

# MR-0802P SERIES

PoE Switch

## 사용자 매뉴얼

Ver. 1.0



# MR-0802P SERIES

---

PoE Switch

사용자 매뉴얼

Ver. 1.0



|                                 |    |
|---------------------------------|----|
| MR-0802P SERIES.....            | I  |
| 사용자 매뉴얼.....                    | I  |
| 1 소개 및 설치 .....                 | 6  |
| 1.1 제품 주요 사양.....               | 6  |
| 1.2 제품 구성품.....                 | 7  |
| 1.3 제품 외관.....                  | 8  |
| 1.4 제품 설치.....                  | 8  |
| 2 WEB PAGE LOGIN.....           | 9  |
| 2.1 네트워크 관리 클라이언트에 로그인.....     | 9  |
| 3 NETWORK ADMIN.....            | 10 |
| 3.1 IP CONFIG.....              | 10 |
| 3.2 IP STATUS.....              | 11 |
| 3.3 NTP .....                   | 12 |
| 3.4 SYSLOG .....                | 13 |
| 3.5 SNMP .....                  | 14 |
| 4 PORT 구성 .....                 | 20 |
| 4.1 PORTS.....                  | 20 |
| 4.2 AGGREGATION .....           | 21 |
| 4.2.1 Static.....               | 22 |
| 4.2.2 LACP.....                 | 23 |
| 4.3 MIRRORING.....              | 25 |
| 4.4 GREEN ETHERNET .....        | 27 |
| 4.5 DDM .....                   | 27 |
| 5 POE.....                      | 29 |
| 5.1 PoE SETTING.....            | 29 |
| 5.2 PoE STATUS .....            | 30 |
| 6 ADVANCED CONFIGURE .....      | 31 |
| 6.1 MAC TABLE .....             | 31 |
| 6.2 VLANS .....                 | 31 |
| 6.3 PORT ISOLATION .....        | 36 |
| 6.4 LOOP PROTECTION.....        | 38 |
| 6.5 SPANNING TREE.....          | 39 |
| 6.5.1 Bridge Configuration..... | 40 |
| 6.5.2 MSTI Mapping.....         | 41 |
| 6.5.3 MSTI Priorities.....      | 42 |
| 6.5.4 CIST Ports.....           | 43 |
| 6.5.5 MSTI Ports.....           | 44 |
| 6.6 IPMC PROFILE .....          | 45 |

|                                   |    |
|-----------------------------------|----|
| 6.7 IGMP SNOOPING.....            | 45 |
| 6.7.1 Basic Configuration.....    | 45 |
| 6.7.2 VLAN Configuration.....     | 47 |
| 6.7.3 Port Filtering Profile..... | 48 |
| 6.8 IPV6 MLD SNOOPING.....        | 48 |
| 6.8.1 Basic Configuration.....    | 49 |
| 6.8.3 Port Filtering Profile..... | 50 |
| 6.9 ERPS.....                     | 50 |
| 6.10 LLDP .....                   | 53 |
| 7 SECURITY CONFIGURE.....         | 54 |
| 7.1 USERS.....                    | 54 |
| 7.2 PRIVILEGE LEVELS .....        | 54 |
| 7.3 SSH.....                      | 54 |
| 7.4 PORT SECURITY LIMIT .....     | 55 |
| 7.5 ACCESS MANAGEMENT.....        | 55 |
| 7.6 802.1X .....                  | 56 |
| 7.7 ACL .....                     | 57 |
| 7.7.1 ACL Ports.....              | 57 |
| 7.7.2 Rate Limiter.....           | 58 |
| 7.8 DHCP SNOOPING.....            | 60 |
| 7.8.1 DHCP Snooping.....          | 62 |
| 7.8.2 DHCP Snooping Table.....    | 63 |
| 7.9 IP & MAC SOURCE GUARD.....    | 63 |
| 7.9.1 Configuration.....          | 64 |
| 7.9.2 Static Table.....           | 64 |
| 7.9.3 Dynamic Table.....          | 66 |
| 7.10 ARP INSPECTION.....          | 66 |
| 7.10.1 Port Configuration.....    | 67 |
| 7.10.2 VLAN Configuration.....    | 68 |
| 7.10.3 Static Table.....          | 69 |
| 7.10.4 Dynamic Table.....         | 70 |
| 7.11 AAA.....                     | 70 |
| 7.11.1 RADIUS.....                | 70 |
| 7.11.2 TACACS+.....               | 71 |
| 8 QOS.....                        | 71 |
| 8.1 PORT CLASSIFICATION.....      | 73 |
| 8.2 PORT POLICING.....            | 74 |
| 8.3 QUEUE POLICING .....          | 75 |
| 8.4 PORT SCHEDULER .....          | 76 |
| 8.5 PORT SHAPING.....             | 77 |
| 8.6 PORT TAG REMARKING.....       | 77 |
| 8.7 PORT DSCP .....               | 78 |
| 8.8 DSCP-BASED QOS.....           | 79 |

|                                |           |
|--------------------------------|-----------|
| 8.9 DSCP TRANSLATION .....     | 79        |
| 8.10 DSCP CLASSIFICATION ..... | 80        |
| 8.11 QoS CONTROL LIST.....     | 81        |
| 8.12 STORM POLICING .....      | 81        |
| <b>9 DIAGNOSTICS .....</b>     | <b>82</b> |
| 9.1 PING .....                 | 82        |
| 9.2 CABLE DIAGNOSTICS.....     | 83        |
| 9.3 CPU LOAD.....              | 83        |
| <b>10 MAINTENANCE .....</b>    | <b>84</b> |
| 10.1 RESTART DEVICE .....      | 84        |
| 10.2 FACTORY DEFAULTS .....    | 84        |
| 10.3 FIRMWARE UPGRADE .....    | 85        |
| 10.4 FIRMWARE SELECT.....      | 85        |
| 10.5 CONFIGURATION .....       | 86        |

## Revision history

| 일자         | 버전    | 설명    |
|------------|-------|-------|
| 2020-11-30 | V 1.0 | 최초 작성 |

※ 본 문서는 Firmware 버전 V1.1-2020-11-20 을 기준으로 작성되었으며, 펌웨어에 따라 WEB UI 의 디자인 및 메뉴 구성에 차이가 있을 수 있습니다.

# 1 소개 및 설치

## 1.1 제품 주요 사양

| General Performance Indicator |  |
|-------------------------------|--|
| Product Model                 | MR-0802P Series  |
| Interface                     | 8×10/100/1000M PoE Ports + 2×2.5G SFP Ports + 1×Console Port         |
| Poe Parameters                | PoE Standard: IEEE802.3at(30W) and IEEE802.3af(15.4W)                |
|                               | PoE compatibility: IEEE 802.3af/at adaptive                          |
| Power Supply                  | Machine input voltage: DC48~55V                                      |
|                               | 4PIN Industrial Terminal   |
| Physical Dimension            | Product size: 270×180×44.5mm   |
|                               | Product weight: 1.2kg  |
|                               | Protect grade: IP40  |
| Working Environment           | Operating Temperature: -40 ~ 85 °C                                   |
|                               | Storage Temperature: -40 ~ 85 °C                                     |
|                               | Humidity: 5% ~ 95%, non-condensing                                   |
| Technical Indicators          |  |
| Bandwidth                     | 26Gbps   |
| Packet Forwarding rate        | 19.34Mpps  |
| Flash Capacity                | 16M  |
| MAC                           | 8K   |
| Layer 2 Software Function     |  |
| Port Management               | Enable/Disable Port, Speed, Duplex, MTU Setting, Flow-control        |
| Port Mirroring                | Support port mirroring   |
| Port Speed Limit              | Support port speed limit   |
| Port Isolation                | Support port isolation settings                                      |
| Storm Suppression             | Support unknown unicast, multicast, broadcast type storm suppression |
| Link Aggregation              | Support static manual aggregation and LACP dynamic aggregation       |
| VLAN                          | Support, VLAN and IEEE 802.1Q VLAN                                   |
| MAC                           | Support static addition, deletion                                    |
| Spanning Tree                 | STP, RSTP, MSTP  |
| Ring Network Protocol         | ERPS   |
| Extended Function             |  |
| ACL                           | Based on MAC, IP, protocol type, L4 port                             |
| QoS                           | Based on 802.1p(CoS) and DSCP classification(MR-0802P-S only)        |
| LLDP                          | Support LLDP link discovery protocol                                 |
| User Setting                  | Add/delete users   |
| Log                           | User login, operation, status, events                                |

|                            |  |
|----------------------------|--|
| System management          | Device reset, configuration save/restore, upgrade management |
| <b>Management Function</b> |  |
| CLI                        | Support serial port command line management                  |
| SSH                        | Support SSHv1/2 remote management                            |
| Telnet                     | Support telnet remote management                             |
| Web                        | Support Layer2 settings                                      |
| SNMP                       | SNMP V1/V2/V3  |
| PoE                        | PoE Power Management   |
| Other functions            | TACACS+ and RADIUS Certification(MR-0802P-S only)            |

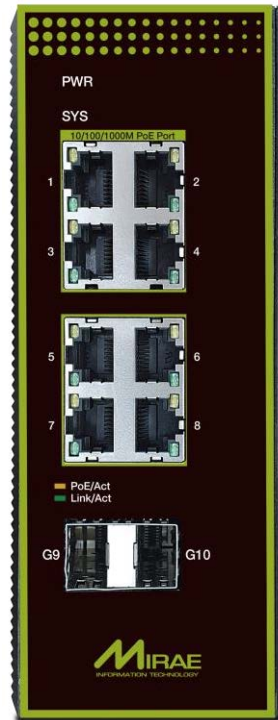
## 1.2 제품 구성품

- ▶ MR-0802P Switch × 1 대
- ▶ 제품 사양서 × 1 개
- ▶ 접지케이블 × 1 개
- ▶ 콘솔케이블 × 1 개
- ▶ 월마운트 브래킷 × 1 개

※ 본 제품에 전원공급장치는 포함되어 있지 않습니다.

## 1.3 제품 외관

### ▶ 제품 전면부



## 1.4 제품 설치

### ▶ 제품 설치 방법

1. 제품에 부착되어 있는 DIN-Rail 마운트 브라켓을 이용하여 DIN-Rail 에 설치합니다. 본 제품은 Fanless 제품으로 설치 시 통풍에 유의하십시오.
2. DC 전원(48~55V)을 연결하고, 제품 전면부의 PWR 와 SYS LED 점등을 확인합니다. 웹 UI 또는 콘솔 포트를 이용해 제품이 정상 동작하는지 확인합니다.
3. SFP 모듈(GBIC)을 사용할 경우 9~10 번 포트에 장착합니다.
4. TP 포트 또는 SFP 포트에 케이블을 이용하여 네트워크 디바이스를 연결합니다. PoE 장치를 연결할 경우 본 제품에서 PoE 기능이 포트별로 자동 활성화 됩니다.

## 2 Web Page Login

### 2.1 네트워크 관리 클라이언트에 로그인

기본 스위치 주소 : http://192.168.2.1 을 입력하고 "Enter"를 누릅니다.

PC 의 IP 네트워크 세그먼트를 스위치의 IP 네트워크 세그먼트와 동일하게 유지하되 로그인 할 때 IP 주소를 구분하십시오. 첫 번째 로그인에 대해 PC 의 IP 주소를 192.168.2.x 로 설정하고 서브넷 마스크를 255.255.255.0 으로 설정하십시오 (1 < x ≤ 254 ).

다음과 같은 로그인 창이 나타납니다. 기본 사용자 이름 "admin"과 암호 "admin"을 입력합니다. 스위치 시스템을 보려면 "로그인"을 클릭하십시오.

로그인

http://192.168.2.3

이 사이트로의 연결은 비공개가 아닙니다.

사용자이름


비밀번호

로그인

취소

MR-0802P Series

192.168.2.1



1 2 3 4 5 6 7 8 9 10

Information & Status

Network Admin

Port Configure

PoE

Advanced Configure

Security Configure

QoS Configure

Diagnostics

Maintenance

System Information

System Information

|                     |                              |
|---------------------|------------------------------|
| Company Name        | MIRAE Information Technology |
| Website and Contact | www.mreit.co.kr              |
| Hardware            |                              |
| Model Name          | MR-0802P Series              |
| MAC Address         | 34-58-7C-00-35-E9            |
| SN                  | 078452103310001              |
| Time                |                              |
| System Date         | 1970-01-01T00:16:47+00:00    |
| System Uptime       | 0d 00:16:47                  |
| Firmware            |                              |
| Firmware Version    | V1.1-2020-11-20              |
| Firmware Date       | 2020-11-20T06:33:21-08:00    |

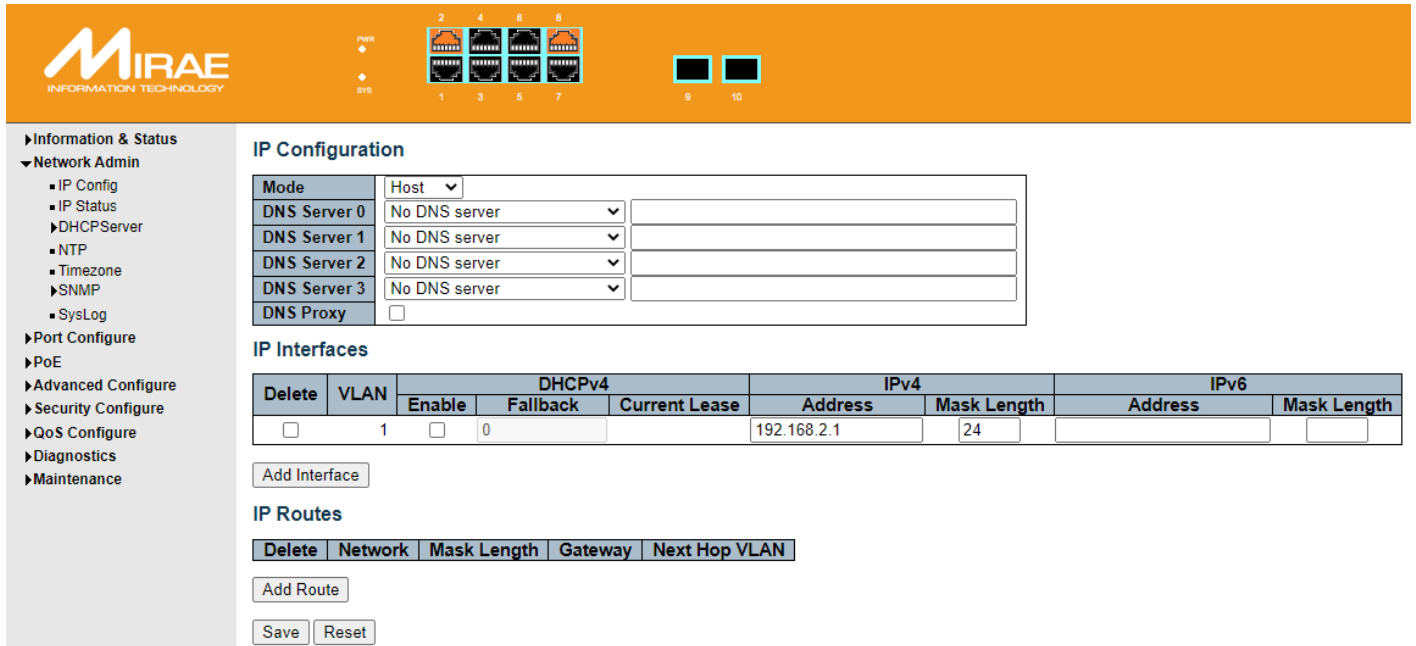
Auto-refresh ☐ Refresh



## 3 Network Admin

### 3.1 IP Config

다음과 같이 “Network Admin - IP Config” 를 클릭합니다.



IP Config 에 대한 설명:

| 구성 항목          | 설 명   |
|----------------|---|
| Mode           | 호스트 모드 및 라우터 모드에서 선택  |
| DNS Server     | DNS 서버 없음, 구성 가능한 IPv4, IPv4, 모든 DHCPv4 인터페이스 및 이 DHCPv4 인터페이스에서 선택   |
| DNS Proxy      | DNS Proxy   |
| Interface Name | 시스템 인터페이스의 이름을 표시합니다.   |
| VLAN           | 스위치에 액세스하고 관리하려면 VLAN 을 입력하십시오.   |
| IPv4 DHCP      | <ul style="list-style-type: none"> <li>- Enabled 상태는 VLAN 인터페이스가 IPv4 DHCP 클라이언트를 통해 스위치 IPv4 주소를 동적으로 가져 오는 것을 의미합니다. 그렇지 않으면 고정 IP 구성이 수행됩니다.</li> <li>- Waiting time (단위 : s)은 스위치가 DHCP 를 통해 유동 IP 주소를 얻으려고 시도하는 시간을 의미합니다. 0 초의 경우 시간 초과되지 않습니다.</li> <li>- 현재 IP 주소는 DHCP 를 통해 얻습니다.</li> </ul> |
| IPv4           | <ul style="list-style-type: none"> <li>- IP address: 사용자가 입력한 고정 IPv4 주소입니다.</li> <li>- IP mask: 사용자가 입력한 고정 IPv4 서브넷 마스크입니다.</li> </ul>  |

|           |   |
|-----------|---|
| IPv6      | <ul style="list-style-type: none"> <li>- IP address: 사용자가 입력한 고정 IPv6 주소입니다.</li> <li>- IP mask: 사용자가 입력한 고정 IPv6 서브넷 마스크입니다.</li> </ul>  |
| IP Routes | <ul style="list-style-type: none"> <li>- Destination segment: 사용자가 입력한 IPv4 주소입니다.</li> <li>- IP mask: 사용자가 입력한 고정 IPv4 서브넷 마스크입니다.</li> <li>- Next hop address: 사용자가 입력한 다음 IPv4 주소입니다.</li> </ul> |

“Add” 를 클릭하여 새 관리 VLAN 및 IP 주소를 만들고 “Save” 하고 마칩니다.

참고 : 스위치는 기본적으로 VLAN1 만 생성합니다. 다른 관리 스위치를 사용해야하는 사용자는 먼저 VLAN 모듈에 VLAN 및 관련 포트를 추가하여 VLAN 간의 레이어 3 통신을 실현해야 합니다.

## 3.2 IP Status

다음과 같이 “Network Admin - IP Status” 를 클릭합니다

**Information & Status**

- Network Admin
  - IP Config
  - IP Status
  - DHCP Server
  - NTP
  - Timezone
  - SNMP
  - SysLog
- Port Configure
- PoE
- Advanced Configure
- Security Configure
- QoS Configure
- Diagnostics
- Maintenance

**IP Interfaces**

| Interface | Type | Address                      | Status                           |
|-----------|------|------------------------------|----------------------------------|
| OS:lo     | LINK | 00-00-00-00-00-00            | <UP LOOPBACK RUNNING MULTICAST>  |
| OS:lo     | IPv4 | 127.0.0.1/8                  |                                  |
| OS:lo     | IPv6 | fe80::1/64                   |                                  |
| OS:lo     | IPv6 | ::1/128                      |                                  |
| VLAN1     | LINK | 34-58-7c-00-35-e9            | <UP BROADCAST RUNNING MULTICAST> |
| VLAN1     | IPv4 | 192.168.2.3/24               |                                  |
| VLAN1     | IPv6 | fe80::3658:7cff:fe00:35e9/64 |                                  |

**IP Routes**

| Network      | Gateway   | Status    |
|--------------|-----------|-----------|
| 127.0.0.1/32 | 127.0.0.1 | <UP HOST> |
| 224.0.0.0/4  | 127.0.0.1 | <UP>      |
| ::1/128      | ::1       | <UP HOST> |

**ARP Table**

| IP Address                | Link Address            |
|---------------------------|-------------------------|
| 192.168.2.234             | VLAN1:00-e0-4c-60-60-b7 |
| fe80::3658:7cff:fe00:35e9 | VLAN1:34-58-7c-00-35-e9 |

| 구성 항목         | 설 명           |
|---------------|---------------|
| IP Interfaces | IP 포트 테이블 확인  |
| IP Routes     | IP 라우팅 테이블 확인 |
| ARP Table     | ARP 테이블 확인    |

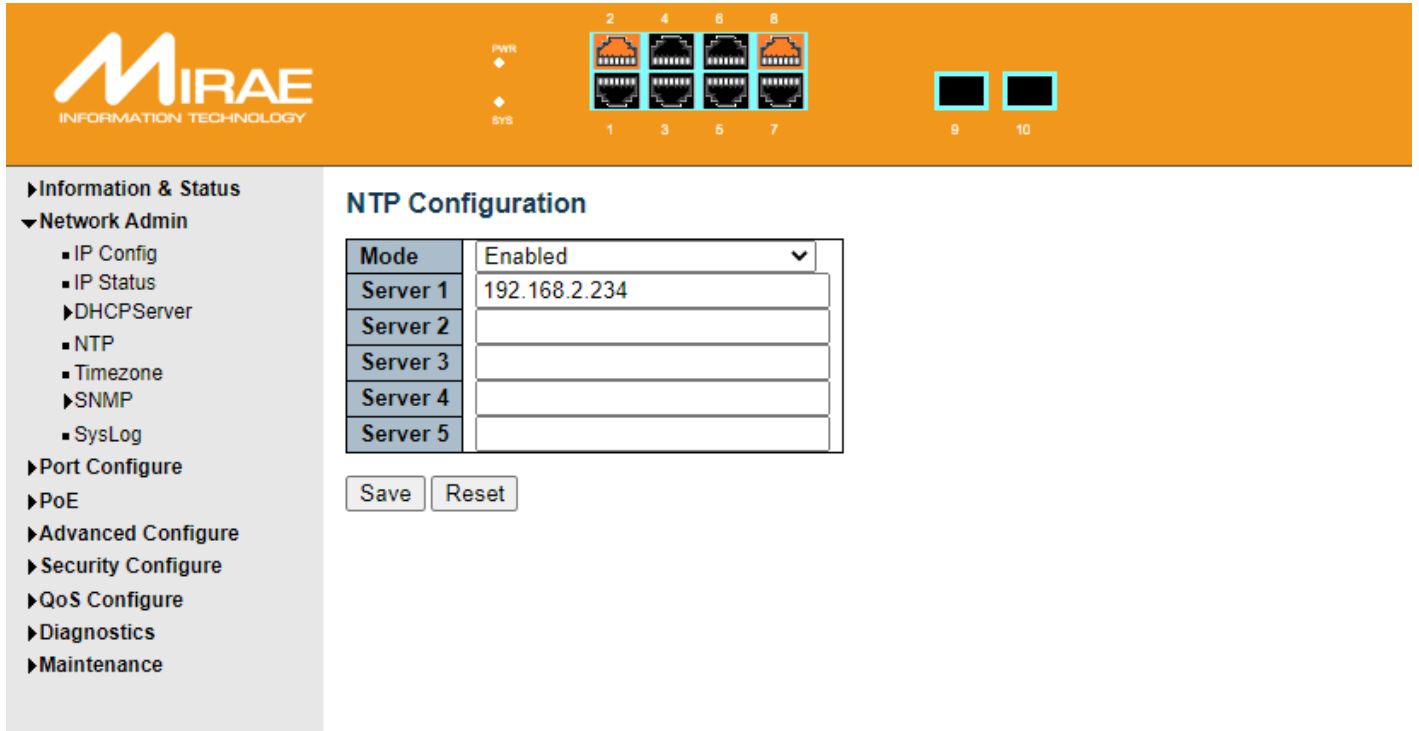
### 3.3 NTP

시간 서버와 클라이언트 간의 시계 동기화에 적용되는 NTP (Network Time Protocol)는 IP 및 UDP 를 기반으로 구현되는 TCP / IP 프로토콜 제품군의 응용 프로그램 계층에 있습니다.

NTP 메시지는 123 번 포트에 UDP 를 통해 전송됩니다. 모든 네트워크 장치의 클럭 동기화는 점점 복잡해지는 네트워크 토폴로지에서 결정적인 역할을 합니다.

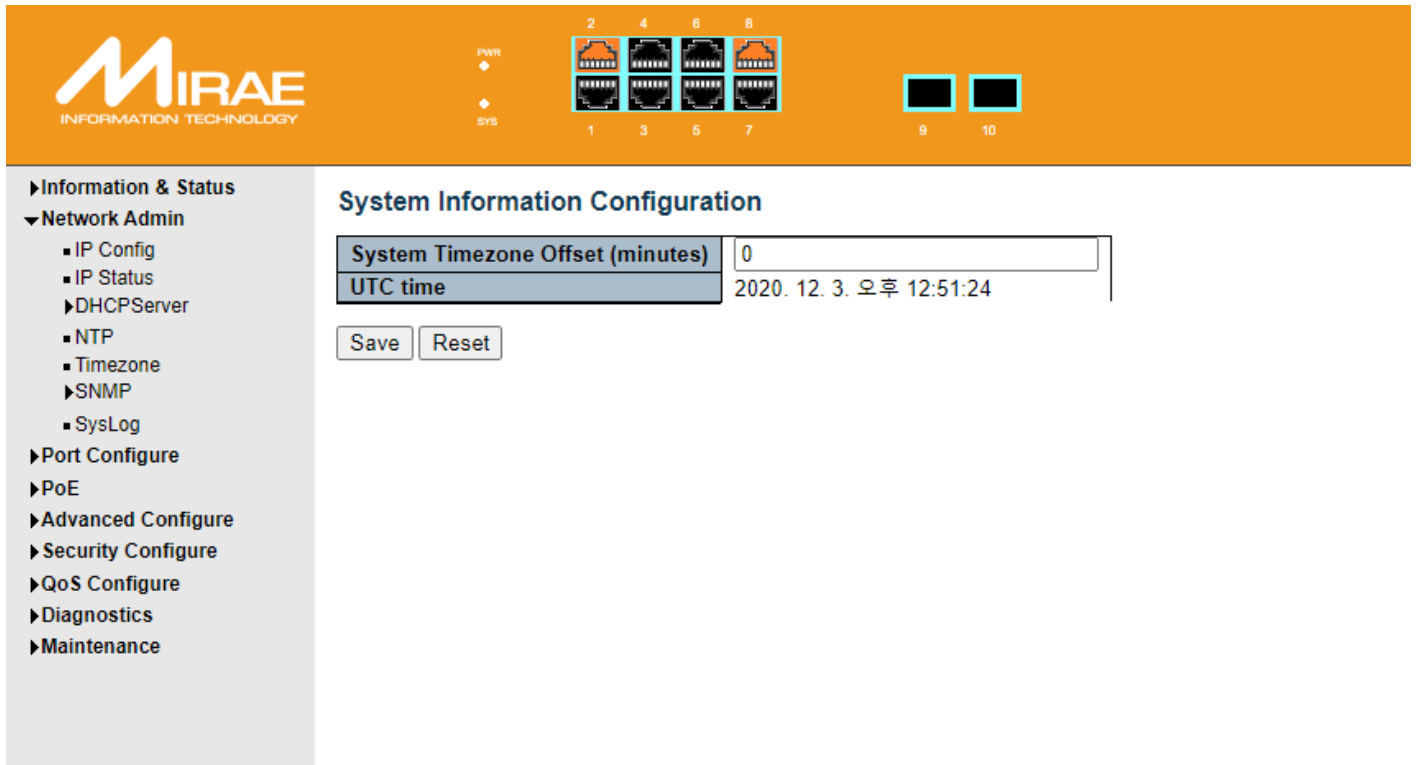
관리자가 시스템 시계를 수동으로 수정하면 작업 부하와 부정확한 시간이 발생하므로 NTP 가 유용합니다.

1. 다음과 같이 탐색 모음에서 “Network Admin - NTP” 를 클릭합니다.



| 구성 항목      | 설 명                               |
|------------|-----------------------------------|
| Mode       | 목록을 드롭 다운하여 NTP 를 활성화 또는 비활성화합니다. |
| NTP Server | 해당 IP 주소와 NTP 정보는 NTP 서버에서 가져옵니다. |

1. 다음과 같이 탐색 표시 줄에서 “Network Admin - Timezone” 을 클릭합니다.

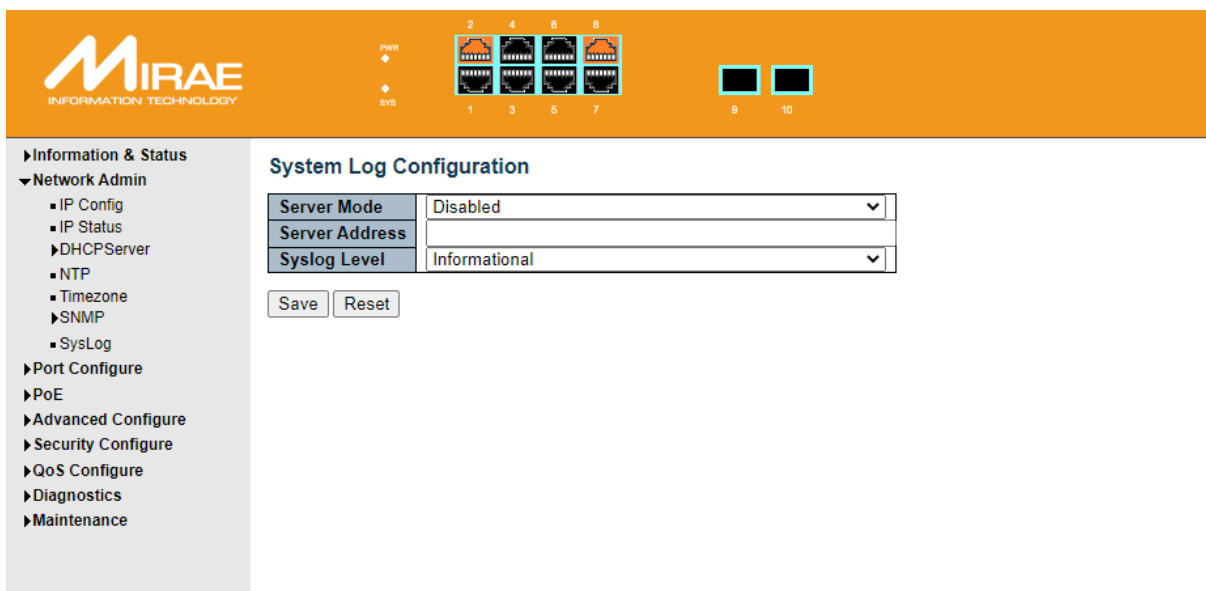


| 구성 항목                             | 설 명            |
|-----------------------------------|----------------|
| System Time-zone Offset (minutes) | 수정할 시간을 설정합니다. |
| UTC Time                          | 현재 인터넷 시간      |

## 3.4 Syslog

사용자는 스위치 로그를 TFTP 서버에 업로드 할 수 있습니다.

1. 다음과 같이 “Network Admin - SysLog” 를 클릭합니다:



| 구성 항목             | 설 명   |
|-------------------|---|
| Mode              | Syslog 기능을 활성화 또는 비활성화합니다. 활성화 된 경우 스위치는 syslog 를 지정된 서버로 보냅니다.               |
| Server IP Address | 지정된 로그 서버의 IP 주소  |
| Log Levels        | <b>Info</b> : 정보, 경고 및 오류.<br><b>Warning</b> : 경고 및 오류.<br><b>Error</b> : 오류. |

### 3.5 SNMP

SNMP (Simple Network Management Protocol)는 TCP / IP 네트워크에서 널리 사용됩니다.

네트워크 관리 소프트웨어 (예 : 네트워크 관리 워크 스테이션)를 운영하는 중앙 컴퓨터로 장치를 관리합니다. SNMP의 특징은 다음과 같습니다:

**Simple**: 폴링 구동 SNMP에는 빠른 속도와 저렴한 비용으로 소규모 환경에 적용할 수 있는 기본 기능 세트가 있습니다. 또한 UDP 기반 SNMP는 대부분의 장치와 호환됩니다.

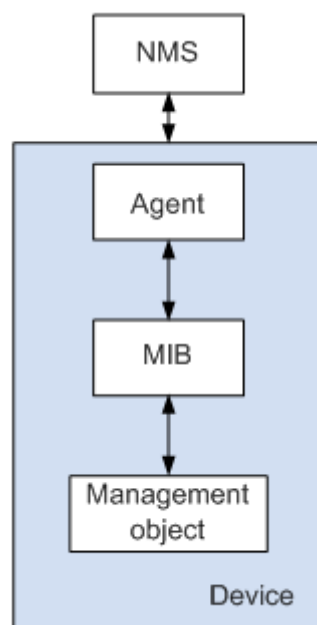
**Powerful**: SNMP는 관리자가 정보를 쉽게 검색, 수정 및 문제를 해결할 수 있도록 두 노드 간의 관리 정보 전송을 보장하는 것을 목표로합니다.

세 가지 공통 버전, 즉 SNMPv1, v2c 및 v3이 있습니다. 시스템에는 NMS (네트워크 관리 시스템), 에이전트, 관리 개체 및 MIB (관리 정보베이스)가 포함됩니다.

관리 센터인 NMS는 모든 장치를 관리합니다.

관리 중인 각 장치에는 상주 에이전트, MIB 및 관리 개체가 포함됩니다. NMS는 MIB를 작동하여 NMS 주문을 실행하는 관리 개체에서 실행되는 에이전트와 상호 작용합니다.

#### SNMP 관리 모델



NMS

- 네트워크 관리자로서 NMS는 서버에서 SNMP를 통해 네트워크 장치를 관리 / 모니터링합니다.

에이전트가 구성 항목 값을 조회하거나 수정해야 할 수 있습니다. NMS 는 에이전트가 능동적으로 보낸 트랩을 수신하여 관리되는 장치의 상태를 업데이트할 수 있습니다.

#### Agent

- 관리 장치의 에이전트 프로세스로서 장치 데이터를 유지하고 관리 데이터를 보고하여 NMS 요청에 응답합니다. 에이전트는 MIB Table 을 통해 관련 주문을 처리하고 요청을 받은 후 결과를 NMS 로 다시 보냅니다. 장치는 장애 또는 기타 이벤트가 발생하면 에이전트를 통해 현재 장치 상태와 관련된 정보를 NMS 로 전송합니다.

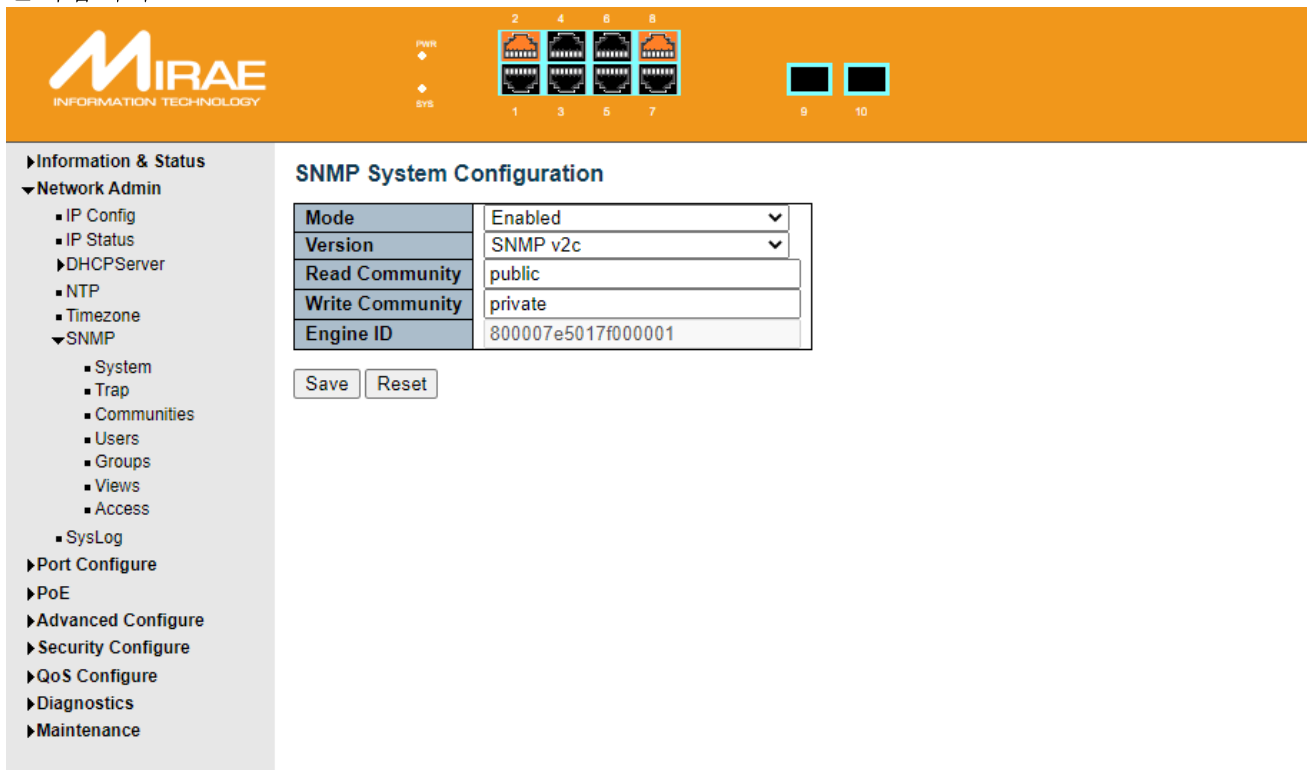
#### Management object

- 관리중인 개체를 나타냅니다. 각 장치는 하드웨어 (예 : 인터페이스 보드), 부분적인 하드웨어 및 소프트웨어 (예 : 라우팅 프로토콜), 기타 구성 항목 세트를 포함하여 둘 이상의 개체를 가질 수 있습니다.

