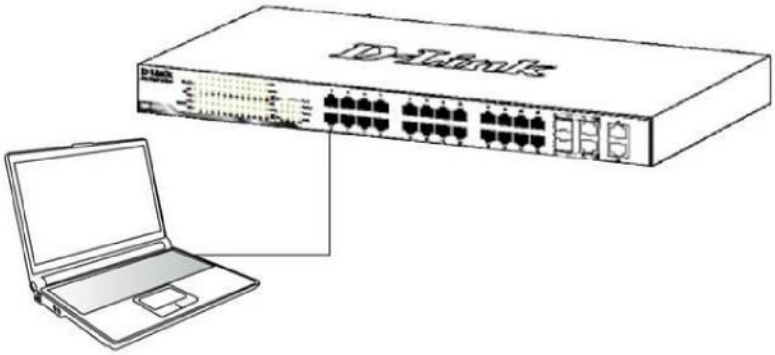
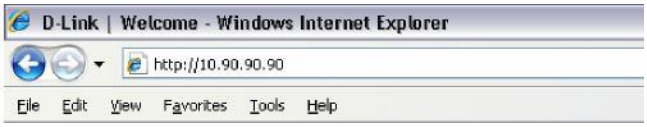
DGS-1210-28P
Web Smart Switch
사용자 매뉴얼
V2.01

Smart Wizard 설정



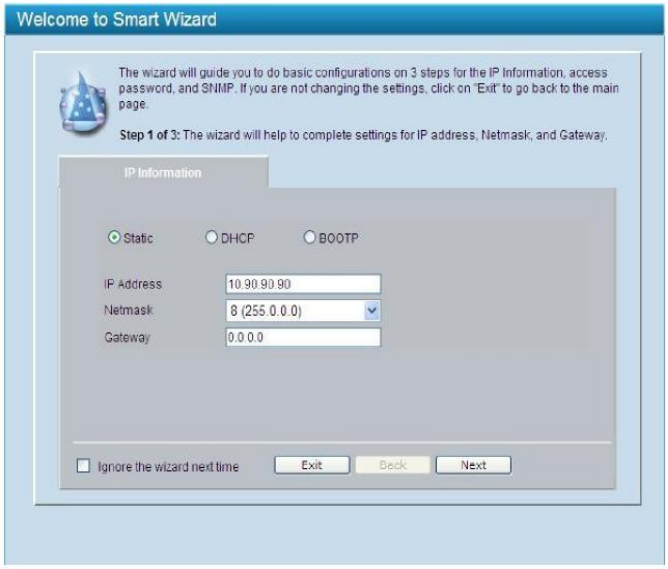
우선 컴퓨터와 DGS-1210-28P를 바로 인터넷 선으로 연결합니다.



그 다음 인터넷 창을 열고 http://10.90.90.90 을 입력해서 스위치 화면에 접속합니다.

1) **로그인: 초기 패스워드는 없거나 admin 입니다.** (Default: admin)

2) **관리 IP 설정**: 관리용(Management) IP 설정(Default: 10.90.90.90/8)

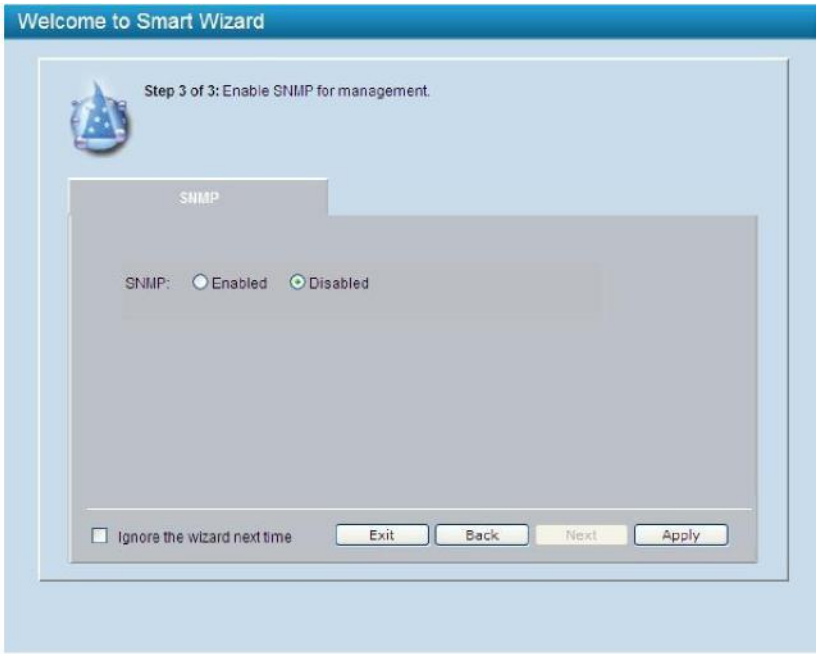


(그림 1) 로그인 IP 설정 화면

3) 관리자 암호 설정 : 스위치 로그인 시 암호를 설정합니다.

(그림 2) 로그인 암호 설정 화면

4) **SNMP Setting**: SNMP 활성화 설정 (Default: Disabled)



(그림 3) Smart Wizard SNMP 설정 화면

주의1) IP 변경 시 현재 연결 세션이 끊어지게 되므로 새로 입력한 IP 주소로 접속을 하셔야 합니다.

주의2) 해당 설정 화면으로 들어가 지지 않거나 암호를 분실시 스위치 앞 부분의 리셋 버튼을 15초 가량 눌러서 초기화 후 재설정 하시기 바랍니다.

Save 설정

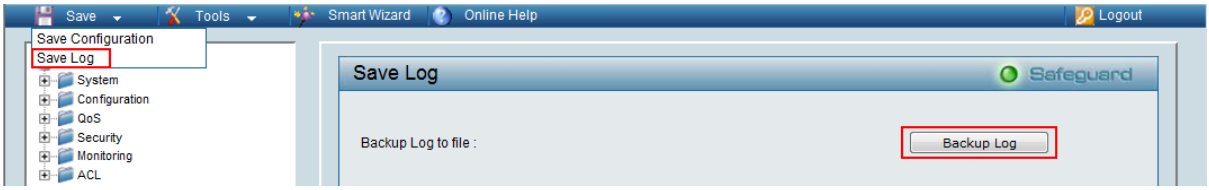
1) Save Configuration

(그림 4) Configuration save 화면

- 현재 스위치의 구성(Configuration) 정보를 저장 할 수 있습니다.

주의) 저장하지 않으면 스위치 재부팅시 이전 설정으로 돌아갑니다.

2) Save Log

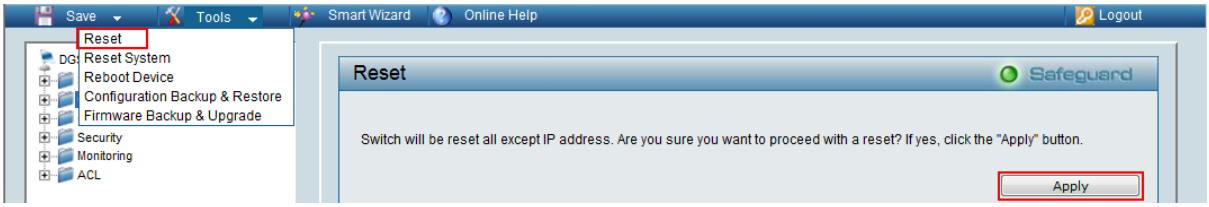


(그림 5) Configuration log 화면

- 현재 스위치의 로그 정보를 저장 할 수 있습니다.

Tools 설정

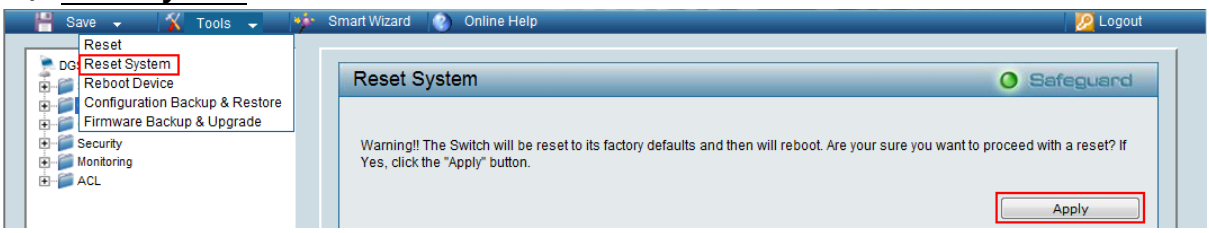
1) Reset



(그림 6) Switch reset 화면

- Reset을 하시면 IP 주소를 제외한 모든 설정 값이 초기화 됩니다.

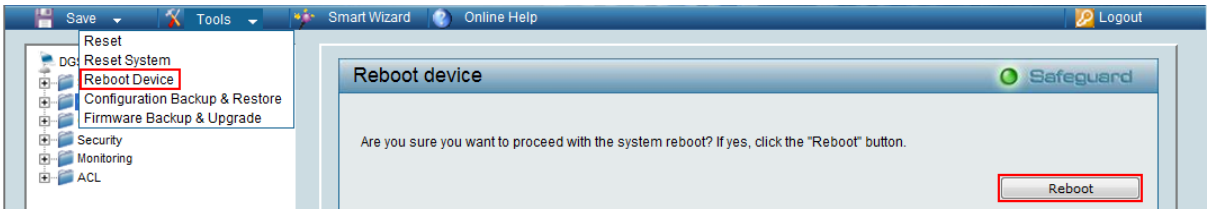
2) Reset System



(그림 7) Switch 공장도 초기화 화면

- Reset System을 실행 하시면 모든 설정 값이 공장 기본값으로 초기화 됩니다.

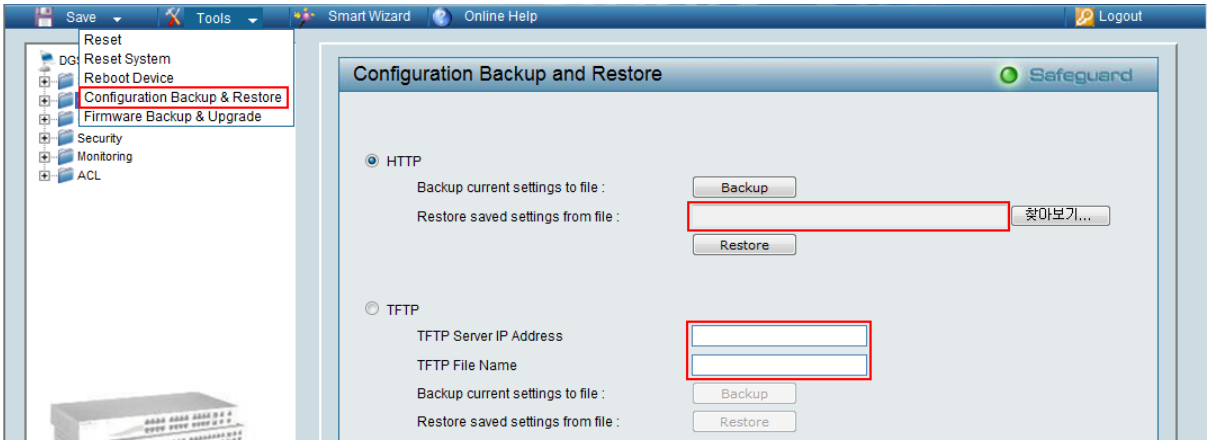
3) Reboot Device



(그림 8) Switch 재시작 화면

- Reboot Device 실행 시 스위치가 재 시작 됩니다.

4) Configuration Backup and Restore

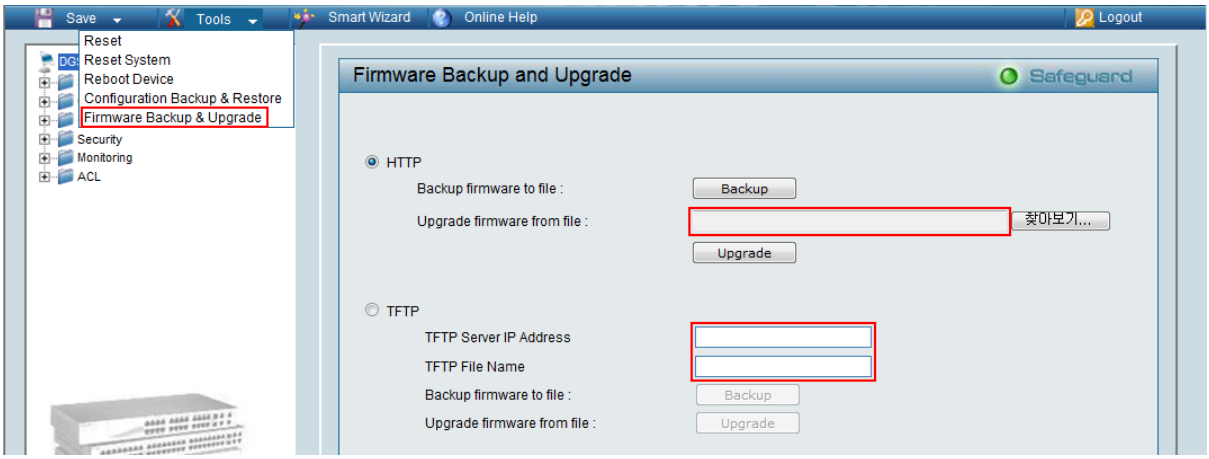


(그림 9) Switch 설정 백업 및 복원 화면

- 스위치의 현재 설정 값을 백업하거나 저장된 설정 값을 불러올 때 사용 합니다.
HTTP나 TFTP 중 원하는 방식을 선택하여 백업이나 불러오기를 할 수 있습니다.

주의) 설정 값 불러오기를 하면 현재 설정 값은 모두 사라지게 되며 TFTP 방식으로 백업 및 불러오기를 할 시 유효한 TFTP 서버 주소 와 파일 경로여야 합니다.

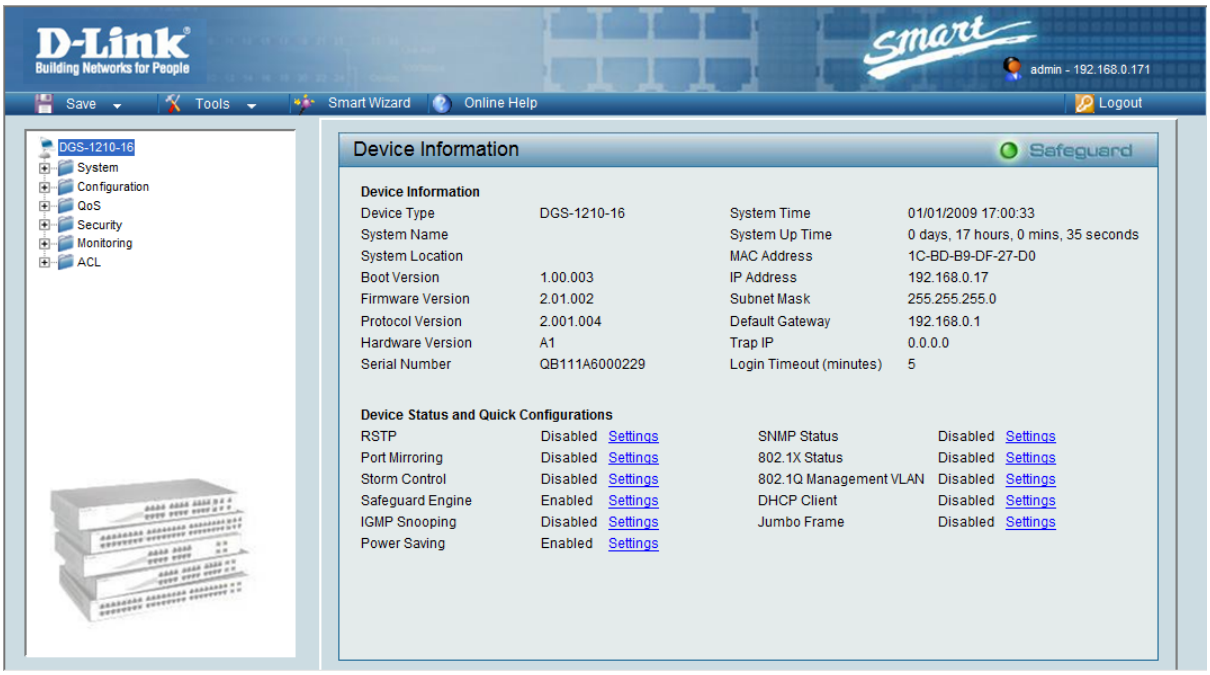
5) Firmware Backup & Upgrade



(그림 10) Switch 펌웨어 백업 및 업그레이드 화면

- 스위치의 현재 Firmware를 백업하거나 업그레이드 시 사용 됩니다.
HTTP나 TFTP 중 원하는 방식을 선택하여 백업이나 업그레이드를 할 수 있습니다.

Device Information

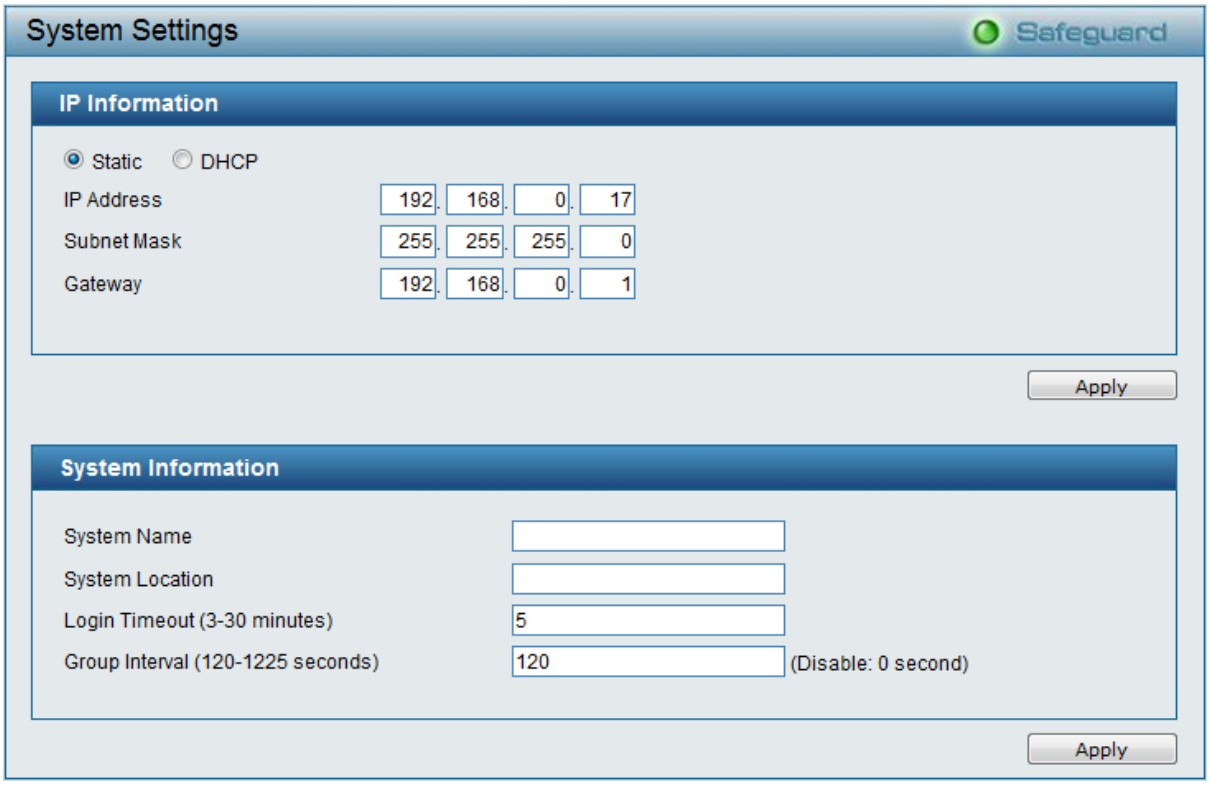


(그림 11) Switch 정보 화면

- 스위치에 접속 시 보이는 초기화면 입니다. 장비의 모델, 펌웨어, S/N 및 기본 정보들을 확인 할 수 있습니다.

Device Status and Quick Configuration의 링크를 이용하여 해당 설정 창으로 바로 이동할 수 있습니다.

System>>System Setting



(그림 12) Switch 시스템 설정 화면

- 스위치 관리용 IP를 고정(Static) 또는 유동(DHCP)으로 설정 할 수 있으며 스위치 System 정보를 입력하여 관리 프로그램(**D-Link WebSmart Console**)에서 제어 및 확인 가능합니다.

