



## 목 차

1. 안전 사항	4
2. 장비 외관	8
2.1 장비 전면	8
2.2 장비 후면	9
3. 스위치 장비	10
3.1 장비 사양	10
3.2 장비 구성품	11
3.3 콘솔 연결	12
3.4 MGMT 포트	12
4. CLI 기본 사용법	13
4.1 명령어 체계	13
4.1.1 사용 가능한 명령어 보기	15
4.1.2 이전 명령어 불러오기	15
4.1.3 단축 명령어	15
4.2 접속 및 관리 IP 설정	16
4.2.1 로그인	16
4.2.2 Password 변경	16
4.2.3 자동 로그 아웃 기능	17
4.2.4 관리 IP 설정	18
4.2.5 설정 내용 관리	19
4.3 환경 설정	20
4.4 시스템 상태 정보	21

4.5	유해트래픽 차단(MDS)	22
4.5.1	MDS 자동 차단 기능 설정 확인	24
4.5.2	실시간 MDS 차단현황 모니터링	26
4.5.3	실시간 MDS 차단현황 세부 내역 보기	27
4.5.4	MDS 차단로그(detect-history) 보기	28
4.5.5	MDS 차단로그(detect-history) 세부 내역 보기	29
4.5.6	MDS 예외처리	30
4.5.7	Self Loop 차단	31
4.5.8	패킷 필터링	32
4.6	Visual Node Manager 연동	33
4.7	포트 상태 정보 보기 및 변경	34
4.8	Link Aggregation	39
4.8.1	Static Channel Group	39
4.8.2	LACP	40
5	Sample Config	42
5.1	Port VLAN 설정	42
5.2	802.1Q VLAN 설정	43
5.3	Shared VLAN 설정	44
5.4	Shared VLAN egress-port 설정	45
5.5	QoS 설정	47
5.5.1	SPQ를 이용한 QoS 설정	47
5.5.2	WRR을 이용한 QoS 설정	48

# 1. 안전 사항





## ▶ 안전상의 주의

▷ 이 취급 설명서는 사용 고객 및 타인의 신체적 위험 및 재산상의 손실을 미연에 방지하기 위하여 본 제품을 안전하게 사용하는 것을 목적으로 주요 사항을 기재하고 있습니다.

본 내용을 반드시 숙지하여, 사용 방법을 이해 하신 후에 사용하셔야 합니다.

본 내용은 제품의 설치 및 운용에 대한 전반적인 주의사항을 기재하고 있습니다.

## ▶ 경고 표시

	경 고	절대로 행하지 않아야 할 것을 기재하고 있습니다. 이 표시의 주의 사항을 지키지 않으면, 사용자가 사망 또는 부상을 당할 수도 있습니다. 또 중대한 물적 손실이 발생할 가능성이 있다는 내용을 표시하고 있습니다.
	주 의	이 표시의 주의사항을 지키지 않으면 사용자가 부상을 당하거나 물적 손실이 발생할 가능성이 있다는 내용을 표시하고 있습니다.
	금 지	이 표시는 행위를 금지하고 있습니다.
	강 제	이 표시는 행위를 강제하고 있습니다.



경 고





▶ 연기가 나는 경우

	<p>강 제</p>	<p>제품에서 연기가 나는 것이 발견될 때에는 본 제품에 연결된 전원 Cable 을 즉시 제거하여 주십시오. (계속 사용하면 화재 및 감전의 원인이 됩니다. 제품에서 연기가 나는 경우에는 전원을 끄고, 전원 Cable을 즉시 제거한 후에 고객 센터에 연락하여 주십시오.)</p>
--	------------	---

▶ 취급에 관하여

	<p>금 지</p>	<p>분해, 개조, 수리를 하지 말아 주십시오. (화재나 감전의 원인이 될 수 있습니다.)</p>
	<p>금 지</p>	<p>제품을 낙하시키거나 강한 충격을 주지 말아 주십시오. (내부가 손상된 상태로 사용하면 화재나 감전의 원인이 됩니다.)</p>
	<p>금 지</p>	<p>내부에 이물질이 투입하지 말아 주십시오. (내부에 이물질이 투입된 경우에는 전원을 끄고, 전원 Cable을 즉시 제거한 후에 고객 센터에 연락하여 주십시오. 이물질이 투입된 상태에서 제품을 계속 사용하면 화재나 감전의 원인이 됩니다.)</p>
	<p>금 지</p>	<p>젖은 손으로 제품을 만지지 말아 주십시오. (내부에 물이 들어간 경우에는 전원 Cable을 즉시 제거하고, 고객 센터에 연락하여 주십시오. 그대로 사용하면 화재나 감전의 원인이 됩니다.)</p>
	<p>금 지</p>	<p>제품의 통풍구를 막지 말아 주십시오. (내부에 열이 높아져 화재나 고장의 원인이 됩니다.)</p>



