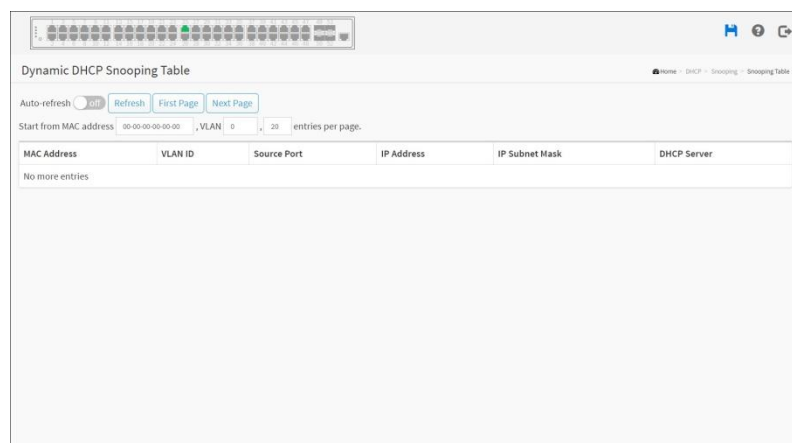
변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## 스누핑 테이블

이 페이지에서는 DHCP 스누핑 모드 활성화 후 정보에 할당된 동적 IP를 표시합니다. 로컬 VLAN 인터페이스 IP 주소를 제외하고 DHCP 서버로부터 동적 IP 주소를 포함하는 모든 DHCP 클라이언트가 이 표에 나타납니다. 동적 DHCP 스누핑 테이블의 엔트리는 다음과 같이 나타납니다.



| MAC Address     | VLAN ID | Source Port | IP Address | IP Subnet Mask | DHCP Server |
|-----------------|---------|-------------|------------|----------------|-------------|
| No more entries |         |             |            |                |             |

## 웹 인터페이스

웹 인터페이스에서 DHCP를 모니터링 하려면:

1. DHCP, 스누핑 및 스노핑 테이블을 클릭합니다.
2. 정보를 새로 고침하려면 "자동 새로 고침"을 클릭합니다.
3. "새로 고침"을 클릭해 MVR 그룹 정보 엔트리를 새로 고침 하세요.
4. 첫/다음 페이지를 클릭해 페이지를 이동합니다.

## ■ 항목 설명:

엔트리 표시 (Show entries):

표시하고자 하는 항목 수를 선택합니다.

MAC 주소 (MAC Address):

엔트리의 유저 MAC 주소입니다.

VLAN ID:

DHCP 트래픽이 허용하는 VLAN-ID입니다.

소스 포트 (Source Port):

엔트리가 표시된 스위치 포트 번호입니다.

IP 주소:

엔트리의 유저 IP 주소입니다.

IP 서브넷 마스크 (IP Subnet Mask):

엔트리의 유저 IP 서브넷 마스크입니다.

DHCP 서버 (DHCP Server):

엔트리의 DHCP 서버 주소입니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):



클릭해 페이지를 새로 고침 합니다.

첫 페이지 (First Page):

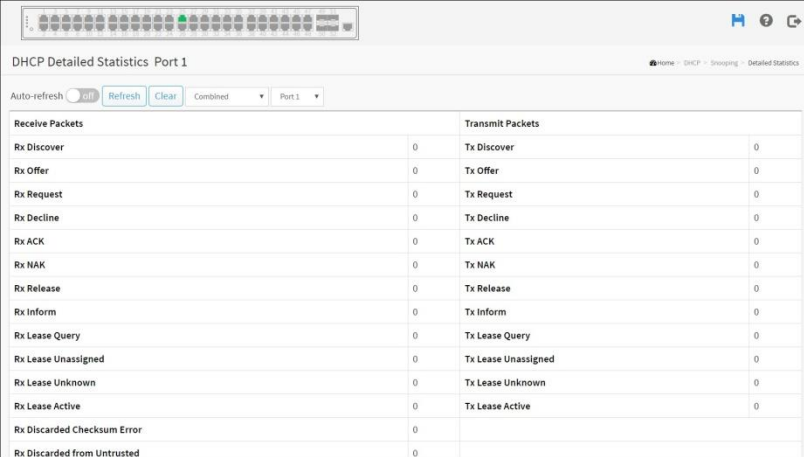
시스템 로그 엔트리를 업데이트 하고 첫 페이지로 이동합니다.

다음 페이지 (Next Page):

그룹 정보 엔트리를 업데이트 하면 다음 페이지로 이동합니다.

## 상세 현황

이 페이지에서는 DHCP 스누핑 현황을 제공합니다. 입력 DHCP 패킷이 L3 포워딩 매커니즘으로 완료되지 않으면 정상 포워딩 포트 당 TX 통계는 증가하지 않습니다. 특정 포트에서 통계를 삭제하는 것은 다른 레이어 개요를 사용하므로 전체 현황에 영향을 미치지 않습니다.



| Receive Packets             |   | Transmit Packets    |   |
|-----------------------------|---|---------------------|---|
| Rx Discover                 | 0 | Tx Discover         | 0 |
| Rx Offer                    | 0 | Tx Offer            | 0 |
| Rx Request                  | 0 | Tx Request          | 0 |
| Rx Decline                  | 0 | Tx Decline          | 0 |
| Rx ACK                      | 0 | Tx ACK              | 0 |
| Rx NAK                      | 0 | Tx NAK              | 0 |
| Rx Release                  | 0 | Tx Release          | 0 |
| Rx Inform                   | 0 | Tx Inform           | 0 |
| Rx Lease Query              | 0 | Tx Lease Query      | 0 |
| Rx Lease Unassigned         | 0 | Tx Lease Unassigned | 0 |
| Rx Lease Unknown            | 0 | Tx Lease Unknown    | 0 |
| Rx Lease Active             | 0 | Tx Lease Active     | 0 |
| Rx Discarded Checksum Error | 0 |                     |   |
| Rx Discarded from Untrusted | 0 |                     |   |

## 웹 인터페이스

웹 인터페이스에서 DHCP 릴레이 통계를 표시하려면:

1. DHCP 스누핑 및 상세 현황을 클릭합니다.
2. 표시하고자 하는 DHCP 상세 현황 포트를 선택합니다.
3. 정보를 새로 고침 하려면 "자동 새로 고침"을 클릭합니다.
4. "새로 고침"을 클릭해 DHCP 상세 현황 엔트리를 새로 고침 하세요.

## ■ 항목 설명:

### 서버 현황

Rx and Tx Discover:

수신 및 전송되는 탐지(1의 값을 가진 53개 옵션) 패킷의 수입입니다.

Rx and Tx Offer:

수신 및 전송되는 제안(2의 값을 가진 53개 옵션) 패킷의 수입입니다.

Rx and Tx Request:

수신 및 전송되는 제안(3의 값을 가진 53개 옵션) 패킷의 수입입니다.

Rx and Tx Decline:

수신 및 전송되는 제안(4의 값을 가진 53개 옵션) 패킷의 수입입니다.

Rx and Tx ACK:

수신 및 전송되는 ACK (5의 값을 가진 53개 옵션) 패킷의 수입입니다.

Rx and Tx NAK:

수신 및 전송되는 NAK (6의 값을 가진 53개 옵션) 패킷의 수입입니다.

Rx and Tx Release:

수신 및 전송되는 릴리즈 (7의 값을 가진 53개 옵션) 패킷의 수입입니다.

Rx and Tx Inform:

수신 및 전송되는 정보 (8의 값을 가진 53개 옵션) 패킷의 수입입니다.

Rx and Tx Lease Query:

수신 및 전송되는 리스 쿼리 (10의 값을 가진 53개 옵션) 패킷의 수입입니다.

Rx and Tx Lease Unassigned:

수신 및 전송되는 미할당된 리스(11의 값을 가진 53개 옵션) 패킷의 수입입니다.

Rx and Tx Lease Unknown:

수신 및 전송되는 미확인 리스 (12의 값을 가진 53개 옵션) 패킷의 수입입니다.

Rx and Tx Lease Active:

수신 및 전송되는 리스 동작 (13의 값을 가진 53개 옵션) 패킷의 수입입니다.

Rx Discarded checksum error:

IP/UDP 합산에 에러가 생긴 삭제 패킷 수 입니다.

Rx Discarded from Untrusted:

신뢰성 없는 포트에서 오는 삭제 패킷 수 입니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 즉시 새로 고침 합니다.

포트 1 (Port 1):

표시하고자 하는 DHCP 상세 현황 포트를 선택합니다.

## 릴레이

### 설정

DHCP 릴레이 에이전트는 동일한 서브넷 도메인 내에 있지 않은 경우 클라이언트와 서버 간 DHCP 메시지를 전달 및 전송하는데 사용합니다. DHCP 패킷의 GIADDR 필드 내의 입력 인터페이스 IP 주소를 저장합니다. DHCP 서버는 할당된 서브넷을 정의하기 위해 GIADDR 필드 값을 사용할 수 있습니다. 이러한 조건을 위해, VLAN 인터페이스 IP 주소와 PVID (포트 VLAN ID) 스위치 설정일 올바른지 확인하십시오.

| DHCP Relay Configuration |          |
|--------------------------|----------|
| Relay Mode               | Off      |
| Relay Server             | 0.0.0.0  |
| Relay Information Mode   | Disabled |
| Relay Information Policy | Keep     |

Reset Apply

### 웹 인터페이스

웹 인터페이스 내에서 DHCP 릴레이를 설정하려면:

1. DHCP 릴레이 및 설정을 클릭합니다.
2. 릴레이 모드, 릴레이 서버, 릴레이 정보 모드, 릴레이 정보 규정을 지정합니다.
3. 적용을 클릭합니다.

### ■ 항목 설명:

릴레이 모드 (Relay Mode):

DHCP 릴레이 모드 동작을 표시합니다.

가능한 모드는 다음과 같습니다:

On: DHCP 릴레이 모드 동작을 활성화 합니다. DHCP 릴레이 모드 동작이 활성화 되면, 에이전트는 동일 서브넷 도메인 내에 있지 않은 경우 DHCP 메시지를 클라이언트와 서버 사이를 전달 및 전송합니다. 따라서 보안 우려에 대한 DHCP 브로드캐스트 메시지가 쇄도하지 않을 것 입니다.

Off: DHCP 릴레이 모드 동작을 비활성화 합니다.

릴레이 서버 (Relay Server):

DHCP 릴레이 서버 IP 주소를 표시합니다.

릴레이 정보 모드 (Relay Information Mode):

DHCP 릴레이 정보 모드 옵션 동작을 표시합니다. 옵션 82 서킷 ID 포맷은

"[vlan\_id][module\_id][port\_no]" 입니다. 처음 4자는 VLAN ID를 나타내며, 5번째와 6번째 글자는 모듈 ID(0과 동일한 독립형 장치에서, 스위치 ID를 뜻하는 스택 가능한 장치에서) 그리고 마지막 2 글자는 포트 번호를 뜻합니다. 예를 들어, "00030108"는 VLAN ID 3, 스위치 ID 1, 포트 No 8의 DHCP 메시지를 수신한다는 뜻 입니다. 그리고 옵션 82 원격 ID 값은 스위치 MAC 주소와 동일 합니다.

가능한 모드는 다음과 같습니다:

Enabled: DHCP 릴레이 정보 모드 동작을 활성화 합니다. DHCP 릴레이 정보 모드 동작이 활성화 되면, 에이전트는 DHCP 서버에 전달할 때 특정 정보(옵션 82)를 DHCP 메시지에 삽입하고, DHCP 클라이언트에 전송 시 DHCP 메시지로부터 삭제합니다. DHCP 릴레이 동작 모드가 활성화 된 경우에만 동작합니다.

Disabled: DHCP 릴레이 정보 모드 동작을 비활성화 합니다.

릴레이 정보 규정 (Relay Information Policy):

DHCP 릴레이 정보 옵션 규정을 표시합니다. DHCP 릴레이 정보 모드 동작이 활성화 시, 에이전트가 이미 릴레이 에이전트 정보를 포함한 DHCP 메시지를 수신하면, 규정을 실행합니다. 'Replace' 규정은 릴레이 정보 모드 비활성화 시 무효화 됩니다. 가능한 규정은 다음과 같습니다:

Replace: DHCP 메시지가 담긴 DHCP 메시지 수신 시 본래의 릴레이 정보를 변경합니다.

Keep: DHCP 메시지가 담긴 DHCP 메시지 수신 시 본래의 릴레이 정보를 유지합니다.

Drop: 릴레이 정보가 담긴 DHCP 메시지 수신 시 패킷을 삭제합니다.

## ■ 버튼

적용 (Apply):

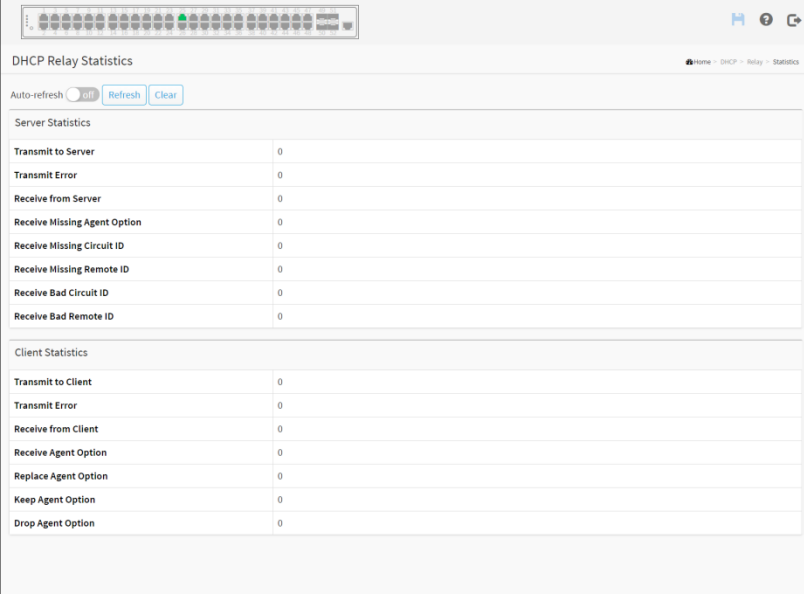
변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## 현황

이 페이지에서는 DHCP 릴레이 현황을 제공합니다.



| DHCP Relay Statistics                                |   |
|--|---|
| Auto-refresh: <input type="checkbox"/> Refresh Clear |   |
| Server Statistics                                    |   |
| Transmit to Server                                   | 0 |
| Transmit Error                                       | 0 |
| Receive from Server                                  | 0 |
| Receive Missing Agent Option                         | 0 |
| Receive Missing Circuit ID                           | 0 |
| Receive Missing Remote ID                            | 0 |
| Receive Bad Circuit ID                               | 0 |
| Receive Bad Remote ID                                | 0 |
| Client Statistics                                    |   |
| Transmit to Client                                   | 0 |
| Transmit Error                                       | 0 |
| Receive from Client                                  | 0 |
| Receive Agent Option                                 | 0 |
| Replace Agent Option                                 | 0 |
| Keep Agent Option                                    | 0 |
| Drop Agent Option                                    | 0 |

## 웹 인터페이스

웹 인터페이스에서 DHCP 릴레이 현황을 모니터링 하려면:

1. DHCP, 릴레이 및 현황을 클릭합니다.
2. DHCP 릴레이 현황을 표시합니다.
3. 정보를 새로 고침 하려면 "자동 새로 고침"을 클릭합니다.
4. "새로 고침"을 클릭해 DHCP 상세 현황 엔트리를 새로 고침 하세요.

**■ 항목 설명:****서버 통계:**

서버로 전송 (Transmit to Server):

클라이언트에서 서버로 전송되는 패킷 수 입니다.

전송 에러 (Transmit Error):

클라이언트에 전송되는 동안 문제를 일으키는 패킷 수 입니다.

서버에서 수신 (Receive from Server):

서버로부터 수신되는 패킷 수 입니다.

누락된 에이전트 옵션 수신 (Receive Missing Agent Option):

에이전트 정보 옵션 없이 수신되는 패킷 수 입니다.

누락된 서킷 ID 수신 (Receive Missing Circuit ID):

누락된 서킷 ID 옵션과 함께 수신되는 패킷 수 입니다.

누락된 원격 ID 수신 (Receive Missing Remote ID):

누락된 원격 ID 옵션과 함께 수신되는 패킷 수 입니다.

불량 서킷 ID (Receive Bad Circuit ID):

서킷 ID 옵션이 확인된 서킷 ID와 일치하지 않는 패킷 수 입니다.

불량 원격 ID 수신 (Receive Bad Remote ID):

원격 ID 옵션이 알려진 원격 ID와 일치하지 않는 패킷 수 입니다.

**클라이언트 통계**

클라이언트로 전송 (Transmit to Client):

서버에서 클라이언트로 전송되는 패킷 수 입니다.

전송 에러 (Transmit Error):

서버에 전송되는 동안 문제를 일으키는 패킷 수 입니다.

클라이언트에서 수신 (Receive from Client):

서버로부터 수신되는 패킷 수 입니다.

에이전트 옵션 수신 (Receive Agent Option):

릴레이 에이전트 정보 옵션과 함께 수신되는 패킷 수입니다.

에이전트 옵션 변경 (Replace Agent Option):

릴레이 에이전트 정보와 변경된 패킷 수입니다.

에이전트 옵션 유지 (Keep Agent Option):

릴레이 정보가 유지되는 패킷 수입니다.

에이전트 옵션 삭제 (Drop Agent Option):

릴레이 에이전트 정보와 함께 수신되는 패킷이 삭제되는 수입니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 즉시 새로 고침 합니다.

삭제 (Clear):

클릭해 페이지의 내용을 삭제합니다.



# 서버

## 설정

이 페이지에서 시스템 및 VLAN 별로 DHCP 서버를 활성화/비활성화 하기 위해 모드를 설정합니다. 또한 시작 IP와 종료 IP 주소를 설정합니다. DHCP 서버는 이러한 IP 주소를 DHCP 클라이언트에 할당합니다. DHCP 클라이언트에 설정 항목을 전송합니다.

| VLAN | Mode | Start IP | End IP  | Lease Time | Subnet Mask | Default Router | DNS Server |
|------|------|----------|---------|------------|-------------|----------------|------------|
| 1    | On   | 0.0.0.0  | 0.0.0.0 | 86400      | 0.0.0.0     | 0.0.0.0        | 0.0.0.0    |

웹 인터페이스

웹 인터페이스에서 DHCP 서버 설정을 구성하려면:

1. DHCP, 서버 및 설정을 클릭합니다.
2. "인터페이스 추가"를 클릭합니다.
3. VLAN, 모드, 시작 IP, 종료 IP, 리스 타임, 서브넷 마스크, 초기값 라우터, DNS 서버를 지정합니다.
4. 적용을 클릭합니다.

### ■ 항목 설명:

VLAN:

DHCP 서버가 활성화 또는 비활성화되는 VLAN을 설정합니다. 허용된 VLAN의 범위는 1에서 4095입니다.

모드 (Mode):

VLAN 별로 동작 모드를 표시합니다. 가능한 모드는 다음과 같습니다:

Enable: VLAN 별로 DHCP 서버를 활성화 합니다.

Disable: VLAN 별로 DHCP 서버를 비활성화 합니다.

시작 IP 및 종료 IP (Start IP and End IP):

IP 범위를 정의합니다. 시작 IP는 종료 IP 보다 적거나 동일해야 합니다.

리스 타임:

Pool의 리스 타임을 설정합니다.

서브네 마스크 (Subnet Mask):

DHCP 주소의 서브넷 마스크를 설정합니다.

초기값 라우터 (Default router):

지정 IP 네트워크 또는 이 경로의 호스트 주소를 설정합니다.

DNS

서버 (Server):

DNS 서버를 지정합니다.

## ■ 버튼

삭제 (Delete):

엔트리를 삭제하려면 클릭하세요. 다음 저장 동안 삭제됩니다.

인터페이스 추가 (Add Interface):

클릭해 새로운 DHCP 서버를 추가합니다.

적용 (Apply):

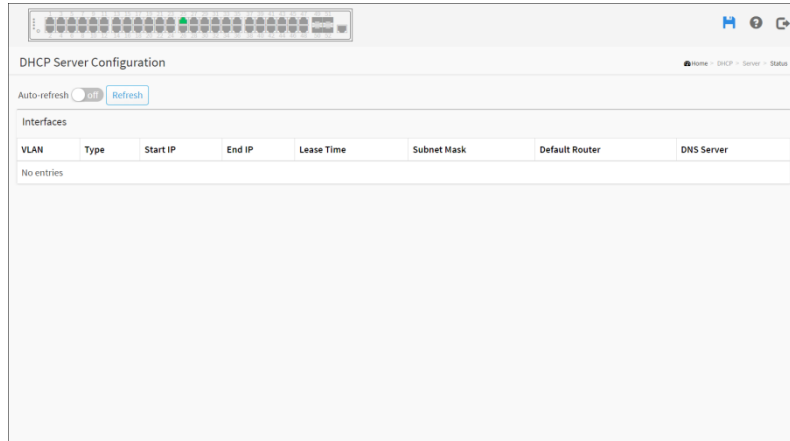
변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## 상태

이 페이지는 DHCP 서버 상태를 표시합니다.



## 웹 인터페이스

웹 인터페이스에서 DHCP 서버 상태를 표시하려면:

1. DHCP 서버 및 상태를 클릭합니다.
2. 정보를 새로 고침 하려면 "자동 새로 고침"을 클릭합니다.
3. "새로 고침"을 클릭해 DHCP 서버 상태 엔트리를 새로 고침 하세요.

## ■ 항목 설명:

VLAN:

엔트리의 VLAN ID입니다.

타입:

VLAN 별 동작 타입을 표시합니다. 가능한 타입은 Static과 Dynamic입니다.

시작 IP 및 종료 IP (Start IP and End IP):

시작 IP와 종료 IP를 표시합니다.

리스 타임:

Pool의 리스 타임을 표시합니다.

서브넷 마스크 (Subnet Mask):

DHCP 주소의 서브넷 마스크를 표시합니다.

초기값 라우터 (Default router):

지정 IP 네트워크 또는 이 경로의 호스트 주소를 표시합니다.

DNS

서버 (Server):

DNS 서버를 표시합니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 즉시 새로 고침 합니다.

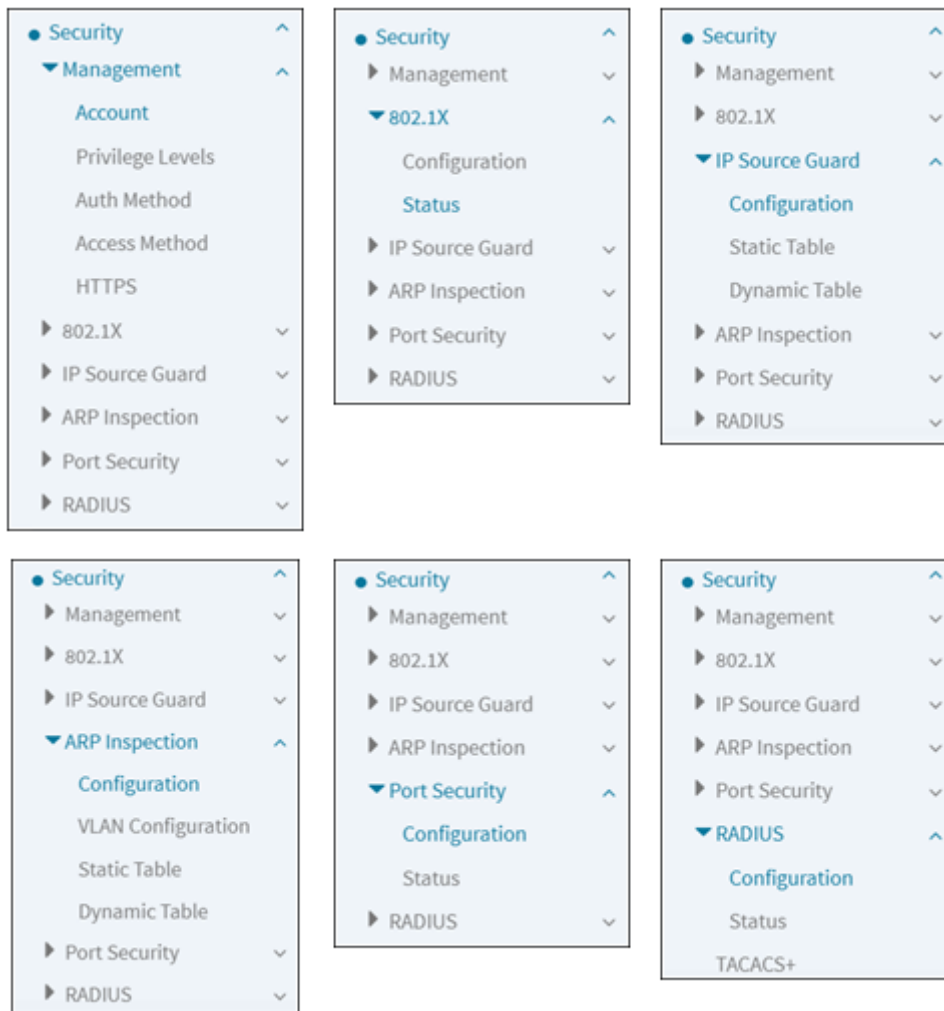
# 12장

## 보안

### 개요

이 섹션에서는 스위치 포트 보안 설정을 나타냅니다. MAC 주소 제한 및 식별을 통해 인터페이스에 입력을 제한하는 포트 보안 기능을 사용할 수 있습니다.

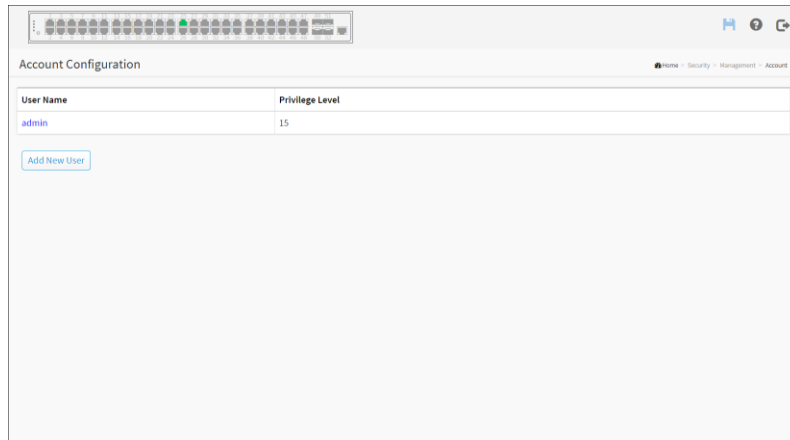
메뉴 및 하위 메뉴는 다음과 같습니다:



## 매니지먼트

### 계정

이 페이지에서 현재 유저의 개요를 제공합니다. 현재 웹 서버의 다른 유저가 로그인 할 수 있는 유일한 방법은 브라우저를 닫고 다시 여는 것 뿐 입니다.



The screenshot shows the 'Account Configuration' page. At the top, there is a breadcrumb trail: Home > Security > Management > Account. Below this is a table with two columns: 'User Name' and 'Privilege Level'. The table contains one entry with 'admin' as the user name and '15' as the privilege level. Below the table is a button labeled 'Add New User'.

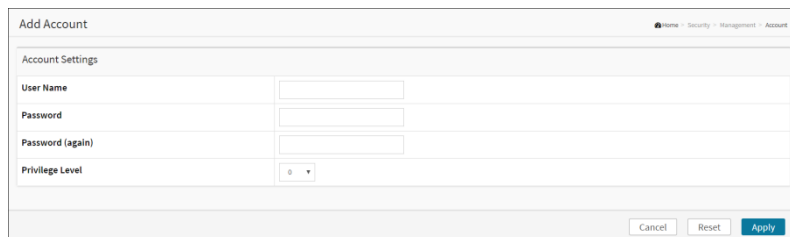
| User Name | Privilege Level |
|-----------|-----------------|
| admin     | 15              |

[Add New User](#)

#### 웹 인터페이스

웹 인터페이스에서 유저를 설정하려면:

1. 보안, 매니지먼트 및 계정을 클릭합니다.
2. 새 유저를 추가를 클릭합니다.



The screenshot shows the 'Add Account' page. At the top, there is a breadcrumb trail: Home > Security > Management > Account. Below this is a form titled 'Account Settings'. The form has four fields: 'User Name', 'Password', 'Password (again)', and 'Privilege Level'. The 'Privilege Level' field is a dropdown menu with '0' selected. At the bottom right of the form are three buttons: 'Cancel', 'Reset', and 'Apply'.

|                  |                          |
|------------------|--------------------------|
| User Name        | <input type="text"/>     |
| Password         | <input type="password"/> |
| Password (again) | <input type="password"/> |
| Privilege Level  | 0 ▼                      |

[Cancel](#) [Reset](#) [Apply](#)

3. 유저 이름 항목을 지정합니다.
4. 적용을 클릭합니다.

## ■ 항목 설명:

유저 이름 (User Name):

유저를 식별하는 이름입니다. 필드는 31자 입력입니다. 이 것은 또한 유저 추가/편집으로 링크됩니다.

패스워드 (Password):

패스워드를 입력합니다. 필드는 31자 입력이며 ASCII 글자 32에서 126을 허용합니다.

패스워드 재입력 (Password (again) ):

패스워드를 다시 입력합니다. 필드에 동일한 패스워드를 다시 입력해야 합니다.

권한 레벨 (Privilege Level):

유저 권한 레벨을 지정합니다. 허용 범위는 0에서 15입니다. 권한 레벨 값이 15이면 모든 그룹에 액세스할 수 있습니다. 즉, 장치에 대한 모든 권한이 있습니다. 그러나 다른 값은 각 그룹 권한 레벨에 따라 달라집니다. 유저의 권한은 그룹에 대한 액세스 권한을 위해 그룹 권한 레벨과 동일하거나 더 커야 합니다. 기본 설정으로 모든 그룹 권한 레벨은 읽기만 가능한 5이며 권한 레벨 10은 읽기-쓰기 권한이 주어집니다. 그리고 시스템 유지 보수 (소프트웨어 업로드, 공장 초기값 등)에는 유저 권한 레벨 15가 필요합니다. 일반적으로 권한 레벨 15는 관리자 계정에 필요하면 권한 레벨 10은 일반 유저 계정에, 그리고 권한 레벨 5는 게스트 계정에 필요합니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

취소 (Cancel):

클릭해 로컬의 변경 사항을 취소하고 유저로 되돌아 갑니다.

유저 삭제 (Delete User):

현재 유저를 삭제합니다. 이 버튼은 새로운 설정에는 사용할 수 없습니다.

(새 유저 추가)

## **권한 레벨**

이 페이지에서는 권한 레벨의 개요를 제공합니다. 스위치는 유저 설정 계정, 집합, 진단, EEE, GARP, GVRP, IP, IPMC 스누핑 LACP LLDP LLDP MED MAC 테이블 MRP MVR MVRP 유지 보수 미러링 POE 포트 권한 VLAN QoS SMTP SNMP 보안 스페닝 트리 시스템 트랩 이벤트 VCL VLANs Voice VLAN 권한 레벨을 1에서 15까지 제공합니다.



### Privilege Levels Configuration

Home > Security > Management > Privilege Levels

| Group Name           | Privilege Levels |            |
|----------------------|------------------|------------|
|                      | Read-only        | Read-write |
| Aggregation          | 5 ▼              | 10 ▼       |
| Debug                | 15 ▼             | 15 ▼       |
| DHCP                 | 5 ▼              | 10 ▼       |
| DHCPv6_Client        | 5 ▼              | 10 ▼       |
| Diagnostics          | 1 ▼              | 10 ▼       |
| DMS_client           | 5 ▼              | 10 ▼       |
| DMS_Trouble_Shooting | 5 ▼              | 10 ▼       |
| DMS_Vbatch           | 5 ▼              | 10 ▼       |
| Firmware             | 5 ▼              | 10 ▼       |
| FRR                  | 5 ▼              | 10 ▼       |
| Green_Ethernet       | 5 ▼              | 10 ▼       |
| Install_Wizard       | 5 ▼              | 10 ▼       |
| IP                   | 5 ▼              | 10 ▼       |
| IPMC_Snooping        | 5 ▼              | 10 ▼       |
| LACP                 | 5 ▼              | 10 ▼       |
| LLDP                 | 5 ▼              | 10 ▼       |
| Loop_Protect         | 5 ▼              | 10 ▼       |
| MAC_Table            | 5 ▼              | 10 ▼       |
| Miscellaneous        | 1 ▼              | 10 ▼       |
| MRP                  | 5 ▼              | 10 ▼       |
| MVR                  | 5 ▼              | 10 ▼       |
| NTP                  | 5 ▼              | 10 ▼       |
| POE                  | 5 ▼              | 10 ▼       |
| Ports                | 1 ▼              | 10 ▼       |
| Private_VLANs        | 5 ▼              | 10 ▼       |
| QoS                  | 5 ▼              | 10 ▼       |
| RMirror              | 5 ▼              | 10 ▼       |
| Security(access)     | 5 ▼              | 10 ▼       |
| Security(network)    | 5 ▼              | 10 ▼       |
| sFlow                | 5 ▼              | 10 ▼       |
| SMTP                 | 5 ▼              | 10 ▼       |
| Spanning_Tree        | 5 ▼              | 10 ▼       |
| System               | 1 ▼              | 10 ▼       |
| Trap_Event           | 5 ▼              | 10 ▼       |
| UDLD                 | 5 ▼              | 10 ▼       |
| uFDMA_AIL            | 5 ▼              | 10 ▼       |
| uFDMA_CIL            | 5 ▼              | 10 ▼       |
| UPnP                 | 5 ▼              | 10 ▼       |
| VCL                  | 5 ▼              | 10 ▼       |
| VLAN_Translation     | 5 ▼              | 10 ▼       |
| VLANs                | 5 ▼              | 10 ▼       |
| Voice_VLAN           | 5 ▼              | 10 ▼       |
| Watchdog             | 5 ▼              | 10 ▼       |
| XXRP                 | 5 ▼              | 10 ▼       |

Reset
Apply

## 웹 인터페이스

웹 인터페이스에서 권한 레벨을 설정하려면:

1. 보안, 매니지먼트 및 권한 레벨을 클릭합니다.
2. 권한 항목을 지정합니다.
3. 적용을 클릭합니다.

### ■ 항목 설명:

그룹 이름 (Group Name):

권한 그룹을 식별하는 이름입니다. 대부분의 경우 권한 레벨 그룹은 싱글 모듈 (예 LACP, STP 또는 QoS)를 포함하지만, 일부는 하나 이상을 포함합니다. 다음은 권한 레벨 그룹 상세 정의에 대한 설명입니다:

시스템 (System): 연락처, 이름, 위치, 시간대, 일광 절약 시간, 기록

권한 레벨 (Privilege Levels):

모든 그룹은 다음의 하위 그룹에 대한 인증 권한 레벨을 갖습니다:

설정 읽기만, 설정/실행 읽기-쓰기.

유저 권한은 그룹에 액세스하기 위해 인증 권한 레벨보다 동일하거나 커야 합니다.

### ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## 인증 방법

이 페이지에서 매니지먼트 클라이언트 인터페이스 중 하나를 통해 스위치에 로그인 시 유저 인증 방식을 설정하는 방법을 나타냅니다.

**Authentication Method Configuration**

Home > Security > Management > Auth Method

**Authentication Method**

| Client  | Method | Service Port |
|---------|--------|--------------|
| console | local  |              |
| telnet  | local  | 23           |
| ssh     | local  | 22           |
| http    | local  | 80           |
| https   | no     | 443          |

**Command Authorization Method**

| Client  | Method | Cmd Lvl | Cfg Cmd                  |
|---------|--------|---------|--------------------------|
| console | no     | 0       | <input type="checkbox"/> |
| telnet  | no     | 0       | <input type="checkbox"/> |
| ssh     | no     | 0       | <input type="checkbox"/> |

**Accounting Method**

| Client  | Method | Cmd Lvl | Exec                     |
|---------|--------|---------|--------------------------|
| console | no     |         | <input type="checkbox"/> |
| telnet  | no     |         | <input type="checkbox"/> |
| ssh     | no     |         | <input type="checkbox"/> |

Reset Apply

웹 인터페이스

웹 인터페이스에서 인증 방식 구성을 설정하려면

1. 보안, 매니지먼트 및 인증 방식을 클릭합니다.
2. 모니터링 하고자 하는 클라이언트 (콘솔, 텔넷, ssh, 웹)를 지정합니다.
3. 방식 (none, local, radius, tacacs), 서비스 포트, Cmd Lvl, Cfg Cmd, Fallback, Exec를 지정합니다.
4. 적용을 클릭합니다.

### ■ 항목 설명:

#### 인증 방식 설정

클라이언트 (Client):

아래의 설정이 적용되는 매니지먼트 클라이언트 입니다.

방식 (Method):

인증 방식은 다음의 값 중 하나로 설정 가능합니다:

none: 인증이 비활성 되며 로그인이 불가능합니다.

local: 인증에 스위치의 로컬 유저 데이터베이스를 사용합니다.

radius: 인증에 원격 RADIUS 서버를 사용합니다.

tacacs: 인증에 원격 TACACS 서버를 사용합니다.

원격 서버와 관련된 방식은 원격 서버가 오프라인인 경우 시간이 초과됩니다. 이러한 경우 다음 방식을 시도합니다. 각 방식은 왼쪽에서 오른쪽으로 시도되며 방식이 유저를 승인하거나 거부할 때까지 지속적으로 시도합니다. 원격 서버가 주 인증으로 사용되면, 부 인증은 'local'로 사용할 것을 권장합니다. 이 것은 설정된 인증 서버가 동작하지 않는 경우 매니지먼트 클라이언트가 로컬 유저 데이터베이스를 통해 로그인 할 수 있도록 합니다.

서비스 포트 (Service Port):

각 클라이언트 서비스의 TCP 포트입니다. 유효 포트 번호는 1 ~ 65534입니다.

HTTP 리디렉트 (HTTP Redirect):

http 자동 재전송을 활성화 합니다.

### **명령어 인증 방식 설정**

클라이언트 (Client):

다음의 방식이 적용되는 매니지먼트 클라이언트입니다.

방식 (Method):

인증 방식은 다음의 값 중 하나로 설정 가능합니다:

none: 인증이 비활성 되며 로그인이 불가능합니다.

tacacs: 인증에 원격 TACACS+ 서버를 사용합니다.

Cmd Lvl:

지정된 권한 레벨의 모든 명령어에 대한 인증을 실행합니다. 인증이 필요한 특정 명령어 레벨입니다. 유효 엔트리는 1에서 15입니다.

Cfg Cmd:

설정 명령어를 활성화 또는 비활성화 합니다.

Fallback:

로컬 데이터베이스는 여러 기능의 대비책 기능으로 동작합니다. 이 동작은 보안 장치의 우발적 잠금을 방지하기 위해 고안되었습니다.

계정 방식 설정

클라이언트 (Client):

다음의 방식이 적용되는 매니지먼트 클라이언트입니다.

방식 (Method):

계정 방식은 다음의 값 중 하나로 설정 가능합니다:

none: 계정이 비활성 되며 로그인이 불가능합니다.

tacacs: 계정에 원격 TACACS+ 서버를 사용합니다.

Cmd Lvl:

지정된 권한 레벨의 모든 명령어에 대한 계정을 실행합니다. 인증이 필요한 특정 명령어 레벨입니다. 유효 엔트리는 1에서 15입니다.

Exec:

유저가 EXEC 구조 실행을 하도록 허용이 되는 경우 계정을 지정하기 위해 실행합니다. 이 것 유저 프로파일 정보를 자동 명령어 정보처럼 돌려 보낼 수 있습니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## 액세스 방법

이 섹션에서는 HTTP/HTTPS, SNMP 그리고 TELNET/SSH를 포함한 스위치의 액세스 매니지먼트 테이블 설정을 보여줍니다.

Access Method Configuration

Mode: ☐ on ☒ off

| Delete                        | VLAN ID | Start IP Address | End IP Address | HTTP/HTTPS | SNMP | TELNET/SSH |
|-------------------------------|---------|------------------|----------------|------------|------|------------|
| <a href="#">Add New Entry</a> |         |                  |                |            |      |            |

[Reset](#) [Apply](#)

### 웹 인터페이스

웹 인터페이스에서 액세스 방법 설정을 구성하려면:

1. 보안, 매니지먼트 및 액세스를 클릭합니다.
2. 액세스 매니지먼트 설정에서 "on"을 선택합니다.
3. "새 엔트리 추가"를 클릭합니다.

| Delete                 | VLAN ID | Start IP Address | End IP Address | HTTP/HTTPS               | SNMP                     | TELNET/SSH               |
|------------------------|---------|------------------|----------------|--------------------------|--------------------------|--------------------------|
| <a href="#">Delete</a> | 1       | 0.0.0.0          | 0.0.0.0        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

[Add New Entry](#)

[Reset](#) [Apply](#)

4. VLAN ID, 시작 IP 주소, 종료 IP 주소를 지정합니다.
5. 엔트리의 액세스 매니지먼트 방식(HTTP/HTTPS, SNMP 그리고 TELNET/SSH)을 확인합니다.
6. 적용을 클릭합니다.

### ■ 항목 설명:

모드 (Mode):

액세스 매니지먼트 모드 동작을 표시합니다. 가능한 모드는 다음과 같습니다:

On: 액세스 매니지먼트 모드 동작을 활성화 합니다.

Off: 액세스 매니지먼트 모드 동작을 비활성화 합니다.

VLAN ID:

액세스 매니지먼트 엔트리에 대한 VLAN ID를 표시합니다.

삭제 (Delete):

체크해 엔트리를 삭제합니다. 다음 저장 동안 삭제됩니다.

시작 IP 주소 (Start IP address):

액세스 매니지먼트 엔트리에 대한 시작 IP 유니캐스트 주소를 표시합니다.

종료 IP 주소 (End IP address):

액세스 매니지먼트 엔트리에 대한 종료 IP 유니캐스트 주소를 표시합니다.

HTTP/HTTPS:

호스트 IP 주소가 엔트리에 제공된 IP 주소 범위와 일치하면, 호스트는 HTTP/HTTPS 인터페이스에서 스위치에 액세스할 수 있음을 표시합니다.

SNMP:

호스트 IP 주소가 엔트리에 제공된 IP 주소 범위와 일치하면, 호스트는 SNMP 인터페이스에서 스위치에 액세스할 수 있음을 표시합니다.

TELNET/SSH:

호스트 IP 주소가 엔트리에 제공된 IP 주소 범위와 일치하면, 호스트는 TELNET/SSH 인터페이스에서 스위치에 액세스할 수 있음을 표시합니다.

## ■ 버튼

새 엔트리 추가(Add New Entry):

새 액세스 매니지먼트 엔트리를 추가하려면 클릭하세요.

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## HTTPS

이 페이지에서 HTTPS 구성 설정과 스위치의 현재 인증을 유지 보수 할 수 있습니다.

## 웹 인터페이스

웹 인터페이스에서 액세스 매니지먼트 설정을 구성하려면:

1. 설정, 보안, 매니지먼트 및 HTTPS를 클릭합니다.
2. 인증 유지보수, 인증 패스 단계, 인증 업로드를 지정합니다.
3. 브라우저를 클릭해 업로드 할 파일을 선택합니다.
4. 적용을 클릭합니다.

## ■ 항목 설명:

인증 유지보수 (Certificate Maintain):

인증 유지보수 동작입니다.

가능한 동작은 다음과 같습니다:

Upload: 인증 PEM 파일을 업로드합니다. 가능한 방식은 웹, 브라우저 또는 URL입니다.

Generate: 새로운 자체 서명 RSA 인증을 동작합니다.

인증 패스 단계 (Certificate Pass Phrase):

업로드하는 인증이 특정 패스 단계로 보호되는 경우 이 필드에 패스 단계를 입력합니다.

인증 업로드 (Certificate Upload):

스위치에 인증 PEM 파일을 업로드 합니다. 파일은 인증과 개인 키를 함께 포함해야 합니다. 인증 및 개인 키 저장에 대한 2개의 분리된 파일이 있다면, Linux cat 명령을 사용해 싱글 PEM 파일에 조합합니다.



예시: `cat my.cert my.key > my.pem`

대부분의 브라우저의 새 버전이 인증의 DSA 지원 (즉, Firefox v37 및 Chrome v39)을 삭제하므로 RSA 인증이 권장됩니다.