IP Information: 스위치의 기본 IP Address 10.90.90.90 / Subnet mask 255.0.0.0 / Gateway 0.0.0.0

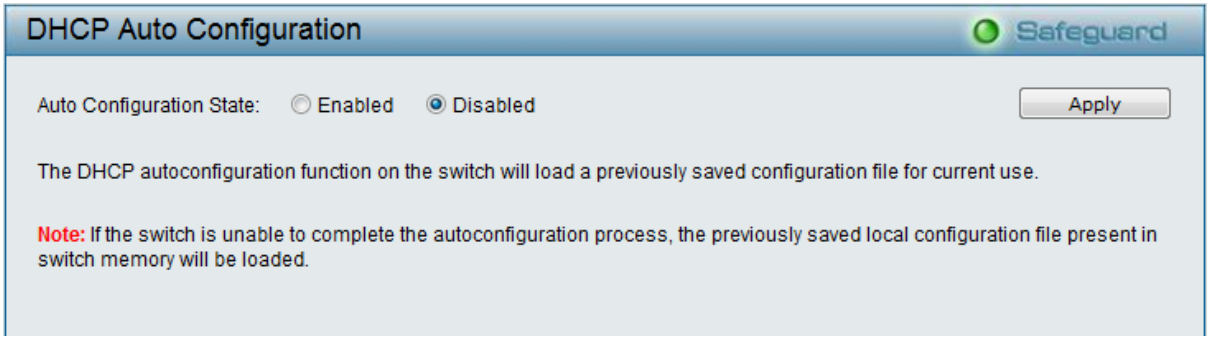
System Information: System Name, Location을 설정 합니다.

Login Timeout(3-30 minutes): 웹 페이지 접속 후 지정된 시간만큼 동작이 없으면 자동으로 로그아웃이 되는 시간 입니다. 분 단위로 3분부터 30분까지 설정이 가능 합니다.

Group Interval(120-1255 seconds): 스위치 시스템 정보를 **D-Link WebSmart Console** 프로그램으로 전송하는 주기 입니다. 초 단위며 0 설정 시는 정보를 보내지 않습니다.

주의) 스위치 관리 IP 방식을 DHCP로 사용 할 경우 상단 장비에서 자동으로 할당 받은 IP가 스위치의 관리 IP로 사용되며 이 경우 DHCP Release 시간에 따라 스위치 관리 IP가 변경될 수도 있음으로 특별한 경우가 아니라면 DHCP 방식 사용을 권장하지 않습니다.

System>>DHCP Auto Configuration



(그림 13) Switch DHCP 자동 설정 화면

- **DHCP Auto Configuration** 기능이 활성화 되면 스위치는 DHCP Client로 동작하게 되며 다음 부팅 시 TFTP 서버에서 자동으로 설정 파일을 가져옵니다.

이를 위해, DHCP 서버는 DHCP 응답 Packet에 TFTP 서버 IP 주소 및 구성 파일 이름 정보를 제공 해야 하며 TFTP 서버가 구동되어 있어야 합니다.

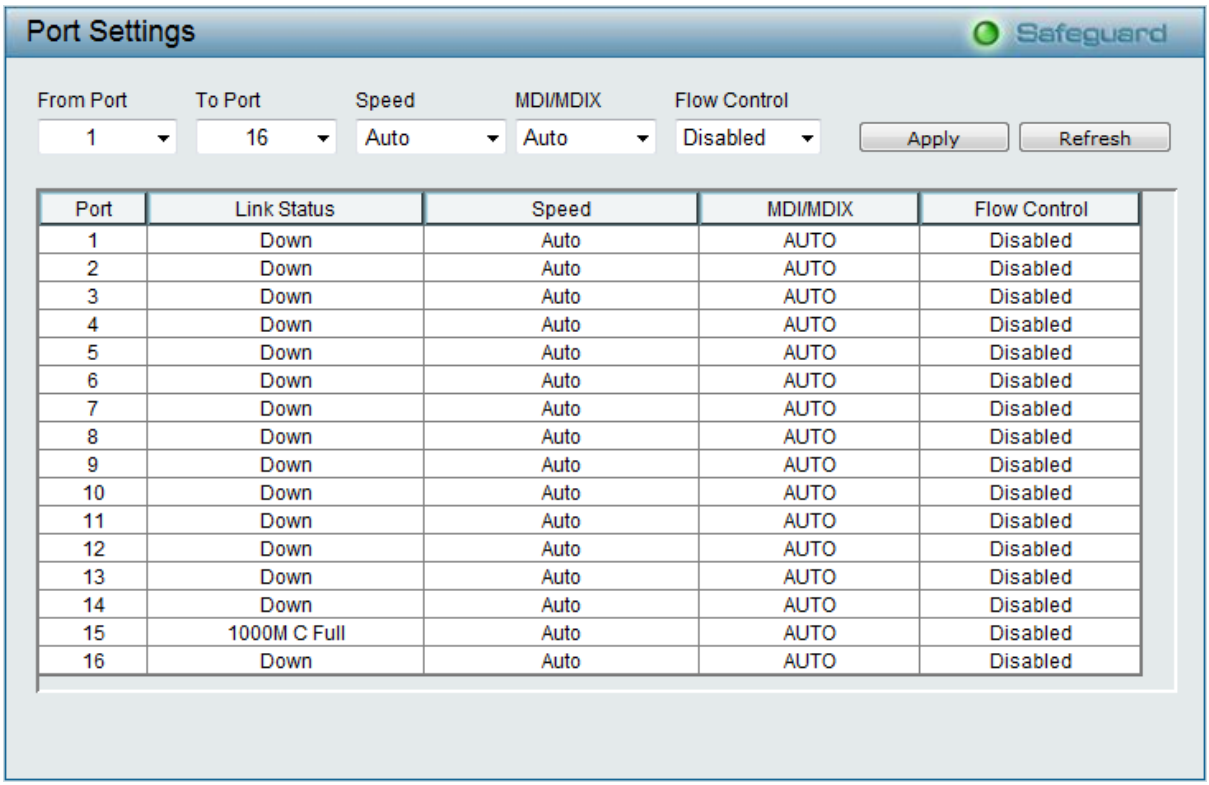
스위치로부터 요청을 받으면 기본 Directory 내에 필요한 구성 파일들을 저장해 놓아야 합니다.

System>>Trap Setting

(그림 14) Switch Trap 설정 화면

- **SmartConsole**이 설치되어 있는 트랩 서버에 장비 재 시작 및 인가되지 않은 사용자의 접속, Fiber, UTP 포트의 Event log, POE Event log 등 전송하려는 로그 상황을 직접 선택하여 설정 할 수 있습니다.

System>>Port Setting



Port	Link Status	Speed	MDI/MDIX	Flow Control
1	Down	Auto	AUTO	Disabled
2	Down	Auto	AUTO	Disabled
3	Down	Auto	AUTO	Disabled
4	Down	Auto	AUTO	Disabled
5	Down	Auto	AUTO	Disabled
6	Down	Auto	AUTO	Disabled
7	Down	Auto	AUTO	Disabled
8	Down	Auto	AUTO	Disabled
9	Down	Auto	AUTO	Disabled
10	Down	Auto	AUTO	Disabled
11	Down	Auto	AUTO	Disabled
12	Down	Auto	AUTO	Disabled
13	Down	Auto	AUTO	Disabled
14	Down	Auto	AUTO	Disabled
15	1000M C Full	Auto	AUTO	Disabled
16	Down	Auto	AUTO	Disabled

(그림 16) Switch Port 설정 화면

- 포트의 속도/케이블 타입/흐름 제어를 설정 할 수 있습니다.

From Port: 시작 포트를 선택 합니다.

To Port: 마지막 포트를 선택 합니다.

Speed: Speed 및 Duplex을 수동으로 선택 합니다. 기본값은 Auto로 설정되어 있으며 선

택 시 Disable, 10M Half/Full, 100M Half/Full, 1000M Full 중 설정이 가능 합니다.

MDI(Media Dependent Interface) / MDIX(Media Dependent Interface Crossover): MDI는 AUTO로 구성 시 상대 인터페이스를 자동으로 감지하여 그에 맞는 인터페이스를 형태를 제공 하는 기능 입니다.

- **Flow Control**: 포트의 흐름제어를 설정 할 수 있습니다.

주의) Speed지정 시 상대편 장비의 포트(Interface)의 Speed 및 Duplex 적용상태를 확인 한 후 설정해야 합니다.

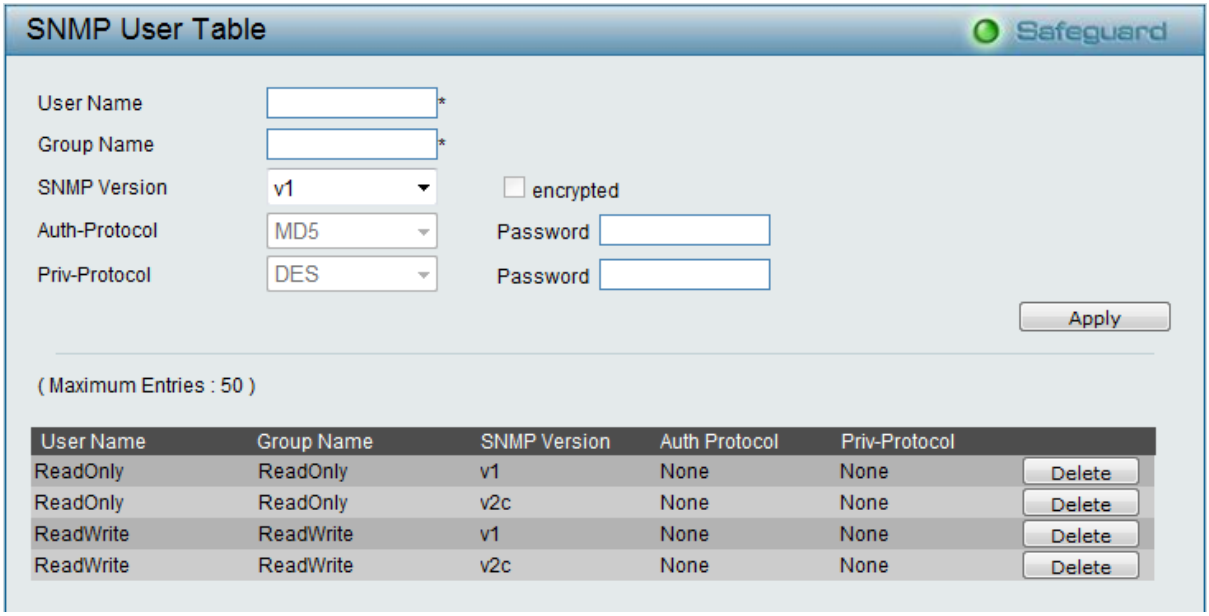
System>>SNMP Setting

1) SNMP Global State

(그림 17) SNMP 설정 화면

- SNMP 활성화 설정

2) User/Group Table



(그림 18) SNMP 사용자 설정 화면

- SNMP User Table을 생성 합니다.

User Name: SNMP 사용자 이름을 32글자 이내로 설정 합니다.

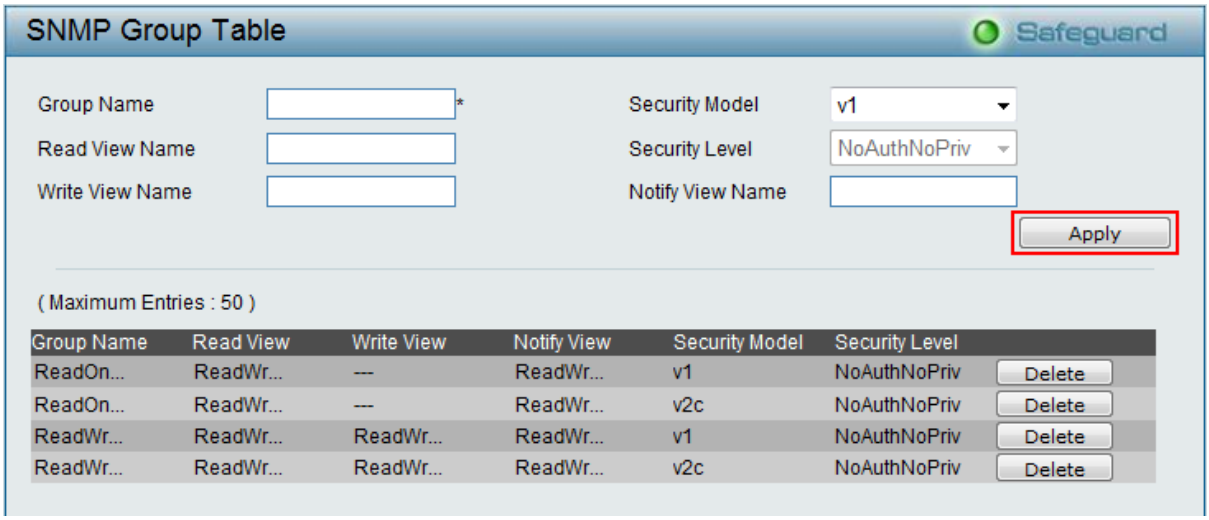
Group Name: SNMP Group 이름을 설정 합니다.

SNMP Version: SNMP 사용자에 대한 SNMP 버전을 설정 합니다.v3만 메시지 Encrypted 이 가능 합니다.

Auth-Protocol/Password: HMAC-MD5-96 또는 HMAC-SHA 프로토콜 선택 합니다.
암호는 SNMP v3 암호화를 위한 암호를 입력 합니다.

Priv-Protocol/Password: 무 인증 또는 DES 56-bit encryption을 선택 합니다.
암호는 SNMP v3 암호화를 위한 암호를 입력 합니다.

3) Group Access Table



(그림 19) SNMP 그룹 설정 화면

Group Name: SNMP 그룹 이름을 32글자 이내로 설정 합니다.

Read View Name: SNMP 읽기 권한을 부여하는 사용자의 그룹 이름을 설정 합니다.

Write View Name: SNMP 쓰기 권한을 부여하는 사용자의 그룹 이름을 설정 합니다.

Security Model: SNMPv1 / SNMPv2c / SNMPv3

Security Level

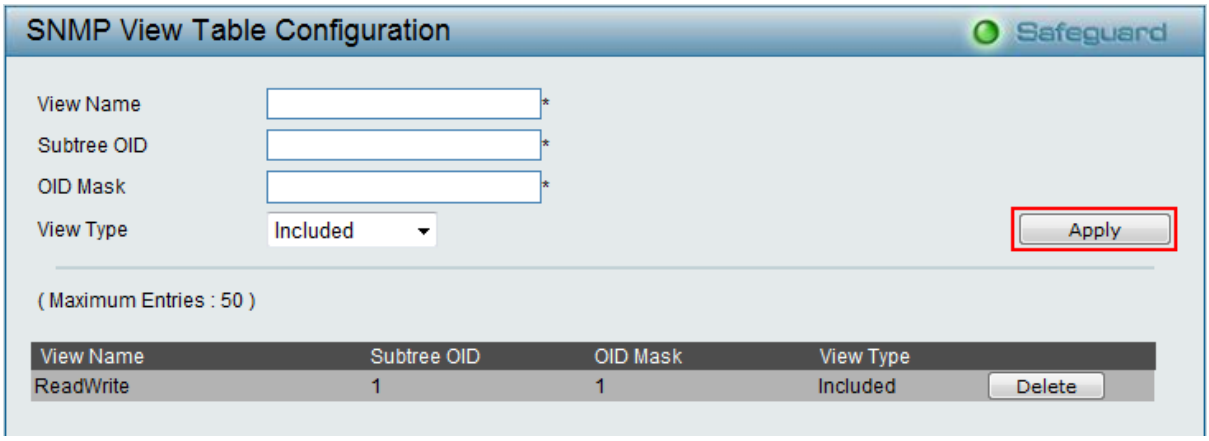
NoAuthNoPriv: 스위치와 SNMP Manager간에 Packet 전송 시 Authorization와 Encryption을 하지 않습니다.

AuthNoPriv: 스위치와 SNMP Manager 간에 Packet 전송 시 Authorization 은 시도 하지만 Encryption은 하지 않습니다.

AuthPriv: 스위치와 SNMP Manager 간에 Packet 전송 시 Authorization 와 Encryption 모두 사용 합니다.

Notify View Name: 스위치 SNMP Agent에 의해 발생되는 SNMP Trap을 수신 할 수 있는 사용자에 대한 SNMP 그룹 이름 설정 합니다.

4) SNMP View Table Configuration



(그림 20) SNMP View Table 설정 화면

View Name: View 이름을 32글자 이내로 설정 합니다.

Subtree OID: SNMP Manager로 접근을 가능하게 할 MIB Tree내 OID 값 을 지정 함

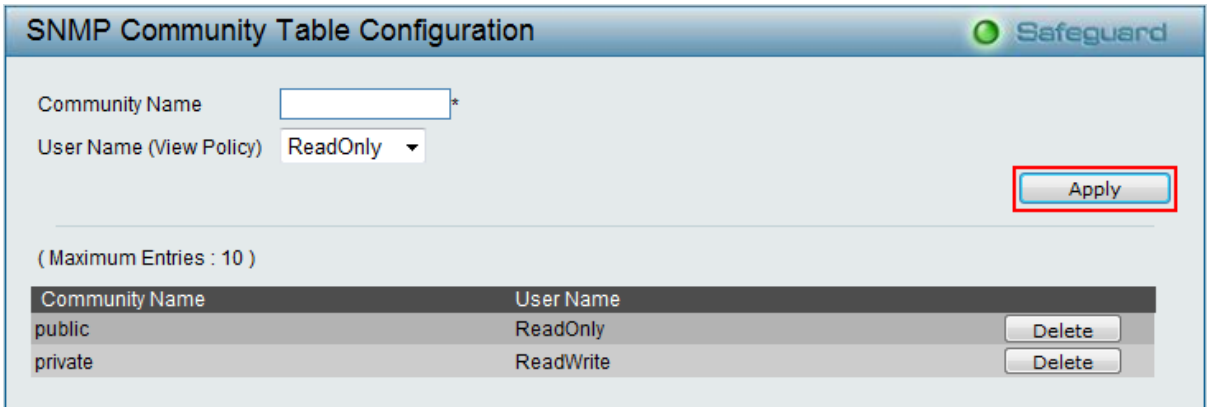
OID Mask: Subtree OID 값에 대한 Mask 값. 1은 care bit 0은 don't care bit 를 의미 함

예) OID: 1.3.6.1.2.1.1, Mask: 1.1.1.1.1.1.0 → 1.3.6.1.2.1.X 를 의미 합니다.

즉, care bit인 1은 OID 값 중 상위 서브 tree를 모두 포함 하고 있습니다.

View Type: 위에서 정의한 Configured OID 값을 SNMP Manager가 접근 시 적용여부를 선택 합니다.

5) SNMP Community Table Configuration



(그림 21) SNMP Community Table 설정 화면

Community Name: Community 이름을 설정 합니다.

User Name: SNMP Community에 접근 가능한 MIB Object의 Read/Write 또는 Read only 권한을 정의 합니다.

주의)스위치의 SNMP Agent 와 SNMP Manager 간의 Community 값은 반드시 일치해야 합니다.

6) SNMP Host Table

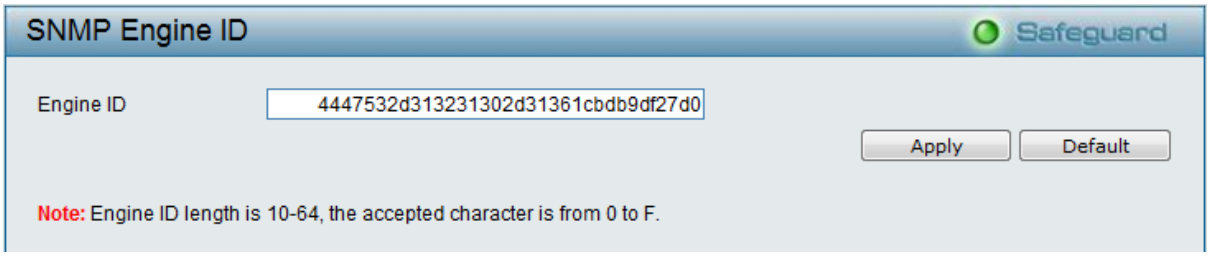
(그림 22) SNMP Host Table 설정 화면

Host IP Address: SNMP Management 호스트의 IP 주소를 설정 합니다.

SNMP Version: SNMP Management 호스트의 SNMP 버전을 설정 합니다.

Community String/SNMPv3 User Name: Community 명 또는 SNMPv3 사용자 이름 입력 합니다.

7) Engine ID



(그림 23) Engine ID 설정 화면

- SNMP Engine ID는 스위치의 SNMPv3 Engine 사용을 확인하기 위한 고유 식별 ID 입니다.

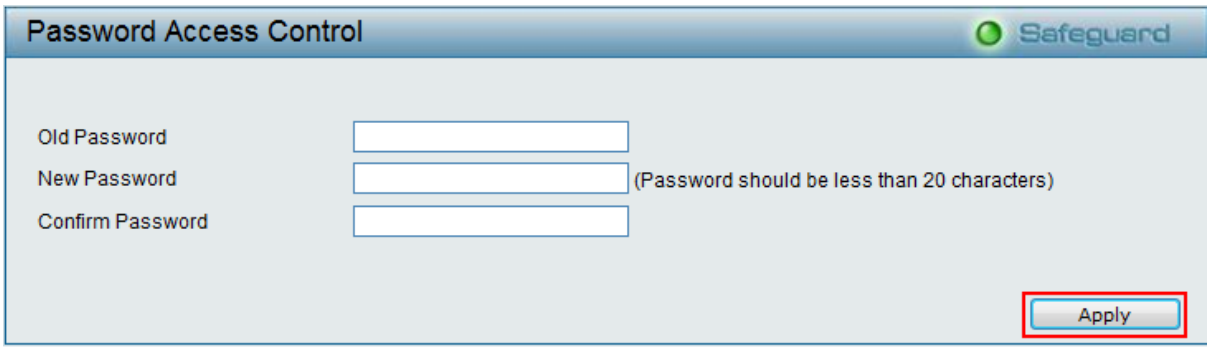
8) SNMP Trap Configuration

(그림 24) Engine ID 설정 화면

- 체크한 Trap에 대한 이벤트 발생 시 SNMP Management 호스트에 Message 전송 기능

입니다.