▶ 전원에 관하여

	금 지	정해진 전원 전압 이외에는 사용하지 않아 주십시오. (화재나 고장의 원인이 됩니다.)
	강 제	전원 Cable은 확실하게 전원 콘센트에 삽입하여 주십시오. (전원Cable이 전원 콘센트에 불완전하게 연결된 상태에서 제품을 계속 사용하면 화재나 감전의 원인이 됩니다.)
	금 지	본 제품의 전원 Cable을 연결할 때 너무 많은 장비가 연결된 전원 배선을 이용하지 않아 주십시오. (화재의 원인이 될 수 있으며, 제품 성능에 문제가 발생할 수 있습니다.)
	금 지	전원 Cable을 절단하거나 손상시키지 않아 주십시오. (전원 Cable이 손상된 상태로 계속 사용하면 화재나 감전의 원인이 됩니다.)



주 의

▶ 전원에 관하여

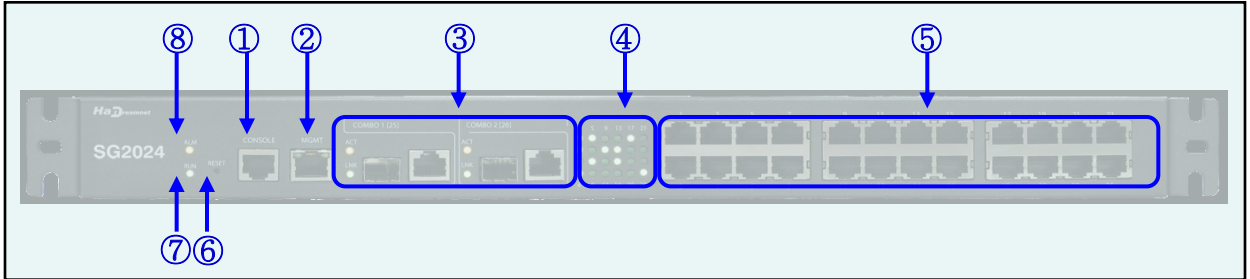
	강 제	장기간 사용하지 않는 경우에는 전원코드를 뽑아 주십시오. (절연 열화에 의한 감전 또는 누전의 원인이 됩니다.)
	금 지	전원 Cable을 잡아당기지 않아 주십시오. (전원 Cable을 잡아당기면 심선의 일부가 단선되어 발열 또는 발화의 원인이 됩니다.)

## ▶ 설치 장소에 관하여

	금 지	실외에 설치하지 말아 주십시오. (본 제품은 실내용이므로 실외에서 절대 사용하지 말아 주십시오.)
	강 제	직사광선에 직접 노출된 장소나 발열 장치에서 가까운 장소 등 온도가 높은 장소에 설치하지 말아 주십시오. (고온에 의해 화재의 원인이 될 수 있습니다. 또 제품 동작에 문제가 생길 수 있습니다.)
	금 지	냉/온방기 등 온도 변화가 급격히 변하는 장소에는 사용하지 말아 주십시오. (급격한 온도변화가 발생하면 내부에 이슬이 생겨 화재나 감전의 원인이 됩니다.)
	금 지	습도가 너무 높거나 건조한 장소에는 사용하지 말아 주십시오. (습도가 너무 높으면 화재나 감전의 원인이 될 수 있으며 또한 너무 건조하면 전기적인 쇼크 및 화재의 원인이 됩니다.)
	강 제	통풍이 잘 되는 장소에 사용하여 주십시오. (통풍이 나쁜 장소에서는 내부에 열이 높아져 화재나 고장의 원인이 됩니다.)
	금 지	안정되지 않은 높은 장소에 설치하지 말아 주십시오. (낙하되어 큰 충격을 받으면 고장의 원인이 됩니다.)
	금 지	위에 물기가 있는 음식물이나 컵 등을 올려놓지 말아 주십시오. (컵 등이 옆질러져 물이 스며들면 화재나 감전의 원인이 됩니다.)

## 2. 장비 외관

### 2.1 장비전면




항목	용도 및 기능
(1) Console Interface	시리얼 관리 포트 9,600 baud, data 8bit, no parity bit, stop 1 bit
(2) Management Ethernet Interface (MGMT)	Firmware Upgrade Fail이나 기타 정상적 Booting 불능발생시 및 Debug용으로 사용되는 Management Ethernet Interface로, 일반적으로 사용되지 않음.
(3) Uplink Module (Giga Combo Port)	상위단의 집선 Switch에 연결되는 Uplink Interface 모듈 10/100/1000Base-Tx 기본 장착 100BaseFX, 1000BaseXInterface SFP Type, 광Cable 연결
	Link LED (Green)
	ACT LED (Yellow)
(4) 10/100BaseTX LED	10/100BaseTX의 LED 동작 상태 ON (Green) : Link 상태 점멸 상태(Green) : Active 상태 OFF 상태 : 미 연결 상태
(5) Downlink Interface (10/100BaseTX Port)	가입자 단의 PC 또는 HUB에 연결되는 Fast Ethernet Port 10/100BaseTX Interface, UTP-5 Cable 연결
(6) Reset Switch	시스템 하드웨어 Reset Switch
(7) Power LED	동작 상태 ON (Green) : 전원 입력 상태 OFF 상태 : 전원 미 입력 상태



