



SAMSUNG TECHWIN

SAMSUNG PoE Switch SPN-12080P / SPN-14240P

상세 매뉴얼



REV. 2.00
Nov 2014

삼성테크윈 (주)

SAMSUNGTECHWIN.CO.,LTD

목차

목차.....	i
개요.....	1
용어 및 사용권.....	1
저작권 및 상표권.....	1
1 제품 소개.....	2
SPN-12080P.....	3
전면.....	3
후면.....	3
SPN-14240P.....	3
전면.....	3
후면.....	3
2 제품 설치.....	3
1 단계 : 포장.....	3
2 단계 : 제품 설치.....	3
책상 혹은 선반에 설치시.....	3
랙 설치시.....	3
3 단계 : 전원 케이블 연결.....	3
정전시 주의사항.....	3
3 초기 설정.....	3
관리를 위한 참고사항.....	3
웹 브라우저를 통한 GUI 접속 관리.....	3
지원되는 웹 브라우저.....	3
스위치와 연결하기.....	3
GUI 로그인.....	3
Smart Wizard.....	3
GUI 관리.....	3
4 세부 설정.....	3
Smart Wizard 설정.....	3
IP Information.....	3
Password.....	3
SNMP.....	3
웹 브라우저 기반 관리.....	3
Tool Bar > Save Menu.....	3
Save Configuration.....	3
Save Log.....	3
Tool Bar > Tool Menu.....	3
Reset.....	3
Reset System.....	3
Reboot Device.....	3
Configuration Backup and Restore.....	3
Firmware Backup and Upgrade.....	3
Tool Bar > Smart Wizard.....	3
Function Tree.....	3
Device Information.....	3
System > System Settings.....	3

System > IPv6 System Settings	3
System > IPv6 Route Settings	3
System > IPv6 Neighbor Settings	3
System > Password.....	3
System > Port Settings.....	3
System > DHCP Auto Configuration	3
System > SysLog Host.....	3
System > Time Profile	3
System > Power Saving	3
System > IEEE802.3az EEE Settings	3
VLAN > 802.1Q VLAN.....	3
VLAN > 802.1Q VLAN PVID	3
VLAN > 802.1Q Management VLAN.....	3
VLAN > Voice VLAN > Voice VLAN Global Settings	3
VLAN > Voice VLAN > Voice VLAN Port Settings	3
VLAN > Voice VLAN > Voice Device List.....	3
VLAN > Auto Surveillance VLAN Settings	3
L2 Functions > Jumbo Frame	3
L2 Functions > Port Mirroring.....	3
L2 Functions > Loopback Detection.....	3
L2 Functions > MAC Address Table > Static MAC	3
L2 Functions > MAC Address Table > Dynamic Forwarding Table	3
L2 Functions > Spanning Tree > STP Global Settings	3
L2 Functions > Spanning Tree > STP Port Settings	3
L2 Functions > Link Aggregation > Port Trunking.....	3
L2 Functions > Link Aggregation > LACP Port Settings	3
L2 Functions > Multicast > IGMP Snooping	3
L2 Functions > Multicast > Multicast Forwarding.....	3
L2 Functions > Multicast > Multicast Filtering Mode	3
L2 Functions > SNTP > Time Settings	3
L2 Functions > SNTP > TimeZone Settings.....	3
L2 Functions > LLDP > LLDP Global Settings	3
L2 Functions > LLDP > LLDP MED Settings	3
L2 Functions > LLDP > LLDP Port Settings.....	3
L2 Functions > LLDP > 802.1 Extension TLV	3
L2 Functions > LLDP > 802.3 Extension TLV	3
L2 Functions > LLDP > LLDP Management Address Settings	3
L2 Functions > LLDP > LLDP Management Address Table	3
L2 Functions > LLDP > LLDP Local Port Table	3
L2 Functions > LLDP > LLDP Remote Port Table	3
L2 Functions > LLDP > LLDP Statistics	3
QoS > Bandwidth Control.....	3
QoS > 802.1p/DSCP/ToS.....	3
QoS > IPv6 Traffic Class Priority Settings.....	3
QoS > TCP/UDP Port Priority Settings	3
Security > Trusted Host.....	3
Security > Port Security.....	3
Security > Traffic Segmentation	3
Security > Safeguard Engine.....	3

Security > Storm Control	3
Security > ARP Spoofing Prevention	3
Security > DHCP Server Screening	3
Security > SSL Settings.....	3
Security > Smart Binding > Smart Binding Settings.....	3
Security > Smart Binding > Smart Binding	3
Security > Smart Binding > White List.....	3
Security > Smart Binding > Black List	3
AAA > 802.1X > 802.1X Settings	3
ACL > ACL Wizard	3
ACL > ACL Profile List.....	3
ACL > ACL Finder	3
PoE > PoE Global Settings	3
PoE > PoE Port Settings	3
SNMP > Trap to SmartConsole Utility	3
SNMP > SNMP > SNMP Global Settings	3
SNMP > SNMP > SNMP User	3
SNMP > SNMP > SNMP Group Table	3
SNMP > SNMP > SNMP View	3
SNMP > SNMP > SNMP Community.....	3
SNMP > SNMP > SNMP Host.....	3
SNMP > SNMP > SNMP Engine ID	3
SNMP > RMON > RMON Global Settings	3
SNMP > RMON > RMON Statistics	3
SNMP > RMON > RMON History.....	3
SNMP > RMON > RMON Alarm Settings	3
SNMP > RMON > RMON Event.....	3
Monitoring > Port Statistics.....	3
Monitoring > Cable Diagnostics	3
Monitoring > System Log.....	3
6 Command Line Interface.....	3
TELNET 으로 스위치에 접속하기	3
Telnet 로그인	3
CLI 명령어	3
?.....	3
download	3
upload	3
config ipif system	3
logout.....	3
ping	3
ping6.....	3
reboot	3
reset config	3
show ipif.....	3
show switch	3
config account admin password	3
save	3
debug info.....	3
Appendix A - 제품사양	3

Hardware Specifications	3
Key Components / Performance	3
Port Functions	3
Physical & Environment	3
Emission (EMI) Certifications	3
Safety Certifications.....	3
Features	3
L2 Features	3
VLAN	3
QoS (Quality of Service).....	3
Security.....	3
OAM	3
Management.....	3
Green Technology	3

개요

삼성 PoE 스위치 SPN-12080P/SPN-14240P 의 설치방법과 GUI 를 이용한 단계별 설정방법입니다.



참고: 본 스위치 장비의 구성품, 네트워크 구성도 및 하드웨어 사양은 해당 모델 전용의 제품 사양서 및 기술사양서를 참고하여 주십시오.

본 매뉴얼은 아래와 같이 3 개의 부분으로 구성되어 있습니다.

1. 제품 설치: 제품의 단계별 설치 방법입니다.
2. 초기 설정: 제품의 운용을 위한 초기 설정 방법입니다.
3. 세부 설정: 각 기능에 대한 설명 및 설정 방법입니다.

용어 및 사용권

본 매뉴얼에 사용된 “Switch” (첫글자 대문자) 는 PoE 스위치를 의미하며 “switch” (첫글자 소문자) 는 다른 일반 스위치 장비를 의미합니다. 일부 기술서에는 “switch”, “bridge”, “switching hubs” 라는 용어가 사용되기도 하며, 모두 일반 스위치 장비를 의미합니다.



참고

제품을 효율적으로 운용할 수 있는 정보입니다.



주의

제품의 손상 혹은 사용자의 부상이 발생할 수 있는 주의사항입니다.

저작권 및 상표권

본 문서상의 정보는 공지없이 일부 변경될 수 있습니다.

© 2012 SAMSUNG TECHWIN CO., LTD. All rights reserved.

SAMSUNG TECHWIN CO., LTD. 의 승인없이 본 문서의 재배포를 금지합니다.

상표권

SAMSUNG 과 SAMSUNG 로고는 SAMSUNG TECHWIN CO., LTD.의 상표입니다.

Microsoft 와 Windows 는 Microsoft Corporation 에 등록된 상표입니다.

1 제품 소개

SAMSUNG PoE 스위치 제품을 구입해 주신 고객님께 감사드립니다.

본 PoE 스위치는 간단하게 운용할 수 있는 **Plug and Play** 방식으로 중소규모 네트워크에 적합하게 설계되어 있습니다. 표준 랙(Rack)에 장착할 수 있으며, 전면 LED를 통하여 쉽게 동작여부 및 이상여부를 확인하실 수 있습니다. 기능상으로는 네트워크 보안, 트래픽 분산처리, QoS 등을 갖추고 있으며, GUI 방식으로 쉽게 설정/운용하실 수 있습니다.

다양한 포트 구성

SPN-12080P는 8개의 기가비트 PoE 포트와 2개의 SFP 콤보 포트에 구성되어 있으며, PoE 포트는 모두 802.3af/at 규격을 모두 지원합니다. SPN-14240P는 24개의 기가비트 PoE 포트와 4개의 SFP 포트에 구성되어 있으며, 1~4번 포트만 802.3af/at 규격을 모두 지원하고 5~24번 포트는 802.3af 규격만 지원합니다.

- IEEE 802.3af : 최대 15.4W / 전압범위 37V ~ 57V / 최대 전류 350mA 지원
- IEEE 802.3at : 최대 30.0W / 전압범위 42.5V ~ 57V / 최대 전류 600mA 지원

전력소비 절감(Green Technology)

본 제품은 성능의 저하없이 전력소비를 절감할 수 있는 친환경 제품으로 다음과 같은 전력 절감 기술이 적용되어 있습니다.

- 사용되지 않은 포트에 대해 전력 차단
- 일부 LED 표시등 끄기
- 이더넷 케이블 길이에 따라 전력 사용량 조절
- 스케줄을 적용하여 PoE 기능 동작 제어

L2 기능 지원

IGMP Snooping, Port mirroring, Spanning Tree, 802.3ad LACP, Loopback Detection 등 L2 기능을 일부 지원합니다.

트래픽 분산, QoS, Auto Surveillance VLAN

802.1Q VLAN 표준을 지원하여 보안과 성능을 향상시킬 수 있으며, 802.1p priority queues를 지원하여 지정한 트래픽을 효과적으로 전송할 수 있습니다. Auto Surveillance VLAN은 지정한 IP 주소로부터 수신된 데이터의 종류(영상 등)를 자동으로 감지하여 할당한 VLAN으로 최우선하여 전송하는 기능입니다.

네트워크 보안

Safeguard Engine은 Virus 공격에 의한 Traffic Flooding을 차단하여 장비를 보호하는 기능입니다.

802.1X port-based authentication을 지원함으로써 외부 RADIUS 서버와 연동할 수 있으며, IP 및 MAC ACL 기능을 통하여 허용되지 않은 사용자의 네트워크 접속을 차단할 수 있습니다. Storm Control은 비정상적인 트래픽 유입으로 인하여 발생할 수 있는 네트워크 장애발생을 방지할 수 있습니다.

다양한 관리방식 지원

GUI 방식으로 관리자가 웹 브라우저를 이용하여 스위치의 모든 기능을 쉽게 설정할 수 있으며, TELNET으로 접속하여 IP 주소 변경, 초기화, 관리자 비밀번호 설정, 재부팅, 펌웨어 업그레이드 등 일부 기능은 CLI 방식으로 설정 진행하실 수 있습니다.

SNMP MIB을 이용하여 스위치의 상태, 비정상적인 동작등의 정보를 불러올 수 있습니다.

SPN-12080P

8 포트 10/100/1000Mbps, 2 포트 1000Base-T/SFP 콤보 지원

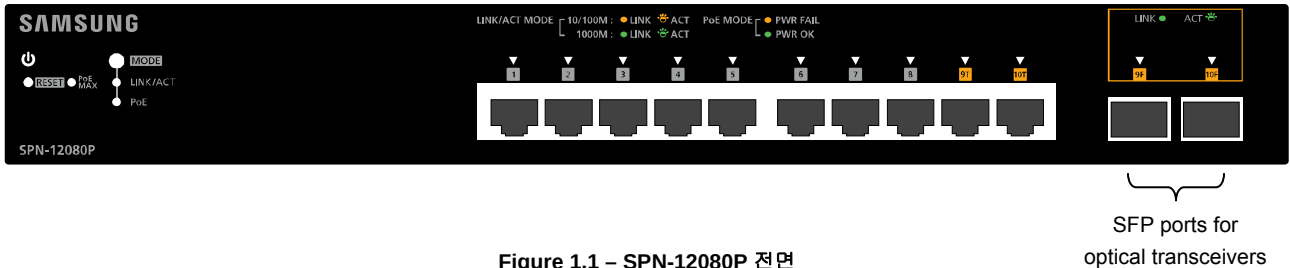
전면

Figure 1.1 – SPN-12080P 전면

Power LED : 제품에 전원을 연결한 경우 켜집니다.

PoE Max: PoE 설정 메뉴에서 설정한 PoE 용량이 모두 사용된 경우 켜집니다. (기본값 : 78W)

Reset: 5초간 눌러 제품을 초기화할 수 있습니다. 모든 설정이 공장 출하시 값으로 변경됩니다.

Mode: 포트별 LED 동작을 Link/Act 상태표시 또는 PoE 상태표시 방식으로 변경합니다.

Port Link/Act/Speed LED (1-8, 9T, 10T 9F, 10F): Link/Act 모드인 경우 케이블이 정상적으로 연결된 포트의 LED 가 켜지며, 데이터가 전송시 점멸합니다. 주황색은 10Mbps/100Mbps 로 동작함을 의미하며, 초록색은 1000Mbps 로 동작함을 의미합니다.

**주의**

MiniGBIC 포트에는 UL 에 등록된 광트랜시버 제품을 사용하여 주십시오. (Laser Class I. 3.3Vdc)

Port PoE LED (1-8): PoE 모드인 경우, PoE 장비(PD)가 연결되어 있는 포트의 LED 가 켜집니다.

후면

Figure 1.2 – SPN-12080P 후면

Power: AC 전원 케이블을 연결합니다.

SPN-14240P

24 포트 10/100/1000Mbps, 4 포트 SFP 지원

전면

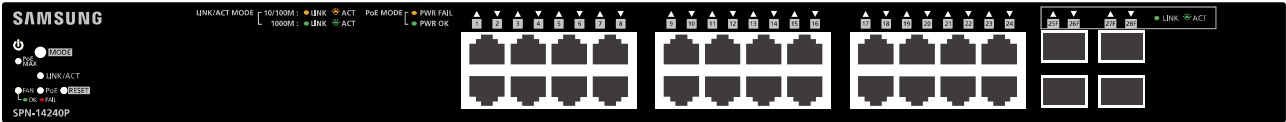


Figure 2.7 – SPN-14240P 전면

Power LED : 제품에 전원을 연결한 경우 켜집니다.

PoE Max: PoE 설정 메뉴에서 설정한 PoE 용량이 모두 사용된 경우 켜집니다. (기본값 : 185W)

Reset: 5초간 눌러 제품을 초기화할 수 있습니다. 모든 설정이 공장 출하시 값으로 변경됩니다.

Mode: 포트별 LED 동작을 Link/Act 상태표시 또는 PoE 상태표시 방식으로 변경합니다.

Port Link/Act/Speed LED (1-24, 25F, 26F, 27F, 28F): Link/Act 모드인 경우 케이블이 정상적으로 연결된 포트의 LED 가 켜지며, 데이터가 전송시 점멸합니다. 주황색은 10Mbps/100Mbps 로 동작함을 의미하며, 녹색은 1000Mbps 로 동작함을 의미합니다.

Fan: 제품의 팬동작 상태를 표시합니다. (녹색 – 정상 / 적색 – 이상발생)



주의

MiniGBIC 포트에는 UL 에 등록된 광트랜시버 제품을 사용하여 주십시오. (Laser Class I. 3.3Vdc)

Port PoE LED (1-24): PoE 모드인 경우, PoE 장비(PD)가 연결되어 있는 포트의 LED 가 켜집니다.

SPN-14240P 는 1~4 번 포트만 IEEE 802.3af/at(최대 30W) 를 지원하고 5~24 번 포트는 IEEE 802.3af (최대 15.4W) 만 지원합니다.

후면



Figure 1.8 – SPN-14240P 후면

Power: AC 전원 케이블을 연결합니다.

2 제품 설치

제품 구성품 및 설치방법입니다.

1 단계 : 포장

포장을 주의하여 개봉하여 주시고, 아래의 구성품 중 누락되거나 손상된 부분은 없는지 확인합니다.
누락되거나 손상된 품목이 있으시면 해당 판매점에 교체를 요청하여 주시길 바랍니다.

- PoE 스위치 (1 대)
- AC 전원 케이블 (1 개)
- 미끄럼 방지 고무받침 (4 개)
- 고정나사 및 랙마운트 브라켓 (2 개)
- 설치 가이드 (1 부)
- 매뉴얼 CD (1 개)

2 단계 : 제품 설치

안전한 제품 설치 및 운용을 위하여 다음 사항을 참고하여 주십시오.

- 전원 케이블에 손상된 부분이 없는 확인하여 주십시오.
- 제품의 주변으로 발열을 막기 위한 통풍 공간이 충분하게 확보되어 있는지 확인하여 주십시오.
- 제품 위에 무거운 제품을 올려두지 마십시오.

책상 혹은 선반에 설치시

동봉된 미끄럼 방지용 고무받침을 제품하단 네모서리에 부착합니다. 제품의 주변으로는 충분한 통풍공간을 확보하여 주십시오.

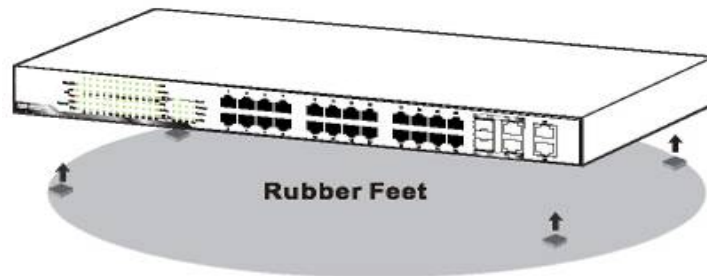


Figure 2.1 – 고무받침 부착

랙 설치시

EIA 표준 19 인치 랙에 장착하실 수 있습니다. 랙마운트 브라켓을 제품의 측면에 동봉된 나사를 이용하여 부착합니다.

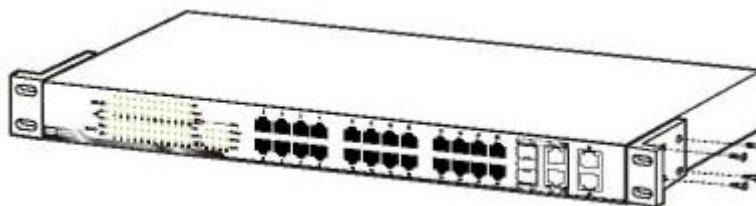


Figure 2.2 – 측면에 랙마운트 브라켓 부착

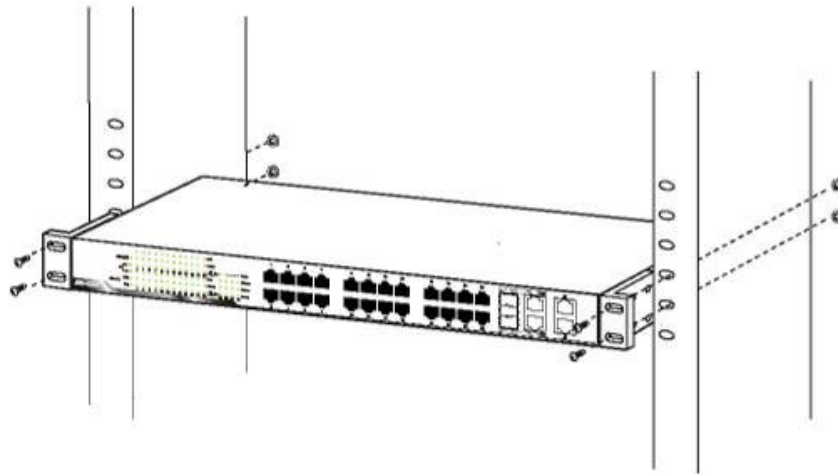


Figure 2.3 - 랙마운트

설치시 다음 사항을 주의하여 주십시오.

- A) 장비간 간격 확보 - 랙에 설치된 장비간의 간격이 좁을 경우, 장비마다 발생하는 열로 인하여 동작 환경 기준치 온도보다 상회할 수 있습니다. 1U 정도의 간격을 확보하여 주시길 권장드립니다.
- B) 통풍 확보 - 안정적인 동작을 위하여 공기의 흐름이 원활하게 될 수 있도록 설치하여 주십시오.
- C) 하중 배분 - 장비들의 무게를 점검하여 편중되지 않도록 주의하여 주십시오.
- D) 과부하 주의 - 장비들의 소비 전력을 점검하여 전원 공급 장치에 과부하가 걸리지 않도록 주의하여 주십시오.
- E) 접지 - 장비의 접지가 유지되어 있는지 확인하여 주십시오.

3 단계 : 전원 케이블 연결

전원케이블을 연결합니다.

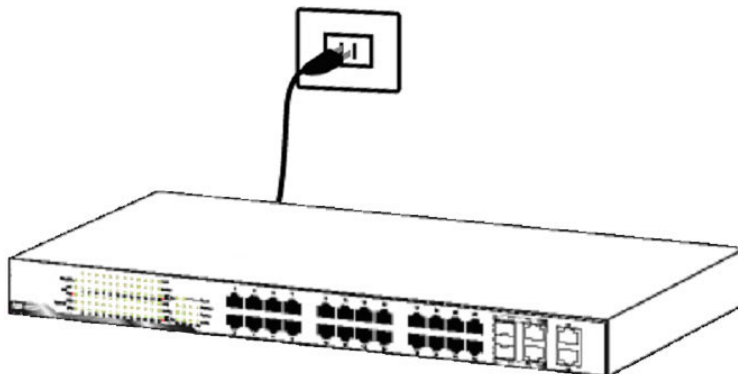


Figure 2.4 - 전원케이블 연결

정전시 주의사항

정전시에는 제품의 전원케이블을 분리하여 주시고, 전원이 재개되면 다시 연결하여 주십시오.

3 초기 설정

제품의 초기 설정을 진행하기 위한 방법입니다.