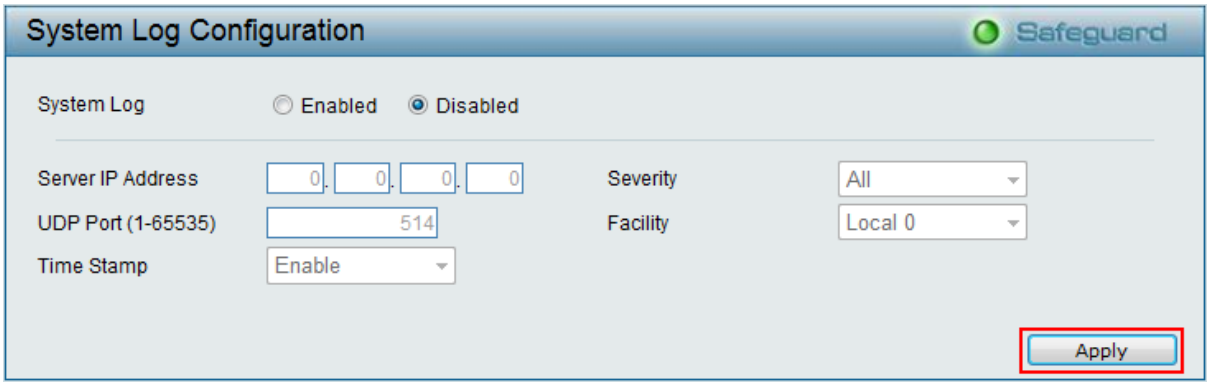
System>>Password Access Control



(그림 25) 패스워드 설정 화면

- 스위치에 접속 하기 위한 패스워드를 설정 할 수 있습니다.(20자 미만)

System>>System Log Setting



(그림 26) 시스템 로그 설정 화면

- 스위치의 로그를 저장 할 수 있는 시스템 로그 서버를 지정 할 수 있습니다.

Server IP Address: Sys Log 서버 IP를 지정 합니다.

UDP Port(1-65535): 서버로 로그를 전송할 때 사용하는 UDP 포트 번호 지정. 기본 포트는 514로 설정되어 있습니다.

Time Stamp: 로그 메시지에 시간 정보를 표시 합니다.

Severity: 위험성 알림 레벨 설정 합니다. (All, Warning, Informational)

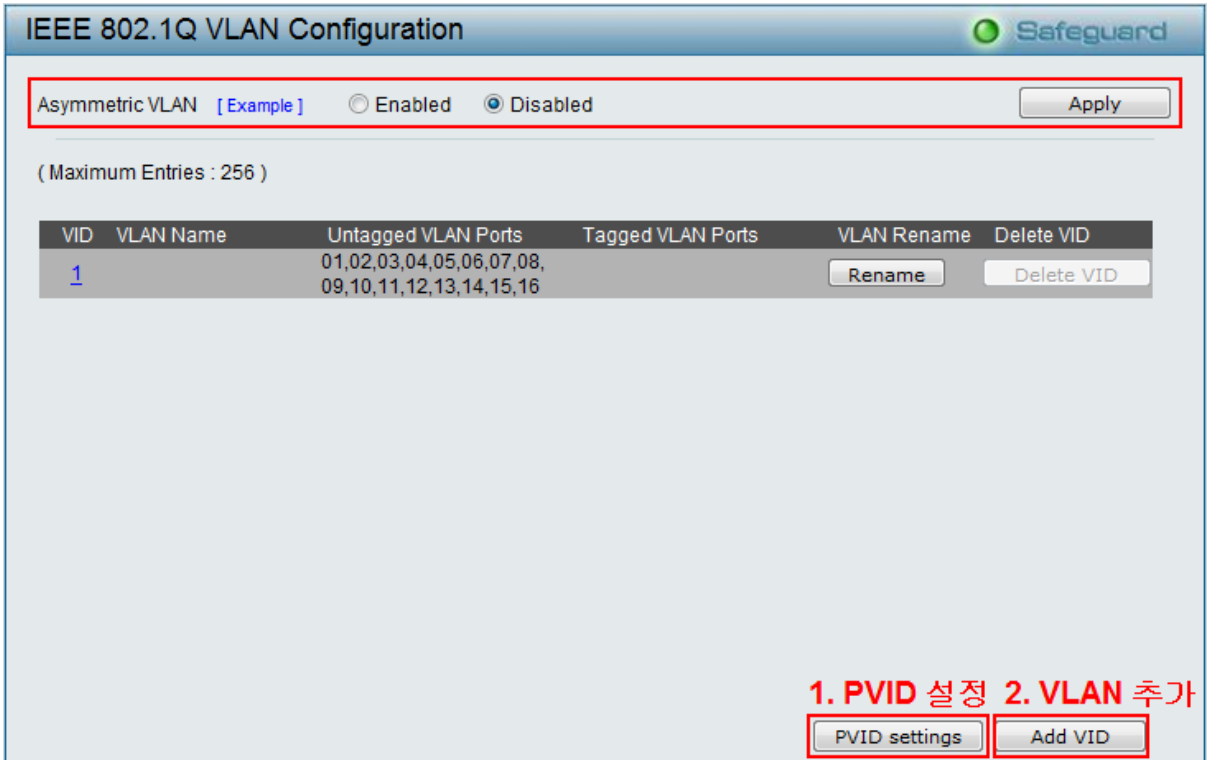
Facility: Remote Server에 전송 할 Facility Level 설정 합니다. (Level 0 ~ Level 7)

Configuration>>Jumbo Frame

(그림 26) 점보 프레임 설정 화면

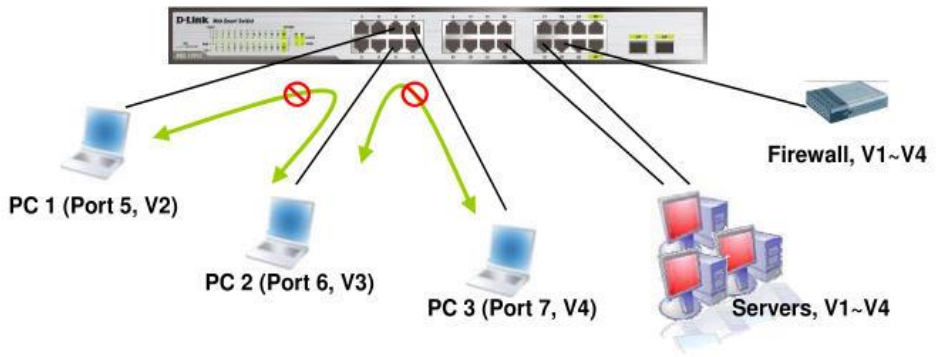
- 최대 전송 사이즈를 뜻합니다. 보통 데이터가 전송될 시 한번에 최대 1500Byte가 전송되는데 이를 MTU(Maximum Transmission Unit)라 합니다. 스위치에서 점보 프레임을 사용하게 되면 한번 전송 시 최대 10000Bytes까지 전송이 가능 합니다.
해당 기능은 NIC(Network Interface Card)도 점보 프레임을 지원해야 정상적으로 사용 할 수 있습니다.

Configuration>>802.1Q VLAN



(그림 27) VLAN 설정 화면

- VLAN을 추가 및 수정 할 수 있습니다.

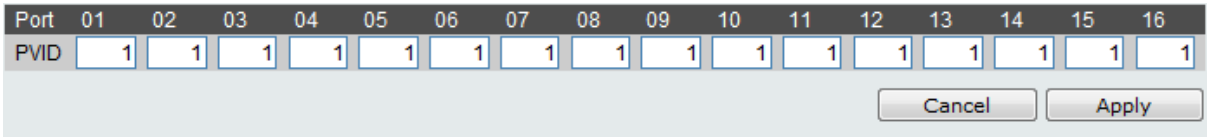


(그림 28) Asymmetric VLAN 구현 예

Asymmetric VLAN: 서로 다른 VLAN에 속한 멤버 포트에서 Shared VLAN으로 설정한 서버 및 인터넷 망으로만 통신이 가능하게 설정 가능 합니다.
서로 다른 VLAN에 속한 멤버 포트 간에는 통신이 불가능 합니다.

주의) Asymmetric VLAN 사용 시 VLAN, IGMP Snooping, Management VLAN, Mac Address Table은 기본값으로 초기화 됩니다.

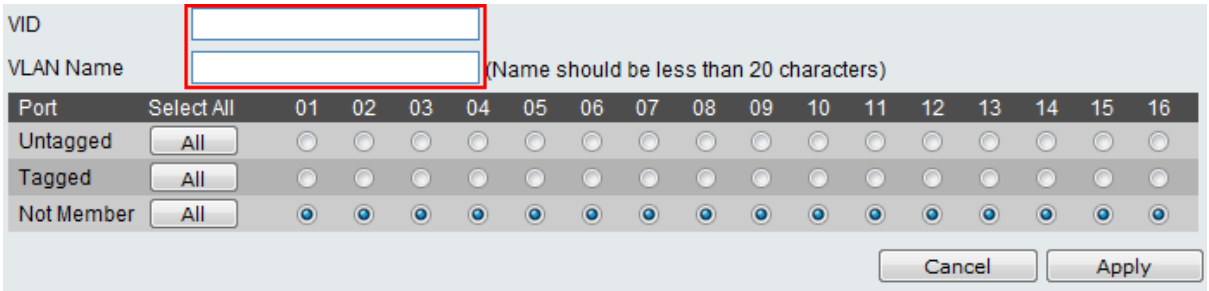
1) PVID 설정



(그림 29) VLAN PVID 설정

VLAN 설정 화면에서 **PVID Setting**을 누르시면 위 그림이 나오게 됩니다. 생성한 VID를 포트에 맵핑 할 수 있습니다.

2) VLAN 추가



(그림 30) VLAN 추가 화면

VID: 생성할 VID를 입력 합니다.

VLAN Name: VID의 이름을 20자 이내로 설정 합니다.

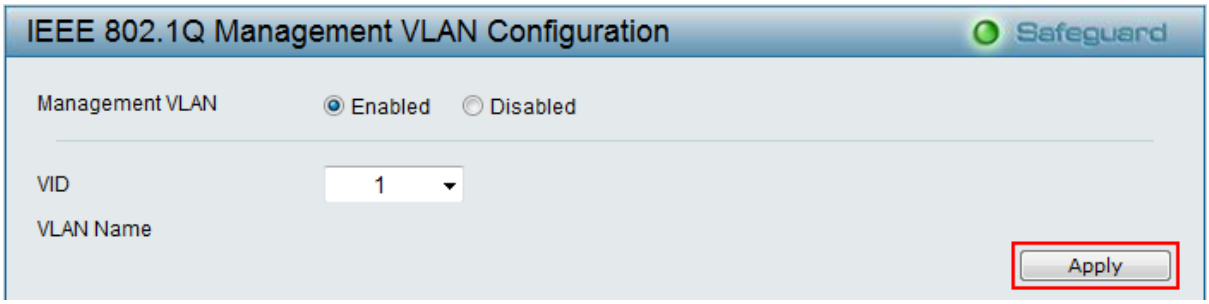
Untagged: Cisco의 Native VLAN과 같은 의미 입니다. 하나의 VLAN만 지정 가능 합니다.

Tagged: Cisco사의 Trunk와 비슷한 의미 입니다. 프레임에 tag정보를 삽입하여 구분 되며, 복수개의 VLAN을 지정 할 수 있습니다.

새로운 VID를 생성하면 기본적으로 모든 포트가 Not Member Port 입니다.

새로 생성한 VID에 특정 포트를 Untagged 할당 하기 위해서는 다른 VID에서 Not Member 포트로 반드시 변경 해야 합니다. 즉, Untagged 포트는 반드시 하나의 VID에만 소속 되어 있어야 합니다.

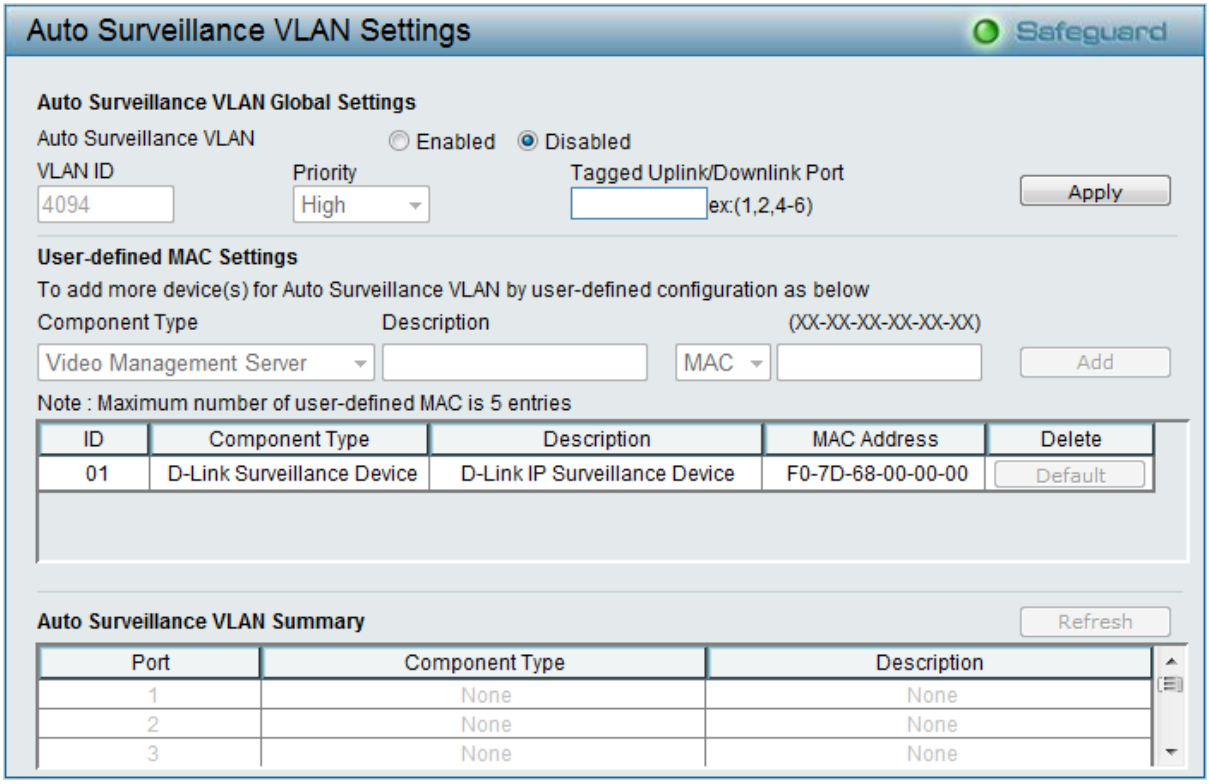
Configuration>>802.1Q Management VLAN



(그림 31)Management VLAN 설정 화면

스위치 Management IP의 VID를 지정하여 사용할 수 있습니다. (기본 설정 값: **Disabled**)

Configuration>>Auto Surveillance VLAN Settings



(그림 32) Auto Surveillance VLAN 설정 화면

Auto Surveillance VLAN은 Voice VLAN과 비슷하게 IP카메라 와 같은 IP Surveillance 제품이 스위치에 직접 연결된 경우 Surveillance VLAN으로 지정할 수 있으며 이러한 Traffic에 대한 우선순위를 부여하여 Service 품질을 향상 시킬 수 있습니다.

주의) Auto Surveillance VLAN 으로 지정된 VLAN은 일반적인 VLAN 기능을 수행 할 수 없습니다.

Auto Surveillance VLAN State: Auto Surveillance VLAN 활성화 여부를 선택 합니다.

VLAN ID: Auto Surveillance VLAN 으로 동작하게 할 VLAN 선택 합니다.

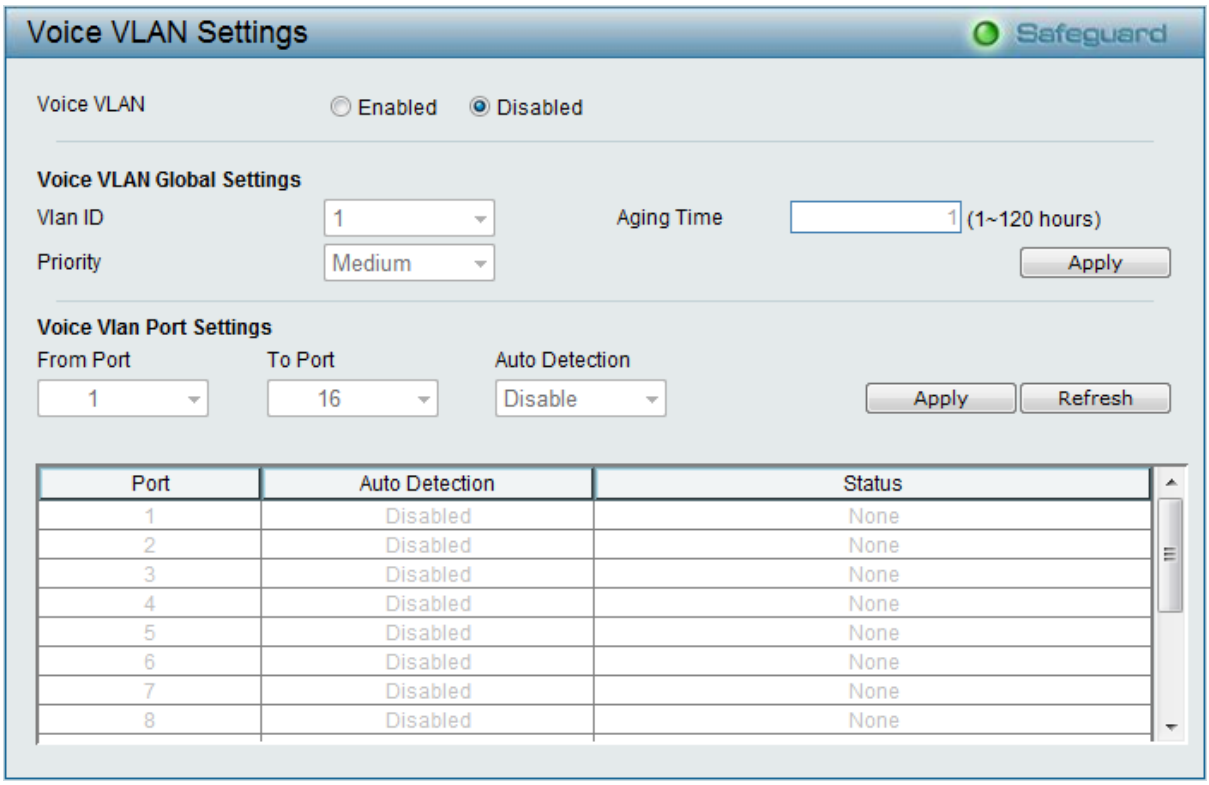
Priority: 802.1P 우선순위를 설정 합니다. (Low ~ Highest)

Aging Time: 특정 포트가 Auto Surveillance VLAN 멤버가 된 경우 해당 포트로 통해 Aging Time 안에 Surveillance Traffic 전송이 있어야 하며 그렇지 않을 경우 멤버 포트에서 제외 됩니다.

From Port/To Port: Auto Surveillance VLAN 멤버 포트로 적용할 포트 범위 설정 합니다.

Auto Detect: Auto Surveillance VLAN OUI 설정에서 정의한 통신사 OUI 값을 가지는 Surveillance Traffic이 해당 포트로 들어 올 경우 자동으로 Auto Surveillance VLAN을 할당 합니다.

Configuration>> Voice VLAN Settings



(그림 33) Voice VLAN 설정 화면

Voice VLAN은 VoIP 전화와 같은 Voice 단말이 스위치에 직접 연결 될 경우 Voice 전용 VLAN을 지정할 수 있으며 Voice Traffic에 대한 우선순위를 부여하여 Voice Service 품질을 향상 시킬 수 있습니다.

주의) Voice VLAN으로 지정된 VLAN은 일반적인 VLAN 기능을 수행 할 수 없습니다.

Voice VLAN State: Voice VLAN 활성화 여부를 선택 합니다.

VLAN ID: Voice VLAN으로 동작하게 할 VLAN 선택 합니다.