#### MIB

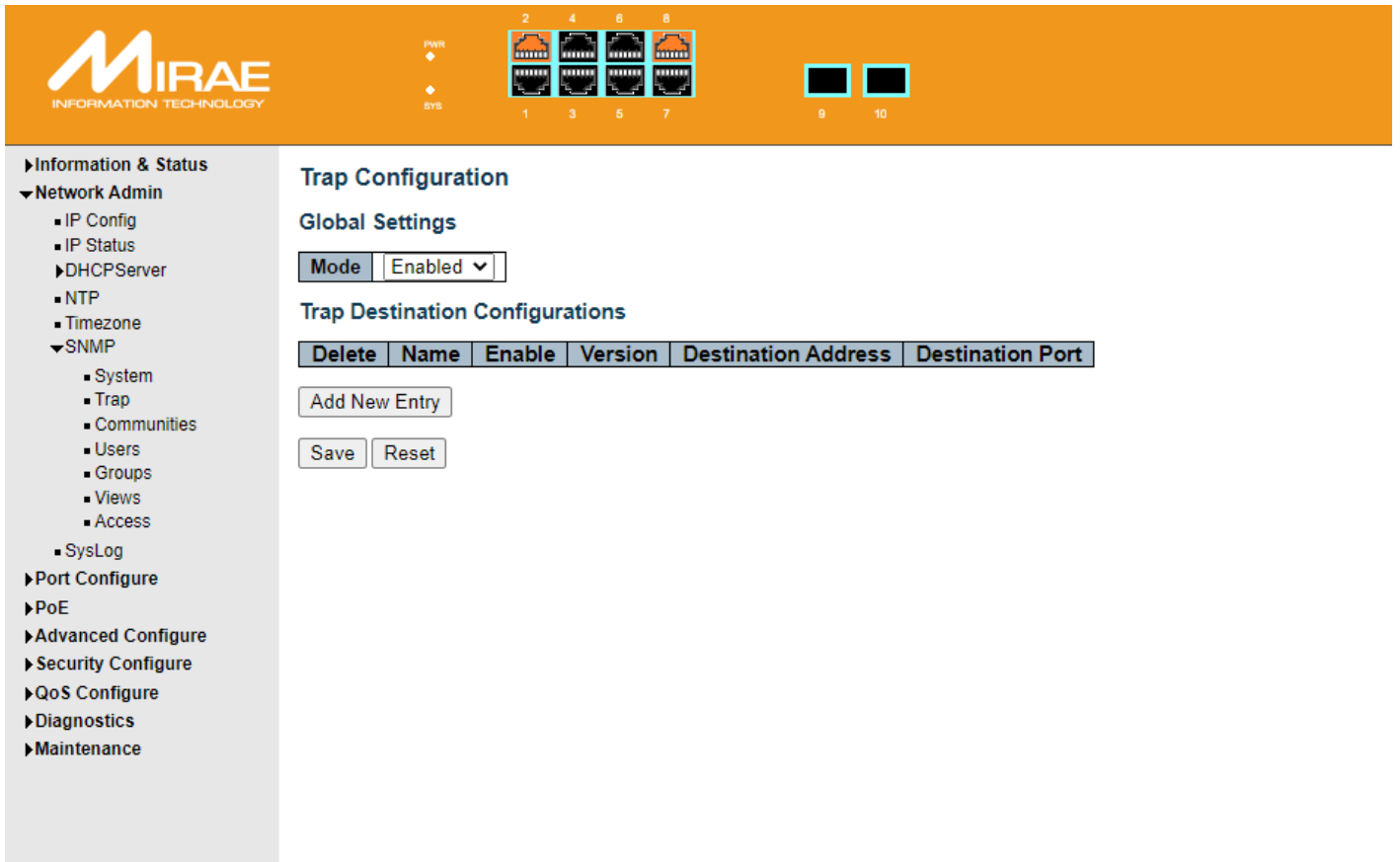
- MIB 는 관리 개체가 유지 관리하는 변수 (예 : 에이전트가 조회하고 설정할 수 있는 정보)를 지정하는 데이터베이스입니다. MIB 는 이름, 상태, 액세스 권한 및 데이터 유형을 포함하여 관리 개체의 속성을 정의합니다. MIB 를 통해 다음과 같은 기능을 구현할 수 있습니다. 에이전트는 MIB 를 조회하여 즉각적인 장치 정보를 마스터하고 MIB 를 변경하여 상태 구성 항목을 설정합니다.

1. 다음과 같이 탐색 트리에서 “SNMP System Configuration” 의 “Network Admin - SNMP” 를 클릭합니다.



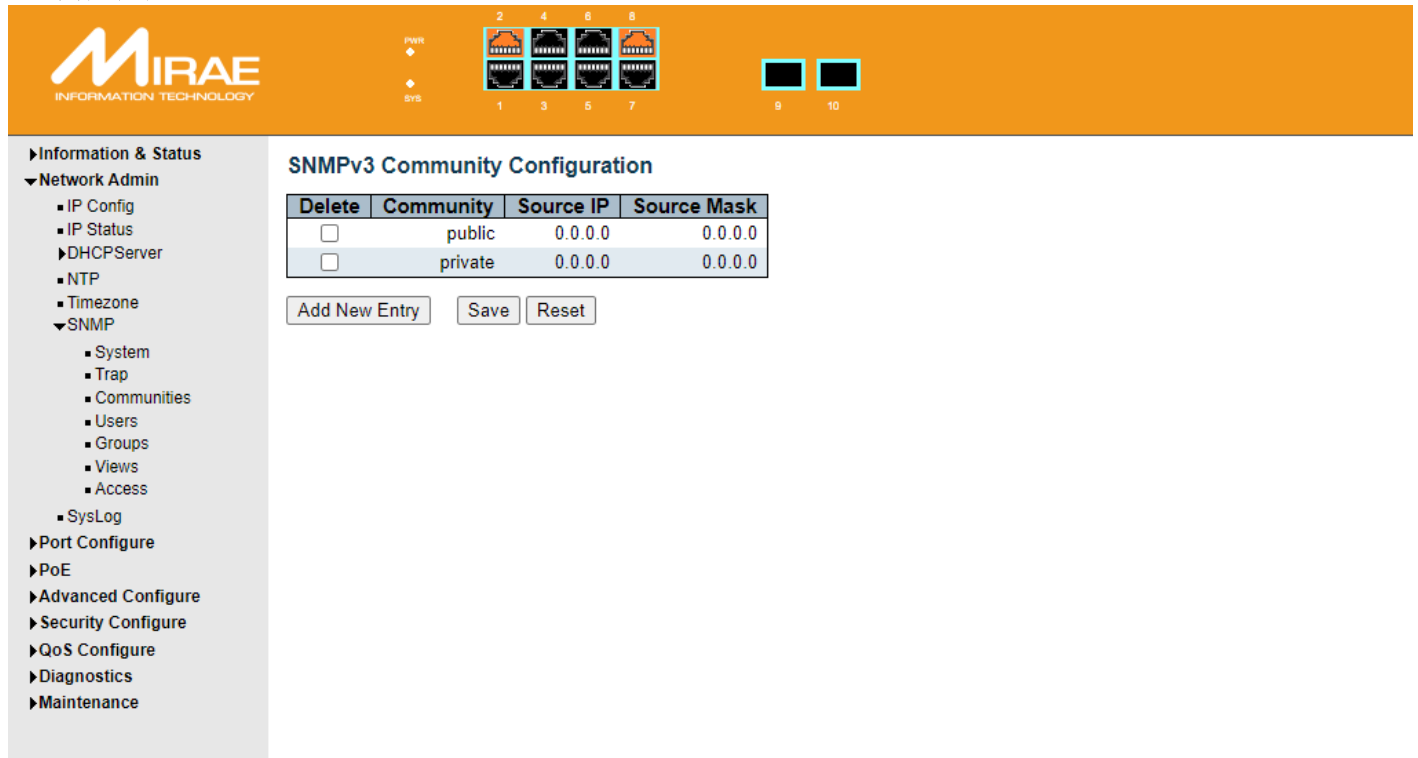
| 구성 항목           | 설 명  |
|-----------------|--|
| SNMP Mode       | SNMP 기능 활성화 또는 비활성화                                      |
| Version         | 목록을 드롭 다운하여 SNMPv1, v2c 또는 v3 을 선택합니다                    |
| Read Community  | 인증 된 관리 사이트는 기본적으로 “public” 라고하는 MIB 개체를 읽을 수 있습니다       |
| Write Community | 인증 된 관리 사이트는 기본적으로 “private” 이라고하는 MIB 개체를 읽고 수정할 수 있습니다 |

2. 사용자는 스위치의 SNMP 트랩 및 SNMP 인증 트랩 기능을 활성화 및 비활성화 할 수 있습니다. 다음과 같이 “Network Admin - SNMP - Trap” 을 클릭합니다:



| 구성 항목                                  | 설 명                       |
|--|---------------------------|
| Trap Name                              | SNMP 트랩 별칭                |
| Trap Mode                              | SNMP 트랩 활성화 또는 비활성화       |
| Trap Version                           | SNMPv1, v2c 및 v3          |
| Trap Community                         | 지정된 SNMP 트랩 커뮤니티의 그룹 이름   |
| Trap Destination IP Address            | 지정된 SNMP 트랩 서버의 IP 주소     |
| Trap Destination UDP Port              | 지정된 SNMP 트랩 서버의 UDP 포트 번호 |
| Trap Inform/Response Mode              | 활성화 또는 비활성화               |
| Trap Inform/Response Timeout (seconds) | 기간                        |
| Trap Inform/Response Retry Times       | 횟수                        |

3. 사용자는 커뮤니티 이름을 바꿀 수 있습니다. 다음과 같이 “Network Admin - SNMP - Communities” 를 클릭합니다:

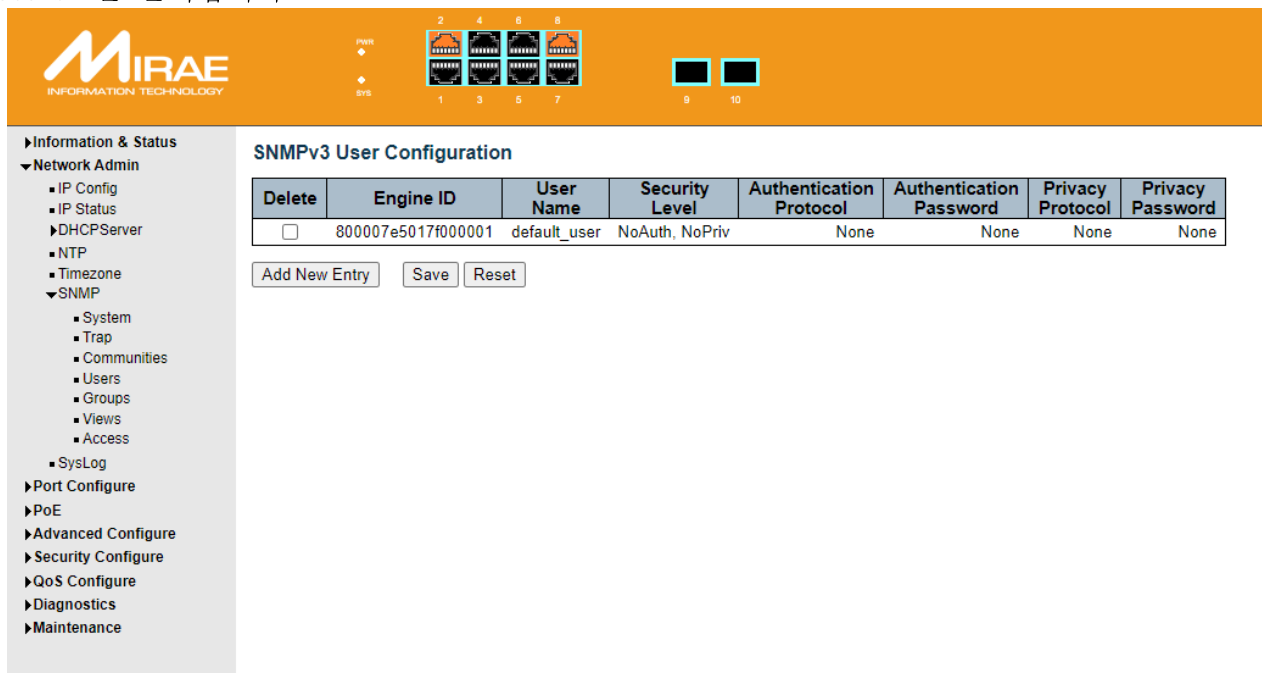


**SNMPv3 Community Configuration**

| Delete                   | Community | Source IP | Source Mask |
|--------------------------|-----------|-----------|-------------|
| <input type="checkbox"/> | public    | 0.0.0.0   | 0.0.0.0     |
| <input type="checkbox"/> | private   | 0.0.0.0   | 0.0.0.0     |

| 구성 항목       | 설 명                |
|-------------|--------------------|
| Community   | 새 이름 입력            |
| Source IP   | IPv4 소스 주소를 입력하십시오 |
| Source Mask | IPv4 서브넷 마스크 입력    |

4. SNMP v3 사용자를 만들고 개인 정보 보호 방법을 선택합니다. 다음과 같이 “Network Admin - SNMP - Users” 를 클릭합니다:



**SNMPv3 User Configuration**

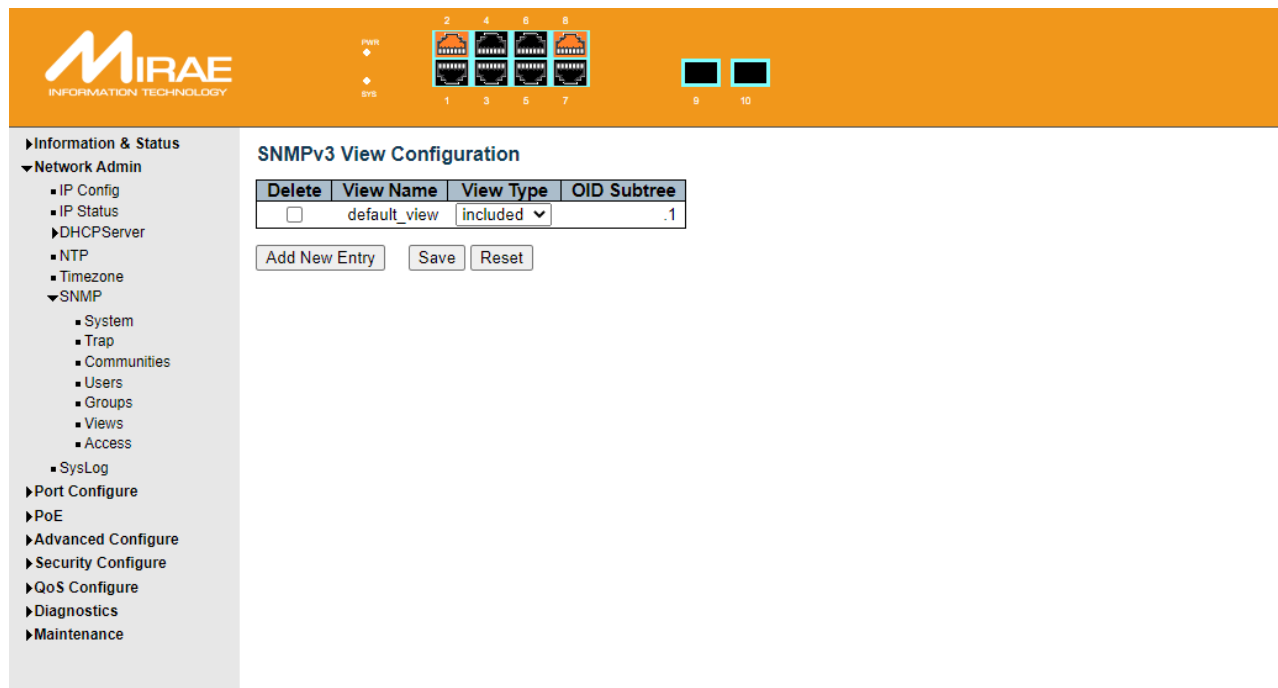
| Delete                   | Engine ID          | User Name    | Security Level | Authentication Protocol | Authentication Password | Privacy Protocol | Privacy Password |
|--------------------------|--------------------|--------------|----------------|-------------------------|-------------------------|------------------|------------------|
| <input type="checkbox"/> | 800007e5017f000001 | default_user | NoAuth, NoPriv | None                    | None                    | None             | None             |



| 구성 항목                   | 설명   |
|-------------------------|--|
| Engine ID               | 스위치에는 기본값 800007e5017f000001 이 권장됩니다                             |
| Username                | SNMPv3 사용자의 새 이름을 입력하십시오   |
| Security Level          | 목록을 드롭 다운하여 noAuthnoPriv, authNoPriv 및 authPriv 에서 암호화 방법을 선택합니다 |
| Authentication Protocol | 목록을 드롭 다운하여 MD5 또는 SHA 에서 개인 정보 보호 프로토콜을 선택합니다.                  |
| Authentication Password | 개인 정보 비밀번호를 입력하세요.   |
| Privacy Protocol        | 목록을 드롭 다운하여 DES 또는 AES 에서 개인 정보 보호 프로토콜을 선택합니다.                  |
| Privacy Password        | 개인 정보 비밀번호를 입력하세요  |

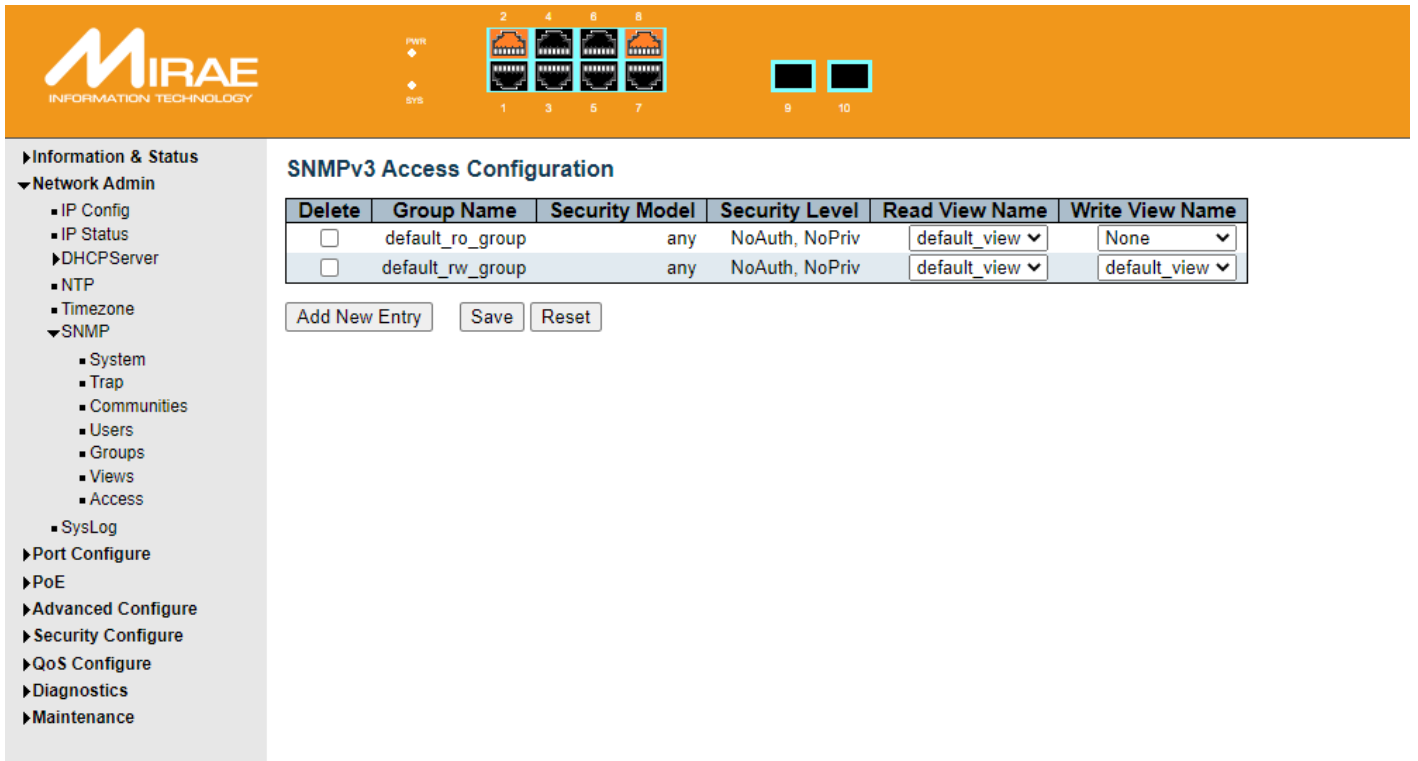
“Save” 하고 완료합니다.

5. 사용자는 SNMPv3 의 새 View 를 만들 수 있습니다. 다음과 같이 “Network Admin - SNMP - Views” 를 클릭합니다:



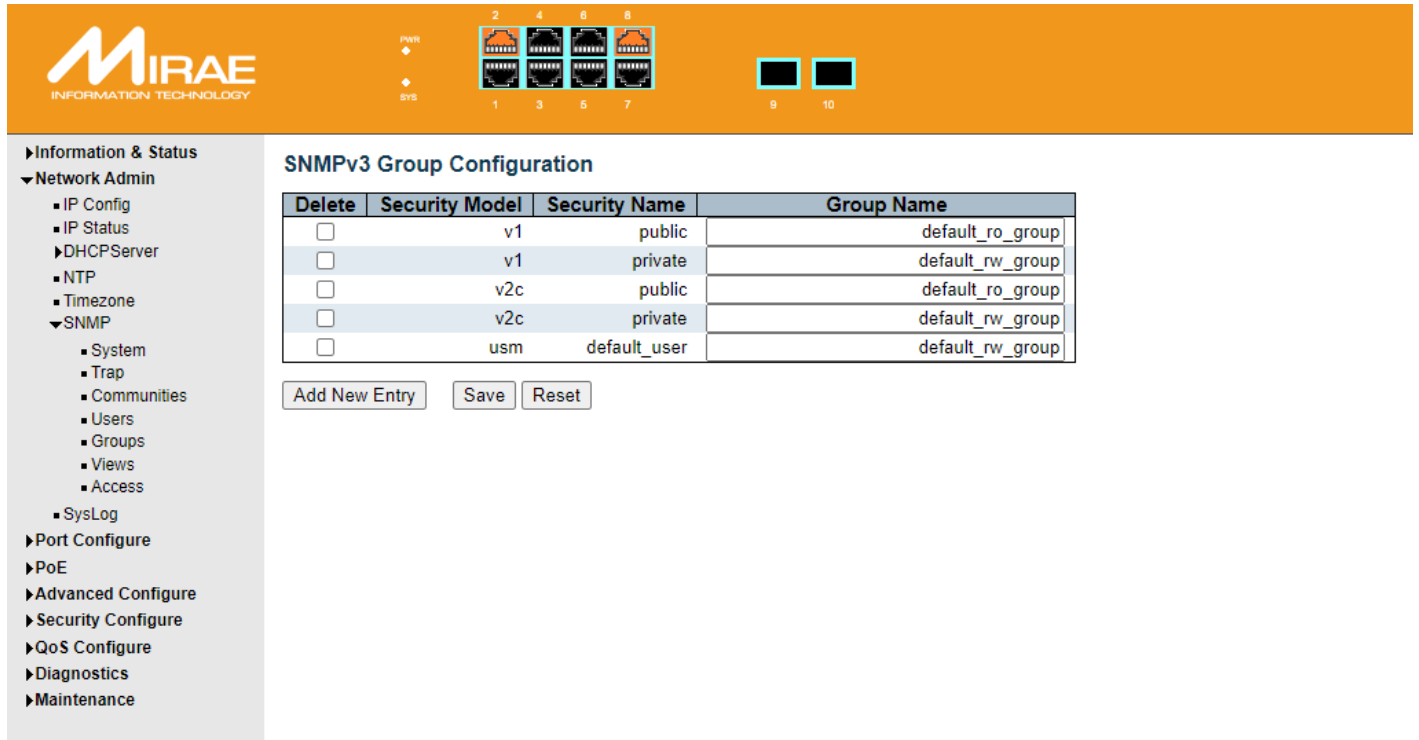
| 구성 항목       | 설명                       |
|-------------|--------------------------|
| View Name   | 이름을 입력하세요                |
| View Type   | 목록을 드롭 다운하여 포함 및 제외에서 선택 |
| OID Subtree | OID 하위 트리를 입력합니다         |

6. 사용자는 새 액세스를 통해 생성 된 뷰를 호출 할 수 있습니다. 다음과 같이 “Network Admin - SNMP - Access” 를 클릭합니다:



| 구성 항목           | 설명   |
|-----------------|--|
| Group Name      | 이름을 입력하세요  |
| Security Model  | 목록을 드롭 다운하여 임의, v1, v2c 및 usm 중에서 선택하십시오                         |
| Security Level  | 목록을 드롭 다운하여 noAuthnoPriv, authNoPriv 및 authPriv 에서 암호화 방법을 선택합니다 |
| Read View Name  | 목록을 드롭 다운하여 생성 된 View 를 선택합니다                                    |
| Write View Name | 목록을 드롭 다운하여 생성 된 View 를 선택합니다                                    |

7. 사용자는 새 그룹을 통해 생성 된 사용자 및 액세스를 호출 할 수 있습니다. 다음과 같이 “Network Admin - SNMP - Groups” 를 클릭합니다:



| 구성 항목          | 설명  |
|----------------|---|
| Security Model | 목록을 드롭 다운하여 v1, v2c 및 usm 중에서 선택합니다                       |
| Security Name  | 생성 된 사용자 이름, 그룹 이름 (v1 v2c) 및 사용자 이름 (usm)을 드롭 다운하고 선택합니다 |
| Group Name     | 허용 된 액세스 이름을 입력하세요  |

## 4 Port 구성

### 4.1 Ports

사용자가 필요에 따라 이더넷 인터페이스를 조회하고 구성할 수 있도록 인터페이스를 식별해야 합니다.

1. 탐색 모음에서 “Port Configure - Ports” 를 클릭합니다.

2. 다음과 같이 구성할 데이터와 구성 항목의 포트 설명, “Autonegotiation”, “Flow Control” 및 “Maximum Frame Size” 를 선택합니다.

| Port | Description | Link | Current | Speed | Configured | Adv Fdx | Hdx  | Adv speed | 10M  | 100M | 1G   | Enable | Flow Control | Maximum Frame Size | Excessive Collision Mode | Frame Length Check |
|------|-------------|------|---------|-------|------------|---------|------|-----------|------|------|------|--------|--------------|--------------------|--------------------------|--------------------|
| 1    |             | Down | Auto    | Auto  | Auto       | Auto    | Auto | Auto      | Auto | Auto | Auto | Auto   | Auto         | 9600               | Discard                  | Auto               |
| 2    |             | 1Gdx | Auto    | Auto  | Auto       | Auto    | Auto | Auto      | Auto | Auto | Auto | Auto   | Auto         | 9600               | Discard                  | Auto               |
| 3    |             | Down | Auto    | Auto  | Auto       | Auto    | Auto | Auto      | Auto | Auto | Auto | Auto   | Auto         | 9600               | Discard                  | Auto               |
| 4    |             | Down | Auto    | Auto  | Auto       | Auto    | Auto | Auto      | Auto | Auto | Auto | Auto   | Auto         | 9600               | Discard                  | Auto               |
| 5    |             | Down | Auto    | Auto  | Auto       | Auto    | Auto | Auto      | Auto | Auto | Auto | Auto   | Auto         | 9600               | Discard                  | Auto               |
| 6    |             | Down | Auto    | Auto  | Auto       | Auto    | Auto | Auto      | Auto | Auto | Auto | Auto   | Auto         | 9600               | Discard                  | Auto               |
| 7    |             | Down | Auto    | Auto  | Auto       | Auto    | Auto | Auto      | Auto | Auto | Auto | Auto   | Auto         | 9600               | Discard                  | Auto               |
| 8    |             | 1Gdx | Auto    | Auto  | Auto       | Auto    | Auto | Auto      | Auto | Auto | Auto | Auto   | Auto         | 9600               | Discard                  | Auto               |
| 9    |             | Down | Auto    | Auto  | Auto       | Auto    | Auto | Auto      | Auto | Auto | Auto | Auto   | Auto         | 9600               | Discard                  | Auto               |
| 10   |             | Down | Auto    | Auto  | Auto       | Auto    | Auto | Auto      | Auto | Auto | Auto | Auto   | Auto         | 9600               | Discard                  | Auto               |

구성 항목은 다음과 같습니다.

| 구성 항목              | 설 명   |
|--------------------|---|
| Autonegotiation    | 필수 10Mb, 100Mb 및 1,000Mb 상태로 구성 가능한 자동 협상. 10Mbps / s, 100Mbps / s 및 1,000Mbit / s 를 포함한 인터페이스 속도는 이더넷 전기 인터페이스에서 사용할 수 있으며 필요에 따라 선택 사항입니다.  |
| Flow Control       | 로컬 네트워크와 반대 네트워크 장치 모두에서 활성화되면 로컬 네트워크가 네트워크 정체가있는 경우 메시지 전송을 중지하도록 다른 장치에 알립니다.<br>반대쪽은 메시지 손실을 방지하기 위해 일시적으로 명령을 실행합니다.<br>Disable-Disabled 수신 및 PAUSE 프레임 전송;<br>Rx (RX Pause) -PAUSE 프레임을 수신합니다.<br>Both (Rx / Tx Pause)-PAUSE 프레임을 수신하고 전송합니다.<br>Tx (Tx Pause) -PAUSE 프레임을 전송합니다. |
| Maximum Frame Size | 9,600   |
| Enabled            | 포트 전환   |
| Port Description   | 설명 가능한 포트   |

## 4.2 Aggregation

Link Aggregation 은 물리적 인터페이스 그룹을 단일 논리적 인터페이스로 묶어 대역폭과 안정성을 높입니다.

LAG (Link Aggregation Group)는 여러 이더넷 링크 (Eth-Trunk)로 묶은 논리적인 링크입니다.

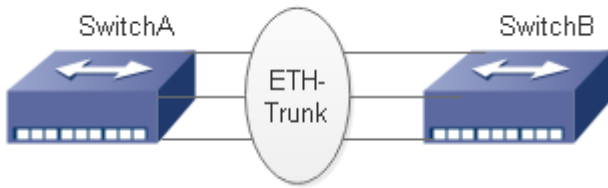
네트워크의 크기를 끊임없이 확장하면 링크 대역폭과 안정성에 대한 사용자의 요구가 증가합니다. 일반적으로 고속 인터페이스 장비는 대역폭을 최적화하기 위해 교체되지만 비용이 많이 들고 유연성이 떨어집니다.

Link Aggregation Technology 는 하드웨어를 업그레이드하지 않고 여러 물리적 인터페이스를 단일 논리적 인터페이스로 묶습니다. 백업 메커니즘은 안정성을 향상시킬뿐만 아니라 다른 물리적 링크에서 부하를 공유합니다.

아래와 같이 스위치 A 는 Eth-Trunk 논리 링크에 속한 3 개의 이더넷 링크를 통해 스위치 B 와 연결됩니다. 대역폭은 총 3 개 링크의 대역폭과 동일하므로 대역폭이 넓어집니다. 한편, 이 세 링크는

서로 백업되어 더 안정적입니다.

## Link Aggregation Diagram



Link Aggregation 은 다음의 상황에서 요구 사항을 충족할 수 있습니다.

- 하나의 링크로 연결된 두 스위치의 대역폭이 충분하지 않습니다.
- 하나의 링크로 연결된 두 개의 스위치의 신뢰성이 부족합니다.

Link Aggregation 은 LACP (Link Aggregation Control Protocol) 상태에 따라 수동 모드와 LACP 모드로 나눌 수 있습니다.

첫 번째 모드인 Eth-Trunk 설정에서 멤버 인터페이스 액세스는 LACP 없이 수동으로 추가해야 합니다. 모든 링크가 데이터 전달 및 부하 분산에 관련되기 때문에 로드 공유 모드(Load Sharing mode)라고도 합니다. 활성 링크 중 일부에 장애가 발생하는 경우 LAG 는 나머지 링크를 이용하여 부하 분산을 수행합니다. 이 모드는 직접 연결된 두 장치가 더 큰 링크 대역폭을 필요로 하지만 LACP 에 액세스 할 수 없는 상황에 적합합니다.

### 4.2.1 Static

Static Link Aggregation 를 추가하는 방법 (예 : 수동 모드):

1. “Port Configure - Aggregation - Static” 을 클릭합니다. 그룹 ID (1-16), Aggregation Mode Configuration(Src Mac, Dst Mac, IP 주소, TCP / UDP 포트 번호) 및 사용 포트를 선택합니다.

The screenshot shows the web interface of a MIRAE network switch. The top navigation bar includes the MIRAE logo, PWR, SYS, and a row of 10 port status icons. The left sidebar contains a menu with options like Information & Status, Network Admin, Port Configure, PoE, Advanced Configure, Security Configure, QoS Configure, Diagnostics, and Maintenance. The main content area is titled 'Aggregation Mode Configuration' and includes a 'Hash Code Contributors' section with checkboxes for Source MAC Address, Destination MAC Address, IP Address, and TCP/UDP Port Number. Below this is the 'Aggregation Group Configuration' section, which features a table for selecting port members for different group IDs.

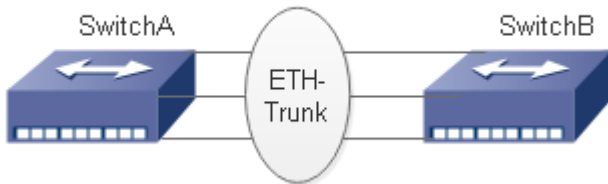
| Group ID | Port Members                     |                                  |                                  |                                  |                                  |                                  |                                  |                                  |                                  |                                  |
|----------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|
|          | 1                                | 2                                | 3                                | 4                                | 5                                | 6                                | 7                                | 8                                | 9                                | 10                               |
| Normal   | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> |
| 1        | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            |
| 2        | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            |
| 3        | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            |
| 4        | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            |
| 5        | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            |

At the bottom of the configuration area, there are 'Save' and 'Reset' buttons.

구성 항목은 다음과 같습니다.

| 구성 항목    | 설명   |
|----------|--|
| Group ID | 1 에서 16 까지 번호가 매겨진 16 개의 집계 그룹과 LAG ID 가 있습니다. |

이더넷 스위치 A 는 각 구성원 포트의 부하를 공유하기 위해 GE1 에서 GE3 까지 3 개의 포트를 통합합니다. 다음 구성은 Static Aggregation 의 예시입니다.



1. 스위치 B 구성 단계와 유사하게 스위치 A 는 Eth-Trunk 인터페이스를 생성하고 멤버 인터페이스에 액세스하여 링크 대역폭을 확장합니다. 그룹 ID "1", 부하 공유 모드(Src Mac, Dst Mac, IP 주소) 및 통합할 포트 (GE1, GE2 및 GE3) 를 선택하려면 “Port Configure - Aggregation - Static” 을 클릭하여 설정하십시오.

1

2

3

4

5

6

7

8

9

10

1

2

3

4

5

6

7

8

9

10

Information & Status

Network Admin

Port Configure

Ports

Aggregation

Static

LACP

Mirroring

Green Ethernet

DDM

PoE

Advanced Configure

Security Configure

QoS Configure

Diagnostics

Maintenance

Aggregation Mode Configuration

Hash Code Contributors

Source MAC Address

Destination MAC Address

IP Address

TCP/UDP Port Number

Aggregation Group Configuration

| Group ID | 1                                | 2                                | 3                                | 4                     | 5                     | 6                     | 7                     | 8                     | 9                     | 10                    |
|----------|----------------------------------|----------------------------------|----------------------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Normal   | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 1        | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 2        | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 3        | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 4        | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 5        | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/>            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Save

Reset

## 4.2.2 LACP

### 동적 링크 집계

IEEE 802.3ad 표준을 기반으로하는 LACP(Link Aggregation Control Protocol)는 링크를 동적으로 집계 및 분리합니다. LACP 는 LACPDU(Link Aggregation Control Protocol Data Unit)를 통해 상대방 네트워크 장치와 정보를 교환합니다. 포트가 LACP 를 사용하면 LACPDU를 전송하여 시스템 우선 순위, 시스템 MAC, 포트 우선 순위 및 번호, 작동 키를 상대 네트워크 장치에 알려줍니다. 상대방 장치는 이러한 정보를 수신한 후 다른 포트에서 저장한 정보와 비교하여 Dynamic Aggregation 에 대한 포트 참여 또는 종료에 대한 동의를 도달합니다. 동적 LACP 집계는 시스템에 의해 자동으로 생성 또는 삭제됩니다. 즉, 내부 포트를 자체적으로 추가하거나 제거할 수 있습니다. 속도, Duplex 가 동일한 장치에 연결된 포트만 통합할 수 있습니다.

동적 링크 통합을 추가하기 위한 지침 :

1. 탐색 모음에서 "Port Configure - Aggregation - LACP"를 클릭하여 포트, 유형 (LACP), 모드 (활성 또는 수동) 및 포트 우선 순위 (0-65,535, 기본 32,768)를 다음과 같이 선택합니다.

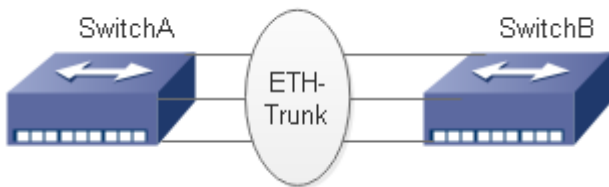
구성 항목은 다음과 같습니다

| 구성 항목         | 설 명   |
|---------------|---|
| LACP Enabled  | 활성화 및 비활성화  |
| Mode          | 액티브 또는 패시브<br>패시브 포트는 LACP 패킷을 수동으로 보내고 반대 네트워크 장치에서 보낸 패킷에만 응답합니다.<br>Active Port 는 LACP 데이터 패킷을 자동으로 보냅니다.<br>하나 또는 두 개의 활성 LACP 포트가 있는 링크를 동적으로 Aggregation 할 수 있습니다. 그러나 연결된 LACP 포트가 둘 다 패시브일 경우에는 서로 상대방의 패킷을 기다리고 있기 때문에 동작하지 않습니다 |
| Port Priority | LACP 는 포트 ID 우선 순위 에 따라 동적 집계 의 그룹 구성원 을 결정합니다. 이 중 장치 ID 는 2 바이트 시스템 우선 순위 와 6 바이트 시스템 MAC 으로 구성됩니다. 즉, 장치 ID 는 시스템 우선 순위 와 MAC 으로 구성됩니다. 동일한 경우 시스템 우선 순위를 먼저 비교하고 시스템 MAC 주소 를 다음으로 비교하며, 값이 작은 것이 우선합니다. 범위 : 0 ~ 65,535. 기본값은 32,768 |
| Key           | 자동 및 수동 모드  |

작업 패턴을 변경하기 전에 Eth-Trunk 에 대한 구성원 인터페이스 액세스 권한이 있는지 확인하십시오. 로컬 및 반대 네트워크 장치의 작업 패턴은 동일해야 합니다.

이더넷 스위치 A 는 각 구성원 포트의 부하를 공유하기 위해 GE1 에서 GE3, 스위치 B 까지 3 개의 포트를 통합합니다.

다음 구성은 Dynamic Aggregation 을 통해 예시됩니다.



다음은 스위치 A 의 구성으로, 포트를 통합하려면 스위치 B 의 구성과 동일해야 합니다.