가능한 방식은 다음과 같습니다:

Web Browser: 웹 브라우저를 통해 인증서를 업로드 합니다.

URL: URL을 통해 인증서를 업로드합니다. 지원되는 프로토콜은 HTTP, HTTPS, TFTP 그리고 FTP입니다. URL 포맷은 `<protocol>:// [<username>[:<password>]@]<`

`host>[:<port>][/<path>]/<file_name>` 입니다.

예: `tftp://10.10.10.10/new_image_path/new_image.dat`, `http://`

`username:password@10.10.10.10:80/new_image_path/new_image.dat`.

유효한 파일 이름 문자열은 알파벳 (A-Za-z), 숫자(0-9), 점(.), 하이픈(-), 언더라인(\_)입니다. 최대 길이는 63이며 하이픈이 첫번째 글자가 되어서는 안됩니다. 파일 이름에 "."만 있어서는 안됩니다.

인증서 상태 (Certificate Status):

스위치의 인증서의 현재 상태를 표시합니다.

가능한 상태는 다음과 같습니다:

스위치 보안 HTTP 인증서가 표시됩니다.

스위치 보안 HTTP 인증서가 표시되지 않습니다.

스위치 보안 HTTP 인증서가 동작 중 입니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## 802.1X

### 설정

이 섹션에서는 스위치의 802.1X 항목 설정을 설명합니다. 802.1X는 사용자가 인터넷 액세스, 전화 회의, 공유된 프린터 상의 문서 출력을 포함한 다양한 리소스에 연결하거나 인터넷 상에서 간단하게 로그인 하는데 이용됩니다.

802.1X Configuration

Refresh

System Configuration

Mode ☒

Reauthentication Enabled ☐

Reauthentication Period 3600 seconds

EAPOL Timeout 30 seconds

Aging Period 300 seconds

Hold Time 10 seconds

RADIUS-Assigned QoS Enabled ☐

RADIUS-Assigned VLAN Enabled ☐

Guest VLAN Enabled ☐

Guest VLAN ID 1

Max. Reauth. Count 2

Allow Guest VLAN if EAPOL Seen ☐

Port Configuration

| Port | Admin State      | RADIUS-Assigned QoS Enabled | RADIUS-Assigned VLAN Enabled | Guest VLAN Enabled       | Port State        | Restart  |
|------|------------------|-----------------------------|------------------------------|--------------------------|-------------------|--|
| 1    | Force Authorized | <input type="checkbox"/>    | <input type="checkbox"/>     | <input type="checkbox"/> | Globally Disabled | <a href="#">Reauthenticate</a> <a href="#">Reset</a> |
| 2    | Force Authorized | <input type="checkbox"/>    | <input type="checkbox"/>     | <input type="checkbox"/> | Globally Disabled | <a href="#">Reauthenticate</a> <a href="#">Reset</a> |
| 3    | Force Authorized | <input type="checkbox"/>    | <input type="checkbox"/>     | <input type="checkbox"/> | Globally Disabled | <a href="#">Reauthenticate</a> <a href="#">Reset</a> |
| 4    | Force Authorized | <input type="checkbox"/>    | <input type="checkbox"/>     | <input type="checkbox"/> | Globally Disabled | <a href="#">Reauthenticate</a> <a href="#">Reset</a> |
| 5    | Force Authorized | <input type="checkbox"/>    | <input type="checkbox"/>     | <input type="checkbox"/> | Globally Disabled | <a href="#">Reauthenticate</a> <a href="#">Reset</a> |

Reset Apply

### 웹 인터페이스

웹 인터페이스에서 IEEE 802.1 X를 설정하려면:

1. 보안, 802.1 X 및 설정을 클릭합니다.
2. IEEE 802.1 X 설정 모드에서 "on"을 클릭합니다.
3. 재인증 활성화를 체크합니다.
4. 재인증 시간을 설정합니다. (초기값은 3600초입니다.)

5. EAPOL 시간 제한을 설정합니다. (초기값은 30초입니다)
6. 에이징 시간을 설정합니다. (초기값은 300초입니다)
7. 보류 시간을 설정합니다. (초기값은 10초입니다)
8. RADIUS-Assigned QoS 활성화를 체크합니다.
9. RADIUS-Assigned VLAN 활성화를 체크합니다.
10. 게스트 VLAN을 활성화를 체크합니다.
11. 게스트 VLAN ID를 지정합니다.
12. 최대 재인증 수를 지정합니다.
13. EAPOL가 표시되면 게스트 VLAN 허용을 체크합니다.
14. 관리 상태를 선택하고 포트 상태를 표시합니다.
15. 적용을 클릭해 설정을 저장합니다.
16. 설정을 취소하려면 리셋 버튼을 클릭하세요. 이전 저장 값으로 되돌아 갑니다.

## ■ 항목 설명:

### 시스템 설정

모드 (Mode):

on 또는 off

IEEE 802.1X가 스위치 전체에 활성화 또는 비활성화 되면 표시됩니다. 전체적으로 비활성 상태이면 모든 포트는 프레임 전송을 허용합니다.

재인증 활성화 (Reauthentication Enabled):

체크하면 지정된 재인증 시간 간격 후에 성공적으로 인증된 신청자/클라이언트가 재인증 됩니다.

802.1X-활성화 포트에 대한 재인증이 새로운 장치가 스위치 포트에 연결되었는지 또는 연결된 신청자가 더 없는지 탐지하는데 사용됩니다.

MAC 기반 포트의 경우, 재인증은 RADIUS 서버 설정 변경 시에만 유용합니다. 스위치와 클라이언트 간 통신에는 관여하지 않으므로 클라이언트가 포트에 여전히 남아있는지 나타내지 않습니다.

(아래의 에이징 시간 참조)

재인증 시간 (Reauthentication Period):

연결된 클라이언트 재인증 후 초당 시간을 설정합니다. 재인증 활성 체크박스에 체크된 경우에만 동작합니다. 유효값은 1에서 3600초입니다.

EAPOL 시간 제한 (EAPOL Timeout):

Request Identity EAPOL 프레임의 재전송 시간을 지정합니다.

유효 값은 1에서 65535초입니다. MAC 기반 포트에 영향을 미치지 않습니다.

에이징 시간 (Aging Period):

이 설정은 다음의 모드를 적용합니다. 즉, MAC 주소 보안을 위해 포트 보안 기능을 사용하는 모드입니다.

- 싱글 802.1X
- 멀티 802.1X
- MAC 기반 인증

MAC 주소 보안을 위해 NAS 모듈이 포트 보안 모듈을 사용할 때, 주어진 시간 내에 보이는 동작이 없으면 포트 보안 모듈은 주기적인 간격과 무료 리소스에서 문제가 있는 MAC 주소 상의 동작에 대해 확인할 필요가 있습니다. 이 항목은 정확하게 이 시간을 제어하며 10에서 1000000초 사이의 숫자로 설정할 수 있습니다.

재인증은 활성화 되고 포트가 802.1X 기반 모드이면, 포트와 더 이상 연결되지 않은 신청자가 실패할 다음 인증상에서 삭제되기 때문에 더 이상 중요하지 않습니다. 재인증이 활성화 되지 않으면 프리 리소스의 유일한 방법은 엔트리 에이징을 이용하는 것입니다.

MAC 기반 인증 모드의 경우, 재인증은 스위치와 클라이언트 간 직접 통신을 일으키지 않습니다. 따라서 클라이언트가 여전히 연결되어 있는지 여부를 탐지하지 못하며 프리 리소스의 유일한 방법은 엔트리를 에이징하는 것입니다.

보류 시간 (Hold Time):

이 설정은 다음의 모드를 적용합니다. 즉, MAC 주소를 보안하기 위한 포트 보안 기능을 사용하는 모드입니다:

- 싱글 802.1X
- 멀티 802.1X
- MAC 기반 인증

클라이언트가 액세스를 거부하면 - RADIUS 서버가 클라이언트 액세스를 거부하기 때문이거나 RADIUS 서버가 시간 종료("설정→보안→AAA"페이지)를 요청하기 때문에- 클라이언트는 승인되지 않은 상태에서 보류 상태가 됩니다. 보류 타이머는 진행중인 인증 동안 시간을 세지 않습니다.

MAC 기반 인증 모드에서, 스위치는 보류 시간 동안 클라이언트로부터 받는 새 프레임을 무시합니다.

보류 시간은 10에서 1000000 초 사이의 수를 설정합니다.

RADIUS-할당 QoS 활성화 (RADIUS-Assigned QoS Enabled):

RADIUS-할당 QoS은 스위치에 할당된 성공적으로 인증된 신청자로부터 오는 트래픽에 트래픽 클래스를 중앙에서 제어하기 위한 수단을 제공합니다. RADIUS 서버는 특정 RADIUS 특성을 전송하도록 설정되어 이 기능을 이용할 수 있어야 합니다. (상세 정보는 다음의 활성화된 RADIUS-할당 QoS 참조)

“RADIUS-할당 QoS 활성화” 체크 박스는 전체적인 RADIUS-할당 QoS 클래스 기능 활성화/비활성화를 하는 빠른 방법을 제공합니다. 체크하면, 각 포트 동일한 설정은 RADIUS-할당 QoS 클래스가 해당 포트에 활성화 여부를 지정합니다. 체크 해제하면 RADIUS-서버 지정된 QoS 클래스가 모든 포트에 비활성화 됩니다.

RADIUS-할당 VLAN 활성화 (RADIUS-Assigned VLAN Enabled):

RADIUS-할당 VLAN은 스위치 상에 인증된 신청자가 성공적으로 위치한 VLAN을 중앙에서 제어하기 위한 수단입니다.

입력 트래픽은 RADIUS-할당 VLAN에 분류되고 전환됩니다. RADIUS 서버는 특정 RADIUS 특성을 전송하도록 설정되어 이 기능을 이용할 수 있도록 합니다. (상세 정보는 다음의 활성화된 RADIUS-할당 VLAN 참조)

“RADIUS-할당 VLAN 활성화” 체크 박스는 VLAN 기능에 할당된 RADIUS 서버를 전체적으로 활성화/비활성화 하는데 빠른 방법을 제공합니다. 체크하면, 각 포트 동일한 설정은 RADIUS-할당 VLAN이 해당 포트에 활성화 여부를 지정합니다. 체크 해제하면 RADIUS-할당 VLAN이 모든 포트에 비활성화 됩니다.

게스트 VLAN 활성화 (Guest VLAN Enabled):

게스트 VLAN은 특정 VLAN입니다 – 일반적으로 제한된 네트워크 액세스와 함께 – 802.1X에 관련된 – 미인식 클라이언트가 네트워크 관리자 지정 타임 아웃 이후 위치합니다. 스위치는 다음의 목록대로 게스트 VLAN에 들어가고 나오는 것에 대한 규정을 따릅니다.

“게스트 VLAN 활성화” 체크박스는 게스트 VLAN 기능을 활성화/비활성화 하는데 빠른 방법을 제공합니다. 체크하면, 각 포트 동일한 설정은 게스트 VLAN으로 이동할 포트를 지정합니다. 체크 해제 하면 모든 포트의 게스트 VLAN으로 이동 기능은 비활성화 됩니다.

게스트 VLAN ID (Guest VLAN ID):

이 것은 포트가 게스트 VLAN에 이동되는 경우 포트의 포트 VLAN ID이 설정되는 값입니다. 게스트 VLAN 옵션이 전부 활성화 된 경우에만 변경 가능합니다.

유효 값은 [1; 4094]의 범위입니다.

최대 재인증 수 (Max. Reauth. Count):

게스트 VLAN 입력을 고려하기 전 스위치가 응답없이 EAPOL Request Identity 프레임을 전송하는 횟수가 이 설정에서 조정됩니다. 이 값은 게스트 VLAN 옵션이 전부 활성화 된 경우에만 변경 가능합니다.

유효 값은 [1; 255]의 범위입니다.

EAPOL이 보이면 게스트 VLAN 허용 (Allow Guest VLAN if EAPOL Seen):

스위치는 EAPOL 프레임이 포트 수명 동안 포트 상에 수신되는지 기억합니다. 스위치가 게스트 VLAN을 입력하는지 여부를 고려하면, 이 옵션의 활성화/비활성화 여부를 먼저 확인할 것 입니다. 비활성화 (체크 해제;초기값) 되면 EAPOL 프레임이 포트에 포트 수명 동안 수신되지 않는 경우 스위치는 게스트 VLAN만 입력합니다. 활성화 (체크)되면 스위치는 EAPOL 프레임이 포트에 포트 수명 동안 수신되더라도 게스트 VLAN 입력을 고려할 것 입니다.

이 값은 게스트 VLAN 옵션이 전부 활성화 된 경우에만 변경 가능합니다.

### **포트 설정**

포트 (Port):

다음의 설정이 적용되는 포트 번호입니다.

관리자 상태 (Admin State):

802.1X가 전체적으로 활성화 되면 이 섹션은 포트의 인증 모드를 제어합니다. 다음의 모드가 가능합니다:

- ◆ Force Authorized:  
이 모드에서, 스위치는 포트 링크가 나타나면 하나의 EAPOL 성공 프레임을 전송할 것 입니다. 그리고 포트의 모든 클라이언트는 인증 없이 네트워크 액세스가 허용됩니다.
- ◆ Force Unauthorized:  
이 모드에서 스위치는 포트 링크가 나타나면 하나의 EAPOL 실패 프레임을 전송할 것 입니다. 그리고 포트의 모든 클라이언트는 인증 없이 네트워크 액세스가 허용되지 않습니다.
- ◆ Port-based 802.1X:  
802.1X-world에서 유저는 신청자라고 불리며, 스위치는 인증자 그리고 RADIUS 서버는 인증 서버라고 불립니다. 인증자는 중간자로서 동작하며 신청자와 인증 서버간 요청과 응답을 전송합니다. 신청자와 스위치 간 전송된 프레임은 특정 802.1X 프레임이며, EAPOL (EAP Over LANs)로 알려져 있습니다. EAPOL 프레임은 EAP PDU (RFC3748)을 압축합니다. 스위치와 RADIUS 서버 간 전송된 프레임은 RADIUS 패킷입니다. RADIUS 패킷은 또한

스위치의 IP 주소, 이름 및 신청자의 포트 번호와 같이 EAP PDU를 다른 특징과 함께 압축합니다. EAP는 매우 유연하며 MD5-Challenge, PEAP 및 TLS와 같은 다른 인증 방식을 허용합니다. 중요한 것은 인증자(스위치)가 신청자 및 인증 서버가 사용하는 인증 방식과 특정 방식에 필요한 프레임 교환 정보의 수를 알 필요가 없습니다. 스위치는 간단히 관련 타입(EAPOL 또는 RADIUS)으로의 프레임의 EAP 부분을 압축하고 전송합니다.

인증이 완료되면 RADIUS 서버는 성공 또는 실패 식별을 담은 특정 패킷을 전송합니다. 신청자에게 이 결정을 전송하는 것 외에 스위치는 신청자에 연결된 스위치 포트의 트래픽을 열거나 막는데 사용합니다.

---

**주의:** 2개의 후단부 서버가 활성화 되고 서버 타임아웃이 X 초로 설정(AAA 설정 페이지를 사용)된다고 추정하며 목록의 첫 번째 서버는 현재 동작하지 않습니다. (완전 동작이 안되는 것으로 아닙니다.)

현재, 신청자가 X초보다 더 빠른 속도에서 EAPOL 시작 프레임을 전송하면, 신청자로부터 새로운 EAPOL 시작 프레임을 수신할 때 마다 스위치가 동작 중인 후반부 인증 서버 요청을 취소하므로 인증이 되지 않을 것 입니다.

- ◆ Single 802.1X:

포트 기반 Single 802.1X 인증에서, 일단 신청자가 성공적으로 포트에서 인증되면 모든 포트는 네트워크 트래픽에 대해 개방됩니다. 이 것은 포트에 연결된 다른 클라이언트 (허브를 통하는 것과 같은)가 성공적으로 인증된 클라이언트에 편승되도록 하고 인증되지 않아도 네트워크 액세스를 얻을 수 있도록합니다. 이러한 보안 위험을 극복하려면, Single 802.1X 변량을 사용합니다. Single 802.1X는 실제로 IEEE 표준이 아닌 포트 기반 802.1X로 동작하는 많은 동일한 특성의 기능을 합니다. Single 802.1X에서 한 번에 최대 하나의 신청자가 인증 가능합니다. 정상 EAPOL 프레임은 신청자와 스위치 간 통신에 사용됩니다. 하나 이상의 신청자가 포트에 연결되면, 포트의 링크가 나타나는 것이 처음으로 고려될 것 입니다.

특정 시간 내에 신청자가 유효한 자격을 제공하지 않는다면, 다른 신청자가 기회를 얻게 됩니다. 신청자가 성공적으로 인증되면 신청자에게 액세스가 허용됩니다. 이 것은 지원되는 모드의 최대 보안입니다. 이 모드에서, 성공적으로 인증되면 포트 보안 모듈은 신청자의 MAC 주소를 보안하기 위해 사용됩니다.

- ◆ Multi 802.1X:

포트 기반 802.1X 인증에서, 포트 상에서 신청자가 성공적으로 인증되면, 전체 포트는 네트워크 트래픽에 대해 개방됩니다. 포트에 연결된 다른 클라이언트(허브를 통하는 것과 같은)가 성공적으로 인증된 클라이언트 상에 편승되고 인증되지 않더라도 네트워크 액세스가 되도록 허용합니다. 이러한 보안 위험을 극복하려면 Multi 802.1X 변량을 사용합니다.

Multi 802.1X은 실제로 IEEE 표준이 아닌 포트 기반 802.1X로 동작하는 많은 동일한 특성의 기능을 합니다. Multi 802.1X는 - Single 802.1X처럼 - IEEE 표준이 나뉜 동일한 많은 특성의 기능을 하는 변량입니다. Multi 802.1X에서, 포트 보안 모듈을 이용해 하나 이상의 신청자가 독립적으로 인증되고 MAC 테이블에 보안됩니다.

Multi 802.1X에서, 모든 신청자가 스위치에서 전송되는 요청에 응답하기 위한 포트 연결을 발생시키므로 신청자에 대한 스위치로부터 전송되는 EAPOL 프레임을 위해 멀티캐스트 BPDU MAC 주소를 대상 MAC 주소로써 사용할 수 없습니다. 대신 스위치는 신청자에 의해 전송되는 첫 번째 EAPOL 시작 또는 EAPOL 응답 식별 프레임을 포함하는 신청자의 MAC 주소를 사용합니다. 이에 대한 예외는 신청자가 연결된 것이 없을 때입니다. 이 경우 스위치는 포트 상에 있을 수 있는 신청자를 동작시키기 위해 대상으로서 BPDU 멀티캐스트 MAC 주소를 EAPOL 응답 식별 프레임을 전송합니다.

포트에 연결 가능한 신청자의 최대 수는 포트 보안 제한 컨트롤 기능을 이용해 제한할 수 있습니다.

- ◆ MAC-based Auth.:

port-based 802.1X과 달리 MAC 기반 인증은 표준은 아니며, 그저 산업에 사용된 가장 실용적인 방법입니다. MAC 기반 인증에서, 유저는 클라이언트라 불리며 스위치는 클라이언트 대신 신청자로서 동작합니다. 클라이언트에 의해 전송된 초기 프레임(모든 종류의 프레임)은 스위치에 의해 스누핑 되며, RADIUS 서버와 교체하는 EAP에서 유저이름과 패스워드로써 클라이언트의 MAC 주소를 차례로 사용합니다.



6-바이트 MAC 주소는 다음의 형식 "xx-xx-xx-xx-xx-xx"의 문자열로 변환합니다. 이 것은 대시 (-)는 소문자 16진수 숫자 간 선별기로 사용됩니다. 스위치는 MD5-Challenge 인증 방식만 지원하므로 RADIUS 서버는 그에 따라 설정됩니다.

인증이 완료되면 RADIUS 서버는 스위치가 포트 보안 모듈을 사용해 특정 클라이언트에 대한 트래픽을 개방하거나 차단하게 하는 성공 또는 실패 표시를 전송합니다. 그런 이후에만 스위치에서 클라이언트로부터의 프레임이 전송됩니다. 인증과 관련된 EAPOL 프레임이 없으므로 MAC 기반 인증은 802.1X 표준과 관련이 없습니다.

포트 기반 802.1X를 통한 MAC 기반 인증의 장점은 여러 클라이언트가 같은 포트(예, 외부 스위치 또는 허브를 통해)에 연결 가능하며 독립적인 인증이 가능합니다. 그리고 클라이언트는 인증을 위해 특정 신청자 소프트웨어가 필요없습니다. 802.1X를 통한 MAC 기반 인증의 장점은 클라이언트는 인증에 특별한 신청자 소프트웨어를 필요로 하지 않는다는 것입니다. 단점은 MAC 주소가 악성 유저- 유저의 MAC 주소가 유효한 RADIUS 유저 장비는 누구에게든 사용될 수 있습니다 - 에 의해 스푸핑 될 수 있다는 것입니다. 또한 MD5-Challenge 방식만 지원됩니다. 포트에 연결 가능한 최대 클라이언트 수는 포트 보안 제한 컨트롤 기능을 사용해 제한할 수 있습니다.

RADIUS-할당 QoS 활성화 (RADIUS-Assigned QoS Enabled):

RADIUS-할당 QoS 활성화는 주어진 포트 상의 전체 활성화 및 활성화 (체크된 것) 되었을 때, 신청자가 성공적으로 인증된 경우 스위치는 RADIUS 서버에 의해 전송된 RADIUS Access-Accept 패킷에서 실행되는 QoS 클래스 정보에 반응합니다. 표시되고 유효하면, 신청자 포트 상의 수신된 트래픽은 주어진 QoS 클래스 정보에 반응합니다. 만일 (재)인증이 실패하거나 RADIUS Access-Accept 패킷이 더 이상 QoS 클래스 실행하지 않거나 유효하지 않거나 또는 그 반대로 신청자가 포트에 더 이상 표시되지 않으면, 포트의 QoS 클래스 정보는 즉시 본래의 QoS 클래스 정보 (RADIUS-할당에 영향을 주지 않고 관리자에 의해 변경 가능)로 되돌아 갑니다.

이 옵션은 싱글 클라이언트 모드에서만 가능합니다:

- Port-based 802.1X
- Single 802.1X

QoS 클래스 식별에 사용되는 RADIUS 특성:

RFC4675에서 정의되는 유저-우선-테이블 특징은 Access-Accept 패킷의 QoS 클래스 식별에 을 기준으로 생성합니다.

패킷에서 첫 특성 발생만 간주되며 유효합니다.

이 것은 다음의 규칙을 따릅니다:

- 특성 값의 모든 8 옥텟은 동일해야 하며 범위 [0; 7]에서 필요한 QoS 클래스로 변환하는 범위 '0' - '7'의 ASCII 글자를 포함해야 합니다.

RADIUS-할당 VLAN 활성화 (RADIUS-Assigned VLAN Enabled):

RADIUS-할당 VLAN은 주어진 포트에 전체적으로 활성화 또는 활성화 (체크된 것) 일 때, RADIUS 서버에 의해 전송된 RADIUS Access-Accept 패킷에서 실행되는 VLAN ID 정보에 반응합니다.

표시되고 유효하면, 포트의 포트 VLAN ID는 이 VLAN ID로 변경되며 포트는 VLAN ID 멤버가 되도록 설정되며 포트는 강제로 VLAN 미인식 모드가 됩니다. 일단 할당되면, 포트에 도달하는 모든 트래픽은 RADIUS-할당 VLAN ID 상에 분류되고 전환됩니다.

만일 (재)인증이 실패 또는 RADIUS Access-Accept 패킷이 더 이상 VLAN ID를 실행하지 않거나 또는 무표화 되거나 또는 그 반대로 신청자가 포트에 더 이상 표시되지 않으면, VLAN ID는 즉시 본래의 VLAN ID(RADIUS-할당에 영향을 주지 않고 관리자에 의해 변경 가능)로 되돌아 갑니다.

이 옵션은 싱글 클라이언트 모드에서만 가능합니다:

- Port-based 802.1X
- Single 802.1X

문제 해결 VLAN 할당은 “모니터→VLAN→VLAN 멤버십 및 VLAN 포트” 페이지를 참조하십시오.

이 페이지는 어느 모듈이 (한시적으로) 현재 포트 VLAN 설정을 중복하는지 표시합니다.

VLAN ID 식별에 사용되는 RADIUS 특성 (RADIUS attributes used in identifying a VLAN ID):

RFC2868와 RFC3580는 Access-Accept 패킷에서 VLAN ID를 식별하는데 사용되는 특성을 기준으로 생성합니다. 다음의 기준이 사용됩니다:

- Tunnel-Medium-Type, Tunnel-Type 및 Tunnel-Private-Group- ID 특성은 Access-Accept 패킷에서 최소한 한번은 표시되어야 합니다.
- 스위치는 동일한 태그 값을 가진 이러한 특성의 첫 설정을 찾으며 다음의 요구사항을 충족합니다. (Tag == 0이 사용되면, Tunnel-Private-Group-ID는 태그를 포함할 필요가 없습니다):
  - Tunnel-Medium-Type 값이 “IEEE-802” (ordinal 6)으로 설정되어야 합니다.
  - Tunnel-Type 값이 “VLAN” (ordinal 13)으로 설정되어야 합니다.
  - Tunnel-Private-Group- ID 값이 '0' - '9' 범위 내의 ASCII 문자열이어야 하며, VLAN ID를 표시하는 십진법 글자로 해석됩니다. 앞 글자의 '0'은 삭제됩니다. 최종 값은 [1; 4095] 범위입니다.

게스트 VLAN 활성화 (Guest VLAN Enabled):

게스트 VLAN이 주어진 포트에 전체적으로 활성화 또는 활성화 (체크된 것) 일 때, 스위치는 다음의 규칙에 따라 포트를 게스트 VLAN으로 이동하려고 합니다.

이 옵션은 EAPOL-기반 모드에서만 가능합니다:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

문제 해결 VLAN 할당은 “모니터→VLAN→VLAN 멤버십 및 VLAN 포트” 페이지를 참조하십시오.

이 페이지는 어느 모듈이 (한시적으로) 현재 포트 VLAN 설정을 중복하는지 표시합니다.

게스트 VLAN 동작 (Guest VLAN Operation):

포트 링크에 활성화 된 게스트 VLAN이 나타나면, 스위치는 EAPOL 요청 식별 프레임 전송을 시작합니다. 이 프레임의 전송 수가 최대 재인증 수를 초과하고 그 동안 EAPOL 프레임이 수신되지 않으면, 스위치는 게스트 VLAN 입력을 고려합니다. EAPOL 요청 식별 프레임 간 간격은 EAPOL 타임아웃과 설정됩니다. 표시되는 EAPOL이 활성화 되는 경우 게스트 VLAN을 허용하면, 포트는 게스트 VLAN에 위치할 것 입니다. 비활성화 시 스위치는 EAPOL 프레임이 이전에 포트에 수신되었는지 기록을 먼저 확인합니다. (포트 링크가 내려가거나 포트 관리 상태가 변경되면 기록이 삭제됩니다.) 수신되지 않으면 포트는 게스트 VLAN에 위치할 것 입니다. 그렇지 않은 경우 게스트 VLAN으로 이동하지 않으나 계속해서 EAPOL 요청 식별 프레임을 EAPOL 타임아웃에 의해 지정된대로 전송합니다.

게스트 VLAN에서 일단 포트가 인증이 고려가 되면 모든 연결된 포트의 클라이언트는 이 VLAN에 액세스가 허용됩니다. 게스트 VLAN 입력 시 스위치는 EAPOL 성공 프레임을 전송하지 않습니다. 게스트 VLAN에서 스위치는 EAPOL 프레임에 대한 링크를 모니터하며 하나의 프레임이 수신되면 스위치는 즉시 포트를 게스트 VLAN에서 빼어 포트 모드에 맞게 신청자 인증을 시작합니다. EAPOL 프레임이 수신되면 “Allow Guest VLAN if EAPOL Seen” 비활성화 시 포트는 게스트 VLAN으로 돌아갈 수 있습니다.

포트 상태 (Port State):

포트의 현재 상태입니다. 다음의 값 중 하나를 실행할 수 있습니다:

Globally Disabled: IEEE 802.1X가 전체 비활성화 입니다.

Link Down: IEEE 802.1X가 전체 활성화이나 포트에 링크가 없습니다.

Authorized: 포트는 Force Authorized 또는 single-supPLICant 모드에 있으며 신청자는 인증되었습니다.

Unauthorized: 포트는 Force Unauthorized 또는 single-supPLICant 모드에 있으며, 신청자는 RADIUS 서버에 의해 성공적으로 인증되지 않았습니다.

X Auth/Y Unauth: 포트가 multi-supPLICant에 있습니다. 현재 X 클라이언트는 인증되었으며 Y는 미인증 상태입니다.

재시작 (Restart):

각 열에는 2개의 버튼이 있습니다. 버튼은 전체 인증 상태 또는 포트의 관리자 상태가 EAPOL 기반이거나 MAC 기반 모드에 있는 경우에만 활성화 됩니다.

버튼 클릭이 실행되는 페이지에서 변경된 설정의 원인이 되지 않습니다.

재인증 (Re-authenticate): 포트의 유지 기간이 종료(EAPOL 기반 인증)될 때마다 재인증 일정을 생성합니다. MAC 기반 인증, 재인증이 즉시 시도됩니다.

버튼은 포트의 성공적으로 인증이 된 클라이언트에만 적용되며 클라이언트가 한시적으로 미인증 되도록 하지 않습니다.

재초기화 (Reinitialize): 포트 상의 클라이언트의 재인증을 강제로 실행하므로 재인증이 즉시 실행됩니다. 클라이언트는 재인증이 진행되는 동안 미인증된 상태로 전송할 것 입니다.

## ■ 버튼

적용 (Apply):

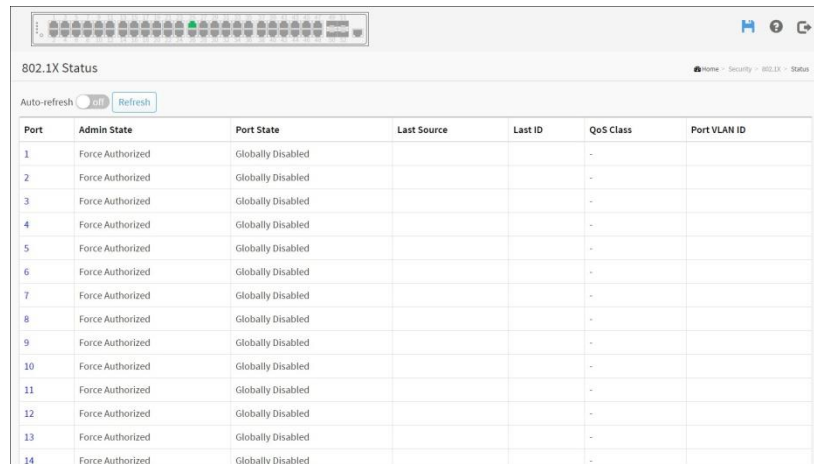
변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## 상태

이 섹션에서 스위치의 각 포트 802.1X 상태 표시를 설명합니다. 상태는 관리 상태, 포트 상태, 마지막 소스, 마지막 ID 및 포트 VLAN ID를 포함합니다.



| Port | Admin State      | Port State        | Last Source | Last ID | QoS Class | Port VLAN ID |
|------|------------------|-------------------|-------------|---------|-----------|--------------|
| 1    | Force Authorized | Globally Disabled |             |         | -         |              |
| 2    | Force Authorized | Globally Disabled |             |         | -         |              |
| 3    | Force Authorized | Globally Disabled |             |         | -         |              |
| 4    | Force Authorized | Globally Disabled |             |         | -         |              |
| 5    | Force Authorized | Globally Disabled |             |         | -         |              |
| 6    | Force Authorized | Globally Disabled |             |         | -         |              |
| 7    | Force Authorized | Globally Disabled |             |         | -         |              |
| 8    | Force Authorized | Globally Disabled |             |         | -         |              |
| 9    | Force Authorized | Globally Disabled |             |         | -         |              |
| 10   | Force Authorized | Globally Disabled |             |         | -         |              |
| 11   | Force Authorized | Globally Disabled |             |         | -         |              |
| 12   | Force Authorized | Globally Disabled |             |         | -         |              |
| 13   | Force Authorized | Globally Disabled |             |         | -         |              |
| 14   | Force Authorized | Globally Disabled |             |         | -         |              |

### 웹 인터페이스

웹 인터페이스에서 802.1X 상태를 표시하려면:

1. 보안, IEEE 802.X 및 상태를 클릭합니다.
2. "자동 새로고침"을 체크합니다.
3. "새로 고침"을 클릭해 포트 상세 현황을 새로 고침하세요.
4. 802.1X 현황을 표시하고자 하는 포트를 선택합니다.

### ■ 항목 설명:

#### 802.1X 상태

포트 (Port):

스위치 포트 번호입니다. 클릭해 이 포트에 대한 802.1X 상세 상태를 탐색합니다.

관리 상태 (Admin State):

포트 현재 관리 상태입니다. 가능한 값의 설명에 대한 802.1X 상세 상태를 참조하세요.

포트 상태 (Port State):

포트의 현재 상태입니다. 각 상태의 설명에 대한 802.1X 포트 상태를 참조하세요.

마지막 소스 (Last Source):

EAPOL 기반 인증을 위한 EAPOL 프레임에서 가장 최근 수신되었거나 또는 MAC 기반 인증을 위한 새 클라이언트에서 가장 최근 수신된 소스 MAC 주소입니다.

마지막 ID (Last ID):

EAPOL 기반 인증을 위한 가장 최근 Response Identity EAPOL 프레임에서 수신되었거나 MAC 기반 인증을 위한 새 클라이언트에서 가장 최근 수신된 프레임에서 수신된 유저 이름 (신청자 ID)입니다.

QoS 클래스 (QoS Class):

활성화 되면 RADIUS 서버에 의해 포트에 할당된 QoS 클래스입니다.

포트 VLAN ID (Port VLAN ID):

802.1X가 포트를 입력하는 VLAN ID입니다. 포트 VLAN ID는 802.1X로 중복되지 않으면 필드는 공백입니다.

VLAN ID가 RADIUS 서버에 의해 할당되면, "(RADIUS-assigned)"가 VLAN ID에 추가됩니다. 이 곳에서 RADIUS 할당 VLAN에 대한 상세 정보를 알 수 있습니다.

포트가 게스트 VLAN으로 이동되면 VLAN ID에 "(Guest)"가 추가됩니다. 이 곳에서 게스트 VLAN에 대한 상세 정보를 알 수 있습니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

포트 1-52 상태 (Port 1-52 Status):

포트 상태를 개별적으로 보려면 포트 번호를 클릭합니다.



## ■ 항목 설명:

포트 (Port):

드롭 다운 메뉴를 사용해 표시하고자 하는 포트를 선택합니다.

관리 상태 (Admin State):

포트 현재 관리 상태입니다. 가능한 값의 설명에 대한 802.1X 상세 상태를 참조하세요.

포트 상태 (Port State):

포트의 현재 상태입니다. 각 상태의 설명에 대한 802.1X 포트 상태를 참조하세요.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

## IP 소스 보호

이 섹션에서 스위치의 IP 소스 보호 상세 항목을 설정하는 방법을 설명합니다. 스위치 포트에 IP 소스 가드를 활성화 또는 비활성화 설정할 수 있습니다.

### 설정

이 섹션은 다음을 포함한 IP 소스 보호 설정 방법을 설명합니다:

모드 (활성화 및 비활성화)

최대 동적 클라이언트 (0, 1, 2 제한 없음)

| Port | Mode     | Max Dynamic Clients |
|------|----------|---------------------|
| 1    | Disabled | Unlimited           |
| 2    | Disabled | Unlimited           |
| 3    | Disabled | Unlimited           |
| 4    | Disabled | Unlimited           |
| 5    | Disabled | Unlimited           |
| 6    | Disabled | Unlimited           |
| 7    | Disabled | Unlimited           |

### 웹 인터페이스

웹 인터페이스에서 IP 소스 보호 설정을 구성하려면:

1. 보안, IP 소스 보호 및 설정을 클릭합니다.
2. IP 소스 보호 설정 모드에서 "on"을 선택합니다.
3. 포트 모드 설정 모드에서 특정 포트의 "Enabled"를 선택합니다.
4. 포트 모드 설정 모드에서 특정 포트의 최대 동적 클라이언트 (0, 1, 2 제한 없음)를 선택합니다.
5. 적용을 클릭합니다.



## ■ 항목 설명:

IP 소스 보호 설정 모드 (Mode of IP Source Guard Configuration):

글로벌 IP 소스 보호를 활성화 또는 비활성화 합니다. 모든 설정된 ACE는 모드 활성화 시 없어질 것 입니다.

포트 모드 설정 (Port Mode Configuration):

IP 소스 보호가 어느 포트에서 활성화 될 지 지정합니다. 주어진 포트의 글로벌 모드 및 포트 모드에서만 활성화되며, IP 소스 보호는 이 주어진 포트상에서 활성화됩니다.

최대 동적 클라이언트 (Max Dynamic Clients):

주어진 포트 상에서 표시될 수 있는 동적 클라이언트 최대 수를 지정합니다. 이 값은 0, 1, 2 또는 무제한입니다. 포트 모드가 활성화 되고 최대 동적 클라이언트 값이 0과 동일하면, 특정 포트 상의 정적 엔트리에 일치하는 IP 패킷 전송만 허용한다는 것을 의미합니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

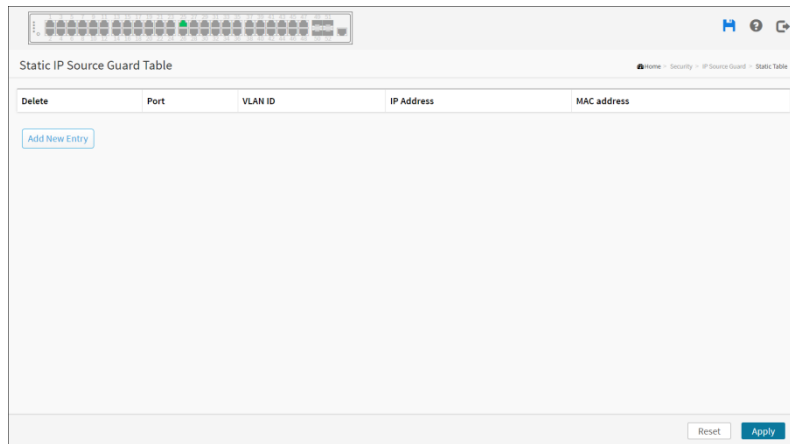
로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

동적에서 정적으로 변환 (Translate dynamic to static):

모든 동적 엔트리를 정적 엔트리로 변환하려면 클릭합니다.

## 정적 테이블

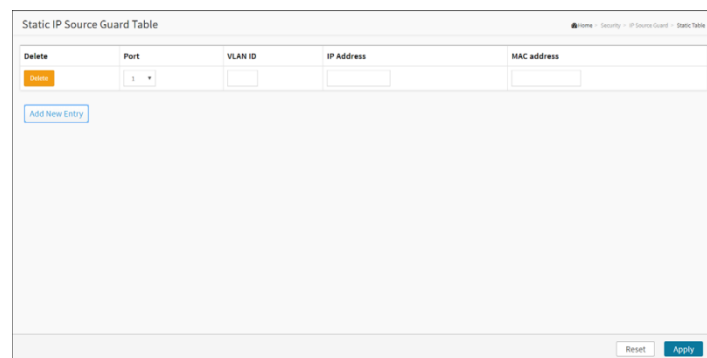
이 섹션에서 스위치의 정적 IP 소스 보호 테이블 항목 설정을 설명합니다. 엔트리를 관리하도록 설정하려면 정적 IP 소스 보호 테이블을 사용합니다.



## 웹 인터페이스

웹 인터페이스에서 정적 IP 소스 보호 테이블 설정을 구성하려면:

1. 보안, IP 소스 보호 및 정적 테이블을 클릭합니다.
2. “새 엔트리 추가”를 클릭합니다.



3. 엔트리의 포트, VLAN ID, IP 주소 및 MAC 주소를 지정합니다.
4. 적용을 클릭합니다.

## ■ 항목 설명:

포트 (Port):

설정에 대한 논리적 포트입니다.

VLAN ID:

설정의 vlan id 입니다.

IP 주소 (IP Address):

허용된 소스 IP 주소입니다.

MAC 주소 (MAC address):

허용된 소스 MAC 주소입니다.

## ■ 버튼

새 엔트리 추가 (Add New Entry):

정적 IP 소스 보호 테이블에 새 엔트리를 클릭합니다. 새 엔트리의 포트, IP 주소 및 MAC 주소를 지정합니다. "적용"을 클릭합니다.

삭제 (Delete):

엔트리를 삭제하려면 확인합니다. 다음 저장 동안 삭제될 것 입니다.

적용 (Apply):

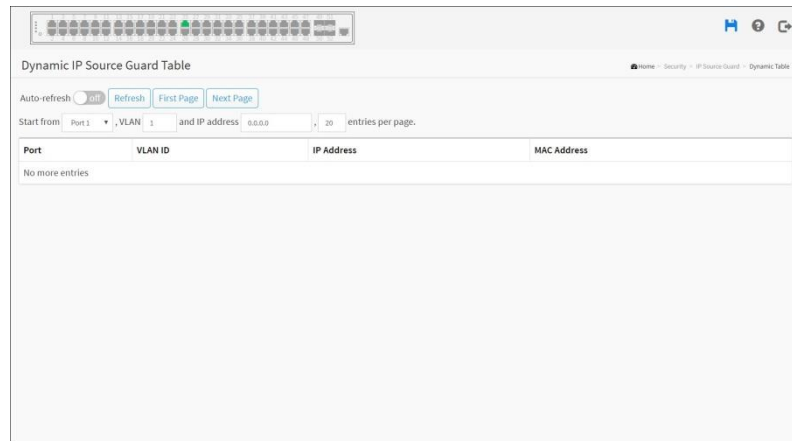
변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## 동적 테이블

동적 IP 소스 보호 테이블의 엔트리가 이 페이지 상에 보여 줍니다. 동적 IP 소스 보호 테이블은 포트, IP 주소 및 MAC 주소 순으로 정렬됩니다.



## 웹 인터페이스

웹 인터페이스에서 동적 IP 소스 보호 테이블 설정을 구성하려면:

1. 보안, IP 소스 보호 및 동적 테이블을 클릭합니다.
2. "자동 새로 고침"을 확인합니다.
3. "새로 고침"을 클릭해 포트 상세 현황을 새로 고침 합니다.
4. 첫/다음 페이지를 클릭해 페이지를 변경합니다.
5. 페이지 당 포트, VLAN, IP 주소 및 엔트리를 지정합니다.

## ■ 항목 설명:

### IP 소스 보호 테이블 탐색

각 페이지는 동적 IP 소스 보호 테이블에서 최대 99 엔트리를 표시합니다. 초기값은 20이며 "페이지 당 엔트리" 입력 필드를 통해 선택됩니다. 처음 방문 시, 웹 페이지는 동적 IP 소스 보호 테이블의 처음부터 첫 20개 엔트리를 표시합니다.

"포트 주소부터 시작", "VLAN" 및 "IP 주소" 입력 필드에서 유저는 동적 IP 소스 보호 테이블의 시작 포인트를 선택할 수 있습니다.

"새로 고침" 버튼을 클릭해 동적 IP 주소 보호 테이블과 일치하는 것부터 또는 가장 가까운 것 부터 표시된 테이블을 업데이트합니다. 또한 2개의 입력 필드 - "새로 고침" 버튼 클릭 시 - 는 처음 표시된 엔트리 값을 추정하므로, 동일한 시작 주소와 함께 지속적으로 새로 고침 합니다. "다음 페이지"는 다음 탐색을 기준으로 현재 표시된 테이블의 마지막 엔트리를 사용합니다.

마지막에 도달하면 나타난 테이블에 "No more entries"가 표시됩니다. "첫 페이지" 버튼을 사용해 다시 시작합니다.

포트 (Port):

엔트리가 표시된 스위치 포트 번호입니다.

VLAN ID:

IP 트래픽이 허용된 VLAN ID입니다.

IP 주소 (IP Address):

엔트리의 유저 IP 주소입니다.

MAC 주소 (MAC Address):

소스 MAC 주소입니다.