관리를 위한 참고사항

본 스위치 장비는 모든 포트에서 GUI에 접속하여 설정하실 수 있습니다.

여러 대의 스위치 장비를 하나의 네트워크로 설치하게 될 경우, 각각의 장비마다 고유의 IP 주소를 설정하여 주십시오. 또한, 스위치를 관리하고자 하는 PC는 해당 스위치와 동일한 네트워크 주소로 설정되어야 합니다. 본 스위치는 최대 4명까지 동시에 관리자 페이지(GUI)로 접속할 수 있습니다.

웹 브라우저를 통한 GUI 접속 관리

제품의 설치가 완료된 후, 웹 브라우저를 이용하여 내부설정변경, 상태 모니터링 등을 하실 수 있습니다.

지원되는 웹 브라우저

- Internet Explorer 6 이상
- Netscape 8 이상
- Firefox 3.0 이상
- Chrome 5.0 이상
- Safari 4.0 이상
- Opera 10 이상

스위치와 연결하기

필요한 장비

1. RJ-45 이더넷 연결이 지원되는 PC
2. 표준 이더넷 케이블

표준 이더넷 케이블을 이용하여 PC를 스위치 포트에 연결합니다.

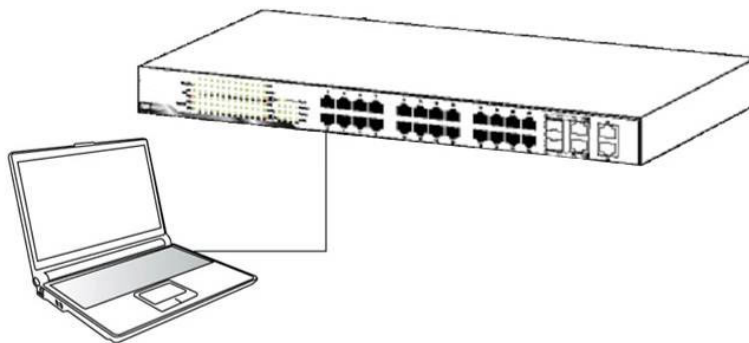


Figure 3.1 – PC 연결

GUI 로그인

GUI에 접속하기 위해서는 PC의 IP 주소가 스위치와 동일한 네트워크 주소로 설정되어 있어야 합니다. 예를 들어, 스위치의 IP 주소가 **10.90.90.90** 이라고 할 경우, PC의 IP 주소는 **10.x.y.z** (x/y: 0~254 사이의 숫자, z: 1~254 사이의 숫자)가 되어야 하며, 서브넷 마스크는 **255.0.0.0** 이 되어야 합니다. 설정을 완료한 후, 웹 브라우저를 실행하고 인터넷 주소란에 **10.90.90.90** 을 입력/이동(엔터) 합니다.

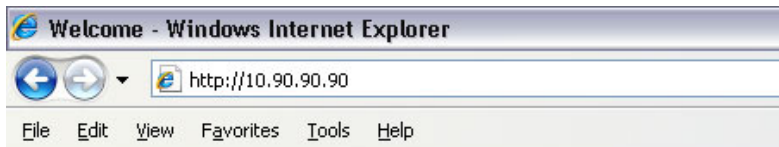


Figure 3.2 – 인터넷 주소란에 10.90.90.90 입력

**참고**

본 스위치의 기본 IP 주소는 10.90.90.90 이며, 서브넷 마스크는 255.0.0.0 입니다.

다음과 같은 로그인 창이 표시됩니다. 설정된 비밀번호를 입력하고 [OK] 버튼을 클릭합니다.

필요에 따라 설정언어를 변경하실 수 있으며, 지원되는 언어는 아래와 같습니다.

English, Chinese, German, Spanish, French, Italian, Portuguese, Japanese, Russian

비밀번호 **admin** / 언어 **English** 가 기본값으로 설정되어 있습니다.



Figure 3.3 – 로그인

Smart Wizard

로그인 후, Smart Wizard 를 이용하여 기본 설정을 진행하실 수 있습니다.

Smart Wizard 설정 내용은 본 매뉴얼의 [4 장. 세부 설정]을 참고하여 주십시오.

GUI 관리

Smart Wizard 에서 **Exit** 버튼을 클릭하여 세부설정을 하실 수 있습니다.

세부 설정 내용은 [4 장. 세부 설정]을 참고하여 주십시오.

4 세부 설정

GUI 를 이용하여 설정할 수 있는 스위치의 각 기능과 설정 방법입니다.

Smart Wizard 설정

로그인 하신 후, Smart Wizard 를 통해 스위치의 기본 설정을 진행합니다.

Smart Wizard 에서 변경할 설정이 없으신 경우, **Exit** 버튼을 클릭하여 GUI 로 이동하실 수 있습니다.

다음 접속시, Smart Wizard 가 자동 실행됨을 차단하시려면 **Ignore the Wizard next time** 항목을 체크하여 주십시오.

Smart Wizard 는 IP Information ▶ Access Password ▶ SNMP 의 3 단계로 진행됩니다.

IP Information

Static : 스위치의 IP 주소를 고정값으로 설정합니다. IP Address, Netmask, Gateway 를 모두 입력합니다.

DHCP/ BOOTP : 스위치의 IP 주소를 해당 서버로부터 자동으로 할당받습니다.

IPv6 로 구성하시려면, Smart Wizard 를 취소하고 [System > IPv6 System Settings](#) 에서 설정하여 주십시오.

Figure 5.1 – IP Information in Smart Wizard



참고

Smart Wizard 는 IPv4 네트워크 설정만 지원합니다.

Password

Password 란과 **Confirm Password** 란에 관리자 비밀번호로 사용할 값을 입력하고 **Next** 버튼을 클릭합니다.

Welcome to Smart Wizard

Step 2 of 3: Set up the password for authorized access.

Password

Password: Confirm Password:

☐ Ignore the wizard next time

Exit Back Next

Figure 5.2 – Password in Smart Wizard

SNMP

SNMP 사용여부를 설정하고 **Apply** 버튼을 클릭합니다.

Welcome to Smart Wizard

Step 3 of 3: Enable SNMP for management.

SNMP

SNMP: ☐ Enabled ☒ Disabled

☐ Ignore the wizard next time

Exit Back Next Apply

Figure 5.3 – SNMP in Smart Wizard

**참고**

스위치의 IP 주소를 변경하고 **Apply** 버튼을 클릭한 경우에는 설정화면의 접속이 끊어집니다. PC의 IP 주소를 다시 한번 스위치의 IP 주소와 동일 네트워크 대역으로 변경한 후 재접속하여 주십시오.

웹브라우저 기반 관리

Smart Wizard 에서 **Exit** 버튼을 클릭하면 다음과 같은 세부 설정 화면이 표시됩니다.

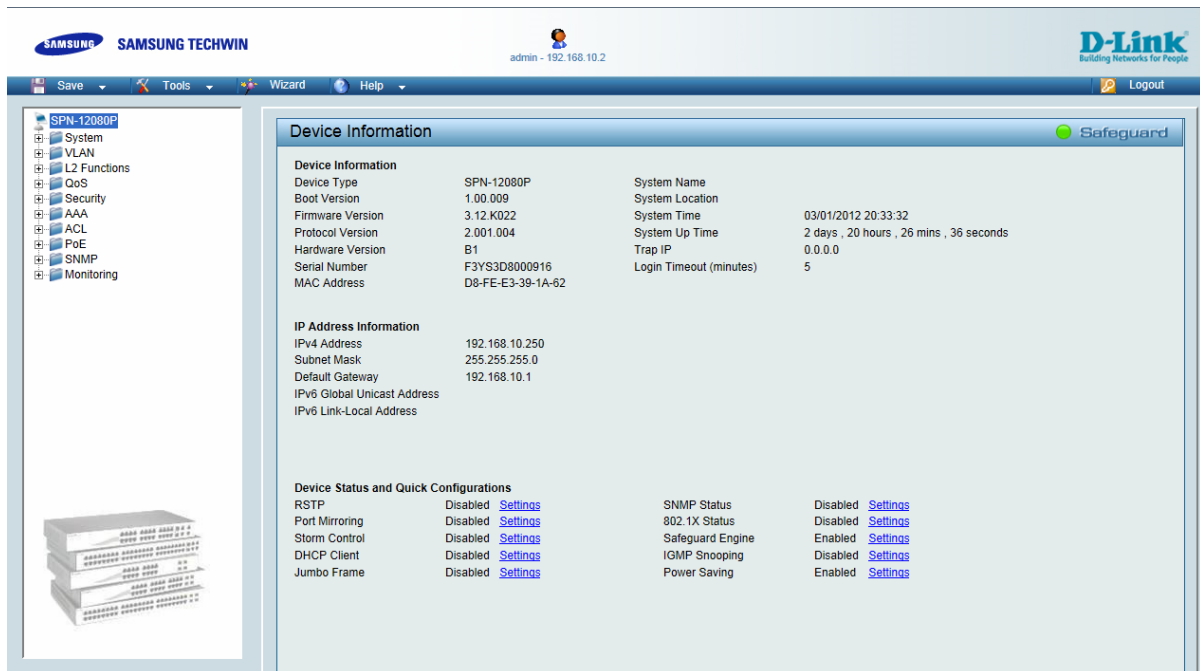


Figure 5.5 – 웹브라우저 기반 관리

상기의 화면을 **Web-based Management** 라고 합니다.(GUI 설정, 관리자 페이지, 웹브라우저 기반 관리 등) 상단의 **Tool Bar**, 왼쪽의 **Function Tree**, 중앙의 **Main Configuration** 로 구성됩니다.

Tool Bar 는 펌웨어 및 설정파일 관리와 같은 기본 유틸리티 기능을 제공합니다.

Function Tree 에서 변경하고자 하는 기능을 선택하고 **Main Configuration** 에서 세부 설정을 진행합니다. **Function Tree** 의 최상단에 있는 제품 모델명을 클릭하면 현재 스위치의 상태를 확인하실 수 있습니다.

최상단 배너 이미지의 중앙에는 현재 설정화면에 접속한 사용자 이름과 IP 주소가 표시됩니다.

Logout 버튼을 클릭하여, 접속을 종료하실 수 있습니다.



참고

Logout 버튼을 클릭하지 않고 웹브라우저를 종료한 경우, 비정상 종료로 간주되어 로그인 연결이 일정시간 유지됩니다.

Tool Bar > Save Menu

설정값을 스위치의 메모리상에 저장하고 로그를 파일로 저장합니다.

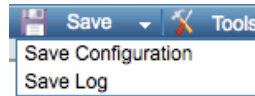


Figure 5.6 – Save Menu

Save Configuration

스위치의 설정을 변경한 후, 해당 설정값을 스위치 내의 메모리에 저장합니다.

스위치의 전원을 껐다 켜더라도 해당 설정이 유지됩니다.

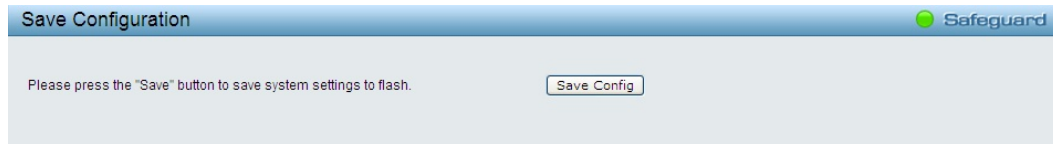


Figure 5.7 – Save Configuration

Save Log

로그를 파일로 저장합니다.

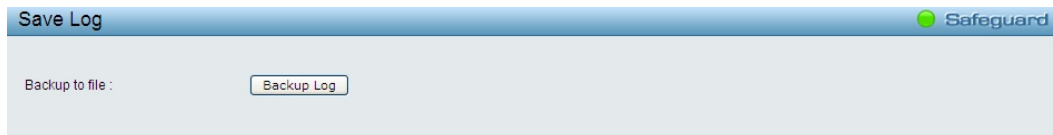


Figure 5.8 – Save Log

Tool Bar > Tool Menu

스위치 설정 초기화, 스위치 재부팅, 펌웨어 백업 및 업그레이드, 설정값 백업 및 복구 기능을 진행합니다.

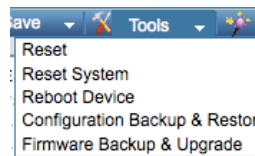


Figure 5.9 – Tool Menu

Reset

스위치의 IP 주소를 제외한 다른 모든 설정값을 초기화합니다.

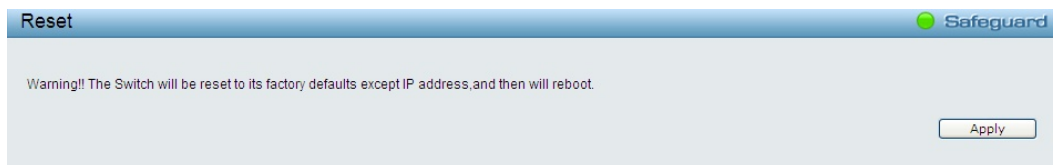


Figure 5.10 – Tool Menu > Reset

Reset System

모든 스위치 설정값을 초기화하여 공장 출하시 상태로 변경합니다.

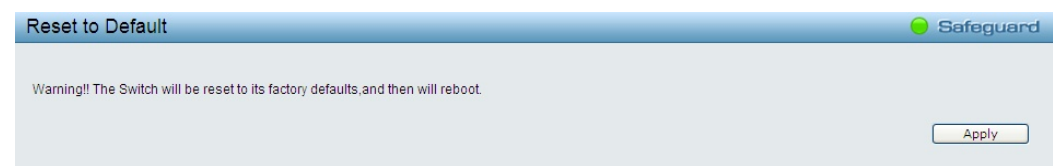


Figure 5.11 – Tool Menu > Reset System

Reboot Device

스위치를 재부팅합니다. 앞서 설명한 [Save Configuration] 이 적용된 설정값은 유지됩니다.

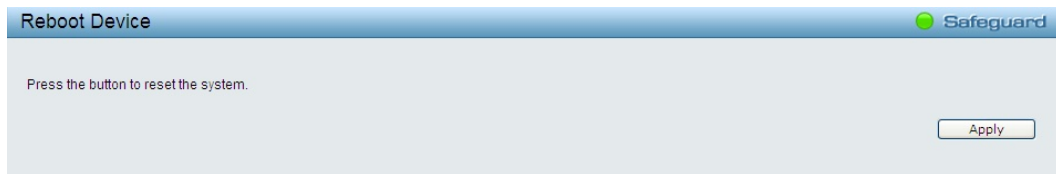


Figure 5.12 – Tool Menu > Reboot Device

Configuration Backup and Restore

스위치의 현재 설정된 값을 파일로 저장합니다.(단, 관리자 비밀번호는 제외)

필요한 경우, 해당 파일을 이용하여 스위치 설정을 복원할 수 있습니다.(HTTP / TFTP 방식 지원)

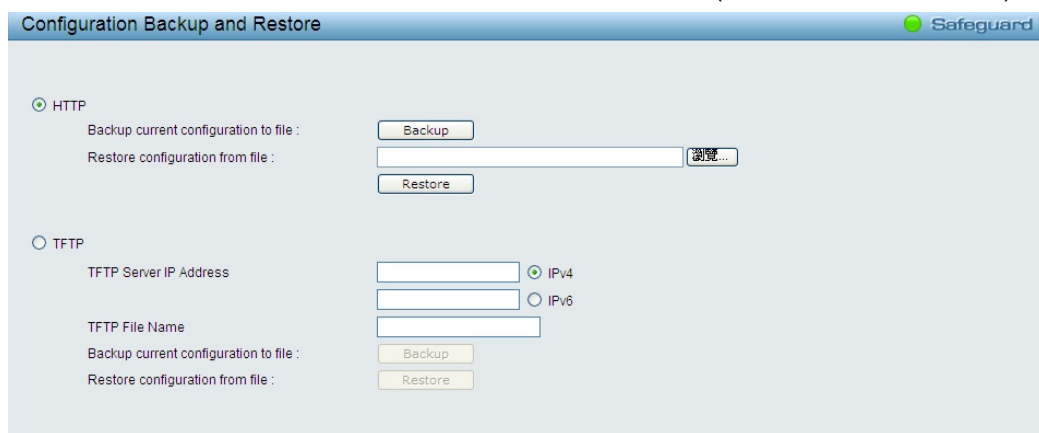


Figure 5.13 – Tool Menu > Configure Backup and Restore

HTTP: 현재 설정화면 접속에 사용한 PC 의 하드디스크로 설정값을 백업하거나 백업된 파일로 복구합니다.

설정값을 하드디스크로 백업하시려면 **Backup** 버튼을 클릭합니다.

백업된 파일을 이용하여 설정을 복구하시려면, **Browse** 버튼을 클릭하여 백업파일을 선택하고 **Restore** 버튼을 클릭합니다.

TFTP: TFTP 서버로 설정값을 백업하거나 서버에 저장된 파일로 설정을 복구합니다.

- **TFTP Server IP Address** : TFTP 서버 IP 주소를 입력합니다.

- **TFTP File Name** : 백업 혹은 복구할 파일명을 입력합니다.

- **Backup** : 현재의 설정값을 서버로 백업하시려면 클릭합니다.

- **Restore** : 서버에 저장된 파일을 이용하여 설정을 복구하시려면 클릭합니다.



참고

스위치는 복구 후에 자동으로 재부팅되며, 모든 설정값이 백업파일 내용으로 변경됩니다.

Firmware Backup and Upgrade

현재의 펌웨어를 백업하거나 업그레이드된 펌웨어 파일을 이용하여 스위치 업그레이드를 진행합니다.

(HTTP / TFTP 방식 지원)

Figure 5.14 – Tool Menu > Firmware Backup and Upload

HTTP: 현재 설정화면 접속에 사용한 PC 의 하드디스크로 펌웨어를 백업하거나 업그레이드를 진행합니다. 펌웨어를 하드디스크로 백업하시려면 **Backup** 버튼을 클릭합니다. 펌웨어를 업그레이드 하시려면, **Browse** 버튼을 클릭하여 업그레이드된 펌웨어 파일을 선택하고 **Upgrade** 버튼을 클릭합니다.

TFTP: TFTP 서버로 펌웨어를 백업하거나 서버에 저장된 펌웨어 파일로 업그레이드를 진행합니다.

- **TFTP Server IP Address** : TFTP 서버 IP 주소를 입력합니다.
- **TFTP File Name** : 백업 혹은 업그레이드를 진행할 파일명을 입력합니다.
- **Backup** : 현재의 펌웨어를 서버로 백업하시려면 클릭합니다.
- **Upgrade** : 서버에 저장된 펌웨어 파일로 스위치 업그레이드를 진행하시려면 클릭합니다.



주의

펌웨어 업그레이드가 완료되지 않은 상태에서 PC 의 연결을 끊거나 스위치 전원을 차단하게 되면 장비가 손상될 수 있습니다.

Tool Bar > Smart Wizard

Smart Wizard 를 실행하여 해당 설정을 진행하실 수 있습니다.

Function Tree

설정 화면의 왼편에 위치한 **Function Tree** 를 이용하여 스위치의 모든 설정을 조정하실 수 있습니다.

Function Tree 에서 지원하는 설정항목은 아래 이미지와 같습니다.

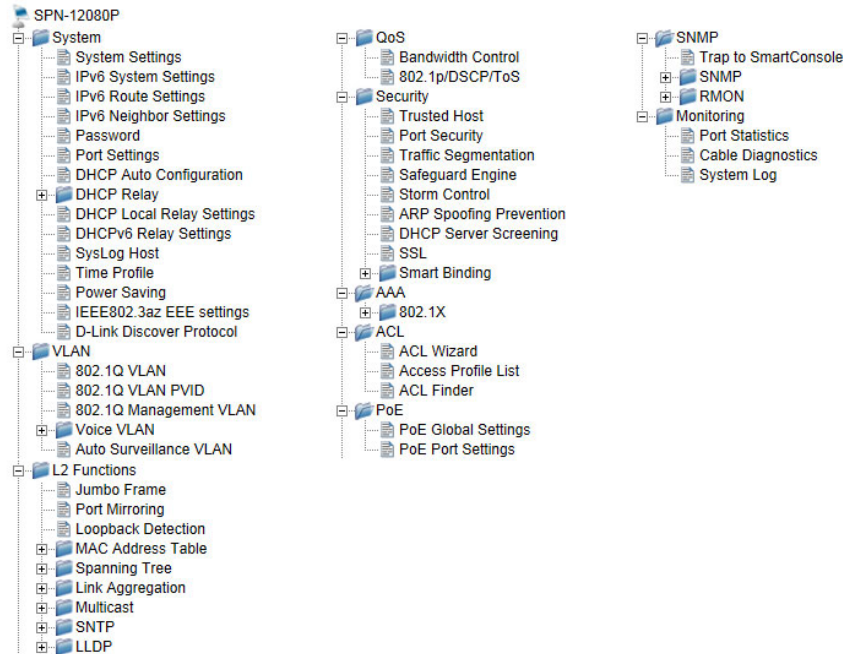


Figure 5.17 –Function Tree

Device Information

The Device Information 은 장비의 펌웨어 및 하드웨어 정보, IP 주소를 포함한 기본적인 정보를 표시합니다.

또한, 아래 기능들의 현재 상태를 표시하고 필요한 경우, 각 설정으로 빠르게 이동할 수 있습니다.