## 2.2 장비후면



항목	용도 및 기능
(9) 통신접지단자	전원 안정화 및 외부 Noise 차단을 위한 접지 단자
(10) AC Inlet	100~240VAC, 50/60Hz
(11) Fuse	외장 Fuse (FUSE T 2A 250VAC), 교체 가능
(12) ON/OFF Switch	AC 전원Switch, 입력전원 차단 및 공급

 참고1	<b>INTERFACE 명칭 설명</b>
	ge : Gigabit Ethernet 전체 (Combo1, 2 : 25, 26번 Interface)
	ge1 : Gigabit Ethernet 1번 Interface (Combo1 : 25번 Interface)
	ge2 : Gigabit Ethernet 2번 Interface (Combo2 : 26번 Interface)
	fe : Fast-Ethernet 전체 (1~24번 Interface)
	fe1 : Fast-Ethernet 1번 Interface (1번 Interface)
	fe1-5 : Fast-Ethernet 1~5번 Interface (1~5번 Interface)
	all : INTERFACE 전체 Interface (1~26번 Interface)

 참고2	The socket-outlet shall be installed near the equipment and shall be easily accessible.
--	---

 주의	RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.
---	---

### 3. 스위치장비

#### 3.1 장비사양

기본 사양		
스위칭 용량	28.8 Gbps	
Interface 수	Downlink	24 Ports 10/100Base-TX
	Uplink	Combo 2 Ports. 10/100/1000Base-TX 또는 100Base-FX SFP (MMF/SMF) 또는 1000Base-X SFP
지원 MAC 주소	8K MAC entries	
지원 VLAN 수	4K	
지원 기능		
Layer 2 기능	802.1Q VLAN Link aggregation (6개) Group, Group당 8개 Interface까지 지원 Spanning Tree Protocol (802.1d STP, 802.1w RSTP, 802.1s MSTP)	
보안 기능	DoS, DDoS등 자동 Filtering Layer 2 ~ 4 Packet Filtering (ACL) NetBIOS/DHCP Packet Filtering Interface별 MAC Address 제한 Interface별 ingress & egress 속도 제한 Broadcast/Multicast/DLF Packet 제한 기능	
QoS	802.1p Traffic 제어, Interface 당 8개의 queue 지원 SPQ, WRR, DRR, WFQ 스케줄링 지원	
멀티캐스팅	IGMP snooping	
관리 관리		
관리 방법	Console, Telnet, SSH을 통한 CLI SNMP agent 탑재	
업그레이드	TFTP, FTP를 통한 remote 소프트웨어 업그레이드 지원	
LED	FAN 및 온도 Alarm, Interface별 link/activity	
물리적 특징		
제품 크기	440 x 43.6 x 246 mm (WxDxH) , 19" Rack 설치 가능	
입력 전원	110~220 VAC 50/60Hz	
소비 전력	34.7W 이하	
팬	FAN 내장	
환경 조건		
동작 온도	0 °C ~ 40 °C	
동작 습도	0 ~ 80 % (비응축)	

### 3.2 장비 구성품

품 명		단위	수량	용도 및 기능
시스템본체	SG2024	대	1	10/100/1000Base-TX 20포트용 L2 Switch 10/100/1000Base-TX 4 Port (Combo)
업링크모듈 (선택)	MMF	개	4	100Base-FX, 1포트, SFP Multi-mode, 2-Core, 2km
	SMF-20	개	4	100Base-FX, 1포트, SFP Single-mode, 2-Core, 15/20km
	SMF-40	개	4	100Base-FX, 1포트, SFP Single-mode, 2-Core, 40km
	MMF BIDI	개	4	100Base-FX, 1포트, SFP Multi-mode, Single-Core, 2km
	SMF-20 BIDI	개	4	100Base-FX, 1포트, SFP Single-mode, Single-Core, 15/20km
	SMF-40 BIDI	개	4	100Base-FX, 1포트, SFP Single-mode, Single-Core, 40 km
	1000B-SX	개	4	1000Base-SX, 1포트, SFP Multi-mode, 2-Core, 550m
	1000B-LX	개	4	1000Base-LX, 1포트, SFP Single-mode, 2-Core, 15km
첨부품	RJ-45~RS232(9p), 1.5m	개	1	콘솔케이블, 장비 셋업용
	BLACKET & SCREW	세트	1	장비 고정용 브라켓 & 스크류
	전원코드, AC220V용	개	1	장비 전원 입력용
	사용자설명서	권	1	장비 설치 및 운용설명서

- 업링크 모듈은 별도 구매품으로 시스템 본체에 기본 실장되지 않으며, 위 업링크 모듈 수량은 시스템 본체에 Full 실장 시 수량입니다.