엔트리 표시 (Show entries):

표시하고자 하는 항목 수를 선택할 수 있습니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

첫 페이지 (First Page):

시스템 로그 엔트리를 업데이트 해 첫 페이지로 이동합니다.

다음 페이지 (Next Page):

그룹 정보 엔트리를 업데이트 해 다음 페이지로 이동합니다.

## ARP 검사

이 섹션은 스위치의 ARP 검사 항목 설정을 설명합니다. ARP 테이블을 관리하려면 ARP 검사 설정을 사용합니다.

### 설정

이 섹션에서 다음과 같은 ARP 검사 설정 방법을 설명합니다:

모드 (on / off)

포트 (활성화 / 비활성화)

| Port | Mode     | Check VLAN | Log Type |
|------|----------|------------|----------|
| *    | on       | on         | on       |
| 1    | Disabled | Disabled   | None     |
| 2    | Disabled | Disabled   | None     |
| 3    | Disabled | Disabled   | None     |
| 4    | Disabled | Disabled   | None     |
| 5    | Disabled | Disabled   | None     |
| 6    | Disabled | Disabled   | None     |
| 7    | Disabled | Disabled   | None     |

### 웹 인터페이스

웹 인터페이스에서 ARP 검사 설정을 구성하려면:

1. 보안, ARP 검사 및 설정을 클릭합니다.
2. ARP 검사 설정 모드에서 "on"을 선택합니다.
3. 포트 모드 설정 모드에서 지정 포트의 "Enabled"를 선택합니다.
4. 적용을 클릭합니다.

### ■ 항목 설명:

ARP 검사 설정 모드 (Mode of ARP Inspection Configuration):

글로벌 ARP 검사 활성화 또는 글로벌 ARP 검사 비활성화 입니다.

포트 모드 설정 (Port Mode Configuration):

ARP 검사가 어느 포트 상에 활성화 될지 지정합니다. 글로벌 모드와 주어진 포트 상의 포트 모드가 활성화 될 때만 ARP 검사가 주어진 포트 상에 활성화 됩니다. 가능한 문는 다음과 같습니다:

Enabled: ARP 검사 동작을 활성화 합니다.

Disabled: ARP 검사 동작을 비활성화 합니다.

VLAN 설정을 검사하고자 하면, "VLAN 확인" 설정을 활성화 해야 합니다. 기본 설정은 비활성 입니다. "VLAN 확인"이 비활성 시, ARP 검사 로그 타입은 포트 설정을 참조합니다. "VLAN 확인" 설정을 활성화 되면 ARP 검사 로그 타입은 VLAN 설정을 참조합니다. "VLAN 확인"의 가능한 설정은 다음과 같습니다:

Enabled: VLAN 확인 동작을 활성화 합니다.

Disabled: LAN 확인 동작을 비활성화 합니다.

글로벌 모드 및 주어진 포트의 포트 모드가 활성화 되고, "VLAN 확인" 설정이 비활성화 되는 경우에만 ARP 검사 로그 타입은 포트 설정을 참조합니다. 4개의 로그 타입이 있으며 가능한 타입은 다음과 같습니다:

None: 로그 없음

Deny: 엔트리가 거부된 로그

Permit: 엔트리가 허용된 로그

ALL: 모든 엔트리 로그

VLAN 확인 (Check VLAN):

VLAN 설정을 검사하려면, "VLAN 확인" 설정을 활성화 해야 합니다. "VLAN 확인" 기본 설정은 비활성화 됩니다. "VLAN 확인" 설정 비활성화 시, ARP 검사 로그 타입은 포트 설정을 참조할 것 입니다. "VLAN 확인" 설정이 활성화 되면, ARP 검사 로그 타입은 VLAN 설정을 참조할 것 입니다. 가능한 "VLAN 확인" 설정은 다음과 같습니다:

Enabled: VLAN 확인 동작을 활성화 합니다.

Disabled: VLAN 확인 동작을 비활성화 합니다.

로그 타입 (Log Type):

글로벌 모드 및 주어진 포트의 포트 모드가 활성화 되고, "VLAN 확인" 설정이 비활성화 되는 경우에만 ARP 검사 로그 타입이 포트 설정을 참조할 것 입니다. 개의 로그 타입이 있으며 가능한 타입은 다음과 같습니다:

None: 로그 없음

Deny: 엔트리가 거부된 로그

Permit: 엔트리가 허용된 로그

ALL: 모든 엔트리 로그

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

동적에서 정적으로 변환 (Translate dynamic to static):

모든 동적 엔트리를 정적 엔트리로 변환하려면 클릭하세요.

## VLAN 설정

ARP 검사가 어느 VLAN에서 활성화 될지 지정합니다.

VLAN Mode Configuration

Home > Security > ARP Inspection > VLAN Configuration

Refresh First Entry Next Entry

Start from VLAN 1, 20 entries per page.

| Delete | VLAN ID | Log Type |
|--------|---------|----------|
|--------|---------|----------|

Add New Entry

Reset Apply

웹 인터페이스

웹 인터페이스에서 VLAN 모드를 설정하려면:

1. 보안, ARP 검사 및 VLAN 설정을 클릭합니다.
2. "새 엔트리 추가"를 클릭합니다.



3. VLAN ID, 로그 타입을 지정합니다.
4. 적용을 클릭합니다.
5. 첫 엔트리/다음 엔트리를 클릭해 엔트리를 변경합니다.

## ■ 항목 설명:

### VLAN 설정 탐색

각 페이지는 VLAN 테이블에서 9999 엔트리를 표시합니다. 초기값은 20이며 “페이지 당 엔트리” 입력 필드를 통해 선택됩니다. 처음 방문 시, 웹 페이지는 VLAN 테이블의 처음부터 첫 20개 엔트리를 표시합니다. 표시된 것은 VLAN 테이블에서 발견된 가장 낮은 VLAN ID 중 하나입니다.

“VLAN” 입력 필드에서 유저는 VLAN 테이블에서 시작 포인트를 선택할 수 있습니다. “새로 고침” 버튼을 클릭해 VLAN 테이블과 일치하는 것부터 또는 가장 가까운 것 부터 표시된 테이블을 업데이트합니다. 또한 2개의 입력 필드 – “새로 고침” 버튼 클릭 시 – 는 처음 표시된 엔트리 값을 추정하므로, 동일한 시작 주소와 함께 지속적으로 새로 고침 합니다. “다음 페이지”는 다음 탐색을 기준으로 현재 표시된 테이블의 마지막 엔트리를 사용합니다. 마지막에 도달하면 표시된 테이블에 경고 메시지가 나타납니다. “첫 번째 엔트리” 버튼을 사용해 다시 시작합니다.

VLAN 모드 설정 (VLAN Mode Configuration):

ARP 검사가 활성화될 VLAN을 지정합니다. 먼저, 포트 모드 설정 웹 페이지의 포터 설정을 활성화 해야 합니다. 글로벌 모드 및 주어진 포트 모드가 활성화 되면, ARP 검사는 이 주어진 포트에 활성화 됩니다. 그 다음 VLAN 모드 설정 페이지 상에서 검사될 VLAN을 지정할 수 있습니다. 로그 타입은 또한 VLAN 설정 별로 구성 가능합니다.

가능한 타입은 다음과 같습니다:

None: 로그 없음

Deny: 엔트리가 거부된 로그

Permit: 엔트리가 허용된 로그

ALL: 모든 엔트리 로그

## ■ 버튼

새 엔트리 추가 (Add New Entry):

새로운 VLAN을 ARP 검사 VLAN 테이블에 추가하려면 클릭합니다.

삭제 (Delete):

엔트리를 삭제하려면 체크합니다. 다음 저장 동안 삭제됩니다.

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

첫 엔트리 (First Entry):

IPMC 프로파일 주소 설정에서 첫 엔트리로부터 시작하는 테이블을 업데이트 합니다.

다음 엔트리 (Next Entry):

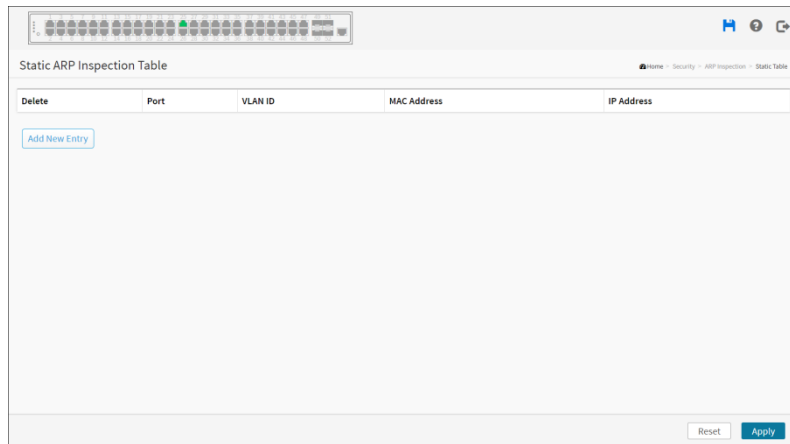
현재 표시된 마지막 엔트리 이후 엔트리와 시작하는 테이블을 업데이트 합니다.

새로 고침 (Refresh):

클릭해 페이지를 즉시 새로 고침합니다.

## 정적 테이블

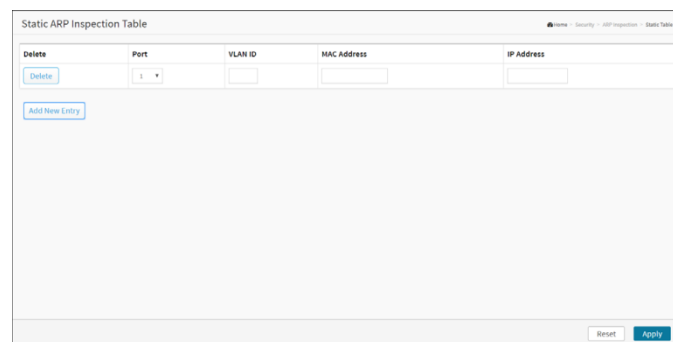
이 섹션에서 스위치의 정적 ARP 검사 테이블 항목 설정을 설명합니다. ARP 엔트리를 관리하도록 설정하려면 정적 ARP 검사 테이블을 사용합니다.



### 웹 인터페이스

웹 인터페이스에서 정적 ARP 검사 테이블 설정을 구성하려면:

1. 보안, ARP 검사 및 정적 테이블을 클릭합니다.
2. “새 엔트리 추가”를 클릭합니다.



3. 엔트리의 포트, VLAN ID, IP 주소, MAC 주소 및 IP 주소를 지정합니다.
4. 적용을 클릭합니다.

### ■ 항목 설명:

포트 (Port):

설정에 대한 논리적 포트입니다.

VLAN ID:

설정의 vlan id 입니다.

MAC 주소 (MAC address):

ARP 요청 패킷에 허용된 소스 MAC 주소입니다.

IP 주소 (IP Address):

ARP 요청 패킷에 허용된 소스 IP 주소입니다.

## ■ 버튼

새 엔트리 추가 (Add New Entry):

정적 ARP 검사 테이블에 새 엔트리를 클릭합니다.

삭제 (Delete):

엔트리를 삭제하려면 확인합니다. 다음 저장 동안 삭제될 것 입니다.

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## 동적 테이블

동적 ARP 검사 테이블의 엔트리가 이 페이지 상에 보여 줍니다. 동적 ARP 검사 테이블은 최대 256 엔트를 포함하며 포트, VLAN ID, MAC 주소 및 IP 주소 순으로 정렬됩니다. 모든 동적 엔트리는 DHCP 스누핑에서 전송됩니다.

### **ARP 검사 테이블 탐색**

각 페이지는 동적 ARP 검사 테이블에서 9999 엔트리를 표시합니다. 초기값은 20이며 “페이지 당 엔트리” 입력 필드를 통해 선택됩니다. 처음 방문 시, 웹 페이지는 동적 ARP 검사 테이블의 처음부터 첫 20개 엔트리를 표시합니다.

“포트 주소부터 시작”, “VLAN”, “MAC 주소” 및 “IP 주소” 입력 필드에서 유저는 동적 ARP 검사 테이블에서 시작 포인트를 선택할 수 있습니다. “새로 고침” 버튼을 클릭해 동적 ARP 검사 테이블과 일치하는 것부터 또는 가장 가까운 것 부터 표시된 테이블을 업데이트합니다. 또한 2개의 입력 필드 – “새로 고침” 버튼 클릭 시 – 는 처음 표시된 엔트리 값을 추정하므로, 동일한 시작 주소와 함께 지속적으로 새로 고침 합니다.

“다음 페이지”는 다음 탐색을 기준으로 현재 표시된 테이블의 마지막 엔트리를 사용합니다. 마지막이 되면 “No more entries” 문구가 표시된 테이블에 나타납니다. 다시 시작하려면 “첫 페이지” 버튼을 사용합니다.

## 웹 인터페이스

웹 인터페이스에서 동적 arp 검사 테이블 설정을 구성하려면:

1. 보안, ARP 검사 및 동적 테이블을 클릭합니다.
2. “자동 새로 고침”을 체크합니다.
3. “새로 고침”을 클릭해 상세 현황 포트를 새로 고칩니다.
4. 첫/다음 페이지를 클릭해 페이지를 변경합니다.
5. 페이지 당 포트, VLAN, MAC 주소, IP 주소 및 엔트리에서 시작을 지정합니다.

## ■ 항목 설명:

### ARP 검사 테이블 항목

포트 (Port):

엔트리가 표시되는 스위치 포트 번호입니다.

VLAN ID:

ARP 트래픽이 허용된 VLAN ID입니다.

MAC 주소 (MAC Address):

엔트리의 유저 MAC 주소입니다.

IP 주소 (IP Address):

엔트리의 유저 IP 주소입니다.

엔트리 표시 (Show entries):

표시하고 싶은 항목 수를 선택할 수 있습니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

첫 페이지 (First Page):

시스템 로그 엔트리를 업데이트 해 첫 페이지로 이동합니다.

다음 페이지 (Next Page):

그룹 정보 엔트리를 업데이트 해 다음 페이지로 이동합니다.

## 포트 보안

### 설정

이 섹션에서 스위치의 포트 보안 설정을 구성하는 방법을 설명합니다. MAC 주소 제한 및 식별을 통해 인터페이스에 입력을 제한하도록 포트 보안 기능을 사용할 수 있습니다.

Port Security Configuration

System Configuration

Aging Enabled: ☒ On

Aging Period: 3600 seconds

Hold Time: 300 seconds

Port Configuration

| Port | Mode     | Limit | Violation Mode | Violation Limit | State    | Re-open | Sticky   | Clear |
|------|----------|-------|----------------|-----------------|----------|---------|----------|-------|
| *    | ↕        | 4     | ↕              | 4               |          |         | ↕        |       |
| 1    | Disabled | 4     | Protect        | 4               | Disabled | Re-open | Disabled | Clear |
| 2    | Disabled | 4     | Protect        | 4               | Disabled | Re-open | Disabled | Clear |
| 3    | Disabled | 4     | Protect        | 4               | Disabled | Re-open | Disabled | Clear |

Reset Apply

#### 웹 인터페이스

웹 인터페이스에서 포트 보안 기능을 설정하려면:

1. 보안, 포트 보안 및 설정을 클릭합니다.
2. 특정 에이징 시간에 에이징 활성화를 클릭합니다.
3. 모드(Enabled, Disabled), 제한, 위반 모드, 각 포트의 침입 제한 모드를 설정합니다.
4. 적용을 클릭해 설정을 저장합니다.
5. 설정을 취소하려면 리셋 버튼을 클릭합니다. 이전에 저장된 값으로 되돌아 갑니다.

#### ■ 항목 설명:

##### 시스템 설정

에이징 활성화 (Aging Enabled):

확인하면, 보안 MAC 주소는 아래의 에이징 시간대로 에이징 대상이 됩니다.

에이징 시간 (Aging Period):

에이징 활성화에 체크되면, 에이징 시간은 이 입력과 제어됩니다. 다른 모듈이 보안 MAC 주소에 대해 잠재적인 기능을 사용한다면, 에이징 시간에 다른 요청이 있을 수 있습니다. 잠재적인 기능은 에이징 활성화가 있는 모든 모듈의 요청된 에이징 시간을 사용합니다.

에이징 시간은 3600초의 기본값과 함께 10에서 10000000초 사이의 수를 설정할 수 있습니다.

에이징이 필요한 이유를 이해하려면, 다음 시나리오를 참조하십시오:

최종 호스트가 포트 보안이 활성화 된 스위치의 포트에 차례로 연결되는 외부 스위치 또는 허브라고 가정합니다. 최종 호스트는 제한이 초과되지 않는 경우 전송을 허용합니다. 이제 최종 호스트는 로그 오프하거나 전원이 꺼진다고 가정해 봅시다. 에이징이 아니라면 최종 호스트는 리소스가 계속해서 스위치를 차지할 것 입이며 전송이 가능할 것 입니다. 이 상황을 해결하려면, 에이징을 활성화 합니다. 타이머 시간이 종료되면 스위치는 최종 호스트에서 프레임을 찾기 시작하며, 프레임이 다음 에이징 시간 내에 나타나지 않으면 최종 호스트는 연결 해제된 것으로 추정되고 해당 리소스는 스위치 상에서 해제됩니다.

보류 시간 (Hold Time):

제한 위반이 발견된 경우 보류 시간 - 초 단위 측정 - 은 MAC 주소가 MAC 테이블에 얼마나 오래 보류가 될지 정의합니다. 유효 범위는 300초 기본값의 10에서 10000000초입니다. MAC 테이블에서 MAC 주소 위반 보류에 대한 이유는 기본적으로 같은 MAC 주소가 지속적인 알림을 보내지 않도록 하는 것 입니다. (위반 수에 대한 알림 활성화 시)

### **포트 설정**

테이블은 선택된 스위치 상에 다음처럼 각 포트 당 하나의 열과 항목 수가 있습니다:

포트 (Port):

아래 설정이 적용되는 포트 번호입니다.

모드 (Mode):

제어 컨트롤이 이 포트 상에 활성화 되는지 여부를 제어합니다. 적용하려면 이 것과 글로벌 모드는 제한 컨트롤에 활성화 상태로 설정되어야 합니다. 다른 모듈이 주어진 포트의 제어 컨트롤 활성화 없이 잠재적인 포트 보안 기능을 계속해서 사용할 수 있음을 유의하십시오.

제한 (Limit):



이 포트 상에 보안 가능한 MAC 주소의 최대 수입니다. 이 수는 1024를 초과할 수 없습니다. 제한이 초과되면 해당 동작이 실행됩니다.

새로운 MAC 주소가 새 MAC 주소가 포트 보안 활성화 포트 상에 보일 때 마다 모든 포트가 가져오는 MAC 주소의 총 합계와 함께 스위치는 "born" 입니다. 모든 포트를 같은 pool에서 온 것이므로, 남아있는 포트가 이미 모든 가능 MAC 주소를 갖는다면 설정된 최대 수가 보장되지 않을 수 있습니다.

위반 모드 (Violation Mode):

제한이 되면 스위치는 다음의 동작 중 하나를 실행합니다:

Protect: 포트 상에 제한 MAC 주소 이상을 허용하지 않지만 추가 동작을 실행하지 않습니다.

Restrict: 제한이 되면 포트의 차후 MAC 주소 수를 위반으로 세며 표시됩니다. 이러한 MAC 주소는 보류 시간 만료 시 MAC 테이블에서 제거됩니다. 위반 제한 MAC 주소는 주어진 시간에서만 위반으로 표시됩니다.

Shutdown: 제한이 되면 추가 MAC 주소는 포트의 셧다운을 초래합니다. 이 것은 모든 보안된 MAC 주소가 포트로부터 제거되었으며, 새 주소가 없음을 의미합니다. 포트를 다시 여는데 3가지 방법이 있습니다:

- 1) "설정→포트" 페이지의 "Configured" 항목에서, 먼저 포트를 비활성화 하고 원래의 모드를 복구합니다.
- 2) 포트에서 포트 보안 설정을 생성합니다.
- 3) 스위치를 켭니다.

위반 제한 (Violation Limit)

포트 상에 위반으로 표시될 수 있는 MAC 주소의 최대 수입니다. 이 번호는 1023를 초과할 수 없습니다. 기본값은 4입니다. 위반 모드가 Restrict일때만 사용할 수 있습니다.

상태 (State):

이 항목은 제한 컨트롤의 관점에서 보이는 대로 포트의 현재 상태를 표시합니다. 상태는 다음 4개의 값입니다:

Disabled: 제한 컨트롤은 전체적으로 비활성화 또는 포트 비활성화 중 하나입니다.

Ready: 제한이 아직 적용된 상태가 아닙니다. 모든 행동을 표시할 수 있습니다.

Limit Reached: 이 포트 상에 제한이 적용된 것을 표시합니다. 이 상태는 동작이 none 또는 Trap 일 때 보여집니다.

Shutdown: 제한 컨트롤 모듈에 의해 포트가 셧다운 되었음을 표시합니다. 이 상태는 동작이 Shutdown 또는 Trap & Shutdown 인 경우에만 표시 가능합니다.

## ■ 버튼

적용 (Apply):

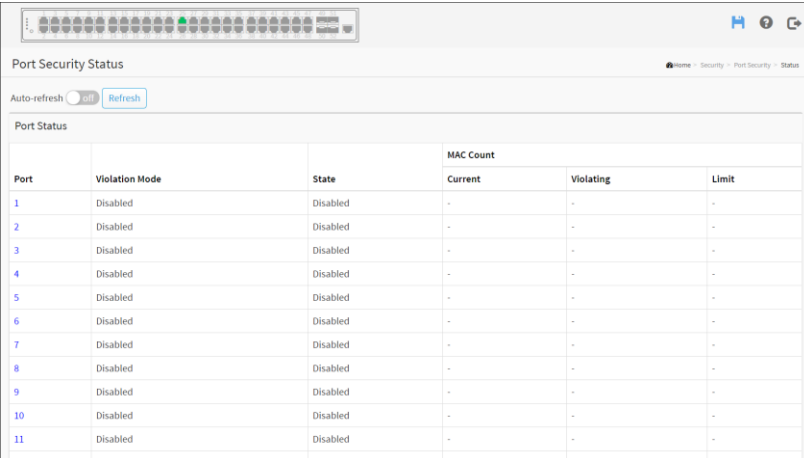
변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## 상태

이 섹션에서 포트 보안 상태를 표시합니다. 포트 보안은 직접 설정이 없는 모듈입니다. 설정은 다른 모듈 – 유저 모듈 에서 간접적으로 생깁니다. 유저 모듈이 포트 상의 활성화 된 포트 보안을 갖는 경우, 포트는 소프트웨어 기반 러닝에 대해 설정합니다. 이 모드에서, 알려지지 않는 MAC 주소의 프레임이 포트 보안 모듈에 통과되며, 모든 유저 모듈이 이 새 MAC 주소가 전송 또는 차단되는 것에 대해 허용 여부를 차례로 확인합니다. 전송 상태에서 설정된 MAC 주소의 경우, 모든 활성화 된 유저 모듈은 만장일치로 전송할 MAC 주소 허용에 대해 동의해야 합니다. 하나만 차단을 결정하면, 유저 모듈이 다르게 결정할 때까지 차단됩니다. 상태 페이지는 2개의 부분으로 나뉘어 집니다. 기존 유저 모듈 실제 포트 상태입니다.



| Port | Violation Mode | State    | MAC Count |           |       |
|------|----------------|----------|-----------|-----------|-------|
|      |                |          | Current   | Violating | Limit |
| 1    | Disabled       | Disabled | -         | -         | -     |
| 2    | Disabled       | Disabled | -         | -         | -     |
| 3    | Disabled       | Disabled | -         | -         | -     |
| 4    | Disabled       | Disabled | -         | -         | -     |
| 5    | Disabled       | Disabled | -         | -         | -     |
| 6    | Disabled       | Disabled | -         | -         | -     |
| 7    | Disabled       | Disabled | -         | -         | -     |
| 8    | Disabled       | Disabled | -         | -         | -     |
| 9    | Disabled       | Disabled | -         | -         | -     |
| 10   | Disabled       | Disabled | -         | -         | -     |
| 11   | Disabled       | Disabled | -         | -         | -     |

## 웹 인터페이스

웹 인터페이스에서 포트 보안 상태를 표시하려면:

1. 보안, 포트 보안 및 상태를 클릭합니다.
2. “자동 새로고침”을 확인합니다.

3. "새로 고침"을 클릭해 포트 상세 현황을 새로 고칩니다.
4. 포트 번호를 클릭해 이 특정 포트에 대한 상태를 표시합니다.

### ■ 항목 설명:

포트(Port):

상태를 적용할 포트 번호입니다. 포트 번호를 클릭해 이 특정 포트에 대한 상태를 확인합니다.

위반 모드 (Violation Mode)

포트의 설정 위반 모드를 표시합니다. 4개의 값 중 하나를 실행합니다:

Disabled: 포트 보안이 이 포트 상에서 관리상 활성화 되지 않습니다.

Protect: 보호 모드에서 포트 상에서 관리상 활성화 됩니다.

Restrict: 제한 모드에서 포트 상에서 관리상 활성화 됩니다.

Shutdown: 셧다운 모드에서 포트 상에서 관리상 활성화 됩니다.

상태 (State):

포트의 현재 상태를 표시합니다. 4개의 값 중 하나를 실행합니다:

Disabled: 유저 모듈이 현재 포트 보안 서비스를 사용하고 있지 않습니다.

Ready: 포트 보안 서비스가 최소한 하나의 유저 모듈로 사용되고 있으며, 알려지지 않은 MAC 주소에서 수신할 프레임을 위해 대기 중입니다.

Limit Reached: 포트 보안 서비스는 최소 제한 컨트롤 유저 모듈에 의해 활성화 되며, 모듈은 제한이 적용되고 MAC 주소가 더 이상 실행되지 않는다는 것을 표시합니다.

Shutdown: 포트 보안 서비스는 최소 제한 컨트롤 유저 모듈에 의해 활성화 되며, 모듈이 제한이 초과되지 않는 것을 표시합니다. 제한 컨트롤 설정 웹 페이지 상에 관리상 재오픈될 때 까지 포트 상에 표시되는 MAC 주소는 없습니다.

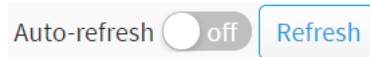
MAC Count (Current, Violating, Limit)

3개의 항목은 현재 알려진 (전송 및 차단된) MAC 주소의 수, 위반 MAC 주소(제한 모드에서만 카운트) 및 포트에 표시 가능한 MAC 주소 최대 수를 각각 표시합니다.

포트 상에서 활성화 되는 모듈이 없으면, 현재 항목은 대시(-)로 표시됩니다.

포트 보안이 관리상 포트 상에서 활성화 되면, 위반 및 제한 항목은 대시 (-)로 표시됩니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

포트 1-52 상태 (Port 1-52 Status):

포트 번호를 클릭해 포트 상태를 개별적으로 표시합니다.



## ■ 항목 설명:

MAC Address & VLAN ID:

이 포트 상에 표시되는 MAC 주소 및 VLAN ID입니다. 알려진 MAC 주소가 없다면 "No MAC addresses attached" 글자가 나타납니다.

상태 (State):

해당 MAC 주소의 차단 또는 전송 여부를 표시합니다. 차단된 상태에서, 트래픽 전송 또는 수신 이 허용되지 않습니다.

추가 시간 (Time of Addition):

이 MAC 주소가 포트에 처음 표시되었을 때 날짜 및 시간을 표시합니다.

에이지/보류 (Age/Hold):

최소한 한 명의 유저 모듈이 이 MAC 주소 차단을 결정하면, 보유 시간(초 단위 측정)이 만료될 때 까지 차단된 상태에서 유지됩니다. 모든 유저 모듈이 MAC 주소가 전송되도록 결정하면 에이징이 활성화 되어, 포트 보안 모듈은 MAC 주소가 계속 트래픽을 전송하는지 주기적으로 확인합니다. 에이징 시간 (초 단위 측정)이 만료되고 나타나는 프레임이 없으면, MAC 주소는 MAC 테이블에서 제거될 것 입니다. 그렇지 않으면 새 에이징 기간이 시작됩니다.

에이징이 비활성화 되거나 유저 모듈이 MAC 주소를 무기한으로 보류할 것을 결정하면, 대시 (-) 가 나타날 것 입니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

삭제 (Clear):

MAC 테이블에서 특정 MAC 주소를 제거하려면 클릭하세요.

포트 1 (Port 1):

포트 보안 상태에 표시하고자 하는 포트를 선택합니다.

뒤로 가기 (Back):

포트 보안 상태로 돌아 가려면 클릭합니다.

# RADIUS

## 설정

RADIUS Server Configuration

Global Configuration

Timeout: 5 seconds

Retransmit: 3 times

Deadtime: 0 minutes

Key:

NAS-IP-Address:

NAS-IPv6-Address:

NAS-Identifier:

Server Configuration

| Delete  | Hostname | Auth Port | Acct Port | Timeout | Retransmit | Key |
|---|----------|-----------|-----------|---------|------------|-----|
| <input type="button" value="Add New Server"/> |          |           |           |         |            |     |

Reset Apply

### 웹 인터페이스

웹 인터페이스에서 RADIUS를 설정하려면:

1. 보안, RADIUS 및 설정을 클릭합니다.
2. 타임아웃, 재전송, 불감 시간, 키, NAS-IP-주소, NAS IPv6-주소, NAS-식별자를 설정합니다.
3. "새 엔트리 추가"를 클릭합니다.

Global Configuration

Timeout: 5 seconds

Retransmit: 3 times

Deadtime: 0 minutes

Key:

NAS-IP-Address:

NAS-IPv6-Address:

NAS-Identifier:

Server Configuration

| Delete                                | Hostname             | Auth Port | Acct Port | Timeout              | Retransmit           | Key                  |
|---------------------------------------|----------------------|-----------|-----------|----------------------|----------------------|----------------------|
| <input type="button" value="Delete"/> | <input type="text"/> | 1812      | 1813      | <input type="text"/> | <input type="text"/> | <input type="text"/> |

Add New Server

Reset Apply

4. 호스트 이름, 인증 포트, Acct 포트, 타임아웃, 재전송 키를 설정합니다.
5. 적용을 클릭해 설정을 저장하세요.

6. 설정을 취소하려면 리셋 버튼을 클릭해야 합니다. 이전에 저장된 값으로 되돌아 갑니다.

## ■ 항목 설명:

### 글로벌 설정

이러한 설정은 모든 RADIUS 서버에 공통입니다.

타임아웃 (Timeout):

타임아웃은 요청을 재전송 하기 전 RADIUS 서버에서 응답을 기다리기 위한 1에서 1000 범위의 초 단위 시간입니다.

재전송 (Retransmit):

재전송은 1에서 1000 범위의 초 단위 시간입니다. RADIUS 요청은 응답하지 않는 서버에 재전송 됩니다. 서버가 마지막 재전송 후 응답하지 않으면, 작동하지 않는 것으로 간주합니다.

불감 시간 (Deadtime):

0에서 1440 분 사이 값으로 설정 가능한 불감 시간은 스위치가 이전 요청에 대한 응답을 실패한 서버에 새 요청을 전송하지 않는 동안의 시간입니다. 이 것은 이미 동작하지 않는 것으로 지정된 서버에 액세스하려는 지속적인 시도에서 스위치를 중지합니다. 불감 시간을 0보다 큰 값으로 설정하는 것은 이 기능을 활성화 하지만, 하나 이상의 서버에서만 설정됩니다.

키 (Key):

RADIUS 서버 및 스위치 간 공유된 보안 키 - 최대 63자 - 입니다.

NAS-IP-주소 (NAS-IP-Address):

RADIUS Access-Request 패킷의 특성 4로써 사용되는 IPv4 주소입니다. 이 필드가 공백으로 남겨져 있으면, 송신 인터페이스의 IP 주소가 사용됩니다.

NAS-IPv6-주소 (NAS-IPv6-Address):

RADIUS Access-Request 패킷의 특성 95로써 사용되는 IPv6 주소입니다. 이 필드가 공백으로 남겨져 있으면, 송신 인터페이스의 IP 주소가 사용됩니다.

NAS-식별자 (NAS-Identifier):

RADIUS Access-Request 패킷의 특성 32로써 사용되는 식별자 - 최대 255자 - 입니다. 이 필드가 공백으로 남겨져 있으면, NAS-식별자가 패킷에 포함되지 않습니다.

## 서버 설정

테이블에는 다음과 같이 각 RADIUS 서버에 하나의 열과 여러 항목이 있습니다:

호스트 이름 (Hostname):

RADIUS 서버의 IP 주소 또는 호스트이름입니다.

인증 포트 (Auth Port):

인증을 위해 RADIUS 서버에서 사용하는 UDP 포트입니다.

Acct 포트 (Acct Port):

계정을 위해 RADIUS 서버에서 사용하는 UDP 포트입니다.

타임아웃 (Timeout):

이 선택적 설정은 전체 전송 값을 중복합니다. 공백 상태는 전체 전송 값을 사용할 것 입니다.

키 (Key):

이 선택적 설정은 전체 키를 중복합니다. 공백 상태는 전체 키를 사용할 것 입니다.

## ■ 버튼

삭제(Delete):

RADIUS 서버 엔트리를 삭제하려면 이 박스를 체크합니다. 엔트리는 다음 저장 동안 삭제될 것입니다.

새 엔트리 추가 (Add New Entry):

새 RADIUS 서버 엔트리를 추가하려면 클릭합니다. 빈 열은 테이블에 추가되고 RADIUS 서버는 필요한대로 설정 가능합니다. 최대 5 서버가 지원됩니다. 버튼은 새 서버의 추가를 취소하는데 사용할 수 있습니다.

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

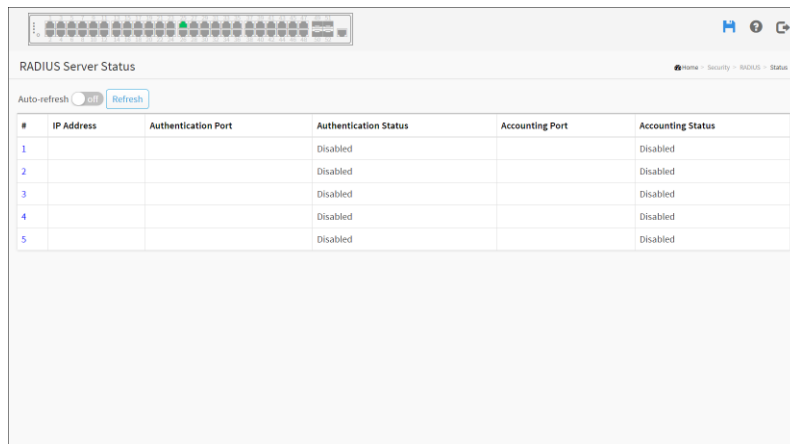
리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.



## 상태

이 섹션에서 RADIUS 인증 개요/상세를 표시하며 계정 서버 상태는 기능이 동작하도록 합니다.



| # | IP Address | Authentication Port | Authentication Status | Accounting Port | Accounting Status |
|---|------------|---------------------|-----------------------|-----------------|-------------------|
| 1 |            |                     | Disabled              |                 | Disabled          |
| 2 |            |                     | Disabled              |                 | Disabled          |
| 3 |            |                     | Disabled              |                 | Disabled          |
| 4 |            |                     | Disabled              |                 | Disabled          |
| 5 |            |                     | Disabled              |                 | Disabled          |

웹 인터페이스

웹 인터페이스에서 RADIUS 상태를 표시하려면:

1. 보안, RADIUS 및 상태를 클릭합니다.
2. 특정 RADIUS에 대한 상세 현황을 표시하기 위한 서버를 선택합니다.

### ■ 항목 설명:

#:

RADIUS 서버 번호입니다. 클릭해 이 서버에 대한 상세 현황에 탐색합니다.

IP 주소 (IP Address):

이 서버의 IP 주소와 UDP 포트 번호(in <IP Address>:<UDP Port> notation) 입니다.

인증 포트 (Authentication Port):

인증을 위한 UDP 포트 번호입니다.

인증 상태 (Authentication Status):

서버의 현재 상태입니다. 이 필드는 다음의 값 중 하나입니다:

Disabled: 서버가 비활성화 됩니다.

Not Ready: 서버가 활성화 되었으나 IP 통신이 아직 동작하지 않습니다.

Ready: 서버가 활성화 되며, IP 통신이 동작하고 RADIUS 모듈은 액세스 시도를 허용할 준비가 됩니다.

Dead (X 초 남음): 이 서버에 액세스 시도가 있으나 설정된 타임아웃 내에 응답하지 않습니다. 서버가 한시적으로 비활성화 되지만 불감 시간 종료 시 재 활성화 될 것 입니다. 이 동작 전에 남은 초 시간이 괄호에 표시됩니다. 이 상태는 하나 이상의 서버가 활성화 될 때만 가능합니다.

계정 포트 (Accounting Port):

계정에 대한 UDP 포트 번호입니다.

계정 상태 (Accounting Status):

서버의 현재 상태입니다. 이 필드는 다음 값 중 하나입니다:

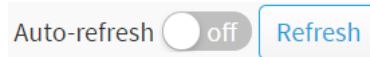
Disabled: 서버가 비활성화 상태입니다.

Not Ready: 서버가 활성화 되지만 IP 통신이 아직 동작하지 않습니다.

Ready: 서버가 활성화 되며, IP 통신이 동작하고 RADIUS 모듈은 액세스 시도를 허용할 준비가 됩니다.

Dead (X 초 남음): 이 서버에 액세스 시도가 있으나 설정된 타임아웃 내에 응답하지 않습니다. 서버가 한시적으로 비활성화 되지만 불감 시간 종료 시 재 활성화 될 것 입니다. 이 동작 전에 남은 초 시간이 괄호에 표시됩니다. 이 상태는 하나 이상의 서버가 활성화 될 때만 가능합니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

포트 1 ~ 52 상태

포트 번호를 클릭해 각각의 포트를 볼 수 있습니다.

RADIUS Authentication Statistics

Home
Security
RADIUS
Status

Auto-refresh
☐
Refresh
Clear
Server #1

RADIUS Authentication Statistics for Server #1

| Receive Packets            |   | Transmit Packets       |   |
|----------------------------|---|------------------------|---|
| Access Accepts             | 0 | Access Requests        | 0 |
| Access Rejects             | 0 | Access Retransmissions | 0 |
| Access Challenges          | 0 | Pending Requests       | 0 |
| Malformed Access Responses | 0 | Timeouts               | 0 |
| Bad Authenticators         | 0 |                        |   |
| Unknown Types              | 0 |                        |   |
| Packets Dropped            | 0 |                        |   |
| Other Info                 |   |                        |   |
| IP Address                 |   |                        |   |
| State                      |   | Disabled               |   |
| Round-Trip Time            |   | 0 ms                   |   |

RADIUS Accounting Statistics for Server #1

| Receive Packets     |   | Transmit Packets |   |
|---------------------|---|------------------|---|
| Responses           | 0 | Requests         | 0 |
| Malformed Responses | 0 | Retransmissions  | 0 |
| Bad Authenticators  | 0 | Pending Requests | 0 |
| Unknown Types       | 0 | Timeouts         | 0 |
| Packets Dropped     | 0 |                  |   |
| Other Info          |   |                  |   |
| IP Address          |   |                  |   |
| State               |   | Disabled         |   |
| Round-Trip Time     |   | 0 ms             |   |

## ■ 항목 설명:

서버 (Server):

RADIUS를 표시하고자 하는 서버를 선택할 수 있습니다.

서버 #1에 대한 RADIUS 인증 현황 (RADIUS Authentication Statistics for Server #1):

현황은 가까이 지정된 RFC4668 - RADIUS 인증 클라이언트 MIB를 나타냅니다.

서버 선택 박스를 이용해 백엔드 서버 사이를 전환해 상세 내용을 표시합니다.

액세스 허용 (Access Accepts):

서버에서 수신되는 RADIUS Access-Accept 패킷 (유효 또는 무효) 수입니다.

액세스 거부 (Access Rejects):

서버에서 수신되는 RADIUS Access-Reject 패킷 (유효 또는 무효) 수입니다.

액세스 시도 (Access Challenges):

서버에서 수신되는 RADIUS Access-Challenge 패킷 (유효 또는 무효) 수입니다.

손상된 액세스 응답 (Malformed Access Responses):

서버에서 수신되는 RADIUS Malformed Access Responses 패킷 (유효 또는 무효) 수입니다.

손상된 패킷은 무효 길이의 패킷을 포함합니다. 잘못된 인증자 또는 메시지 인증자 특성 또는 미확인 타입은 손상된 액세스 응답으로써 포함되지 않습니다.

잘못된 인증자 (Bad Authenticators):

서버의 무효 인증자 또는 메시지 인증자 특성을 포함한 RADIUS Access-Response 패킷의 수입니다.

미확인 타입 (Unknown Types):

인증 포트의 서버에서 미확인 타입과 함께 수신되고 삭제되는 RADIUS 패킷의 수입니다.

삭제된 패킷 (Packets Dropped):

인증 포트 상의 서버에서 수신되고 기타 이유로 삭제된 RADIUS 패킷의 수입니다.

액세스 요청 (Access Requests):

서버에 전송된 RADIUS Access-Request 패킷 수입니다. 이 것은 재전송을 포함하지 않습니다.

액세스 재전송 (Access Retransmissions):

RADIUS 인증 서버에 재전송된 RADIUS Access-Request 패킷 수입니다.

대기 요청 (Pending Requests):

아직 시간이 종료되지 않거나 응답을 수신하지 않은 대상 서버에 대한 RADIUS Access-Request 패킷의 수입입니다. 이 변수는 Access-Request가 전송될 때 증가되며, Access- Accept, Access-Reject, Access-Challenge, 타임아웃 또는 재전송 수신으로 인해 감소됩니다.

타임아웃 (Timeouts):

서버 인증 타임아웃 수입입니다. 타임아웃 후에 클라이언트는 동일한 서버에 재시도하며, 다른 서버로 전송되거나 중지합니다. 동일한 서버로의 재시도는 타임아웃과 마찬가지로 재전송으로 간주됩니다. 다른 서버로의 전송은 요청 및 타임아웃으로 간주됩니다.

IP 주소 (IP Address):

문제가 있는 인증 서버에 대한 IP 주소 및 UDP 포트입니다.

상태 (State):

서버의 상태를 표시합니다. 다음의 값 중 하나입니다:

- ◆ Disabled:  
선택된 서버는 비활성화 입니다.
- ◆ Not Ready:  
서버가 활성화 되지만, IP 통신은 아직 동작하지 않습니다.
- ◆ Ready:  
서버가 활성화되며, IP 통신이 동작하고 있습니다. 그리고 RADIUS 모듈은 액세스 시도 허용 준비가 되었습니다.
- ◆ Dead (X 초 남음):  
이 서버에 액세스 시도가 있었으나 설정된 타임아웃 내에서 응답하지 않습니다. 서버가 한시적으로 비활성화되지만 불감 시간이 종료되면 재활성화 될 것 입니다. 동작 전 남은 시간이 괄호 안에 표시됩니다. 이 상태는 하나 이상의 서버가 활성화 될 때만 가능합니다.

왕복 시간 (Round-Trip Time):

RADIUS 인증 서버에서 일치하는 가장 최근 액세스 응답/액세스 시도 및 액세스 요청 사이의 시간 단격 (1000분의 1초 단위)입니다. 이 측정 단위는 100ms입니다. 0ms 값은 서버와 아직 왕복 통신이 아닌 것을 나타냅니다.

서버 #1의 RADIUS 계정 현황 (RADIUS Accounting Statistics for Server #1)

RFC4670 - RADIUS Accounting Client MIB에 가까이 지정된 현황 상태입니다.

서버 선택 박스를 이용해 백엔드 서버 사이를 전환해 상세 내용을 표시합니다.

응답 (Responses):

서버로부터 수신된 RADIUS 패킷 (유효 또는 무효) 수입입니다.

잘못된 응답 (Malformed Responses):

서버로부터 수신된 잘못된 RADIUS 패킷 수입입니다. 잘못된 패킷은 무효 길이의 패킷을 포함합니다. 잘못된 인증자 또는 미확인 타입은 잘못된 액세스 응답으로써 포함됩니다.

잘못된 인증자 (Bad Authenticators):

서버로부터 수신된 무효한 인증자를 포함한 RADIUS 패킷 수입입니다.