기능	기본값	Settings 클릭시 이동
RSTP	Disabled (사용안함)	L2 Functions > Spanning Tree > STP Global Settings
Port Mirroring	Disabled (사용안함)	L2 Functions > Port Mirroring
Storm Control	Disabled (사용안함)	Security > Storm Control
DHCP Client	Disabled (사용안함)	System > System Settings
Jumbo Frame	Disabled (사용안함)	L2 Functions > Jumbo Frame
SNMP Status	Disabled (사용안함)	SNMP > SNMP > SNMP Global Settings
802.1X Status	Disabled (사용안함)	AAA > 802.1X > 802.1X Settings
Safeguard Engine	Enabled(사용함)	Security > Safeguard Engine
IGMP Snooping	Disabled (사용안함)	L2 Functions > Multicast > IGMP Snooping
Power Saving	Disabled (사용안함)	System > Power Saving

Device Information			
Device Information			
Device Type	SPN-12080P	System Name	
Boot Version	1.00.009	System Location	
Firmware Version	3.12.K022	System Time	03/01/2012 20:37:10
Protocol Version	2.001.004	System Up Time	2 days , 20 hours , 30 mins , 14 seconds
Hardware Version	B1	Trap IP	0.0.0.0
Serial Number	F3YS3D8000916	Login Timeout (minutes)	5
MAC Address	D8-FE-E3-39-1A-62		
IP Address Information			
IPv4 Address	192.168.10.250		
Subnet Mask	255.255.255.0		
Default Gateway	192.168.10.1		
IPv6 Global Unicast Address			
IPv6 Link-Local Address			
Device Status and Quick Configurations			
RSTP	Disabled	SNMP Status	Disabled
Port Mirroring	Disabled	802.1X Status	Disabled
Storm Control	Disabled	Safeguard Engine	Enabled
DHCP Client	Disabled	IGMP Snooping	Disabled
Jumbo Frame	Disabled	Power Saving	Enabled

Figure 5.18 – Device Information

System > System Settings

스위치의 IP 주소 및 System Name 등의 정보를 설정합니다.

IP Information: 스위치 관리에 사용할 IP 주소를 설정합니다.

- Static : 스위치 IP 주소를 고정값으로 설정합니다. IP Address, Netmask, Gateway 를 모두 입력합니다.

- DHCP/BOOTP : 스위치 IP 주소를 서버로부터 자동으로 할당받습니다.

(기본값 : Static 모드 / IP address **10.90.90.90** / Netmask **255.0.0.0**)

System Information: SNMP 호환 프로그램을 이용하여 관리할 경우, 관리자가 쉽게 확인할 수 있도록 입력한 **System Name**(장비명) 과 **System Location**(장비의 위치) 정보를 전송합니다.

Login Timeout: 설정화면에 로그인된 상태에서 설정을 진행하지 않을 경우, 자동으로 로그아웃하는 시간을 설정합니다.(기본값 : 5 분 / 설정범위 : 3~30 분)

Group Interval: 스위치의 각종 정보를 SNMP 프로그램에 전송할 시간 간격을 설정합니다.

(기본값 : 120 초 / 설정범위 : 120~1225 초 / 0 초 : 전송안함)

System Settings	
IP Information	
☒ Static ☐ DHCP ☐ BOOTP	
IP Address	10.90.90.90
Netmask	8 (255.0.0.0)
Gateway	0.0.0.0
Apply	
System Information	
System Name	
System Location	
Login Timeout (3-30 minutes)	5
Group Interval (120-1225 seconds)	120 (Disable: 0 second)
Apply	

Figure 5.19 – System > System Settings

System > IPv6 System Settings

IPv6 네트워크에 스위치를 설치할 경우, 해당 IPv6 정보를 입력합니다.

Figure 5.20 – System > IPv6 System Settings

IPv6 System Settings:

Interface Name: IPv6 의 인터페이스 이름이 표시됩니다.

IPv6 State: IPv6 기능의 사용여부를 선택합니다. (Enabled : 사용함)

DHCPv6 Client: DHCPv6 클라이언트 기능의 사용여부를 선택합니다. (Enabled : 사용함)

IPv6 Network Address: 사용할 IPv6 Network Address 를 입력합니다.

NS Retransmit Time Settings:

NS Retransmit Time (1-3600): IPv6 의 NS retransmit time 을 설정합니다. (기본값 : 1 초 / 범위 : 1~3600 초)

Automatic Link Local State Settings:

Automatic Link Local Address: Automatic link 사용여부를 선택합니다.

Apply 버튼을 클릭하면 변경한 설정이 적용됩니다.

System > IPv6 Route Settings

IPv6 Route(경로) 설정입니다.

Figure 5.21 – System > IPv6 Route Settings

IP Interface: IP 인터페이스 이름을 입력합니다.

Default Gateway: 사용할 다음 경로의 IPv6 주소를 입력합니다.

Metric: 해당 목록에 적용할 매트릭 값을 입력합니다. (입력범위 : 1 ~ 65535)

입력하신 값을 등록하시려면 **Create** 버튼을 클릭합니다. 삭제하시려면 **Delete** 버튼을 클릭합니다.

System > IPv6 Neighbor Settings

IPv6 neighbor 설정입니다.

Figure 5.22 – System > IPv6 Neighbor Settings

Interface Name: IPv6 Neighbor 인터페이스 이름을 입력합니다.

Neighbor IPv6 Address: 등록할 Neighbor 의 IPv6 주소를 입력합니다.

Link Layer MAC Address: 해당하는 Link layer MAC 주소를 입력합니다.

입력하신 사항을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

Interface Name: 검색할 IPv6 Neighbor 의 인터페이스 이름을 입력합니다.

State: All, Address, Static, Dynamic 중 검색하고자 하는 항목을 선택합니다.

입력하신 사항을 검색하시려면 **Find** 버튼을 클릭합니다.

목록에 표시된 내용을 삭제하시려면 **Clear** 버튼을 클릭합니다.

System > Password

스위치 설정 로그인에 사용할 관리자 비밀번호를 변경하실 수 있습니다.

변경하고자 하는 비밀번호를 입력하신 후, **Apply** 버튼을 클릭합니다.

Figure 5.23 – System > Password Access Control

System > Port Settings

포트별 동작속도, MDI/MDIX, 802.3x Flow Control 사용여부를 설정할 수 있습니다.

Port Settings Safeguard

From Port: 01 To Port: 10 Speed: Auto MDI/MDIX: Auto Flow Control: Disabled Refresh Apply

Port	Link Status	Speed	MDI/MDIX	Flow Control
01	1000M Full	Auto	Auto	Disabled
02	Link down	Auto	Auto	Disabled
03	Link down	Auto	Auto	Disabled
04	Link down	Auto	Auto	Disabled
05	Link down	Auto	Auto	Disabled
06	Link down	Auto	Auto	Disabled
07	Link down	Auto	Auto	Disabled
08	Link down	Auto	Auto	Disabled
09	Link down	Auto	Auto	Disabled
10	Link down	Auto	Auto	Disabled

Figure 5.24 – System > Port Settings

Speed

1000M Full, 100M Full, 100M Half, 10M Full, 10M Half, Auto, Disabled 중 선택할 수 있습니다.

기본값은 **Auto** 입니다. 참고로, 기가비트(1000Mbps) 속도가 지원되기 위해서는 본 항목의 값이 1000M Full, Auto, Disabled 중 하나로 되어 있어야 합니다.

MDI/MDIX

MDI(Medium Dependent Interface) 는 일반적으로 스위치 장비와 NIC(Network Interface Card) 를 장착한 PC 간의 연결에 사용되는 방식이며, **MDIX(Medium Dependent Interface Crossover)** 는 스위치 장비 및 허브간의 연결에 사용되는 방식입니다.

다만, 대부분의 스위치 및 네트워크 장비가 자동으로 감지하여 연결해 주는 **Auto MDI/MDIX** 기능이 지원되어 특수한 경우가 아니라면 기본값인 **"Auto"** 로 사용하여 주십시오.

Flow Control

네트워크 트래픽 간의 충돌을 완화하기 위한 기능으로 표준은 IEEE 802.3x 입니다.

기본값은 Disabled(사용안함) 입니다.

Link Status 표시

스위치의 해당 포트가 사용중인 경우, 현재의 Link Speed 가 표시됩니다.

Link down 은 해당 포트가 미사용중이거나 단선된 경우 표시됩니다.

System > DHCP Auto Configuration

본 기능은 스위치가 부팅하는 동안 DHCP 서버에 저장된 스위치 Configuration file 을 자동으로 불러들여 설정을 적용하는 기능으로 DHCP 서버 상에 TFTP 서버 IP 주소와 Configuration File 을 전송하는 기능이 우선 구현되어 있어야 합니다.

본 기능을 사용하려면 Enabled(사용함)에 체크 후, [Apply] 버튼을 클릭하여 주십시오.

DHCP Auto Configuration Settings Safeguard

DHCP Auto Configuration ☐ Enabled ☒ Disabled Apply

If DHCP Auto Configuration is enabled, the switch will load a previously saved configuration file from TFTP server after every boot up.

If the switch is unable to complete the Auto Configuration process, the last configuration file saved in switch flash memory will be loaded.

Figure 5.25 – System > DHCP Auto Configuration

System > SysLog Host

로그 기록을 지정한 서버로 전송하는 기능입니다.

본 기능을 사용하려면 **Enabled(사용함)**에 체크하고 **[Apply]** 버튼을 클릭하신 후, 아래에 설명된 항목의 값을 등록하여 주십시오.

Figure 5.26 – System > SysLog Host Settings

Server IP Address: 로그 서버 IP 주소를 입력합니다.

UDP Port: 로그를 전송할 UDP 포트 번호를 입력합니다. (기본값 : 514 / 입력범위 : 1 ~ 65535)

Time Stamp: 로그 메시지 상에 시간기록 여부를 선택합니다.

Severity: 전송할 로그 레벨을 선택합니다.

Warning - 장비 운용간 발생한 문제와 관련된 로그만 전송합니다.

Informational - 장비의 정보와 관련된 로그만 전송합니다.

All - 모든 로그를 전송합니다.

Facility: 로그서버에 적용된 Facility 값을 선택하여 주십시오. (Local 0 ~ Local 7)

입력하신 설정을 적용하시려면 **[Apply]** 버튼을 클릭합니다.

System > Time Profile

Power Saving, PoE Port Settings 와 같이 스케줄을 적용할 수 있는 스위치 기능에 설정할 규칙을 등록합니다.

Figure 5.27 – System > Time Profile

Profile Name: 등록할 스케줄 규칙명을 입력합니다.

Time(HH MM): 시작시간과 종료시간을 각각 선택합니다.

Weekdays: 적용할 요일을 체크합니다.

Date: 본 항목에 체크시, 해당 규칙을 적용할 기간을 입력하실 수 있습니다.

스케줄 규칙 입력이 완료된 후, **Add** 버튼을 클릭합니다.

규칙을 삭제하시려면, 등록된 각 항목에 있는 **Delete** 버튼을 클릭하여 주십시오.

System > Power Saving

전원 절약은 포트에 연결된 장비가 미사용중인 경우, 자동으로 링크를 해제하고 대기 전력 공급을 차단하거나 랜케이블 길이에 따라 사용되는 전력을 조정함으로써 전력 소비를 줄이는 기능입니다.

소비 전력이 감소됨으로써, 제품의 발열이 줄어들기 때문에 제품의 수명이 증가하고 운용비용이 절감되는 효과를 보실 수 있습니다. 기본값으로 **Cable Length Detection** (케이블 길이 감지) 와 **Link Status Detection** (링크 상태 감지) 기능이 켜져 있습니다.

Port	01	02	03	04	05
	☐	☐	☐	☐	☐
Port	6	7	8	9	10
	☐	☐	☐	☐	☐

Type	State	Time Profile 1	Time Profile 2	Port
LED Shut-off	Disabled			None
Port Shut-off	Disabled			None
Port Standby	Disabled			None
System Hibernation	Disabled			All Port

Figure 5.28 – System > Power Saving

Advanced Power Saving Settings:

Type: LED Shut-off, Port Shut-off, Port Standby, System Hibernation 중 선택합니다.(추가 절감 기능)

LED Shut-off - 포트 LED 동작을 끄는 기능으로 본 기능을 사용하시려면 **State** 값을 **Enabled** 로 선택하여 주십시오. **Time-Profile** 을 적용할 경우, LED 를 해당 일정에 따라 동작토록 할 수 있습니다.

Port Shut-off - 포트의 연결을 차단하는 기능으로 **State** 값을 **Enabled** 로 변경하고 **Time-Profile** 적용시 해당 일정에 따라 포트의 동작을 제어할 수 있습니다.

Port Standby - 포트가 대기 모드로 변환되어 **Wake-Up** 신호가 감지되었을 때, 대기모드에서 자동해제됩니다.

System Hibernation - 시스템의 주요 구성 칩 중에서 CPU 에만 전원을 공급하고 스위칭 칩셋(MAC / PHY) 에는 전원을 공급하지 않음으로써 전력 소비를 줄입니다.

State: 선택한 전원 절약 기능의 동작여부를 선택합니다. (**Enabled** : 사용함)

Time Profile 1: 해당 기능이 적용될 스케줄 규칙을 선택합니다.

Time Profile 2: 해당 기능이 적용될 스케줄 규칙을 선택합니다.

Port: 전원 절약 기능을 적용할 포트를 선택합니다.

모든 포트를 한번에 선택하시려면 **Select All** 을 클릭하여 주십시오.

모든 포트를 한번에 해제하시려면 **Clear** 을 클릭하여 주십시오.
 지정한 기능을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

System > IEEE802.3az EEE Settings

포트별 IEEE 802.3az EEE 표준 전원 절약 기능의 적용여부를 설정합니다.

Port	State
1	Enabled
2	Enabled
3	Enabled
4	Enabled
5	Enabled
6	Enabled
7	Enabled
8	Enabled
9	Enabled
10	Enabled

Figure 5.29 – System > IEEE802.3az EEE Settings

From Port / To Port: 기능을 적용할 시작 포트 번호와 마지막 포트 번호를 선택합니다.

State: 선택한 포트에 대하여 IEEE802.3az EEE 동작 여부를 선택합니다. (Enabled : 사용함)
 적용하시려면, **Apply** 버튼을 클릭하여 주십시오.

링크 속도가 1000Mbps 에서 100Mbps 로 저하되거나, 초기 연결되는 시간이 오래 걸리는 경우, 연결된 장비가 IEEE 802.3az EEE 를 지원하지 않은 경우로

1. PC 에 장착된 LAN Controller 드라이버를 최신 버전으로 업데이트하여 주십시오.
2. 본 스위치에서 해당 기능을 꺼주십시오.

VLAN > 802.1Q VLAN

VLAN 은 하나의 장비에서 포트를 그룹으로 구성하여, 지정한 그룹 내에서만 네트워크 통신이 이루어지도록 하는 기능입니다. 멀티캐스트 및 브로드캐스트 트래픽이 그룹내에서만 전달됨으로써 전체 네트워크 성능에 영향을 주지 않으며, 운용 방식에 따라 부서를 구분할 수 있어 효과적인 네트워크 관리가 가능합니다.

본 기능은 IEEE 802.1Q VLAN 표준에 의거하여 동작합니다.

(기본값 : VID 1 / VLAN 이름없음 / 전포트 Untagged)

Rename: VLAN 그룹명을 수정하시려면 클릭하여 주십시오.

Delete VID: VLAN 그룹을 삭제하시려면 클릭하여 주십시오.

Add New VID: VID 그룹을 새로 구성합니다. 포트를 Untag, Tag, Not Member 중에 선택하여 그룹으로 구성하여 주십시오.

VID	VLAN Name	Untagged	Tagged	Delete
1	default	01-10		Delete

Figure 5.30 – Configuration > 802.1Q VLAN

VID Settings

VID:

VLAN Name: (Maximum 20 characters.)

Back Apply

Port	Select All	01	02	03	04	05	06	07	08	09	10
Untagged	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Tagged	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Not member	All	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Figure 5.31 – Configuration > 802.1Q VLAN > Add VLAN

VLAN > 802.1Q VLAN PVID

포트별로 PVID 값을 할당하는 기능입니다.

802.1Q VLAN PVID Settings

Port	01	02	03	04	05	06	07	08	09	10
PVID	1	1	1	1	1	1	1	1	1	1

Apply

Figure 5.32 – Configuration > 802.1Q VLAN PVID

VLAN > 802.1Q Management VLAN

여러 개의 VID 로 구성되어 있는 경우, 802.1Q VLAN 관리를 위한 관리자 VLAN 을 지정합니다.
네트워크 관리자가 소속된 VID 를 선택하여 주십시오.

IEEE 802.1Q Management VLAN Configuration

Management VLAN: ☐ Enabled ☒ Disabled

VID:

VLAN Name: default

Apply

Figure 5.33 – Configuration > 802.1Q Management VLAN

VLAN > Voice VLAN > Voice VLAN Global Settings

VoIP 트래픽 품질 향상을 위하여 자동으로 VoIP 트래픽을 지정한 VLAN 으로 구성합니다.

Voice VLAN Global Settings

Voice VLAN: ☐ Enabled ☒ Disabled

VLAN ID: Aging Time (1~120): hour

Priority:

Apply

Voice VLAN OUI Settings

☒ Default OUI Description: Telephony OUI:

☐ User defined OUI (XX-XX-XX-XX-XX-XX)

Maximum number of user defined OUI is 10 entries.

Add

ID	Description	Telephony OUI	OUI Mask	Delete

Figure 5.34 – VLAN > Voice VLAN > Voice VLAN Global Settings

Voice VLAN: Voice VLAN 사용여부를 선택합니다. (기본값 : Disabled, 사용안함)

VLAN ID: Voice VLAN 으로 할당할 VLAN ID 를 선택합니다.

VLAN ID 를 할당하기 전에 802.1Q VLAN 설정에서 VLAN 이 먼저 구성되어 있어야 합니다.

Priority: Voice VLAN 을 위한 802.1p priority 값을 선택합니다.

Aging Time (1-120): 해당 포트가 자동 VLAN 으로 구성되어 있을 경우, Voice VLAN 으로부터 해당 포트를 제외해 둘 대기 시간을 설정합니다. VoIP 통화가 마지막으로 완료된 후부터 본 시간이 시작됩니다.

지정한 Aging Time 이 만료된 후 해당 포트는 Voice VLAN 포트에서 원래의 VLAN 으로 자동 소속됩니다.

(기본값 : 1 시간 / 지정범위 : 1 ~ 120 시간)

설정을 적용하려면 **Apply** 버튼을 클릭하여 주십시오.

Voice VLAN OUI Settings: Voice VLAN 으로 지정할 VoIP 단말의 OUI 를 선택 혹은 원하는 값으로 설정합니다.

아래의 OUI 값이 기본 지원됩니다.

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

Default OUI: 상기의 표와 같이 기본으로 입력되어 있는 OUI 값 중에 선택하여 적용할 수 있습니다.

User defined OUI: 상기의 표 이외의 OUI 를 적용하고자 할 경우 선택하고 입력합니다.

OUI 입력 후, **Add** 버튼을 클릭하면 목록으로 등록됩니다.



Note: Voice VLAN 은 다른 기능보다 우선순위가 높아 QoS 기능 설정에 영향을 받지 않습니다.



Note: VoIP 트래픽의 품질 향상을 위하여 우선순위를 Highest 로 설정하시길 권장드립니다.

VLAN > Voice VLAN > Voice VLAN Port Settings

Voice 트래픽을 자동으로 할당할 포트를 설정합니다.

Voice VLAN Port Settings

From Port: 01 To Port: 10 Auto Detection: Disabled Tagged / Untagged: Untagged Refresh Apply

Port	Auto Detection	Tagged / Untagged	Current State	Status
01	Disabled	Untagged	None	None
02	Disabled	Untagged	None	None
03	Disabled	Untagged	None	None
04	Disabled	Untagged	None	None
05	Disabled	Untagged	None	None
06	Disabled	Untagged	None	None
07	Disabled	Untagged	None	None
08	Disabled	Untagged	None	None
09	Disabled	Untagged	None	None
10	Disabled	Untagged	None	None

Figure 5.35 – VLAN > Voice VLAN > Voice VLAN Port Settings

From Port / To Port: Voice VLAN 포트에 사용할 시작포트와 마지막 포트를 선택합니다.

Auto Detection: 설정한 OUI 와 동일한 단말에서 전송되는 트래픽을 스위치가 자동 감지합니다. 본 기능을 사용하려면 **Enabled(사용함)** 을 선택하여 주십시오.

Tagged / Untagged: 해당 포트에 대한 Tagged 혹은 Untagged 항목을 선택합니다. 변경한 내용을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

VLAN > Voice VLAN > Voice Device List

Voice VLAN 정보를 표시합니다.

Voice Device List

Port: All Search

ID	Port	MAC Address	Priority	Type	Delete
----	------	-------------	----------	------	--------

Figure 5.36 – VLAN > Voice VLAN > Voice Device List

확인할 포트 혹은 All 을 선택하고 **Search** 버튼을 클릭하여 Voice Device 정보를 확인하실 수 있습니다.

VLAN > Auto Surveillance VLAN Settings

Auto Surveillance VLAN 은 특정 IP 카메라의 영상 트래픽을 지정한 VLAN 으로 할당함으로써 비디오 품질을 향상/보장합니다. 스위치가 자동으로 데이터 패킷내의 Source MAC Address 와 VLAN ID 를 확인하고 일치하는 패킷을 높은 우선순위를 부여하여 전송합니다.

Auto Surveillance VLAN Settings Safeguard

Auto Surveillance VLAN Global Settings

Auto Surveillance VLAN ☐ Enabled ☒ Disabled

VLAN ID: 4094 Priority: Medium Tagged Uplink/Downlink Port: Ex: 1,2,4-6 Apply

User-defined MAC Settings

To add more device(s) for Auto Surveillance VLAN by user-defined configuration as below

Component Type: Video Management Server Description: (XX-XX-XX-XX-XX-XX) MAC: Add

Maximum number of user-defined MAC is 5 entries.

ID	Component Type	Description	MAC Address	Delete
01	D-Link Surveillance Device	D-Link IP Surveillance Device	28-10-7B:XXXXXX	Default
02	D-Link Surveillance Device	D-Link IP Surveillance Device	F0-7D-68:0XXXXX	Default

Auto Surveillance VLAN Summary Refresh

Port	Component Type	Description
1	None	None
2	None	None
3	None	None
4	None	None
5	None	None
6	None	None
7	None	None
8	None	None

Figure 5.37 – VLAN > Auto Surveillance VLAN

Auto Surveillance VLAN Global Settings:

Auto Surveillance VLAN State: 본 기능의 사용여부를 선택합니다. (Enabled : 사용함)

VLAN ID: Auto Surveillance VLAN 의 기본 VLAN ID 는 4094 입니다. 802.1Q VLAN 설정에서 VLAN 을 구성한 후, 원하는 값으로 선택하실 수 있습니다. 802.1Q VLAN 에서 해당 VLAN ID 로 구성된 포트는 자동으로 Auto Surveillance VLAN 으로 구성됩니다.