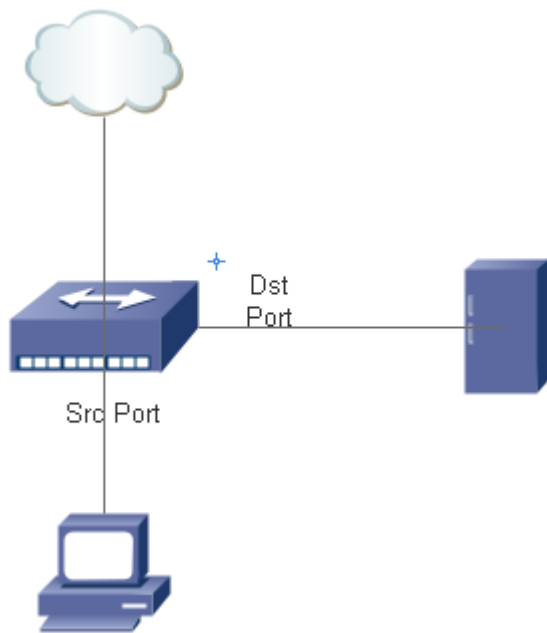
1. LACP 활성 포트 역할을 하려면 스위치 A 에서 시스템 우선 순위(Priority)를 100 으로 설정합니다. 탐색 모음에서 "Port Configure - Aggregation - LACP"를 클릭하여 다음과 같이 우선 순위를 "100"으로 설정합니다.

| Port | LACP Enabled                        | Key  | Role   | Timeout | Prio  |
|------|-------------------------------------|------|--------|---------|-------|
| *    | <input type="checkbox"/>            | <>   | <>     | <>      | 32768 |
| 1    | <input checked="" type="checkbox"/> | Auto | Active | Fast    | 100   |
| 2    | <input checked="" type="checkbox"/> | Auto | Active | Fast    | 100   |
| 3    | <input checked="" type="checkbox"/> | Auto | Active | Fast    | 100   |
| 4    | <input type="checkbox"/>            | Auto | Active | Fast    | 32768 |
| 5    | <input type="checkbox"/>            | Auto | Active | Fast    | 32768 |
| 6    | <input type="checkbox"/>            | Auto | Active | Fast    | 32768 |
| 7    | <input type="checkbox"/>            | Auto | Active | Fast    | 32768 |
| 8    | <input type="checkbox"/>            | Auto | Active | Fast    | 32768 |
| 9    | <input type="checkbox"/>            | Auto | Active | Fast    | 32768 |
| 10   | <input type="checkbox"/>            | Auto | Active | Fast    | 32768 |

## 4.3 Mirroring

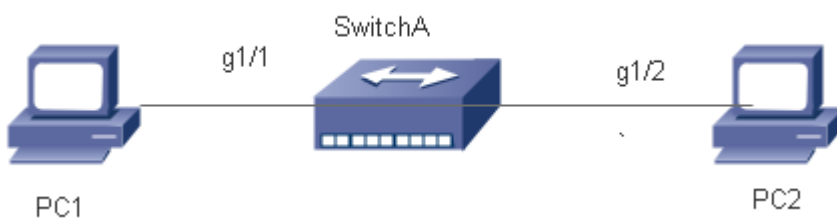
포트 미러링은 지정된 스위치 포트의 메시지를 대상 포트에 복사합니다. 복사된 포트는 소스 포트(Source)이고 복사 포트는 대상 포트(Destination)입니다. 대상 포트는 데이터 검사 장치를 사용하여 사용자가 수신된 메시지를 분석하여 다음과 같이 네트워크를 모니터링하고 문제를 해결합니다:





## 구성 예

PC1은 인터페이스 GE1-1을 통해 스위치 A에 액세스하고 PC2는 인터페이스 GE1-2에 직접 연결됩니다. 사용자는 관련 장치에서 PC2에서 PC1로 보낸 메시지를 모니터링하려고 합니다.



1. 탐색 모음에서 "Port Configure - Mirroring"을 클릭하여 세션 ID를 선택합니다.
2. 소스 포트 GE1-2를 확인하고 대상 포트 GE1-1 및 “Enabled” 모드를 선택한 후 다음과 같이 추가합니다.

The screenshot displays the Mirae Information Technology web interface. The top navigation bar includes links such as Information & Status, Network Admin, Port Configure, PoE, Advanced Config, Security Config, QoS Config, Diagnostics, and Maintenance. The main content area shows the "Mirror Configuration" section, which includes a "Port to mirror to" dropdown menu set to "1". Below this is the "Mirror Port Configuration" table, which lists ports 1 through 10 and the CPU, each with a "Mode" column set to "Disabled".

| Port | Mode     |
|------|----------|
| *    | <>       |
| 1    | Disabled |
| 2    | Enabled  |
| 3    | Disabled |
| 4    | Disabled |
| 5    | Disabled |
| 6    | Disabled |
| 7    | Disabled |
| 8    | Disabled |
| 9    | Disabled |
| 10   | Disabled |
| CPU  | Disabled |

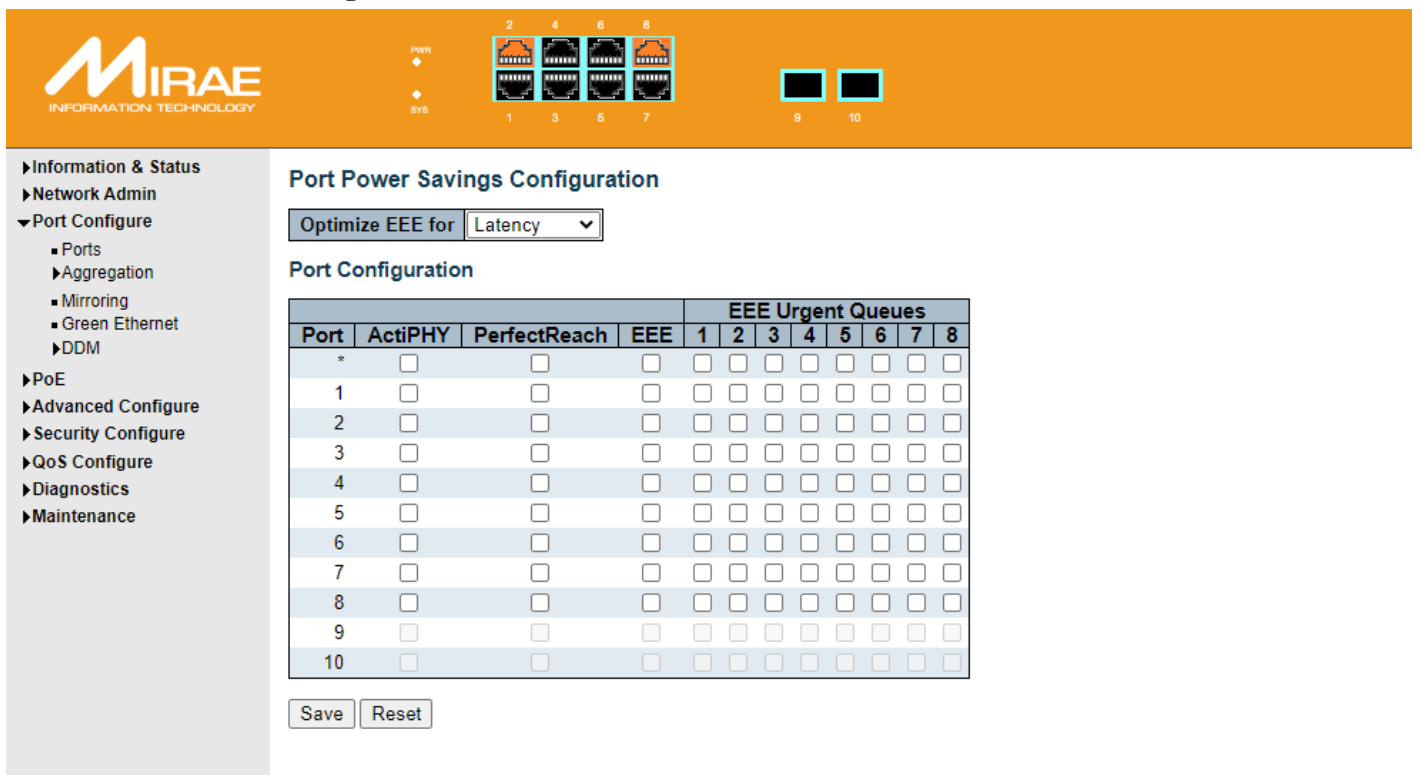
구성 항목은 다음과 같습니다

| 구성 항목            | 설 명  |
|------------------|--|
| Source Port      | 여러 포트를 사용할 수 있습니다.   |
| Destination Port | 링크 싱크 포트와 소스 포트를 제외하고 하나의 포트만 선택할 수 있습니다.  |
| Mode             | Rx only: 수신된 모든 메시지가 대상 포트에 미러링됩니다.<br>Tx only: 전송된 모든 메시지가 대상 포트에 미러링됩니다.<br>Enabled: 전송 및 수신된 모든 메시지를 대상 포트에 미러링합니다. |

## 4.4 Green Ethernet

흐름이 0 이하인 경우 포트 전원이 꺼집니다.

다음과 같이 “Port Configure - Green Ethernet” 을 클릭합니다:



**Port Power Savings Configuration**

Optimize EEE for: Latency

**Port Configuration**

| Port | ActiPHY                  | PerfectReach             | EEE                      | EEE Urgent Queues        |                          |                          |                          |                          |                          |                          |                          |                          |                          |
|------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
|      |                          |                          |                          | 1                        | 2                        | 3                        | 4                        | 5                        | 6                        | 7                        | 8                        |                          |                          |
| *    | <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"/> |
| 1    | <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"/> |
| 2    | <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"/> |
| 3    | <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"/> |
| 4    | <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"/> |
| 5    | <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    | <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"/> |
| 7    | <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"/> |
| 8    | <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"/> |
| 9    | <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"/> |
| 10   | <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"/> |

Save Reset

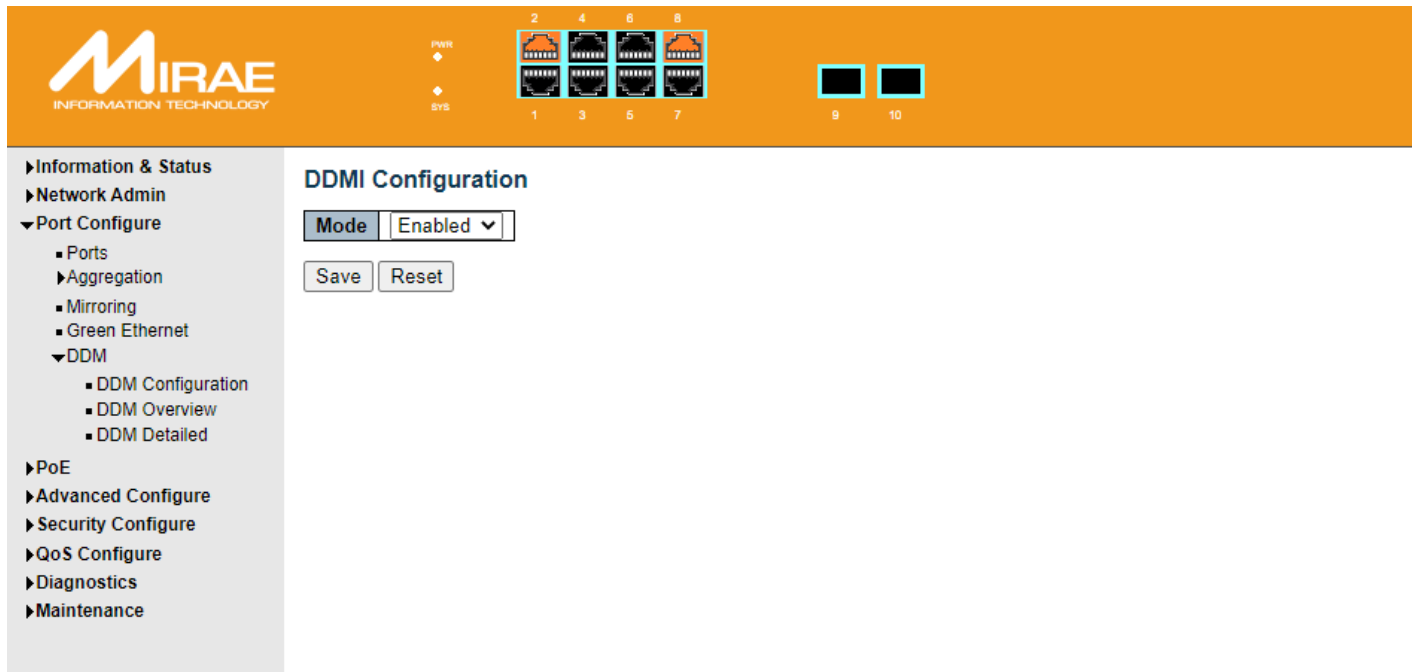
구성 항목은 다음과 같습니다

| 구성 항목              | 설 명   |
|--------------------|---|
| Optimize EEE for   | 전력 및 대기 시간에서 선택   |
| Port Configuration | “ActiPHY, PerfectReach, EEE, and EEE Urgent Queues” 에서 선택 |

## 4.5 DDM

DDM은 광 모듈의 정보를 볼 수 있습니다.

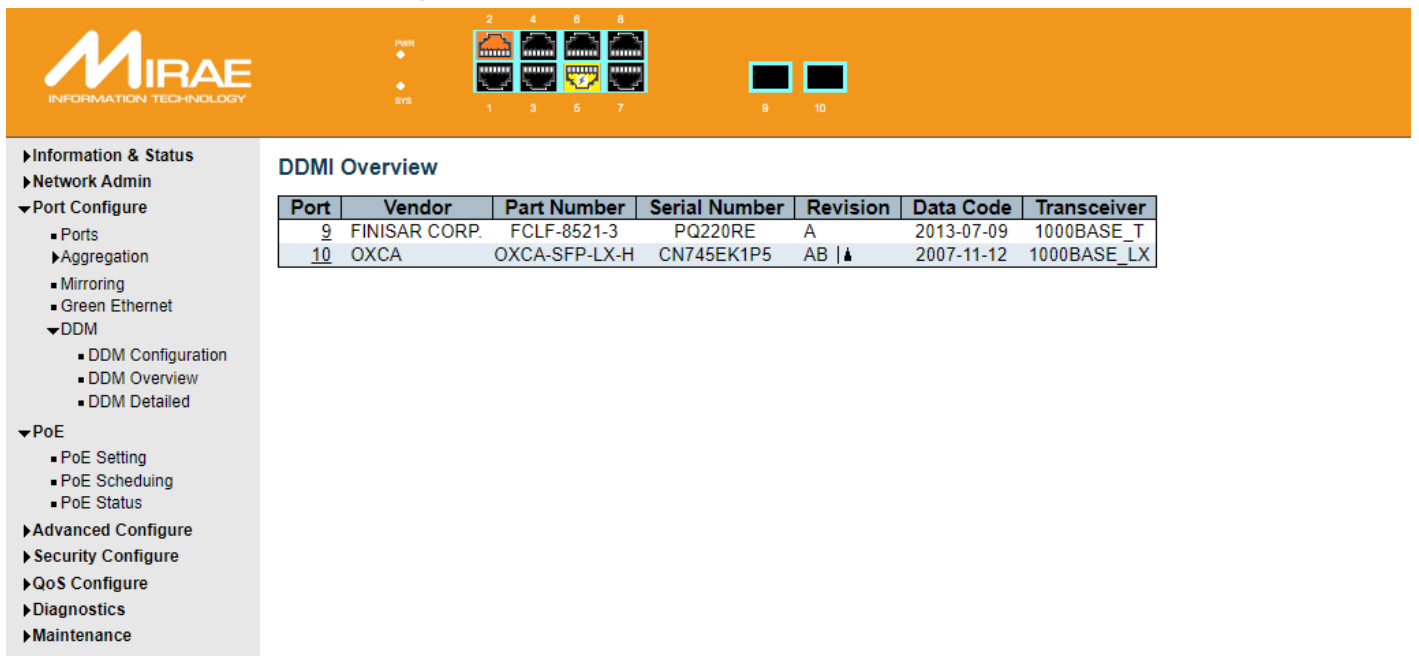
1. 다음과 같이 “Port Configure - DDM - DDMI Configuration” 을 클릭하십시오:



구성 항목은 다음과 같습니다

| 구성 항목              | 설 명        |
|--------------------|------------|
| DDMI Configuration | 활성화 및 비활성화 |

2. 다음과 같이 “Port Configure - DDM - DDMI Overview” 를 클릭하십시오:



구성 항목은 다음과 같습니다

| 구성 항목         | 설 명  |
|---------------|--|
| DDMI Overview | "포트, 공급 업체, 부품 번호, 일련 번호, 개정판, 데이터 코드 및 트랜시버"의 정보를 표시합니다." |

3. 다음과 같이 “Port Configure - DDM - DDM Detailed” 를 클릭합니다. 화면 우측에서 포트를 선택하여 트랜시버 정보를 확인합니다.

**Transceiver Information**

|               |               |
|---------------|---------------|
| Vendor        | FINISAR CORP. |
| Part Number   | FCLF-8521-3   |
| Serial Number | PQ220RE       |
| Revision      |               |
| Data Code     | 2013-07-09    |
| Transceiver   | 1000BASE_T    |

**DDMI Information**

| Type           | Current | High Alarm Threshold | High Warn Threshold | Low Warn Threshold | Low Alarm Threshold |
|----------------|---------|----------------------|---------------------|--------------------|---------------------|
| Temperature(C) | -       | -                    | -                   | -                  | -                   |
| Voltage(V)     | -       | -                    | -                   | -                  | -                   |
| Tx Bias(mA)    | -       | -                    | -                   | -                  | -                   |
| Tx Power(dBm)  | -       | -                    | -                   | -                  | -                   |
| Rx Power(dBm)  | -       | -                    | -                   | -                  | -                   |

## 5 PoE

PoE (Power over Ethernet)는 기존 Cat-5 네트워크 케이블 연결 상태를 변경하지 않고 IP (예 : IP 전화, WAP, IP 카메라)를 기반으로 단말기에 데이터 신호와 직류 전원을 공급합니다.

### 5.1 PoE Setting

1. 다음과 같이 탐색 표시 줄에서 “PoE - PoE Setting” 을 클릭합니다.

**Power Over Ethernet Configuration**

Reserved Power determined by ☒ Auto ☐ Manual

Power Management Mode ☒ Actual Consumption ☐ Reserved Power

**PoE Power Supply Configuration**

Primary Power Supply [W]

250

**PoE Port Configuration**

| Port | PoE Mode | Priority | PD Alive Check | Maximum Power [W] | Description |
|------|----------|----------|----------------|-------------------|-------------|
| *    | <>       | <>       | <>             | 30                |             |
| 1    | PoE+     | Low      | OFF            | 30                |             |
| 2    | PoE+     | Low      | OFF            | 30                |             |
| 3    | PoE+     | Low      | OFF            | 30                |             |
| 4    | PoE+     | Low      | OFF            | 30                |             |
| 5    | PoE+     | Low      | OFF            | 30                |             |
| 6    | PoE+     | Low      | OFF            | 30                |             |
| 7    | PoE+     | Low      | OFF            | 30                |             |
| 8    | PoE+     | Low      | OFF            | 30                |             |

Save Reset

구성 항목은 다음과 같습니다

| 구성 항목                        | 설 명  |
|------------------------------|--|
| Reserved Power determined by | 이 스위치에서는 두 가지 모드를 사용할 수 있습니다:<br>1. Auto distribution: 스위치 포트는 검사된 PD 등급에 따라 최대 전력을 자동으로 할당합니다. 해당 전원 표에서 802.3af / 802.3at 의 정의를 참조하십시오.<br>2. Manual distribution: 사용자가 직접 정의합니다.  |
| Power Management Mode        | 이 스위치에서는 두 가지 모드를 사용할 수 있습니다:<br>1. Actual consumption: 이 작업 패턴에서는 실제 소비 전력이 스위치의 정격 전력보다 많을 때 우선 순위가 가장 낮은 포트가 꺼집니다. 모든 우선 순위가 동일한 수준에 있으면 우선 순위가 가장 높은 포트가 꺼집니다<br>2. Reserved power: 이 작업 패턴에서 모든 포트의 최대 예비 전력이 스위치의 정격 전력을 초과하면 새 PD 장치가 있는 포트가 비활성화됩니다. |
| Primary Power Supply         | 사용자는 최대 전력을 직접 설정할 수 있습니다.   |
| PoE Mode                     | 스위치는 802.3af(PoE) 및 802.3at(PoE +) 모드를 지원합니다. 그리고 802.3at 는 공장 기본값입니다.   |
| Priority                     | PoE 포트의 우선 순위를 낮음에서 높음(낮음, 높음, 위험)으로 지정합니다   |
| Maximum Power (W)            | 전원 예약을 위한 “Manual Allocation” 모드는 포트의 최대 전원 공급을 지정합니다.   |

## 5.2 PoE Status

1. 다음과 같이 “PoE - PoE Status” 를 클릭합니다.

**Power Over Ethernet Status** Auto-refresh ☐

| Local Port | Description | PD class | Power Requested | Power Allocated | Power Used | Current Used | Priority | PD Alive Check | Reset Count | Port Status    |
|------------|-------------|----------|-----------------|-----------------|------------|--------------|----------|----------------|-------------|----------------|
| 1          |             | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | 0              | 0           | No PD detected |
| 2          |             | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | 0              | 0           | No PD detected |
| 3          |             | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | 0              | 0           | No PD detected |
| 4          |             | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | 0              | 0           | No PD detected |
| 5          |             | 3        | 15.4 [W]        | 15.4 [W]        | 3.6 [W]    | 67 [mA]      | Low      | 0              | 0           | PoE turned ON  |
| 6          |             | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | 0              | 0           | No PD detected |
| 7          |             | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | 0              | 0           | No PD detected |
| 8          |             | -        | 0 [W]           | 0 [W]           | 0 [W]      | 0 [mA]       | Low      | 0              | 0           | No PD detected |
| Total      |             |          | 15.4 [W]        | 15.4 [W]        | 3.6 [W]    | 67 [mA]      |          |                |             |                |

구성 항목은 다음과 같습니다

| 구성 항목                      | 설 명  |
|----------------------------|--|
| Power Over Ethernet Status | "로컬 포트, 설명, PD 등급, 요청된 전력, 할당된 전력, 사용된 전력, 현재 사용된 전력, 우선 순위 및 포트 상태"의 정보를 표시합니다. |

## 6 Advanced Configure

### 6.1 MAC Table

사용자는 스위치에서 MAC 주소와 관련된 구성을 조정할 수 있습니다.  
다음과 같이 “Advanced Configure - MAC Table” 을 클릭합니다:

구성 항목은 다음과 같습니다

| 구성 항목                       | 설 명   |
|-----------------------------|---|
| Disable Automatic Aging     | 이 옵션을 선택하면 스위치가 인식한 동적 MAC 주소가 자동으로 에이징되지 않습니다.   |
| Aging Time                  | 스위치가 학습한 동적 MAC 주소는 공장 기본값으로 300 초 후에 자동으로 에이징됩니다. 기간은 10 초에서 1,000,000 초까지입니다.   |
| Learn the MAC Address Table | 스위치는 MAC 주소의 3 가지 학습 모드와 호환됩니다.<br>Auto mode: 포트가 MAC 주소를 자동으로 학습합니다.<br>Disabled mode: 포트가 MAC 주소를 학습하지 않습니다.<br>Safe mode: 포트는 구성된 정적 (소스) MAC 주소의 데이터 흐름을 전달합니다. |

### 6.2 VLANS

VLAN 은 물리적 위치의 제한없이 동일한 VLAN 의 호스트를 개별적으로 배치할 수 있습니다. 각 VLAN 은 브로드캐스트 도메인으로서 물리적 LAN 을 여러 논리적 LAN 으로 나눕니다. 호스트는 기존 통신 방식으로 메시지를 교환할 수 있습니다. 다른 VLAN 에 있는 경우 라우터 또는 레이어 3 스위치와 같은 장치가 필요합니다.

VLAN 은 다음과 같은 측면에서 우수합니다:

Broadcast domain coverage: LAN 의 브로드캐스트 메시지는 대역폭을 절약하고 네트워크 관련 문제를 보다 효율적으로 처리하기 위해 VLAN 에서 제한됩니다.

LAN security: 데이터 링크 계층에서 메시지가 브로드 캐스트 도메인으로 분리되기 때문에 VLAN 호스트가 서로 통신하지 못합니다. 레이어 3 포워딩을 위해 라우터 또는 레이어 3 스위치가 필요합니다.

가상 작업 팀을 만드는 유연성: VLAN 은 물리적 네트워크의 제어를 넘어 가상 작업 팀을 만들 수 있습니다. 사용자는 물리적 위치가 범위 내에서 이동하는 경우 구성을 변경하지 않고도 네트워크에 액세스 할 수 있습니다.

본 제품은 IEEE 802.1Q 프로토콜(MAC 및 포트 기반 VLAN)을 지원합니다. 기본 구성의 경우 802.1Q VLAN 모드를 채택해야 합니다. 포트 기반 VLAN 은 스위치의 인터페이스 번호에 따라 구분됩니다. 네트워크 관리자는 각 스위치 인터페이스에 서로 다른 PVID, 즉 포트 기반 VLAN 을 제공합니다. VLAN 태그가 없는 데이터 프레임이 PVID 를 사용하여 스위치 인터페이스로 유입되면 동일한 PVID 로 표시되거나 인터페이스에 PVID 가 있어도 추가 태그가 제거됩니다.

1. 다음과 같이 “Advanced Configure - VLANs” 를 클릭합니다.

구성 항목은 다음과 같습니다.

| 구성 항목                        | 설 명   |
|------------------------------|---|
| Allowed Access VLANs         | 공장 기본적으로 VLAN 1 과 함께 허용된 액세스 VLAN 의 ID 목록을 표시합니다. 새 VLAN 의 ID 를 추가하십시오.   |
| Ethertype for Custom S-ports | 이 필드는 사용자 지정 S- 포트에 사용되는 Ethertype / TPID (16 진수로 지정)를 지정합니다. 이 설정은 포트 유형이 S-Custom-Port 로 설정된 모든 포트에 적용됩니다.  |
| Mode                         | <p>포트 모드 (기본값 : 액세스)는 해당 포트의 기본 동작을 결정합니다. 포트는 아래 설명된 세 가지 모드 중 하나일 수 있습니다.</p> <p>특정 모드가 선택될 때마다 해당 행의 나머지 필드가 회색으로 표시되거나 해당 모드에 따라 변경 가능하게 됩니다.</p> <p>회색으로 표시된 필드는 모드가 적용될 때 포트가 가져올 값을 보여줍니다.</p> <p><b>Access:</b><br/>           액세스 포트는 일반적으로 최종 스테이션에 연결하는 데 사용됩니다. 액세스 포트에는 다음과 같은 특성이 있습니다:</p> <ul style="list-style-type: none"> <li>정확히 하나의 VLAN 인 포트 VLAN (일명 액세스 VLAN)의 구성원이며 기본적으로 1 입니다</li> <li>태그가없는 프레임과 C 태그가 지정된 프레임 허용</li> <li>액세스 VLAN 으로 분류되지 않은 모든 프레임을 삭제합니다</li> </ul> |



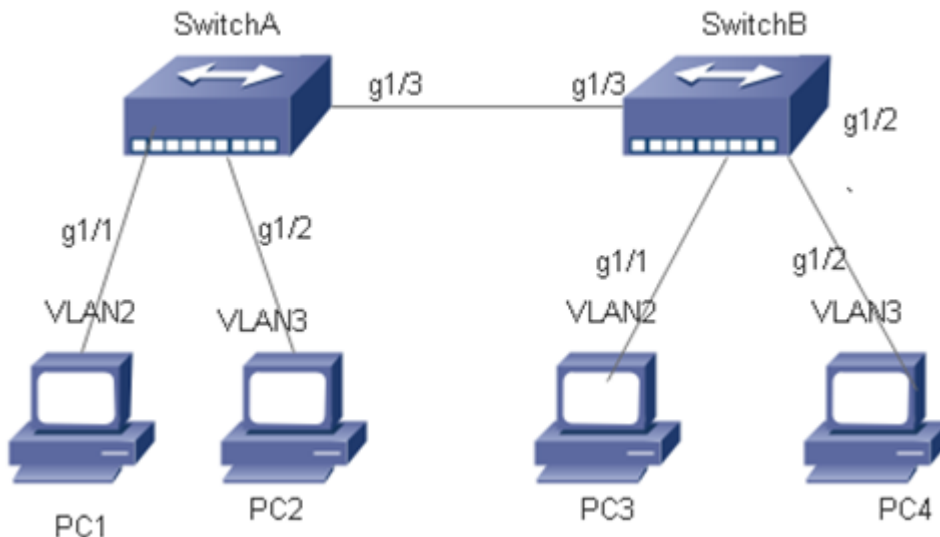
|           |   |
|-----------|---|
|           | <ul style="list-style-type: none"> <li>송신시 액세스 VLAN 으로 분류 된 모든 프레임은 태그없이 전송됩니다. 기타 (동적으로 추가 된 VLAN)는 태그로 전송됩니다</li> </ul> <p><b>Trunk:</b><br/>트렁크 포트는 여러 VLAN 에서 동시에 흐름을 전달할 수 있으며 일반적으로 다른 스위치에 연결하는 데 사용됩니다. 트렁크 포트에는 다음과 같은 특성이 있습니다:</p> <ul style="list-style-type: none"> <li>기본적으로 트렁크 포트는 모든 VLAN (1-4094)의 구성원입니다.</li> <li>트렁크 포트가 속한 VLAN 은 허용 된 VLAN 의 사용에 의해 제한될 수 있습니다.</li> <li>포트가 구성원이 아닌 VLAN 으로 분류된 프레임은 폐기됩니다.</li> <li>기본적으로 포트 VLAN (a.k.a. Native VLAN)으로 분류된 프레임을 제외한 모든 프레임은 송신시 태그가 지정됩니다. 포트 VLAN 으로 분류된 프레임은 송신시 C 태그가 지정되지 않습니다.</li> <li>송신 태그 지정을 변경하여 모든 프레임에 태그를 지정할 수 있습니다. 이 경우 태그가 지정된 프레임만 수신에 허용됩니다.</li> </ul> <p><b>Hybrid:</b><br/>하이브리드 포트는 여러면에서 트렁크 포트와 유사하지만 추가 포트 구성 기능을 추가합니다. 트렁크 포트에 대해 설명된 특성 외에도 하이브리드 포트에는 다음과 같은 기능이 있습니다:</p> <ul style="list-style-type: none"> <li>VLAN 태그를 인식하지 않거나 C- 태그 인식, S- 태그 인식 또는 S-custom-tag 인식으로 구성할 수 있습니다;</li> <li>수신 필터링을 제어 할 수 있습니다;</li> <li>프레임 수신 허용 및 송신 태깅 구성을 독립적으로 구성할 수 있습니다;</li> </ul> |
| Port VLAN | <p>포트의 VLAN ID (일명 PVID)를 결정합니다. 허용되는 VLAN 의 범위는 1 ~ 4094 이며 기본값은 1 입니다.</p> <p>수신시 포트가 VLAN 을 인식하지 못하도록 구성되었거나 프레임이 태그가 지정되지 않았거나 VLAN 인식이 포트에서 활성화되었지만 프레임이 우선 순위가 태그 된 경우 (VLAN ID = 0) 프레임은 포트 VLAN 으로 분류됩니다. 송신시 송신 태그 지정 구성이 포트 VLAN 태그 해제로 설정된 경우 포트 VLAN 으로 분류 된 프레임에 태그가 지정되지 않습니다.</p> <p>포트 VLAN 은 액세스 모드의 포트에 대해서는 "액세스 VLAN", 트렁크 또는 하이브리드 모드의 포트에 대해서는 기본 VLAN 이라고합니다.</p>  |
| Port Type | <p>하이브리드 모드의 포트는 포트 유형, 즉 프레임의 VLAN 태그가 특정 VLAN 에 대한 수신시 프레임을 분류하는 데 사용되는지 여부와 그럴 경우 반응하는 TPID 를 변경할 수 있습니다. 마찬가지로 송신시 포트 유형은 태그가 필요한 경우 태그의 TPID 를 결정합니다.</p> <p><b>Unaware:</b><br/>수신시 VLAN 태그를 전달하는지 여부에 관계없이 모든 프레임은 포트 VLAN 으로 분류되며 가능한 태그는 송신시 제거되지 않습니다.</p> <p><b>C-Port:</b><br/>수신시 TPID = 0x8100 인 VLAN 태그가있는 프레임은 태그에 포함 된 VLAN ID 로 분류됩니다. 프레임에 태그가 지정되지 않았거나 우선 순위가 지정되어 있으면 프레임이 포트 VLAN 으로 분류됩니다. 송신시 프레임에 태그를</p>   |



|                    |   |
|--------------------|---|
|                    | <p>지정해야하는 경우 C- 태그로 태그가 지정됩니다.</p> <p><b>S-Port:</b><br/>수신시 TPID = 0x8100 또는 0x88A8 인 VLAN 태그가있는 프레임은 태그에 포함된 VLAN ID 로 분류됩니다. 프레임에 태그가 지정되지 않았거나 우선 순위가 지정되어 있으면 프레임이 포트 VLAN 으로 분류됩니다. 송신시 프레임에 태그를 지정해야하는 경우 <b>S-tag</b> 로 태그가 지정됩니다.</p> <p><b>S-Custom-Port:</b><br/>수신시 TPID = 0x8100 이거나 Custom-S 포트 용으로 구성된 Ethertype 과 동일한 VLAN 태그가있는 프레임은 태그에 포함된 VLAN ID로 분류됩니다. 프레임에 태그가 지정되지 않았거나 우선 순위가 지정되어 있으면 프레임이 포트 VLAN 으로 분류됩니다. 송신시 프레임에 태그를 지정해야하는 경우 사용자 지정 <b>S-tag</b> 로 태그가 지정됩니다.</p> |
| Ingress Filter     | <p>하이브리드 포트를 통해 수신 필터링을 변경할 수 있습니다. 액세스 및 트렁크 포트에는 항상 수신 필터링이 활성화되어 있습니다.</p> <p>수신 필터링이 활성화된 경우 (확인란이 선택됨) 포트가 구성원이 아닌 VLAN 으로 분류된 프레임은 삭제됩니다.</p> <p>수신 필터링이 활성화된 경우 (확인란이 선택됨) 포트가 구성원이 아닌 VLAN 으로 분류된 프레임은 삭제됩니다. 그러나 포트는 구성원이 아닌 VLAN 으로 분류된 프레임을 전송하지 않습니다</p>  |
| Ingress Acceptance | <p>하이브리드 포트를 사용하면 수신시 허용되는 프레임 유형을 변경할 수 있습니다.</p> <p><b>Tagged and Untagged</b><br/>태그가 있는 프레임과 태그가 없는 프레임이 모두 허용됩니다.</p> <p><b>Tagged Only</b><br/>태그가 지정된 프레임 만 수신시 허용됩니다. 태그가 지정되지 않은 프레임은 삭제됩니다.</p> <p><b>Untagged Only</b><br/>태그가 지정되지 않은 프레임 만 수신시 허용됩니다. 태그가 지정된 프레임은 삭제됩니다.</p>  |
| Egress Tagging     | <p>트렁크 및 하이브리드 모드의 포트는 송신시 프레임 태그 지정을 제어 할 수 있습니다.</p> <p><b>Untag Port VLAN</b><br/>포트 VLAN 으로 분류 된 프레임은 태그없이 전송됩니다. 다른 프레임은 관련 태그와 함께 전송됩니다.</p> <p><b>Tag All</b><br/>포트 VLAN 으로 분류되었는지 여부에 관계없이 모든 프레임은 태그와 함께 전송됩니다.</p> <p><b>Untag All</b><br/>포트 VLAN 으로 분류되었는지 여부에 관계없이 모든 프레임은 태그없이 전송됩니다.<br/>이 옵션은 하이브리드 모드의 포트에만 사용할 수 있습니다.</p>   |
| Allowed VLANs      | <p>트렁크 및 하이브리드 모드의 포트는 구성원이 될 수있는 VLAN 을 제어 할 수 있습니다. 액세스 포트는 하나의 VLAN 인 액세스 VLAN에만 속할 수 있습니다. 필드의 구분은 Enabled VLANs 필드에 사용 된 구분과 동일합니다. 기본적으로</p>  |

|                 |   |
|-----------------|---|
|                 | 트렁크 또는 하이브리드 포트는 모든 VLAN 의 구성원이되므로 1-4094 로 설정됩니다.<br>이 필드는 비어있을 수 있습니다. 이는 포트가 VLAN 의 구성원이되지 않음을 의미합니다.  |
| Forbidden VLANs | 포트는 하나 이상의 VLAN 에 속하지 않도록 구성 될 수 있습니다. 이는 MVRP 및 GVRP 와 같은 동적 VLAN 프로토콜이 VLAN 에 포트를 동적으로 추가하는 것을 방지해야 할 때 특히 유용합니다.<br>트릭은 이러한 VLAN 을 해당 포트에서 금지 된 것으로 표시하는 것입니다. 구문은 Enabled VLANs 필드에 사용 된 구문과 동일합니다.<br>기본적으로이 필드는 비어 있습니다. 이는 포트가 가능한 모든 VLAN 의 구성원이 될 수 있음을 의미합니다. |
| Non-static port | 라디오 버튼을 클릭하고 포트를 비 정적 포트로 지정합니다. 모든 포트를 확인하려면 "Select all" 을 클릭하십시오 .   |

스위치 A 와 스위치 B 사이의 링크 중 VLAN 2 와 3 에서 사용자 통신을 지원하려면 연결 인터페이스와 2 개의 VLAN 을 추가해야 합니다. 즉, VALN 2 와 3 을 추가하고 스위치 A 와 스위치의 GE1-3 이더넷 인터페이스를 추가해야 합니다. B 를 구성해야 합니다.



1. 스위치 A 에서 VLAN 2 및 3 을 만들고 사용자 인터페이스에 VLAN 을 추가 한 다음 트렁크 모드에서 GE1-3 을 설정합니다. 스위치 B 도 같은 방법으로 탐색 트리에서 “Advanced Configure - VLANs” 을 클릭하고 관련 항목을 입력한 후 다음과 같이 구성을 저장하십시오.

1 2 3 4 5 6 7 8 9 10

1 2 3 4 5 6 7 8 9 10

Information & Status

Network Admin

Port Configure

PoE

Advanced Configure

- MAC Table
- VLANs
- GVRP
- Port Isolation
- Loop Protection
- Spanning Tree
- IPMC Profile
- MEP
- ERPS
- IGMP Snooping
- IPv6 MLD Snooping
- LLDP
- Security Configure
- QoS Configure
- Diagnostics
- Maintenance

### Global VLAN Configuration

|                              |        |
|------------------------------|--------|
| Allowed Access VLANs         | 1-4094 |
| Ethertype for Custom S-ports | 88A8   |

### Port VLAN Configuration

| Port | Mode   | Port VLAN | Port Type | Ingress Filtering                   | Ingress Acceptance  | Egress Tagging  | Allowed VLANs | Forbidden VLANs |
|------|--------|-----------|-----------|-------------------------------------|---------------------|-----------------|---------------|-----------------|
| *    | <>     | 1         | <>        | <input checked="" type="checkbox"/> | <>                  | <>              | 1             |                 |
| 1    | Access | 1         | C-Port    | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1             |                 |
| 2    | Access | 2         | C-Port    | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 2             |                 |
| 3    | Access | 3         | C-Port    | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 3             |                 |
| 4    | Access | 1         | C-Port    | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1             |                 |
| 5    | Access | 2         | C-Port    | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 2             |                 |
| 6    | Access | 1         | C-Port    | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1             |                 |
| 7    | Access | 1         | C-Port    | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1             |                 |
| 8    | Access | 1         | C-Port    | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1             |                 |
| 9    | Access | 1         | C-Port    | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1             |                 |
| 10   | Access | 1         | C-Port    | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag Port VLAN | 1             |                 |

Save
Reset

2. 스위치 A 의 인터페이스 타입과 VLAN 을 구성합니다. 스위치 B 도 같은 방법으로 탐색 트리에서 “Advanced Configure - VLANs” 을 클릭하고 관련 항목을 입력한 후 다음과 같이 구성을 저장하십시오. 다음은 VLAN 3 을 추가하는 단계와 유사한 VLAN 2 를 추가하는 방법을 보여줍니다.