미확인 타입 (Unknown Types):

계정 포트 상의 서버로부터 수신된 미확인 타입의 RADIUS 패킷 수입입니다.

삭제된 패킷 (Packets Dropped):

계정 포트 상의 서버로부터 수신되고 기타 이유로 삭제된 RADIUS 패킷 수입입니다.

요청 (Requests):

서버에 전송된 RADIUS 패킷 수입입니다. 이 것은 재전송을 포함하지 않습니다.

재전송 (Retransmissions):

RADIUS 계정 서버에 재전송된 RADIUS 패킷 수입입니다.

대기 요청 (Pending Requests):

시간 종료되지 않거나 응답을 수신하지 않은 서버 대상의 RADIUS 패킷 수입입니다. 이 변수는 요청이 전송될 때 증가하며, 요청, 타임아웃 또는 재전송 수신으로 인해 감소됩니다.

타임아웃 (Timeouts):

서버로 계정 타임아웃 수입입니다. 타임아웃 후 클라이언트는 동일한 서버로 재전송을 시도하며 다른 서버로 전송 또는 중지합니다.

동일한 서버로의 재시도는 재전송 및 타임아웃으로 간주됩니다. 다른 서버로의 전송은 요청 및 타임아웃으로 간주됩니다.

IP 주소 (IP Address):

문제가 있는 계정 서버에 대한 IP 주소 및 UDP 포트입니다.

상태 (State):

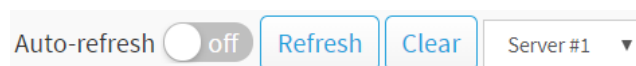
서버 상태를 표시합니다. 다음의 값 중 하나를 동작합니다:

- ◆ Disabled:  
선택된 서버는 비활성화 입니다.
- ◆ Not Ready:  
서버가 활성화 되지만, IP 통신은 아직 동작하지 않습니다.
- ◆ Ready:  
서버가 활성화되며, IP 통신이 동작하고 있습니다. 그리고 RADIUS 모듈은 계정 시도 허용 준비가 되었습니다.
- ◆ Dead (X 초 남음):  
이 서버에 계정 시도가 있었으나 설정된 타임아웃 내에서 응답하지 않습니다. 서버가 한시적으로 비활성화되지만 불감 시간이 종료되면 재활성화 될 것 입니다. 동작 전 남은 시간이 괄호 안에 표시됩니다. 이 상태는 하나 이상의 서버가 활성화 될 때만 가능합니다.

왕복 시간 (Round-Trip Time):

RADIUS 계정 서버에서 일치하는 가장 최근 액세스 응답 및 요청 사이의 시간 단격 (1000분의 1 초 단위)입니다. 이 측정 단위는 100ms입니다. 0ms 값은 서버와 아직 왕복 통신이 아닌 것을 나타냅니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고침 합니다. 자동 새로 고침은 3초 마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고침 합니다.

삭제 (Clear):

선택된 서버에 대한 카운터를 삭제합니다. "대기 요청" 카운터는 이 동작으로 삭제되지 않습니다.



## TACACS+

이 페이지에서 최대 TACACS+ 서버를 설정할 수 있습니다.

웹 인터페이스

웹 인터페이스에서 TACACS+ 서버를 설정하려면:

1. 보안과 TACACS+를 클릭합니다.
2. "새 엔트리 추가"를 클릭합니다.

3. 타임아웃, 불감시간, 키를 지정합니다.
4. 서버의 호스트이름, 포트, 타임아웃과 키를 지정합니다.
5. 적용을 클릭합니다.

### ■ 항목 설명:

#### 글로벌 설정

모든 TACACS+ 서버에 대해 공통적이 설정입니다.

타임아웃 (Timeout):

동작 불능으로 간주되기 전 타임아웃은 TACACS+ 서버 응답을 대기하는 1에서 1000 범위의 초 단위 시간입니다.

불감시간 (Deadtime):

0에서 1440분 사이의 숫자로 설정 가능하는 불감 시간은 스위치가 새 요청을 이전 요청에 대한 응답을 실패한 서버에 전송하지 않는 동안의 시간입니다. 이 것은 동작 불능으로 간주된 서버에 액세스할 지속적인 시도에서 스위치를 중지합니다. 불감시간 값이 0보다 더 큰 설정이 이 기능을 활성화 하지만, 하나 이상의 서버만 설정됩니다.

키 (Key):

TACACS+ 서버와 스위치 사이를 공유한 보안키 - 최대 63자 길이 - 입니다.

### **서버 설정**

테이블은 다음과 같이 각 TACACS+ 서버에 하나의 열과 항목을 갖습니다:

삭제 (Delete):

TACACS+ 서버 엔트리를 삭제하려면 이 박스를 체크하십시오. 엔트리는 다음 저장 동안 삭제될 것 입니다.

호스트이름 (Hostname):

TACACS+ 서버의 IP 주소 또는 호스트이름입니다.

포트 (Port):

인증을 위한 TACACS+ 서버 상에 사용하기 위한 TCP 포트입니다.

타임아웃 (Timeout):

이 선택 가능한 설정은 글로벌 타임아웃 값을 중복합니다. 공백으로 두면 글로벌 타임아웃 값을 사용합니다.

키 (Key):

이 선택 가능한 설정은 글로벌 키를 중복합니다. 공백으로 두면 글로벌 키를 사용합니다.

### **■버튼**

삭제 (Delete):

이 버튼은 새 서버 추가를 취소하는데 사용할 수 있습니다.

새 서버 추가 (Add New Server):

새로운 TACACS+ 서버를 추가하려면 클릭합니다. 빈 열이 테이블에 추가되며 TACACS+ 서버는 필요한대로 설정할 수 있습니다. 최대 5 서버가 지원됩니다.

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

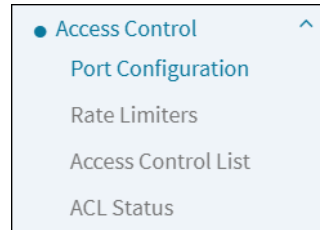
로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

이 페이지는 의도적으로 비워 두었습니다.

### 개요

---

메뉴는 다음과 같습니다:



## 포트 설정

각 스위치 포트의 ACL 항목 (ACE)을 설정합니다. 프레임이 특정 ACE와 일치하지 않는 이상 이 항목은 포트에 수신된 프레임에 영향을 미칩니다.

### 웹 인터페이스

웹 인터페이스 유저를 설정하려면:

1. 액세스 컨트롤 및 포트 설정을 클릭합니다.
2. 특정 항목 값을 스크롤해 포트 ACL 설정에 대한 올바른 값을 선택합니다.
3. 적용을 클릭해 설정을 저장합니다.
4. 설정을 취소하고자 하면 리셋 버튼을 클릭합니다. 이전 저장 값으로 되돌아 갑니다.
5. 설정을 완료하면 포트의 카운터를 볼 수 있습니다. 새로 고침을 클릭해 카운터를 업데이트 하거나 정보를 삭제할 수 있습니다.

### ■ 항목 설명:

포트 (Port):

동일한 열에 포함된 설정에 대한 논리적 포트입니다.

규정 ID (Polish ID):

이 포트에 적용할 규정을 선택합니다. 허용된 값은 1에서 8입니다. 기본 값은 1입니다.

**동작 (Action):**

전송 허용 ("Permit") 또는 거부("Deny")를 선택합니다. 기본값은 허용 ("Permit")입니다.

**속도 제한 장치 ID (Rate Limiter ID):**

이 포트에 적용할 속도 제한 장치를 선택합니다. 허용된 값은 Disabled 또는 1에서 16 사이의 값입니다. 기본 값은 "Disabled"입니다.

**포트 리디렉트 (Port Redirect):**

재전송할 포트 프레임을 선택합니다. 허용된 값은 Disabled 또는 특정 포트 번호이며, 동작이 허용되는 경우 설정할 수 없습니다. 기본값은 "Disabled"입니다.

**미러 (Mirror)**

이 포트의 미러 동작을 지정합니다. 허용된 값은 다음과 같습니다:

Enabled: 포트의 수신된 프레임이 미러링 됩니다.

Disabled: 포트의 수신된 프레임이 미러링 되지 않습니다.

**기록 (Logging):**

이 포트의 로깅 동작을 지정합니다. 허용된 값은 다음과 같습니다:

Enabled: 포트의 수신된 프레임은 시스템 로그에 저장됩니다.

Disabled: 포트의 수신된 프레임은 저장되지 않습니다.

기본값은 "Disabled"입니다. 시스템 로그 메모리 크기와 기록 속도는 제한되어 있음을 주의하십시오.

**셴다운 (Shutdown):**

이 포트의 포트 상태를 지정합니다. 허용된 값은 다음과 같습니다:

Enabled: ACL 유저 모듈의 불안한 포트 설정 변경으로 포트를 재오픈 합니다.

Disabled: ACL 유저 모듈의 불안한 포트 설정 변경으로 포트를 닫습니다.

기본값은 "Enabled"입니다.

카운터 (Counter):

이 ACE와 일치하는 프레임의 수를 셉니다.

## ■ 버튼

새로고침, 삭제 (Refresh, clear):

클릭하면 ACL 포트 설정을 새로 고침 하거나 수동으로 삭제할 수 있습니다.

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.



## 속도 제한 장치

이 섹션은 스위치의 ACL 속도 제한 장치 항목을 설정하는 방법을 설명합니다. 사용자가 속도 제한 장치 값과 pps 장치를 설정할 수 있는 속도 제한 장치 단계는 1에서 16입니다.

| Rate Limiter ID | Rate | Unit |
|-----------------|------|------|
| *               | 1    | pps  |
| 1               | 1    | pps  |
| 2               | 1    | pps  |
| 3               | 1    | pps  |
| 4               | 1    | pps  |
| 5               | 1    | pps  |
| 6               | 1    | pps  |
| 7               | 1    | pps  |
| 8               | 1    | pps  |
| 9               | 1    | pps  |
| 10              | 1    | pps  |

### 웹 인터페이스

웹 인터페이스에서 ACL 속도 제한 장치를 설정하려면:

1. 액세스 컨트롤 및 속도 제한 장치를 클릭합니다.
2. 속도 필드, 유닛을 지정합니다.
3. 적용을 클릭하고 설정을 저장합니다.
4. 설정을 취소하고자 하면 리셋 버튼을 클릭합니다. 이전 저장 값으로 되돌아 갑니다.

### ■ 항목 설명:

속도 제한 장치 ID (Rate Limiter ID):

같은 열에 포함된 설정에 대한 속도 제한 장치 ID이며 1에서 16 범위 사이의 값입니다.

속도 (Rate):

유효 속도는 pps의 0, 10, 20, 30, ..., 5000000입니다.

유닛 (Unit)

속도 유닛을 지정합니다. 허용된 값은 다음과 같습니다:

10pps: 초당 패킷입니다.

25kbps: 초당 Kbits입니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

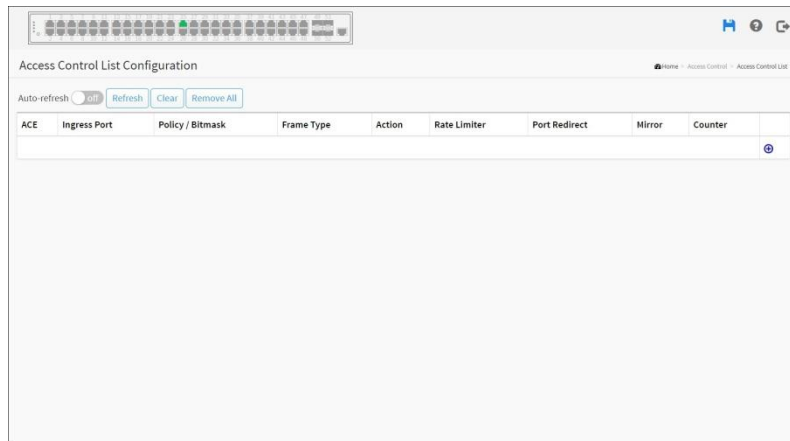
리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## 액세스 컨트롤 목록


이 페이지에서 이 스위치 상에 지정된 ACE로 이루어진 액세스 컨트롤 목록(ACL)을 표시합니다. 각 열은 정의된 ACE를 설명합니다. ACE의 최대 수는 스위치 당 512입니다.

가장 낮은 플러스 아이콘을 클릭해 새 ACE를 목록에 추가하십시오. 내부프로토콜에 사용되는 보류된 ACE는 편집 또는 삭제할 수 없습니다. 순서를 변경할 수 없으면 우선 순위가 있는 것이 가장 높습니다.



웹 인터페이스

웹 인터페이스에서 액세스 컨트롤 목록을 설명하려면:

1. 액세스 컨트롤과 액세스 컨트롤 목록을 클릭하세요.
2.  버튼을 클릭해 새로운 ACL을 추가하거나 다른 ACL 조정 버튼을 사용해 편집 동작을 지정합니다. (예: 편집, 삭제 또는 목록의 엔트리 관련 위치 이동)

3. ACE 항목을 지정합니다.
4. 저장을 클릭해 설정을 저장합니다.
5. 설정을 취소하려면 리셋 버튼을 클릭하십시오. 이전 저장 값으로 되돌아 갑니다.
6. ACE 설정 페이지의 엔트리를 편집하는 경우, 표시되는 항목은 프레임 타입 및 IP 프로토콜 타입과 같은 다양한 선택에 따라 달라집니다. 이 규칙과 일치하게 하려면 관련 기준을 지정해 규칙과 일치할 때 실행할 동작을 설정합니다. (예: 속도 제한 장치, 포트 복사, 기록 및 섯다운)

## ■ 항목 설명:

ACE:

ACE ID를 표시합니다.

내부포트 (Ingress Port):

ACE의 내부포트를 표시합니다. 가능한 값은 다음과 같습니다:

Any: ACE가 모든 내부포트와 일치합니다.

Policy: ACE가 특정 규정의 내부포트와 일치합니다.

Port: ACE가 특정 포트와 일치합니다.

규정 / 비트마스크 (Policy / Bitmask):

규정 번호 및 ACE의 비트마스크를 표시합니다.

프레임 타입 (Frame Type):

ACE의 프레임 타입을 표시합니다. 가능한 값은 다음과 같습니다:

Any: ACE가 모든 프레임 타입과 일치합니다.

EType: ACE는 이더넷 타입 프레임과 일치합니다. ACE 기반 이더넷 타입은 IP와 ARP 프레임에 의해 일치되지 않습니다.

ARP: ACE는 ARP/RARP 프레임과 일치합니다.

IPv4: ACE는 IPv4 프레임과 일치합니다.

IPv4/ICMP: ACE는 ICMP 프로토콜의 IPv4 프레임과 일치합니다.

IPv4/UDP: ACE는 UDP 프로토콜의 IPv4 프레임과 일치합니다.

IPv4/TCP: ACE는 TCP 프로토콜의 IPv4 프레임과 일치합니다.

IPv4/Other: ACE는 ICMP/UDP/TCP이 아닌 IPv4 프레임과 일치합니다.

IPv6: ACE는 IPv6 표준 프레임과 일치합니다.

동작 (Action):

ACE의 전송 동작을 표시합니다.

Permit: ACE와 일치하는 프레임이 전송 및 표시됩니다.

Deny: ACE와 일치하는 프레임이 삭제됩니다.

Filter: ACE와 일치하는 프레임이 필터링 됩니다.

속도 제한 장치 (Rate Limiter):

ACE 속도 제한 장치 수를 표시합니다. 허용 범위는 1에서 16입니다. Disabled가 표시되면, 속도 제한 장치 동작은 비활성화 됩니다.

포트 리디렉트 (Port Redirect):

ACE 포트 리디렉트 동작을 표시합니다. ACE와 일치하는 프레임이 포트 번호로 재전송됩니다. 허용된 값은 Disabled 또는 지정 포트 번호입니다. Disabled가 표시되면 포트 리디렉트 동작이 비활성화 됩니다.

미러 (Mirror):

이 포트의 미러링 동작을 지정합니다. ACE와 일치하는 프레임이 대상 미러 포트에 미러링 됩니다.

허용된 값은 다음과 같습니다:

Enabled: 포트 상에 수신된 프레임이 미러링 됩니다.

Disabled: 포트 상에 수신된 프레임이 미러링 되지 않습니다.

기본 값은 "Disabled"입니다.

카운터 (Counter):

카운터는 ACE가 프레임에 의해 영향을 받은 횟수를 표시합니다.

조정 버튼:

다음의 버튼을 사용해 테이블의 각 ACE (Access Control Entry)를 조정할 수 있습니다.

⊕ : 현재 열 전에 새로운 ACE를 삽입합니다.

Ⓜ : ACE 열을 편집합니다.

⬆ : ACE를 목록 위로 이동합니다.

⬇ : ACE를 목록 아래로 이동합니다.

⊗ : ACE를 삭제합니다.

⊕ : 가장 낮은 플러스 기호는 ACE 목록 가장 아래에 새 엔트리를 추가합니다.

### ACE 설정

ACE는 다양한 항목을 포함합니다. 이 항목은 선택하는 프레임 타입에 따라 다릅니다. 먼저 ACE의 내부포트를 선택한 후 프레임 타입을 선택합니다. 다른 항목 옵션은 선택된 프레임 타입에 따라 다릅니다.

이 ACE에 영향을 주는 프레임은 이 곳에 지정된 설정에 일치합니다.

내부포트 (Ingress Port):

이 ACE를 적용할 내부포트를 선택합니다.

All: ACE를 모든 포트에 적용합니다.

Port n: ACE는 이 포트 번호에 적용됩니다. n은 스위치 포트 번호입니다.

규정 필터 (Policy Filter):

ACE의 규정 번호 필터를 지정합니다.

**Any:** 아무런 규정 필터가 지정되어 있지 않습니다. (규정 필터 상태는 “관계 없음”입니다.)

**Specific:** ACE의 특정 규정을 필터링 하려면 이 값을 선택하세요. 규정값과 비트마스크를 입력할 수 있는 2개의 필드가 나타납니다.

규정 값 (Policy Value):

규정 필터에 “Specific”이 선택되면 특정 규정 값을 입력할 수 있습니다. 허용 범위는 0에서 255입니다.

규정 비트마스크 (Policy Bitmask):

규정 필터에 “Specific”이 선택되면 특정 규정 비트마스크를 입력할 수 있습니다. 허용 범위는 0x0에서 0xff입니다. 비트마스크 사용에서 이진법 값이 0인 경우, 이 비트는 “관계 없음”을 뜻합니다.

실제 일치하는 패턴은 [policy\_value & policy\_bitmask]입니다. 예를 들어, 규정 값이 3이고 규정 비트마스크가 is 0x10 (비트 0은 “관계 없음” 비트)이면 규정 2와 3이 이 규칙에 적용됩니다.

프레임 타입 (Frame Type):

이 ACE에 대한 프레임 타입을 선택합니다. 이 프레임 타입은 상호 전용입니다.

Any: 모든 프레임이 이 ACE와 일치할 수 있습니다.

Ethernet Type: 이더넷 타입 프레임만 이 ACE와 일치합니다. IEEE 802.3는 1536 십진수보다 크거나 동일하도록 (0600 16진법과 동일) 길이/타입 필드 규격 값을 설명합니다.

ARP: ARP 프레임만 ACE와 일치합니다. ARP 프레임이 이더넷 타입의 ACE와 일치하지 않음을 유의하십시오.

IPv4: IPv4 프레임만 ACE와 일치합니다. IPv4 프레임이 이더넷 타입의 ACE와 일치하지 않음을 유의하십시오.

IPv6: IPv6 프레임만 ACE와 일치합니다. IPv6 프레임이 이더넷 타입의 ACE와 일치하지 않음을 유의하십시오.

동작 (Action):

ACE에 영향을 미치는 프레임과 동작할 동작을 지정합니다.

Permit: ACE 동작에 대해 ACE에 영향을 미치는 프레임을 승인합니다.

Deny: ACE에 영향을 미치는 프레임을 삭제합니다.

Filter: ACE에 일치하는 프레임을 필터링 합니다.

속도 제한 장치 (Rate Limiter):

기본 유닛 수의 속도 제한 장치를 지정합니다. 허용 범위는 1에서 16입니다. Disabled가 표시되면 속도 제한 장치 동작이 비활성화 상태가 됩니다.

포트 리디렉트 (Port Redirect):

ACE에 영향을 미치는 프레임은 이 곳에 지정된 포트 번호에 재전송됩니다. 속도 제한 장치가 이 포트에 영향을 미칩니다. 허용 범위는 스위치 포트 번호 범위와 동일합니다. Disabled가 표시되면 포트 리디렉트 동작이 비활성화 상태가 되며, 동작 허용 시 특정 '포트 리디렉트' 포트 번호는 설정 불가능합니다.

미러(Mirror):

이 포트의 미러 동작을 지정합니다. ACE에 일치하는 프레임은 대상 미러 포트에 미러링합니다. 속도 제한 장치는 미러 포트 상의 프레임에 영향을 주지 않습니다. 허용 범위는 다음과 같습니다:

Enabled: 포트 상에 수신된 프레임이 미러링 됩니다.

Disabled: 포트 상에 수신된 프레임이 미러링 되지 않습니다.

기본 값은 "Disabled"입니다.

**기록 (Logging):**

ACE 기록 동작을 지정합니다. 기록 메시지는 4바이트 CRC 정보를 포함하지 않음을 주의하십시오.

허용 값은 다음과 같습니다:

Enabled: ACE와 일치하는 프레임이 시스템 로그에 저장됩니다.

Disabled: ACE와 일치하는 프레임이 기록되지 않습니다.

주의: 기록 기능은 패킷 길이가 1518(VLAN 태그없이) 이하일 때만 동작하며 시스템 로그 메모리 크기와 기록 속도가 제한됩니다.

**셧다운 (Shutdown):**

ACE 동작 포트 셧다운을 지정합니다. 허용 값은 다음과 같습니다.

Enabled: 프레임이 ACE에 일치하면 내부포트가 비활성화 됩니다.

Disabled: 포트 셧다운이 ACE에 비활성화 됩니다.

주의: 셧다운 기능은 패킷 길이가 1518(VLAN 태그없이) 이하일 때만 동작합니다.

**카운터 (Counter):**

카운터는 ACE가 프레임에 의해 영향을 받는 횟수를 표시합니다.

**MAC 항목****SMAC 필터 (SMAC Filter):**

(프레임 타입이 이더넷 타입 또는 ARP일 대만 표시됩니다.)

이 ACE에 대한 소스 MAC 필터를 지정합니다.

Any: 지정된 SMAC 필터가 없습니다. (SMAC 필터 상태가 "관계 없음"입니다.)

Specific: ACE와 특정 소스 MAC 주소를 필터링 하려면, 이 값을 선택합니다. SMAC 값 입력을 위한 필드가 나타납니다.

**SMAC 값 (SMAC Value):**

"Specific"이 SMAC 필터를 위해 선택되면, 특정 소스 MAC 주소를 입력할 수 있습니다. 유효한 형식은 is "xx-xx-xx-xx-xx-xx" 또는 "xx.xx.xx.xx.xx.xx" 또는 "xxxxxxxxxxxx" (x는 16진 수입니다)입니다.

이 ACE에 영향을 주는 프레임은 SMAC 값에 일치합니다.

**DMAC 필터 (DMAC Filter):**

이 ACE를 위한 대상 MAC 필터를 지정합니다.

Any: 지정된 DMAC 필터가 없습니다. (DMAC 필터 상태가 "관계 없음"입니다.)



MC: 프레임이 멀티캐스트이어야 합니다.

BC: 프레임이 브로드캐스트이어야 합니다.

UC: 프레임이 유니캐스트를이어야 합니다.

Specific: 특정 대상 MAC 주소를 이 ACE와 필터링 하고자 하는 경이 이 값을 선택합니다. DMAC 값을 위한 필드가 나타납니다.

DMAC 값 (DMAC Value):

DMAC 필터를 위해 "Specific"을 선택하면, 특정 대상 MAC 주소를 선택할 수 있습니다. 유효한 형식은 is "xx-xx-xx-xx-xx-xx" 또는 "xx.xx.xx.xx.xx.xx" 또는 "xxxxxxxxxxxx" (x는 16진 수입니다)입니다. 이 ACE에 영향을 주는 프레임은 DMAC 값에 일치합니다.

### VLAN 항목

802.1Q 태그 지정 (802.1Q Tagged):

프레임이 802.1Q 태그 지정에 따른 동작 실행 가능성 여부를 지정합니다. 허용된 값은 다음과 같습니다:

Any: 모든 값이 허용됩니다. ("관계 없음")

Enabled: 태그된 프레임만 허용됩니다.

Enabled: 태그 되지 않은 프레임만 허용됩니다.

기본 값은 "Any"입니다.

VLAN ID 필터 (VLAN ID Filter):

이 ACE에 대한 VLAN ID 필터를 지정합니다.

Any: 지정된 VLAN ID 가 없습니다. (VLAN ID 필터 상태가 "관계 없음")입니다.

Specific: 특정 VLAN ID를 이 ACE와 필터링 하려면 이 값을 선택합니다. VLAN ID 번호 입력을 위한 필드가 나타납니다.

VLAN ID:

"Specific"이 VLAN ID 필터를 위해 선택하면, 특정 VLAN ID 번호를 입력할 수 있습니다. 허용 범위는 1에서 4095입니다. 이 ACE를 실행할 프레임은 이 VLAN ID 값과 일치합니다.

태그 우선권 (Tag Priority):

이 ACE에 대한 태그 우선권을 지정합니다. 이 ACE를 실행할 프레임이 이 태그 우선권과 일치합니다. 허용 범위는 0에서 7 또는 0-1, 2-3, 4-5, 6-7, 0-3 및 4-7입니다. 'Any' 값은 태그 우선 순위가 지정되지 않음을 뜻합니다. (태그 우선권은 "관계 없음"입니다.)

## ARP 항목

ARP 항목은 프레임이 타입 "ARP"가 선택되었을 때 설정할 수 있습니다.

### ARP/RARP:

ACE를 위해 가능한 ARP/RARP 연산 코드 (OP) 플래그를 지정할 수 있습니다.

Any: 지정된 ARP/RARP OP 플래그가 없습니다. (OP는 "관계 없음"입니다)

ARP: 프레임이 ARP에 ARP 연산 코드로 설정되어야 합니다.

RARP: 프레임이 RARP에 RARP 연산 코드로 설정되어야 합니다.

Other: 프레임이 미확인 ARP/RARP 연산코드 플래그를 갖습니다.

### 요청/응답 (Request/Reply):

이 ACE에 대한 요청/응답 연산코드(OP)플래그를 지정합니다.

Any: 지정된 요청/응답 OP 플래그가 없습니다. (OP는 "관계 없음"입니다)

Request: 프레임은 ARP 요청 또는 RARP 요청 OP 플래그 설정을 갖습니다.

Reply: 프레임은 ARP 응답 또는 RARP 응답 OP 플래그 설정을 갖습니다.

### 발송자 IP 필터 (Sender IP Filter):

이 ACE에 대한 발송자 IP 필터를 지정합니다.

Any: 지정된 발송자 IP 필터가 없습니다. (발송자 IP 필터는 "관계 없음"입니다.)

Host: 지정된 발송자 IP 필터가 Host로 지정됩니다. 나타나는 SIP 주소 필드의 발송자 IP 필터를 지정합니다.

Network: 지정된 발송자 IP 필터가 Network로 지정됩니다. 나타나는 SIP 주소 필드의 발송자 IP 마스크를 지정합니다.

### 발송자 IP 주소 (Sender IP Address):

발송자 IP 필터에 "Host" 또는 "Network"가 선택되면, 점 소수 표기법에서 특정 발송자 IP 주소를 입력할 수 있습니다.

### 발송자 IP 마스크 (Sender IP Mask):

발송자 IP 필터에 "Network"가 선택되면, 점 소수 표기법에서 특정 발송자 IP 마스크를 입력할 수 있습니다.

### 타겟 IP 필터 (Target IP Filter):

이 특정 ACE에 대한 타겟 IP 필터를 지정합니다.

Any: 지정된 타겟 IP 필터가 없습니다. (타겟 IP 필터는 "관계 없음"입니다.)

Host: 타겟 IP 필터가 Host로 설정됩니다. 나타나는 타겟 IP 주소 필드에서 타겟 IP 주소를 지정합니다.

Network: 타겟 IP 필터가 Network로 지정됩니다. 나타나는 타겟 IP 주소 및 타겟 IP 마스크 필드의 타겟 IP 주소 및 타겟 IP 마스크를 지정합니다.

타겟 IP 주소 (Target IP Address):

타겟 IP 필터에 "Host" 또는 "Network"가 선택되면, 점 소수 표기법에서 특정 타겟 IP 주소를 입력할 수 있습니다.

타겟 IP 마스크 (Target IP Mask):

타겟 IP 필터에 "Network"가 선택되면, 점 소수 표기법에서 특정 타겟 IP 마스크를 입력할 수 있습니다.

ARP 발송자 MAC 매치 (ARP Sender MAC Match):

sender hardware address 필드 (SHA) 설정에 따라 프레임이 동작을 실행할 수 있는지 여부를 지정합니다.

0: SHA가 SMAC 주소와 동일하지 않은 ARP 프레임입니다.

1: SHA가 SMAC 주소와 동일한 ARP 프레임입니다.

Any: 모든 값이 허용됩니다. ("관계 없음")

RARP 타겟 MAC 매치 (RARP Target MAC Match):

target hardware address 필드 (THA) 설정에 따라 프레임이 동작을 실행할 수 있는지 여부를 지정합니다.

0: THA가 MAC 주소와 동일하지 않은 RARP 프레임입니다.

1: THA가 MAC 주소와 동일한 RARP 프레임입니다.

Any: 모든 값이 허용됩니다. ("관계 없음")

IP/이더넷 길이 (IP/Ethernet Length):

ARP/RARP hardware address length (HLN)과 protocol address length (PLN) 설정에 따라 프레임이 동작을 실행할 수 있는지 여부를 지정합니다.

0: HLN이 이더넷 (0x06)과 동일하지 않거나 (PLN)이 IPv4 (0x04)과 동일하지 않은 ARP/RARP 프레임입니다.

1: HLN이 이더넷 (0x06)과 동일하거나 (PLN)이 IPv4 (0x04)과 동일한 ARP/RARP 프레임입니다.

Any: 모든 값이 허용됩니다. ("관계 없음")

이더넷 (Ethernet):

ARP/RARP hardware address space (HRD) 설정에 따라 프레임이 동작을 실행할 수 있는지 여부를 지정합니다.

0: HLD가 이더넷 (1)과 동일하지 않은 ARP/RARP 프레임입니다.

1: HLD가 이더넷 (1)과 동일한 ARP/RARP 프레임입니다.

Any: 모든 값이 허용됩니다. ("관계 없음")

IP:

ARP/RARP protocol address space (PRO) 설정에 따라 프레임이 동작을 실행할 수 있는지 여부를 지정합니다.

0: PRO가 IP (0x800)와 동일하지 않은 ARP/RARP 프레임입니다.

0: PRO가 IP (0x800)와 동일한 ARP/RARP 프레임입니다.

Any: 모든 값이 허용됩니다. ("관계 없음")

### **IP 항목**

IP 항목은 프레임 타입 "IPv4" 선택 시 설정할 수 있습니다.

IP 프로토콜 필터 (IP Protocol Filter):

이 ACE에 대한 IP 프로토콜 필터를 지정합니다.

Any: 지정된 IP 프로토콜 필터가 없습니다. ("관계 없음")

Specific: ACE와 특정 IP 프로토콜 필터를 지정하려면 이 값을 선택합니다. IP 프로토콜 필터를 입력하는 필드가 나타납니다.

ICMP: IPv4 ICMP 프로토콜 프레임을 필터링 하려면 ICMP를 선택합니다. ICMP 항목 정의에 대한 추가 필드가 나타납니다. 이 필드는 차후 도움 파일에서 설명합니다.

UDP: IPv4 UDP 프로토콜 프레임을 필터링 하려면 UDP를 선택합니다. UDP 항목 정의에 대한 추가 필드가 나타납니다. 이 필드는 차후 도움 파일에서 설명합니다.

TCP: IPv4 TCP 프로토콜 프레임을 필터링 하려면 TCP를 선택합니다. TCP 항목 정의에 대한 추가 필드가 나타납니다. 이 필드는 차후 도움 파일에서 설명합니다.

IP 프로토콜 값 (IP Protocol Value):

IP 프로토콜 값을 위해 "Specific"이 선택되면, 특정 값을 입력할 수 있습니다. 허용 범위는 0에서 255입니다. ACE를 실행하는 프레임이 이 IP 프로토콜 값과 일치합니다.

IP TTL:

이 ACE에 대한 Time-to-Live 설정을 지정합니다.

zero: 0보다 큰 Time-to-Live 필드의 IPv4 프레임은 이 엔트리와 일치해서는 안됩니다.

non-zero: 0보다 큰 Time-to-Live 필드의 IPv4 프레임은 이 엔트리와 일치해야 합니다.

Any: 모든 값이 허용됩니다. ("관계 없음")

IP 프래그먼트 (IP Fragment):

이 ACE에 대한 프래그먼트 오프셋 설정을 지정합니다. 이 것은 IPv4 프레임을 위한 More Fragments (MF) 비트와 Fragment Offset (FRAG OFFSET) 필드에 대한 설정을 포함합니다.

No: MF 비트가 설정되거나 FRAG OFFSET 필드가 0보다 큰 IPv4 프레임은 이 엔트리에 일치해서는 안됩니다.

Yes: MF 비트가 설정되거나 FRAG OFFSET 필드가 0보다 큰 IPv4 프레임은 이 엔트리에 일치해야 합니다.

Any: 모든 값이 허용됩니다. ("관계 없음")

IP 옵션 (IP Option):

이 ACE에 대한 옵션 플래그 설정을 지정합니다.

No: 옵션 플래그가 설정된 IPv4 프레임이 이 엔트리에 일치해서는 안됩니다.

Yes: 옵션 플래그가 설정된 IPv4 프레임이 이 엔트리에 일치해야 합니다.

Any: 모든 값이 허용됩니다. ("관계 없음")

SIP 필터 (SIP Filter):

이 ACE에 대한 소스 IP 필터를 지정합니다.

Any: 지정된 소스 IP 필터가 없습니다. (소스 IP 필터는 "관계 없음"입니다.)

Host: 소스 IP 필터가 Host로 설정됩니다. 나타나는 SIP 주소 필드 내의 소스 IP 주소를 지정합니다.

Network: 소스 IP 필터가 Network 로 설정됩니다. 나타나는 SIP 주소 및 SIP 마스크 필드에서 소스 IP 주소와 소스 IP 마스크를 지정합니다.

SIP 주소 (SIP Address):

소스 IP 필터에 "Host" 또는 "Network"가 지정되면 점 소수 표기법에서 특정 SIP 주소를 입력할 수 있습니다.

SIP 마스크 (SIP Mask):

소스 IP 필터에 "Network"가 선택되면, 점 소수 표기법에서 특정 SIP 마스크를 입력할 수 있습니다.

DIP 필터 (DIP Filter):

이 ACE에 대한 대상 IP를 지정합니다.

Any: 지정된 대상 IP 필터가 없습니다. (대상 IP 필터는 "관계 없음"입니다.)

Host: 대상 IP 필터가 Host로 설정됩니다. 나타나는 DIP 주소 필드 내의 대상 IP 주소를 지정합니다.

Network: 대상 IP 필터가 Network 로 설정됩니다. 나타나는 DIP 주소 및 DIP 마스크 필드에서 대상 IP 주소와 대상 IP 마스크를 지정합니다.

DIP 주소 (DIP Address):

대상 IP 필터에 "Host" 또는 "Network"가 지정되면 점 소수 표기법에서 특정 DIP 주소를 입력할 수 있습니다.

DIP 마스크 (DIP Mask):

"Network"가 대상 IP 필터에 선택되면, 점 소수 표기법에서 특정 IP 주소를 입력합니다.

### **IPv6 항목**

프레임 타임 "IPv6"가 선택되면 IPv6 항목을 설정할 수 있습니다.

다음 헤더 필터 (Next Header Filter):

이 ACE에 대한 IPv6 다음 헤더 필터를 지정합니다.

Any: 지정된 IPv6 다음 헤더 필터를 지정합니다. ("관계 없음")

Specific: 이 ACE와 특정 IPv6 다음 헤더 필터를 필터링 하고자 하는 경우 이 값을 선택합니다.

IPv6 다음 헤더 필터 입력 필드가 나타납니다.

ICMP: ICMP를 선택해 IPv6 ICMP 프로토콜 프레임을 필터링합니다. 대상 ICMP 항목에 대한 추가 필드가 나타납니다. 이 필드는 차후 도움 파일에서 설명합니다.

UDP: UDP를 선택해 IPv6 UDP 프로토콜 프레임을 필터링합니다. 대상 UDP 항목에 대한 추가 필드가 나타납니다. 이 필드는 차후 도움 파일에서 설명합니다.

TCP: TCP를 선택해 IPv6 TCP 프로토콜 프레임을 필터링합니다. 대상 TCP 항목에 대한 추가 필드가 나타납니다. 이 필드는 차후 도움 파일에서 설명합니다.

다음 헤더 값 (Next Header Value):

"Specific"이 IPv6 다음 헤더 값에 대해 선택되면, 특정 값을 선택할 수 있습니다. 허용 범위는 0에서 255입니다. ACE를 실행하는 프레임이 이 IPv6 프로토콜 값에 일치합니다.

SIP 필터 (SIP Filter):

ACE에 대한 소스 IPv6 필터를 지정합니다.

Any: 지정된 소스 IPv6 필터가 없습니다. (소스 IPv6 필터는 "관계 없음"입니다.)

Specific: 소스 IPv6 필터가 Network에 설정됩니다. 나타나는 SIP 주소 필드에서 소스 IPv6 주소와 소스 IPv6 마스크를 지정합니다.

SIP 주소 (SIP Address):

"Specific"이 소스 IPv6 필터에 대해 선택되면, SIPv6 주소를 입력할 수 있습니다. IPv6 주소에 대한 마지막 32비트가 지원되는 필드입니다.

SIP 비트마스크 (SIP BitMask):

"Specific"이 소스 IPv6 필터에 대해 선택되면, 특정 SIPv6 마스크를 입력할 수 있습니다. IPv6 주소에 대한 마지막 32비트가 지원되는 필드입니다. 비트마스크 사용을 유의하십시오. 이진법 값이 "0"인 경우, 이 비트는 "관계 없음"을 뜻합니다. 실제 일치되는 패턴은 [sipv6\_address & sipv6\_bitmask] (마지막 32비트) 입니다. 예를 들어, SIPv6 주소가 2001::3이고 SIPv6 비트마스크가 0xffffffff (비트 0이 "관계 없음"입니다.) 이면 SIPv6 주소 2001::2와 2001::3는 이 규칙에 적용됩니다.

Hop Limit:

이 ACE에 대한 Hop Limit을 지정합니다.

zero: 0보다 큰 Hop Limit 필드의 IPv6 프레임은 이 엔트리에 일치해서는 안됩니다.

non-zero: 0보다 큰 Hop Limit 필드의 IPv6 프레임은 이 엔트리에 일치해야 합니다.

Any: 모든 값이 허용됩니다. ("관계 없음")

## ICMP 항목

ICMP 타입 필터 (ICMP Type Filter):

ACE에 대한 ICMP 필터를 지정합니다.

Any: 지정된 ICMP 필터가 없습니다. (ICMP 필터 상태가 "관계 없음"입니다.)

Specific: 특정 ICMP 필터가 이 ACE와 필터링 되길 원한다면, 특정 ICMP 값을 입력할 수 있습니다. ICMP 값 입력 필드가 나타납니다.

ICMP 타입 값 (ICMP Type Value):

"Specific"이 ICMP 필터에 선택되면, 특정 ICMP 값을 입력할 수 있습니다. 허용 범위는 0에서 255입니다. ACE를 실행하는 프레임이 이 ICMP 값에 일치합니다.

ICMP 코드 필터 (ICMP Code Filter):

ACE에 대한 ICMP 코드 필터를 지정합니다.

Any: 지정된 ICMP 코드 필터가 없습니다. (ICMP 필터 코드 상태가 "관계 없음"입니다.)

Specific: 특정 ICMP 코드 필터가 이 ACE와 필터링 되길 원한다면, 특정 ICMP 코드 값을 입력할 수 있습니다. ICMP 코드 값 입력 필드가 나타납니다.

ICMP 코드 값 (ICMP Code Value):

"Specific"이 ICMP 코드 필터에 선택되면, 특정 ICMP 코드 값을 입력할 수 있습니다. 허용 범위는 0에서 255입니다. ACE를 실행하는 프레임이 이 ICMP 코드 값에 일치합니다.

TCP/UDP 항목

TCP/UDP 소스 필터 (TCP/UDP Source Filter):

ACE에 대한 TCP/UDP 소스 필터를 지정합니다.

Any: 지정된 TCP/UDP 필터가 없습니다. (TCP/UDP 소스 필터 상태가 "관계 없음"입니다.)

Specific: 특정 TCP/UDP 소스 필터가 이 ACE와 필터링 되길 원하면, 특정 TCP/UDP 소스 값을 입력할 수 있습니다. TCP/UDP 소스 값 입력 필드가 나타납니다.

Range: 지정된 TCP/UDP 소스 범위 필터가 이 ACE와 필터링 되길 원하면, 특정 TCP/UDP 소스 범위 값을 입력할 수 있습니다. TCP/UDP 소스 값에 대한 필드가 나타납니다.

TCP/UDP 소스 번호 (TCP/UDP Source No.):

"Specific"이 TCP/UDP 소스 필터에 선택되면, 특정 TCP/UDP 소스 값을 입력할 수 있습니다. 허용 범위는 0에서 65535입니다. ACE를 실행하는 프레임이 TCP/UDP 소스 값에 일치합니다.

TCP/UDP 소스 범위 (TCP/UDP Source Range):

"Range"가 TCP/UDP 소스 필터에 선택되면, 특정 TCP/UDP 소스 범위 값을 입력할 수 있습니다.

허용 범위는 0에서 65535입니다. ACE를 실행하는 프레임이 TCP/UDP 소스 값에 일치합니다.

TCP/UDP 대상 필터 (TCP/UDP Destination Filter):



이 ACE에 대한 TCP/UDP 대상 필터를 지정합니다.

Any: 지정된 TCP/UDP 대상 필터가 없습니다. (TCP/UDP 대상 필터 상태는 "관계 없음"입니다.)

Specific: 특정 TCP/UDP 대상 필터가 ACE와 필터링 되길 원하면, 특정 TCP/UDP 대상 필터 값을 입력할 수 있습니다. TCP/UDP 대상 값 입력 필드가 나타납니다.

Range: 특정 TCP/UDP 대상 필터가 ACE와 필터링 되길 원하면, 특정 TCP/UDP 대상 범위 값을 입력할 수 있습니다. TCP/UDP 대상 값 입력 필드가 나타납니다.

TCP/UDP 대상 번호 (TCP/UDP Destination Number):

"Specific"이 TCP/UDP 대상 필터에 선택되면, 특정 TCP/UDP 대상 값을 입력할 수 있습니다. 허용 범위는 0에서 65535입니다. ACE를 실행하는 프레임이 TCP/UDP 대상 값에 일치합니다.

TCP/UDP 대상 범위 (TCP/UDP Destination Range):

"Range"가 TCP/UDP 대상 필터에 선택되면, 특정 TCP/UDP 대상 범위 값을 입력할 수 있습니다. 허용 범위는 0에서 65535입니다. ACE를 실행하는 프레임이 TCP/UDP 대상 값에 일치합니다.

TCP FIN:

이 ACE에 대한 TCP "발소자로부터 데이터 없음" (FIN) 값을 지정합니다.

0: FIN 필드가 설정된 TCP 프레임이 이 엔트리에 일치해서는 안됩니다.

1: FIN 필드가 설정된 TCP 프레임이 이 엔트리에 일치해야 합니다.

Any: 모든 값이 허용됩니다. ("관계 없음")

TCP SYN:

TCP "순차 번호 동기화" (SYN) 값이 이 ACE에 지정됩니다.

0: SYN 필드가 설정된 TCP 프레임이 이 엔트리에 일치해서는 안됩니다.

1: SYN 필드가 설정된 TCP 프레임이 이 엔트리에 일치해야 합니다.

Any: 모든 값이 허용됩니다. ("관계 없음")

TCP RST:

TCP "연결 리셋" (RST) 값이 이 ACE에 지정됩니다.