Priority: Auto Surveillance VLAN 으로 할당할 802.1p Priority 값을 선택합니다.

Tagged Uplink/Downlink Port: 본 기능을 위해 Tagged 포트를 입력합니다.

변경한 설정을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

User-defined MAC Settings:

Component Type: Auto Surveillance VLAN 은 기본적으로는 특정 장비를 자동으로 감지하지만, Video Management Server (VMS), VMS Client/Remote viewer, Video Encoder, Network Storage and Other IP Surveillance Devices 를 직접 선택하여 등록하실 수 있습니다.

Description: 선택한 Component Type 에 대한 참고 설명을 입력합니다.

MAC/OUI: Auto Surveillance VLAN 규칙을 적용할 MAC Address 혹은 OUI 값을 입력합니다.

설정을 적용하시려면 **Add** 버튼을 클릭하여 주십시오.

L2 Functions > Jumbo Frame

정보프레임을 설정합니다. 최대 10,000 bytes 를 지원합니다.

Jumbo Frame Settings Safeguard

Jumbo Frame ☐ Enabled ☒ Disabled

Maximum Length is 10000 bytes. Apply

Figure 5.38 – L2 Functions > Jumbo Frame

L2 Functions > Port Mirroring

스위치의 특정 포트에서 다른 포트에 송수신하는 트래픽을 모니터링 하는 기능입니다.

Port Mirroring Settings Safeguard

Port Mirroring: ☐ Enabled ☒ Disabled

Target Port: 01

Source Port Selection

Sniffer Mode	Select All	01	02	03	04	05	06	07	08	09	10
TX	All										
RX	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
TX/RX	All										
None	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Apply

Figure 5.39 – L2 Functions > Port Mirroring

Source 포트 선택값은 아래 내용을 참고하여 주십시오.

TX (transmit) mode: Source 포트에서 송신되는 데이터를 Target 포트에 복제합니다.

RX (receive) mode: Source 포트에 수신되는 데이터를 Target 포트에 복제합니다.

TX/RX (transmit and receive) mode: Source 포트에 송수신되는 데이터를 Target 포트에 복제합니다.

None: 포트 미러링 기능을 적용하지 않습니다.

L2 Functions > Loopback Detection

일반 HUB 장비와 같이 Spanning Tree Protocol(STP) 이 지원되지 않는 장비와 연동하는 네트워크 망에서 지정한 포트에 대하여 Loopback Detection 기능을 사용합니다. Loopback 이 감지된 경우, 해당 포트를 지정한 Recover Time 동안 자동으로 차단합니다.

Loopback Detection Settings Safeguard

Loopback Detection: ☐ Enabled ☒ Disabled

Mode: Port-based

Interval (1-32767): 2 sec

Recover Time (0 or 60-1000000): 60 sec

Apply

From Port: 01 To Port: 10 State: Disabled

Refresh Apply

Port	State	Loop Status
01	Disabled	Normal
02	Disabled	Normal
03	Disabled	Normal
04	Disabled	Normal
05	Disabled	Normal
06	Disabled	Normal
07	Disabled	Normal
08	Disabled	Normal
09	Disabled	Normal
10	Disabled	Normal

Figure 5.40 – L2 Functions > Loopback Detection

Loopback Detection: 본 기능의 사용여부를 선택합니다.

Mode: 동작방식을 Port-based(포트 기준) 혹은 VLAN-based(VLAN 기준) 중 하나로 선택합니다.

VLAN-based 선택시에는 Loopback Detection 이 해당 VLAN 그룹으로 구성된 포트에 한하여 동작합니다.

Interval (1-32767): Loop 감지 간격을 선택합니다. (기본값 : 2 초 / 범위 : 1 ~ 32767 초)

Recover Time (0 or 60-1000000): Loopback 이 감지되어 포트가 차단되었을 때, 해당 포트가 재가동되는 시간을 설정합니다. (범위 : 60 ~ 1000000 초, 0 초는 Loopback Detection 기능이 동작하지 않습니다.)

From Port: Port-based 선택시, 본 기능을 적용할 시작포트를 선택합니다.

To Port: Port-based 선택시, 본 기능을 적용할 마지막포트를 선택합니다.

State: 지정한 포트에 대하여 본 기능에 대해 적용 여부를 선택합니다. (Enabled : 사용함)

설정된 내용을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

L2 Functions > MAC Address Table > Static MAC

지정한 포트에 대하여 지정한 MAC Address 과 VID 를 지닌 단말에서 보내는 트래픽만 통과시킵니다.

Static MAC Settings Safeguard

MAC Address Learning ☐ Enabled ☒ Disabled Select All Clear Apply

Port	01	02	03	04	05	06	07	08	09	10
Learning	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Add Static MAC Address

Port MAC Address VID Add

Static MAC Address Lists Delete All

Maximum 256 entries.

ID	Port	MAC Address	VID	Delete
----	------	-------------	-----	--------

Figure 5.41 – L2 Functions > MAC Address Table > Static Mac Address

L2 Functions > MAC Address Table > Dynamic Forwarding Table

스위치에 연결된 단말의 MAC 주소 정보를 표시합니다. **Add Static MAC** 에 체크할 경우, 자동으로 Static MAC 기능에 등록됩니다.

Dynamic Forwarding Table Safeguard

Port Search Select All Clear Apply

Static MAC entries used/maximum: 0/256

ID	Port	MAC Address	VID	Type	Add to Static MAC
1	1	00-17-9A-9E-1C-57	1	Dynamic	☐
2	1	C8-60-00-89-8C-74	1	Dynamic	☐

Figure 5.42 – L2 Functions > MAC Address Table > Dynamic Forwarding Table

L2 Functions > Spanning Tree > STP Global Settings

IEEE 802.1w 표준의 RSTP(Rapid Spanning Tree Protocol) 와 IEEE 802.1D STP 의 사용여부를 설정합니다.

STP Global Settings Safeguard

Spanning Tree Protocol ☐ Enabled ☒ Disabled

STP Version Maximum Age (6-40) sec

Bridge Priority Hello Time (1-10) sec

Tx Hold Count (1-10) Forward Delay (4-30) sec Refresh Apply

Root Bridge Information

Root Bridge	00:00:00:00:00:00:00
Root Cost	0
Root Maximum Age	20
Root Forward Delay	15
Root Port	0

Figure 5.43 – L2 Functions > Spanning Tree > STP Global Settings

STP Version: RSTP 와 STP 중에 적용하고자 하는 프로토콜을 선택합니다. (기본값 : RSTP)

Bridge Priority: 0 ~ 61410 중에 적용하고자 하는 값으로 설정합니다. (기본값 : 32768)

TX Hold Count (1-10): Hello 패킷을 전송할 간격을 입력합니다. (기본값 : 6 / 범위 : 1 ~ 10)

Maximum Age (6-40 sec): 최대 시간은 Hellow Time 보다 커야 합니다.

Hello Time (1-10 sec): Hello Time 을 설정합니다.

Forward Delay (4-30 sec): 기본값은 15 초로 4~30 초로 설정할 수 있습니다.

L2 Functions > Spanning Tree > STP Port Settings

STP Port Settings Safeguard

From Port: 01 To Port: 10 State: Enabled

External Cost (0-200000000; 0=Auto): 2000000 Migrate: Disabled Edge: Auto

Priority: 128 P2P: Auto Restricted Role: False

Restricted TCN: False

Refresh Apply

Port	State	Priority	External Cost	Edge	P2P	Restricted Role	Restricted TCN	Port Status
01	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
02	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
03	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
04	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
05	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
06	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
07	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
08	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
09	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled
10	Enable	128	AUTO/20000	Auto	Auto	False	False	Disabled

Figure 5.44 – L2 Functions > Spanning Tree > STP Port Settings

From Port/To Port: STP 를 적용할 포트의 시작과 마지막 값을 선택합니다.

State: 지정한 포트에 대해 STP 의 적용여부를 결정합니다.

External Cost: 패킷 Forwarding Cost 를 입력합니다.

0 (auto) - 자동으로 Cost 를 산정합니다. (기본값 : 100Mbps=200000 / 1000Mbps=20000)

Value 1-200000000 - 1 ~ 200000000 사이의 숫자로 설정하실 수 있습니다.

Migrate: 본 기능의 사용여부를 선택합니다.

Edge: Edge 로 지정할 포트들의 True Parameter 값을 선택합니다.

Priority: 포트의 우선순위를 선택합니다. (기본값 : 128 / 범위 : 0 ~ 240)

P2P: P2P 연결에 대한 True Parameter 값을 선택합니다.

Restricted Role: 패킷에 대한 Restricted Role 을 선택합니다.

Restricted TCN: 패킷에 대한 Restricted TCN 을 선택합니다.

변경하신 사항을 적용하시려면 **Apply** 버튼을 클릭합니다.

L2 Functions > Link Aggregation > Port Trunking

대역폭을 늘리기 위하여 둘 이상의 포트를 하나의 논리 포트로 구성합니다.

Static - Static link aggregation.

LACP - LACP (Link Aggregation Control Protocol)

Disable - Trunk 그룹에서 해제합니다.

Port Trunking Safeguard

Link Aggregation ☐ Enabled ☒ Disabled Apply

Link Aggregation Settings

Group Type Apply

Port	01	02	03	04	05
	☐	☐	☐	☐	☐
Port	06	07	08	09	10
	☐	☐	☐	☐	☐

Maximum 8 ports in static group and 8 ports in LACP group.

Trunking list	Group	Type	Ports	Delete

Figure 5.45 – L2 Functions > Link Aggregation > Port Trunking



NOTE: Each combined trunk port must be connected to devices within the same VLAN group.

L2 Functions > Link Aggregation > LACP Port Settings

LACP 포트를 선택 설정합니다.

LACP Port Settings Safeguard

From Port To Port Activity Timeout Apply

Port	Activity	Timeout
01	Active	Long (90 sec)
02	Active	Long (90 sec)
03	Active	Long (90 sec)
04	Active	Long (90 sec)
05	Active	Long (90 sec)
06	Active	Long (90 sec)
07	Active	Long (90 sec)
08	Active	Long (90 sec)
09	Active	Long (90 sec)
10	Active	Long (90 sec)

Figure 5.46 – L2 Functions > Link Aggregation > LACP Port Settings

From Port: LACP 로 구성할 시작 포트를 선택합니다.

To Port: LACP 로 구성할 마지막 포트를 선택합니다.

Activity

Active / Passive 모드 중에서 선택할 수 있습니다.

Timeout: LACP 만료시간을 선택합니다.

Short (3 Sec) - LACP 만료시간이 3 초로 설정됩니다.

Long (90 Sec) - LACP 만료시간이 90 초로 설정됩니다. (기본값)

변경한 설정을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

L2 Functions > Multicast > IGMP Snooping

IGMP snooping 는 LAN 망의 과도한 트래픽 발생을 감소시킵니다. IGMP snooping 기능이 켜져 있을 경우, 스위치는 멀티캐스트 트래픽을 그룹내 단말로만 전송시킵니다.

IGMP snooping 설정은 각 VLAN 마다 개별적으로 설정할 수 있습니다.

Figure 5.47 – L2 Functions > Multicast > IGMP Snooping

Host Timeout (130-153025 sec): Host Port 목록을 삭제하는 간격입니다. Host 로부터 리포트 메시지를 수신할 때마다 본 시간의 카운트가 재시작되며, 리포트 메시지를 수신하지 못하였을 경우에는 Host 를 멀티캐스트 그룹에서 삭제합니다. (기본값 : 260 초)

Robustness Variable (2-255 sec): 본 설정값은 서브넷 상의 패킷 손실을 조정합니다. 패킷의 손실이 높을 경우, 본 항목의 값을 증가시켜 주십시오. (기본값 : 2 초)

Query Interval (60-600 sec): General Queries 를 보낼 간격입니다. 본 항목의 값에 따라 IGMP 메시지가 증가하거나 감소될 수 있습니다. 값이 클수록 메시지를 보내는 횟수가 적어집니다. (기본값 : 125 초)

Router Timeout (60-600 sec): Router Port 목록을 삭제하는 간격입니다. 본 시간은 Query 메시지를 수신할 때마다 카운트가 재시작되며, 메시지를 수신하지 못하였을 경우에는 Router Port 목록을 삭제합니다. (기본값 : 260 초)

Last Member Query Interval (1-25 sec): Leave 메시지에 대한 응답 대기 시간입니다.

Leave latency 를 조정할 수 있으며, 수치가 낮을수록 그룹 손실을 감지하는 시간을 줄일 수 있습니다.

Max Response Time (10-25 sec): 응답 메시지를 보내기 전, 대기하는 시간입니다. 서브넷 상에 IGMP 트래픽 횟수를 조절할 수 있습니다. (기본값 : 10 초)

Figure 5.48 – L2 Functions > Multicast > IGMP Snooping VLAN Settings

State : 본 기능의 사용여부를 선택합니다. (Enabled : 사용함)

Querier State: 멀티캐스트 클라이언트 상태를 확인하기 위하여 IGMP Query 를 전송합니다.

Fast Leave: Fast Leave 의 사용여부를 선택합니다.

View 버튼을 클릭하면 선택한 VLAN 에 대한 IGMP 내용을 살펴보실 수 있습니다.

Multicast Entry Table						Safeguard
						Back Delete All
Group ID	VLAN ID	VLAN Name	Multicast Group	Multicast MAC address	Member Port	Delete
001	1	default	239.255.255.250	01-00-5E-7F-FF-FA	01	Delete

Figure 5.45 – L2 Functions > Multicast > IGMP Multicast Entry Table

특정 목록을 삭제하시려면 해당 목록의 **Delete** 버튼을 클릭하여 주십시오. **Delete All** 을 클릭하시면 모든 목록이 삭제됩니다.

L2 Functions > Multicast > Multicast Forwarding

고정 멀티캐스트 목록을 표시합니다.

Multicast Forwarding Settings												Safeguard
VID												
Multicast MAC Address												Add
Port	Select All	01	02	03	04	05	06	07	08	09	10	
Member	All	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
None	All	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	
Total Static Entries: 0												
VID	MAC Address	Member Ports								Delete		

Figure 5.49 – L2 Functions > Multicast > Multicast Forwarding

VID: MAC Address 가 포함된 VID 를 입력합니다.

Multicast MAC Address: 멀티캐스트 패킷을 전송하는 고정 MAC Address 를 입력합니다.

Port Settings: 고정 멀티캐스트 그룹으로 포함할 포트를 선택합니다.

Member - 멀티캐스트 고정 그룹으로 포함시킵니다.

None - 멀티캐스트 그룹에 포함시키지 않습니다.

L2 Functions > Multicast > Multicast Filtering Mode

VLAN 기반의 IGMP 그룹 필터 규칙을 설정합니다.

Multicast Filtering		Safeguard
VLAN ID	Filtering Mode	
	Forward Unregistered Groups	
		Apply
Multicast Filtering Mode Table		
Multicast Filtering Mode	VLAN ID	
Forward Unregistered Groups	1	
Filter Unregistered Groups		

Figure 5.50 – L2 Functions > Multicast > Multicast Filtering Mode

VLAN ID: 설정할 VLAN ID 를 입력합니다.

Filtering Mode:

Forward Unregistered Groups: 등록하지 않은 VLAN 그룹까지도 멀티캐스트 패킷을 전송합니다.

Filter Unregistered Groups: 등록된 VLAN 그룹내에만 멀티캐스트 패킷을 전송합니다.

변경한 설정을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

L2 Functions > SNTP > Time Settings

본 스위치 장비의 시스템 시간을 현재 시간과 동기화합니다.

Time Settings Safeguard

Clock Source: ☒ Local ☐ SNTP

Current Time: 01/01/2012 04:48:14

SNTP Server Settings

SNTP First Server: ☒ IPv4 ☐ IPv6

SNTP Second Server: ☒ IPv4 ☐ IPv6

SNTP Poll Interval (30-99999): sec

☒ **Manually Time Settings**

Date (DD/MM/YYYY):

Time (HH:MM:SS):

☐ **Sync To PC**

Date (DD/MM/YYYY):

Time (HH:MM:SS):

Figure 5.51 – L2 Functions > SNTP > Time Settings

Clock Source: 시스템 시간을 동기화할 서버의 위치를 지정합니다.

Local - 직접 시스템 시간을 설정하거나 스위치에 연결된 PC의 시간과 동기화합니다.

SNTP - 외부 네트워크 망의 SNTP 서버와 동기화합니다.

Current Time: 현재의 시스템 시간이 표시됩니다.

SNTP를 이용하여 시스템 시간을 동기화하고자 할 경우,

SNTP First Server: 기본 SNTP 서버 주소를 입력합니다.

SNTP Second Server: 보조 SNTP 서버 주소를 입력합니다.

SNTP Poll Interval in Seconds (30-99999): SNTP 서버와 동기화하는 주기(간격)를 설정합니다.

변경한 설정을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

Local을 선택한 경우,

Manually set current time: 시스템 시간을 직접 입력합니다.

Set time from PC: 현재 설정화면에 접속한 PC의 시간과 동기화합니다.

L2 Functions > SNTP > TimeZone Settings

SNTP와 동기화하기 위한 TimeZone을 설정합니다.

TimeZone Settings Safeguard

Daylight Saving Time: ☐ Enabled ☒ Disabled

Daylight Saving Time Offset: min

Time Zone Offset GMT +/-HH:MM:

Daylight Saving Time Settings

From: Month / Day:

From: HH / MM:

To: Month / Day:

To: HH / MM:

Figure 5.52 – L2 Functions > SNTP > TimeZone Settings

Daylight Saving Time State: DST 사용여부를 선택합니다. (Enabled : 사용함)

Daylight Saving Time Offset: DST offset 시간을 설정합니다. (30, 60, 90, 120 분)

Time Zone Offset GMT +/- HH:MM: 표준시간대를 선택합니다.

Daylight Saving Time Settings:

From: Month / Day: DST 적용 시작일을 선택합니다.

From: HH:MM: DST 적용 시작 시간을 선택합니다.

To: Month / Day: DST 적용 종료일을 선택합니다.

To: HH:MM: DST 적용 종료 시간을 선택합니다.

변경한 설정을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

L2 Functions > LLDP > LLDP Global Settings

IEEE 802.1AB 표준의 **LLDP (Link Layer Discovery Protocol)** 지원 기능을 설정합니다.

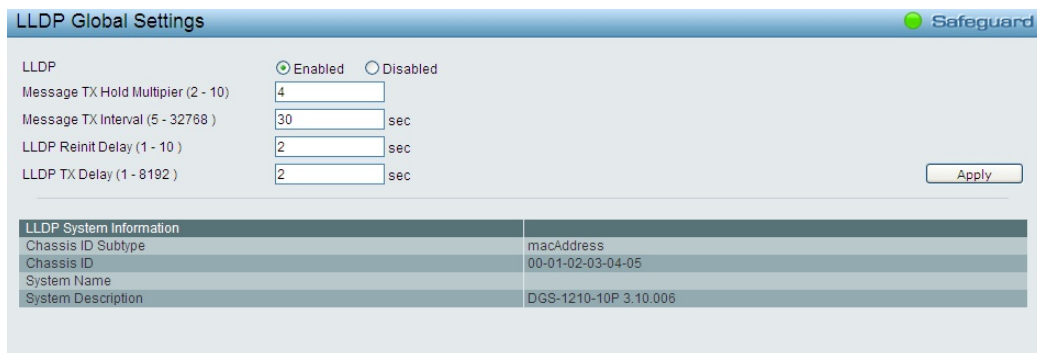


Figure 5.53 – L2 Functions > LLDP > LLDP Global Settings

LLDP: LLDP 사용여부를 선택합니다. (Enabled : 사용함)

Message TX Hold Multiplier (2-10): LLDPDU의 TTL 값을 입력합니다. (기본값 : 4)

Message TX Interval (5-32768): LLDP 프레임 간격을 입력합니다. (기본값 : 30 초)

LLDP Reinit Delay (1-10): LLDP 재시도 시간을 설정합니다. (기본값 : 2 초)

LLDP TX Delay (1-8192): LLDP 프레임 전송 대기 시간을 설정합니다. (기본값 : 2 초)

L2 Functions > LLDP > LLDP MED Settings

LLDP MDI TLV를 이용하여 802.3at 장비의 소비 전력량을 예측하게 됩니다.

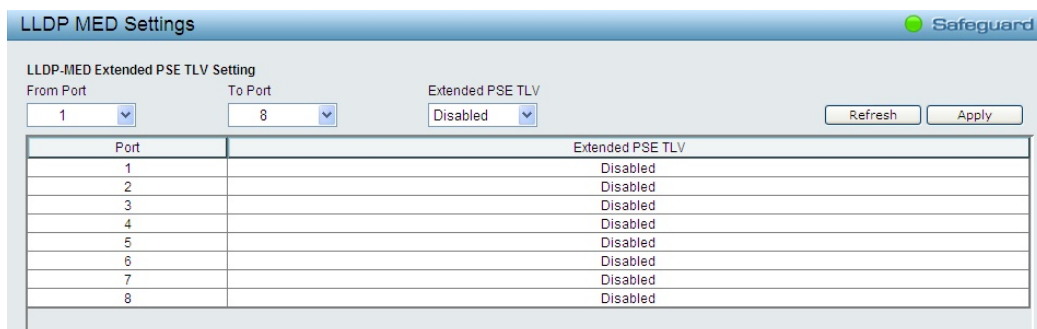


Figure 5.54 – L2 Functions > LLDP > LLDP MED Settings

L2 Functions > LLDP > LLDP Port Settings

LLDP 포트 정보를 표시합니다.

Port	Notification State	Admin Status	Port Description	System Name	System Description	System Capabilities
1	Disabled	TX_and_RX	Disabled	Enabled	Enabled	Disabled
2	Disabled	TX_and_RX	Disabled	Enabled	Enabled	Disabled
3	Disabled	TX_and_RX	Disabled	Enabled	Enabled	Disabled
4	Disabled	TX_and_RX	Disabled	Enabled	Enabled	Disabled
5	Disabled	TX_and_RX	Disabled	Enabled	Enabled	Disabled
6	Disabled	TX_and_RX	Disabled	Enabled	Enabled	Disabled
7	Disabled	TX_and_RX	Disabled	Enabled	Enabled	Disabled
8	Disabled	TX_and_RX	Disabled	Enabled	Enabled	Disabled
9	Disabled	TX_and_RX	Disabled	Enabled	Enabled	Disabled
10	Disabled	TX_and_RX	Disabled	Enabled	Enabled	Disabled

Figure 5.55 – L2 Functions > LLDP > LLDP Port Settings

From Port/ To Port: 포트의 범위를 선택합니다.