### 3. 구성 결과 확인

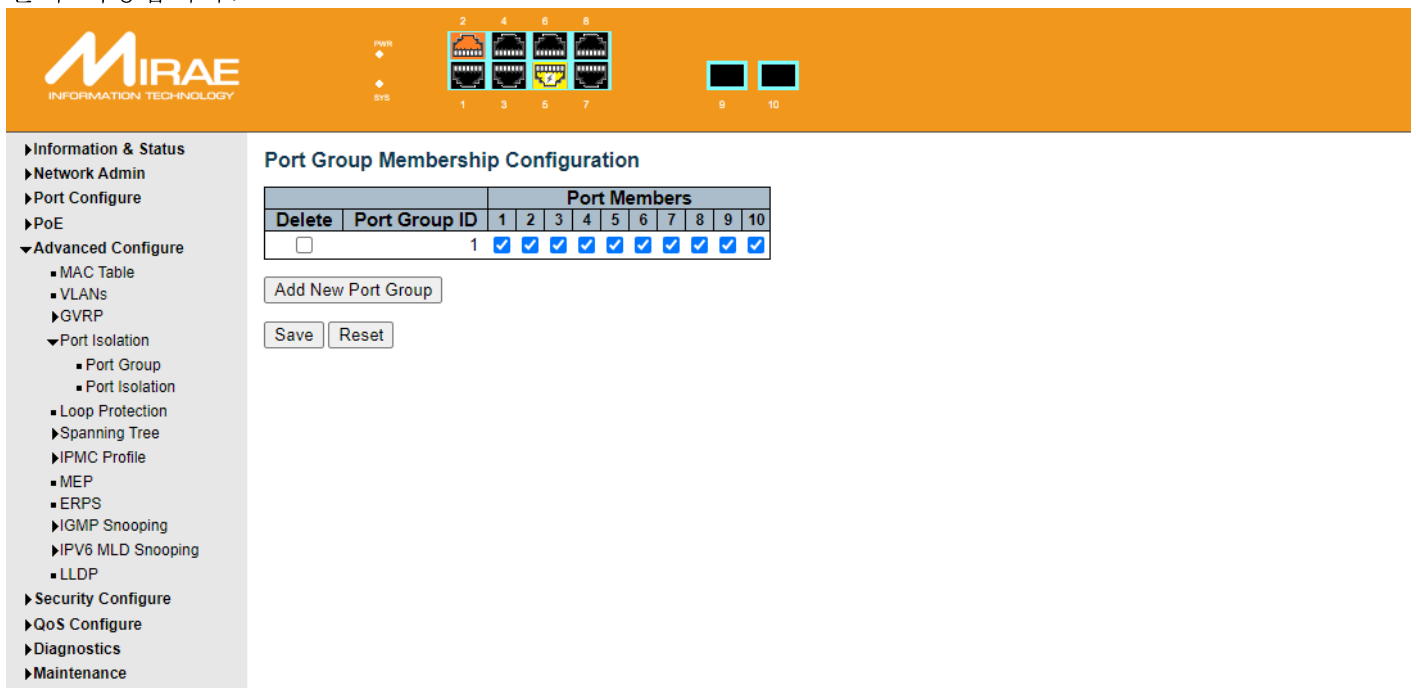
192.168.100.0/24 와 같은 동일한 세그먼트에서 사용자 1 과 2 를 구성합니다. 192.168.200.0/24 와 같은 동일한 세그먼트에서 사용자 3 과 4 를 구성합니다. 사용자 1 과 2 는 서로 ping 할 수 있지만 사용자 3 또는 4 는 ping 할 수 없으며 그 반대의 경우도 마찬가지입니다.

## 6.3 Port Isolation

### Port Group

하나의 포트가 동시에 여러 포트 그룹에 종속될 수 있습니다. 두 포트는 동일한 그룹에 있는 경우 데이터 흐름을 전달할 수 있습니다.

1. “Advanced Configure - Port Isolation” 를 클릭하고 격리 그룹을 구성할 포트를 확인하고 다음과 같이 저장합니다.



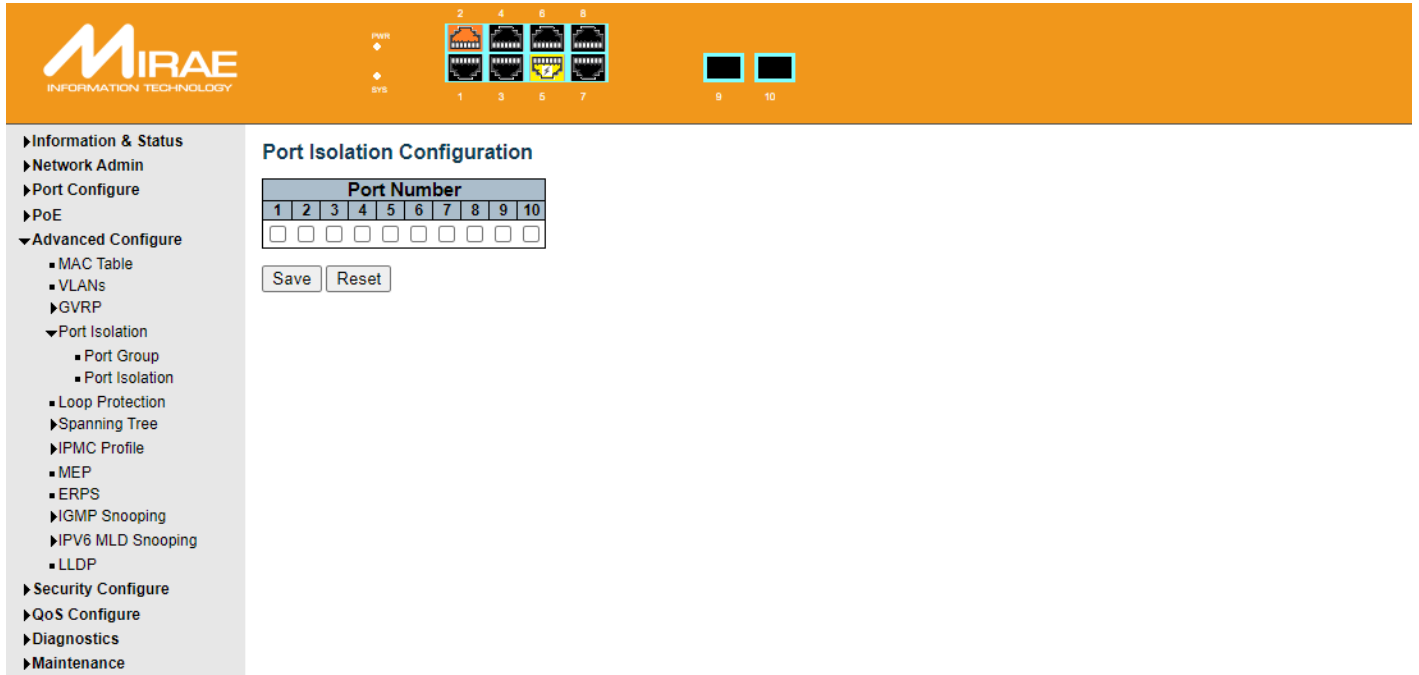
**Port Group Membership Configuration**

| Delete                   | Port Group ID | Port Members                        |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |
|--------------------------|---------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
|                          |               | 1                                   | 2                                   | 3                                   | 4                                   | 5                                   | 6                                   | 7                                   | 8                                   | 9                                   | 10                                  |
| <input type="checkbox"/> | 1             | <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"/> |

## 포트 격리

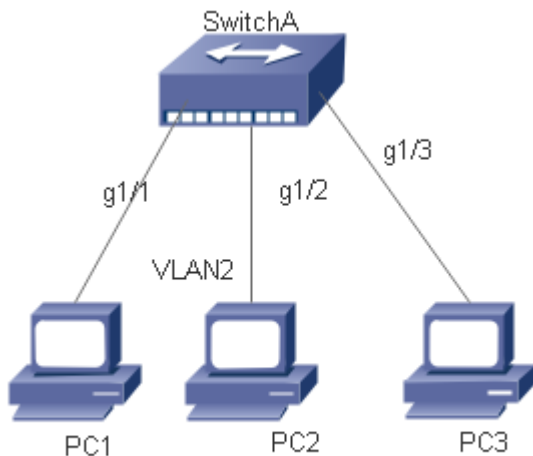
동일한 그룹의 인터페이스는 서로 격리되며 다른 그룹의 인터페이스에는 발생하지 않습니다.

1. “Advanced Configure - Port Isolation” 를 클릭하고 격리 그룹을 구성할 포트를 확인한 후 다음과 같이 저장합니다.

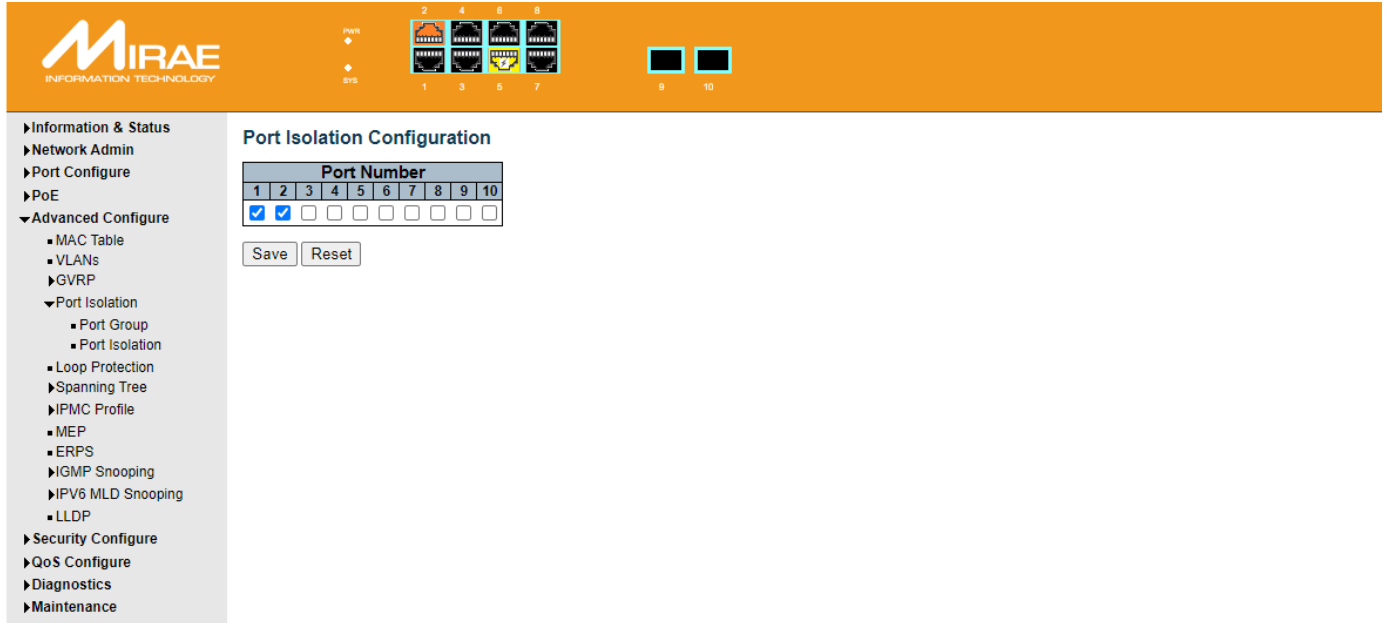


다음 예는 PC1, 2 및 3 이 VLAN 1 에 종속되어 있음을 보여줍니다. 사용자는 VLAN 1 에서 PC1 과 2 사이의 액세스를 차단하지만 PC2 와 3 은 물론 PC1 과 3 사이의 액세스를 허용합니다.

## 포트 격리 구성 예제의 네트워킹 다이어그램



1. GE1-1 및 GE1-2 포트 격리 구성의 경우 “Port Configure - Port Isolation - Port Isolation” 을 클릭하고 포트 GE1-1 및 GE1-2 를 확인하여 격리 그룹을 만들고 다음과 같이 저장합니다.



2. 구성 결과 확인

- # PC1 과 PC2 는 서로 Ping 할 수 없습니다.
- # PC1 과 PC3 는 서로 Ping 할 수 있습니다.
- # PC2 와 PC3 는 서로 Ping 할 수 있습니다.

## 6.4 Loop Protection

루프 보호는 다음과 같이 구성됩니다. 사용자가 검사 간격 및 포트 종료 시간을 수정할 수 있도록 글로벌 링 네트워크를 활성화하고 스위치 포트 구성을 비활성화합니다.

하나 이상의 포트의 루프를 구성하고 글로벌 링 네트워크를 활성화하는 상황에서 자동 검사 모드를 채택할지 여부를 결정합니다.

링 네트워크가 포트에 의해 감지될 때 처리하는 방법에는 세 가지가 있습니다. 포트 비활성화, 로그를 유지하면서 포트 비활성화, 로그만 유지;

다음과 같이 “Advanced Configure - Loop Protection” 를 클릭합니다.

구성 항목은 다음과 같습니다.

| 구성 항목              | 설 명                                |
|--------------------|------------------------------------|
| General Settings   | 루프 보호 활성화, 전송 시간 및 종료 시간 중에서 선택합니다 |
| Port Configuration | 활성화, 작업 및 Tx 모드에서 선택               |

## 6.5 Spanning Tree

링크를 백업하고 네트워크 안정성을 향상시키기 위해 이더넷 스위칭은 일반적으로 중복 링크를 사용합니다. 그러나 이러한 링크는 스위칭 네트워크에 루프를 생성하여 브로드캐스트 스톰, 불안정한 MAC 주소 목록 및 기타 오류를 유발하여 사용자의 통신 품질을 저하시키거나 통신을 방해할 수도 있습니다. 이에 대한 해결책으로 STP(Spanning Tree Protocol)가 사용됩니다. 본 제품은 IEEE 802.1D에 정의된 STP부터 IEEE 802.1W에 정의된 RSTP(Rapid Spanning Tree Protocol), 최근 IEEE 802.1S에 정의된 MSTP(Multiple Spanning Tree Protocol)에 이르기까지 다양한 프로토콜을 지원합니다. MSTP는 RSTP 및 STP와 호환되며, RSTP는 STP와 호환됩니다.

3 가지 프로토콜의 차이점은 다음과 같습니다.

### 3 가지 프로토콜의 차이점:

| 구분   | 특징   | 적용  |
|------|--|---|
| STP  | 루프없는 트리가 형성됩니다.<br>수렴 시간이 깁니다.   | 모든 VLAN 은 사용자 또는 비즈니스 흐름에 대한 차별없이 동일한 스페닝 트리를 공유합니다.                        |
| RSTP | 루프없는 트리가 형성됩니다.<br>수렴 시간이 짧습니다.  |   |
| MSTP | 루프없는 트리가 형성됩니다.<br>수렴 시간이 짧습니다.<br>스페닝 트리는 VLAN 간의 로드 균형을 조정합니다. 다른 VLAN 의 흐름은 경로에 따라 전달됩니다. | 부하 공유를 위해 사용자 흐름과 비즈니스 흐름을 구분해야 합니다. 서로 다른 VLAN 은 별도의 스페닝 트리를 통해 흐름을 전달합니다. |

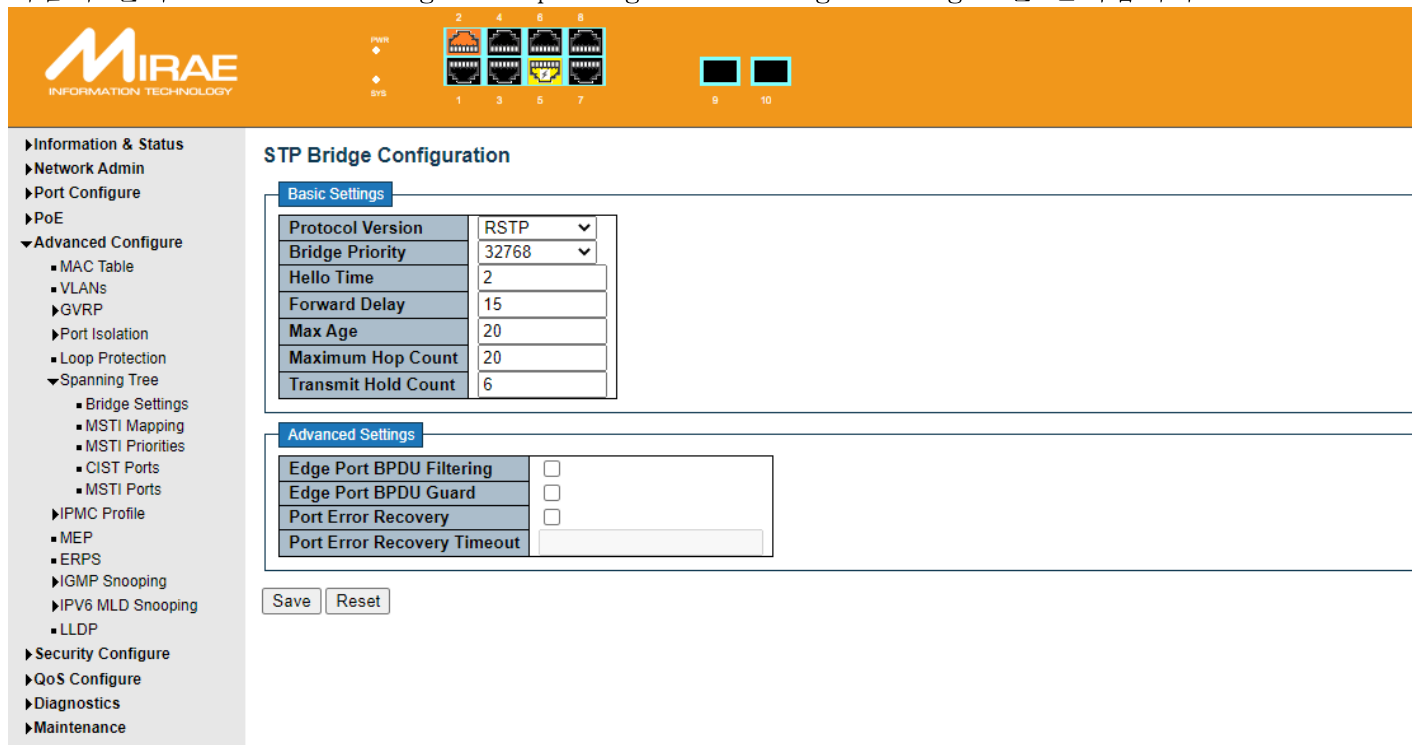
STP 가 배포된 후 토폴로지를 사용하여 네트워크 루프를 계산하여 다음을 달성합니다:

- Loop elimination: 중복 링크를 차단하여 네트워크에서 가능한 통신 루프를 제거합니다.
- Link backups: 활성 경로가 실패할 경우 네트워크 연결을 복원하기 위해 중복 링크를 활성화합니다.

## 6.5.1 Bridge Configuration

사용자는 이 페이지에서 STP Bridge 의 전역 항목을 구성할 수 있습니다.

다음과 같이 “Advanced Configure - Spanning Tree - Bridge Settings” 을 클릭합니다:



**STP Bridge Configuration**

**Basic Settings**

|                     |       |
|---------------------|-------|
| Protocol Version    | RSTP  |
| 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    | <input type="checkbox"/> |
| Edge Port BPDU Guard        | <input type="checkbox"/> |
| Port Error Recovery         | <input type="checkbox"/> |
| Port Error Recovery Timeout |                          |

Save Reset

구성 항목은 다음과 같습니다.

| 구성 항목                      | 설 명  |
|----------------------------|--|
| Protocol Ver.              | STP 버전을 선택합니다. 다음에서 목록을 드롭 다운하여 스위치에서 실행할 수 있습니다:<br>STP- 스위치에 STP 를 전역적으로 설정합니다.<br>RSTP- 스위치에 RSTP 를 전역적으로 설정합니다.<br>MSTP- 스위치에 MSTP 를 전역적으로 설정합니다.            |
| Bridge Priority            | 브리지 우선 순위를 제어합니다. 숫자 값이 낮을수록 우선 순위가 높습니다. 브리지 우선 순위와 스위치의 6 바이트 MAC 주소와 연결된 MSTI 인스턴스 번호가 브리지 식별자를 형성합니다.  |
| Forward Delay (4-30s)      | 4 초에서 30 초 사이이며 기본적으로 15 초입니다.   |
| Max Age (6-40s)            | 최대 에이징 시간은 중복 경로의 무한 루프에서 오래된 정보를 멀리하고 새로운 정보의 효과적인 확산을 방지하기 위해 설정됩니다. 에이징 시간은 기본적으로 20 초입니다.  |
| Max hops (6-40)            | 스위치에서 보낸 BPDU (Bridge Protocol Data Unit) 패킷을 버리기 전에 스페닝 트리 영역에서 장치 간의 홉을 설정합니다. 홉은 패킷이 스위치를 지날 때마다 하나씩 감소합니다. 사용자는 기본적으로 20 개를 사용하여 6 에서 40 까지 홉 수를 설정할 수 있습니다. |
| Transmit Hold Count (1-10) | 각 간격에서 전송할 최대 Hello 패킷 수를 1 ~ 10 범위로 설정합니다. 기본값은 6 입니다.  |

## 6.5.2 MSTI Mapping

다음과 같이 “Advanced Configure - Spanning Tree - MSTI Mapping” 을 클릭합니다:

**MSTI Configuration**

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

**Configuration Identification**

|                        |                   |
|------------------------|-------------------|
| Configuration Name     | 82-26-03-11-01-E1 |
| Configuration Revision | 0                 |

**MSTI Mapping**

| MSTI  | VLANs Mapped |
|-------|--------------|
| MSTI1 |              |
| MSTI2 |              |
| MSTI3 |              |
| MSTI4 |              |
| MSTI5 |              |
| MSTI6 |              |
| MSTI7 |              |

Save Reset



구성 항목은 다음과 같습니다.

| 구성 항목                  | 설 명                |
|------------------------|--------------------|
| Configuration Name     | MSTP 도메인 이름 구성     |
| Configuration Revision | 개정 구성              |
| MSTI Mapping           | 매핑 할 VLAN 을 입력하십시오 |

설 명:

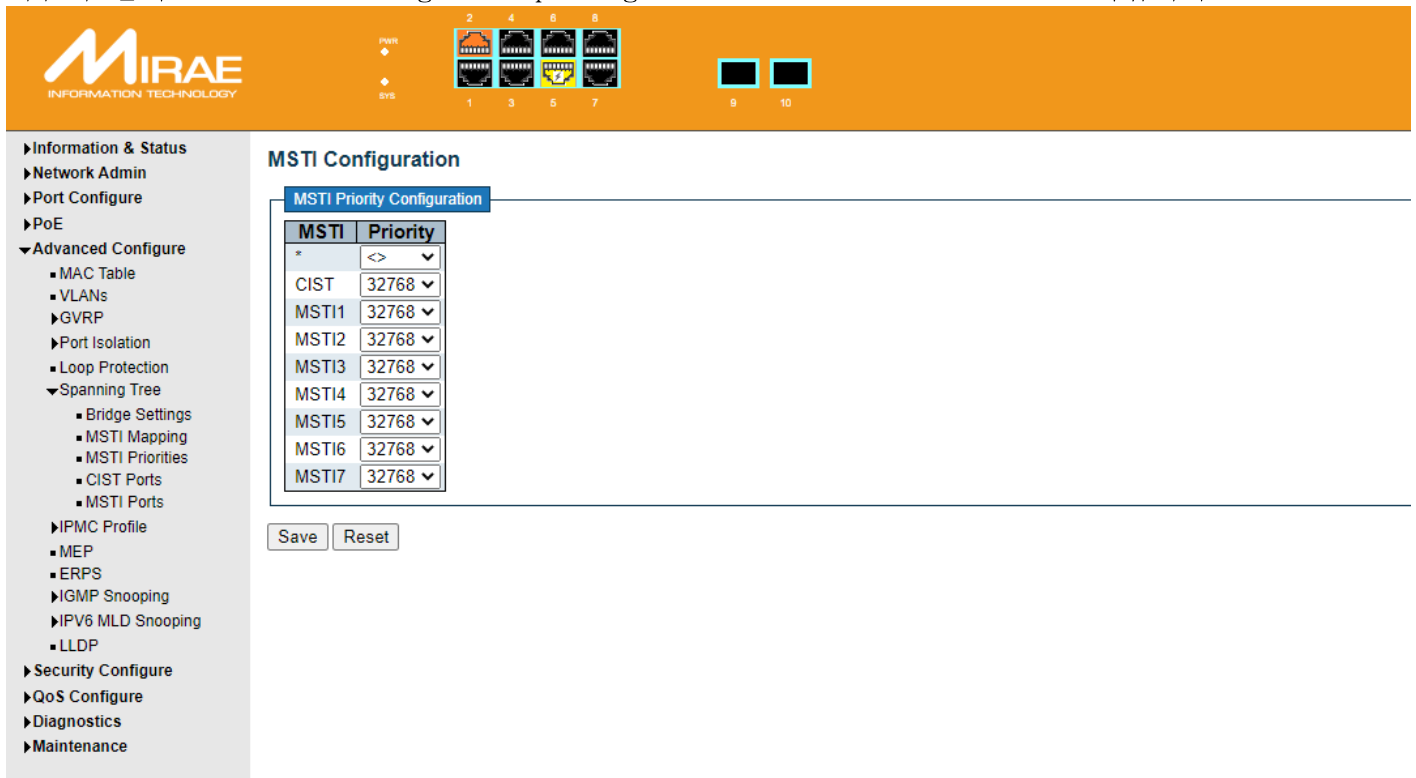
인스턴스는 통신 코스트와 리소스 사용률을 줄이는 VLAN 그룹입니다.

독립적으로 계산된 각 인스턴스는 로드 균형을 맞출 수 있습니다. 토폴로지가 동일한 VLAN 은 동일한 인스턴스에 매핑될 수 있으며 해당 MSTP 인스턴스의 포트 상태에 따라 전달됩니다.

즉, 한 번에 하나 이상의 VLAN 이 MSTP 인스턴스의 스페닝 트리에 매핑됩니다.

### 6.5.3 MSTI Priorities

다음과 같이 “Advanced Configure - Spanning Tree - MSTI Priorities” 를 클릭합니다:



구성 항목은 다음과 같습니다.

| 구성 항목           | 설 명                                |
|-----------------|------------------------------------|
| MSTI Priorities | 구성된 인스턴스 우선 순위 범위는 0 ~ 61,440 입니다. |

설 명:

구성된 인스턴스 우선 순위는 0 에서 61,440 사이의 4,094 의 배수여야 합니다.

## 6.5.4 CIST Ports

다음과 같이 “Advanced Configure - Spanning Tree - CIST Ports” 를 클릭합니다:

| Port | STP Enabled                         | Path Cost | Priority | Admin Edge | Auto Edge                           | Restricted Role          | TCN                      | BPDU Guard               | Point-to-point |
|------|-------------------------------------|-----------|----------|------------|-------------------------------------|--------------------------|--------------------------|--------------------------|----------------|
| *    | <input checked="" type="checkbox"/> | <>        | <>       | <>         | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <>             |
| 1    | <input type="checkbox"/>            | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto           |
| 2    | <input type="checkbox"/>            | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto           |
| 3    | <input type="checkbox"/>            | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto           |
| 4    | <input type="checkbox"/>            | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto           |
| 5    | <input type="checkbox"/>            | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto           |
| 6    | <input type="checkbox"/>            | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto           |
| 7    | <input type="checkbox"/>            | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto           |
| 8    | <input type="checkbox"/>            | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto           |
| 9    | <input checked="" type="checkbox"/> | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto           |
| 10   | <input checked="" type="checkbox"/> | Auto      | 128      | Non-Edge   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto           |

구성 항목은 다음과 같습니다

| 구성 항목                | 설 명   |
|----------------------|---|
| Ring Network Enabled | 포트의 STP 기능을 활성화하려면 선택하십시오.  |
| Path Cost (0=Auto)   | 기본적으로 0(자동)을 사용하여 지정된 포트 목록으로 패킷을 전달하는 것과 관련된 비용 측정을 자동으로 정의합니다. 숫자가 작을수록 패킷 전달에 이 포트를 사용할 가능성이 높습니다. 포트에서 발생하는 경로 비용을 제어합니다. 자동 설정은 802.1D 권장 값을 사용하여 물리적 링크 속도에 따라 경로 비용을 적절하게 설정합니다. 특정 설정을 사용하여 사용자 정의 값을 입력할 수 있습니다. 경로 비용은 네트워크의 활성 토폴로지를 설정할 때 사용됩니다. 더 높은 경로 비용 포트를 선호하는 전달 포트는 낮은 경로 비용 포트가 선택됩니다. 유효한 값의 범위는 1 ~ 200,000,000 입니다. |
| Priority             | 우선 순위는 경로 비용이 동일 할 때 포트의 전달 상태를 결정합니다.  |
| Auto Boundary        | True 모드를 선택하여 포트를 경계 포트 지정합니다.<br>False 모드를 선택하여 경계 상태를 벗어납니다.<br>Auto 모드를 선택하면 포트에서 수신한 BPDU 메시지로 경계 상태를 판단합니다.  |

|                 |  |
|-----------------|--|
| Restricted Role | 목록을 드롭 다운하여 True 및 False 모드 (기본적으로 "False" 모드 사용)에 따라 제한된 역할을 전환합니다. "True" 모드에서는 루트 포트가 아닙니다. |
| Restricted TCN  | TCN 은 브리지가 루트 포트로 전송하는 간단한 BPDU 로 True 모드와 False 모드 사이에서 전환되며 기본적으로 "False" 모드가 있습니다.          |
| BPDU Protection | 이 기능이 활성화되면 BPDU 메시지 수신시 포트가 비활성화 (종료)됩니다.   |
| P2P             | 링크는 True 모드에서 피어 투 피어로 공유됩니다. P2P 포트는 에지 포트와 유사하며 기본적으로 "Auto" 모드가 있습니다.                       |

## 6.5.5 MSTI Ports

사용자는 인스턴스 포트의 우선 순위 및 경로 코스트를 설정할 수 있습니다.

다음과 같이 “Advanced Configure - Spanning Tree - MSTI Ports” 를 클릭합니다:

구성 항목은 다음과 같습니다.

| 구성 항목     | 설 명   |
|-----------|---|
| Path Cost | 기본적으로 0 (자동)을 사용하여 지정된 포트 목록으로 패킷을 전달하는 것과 관련된 비용 측정을 자동으로 정의합니다. 숫자가 작을수록 패킷 전달에 이 포트를 사용할 가능성이 높아집니다. 포트에서 발생하는 경로 비용을 제어합니다. 자동 설정은 802.1D 권장 값을 사용하여 물리적 링크 속도에 따라 경로 비용을 적절하게 설정합니다. 특정 설정을 사용하여 사용자 정의 값을 입력 할 수 있습니다. 경로 비용은 네트워크의 활성 토폴로지를 설정할 때 사용됩니다. 더 높은 경로 비용 포트를 선호하는 전달 포트는 낮은 경로 비용 포트가 선택됩니다. 유효한 값은 1 에서 200,000,000 사이입니다. |

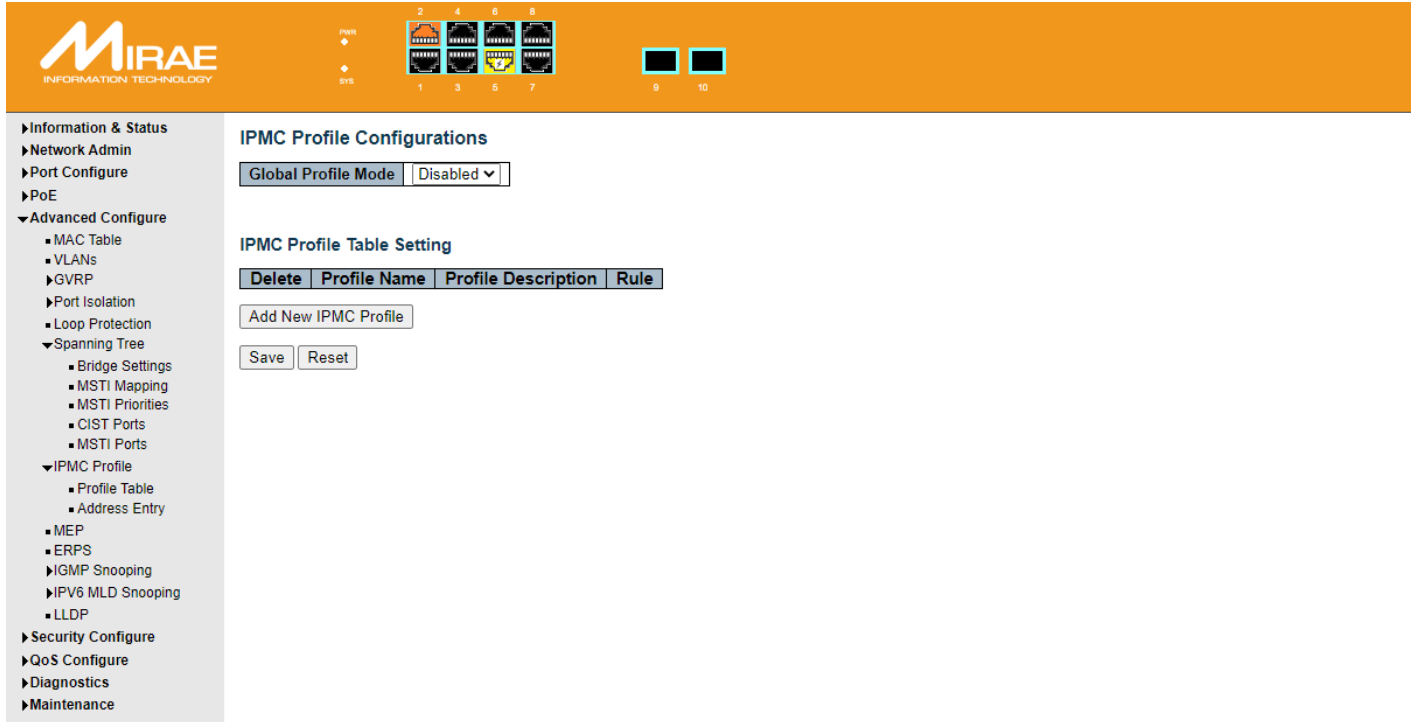
Priority

우선 순위는 경로 비용이 동일 할 때 포트의 전달 상태를 결정합니다.

## 6.6 IPMC Profile

사용자는 필터 멀티 캐스트 목록을 구성할 수 있습니다.

다음과 같이 “Advanced Configure - IPMC Profile - Address Entry” 을 클릭합니다:



구성 항목은 다음과 같습니다.

| 구성 항목         | 설 명                     |
|---------------|-------------------------|
| Entry Name    | 필터링 할 멀티 캐스트 이름을 입력하십시오 |
| Start Address | 시작 멀티 캐스트 주소를 입력하십시오    |
| End Address   | 끝 멀티 캐스트 주소 입력          |


## 6.7 IGMP Snooping

IGMP 스누핑 (인터넷 그룹 관리 프로토콜 스누핑)은 레이어 2 이더넷 스위치에서 작동하는 멀티캐스트 관리 및 제어 메커니즘입니다.

스위치는 인터페이스를 멀티캐스트 그룹 주소로 매핑하고 IGMP 스누핑이 활성화된 경우 각 인터페이스에서 수신한 IGMP 메시지를 스누핑하여 그에 따라 멀티캐스트 데이터 스트림을 전달합니다.