0: RST 필드가 설정된 TCP 프레임이 이 엔트리에 일치해서는 안됩니다.

1: RST 필드가 설정된 TCP 프레임이 이 엔트리에 일치해야 합니다.

Any: 모든 값이 허용됩니다. ("관계 없음")

TCP PSH:

TCP "푸시 기능" (PSH) 값이 이 ACE에 지정됩니다.

0: PSH 필드가 설정된 TCP 프레임이 이 엔트리에 일치해서는 안 됩니다.

1: PSH 필드가 설정된 TCP 프레임이 이 엔트리에 일치해야 합니다.

Any: 모든 값이 허용됩니다. ("관계 없음")

TCP ACK:

TCP "주요 확인 필드" (ACK) 값이 이 ACE에 지정됩니다.

0: ACK 필드가 설정된 TCP 프레임이 이 엔트리에 일치해서는 안 됩니다.

1: ACK 필드가 설정된 TCP 프레임이 이 엔트리에 일치해야 합니다.

Any: 모든 값이 허용됩니다. ("관계 없음")

TCP URG:

TCP "주요 긴급 포인터 필드" (URG) 값이 이 ACE에 지정됩니다.

0: URG 필드가 설정된 TCP 프레임이 이 엔트리에 일치해서는 안 됩니다.

1: URG 필드가 설정된 TCP 프레임이 이 엔트리에 일치해야 합니다.

Any: 모든 값이 허용됩니다. ("관계 없음")

## 이더넷 타입 항목

프레임 타입 "Ethernet Type"이 선택되면 이더넷 타입 항목을 설정할 수 있습니다.

EtherType Filter:

이 ACE에 대한 이더넷 타입 필터를 지정합니다.

Any: 지정된 EtherType 필터가 없습니다. (EtherType 필터 상태가 "관계 없음"입니다)

Specific: EtherType 필터가 ACE와 필터링 되길 원한다면, 특정 EtherType 값을 입력할 수 있습니다. EtherType 값 입력 필드가 나타납니다.

이더넷 타입 값 (Ethernet Type Value):

"Specific"이 EtherType 필터에 선택되면, 특정 EtherType 값을 입력할 수 있습니다. 허용 범위는 0x600 에서 0xffff 이지만 0x800(IPv4), 0x806(ARP) 및 0x86DD(IPv6)를 제외합니다. 이 ACE를 실행하는 프레임이 EtherType 값에 일치합니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

자동 새로 고침 (Auto-refresh):

자동 새로 고침을 이용해 정보를 자동으로 새로 고침 합니다.

새로 고침 삭제, 전체 삭제 (Refresh, clear, Remove All):

수동으로 ACL 설정을 새로 고침하거나 삭제하려면 클릭합니다.

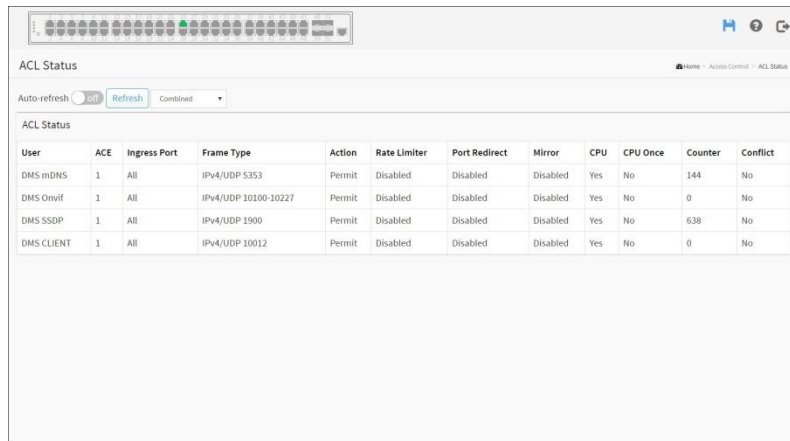
표의 모든 ACL 설정을 삭제합니다.

취소 (Cancel):

이전 페이지로 되돌아 갑니다.

## ACL 상태

이 섹션에서 다른 ACL 유저에 의해 ACL 상태 표시 방법을 설명합니다. 각 열은 지정된 ACE를 설명합니다. 하드웨어 제한 때문에 특정 ACE가 하드웨어에 적용되면 충돌이 된 것 입니다. 각 스위치의 ACE의 최대 수는 512입니다.



The screenshot shows the 'ACL Status' page in a web interface. At the top, there's a breadcrumb trail: Home > Access Control > ACL Status. Below the title, there are controls for 'Auto-refresh' (set to 'Off') and a 'Refresh' button. The main content is a table titled 'ACL Status' with the following columns: User, ACE, Ingress Port, Frame Type, Action, Rate Limiter, Port Redirect, Mirror, CPU, CPU Once, Counter, and Conflict. The table contains four rows of data:

| User       | ACE | Ingress Port | Frame Type           | Action | Rate Limiter | Port Redirect | Mirror   | CPU | CPU Once | Counter | Conflict |
|------------|-----|--------------|----------------------|--------|--------------|---------------|----------|-----|----------|---------|----------|
| DMS mDNS   | 1   | All          | IPv4/UDP 5353        | Permit | Disabled     | Disabled      | Disabled | Yes | No       | 144     | No       |
| DMS Onvif  | 1   | All          | IPv4/UDP 10100-10227 | Permit | Disabled     | Disabled      | Disabled | Yes | No       | 0       | No       |
| DMS SSDP   | 1   | All          | IPv4/UDP 1900        | Permit | Disabled     | Disabled      | Disabled | Yes | No       | 638     | No       |
| DMS CLIENT | 1   | All          | IPv4/UDP 10012       | Permit | Disabled     | Disabled      | Disabled | Yes | No       | 0       | No       |

### 웹 인터페이스

웹 인터페이스에서 ACL 상태를 표시하려면:

1. 액세스 컨트롤 및 ACL 상태를 클릭합니다.
2. 정보를 자동 새로 고침하려면 "자동 새로 고침"을 사용합니다.
3. "새로 고침"을 클릭해 ACL 상태를 새로 고칩니다.

### ■ 항목 설명:

유저 (User):

ACL 유저를 표시합니다.

ACE:

로컬 스위치의 ACE ID를 표시합니다.

프레임 타입 (Frame Type):

ACE 프레임 타입을 표시합니다. 가능한 값은 다음과 같습니다:

Any: ACE가 모든 프레임 타입과 일치합니다.

EType: ACE는 이더넷 타입 프레임에 일치합니다. ACE 기반 이더넷 타입이 IP와 ARP 프레임에 의해 일치되지 않습니다.

ARP: ACE는 ARP/RARP 프레임에 일치합니다.

IPv4: ACE는 모든 IPv4 프레임에 일치합니다.

IPv4/ICMP: ACE는 IPv4 프레임과 ICMP 프로토콜에 일치합니다.

IPv4/UDP: ACE는 IPv4 프레임과 UDP 프로토콜에 일치합니다.

IPv4/TCP: ACE는 IPv4 프레임과 TCP 프로토콜에 일치합니다.

IPv4/Other: ACE는 ICMP / UDP / TCP가 아닌 IPv4 프레임에 일치합니다.

IPv6: ACE는 모든 IPv6 표준 프레임에 일치합니다.

동작 (Action):

ACE 전송 동작을 표시합니다.

Permit: ACE를 일치하는 프레임이 전송되고 표시됩니다.

Deny: ACE를 일치하는 프레임이 삭제됩니다.

Filter: ACE를 일치하는 프레임이 필터링 됩니다.

속도 제한 장치 (Rate Limiter):

ACE 속도 제한 장치 수를 표시합니다. 허용 범위는 1에서 16입니다. Disabled가 표시되면 속도 제한 장치 동작이 비활성화 됩니다.

CPU:

특정 ACE에서 CPU에 일치하는 패킷을 전송합니다.

카운터 (Counter):

카운터가 프레임에 의해 실행된 ACE 횟수를 표시합니다.

충돌 (Conflict):

특정 ACE 하드웨어 상태를 표시합니다. 하드웨어 제한으로 인해 특정 ACE는 하드웨어에 적용되지 않습니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크하면 자동으로 페이지를 새로 고침 합니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 즉시 새로 고침 합니다.

# 14장

## SNMP

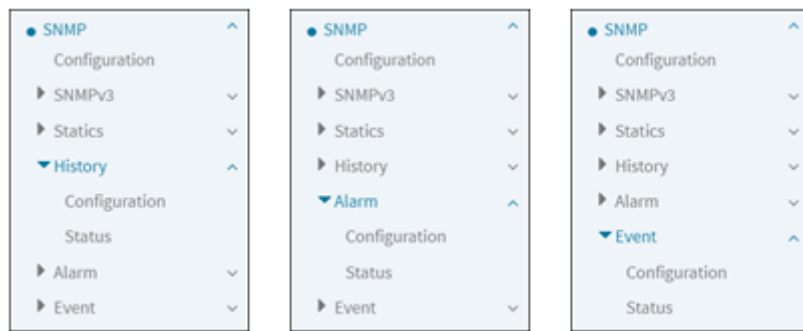
### 개요

Simple Network Management Protocol (SNMP)가 동작하는 모든 Network Management System (NMS)는 SNMP 에이전트가 내장된 관리 장치를 관리할 수 있으며, Management Information Base (MIB)는 관리 장치 상에서 올바르게 설치됩니다. SNMP는 SNMP 매니저 및 에이전트 사이의 정보 전송을 제어하는데 사용되며, management Information Base (MIB)의 Object Identity (OID)를 가로지르는데 사용되는 프로토콜로 SMI 구문 형식에서 설명됩니다. SNMP 에이전트는 SNMP 매니저에 의해 생긴 요청을 응답하도록 스위치 상에서 동작합니다.

기본적으로 트랩 정보 발행을 제외하고는 수동적입니다. 스위치는 SNMP 에이전트를 on/off하는 스위치를 지원합니다. 필드 SNMP를 "Enable"로 설정하면 SNMP 에이전트가 시작될 것입니다. 모든 지원되는 RMON MIB를 포함한 MIB OID는 SNMP 매니저를 통해 액세스 가능합니다. 필드 SNMP가 "Disable"로 설정되면 SNMP 에이전트는 비활성화 되고, 관련 커뮤니티 이름, 트랩 호스트 IP 주소, 트랩 및 모든 MIB 카운터가 무시됩니다.

메뉴는 다음과 같습니다:

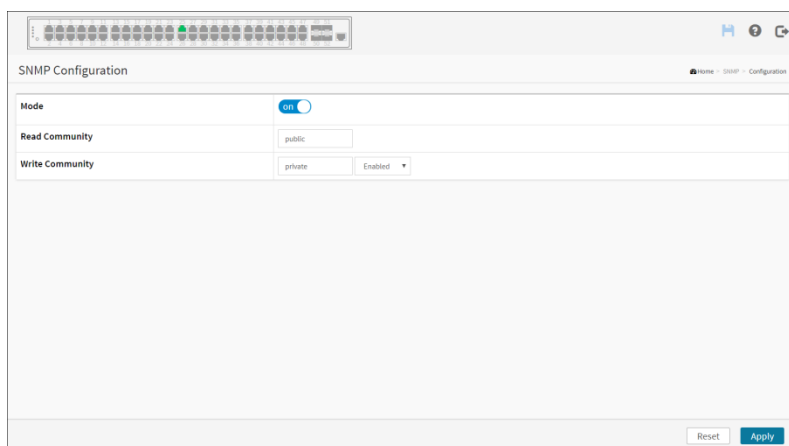






## 설정

이 섹션은 스위치의 SNMP 시스템 설정 방법을 설명합니다. 이 기능은 SNMP 설정, 커뮤니티 이름, 트랩 호스트 및 퍼블릭 트랩, SNMP 조정을 설정하는데 사용됩니다. SNMP 매니저는 커뮤니티 이름 모두를 식별해 인증을 통과해야 합니다. 그러면 해당 장치의 MIB 정보에 액세스할 수 있습니다. 따라서 두 그룹이 동일한 커뮤니티 이름을 갖습니다. 일단 설정을 완료하면 설정 실행을 위해 적용을 클릭합니다.



### 웹 인터페이스

웹 인터페이스에서 유저를 설정하려면:

1. SNMP와 설정을 클릭합니다.
2. SNMP 상태를 사용해 SNMP 기능을 활성화 또는 비활성화 합니다.
3. 읽기 커뮤니티, 쓰기 커뮤니티를 지정합니다.
4. 적용을 클릭합니다.

### ■ 항목 설명:

모드 (Mode):

SNMP 모드 동작을 식별합니다. 가능한 모드는 다음과 같습니다:

On: SNMP 모드 동작을 활성화 합니다.

Off: SNMP 모드 동작을 비활성화 합니다.

읽기 커뮤니티 (Read Community):

SNMP 에이전트로 액세스를 허용하기 위해 커뮤니티 읽기 액세스 문자열을 식별합니다. 허용 문자열 길이는 1에서 31입니다. 허용되는 내용은 33에서 126의 ASCII 글자입니다.

필드는 SNMP 버전이 SNMPv1 또는 SNMPv2c일 때만 적용 가능합니다. SNMP 버전이 SNMPv3인 경우 커뮤니티 문자열이 SNMPv3 커뮤니티 테이블과 연관됩니다. SNMPv1 및 SNMPv2c 커뮤니티 문자열 보다 보안 이름 설정에 더욱 유연함을 제공합니다. 커뮤니티 문자열에 더해, 특정 소스 주소 범위는 소스 서브넷을 제한하는데 사용될 수 있습니다.

쓰기 커뮤니티 (Write Community):

SNMP 에이전트로 액세스를 허용하기 위해 커뮤니티 쓰기 액세스 문자열을 식별합니다. 허용 문자열 길이는 1에서 31입니다. 허용되는 내용은 33에서 126의 ASCII 글자입니다.

필드는 SNMP 버전이 SNMPv1 또는 SNMPv2c일 때만 적용 가능합니다. SNMP 버전이 SNMPv3인 경우 커뮤니티 문자열이 SNMPv3 커뮤니티 테이블과 연관됩니다. SNMPv1 및 SNMPv2c 커뮤니티 문자열 보다 보안 이름 설정에 더욱 유연함을 제공합니다. 커뮤니티 문자열에 더해, 특정 소스 주소 범위는 소스 서브넷을 제한하는데 사용될 수 있습니다.

## ■버튼

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

# SNMPv3

## 커뮤니티

이 페이지의 SNMPv3 커뮤니티 테이블을 설정합니다. 엔트리 인덱스 키는 커뮤니티입니다.

The screenshot shows the 'SNMPv3 Community Configuration' page. At the top, there is a breadcrumb trail: Home > SNMP > SNMPv3 > Communities. Below this is a table with four columns: 'Delete', 'Community', 'Source IP', and 'Source Mask'. The 'Community' column is currently empty. To the left of the table is an 'Add New Entry' button. At the bottom right of the page are 'Reset' and 'Apply' buttons.

### 웹 인터페이스

웹 인터페이스에서 SNMP 커뮤니티를 설정하려면:

1. SNMP, SNMPv3 및 커뮤니티를 클릭합니다.
2. 새 엔트리 추가를 클릭합니다.

The screenshot shows the 'SNMPv3 Community Configuration' page after adding a new entry. The table now contains one row. The 'Delete' column has a 'Delete' button. The 'Community' column is empty. The 'Source IP' and 'Source Mask' columns both contain '0.0.0.0'. The 'Add New Entry' button is still present. At the bottom right are 'Reset' and 'Apply' buttons.

3. SNMP 커뮤니티 항목을 지정합니다.
4. 적용을 클릭합니다.

5. 설정을 조정 또는 삭제하려면 리셋을 클릭하세요.

### ■ 항목 설명:

커뮤니티 (Community):

커뮤니티를 SNMP 그룹 설정에 표시하도록 보안 이름을 나타냅니다. 허용 문자열 길이는 1에서 32이며 허용되는 내용은 33에서 126의 ASCII 글자입니다.

소스 IP (Source IP):

SNMP 액세스 소스 주소를 표시합니다. 소스 주소의 특정 범위는 소스 마스크와 조합되는 경우 소스 서브넷을 제한하는데 사용 가능합니다.

소스 IP 프리픽스 (Source IP Prefix):

SNMP 액세스 소스 주소 프리픽스를 표시합니다.

### ■ 버튼

새 엔트리 추가 (Add New Entry):

새 엔트리를 추가하려면 클릭하세요. 이름을 지정하고 새 엔트리를 설정합니다. "적용"을 클릭하세요.

삭제 (Delete):

엔트리를 삭제하려면 체크하세요. 다음 저장 동안 삭제될 것 입니다.

적용 (Apply):

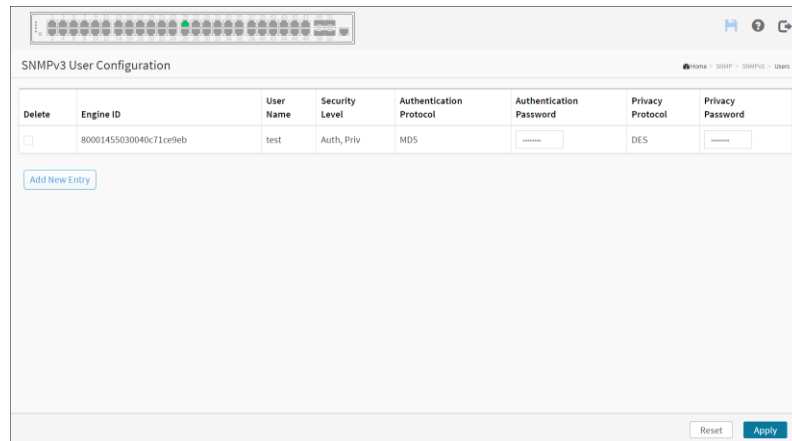
변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

### 유저

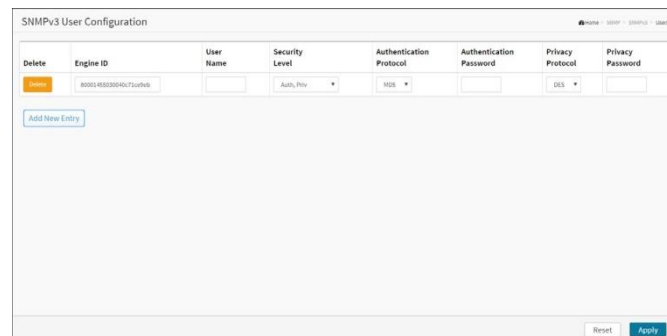
기능이 SNMPv3 유저를 설정하는데 사용됩니다. 엔트리 인덱스 키는 UserName입니다. 새로운 유저 이름 계정을 생성하려면 <Add new user> 버튼을 체크하고 유저 정보를 입력한 후 <Apply>를 체크합니다. 최대 그룹 수: 6



웹 인터페이스

웹 인터페이스에서 SNMP 유저를 설정하려면:

1. SNMP, SNMPv3 및 유저를 클릭합니다.
2. 새 엔트리 추가를 클릭합니다.



3. SNMPv3 유저 항목을 지정합니다.
4. 적용을 클릭합니다.

### ■ 항목 설명:

엔진 ID (Engine ID):

이 엔트리가 속해야 하는 엔진 ID를 식별하는 옥텟 글자입니다. 문자열은 10과 64 사이의 숫자로 이루어진 짝수 (16진법 형식)를 포함하지만, 모든 0과 모든 F는 허용되지 않습니다.

SNMPv3 구조가 메시지 보안을 위한 User-based Security Model (USM)과 액세스 컨트롤을 위한 View-based Access Control Model (VACM)를 사용합니다. USM 엔트리의 경우, usmUserEngineID 과 usmUserName이 엔트리의 키입니다. 간단한 에이전트의 경우, usmUserEngineID는 항상 에이전트 고유의 snmpEngineID 값입니다. 그 값은 또한 사용자가 의사소통을 할 수 있는 원격 SNMP 엔진의 snmpEngineID 값을 취할 수 있습니다. 다른 말로, 유저 엔진 ID가 시스템 엔진 ID와 일치하면, 로컬 유저라는 뜻입니다; 그렇지 않으면 원격 유저입니다.

유저 이름 (User Name):

이 엔트리가 속해야 하는 유저 이름을 식별하는 문자열입니다. 허용 글자 길이는 1에서 31입니다. 허용되는 내용은 33에서 126의 ASCII 글자입니다.

보안 레벨 (Security Level):

이 엔트리가 속해야 하는 보안 모델을 표시합니다. 가능한 보안 모델은 다음과 같습니다:

NoAuth, NoPriv: 인증 없음, 개인정보 보호 없음

Auth, NoPriv: 인증, 개인정보 보호 없음

Auth, Priv: 인증, 개인정보 보호

엔트리가 이미 존재한다면 보안 레벨 값은 조정 불가능합니다. 이 것은 먼저 값이 올바르게 설정되어 있는지 확인해야 한다는 뜻입니다.

인증 프로토콜 (Authentication Protocol):

이 엔트리가 속해야 하는 인증 프로토콜을 표시합니다. 가능한 인증 프로토콜은 다음과 같습니다:

MD5: 이 유저가 MD5 인증 프로토콜 사용을 표시하기 위한 선택 가능한 플래그입니다.

SHA: 이 유저가 SHA 인증 프로토콜 사용을 표시하기 위한 선택 가능한 플래그입니다.

엔트리가 이미 존재한다면 보안 레벨 값이 조정 불가능합니다. 이 것은 먼저 값이 올바르게 설정되어 있는지 확인해야 한다는 뜻입니다.

인증 패스워드 (Authentication Password):

인증 패스워드 단계를 식별하는 문자열입니다. MD5 인증 프로토콜의 경우 허용 문자 길이는 8에서 39입니다. SHA 인증 프로토콜의 경우, 허용된 문자 길이는 8에서 39입니다. 허용되는 내용은 33에서 126의 ASCII 글자입니다.

개인정보 보호 프로토콜 (Privacy Protocol):

이 엔트리가 속해야 하는 개인정보 프로토콜을 표시합니다. 가능한 개인정보 보호 프로토콜은 다음과 같습니다:

DES: 이 사용자가 DES 인증 프로토콜 사용을 표시하는 선택 가능한 플래그입니다.

AES: 이 사용자가 AES 인증 프로토콜 사용을 표시하는 선택 가능한 플래그입니다.

개인정보 보호 패스워드 (Privacy Password):

개인정보 보호 패스워드 단계를 표시하는 문자열입니다. 허용 문자 길이는 8에서 31입니다. 허용되는 내용은 33에서 126의 ASCII 글자입니다.

## ■ 버튼

새 엔트리 추가 (Add New Entry):

새 엔트리를 추가하려면 클릭하세요. 이름을 지정하고 새 엔트리를 설정합니다. "적용"을 클릭하세요.

삭제 (Delete):

엔트리를 삭제하려면 체크하세요. 다음 저장 동안 삭제될 것입니다.

적용 (Apply):

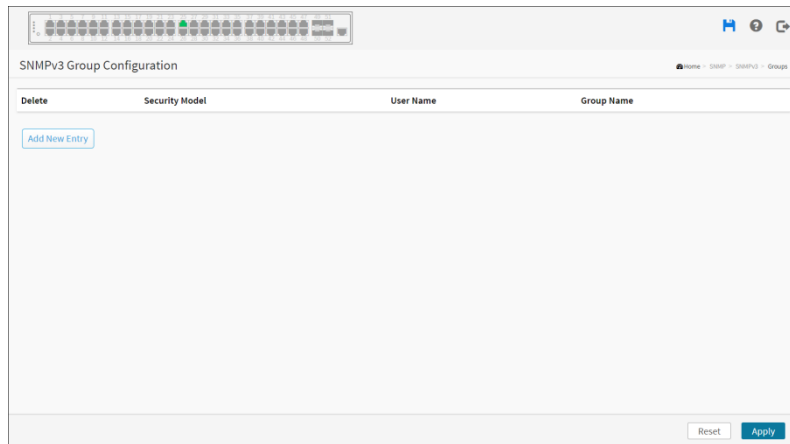
변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## 그룹

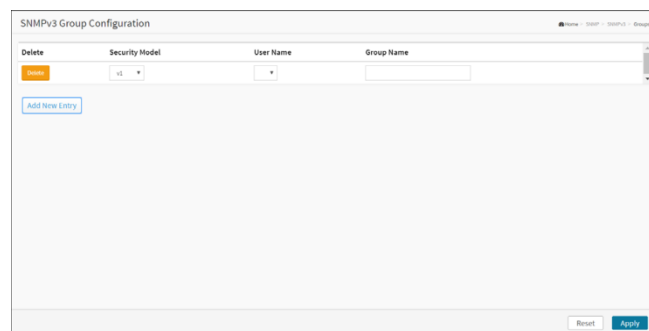
기능은 SNMPv3 그룹을 설정하는데 사용됩니다. 엔트리 인덱스 키는 Security Model과 Security Name입니다. 새 그룹 계정을 생성하려면 <Add new group>버튼을 체크하고 그룹 정보를 입력한 후 <Apply>를 체크하세요. 최대 그룹 번호: 12



## 웹 인터페이스

웹 인터페이스에서 SNMP 그룹을 설정하려면:

1. SNMP, SNMPv3 와 그룹을 클릭합니다.
2. 새 엔트리 추가를 클릭합니다.



3. SNMP 그룹 항목을 지정합니다.
4. 적용을 클릭합니다.

## ■ 항목 설명:

보안 모델 (Security Model):

이 엔트리가 속해야 할 보안 모델을 표시합니다. 가능한 보안 모델은 다음과 같습니다:

v1: SNMPv1 보류



v2c: SNMPv2c 보류

usm: 유저 기반 보안 모델 (USM)

보안 이름 (Security Name):

이 엔트리가 속해야 할 보안 이름을 표시하는 문자열입니다. 허용 글자 길이는 1에서 31입니다. 허용되는 내용은 33에서 126의 ASCII 글자입니다.

그룹 이름 (Group Name):

이 엔트리가 속해야 할 그룹 이름을 표시하는 문자열입니다. 허용 글자 길이는 1에서 32입니다. 허용되는 내용은 33에서 126의 ASCII 글자입니다.

## ■ 버튼

새 엔트리 추가 (Add New Entry):

새 엔트리를 추가하려면 클릭하세요. 이름을 지정하고 새 엔트리를 설정합니다. "적용"을 클릭하세요.

삭제 (Delete):

엔트리를 삭제하려면 체크하세요. 다음 저장 동안 삭제될 것 입니다.

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

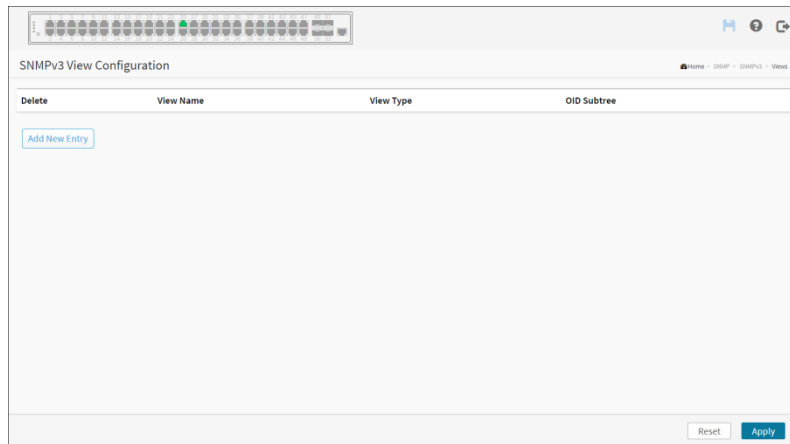
리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## 뷰

이 기능은 SNMPv3 뷰를 설정하는데 사용됩니다. 엔트리 인덱스 키는 OID Subtree 및 View Name입니다. 새 뷰 계정을 생성하려면 <Add new view> 버튼을 체크하고 뷰 정보를 입력한 후 <Apply>를 클릭합니다. 최대 그룹 번호: 12

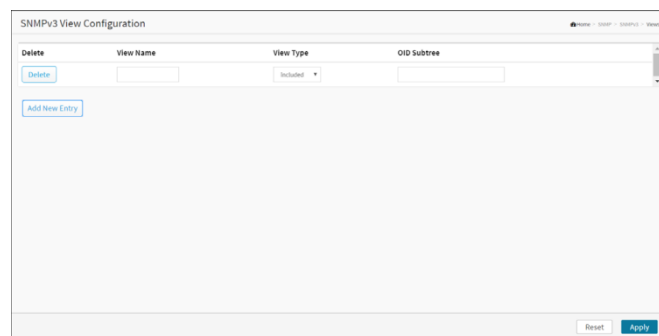
이 페이지의 SNMPv3 뷰 테이블을 설정합니다. 엔트리 인덱스 키는 View Name 및 OID Subtree입니다.



## 웹 인터페이스

웹 인터페이스에서 SNMP 뷰를 설정하려면:

1. SNMP, SNMPv3 및 뷰를 클릭합니다.
2. 새 엔트리 추가를 클릭합니다.



3. SNMP 뷰 항목을 지정합니다.
4. 적용을 클릭합니다.
5. 설정을 조정 또는 삭제하려면 리셋을 클릭합니다.

## ■ 항목 설명:

뷰 이름 (View Name):

이 엔트리가 속해야 할 뷰 이름을 표시하는 문자열입니다. 허용 문자 길이는 1에서 31입니다. 허용되는 내용은 33에서 126의 ASCII 글자입니다.

뷰 타입 (View Type):

이 엔트리가 속해야 할 뷰 타입을 표시합니다. 가능한 뷰 타입은 다음과 같습니다:

Included: 포함되어야 하는 뷰 서브트리가 표시되는 선택 가능한 플래그입니다.

Excluded: 제외되어야 하는 뷰 서브트리가 표시되는 선택 가능한 플래그입니다.

일반적으로 뷰 엔트리의 뷰 타입이 'excluded' 이면, 'included' 뷰 타입이 있는 뷰 엔트리가 있으며 OID 서브트리가 'excluded' 뷰 엔트리를 넘어서게 됩니다.

OID 서브트리 (ID Subtree):

## ■ 버튼

새 엔트리 추가 (Add New Entry):

새 엔트리를 추가하려면 클릭하세요. 이름을 지정하고 새 엔트리를 설정합니다. "적용"을 클릭하세요.

삭제 (Delete):

엔트리를 삭제하려면 체크하세요. 다음 저장 동안 삭제될 것 입니다.

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

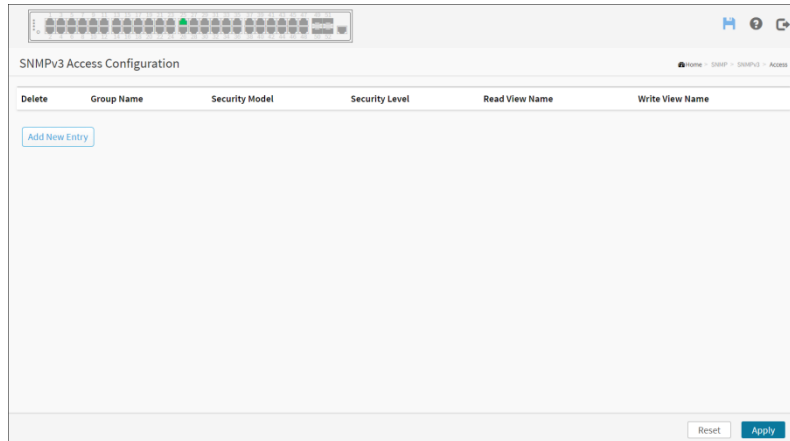
리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## 액세스

기능이 SNMPv3 액세스 설정을 위해 사용되면, 엔트리 인덱스 키는 그룹 이름, 보안 모델 및 보안 레벨입니다. 새 액세스 계정을 생성하려면,

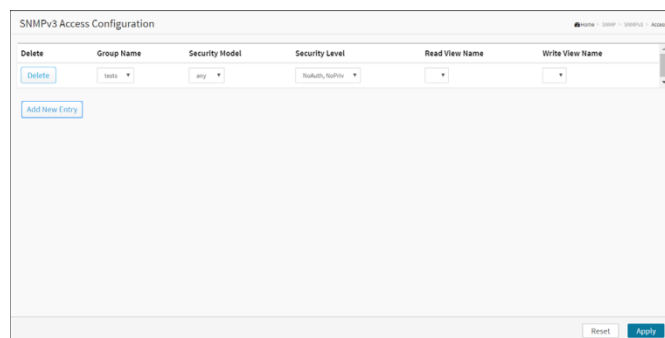
<Add new access> 버튼을 체크하고 계정 정보 입력 후 <Apply>를 체크합니다. 최대 그룹 수:12



웹 인터페이스

웹 인터페이스에서 SNMP 액세스 설정을 표시하려면:

1. SNMP, SNMPv3 및 액세스를 클릭합니다.
2. 새 엔트리 추가를 클릭합니다.



3. SNMP 액세스 항목을 지정합니다.
4. 적용을 클릭합니다.
5. 설정을 수정 또는 삭제하려면 리셋을 클릭하세요.

**■ 항목 설명:**

그룹 이름 (Group Name):

이 엔트리가 속해야 할 그룹 이름을 표시하는 문자열입니다. 허용 문자 길이는 1에서 31입니다. 허용되는 내용은 33에서 126의 ASCII 글자입니다.

보안 모델 (Security Model):

이 엔트리가 속해야 할 보안 모델을 표시합니다. 가능한 보안 모델은 다음과 같습니다:

v1: SNMPv1 보류

v2c: SNMPv2c 보류

usm: 유저 기반 보안 모델 (USM)

보안 레벨 (Security Level):

이 엔트리가 속해야 하는 보안 모델을 표시합니다. 가능한 보안 모델은 다음과 같습니다:

NoAuth, NoPriv: 인증 없음, 개인정보 보호 없음

Auth, NoPriv: 인증, 개인정보 보호 없음

Auth, Priv: 인증, 개인정보 보호

읽기 뷰 이름 (Read View Name):

현재 값을 요청할 수 있는 MIB 오브젝트를 정의하는 MIB 뷰 이름입니다. 허용 문자 길이는 1에서 31입니다. 허용되는 내용은 33에서 126의 ASCII 글자입니다.

쓰기 뷰 이름 (Write View Name):

잠재적 설정의 새 값을 요청할 수 있는 MIB 오브젝트를 정의하는 MIB 뷰 이름입니다. 허용 문자 길이는 1에서 31입니다. 허용되는 내용은 33에서 126의 ASCII 글자입니다.

**■ 버튼**

새 엔트리 추가 (Add New Entry):

새 엔트리를 추가하려면 클릭하세요. 이름을 지정하고 새 엔트리를 설정합니다. "적용"을 클릭하세요.

삭제 (Delete):

엔트리를 삭제하려면 체크하세요. 다음 저장 동안 삭제될 것 입니다.

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

# 상태

## 설정

이 페이지 상태 테이블을 설정합니다. 엔트리 인덱스 키는 ID입니다.

웹 인터페이스

웹 인터페이스에서 상태 설정을 구성하려면:

1. SNMP, 상태 및 설정을 클릭합니다.
2. 새 엔트리 추가를 클릭합니다.

3. ID 항목을 지정합니다.
4. 적용을 클릭합니다.

**■ 항목 설명:**

이 항목들은 RMON 현황 설정 페이지에 표시됩니다:

ID:

엔트리 인덱스를 표시합니다. 허용 점위는 1에서 65535입니다.

데이터 소스 (Data Source):

모니터링 하고자 하는 포트 ID를 표시합니다. 값은 1000\*(switch ID-1)이어야 합니다. 예를 들어 포트가 스위치 3 포트 5인 경우, 값은 2005입니다.

**■ 버튼**

삭제 (Delete):

엔트리를 삭제하려면 체크하세요. 다음 저장 동안 삭제될 것 입니다.

새 엔트리 추가 (Add New Entry):

새 엔트리를 추가하려면 클릭하세요. 이름을 지정하고 새 엔트리를 설정합니다. "적용"을 클릭하세요.

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

**현황**

이 페이지는 RMON 현황 엔트리 개요를 제공합니다. 각 페이지는 현황 테이블에서 최대 99엔트리를 표시하며, 기본값은 20으로 "페이지 당 엔트리" 입력 필드를 통해 선택됩니다. 첫 방문 시 웹 페이지는 현황 테이블의 처음부터 20 엔트리를 먼저 표시합니다. 처음 표시된 것은 현황 테이블에서 발견된 가장 낮은 ID입니다.

"컨트롤 인덱스에서 시작"으로 유저는 현황 테이블에서 시작 포인트를 선택할 수 있습니다. 새로 고침 버튼을 클릭해 현황테이블과 일치하거나 가장 근접한 것부터 시작을 표시되는 테이블을 업데이트합니다.

다음 엔트리는 다음 탐색을 위해 기준이 되는 현재 표시된 엔트리의 마지막 엔트리를 사용합니다. 마지막에 도달하면 "No more entries"가 테이블에 표시됩니다. 다시 시작하려면 첫 엔트리 버튼을 사용하십시오.



## 웹 인터페이스

웹 인터페이스에서 RMON 현황 상태를 표시하려면:

1. SNMP 상태 및 현황을 클릭합니다.
2. 체크할 포트를 지정합니다.
3. "자동 새로 고침"을 확인합니다.
4. "새로 고침"을 클릭해 포트 상세 현황을 새로 고칩니다.

## ■ 항목 설명:

ID:

현황 엔트리 인덱스를 표시합니다.

데이터 소스 (Data Source) (인덱스인 경우) :

모니터링 하고자 하는 포트 ID입니다.

삭제 (Drop):

리소스 부족으로 인한 시도로 삭제되는 패킷의 이벤트의 총 합계입니다.

옥텟 (Octets):

네트워크 상에 수신되는 데이터 (불량 패킷 포함)의 옥텟 총 합계입니다.

Pkts:

수신되는 패킷 (불량 패킷, 브로드캐스트 패킷 및 멀티캐스트 패킷) 패킷의 총 합계입니다.

브로드캐스트 (Broadcast):

브로드캐스트 주소로 전송 수신된 양호한 패킷의 총 합계입니다.

멀티캐스트 (Multicast):

멀티캐스트 주소로 전송 수신된 양호한 패킷의 총 합계입니다.

CRC 에러 (CRC Errors):

64와 1518 옥텟 사이의 길이 (프레이밍 비트, FCS 옥텟 포함)를 포함하지만, 필수 옥텟 수의 불량 Frame Check Sequence (FCS) 또는 필수가 아닌 옥텟 수 (정렬 에러)의 불량 FCS를 갖는 수신된 패킷 총 합계 입니다.

크기 이하 (Under-size):

64 옥텟 이하로 수신된 패킷의 총 합계입니다.

크기 이상 (Over-size):

1518 옥텟보다 길게 수신된 패킷의 총 합계입니다.

프래그 (Frag.):

무효 CRC와 수신된 64 옥텟보다 적은 크기의 프레임 수입니다.

Jabb.:

무효 CRC와 수신된 64 옥텟보다 큰 크기의 프레임 수입니다.

Coll.:

이 이더넷 세그먼트 상의 충돌 총 합계의 최대 추정치입니다.

64 Bytes:

64옥텟 길이로 수신된 패킷 (불량 패킷 포함)의 총 합계입니다.

65-127:

65에서 127 옥텟 사이 길이로 수신된 패킷 (불량 패킷 포함)의 총 합계입니다.

128-255:

128에서 255 옥텟 사이 길이로 수신된 패킷 (불량 패킷 포함)의 총 합계입니다.

256-511:

256에서 511 옥텟 사이 길이로 수신된 패킷 (불량 패킷 포함)의 총 합계입니다.

512-1023:

512에서 1023 옥텟 사이 길이로 수신된 패킷 (불량 패킷 포함)의 총 합계입니다.

1024-1588:

1024에서 1588 옥텟 사이 길이로 수신된 패킷 (불량 패킷 포함)의 총 합계입니다.

검색 (Search):

확인하고자 하는 정보를 검색할 수 있습니다.

엔트리 표시 (Show entries):

표시하고자 하는 항목 수를 선택할 수 있습니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh)

페이지를 새로 고침 하려면 클릭합니다.

첫 엔트리 (First Entry):

첫 엔트리부터 시작하는 테이블을 업데이트합니다.

다음 엔트리 (Next Entry):

현재 표시된 마지막 엔트리 다음의 엔트리와 시작하는 테이블을 업데이트 합니다.

# 기록

## 설정

이 페이지 상의 RMON 기록 테이블을 설정합니다. 엔트리 인덱스 키는 ID입니다.

웹 인터페이스

웹 인터페이스에 RMON 기록 설정을 구성하려면:

1. SNMP 기록 및 설정을 클릭합니다.
2. 새 엔트리 추가를 클릭합니다.

3. ID 항목을 지정합니다.
4. 적용을 클릭합니다.

**■ 항목 설명:**

RMON 기록 설정 페이지 상의 표시된 항목입니다.

ID:

엔트리 인덱스를 표시합니다. 범위는 1에서 65535입니다.

데이터 소스 (Data Source):

모니터링 하고자 하는 포트 ID를 표시합니다. 스위치 스택킹의 경우, 값은  $1000 * (\text{switch ID} - 1)$ 이어야 합니다. 예를 들어 포트가 스위치 3 포트 5인 경우, 값은 2005입니다.

간격 (Interval):

기록 현황 데이터 샘플링을 위한 초당 간격을 표시합니다. 범위는 1에서 3600이며 기본 값은 1800초입니다.

버킷 (Buckets):

RMON에 저장된 기록 제어 엔트리와 관련된 최대 데이터 엔트리를 포함합니다. 범위는 1에서 3600이며 기본 값은 50입니다.

승인된 버킷 (Buckets Granted):

RMON에 저장된 데이터 셀의 수입입니다.

**■ 버튼**

삭제 (Delete):

엔트리를 삭제하려면 체크하세요. 다음 저장 동안 삭제될 것 입니다.

새 엔트리 추가 (Add New Entry):

새 엔트리를 추가하려면 클릭하세요.

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

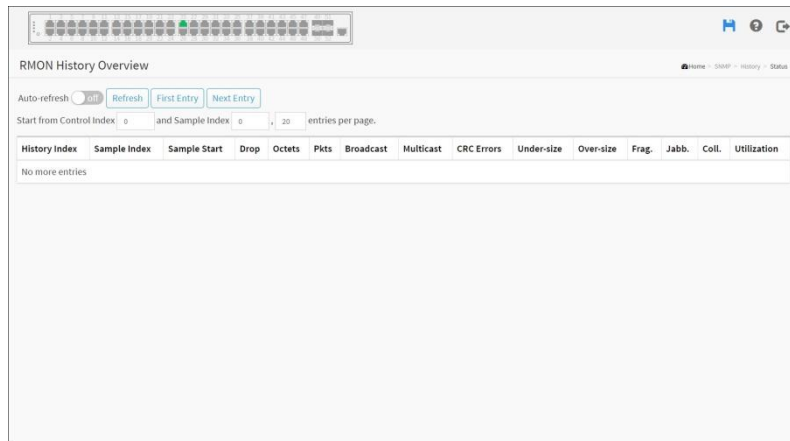
**현황**

이 페이지는 RMON 기록 엔트리 개요를 제공합니다. 각 페이지는 기록 테이블에서 최대 99엔트리를 표시하며, 기본값은 20으로 “페이지 당 엔트리” 입력 필드를 통해 선택됩니다. 첫 방문 시 웹 페이지는 기록 테이블의 처음부터 20 엔트리를 먼저 표시합니다.

처음 표시된 것은 기록 테이블에서 발견된 가장 낮은 히스토리 인덱스와 샘플 인덱스입니다.

“히스토리 인덱스와 샘플 인덱스에서 시작”으로 유저는 기록 테이블에서 시작 포인트를 선택할 수 있습니다. 새로 고침 버튼을 클릭해 기록 테이블과 일치하거나 가장 근접한 것부터 시작을 표시되는 테이블을 업데이트합니다.

다음 엔트리는 다음 탐색을 위해 기준이 되는 현재 표시된 엔트리의 마지막 엔트리를 사용합니다. 마지막에 도달하면 “No more entries”가 테이블에 표시됩니다. 다시 시작하려면 첫 엔트리 버튼을 사용하십시오.