Notification State: LLDP 구성값이 변경되었을 때, 알림 전송여부를 선택합니다.

Enabled – LLDP notification 보냅니다.

Disabled – LLDP notification 보내지 않습니다. (기본값)

Admin Status: LLDP 전송방식을 선택합니다.

TX_Only – LLDP 패킷을 송신만 합니다.

RX_Only – LLDP 패킷을 수신만 합니다.

TX_and_RX – LLDP 패킷을 송수신 합니다.

Disabled – LLDP 패킷 송수신을 하지 않습니다.

Port Description: Port Description TLV 사용여부를 선택합니다.

Enabled – Port Description TLV 를 사용합니다.

Disabled – Port Description TLV 를 사용하지 않습니다.

System Name: System Name TLV 사용여부를 선택합니다.

Enabled – System Name TLV 를 사용합니다.

Disabled – System Name TLV 를 사용하지 않습니다.

System Description: System Description TLV 사용여부를 선택합니다.

Enabled –System Description TLV 를 사용합니다.

Disabled –System Description TLV 를 사용하지 않습니다.

System Capabilities: System Capabilities TLV 사용여부를 선택합니다.

Enabled –System Capabilities TLV 를 사용합니다.

Disabled –System Capabilities TLV 를 사용하지 않습니다.

변경한 설정을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

L2 Functions > LLDP > 802.1 Extension TLV

802.1 Extension TLV 를 설정합니다.

Port	Port VLAN ID	VLAN ID	Protocol Identity
1	Disabled	(None)	(None)
2	Disabled	(None)	(None)
3	Disabled	(None)	(None)
4	Disabled	(None)	(None)
5	Disabled	(None)	(None)
6	Disabled	(None)	(None)
7	Disabled	(None)	(None)
8	Disabled	(None)	(None)
9	Disabled	(None)	(None)
10	Disabled	(None)	(None)

Figure 5.56 – L2 Functions > LLDP > 802.1 Extension TLV Port Settings

From Port / To Port : 본 기능을 적용할 포트 범위를 선택합니다.

Port VLAN ID : VLAN ID 사용여부를 선택합니다.

VLAN Name : LLDP 포트에 대하여 VLAN 이름의 사용여부를 선택 입력합니다.

Protocol Identity : EAPOL, LACP, GVRP, STP, ALL 중에 사용하고자 하는 Identity 를 선택합니다.

변경한 설정을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

L2 Functions > LLDP > 802.3 Extension TLV

802.3 Extension 정보와 Parameter 값의 표시여부를 설정합니다.

Port	MAC/PHY Configuration/Status	Power Via MDI	Link Aggregation	Maximum Frame Size
1	Disabled	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled	Disabled

Figure 5.57 – L2 Functions > LLDP > 802.3 Extension TLV Port Settings

From Port/To Port: 설정을 적용할 포트범위를 선택합니다.

MAC/PHY Configuration/Status: MAC/PHY Configuration 상태의 표시여부를 선택합니다.

Enabled – MAC/PHY Configuration Status 상태를 표시합니다.

Disabled – MAC/PHY Configuration Status 상태를 표시하지 않습니다.

Power via MDI: Power via MDI 지원여부를 선택합니다.

Enabled – Power via MDI 를 사용합니다.

Disabled – Power via MDI 를 사용하지 않습니다.

Link Aggregation: Link Aggregation 상태의 표시여부를 선택합니다.

Enabled – Link Aggregation 상태를 표시합니다.

Disabled – Link Aggregation 상태를 표시하지 않습니다.

Maximum Frame Size: Maximum Frame Size 표시여부를 선택합니다.

Enabled – Maximum Frame Size 를 표시합니다.

Disabled – Maximum Frame Size 를 표시하지 않습니다.

변경한 설정을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

L2 Functions > LLDP > LLDP Management Address Settings

전송된 LLDP 정보가 포함된 관리 주소를 설정할 수 있습니다.

Port	Enabled Management Address	Port State
01	None	Disabled
02	None	Disabled
03	None	Disabled
04	None	Disabled
05	None	Disabled
06	None	Disabled
07	None	Disabled
08	None	Disabled
09	None	Disabled
10	None	Disabled

Figure 5.58 – L2 Functions > LLDP > LLDP Management Address Settings

From Port/To Port: 설정을 적용할 포트범위를 선택합니다.

Address Type: LLDP 주소 방식을 선택하는 부분으로 IPv4 고정입니다.

Address: IPv4 주소를 입력합니다.

Port State: 해당 포트의 동작/사용여부를 선택합니다.

Enabled – 지정한 포트를 사용합니다.

Disabled – 지정한 포트를 사용하지 않습니다.

변경한 설정을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

L2 Functions > LLDP > LLDP Management Address Table

세부 LLDP 관리 주소 정보를 표시합니다.

No.	Subtype	Management Address	IF Type	OID	Advertising Ports
1	IPv4	10.90.90.90	ifIndex	1.3.6.1.2.1.2.2.1.1	(NONE)

Figure 5.59 – L2 Functions > LLDP > LLDP Management Address Table

Management Address: IPv4 혹은 IPv6 주소를 입력한 후, **Search** 버튼을 클릭합니다. 해당 정보가 목록에 표시됩니다.

Subtype: 관리 주소 형식(종류)을 표시합니다. (IPv4, MAC 등)

Management Address: IP 주소가 표시됩니다.

IF Type: IF 형식이 표시됩니다.

OID: SNMP OID 가 표시됩니다.

Advertising Ports: Advertising 포트가 표시됩니다.

L2 Functions > LLDP > LLDP Local Port Table

LLDP 로컬 포트 정보를 표시합니다.

LLDP Local Port Brief Table					Safeguard	
Port	Port ID Subtype	Port ID	Port Description	Normal	Detailed	
01	Interface Alias	Slot0/1	Ethernet Interface	View	View	
02	Interface Alias	Slot0/2	Ethernet Interface	View	View	
03	Interface Alias	Slot0/3	Ethernet Interface	View	View	
04	Interface Alias	Slot0/4	Ethernet Interface	View	View	
05	Interface Alias	Slot0/5	Ethernet Interface	View	View	
06	Interface Alias	Slot0/6	Ethernet Interface	View	View	
07	Interface Alias	Slot0/7	Ethernet Interface	View	View	
08	Interface Alias	Slot0/8	Ethernet Interface	View	View	
09	Interface Alias	Slot0/9	Ethernet Interface	View	View	
10	Interface Alias	Slot0/10	Ethernet Interface	View	View	

Figure 5.60 – L2 Functions > LLDP > LLDP Local Port Table

Port : 포트 번호입니다.

Port ID Subtype: Port ID Subtype 을 표시합니다.

Port ID: Port ID (Unit number/Port number) 를 표시합니다.

Port Description: Port description 을 표시합니다.

세부 정보를 확인하시려면 **View** 버튼을 클릭하여 주십시오.

LLDP Local Port Normal Table		Safeguard	
No.	1		
Port Id Subtype	Interface Alias		
Port Id	Slot0/1		
Port Description	Ethernet Interface		
Port VID	1		
Management Address Count	1		
PPVID Entries Count	0		
VLAN Name Entries Count	1		
Protocol Identity Entries Count	0		
MAC/PHY Configuration/Status	See detail		
Power Via MDI	See detail		
Link Aggregation	See detail		
Maximum Frame Size	1522		
Show LLDP Local Port Brief Table			
Show LLDP Local Port Detailed Table			

Figure 5.61 – L2 Functions > LLDP > LLDP Local Port Normal Table

LLDP Local Port Detailed Table



Port ID : 1

Port Id Subtype : Interface Alias

Port Id : Slot0/1

Port Description : Ethernet Interface

Port PVID : 1

Management Address Count : 1

SubType : IPv4

Address : 10.90.90.90

IF Type : ifindex

OID : 1.3.6.1.2.1.2.2.1.1

PPVID Entries Count : 0

(NONE)

VLAN Name Entries Count : 1

Entry : 1

VLAN ID : 1

VLAN Name : default

Protocol Identity Entries Count : 0

(NONE)

MAC/PHY Configuration/Status :

Auto-negotiation Support : Supported

Auto-negotiation Enabled : Enabled

Auto-negotiation Advertised Capability : 0000(hex)

Auto-negotiation Operational MAU Type : 001e(hex)

Power Via MDI :

Link Aggregation :

Aggregation Capability : Not Aggregated

Aggregation Status : Not Currently In Aggregation

Aggregation Port ID : 1

Maximum Frame Size : 1522

[Show LLDP Local Port Brief Table](#)

[Show LLDP Local Port Normal Table](#)

Figure 5.62 – L2 Functions > LLDP > LLDP Local Port Detailed Table

L2 Functions > LLDP > LLDP Remote Port Table

LLDP Remote Port Brief 를 확인하시려면, 포트 번호를 선택하고 Search 버튼을 클릭하여 주십시오.

LLDP Remote Port Brief Table

Safeguard

Port

01

▼

Search

Port ID : 1

Remote Entities Count : 0

(NONE)

Normal : [View Normal](#)

Detailed : [View Detailed](#)

Figure 5.63 – L2 Functions > LLDP > LLDP Remote Port Table

LLDP Remote Port Normal Table		Safeguard
Port ID : 1		
Remote Entities Count : 0		
(NONE)		
Show LLDP Remote Port Brief Table Show LLDP Remote Port Detailed Table		

Figure 5.64 – L2 Functions > LLDP > LLDP Remote Port Normal Table

LLDP Remote Port Detailed Table		Safeguard
Port ID : 1		
Remote Entities Count : 0		
(NONE)		
Show LLDP Remote Port Brief Table Show LLDP Remote Port Normal Table		

Figure 5.65 – L2 Functions > LLDP > LLDP Remote Port Detailed Table

L2 Functions > LLDP > LLDP Statistics

LLDP 트래픽 상태를 표시합니다.

LLDP Statistics Table

Safeguard

LLDP Statistics System

Last Change Time	0
Number of Table Insert	0
Number of Table Delete	0
Number of Table Drop	0
Number of Table Age Out	0

LLDP Port Statistics

Refresh

Clear

Port	TxPort Frames	RxPortFrames Discarded	RxPort FramesErrors	RxPort Frames	RxPortTLVs Discarded	RxPortTLVs Unrecognized	RxPort Ageouts
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0

Figure 5.66 – L2 Functions > LLDP > LLDP Statistics

LLDP Statistics System

Last Change Time – 목록이 최종 갱신된 시간을 표시합니다.

Number of Table Insert – 새롭게 추가된 목록의 개수를 표시합니다.

Number of Table Delete – 삭제된 목록의 개수를 표시합니다.

Number of Table Drop – 테이블 목록 허용 용량의 초과로 인하여 폐기된 목록의 개수를 표시합니다.

Number of Table Age Out – 시간이 만료된 목록의 개수를 표시합니다.

LLDP Port Statistics

TxPort FramesTotal – LLDP 프레임 전송량을 표시합니다.

RxPort FramesDiscarded – 수신된 LLDP 프레임 중 폐기된 프레임수를 표시합니다.

RxPort FramesErrors – 수신된 LLDP 프레임 중 오류가 발생한 프레임수를 표시합니다.

RxPort Frames – 수신된 LLDP 프레임수를 표시합니다.

RxPortTLVsDiscarded – LLDP-TLV 프레임중 폐기된 프레임수를 표시합니다.

RxPortTLVsUnrecognized – 규정된 TLV 프레임수를 표시합니다.

RxPort Ageouts – LLDP 프레임의 유효시간을 표시합니다.

내용을 갱신하시려면 **Refresh** 버튼을 클릭하여 주십시오.

데이터를 초기화하시려면 **Clear** 버튼을 클릭하여 주십시오.

QoS > Bandwidth Control

지정한 포트에 대한 데이터 전송 속도를 조정할 수 있습니다.

Bandwidth Control				
From Port	To Port	Type	No Limit	Rate(64-1024000)
01	10	Rx	Disabled	Kbits/sec
Apply				
Port	Tx Rate (kbits/sec)		Rx Rate (kbits/sec)	
01	No Limit		No Limit	
02	No Limit		No Limit	
03	No Limit		No Limit	
04	No Limit		No Limit	
05	No Limit		No Limit	
06	No Limit		No Limit	
07	No Limit		No Limit	
08	No Limit		No Limit	
09	No Limit		No Limit	
10	No Limit		No Limit	

Figure 5.67 – QoS > Bandwidth Control

From Port / To Port: 설정할 포트 범위를 선택합니다.

Type: RX (수신), TX (송신), Both(양방향) 중에 설정을 적용할 항목을 선택합니다.

No Limit: 전송 속도를 제한하지 않으시려면 본 항목의 값을 **Enabled** 로 선택하여 주십시오.

Rate (64-1024000): 제한할 전송속도를 입력합니다. (범위 : 64 ~ 1024000 kbps)

변경한 설정을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

QoS > 802.1p/DSCP/ToS

QoS 는 IEEE 802.1p 표준 규격을 지원합니다.

VoIP, 웹브라우저, 파일서버 및 화상회의 등 더 넓은 대역폭이 요구되거나 전송에 대한 우선순위가 요구되는 트래픽에 대하여 전송에 대한 안정성을 확보할 수 있습니다.

Figure 5.68 – QoS > 802.1p/DSCP/ToS

Select QoS Mode: 802.1p, DSCP, ToS 중 설정하고자 하는 QoS 방식을 선택합니다.

Queuing Mechanism

Strict Priority: 절대적인 전송의 우선순위를 부여하는 방식입니다.

WRR: Weighted Round-Robin 알고리즘으로 전송할 패킷 대역폭 비중을 조정하는 방식입니다.

From Port / To Port: 적용할 포트의 범위를 선택합니다.

Priority: Highest, High, Medium, Low 중 설정하고자 하는 우선순위를 선택합니다.

변경을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

QoS > IPv6 Traffic Class Priority Settings

IPv6 트래픽에 대한 우선순위를 설정합니다.

Figure 5.69 – QoS > IPv6 Traffic Class Priority Settings

IPv6 Traffic Class (0-255): IPv6 클래스 값을 입력합니다.

Priority: Highest, High, Medium, Low 중 설정할 우선순위를 선택합니다.

변경한 사항을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

QoS > TCP/UDP Port Priority Settings

TCP/UDP 포트 기반의 우선순위를 설정합니다.

Figure 5.70 – QoS > TCP/UDP Port Priority Settings

TCP/UDP: 사용할 프로토콜의 종류를 선택합니다.

TCP/UDP Port (0-65535): 설정할 포트번호를 입력합니다.

Priority: Highest, High, Medium, Low 중 설정할 우선순위를 선택합니다.

변경한 사항을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

Security > Trusted Host

본 스위치 장비에 대한 원격 관리를 허용할 Host 를 지정하는 기능입니다.

Figure 5.71 Security > Trusted Host

Trusted Host: 본 기능의 사용여부를 선택합니다.

지정할 IP 주소값을 입력합니다.

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

등록한 목록을 삭제하시려면 **Delete** 버튼을 클릭하여 주십시오.

Security > Port Security

포트별 최대 MAC Address 수를 지정함으로써 추가로 인가되지 않은 MAC Address 로부터 전송되는 트래픽을 차단하는 기능입니다.

설정할 포트의 범위를 선택하고, Admin State 를 Enabled 로 변경합니다.

Max Learning Address 를 입력하고 Apply 버튼을 클릭하여 주십시오.

Port	Admin State	Max Learning Address
01	Disabled	0
02	Disabled	0
03	Disabled	0
04	Disabled	0
05	Disabled	0
06	Disabled	0
07	Disabled	0
08	Disabled	0
09	Disabled	0
10	Disabled	0

Figure 5.72 – Security > Port Security

Security > Traffic Segmentation

지정한 포트에서 수신되는 트래픽을 선택한 포트만 송신하도록 하는 기능입니다.

Port	Forwarding Port
1	1-10
2	1-10
3	1-10
4	1-10
5	1-10
6	1-10
7	1-10
8	1-10
9	1-10
10	1-10

Figure 5.73 – Security > Traffic Segmentation

설정하시려면 From Port 에 출발지 포트를 선택하고 목적지 포트를 체크하신 후, Apply 버튼을 클릭하여 주십시오

Security > Safeguard Engine

Virus 나 Worm 과 같은 네트워크 공격으로 인하여 CPU 부하가 발생하는 문제를 자동으로 차단합니다.

D-Link Safeguard Engine is a robust and innovative technology developed by D-Link, which will automatically throttle the impact of packet flooding into the switch's CPU.
It will keep D-Link Switches better protected from being too frequently interrupted by malicious viruses or worm attacks.

Figure 5.74 – Security > Safeguard Engine

Security > Storm Control

브로드캐스트, 멀티캐스트, 미확인된 유니캐스트 패킷에 대해 지정한 수치보다 초과하는 트래픽에 대해서는 Storm 으로 간주하고 해당 패킷의 전송을 차단합니다.

Figure 5.75 – Security > Storm Control

Storm Control Type: Broadcast Only, Multicast & Broadcast, Multicast & Broadcast & Unknown Unicast 중 설정하고자 하는 Storm 의 종류를 선택합니다.

Threshold (64Kbps * N): 허용치를 64Kbps X N 으로 계산하여 해당 수치를 입력합니다.

변경된 설정을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.

Security > ARP Spoofing Prevention

ARP spoofing (일명 ARP poisoning) 에 대한 공격을 차단하기 위한 보안설정입니다.

IP Address, MAC Address 및 Ports 번호가 모두 일치한 패킷만 전송합니다.

Figure 5.76 – Security > ARP Spoofing Prevention

IP Address, MAC Address, Ports 를 모두 입력하고 **Add** 버튼을 클릭합니다.

Security > DHCP Server Screening

DHCP Server Trusted Port 로 지정한 포트 외에 전송되는 DHCP 패킷을 차단합니다.

DHCP Server Screening Settings

DHCP Server Trusted Port Settings

Port	01	02	03	04	05
	☒	☒	☒	☒	☒
Port	6	7	8	9	10
	☒	☒	☒	☒	☒

Trusted DHCP Server IP Settings

☒ IPv4

☐ IPv6 Ex(1234::1234)

Trusted DHCP Server IP Lists

Maximum 5 entries.

Index	IP Address	Delete
-------	------------	--------

Figure 5.77 – Security > DHCP Server Screening

Trusted DHCP Server IP Settings: Trusted DHCP Server 의 IP 주소를 입력하여 지정한 Server 만 등록할 수 있습니다.

Security > SSL Settings

스위치 설정화면 접속에 대한 보안 접속 여부를 선택합니다.

SSL Settings

SSL State ☐ Enabled ☒ Disabled

HTTP will be disabled if SSL is enabled.

SSL Ciphersuite Settings

RSA-NUL-MD5	☒ Enabled	☐ Disabled
RSA-NUL-SHA1	☒ Enabled	☐ Disabled
RSA-DES-SHA1	☒ Enabled	☐ Disabled
RSA-3DES-SHA1	☒ Enabled	☐ Disabled
DH-RSA-DES-SHA1	☒ Enabled	☐ Disabled
DH-RSA-3DES-SHA1	☒ Enabled	☐ Disabled
RSA-EXP1024-DES-SHA1	☒ Enabled	☐ Disabled

Figure 5.78 – Security > SSL Settings



NOTE: SSL 기능을 사용할 경우, 암호화로 인하여 설정화면 접속 및 설정 페이지 표시가 일반 접속에 비하여 지연될 수 있습니다.

Security > Smart Binding > Smart Binding Settings

MAC 주소와 IP 주소가 일치하는 단말에서 전송된 패킷만 허용하는 보안 기능입니다.

본 기능은 포트 기반으로 동작하며 IMPB white list 리스트에 등록된 단말만 패킷 전송을 허용합니다.

Smart Binding Settings Safeguard

From Port: 01 To Port: 10 State: Disabled

Packet Inspection: ARP Inspection DHCP Snooping: Disabled Apply

Port	Admin State	Also inspect IP packets	DHCP Snooping
01	Disabled	Enabled	Disabled
02	Disabled	Enabled	Disabled
03	Disabled	Enabled	Disabled
04	Disabled	Enabled	Disabled
05	Disabled	Enabled	Disabled
06	Disabled	Enabled	Disabled
07	Disabled	Enabled	Disabled
08	Disabled	Enabled	Disabled
09	Disabled	Enabled	Disabled
10	Disabled	Enabled	Disabled

Figure 5.79 – Security > Smart Binding > Smart Binding Settings

From Port/ To Port: 본 설정을 적용할 포트 범위를 선택합니다.

State: Smart Binding 적용여부를 선택합니다.

Enabled – Smart Binding 적용함.

Disabled – Smart Binding 적용하지 않음

Packet Inspection: ARP Inspection 와 IP+ARP Inspection 중에 선택 적용하실 수 있습니다.

ARP Inspection 은 스위치가 수신된 ARP 패킷을 검사하고 Smart Binding 의 White List 목록과 비교합니다.

ARP 패킷의 IP-MAC 정보가 White List 상에 없을 경우, 해당 MAC 주소를 차단합니다. CPU 의 사용량을 줄이는 효과는 있으나 Unicast IP 패킷 공격(DoS 공격)은 ARP 패킷을 전송하는 방법이 아니기 때문에 이를 차단하진 못합니다.

ARP+IP Inspection 은 스위치가 수신된 ARP 와 IP 패킷을 모두 검사하고 IMPB White List 목록과 비교하여 목록에 없는 MAC 주소를 차단하기에 DoS 공격까지 차단할 수 있습니다.

DHCP Snooping: DHCP 서버와 클라이언트로부터 수신된 패킷을 확인하여 White List 에 등록합니다.

변경된 설정을 적용하시려면 **Apply** 버튼을 클릭합니다.

Security > Smart Binding > Smart Binding

IP-MAC-Port Binding 을 직접 등록하거나 지정한 IP 주소 대역을 모두 검색하고 선택하여 등록할 수 있습니다.