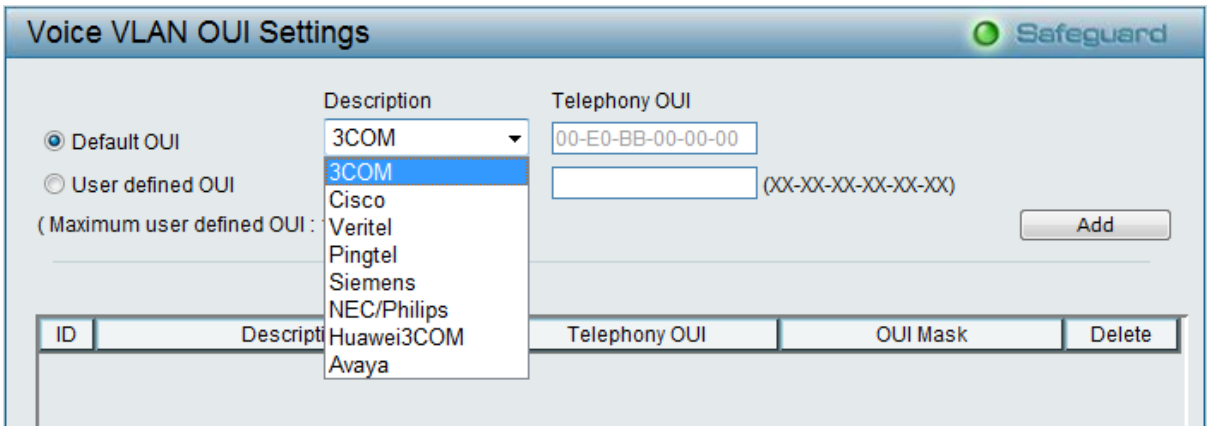
Priority: 802.1P 우선순위를 설정 합니다. (Low ~ Highest)

Aging Time: 특정 포트가 Voice VLAN 멤버가 된 경우 해당 포트로 통해 Aging Time 안에 Voice Traffic 전송이 있어야 하며 그렇지 않을 경우 멤버 포트에서 제외 됩니다.

From Port/To Port: Voice VLAN 멤버 포트로 적용할 포트 범위를 설정 합니다.

Auto Detect: Voice VLAN OUI 설정에서 정의한 통신사 OUI 값을 가지는 Voice Traffic이 해당 포트로 들어 올 경우 자동으로 Voice VLAN을 할당 합니다.

Configuration>> Voice VLAN OUI Settings



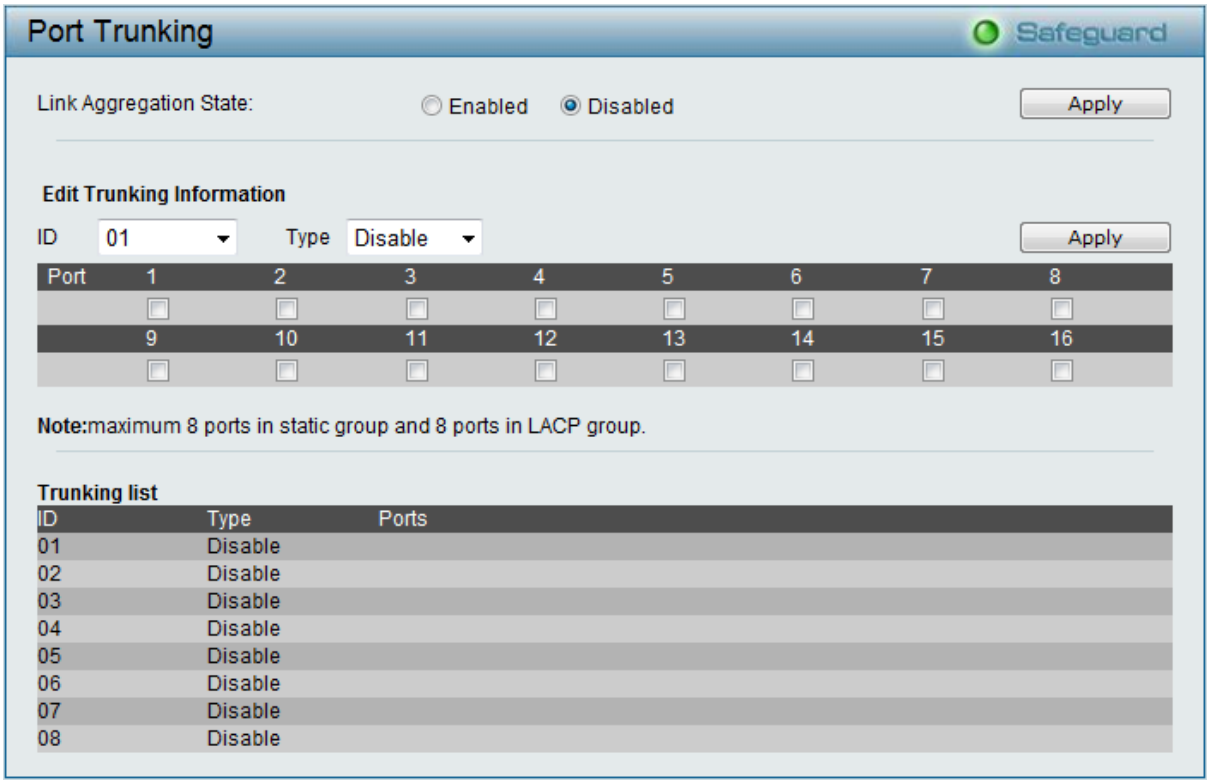
(그림 34) Voice VLAN 설정 화면

Voice VLAN 지정 포트에 연결될 VoIP 단말 제조사의 OUI를 등록 함.

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

(그림 35) 주요 Vender OUI

Configuration>> Port Trunking Settings



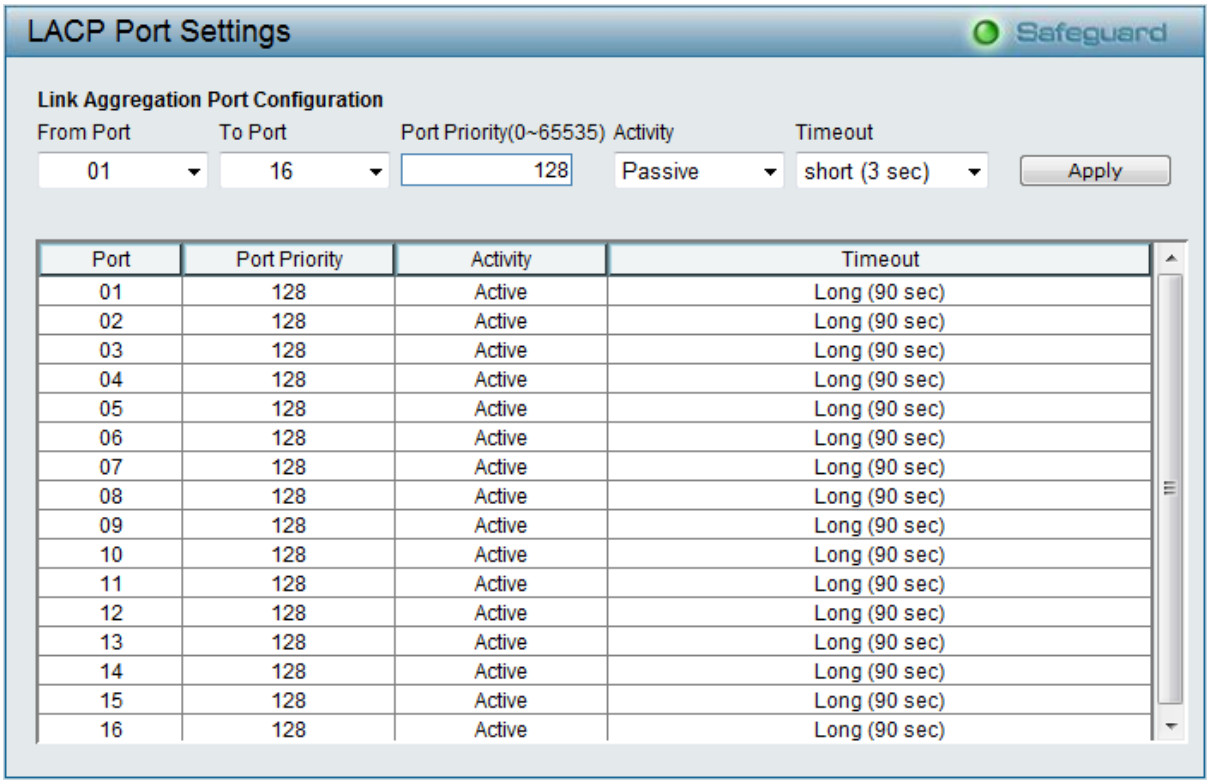
(그림 36) Port Trunking 설정 화면

Port Trunking 기능은 한 개 이상의 물리적인 포트를 논리적인 하나의 포트로 만들어 고속으로 데이터를 처리 할 수 있게 하는 기능으로 총 8개의 Group이 생성 가능 하며 각 그룹은 8개까지의 멤버 포트를 수용 할 수 있습니다.

Static: 수동 Link Aggregation 설정

LACP: 포트 Trunking 설정 시 LACP 모드로 설정

Configuration>> LACP Port Settings



Port	Port Priority	Activity	Timeout
01	128	Active	Long (90 sec)
02	128	Active	Long (90 sec)
03	128	Active	Long (90 sec)
04	128	Active	Long (90 sec)
05	128	Active	Long (90 sec)
06	128	Active	Long (90 sec)
07	128	Active	Long (90 sec)
08	128	Active	Long (90 sec)
09	128	Active	Long (90 sec)
10	128	Active	Long (90 sec)
11	128	Active	Long (90 sec)
12	128	Active	Long (90 sec)
13	128	Active	Long (90 sec)
14	128	Active	Long (90 sec)
15	128	Active	Long (90 sec)
16	128	Active	Long (90 sec)

(그림 37) LACP Port 설정 화면

From/To Port: LACP 설정 값 적용 할 시작 포트 와 마지막 포트를 설정 합니다.

Port Priority(0-65535): 포트 우선순위를 설정 합니다. 기본 값:128

- **Activity**

Active: LACP 포트 모드가 Active 이면 LACP 제어 프레임을 전송하며 상대방과 Link Aggregation을 하기 위한 negotiate 과정이 이루어집니다. LACP 포트를 구성하기 위해서는 반드시 하나 이상의 포트는 Active로 설정 되어있어야 하며 양 측 장비 모두 LACP 기능을 지원해야만 합니다.

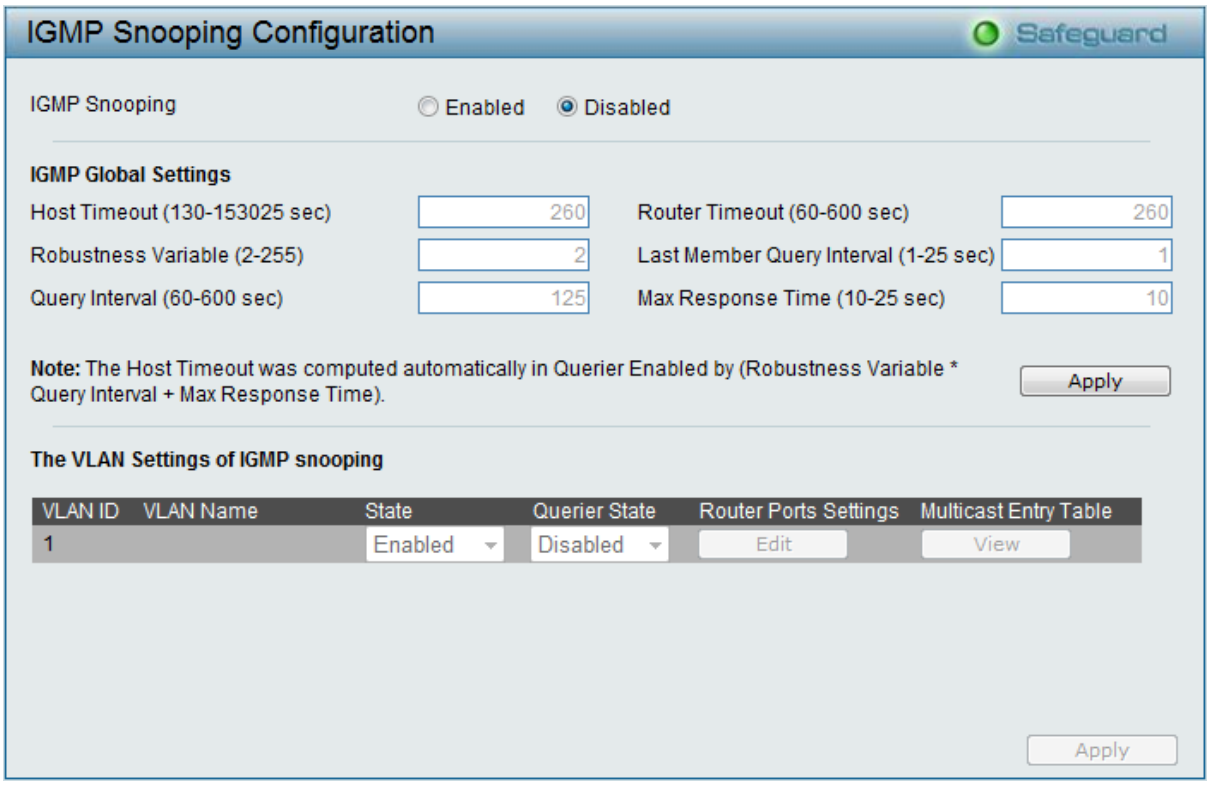
Passive: LACP 포트 모드가 Passive 지정되어 있으면 최초 LACP 제어를 위한 프레임을 전송하지 않습니다. 따라서 반대측 장비는 반드시 Active 모드로 설정되어 있어야 LACP 포트가 활성화 됩니다.

Timeout: 관리자 LACP Timeout 시간을 설정 합니다.

Short: 3 Sec

Long: 90 Sec

Configuration>> IGMP Snooping Configuration

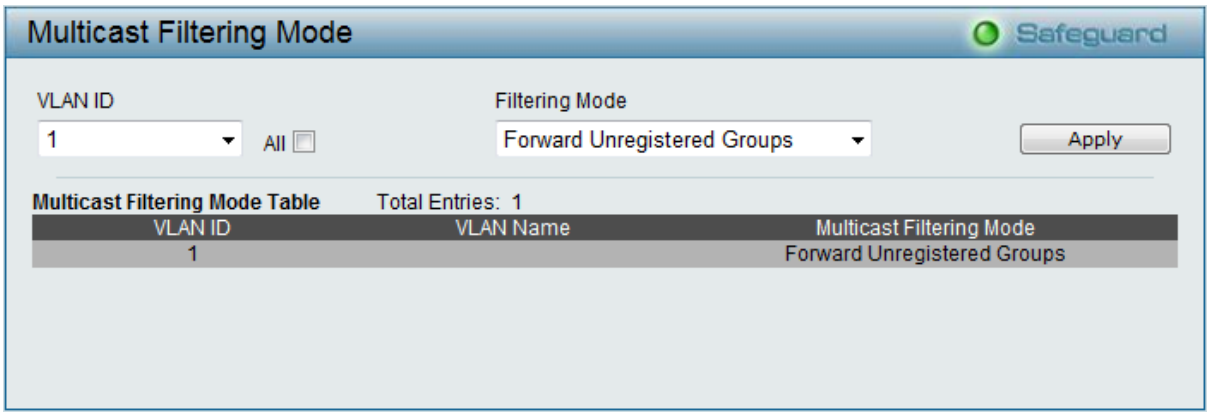


(그림 38) IGMP Snooping 설정 화면

IGMP Snooping 기능은 실시간 영상 전송 서비스 와 같은 RTP(Real Time Protocol) 전송할 때 대부분 Multicast 로 전송이 이루어지게 되는데 이 때 Multicast Traffic의 특성상 모든 포트로 Multicast Traffic이 Flooding 됩니다. 이때 Multicast Flooding을 방지하고 수신하고자 하는 포트로만 해당 Traffic이 Forwarding이 가능하도록 하는 프로토콜이 IGMP Snooping 입니다.

Host Timeout(130-153025 sec): 멀티캐스트 호스트는 해당 멀티캐스트 Group으로 부터 Traffic을 수신 중이라는 Report 해야 하는 시간. Reporting 이 후 이 시간은 갱신되며 Timeout 시간 내에 Report를 하지 않을 시 Entry에서 삭제 됩니다.
Robustness Variable(2-255): Subnet 상에서 Packet loss 발생 예상 값
Query Interval(60-600 sec): IGMP Query 전송 주기
Router Timeout(60-600 sec): Router 포트로 Query 제어 메시지를 수신해야 하는 시간
Last Member Query Interval(1-25 sec): 특정 그룹 Query 메시지를 응답 받기 위해 대기하는 시간
Max Response Time(10-25 sec): 응답 메시지 보내기 전 최대 대기 시간

Configuration>> Multicast Filtering Mode



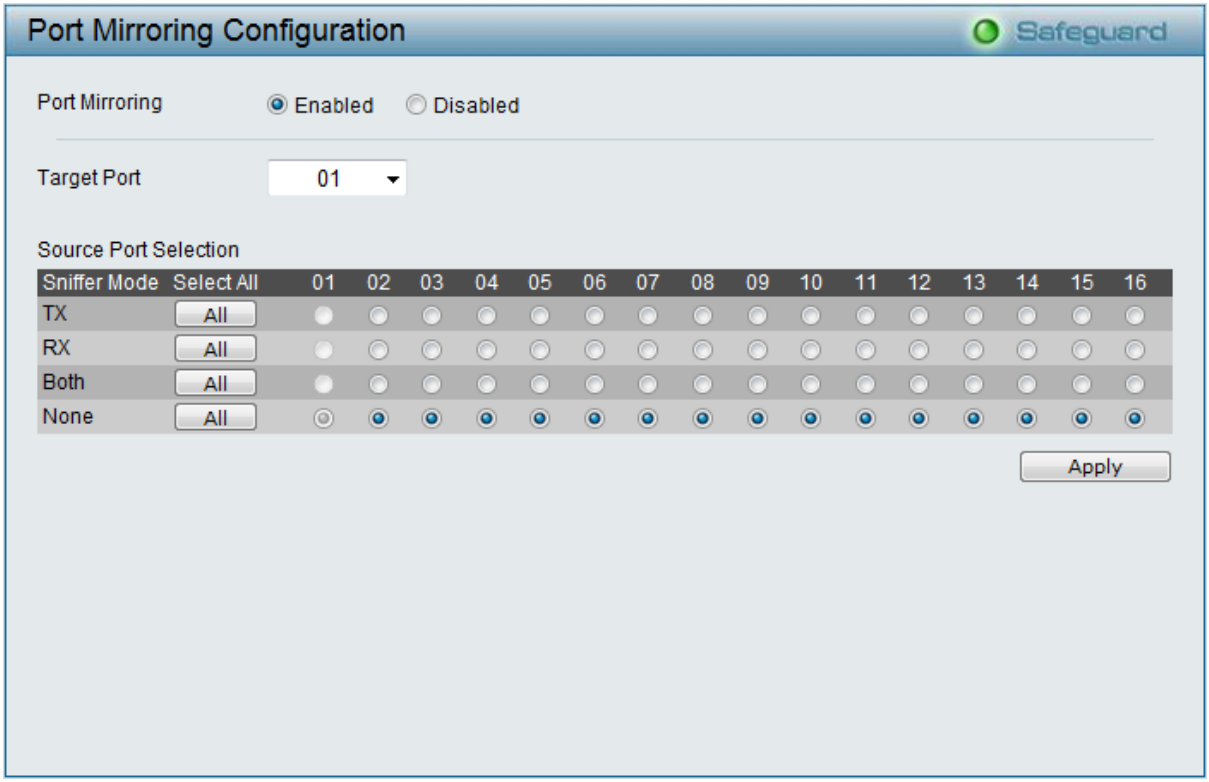
(그림 39) Multicast 필터링 설정 화면

Forward All Groups: 등록 및 비 등록 그룹 모두에 대해 해당 VLAN의 전 포트로 Multicast Traffic이 전송 됩니다.

Forward Unregistered Groups: Register Table에 등록된 Group 기반으로 Multicast Traffic을 전송하지만 비 등록된 Group에 대해서는 VLAN상 모든 포트로 Flooding 됩니다.

Filter Unregistered Groups: Register Table에 등록된 Group 기반으로 Multicast Traffic을 전송하며 비 등록된 Group에 대해서는 Filtering 합니다.

Configuration>> Port Mirroring Configuration



(그림 40) Port Mirroring 설정 화면

Port Mirroring은 네트워크 스위치의 한 개 이상의 포트로부터 관리자가 mirroring을 설정한 해당 포트로 송/수신되는 Packet의 복사본을 전달함으로써 네트워크 Traffic을 감시

하는 기능 입니다.