## 웹 인터페이스

웹 인터페이스에서 RMON 기록 상태를 표시하려면:

1. SNMP 기록 및 상태를 클릭합니다.
2. “자동 새로 고침”을 확인합니다.
3. “새로 고침”을 클릭해 포트 상세 현황을 새로 고칩니다.
4. 첫 엔트리/다음 엔트리를 클릭해 엔트리를 변경합니다.

## ■ 항목 설명:

히스토리 인덱스 (History Index):

히스토리 컨트롤 엔트리 인덱스를 표시합니다.

샘플 인덱스 (Sample Index):

컨트롤 엔트리와 연관된 데이터 엔트리 인덱스를 표시합니다.

샘플 시작 (Sample Start):

샘플이 측정되는 다시 시작 간격의 sysUpTime 값입니다.

삭제 (Drop):

리소스 부족으로 인해 시도되는 패킷이 삭제될 이벤트 총 합계입니다.

옥텟 (Octets):

네트워크 상에 수신되는 데이터 (불량 패킷 포함)의 옥텟 총 합계입니다.

Pkts:

수신되는 패킷 (불량 패킷, 브로드캐스트 패킷 및 멀티캐스트 패킷) 패킷의 총 합계입니다.

브로드캐스트 (Broadcast):

브로드캐스트 주소로 전송 수신된 양호한 패킷의 총 합계입니다.

멀티캐스트 (Multicast):

멀티캐스트 주소로 전송 수신된 양호한 패킷의 총 합계입니다.

CRC 에러 (CRC Errors):

64와 1518 옥텟 사이의 길이 (프레이밍 비트, FCS 옥텟 포함)를 포함하지만, 필수 옥텟 수의 불량 Frame Check Sequence (FCS) 또는 필수가 아닌 옥텟 수 (정렬 에러)의 불량 FCS를 갖는 수신된 패킷 총 합계 입니다.

크기 이하 (Under-size):

64 옥텟 이하로 수신된 패킷의 총 합계입니다.

크기 이상 (Over-size):

1518 옥텟보다 길게 수신된 패킷의 총 합계입니다.

фра그 (Frag.):

무효 CRC와 수신된 64 옥텟보다 적은 크기의 프레임 수입니다.

Jabb.:

무효 CRC와 수신된 64 옥텟보다 큰 크기의 프레임 수입니다.

Coll.:

이 이더넷 세그먼트 상의 충돌 총 합계의 최대 추정치입니다.

64 Bytes:

활용 (Utilization):

100분의 1 샘플링 간격 중 이 인터페이스 상의 물리적 레이어 네트워크 활용 수단의 최대 추정치입니다.

엔트리 표시 (Show entries):

표시하고자 하는 항목 수를 선택할 수 있습니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh)

페이지를 새로 고침 하려면 클릭합니다.

첫 엔트리 (First Entry):

첫 엔트리부터 시작하는 테이블을 업데이트합니다.

다음 엔트리 (Next Entry):

현재 표시된 마지막 엔트리 다음의 엔트리와 시작하는 테이블을 업데이트 합니다.



# 알림

## 설정

이 페이지에서 RMON 알림 테이블을 설정합니다. 엔트리 인덱스 키는 ID입니다.

RMON Alarm Configuration

| Delete        | ID | Interval | Variable | Sample Type | Value | Startup Alarm | Rising Threshold | Rising Index | Falling Threshold | Falling Index |
|---------------|----|----------|----------|-------------|-------|---------------|------------------|--------------|-------------------|---------------|
| Add New Entry |    |          |          |             |       |               |                  |              |                   |               |

Reset Apply

웹 인터페이스

웹 인터페이스에서 RMON 알림 설정을 구성하려면:

1. SNMP, 알림 및 설정을 클릭합니다.
2. 새 엔트리 추가를 클릭합니다.

RMON Alarm Configuration

| Delete | ID | Interval | Variable            | Sample Type | Value | Startup Alarm  | Rising Threshold | Rising Index | Falling Threshold | Falling Index |
|--------|----|----------|---------------------|-------------|-------|----------------|------------------|--------------|-------------------|---------------|
| Delete |    | 30       | 1.3.6.1.2.1.2.2.1.0 | Data        | 0     | Rising/Falling | 0                | 0            | 0                 | 0             |

Add New Entry

Reset Apply

3. ID 항목을 지정합니다.
4. 적용을 클릭합니다.

**■ 항목 설명:**

다음은 RMON 알림 설정 페이지에 표시된 항목입니다:

ID:

엔트리의 인덱스를 식별합니다. 범위는 1에서 65535입니다.

간격 (Interval):

한계점 상승 및 하락 샘플링과 대조를 위한 초당 간격을 표시합니다. 범위는 1에서  $2^{31}-1$ 입니다.

변수 (Variables):

샘플링을 위한 특정 변수를 표시합니다. 가능한 변수는 다음과 같습니다:

InOctets:

프레임 글자를 포함한 인터페이스 상에 수신된 옥텟의 총 합계입니다.

InUcastPkts:

상위 레이어 프로토콜에 전송되는 유니캐스트 패킷 수입니다.

InNUcastPkts:

상위 레이어 프로토콜에 전송되는 멀티캐스트 패킷 수입니다.

InDiscards:

패킷이 정상임에도 폐기된 인바운드 패킷 수입니다.

InErrors:

상위 레이어 프로토콜에 전송되는 것을 막는 에러를 포함한 인바운드 패킷 수입니다.

InUnknownProtos:

미확인 또는 지원하지 않는 프로토콜로 인해 폐기된 인바운드 패킷 수입니다.

OutOctets:

프레임 글자를 포함한 인터페이스에 전송된 옥텟 수입니다.

OutUcastPkts:

전송이 필요한 유니캐스트 패킷 수입니다.

OutNUcastPkts:

전송이 필요한 브로드캐스트 및 멀티캐스트 패킷 수입니다.

OutDiscards:

정상 패킷 이벤트가 삭제된 아웃바운드 패킷 수입니다.

OutErrors:

에러로 인해 전송되지 못한 아웃바운드 패킷입니다.

OutQLen:

(패킷 내의)출력 패킷 라인 길이입니다.

샘플 타입 (Sample Type):

한계점과 비교를 위해 선택된 변수 샘플링 및 변수 계산 방법입니다. 가능한 샘플 타입은 다음과 같습니다:

Absolute: 샘플을 직접 받습니다.

Delta: 샘플 간 차이점을 계산합니다. (기본값)

값 (Value):

마지막 샘플링 기간 동안의 상태 값입니다.

시작 알림 (Startup Alarm):

선택된 변수의 샘플링 및 한계점과 비교하기 위해 변수를 측정하는 방법입니다. 가능한 샘플 타입은 다음과 같습니다:

RisingTrigger: 처음 값이 한계점 상승보다 크면 알립니다.

FallingTrigger: 처음 값이 한계점 하락보다 적으면 알립니다.

RisingOrFallingTrigger: 처음 값이 한계점 상승보다 크거나 한계점 하락보다 적으면 알립니다.

한계점 상승 (Rising Threshold):

한계점 값 상승 (-2147483648-2147483647)

인덱스 상승 (Rising Index):

이벤트 인덱스 상승 (1-65535)

한계점 하락 (Falling Threshold):

한계점 값 하락 (-2147483648-2147483647)

인덱스 하락 (Falling Index):

이벤트 인덱스 하락 (1-65535)

## ■ 버튼

삭제 (Delete):

엔트리 삭제를 체크합니다. 다음 저장동안 삭제됩니다.

새 엔트리 추가 (Add New Entry):

새 엔트리 추가를 위해 클릭합니다.

적용 (Apply):

클릭해 변경 사항을 저장합니다.

리셋 (Reset):

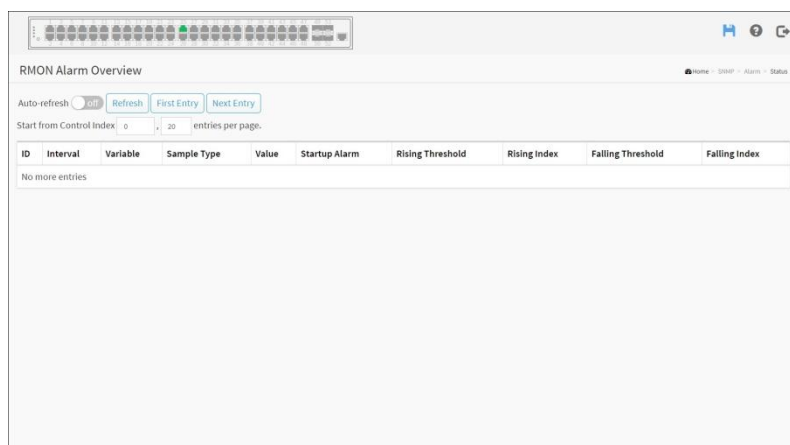
로컬에서 생긴 변경 사항을 취소하려면 클릭합니다. 이전 저장 값으로 되돌아 갑니다.

## **상태**

이 페이지는 RMON 알림 엔트리의 개요를 제공합니다. 각 페이지는 알림 테이블에서 최대 99 엔트리를 표시합니다. 기본값은 20이며 “페이지 당 엔트리” 필드를 통해 선택됩니다. 첫 방문 시 웹 페이지는 알림 테이블의 처음부터 20 엔트리를 먼저 표시합니다. 처음 표시된 것은 알림 테이블에서 발견된 가장 낮은 ID입니다.

“컨트롤 인덱스에서 시작”으로 유저는 알림 테이블에서 시작 포인트를 선택할 수 있습니다. 새로 고침 버튼을 클릭해 알림 테이블과 일치하거나 가장 근접한 것부터 시작을 표시되는 테이블을 업데이트합니다.

다음 엔트리는 다음 탐색을 위해 기준이 되는 현재 표시된 엔트리의 마지막 엔트리를 사용합니다. 마지막에 도달하면 “No more entries”가 테이블에 표시됩니다. 다시 시작하려면 첫 엔트리 버튼을 사용하십시오.



## **웹 인터페이스**

웹 인터페이스에서 RMON 알림 상태를 표시하려면:

1. SNMP, 알림 및 상태를 클릭합니다.

2. “새로 고침”을 체크합니다.
3. “새로 고침”을 클릭해 포트 상태 현황을 새로 고칩니다. 첫 엔트리/다음 엔트리를 클릭해 엔트리를 변경합니다.

### ■ 항목 설명:

ID:

알림 컨트롤 엔트리의 인덱스를 표시합니다.

간격 (Interval):

한계점 상승 및 하락 샘플링과 대조를 위한 초당 간격을 표시합니다.

변수 (Variables):

샘플링을 위한 특정 변수를 표시합니다. 가능한 변수는 다음과 같습니다:

샘플 타입 (Sample Type):

한계점과 비교를 위해 선택된 변수 샘플링 및 변수 계산 방법입니다.

값 (Value):

마지막 샘플링 기간 동안의 상태 값입니다.

시작 알림 (Startup Alarm):

이 엔트리가 먼저 유효로 설정된 경우 알림이 전송됩니다.

한계점 상승 (Rising Threshold):

한계점 값 상승

인덱스 상승 (Rising Index):

한계점 하락 (Falling Threshold):

한계점 값 하락

인덱스 하락 (Falling Index):

이벤트 인덱스 하락

엔트리 표시 (Show entries):

표시하고자 하는 항목 수를 선택합니다.

### ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh)

페이지를 새로 고침 하려면 클릭합니다.

첫 엔트리 (First Entry):

첫 엔트리부터 시작하는 테이블을 업데이트합니다.

다음 엔트리 (Next Entry):

현재 표시된 마지막 엔트리 다음의 엔트리와 시작하는 테이블을 업데이트 합니다.

# 이벤트

## 설정

이 페이지의 RMON 이벤트 테이블을 설정합니다. 엔트리 인덱스 키는 ID입니다.

RMON Event Configuration

| Delete        | ID | Desc | Type | Event Last Time |
|---------------|----|------|------|-----------------|
| Add New Entry |    |      |      |                 |

Reset Apply

웹 인터페이스

웹 인터페이스에서 RMON 이벤트 설정을 구성하려면:

1. SNMP, 이벤트 및 설정을 클릭합니다.
2. 새 엔트리 추가를 클릭합니다.

RMON Event Configuration

| Delete | ID | Desc | Type | Event Last Time |
|--------|----|------|------|-----------------|
| Delete |    |      | none | 0               |

Add New Entry

Reset Apply

3. ID 항목을 지정합니다.
4. 적용을 클릭합니다.

**■ 항목 설명:**

RMON 기록 설정 페이지 상에 표시된 항목입니다.

ID:

엔트리의 인덱스를 표시합니다. 범위는 1에서 65535입니다.

Desc:

0에서 127 문자 길이의 이벤트를 표시합니다. 기본값은 공백입니다.

타입 (Type):

이벤트 알림을 표시합니다. 가능한 타입은 다음과 같습니다:

None: 생성된 SNMP 로그가 없으면 전송된 SNMP 트랩이 없습니다.

Log: 이벤트를 일으키는 SNMP 로그 엔트리를 생성합니다.

Snm trap: 이벤트 발생 시 SNMP 트랩을 전송합니다.

Log and trap: 이벤트 발생 시 SNMP 로그 엔트리 생성 및 SNMP 트랩을 전송합니다.

이벤트 마지막 시간 (Event Last Time):

이벤트 엔트리가 마지막으로 이벤트를 동작한 시간의 sysUpTime 값을 표시합니다.

**■ 버튼**

삭제 (Delete):

엔트리 삭제를 체크합니다. 다음 저장동안 삭제됩니다.

새 엔트리 추가 (Add New Entry):

새 엔트리 추가를 위해 클릭합니다.

적용 (Apply):

클릭해 변경 사항을 저장합니다.

리셋 (Reset):

로컬에서 생긴 변경 사항을 취소하려면 클릭합니다. 이전 저장 값으로 되돌아 갑니다.

**상태**

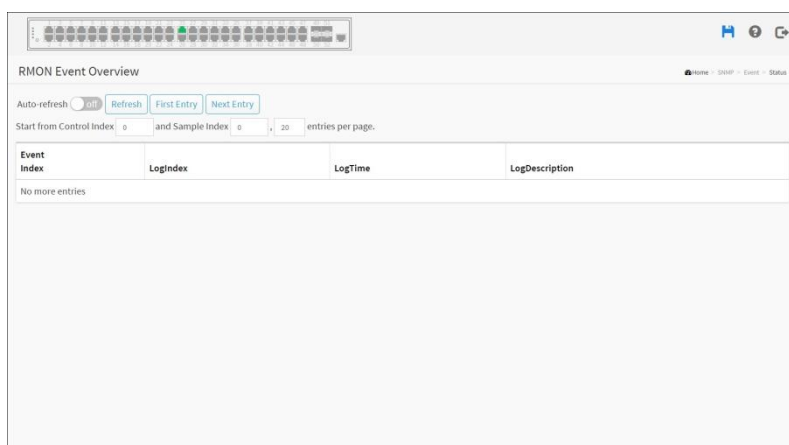
이 페이지는 RMON 알림 엔트리의 개요를 제공합니다. 각 페이지는 이벤트 테이블에서 최대 99 엔트리를 표시합니다. 기본값은 20이며 “페이지 당 엔트리” 필드를 통해 선택됩니다. 첫 방문 시 웹 페이지는 이벤트 테이블의 처음부터 20 엔트리를 먼저 표시합니다.



처음 표시된 것은 이벤트 테이블에서 발견된 가장 낮은 이벤트 인덱스 및 로그 인덱스입니다.

“컨트롤 인덱스 및 로그 인덱스에서 시작”으로 유저는 이벤트 테이블에서 시작 포인트를 선택할 수 있습니다. 새로 고침 버튼을 클릭해 이벤트 테이블과 일치하거나 가장 근접한 것부터 시작을 표시되는 테이블을 업데이트합니다.

다음 엔트리는 다음 탐색을 위해 기준이 되는 현재 표시된 엔트리의 마지막 엔트리를 사용합니다. 마지막에 도달하면 “No more entries”가 테이블에 표시됩니다. 다시 시작하려면 첫 엔트리 버튼을 사용하십시오.



웹 인터페이스

웹 인터페이스에서 RMON 이벤트 상태를 표시하려면:

1. SNMP, 이벤트 및 상태를 클릭합니다.
2. “자동 새로 고침”을 체크합니다.
3. “새로 고침”을 클릭해 포트 상세 현황을 클릭합니다.
4. 첫 엔트리/다음 엔트리를 클릭해 엔트리를 변경합니다.

### ■ 항목 설명:

이벤트 인덱스 (Event Index):

이벤트 엔트리의 인덱스를 표시합니다.

로그 인덱스 (Log Index):

로그 엔트리의 인덱스를 표시합니다.

로그 시간 (LogTime):

이벤트 로그 시간을 표시합니다.

로그 설명 (LogDescription):

이벤트 설명을 표시합니다.

엔트리 표시 (Show entries):

표시할 항목 수를 선택할 수 있습니다.

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh)

페이지를 새로 고침 하려면 클릭합니다.

첫 엔트리 (First Entry):

첫 엔트리부터 시작하는 테이블을 업데이트합니다.

다음 엔트리 (Next Entry):

현재 표시된 마지막 엔트리 다음의 엔트리와 시작하는 테이블을 업데이트 합니다.

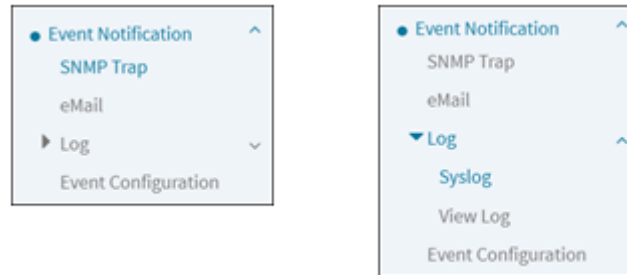
# 15장

## 이벤트 알림

### 개요

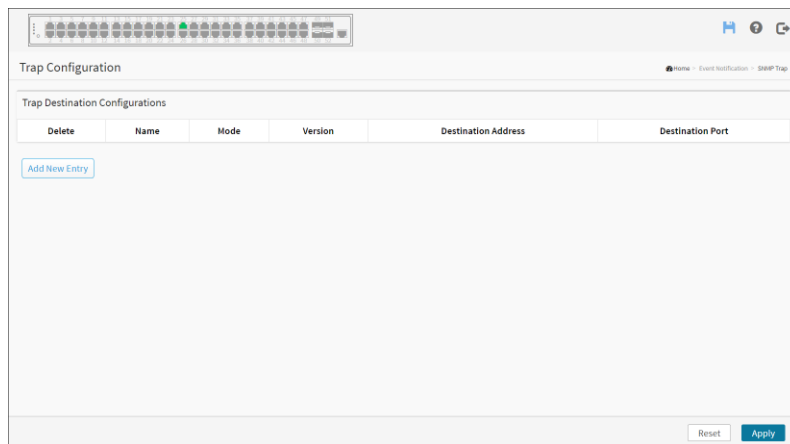
---

메뉴와 하위 메뉴는 다음과 같습니다:



## SNMP 트랩

이 페이지의 트랩을 설정합니다.



웹 인터페이스

웹 인터페이스에서 SNMP 트랩 설정을 구성하려면:

1. 이벤트 알림 및 SNMP 트랩을 클릭합니다.
2. 새 엔트리 추가를 클릭하면 스위치에 새로운 SNMP 트랩을 생성할 수 있습니다.

3. SNMP 트랩 항목을 지정합니다.
4. 적용을 클릭합니다.

## ■ 항목 설명:

### 트랩 대상 설정

이름 (Name):

트랩 설정 이름을 표시합니다. 트랩 대상 이름을 표시합니다.

활성화 (Enable):

트랩 대상 모드 동작을 표시합니다. 가능한 모드는 다음과 같습니다:

Enabled: SNMP 트랩 모드 동작을 활성화 합니다.

Disabled: SNMP 트랩 모드 동작을 비활성화 합니다.

버전 (Version):

지원되는 버전의 SNMP 트랩을 표시합니다. 가능한 버전은 다음과 같습니다:

SNMPv1: 지원되는 버전 1의 SNMP 트랩을 설정합니다.

SNMPv2c: 지원되는 버전 2c의 SNMP 트랩을 설정합니다.

SNMPv3: 지원되는 버전 3의 SNMP 트랩을 설정합니다.

대상 주소 (Destination Address):

SNMP 트랩 대상 주소를 표시합니다. 점 소수 표기법에서 유효 IP 주소를 허용합니다. ('x.y.z.w')

또한 유효 호스트이름을 허용합니다. 유효한 호스트 이름은 알파벳 (A-Za-z), 숫자 (0-9), 대시 (-) 범위의 글자입니다. 처음과 마지막 글자는 점 또는 대시를 허용하지 않습니다.

SNMP 트랩 대상 IPv6 주소를 표시합니다. IPv6 주소는 최대 4개의 16진수 숫자의 8 필드로 표시되는 128비트 레코드로 각 필드는 콜론(:)으로 구분됩니다. 예를 들어, 'fe80::215:c5ff:fe03:4dc7' 입니다. 심볼 '::'는 연속하는 0의 멀티플 16비트 그룹을 표시하는 줄임 표시로 사용 가능한 특정 구분입니다; 그러나 단 한번만 나타납니다. 또한 올바른 유효 IPv4 주소를 표시할 수 있습니다. 예: '::192.1.2.34'

대상 포트 (Destination port):

SNMP 대상 포트를 표시합니다. SNMP 에이전트는 이 포트를 통해 SNMP 메시지를 전송할 것입니다. 포트 범위는 1~65535입니다.

### SNMP 트랩 설정

트랩 설정 이름 (Trap Config Name):

설정을 위한 트랩 설정 이름을 표시합니다. 허용 문자 길이는 1에서 32이며 허용 글자는 33에서 126의 ASCII 글자입니다.

**트랩 모드 (Trap Mode):**

SNMP 모드 동작을 표시합니다. 가능한 모드는 다음과 같습니다:

on: SNMP 모드 동작을 활성화 합니다.

off: SNMP 모드 동작을 비활성화 합니다.

**트랩 버전 (Trap Version):**

지원되는 버전의 SNMP를 표시합니다. 가능한 버전은 다음과 같습니다:

SNMPv1: 지원되는 버전 1의 SNMP를 설정합니다.

SNMPv2c: 지원되는 버전 2c의 SNMP를 설정합니다.

SNMPv3: 지원되는 버전 3의 SNMP를 설정합니다.

**트랩 커뮤니티 (Trap Community):**

SNMP 트랩 패킷 전송 시 커뮤니티 액세스 글자를 표시합니다. 허용 문자 길이는 1에서 32이며 허용 글자는 33에서 126의 ASCII 글자입니다.

**트랩 대상 주소 (Trap Destination Address):**

SNMP 트랩 대상 주소를 표시합니다. 점 소수 표기법에서 유효 IP 주소를 허용합니다. ('x.y.z.w')

또한 유효 호스트이름을 허용합니다. 유효한 호스트 이름은 알파벳 (A-Za-z), 숫자 (0-9), 대시 (-) 범위의 글자입니다. 처음과 마지막 글자는 점 또는 대시를 허용하지 않습니다.

SNMP 트랩 대상 IPv6 주소를 표시합니다. IPv6 주소는 최대 4개의 16진수 숫자의 8 필드로 표시되는 128비트 레코드로 각 필드는 콜론(:)으로 구분됩니다. 예를 들어, 'fe80::215:c5ff:fe03:4dc7' 입니다. 심볼 '::'는 연속하는 0의 멀티플 16비트 그룹을 표시하는 줄임 표시로 사용 가능한 특정 구분입니다; 그러나 단 한번만 나타납니다. 또한 올바른 유효 IPv4 주소를 표시할 수 있습니다. 예: '::192.1.2.34'

**트랩 대상 포트 (Trap Destination port):**

SNMP 트랩 대상 포트를 표시합니다. SNMP 에이전트는 이 포트를 통해 SNMP 메시지를 전송할 것입니다. 포트 범위는 1~65535입니다.

**트랩 보안 엔진 ID (Trap Security Engine ID):**

SNMP 트랩 보안 엔진 ID를 표시합니다. SNMPv3는 트랩을 전송하고 USM을 이용해 인증 및 개인 정보 보호에 대해 알립니다. 이 트랩에 대한 고유 엔진 ID 및 알림이 필요합니다. "트랩 탐색 보안 엔진 ID" 활성화 시, ID는 자동으로 탐색될 것입니다. 그렇지 않으면 이 필드에 지정된 ID가 사용됩니다.

문자열은 짝수 번호 (16진수 형식)로 10에서 64 사이의 숫자이나 전체 열에 0 또는 F를 허용하지 않습니다.

트랩 보안 이름 (Trap Security Name):

SNMP 트랩 보안 이름을 표시합니다. USM을 이용한 인증 및 개인 정보 보호에 대한 SNMPv3 트랩 및 알림입니다. 트랩과 알림이 활성화 되면 고유 보안 이름이 필요합니다.

## ■ 버튼

새 엔트리 추가 (Add New Entry):

새 엔트리 추가를 위해 클릭합니다.

적용 (Apply):

클릭해 변경 사항을 저장합니다.

리셋 (Reset):

로컬에서 생긴 변경 사항을 취소하려면 클릭합니다. 이전 저장 값으로 되돌아 갑니다.

## 이메일

이 페이지의 SMTP (Simple Mail Transfer Protocol)를 설정합니다. Simple Mail Transfer Protocol은 인터넷의 메시지 교환 표준입니다.

스위치는 SMTP 클라이언트로 설정되며 서버는 알림 이벤트가 발생한 스위치에서 메시지를 수신할 원격 장치입니다.

The image shows a web-based configuration page titled "SMTP Configuration". At the top, there is a breadcrumb trail: "Home > Event Notification > email". Below this, the configuration fields are organized into two columns. The left column contains labels for "Mail Server", "User Name", "Password", "Sender", "Return Path", "Email Address 1", "Email Address 2", "Email Address 3", "Email Address 4", "Email Address 5", and "Email Address 6". The right column contains corresponding empty text input boxes for each label. At the bottom right of the form, there are two buttons: "Reset" and "Apply".

### 웹 인터페이스

웹 인터페이스에서 SMTP 설정을 구성하려면:

1. 이벤트 알림 및 이메일을 클릭합니다.
2. SMTP 설정 항목을 지정합니다.
3. 적용을 클릭합니다.

### ■ 항목 설명:

메일 서버 (Mail Server):

IP 주소 또는 메일 서버의 호스트이름입니다. IP 주소는 점 소수 표기법으로 표시됩니다. 이는 메일을 전송하는 장치입니다.

유저 이름 (User Name):

메일 서버의 유저 이름을 지정합니다.

패스워드 (Password):

메일 서버의 유저 패스워드를 지정합니다.

발송자 (Sender):



알림 메일의 발송자 이름을 지정합니다.

리턴 경로 (Return Path):

알림 메일의 발송자 이메일 주소를 지정합니다. 이 주소는 이메일 메시지의 "from" 주소입니다.

이메일 주소 # (Email Address #):

수신기의 이메일 주소를 지정합니다.

## ■ 버튼

적용 (Apply):

클릭해 변경 사항을 저장합니다.

리셋 (Reset):

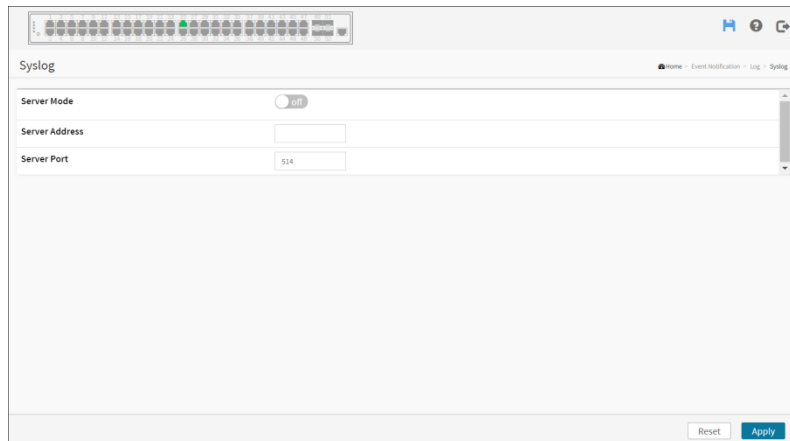
로컬에서 생긴 변경 사항을 취소하려면 클릭합니다. 이전 저장 값으로 되돌아 갑니다.

## 로그

---

### 시스로그

시스로그 설정은 프로그램 메시지 기록을 위한 기준입니다. 이 것은 메시지를 저장하는 시스템으로부터 메시지를 발생하는 소프트웨어와 메시지를 보고하고 분석하는 소프트웨어 분리를 허용합니다. 또한 일반적인 정보, 분석 및 디버깅 메시지로 사용할 수 있습니다. 시스로그는 멀티플 플랫폼을 통해 다양한 장치와 수신기로 지원됩니다.



#### 웹 인터페이스

웹 인터페이스에서 시스로그 설정을 구성하려면:

1. 이벤트 알림, 로그 및 시스로그를 클릭합니다.
2. 서버 모드를 호출해 활성화 합니다.
3. 서버 주소 및 서버 포트를 포함하는 시스로그 항목을 지정합니다.
4. 적용을 클릭합니다.

#### ■ 항목 설명:

서버 모드 (Server Mode):

서버 모드 동작을 표시합니다. 모드 동작을 활성화 하면 시스로그 메시지는 시스로그 서버에 전송됩니다. 시스로그 프로토콜은 UDP 통신을 기반으로 하며 UDP 포트 514 상에서 수신됩니다. UDP는 비엑세스 프로토콜이며 승인을 제공하지 않으므로 시스로그 서버는 발송자에게 승인을 돌려 보내지 않습니다.

시스로그 패킷은 시스로그 서버가 없더라도 전송됩니다. 가능한 모드는 다음과 같습니다:

Enabled: 서버 모드 동작을 활성화 합니다.

Disabled: 서버 모드 동작을 비활성화 합니다.

서버 주소 (Server Address):

시스로그 서버의 IPv4 주소를 표시합니다. 스위치가 DNS 기능을 제공하면 도메인 이름일 수 있습니다.

서버 포트 (Server Port):

시스로그 서버의 서비스 포트를 표시합니다.

## ■ 버튼

적용 (Apply):

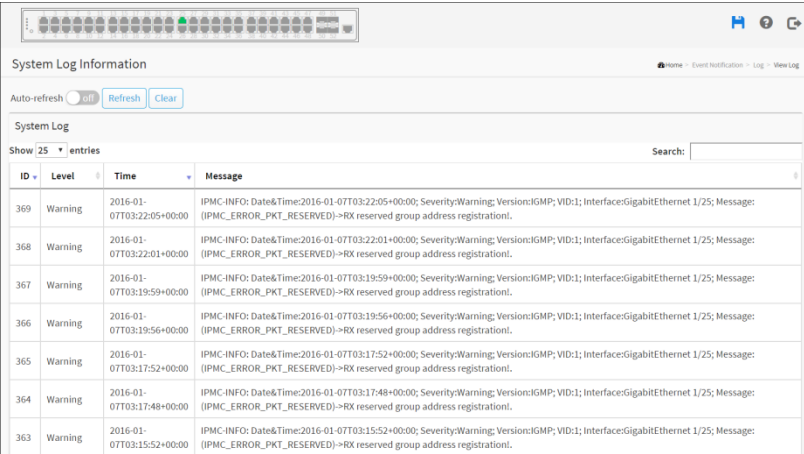
클릭해 변경 사항을 저장합니다.

리셋 (Reset):

로컬에서 생긴 변경 사항을 취소하려면 클릭합니다. 이전 저장 값으로 되돌아 갑니다.

## 로그 보기

이 섹션에서는 스위치의 시스템 로그 정보를 표시를 설명합니다.



| ID  | Level   | Time                      | Message  |
|-----|---------|---------------------------|--|
| 369 | Warning | 2016-01-07T03:22:05+00:00 | IPMC-INFO: Date&Time:2016-01-07T03:22:05+00:00; Severity:Warning; Version:GMP; VID:1; Interface:GigabitEthernet 1/25; Message: (IPMC_ERROR_PKT_RESERVED)->RX reserved group address registrationL. |
| 368 | Warning | 2016-01-07T03:22:01+00:00 | IPMC-INFO: Date&Time:2016-01-07T03:22:01+00:00; Severity:Warning; Version:GMP; VID:1; Interface:GigabitEthernet 1/25; Message: (IPMC_ERROR_PKT_RESERVED)->RX reserved group address registrationL. |
| 367 | Warning | 2016-01-07T03:19:59+00:00 | IPMC-INFO: Date&Time:2016-01-07T03:19:59+00:00; Severity:Warning; Version:GMP; VID:1; Interface:GigabitEthernet 1/25; Message: (IPMC_ERROR_PKT_RESERVED)->RX reserved group address registrationL. |
| 366 | Warning | 2016-01-07T03:19:56+00:00 | IPMC-INFO: Date&Time:2016-01-07T03:19:56+00:00; Severity:Warning; Version:GMP; VID:1; Interface:GigabitEthernet 1/25; Message: (IPMC_ERROR_PKT_RESERVED)->RX reserved group address registrationL. |
| 365 | Warning | 2016-01-07T03:17:52+00:00 | IPMC-INFO: Date&Time:2016-01-07T03:17:52+00:00; Severity:Warning; Version:GMP; VID:1; Interface:GigabitEthernet 1/25; Message: (IPMC_ERROR_PKT_RESERVED)->RX reserved group address registrationL. |
| 364 | Warning | 2016-01-07T03:17:48+00:00 | IPMC-INFO: Date&Time:2016-01-07T03:17:48+00:00; Severity:Warning; Version:GMP; VID:1; Interface:GigabitEthernet 1/25; Message: (IPMC_ERROR_PKT_RESERVED)->RX reserved group address registrationL. |
| 363 | Warning | 2016-01-07T03:15:52+00:00 | IPMC-INFO: Date&Time:2016-01-07T03:15:52+00:00; Severity:Warning; Version:GMP; VID:1; Interface:GigabitEthernet 1/25; Message: (IPMC_ERROR_PKT_RESERVED)->RX reserved group address registrationL. |

웹 인터페이스

웹 인터페이스에서 로그 정보를 표시하려면:

1. 이벤트 알림, 로그 및 로그 보기를 클릭합니다.
2. 로그 정보를 표시합니다.

## ■ 항목 설명:

ID

시스템 로그 엔트리의 ID (>= 1) 입니다.

레벨 (Level):

시스템 로그 엔트리 레벨입니다. 다음의 레벨 타입이 지원됩니다:

Debug: 디버그 레벨 메시지

Info: 정보 메시지

Notice: 정상이나 중요한 상태입니다.

Warning: 경고 상태

Error: 에러 상태

Crit: 위험 상태

Alert: 즉시 실행되어야 하는 동작

Emerg: 시스템이 정상이 아닙니다.

시간 (Time):

장치 시간에 의한 로그 기록을 표시합니다. 시스템 로그 엔트리 시간입니다.

메시지 (Message):

로그 상세 메시지를 표시합니다. 시스템 로그 엔트리 메시지입니다.

검색 (Search):

원하는 정보를 검색합니다.

엔트리 표시 (Show entries):

## ■ 버튼



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh)

페이지를 새로 고침 하려면 클릭합니다.

삭제 (Clear):

페이지 내용을 삭제하려면 클릭하세요.

## 이벤트 설정

이 페이지는 현재 트랩 이벤트 주요 심각도 설정을 표시합니다.

| Group Name       | Severity Level | Syslog                              | Trap                     | SMTP                     |
|------------------|----------------|-------------------------------------|--------------------------|--------------------------|
| ACL              | Info           | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| ACL-Log          | Info           | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Access-Mgmt      | Info           | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Auth-Failed      | Warning        | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Cold-Start       | Warning        | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Config-Info      | Info           | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| DMS              | Info           | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| FAN              | Info           | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Firmware-Upgrade | Info           | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Import-Export    | Info           | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| LACP             | Info           | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

### 웹 인터페이스

웹 인터페이스에서 트랩 이벤트 심각도 정보를 설정하려면:

1. 이벤트 알림 및 이벤트 설정을 클릭합니다.
2. 그룹 이름과 심각도 레벨을 선택하려면 스크롤합니다.
3. 활성화를 클릭해 다른 트랩 이벤트를 선택합니다.
4. 적용을 클릭해 설정을 저장합니다.
5. 설정을 취소하려면 리셋 버튼을 클릭하세요. 이전 저장 값으로 되돌아 갑니다.

### ■ 항목 설명:

그룹 이름 (Group Name):

심각도 그룹을 표시하는 이름입니다.

심각도 레벨 (Severity Level):

각 그룹에는 심각도 레벨이 있습니다. 다음 레벨 타입이 지원됩니다:

<0> Emergency: 시스템을 사용할 수 없습니다.

<1> Alert: 즉시 동작을 실행해야 합니다.

<2> Critical: 위험한 상태입니다.

<3> Error: 에러 상태입니다.

<4> Warning: 경고 상태입니다.

<5> Notice: 정상이나 중요한 상태입니다.

<6> Information: 정보 메시지입니다.

<7> Debug: 디버그-레벨 메시지입니다.

시스로그 (Syslog):

Enable – 시스로그에서 이 그룹 이름을 선택합니다.

트랩 (Trap):

Enable – 트랩에서 이 그룹 이름을 선택합니다.

Switch2go:

Enable – 푸시 알림에서 그룹 이름을 선택합니다.

## ■ 버튼

적용 (Apply):

클릭해 변경 사항을 저장합니다.

리셋 (Reset):

로컬에서 생긴 변경 사항을 취소하려면 클릭합니다. 이전 저장 값으로 되돌아 갑니다.

이 페이지는 의도적으로 비워 두었습니다.



# 16장

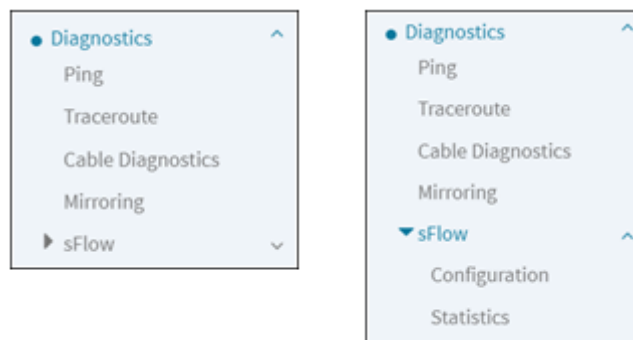
## 진단

### 개요

---

이 챕터는 기본 시스템 진단 세트를 제공합니다. Ping, 추적루트, 케이블 진단 및 포트 미러를 제공합니다.

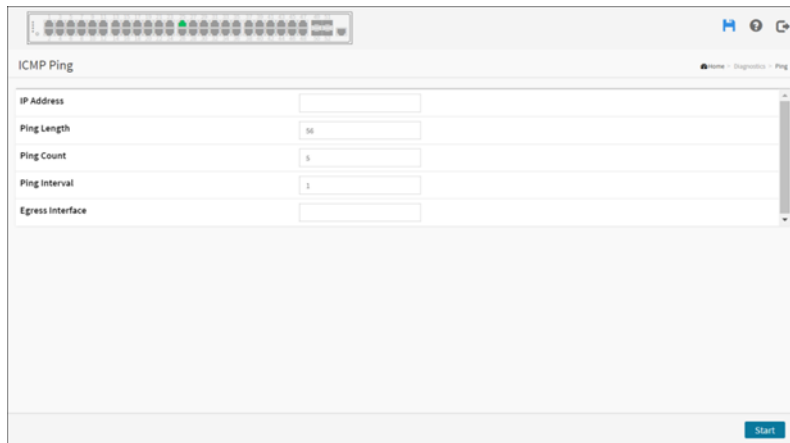
메뉴 및 하위 메뉴는 다음과 같습니다:



## Ping

---

이 섹션에서는 IPv4/6 연결 문제에 대한 해결을 위해 ICMP 에코 패킷을 발행합니다.



### 웹 인터페이스

웹 인터페이스에서 PING을 설정하려면:

1. 진단 및 Ping을 클릭합니다.
2. IP 주소, Ping 길이, Ping 카운트, Ping 간격 및 외부 인터페이스를 지정합니다.
3. 시작을 클릭합니다.

### ■ 항목 설명:

IP 주소 (IP Address):

Ping의 타겟 IP 주소를 지정합니다.

Ping 길이 (Ping Length):

ICMP 패킷의 적재량 크기입니다. 값은 2bytes 에서 1452bytes 범위입니다.

Ping 카운트 (Ping Count):

ICMP 패킷 송비니다. 1번에서 60번의 범위 값입니다.

Ping 간격 (Ping Interval):

ICMP 패킷 간격입니다. 0초에서 30초의 범위 값입니다.

외부 인터페이스 (Egress Interface) (IPv6에 한함):

지정 외부 IPv6 인터페이스의 VLAN ID (VID) 입니다.

1에서 4094DML 주어진 VID 범위이며 해당 IPv6 인터페이스가 유효한 경우에만 효과적입니다.

외부 인터페이스가 없는 경우 PING6는 대상을 위해 가장 적합한 인터페이스를 찾습니다.

루프백 주소에 대한 외부 인터페이스를 지정하지 않습니다.

링크-로컬 또는 멀티캐스트 주소에 대한 외부 인터페이스를 지정합니다.

## ■ 버튼

시작 (Start):

“시작” 버튼을 클릭해 타겟 IP 주소 ping을 시작합니다.

새로운 Ping (New Ping):

ICMP Ping 페이지로 돌아갑니다.

## 추적 경로

이 페이지에서 ICMP, TCP, 또는 UDP 패킷을 발행해 네트워크 연결 문제를 진단합니다.

### 웹 인터페이스

웹 인터페이스에서 추적 경로를 시작하려면:

1. 진단 및 추적 경로를 클릭합니다.
2. IP 주소, 대기 시간, 최대 TTL 및 검색 횟수를 지정합니다.
3. 시작을 클릭합니다.

### ■ 항목 설명:

IP 주소 (IP Address):

대상 IP 주소입니다.

대기 시간 (Wait Time):

검색에 대한 응답 대기 시간을 위한 시간 (초 단위)을 설정합니다. (기본값 5.0초) 1에서 60의 범위 값입니다. ICMP 패킷의 적재량 크기입니다. 2 bytes에서 1452 bytes의 범위 값입니다.

최대 TTL (Max TTL):

추적 경로를 탐색하는 최대 홑 수 (max time-to-live value)를 지정합니다. 1에서 255의 범위 값입니다. 기본값은 30입니다.

검색 횟수 (Probe Count):

홑 당 검색 패킷 수를 설정합니다. 1에서 10의 범위 값입니다. 기본값은 3입니다.

## ■ 버튼

시작 (Start):

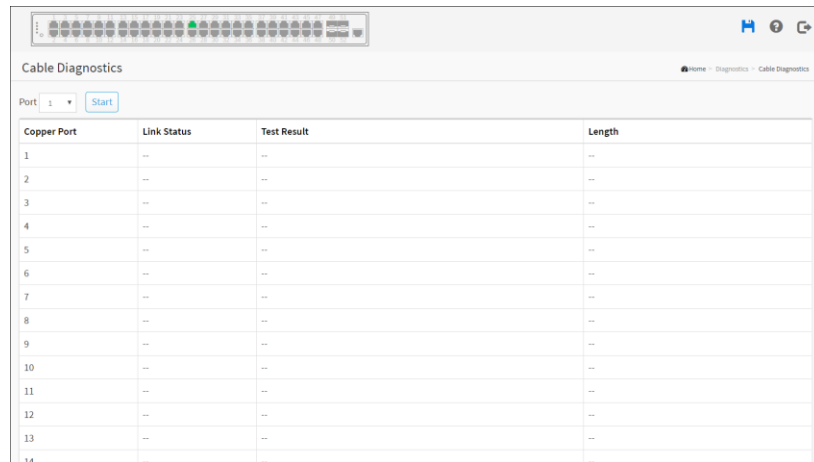
“시작” 버튼을 클릭해 타겟 IP 주소 ping을 시작합니다.

새로운 추적 경로 (New Traceroute):

추적 경로 페이지로 돌아갑니다.

## 케이블 진단

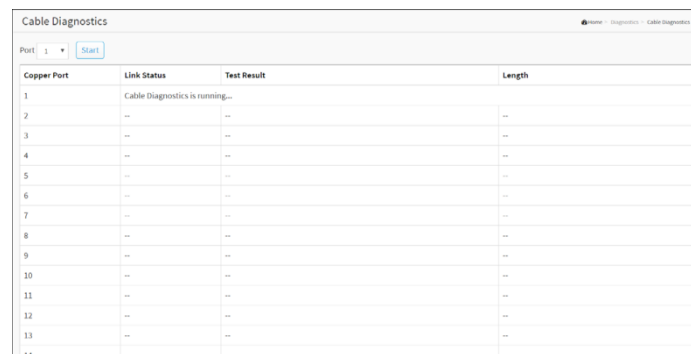
이 섹션에서 구리 포트에 대한 케이블 진단 동작 방법을 표시합니다.