Smart Binding Safeguard

Manual Binding

IP Address: MAC Address: Port: Add

Auto Scan

Enter a range of IP address to scan all devices in the network.

IP Address From: To: Scan

Select All Clear All Apply

VLAN	IP Address	MAC Address	Port	Binding
------	------------	-------------	------	---------

Figure 5.80 – Security > Smart Binding > Smart Binding

Manual Binding 설정

IP Address: IP 주소를 입력합니다.

MAC Address: IP 주소에 해당하는 MAC 주소를 등록합니다.

Port: IP-MAC binding 목록에 등록할 스위치 포트번호를 입력합니다.

Add 버튼을 클릭하여 목록에 등록합니다.

Auto Scan 설정

IP Address From/To: IP 의 범위를 지정합니다. 또는, 스위치에 연결된 모든 단말을 검색하려면 공란으로 둡니다.

Scan 버튼을 클릭하면 검색결과가 표시됩니다.

Binding: 등록하고자 하는 목록에 체크합니다.

Apply 버튼을 클릭하여 Binding 에 체크한 목록을 등록합니다.

Security > Smart Binding > White List

IP+ARP Inspection 모드인 경우, 등록된 IP-MAC-Port Binding 목록을 확인하고 필요한 경우, 등록된 목록을 삭제할 수 있습니다.



Figure 5.81 – Security > Smart Binding > White List

반드시, 스위치 관리를 위한 PC 는 White List 에 등록되어 있어야 합니다.

Security > Smart Binding > Black List

Black List 는 차단할 목록입니다. ARP Inspection 모드인 경우, IP-MAC-Port 정보가 일치하지 않는 ARP 패킷을 보내는 장비가 표시됩니다.

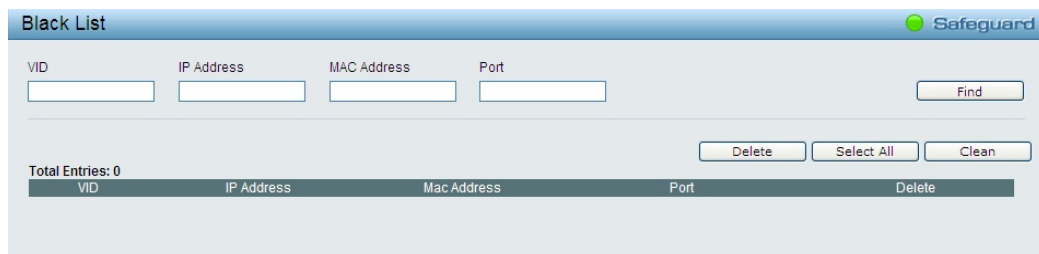


Figure 5.82 – Security > Smart Binding > Black List

해당 조건에 맞게 값을 입력하고 **Find** 버튼을 클릭하여 검색하실 수 있습니다.

VID: 검색하고자 하는 VLAN ID 번호를 입력합니다.

IP Address: 검색하고자 하는 IP Address 를 입력합니다.

MAC Address: 검색하고자 하는 MAC Address 를 입력합니다.

Port: 장치가 연결된 포트번호를 입력합니다.

Delete 항목에 체크후, **Apply** 버튼을 클릭하여 목록을 삭제하실 수 있습니다.

AAA > 802.1X > 802.1X Settings

IEEE 802.1X 는 네트워크 표준 보안을 설정합니다.

802.1X Settings

802.1X ☐ Enabled ☒ Disabled

802.1X Global Settings

Radius Server IP: ☒ IPv4 ☐ IPv6

Key:

Confirm Key:

TxPeriod (1 - 65535 sec):

ReAuthEnabled:

QuietPeriod (0 - 65535 sec):

ServerTimeout (1 - 65535 sec):

SuppTimeout (1 - 65535 sec):

MaxReq (1 - 10):

ReAuthPeriod (1 - 4294967295 sec):

Apply

802.1X Port Access Control

From Port: To Port: Control:

Apply Refresh

Port	Control	Port Status	Session Time	User ID
01	Force Authorized	*	0	*****
02	Force Authorized	*	0	*****
03	Force Authorized	*	0	*****
04	Force Authorized	*	0	*****
05	Force Authorized	*	0	*****
06	Force Authorized	*	0	*****
07	Force Authorized	*	0	*****
08	Force Authorized	*	0	*****
09	Force Authorized	*	0	*****
10	Force Authorized	*	0	*****

Figure 5.83 – Security > 802.1X > 802.1X Settings

RADIUS Server IP: RADIUS 서버 IP 주소를 입력합니다.

Key: RADIUS 서버키를 입력합니다. (최대 32 자)

Confirm Key: 상기 Key 값을 한번 더 입력합니다.

TxPeriod (1 – 65535 sec): TxPeriod 를 설정합니다. 본 값은 클라이언트로 전송된 EAP Request/Identity 패킷에 의해 결정됩니다.

ReAuthEnabled: 재인증 진행 여부를 선택합니다.

QuietPeriod (0 – 65535 sec): 클라이언트 인증 실패시 대기하는 시간을 설정합니다.

SuppTimeout (1 – 65535 sec): 인증서버와 클라이언트간 변경에 대한 만료시간을 설정합니다.

ServerTimeout (1 – 65535 sec): 인증서버의 응답을 재전송하기 전에 클라이언트로부터의 응답을 대기하는 시간입니다.

MaxReq (1 – 10): 인증 세션이 만료되기 전에 EAP 요청(MD-5) 을 재전송하는 횟수입니다.

ReAuthPeriod (1 – 4294967295 sec): 재인증 진행 기능이 켜져 있을 경우에만 적용되며, 스위치가 인증서버와 인증을 진행할 주기를 입력합니다.

From Ports / To Ports: 802.1X 인증을 적용할 포트범위를 선택합니다.

802.1X Port Access Control: "Force Authorized", "Force Unauthorized", "Auto" 중 선택합니다.

- **Force Authorized:** 802.1X 인증을 사용하지 않습니다. 연결된 클라이언트는 인증없이 접속이 가능합니다.
- **Force Unauthorized:** 해당 포트가 항상 미인증 상태로 되어, 클라이언트 인증이 진행되지 않습니다.
- **Auto:** 연결된 클라이언트가 802.1X 인증을 진행한 후, 네트워크 접속이 가능합니다.

ACL > ACL Wizard

MAC 주소 또는 IP 주소 기반의 패킷의 전송여부를 제어합니다.

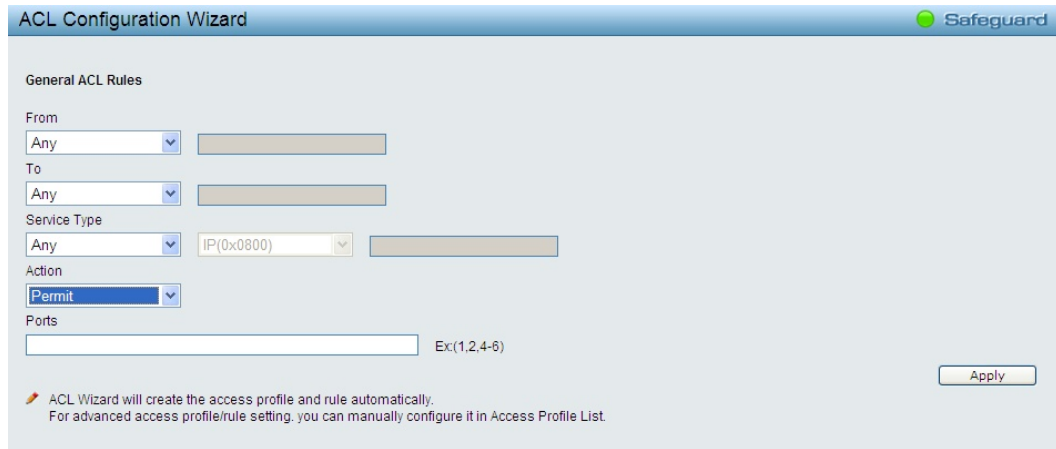


Figure 5.84 – ACL > ACL Wizard

From

Any - 모든 source(송신단말)의 패킷에 대해 규칙을 적용합니다.

MAC Address - 등록된 MAC 주소를 보유한 source(송신단말)에 대해 규칙을 적용합니다.

IPv4 Address - 등록된 IPv4 주소를 보유한 source(송신단말)에 대해 규칙을 적용합니다.

IPv6 Address - 등록된 IPv6 주소를 보유한 source(송신단말)에 대해 규칙을 적용합니다.

To

Any - 모든 destination(수신단말)의 패킷에 대해 규칙을 적용합니다.

MAC Address - 등록된 MAC 주소를 보유한 destination(수신단말)에 대해 규칙을 적용합니다.

IPv4 Address - 등록된 IPv4 주소를 보유한 destination(수신단말)에 대해 규칙을 적용합니다.

IPv6 Address - 등록된 IPv6 주소를 보유한 destination(수신단말)에 대해 규칙을 적용합니다.

Service Type

Any - 모든 패킷을 확인합니다.

Ether type - Ethernet type, IP, ARP 또는 지정한 주소에 대한 패킷을 확인합니다.

ICMP All - 모든 ICMP 패킷을 확인합니다.

IGMP - IGMP 패킷을 확인합니다.

TCP All - 모든 TCP 패킷을 확인합니다.

TCP Source Port - 지정한 송신 TCP 패킷의 포트번호를 확인합니다.

TCP Destination Port - 지정한 수신 TCP 패킷의 포트번호를 확인합니다.

UDP All - 모든 UDP 패킷을 확인합니다.

UDP Source Port - 지정한 송신 UDP 패킷의 포트번호를 확인합니다.

UDP Destination Port - 지정한 수신 UDP 패킷의 포트번호를 확인합니다.

Action: 패킷전송을 허용하시려면 **Permit**를 선택하고, 차단하시려면 **Deny**를 선택합니다.

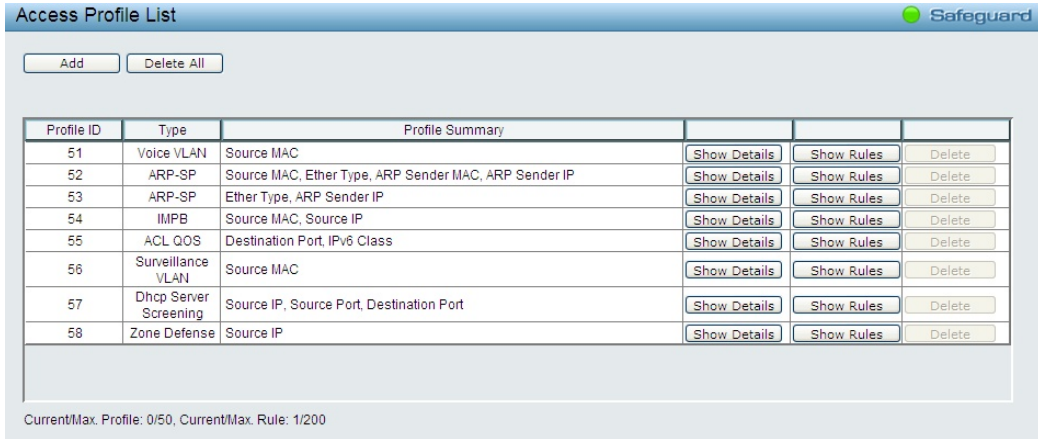
Ports: 적용할 포트 범위를 입력합니다.



NOTE: ACL 규칙이 중복된 경우에는 Rule ID가 낮은 항목이 우선 적용됩니다.

ACL > ACL Profile List

등록된 ACL 규칙을 표시합니다.



Profile ID	Type	Profile Summary			
51	Voice VLAN	Source MAC	Show Details	Show Rules	Delete
52	ARP-SP	Source MAC, Ether Type, ARP Sender MAC, ARP Sender IP	Show Details	Show Rules	Delete
53	ARP-SP	Ether Type, ARP Sender IP	Show Details	Show Rules	Delete
54	IMPB	Source MAC, Source IP	Show Details	Show Rules	Delete
55	ACL QOS	Destination Port, IPv6 Class	Show Details	Show Rules	Delete
56	Surveillance VLAN	Source MAC	Show Details	Show Rules	Delete
57	Dhcp Server Screening	Source IP, Source Port, Destination Port	Show Details	Show Rules	Delete
58	Zone Defense	Source IP	Show Details	Show Rules	Delete

Current/Max. Profile: 0/50, Current/Max. Rule: 1/200

Figure 5.85 – ACL > ACL Profile List

Profile ID: 1~50 번 중 선택하여 등록할 수 있습니다.

Type: Profile 의 Type 을 표시합니다. (예를 들어, Normal, Voice VLAN 등)

Profile Summary: Profile 의 요약설명을 표시합니다.

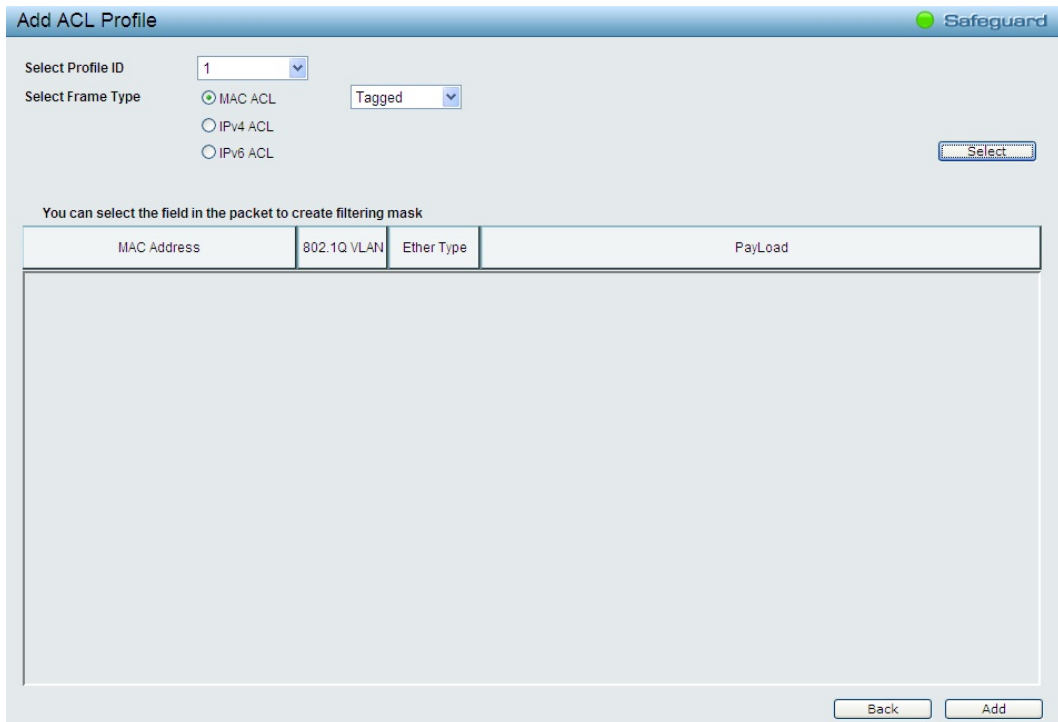
Show Details: Profile 의 세부사항을 표시합니다.

Show Rules: Profile 에 등록된 접속 규칙을 표시합니다.

Edit / New Rules: 선택한 Profile 을 수정하거나 새로운 규칙을 생성합니다.

Delete: 선택한 규칙을 삭제합니다.

Profile 을 추가하시려면 **Add** 버튼을 클릭합니다.



Add ACL Profile

Select Profile ID: 1

Select Frame Type: ☒ MAC ACL ☐ IPv4 ACL ☐ IPv6 ACL

Tagged

Select

You can select the field in the packet to create filtering mask

MAC Address	802.1Q VLAN	Ether Type	PayLoad

Back Add

Figure 5.86 – Add Access Profile

Profile 을 추가하는 방법

1) **Profile ID** 와 **Frame Type** 을 선택합니다.

Figure 5.87 – Add Access Profile

Parameter	Description
Profile ID	1 ~ 50 번 중 선택할 수 있습니다.
Frame Type	ACL 을 적용할 패킷의 Layer 를 선택합니다.
MAC ACL	MAC 주소 Tagged - L2 헤더의 802.1Q 필드를 적용합니다. Untagged - 802.1Q 필드가 없는 L2 헤더를 적용합니다.
IPv4 ACL	IPv4 주소 ICMP - L4 프로토콜인 ICMP 를 확인합니다. IGMP - L4 프로토콜인 IGMP 를 확인합니다. TCP - L4 프로토콜인 TCP 를 확인합니다. UDP - L4 프로토콜인 UDP 를 확인합니다.
IPv6 ACL	IPv6 주소 ICMP - L3 IPv6 프로토콜인 ICMP 를 확인합니다. TCP - L3 IPv6 프로토콜인 TCP 를 확인합니다. UDP - L3 IPv6 프로토콜인 UDP 를 확인합니다.

MAC ACL 의 **Tagged** 를 선택하고 **Select** 버튼을 클릭한 경우, 아래와 같이 각 항목을 추가로 입력합니다.

Figure 5.88 – Add Access Profile (MAC ACL)

항목	설명
Source MAC Mask	source(송신지)의 MAC 주소를 입력합니다. 예)FF-FF-FF-FF-FF-FF
Destination MAC Mask	destination(수신지)의 MAC 주소를 입력합니다.
802.1p	패킷 헤더의 802.1p Priority 값을 확인하시려면 체크합니다.
VLAN ID	패킷 헤더의 802.1Q VLAN ID 를 확인하시려면 체크합니다.
Ether Type	패킷 헤더의 Ether Type 을 확인하시려면 체크합니다.

입력하신 ACL Profile 을 추가하시려면 **Add** 버튼을 클릭합니다.

IPv4 ACL ICMP profile

Figure 5.89 – Add Access Profile (IPv4 ACL ICMP)

항목	설명
Source IP Mask	송신지 IP 주소의 범위를 입력합니다. 예를 들어, 176.212.XX.XX 로 설정하시려면 Mask 값을 255.255.0.0 로 입력합니다.
Destination IP Mask	수신지 IP 주소의 범위를 입력합니다.
ICMP Type	ICMP Type 필드값을 적용하시려면 체크합니다.
ICMP Code	ICMP code 필드값을 적용하시려면 체크합니다.

입력하신 ACL Profile 을 추가하시려면 **Add** 버튼을 클릭합니다.

IPv4 ACL IGMP 프로파일

Add ACL Profile Safeguard

Select Profile ID: 1

Select Frame Type:

- ☐ MAC ACL
- ☒ IPv4 ACL
- ☐ IPv6 ACL

IGMP

Select

You can select the field in the packet to create filtering mask

L2 Header | IPv4 DSCP | IPv4 Address | **IGMP**

IGMP

☐ Type

Back Add

Figure 5.90 – Add Access Profile (IPv4 ACL IGMP)

IPv4 ACL TCP 프로파일

Add ACL Profile Safeguard

Select Profile ID: 1

Select Frame Type:

- ☐ MAC ACL
- ☒ IPv4 ACL
- ☐ IPv6 ACL

TCP

Select

You can select the field in the packet to create filtering mask

L2 Header | IPv4 DSCP | IPv4 Address | **TCP Port** | TCP Flag

TCP Port

☐ Source Port Mask Mask Generate

☐ Destination Port Mask Mask Generate

TCP Flag

☐ TCP Flag

Back Add

Figure 5.91 – Add Access Profile (IPv4 ACL TCP)

항목	설명
Source Port Mask	ACL 규칙에 적용할 송신지 포트범위를 입력합니다. (예를 들어, 0 - 15로 설정하시려면 Mask 값은 FFF0 이 됩니다.)
Destination Port Mask	ACL 규칙에 적용할 수신지 포트범위를 입력합니다. (입력의 예는 상기와 같습니다.)
TCP Flag	TCP Flag Type 필드의 값을 입력합니다.

입력하신 ACL Profile 을 추가하시려면 **Add** 버튼을 클릭합니다.

IPv4 ACL UDP 프로파일

Figure 5.92 – Add Access Profile (IPv4 ACL UDP)

항목	설명
Source Port Mask	ACL 규칙에 적용할 송신지 포트범위를 입력합니다. (예를 들어, 0 - 15로 설정하시려면 Mask 값은 FF 가 됩니다.)
Destination Port Mask	ACL 규칙에 적용할 수신지 포트범위를 입력합니다. (입력의 예는 상기와 같습니다.)

입력하신 ACL Profile 을 추가하시려면 **Add** 버튼을 클릭합니다.



NOTE: 여러 개의 필터링 마스크를 동시에 선택할 수 있습니다.

IPv6 ACL ICMP 프로파일

Figure 5.93 – Add Access Profile (IPv6 ACL ICMP)

항목	설명
Source IP Prefix	ACL 규칙에 적용할 송신지 IPv6 Mask 값을 입력합니다. (예를 들어, 2002:0:0:0:0:0:b0d4:0 를 설정하시려면 Mask 값은 128 이 됩니다.)
Destination IP Prefix	ACL 규칙에 적용할 수신지 IPv6 Mask 값을 입력합니다. (설정의 예는 상기와 같습니다.)
ICMP Type	ICMP Type field 를 적용합니다.
ICMP Code	ICMP code field 를 적용합니다.

입력하신 ACL Profile 을 추가하시려면 **Add** 버튼을 클릭합니다.

IPv6 ACL TCP 프로파일

The screenshot shows the 'Add ACL Profile' window with the following configuration:

- Select Profile ID:** 1
- Select Frame Type:**
 - ☐ MAC ACL
 - ☐ IPv4 ACL
 - ☒ IPv6 ACL
- Protocol:** TCP
- Fields for filtering mask:** L2 Header, IPv6 Class, IPv6 Address (highlighted in red), and TCP Port (highlighted in red).
- IPv6 Address section:**
 - ☐ Source IP Mask [] Mask Generate
 - ☐ Destination IP Mask [] Mask Generate
- TCP Port section:**
 - ☐ Source Port Mask [] Mask Generate
 - ☐ Destination Port Mask [] Mask Generate
- Buttons:** Back, Add, and a Select button.