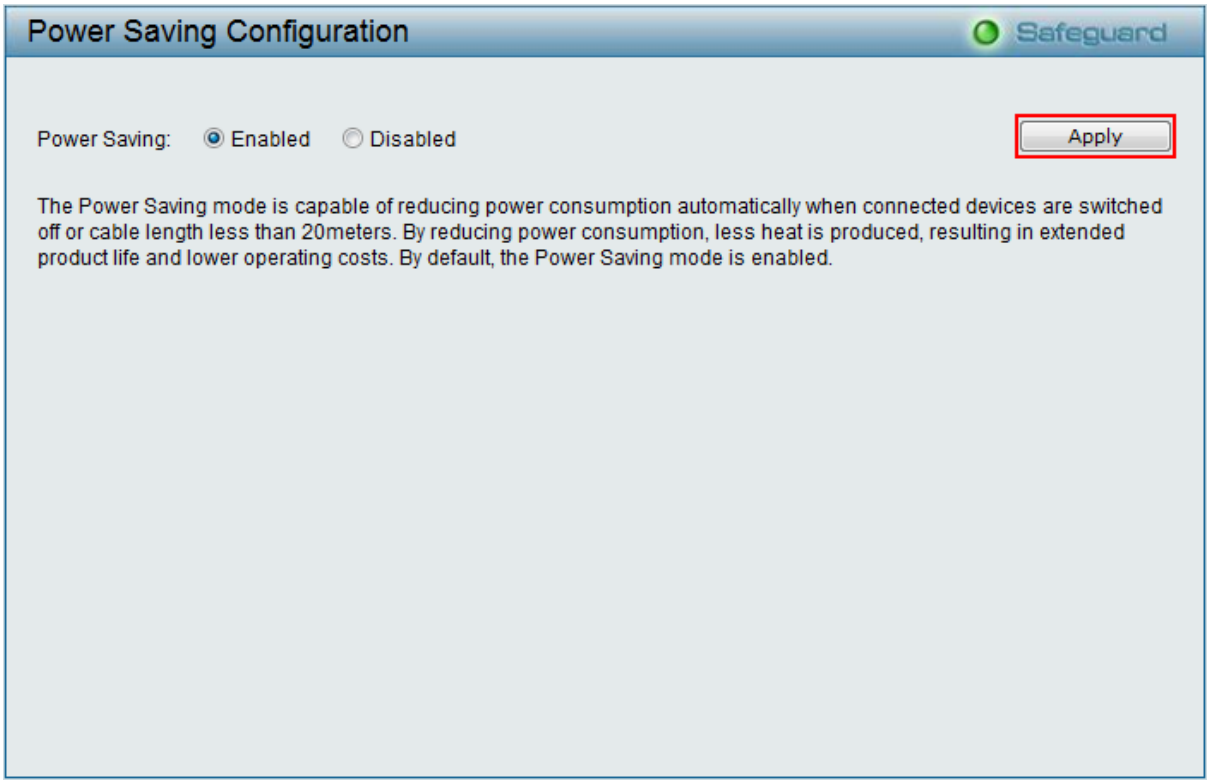
Target Port: 이더리얼,Wireshark 와 같은 Traffic 분석 장치가 연결될 포트

Source Port: Packet 분석을 하고자 하는 대상 포트

- **TX Mode**: Source 포트로 송신하는 Packet 모니터링
- **RX Mode**: Source 포트로 수신되는 Packet 모니터링
- **Both**: Source 포트로 송수신되는 모든 Packet 모니터링

주의) Source 포트는 Target 포트가 될 수 없습니다

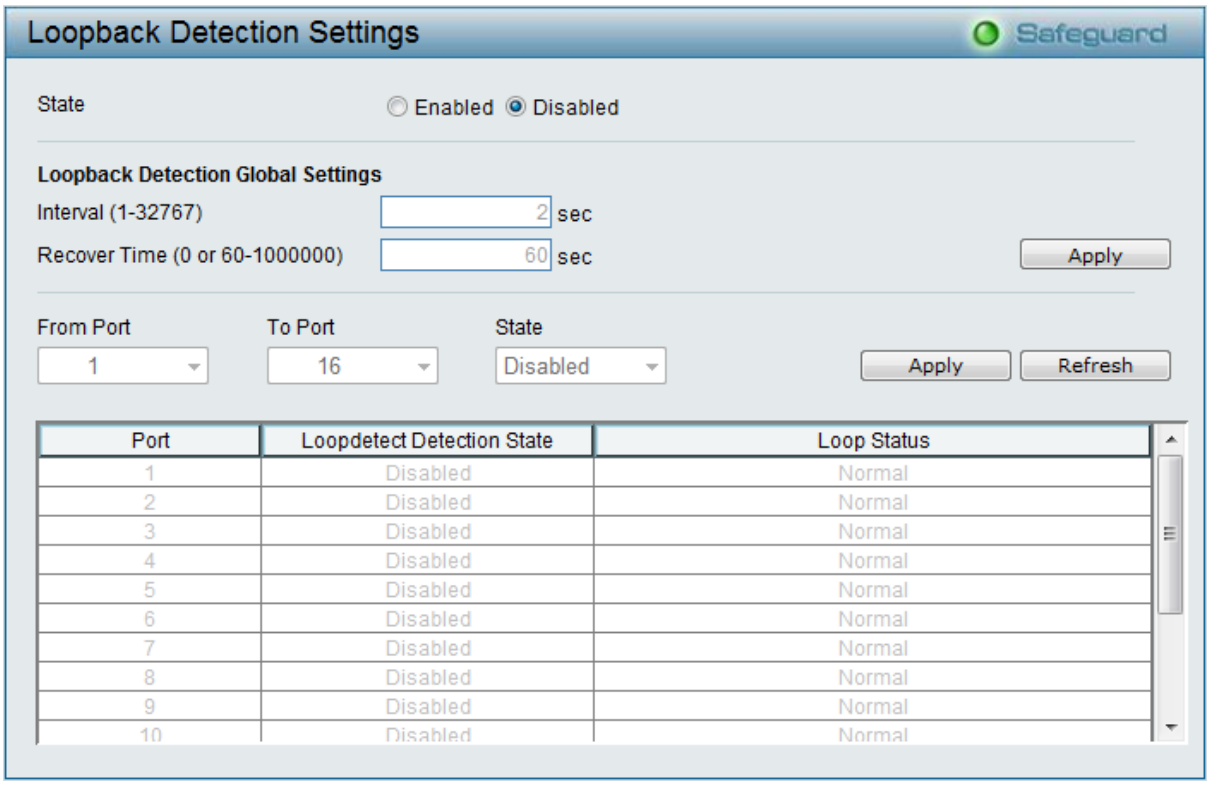
Configuration>> Power Saving



(그림 41) Power Saving 설정 화면

절전 모드는 연결되어 있는 장비의 전원이 끄거나 케이블의 길이가 20미터 이내에 있을 시 자동으로 전력의 소비를 줄일 수 있습니다. 전력 소비를 줄임으로써 낮은 온도로 동작하여 결과적으로 제품의 수명을 늘어나고 관리비용은 낮아지게 됩니다. 기본적으로 절전기능은 활성화 되어 있습니다.

Configuration>> Loopback Detection Setting



(그림 42) Loopback Detection 설정 화면

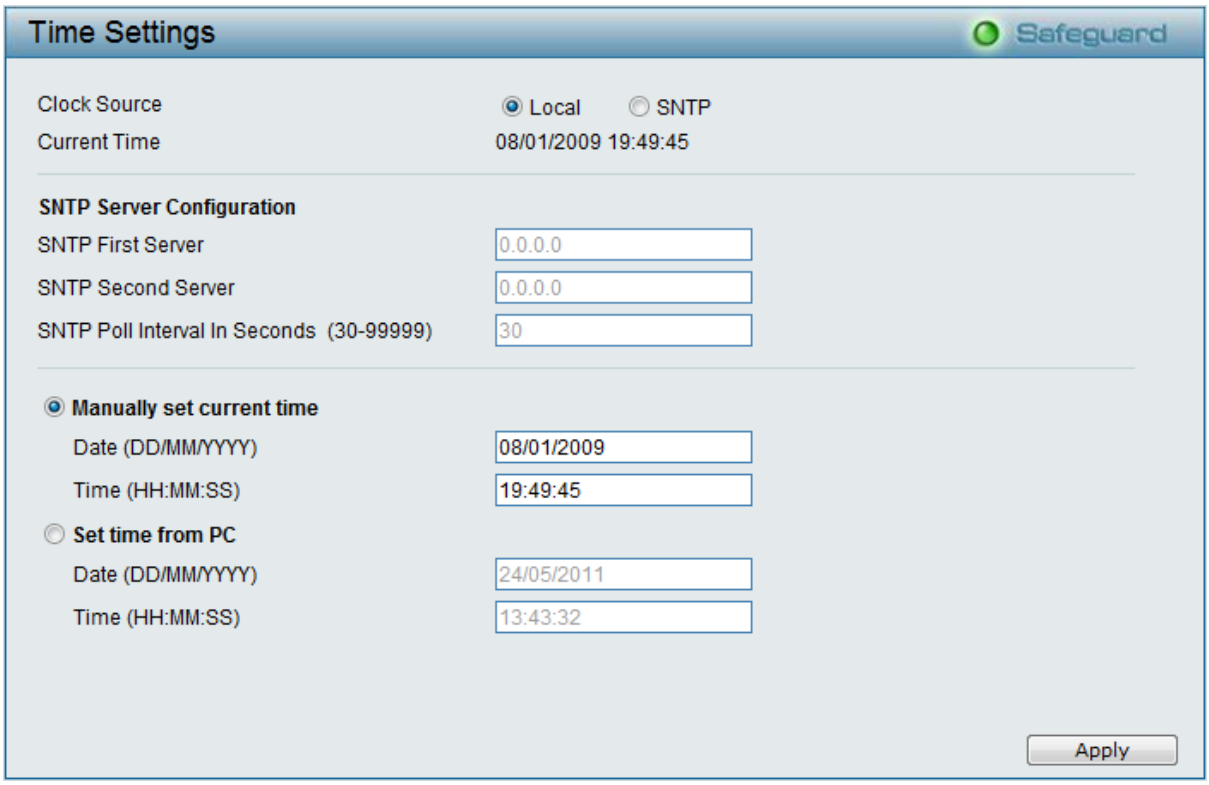
Loopback Detection 기능은 STP가 비활성화된 네트워크 환경이나 특히 다운링크에 허브 또는 비 관리형 스위치 연결로 물리적인 Loop 가 발생하였을 때 이를 감지하는 역할을 합니다.

이 기능이 설정된 스위치는 Loop가 발생된 포트를 자동으로 차단 하며 Recover Time이 경과한 이후에는 다시 차단을 해지 합니다.

Interval(1-32767): Loop 감지 주기. 기본값 1초

Recover Time: Loop가 감지 되었을 때 포트 차단 이후 해당 포트를 다시 복원하는 시간 기본값 60초 이며 0은 Time를 작동 시키지 않습니다.

Configuration>> SNTP Setting>> Time Setting



(그림 43) Time 설정 화면

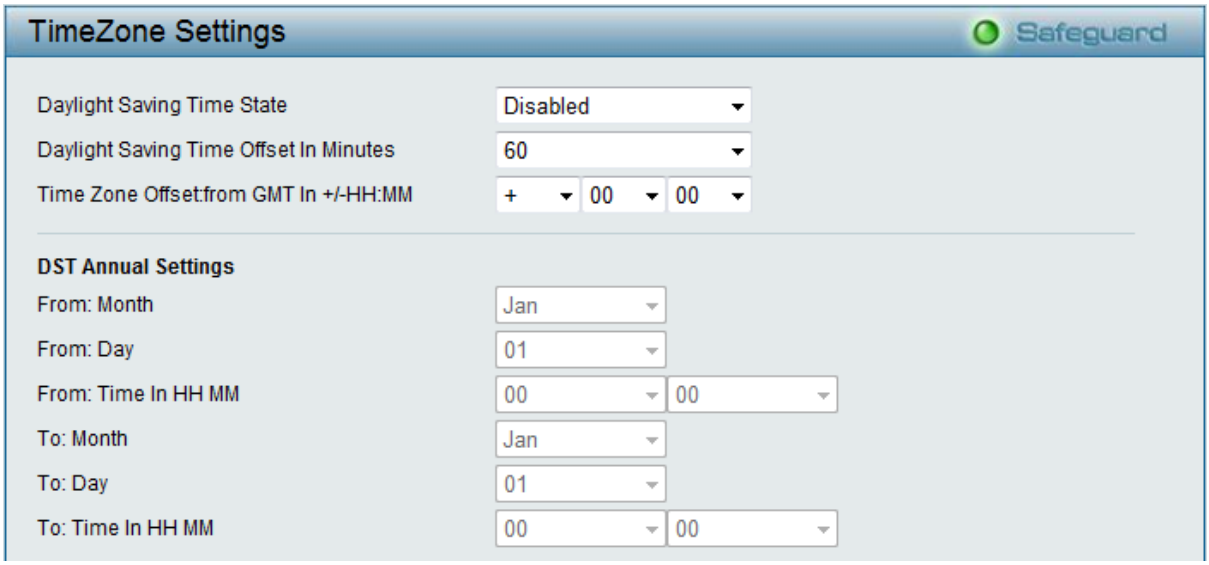
Clock Source

- **Local**: 수동으로 현재의 시간을 설정 할 수 있으며 PC로 부터 받아올 수도 있음
- **SNTP**: SNTP서버의 IP를 지정한 후 서버로부터 시간 정보를 받아옴

SNMP First/Second Server: 메인 SNTP 서버 및 보조 SNTP 서버 IP 설정

SNMP Poll Interval in Second: SNTP 서버 에서 시간 정보를 요청 주기

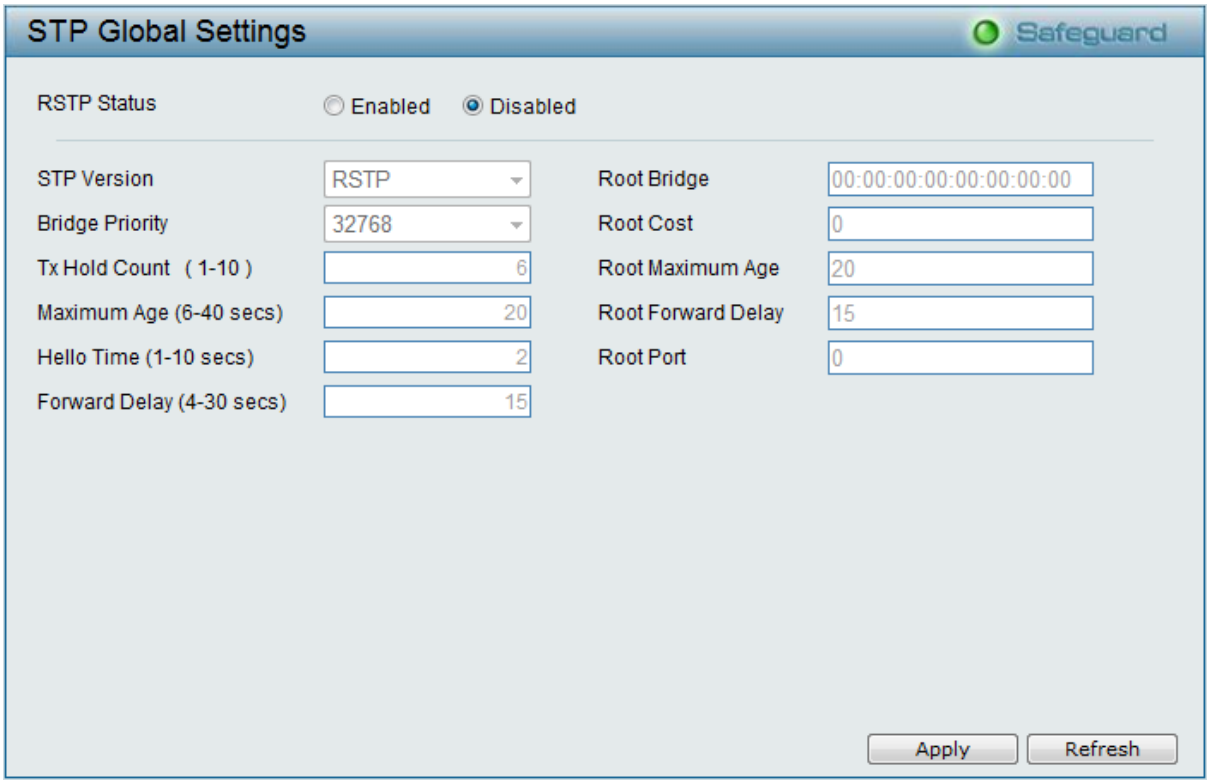
Configuration>> SNTP Setting>> Time Zone Setting



(그림 44) Time Zone 설정 화면

Daylight Saving Time State: 일광절약시간 적용 여부 설정
Daylight Saving Time Offset In Minutes: 일광절약시간 분 단위 설정
Time Zone Offset from GMT in +/-HH:MM: GMT 기준시 설정 예) +9:00
DST Annual Setting: 일광절약시간 설정 시 적용 날짜 및 시간 설정

Configuration>> STP Global Setting



(그림 45) STP Global 설정 화면

Spanning Tree Protocol은 네트워크의 안정성을 위하여 스위치 이중화(Redundancy)를 구성할 경우 물리적인 Loop 구조를 가지게 됩니다.
이 와 같은 물리적인 Loop 구조를 가진 네트워크 환경에서 STP를 사용하여 특정 포트를 논리적으로 차단함으로써 L2 Loop를 방지하는 기능입니다.

STP Version: RSTP / STP Compatible. 기본값 RSTP(RSTP가 STP보다 수렴 시간이 훨씬 빠름)
Bridge Priority: Root Bridge 선출을 위한 Parameter. 낮은 값일수록 높은 우선 순위를 갖습니다. 기본값 32768
Tx Hold Count: Hello Packet 최대 전송 수. 기본값 6
Maximum Age: 최대 BPDU 정보 수신 대기 시간. 기본값 20초
Hello Time: BPDU 정보를 전송 주기. 기본값 2초
Forwarding Time: STP Listen, Learning 상태에서의 대기 시간. 기본값 15초
Root Bridge: Root Bridge의 MAC 정보

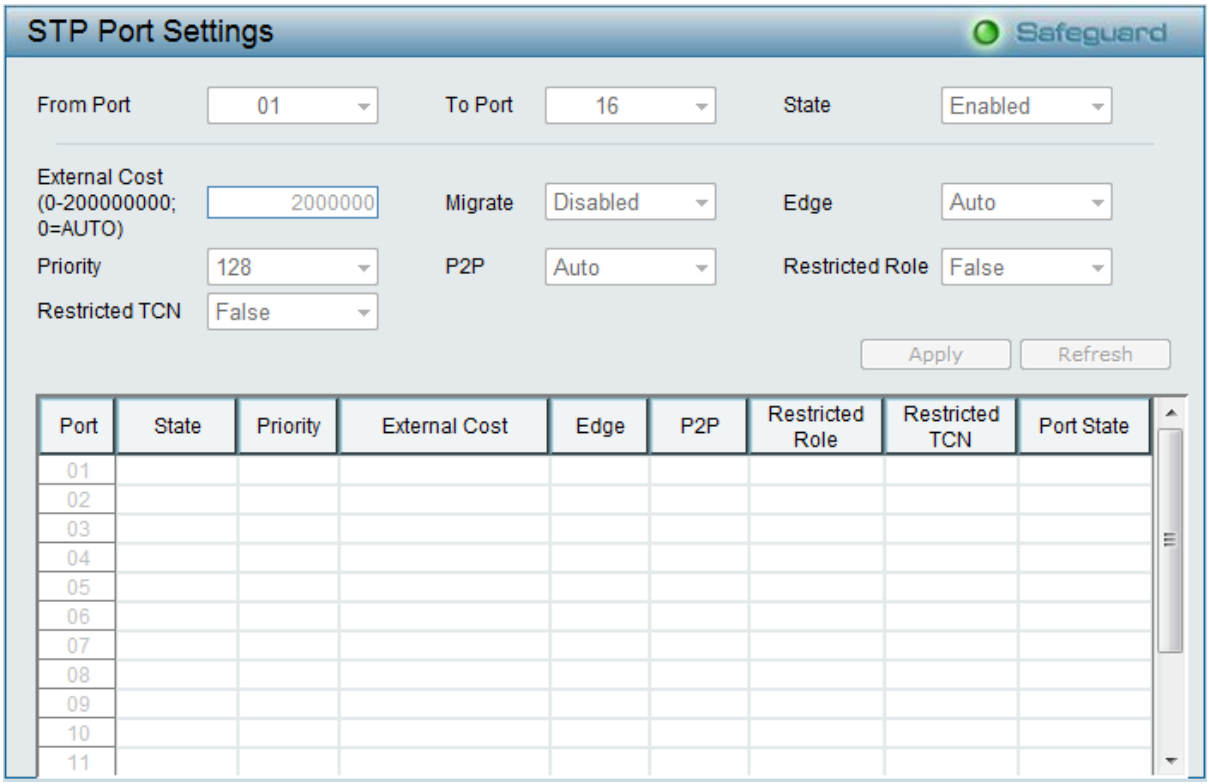
Root Cost: Root Bridge까지의 거리값

Root Maximum Age: Root Bridge의 Maximum Age 값

Root Forward Delay: Root Bridge의 Forward Delay 값

Root Port: Root Port 정보

Configuration>> STP Port Setting



(그림 46) STP Port 설정 화면

From Port/To Port: STP Port 설정을 할 대상 포트의 시작과 마지막을 선택 합니다.

External Cost: 0은 자동을 의미하며 매체의 속도에 따라 자동으로 값이 선택 됩니다.

예) 100M Port: 20000, 1G Port: 2000

수동으로 값을 지정 할 수도 있으며 작은 값이 높은 우선순위를 갖습니다.

Migrate: 이 설정이 활성화되면 BPDU 전송 시 상대방의 STP 설정 정보를 요청 합니다. 만일 상대방이 RSTP가 설정되어 있다면 STP에서 RSTP로 Migrate 가능 합니다.

Edge: PC와 같은 단말이 연결된 경우 설정 하며 Edge 포트로 설정된 포트는 BPDU를 수신 할 수 없으며 수신 시 Loop가 발생 할 수도 있습니다.

Priority: 각 포트의 우선순위. 기본값이 128이며 0부터 240사이의 값으로 설정 가능 낮은 값이 높은 우선순위 갖습니다.