### 3.3 콘솔 연결

운영자는 SG2024 Series에서 제공하는 RJ-45 형태의 콘솔 포트와 운용단말을 연결하여 시스템을 지역적으로 관리할 수 있습니다. 콘솔 포트에 연결된 단말 모드(**terminal mode**)의 설정은 아래와 같습니다.

항 목	Data Bits	Parity	Data Bits	Stop Bits	Flow Control
설 정	<b>9600 bps</b>	<b>None Parity</b>	<b>8 bits</b>	<b>1 stop bit</b>	<b>No Flow Control</b>

스위치 측은 RJ-45 커넥터로 연결되며, 운용 단말측은 9핀 RS-232 커넥터로 연결됩니다. 커넥터 포트의 핀 설정은 다음과 같습니다.

#### ■ 콘솔 포트 Pin-Outs

스위치측(RJ-45)	PC측 (DB-9)	스위치 측 핀 기능	PC측 핀 기능
3	2	TX (데이터 송신)	RX (데이터 수신)
6	3	RX (데이터 수신)	TX (데이터 송신)
4,5	5	GND (접지)	GND (접지)

### 3.4 MGMT 포트

운영자는 SG2024 Series의 MGMT(RJ-45) 포트에 Cable을 연결하여 시스템을 관리할 수 있습니다. MGMT 포트는 디버깅용으로 사용하며, 일반적으로 사용되지 않습니다.



## - TOP 모드

콘솔로 로그인 후 **enable** 명령어를 입력하면 프롬프트가 **SG2024>**에서 **SG2024#**로 바뀌면서 TOP 모드로 들어갑니다. TOP 모드에서는 **SG2024 Series** 전체를 모니터링(**show, ping, traceroute,...**) 할 수 있습니다. 또한 TOP 모드에서 **CONFIG** 모드로 들어갈 수 있습니다.

## - CONFIG 모드

TOP 모드에서 **configure terminal** 명령어를 입력하면 프롬프트가 **SG2024#**에서 **SG2024(config)#**로 바뀌면서 CONFIG 모드로 들어갑니다. CONFIG 모드는 시스템 전체를 통괄하는 전반적인 기능과 **SNMP, syslog**등을 설정하는데 사용합니다. 또한 CONFIG 모드에서 **VLAN, DHCP, INTERFACE** 설정 모드 등으로 들어갈 수 있습니다.

## - VLAN 설정 모드

CONFIG 모드에서 **vlan database** 명령어를 입력하면 프롬프트가 **SG2024(config)#**에서 **SG2024(config-vlan)#**로 바뀌면서 VLAN 설정 모드로 들어갑니다. VLAN 설정 모드에서는 VLAN의 생성, 삭제 등을 설정합니다.

## - DHCP 설정 모드

CONFIG 설정 모드에서 **ip dhcp pool pool-name** 명령어를 입력하여 DHCP Pool Name을 설정하면 시스템 프롬프트가 **SG2024(config)#**에서 **SG2024(config-dhcp)#**로 바뀌면서 DHCP 설정 모드로 들어갑니다. DHCP 설정 모드에서는 DHCP 서버에서 사용하는 IP 주소 범위, 서브넷 및 그룹을 지정하고, 서브넷의 디폴트 게이트웨이 등을 설정합니다.

## - INTERFACE 모드

CONFIG 설정 모드에서 **interface interface-name** 명령어를 입력하면 시스템 프롬프트가 **SG2024(config)#**에서 **SG2024(config-if)#**로 바뀌면서 INTERFACE 설정 모드로 들어갑니다. INTERFACE 설정 모드에서는 각 포트에 대한 DHCP 필터링, NETBIOS 필터링, Negotiation 등을 설정 및 변경합니다.

### 4.1.1 사용 가능한 명령어 보기

사용 가능한 명령어를 알려주는 명령어는 물음표(?)입니다. 각 명령어 모드에서 물음표(?)를 입력하면 해당 모드에서 사용할 수 있는 명령어를 알 수 있으며, 명령어 뒤에 물음표(?)를 입력하면 명령어의 변수 등도 확인할 수 있습니다.

### 4.1.2 이전 명령어 불러오기

반복되는 명령어는 수시로 입력할 필요가 없습니다. 이전에 입력한 명령어를 다시 불러오려면 위 방향 화살표(↑)를 사용하십시오. 위 방향 화살표를 입력하면 최근에 입력한 명령어부터 이전에 입력했던 명령어들을 하나씩 보여줍니다.

다음은 여러 가지 명령어를 사용한 이후 이전 명령어를 불러오는 예입니다.

입력 : show clock → configure terminal → interface vlan1.1 → exit

시스템 프롬프트 상태에서 위 방향 화살표를 누르면

exit → interface vlan1.1 → configure terminal → show clock 순서로 출력

### 4.1.3 단축 명령어

다른 명령어와 구분할 수 있는 최소한의 문자로 명령어를 사용할 수 있습니다.

다음 표는 축약된 명령어 형태의 몇 가지 예입니다.