Figure 5.94 – Add Access Profile (IPv6 ACL TCP)

항목	설명
Source Port Mask	ACL 규칙에 적용할 송신지 포트 마스크 값을 입력합니다. (예를 들어, 0 - 15 를 설정하시려면 Mask 값은 FFF0 이 됩니다.)
Destination Port Mask	ACL 규칙에 적용할 수신지 포트 마스크 값을 입력합니다. (입력의 예는 상기와 같습니다.)

입력하신 ACL Profile 을 추가하시려면 **Add** 버튼을 클릭합니다.

IPv6 ACL UDP 프로파일

The screenshot shows the 'Add ACL Profile' window with the following configuration:

- Select Profile ID:** 1
- Select Frame Type:**
 - ☐ MAC ACL
 - ☐ IPv4 ACL
 - ☒ IPv6 ACL
- Protocol:** UDP
- Fields for filtering mask:** L2 Header, IPv6 Class, IPv6 Address, and UDP Port (highlighted in red).
- UDP Port section:**
 - ☐ Source Port Mask [] Mask Generate
 - ☐ Destination Port Mask [] Mask Generate
- Buttons:** Back, Add, and a Select button.

Figure 5.95 – Add Access Profile (IPv6 ACL UDP)

항목	설명
Source Port Mask	ACL 규칙에 적용할 송신지 포트 마스크값을 입력합니다. (예를 들어, 0 - 15로 설정하시려면 Mask 값은 F가 됩니다.)
Destination Port Mask	ACL 규칙에 적용할 수신지 포트 마스크값을 입력합니다. (입력의 예는 상기와 같습니다.)

입력하신 ACL Profile 을 추가하시려면 **Add** 버튼을 클릭합니다.

2) ACL 규칙을 만드신 후, **Add** 버튼을 클릭합니다.

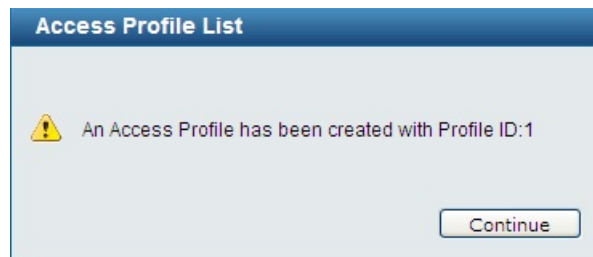


Figure 5.96 – Access Rule List

3) 상기와 같이 **Profile ID** 를 추가하였다는 메시지가 출력됩니다. **Continue** 버튼을 클릭하면 Access Profile List 메인 화면으로 전환되어 추가된 항목을 확인하실 수 있습니다. 해당 규칙의 Access Rule List 를 확인하기 위하여 **Edit / New Rules** 버튼을 클릭합니다.



Figure 5.97 – Access Rule List

Profile ID: 설정한 Profile ID 입니다.

Access ID: Access Rule ID 입니다.

Profile Type: 프로파일 Type 을 표시합니다.

Summary: Access Rule 규칙의 간략 설명을 표시합니다.

Action: 해당 규칙의 동작 여부를 표시합니다.

새로운 규칙을 추가하기 위하여, **Add** 버튼을 클릭합니다.

Figure 5.98 – Add Access Rule

Profile Information 화면으로 **Profile ID** 및 **Ether Type** 등의 정보가 표시됩니다.

아래와 같은 각각의 항목을 입력하여 세부 규칙을 설정합니다.

Access ID: 사용할 Access ID 를 입력합니다. (범위 : 1 ~ 65535)

Type: MAC, IPv4, IPv6 중 Type 이 표시됩니다.

IPv6 Class: 설정할 IPv6 클래스값을 입력합니다. (범위 : 0 ~ 255)

VLAN ID: 설정할 VLAN ID 를 입력합니다.

Destination IPv6 Address: 목적지(수신지) IPv6 address 를 입력합니다.

Source IPv6 Address: 출발지(송신지) IPv6 address 를 입력합니다.

IP Protocol: 설정할 IP 을 표시합니다.

Type: 별도의 Type 을 설정하시려면 해당 값을 입력합니다. (범위 : 0 ~ 255)

Code: 규칙에 적용할 code 값을 입력합니다. (범위 : 0 ~ 255)

Ports: 규칙을 적용할 스위치 포트번호를 입력합니다.

Action: 감지된 패킷이 입력한 규칙과 일치할 경우 해당 패킷의 전송여부를 선택합니다. **Permit** 는 해당 규칙에 해당하는 패킷만 전송하게 됩니다. **Deny** 는 해당하는 패킷을 모두 차단합니다.

설정을 적용하시려면 **Apply** 버튼을 클릭하여 주십시오.



NOTE: Access ID 가 가장 낮은 값이 우선 적용됩니다.

생성된 규칙을 수정하시려면 **Access ID** 를 클릭합니다.

Profile ID	Access ID	Type	Summary	Action	Delete
2	2	IPv6	ICMPv6 Type, ICMPv6 Code, Destination IPv6, Source IPv6, IPv6 class	Permit	Delete

Figure 5.99 – ACL > Access Profile List > Access Rule List

ACL > ACL Finder

설정된 ACL 목록을 검색합니다. 확인하고자 하는 Profile ID 를 선택하시거나 포트 번호를 입력하고 Search 버튼을 클릭합니다. 검색된 Profile 을 삭제하시려면, 해당 목록의 Delete 버튼을 클릭하여 주십시오.

Profile ID	Access ID	Type	Summary	Action	Delete
54	255	IMPB	IP	Deny	Delete

Figure 5.100 – ACL > ACL Finder

PoE > PoE Global Settings

PoE 총 용량과 사용되고 있는 용량을 표시하며, 필요한 경우, 스위치가 지원하는 총 PoE 용량을 조절할 수 있습니다.

PoE Global Settings

PoE Power Threshold (7.1-78.0) Watts

Power Shut Off Sequence

System Power Status

Total PoE Power Budget 78

Power Used 0

Power Left 78

The percentage of system power supplied 0%

1. 7 watts guard band is reserved for system to prevent a PD from being powered off when encountering a sudden increment of PD power supply. When Used Power reaches guard band, a new PD will trigger the action defined in Power Shut Off Sequence.

2. If a sudden increment of a PD power causes PSE power overload, switch will firstly stop power supply to the port with a low priority PD. As a result, high priority PD can work without being affected.

Figure 5.101 – PoE > PoE Global Setting

System Power Threshold: 스위치에 지원할 수 있는 PoE 총량을 조절합니다.

(SPN-12080P : 7.1 ~ 78.0 watts / SPN-14240P : 7.1 ~ 185.0 watts)

Power Shut Off Sequence: 사용되고 있는 PoE 용량이 설정한 PoE 총량을 초과하였을 경우, PoE 동작을 제한하는 방법을 선택합니다.

Deny next port: 포트 우선순위를 무시하고 PoE 를 사용하고 있는 포트 중 마지막 포트의 전력이 차단됩니다.

Deny low priority port: 설정한 포트의 우선 순위에 따라 가장 낮은 순위의 포트의 전력이 차단됩니다.

설정된 내용을 적용하시려면 **Apply** 버튼을 클릭합니다.

System Power Status

Total PoE Power Budget: 스위치가 지원하는 PoE 총량 혹은 현재 설정된 PoE 총량을 표시합니다.

Power Used: 현재 사용되고 있는 PoE 용량을 표시합니다.

Power Left: 남아있는 PoE 용량을 표시합니다.

The percentage of system power supplied: PoE 사용량을 백분율로 표시합니다.

PoE > PoE Port Settings

SPN-12080P/SPN-14240P 는 IEEE 표준 규격 PoE 를 지원합니다. SPN-12080P 는 모든 포트가 IEEE802.3at(15.4W) 와 IEEE802.3at(30W) 를 지원하여 SPN-14240P 는 1~4 번 포트는 두 가지 규격을 모두 지원하고 5~24 번 포트는 IEEE802.3at 만 지원됩니다.

클래스 규격별 지원하는 PoE 는 아래와 같습니다.

Class	Usage	Output power limit by PSE
0	Default	15.4W
1	Optional	4.0W
2	Optional	7.0W
3	Optional	15.4W
4	Reserved	30W

포트별 PoE 사용현황을 표시합니다.

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

Figure 5.102 – PoE > PoE Port Setting

From Port/To Port: PoE 기능을 조절할 포트범위를 선택합니다.

State: Enabled 선택시, PoE 기능이 동작하며, Disabled 는 PoE 기능이 꺼집니다.

Time Range: 설정해 둔 스케줄 규칙을 적용할 경우, 해당 일정에 따라 PoE 동작을 제어할 수 있습니다.

Priority: PoE 전력 공급에 대한 우선순위를 "Low", "Normal", "High" 3 단계로 부여할 수 있습니다.

Power Limit: 상기 PoE 클래스별 기준에 맞추어 PoE 용량을 제한할 수 있습니다. 기본값은 "Auto" 이며, IEEE802.3at(15.4W) 표준에서 자동 조절합니다.

User Define: PoE 용량을 제한하고자 하는 값을 입력할 수 있습니다.(범위 : 1~30W)

변경한 설정을 적용하시려면 **Apply** 버튼을 클릭하고, 목록의 내용을 갱신하려면 **Refresh** 버튼을 클릭합니다.

SNMP > Trap to SmartConsole Utility

스위치 동작을 전용 유틸리티(SmartConsole) 와 연동하여 모니터링할 수 있습니다.

Figure 5.103 – SNMP > Trap to SmartConsole Utility

Destination IP: SmartConsole 이 설치된 서버 IP 주소를 입력합니다.

Illegal Login: 로그인 Password 가 올바르지 않은 사용자의 접속시도를 서버로 전송합니다.

Device Bootup: 시스템 부팅 정보를 서버로 전송합니다.

Port Link Up / Link Down: 포트별 연결 정보를 서버로 전송합니다.

RSTP Port State Change: RSTP 포트의 변경상태를 서버로 전송합니다.

Firmware Upgrade State: 펌웨어 정보 및 업그레이드 상태를 서버로 전송합니다.

PoE Power On / Off: 포트별 PoE 상태를 서버로 전송합니다.

PoE Power Error: Power over loading, Short circuit, Thermal shutdown, Power deny 상태를 전송합니다.



참고: PoE 총용량은 SPN-12080P 가 78W, SPN-14240P 가 185W 입니다. PoE 용량이 7W 남아 있을 경우, Power Deny 메세지가 발송됩니다.

PoE Over Max Power Budget: PoE 총용량이 초과되었을 경우, 해당 메세지를 서버로 전송합니다.

SNMP > SNMP > SNMP Global Settings

표준 SNMP(Simple Network Management Protocol) 를 사용하여 SNMP 프로그램과 연동할 수 있습니다.

Figure 5.104 – SNMP > SNMP > SNMP Global Settings

Trap Settings: 전송할 SNMP 메세지를 선택 적용합니다.

SNMP Authentication Traps: SNMP 접속 인증실패 메세지를 전송합니다.

Device Bootup: 시스템 부팅 정보를 전송합니다.

Illegal Login: 로그인 Password 가 올바르지 않은 사용자의 접속 시도를 전송합니다.

Port Link Up / Link Down: 포트별 연결 상태를 전송합니다.

RSTP Port State Change: RSTP 포트 변경 상태를 전송합니다.

Firmware Upgrade State: 펌웨어 정보 및 업그레이드 상태를 전송합니다.

PoE Power On / Off: 포트별 PoE 상태를 전송합니다.

PoE Power Error: power over loading, short circuit, thermal shutdown, power deny 를 전송합니다.

PoE Over Max Power Budget: PoE 총용량이 초과되었을 때, 해당 메시지를 전송합니다.

SNMP > SNMP > SNMP User

SNMP 사용자 등록 설정 및 사용여부를 설정합니다.

The interface shows the 'SNMP User Table' configuration page. It includes form fields for User Name, Group Name, SNMP Version (v1), Encrypt (Disabled), Auth-Protocol (MD5), Privacy Protocol (DES), and Password fields. An 'Add' button is present. Below the form is a table of existing users.

User Name	Group Name	SNMP Version	Auth Protocol	Privacy Protocol	Delete
ReadOnly	ReadOnly	v1	None	None	Delete
ReadOnly	ReadOnly	v2c	None	None	Delete
ReadWrite	ReadWrite	v1	None	None	Delete
ReadWrite	ReadWrite	v2c	None	None	Delete

Figure 5.105 – SNMP > SNMP > SNMP User Table

User Name: SNMP 사용자 이름을 입력합니다.(최대 32 자)

Group Name: SNMP 그룹명을 입력합니다.

SNMP Version: SNMP 버전을 선택합니다. SNMPv3 만 암호화된 메시지로 전송합니다.

Encrypt: SNMPv3 사용여부를 선택합니다. (Enabled : 사용함)

Auth-Protocol/Password: HMAC-MD5-96 혹은 HMAC-SHA 중 인증 프로토콜 방식을 선택합니다.

Priv-Protocol/Password: no authorization 혹은 DES 56-bit 방식 중 선택하고 해당 비밀번호를 입력합니다.

SNMP 사용자 정보를 등록하시려면 **Add** 버튼을 클릭하고 입력되어 있는 항목을 삭제하시려면 **Delete** 버튼을 클릭합니다.

SNMP > SNMP > SNMP Group Table

Group Name: SNMP 사용자 그룹명을 입력합니다.(최대 32 자)

Read View Name: Read 권한을 허용할 SNMP 그룹명을 입력합니다.

Write View Name: Write 권한을 허용할 SNMP 그룹명을 입력합니다.

Security Model: SNMP 보안 방식을 선택합니다.

SNMPv1 - SNMPv1 은 보안기능을 지원하지 않습니다.

SNMPv2 - SNMPv2 중앙관리 네트워크 망을 지원하며, SMI 정보 및 일부 보안 기능을 지원합니다.

SNMPv3 - SNMPv3 는 인증 및 패킷 암호화를 지원합니다.

Security Level: SNMPv3 에서만 본 기능을 이용하실 수 있습니다.

NoAuthNoPriv - 스위치와 SNMP 관리 프로그램 간의 패킷 암호화 및 인증을 사용하지 않습니다.

AuthNoPriv - 인증만 사용하고 패킷 암호화는 사용하지 않습니다..

AuthPriv – 인증 및 패킷 암호화를 모두 사용합니다.

Notify View Name: SNMP 메시지를 받을 수 있는 SNMP 그룹명을 입력합니다.

Group Name	Read View	Write View	Notify View	Security Model	Security Level	Delete
ReadOnly	ReadWrite	---	ReadWrite	v1	NoAuthNoPriv	Delete
ReadOnly	ReadWrite	---	ReadWrite	v2c	NoAuthNoPriv	Delete
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v1	NoAuthNoPriv	Delete
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v2c	NoAuthNoPriv	Delete

Figure 5.106 – SNMP > SNMP > SNMP Group Table

SNMP > SNMP > SNMP View

원격 SNMP 관리자가 접속할 수 있는 MIB Object 값을 설정합니다.

View Name	Subtree OID	OID Mask	View Type	Delete
ReadWrite	1	1	Included	Delete

Figure 5.107 – SNMP > SNMP > SNMP View

View Name: 확인하고자 하는 이름을 입력합니다. (최대 32 자)

Subtree OID: 확인하고자 하는 OID 값을 입력합니다.

OID Mask: 입력한 Subtree OID 에 해당하는 OID Mask 값을 입력합니다.

View Type: 설정한 OID 가 SNMP 관리자가 접속할 수 있는 요소에 포함시킬지에 대한 여부를 결정합니다.

해당 설정을 적용하시려면 **Add** 버튼을 클릭하고, 입력된 항목을 삭제하시려면 **Delete** 를 클릭합니다.

SNMP > SNMP > SNMP Community

SNMP 통신 내용을 일치하기 위한 SNMP String 을 관리합니다.

Community Name: Community String 값을 입력합니다.

User Name (View Policy): 해당 MIB-Object 에 대한 권한을 선택합니다.

Community Name	User Name	Delete
public	ReadOnly	Delete
private	ReadWrite	Delete

Figure 5.108 –SNMP > SNMP > SNMP Community

설정된 값을 적용하시려면 **Add** 버튼을 클릭하고, 입력된 항목을 삭제하시려면 **Delete** 를 클릭합니다.

SNMP > SNMP > SNMP Host

SNMP 를 수신할 Host 를 설정합니다.



The interface shows the 'SNMP Host Table' configuration page. It includes a 'Host IP Address' field, a radio button selection for 'IPv4' (selected) and 'IPv6', an 'SNMP Version' dropdown menu set to 'V1', and a 'Community String/SNMPv3 User Name' field. An 'Apply' button is located at the bottom right. Below the form is a table with columns: Host IP Address, SNMP Version, Community Name/SNMPv3 User Name, and Delete.

Figure 5.109 – SNMP > SNMP > SNMP Host

Host IP Address: SNMP 서버 IP 주소를 입력합니다.

SNMP Version: 사용할 SNMP 버전을 선택합니다.

Community String/SNMPv3 User Name: Community String 혹은 SNMPv3 사용자 이름을 입력합니다.

설정을 적용하시려면 **Apply** 버튼을 클릭하고, 등록된 항목을 삭제하시려면 **Delete** 를 클릭합니다.

SNMP > SNMP > SNMP Engine ID

Engine ID 는 SNMPv3 를 구분하기 위해 사용되는 ID 값입니다.

변경을 적용하기 위해 사용될 Engine ID 를 입력하고 **Apply** 를 클릭합니다.



The interface shows the 'SNMP Engine ID' configuration page. It features an 'Engine ID' text field containing the value '4447532d313231302d31305000010203040'. There are 'Default' and 'Apply' buttons. A note at the bottom states: 'Engine ID length is 10-64, the accepted character is from 0 to F.'

Figure 5.110 – SNMP > SNMP > SNMP Engine ID

SNMP > RMON > RMON Global Settings

RMON Trap 의 사용여부를 선택합니다.



The interface shows the 'RMON Global Settings' configuration page. It includes a radio button selection for 'Enabled' and 'Disabled' (selected). An 'Apply' button is located at the bottom right.

Figure 5.111 - SNMP > RMON > RMON Global Settings

SNMP > RMON > RMON Statistics

RMON Ethernet 상태와 설정을 허용할 사용자 상태를 표시합니다.



The interface shows the 'RMON Ethernet Statistics Settings' configuration page. It includes fields for 'Index (1~65535)', 'Port', and 'Owner', each marked with an asterisk to indicate mandatory data. There are 'Refresh' and 'Add' buttons. Below the form is a table with columns: Index, Port, Drop Events, Octets, Packets, Broadcast Packets, Multicast Packets, Owner, and Delete.

Figure 5.112 - SNMP > RMON > RMON Ethernet Statistics Configuration

Index (1 - 65535): RMON Ethernet 상태를 숫자로 표시합니다. (1~65535)

Port: RMON 정보를 수신할 포트번호를 입력합니다.

Owner: RMON 정보를 요청한 Station 혹은 사용자를 표시합니다.

설정을 적용하시려면 **Add** 버튼을 클릭하고, 내용을 갱신하려면 **Refresh** 를 클릭합니다.

SNMP > RMON > RMON History

포트로부터 수신된 정보를 표시합니다.

Figure 5.113 - SNMP > RMON > RMON History Control Settings

Index (1 - 65535): 지난 Control 목록을 입력합니다. (1~65535)

Port: RMON 정보를 수신할 포트를 입력합니다.

Buckets Requested (1 ~ 50): Bucket 수치를 입력합니다.

Interval (1 ~ 3600): 포트 정보를 수신할 시간 간격을 입력합니다.(초단위)

Owner: RMON 정보를 요청하는 Station 혹은 사용자명을 입력합니다.

설정을 적용하시려면 **Apply** 버튼을 클릭합니다.

SNMP > RMON > RMON Alarm Settings

RMON 알람을 위한 설정입니다. RMON 알람은 네트워크 이상등이 발생하였을 때 발생합니다.

Figure 5.114 -. SNMP > RMON > RMON Alarm Settings

Index (1 - 65535): 알람 번호를 입력합니다.

Variable: 지정할 MIB 값을 입력합니다.

Rising Threshold (0 ~ 2^31-1): 해당 알람을 확인할 회수를 입력합니다.

Rising Event Index (1 ~ 65535): 지정할 알람을 확인할 이벤트 수치를 입력합니다.

Owner: 알람을 확인할 장치 혹은 사용자 이름을 입력합니다.

Interval (1 ~ 2^31-1): 알람 시간 간격을 입력합니다.

Sample type: Threshold 값과 샘플링 비교할 방법을 선택합니다.

Delta value – 현재의 값과 마지막 샘플값을 확인하고 Thershold 와의 차이를 비교 검토합니다.

Absolute value – Threshold 과 샘플 간격을 직접 비교합니다.

Falling Threshold (0 ~ 2³¹-1): Falling Threshold Alarm 값을 입력합니다.

Falling Event Index (1 ~ 65535): 추적할 알람 Index 번호를 입력합니다.

설정을 적용하시려면 **Add** 버튼을 클릭합니다.

SNMP > RMON > RMON Event

RMON 이벤트를 상태를 정의, 수정 및 모니터링 합니다.

Figure 5.115 - SNMP > RMON > RMON Event Settings

Index (1~ 65535): 이벤트 Index 값을 입력합니다.

Description: 사용자 정의 이벤트 설명을 입력합니다.

Type: 이벤트 방식을 입력합니다.

None – 이벤트를 선택하지 않습니다.

Log – Log 에 기록된 경우에만 이벤트로 감지합니다.

SNMP Trap – SNMP Trap 에 대해서만 이벤트로 감지합니다.

Log and Trap – Log 기록 및 SNMP Trap 을 모두 이벤트로 감지합니다.

Community: 해당 이벤트가 속한 Community 값을 입력합니다.

Owner: 이벤트 발생에 대한 시간을 기록합니다.

해당 RMON 이벤트를 추가하시려면 **Add** 버튼을 클릭합니다.

Monitoring > Port Statistics

각 포트별 패킷량을 표시합니다.

Port	TxOK	RxOK	TxError	RxError
01	30788	134754	0	0
02	0	0	0	0
03	0	0	0	0
04	0	0	0	0
05	0	0	0	0
06	0	0	0	0
07	0	0	0	0
08	0	0	0	0
09	0	0	0	0
10	0	0	0	0

Figure 5.116 – Monitoring > Port Statistics

Refresh: 수집된 내용을 갱신합니다.