### 웹 인터페이스

웹 인터페이스에서 케이블 진단 설정을 구성하려면:

1. 진단 및 케이블 진단을 클릭합니다.
2. 체크하고자 하는 포트를 지정합니다.
3. 시작을 클릭합니다.



### ■ 항목 설명:

포트 (Port):

케이블 진단이 필요한 포트입니다.

구리 포트 (Copper Port):

구리 포트 번호입니다.

링크 상태 (Link Status):

케이블 상태입니다.

10M: 케이블이 바르게 연결되었습니다. 속도는 10Mbps 입니다.

100M: 케이블이 바르게 연결되었습니다. 속도는 100Mbps 입니다.

1G: 케이블이 바르게 연결되었습니다. 속도는 1Gbps 입니다.

Link Down: 연결되지 않았거나 케이블이 바르지 않습니다.

테스트 결과 (Test Result):

케이블 테스트 결과입니다.

OK: 바르게 종료된 페어입니다.

Abnormal: 잘못 종료된 페어 또는 연결이 되지 않습니다.

길이 (Length):

케이블 페어의 길이 (미터 단위) 입니다. 해상도는 3m입니다. 링크 상태가 다음과 같이 표시됩니다. 길이에선 다양한 정의가 있습니다.

1G: 길이는 4-pair 최소 값입니다.

10M/100M: 길이는 2-pair 최소 값입니다.

Link Down: 길이는 4-pair, 0의 최소 값입니다.

## ■버튼

시작 (Start):

선택한 포트의 케이블 진단을 시작합니다.

## 미러링

실시간 분석을 위해 모든 소스 포트에서 타겟 포트에 트래픽을 미러링할 수 있습니다. 논리적 분석기 또는 RMON 검색을 타겟 포트에 연결할 수 있으며, 완전히 비간접적인 방식으로 소스 포트 간 트래픽을 조사합니다.

미러 설정은 네트워크 트래픽을 모니터링 하는 것 입니다. 예를 들어, 포트 A와 포트 B가 각각 모니터링 포트와 모니터링 된 포트라고 추정합니다. 따라서 포트 B에 의해 수신된 트래픽이 모니터링을 위해 포트 A로 복제될 것 입니다.

| Port | Mode     |
|------|----------|
| 1    | Disabled |
| 2    | Disabled |
| 3    | Disabled |
| 4    | Disabled |
| 5    | Disabled |
| 6    | Disabled |
| 7    | Disabled |

### 웹 인터페이스

웹 인터페이스에서 포트 미러 기능을 설정하려면:

1. 진단 및 미러링을 클릭합니다.
2. 모니터링 대상 포트를 선택합니다. (미러 포트)
3. 각 모니터링 된 포트에 대한 모드(disabled, enable, TX Only 및 RX only)를 선택합니다.
4. 적용 버튼을 클릭해 설정을 저장합니다.
5. 설정을 취소하고자 하는 경우 리셋 버튼을 클릭해 이전 저장된 값으로 되돌아 갑니다.



## ■ 항목 설명:

모니터링 대상 포트 (Monitor Destination Port):

미러링 된 트래픽을 출력하기 위한 포트입니다. 또한 미러 포트로도 알려져 있습니다. 활성화 된 소스 (rx) 또는 대상 (tx) 미러링을 가진 포트에서 프레임이 이 포트 상에 미러링 됩니다.

미러 소스 포트 설정 (Mirror Source Port Configuration)

다음의 테이블은 Rx 및 Tx 활성화에 사용됩니다.

포트 (Port):

동일한 열에 포함된 설정에 대한 논리적 포트입니다.

모드 (Mode):

미러 모드를 선택합니다.

Rx only: 이 포트에 수신된 프레임이 미러 포트에 미러링 됩니다. 전송된 프레임이 미러링 되지 않습니다.

Tx only: 이 포트에 전송된 프레임이 미러 포트에 미러링 됩니다. 수신된 포트는 미러링되지 않습니다.

Disabled: 전송된 프레임과 수신된 프레임 모두 미러링 되지 않습니다.

Enabled: 수신 또는 전송된 프레임이 미러 포트에 미러링 됩니다.

## ■ 버튼

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

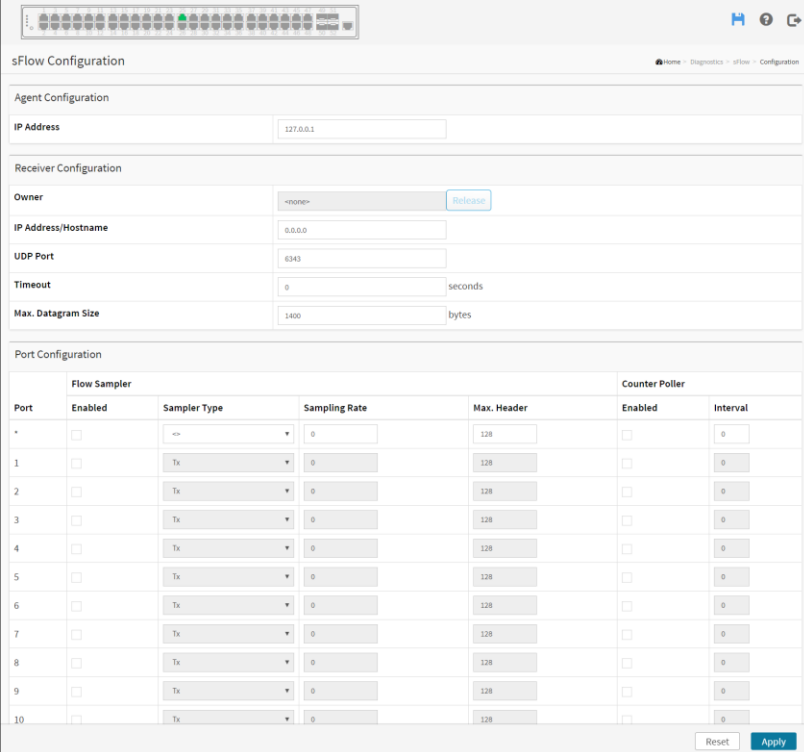
로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

## sFLOW

### 설정

스위치에 대한 sFlow 콜렉터 설정을 이 곳에서 모니터링 할 수 있고 수정할 수 있습니다. 설정은 2개의 부분으로 나뉘어 집니다: sFlow 수신기 (sFlow 콜렉터) 및 포트당 흐름과 카운터 샘플러 설정입니다.

sFlow 설정은 비휘발성 메모리를 지속하지 않습니다. 리부트 또는 마스터 변경이 sFlow 샘플링을 비활성화 할 것 입니다.



The screenshot shows the 'sFlow Configuration' web interface. It is divided into three main sections: Agent Configuration, Receiver Configuration, and Port Configuration.

**Agent Configuration:** IP Address is set to 127.0.0.1.

**Receiver Configuration:** Owner is set to 'none' with a 'Release' button. IP Address/Hostname is 0.0.0.0, UDP Port is 6343, Timeout is 0 seconds, and Max. Datagram Size is 1400 bytes.

**Port Configuration:** A table with columns for Port, Flow Sampler (Enabled), Sampler Type, Sampling Rate, Max. Header, Counter Poller (Enabled), and Interval. The table lists ports 1 through 10, all with 'Tx' as the sampler type and a sampling rate of 0. The Counter Poller is disabled for all ports.

| Port | Flow Sampler             |  | Sampler Type | Sampling Rate | Max. Header | Counter Poller           |          |
|------|--------------------------|--|--------------|---------------|-------------|--------------------------|----------|
|      | Enabled                  |  |              |               |             | Enabled                  | Interval |
| *    | <input type="checkbox"/> |  | <>           | 0             | 128         | <input type="checkbox"/> | 0        |
| 1    | <input type="checkbox"/> |  | Tx           | 0             | 128         | <input type="checkbox"/> | 0        |
| 2    | <input type="checkbox"/> |  | Tx           | 0             | 128         | <input type="checkbox"/> | 0        |
| 3    | <input type="checkbox"/> |  | Tx           | 0             | 128         | <input type="checkbox"/> | 0        |
| 4    | <input type="checkbox"/> |  | Tx           | 0             | 128         | <input type="checkbox"/> | 0        |
| 5    | <input type="checkbox"/> |  | Tx           | 0             | 128         | <input type="checkbox"/> | 0        |
| 6    | <input type="checkbox"/> |  | Tx           | 0             | 128         | <input type="checkbox"/> | 0        |
| 7    | <input type="checkbox"/> |  | Tx           | 0             | 128         | <input type="checkbox"/> | 0        |
| 8    | <input type="checkbox"/> |  | Tx           | 0             | 128         | <input type="checkbox"/> | 0        |
| 9    | <input type="checkbox"/> |  | Tx           | 0             | 128         | <input type="checkbox"/> | 0        |
| 10   | <input type="checkbox"/> |  | Tx           | 0             | 128         | <input type="checkbox"/> | 0        |

Buttons: Reset, Apply

### 웹 인터페이스

웹 인터페이스에서 sFlow를 설정하려면:

1. 진단, sFlow 및 설정을 클릭합니다.
2. sFlow 항목을 설정합니다.

3. 적용을 클릭해 설정을 저장합니다.
4. 설정을 취소하고자 하는 경우 리셋 버튼을 클릭해 이전 저장된 값으로 되돌아 갑니다.

## ■ 항목 설명:

### 에이전트 설정

IP 주소 (IP Address):

SFlow 데이터그램에서 에이전트 IP 주소로 사용되는 IP 주소입니다. 확장된 시간을 통해 에이전트를 표시할 고유 키로써의 역할을 합니다.

IPv4와 IPv6 주소 모두 지원됩니다.

### 수신기 설정

소유자 (Owner):

기본적으로 sFlow는 2가지 방법으로 설정됩니다. 웹 또는 CLI 인터페이스를 이용한 로컬 매니저먼트를 통하거나 SNMP를 이용합니다. 이 읽기 전용 필드는 현재 sFlow 설정 소유자를 표시하며 다음과 같은 값을 추정합니다:

- SFlow가 현재 미설정/소유자 미확인 상태이면, 소유자는 <none>을 포함합니다.
- SFlow가 현재 웹 또는 CLI를 통해 설정된 상태이면, 소유자는 <Configured through local management>를 포함합니다.
- SFlow가 현재 SNMP를 통해 설정된 상태이면, 모든 제어 – 릴리즈 버튼 제외 – 가 비활성화되어 의도하지 않은 재설정을 방지합니다.

릴리즈 버튼을 이용해 현재 소유자를 해제하고, sFlow 샘플링을 비활성화 합니다. 현재 sFlow가 소유자 미확인 상태이면 버튼이 비활성화 됩니다. SNMP를 통해 설정되면 해제가 확인됩니다. (확인 요청이 나타납니다.)

IP 주소/호스트 이름 (IP Address/Hostname):

sFlow 수신기의 IP 주소 또는 호스트이름입니다. IPv4와 IPv6 주소 모두 지원됩니다.

UDP 포트 (UDP Port):

sFlow 수신기가 sFlow 다이어그램을 받아들이는 UDP 포트입니다. 0으로 설정하면 기본 포트 (6343)이 사용됩니다.

타임아웃 (Timeout):

샘플링 전 남아있는 초 단위 시간이 멈추고 현재의 sFlow 소유자를 해제합니다. 동작하는 동안, 현재 남은 시간을 새로 고침 버튼을 클릭해 업데이트 할 수 있습니다.

로컬에서 관리되는 경우 타임아웃은 다른 설정에 영향을 미치지 않고 상황에 맞게 변경할 수 있습니다.

최대 데이터그램 크기 (Max. Datagram Size):

싱글 샘플 데이터그램에서 전송 가능한 데이터 바이트 최대 수입입니다. 이 것은 sFlow 데이터그램 해체를 방지하는 값으로 설정되어야 합니다. 유효 범위는 200에서 1468 바이트이며 기본값은 1400바이트입니다.

### **포트 설정**

포트 (Port):

다음의 설정을 적용하는 포트 번호입니다.

활성화 된 플로우 샘플러 (Flow Sampler Enabled):

이 포트의 플로우 샘플링을 활성화/비활성화 합니다.

플로우 샘플러 샘플링 속도(Flow Sampler Sampling Rate) :

패킷 샘플링에 대한 통계 샘플링입니다. N으로 설정해 포트 상에 전송/수신된 패킷의 1/N 평균을 시도합니다.

모든 샘플링 속도가 가능하지는 않습니다. 지원되지 않는 샘플링 속도가 요청되면, 스위치는 자동으로 가장 가능한 값으로 조정합니다. 이 필드로 다시 돌아갑니다.

플로우 샘플러 최대 헤더 (Flow Sampler Max. Header):

샘플링 된 패킷에서 sFlow 데이터그램으로 복제되어야 하는 바이트 최대 수입입니다. 유효 범위는 14에서 2000 바이트이면 기본 값은 128바이트입니다.

최대 데이터그램 사이즈가 최대 헤더 크기를 고려하지 않는 경우 샘플은 삭제됩니다.

활성화 된 카운터 폴러 (Counter Poller Enabled):

이 포트의 카운터 폴링을 활성화/비활성화 합니다.

카운터 폴러 간격 (Counter Poller Interval):

카운터 폴링 활성화 되어, 카운터 폴러 샘플 간 간격 -초 단위 -을 지정합니다.

### **■버튼**

적용 (Apply):

변경 사항을 저장하려면 클릭하세요.

리셋 (Reset):

로컬에서 만든 변경 사항을 취소하려면 이전에 저장된 값으로 되돌아 갑니다.

릴리즈 (Release):

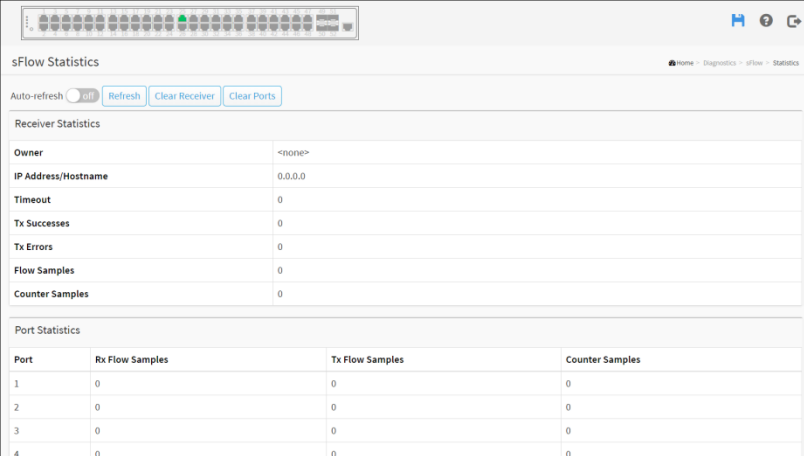
소유자 아래의 설명을 표시합니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고칩니다. 저장되지 않은 변경이 손실되는 것을 주의하십시오.

## 현황

이 세션은 수신기 및 포트 당 sFlow 상태를 표시합니다.



The screenshot shows the 'sFlow Statistics' page in a web interface. At the top, there's a navigation bar with 'Home', 'Diagnostics', 'sFlow', and 'Statistics'. Below the navigation bar, there are buttons for 'Auto-refresh' (set to 10s), 'Refresh', 'Clear Receiver', and 'Clear Ports'. The main content area is divided into two sections: 'Receiver Statistics' and 'Port Statistics'.

**Receiver Statistics**

|                     |         |
|---------------------|---------|
| Owner               | <none>  |
| IP Address/Hostname | 0.0.0.0 |
| Timeout             | 0       |
| Tx Successes        | 0       |
| Tx Errors           | 0       |
| Flow Samples        | 0       |
| Counter Samples     | 0       |

**Port Statistics**

| Port | Rx Flow Samples | Tx Flow Samples | Counter Samples |
|------|-----------------|-----------------|-----------------|
| 1    | 0               | 0               | 0               |
| 2    | 0               | 0               | 0               |
| 3    | 0               | 0               | 0               |
| 4    | 0               | 0               | 0               |

웹 인터페이스

웹 인터페이스에서 포트 sFlow 통계를 표시하려면:

1. 진단, sFlow 및 통계를 클릭합니다.
2. SFlow 정보를 표시합니다.

## ■ 항목 설명:

### 수신기 상태

이 필드는 sFlow 설정의 현재 소유자를 표시합니다. 다음의 3개 값 중 하나를 추정합니다.

- SFlow가 현재 미설정/소유자 미확인 상태이면, 소유자는 <none>을 포함합니다.
- SFlow가 현재 웹 또는 CLI를 통해 설정된 상태이면, 소유자는 <Configured through local management>를 포함합니다.

- SFlow가 현재 SNMP를 통해 설정된 상태이면, 모든 제어 – 릴리즈 버튼 제외 – 가 비활성화되어 의도하지 않은 재설정을 방지합니다.

IP 주소/호스트 이름 (IP Address/Hostname):

IP 주소 또는 SFlow 수신기의 호스트 이름입니다.

타임아웃 (Timeout):

샘플링 전 남은 초 단위 시간이며 현재 sFlow 소유자가 해제됩니다.

Tx 성공 (Tx Successes):

sFlow 수신기에 전송된 성공적인 UDP 데이터그램 수입입니다.

Tx 에러 (Tx Errors):

전송 실패한 UDP 데이터그램 수입입니다.

가장 일반적인 에러 소스는 유효하지 않은 sFlow 수신기 IP/호스트이름 설정입니다. 진단을 위해 수신기의 IP 주소/호스트이름을 Ping 웹 페이지에 붙여넣습니다. (진단→ Ping/Ping6)

플로우 샘플 (low Samples):

sFlow 수신기에 전송된 플로우 샘플 전체 수입입니다.

카운터 샘플 (Counter Samples):

### **포트 상태**

포트 (Port):

다음의 통계를 적용할 포트 번호입니다.

Rx 및 Tx 플로우 샘플 (Rx and Tx Flow Samples):

포트에서 비롯된 sFlow 수신기에 전송된 플로우 샘플 수 입니다. 여기 플로우 샘플은 Rx와 Tx 플로우 샘플로 나뉘며, Rx 플로우 샘플은 포트에 샘플링 된 수신 상태 (내부)인 패킷 수를 포함합니다. 그리고 Tx 플로우 샘플은 포트의 샘플링 된 전송 상태 (외부)인 패킷 수를 포함합니다.

카운터 샘플 (Counter Samples):

포트에서 비롯된 sFlow 수신기에 전송된 카운터 샘플 전체 수 입니다.

### **■ 버튼**



자동 새로 고침 (Auto-refresh):

이 박스를 체크해 페이지를 자동으로 새로 고칩니다. 자동 새로 고침은 3초마다 실행됩니다.

새로 고침 (Refresh):

클릭해 페이지를 새로 고칩니다. 저장되지 않은 변경이 손실되는 것을 주의하십시오.

수신기 삭제 (Clear Receiver):

sFlow 수신기 카운터를 삭제합니다.

포트 삭제 (Clear Ports):

포트 당 카운터를 삭제합니다.

이 페이지는 의도적으로 비워 두었습니다.



# 17장

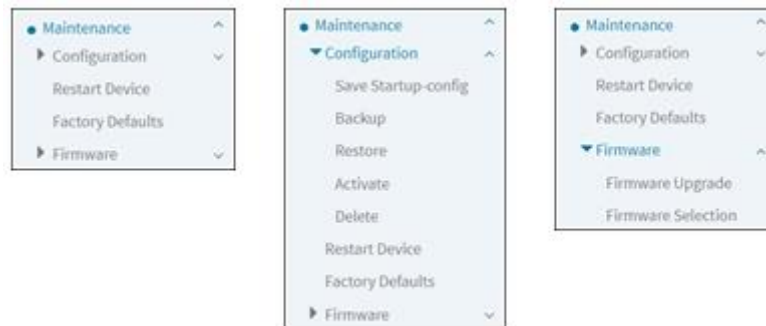
## 유지보수

### 개요

---

이 장에서는 저장/백업/복구/활성화/재시작 장치 삭제, 공장 초기값, 펌웨어 업그레이드를 포함한 전반적인 유지보수 설정 동작을 설명합니다.

메뉴와 하위 메뉴는 다음과 같습니다:



## 설정

---

스위치는 글자 형식의 파일에서 설정을 저장합니다. 파일은 버추얼 (RAM 기본) 이거나 스위치의 플래시에 저장됩니다.

3개의 파일 시스템이 있습니다:

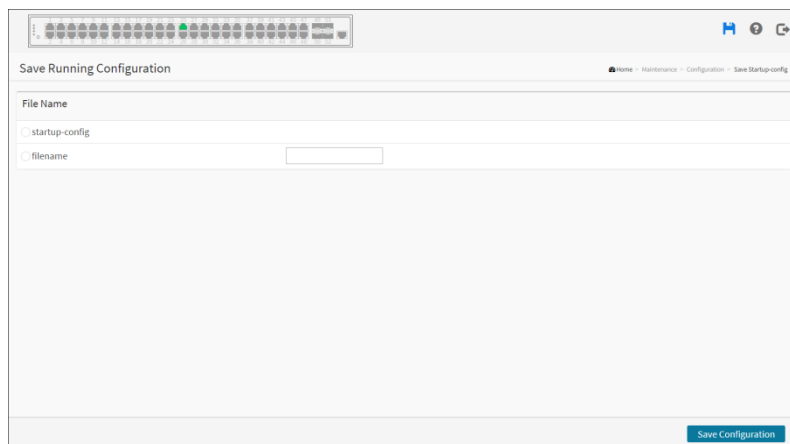
running-config: 현재 스위치 상에 동작 중인 설정을 나타내는 버추얼 파일입니다. 이 파일은 불안정합니다.

startup-config: 스위치에 대한 시작 설정입니다. 부팅 시간을 읽습니다.

default-config: 벤더 지정 설정의 읽기 전용 파일입니다. 시스템이 기본값 설정으로 다시 복구되었을 때 이 파일이 읽힙니다.

### startup-config 저장

running-config를 startup-config 로 복사합니다. 그렇게 함으로써 현재 동작 중인 설정이 다음 재부팅에서 사용될 수 있습니다.



웹 인터페이스

웹 인터페이스에서 동작중인 설정을 저장하려면:

1. 유지보수, 설정 및 startup-config 저장을 클릭합니다.
2. 설정 저장을 클릭합니다.

### ■버튼

설정 저장 (Save Configuration):

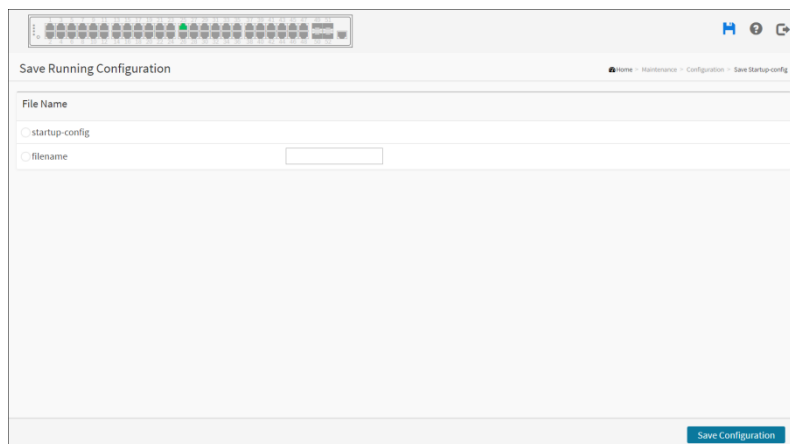
클릭해 설정을 저장합니다. 동작 중인 설정은 이 시작 설정 파일 로드하기 위해 시스템 부팅을 위한 플래시 메모리에 기록됩니다.

## 백업

이 섹션은 유지보수 필요에 대한 스위치 설정을 내보내는 방법을 설명합니다. 현재 설정 파일이 텍스트 형식으로 보내집니다.

스위치의 설정 파일은 동작 중인 웹 브라우저의 스테이션 상에서 백업 및 저장 가능합니다.

스위치의 어떠한 파일도 웹 브라이우저 전송이 가능합니다. 파일은 백업 전 준비가 되어 있어야 하므로, running-config 선택 완료에 시간이 걸릴 것 입니다.



웹 인터페이스

웹 인터페이스에서 설정을 백업하려면:

1. 유지보수, 설정 및 백업을 클릭합니다.
2. 백업을 클릭합니다.

### ■ 항목 설명:

running-config:

현재 스위치 상에 동작 중인 설정을 표시하는 버추얼 파일입니다.

startup-config:

스위치에 대한 시작 설정입니다. 부팅 시간을 읽습니다.

default-config:

벤더 지정 설정의 읽기 전용 파일입니다. 시스템이 기본값 설정으로 다시 복구되었을 때 이 파일이 읽힙니다.

## ■ 버튼

다운로드 설정 (Download Configuration):

버튼을 클릭하면 스위치는 설정 파일을 워크스테이션에 전송할 준비를 시작할 것입니다.

## 복구

웹 브라우저에서 읽기 전용인 default-config을 제외한 스위치의 모든 파일을 가져올 수 있습니다.

복구를 하려면 소스 파일을 선택하고 타겟의 대상 파일을 선택합니다.

대상이 running-config인 경우 파일은 스위치 설정에 적용될 것입니다. 이는 2가지 방법으로 실행할 수 있습니다:

Replace mode: 현재 설정이 소스 파일에 지정된 설정과 완전히 교체됩니다.

Merge mode: 소스 파일 설정이 running-config과 합쳐집니다.

| File Name                             | Parameters   |
|---------------------------------------|--|
| <input type="radio"/> running-config  | <input checked="" type="radio"/> Replace <input type="radio"/> Merge |
| <input type="radio"/> files.zip       |  |
| <input type="radio"/> icon_list       |  |
| <input type="radio"/> Create new file |  |

## 웹 인터페이스

웹 인터페이스에서 설정을 복구하려면:

1. 유지보수, 설정 및 복구를 클릭합니다.
2. 복구를 클릭합니다.

3. 파일 선택을 클릭하고 파일을 선택합니다.
4. 설정 업로드를 클릭합니다.

### ■ 항목 설명:

running-config:

현재 스위치 상에 동작 중인 설정을 표시하는 버추얼 파일입니다. 이 파일은 불안정합니다.

교체 모드 (Replace mode):

현재 설정이 업로드 된 파일의 설정과 완전히 교체됩니다.

병합 모드 (Merge mode):

업로드 파일이 running-config과 합쳐집니다.

startup-config:

스위치에 대한 시작 설정입니다. 부팅 시간을 읽습니다.

새 파일 생성 (Create new file):

새 파일을 생성합니다.

### ■ 버튼

검색 (Browse):

버튼을 클릭해 설정 텍스트 파일과 파일 이름을 검색합니다.

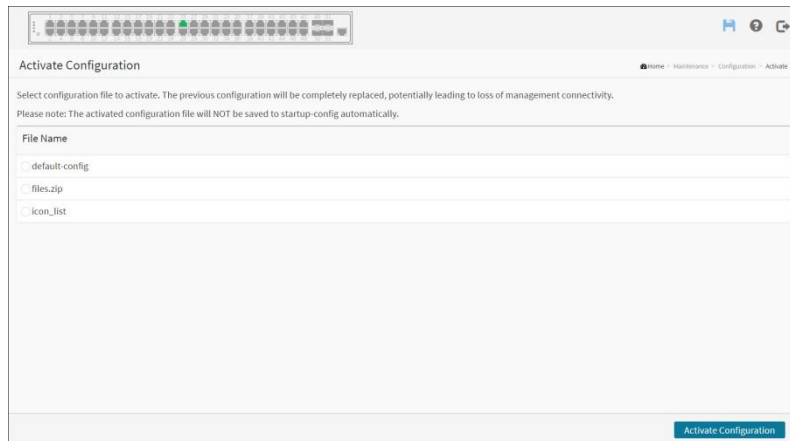
설정 업로드 (Upload Configuration):

버튼을 클릭해 소스 파일에서 대상 파일로 전송을 시작합니다.

### 활성화

현재 동작 중인 설정을 표시하는 running-config를 제외한 스위치의 모든 설정 파일을 활성화 할 수 있습니다.

활성화 하려면 파일을 선택하고 클릭합니다. 기존 설정을 선택된 파일로 완전히 교체하는 프로세스를 초기화 할 것 입니다.



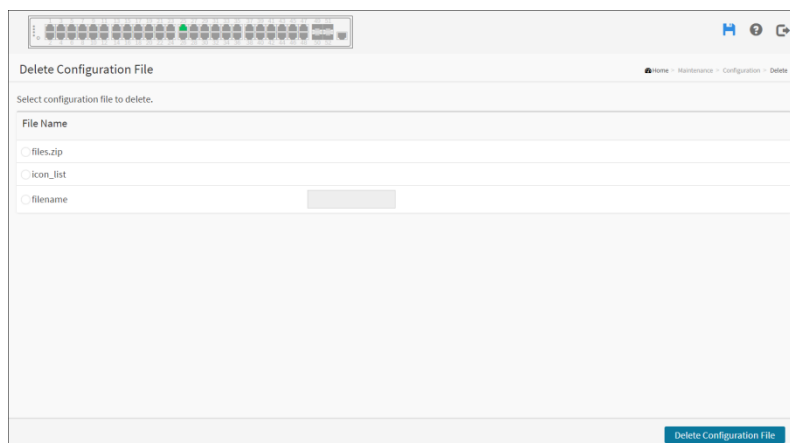
## 웹 인터페이스

웹 인터페이스 설정을 활성화 하려면:

1. 유지보수, 설정 및 활성화를 클릭합니다.
2. 활성화 하려는 동작을 선택합니다.
3. 활성화 설정을 클릭하세요.

## 삭제

startup- config를 포함해 플래시에 저장된 쓰기 가능한 모든 파일을 삭제할 수 있습니다. 완료되면 스위치는 저장 동작 없이 재부팅 되어 효과적으로 스위치를 기본 설정으로 리셋합니다.



#### 웹 인터페이스

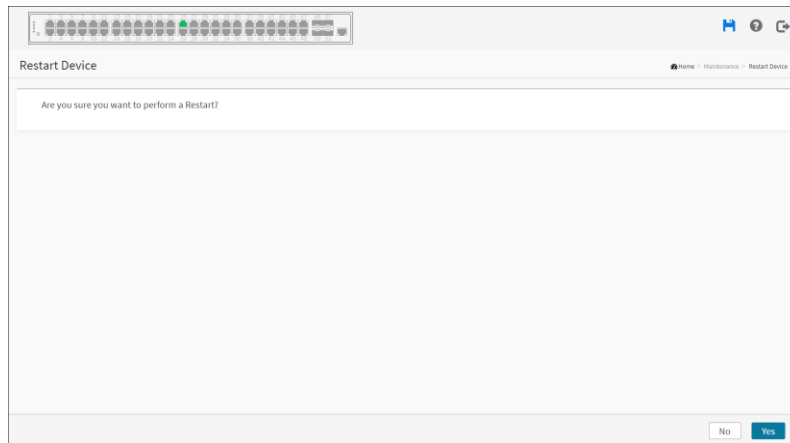
웹 인터페이스에서 설정을 삭제하려면:

1. 유지보수, 설정 및 삭제를 클릭합니다.
2. 삭제하고자 하는 설정을 선택합니다.
3. 설정 파일 삭제를 클릭합니다.

## 장치 재시작

---

이 섹션에서 모든 유지 보수 필요로 인해 장치를 재시작하는 방법을 기술합니다. 스위치에 저장한 모든 설정 파일 또는 스크립트는 그 후에 가능합니다.



웹 인터페이스

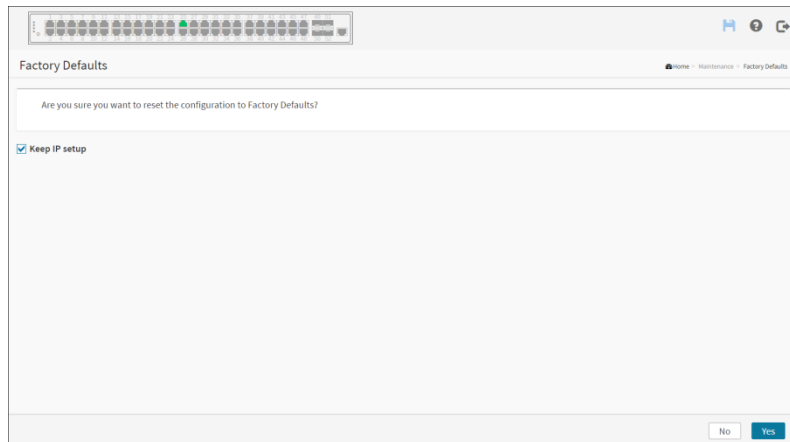
웹 인터페이스의 장치 재시작을 시작하려면:

1. 유지보수 및 장치 재시작을 클릭합니다.
2. Yes를 클릭합니다.



## 공장 초기값

이 섹션에서는 공장 초기값으로 스위치 설정을 복구하는 방법을 설명합니다.



웹 인터페이스

웹 인터페이스에서 공장 초기값으로 복구하려면:

1. 유지보수 및 공장 초기값을 클릭합니다.
2. IP 설정 옵션 유지를 체크해 IP 설정을 유지하려면 선택할 수 있습니다.
3. Yes를 클릭합니다.

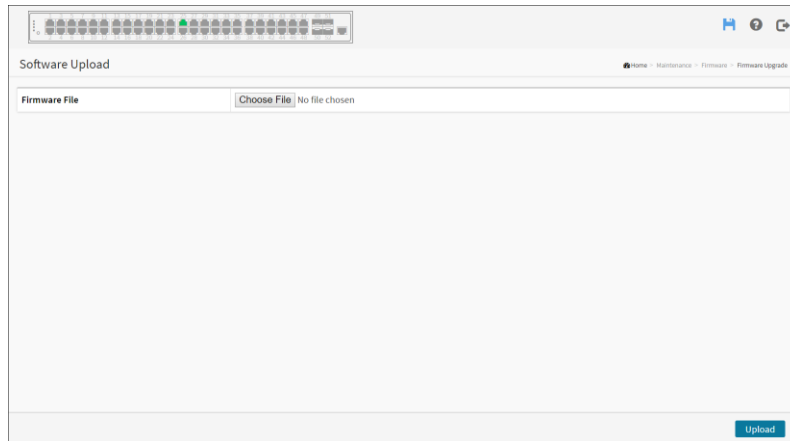
## 펌웨어

---

이 섹션에서는 펌웨어 업그레이드(업데이트) 방법을 설명합니다.

### 펌웨어 업그레이드

이 페이지는 스위치를 제어하는 펌웨어 업데이트를 용이하게 합니다.



웹 인터페이스

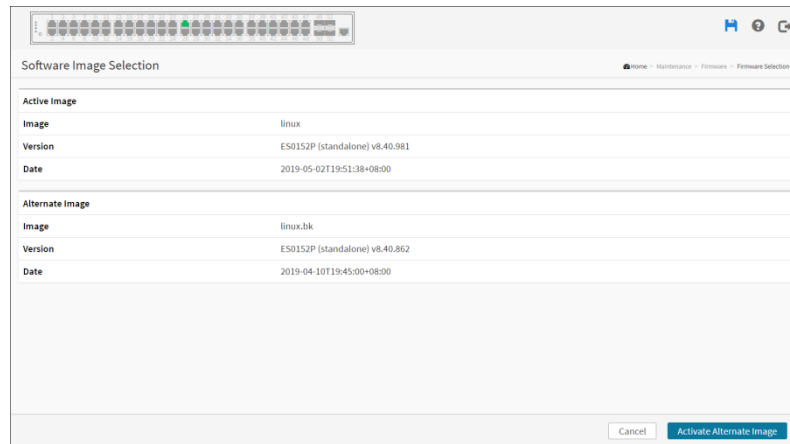
웹 인터페이스에서 장치의 펌웨어를 업데이트 하려면:

1. 유지보수, 펌웨어 및 펌웨어 업그레이드를 클릭합니다.
2. 파일 선택을 클릭해 파일을 선택하세요.
3. 업로드를 클릭합니다.

### 펌웨어 선택

이 페이지에서는 스위치에서 장치의 동작 중이거나 대체 (백업) 펌웨어 이미지에 대한 정보를 제공하며 대체 이미지를 작동합니다.

웹 페이지는 동작 및 대체 펌웨어 이미지에 대한 정보를 가진 2개의 테이블을 표시합니다.



## 웹 인터페이스

웹 인터페이스에서 펌웨어 정보 또는 부팅 펌웨어 교체를 표시하려면:

1. 유지보수, 펌웨어 및 펌웨어 선택을 클릭합니다.
2. 대체 이미지 활성화를 클릭합니다.

## 이미지 정보

이미지 (Image):

이미지가 마지막으로 업데이트 된 이후의 펌웨어 이미지 파일 이름입니다.

버전 (Version):

펌웨어 이미지 버전입니다.

데이트 (Date):

펌웨어가 생성된 날짜입니다.

이 페이지는 의도적으로 비워 두었습니다.

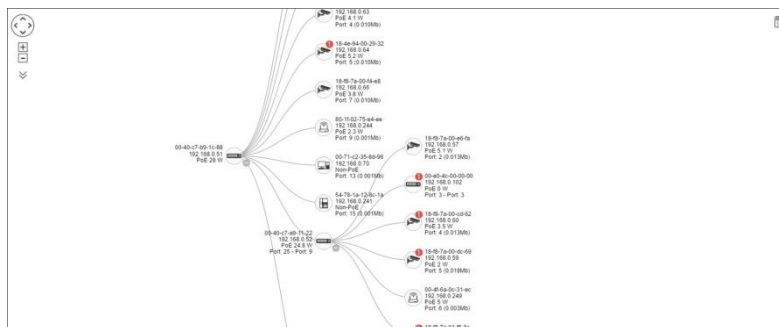
## 장치 매니지먼트 시스템 (DMS)

## 개요

1. DMS는 스위치에 내장된 지능적인 매니지먼트 툴이며 직관적으로 IT/TS가 비용/시간/노력을 줄이는데 도움이 도비니다.
2. LDDP, UPnP, ONVIF, Bonjour 등을 포함한 표준 네트워킹 프로토콜을 사용하는 DMS로 자동으로 스위치에 연결된 모든 장치를 발견하고 표시할 수 있습니다.
3. 유저는 유저는 직관적인 웹 GUI를 통해 다음의 기능을 동작할 수 있습니다.
  - ◆ 원격으로 IP 카메라, NVR, 또는 모든 PoE 장치 전원 끄기
  - ◆ 손상된 케이블 위치를 원격에서 식별
  - ◆ IP 카메라/NVR의 비정상 트래픽 문제를 탐지
  - ◆ 직관적으로 장치 상태를 모니터링, 예: 링크, PoE 전원, 트래픽 등
  - ◆ 우수한 솔루션 품질/신뢰성을 위한 직관적으로 VLAN/QoS 설정
4. DMS는 4 서브넷 이내의 최대 256 장치를 지원합니다.

내장된 장치 관리 시스템은 기업 애플리케이션을 위한 IP 폰, IP 캠 또는 Wifi-AP을 매우 쉽게 이용/관리/설치할 수 있도록 설계되었습니다.

유저는 ip 장치를 토폴로지/플로어/설치 장소 맵 뷰를 통해 IP 장치를 배치할 수 있습니다. 그리고 진단 및 트래픽 모니터를 통해, 링크 상태 확인 및 처리량을 모니터링도 할 수 있습니다.



메인 메뉴는 다음과 같습니다:



## 매니지먼트

매니지먼트 메뉴는 다음과 같습니다.



### DMS 모드

 A screenshot of the 'DMS Mode' configuration page. The page has a title 'Information' and a breadcrumb 'Home > DMS Mode'. It contains several configuration items:
 

|                     |             |
|---------------------|-------------|
| Mode                | Enabled     |
| Controller Priority | Low         |
| Total Device        | 9           |
| On-line Devices     | 9           |
| Off-line Devices    | 0           |
| Controller IP       | 192.168.0.1 |

 At the bottom right, there is a blue 'Apply' button.

- ◆ DMS 모드: DMS 기능을 활성화 / 비활성화 합니다. 또는 “우선 순위”를 선택할 수 있으므로, 장치가 마스터 스위치가 됩니다.
- ◆ Total Device: 이 곳에서는 토폴로지 뷰에 탐지 및 표시되는 IP 장치 수를 나타냅니다.
- ◆ On-Line Devices: 이 곳에서는 토폴로지 뷰에 온라인 상태인 IP 장치 수를 나타냅니다.
- ◆ Off-Line Device: 이 곳에서는 토폴로지 뷰에 오프라인 상태인 IP 장치 수를 나타냅니다.
- ◆ Controller IP: 마스터 IP를 표시합니다.

## **맵 API 키**

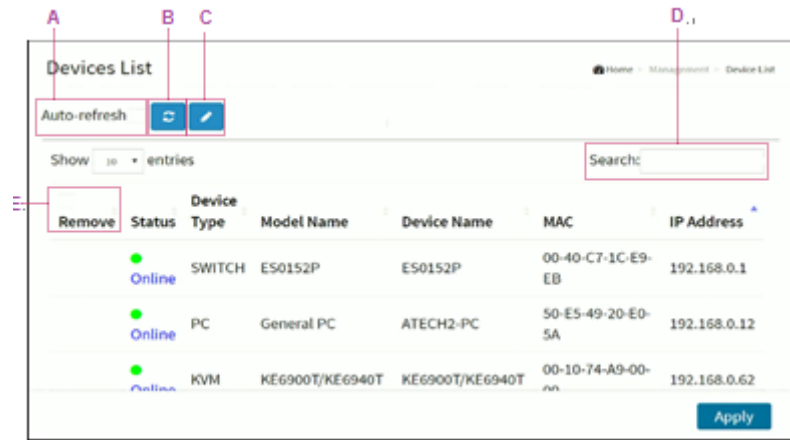
구글 맵 플랫폼 발표에 따라, 구글 주요 제품 액세스를 하려면 2018 6월 11일부터 유효한 API 키와 구글 클라우드 플랫폼 청구 계정이 필요합니다. 청구를 활성화 하면, 구글 맵, 경로 및 장소 사용을 하기 위한 매월 \$200 사용 액세스를 얻을 수 있습니다.

*맵 보기*에서 맵 기능을 사용하려면 API 키 포함하고 이 페이지의 키 필드에 API 키를 입력한 후 **적용**을 클릭합니다.



## 장치 목록

DMS로 탐지되는 모든 장치와 정보를 표시합니다.





- a) ☐ Auto-refresh 정보를 새로 고침하려면 "자동 새로고침"을 사용합니다.
- b) 이 아이콘을 클릭해 모든 장치 상태를 새로고침합니다.
- c) 이 아이콘을 클릭해 장치 이름 및 http 포트를 편집합니다.

유저는 "Edit" 아이콘을 눌러 각 IP 장치에 대해 장치 이름을 편집하고 HTTP 포트를 편집합니다. 이 기능은 또한 토폴로지 뷰의 대시보드에 설정될 수 있습니다.

미확인 장치 및 PC 타입 장치에 대한 HTTP 연결 기능이 없으므로, UI는 이 설정에 대해 "HTTP 포트 편집" 기능을 제공하지 않습니다.



- d)   전체 글자 검색의 키 글자로 장치를 검색합니다.
- e)  오프라인 장치만 "Remove" 기능을 제공해 DMS 장치 목록에서 제거할 수 있습니다.