### 6.7.1 Basic Configuration

“Advanced Configure - IGMP Snooping - Basic Configuration” 을 클릭하여 다음과 같이 IGMP Snooping의 구성 정보를 확인합니다:



↑

↓

↑

↓

↑

↓

↑

↓

↑

↓

↑

↓

Information & Status

▶ Network Admin

▶ Port Configure

▶ PoE

▼ Advanced Configure

■ MAC Table

■ VLANs

▶ GVRP

▶ Port Isolation

■ Loop Protection

▶ Spanning Tree

▶ IPMC Profile

■ MEP

■ ERPS

▼ IGMP Snooping

■ Basic Configuration

■ VLAN Configuration

■ Port Filtering Profile

▶ IPv6 MLD Snooping

■ LLDP

▶ Security Configure

▶ QoS Configure

▶ Diagnostics

▶ Maintenance

IGMP Snooping Configuration

Global Configuration

Snooping Enabled

☐

Unregistered IPMCv4 Flooding Enabled

☒

IGMP SSM Range

232.0.0.0 / 8

Leave Proxy Enabled

☐

Proxy Enabled

☐

Port Related Configuration

| Port | Router Port              | Fast Leave               | Throttling |
|------|--------------------------|--------------------------|------------|
| *    | <input type="checkbox"/> | <input type="checkbox"/> | <>         |
| 1    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 2    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 3    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 4    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 5    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 6    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 7    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 8    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 9    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 10   | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |

Save

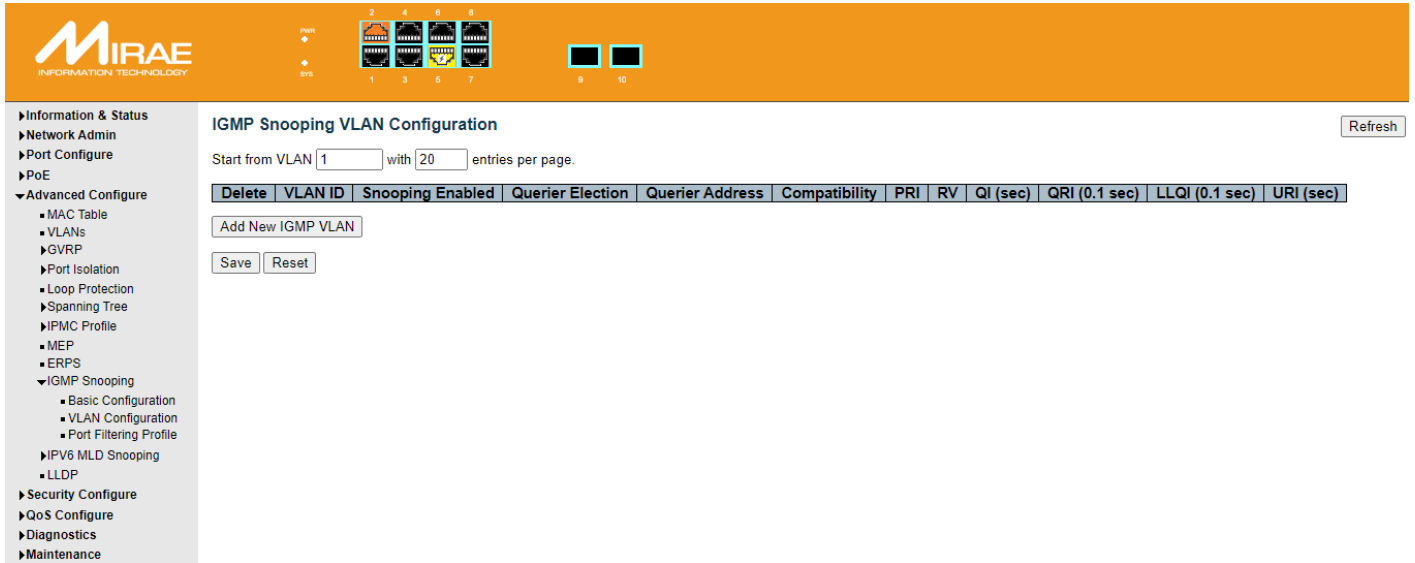
Reset

구성 항목은 다음과 같습니다.

| 구성 항목                                | 설 명  |
|--------------------------------------|--|
| Snooping Enabled                     | IGMP 스누핑을 활성화 또는 비활성화합니다.  |
| Unregistered IPMCv4 Flooding Enabled |  |
| Routing Port                         | Layer3 멀티캐스트 라우터 또는 IGMP 쿼리어에 연결된 포트를 나타냅니다.<br>라우터 포트로 작동하는 포트를 지정합니다. 라우터 포트는 레이어3 멀티캐스트 장치 또는 IGMP 쿼리어로 연결되는 이더넷 스위치의 포트입니다. 통합 멤버 포트가 라우터 포트로 선택되면 전체 통합이 라우터 포트로 작동합니다. |
| Fast Leave                           | 그룹 등록 취소를 위한 메시지 수신 즉시 MAC 전달 항목 삭제를 수행합니다   |

## 6.7.2 VLAN Configuration

“Advanced Configure - IGMP Snooping - VLAN Configuration” 을 클릭하여 다음과 같이 IGMP Snooping 의 구성 정보를 확인합니다:

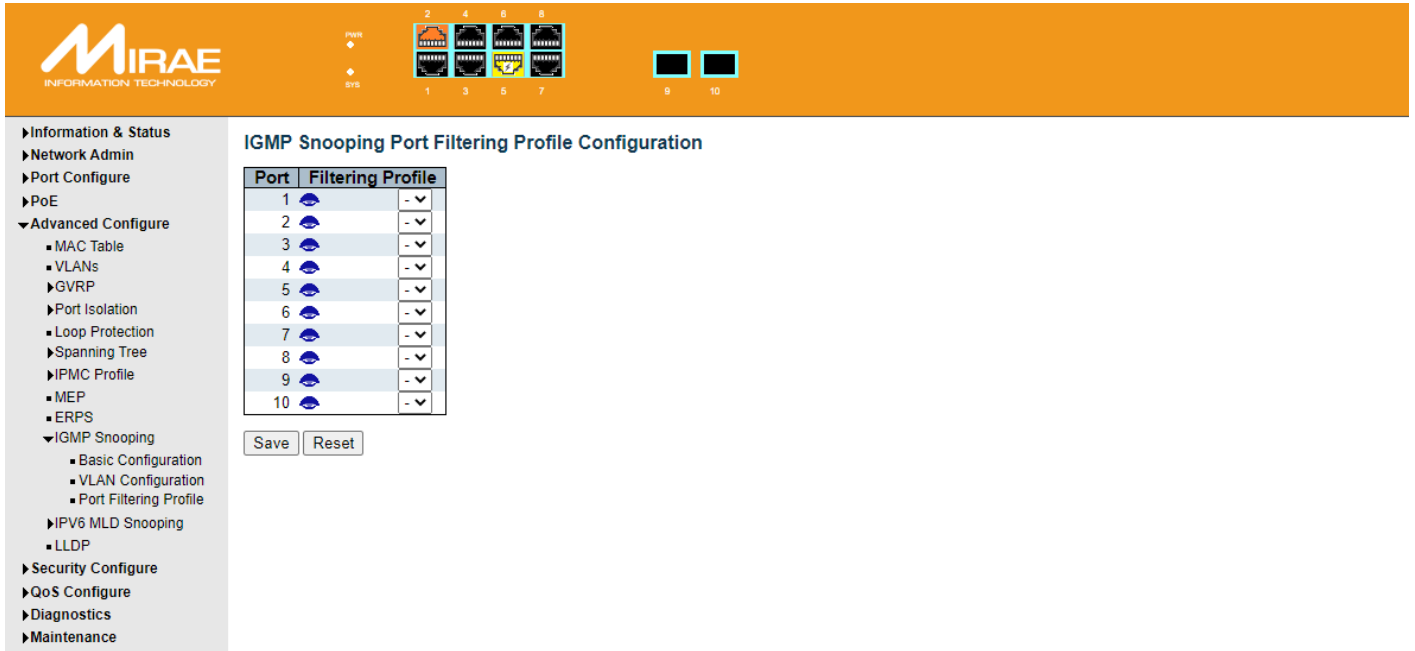


구성 항목은 다음과 같습니다.

| 구성 항목            | 설 명  |
|------------------|--|
| VLAN ID          |  |
| Snooping Enabled | VLAN 별 IGMP 스누핑을 활성화 또는 비활성화합니다. IGMP 스누핑을 위해 최대 32 개의 VLAN 을 선택할 수 있습니다.  |
| Querier Election | IGMP 쿼리어 선택을 활성화하거나 비활성화합니다.<br>VLAN 에서 IGMP 쿼리어 선택에 참여할 수 있습니다. IGMP Non-Querier 로 작동하려면 비활성화합니다.   |
| Querier Address  | IGMP 쿼리어 선택을 위해 IP 헤더에 사용되는 소스 주소로 IPv4 주소를 정의합니다.<br>쿼리어 주소가 설정되지 않은 경우 시스템은 이 VLAN 과 연결된 IP 인터페이스의 IPv4 관리 주소를 사용합니다.<br>IPv4 관리 주소가 설정되지 않은 경우 시스템은 사용 가능한 첫 번째 IPv4 관리 주소를 사용합니다.<br>그렇지 않으면 시스템은 미리 정의된 값을 사용합니다. 기본적으로 이 값은 192.0.2.1 입니다. |

### 6.7.3 Port Filtering Profile

“Advanced Configure - IGMP Snooping - Port Filtering Profile” 을 클릭하여 프로필에 의해 구성된 멀티캐스트 목록을 호출합니다.



구성 항목은 다음과 같습니다.

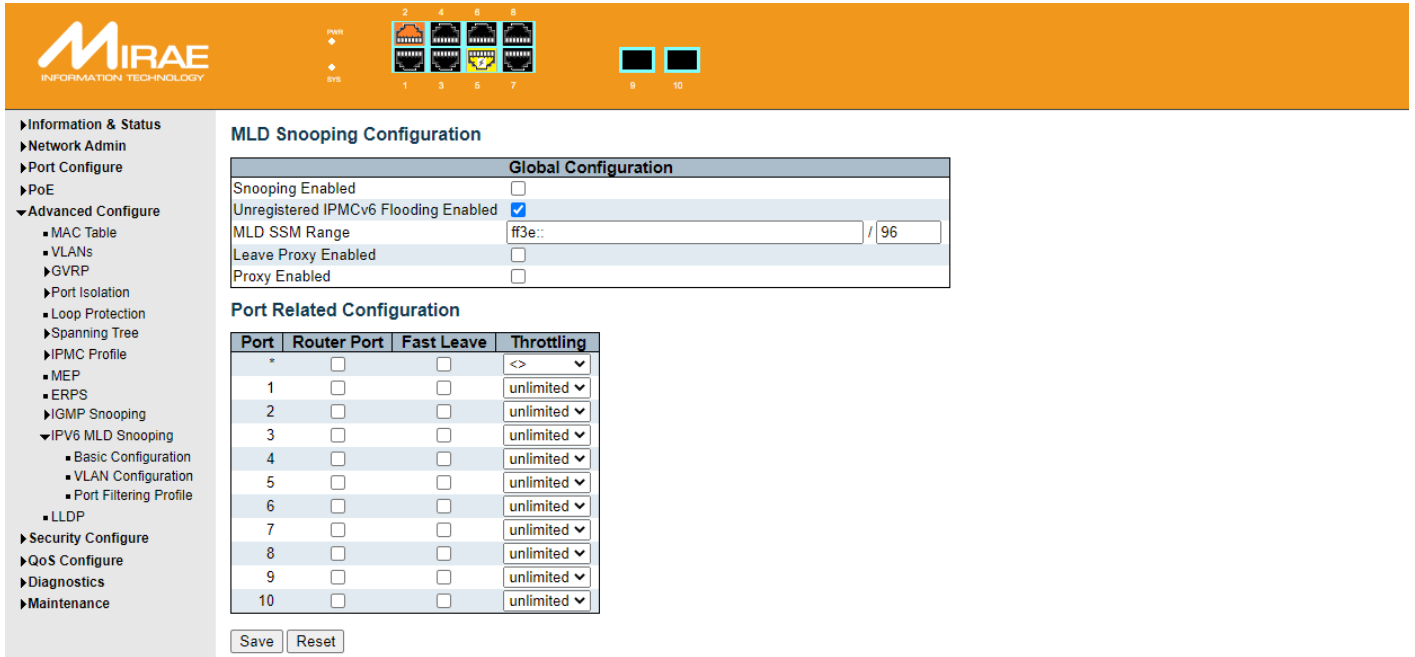
| 구성 항목            | 설 명  |
|------------------|--|
| VLAN ID          |  |
| Snooping Enabled | VLAN 별 IGMP 스누핑을 활성화 또는 비활성화합니다. IGMP 스누핑을 위해 최대 32 개의 VLAN 을 선택할 수 있습니다.  |
| Querier Election | IGMP 쿼리어 선택을 활성화하거나 비활성화합니다.<br>VLAN 에서 IGMP 쿼리어 선택에 참여할 수 있습니다. IGMP Non-Querier 로 작동하려면 비활성화합니다.   |
| Querier Address  | IGMP 쿼리어 선택을 위해 IP 헤더에 사용되는 소스 주소로 IPv4 주소를 정의합니다.<br>쿼리어 주소가 설정되지 않은 경우 시스템은 이 VLAN 과 연결된 IP 인터페이스의 IPv4 관리 주소를 사용합니다.<br>IPv4 관리 주소가 설정되지 않은 경우 시스템은 사용 가능한 첫 번째 IPv4 관리 주소를 사용합니다.<br>그렇지 않으면 시스템은 미리 정의된 값을 사용합니다. 기본적으로 이 값은 192.0.2.1 입니다. |

## 6.8 IPv6 MLD Snooping

IPv6 MLD 스누핑은 레이어 2 이더넷 스위치에서 작동하는 멀티캐스트 관리 및 제어 메커니즘입니다. 스위치는 인터페이스를 멀티캐스트 그룹 주소로 매핑하고 IPv6 MLD 스누핑이 활성화된 경우 각 인터페이스에서 수신한 IPv6 MLD 메시지를 스누핑하여 그에 따라 멀티캐스트 데이터 스트림을 전달합니다.

## 6.8.1 Basic Configuration

“Advanced Configure - IPv6 MLD Snooping - Basic Configuration” 을 클릭하여 다음과 같이 구성 정보를 확인하십시오:



**MLD Snooping Configuration**

**Global Configuration**

Snooping Enabled ☐

Unregistered IPMCv6 Flooding Enabled ☒

MLD SSM Range ff3e:: / 96

Leave Proxy Enabled ☐

Proxy Enabled ☐

**Port Related Configuration**

| Port | Router Port              | Fast Leave               | Throttling |
|------|--------------------------|--------------------------|------------|
| *    | <input type="checkbox"/> | <input type="checkbox"/> | <>         |
| 1    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 2    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 3    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 4    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 5    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 6    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 7    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 8    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 9    | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |
| 10   | <input type="checkbox"/> | <input type="checkbox"/> | unlimited  |

Save Reset

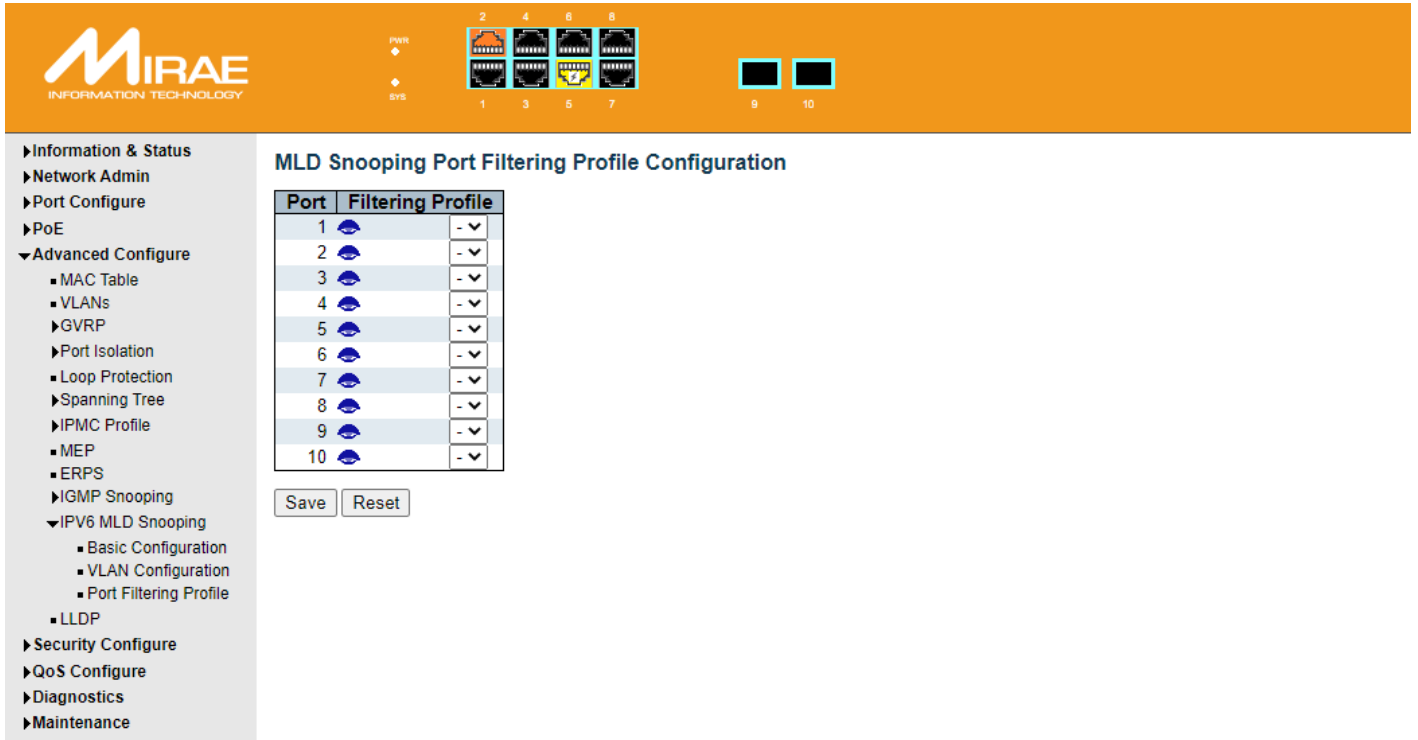
구성 항목은 다음과 같습니다.

| 구성 항목                                | 설 명   |
|--------------------------------------|---|
| Enable Snooping                      | IPv6 MLD 스누핑 활성화 또는 비활성화  |
| Unregistered IPMCv6 Flooding Enabled |   |
| Routing port                         | 레이어 3 멀티캐스트 라우터 또는 IGMP 쿼리어에 연결된 포트를 나타냅니다.<br>라우터 포트 역할을 하는 포트를 지정합니다. 라우터 포트는 레이어 3 멀티캐스트 장치 또는 MLD 쿼리어로 연결되는 이더넷 스위치의 포트입니다.<br>통합 멤버 포트가 라우터 포트로 선택되면 전체 통합이 라우터 포트로 작동합니다. |
| Fast leave                           | 그룹 등록 취소를 위한 메시지 수신 즉시 MAC 전달 항목 삭제를 수행합니다  |



### 6.8.3 Port Filtering Profile

“Advanced Configure - IPv6 MLD Snooping - VLAN Configuration” 을 클릭하여 다음과 같이 구성 정보를 확인합니다:



구성 항목은 다음과 같습니다.

| 구성 항목            | 설 명   |
|------------------|---|
| VLAN ID          |   |
| Snooping Enabled | VLAN 별 MLD 스누핑을 활성화 또는 비활성화합니다. IGMP 스누핑을 위해 최대 32 개의 VLAN 을 선택할 수 있습니다.<br>VLAN 별 IGMP 스누핑을 활성화합니다. IGMP 스누핑을 위해 최대 32 개의 VLAN 을 선택할 수 있습니다. |
| Querier Election | MLD 쿼리어 선택을 활성화 또는 비활성화합니다.<br>VLAN 에서 MLD 쿼리 선택에 참여할 수 있습니다. MLD Non-Querier 로 작동하려면 비활성화하십시오.   |

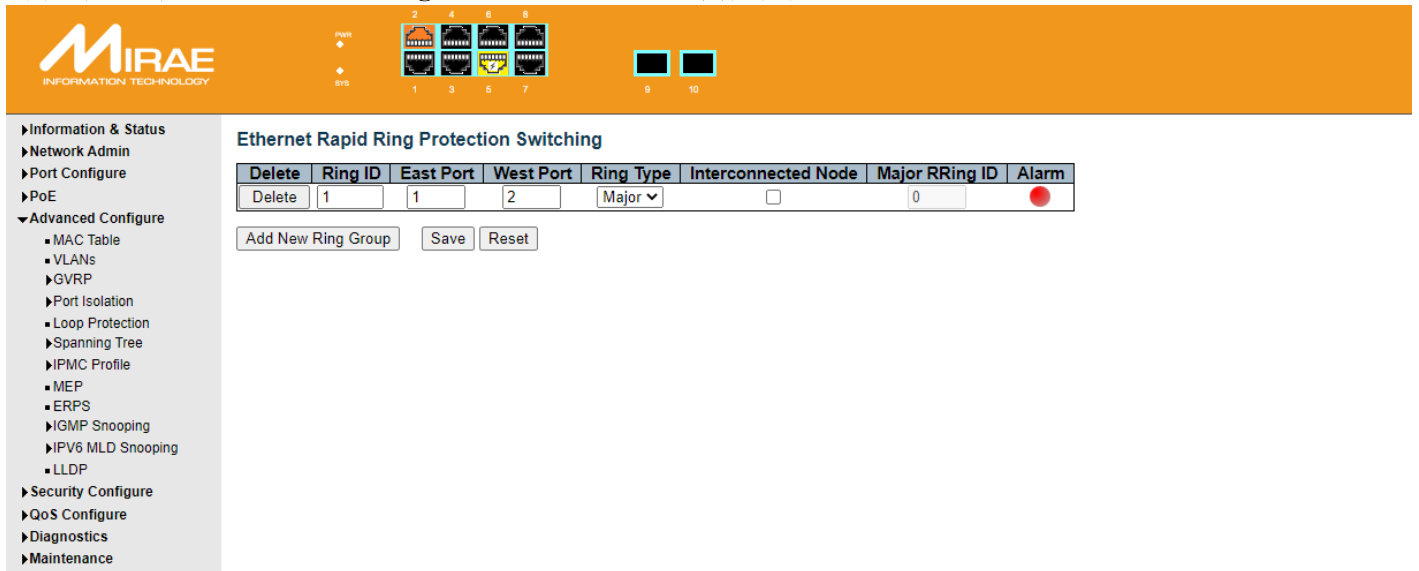
## 6.9 ERPS

ERPS (이더넷 링 보호 스위칭):

ERPS 의 최신 표준인 ITU-TG.8032 ERPS 는 다중 링 및 다중 도메인 구조를 지원하고 EAPS, RPR, SDH, STP 등의 장점을 흡수합니다. 양방향 오류 측면에서 검사 메커니즘을 최적화합니다. 또한 50ms 스위칭으로 주요 장치 백업, 부하 공유 및 기타 작업 방법을 지원합니다.

참고 : ERPS 를 활성화하기 전에 STP 를 비활성화하십시오.

다음과 같이 “Advanced Configure - ERPS” 를 클릭합니다:




구성 항목은 다음과 같습니다

| 구성 항목                | 설 명  |
|----------------------|--|
| Ring ID              | ERPS 링 인스턴스의 ID  |
| East Port            | 링 보호와 관련된 포트 번호를 선택하십시오  |
| West Port            | 링 보호와 관련된 다른 포트 번호를 선택하십시오   |
| Ring Type            | “Main Ring” 또는 “Sub-Ring” (다중 링 응용 프로그램에만 배포됨) 중에서 선택하며 기본적으로 "메인 링"을 사용합니다.   |
| Interconnection Node | 멀티 링 어플리케이션에서 2 개 이상의 링을 동시에 연결하는 노드를 의미합니다                                    |
| Main Ring ID         | 메인 링은 단일 링 애플리케이션에서 링과 동일한 ID 를 공유합니다. 서브 링은 멀티 링 애플리케이션에서 메인 링 ID 를 입력해야 합니다. |
| R-APS VLAN(1-4,094)  | R-APS VLAN 으로 사용되는 VLAN 입니다.   |

“Add New Ring Group”를 클릭하십시오 ;

“Ring ID” 목록에서 링크를 클릭하여 다음과 같이 ERPS Ring 을 구성합니다:



Port

1

2

3

4

5

6

7

8

9

Information & Status

Network Admin

Port Configure

PoE

Advanced Configure

MAC Table

VLANs

GVRP

Port Isolation

Loop Protection

Spanning Tree

IPMC Profile

MEP

ERPS

GMP Snooping

IPv6 MLD Snooping

LLDP

Security Configure

QoS Configure

Diagnostics

Maintenance

Rapid Ring Configuration 1

Auto-refresh ☐ Refresh

Instance Data

| Ring ID | East Port | West Port | East Port SF MEP | West Port SF MEP | East Port APS MEP | West Port APS MEP | Ring Type  |
|---------|-----------|-----------|------------------|------------------|-------------------|-------------------|------------|
| 1       | 1         | 2         | 1                | 2                | 1                 | 2                 | Major Ring |

Instance Configuration

| Configured                          | WTR(Wait to Restore) Time | Revertive                           | VLAN config                 |
|-------------------------------------|---------------------------|-------------------------------------|-----------------------------|
| <input checked="" type="checkbox"/> | 1min                      | <input checked="" type="checkbox"/> | <a href="#">VLAN Config</a> |

RPL Configuration

| RPL Role | RPL Port | Clear                    |
|----------|----------|--------------------------|
| None     | None     | <input type="checkbox"/> |

Instance State

| Protection State | East Port | West Port | Transmit APS | East Port Receive APS | West Port Receive APS | WTR Remaining | RPL Un-blocked                      | No APS Received                     | East Port Block Status | West Port Block Status | FOP Alarm                           |
|------------------|-----------|-----------|--------------|-----------------------|-----------------------|---------------|-------------------------------------|-------------------------------------|------------------------|------------------------|-------------------------------------|
| Pending          | OK        | OK        | NR BPR0      |                       |                       | 0             | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Blocked                | Unblocked              | <input checked="" type="checkbox"/> |

Save

Reset

| 구 성 항 목                    | 설 명  |
|----------------------------|--|
| WTR Time (5-12s)           | 체크 박스를 선택하고 R-APS 기능의 WTR 시간 (기본값은 1 분)을 입력합니다.                |
| Restore the Revertive Mode | 목록을 드롭 다운하여 R-APS 복원 옵션을 활성화 또는 비활성화하려면 확인란을 선택합니다.            |
| VLAN Protection            | 보호 된 VLAN 그룹을 편집하려면 “VLAN Protection” 를 클릭합니다.                 |
| RPL Role                   | 목록을 드롭 다운하여 “None” , “RPL Owner” and “RPL Neighbor” 중에서 선택합니다. |
| RPL Port                   | 목록을 드롭 다운하여 “None” , “East Port” and “West Port” 중에서 선택합니다.    |

“Save” 하고 완료합니다.

보호된 VLAN 구성을 편집하려면 “VLAN Configuration” 을 클릭하십시오.

## Rapid Ring VLAN Configuration 1

| Delete                   | VLAN ID |
|--------------------------|---------|
| <input type="checkbox"/> | 1       |

Add New Entry

Back

Save

Reset

참고 : 사용자는 이 페이지에서 보호를 위해 다른 VLAN (기본적으로 ID 1)을 수정하거나 추가할 수 있습니다.

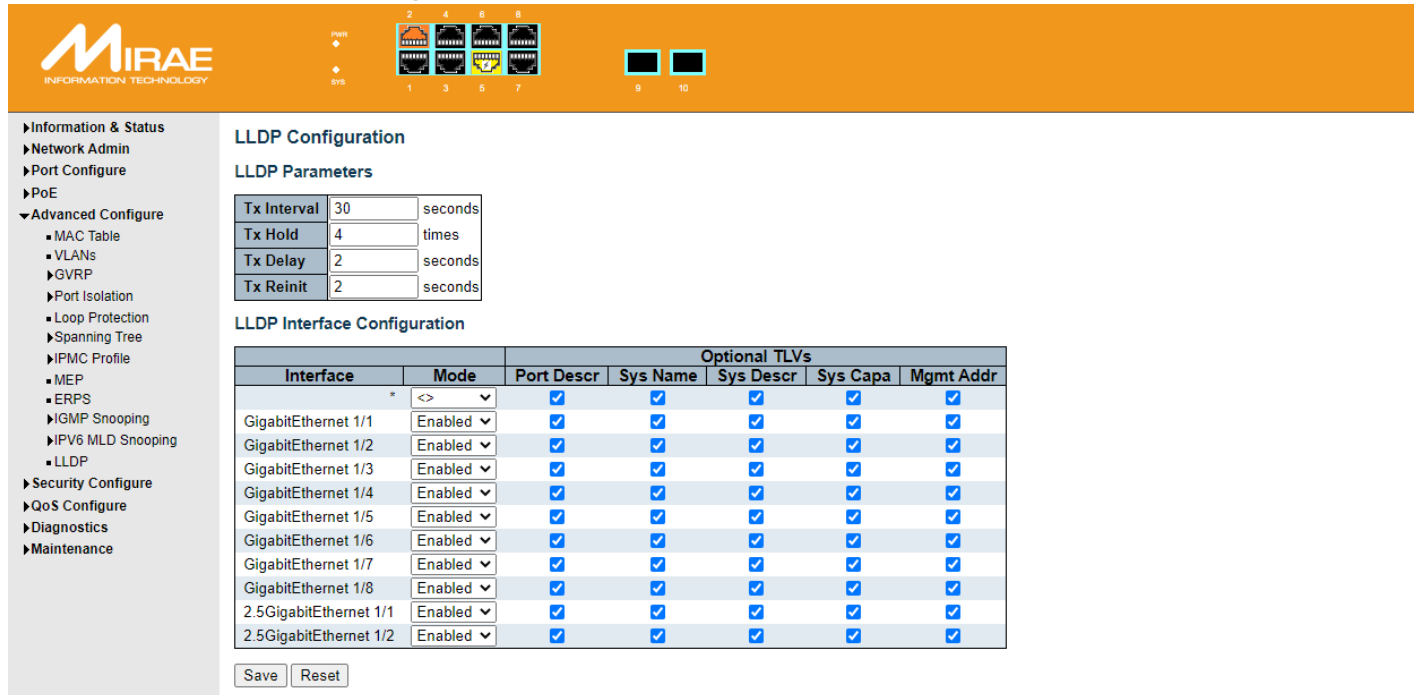
## 6.10 LLDP

LLDP (Link Layer Discovery Protocol)는 네트워크 장치가 식별 및 성능을 로컬 서브넷에 알릴 수 있도록하는 공급 업체 독립적인 Layer2 프로토콜입니다.

현재 복잡한 구성을 가진 다양한 네트워크 장치에는 제조업체가 다른 것들을 발견하고 고유한 시스템 및 구성 정보를 교환 할 수 있는 표준 정보 교환 플랫폼이 필요합니다.

LLDP 는 단말 장치의 주요 기능, 관리 주소, 장치 및 인터페이스 식별과 같은 정보를 TLV (Type / Length / Value)에 통합하여 LLDPDU (Link Layer Discovery Protocol Data Unit)에 캡슐화하는 표준 링크 계층 검색 방법입니다. 직접 연결된 이웃에게 보내고, 정보를 받은 후 NMS 조회 및 링크 통신 판단을 위해 표준 MIB(Management Information Base) 형태로 저장합니다.

다음과 같이 “Advanced Configure - LLDP” 를 클릭합니다:



**LLDP Configuration**

**LLDP Parameters**

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

**LLDP Interface Configuration**

| Interface              | Mode    | Optional TLVs                       |                                     |                                     |                                     |                                     |
|------------------------|---------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
|                        |         | Port Descr                          | Sys Name                            | Sys Descr                           | Sys Capa                            | Mgmt Addr                           |
| *                      | <>      | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/1    | Enabled | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/2    | Enabled | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/3    | Enabled | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/4    | Enabled | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/5    | Enabled | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/6    | Enabled | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/7    | Enabled | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/8    | Enabled | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.5GigabitEthernet 1/1 | Enabled | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.5GigabitEthernet 1/2 | Enabled | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Save Reset

# 7 Security Configure

## 7.1 Users

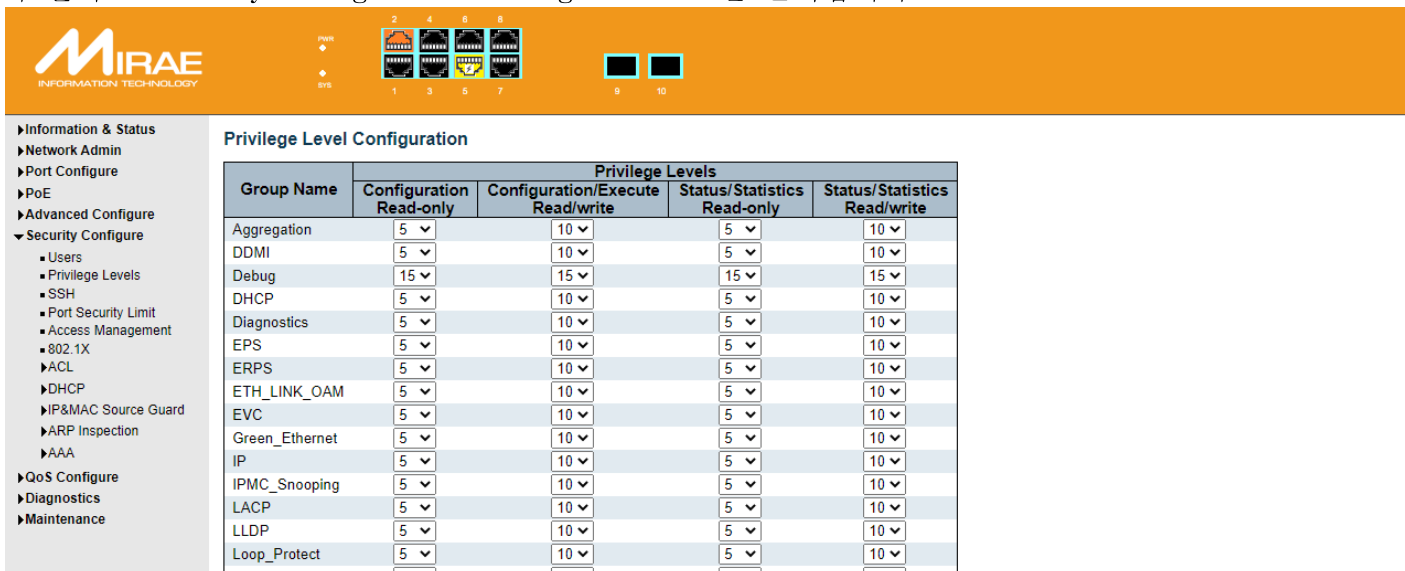
사용자는 스위치에서 비밀번호를 재설정 할 수 있습니다.  
다음과 같이 “Security Configure - Users” 를 클릭합니다:



“Save” 하고 완료합니다.

## 7.2 Privilege Levels

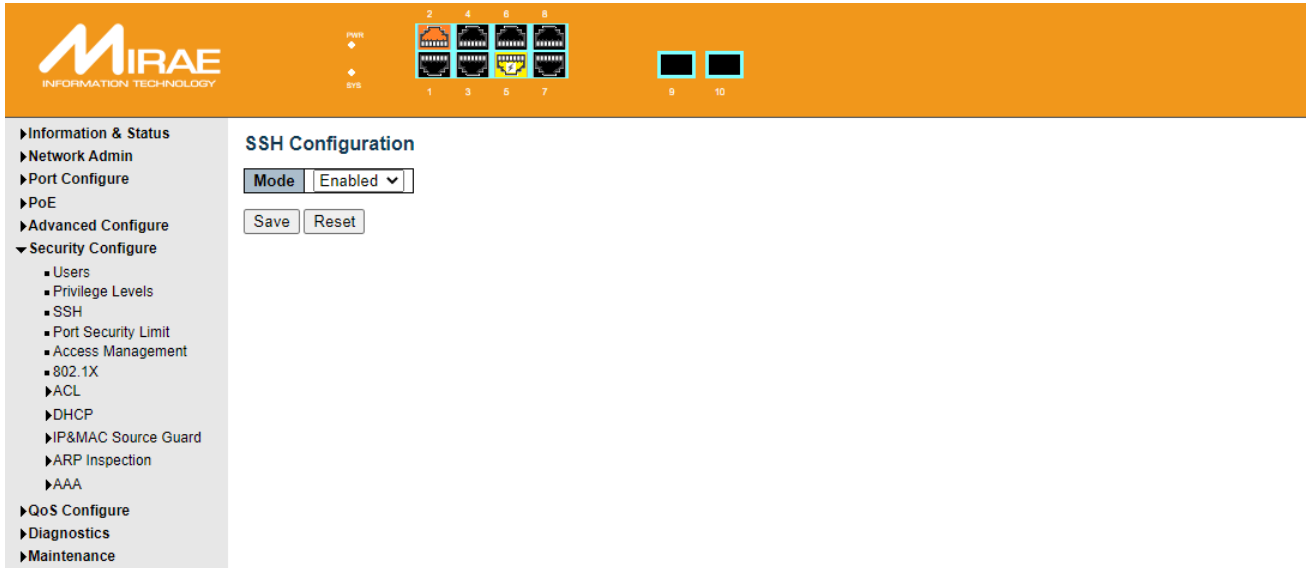
사용자는 스위치에서 로그인 수준을 변경할 수 있습니다.  
다음과 같이 “Security Configure - Privilege Levels” 을 클릭합니다:



## 7.3 SSH

SSH(Secure Shell)는 응용 프로그램 계층을 기반으로하는 보안 프로토콜이며 IETF 의 네트워크 작업 그룹에서 공식화합니다. SSH 는 안정적인 방식으로 안전한 네트워크 서비스, 특히 Rlogin 세션 서비스를 제공합니다. 원격 관리 중 정보 공개를 방지 할 수 있습니다.  
스위치는 SSH 를 관리합니다.

다음과 같이 “Security Configure - SSH” 를 클릭합니다:



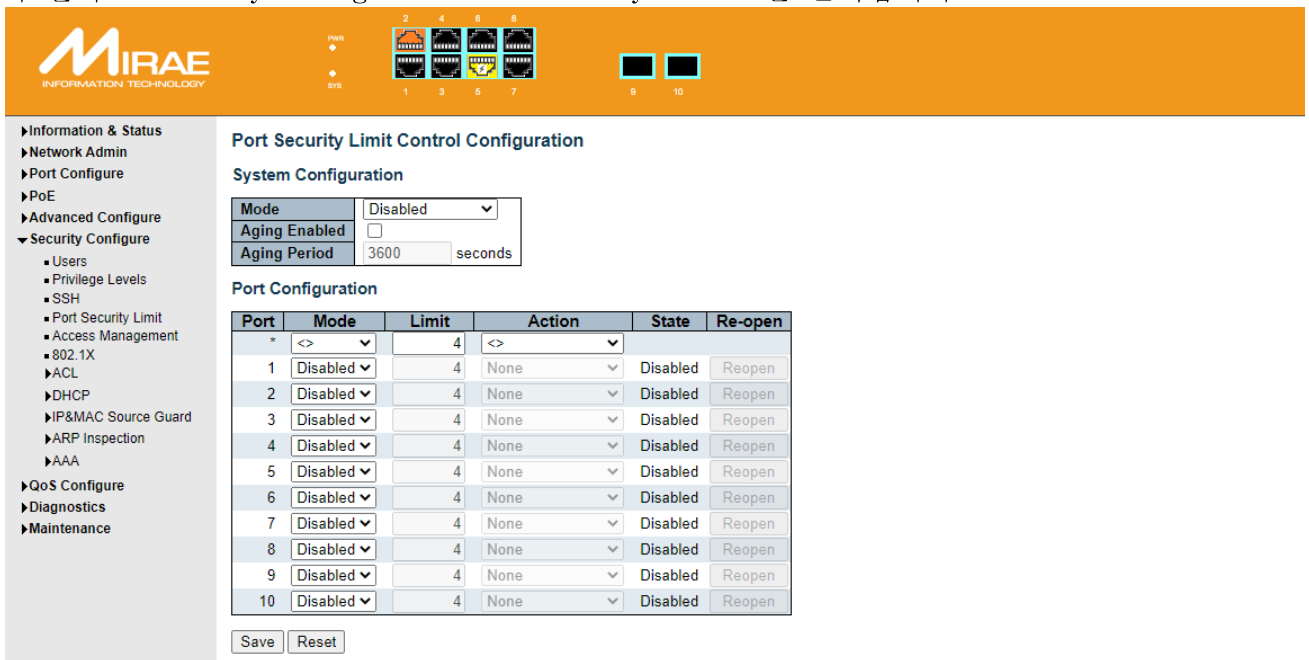
## 7.4 Port Security Limit

포트 보안 :

포트에서 제한된 MAC 주소의 수입니다.

스위치는 포트 보안을 지원합니다.

다음과 같이 “Security Configure - Port Security Limit” 을 클릭합니다:



## 7.5 Access Management

액세스 관리 웹 서비스를 사용하면 스위치 리소스에 안전하게 액세스 할 수 있습니다.

스위치는 액세스 관리를 지원합니다.

다음과 같이 “Security Configure - Access Management” 를 클릭합니다:

## 7.6 802.1X

802.1X 는 액세스 제어 및 인증을 위한 클라이언트 / 서버 기반 프로토콜로 권한이 없는 사용자 / 장치가 액세스 포트를 통해 LAN / WLAN 에 액세스하는 것을 방지합니다. 802.1X 는 스위치 또는 LAN 에서 제공하는 서비스를 획득하기 전에 포트에 연결된 사용자 / 장치를 인증합니다. 인증 전에는 EAPoL (Extensible Authentication Protocol over Lan) 데이터만 스위치 포트를 통해 전달될 수 있습니다. 인증 후 일반 데이터도 이더넷 포트를 통해 원활하게 흐를 수 있습니다.

다음과 같이 “Security Configure - 802.1X” 를 클릭합니다:

구성 항목은 다음과 같습니다

| 구성 항목                | 설 명   |
|----------------------|---|
| System Configuration | "모드, 재인증 활성화, 재인증 기간, EAPOL 시간 초과, 에이징 기간, 보류 시간, RADIUS 할당 QoS 활성화, RADIUS 할당 VLAN 활성화, 게스트 VLAN 활성화, 게스트 VLAN ID 1, 최대 Reauth Count, Allow Guest VLAN if EAPoL See" 중에서 선택하십시오. |

## Port Configuration

"포트, 관리 상태, RADIUS 할당 QoS 활성화, RADIUS 할당 VLAN 활성화, 게스트 VLAN 활성화, 포트 상태, 재시작" 중에서 선택하십시오

“Save” 하고 완료합니다.

## 7.7 ACL

액세스 제어 목록(ACL)은 패킷 수신 및 송신을 제어하는 데 사용되는 스위치 인터페이스의 명령 목록입니다. IP, IPX 및 AppleTalk 와 같은 모든 라우팅 된 프로토콜에 적용됩니다.

정보 지점과 내부 및 외부 네트워크 간의 통신은 엔터프라이즈 네트워크의 필수 비즈니스 요구 사항입니다. 보안 인트라넷의 경우 권한이 없는 사용자가 특정 네트워크 리소스만 사용할 수 있도록 보안 정책을 수립하여 액세스 권한을 제어할 수 있습니다. 간단히 말해서 ACL 필터링 흐름은 액세스 제어를 위한 네트워크 기술입니다.