Clear: 현재 표시된 수치를 초기화합니다.

TxOK: 송신 완료한 패킷의 양을 표시합니다.

RxOK: 수신 완료한 패킷의 양을 표시합니다.

TxError: 송신시 발생한 오류 패킷의 양을 표시합니다.

RxError: 수신시 발생한 오류 패킷의 양을 표시합니다.

포트별로 상태를 확인하시려면 해당 포트 번호를 클릭합니다.

Port Statistics		Safeguard	
Port: 1		Back	Refresh
		Clear	
TX		RX	
OutOctets	16926524	InOctets	37798576
OutUcastPkts	22804	InUcastPkts	16621
OutNUcastPkts	8105	InNUcastPkts	118331
OutErrors	0	InDiscards	0
LateCollisions	0	InErrors	0
ExcessiveCollisions	0	FCSErrors	0
InternalMacTransmitErrors	0	FrameTooLongs	0
		InternalMacReceiveErrors	0

Figure 5.117 – Monitoring > Port Statistics

Back: 패킷 통계화면으로 되돌아 갑니다.

Refresh: 현재의 내용을 갱신합니다.

Clear: 표시된 내용을 초기화합니다.

Monitoring > Cable Diagnostics

선택한 포트에 연결된 케이블 상태를 점검합니다. 포트를 지정하고 **Test Now** 버튼을 클릭합니다.

Cable Diagnostics		Safeguard	
Port	01	Test Now	
Port	Test Result	Cable Fault Distance (meters)	Cable Length (meters)
The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error. 1. If cable length is displayed as "N/A" it means the cable length is "Not Available". This is due to the port being unable to obtain cable length/either because its link speed is 10M or 100M, or the cables used are broken and/or bad in quality. 2. The deviation of "Cable Fault Distance" is +/-10 meters, therefore No cable may be displayed under Test Result, when the cable used is less than 10 m in length. 3. It also measures cable fault and identifies the fault in length according to the distance from this switch.			

Figure 5.118 – Monitoring > Cable Diagnostic

Test Result

•**OK** : 케이블 상태가 정상입니다.

•**Short in Cable:** 연결된 케이블 내 합선된 부분이 있습니다.

•**Open in Cable:** 연결된 케이블이 단선된 부분이 있습니다.

•**Test Failed** 케이블 감지 중 오류가 발생하였습니다. 다시 시도하여 주십시오.

Cable Fault Distance (meters): 연결된 케이블의 길이를 표시합니다. 2m 이내인 경우에 "No Cable" 로 표시됩니다.

Cable Length (meter): 테스트 결과 정상일 경우, 4 단계로 나누어 케이블 길이를 표시합니다.

<50 meters (50m 미만), 50~80 meters, 80~100 meters, >100 meters(100m 초과)



참고: 케이블 길이 감지는 기가비트로 연결되어 있을 경우에만 동작합니다.



참고: 케이블 감지를 실행하기 전에 전원 절약 모드가 꺼져 있는지 확인하여 주십시오.

Monitoring > System Log

스위치의 동작, 사용자의 접속등의 로그를 모니터링 하실 수 있습니다.

System Log			
Maximum 500 entries.			Refresh Clear
ID	Time	Log Description	Severity
1	Jan 2 05:18:41 2012	Successful login through Web (IP: 10.0.0.106)	info
2	Jan 2 05:05:29 2012	Logout through Web(IP: 10.0.0.106)	info
3	Jan 2 05:05:29 2012	Web session timed out (IP: 10.0.0.106)	info
4	Jan 2 04:13:23 2012	Successful login through Web (IP: 10.0.0.106)	info
5	Jan 2 02:05:11 2012	Logout through Web(IP: 10.0.0.106)	info
6	Jan 2 02:05:11 2012	Web session timed out (IP: 10.0.0.106)	info
7	Jan 2 00:52:42 2012	Successful login through Web (IP: 10.0.0.106)	info
8	Jan 1 07:04:33 2012	Logout through Web(IP: 10.0.0.106)	info
9	Jan 1 07:04:33 2012	Web session timed out (IP: 10.0.0.106)	info
10	Jan 1 05:50:46 2012	Successful login through Web (IP: 10.0.0.106)	info
11	Jan 1 05:37:56 2012	Logout through Web(IP: 10.0.0.106)	info
12	Jan 1 05:37:56 2012	Web session timed out (IP: 10.0.0.106)	info
13	Jan 1 04:35:21 2012	Successful login through Web (IP: 10.0.0.106)	info
14	Jan 1 04:33:24 2012	Login failed through Web (IP: 10.0.0.106)	warning
15	Jan 1 04:33:22 2012	Successful login through Web (IP: 10.0.0.106)	info
16	Jan 1 01:55:58 2012	Logout through Web(IP: 10.0.0.106)	info
17	Jan 1 01:55:58 2012	Web session timed out (IP: 10.0.0.106)	info
18	Jan 1 00:18:13 2012	Successful login through Web (IP: 10.0.0.106)	info
19	Jan 1 00:00:07 2012	System started up	critical
20	Jan 1 00:00:02 2012	Port 1 link up, 1Gbps FULL duplex	info

Figure 5.119 – Monitoring > System Log

ID: 로그의 번호입니다.(최대 500 개)

Time: 로그가 발생한 시간을 표시합니다.

Log Description: 발생한 로그 이벤트 내용입니다.

Severity: 로그의 중요도를 표시합니다.

새롭게 내용을 갱신하시려면 **Refresh** 를 클릭하고, 로그를 삭제하시려면 **Clear** 를 클릭합니다.

6 Command Line Interface

Telnet 을 이용하여 일부 기능에 대한 모니터링 및 설정을 하실 수 있습니다.

TELNET 으로 스위치에 접속하기

1. 스위치와 PC 의 네트워크 연결을 확인합니다.
2. Hyper Terminal 과 같은 Terminal 소프트웨어를 실행하고 *telnet 10.90.90.90* 을 입력합니다.
3. 로그인 프롬프트가 표시됩니다.

Telnet 로그인

사용자 이름과 비밀번호를 "admin" 을 입력하고 엔터합니다.

```
SPN-14240P login: admin
Password:
SPN-14240P>
```

Figure 6.1 – Command Prompt

기본 로그인 대기시간은 5 분으로 이 시간이 경과하면 로그아웃됩니다.

CLI 명령어

사용할 수 있는 CLI 명령어는 아래와 같습니다.

Command	Parameter
?	
download	{ firmware_fromTFTP cfg_fromTFTP } {<ipaddr> <ipv6addr>} <path_filename>
Upload	{ firmware_fromTFTP cfg_fromTFTP } {<ipaddr> <ipv6addr>} <path_filename>
config ipif system	{ ipaddress <ip-address> <subnet-mask> gateway <gw-address> dhcp bootp }
config ipif system	{ ipv6 ipv6address <ipv6networkaddr> dhcpv6_client [enable disable] }
logout	
ping	<ip_addr>
ping6	<ipv6addr>
reboot	
reset config	
show ipif	
show switch	
config account admin password	<passwd>
save	
debug info	

각 명령에 대해서는 아래 설명을 참고하여 주십시오.

?	
Purpose	명령어 목록을 표시합니다.
Syntax	?
Description	"?" 는 CLI 명령어 목록을 표시해 줍니다.
Parameters	없음
Restrictions	없음

사용예)

To display a list of commands of the switch:

```
SPN-14240P> ?
USEREXEC commands :
  config account admin password <passwd>
  config ipif System { ipaddress <ip-address> <subnet-mask> gateway <gw-
address> | dhcp }
  debug info
  download { firmware_fromTFTP tftp://ip-address/filename | cfg_fromTFTP
tftp://ip-address/filename }
  logout
  ping <ip_addr>
  reboot
  reset config
  save
  show ipif
  show switch
  upload { firmware_toTFTP tftp://ip-address/filename | cfg_toTFTP tftp://ip-
address/filename }
SPN-14240P>
```

download	
Purpose	TFTP 로부터 스위치 펌웨어, 설정 파일을 다운로드합니다.
Syntax	download { firmware_fromTFTP cfg_fromTFTP } <ipaddr> <ipv6addr> <path_filename>
Description	"download" 명령어는 지정한 TFTP 서버로부터 펌웨어, 설정 파일을 다운로드하여 스위치에 적용합니다.
Parameters	<i>firmware_fromTFTP</i> - 펌웨어 업그레이드 <i>cfg_fromTFTP</i> - 스위치 설정파일 <ipaddr> - TFTP 서버 IPv4 주소 <ipv6addr> - TFTP 서버 IPv6 주소

	<code><path_filename></code> - TFTP 서버에 저장된 해당 파일명을 입력
Restrictions	None.

사용예)

펌웨어 다운로드의 경우

```

SPN-14240P> download firmware_fromTFTP 1.1.1.23 1\dgs_1210-10032.ros
01-Jan-2000 01:19:48 %COPY-I-FILECPY: Files Copy - source URL tftp://1.1.1.23
/1\dgs_1210-10032.ros destination URL Unit all flash://image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
01-Jan-2000 01:22:49 %COPY-W-TRAP:
The copy operation was completed successfully
!
3920460 bytes copied in 00:03:01 [hh:mm:ss]

SPN-14240P>

```



참고: TFTP 를 이용하여 펌웨어 업그레이드 후에는 스위치가 재부팅 됩니다.

upload

Purpose	스위치의 펌웨어 파일이나 설정파일을 TFTP 서버로 업로드합니다.
Syntax	upload { firmware_fromTFTP cfg_fromTFTP } {<ipaddr> <ipv6addr>} <path_filename>
Description	스위치의 현재 설정을 지정한 TFTP 서버로 업로드합니다.
Parameters	<i>firmware_toTFTP</i> - 펌웨어 파일을 업로드 합니다. <i>cfg_toTFTP</i> - 설정파일을 업로드 합니다. <ipaddr> - TFTP 서버의 IPv4 주소를 입력합니다. <ipv6addr> - TFTP 서버의 IPv6 주소를 입력합니다.

<path_filename> - 해당 파일명을 입력합니다.

Restrictions None.

사용예)

펌웨어 업로드의 경우,

```
SPN-14240P>upload firmware_toTFTP 1.1.1.23 1\running-config
01-Jan-2000 01:26:11 %COPY-I-FILECPY: Files Copy - source URL running-
config destination URL tftp://1.1.1.23/1\running-config
.....01-Jan-2000 01:26:16 %COPY-W-TRAP: The copy operation was completed
success fully
!
158 bytes copied in 00:00:05 [hh:mm:ss]
SPN-14240P>
```

config ipif system

Purpose	스위치의 IP 주소를 설정합니다.
Syntax	config ipif system { ipaddress <ip-address> <subnet-mask> gateway <gw-address> dhcp bootp }
Description	스위치의 시스템 IP 주소를 설정합니다.
Parameters	<i>ipaddress <ip-address> <subnet-mask></i> - 설정할 IP 주소와 서브넷 마스크값을 입력합니다. (예,10.1.2.3/255.0.0.0) <i>gateway <gw-address></i> - 사용할 게이트웨이 값을 입력합니다. <i>dhcp</i> - DHCP 서버로부터 자동할당하고자 할 경우 입력합니다. <i>bootp</i> - BOOTP 방식을 사용하고자 할 경우 입력합니다.
Restrictions	None.

사용예)

시스템 IP 주소 설정시,

```
SPN-14240P> config ipif System ipaddress 10.48.74.122/8
Success.
SPN-14240P>
```

logout

Purpose	스위치 Telnet 접속을 종료합니다.
Syntax	logout
Description	스위치 Telnet 접속을 종료합니다.
Parameters	None.

Restrictions	None.
--------------	-------

사용예)

```
SPN-14240P> logout
```



참고: 로그아웃하시기 전에 설정을 저장하여 주십시오.

ping

Purpose	해당 IP 주소와의 네트워크 연결을 확인합니다.
Syntax	<ipaddr>
Description	VLAN 설정이 되어 있을 경우, Managed VLAN(기본값 : VLAN 1)에 연결된 상태에서 본 명령어를 실행하여 주십시오.
Parameters	<ipaddr> - 확인하고자 하는 IP 주소
Restrictions	None.

사용예)

```
SPN-14240P> ping 10.90.90.91
```

```
Reply Received From :10.90.90.91, TimeTaken : 20 msec
```

```
Reply Received From :10.90.90.91, TimeTaken : 20 msec
```

```
Reply Received From :10.90.90.91, TimeTaken : 20 msec
```

```
--- 10.90.90.91 Ping Statistics ---
```

```
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
```

```
SPN-14240P>
```

ping6

Purpose	IPv6 연결을 확인합니다.
Syntax	ping6 <ipv6addr>
Description	VLAN 이 설정되어 있는 경우, Managed VLAN 에 연결된 상태에서 본 명령어를 실행하여 주십시오.
Parameters	<ipv6addr> - IPv6 주소
Restrictions	None.

사용예)

```
SPN-14240P> ping6 3000 ::1
```

```

Reply Received From : 3000 ::1, TimeTaken : 20 msec
Reply Received From : 3000 ::1, TimeTaken : 20 msec
Reply Received From : 3000 ::1, TimeTaken : 20 msec

--- 3000 ::1 Ping Statistics ---
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss

SPN-14240P>

```

reboot

Purpose	스위치를 재부팅합니다.
Syntax	reboot
Description	스위치를 재부팅합니다. 모든 네트워크 연결이 끊어집니다.
Parameters	None.
Restrictions	None.

사용예)

```

SPN-14240P> reboot

% Device will reboot, please wait a few minutes to re-login.

SPN-14240P>

```

reset config

Purpose	스위치 설정을 초기화합니다.
Syntax	reset config
Description	모든 사용자 설정값이 삭제되고 공장 출하 상태로 복구됩니다.
Parameters	None.
Restrictions	None.

사용예)

```

SPN-14240P> reset config

% Device will reboot after reset configuration successfully.

SPN-14240P>

```

show ipif

Purpose	스위치의 현재 IP 주소를 표시합니다.
---------	-----------------------

Syntax	show ipif
Description	현재 스위치에 설정된 시스템 IP 주소를 표시합니다.
Parameters	None.
Restrictions	None.

사용예)

```
SPN-14240P> show ipif

IP Setting Mode      : Static
IP Address           : 10.90.90.90
Subnet Mask          : 255.0.0.0
Default Gateway      : 0.0.0.0
DHCPv6 Client State  : Disabled
IPv6 Global Unicast Address: 3ffe:501:ffff:100:100::1/64

SPN-14240P>
```

show switch

Purpose	스위치의 정보를 표시합니다.
Syntax	show switch
Description	스위치의 상태를 표시합니다.
Parameters	None.
Restrictions	None.

사용예)

```
SPN-14240P> show switch

System Name          :
System Contact        :
System Location       :
System up time        : 0 days, 6 hrs, 32 min, 17 secs
System Time           : 02/01/2012 06:32:19
System hardware version : B1
System firmware version : 3.10.006
System boot version    : 1.00.005
System Protocol version : 2.001.004
System serial number   : 1MB1733K0000A
MAC Address           : 00-01-02-03-04-05

SPN-14240P>
```

config account admin password

Purpose	스위치 관리를 위한 로그인 비밀번호를 설정합니다.
Syntax	config account admin password <passwd>
Description	로그인 비밀번호를 설정합니다.
Parameters	<passwd> - 설정할 비밀번호
Restrictions	None.

사용예)

```
SPN-14240P> config account admin password 1234
SPN-14240P>
```

save

Purpose	스위치의 현재 설정값을 메모리에 저장합니다.
Syntax	save
Description	스위치의 현재 설정값을 메모리에 저장합니다.
Parameters	None.
Restrictions	None.

사용예)

```
SPN-14240P> save
Building configuration ...
[OK]

SPN-14240P>
```

debug info

Purpose	스위치의 ARP 목록과 MAC 목록을 표시합니다.
Syntax	debug info
Description	스위치의 ARP 목록과 MAC 주소 목록을 표시합니다.
Parameters	None.
Restrictions	None.

사용예)

```
SPN-14240P> debug info
% segmentation fault log file:
```

File doesn't exist !!!

% ARP table :

Address	Hardware Address	Type	Interface	Mapping
-----	-----	----	-----	-----
10.90.90.90	00:18:8b:bf:75:30	ARPA	vlan1	Static
10.90.90.98	00:19:5b:14:3d:c4	ARPA	vlan1	Dynamic
10.255.255.255	ff:ff:ff:ff:ff:ff	ARPA	vlan1	Static

% MAC table :

Vlan	Mac Address	Type	Ports
-----	-----	-----	-----
1	00:00:00:00:00:26	Learnt	Gi0/7

Total Mac Addresses displayed: 1

SPN-14240P>

Appendix A - 제품 사양

Hardware Specifications

Key Components / Performance

- Switching Capacity:
 - SPN-12080P: 20Gbps
 - SPN-14240P: 56Gbps
- Max. Forwarding Rate
 - SPN-12080P: 14.88Mpps
 - SPN-14240P: 41.7Mpps
- Forwarding Mode: Store and Forward
- Packet Buffer memory:
 - SPN-12080P: 1MBytes
 - SPN-14240P: 1MBytes
- DDRII for CPU: 128M Bytes
- Flash Memory: 16M Bytes

Port Functions

- 10/100/1000Base-T ports compliant with the following standards:
 - IEEE 802.3
 - IEEE 802.3u
 - IEEE 802.3ab
 - IEEE 802.3az Energy Efficient Ethernet
 - IEEE 802.3af (SPN-12080P/28P only)
 - IEEE 802.3at (SPN-12080P/28P only)
 - Supports Half/Full-Duplex operations
 - IEEE 802.3x Flow Control support for Full-Duplex mode
 - Auto MDI/MDIX
 - IEEE802.3af Power over Ethernet on Port 1 ~ Port 8 GE ports (SPN-12080P only)
 - IEEE802.3af Power over Ethernet on Port 1~ Port 24 GE ports (SPN-14240P)
 - IEEE802.3at Power over Ethernet on Port 1~Port 8 GE ports (SPN-12080P)
 - IEEE802.3at Power over Ethernet on Port 1~ Port 4 GE ports (SPN-14240P only)
- SFP ports compliant with the following standards:
 - IEEE 802.3z
 - Supports Full-Duplex operations
- SFP transceivers supported
- WDM Transceivers Supported:

Physical & Environment

- AC input, 100~240 VAC, 50/60Hz, internal universal power supply
- Acoustic Value:
 - SPN-12080P/20/28: 0dB (Fan-less)
 - SPN-14240P: 52.2dB (3 Smart Fans)
- Operation Temperature:

- SPN-14240P: 5~50°C
- SPN-12080P: 5~40°C
- Storage Temperature -20~70°C
- Operation Humidity: 0%~95% RH
- Storage Humidity: 0%~95% RH

Emission (EMI) Certifications

- FCC class A
- CE Class A
- VCCI Class A
- IC Class A

Safety Certifications

- cUL, LVD, CE

Features

L2 Features

- Supports up to 16K MAC address
- Supports 256 static MAC
- Jumbo frame: Supports up to 10,000 bytes
- IGMP snooping v1/v2:
 - Supports 256 multicast groups
 - Supports at least 64 static multicast groups
- 802.1D Spanning Tree
- 802.1w Rapid Spanning Tree
- Loopback Detection
- 802.3ad Link Aggregation:
 - SPN-12080P: Supports max 5 groups per device and 8 ports per group
 - SPN-14240P: Supports max 14 groups per device and 8 ports per group
- Port mirroring
- STNP
- LLDP/LLDP-MED
- IPv6 neighbor Discovery (ND)
- L2 Multicast Filtering

VLAN

- 802.1Q VLAN standard (VLAN Tagging)
- Up to 256 static VLAN groups
- Asymmetric VLAN
- Management VLAN
- Auto-Voice VLAN
- Auto Surveillance VLAN

QoS (Quality of Service)

- Priority queue mapping by :
 - 802.1p
 - DSCP
 - ToS
 - TCP/UDP port number
 - IPv6 traffic class
- Up to 4 queues per port

- Supports Strict / WRR mode in queue handling
- Bandwidth Control

AAA

- 802.1X port-based access control
- Support RADIUS server

ACL

- Max 50 ingress ACL profiles
- Ingress ACL rules:
 - SPN-14240P: 200 rules (each rule can be associated to a single port or multiple ports)
- Support different ACL policy packet contents:
 - MAC address
 - Ethernet Type
 - IPv4 address
 - IPv6 address
 - ICMP
 - IGMP
 - TCP/UDP port number

Security

- Trusted Host
- Port Security: Support 64 MAC addresses per port
- Traffic Segmentation
- Safeguard Engine
- Broadcast Storm Control
- ARP Spoofing Prevention: Supports max 64 entries
- DHCP Server Screening: Able to configure 5 IP addresses for DHCP server.
- SSL: Support v1/v2/v3
- Smart Binding
 - Support manual configuration and scanning for binding.
 - Supports ARP packet inspection as default, ARP and IP packet inspection as an option.
 - Supports DHCP Snooping

OAM

- Cable Diagnostics
- Reset button (reset to factory default)

Management

- Web-based GUI
- proprietary CLI
- SNMP support
- DHCP client
- Trap setting for destination IP, system events, fiber port events, twisted-pair port events
- Password access control

- Web-based configuration backup / restoration
- Web-based firmware backup/restore
- Firmware upgrade using Web-based management
- Reset, Reboot

Green Technology

- Power Saving: Enabled by default to save power:
 - By Link Status: Drastically save power when the switch port link is down. For example, no PC connection or the connected PC is powered off.
 - By Cable Length: Detects the length of connected RJ-45 cables and adjusts power usage accordingly without affecting performance. Once the RJ-45 connection is less than 20 meters, the switch will reduce the power instead of full power, which is only needed for 100 meters cables.
 - By LED Shut-Off: LEDs can be turned on/off by port or system through schedule.
 - By Port Shut-Off: Each port on the system can be turned on/off by schedule.
 - By Port Standby: Each port on the system enters sleep state by schedule.
 - By System Hibernation: System enters hibernation by schedule. In this mode, switches save most power since main chipsets (both MAC and PHY) are disabled for all ports, and energy required to power the CPU is minimal.