---

**주의:** 장치 이름은 적용 버튼을 누르기 전까지 저장되지 않습니다. 새 장치 이름을 적용하기 전까지 새로 고침, 자동-새로 고침을 또는 편집 버튼을 클릭하지 마십시오.

---

## 그래픽 모니터링

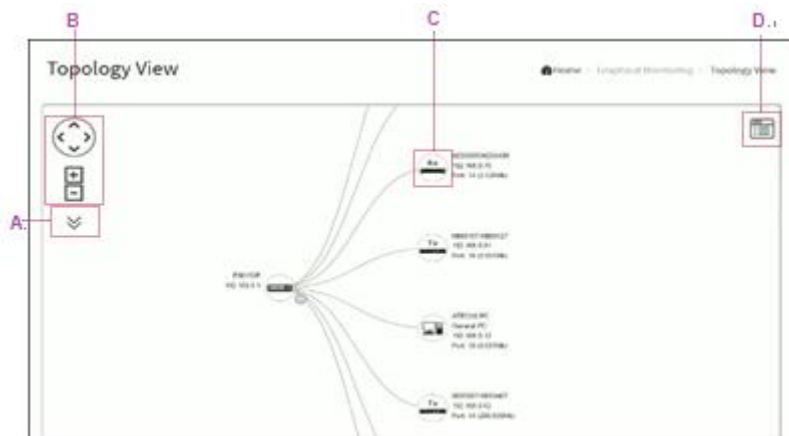
그래픽 모니터링 메뉴는 다음과 같습니다:




### 토폴로지 뷰

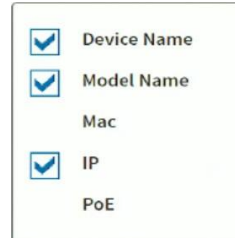
DMS는 자동으로 모든 IP 장치를 탐색하고 그래픽 네트워킹 토폴로지 뷰를 통해 장치를 표시합니다. 장치가 동작을 하지 않을 때 원격에서 케이블 연결 상태 진단, 주요 이벤트에 대한 자동 경고 알림, 원격에서 PoE 장치 재부팅을 포함해, 유저는 토폴로지 뷰를 통해 이들을 관리하고 모니터링할 수 있습니다. 따라서 태블릿 또는 스마트폰으로 비정상적 이슈를 언제, 어디서나 해결하도록 유저는 DMS 플랫폼을 적용할 수 있으며 네트워크 동작을 부드럽게 유지합니다.


그래픽 모니터링 토폴로지 뷰를 클릭해, 네트워크 토폴로지의 시각적 뷰를 볼 수 있습니다.







**항목 설명:**

1. 정보 목록  아이콘: 유저는 각 장치의 토폴로지 뷰에 표시되는 정보의 종류를 선택할 수 있습니다. 최대 3개 항목이 선택됩니다.




2. 플러스와 마이너스 마크의  아이콘 토폴로지 뷰를 줌 인 줌아웃합니다. 유저는 동일한 목적을 위해 마우스로 스크롤을 업데이트할 수 있습니다.




3. 장치 이미지

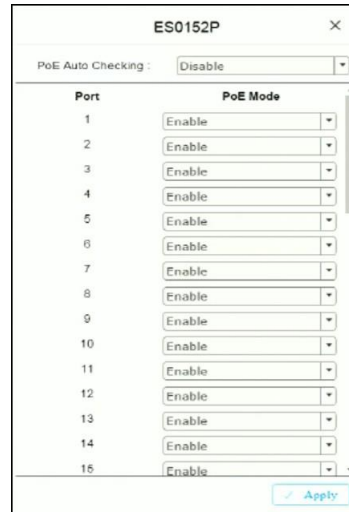
- ◆ 흑색 표시  아이콘: 장치를 연결합니다. 유저는 기능을 선택하고 문제를 확인할 수 있습니다.
- ◆ 적색 표시  아이콘: 장치 연결을 해제합니다. 유저는 연결 상태를 진단할 수 있습니다.
- ◆ 번호가 있는  : IP 장치 상의 문제가 발생했다는 의미입니다. (예: 장치 오프라인, IP 복제 등) 유저는 알림에서 이벤트를 체크할 장치 아이콘을 클릭할 수 있습니다.
- ◆ 물음표 표시  아이콘: IP 장치가 DMS에 의해 탐지된다는 의미입니다. 그러나 미확인 장치 타입으로 분류되는 장치 타입을 인식할 수 없습니다.
- ◆ 장치 아이콘을 왼쪽 클릭해 추가 동작에 대한 장치 콘솔을 표시합니다.

| ES0152P      |                   |
|--------------|-------------------|
| Device Type  | SWITCH            |
| Device Name  | ES0152P           |
| Model Name   | ES0152P           |
| Mac Address  | 00-40-c7-1c-e9-eb |
| DHCP Client  | Disable           |
| IPv4 Address | 192.168.0.1       |
| Subnet Mask  | 255.255.255.0     |
| Gateway      | 192.168.0.254     |
| Http Port    | 80                |
| PoE Supply   | 3.9 W             |

Login Upgrade Find Switch PoE Config  
 Dashboard Notification


- 대시보드 콘솔: 장치에 대한 장치 정보와 관련 동작을 표시합니다.
- 다양한 장치 타입이 여러가지 기능을 지원합니다:
    - IP 장치가 DMS 스위치로 인식되면 "업그레이드", "PoE 설정" 및 "스위치 탐지" 기능을 지원합니다.
    - IP 장치가 PoE로 인식되면 "PoE 재부팅" 기능 및 "업그레이드", "스위치 탐지" 기능을 지원합니다.
    - IP 장치가 ONVIF 프로토콜을 통해 IP 캠으로 인식이 되는 경우입니다.
  - 장치 타입 (Device Type): 자동으로 표시할 수 있습니다. 미확인 타입이 탐지되면 미리 정의된 목록에서 타입을 선택할 수 있습니다.
  - 장치 이름 (Device Name): 사용자 장치 이름 또는 편리한 관리를 위해 1F\_Lobby\_Cam1와 같은 ID를 생성합니다.
  - 모델 이름 (Model Name), MAC 주소 (MAC Address), IPv4 주소 (IPv4 Address), 서브넷 마스크 (Subnet Mask), 게이트웨이 (Gateway), PoE 공급 (PoE Supply) 및 PoE 사용 (PoE Used)이 DMS로 자동으로 표시됩니다.
  - http 포트 (Http Port): 더욱 우수한 보안을 위해 http 포트 번호를 장치에 재할당합니다.
  - DHCP 클라이언트 (DHCP Client): DHCP 클라이언트를 활성화 또는 비활성화 합니다. 이 기능이 활성화 되면 시스템은 DHCP 프로토콜을 사용해 IPv4 주소와 인터페이스의 마스크를 설정합니다. DHCP 클라이언트는 DNS 탐색 제공을 위해 호스트 이름으로 설정된 시스템 이름을 알립니다.
  -  로그인: 추가 설정 및 상태 모니터링을 위해 로그인 동작 아이콘을 클릭해 http를 통해 장치에 로그인합니다.

- ◆  업그레이드: 소프트웨어 버전을 업그레이드 하려면 클릭하세요.
- ◆  스위치 탐색: 이 기능이 동작하면 스위치 LED에 모두 불이 들어오고 15초간 깜빡입니다.
- ◆  PoE 설정: 클릭하면 PoE 기능을 설정합니다. PoE 자동 확인 활성화/비활성화 및 포트 당 PoE 모드를 활성화/비활성화 합니다.



The image shows a configuration window titled "ES0152P". At the top, there is a dropdown menu for "PoE Auto Checking" set to "Disable". Below this is a table with two columns: "Port" and "PoE Mode". The "Port" column lists ports from 1 to 15. The "PoE Mode" column has a dropdown menu for each port, all currently set to "Enable". At the bottom right of the table, there is a blue "Apply" button.

| Port | PoE Mode |
|------|----------|
| 1    | Enable   |
| 2    | Enable   |
| 3    | Enable   |
| 4    | Enable   |
| 5    | Enable   |
| 6    | Enable   |
| 7    | Enable   |
| 8    | Enable   |
| 9    | Enable   |
| 10   | Enable   |
| 11   | Enable   |
| 12   | Enable   |
| 13   | Enable   |
| 14   | Enable   |
| 15   | Enable   |



- ◆  진단: 진단 동작 아이콘을 클릭하면 케이블 진단을 실행해, 손상 케이블을 검사하고 장치 연결이 ping 동작 여부를 확인합니다.

케이블 상태:

- ◆ 녹색 아이콘: 케이블 연결이 올바릅니다.
- ◆ 적색 아이콘: 케이블 연결이 바르지 않습니다. 유저는 거리 정보(XX 미터)를 확인해 손상 케이블 위치를 확인합니다.

연결:

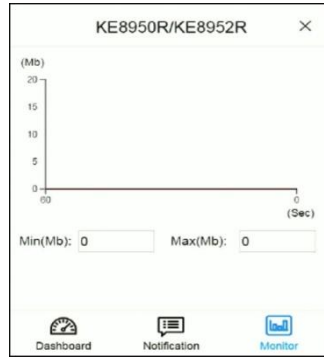
- ◆ 녹색 아이콘: 장치가 올바르게 ping되는 상태입니다.
- ◆ 적색 아이콘: 장치가 올바르게 데이터를 전송/수신하고 있지 않습니다. 성공적으로 ping이 되지 않는다는 의미입니다.


- ◆  PoE 재부팅: 재부팅 동작 아이콘을 클릭하면 장치를 원격에서 재부팅해 장치를 정상 동작으로 복구합니다.
- ◆  공백 노드 아이콘: DMS 스위치가 2개 이상의 IP 장치를 동일한 포트에서 탐지하는 경우, 스위치는 이 IP 장치의 레이아웃을 만들 수 없습니다. 대신 이 상황을 알리기 위해 공백 노드를 표시합니다. 유저는 “상위 노드”기능을 사용해 대시보드에서 레이아웃을 조정할 수 있습니다.

2. 알림 콘솔 (Notification Console): 이벤트에 의해 발생하는 경고 및 로그를 표시합니다.



3. 모니터 콘솔 (Monitor Console): 장치 상태 점검을 위해 한 트래픽을 표시합니다.
- ◆ DMS 스위치를 제외한 각 IP 장치의 경우, 유저는 IP 장치 처리량의 한계점을 설정할 수 있고 처리량이 설정보다 낮거나 높은 경우 알립니다.
  - ◆ 양 쪽 값이 “0”인 경우, 기능이 비활성화 됩니다.
  - ◆ 폴링 간격이 1초 이며 페이지가 닫히면 폴링 간격은 약 5초로 변경됩니다.



d)  상단 오른쪽 구석에 “설정 아이콘”이 있습니다. 사용자가 이 아이콘을 클릭하면 장치, 그룹, 설정, 토폴로지 뷰와 토폴로지 내보내기 및 고급 검색 기능을 사용할 수 있습니다.

◆ 장치 검색 콘솔

모든 장치와 정보가 목록에 나타납니다.



| No. | 기능                            |
|-----|-------------------------------|
| 1   | 장치 타입 별로 장치를 필터링합니다.          |
| 2   | 전체 글자 검색 키워드 별 장치를 검색합니다.     |
| 3   | SVG, PNG 또는 PDF로 전체 뷰를 저장합니다. |



◆ 그룹 설정 콘솔

- ◆ 유저는 OUI 또는 장치 아이콘을 클릭해 각 IP 장치에 대한 VLAN 그룹을 설정할 수 있습니다. 그리고 각 VLAN 그룹 트래픽 우선권 (0~7)을 설정할 수 있습니다.
- ◆ MAC 기반 VLAN을 사용해 그룹을 분리합니다.
- ◆ 하나의 IP 장치가 하나의 VLAN 그룹에만 포함될 수 있습니다.

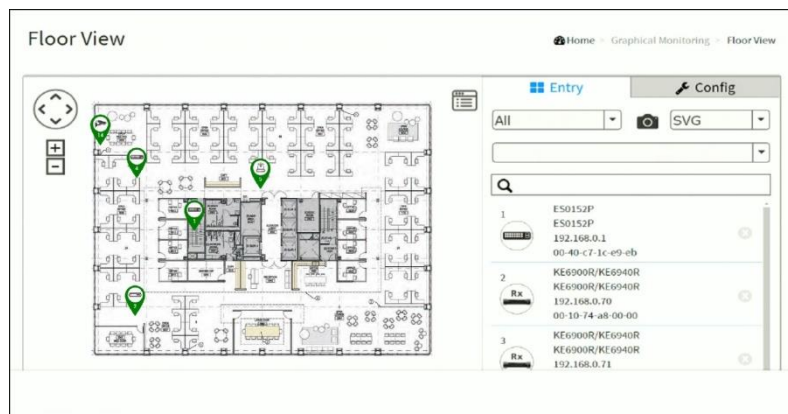
| No. | 기능                                      |
|-----|---|
| 1   | 필터링, 검색, 장치 아이콘 클릭 또는 OUI 지정을 이용한 그룹 장치 |
| 2   | VLAN 트래픽 우선권 설정                         |
| 3   | VLAN ID 또는 그룹 이름 할당                     |

◆ 그룹 설정 콘솔

| No. | 기능   |
|-----|--|
| 1   | 이 곳에서는 토폴로지 뷰에 탐지 및 표시되는 IP 장치 수를 나타냅니다.   |
| 2   | 마스터 IP 입니다.  |
| 3   | DHCP 서버를 활성화/비활성화 할 수 있습니다.  |
| 4   | <ul style="list-style-type: none"> <li>- 싱글 서브넷: DMS는 마스터 스위치의 IP 주소를 기반으로 합니다. 서브넷은 "255.255.255.0"을 뜻합니다.</li> <li>- 멀티플 서브넷: 수동 입력을 위해 4개의 범위를 제공합니다. (이 경우, 스위치 서브넷 마스크를 "255.255.0.0"으로 설정하는 것을 권장하며, IP 장치가 인식이 되지 않을 것 입니다.)</li> </ul> |

## 플로어 뷰

유저는 맞춤 업로드 된 플로어 이미지 상에 IP 장치 설치 위치를 쉽게 계획할 수 있습니다.



- ◆ 플로어 맵의 장치 고정
- ◆ 장치 위치 즉시 검색
- ◆ 10 Maps는 각 스위치에 저장 가능
- ◆ IP 감시/ VoIP/WiFi 애플리케이션
- ◆ 토폴로지 뷰와 동일한 기타 기능
- ◆ 장치 아이콘 위치 및 제거:

- ◆ 장치 목록에서 장치 선택 및 아이콘 클릭
  - ◆ 플로어 이미지의 기본 위치 상에 장치 아이콘 표시
  - ◆ 마우스 클릭을 유지해 플로어 뷰에 올바른 위치로 아이콘을 드래그앤드롭
  - ◆ 장치 아이콘의 오른 쪽 크로스 사인을 클릭해 장치를 모든 플로어 뷰 이미지에서 삭제
- ◆ 2개 이상 플로어 이미지가 있다면, 검색 필드 상의 필드에서 선택할 수 있습니다.

## **지도 뷰**

다른 건물에 설치가 되어 있어도 장치 위치 검색에 유용합니다. 유저는 구글 맵으로 탐색할 지도 뷰 상의 장치 아이콘을 위치시킬 수 있습니다.

다음의 동작이 가능합니다:

- ◆ 구글 지도 상의 장치 고정
- ◆ 지도에서 장치 위치 즉시 검색
- ◆ 회사/주소 온라인 검색
- ◆ 외부 IP 캠/Wifi 애플리케이션
- ◆ 토폴로지 뷰와 동일한 기타 기능

## 유지보수

### 플로어 이미지

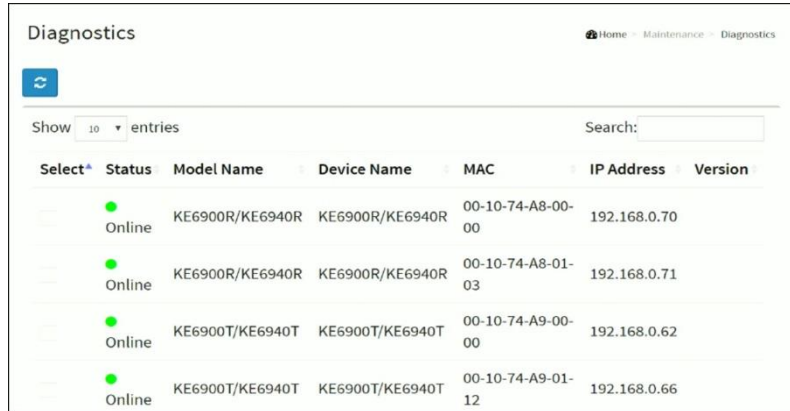
이 페이지에서 유저는 플로어 이미지를 추가 또는 삭제할 수 있습니다.

- ◆ 각 DMS 스위치는 업로드에 10 파일 공간을 제공합니다.
- ◆ JPC와 PNG 포맷만 제공됩니다.
- ◆ 파일 크기는 512KB로 제한됩니다.
- ◆ 동일한 네트워크 상의 모든 DMS 스위치 플로어 이미지를 함께 공유할 수 있습니다.
  - ◆ 예시:
 

스위치1에 10 플로어 이미지, 스위치2에 5 이미지가 있다면, 총 15개 플로어 이미지가 동일한 네트워크에 모든 DMS 스위치를 공유 및 선택할 수 있습니다.
- ◆ 파일 이름은 IP 주소를 포함해 유저는 플로어 이미지가 어느 DMS 스위치 상에 저장되었는지 알 수 있습니다.

## 진단

이 페이지에서, 모든 IP 장치는 테이블에 목록으로 나타나며 유저는 네트워크에서 IP 장치의 연결 상태를 진단할 수 있습니다.



The screenshot shows the 'Diagnostics' page with a breadcrumb trail: Home > Maintenance > Diagnostics. Below the title is a refresh button and a search bar. A table lists network devices with columns: Select, Status, Model Name, Device Name, MAC, IP Address, and Version. There are four entries, all with a green 'Online' status.

| Select                   | Status | Model Name      | Device Name     | MAC               | IP Address   | Version |
|--------------------------|--------|-----------------|-----------------|-------------------|--------------|---------|
| <input type="checkbox"/> | Online | KE6900R/KE6940R | KE6900R/KE6940R | 00-10-74-A8-00-00 | 192.168.0.70 |         |
| <input type="checkbox"/> | Online | KE6900R/KE6940R | KE6900R/KE6940R | 00-10-74-A8-01-03 | 192.168.0.71 |         |
| <input type="checkbox"/> | Online | KE6900T/KE6940T | KE6900T/KE6940T | 00-10-74-A9-00-00 | 192.168.0.62 |         |
| <input type="checkbox"/> | Online | KE6900T/KE6940T | KE6900T/KE6940T | 00-10-74-A9-01-12 | 192.168.0.66 |         |

- ◆ 유저는 장치를 선택해 자동으로 진단 절차를 시작합니다.



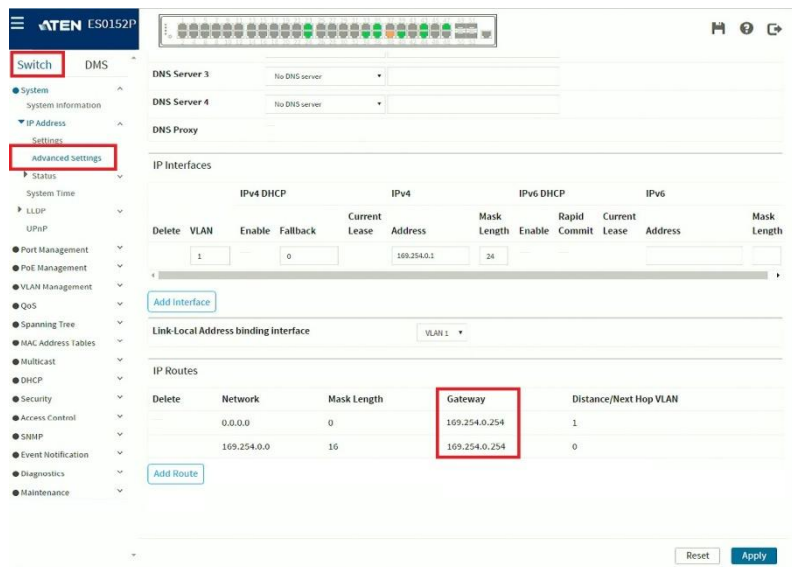
- ◆ [Another Try](#) "Another Try"를 눌러 IP 장치 목록 페이지로 돌아갑니다.
- ◆ 진단 기능은 또한 토폴로지 뷰의 대시보드에서 탐지될 수 있습니다.



## IP 경로 설정

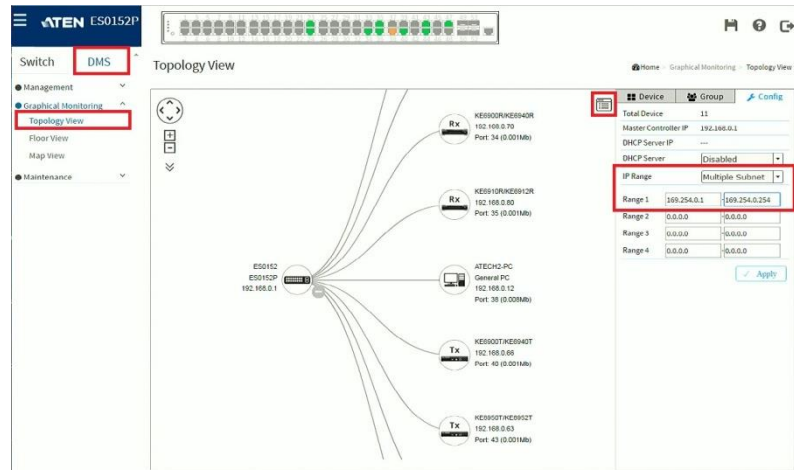
ES0152/ES0152P 연결 시 연결 장치의 IP 주소를 192.168.0.x로 설정하는 것을 권장합니다. IP 주소가 192.168.0.x로 설정되지 않으면 (예, 기본 IP 주소 169.254.0.x의 VE89 시리즈) ES0152/ES0152P 에 의해 발견된 연결된 장치를 위해 ES0152/ES0152P 상의 IP 경로 설정을 요청합니다.

컨트롤러 ES0152/ES0152P를 설정하려면 다음을 따라 하십시오:

1. "스위치 (Switch)" → "IP 주소 (IP Address)" 로 이동해 "고급 설정 (Advanced Settings)"를 선택합니다. 네트워크 **0.0.0.0**을 추가하고 게이트웨이를 **169.254.0.254**로 설정하십시오. 또 다른 네트워크 **169.254.0**을 추가하고 게이트웨이를 **169.254.0.254**로 설정한 후 **적용(Apply)**을 클릭하세요.



2. "DMS" → "그래픽 모니터링 (Graphical Monitoring)"으로 이동해 "토폴로지 뷰(Topology View)"를 선택합니다. 를 클릭해 시스템 패널을 불러온 후 를 선택하세요. "IP 범위 (IP Range)"를 "멀티플 서브넷 (Multiple Subnet)"으로 변경하고 169.254.0.1와 169.254.0.254의 새로운 범위를 추가합니다.



이 페이지는 의도적으로 비워 두었습니다.



## 안전 주의 사항

---

### 일반

- ◆ 본 제품은 실내에서만 사용해야 합니다.
- ◆ 사용 설명서를 다 읽으십시오. 차후 참고를 위해 보관하세요.
- ◆ 본 제품에 설명된 주의사항과 설명서를 따르십시오.
- ◆ 불안정한 표면(카트, 스탠드, 테이블 등)위에 본 제품을 두지 않도록 합니다. 제품이 떨어질 경우 제품에 심각한 파손을 초래할 수 있습니다.
- ◆ 물기가 있는 곳 근처에서 제품을 사용하지 마십시오.
- ◆ 라디에이터나 히터 근처 또는 위에 제품을 두어서는 안됩니다.
- ◆ 제품 외관에는 통풍을 위해 작은 구멍이 있습니다. 원활한 동작과 과열 방지를 위해 이 구멍이 막히거나 가려져서는 안됩니다.
- ◆ 본 제품은 부드러운 표면(침대, 소파, 러그 등) 위에 절대 두지 마십시오. 마찬가지로 통풍이 잘 되지 않는 사방이 막힌 불박이 장소에 놓아서는 안됩니다.
- ◆ 어떠한 액체류도 흘러서는 안됩니다.
- ◆ 서킷 과부하를 피하십시오. 장치를 서킷에 연결하기 전, 전력 공급 제한을 숙지하고 이를 초과해서는 안됩니다. 항상 서킷의 전기 규격을 확인해 위험한 문제를 초래하지 않도록 합니다. 서킷 과부하는 화재 또는 장비 파손의 위험을 일으킬 수 있습니다.
- ◆ 청소 전 벽의 콘센트에서 제품 플러그를 뽑으십시오. 액체 또는 스프레이 타입의 클리너를 사용하지 마십시오. 청소를 위해 젖은 천을 사용하세요.
- ◆ 라벨이 표시되어 있는 전원 소스 타입에 따라 동작되어야 합니다. 전원 타입에 대해 확신할 수 없는 경우 판매자 또는 지역에 문의하세요.
- ◆ 설비 상의 피해를 예방하려면 모든 장치가 적절하게 접지되는 것이 중요합니다.
- ◆ 장치는 선간 전압을 지원하는 IT 전원 분배 시스템에 맞게 설계되었습니다.
- ◆ 장치는 3 와이어 접지 타입 플러그를 갖추고 있습니다. 이 것은 안전 장치입니다. 플러그를 아웃렛에 연결하지 못하는 경우 전기 기술자에게 연락해 사용할 수 없는 아웃렛을 교체하십시오.

접지형 플러그 목적에 맞지 않는 시도를 하지 마십시오. 항상 지역/국가 접지 코드를 따르십시오.

- ◆ 전원 코드나 케이블에 아무 것도 놓아서는 안됩니다. 전원 코드와 케이블을 사용자들이 발로 밟거나 걸리지 않도록 배치하세요.
- ◆ 연장 코드가 이 장치와 사용될 경우 이 코드의 모든 제품의 전체 암페어율이 연장 코드 암페어율을 초과해서는 안됩니다. 벽 콘센트에 연결된 모든 제품의 전체 암페어율이 15암페어를 초과하지 않도록 합니다.
- ◆ 갑작스럽고 일시적인 전력 증가와 감소로부터 시스템을 보호하려면, 과전류 억제기, 라인 컨디셔너 또는 무정전 전원 장치 (UPS)를 사용하세요.
- ◆ 시스템 케이블과 전원 케이블을 주의해서 배치하십시오. 케이블 위에 아무 것도 없도록 해야 합니다.
- ◆ 전원을 핫 플러그 가능한 전원 공급 장치에 전원을 연결하거나 분리할 때 다음의 사항을 주의하십시오:
  - ◆ 전원 케이블을 전원 공급 장치에 연결하기 전 전원 공급 장치를 설치합니다.
  - ◆ 전원 공급 장치를 제거하기 전 전원 케이블을 분리하십시오.
  - ◆ 시스템에 다양한 전원 소스가 있다면, 전원 공급 장치에서 모든 전원 케이블을 분리해 시스템에서 전원을 분리하십시오.
- ◆ 어떠한 종류의 물체도 떨어뜨리거나 외관 틈에 사이로 넣어서는 안됩니다. 위험한 전압 지점을 건드리거나 부품 누전이 되어 화재 또는 전기 충격의 위험을 초래할 수 있습니다.
- ◆ 개인적으로 제품을 보수하려고 하지 마십시오. 모든 보수는 인증된 전문가에게 요청하십시오.
- ◆ 다음의 증상이 발생하면 제품을 콘센트에서 분리한 후 인증된 전문가에게 수리를 요청하십시오.
  - ◆ 전원 코드나 플러그가 손상되거나 닳게 된 경우
  - ◆ 제품에 액체를 흘렸을 경우
  - ◆ 제품이 비 또는 물에 노출된 경우
  - ◆ 제품을 떨어뜨렸거나 외관이 손상된 경우
  - ◆ 제품이 동작 중 보수가 필요한 뚜렷한 변화를 보인 경우
  - ◆ 제품 설명서를 따랐음에도 제품이 정상적으로 작동되지 않은 경우

- ◆ 설명서상에 기재된 범위 안에서만 수정하십시오. 부적절한 제품 컨트롤 수정은 인증된 기술자에 의해 광범위한 보수가 필요한 손상을 일으킬 수 있습니다.
- ◆ 장치가 포개어져 있거나 랙에 설치되어 있는 경우라면, 프레임 나사를 조이거나 기타 비슷한 방식을 이용해 추가 보호 조치로 장치를 보호합니다.
- ◆ 전기 케이블, 변압기 및 조명과 같은 잠재적 EMI 소스에서 가능한 멀리 Cat 5e/6를 보관하십시오. 전기 도선에 케이블을 묶거나 전기 설비에 케이블을 두어서는 안됩니다.
- ◆ 설치할 SFP 모듈은 다음을 준수합니다.
  - ◆ IEC/EN 60825-1에 따른 CLASS 1 LASER PRODUCT
  - ◆ 2007, 6월 24일자의 Laser Notice No. 50에 따른 편차를 제외한 21 CFR 1040.10 and 1040.11

## **랙 마운팅**

- ◆ 랙에서 작업하기 전에 안전 장치가 랙에 고정되어 있는지 확인하고 바닥이 랙 전체 무게를 지탱하는지 확인하세요. 랙에서 작업 전 싱글 랙 상의 앞면과 옆면의 안정장치 또는 여러 대의 랙의 앞면 안정 장치를 설치하세요.
- ◆ 항상 바닥부터 랙을 장착하고 무거운 아이템을 가장 먼저 랙에 장착합니다.
- ◆ 랙에서 장치를 연장하기 전에 랙이 평평하고 안정적인지 확인하십시오.
- ◆ 장치 레일 잠금 장치를 해제하고 장치를 랙의 안쪽으로 밀어 넣거나 뺄 때 조심하십시오; 슬라이드 레일에 손가락이 끼일 수 있습니다.
- ◆ 장치를 랙에 삽입한 후 주의 깊게 레일을 잠금 위치에서 확장한 후 랙에 장치를 밀어 넣습니다.
- ◆ 랙에 전원을 공급하는 AC 공급 분기 회로가 과부하 되지 않도록 하십시오. 전체 랙 부하가 분기 회로용의 80 퍼센트를 초과해서는 안됩니다.
- ◆ 랙에 사용되는 모든 장비- 멀티 콘센트 및 다른 전원 커넥터를 포함한 - 가 알맞게 접지되어 있는지 확인하십시오.
- ◆ 랙의 장치에 통풍이 되도록 하십시오.
- ◆ 랙 환경의 동작 주변 온도는 제조사에 따라 장비에 지정된 최대 주변 온도를 넘지 않습니다.

- ◆ 랙의 다른 장치를 수리할 때 장치를 밟지 않도록 주의하십시오.

---

## Consignes de sécurité

---

### Général

- ♦ Ce produit est destiné exclusivement à une utilisation à l'intérieur.
- ♦ Veuillez lire la totalité de ces instructions. Conservez-les afin de pouvoir vous y référer ultérieurement.
- ♦ Respectez l'ensemble des avertissements et instructions inscrits sur l'appareil.
- ♦ Ne placez jamais l'unité sur une surface instable (chariot, pied, table, etc.). Si l'unité venait à tomber, elle serait gravement endommagée.
- ♦ N'utilisez pas l'unité à proximité de l'eau.
- ♦ Ne placez pas l'unité à proximité de ou sur des radiateurs ou bouches de chaleur.
- ♦ Le boîtier de l'unité est doté de fentes et d'ouvertures destinées à assurer une ventilation adéquate. Pour garantir un fonctionnement fiable et protéger l'unité contre les surchauffes, ces ouvertures ne doivent jamais être bloquées ou couvertes.
- ♦ L'unité ne doit jamais être placée sur une surface molle (lit, canapé, tapis, etc.) car ses ouvertures de ventilation se trouveraient bloquées. De même, l'unité ne doit pas être placée dans un meuble fermé à moins qu'une ventilation adaptée ne soit assurée.
- ♦ Ne renversez jamais de liquides de quelque sorte que ce soit sur l'unité.
- ♦ Evitez toute surcharge du circuit. Avant de connecter l'équipement à un circuit, vérifiez la limite de l'alimentation et ne la dépassez pas. Contrôlez toujours les caractéristiques électriques d'un circuit pour vous assurer de ne pas créer de situation dangereuse ou qu'il n'y en a pas déjà. Les surcharges du circuit peuvent provoquer un incendie et détruire l'équipement.
- ♦ Débranchez l'unité de la prise murale avant de la nettoyer. N'utilisez pas de produits de nettoyage liquide ou sous forme d'aérosol. Utilisez un chiffon humide pour le nettoyage de l'unité.
- ♦ L'appareil doit être alimenté par le type de source indiqué sur l'étiquette. Si vous n'êtes pas sûr du type d'alimentation disponible, consultez votre revendeur ou le fournisseur local d'électricité.
- ♦ Afin de ne pas endommager votre installation, vérifiez que tous les périphériques sont correctement mis à la terre.

- ♦ L'unité est équipée d'une fiche de terre à trois fils. Il s'agit d'une fonction de sécurité. Si vous ne parvenez pas à insérer la fiche dans la prise murale, contactez votre électricité afin qu'il remplace cette dernière qui doit être obsolète. N'essayez pas d'aller à l'encontre de l'objectif de la fiche de terre. Respectez toujours les codes de câblage en vigueur dans votre région/pays.
- ♦ L'équipement doit être installé à proximité de la prise murale et le dispositif de déconnexion (prise de courant femelle) doit être facile d'accès.
- ♦ La prise murale doit être installée à proximité de l'équipement et doit être facile d'accès.
- ♦ Veillez à ce que rien ne repose sur le cordon d'alimentation ou les câbles. Acheminez le cordon d'alimentation et les câbles de sorte que personne ne puisse marcher ou trébucher dessus.
- ♦ En cas d'utilisation d'une rallonge avec cette unité, assurez-vous que le total des ampérages de tous les produits utilisés sur cette rallonge ne dépasse pas l'ampérage nominal de cette dernière. Assurez-vous que le total des ampérages de tous les produits branchés sur la prise murale ne dépasse pas 15 ampères.
- ♦ Pour contribuer à protéger votre système contre les augmentations et diminutions soudaines et transitoires de puissance électrique, utilisez un parasurtenseur, un filtre de ligne ou un système d'alimentation sans coupure (UPS).
- ♦ Placez les câbles du système et les câbles d'alimentation avec précaution ; veillez à ce que rien ne repose sur aucun des câbles.
- ♦ Lors du branchement ou du débranchement à des blocs d'alimentation permettant la connexion à chaud, veuillez respecter les lignes directrices suivantes:
  - ♦ Installez le bloc d'alimentation avant de brancher le câble d'alimentation à celui-ci.
  - ♦ Débranchez le câble d'alimentation avant de retirer le bloc d'alimentation.
- ♦ Si le système présente plusieurs sources d'alimentation, déconnectez le système de l'alimentation en débranchant tous les câbles d'alimentation des blocs d'alimentation.
- ♦ N'insérez jamais d'objets de quelque sorte que ce soit dans ou à travers les fentes du boîtier. Ils pourraient entrer en contact avec des points de tension dangereuse ou court-circuiter des pièces, entraînant ainsi un risque d'incendie ou de choc électrique.

- ♦ N'essayez pas de réparer l'unité vous-même. Confiez toute opération de réparation à du personnel qualifié.
- ♦ Si les conditions suivantes se produisent, débranchez l'unité de la prise murale et amenez-la à un technicien qualifié pour la faire réparer:
  - ♦ Le cordon d'alimentation ou la fiche ont été endommagés ou éraillés.
  - ♦ Du liquide a été renversé dans l'unité.
  - ♦ L'unité a été exposée à la pluie ou à l'eau.
  - ♦ L'unité est tombée ou le boîtier a été endommagé.
- ♦ Les performances de l'unité sont visiblement altérées, ce qui indique la nécessité d'une réparation.
- ♦ L'unité ne fonctionne pas normalement bien que les instructions d'utilisation soient respectées.
- ♦ N'utilisez que les commandes qui sont abordées dans le mode d'emploi. Le réglage incorrect d'autres commandes peut être à l'origine de dommages qui nécessiteront beaucoup de travail pour qu'un technicien qualifié puisse réparer l'unité.
- ♦ Tenez le câble de catégorie 5e/6 le plus éloigné possible des sources potentielles d'interférences électromagnétiques, telles que les câbles électriques, transformateurs et appareils d'éclairage. Ne nouez pas les câbles à des conduits électriques et ne les faites pas passer sur des installations électriques.

## **Montage sur bâti**

- ♦ Avant de travailler sur le bâti, assurez-vous que les stabilisateurs sont bien fixés sur le bâti, qu'ils sont étendus au sol et que tout le poids du bâti repose sur le sol. Installez les stabilisateurs avant et latéraux sur un même bâti ou bien les stabilisateurs avant si plusieurs bâtis sont réunis, avant de travailler sur le bâti.
- ♦ Chargez toujours le bâti de bas en haut et chargez l'élément le plus lourd en premier.
- ♦ Assurez-vous que le bâti est à niveau et qu'il est stable avant de sortir une unité du bâti.
- ♦ Agissez avec précaution lorsque vous appuyez sur les loquets de libération du rail d'unité et lorsque vous faites coulisser une unité dans et hors d'un bâti ; vous pourriez vous pincer les doigts dans les rails.
- ♦ Une fois qu'une unité a été insérée dans le bâti, étendez avec précaution le rail dans une position de verrouillage puis faites glisser l'unité dans le bâti.
- ♦ Ne surchargez pas le circuit de l'alimentation CA qui alimente le bâti. La charge totale du bâti ne doit pas dépasser 80 % de la capacité du circuit.
- ♦ Assurez-vous que tous les équipements utilisés sur le bâti, y-compris les multiprises et autres connecteurs électriques, sont correctement mis à la terre.
- ♦ Assurez-vous que les unités présentes dans le bâti bénéficie d'une circulation d'air suffisante.
- ♦ Assurez-vous que la température ambiante de fonctionnement de l'environnement du bâti ne dépasse pas la température ambiante maximale spécifiée pour l'équipement par le fabricant.
- ♦ Ne marchez sur aucun appareil lors de la maintenance d'autres appareils d'un bâti.



## 기술 지원

### 국제 지역

- ◆ 온라인 기술 지원 – 고장 해결, 설명서, 소프트웨어 업데이트: <http://eservice.aten.com>
- ◆ 전화 지원의 경우 페이지 iii의 *전화 지원*을 참조하십시오.

### 북미 지역

|           |            |   |
|-----------|------------|---|
| 이메일 지원    |            | support@aten-usa.com  |
| 온라인 기술 지원 | 고장 해결      | <a href="http://www.aten-usa.com/support">http://www.aten-usa.com/support</a> |
|           | 설명서        |   |
|           | 소프트웨어 업데이트 |   |
| 전화 지원     |            | 1-888-999-ATEN 내선 4988  |

기술 지원 요청 시 다음의 정보를 미리 준비하십시오:

- ◆ 모델 번호, 시리얼 번호 및 구매일
- ◆ 운영 체제, 변경 정도, 확장 카드 및 소프트웨어를 포함한 사용자 컴퓨터 설정
- ◆ 오류 발생시 표시된 오류 메시지
- ◆ 오류가 발생하게 된 순차적 순서
- ◆ 사용자가 필요하다고 판단되는 기타 모든 정보

## 문제 해결

| 문제  | 가능한 원인                       | 제안 솔루션   |
|---|------------------------------|--|
| 시스템 LED<br>꺼짐                                 | 스위치가 전원을 공급받지 않는 상태입니다.      | <ol style="list-style-type: none"> <li>올바른 전원 코드가 스위치와 AC 아웃렛 소켓에 연결되어 있는지 확인하십시오.</li> <li>전원 코드를 스위치에서 분리 후 다시 연결해 스위치에 전력 순환을 실행합니다.</li> <li>LED가 여전히 꺼진 상태라면, 전원 코드를 다른 AC 아웃렛 소켓에 연결해 올바른 AC 소스가 공급되도록 합니다.</li> </ol>   |
| 적색 시스템<br>LED                                 | 스위치에 의해 비정상 상태가 감지되었습니다.     | 웹 UI에서 스위치 내에 시스템 로그를 확인해 비정상 상태를 확인하고 (예, 동작 온도 범위 초과) 문제 해결에 맞는 동작을 실행합니다.   |
| Link/<br>Act/Speed<br>모드에서 포트<br>상태 LED<br>꺼짐 | 포트가 연결되지 않았거나 연결이 동작하지 않습니다. | <ol style="list-style-type: none"> <li>케이블 커넥터 플러그가 스위치와 연결된 장치 양 쪽에 모두 바르게 연결되었는지 확인합니다.</li> <li>연결된 장치가 바르게 동작하는지 확인하세요.</li> <li>문제 현상이 계속되면 다른 케이블 또는 다른 포트를 시도해, 케이블 또는 특정 포트에 관련된 문제인지 확인합니다.</li> <li>웹 유저 인터페이스를 통해 구성 설정에서 포트가 비활성 상태인지 확인합니다.</li> </ol>      |
| PoE 모드에서<br>포트 상태 LED<br>꺼짐                   | 포트가 전원을 공급하고 있지 않습니다.        | <ol style="list-style-type: none"> <li>케이블 커넥터 플러그가 스위치와 연결된 장치 양 쪽에 모두 바르게 연결되었는지 확인합니다.</li> <li>이더넷 케이블 사용이 바르게 되고 있는지 확인합니다.</li> <li>문제 현상이 계속되면 다른 케이블 또는 다른 포트를 시도해, 케이블 또는 특정 포트에 관련된 문제인지 확인합니다.</li> <li>웹 유저 인터페이스를 통해 구성 설정에서 포트가 비활성 상태인지 확인합니다.</li> </ol> |

## 제품규격

| 기능                   | ES0152                          | ES0152P                                    |
|----------------------|---------------------------------|--|
| <b>커넥터</b>           |                                 |  |
| RJ-45 10/100/1000 포트 | 48                              |  |
| SFP+ 업링크 포트          | 4                               |  |
| 콘솔 포트                | 1 x RJ45                        |  |
| <b>실행</b>            |                                 |  |
| 전환 속도                | 176 Gbps                        |  |
| 포워딩 속도               | 130.95 Mpps                     |  |
| 점보 프레임               | 10240 Bytes                     |  |
| 최대 입력 전력율            | 100–240V AC, 50–60Hz, 1A        | 100–240V AC, 50–60Hz, 10A                  |
| 소비 전력                | AC100V / 45.98W AC220V / 46.55W | AC100V / 885.36W AC220V / 858.09W (PoE on) |
| <b>제품 환경</b>         |                                 |  |
| 동작 온도                | 0–50°C                          |  |
| 보관 온도                | –20–60°C                        |  |
| 습도                   | 비응축 상태에서 10–90% RH              |  |
| <b>제품 외관</b>         |                                 |  |
| 랙 공간                 | 19"                             |  |
| 재질                   | 금속                              |  |
| 무게                   | 4.20 kg                         | 5.60 kg                                    |
| 크기 (L x W x H)       | 44.20 x 30.00 x 4.40 cm         | 44.20 x 37.50 x 4.40 cm                    |
| <b>PoE</b>           |                                 |  |
| 표준 호환                | N/A                             | 802.3af PoE / 802.3at PoE+                 |
| PoE/PoE +를 지원하는 포트 수 | N/A                             | 48   |
| 포트당 최대 PoE 전원 범위     | N/A                             | PoE: 15.4W / PoE+: 30.0W                   |
| 전체 최대 PoE 전원 범위      | N/A                             | 740W                                       |

## 보증 제한

---

ATEN은 구매 지역의 제품 결함에 대해 최초 구매일로부터 [2]년의 보증 기간 (특정 지역/국가에 따라 보증 기간은 달라질 수 있습니다.) 을 제공합니다. 이 보증 기간은 ATEN LCD KVM 스위치의 LCD 패널을 포함합니다. 1년 추가 보증 기간을 제공하는 제품을 선택하세요. (상세 내용은 A+ 보증 참고) 케이블과 액세서리는 표준 보증 기간에 해당되지 않습니다.

### 하드웨어 보증 제한 범위

ATEN은 보증 기간 동안 비용 청구 없는 보수 서비스를 제공합니다. 제품 결함 시 ATEN은 (1) 새 구성품이나 또는 수리된 구성품으로 보수하거나 (2) 결함이 있는 제품과 같은 기능을 충족하는 동일한 제품이나 비슷한 제품으로 교환합니다. 교환된 제품은 본래 제품은 남은 보증 기간을 추정하거나 90일의 기간 중 긴 기간으로 보증합니다. 제품 또는 구성품이 교환될 때 교체한 제품은 고객의 자산이며 교체된 제품은 ATEN의 자산이 됩니다.

보증 정책에 관한 더욱 많은 정보를 위해 ATEN의 웹사이트를 방문하십시오:

<http://www.aten.com/global/en/legal/policies/warranty-policy>