명령어	단축 명령어
show	sh
configure terminal	con t
show running-config	sh run
interface	int
vlan database	vl d

## 4.2 접속 및 관리 IP 설정

### 4.2.1 로그인

스위치의 설치가 끝나면 각 포트가 네트워크와 관리용 PC에 올바르게 연결되어 있는지 최종 점검하십시오. 모든 점검이 끝나면, 전원 스위치를 켜고 부팅시킵니다. 로그인 프롬프트에 로그인명을 입력하면 패스워드 프롬프트가 출력되고, 패스워드를 입력하면 Top 모드로 이동합니다. ID와 패스워드의 초기값은 **root / root** 입니다.

```
SG2024 login: root
Password: *****
SGOS version 1.3.0 SGL2-OS 03/02/09 17:35:23
SG2024>enable
SG2024#
```

### 4.2.2 Password 변경

스위치를 설정 및 관리하는 권한을 가진 사용자는 패스워드를 변경할 수 있습니다. 확실한 보안을 위해서는 패스워드를 수시로 변경해 주는 것이 바람직합니다. 관리자 Password 및 Enable Password 변경은 Config 모드에서 설정합니다.

```
SG2024#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2024(config)#username root password *****
SG2024(config)#enable password *****
SG2024(config)#end
SG2024#write
Building configuration...
[OK]
SG2024#
```



주의

1. 사용자 계정 추가 시 password를 입력하지 않는 경우 계정이 추가되지 않습니다.
2. Password 설정 시 공백이 포함된 경우 공백을 포함하여 password가 설정되므로 주의하시기 바랍니다.




### 4.2.3 자동 로그 아웃 기능

관리자가 콘솔 터미널 스크린을 켜 둔 채 자리를 비우게 되는 경우, 계속 로그인 상태로 방치된다면 다른 사람이 설정을 변경할 수도 있습니다. 따라서 관리자가 정해 놓은 시간 동안 키보드 입력이 없으면 자동으로 로그 아웃 되는 기능을 가지고 있으며, 그 시간은 관리자가 설정할 수 있습니다.

다음은 자동 로그 아웃 기능을 설정하는 명령어입니다.

명령어	모드	기능
<b>exec-timeout 0</b>	Top	자동 로그 아웃 기능을 해제합니다.
<b>exec-timeout &lt;0-35791&gt;</b>	Top	사용자가 설정한 시간 동안 콘솔 터미널에 키보드 입력이 없으면 시스템을 자동 로그 아웃 합니다. 시간의 단위는 분입니다. (Default : 10분)



현재 로그인한 터미널에만 적용되며 저장되지 않습니다.

참고

**자동 로그 아웃 시간 변경 후 저장하려면** 콘솔 및 Telnet 설정 모드로 변경 후 자동 로그 아웃 기능의 시간 설정을 x분 x초 단위로 설정한 후 저장하면 다음 로그인 시에 변경된 내용으로 적용됩니다.

예제1) Console의 자동 로그 아웃 기능 5분으로 설정

```

SG2024#con t
Enter configuration commands, one per line. End with CNTL/Z.
SG2024(config)#line con 0
SG2024(config-line)#exec-timeout 5 0
```

예제2) Telnet의 자동 로그 아웃 기능 5분으로 설정

```

SG2024#con t
Enter configuration commands, one per line. End with CNTL/Z.
SG2024(config)#line vty 0 14
SG2024(config-line)#exec-timeout 5 0
```

#### 4.2.4 관리 IP 주소 설정

시스템 관리자는 시리얼 콘솔을 이용하여 로그인 후 관리용 IP 주소를 설정해야 합니다. 관리용 IP 주소는 Default VLAN(VLAN1.1) 에 설정합니다.

(공장 출하 시 장비에 IP 주소가 설정되어 있지 않습니다. 운영자는 네트워크 구성에 따라 원하는 IP 주소로 설정하여 사용할 수 있습니다.)

다음은 관리 IP를 설정하는 명령어입니다.

명령어	모드	기능
<b>interface</b> <i>IFNAME</i>	config	Interface 모드로 변경합니다.
<b>ip address</b> <i>IPADDR/Mask</i>	Interface	Management IP Address를 설정 및 변경합니다.
<b>ip address</b> <i>IPADDR/Mask secondary</i>	Interface	Secondary IP Address를 추가로 설정합니다.
<b>ip route</b> <i>Network/Mask Gw_addr</i>	config	Default Gateway등을 설정합니다.

##### SG2024#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

SG2024(config)#**interface vlan1.1**

SG2024(config-if)# **ip address 192.168.0.1/24**

SG2024(config-if)#**exit**

SG2024(config)#**ip route 0.0.0.0/0 192.168.0.254**

SG2024(config)#



참고

1. Interface 모드에서 IP Address 를 변경하면, 변경된 IP Address 로 바로 적용됩니다.
2. Default Gateway 를 변경할 경우 기존의 Default Gateway 는 자동으로 삭제되지 않으므로, "no" 명령어를 입력하여 삭제하시기 바랍니다.