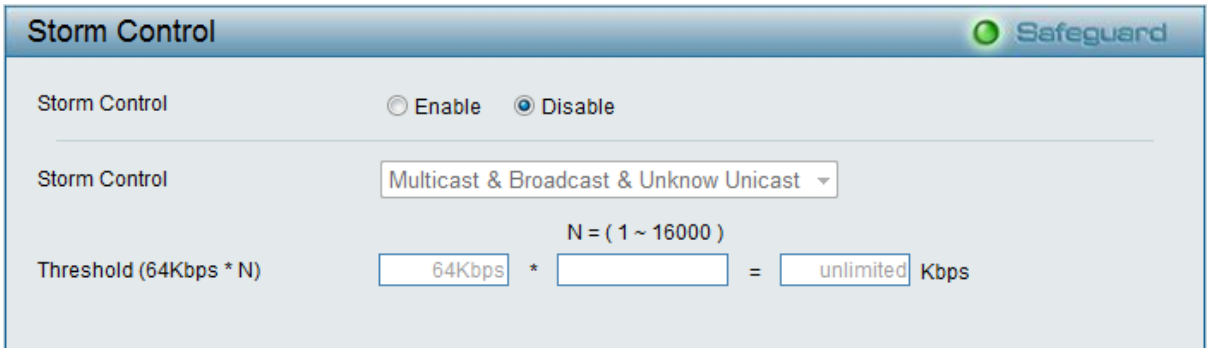
P2P: Edge 포트 와 비슷한 기능을 하며 Point-to-point shared 링크 라고도 하며, 차이점은 해당 포트는 반드시 Full Duplex 모드여야 합니다.

Restricted Role: True로 설정하면 해당 포트는 절대 Root 포트로 선출 될 수 없습니다.

Restricted TCN: STP 활성화 토폴로지에서 물리적인 변화가 발생하면 TCN(Topology

Change Notification) 메시지가 전송되게 됩니다. 해당 포트에 이 값이 활성화가 되면 더 이상 TCN 메시지를 다른 포트로 전송하지 않습니다.

QoS>> Storm Control

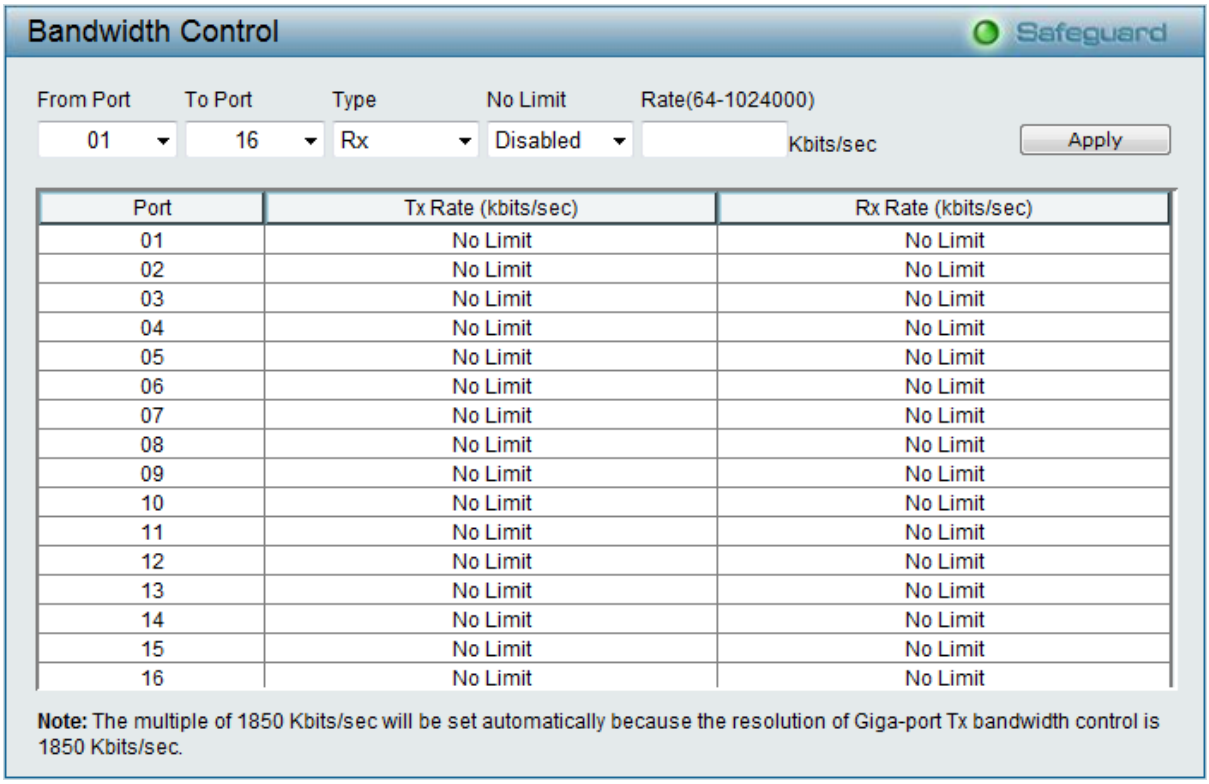


(그림 47) STP Port 설정 화면

Strom Control의 기능은 Multicast, Broadcast, Unknown Unicast 트래픽이 지정한 임계치 이상으로 유입될 경우 해당 Packet을 Drop 함으로써 스위치의 부하를 줄여주는 역할 합니다.

Storm Control: 제어 대상 Traffic 분류 (Multicast, Broadcast, Unknown Unicast)
Threshold: 임계치 설정

QoS>>Bandwidth Control

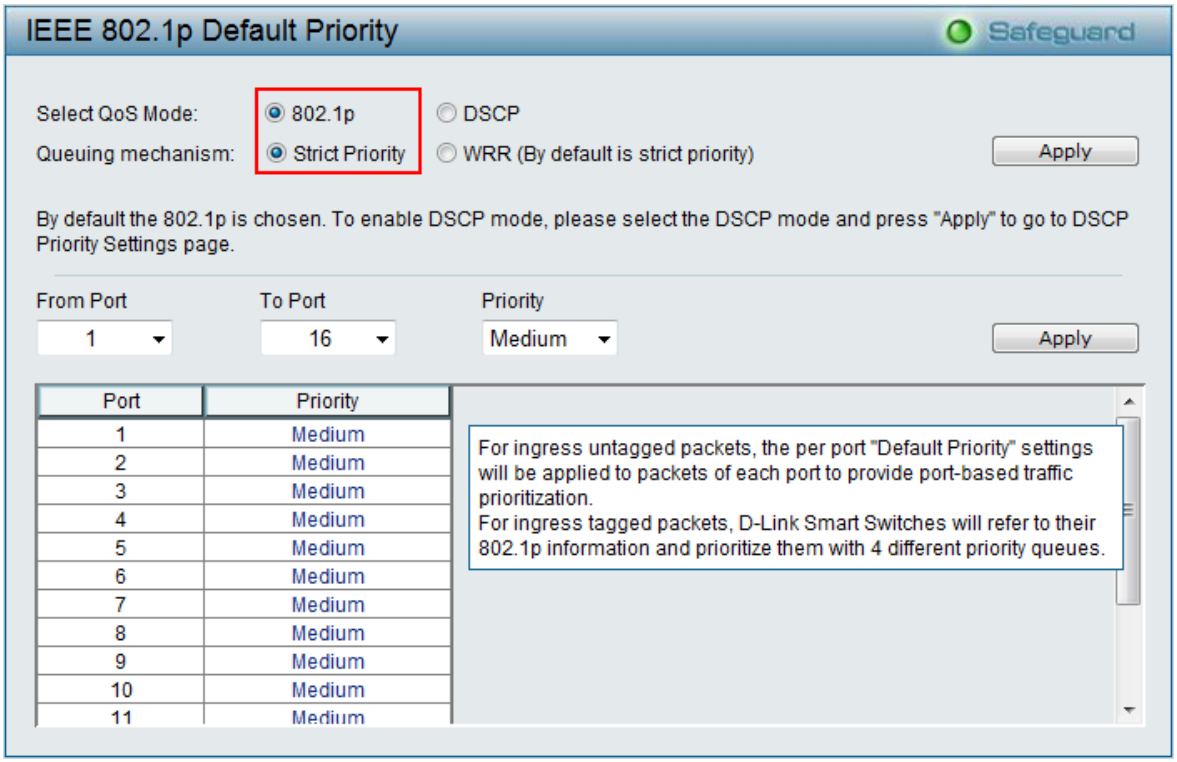


(그림 48) Bandwidth Control 설정 화면

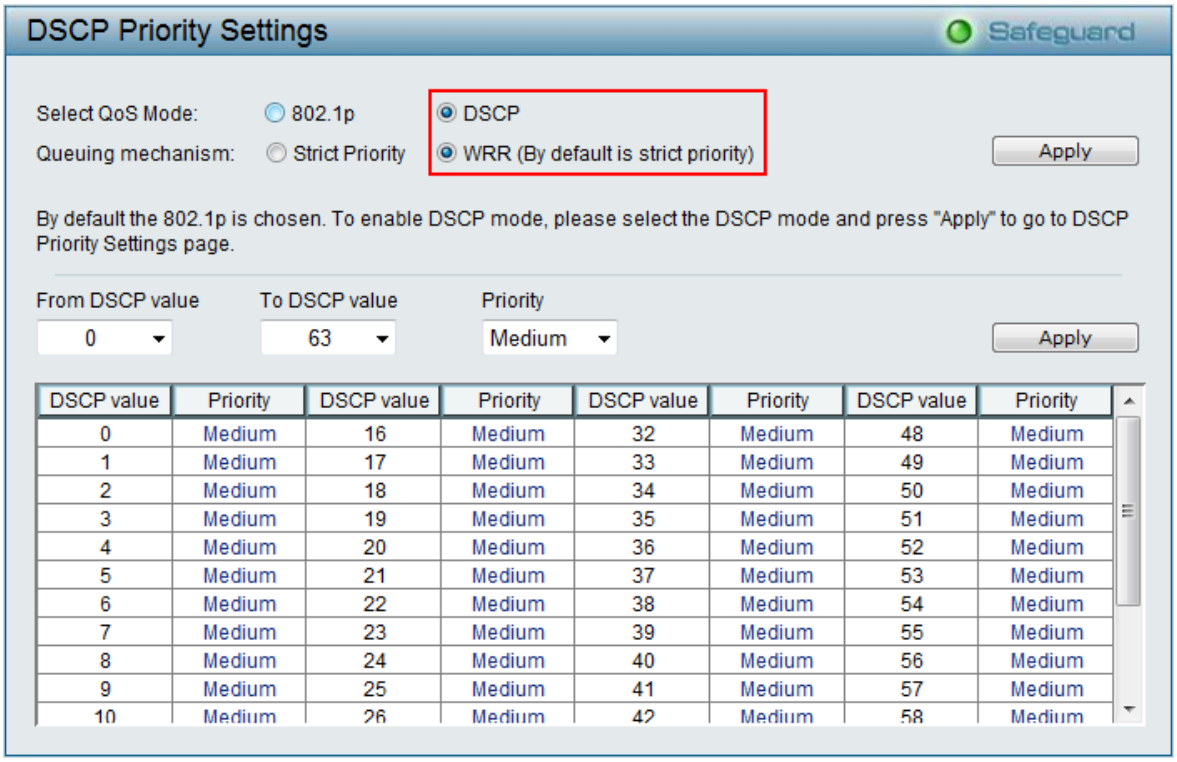
Bandwidth Control은 해당 포트에 업/다운로드 속도를 제한하는 기능입니다.
해당 포트를 지정 후 Type에서 Rx/Tx/Both를 선택 후 제한 값을 지정 합니다.

주의) 기가 포트의 Tx 속도는 1850kbps 배수 단위로만 설정이 가능 합니다.

QoS>>IEEE 802.1p Default Priority



(그림 49) IEEE 802.1p 우선순위 설정 화면



(그림 50) DSCP 우선순위 설정 화면

Select QoS Mode

- **802.1p**: Traffic 우선 순위 지정 할 수 있는 VLAN Header의 COS 필드 값 설정 합니다.
- **DSCP**: 서로 다른 수준의 서비스를 할당 할 수 있도록 하는 IP Packet 내 필드 값 설정 합니다.

Queuing Mechanism

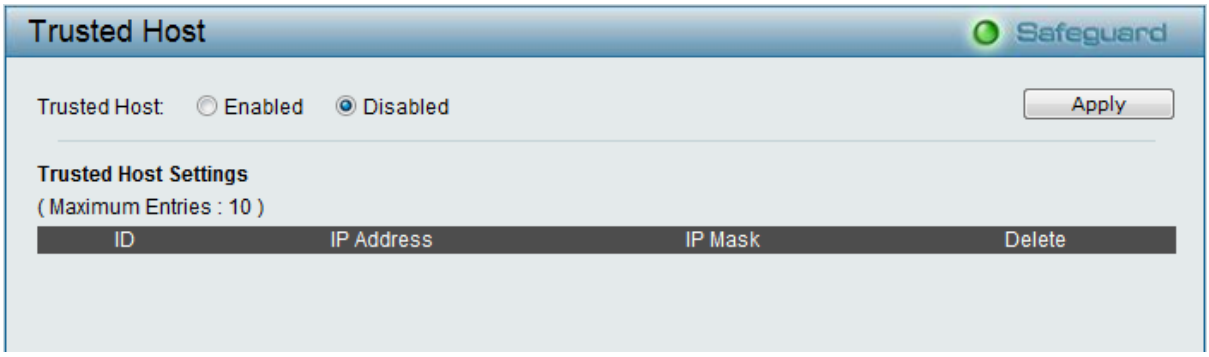
- **Strict Priority**: Packet 처리 시 높은 우선순위를 가진 Packet을 먼저 처리 합니다.
- **WRR**: 우선순위에 따른 Weight 값을 달리 지정하여 Packet을 처리 합니다.

WRR Queuing의 우선순위에 따른 Weight 값은 다음과 같습니다

Highest : 8 , High : 4 , Medium : 2 , Low : 1

Default Priority: 모든 포트의 기본 Priority는 Medium으로 설정 되어 있으며 포트 별로 변경이 가능하다.

Security>>Trusted Host



(그림 51) Trusted Host 설정 화면

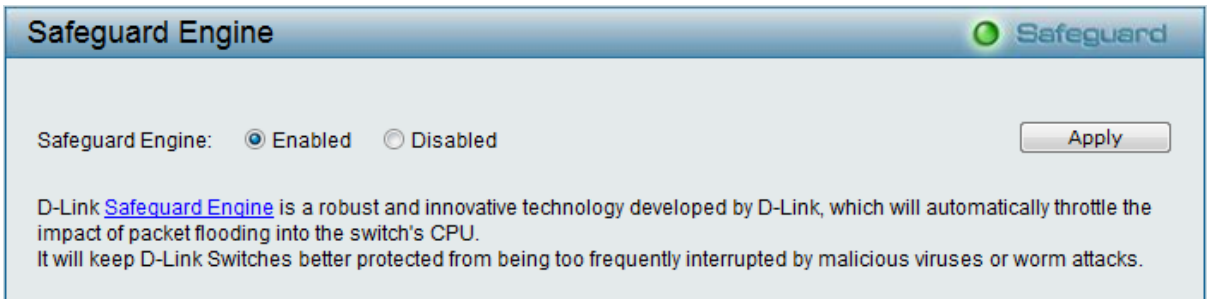
스위치에 접속을 인가할 특정 호스트 또는 네트워크 대역을 입력하여 사전에 정의한 사용자 만이 접속을 할 수 있도록 허용 합니다.

IP Address	Subnet Mask	Permitted IP
192.168.0.1	255.255.255.0	192.168.0.1~192.168.0.255
172.17.5.215	255.0.0.0	172.0.0.1~172.255.255.255

(그림 52) Trusted Host IP 대역 설정 화면

Add Host 버튼으로 추가를 **Delete** 버튼으로 삭제 할 수 있으며 설정 완료 후 **Apply** 버튼을 눌러 활성화 합니다.

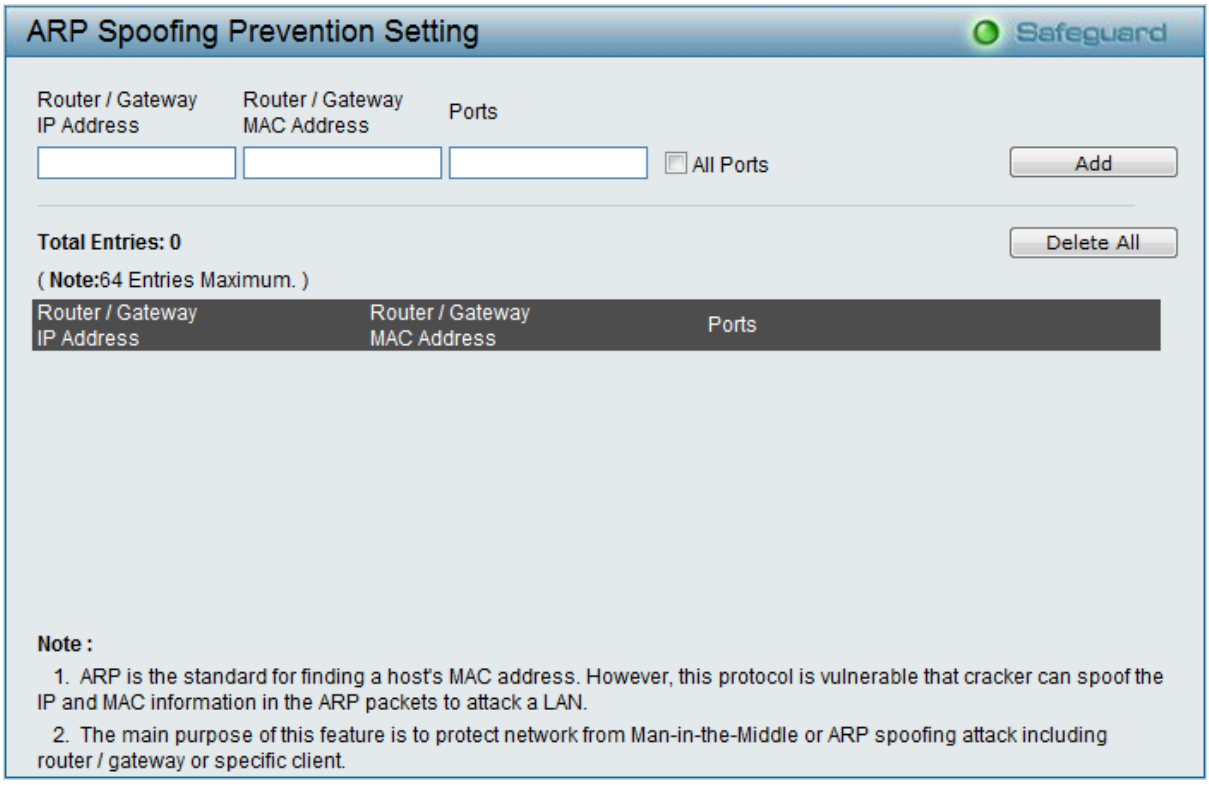
Security>>Safeguard Engine



(그림 53) Safeguard Engine 설정 화면

Safeguard Engine 기능은 **D-Link** 독자적인 기술로 스위치에 순간적으로 Traffic이 폭주하여 CPU 사용률 증가로 중요 Traffic 전송에 병목현상 등이 발생하는 것을 자동으로 방지해 줍니다. 또한 **D-Link Safeguard Engine** 기능은 바이러스 나 Worm 과 같은 악의적인 공격으로부터 보호 해줍니다.