ACL 은 네트워크 흐름 및 승인된 장치를 제한하고 지정된 포트 패킷을 전달하도록 구성됩니다. 예를 들어, 외부 공용 네트워크가 LAN 에 있는 장치의 범위를 벗어나거나 FTP 서비스만 사용할 수 있습니다. ACL 은 라우터 또는 ACL 기능이 있는 비즈니스 소프트웨어에서 구성할 수 있습니다.

장치 하드웨어 계층 보안을 기반으로 하는 ACL 은 IoT 에서 시스템 보안을 보장하는 중요한 기술입니다. 소프트웨어 장치 간의 통신에 대한 액세스를 제어하고 프로그래밍 방식으로 액세스 규칙을 지정함으로써 ACL 은 불법 장치를 시스템 보안 손상 및 데이터 획득으로부터 분리합니다.

### 7.7.1 ACL Ports

다음과 같이 “Security Configure - ACL - Ports” 를 클릭합니다.

구성 항목은 다음과 같습니다

| 구성 항목           | 설 명  |
|-----------------|--|
| Action          | “Permit” : 데이터가 이 포트를 통해 흐를 수 있습니다.<br>“Deny” : 데이터가 이 포트를 통해 흐를 수 없습니다. |
| Rate Limiter ID | 포트와 함께 제공되는 속도 제한기 ID 입니다. 속도 제한기 구성에서 자세한 내용을 참조하십시오.                   |

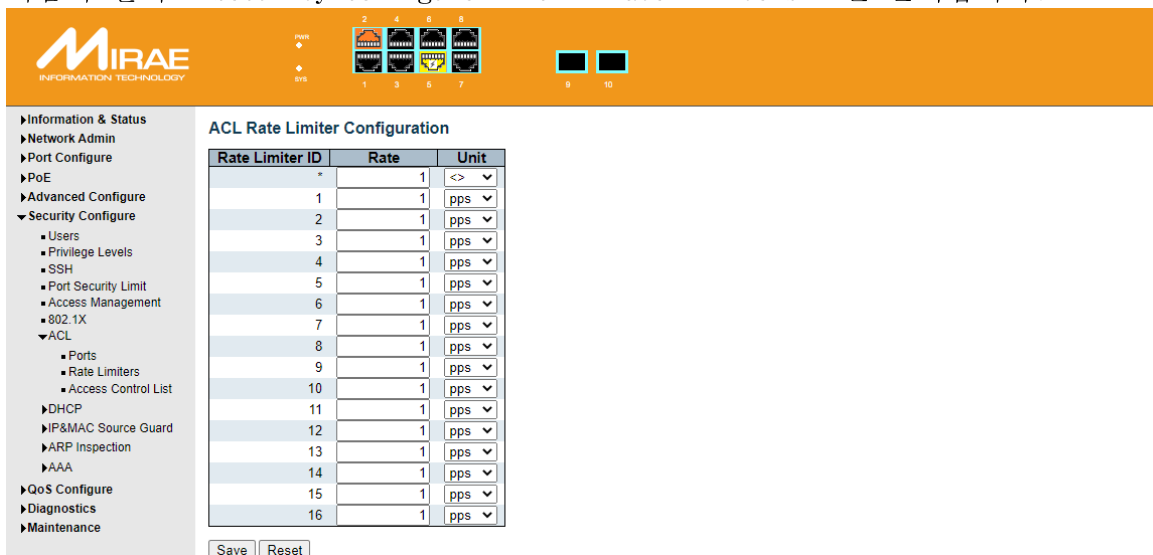


|               |   |
|---------------|---|
| Port Redirect | 리디렉션되는 포트 프레임을 선택합니다. 허용되는 값은 Disabled 또는 특정 포트 번호이며 작업이 허용될 때 설정할 수 없습니다. 기본값은 "Disabled"입니다.  |
| Mirror        | 이 포트의 미러 작업을 지정합니다. 허용되는 값은 다음과 같습니다:<br><b>Enabled:</b> 포트에서 수신된 프레임이 미러링됩니다.<br><b>Disabled:</b> 포트에서 수신된 프레임이 미러링되지 않습니다.<br>기본값은 "Disabled"입니다.   |
| Logging       |   |
| Shutdown      | 이 포트의 포트 종료 작업을 지정합니다. 허용되는 값은 다음과 같습니다:<br><b>Enabled:</b> 포트에서 프레임이 수신되면 포트가 비활성화됩니다.<br><b>Disabled:</b> 포트 종료가 비활성화됩니다.<br>기본값은 "Disabled"입니다.<br>참고 : 종료 기능은 패킷 길이가 1,518 (VLAN 태그 제외) 미만인 경우에만 작동합니다. |
| State         | 이 포트의 포트 상태를 지정하십시오. 허용되는 값은 다음과 같습니다:<br><b>Enabled:</b> ACL 사용자 모듈의 휘발성 포트 구성을 변경하여 포트를 다시 엽니다.<br><b>Disabled:</b> ACL 사용자 모듈의 휘발성 포트 구성을 변경하여 포트를 닫습니다.<br>기본값은 “Enabled” 입니다.                          |
| Counter       | 이 규칙과 일치하는 프레임 수를 계산합니다.  |

“Save” 하고 완료합니다.

## 7.7.2 Rate Limiter

다음과 같이 “Security Configure - ACL - Rate Limiters” 를 클릭합니다.



| Rate Limiter ID | Rate | Unit |
|-----------------|------|------|
| 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  |
| 11              | 1    | pps  |
| 12              | 1    | pps  |
| 13              | 1    | pps  |
| 14              | 1    | pps  |
| 15              | 1    | pps  |
| 16              | 1    | pps  |

### 7.7.3 Access Control List

다음과 같이 “Security Configure - ACL - Access Control List” 를 클릭합니다:

**Access Control List Configuration**

| ACE | Ingress Port | Policy / Bitmask | Frame Type | Action | Rate Limiter | Port Redirect | Mirror | Counter |
|-----|--------------|------------------|------------|--------|--------------|---------------|--------|---------|
| +   |              |                  |            |        |              |               |        |         |

엑세스 제어 목록을 편집하려면 “+” 를 클릭하십시오.

**ACE Configuration**

|               |   |
|---------------|---|
| Ingress Port  | All<br>Port 1<br>Port 2<br>Port 3<br>Port 4 |
| Policy Filter | Any   |
| Frame Type    | Any   |

Save Reset Cancel

**Action**

|              |          |
|--------------|----------|
| Action       | Permit   |
| Rate Limiter | Disabled |
| EVC Policer  | Disabled |
| Mirror       | Disabled |
| Logging      | Disabled |
| Shutdown     | Disabled |
| Counter      | 0        |

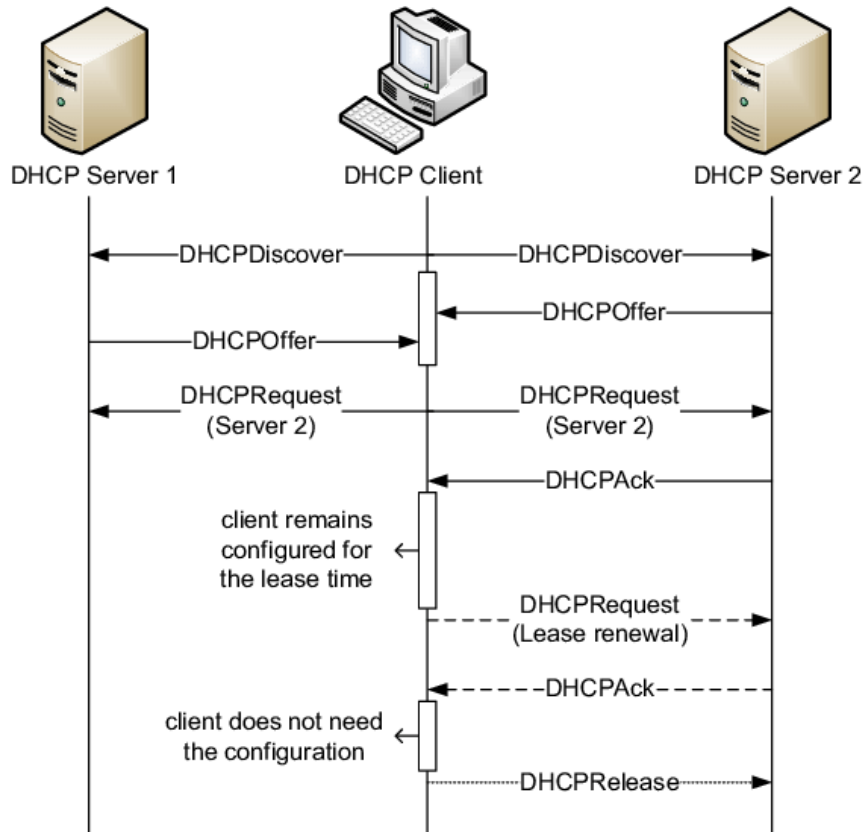
**VLAN Parameters**

|                |     |
|----------------|-----|
| 802.1Q Tagged  | Any |
| VLAN ID Filter | Any |
| Tag Priority   | Any |

## 7.8 DHCP Snooping

### DHCP 원리

DHCP 는 UDP 를 전송 프로토콜로 사용합니다. 호스트는 호스트의 포트 67 에 응답하는 DHCP 서버의 포트 68 에 요청을 보냅니다. 대화형 프로세스는 다음과 같이 자세히 설명됩니다.



1. DHCP 클라이언트는 DHCP Discover 메시지를 브로드캐스트합니다.
2. 메시지를 받은 후 모든 DHCP 서버는 DHCP 클라이언트에게 DHCP Offer 메시지를 회신합니다.
3. DHCP 서버는 메시지의 IP 주소로 "Your (Client) IP Address" 필드를 DHCP Client 에 전송하고 구별을 위해 "Option" 필드에 자체 IP 주소를 입력합니다. DHCP 서버는 메시지를 보낸 후 할당 된 IP 주소를 기록합니다.
4. 일반적으로 DHCP 클라이언트는 수신한 첫 번째 DHCP Offer 메시지만 처리할 수 있습니다. DHCP 요청 메시지를 브로드캐스트하고 선택한 DHCP 서버와 필요한 IP 주소를 옵션 필드에 추가합니다.
5. DHCP Request 메시지를 받은 후 DHCP 서버는 IP 주소를 자신의 주소와 비교합니다. DHCP 서버는 다른 경우에만 해당 IP 주소 할당 기록을 지웁니다. 또는 DHCP ACK 메시지로 DHCP 클라이언트에 응답하고 옵션 필드에 IP 주소에 대한 임대 기간을 추가합니다.
6. DHCP 클라이언트는 DHCP ACK 메시지에서 DHCP 서버가 할당한 IP 주소의 가용성을 확인합니다. DHCP 클라이언트는 IP 주소를 소유하고 주소가 유효한 경우 자동으로 임대를 갱신하거나 DHCP 서버에 이 IP 주소를 비활성화하고 새 주소를 신청하도록 알리는 DHCP 거부 메시지를 보냅니다.
7. DHCP Client 는 언제든지 DHCP Release 메시지를 전송하여 획득한 IP 주소를 해제할 수 있으며, DHCP Server 는 해당 IP 주소를 복구 및 재배포합니다.

8. 임대 기간의 절반이 지나면 DHCP 클라이언트는 유니 캐스트 형식으로 DHCP 요청 메시지를 보내 IP 주소를 갱신합니다. DHCP ACK 메시지를 받으면 DHCP 클라이언트는 필요에 따라 기간을 연장해야 합니다. 그렇지 않으면 DHCP 클라이언트는 이 IP 주소를 계속 사용해야 합니다.
  9. 임대 기간의 87.5 %가 지나면 DHCP 클라이언트는 DHCP 요청 메시지를 브로드 캐스트하여 IP 주소를 갱신합니다. DHCP 클라이언트가 DHCP ACK 메시지를 수신하면 기간이 필요에 따라 연장됩니다. 또는 DHCP 클라이언트는 만료 될 때까지 주소를 계속 사용해야 합니다. 그런 다음이 IP 주소를 해제하고 새 주소를 신청하기 위해 DHCP 해제 메시지를 DHCP 서버에 보내야 합니다.
  10. 설명이 필요한 것은 DHCP 클라이언트가 일반적으로 여러 DHCP 서버에서 첫 번째 DHCP 제안 패킷을 받을 수 있다는 것입니다. 또한 DHCP 서버에서 보낸 DHCP Offer 에 지정된 주소는 배포 할 최종 주소가 아닐 수 있으며, 클라이언트가 요청할 때까지 DHCP 서버에 보관됩니다.
  11. DHCP 클라이언트는 브로드 캐스트 패킷을 통해 DHCP 요청을 보내 주소 배포를 위해 DHCP 서버를 공식적으로 요청하므로 Offer 패킷을 보내는 다른 DHCP 서버도 요청 패킷을 수신할 수 있으므로 DHCP 클라이언트에 제공된 (사전 할당 된) IP 주소를 해제합니다.
  12. DHCP 클라이언트는 다른 사람이 사용하는 주소를 거부하기 위해 DHCP 거부 정보 패킷을 DHCP 서버로 보냅니다.
- DHCP 서버는 잘못된 주소 정보 (예 : 새 서브넷으로 이동 또는 날짜 만료)로 인해 협상 중에 주소 재 신청을 위해 DHCP NAK 메시지를 DHCP 클라이언트에 보냅니다.
13. DHCP 클라이언트는 DHCP 검색 메시지를 DHCP 서버로 브로드 캐스트합니다. DHCP 서버가 응답하지 않으면 메시지를 다시 보냅니다.
  14. 메시지를 받으면 DHCP 서버는 전략에 따라 리소스 (예 : IP 주소)를 배포하고 DHCP Offer 메시지를 DHCP Client 에 보냅니다.
  15. DHCP 클라이언트는 DHCP 요청을 전송하여 서버 임대를 신청하고 다른 서버에이 분산 주소를 수락 함을 알립니다.
  16. DHCP 서버는 배포 가능한 리소스에 대해서는 DHCP ACK 메시지를 보내거나 배포 할 수 없는 리소스에 대해서는 DHCP NAK 메시지를 보냅니다. DHCP 클라이언트는 DHCP ACK 메시지를 받으면 리소스를 사용할 수 있으며 DHCP NAK 메시지를 받으면 DHCP Discover 메시지를 다시 보낼 것입니다.

## DHCP 스누핑 원칙

클라이언트와 서버 간의 DHCP 대화 형 메시지를 스누핑함으로써 DHCP 스누핑 기능은 사용자의 행동을 모니터링하고 적절한 구성으로 DHCP 메시지와 불법 서버를 필터링합니다. 다음은 DHCP Snooping의 용어와 기능에 대한 설명입니다:

- 1) DHCP Snooping Trust Port: DHCP가 브로드캐스트를 통해 IP 인터랙티브 메시지를 획득한다는 점을 감안할 때 사용자에게 정상적인 IP를 획득하도록 영향을 주는 불법 서버가 있으며 일부는 사용자를 속이고 정보를 도용하기도 합니다. 결과적으로 DHCP 스누핑은 포트를 Trust 포트와 Untrust 포트로 분류합니다. 장치는 DHCP 서버와 연결된 적절한 포트를 Trust 포트에 설정하고 다른 포트를 Untrust 포트에 설정하여 불법 서버를 차단하기 위해 Trust 포트에서 수신한 DHCP Reply 메시지만 전달하고 Untrust 포트에서 보낸 메시지는 버립니다.
2. IP 주소를 비공개로 설정하는 것은 일반적으로 DHCP 네트워크에서 볼 수 있으며, 이는 네트워크 유지 관리의 어려움을 증가시킬 뿐만 아니라 충돌로 인해 합법적인 사용자가 네트워크에 액세스하지 못하게 합니다. 클라이언트와 서버 간의 대화형 메시지를 스누핑함으로써 사용자가 획득한 IP, MAC, VID, PORT, 임대 및 기타 정보는 사용자 레코드 항목으로 컴파일되어 DHCP 스누핑 데이터베이스를 형성합니다. ARP 검사 또는 확인 기능을 사용하여 사용자의 인터넷 액세스를 제어합니다. DHCP 스누핑은 장치를 통해 흐르는 메시지의 유효성을 검사하고, 불법 메시지를 버리고, 사용자 정보를 기록하고, 다른 기능 쿼리에 대한 바인딩 데이터베이스를 만듭니다. 다음은 몇 가지 유형의 불법 메시지입니다:

- 1) DHCP ACK, DHCP NACK, DHCP OFFER 등 Untrust 포트에서 수신한 DHCP Reply 메시지.
- 2) 네트워크 관리 정보 [giaddr]와 함께 Untrust 포트에서 수신한 DHCP Reply 메시지.
- 3) MAC 검증시 Source MAC 및 DHCP 메시지의 DHCP Client 필드 값은 각각 다른 패킷을 나타냅니다.
- 4) DHCP 스누핑 바인딩 데이터베이스에 저장된 사용자 정보로 인해 DHCP Release 메시지는 장치별로 데이터베이스에 저장된 포트 정보와 일치하지 않습니다.

## 7.8 DHCP Snooping 의 보안 관련 기능

DHCP 네트워크 환경에서 관리자는 사용자가 허가없이 동적 IP 주소가 아닌 고정 IP 주소를 수정하고 사용하는 경우가 많습니다. 따라서 동적 IP 주소를 사용하는 일부 사용자는 네트워크에 정상적으로 액세스하지 못하여 네트워크 애플리케이션 환경이 복잡해지고 관리자의 관리가 어려워집니다. DHCP 동적 바인딩은 장치가 DHCP 스누핑 중에 합법적인 사용자의 IP를 기록하여 정보를 얻는 보안 프로세스입니다. 세 가지 제어 유형이 있습니다. 첫 번째는 IP Source Guard를 사용하여 합법적인 사용자의 주소를 바인딩하는 것입니다. 두 번째는 소프트웨어의 DAI (Dynamic ARP Inspection)를 사용하여 ARP를 제어하여 사용자의 유효성을 확인하는 것입니다. 마지막은 ARP Check를 통해 합법적인 사용자의 ARP 메시지를 바인딩하는 것입니다.

참고 : IP 소스 가드를 사용하여 주소를 바인딩하는 경우 스위치가 지원할 수 있는 DHCP 사용자 수는 하드웨어 항목에 의해 제한됩니다. 합법적인 사용자는 너무 많은 사용자로 인해 하드웨어 항목을 추가하고 네트워크를 올바르게 사용하지 못할 수 있습니다. 모든 ARP는 DAI 기능을 사용할 때 CPU에 의해 전달되고 처리되므로 스위치 성능에 심각한 영향을 미칩니다.

### DHCP 스누핑과 IP 소스 가드 간의 주소 바인딩 관계

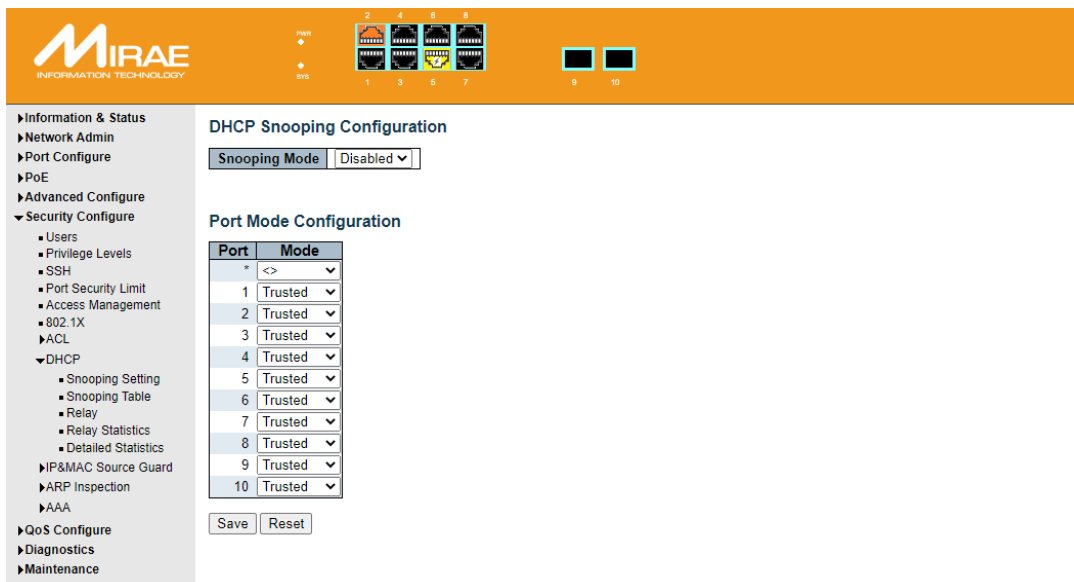
IP Source Guard는 데이터베이스의 사용자 정보 [IP, MAC]를 하드웨어 필터링 항목으로 설정하고 사용자의 네트워크 액세스를 제한하여 IP 소스 주소 데이터베이스를 유지합니다. 자세한 내용은 IP & MAC 소스 가드 구성 섹션을 참조하십시오.

DHCP 스누핑은 사용자가 DHCP 프로세스에서 스누핑하고, 사용자 IP 데이터베이스를 유지하고, 필터링을 위해 IP Source Guard에 데이터를 제출하여 DHCP를 통해 IP를 획득 한 사용자 만 네트워크에 액세스 할 수 있도록함으로써 사용자가 개인 IP 주소를 설정하는 것을 방지합니다.

또한 DHCP 바인딩은 IP 메시지 만 필터링하므로 ARP 스누핑과 같은 보안 및 문제 방지를 위해 DHCP 바인딩 사용자의 유효성을 검사합니다. 자세한 내용은 ARP 검사 구성 섹션을 참조하십시오.

### 7.8.1 DHCP Snooping

설정을 위해 다음과 같이 “Security Configure - DHCP - Snooping Setting” 을 클릭하십시오:



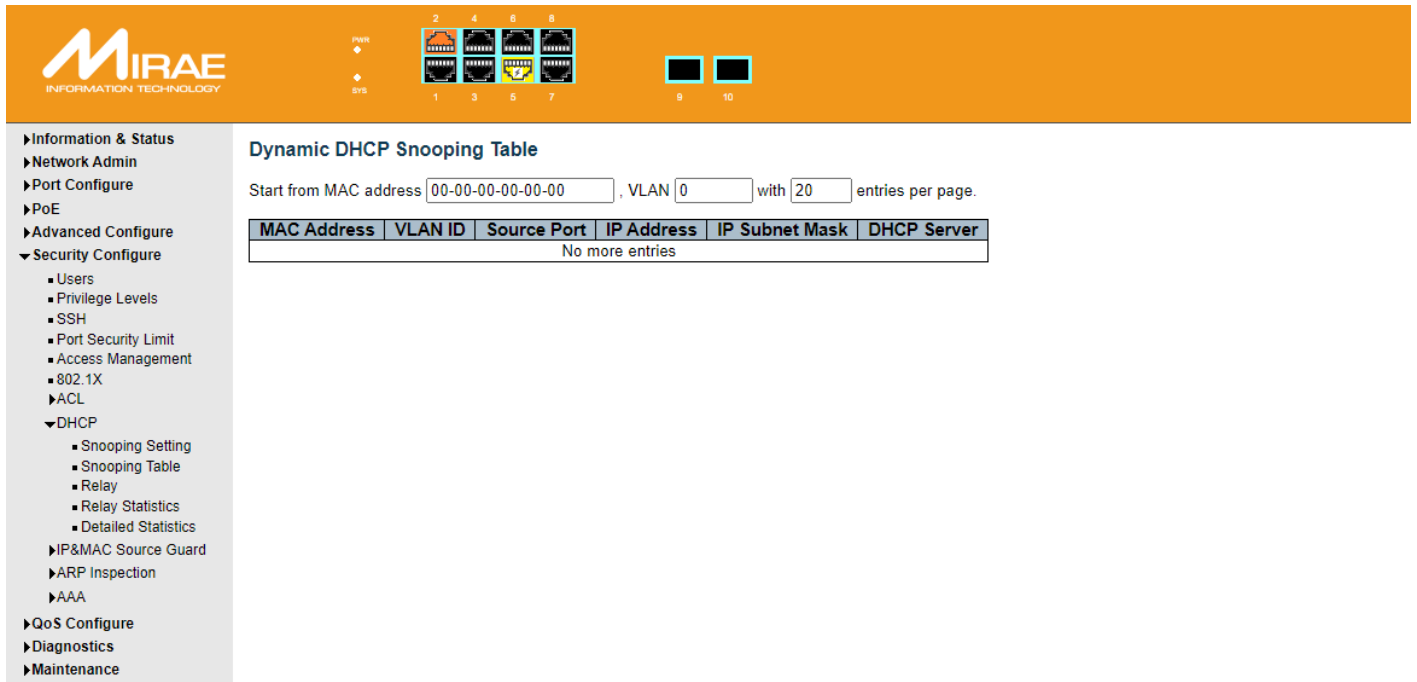
구성 항목은 다음과 같습니다

| 구성 항목              | 설 명  |
|--------------------|--|
| DHCP Snooping Mode | DHCP 스누핑을 활성화 또는 비활성화합니다.  |
| Port Mode          | DHCP 스누핑 포트 모드를 나타냅니다. 가능한 포트 모드는 다음과 같습니다:<br><b>Trusted:</b> 포트를 DHCP 메시지의 신뢰할 수 있는 소스로 구성합니다..<br><b>Untrusted:</b> 포트를 DHCP 메시지의 신뢰할 수 없는 소스로 구성합니다. |

모든 변경 사항을 저장하려면 “Save” 을 클릭하십시오.

## 7.8.2 DHCP Snooping Table

“Advanced Configure - DHCP - Snooping Table” 을 클릭하여 다음과 같이 DHCP 스누핑 구성을 확인합니다:



The screenshot shows the web interface of the MIRAE network switch. The left sidebar contains a navigation menu with options like Information & Status, Network Admin, Port Configure, PoE, Advanced Configure, Security Configure, Users, Privilege Levels, SSH, Port Security Limit, Access Management, 802.1X, ACL, DHCP, Snooping Setting, Snooping Table, Relay, Relay Statistics, Detailed Statistics, IP&MAC Source Guard, ARP Inspection, AAA, QoS Configure, Diagnostics, and Maintenance. The main content area is titled 'Dynamic DHCP Snooping Table'. It includes a search filter: 'Start from MAC address 00-00-00-00-00-00, VLAN 0 with 20 entries per page.' Below this is a table with columns: MAC Address, VLAN ID, Source Port, IP Address, IP Subnet Mask, and DHCP Server. The table is currently empty, showing 'No more entries'.

## 7.9 IP & MAC Source Guard

IP 및 MAC Source Guard 는 Source IP 및 MAC 바인딩 데이터베이스를 유지하여 해당 포트의 Source IP 및 MAC 을 기반으로 호스트 메시지를 필터링하여 Source IP 및 MAC 바인딩 데이터베이스의 호스트에 대한 유일한 네트워크 액세스를 보장합니다.

## 7.9.1 Configuration

다음과 같이 “Security Configure - IP & MAC Source Guard - Configuration” 을 클릭합니다.

**IP Source Guard Configuration**

Mode: Disabled

Translate dynamic to static

**Port Mode Configuration**

| 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           |
| 8    | Disabled | Unlimited           |
| 9    | Disabled | Unlimited           |
| 10   | Disabled | Unlimited           |

Save Reset

구성 항목은 다음과 같습니다.

| 구성 항목               | 설 명                                     |
|---------------------|---|
| Global Pattern      | 글로벌 패턴을 기반으로 IP 및 MAC 소스 가드 활성화 또는 비활성화 |
| Port Mode           | 포트에 따라 IP 및 MAC 소스 가드 활성화 또는 비활성화       |
| Max Dynamic Clients | 무제한, 0, 1, 2 중에서 지원되는 최대 고객 수를 선택합니다.   |

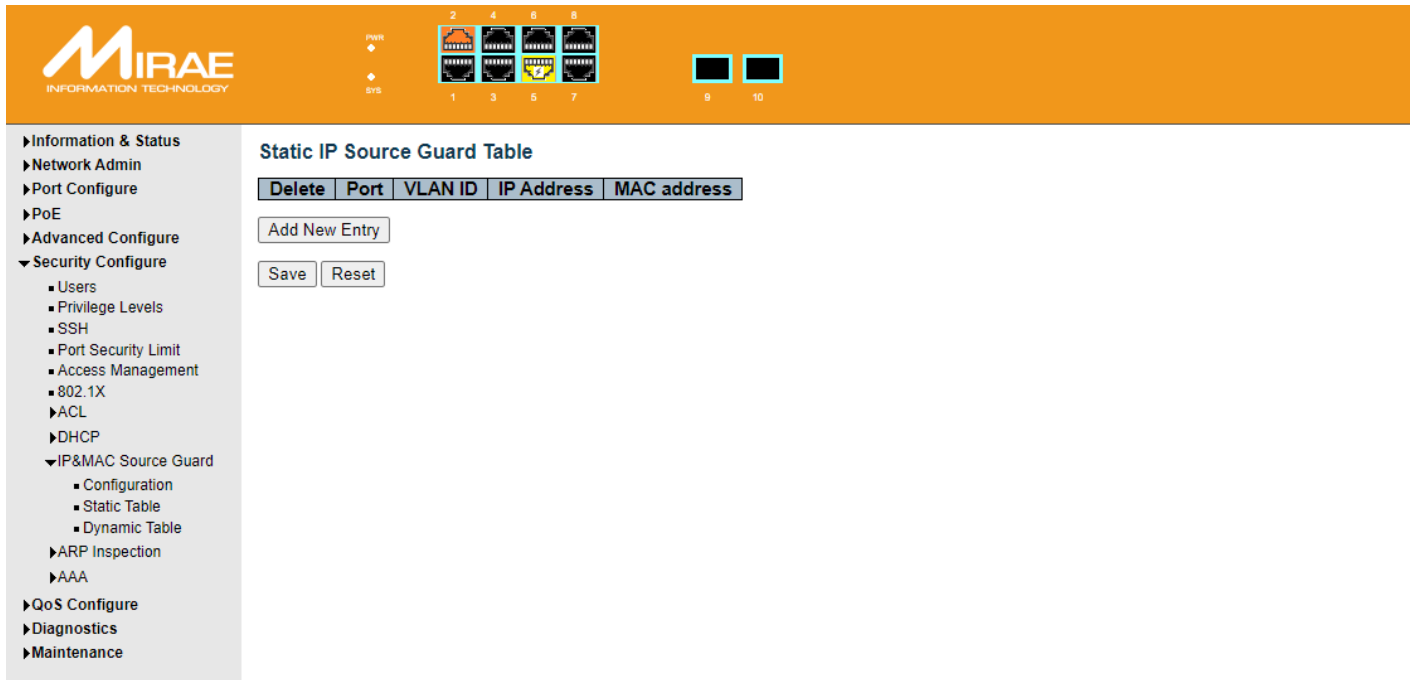
“Save” 하고 완료합니다.

## 7.9.2 Static Table

사용자가 페이지의 포트를 제어하기 위해 IP 및 MAC Guard 의 바인딩 항목을 수동으로 구성할 수 있습니다.

다음과 같이 “Security Configure - IP & MAC Source Guard - Static Table” 을 클릭합니다.





구성 항목은 다음과 같습니다

| 구성 항목       | 설 명                     |
|-------------|-------------------------|
| Port        | 바인딩 할 포트 ID 를 입력하십시오.   |
| VLAN        | 바인딩 할 VLAN ID 를 입력하십시오. |
| IP Address  | 바인딩 할 IP 주소를 입력합니다.     |
| MAC Address | 바인딩 할 MAC 주소를 입력합니다.    |

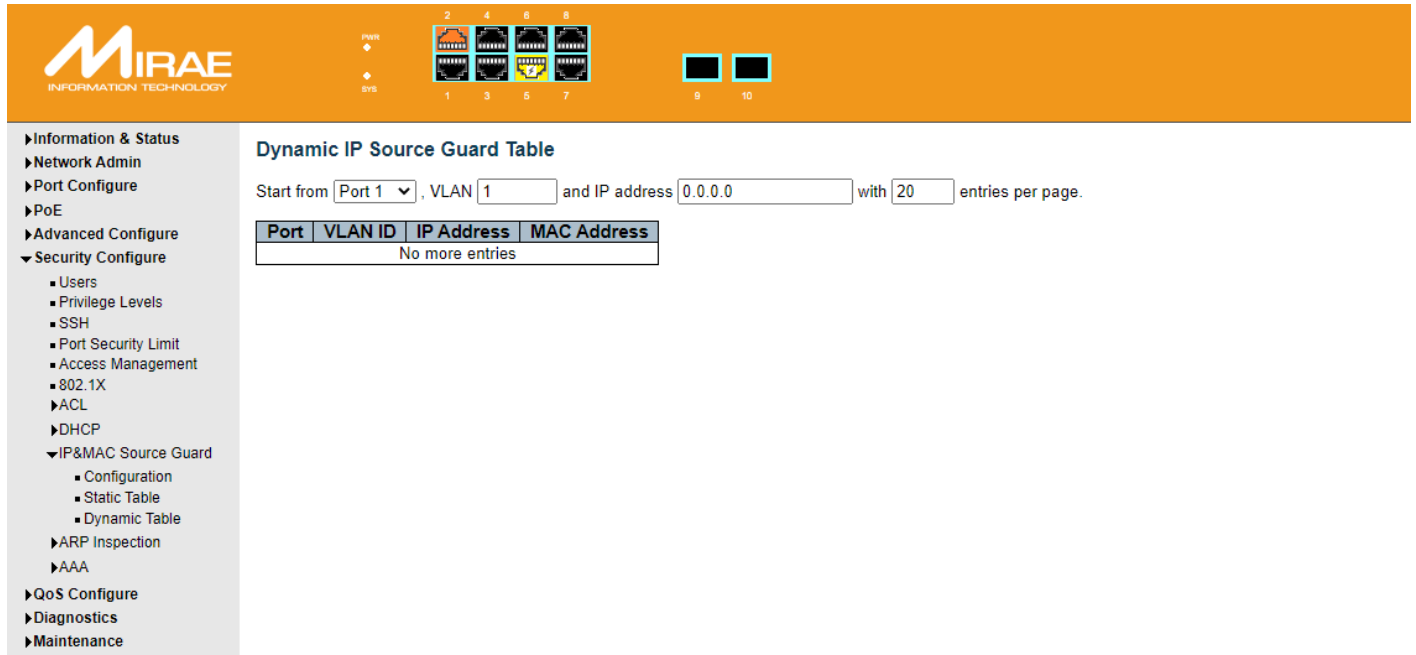
입력 정보에 따라 “Add a New Entry” 를 클릭합니다.

“Save” 하고 완료합니다.



### 7.9.3 Dynamic Table

사용자님이 페이지의 포트를 제어하기 위해 IP 및 MAC Guard 의 바인딩 항목을 수동으로 구성할 수 있습니다. 다음과 같이 “Security Configure - IP & MAC Source Guard - Static Table” 을 클릭합니다.



구성 항목은 다음과 같습니다

| 구성 항목       | 설 명        |
|-------------|------------|
| Port        | 포트 ID 표시   |
| VLAN        | VLAN ID 표시 |
| IP Address  | IP 주소 표시   |
| MAC Address | MAC 주소 표시  |

### 7.10 ARP Inspection

IP 및 MAC Source Guard 는 Source IP 및 MAC 바인딩 데이터베이스를 유지하여 해당 포트의 Source IP 및 MAC 을 기반으로 호스트 메시지를 필터링하여 Source IP 및 MAC 바인딩 데이터베이스의 호스트에 대한 유일한 네트워크 액세스를 보장합니다.

## 7.10.1 Port Configuration

사용자는 이 페이지에서 포트 구성을 편집할 수 있습니다.

다음과 같이 “Security Configure - ARP Inspection - Port Configuration” 을 클릭합니다.

| Port | Mode     | Check VLAN | Log Type |
|------|----------|------------|----------|
| *    | <>       | <>         | <>       |
| 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     |
| 8    | Disabled | Disabled   | None     |
| 9    | Disabled | Disabled   | None     |
| 10   | Disabled | Disabled   | None     |

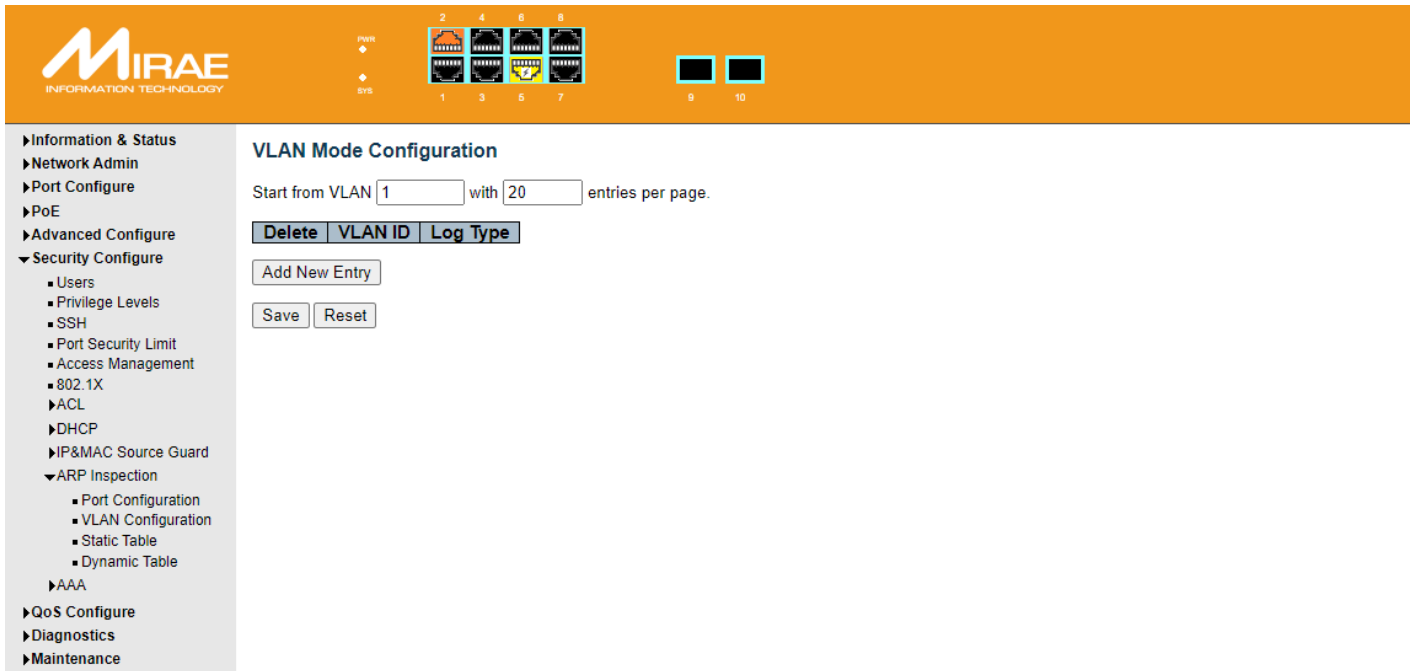
구성 항목은 다음과 같습니다

| 구성 항목          | 설 명  |
|----------------|--|
| Global Pattern | 글로벌 패턴을 기반으로 ARP 검사 활성화 또는 비활성화  |
| Port Mode      | 포트 기반 ARP 검사 활성화 또는 비활성화   |
| Check VLAN     | VLAN 구성을 검사하려면 "Check VLAN" 설정을 활성화해야 합니다. "Check VLAN"의 기본 설정은 비활성화되어 있습니다. "Check VLAN" 설정이 비활성화 된 경우 ARP 검사의 로그 유형은 포트 설정을 참조합니다. "Check VLAN" 설정이 활성화되면 ARP 검사의 로그 유형은 VLAN 설정을 참조합니다. "Check VLAN"의 가능한 설정은 다음과 같습니다:<br><b>Enabled:</b> VLAN 작동 확인을 활성화합니다.<br><b>Disabled:</b> VLAN 작동 확인을 비활성화합니다. |
| Log Type       | 지정된 포트에서 글로벌 모드 및 포트 모드 만 활성화되고 "Check VLAN " 설정은 비활성화되며 ARP 검사의 로그 유형은 포트 설정을 참조합니다. 네 가지 로그 유형이 있으며 가능한 유형은 다음과 같습니다:<br><b>None:</b> 아무것도 기록하지 않습니다.<br><b>Deny:</b> 거부 된 항목을 기록합니다.<br><b>Permit:</b> 허용 된 항목을 기록합니다.<br><b>All:</b> 모든 항목을 기록합니다.   |

“Save” 하고 완료합니다.