주의

Secondary IP 입력 시 Management IP가 변경되지 않도록 주의하시기 바랍니다.

## 4.2.5 설정 내용 관리

### ➤ 설정 내용 확인


사용자가 CLI 명령어를 사용하여 설정 내용을 변경한 후에는 아래의 명령어를 이용하여 설정된 모든 내용을 쉽게 확인할 수 있습니다.

명령어	모드	기 능
<b>show running-config</b>	Top Config	설정된 모든 내용을 보여줍니다.

### ➤ 설정 내용 저장

동작 모드 및 환경 설정 변경 후 시스템 재 부팅 후에도 계속하여 설정된 내용을 유지 하기 위해서는 반드시 설정한 내용을 시스템 내의 저장영역에 저장하여야 합니다. 설정 내용을 시스템에 저장하기 위해서 Top 모드에서 “**write**” 명령어를 사용합니다.


명령어	모드	기 능
<b>write</b>	Top	변경된 내용을 저장영역에 저장합니다.

 주의	설정 내용을 저장 중일 때 시스템의 전원을 Off하면 설정 내용을 잃어버리고 시스템 동작에 문제가 발생할 수 있습니다.
--	--

### ➤ 설정 내용 초기화

SG2024 Series 시스템을 공장 출하시의 값으로 초기화하고자 하는 경우에는 아래의 명령어를 이용합니다.

명령어	모드	기 능
<b>factory-default</b>	Config	설정 내용을 공장 출하시의 기본값으로 초기화합니다.

 참고	“factory-default” 명령을 입력하면 자동으로 reboot 후 설정이 초기화됩니다.
---	--

## 4.3 환경 설정

### ➤ Host Name 설정

관리의 편의를 위해 프롬프트에 나타나는 호스트 이름을 변경할 수 있습니다.  
(Default : SG2024)

명령어	모드	기능
<b>hostname</b> <i>name</i>	Config	Host Name을 변경합니다.

### ➤ 날짜 및 시간 설정 (NTP)

관리의 편의를 위해 시스템 시간을 설정 및 변경할 수 있습니다.

명령어	모드	기능
<b>clock</b> <i>HH:MM:SS dd mm yyyy</i>	Top	시스템에 현재 시간을 설정합니다. (자동 저장)
<b>show clock</b>	Top	시스템에 설정된 시간을 확인합니다.
<b>ntp server</b> <i>IPADDR</i>	config	NTP server의 ip address를 설정합니다.



참고

1. 시간을 변경하면 변경된 시간으로 자동 저장됩니다.
2. NTP를 설정한 경우 수동으로 시간을 설정할 수 없습니다.

### ➤ 로그인 배너 설정

콘솔 및 Telnet을 통해 접속하는 사용자에게 로그인 시 등록된 메시지를 표시합니다.

명령어	모드	기능
<b>banner motd</b> <i>word</i>	config	로그인 했을 때 출력되는 메시지를 등록합니다.

## 4.4 시스템 상태 정보

### ➤ 케이블 길이 확인

이상 발생 시 Cable 단절 등의 이상 유무를 확인하여, 단절된 부분까지의 케이블 길이를 확인할 수 있습니다. (“open”인 경우에만 Cable 길이 표시)

장비간 연결이 정상인 경우 “ok”로 표시되며, 케이블 길이를 표시하지 않습니다.

명령어	모드	기 능
<b>show cable-diag [IFNAME]</b>	Top	인터페이스에 연결된 케이블 길이를 알려줍니다.

### ➤ Mac Table 확인

명령어	모드	기 능
<b>show mac-table</b>	Top	MAC 주소를 출력합니다.
<b>show mac-table   include [IFNAME]</b>	Top	특정 포트의 MAC 주소를 출력합니다.

### ➤ ARP 정보 확인

명령어	모드	기 능
<b>show ip arp</b>	Top	ARP 정보를 출력합니다.
<b>arp ip-address mac-address</b>	Config	IP 주소와 MAC 주소를 ARP 테이블에 등록한다.
<b>no arp ip-address</b>	Config	수동으로 등록한 ARP 테이블을 삭제합니다.

### ➤ CPU 사용량 확인

명령어	모드	기 능
<b>show system cpu-load</b>	Top	사용자 스위치의 CPU 사용량 임계값과 CPU 평균 사용량을 확인할 수 있습니다.

### ➤ Memory 사용량 확인

명령어	모드	기 능
<b>show system memory</b>	Top	사용자 스위치의 메모리 사용 정보를 확인합니다.

### ➤ Version 확인

명령어	모드	기 능
<b>show version</b>	Top	시스템 이미지 버전을 확인합니다.
<b>show system system-info</b>	Top	시스템 정보를 확인합니다.