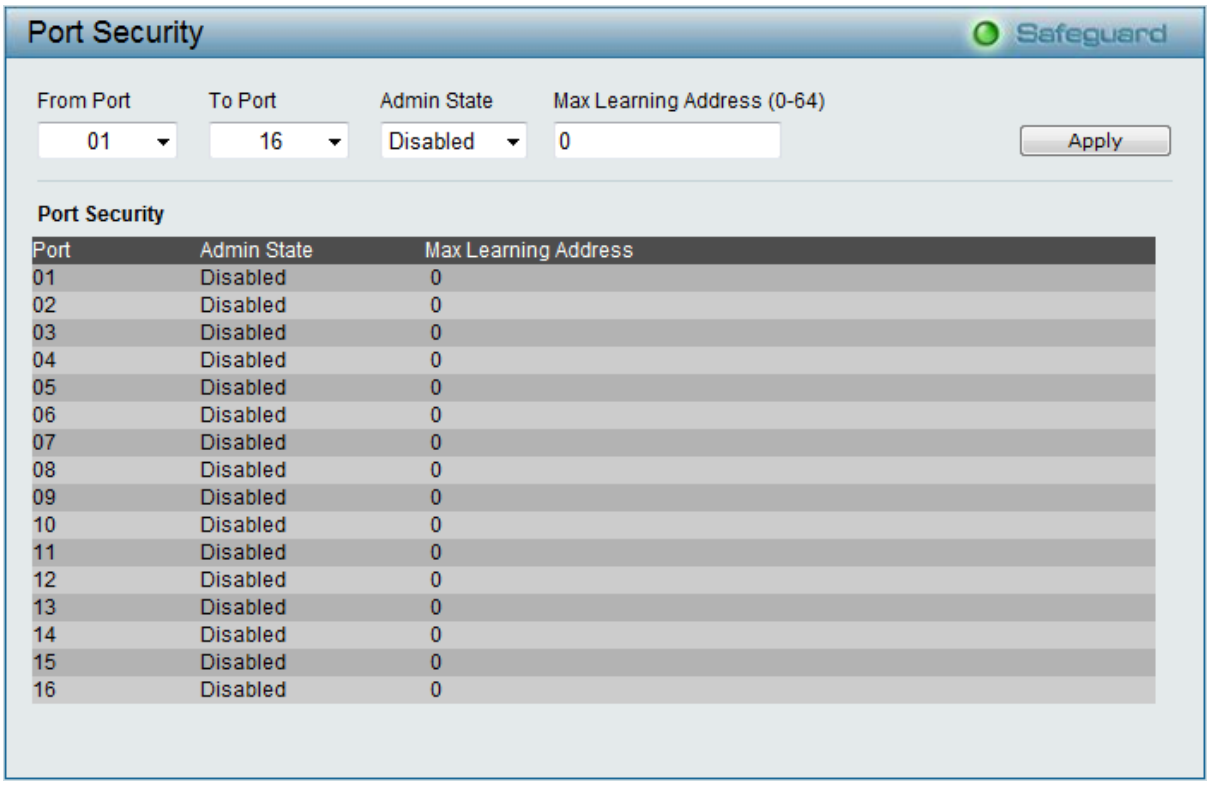
Security>>ARP Spoofing Prevention Setting



(그림 54) ARP Spoofing Prevention 설정 화면

ARP Spoofing Prevention 기능은 상단 Router 또는 Gateway 장비의 IP 주소 및 MAC 주소 와 물리적으로 연결된 포트를 Binding 하여 ARP Spoofing 공격으로 Gateway 정보가 변조 되어 장애가 발생하는 것을 방지 합니다.

Security>>Port Security

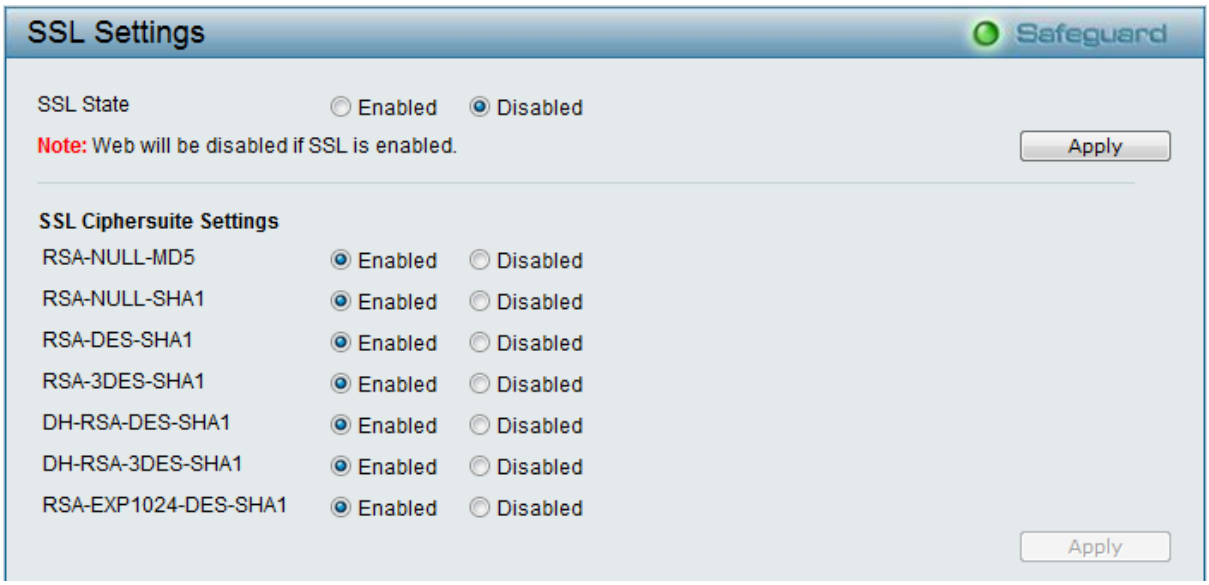


(그림 55) Port Security 설정 화면

Port Security 기능은 해당 포트로 학습 가능한 MAC 주소 수를 지정하여 현재 사용중인 Client MAC에 대해서만 포트보안을 적용할 수 있으며 Port Security 적용 이후 해당 포트로 접속하는 비인가 MAC 주소에 대해서는 자동으로 차단 됩니다.

주의) 수동 또는 자동으로 학습한 MAC에 대해 정확한 포트보안을 적용하려면 해당 포트를 통해 연결된 Client의 수를 정확히 파악하여야 합니다.

Security>>SSL

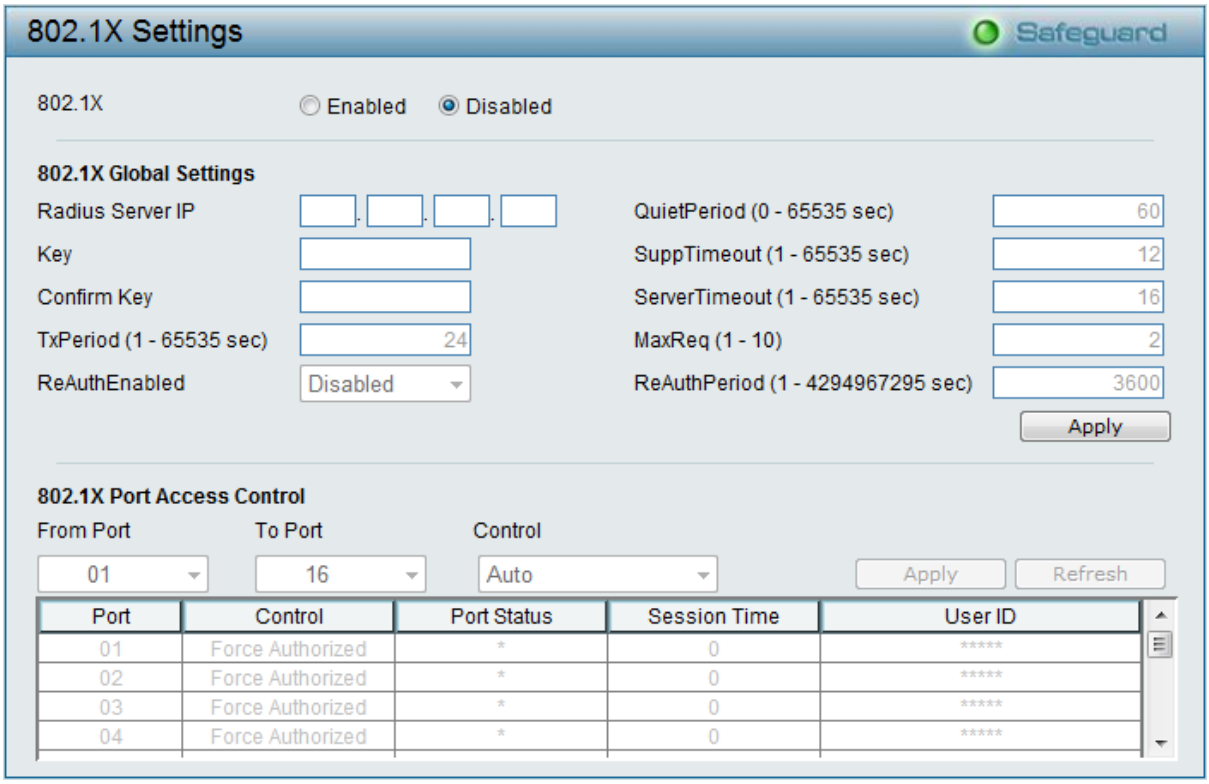


(그림 55) Port Security 설정 화면

스위치 접속 방식을 SSL 인증서 기반으로 동작 시키고자 할 때 사용 합니다.

주의)SSL 기능을 활성화 하면 현재 접속중인 Web 페이지가 비활성화 됩니다.

Security>>802.1X>>802.1X Setting



(그림 56) 802.1X 설정 화면

Radius Server IP: 802.1x 인증을 담당할 서버의 IP 입력 합니다.

Key: 인증 서버에서 사전 등록된 Key 값을 입력 합니다.

Confirm Key: 확인 키를 재입력 합니다.

TxPeriod(1 - 65535): 인증자의 PAE 상태를 위한 시간 입력. 이 값은 클라이언트에게 EAP Request/Identity Packet 전송 주기를 결정 합니다. 기본값 24초

ReAuthEnabled: 재 인증 메시지 전송 설정

QuietPeriod(0 - 65535): 클라이언트와 인증 교환 실패 시 스위치가 quiet 상태로 남아있는 시간 설정 합니다.

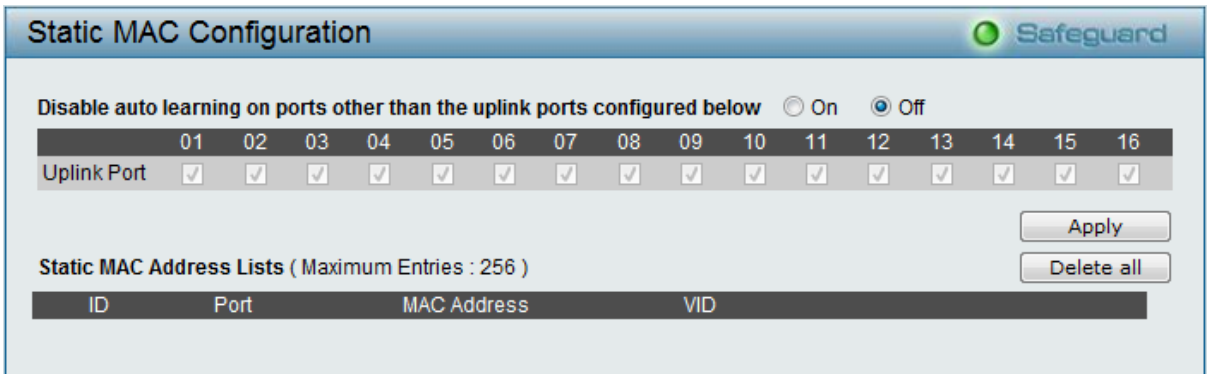
SuppTimeout(1-65535): 인증자와 클라이언트 간의 인증 교환 타임아웃 시간 입니다.

ServerTimeout(1-65535): 스위치가 인증서버에 인증 재전송 요청 전에 클라이언트로부터 응답대기 시간 입니다.

MaxReq(1-10): 인증 세션을 종료하기 전에 스위치가 클라이언트에게 EAP request를 재 요청하는 횟수 입니다.

ReAuthPeriod(1 – 4294967295): 재인증 시간. 재인증이 활성화 된 경우에만 유효합니다.

Security>>MAC Address Table>>Static MAC

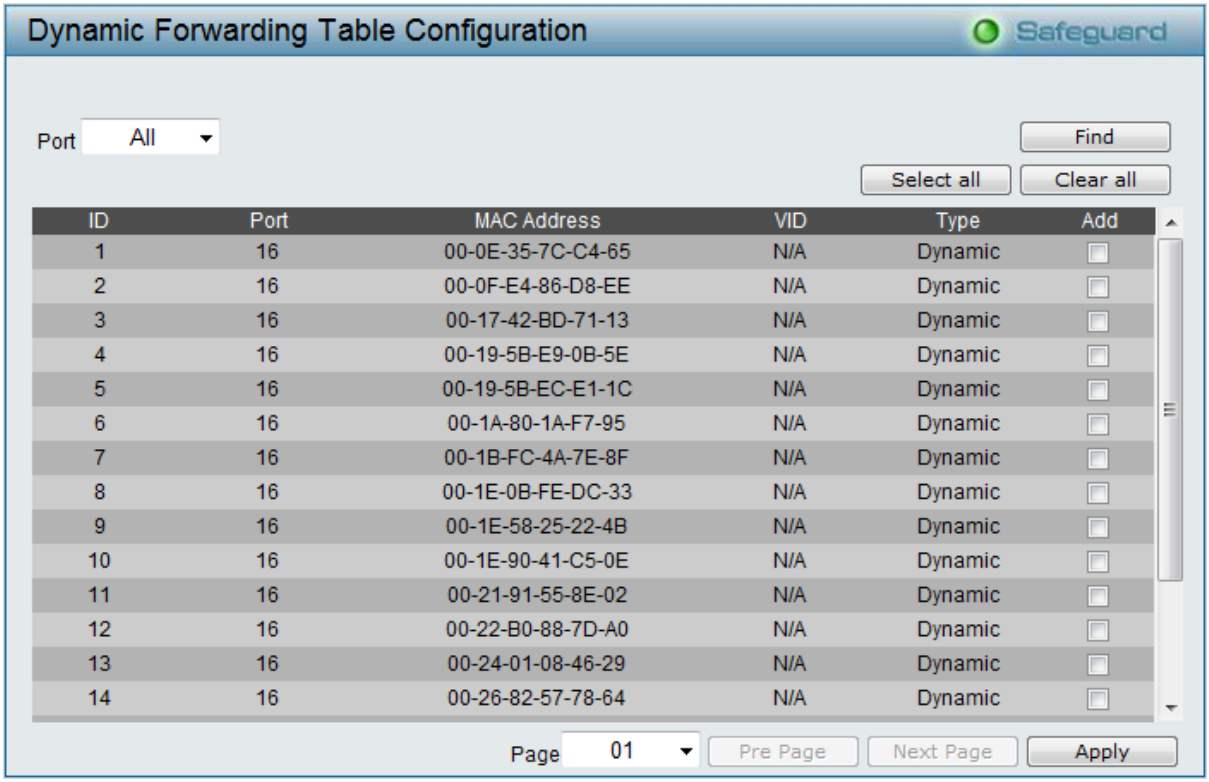


(그림 57) Static MAC 설정 화면

Static MAC 설정 메뉴는 특정 업 링크 포트에서만 MAC 주소를 학습가능 하도록 하는 기능이 있습니다. 이 경우 Gateway 또는 DHCP 서버 와 같은 상단 장비가 직접 연결 되어있는 경우에 사용가능하며 기본적으로 기능이 비활성화 되어 있습니다.

특정 포트에 수동으로 MAC 주소 와 VID를 결합하여 등록할 수 있습니다.(최대 256개)

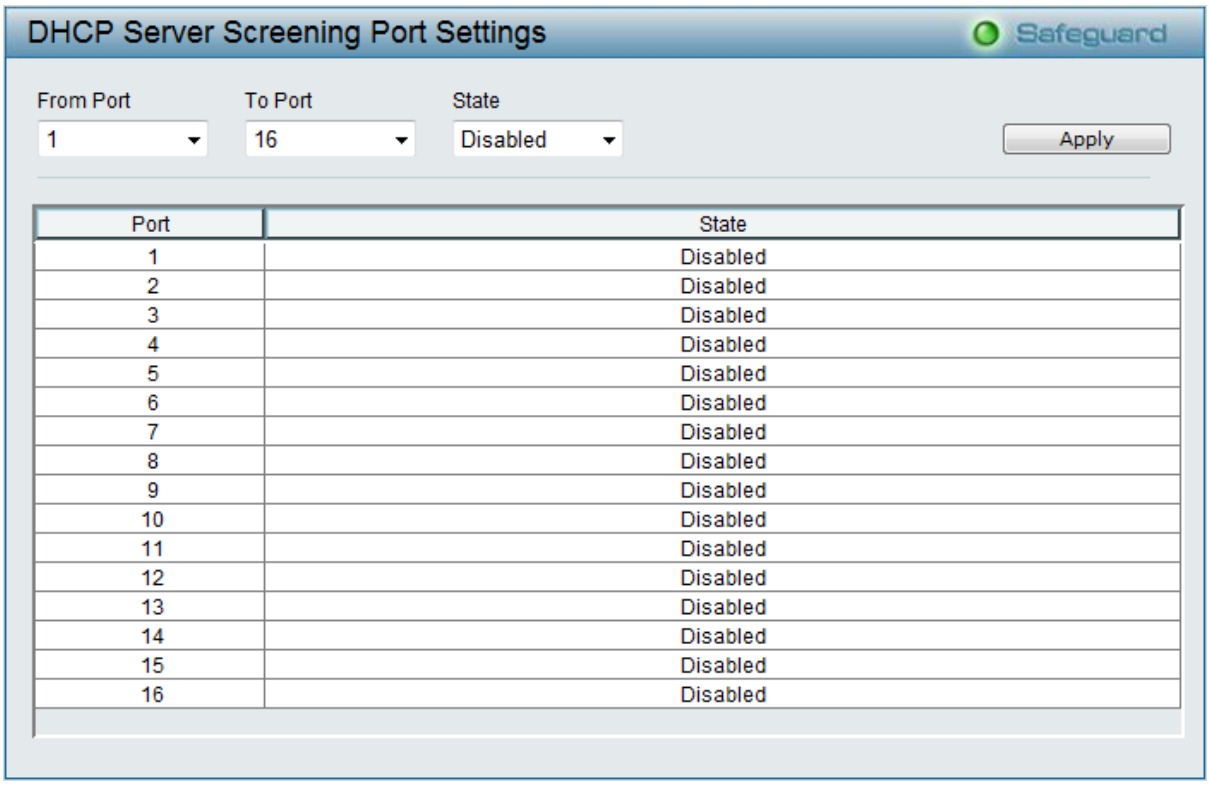
Security>>MAC Address Table>>Dynamic Forwarding Table



(그림 58) Dynamic Forwarding Table 설정 화면

자동으로 학습한 MAC 주소를 검색 할 수 있으며 **Add** 버튼을 눌러 자동으로 학습한 MAC주소를 수동으로 등록할 수도 있습니다.

Security>>DHCP Server Screening

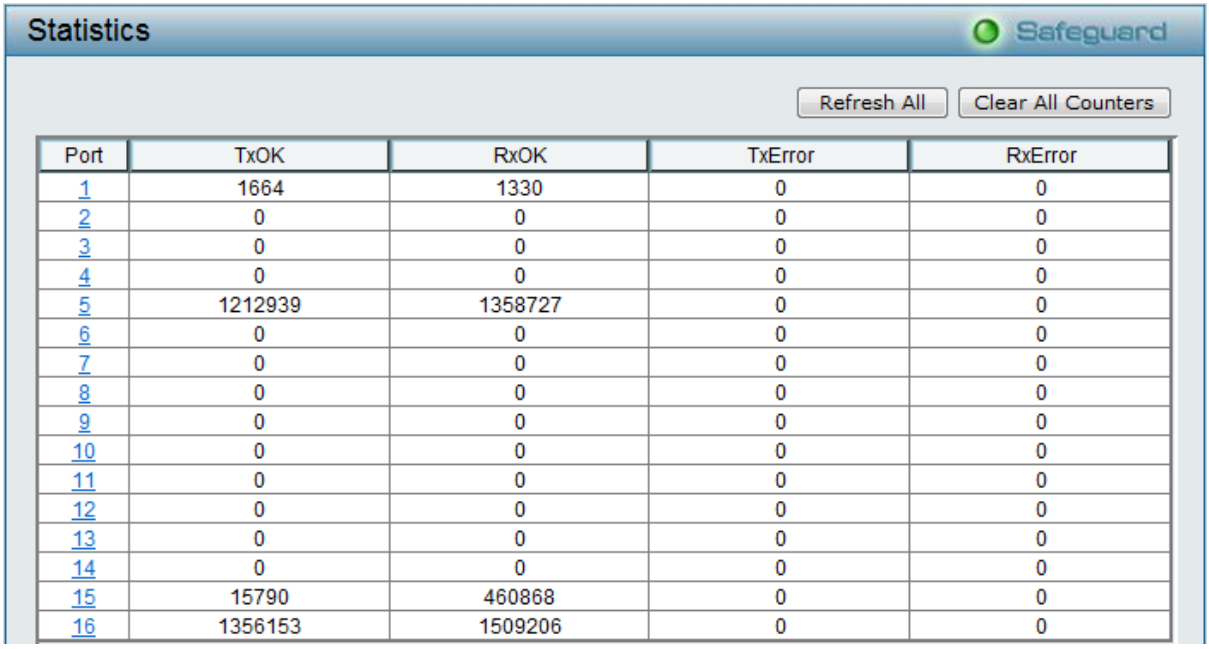


Port	State
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled

(그림 59) DHCP Server Screening 설정 화면

DHCP Server Screening 기능은 비 인가된 DHCP 서버로부터의 DHCP Packet 차단 하는 기능으로 네트워크 상에 복수개의 DHCP 서버가 존재하는 경우 유용하게 사용할 수 있습니다.