## 7.10.2 VLAN Configuration

다음과 같이 “Security Configure - ARP Inspection - VLAN Configuration” 를 클릭합니다.



구성 항목은 다음과 같습니다

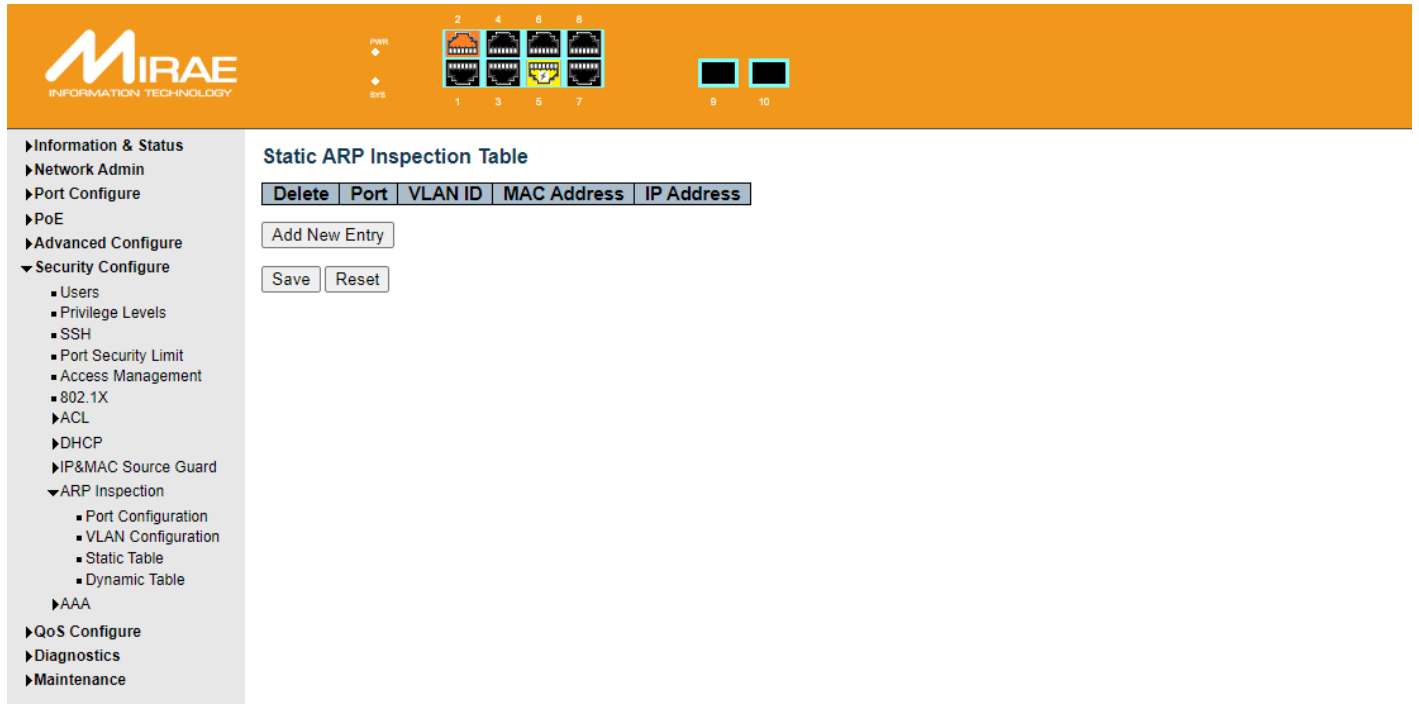
| 구성 항목      | 설 명   |
|------------|---|
| VLAN ID    | ARP 검사의 VLAN 별 구성   |
| Log Type   | 포트 기반 ARP 검사를 활성화 또는 비활성화합니다.   |
| Check VLAN | 어떤 VLAN 에서 ARP 검사가 활성화되었는지 지정합니다. 먼저 포트 모드 설정 웹 페이지에서 포트 설정을 활성화해야 합니다. 지정된 포트에서 글로벌 모드와 포트 모드가 모두 활성화 된 경우에만 지정된 포트에서 ARP 검사가 활성화됩니다. 둘째, VLAN 모드 구성 웹 페이지에서 검사 할 VLAN 을 지정할 수 있습니다. 로그 유형은 VLAN 설정별로 구성할 수도 있습니다. 가능한 유형은 다음과 같습니다:<br><b>None</b> : 아무 것도 기록하지 않습니다.<br><b>Deny</b> : 거부된 항목을 기록합니다.<br><b>Permit</b> : 허용된 항목을 기록합니다.<br><b>All</b> : 모든 항목을 기록합니다. |

“Save” 하고 완료합니다.

“Add New Entry” 를 클릭하여 새 VLAN 구성을 만듭니다.

### 7.10.3 Static Table

사용자는 ARP 검사의 바인딩 테이블을 수동으로 구성하여 이 페이지의 포트를 제어할 수 있습니다. 다음과 같이 “Security Configure - ARP Inspection - Static Table” 을 클릭합니다.



구성 항목은 다음과 같습니다

| 구성 항목       | 설 명                     |
|-------------|-------------------------|
| Port        | 바인딩 할 포트 ID 를 입력하십시오.   |
| VLAN        | 바인딩 할 VLAN ID 를 입력하십시오. |
| IP Address  | 바인딩 할 IP 주소를 입력합니다.     |
| MAC Address | 바인딩 할 MAC 주소를 입력합니다.    |

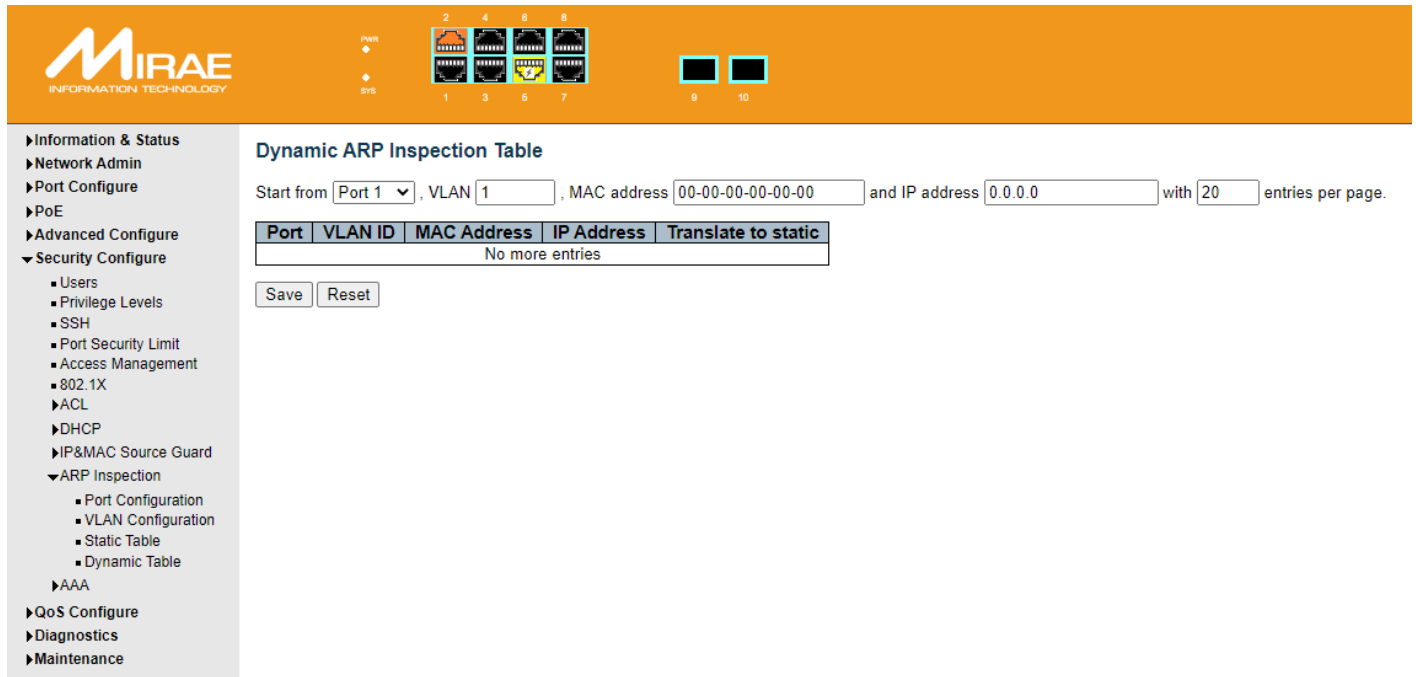
입력 정보에 따라 “Add New Entry” 를 클릭합니다.

“Save” 하고 완료합니다.

## 7.10.4 Dynamic Table

사용자는 이 페이지에서 포트를 제어하기 위해 IP 및 MAC Guard 의 바인딩 테이블을 수동으로 구성할 수 있습니다.

다음과 같이 “Security Configure - ARP Inspection - Dynamic Table” 을 클릭합니다.



구성 항목은 다음과 같습니다

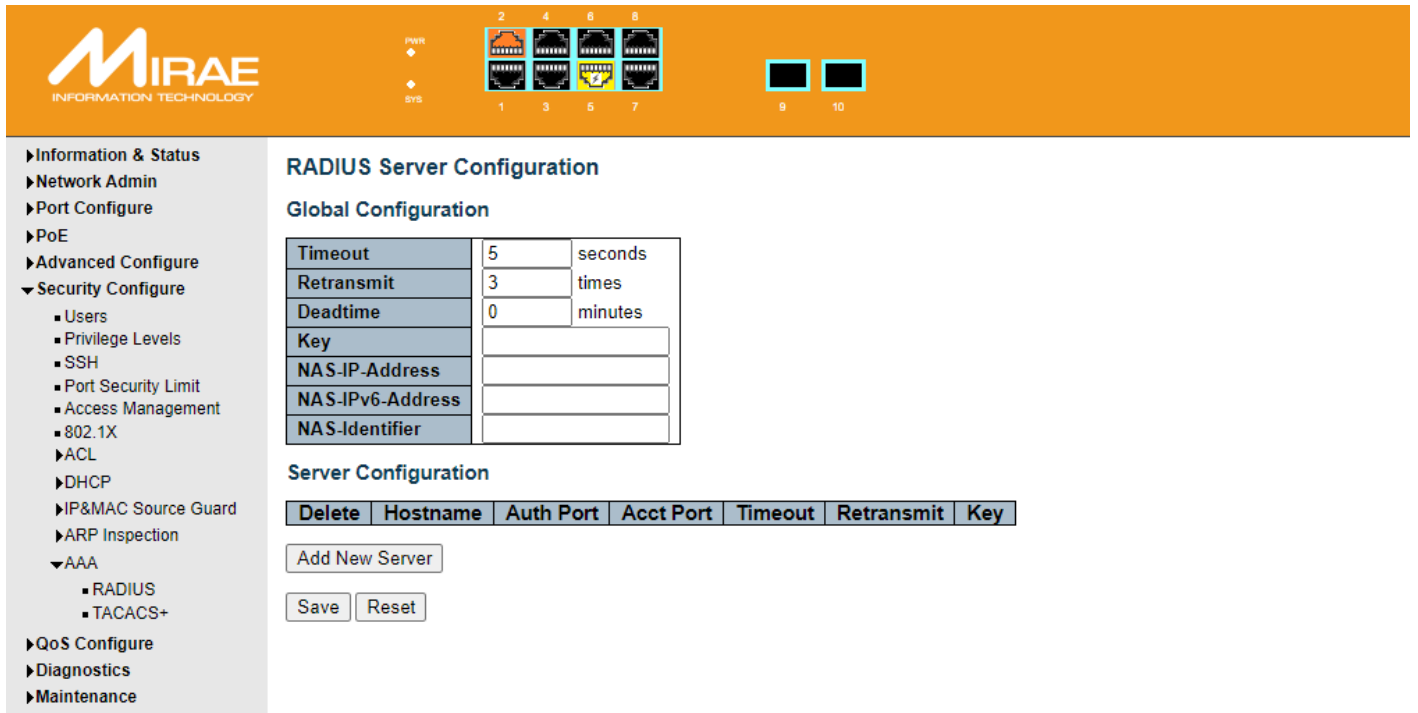
| 구성 항목       | 설 명        |
|-------------|------------|
| Port        | 포트 ID 표시   |
| VLAN        | VLAN ID 표시 |
| IP Address  | IP 주소 표시   |
| MAC Address | MAC 주소 표시  |

## 7.11 AAA

AAA 는 Authentication, Authorization 및 Accounting 의 약자입니다. 네트워크 접근 통제를 위한 보안 관리 메커니즘으로 3 가지 보안 서비스를 제공합니다.

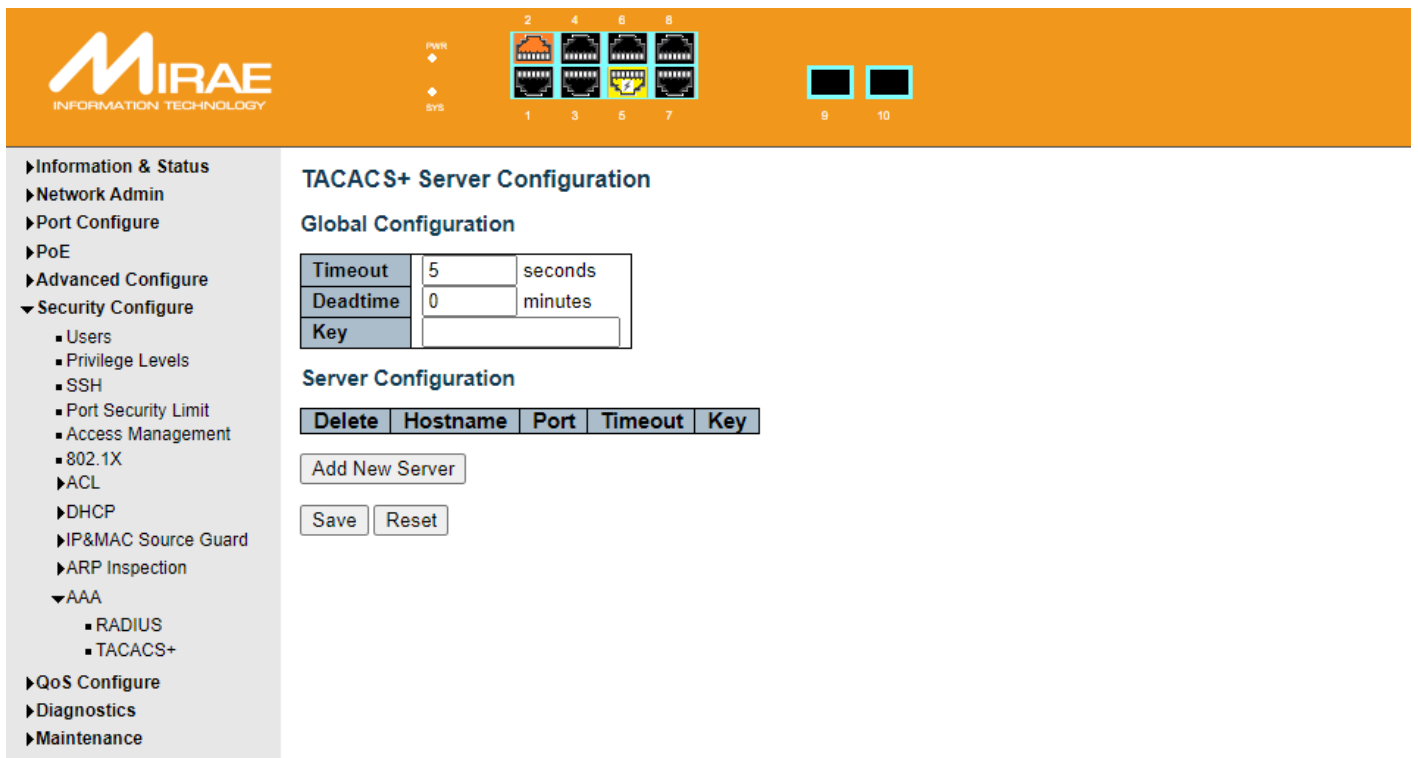
### 7.11.1 RADIUS

다음과 같이 “Security Configure - AAA - RADIUS” 를 클릭합니다:



## 7.11.2 TACACS+

다음과 같이 “Security Configure - AAA - TACACS+” 를 클릭합니다:



## 8 QoS

QoS(Quality of Service)는 고객의 요구 사항을 충족하는 서비스 제공 업체의 능력과 인터넷을 통해 패킷을 보내는 능력을 평가합니다. 다양한 측면에 따라 다양한 서비스를 평가할 수 있습니다. QoS 는 일반적으로 대역폭, 지연, 지연 변동 및 전달 중 패킷 손실률과 같은 핵심 요구 사항을 지원하는 서비스 기능의 평가를 나타냅니다. 처리량이라고도 하는 대역폭은 kbit / s 단위로 지정된 시간 동안

비즈니스 흐름의 평균 속도를 나타냅니다. 지연은 네트워크를 통한 비즈니스 흐름에 필요한 평균 시간을 나타냅니다. 네트워크 장치의 경우 일반적인 지연 요구 사항은 다음과 같습니다.

두 가지 지연 수준이 있습니다. 즉, 우선 순위가 높은 비즈니스는 우선 순위 대기열의 스케줄링 방법을 통해 가능한 한 빨리 서비스를 제공할 수 있고, 낮은 우선 순위 비즈니스는 그 후에 서비스를 받습니다.

지연 변동은 네트워크를 통해 흐르는 비즈니스의 시간 변화를 나타냅니다. 패킷 손실률은 전송 중 손실된 비즈니스 흐름의 비율을 나타냅니다. 최신 전송 시스템은 매우 안정적이므로 네트워크 정체로 인해 정보가 손실되는 경우가 많습니다. 대기열 오버플로로 인한 패킷 손실이 가장 일반적인 상황입니다.

기존 IP 네트워크의 모든 메시지는 동일하게 취급됩니다. 모든 네트워크 장치는 FIFO 기반으로 메시지를 처리하고 안정성, 전송 지연 또는 기타 성능을 보장하지 않고 메시지를 대상으로 보내기 위해 최선을 다합니다. 빠르게 변화하는 IP 네트워크에서 새로운 애플리케이션이 계속 등장함에 따라 네트워크 서비스 품질이 지속적으로 향상됩니다. 예를 들어 VoIP, 비디오 및 기타 지연에 민감한 서비스는 메시지 전송 지연에 대해 더 높은 표준을 설정했습니다. 단기간 메시지 전송이 일반적인 추세였습니다. 요구 사항이 다른 음성, 비디오 및 데이터 서비스를 지원하기 위해 네트워크는 비즈니스 유형을 식별하고 해당 서비스를 제공해야 합니다. 비즈니스 유형을 구별하는 기능은 해당 서비스를 제공하기 위한 전제 조건이므로 기존의 최선형 서비스는 더 이상 애플리케이션 요구 사항을 충족하지 못합니다. 그래서 QoS 가 등장합니다. 네트워크 정체를 방지 및 처리하고 패킷 손실률을 줄이기 위해 네트워크 흐름을 조절합니다. 한편, 사용자는 전용 대역폭을 즐길 수 있으며 비즈니스는 서비스 품질을 향상시켜 네트워크 서비스 용량을 완벽하게 할 수 있습니다.

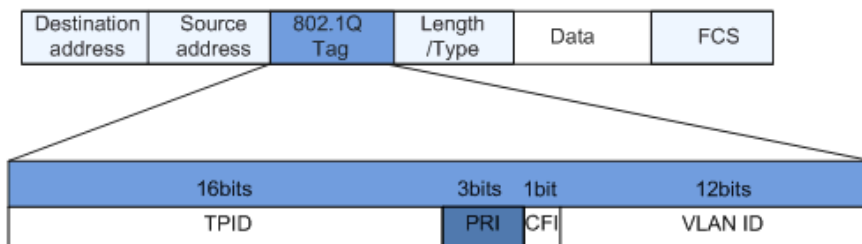
QoS 우선 순위는 메시지 유형에 따라 다릅니다. 예를 들어 VLAN 메시지는 CoS (Class of Service) 필드라고도 하는 802.1p 를 사용하는 반면 IP 메시지는 DSCP 를 사용합니다.

우선 순위를 유지하려면 메시지가 네트워크를 통해 흐를 때 다양한 네트워크에 연결된 게이트웨이에서 이러한 필드를 매핑해야 합니다.

### VLAN 프레임 헤더의 802.1p 우선 순위

일반적으로 VLAN 프레임은 레이어 2 장치간에 상호 작용합니다. VLAN 프레임 헤더의 PRI 필드 (즉, 802.1p 우선 순위) 또는 CoS 필드는 IEEE 802.1Q 의 정의에 따라 서비스 품질 요구 사항을 식별합니다.

#### VLAN 프레임의 802.1p 우선 순위

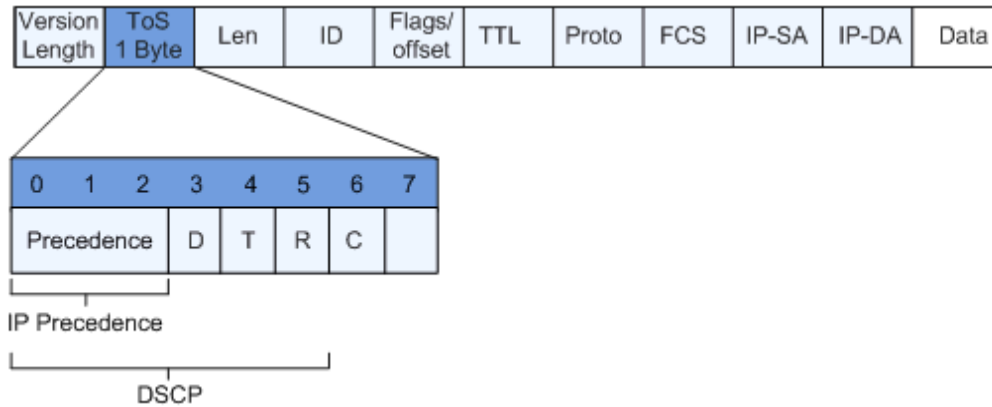


802.1Q 헤더에는 3 비트 PRI 필드가 있습니다. PRI 필드는 높음에서 낮음까지 7 에서 0 까지의 8 CoS 비즈니스 우선 순위를 정의합니다.

#### IP 우선 순위 / DSCP 필드

RFC791 정의에 따르면 IP 메시지 헤더의 ToS (Type of Service) 도메인은 8 비트로 구성됩니다. 그 중에서 다음과 같이 3 비트 long Precedence 필드는 IP 메시지 우선 순위를 식별합니다.

## IP 우선 순위 / DSCP 필드



0 ~ 2 비트는 7 ~ 0 범위의 메시지 전송 우선 순위를 나타내는 우선 순위 필드이며, 네트워크 제어 통신을 라우팅하거나 업데이트하기 위해 일반적으로 예약된 최고 우선 순위는 레벨 7 또는 6 입니다. 사용자 수준 응용 프로그램은 수준 0 ~ 5에만 액세스 할 수 있습니다.

ToS 도메인은 Precedence 필드 외에 D, T 및 R 비트도 포함합니다. D- 비트는 지연 요구 사항을 나타냅니다 (일반 지연의 경우 0, 낮은 지연의 경우 1). T- 비트는 처리량을 나타냅니다 (일반 처리량의 경우 0, 높은 처리량의 경우 1). R- 비트는 신뢰성을 나타냅니다 (일반 신뢰성의 경우 0, 높은 신뢰성의 경우 1). ToS 도메인은 6 비트와 7 비트를 예약합니다.

RFC1349는 통화 비용을 나타내는 C 비트를 추가하여 ToS 도메인을 재정의합니다. IETF DiffServ 그룹은 RFC2474의 IPv4 메시지 헤더에있는 ToS 도메인의 0 ~ 5 비트를 DSCP로 재정의하고 위 그림과 같이 DS (Differentiated Service) 바이트로 이름을 바꿉니다.

DS 필드의 처음 6 비트 (0-5 비트)는 DSCP (DS 코드 포인트)를 구분하며 상위 2 비트 (6-7 비트)는 예약됩니다. 하위 3 비트 (0-2 비트)는 CSCP (Class Selector Code Point)이며 동일한 CSCP 값은 동일한 클래스의 DSCP를 나타냅니다. DS 노드는 DSCP 값에 따라 해당 PHB (호당 동작)를 선택합니다.

## 8.1 Port Classification

스위치는 기본적으로 802.1p 우선 순위를 구성하고 DPL, PCP 및 DEI와 같은 정보를 각 포트에 배포합니다. 우선 순위와 유효한 우선 순위는 0 (가장 낮음)과 7 (가장 높음)으로 표시됩니다.

다음과 같이 “QoS Configure - Port Classification”을 클릭합니다:

The screenshot shows the 'QoS Ingress Port Classification' configuration page. The left sidebar contains a navigation menu with options like Information & Status, Network Admin, Port Configure, PoE, Advanced Configure, Security Configure, and QoS Configure. The main area displays a table for configuring port classification for ports 1 through 10. The table columns are Port, CoS, DPL, PCP, DEI, Tag Class., DSCP Based, and Address Mode. The 'Tag Class.' column is set to 'Disabled' for all ports, and the 'DSCP Based' column is set to 'Source' for all ports. The 'Address Mode' column is set to 'Source' for all ports. Below the table are 'Save' and 'Reset' buttons.

| Port | CoS | DPL | PCP | DEI | Tag Class. | DSCP Based               | Address Mode |
|------|-----|-----|-----|-----|------------|--------------------------|--------------|
| 1    | 0   | 0   | 0   | 0   | Disabled   | <input type="checkbox"/> | Source       |
| 2    | 0   | 0   | 0   | 0   | Disabled   | <input type="checkbox"/> | Source       |
| 3    | 0   | 0   | 0   | 0   | Disabled   | <input type="checkbox"/> | Source       |
| 4    | 0   | 0   | 0   | 0   | Disabled   | <input type="checkbox"/> | Source       |
| 5    | 0   | 0   | 0   | 0   | Disabled   | <input type="checkbox"/> | Source       |
| 6    | 0   | 0   | 0   | 0   | Disabled   | <input type="checkbox"/> | Source       |
| 7    | 0   | 0   | 0   | 0   | Disabled   | <input type="checkbox"/> | Source       |
| 8    | 0   | 0   | 0   | 0   | Disabled   | <input type="checkbox"/> | Source       |
| 9    | 0   | 0   | 0   | 0   | Disabled   | <input type="checkbox"/> | Source       |
| 10   | 0   | 0   | 0   | 0   | Disabled   | <input type="checkbox"/> | Source       |

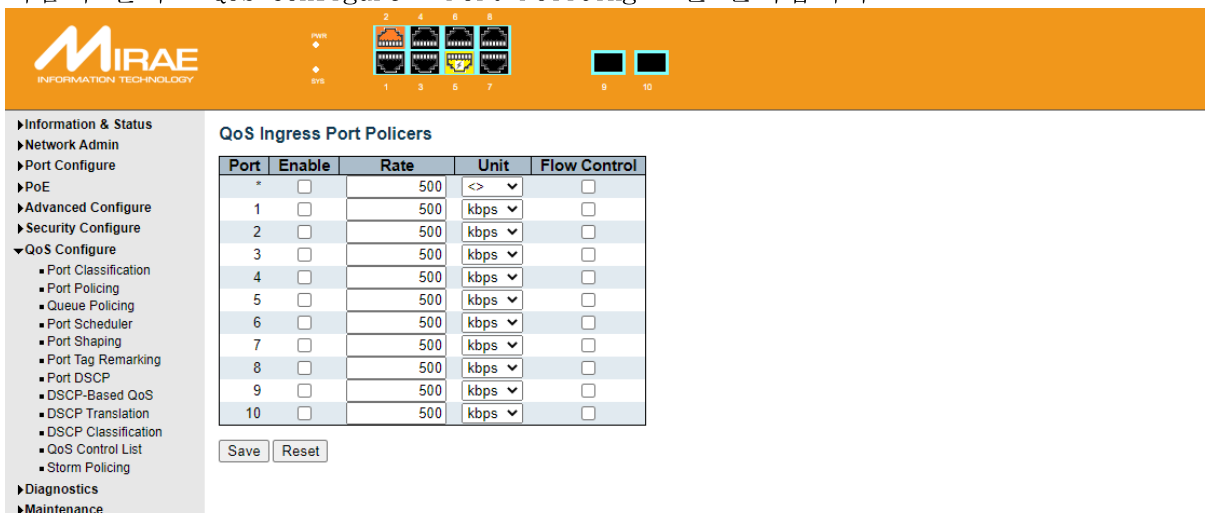


구성 항목은 다음과 같습니다.

| 구성 항목        | 설 명  |
|--------------|--|
| CoS          | 기본 서비스 클래스를 제어합니다.<br>모든 프레임은 CoS 로 분류됩니다. CoS, 대기열 및 우선 순위간에 일대일 매핑이 있습니다. CoS 가 0 (영)이면 우선 순위가 가장 낮습니다.<br>분류된 CoS 는 QCL 항목에 의해 무시 될 수 있습니다.<br>참고 : 기본 CoS 가 동적으로 변경된 경우 구성된 기본 CoS 뒤에 실제 기본 CoS 가 괄호 안에 표시됩니다. |
| DPL          | 기본 드롭 우선 순위 수준을 제어합니다.<br>모든 프레임은 드롭 우선 순위 수준으로 분류됩니다.<br>분류 된 DPL 은 QCL 항목에 의해 무시 될 수 있습니다.   |
| PCP          | 기본 PCP 값을 제어합니다.<br>모든 프레임은 PCP 값으로 분류됩니다.<br>포트가 VLAN 을 인식하고 프레임에 태그가 지정된 경우 프레임은 태그의 PCP 값으로 분류됩니다. 그렇지 않으면 프레임이 기본 PCP 값으로 분류됩니다  |
| DEI          | 기본 DEI 값을 제어합니다.<br>모든 프레임은 DEI 값으로 분류됩니다.<br>포트가 VLAN 을 인식하고 프레임에 태그가 지정된 경우 프레임은 태그의 DEI 값으로 분류됩니다. 그렇지 않으면 프레임은 기본 DEI 값으로 분류됩니다.   |
| Address Mode | QCL 분류가이 포트의 소스 (SMAC / SIP) 또는 대상 (DMAC / DIP) 주소를 기반으로해야하는지 여부를 지정하는 IP / MAC 주소 모드입니다. 허용되는 값은 다음과 같습니다:<br><br>Source: SMAC / SIP 일치를 활성화합니다.<br><br>Destination: DMAC / DIP 일치를 활성화합니다.                       |

## 8.2 Port Policing

다음과 같이 “QoS Configure - Port Policing” 를 클릭합니다:



The screenshot shows the MIRAE network switch web interface. The sidebar on the left contains the following navigation links: Information & Status, Network Admin, Port Configure, PoE, Advanced Configure, Security Configure, QoS Configure (selected), Diagnostics, and Maintenance. Under QoS Configure, the following sub-links are listed: Port Classification, Port Policing (selected), Queue Policing, Port Scheduler, Port Shaping, Port Tag Remarking, Port DSCP, DSCP-Based QoS, DSCP Translation, DSCP Classification, QoS Control List, and Storm Policing.

The main content area is titled "QoS Ingress Port Policers" and contains a table with the following columns: Port, Enable, Rate, Unit, and Flow Control. The table lists 10 ports, each with a rate of 500 kbps and a flow control checkbox.

| 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"/> |

At the bottom of the table, there are "Save" and "Reset" buttons.

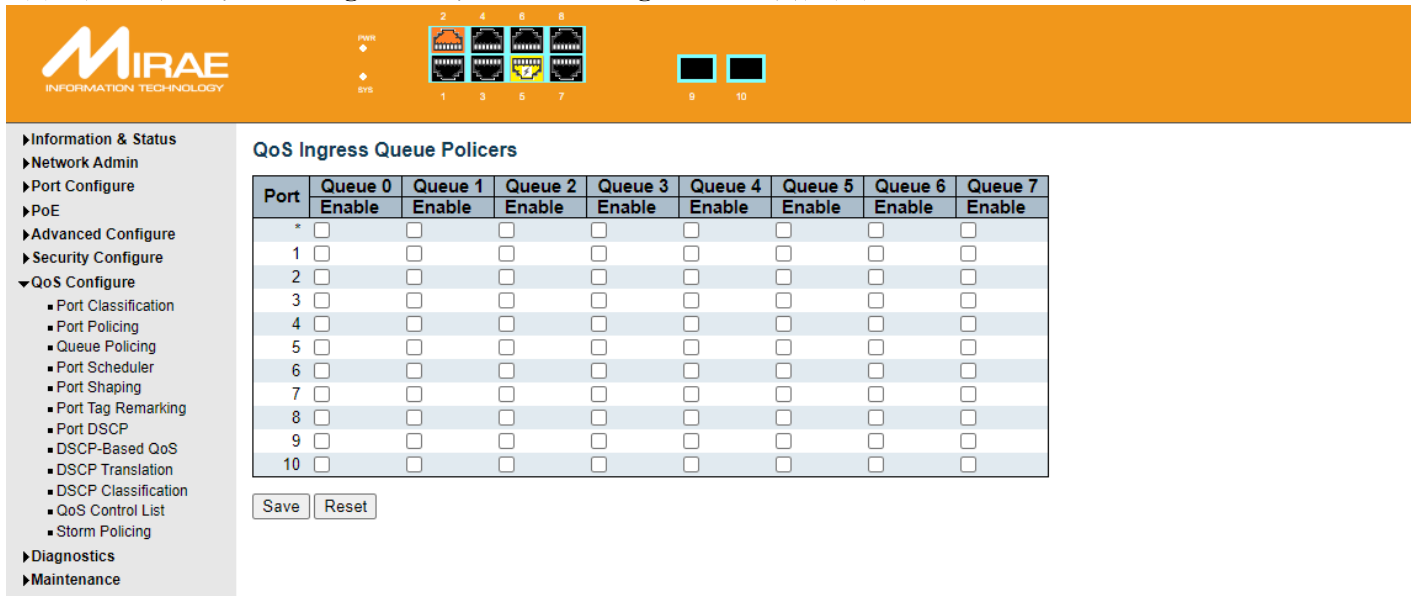
구성 항목은 다음과 같습니다.

| 구성 항목        | 설 명   |
|--------------|---|
| Enabled      | 포트 수신 정책을 활성화 또는 비활성화합니다.   |
| Rate         | 폴리서의 비율을 제어합니다. 기본값은 500 입니다. 이 값은 "Unit"이 "kbps" 또는 "fps"인 경우 100-1,000,000 으로 제한되고 "Unit"이 "Mbps" 또는 "kfps"인 경우 1-3,300 으로 제한됩니다. |
| Unit         | 폴리서 비율의 측정 단위를 kbps, Mbps, fps 또는 kfps 로 제어합니다. 기본값은 "kbps"입니다.   |
| Flow Control | 흐름 제어가 활성화되고 포트가 흐름 제어 모드에 있으면 프레임을 버리는 대신 일시 중지 프레임이 전송됩니다.  |

“Save” 하고 작업을 마칩니다.

## 8.3 Queue Policing

다음과 같이 “QoS Configure - Queue Policing” 를 클릭합니다:



**QoS Ingress Queue Policers**

| Port | Queue 0 Enable           | Queue 1 Enable           | Queue 2 Enable           | Queue 3 Enable           | Queue 4 Enable           | Queue 5 Enable           | Queue 6 Enable           | Queue 7 Enable           |
|------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| *    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5    | <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    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 9    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 10   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Save Reset

구성 항목은 다음과 같습니다.

| 구성 항목    | 설 명       |
|----------|-----------|
| Queue0-7 | 수신 대기열 정책 |

“Save” 하고 작업을 마칩니다.

## 8.4 Port Scheduler

다음과 같이 “QoS Configure - Port Scheduler” 를 클릭합니다:

**QoS Egress Port Schedulers**

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

구성 항목은 다음과 같습니다.

| 구성 항목                      | 설 명        |
|----------------------------|------------|
| QoS Egress Port Schedulers | 송신 포트 스케줄러 |

Port “1” 을 클릭합니다.

**QoS Egress Port Scheduler and Shapers Port 1**

Scheduler Mode: Strict Priority

Queue Shaper

| Queue | Enable                   | Rate | Unit | Excess                   |
|-------|--------------------------|------|------|--------------------------|
| Q7    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| Q6    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| Q5    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| Q4    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| Q3    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| Q2    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| Q1    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |
| Q0    | <input type="checkbox"/> | 500  | kbps | <input type="checkbox"/> |

Port Shaper

| Enable                   | Rate | Unit | Burst | Unit |
|--------------------------|------|------|-------|------|
| <input type="checkbox"/> | 500  | kbps | 12288 | Byte |

Save Reset Back

“Save” 하고 완료합니다.

## 8.5 Port Shaping

다음과 같이 “QoS Configure - Port Shaping” 를 클릭합니다:

**QoS Egress Port Shapers**

| Port | Shapers |    |    |    |    |    |    |    | Port |
|------|---------|----|----|----|----|----|----|----|------|
|      | Q0      | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 |      |
| 1    | -       | -  | -  | -  | -  | -  | -  | -  | -    |
| 2    | -       | -  | -  | -  | -  | -  | -  | -  | -    |
| 3    | -       | -  | -  | -  | -  | -  | -  | -  | -    |
| 4    | -       | -  | -  | -  | -  | -  | -  | -  | -    |
| 5    | -       | -  | -  | -  | -  | -  | -  | -  | -    |
| 6    | -       | -  | -  | -  | -  | -  | -  | -  | -    |
| 7    | -       | -  | -  | -  | -  | -  | -  | -  | -    |
| 8    | -       | -  | -  | -  | -  | -  | -  | -  | -    |
| 9    | -       | -  | -  | -  | -  | -  | -  | -  | -    |
| 10   | -       | -  | -  | -  | -  | -  | -  | -  | -    |

구성 항목은 다음과 같습니다.

| 구성 항목          | 설 명                            |
|----------------|--------------------------------|
| Scheduler Mode | 정적 및 WRR 에서 송신 포트 스케줄러를 선택하십시오 |

“Save” 하고 완료합니다.