## 4.5 유해트래픽 차단(Multi Dimension Security) Engine

스위칭 패브릭을 통해 전송되는 트래픽은 동시에 MDS 엔진에 전달되고, MDS 엔진은 트래픽의 양과 시간을 한 축으로 하고 호스트와 TCP/UDP Port별 보안 상황 정보를 한 축으로 하여 트래픽을 분석합니다.

분석단계에서 S-IP, S-Port, D-IP, D-Port 네 가지의 집합을 이용한 다차원 매트릭스와 군집에서 얻어지는 고유 분산도 및 엔트로피를 이용하여 각 프로토콜 단위로 6개의 Cube에 의해 트래픽을 분류합니다.

이상 현상이 탐지되면 공격자와 피해자의 L3, L4 세부정보를 이용하여 자동으로 보안 필터를 생성하여 실시간으로 차단하며, 보안 필터의 경우 공격자에게서 발생된 트래픽 중 공격 트래픽만을 선별하여 차단(Smart Protection)하여 정상 서비스 트래픽을 안전하게 보장하여 줍니다.

DoS, DDoS, Flooding 등의 유해트래픽이 발생하는 경우 실시간으로 공격을 차단하나, SCAN 유형의 경우에는 트래픽의 변화 추이를 확인한 후 차단합니다. MDS 엔진에서 생성된 보안 필터로 인해 차단된 트래픽은 공격자로부터 같은 유형의 공격이 더 이상 발생하지 않으면 생성됐던 보안 필터를 자동으로 해제합니다.

다음은 MDS 관련 명령어입니다.

명령어	모드	기능
<code>mds uplink IFNAME</code>	CONFIG	mds를 enable하기 위해 Uplink Interface를 지정합니다. (default : ge)
<code>mds enable IFNAME {drop   detect}</code>	CONFIG	mds를 enable하기 위해 User Interface를 지정합니다. (default : fe detect)
<code>mds ddos disable</code>	CONFIG	mds ddos 차단 기능을 Disable 합니다.
<code>mds arp-spoofing-detect IFNAME</code>	Config	Interface 범위를 지정하여 ARP Spoofing 차단 기능을 설정합니다.
<code>no mds uplink IFNAME</code>	CONFIG	Uplink Interface를 삭제합니다.
<code>no mds enable [IFNAME [drop   detect]]</code>	CONFIG	유해Traffic 자동 차단 기능을 해제합니다.
<code>no mds arp-spoofing-detect IFNAME</code>	Config	Interface 범위를 지정하여 arp spoofing에 대한 탐지/차단 기능을 해제합니다.
<code>show mds config</code>	TOP	mds 설정 내역을 확인합니다.
<code>show mds arp-table</code>	Top	mds에 등록된 arp 정보를 보여줍니다.
<b><code>show mds detect-list</code></b>	Top	실시간 차단현황을 확인합니다.
<b><code>show mds detect-list log log_num</code></b>	Top	실시간 차단 세부 내역을 확인합니다.
<b><code>show mds detect-history</code></b>	Top	유해트래픽 차단로그를 확인합니다.
<b><code>show mds detect-history log log_num</code></b>	Top	유해트래픽 차단 세부 내역을 확인합니다.



참고

Uplink 포트 및 사용자 포트에 대한 설정은 내/외부 네트워크를 구분하여 유해트래픽을 차단하기 위해 설정합니다.



주의

상단의 네트워크 장비와 연결되는 Cable을 사용자 포트 쪽에 연결한 경우 외부로부터의 공격 발생 시 공격의 유형에 따라 상단에 설치되어 있는 네트워크 장비의 Mac-Address를 차단 할 수 있으므로, 반드시 Uplink 포트와 사용자 포트를 구분하여 설정하시기 바랍니다.

### 4.5.1 MDS 자동 차단 기능 설정 확인

MDS 설정은 Default로 enable되어 있습니다. MDS 설정상태는 Config 모드에서 확인할 수 있으며, default 설정은 ge 전체를 Uplink 포트, fe 전체를 사용자 포트르 사용하도록 설정되어 있습니다.

예제 1) Default Config 예제

```
SG2024(config)# show running-config
```

```
!
service password-encryption
!
username root password 8 4DBfucrfjXL6o
!
ip domain-lookup
!
spanning-tree mst config
!
maximum-paths 8
bridge 1 protocol rstp vlan-bridge
bridge 1 acquire
mls qos enable
no mls dos
mds enable fe detect
mds uplink ge
bridge 1 rstp errdisable-timeout interval 10
!
```

Uplink 포트를 ge가 아닌 포트에 연결한 경우, 해당 Uplink 포트를 지정하셔야 합니다.

fe를 User Interface로 설정 및 mds detect mode enable

ge를 Uplink Interface로 설정



예제2) ge1 만 Uplink 포트로 사용하고, fe전체 및 ge2를 사용자 포트 사용

```
SG2024(config)# show running-config
```

```
!  
service password-encryption  
!  
username root password 8 4DBfucrfjXL6o  
!  
ip domain-lookup  
!  
spanning-tree mst config  
!  
maximum-paths 8  
bridge 1 protocol rstp vlan-bridge  
bridge 1 acquire  
mls qos enable  
no mls dos  
mds enable fe,ge2 detect  
mds uplink ge1  
bridge 1 rstp errdisable-timeout interval 10  
!
```

fe,ge2를 User Interface로 설정 및  
mds detect mode enable  
ge1을 Uplink Interface로 설정