Monitoring>>Statistics



Port	TxOK	RxOK	TxError	RxError
1	1664	1330	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	1212939	1358727	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	15790	460868	0	0
16	1356153	1509206	0	0

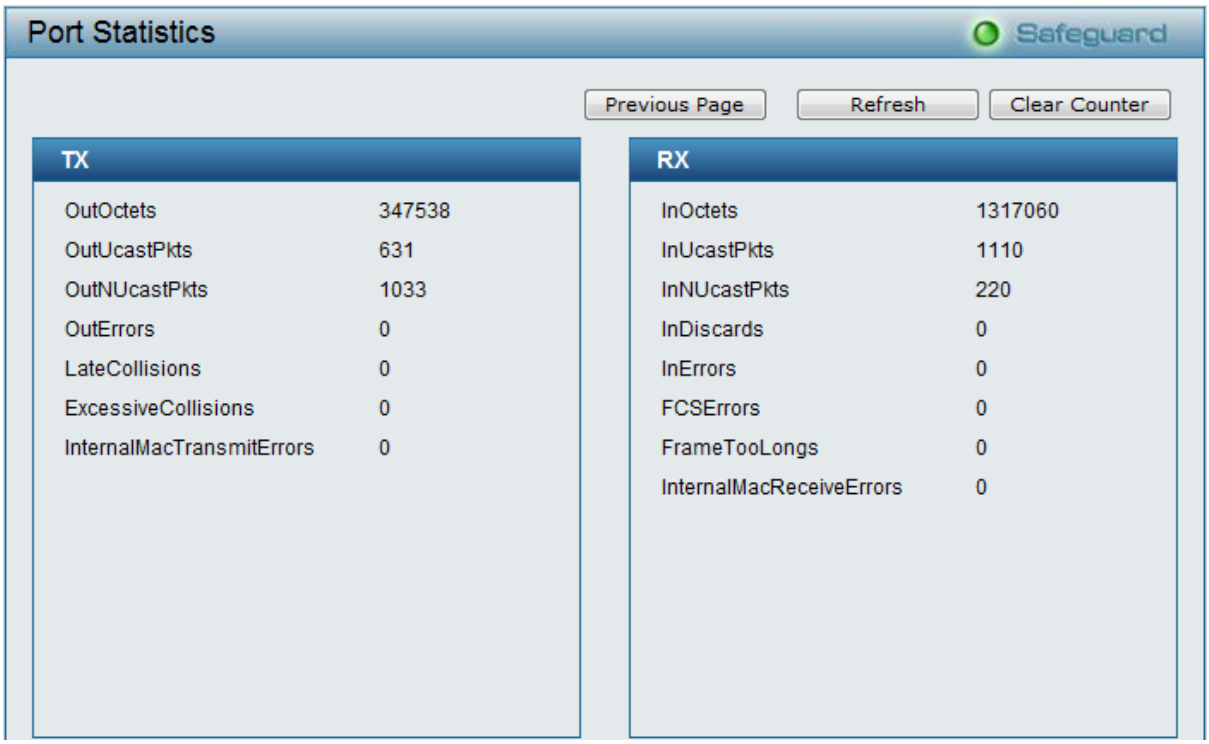
(그림 60) Statistics 화면

TxOK: 정상적인 송신 Traffic 양

RxOK: 정상적인 수신 Traffic 양

TxError: 에러 송신 Traffic 양

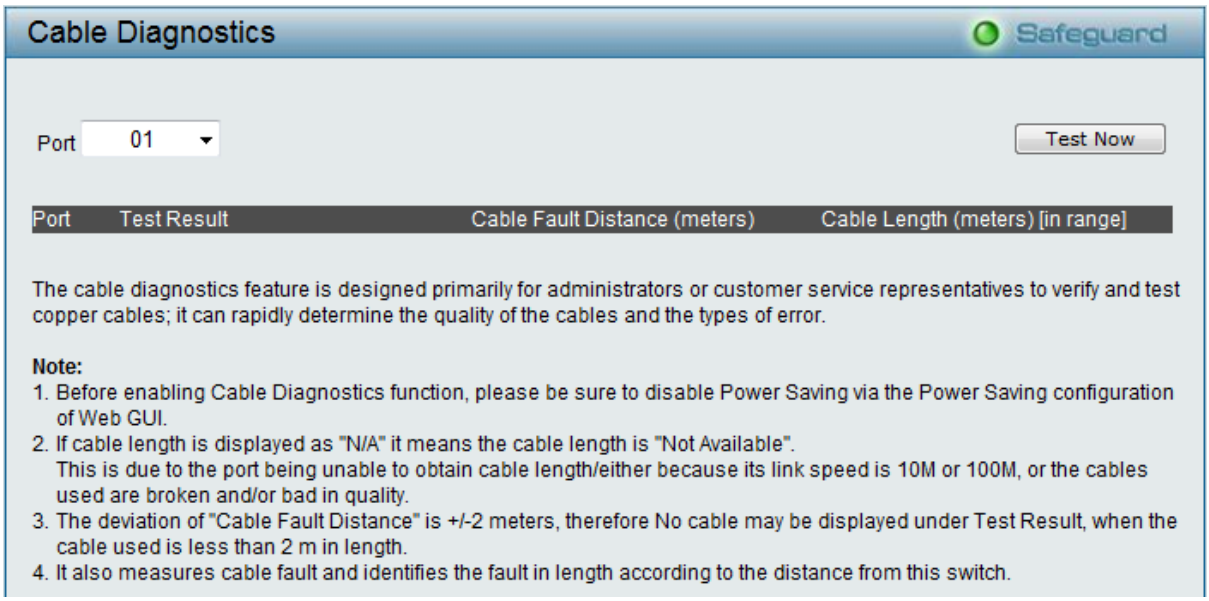
RxError: 에러 수신 Traffic 양



(그림 61) Port Statistics 화면

Port의 번호를 누르게 되면 위 그림화면으로 이동 합니다. 해당 포트의 상세 정보를 확인 할 수 있습니다.

Monitoring>>Diagnostics



(그림 62) Cable Diagnostics 화면

해당 포트를 선택하고 Test Now 버튼을 누르시면 아래 화면과 같이 대략적인 케이블 길이와 장애 여부를 확인 할 수 있는 결과값이 보여 집니다.

Port	Test Result	Cable Fault Distance (meters)	Cable Length (meters) [in range]
5	Pair1:OK Pair2:OK Pair3:OK Pair4:OK	Pair1:N/A Pair2:N/A Pair3:N/A Pair4:N/A	< 50

(그림 63) Cable Test 결과 화면

Monitoring>>Switch History Log

Switch History Log Safeguard

Refresh Clear

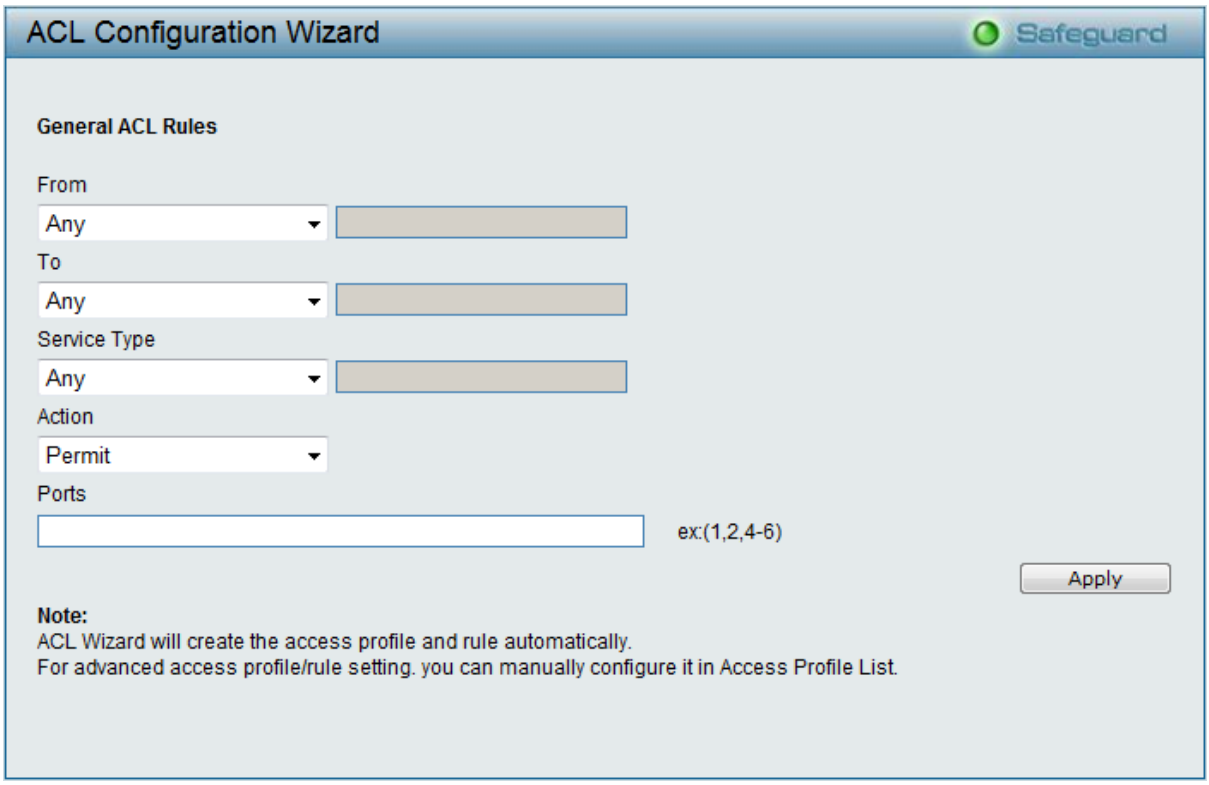
(Maximum Entries : 500)

ID	Time	Log Description	Severity
1	Jan 8 20:29:01 2009	Logout through Web(IP: 192.168.0.146)	info
2	Jan 8 20:29:01 2009	Web session timed out (IP: 192.168.0.146)	info
3	Jan 8 19:58:56 2009	Successful login through Web (IP: 192.168.0.146)	info
4	Jan 8 19:14:21 2009	Successful login through Web (IP: 192.168.0.171)	info
5	Jan 8 17:38:04 2009	Logout through Web(IP: 192.168.0.171)	info
6	Jan 8 17:38:04 2009	Web session timed out (IP: 192.168.0.171)	info
7	Jan 8 17:07:49 2009	Successful login through Web (IP: 192.168.0.171)	info
8	Jan 8 16:38:45 2009	port 1 link down	info
9	Jan 8 16:34:48 2009	Port 1 link up, 1Gbps FULL duplex	info
10	Jan 8 14:53:09 2009	Port 5 link up, 1Gbps FULL duplex	info
11	Jan 8 14:53:07 2009	port 5 link down	info
12	Jan 8 14:52:37 2009	Port 5 link up, 100Mbps FULL duplex	info
13	Jan 8 14:52:35 2009	port 5 link down	info
14	Jan 8 14:52:30 2009	Port 5 link up, 100Mbps FULL duplex	info

(그림 64) Switch History Log 화면

스위치 History Log 를 확인 할 수 있습니다.(버퍼 사이즈 : 500 Line)

ACL>>ACL Configuration Wizard



(그림 65) ACL Configuration Wizard 화면

From: 분류 Traffic 출발지 정의

- **Any**: 모든 Traffic
- **MAC Address**: 특정 MAC 주소. 작성 양식은 XX-XX-XX-XX-XX-XX
- **IP Address**: 특정 IP 주소 또는 대역

To: 분류 Traffic 목적지 정의

- **Any**: 모든 Traffic
- **MAC Address**: 특정 MAC 주소. 작성 양식은 XX-XX-XX-XX-XX-XX
- **IP Address**: 특정 IP 주소 또는 대역

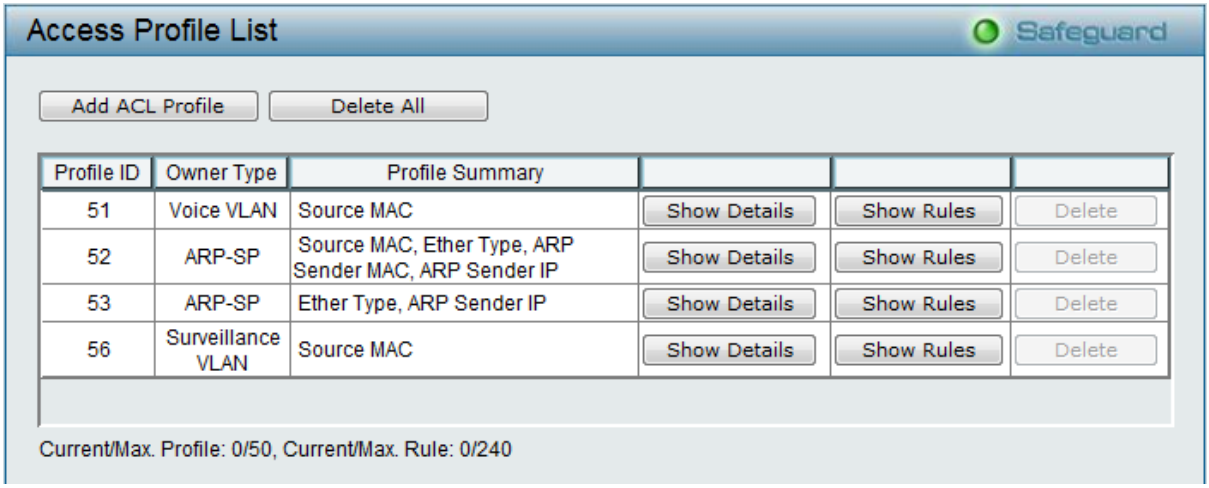
Service Type: 특정 서비스 타입을 정의

- **Any**: 모든 서비스 타입
- **Ether Type**: 특정 Ether Type 별로 Packet Filtering (예: 1501 ~ 65535)
- **ICMP All**: 모든 ICMP Packet
- **IGMP**: IGMP Packet(예: 0~255)
- **TCL All**: 모든 TCP Traffic
- **TCP Source Port**: TCP 출발 포트 정의(예: 0 ~ 65535)
- **TCP Destination Port**: TCP 목적지 포트 정의(예: 0 ~ 65535)
- **UDP All**: 모든 UDP Traffic
- **UDP Source Port**: UDP 출발 포트 정의(예: 0 ~ 65535)
- **UDP Destination Port**: UDP 목적지 포트 정의(예: 0 ~ 65535)

Action: 위에서 정의한 Traffic을 허용 할 것 인지 거부 할 것 인지 선택 합니다.

- **Permit**: 정의한 Traffic 허용
- **Deny**: 정의한 Traffic 거부
- **Ports**: 작성한 ACL Rule을 적용할 포트 지정. Inbound(Packet 수신 시)Rule 로 자동 적용 됩니다.

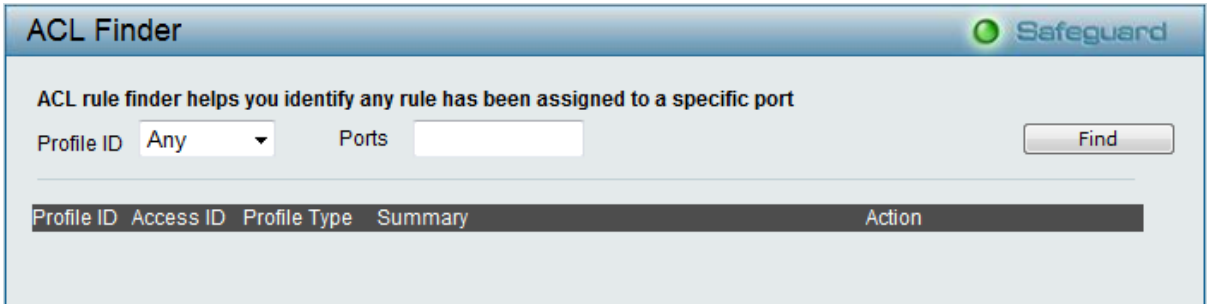
ACL>>ACL Profile List



(그림 66) ACL Profile List 화면

ACL Configuration Wizard에서 작성한 프로파일 List들이 확인 가능하며 상세보기를 통해 Rule 수정 및 삭제가 가능 합니다

ACL>>Finder

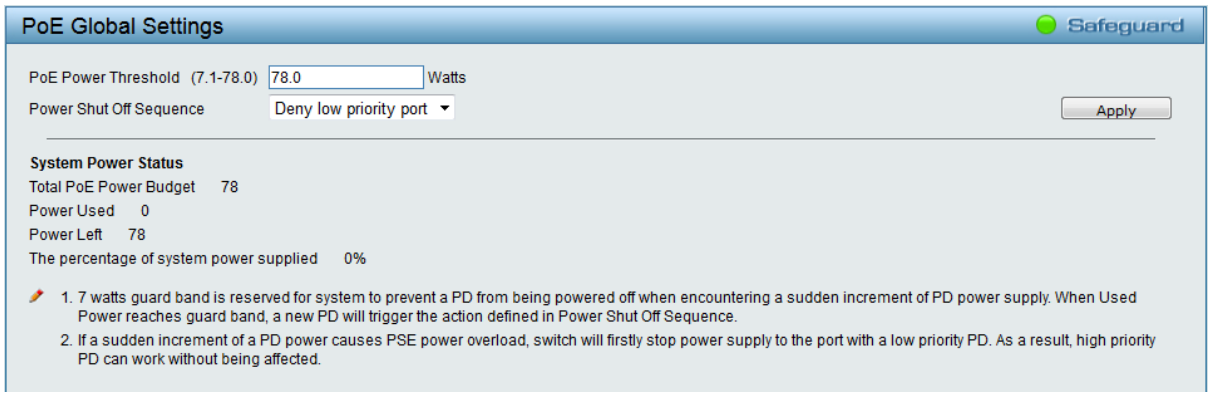


(그림 67) ACL Finder 화면

작성된 ACL Profile을 ID별, 적용 포트 별 검색이 가능하며 검색한 Profile을 삭제 할 수 있습니다.

주의) 한 포트에 복수개의 Profile이 등록되어 있는 경우 Access ID 가 낮은 Rule이 우선입니다.

PoE>>PoE Global Setting



(그림 68) PoE Global Setting 화면

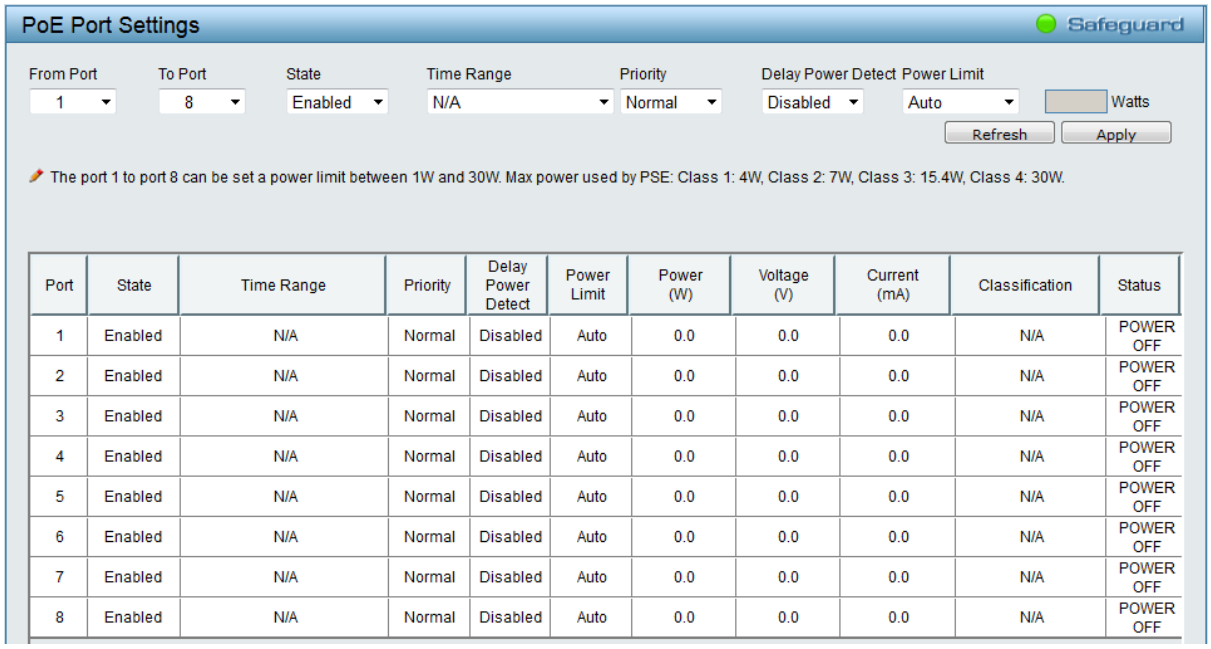
PoE Power Threshold : 수동으로 PoE 시스템 전력 예산을 조절합니다.

Power Shut Off Sequence : 전력 예산을 초과하면 설정에 따라 전력양을 조절합니다.

Deny next port : 전력 예산 초과시 다음 접속을 시도하는 포트를 거부합니다.

Deny low priority port : 전력 예산 초과시 우선순위가 낮은 포트를 거부합니다.

PoE>>PoE Port Setting



Port	State	Time Range	Priority	Delay Power Detect	Power Limit	Power (W)	Voltage (V)	Current (mA)	Classification	Status
1	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
2	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
3	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
4	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
5	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
6	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
7	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
8	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF

(그림 69) PoE Port Setting 화면

PoE 스위치의 포트별 설정을 할 수 있습니다.

From Port~To Port : 설정할 PoE 포트를 범위로 지정합니다.

State : POE 포트의 동작 상태를 결정합니다. Enabled 는 켜짐. Disabled 는 PoE를 끕니다.

Time Range : PoE 포트에 타임 테이블을 동작시킵니다. 타임테이블은 특정 요일이나 특정 시간에 PoE를 끄고 켤 수 있도록 스케쥴을 적용할 수 있습니다.

Priority : 우선순위를 결정합니다.

MeMo