## 8.6 Port Tag Remarking

다음과 같이 “QoS Configure - Port Tag Remarking” 를 클릭합니다:

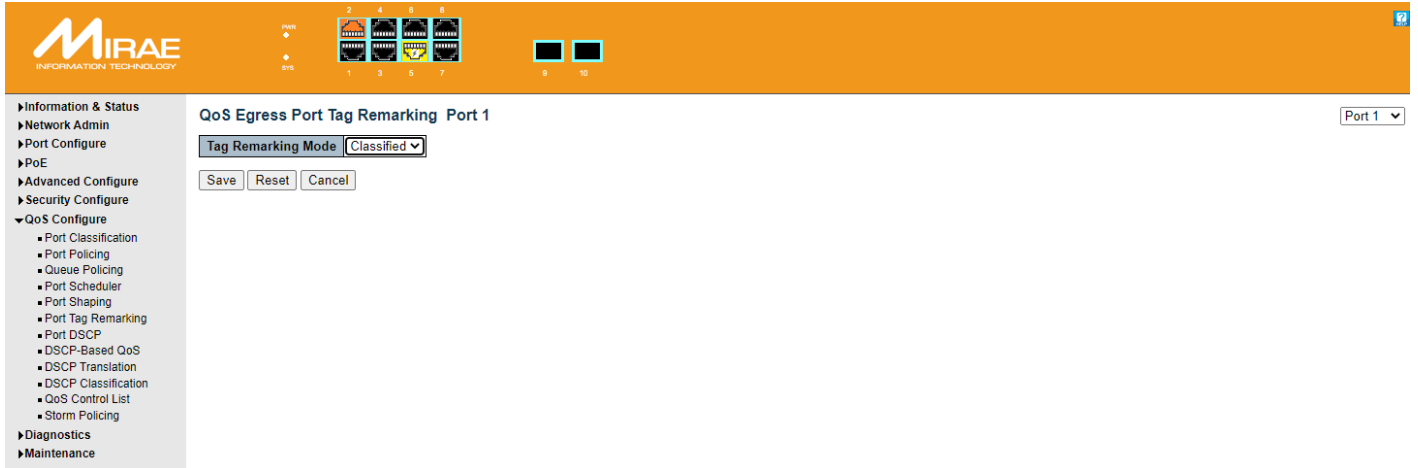
**QoS Egress Port Tag Remarking**

| Port | Mode       |
|------|------------|
| 1    | Classified |
| 2    | Classified |
| 3    | Classified |
| 4    | Classified |
| 5    | Classified |
| 6    | Classified |
| 7    | Classified |
| 8    | Classified |
| 9    | Classified |
| 10   | Classified |

구성 항목은 다음과 같습니다.

| 구성 항목                         | 설 명         |
|-------------------------------|-------------|
| QoS Egress Port Tag Remarking | 송신 포트 태그 설명 |

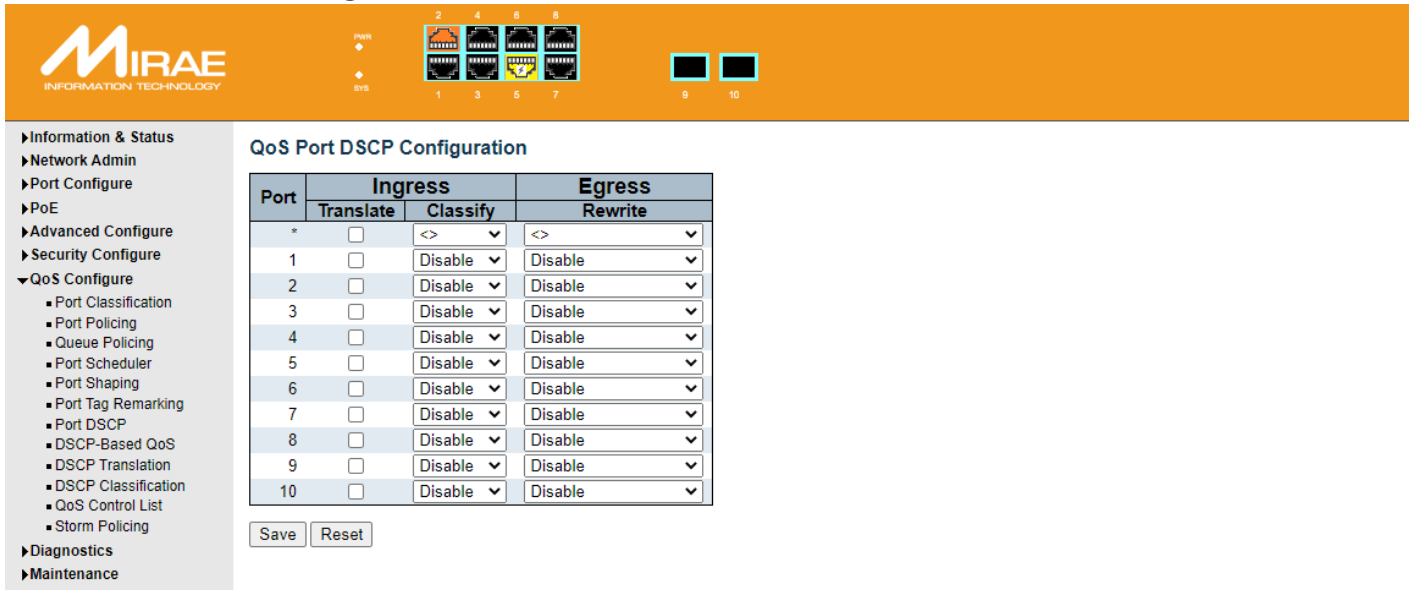
Port “1” 을 클릭합니다.



“Save” 하고 완료합니다.

## 8.7 Port DSCP

다음과 같이 “QoS Configure - Port DSCP” 를 클릭합니다:



구성 항목은 다음과 같습니다.

| 구성 항목                       | 설 명       |
|-----------------------------|-----------|
| QoS Port DSCP Configuration | DSCP 재 작성 |

“Save” 하고 완료합니다.

## 8.8 DSCP-Based QoS

다음과 같이 “QoS Configure - DSCP-Based QoS” 를 클릭합니다:

**DSCP-Based QoS Ingress Classification**

| DSCP      | Trust                    | QoS Class | DPL |
|-----------|--------------------------|-----------|-----|
| *         | <input type="checkbox"/> | <>        | <>  |
| 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   |
| 10 (AF11) | <input type="checkbox"/> | 0         | 0   |
| 11        | <input type="checkbox"/> | 0         | 0   |
| 12 (AF12) | <input type="checkbox"/> | 0         | 0   |
| 13        | <input type="checkbox"/> | 0         | 0   |

구성 항목은 다음과 같습니다.

| 구성 항목                                 | 설 명             |
|---------------------------------------|-----------------|
| DSCP-Based QoS Ingress Classification | 신뢰할 수있는 DSCP 선택 |

## 8.9 DSCP Translation

다음과 같이 “QoS Configure - DSCP Translation” 를 클릭합니다:

**DSCP Translation**

| DSCP      | Ingress   |                          | Egress    |           |
|-----------|-----------|--------------------------|-----------|-----------|
|           | Translate | Classify                 | Remap DP0 | Remap DP1 |
| *         | <>        | <input type="checkbox"/> | <>        | <>        |
| 0 (BE)    | 0 (BE)    | <input type="checkbox"/> | 0 (BE)    | 0 (BE)    |
| 1         | 1         | <input type="checkbox"/> | 1         | 1         |
| 2         | 2         | <input type="checkbox"/> | 2         | 2         |
| 3         | 3         | <input type="checkbox"/> | 3         | 3         |
| 4         | 4         | <input type="checkbox"/> | 4         | 4         |
| 5         | 5         | <input type="checkbox"/> | 5         | 5         |
| 6         | 6         | <input type="checkbox"/> | 6         | 6         |
| 7         | 7         | <input type="checkbox"/> | 7         | 7         |
| 8 (CS1)   | 8 (CS1)   | <input type="checkbox"/> | 8 (CS1)   | 8 (CS1)   |
| 9         | 9         | <input type="checkbox"/> | 9         | 9         |
| 10 (AF11) | 10 (AF11) | <input type="checkbox"/> | 10 (AF11) | 10 (AF11) |
| 11        | 11        | <input type="checkbox"/> | 11        | 11        |
| 12 (AF12) | 12 (AF12) | <input type="checkbox"/> | 12 (AF12) | 12 (AF12) |
| 13        | 13        | <input type="checkbox"/> | 13        | 13        |
| 14 (AF13) | 14 (AF13) | <input type="checkbox"/> | 14 (AF13) | 14 (AF13) |
| 15        | 15        | <input type="checkbox"/> | 15        | 15        |
| 16 (CS2)  | 16 (CS2)  | <input type="checkbox"/> | 16 (CS2)  | 16 (CS2)  |
| 17        | 17        | <input type="checkbox"/> | 17        | 17        |

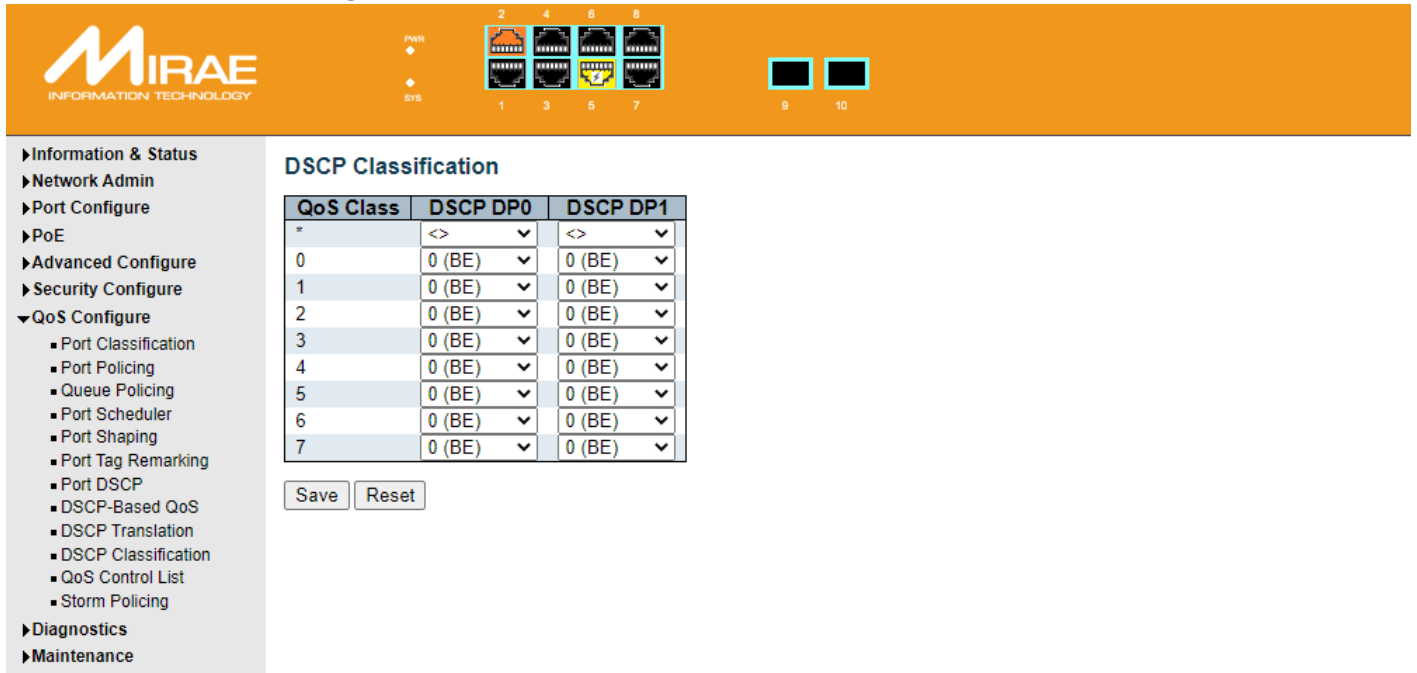
구성 항목은 다음과 같습니다

| 구성 항목            | 설 명     |
|------------------|---------|
| DSCP Translation | DSCP 번역 |

“Save” 하고 완료합니다.

## 8.10 DSCP Classification

다음과 같이 “QoS Configuration - DSCP Classification” 를 클릭합니다:



**DSCP Classification**

| QoS Class | DSCP DP0 | DSCP DP1 |
|-----------|----------|----------|
| *         | <>       | <>       |
| 0         | 0 (BE)   | 0 (BE)   |
| 1         | 0 (BE)   | 0 (BE)   |
| 2         | 0 (BE)   | 0 (BE)   |
| 3         | 0 (BE)   | 0 (BE)   |
| 4         | 0 (BE)   | 0 (BE)   |
| 5         | 0 (BE)   | 0 (BE)   |
| 6         | 0 (BE)   | 0 (BE)   |
| 7         | 0 (BE)   | 0 (BE)   |

Save Reset

구성 항목은 다음과 같습니다.

| 구성 항목               | 설 명     |
|---------------------|---------|
| DSCP Classification | DSCP 분류 |

“Save” 하고 완료합니다.

## 8.11 QoS Control List

다음과 같이 “QoS Configure - QoS Control List” 를 클릭합니다:

구성 항목은 다음과 같습니다.

| 구성 항목 | 설 명     |
|-------|---------|
| QCL   | QoS ACL |

“+” 를 클릭합니다

“ Save ” 하고 완료합니다.

## 8.12 Storm Policing

다음과 같이 “QoS Configure - Storm Policing” 를 클릭합니다:

구성 항목은 다음과 같습니다.



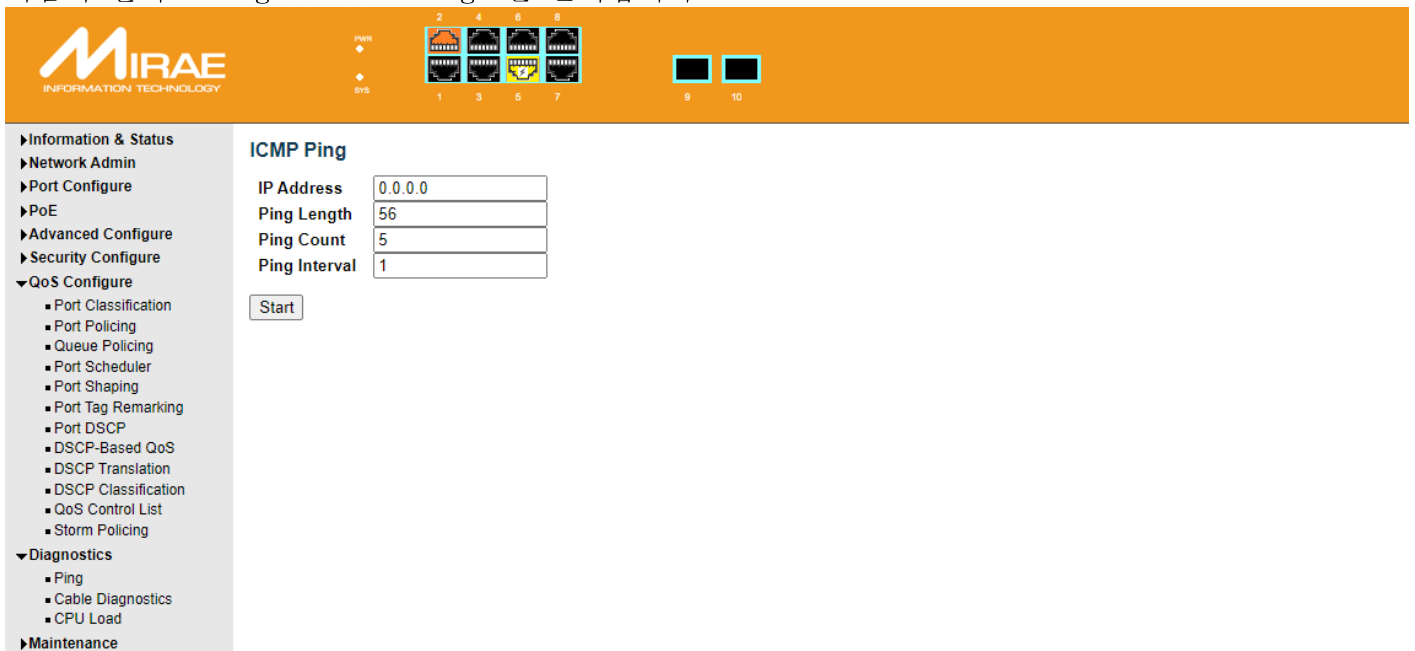
| 구성 항목      | 설 명   |
|------------|---|
| Frame Type | 스위치는 알 수 없는 유니 캐스트, 알 수 없는 멀티 캐스트 및 브로드 캐스트를 지원합니다  |
| Enabled    | Storm 정책 활성화 또는 비활성화  |
| Rate       | 속도 단위는 초당 패킷 (pps)입니다. 유효한 값은 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K 또는 1,024K 입니다. |

“Save” 하고 완료합니다.

## 9 Diagnostics

### 9.1 Ping

대상 노드는 Ping 에서 지정된 IP 주소로 보낸 ICMP Echo 패킷에 응답합니다.  
다음과 같이 “Diagnostics - Ping” 을 클릭합니다:



다음은 구성하거나 표시 할 수있는 필드입니다:

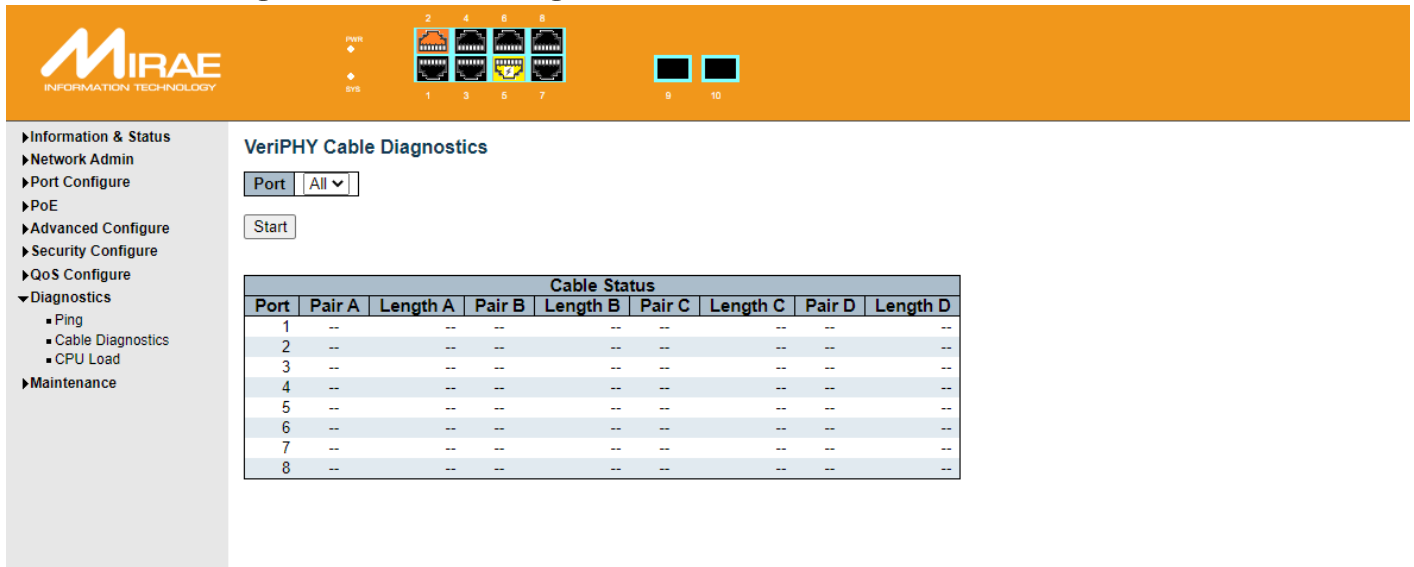
| 구성 항목         | 설 명   |
|---------------|---|
| IP Address    | ping 할 IP 주소를 입력하십시오.                       |
| Ping Count    | IPv4 또는 IPv6 주소를 ping 할 횟수 (1 ~ 60)를 입력합니다. |
| Ping Length   | 1-1,452 범위의 숫자를 입력하십시오 (기본값은 56).           |
| Ping Interval | ping 간격 입력                                  |

ping 테스트를 위해 “Start” 를 클릭하십시오.

## 9.2 Cable Diagnostics

10 / 100 / 1,000 BASE-T 전기 인터페이스를 검사합니다.

다음과 같이 “Diagnostics - Cable Diagnostics” 을 클릭합니다:

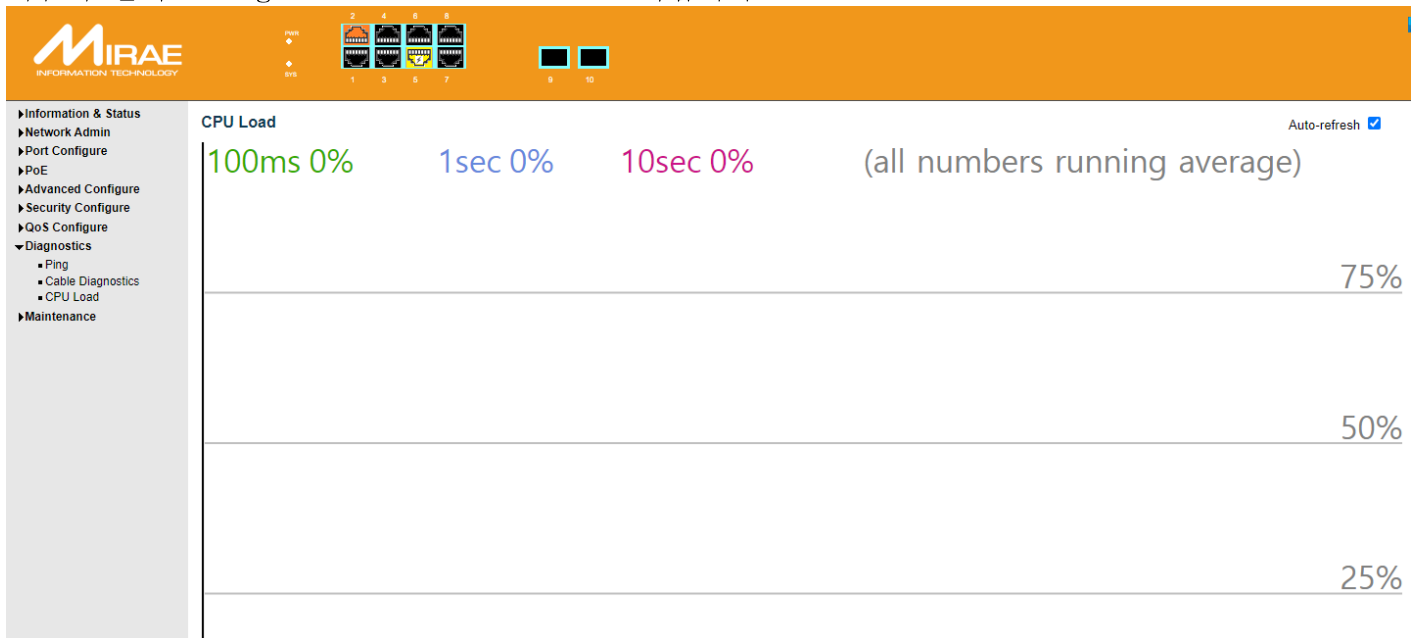


"케이블 진단"테스트를 위해 “Start” 을 클릭합니다.

## 9.3 CPU Load

사용자의 CPU 부하를 백분율로 표시하고 시간 간격으로 평균을 계산합니다.

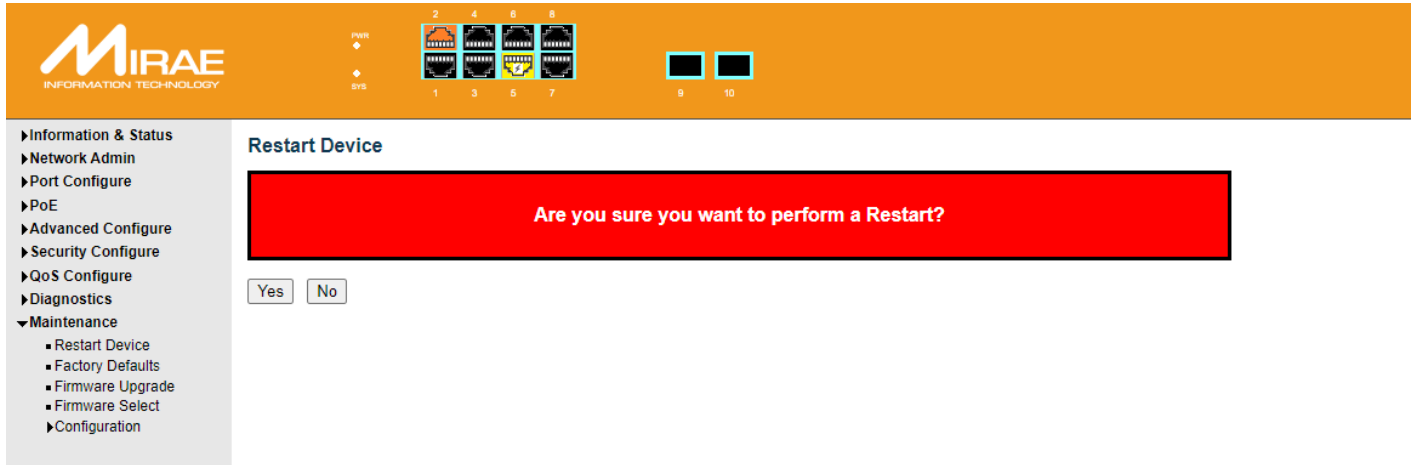
다음과 같이 “Diagnostics - CPU Load” 를 클릭합니다:



# 10 Maintenance

## 10.1 Restart Device

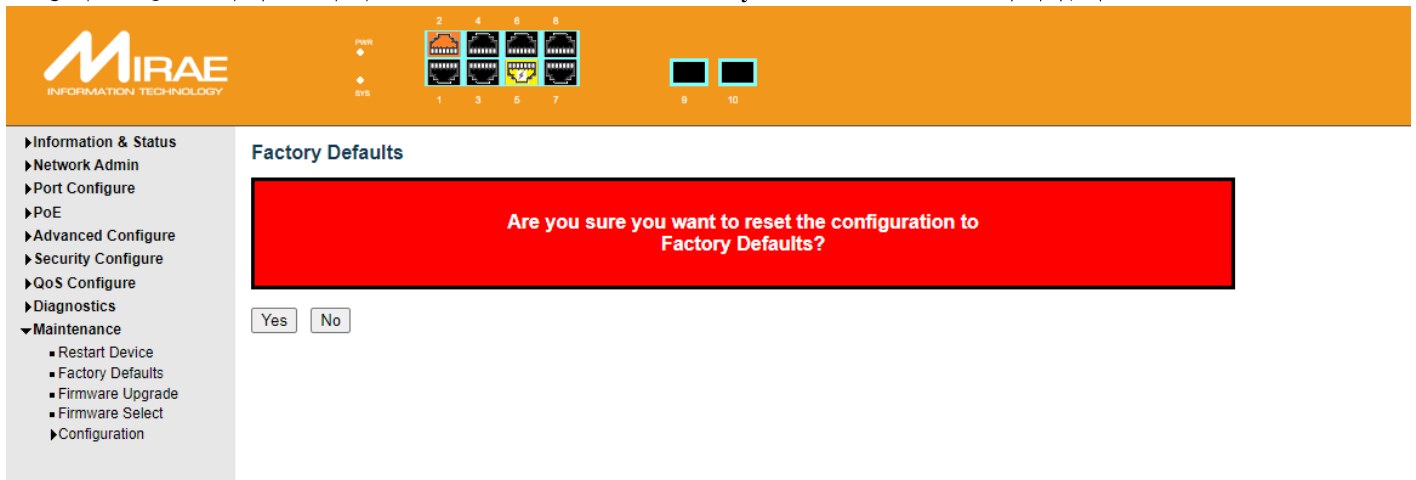
다시 시작하려면 “Maintenance - Restart Device” 를 클릭하십시오.



“Yes” 를 클릭하십시오.

## 10.2 Factory Defaults

설정의 공장 초기화를 하려면 “Maintenance - Factory Defaults” 를 클릭하십시오.



“Yes” 를 클릭하십시오.

## 10.3 Firmware Upgrade

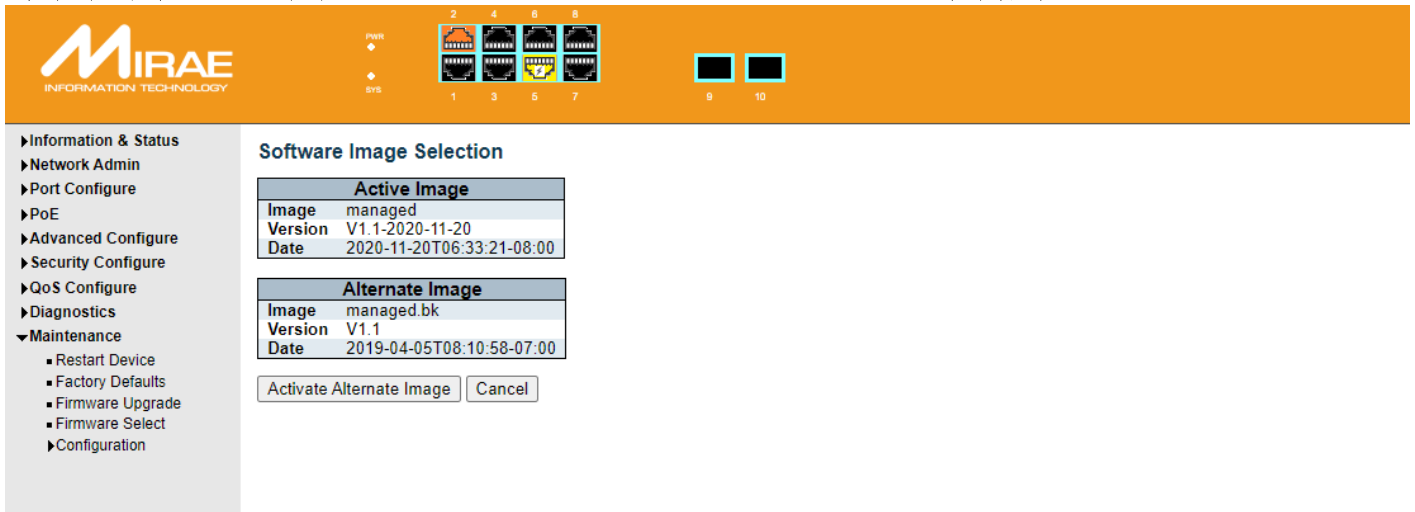
업그레이드하려면 “Maintenance - Firmware Upgrade” 를 클릭하십시오.



“Browse” 를 클릭하여 업그레이드 할 펌웨어 문서를 선택합니다.  
펌웨어 업그레이드를 위해 “Upload” 를 클릭하십시오.

## 10.4 Firmware Select

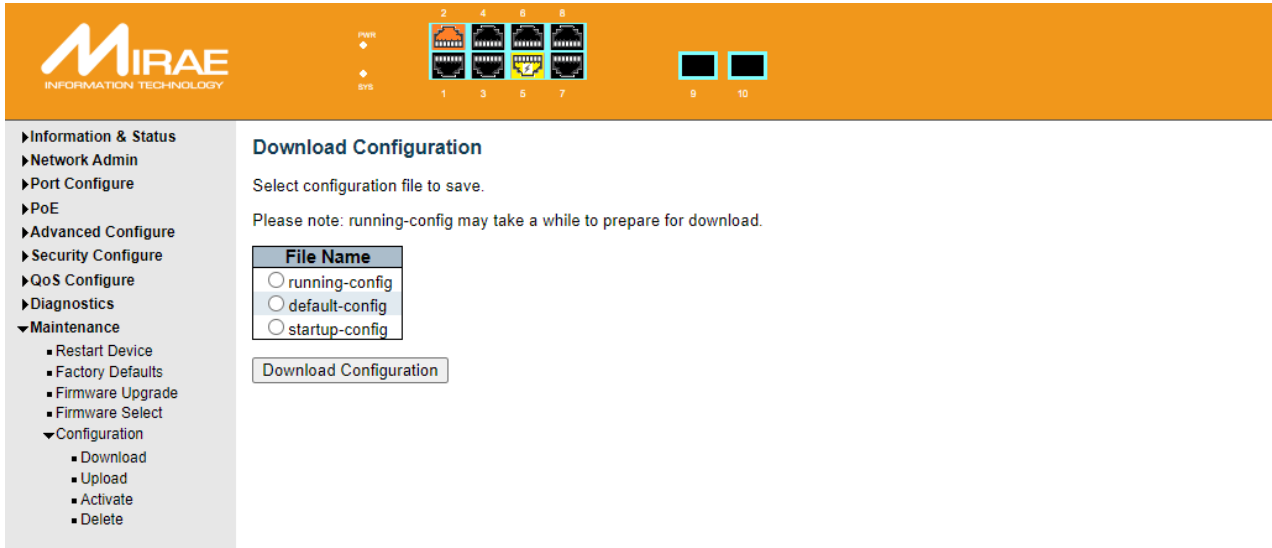
예비 펌웨어를 전환하려면 “Maintenance - Firmware Select” 을 클릭하십시오.



펌웨어를 전환하려면 “Activate Alternate Image” 를 클릭하십시오.

## 10.5 Configuration

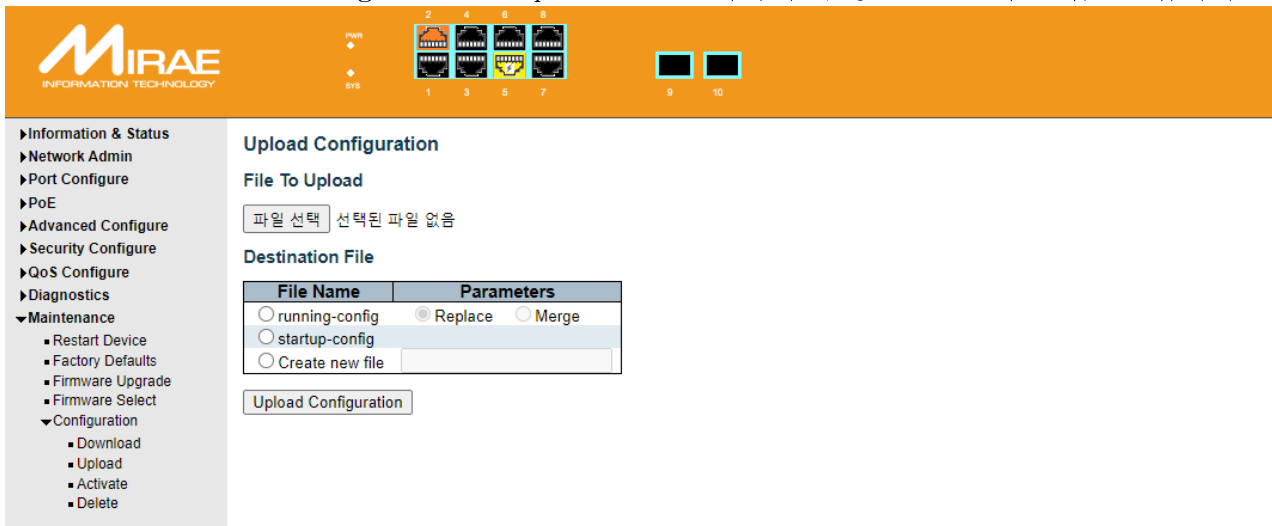
1. “Maintenance - Configuration - Download” 를 클릭하여 구성 관련 문서를 다운로드합니다.



The screenshot shows the MIRAE network switch web interface. The top navigation bar includes a logo and status indicators. The left sidebar lists various configuration options, with 'Maintenance' expanded to show 'Configuration' options. The main content area is titled 'Download Configuration' and contains a 'File Name' section with three radio buttons: 'running-config', 'default-config', and 'startup-config'. Below this is a 'Download Configuration' button.

“Download Configuration” 를 클릭합니다.

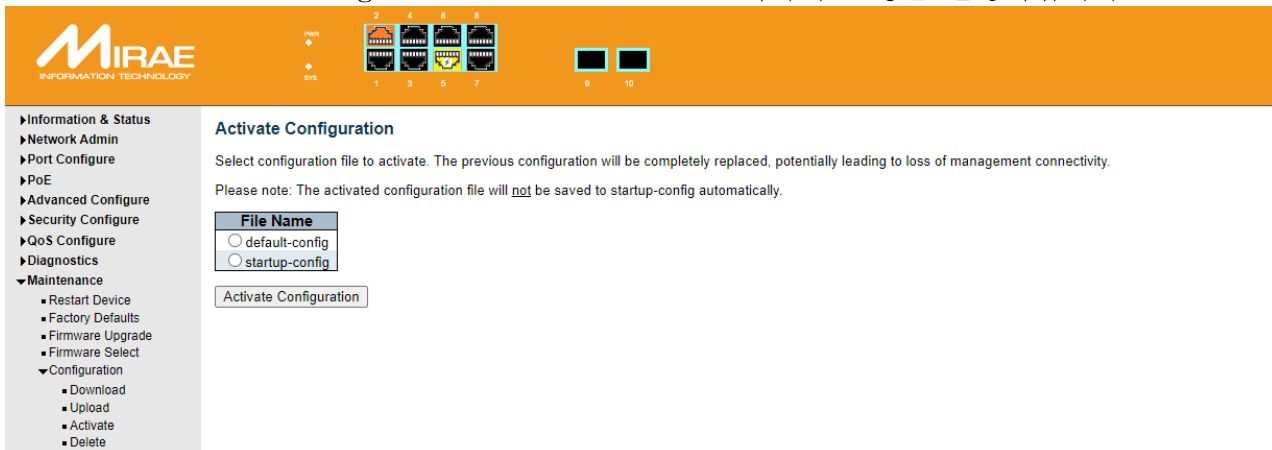
2. “Maintenance - Configuration - Upload” 를 클릭하여 구성 관련 문서를 업로드합니다.



The screenshot shows the MIRAE network switch web interface. The top navigation bar includes a logo and status indicators. The left sidebar lists various configuration options, with 'Maintenance' expanded to show 'Configuration' options. The main content area is titled 'Upload Configuration' and contains a 'File To Upload' section with a '파일 선택' button and a '선택된 파일 없음' message. Below this is a 'Destination File' section with a table containing 'File Name' and 'Parameters' columns. The table has three rows: 'running-config' with 'Replace' and 'Merge' options, 'startup-config', and 'Create new file'. Below the table is an 'Upload Configuration' button.

“Upload” 를 클릭합니다.

3. “Maintenance - Configuration - Activate” 를 클릭하여 설정을 활성화합니다.



The screenshot shows the MIRAE network switch web interface. The top navigation bar includes a logo and status indicators. The left sidebar lists various configuration options, with 'Maintenance' expanded to show 'Configuration' options. The main content area is titled 'Activate Configuration' and contains a 'File Name' section with two radio buttons: 'default-config' and 'startup-config'. Below this is an 'Activate Configuration' button.

“Activate Configuration” 를 클릭합니다.

4. “Maintenance - Configuration - Delete” 를 클릭하여 구성 관련 문서를 삭제합니다.



“Delete Configuration File” 를 클릭합니다.