## 4.5.2 실시간 MDS 차단 현황 모니터링

유해트래픽이 탐지되면 공격자와 피해자의 L3, L4 세부정보를 이용하여 자동으로 보안 필터를 생성하여 실시간으로 차단하며, 자동 보안 필터의 경우 공격자에게서 발생된 트래픽 중 공격 트래픽만을 선별하여 차단하여 정상 서비스 트래픽을 안전하게 보장하여 줍니다. 또한, 일정 시간 동안 공격자로부터 동일한 형태의 공격이 더 이상 발생하지 않는 경우 차단을 자동 해제하여 줍니다

실시간 차단 현황의 리스트를 확인하는 예제입니다.

SG2024#show mds detect-list									
KeyNo	Phy	SourceIP & MAC	DestIP	Proto	SPort	Dport	SigName	DropPkt	TimeOut
12	14	100.111.1.2	Any	TCP	Any	445	Scan_Attack	115520	161
13	14	200.1.1.2	Any	TCP	Any	Any	Scan_Flooding	66987	61

KeyNo : MDS 차단 필터 번호  
 Phy : 유해트래픽이 발생한 물리적 포트 번호  
 SourceIP & MAC : 출발지 IP 정보 (Spoofing 공격등은 Mac Address로 표시)  
 DestIP : 목적지 IP 정보 (Flooding, Scan등의 경우 any로 표시)  
 Proto : 프로토콜 Type  
 Sport : 출발지 서비스 포트  
 DPort : 목적지 서비스 포트  
 SigName : 차단 정책명  
 DropPkt : 차단된 패킷 수  
 TimeOut : 차단 해제를 위해 대기 중인 시간

### 4.5.3 실시간 MDS 차단 현황 세부 내역 보기

실시간으로 차단된 유해트래픽의 세부 내역을 통해 차단된 유해트래픽의 공격 형태 등을 확인할 수 있습니다. 실시간 차단 현황의 세부 내역을 확인하는 예제입니다.

```

SG2024#show mds detect-list log 13
detect code : 13
Sig Name    : Scan_Flooding
from Date   : 07/01/15 13:25:25
to Date     : 07/01/15 13:25:29 (4 Sec)
Phy. Port No: 14
Source MAC  : 0090.fb03.22db
Source IP   : 200.1.1.2
Dest IP     : Any
Protocol    : TCP
Source Port : Any
Dest Port   : Any
Drop Count  : 66987
    
```

→ detect-list의 KeyNo.

No.	SourceIP	DestIP	Proto	SPort	DPort
1	200.1.1.2	220.168.2.78	TCP	2341	82
2	200.1.1.2	220.168.1.78	TCP	2294	90
3	200.1.1.2	220.168.2.77	TCP	2341	81
4	200.1.1.2	220.168.1.77	TCP	2294	89
5	200.1.1.2	220.168.2.76	TCP	2341	80
6	200.1.1.2	220.168.1.76	TCP	2294	88
7	200.1.1.2	220.168.2.75	TCP	1584	90
8	200.1.1.2	220.168.1.75	TCP	2294	87
9	200.1.1.2	220.168.2.74	TCP	1584	89
10	200.1.1.2	220.168.1.74	TCP	2294	86
11	200.1.1.2	220.168.2.73	TCP	1584	88

- detect code : 실시간 차단 로그 번호
- Sig Name : 차단 정책명
- from Date, to Date : 유해트래픽 차단 시간
- Phy. Port No : 유해트래픽이 발생한 물리적 포트 번호
- Source Mac : 공격자 Mac Address
- SourceIP : 공격자 IP Address 정보
- DestIP : 목적지 IP 정보 (Flooding, Scan등의 경우 any로 표시)
- Protocol : 프로토콜 Type
- Source Port : 출발지 서비스 포트
- Dest Port : 목적지 서비스 포트
- Drop Count : 차단된 패킷 수

#### 4.5.4 MDS 차단 로그(detect-history) 보기

유해트래픽이 차단된 후 더 이상의 유해트래픽이 발생하지 않으면 일정 시간 후 자동으로 생성되었던 차단정책이 해제되며 해제된 로그는 탐지(차단) 로그에 기록됩니다.

유해트래픽으로 확인되어 탐지(차단)되었던 로그를 확인하는 예제입니다.

SG2024#show mds detect-history											
SeqNo	Date Time	Phy	SourceIP & MAC	DestIP	Proto	SPort	DPort	SigName	DropPkt		
1	07/01/15 13:14:21	14	200.1.1.2	Any	TCP	Any	Any	Scan_Flooding	96		
2	07/01/15 13:18:15	14	100.111.1.2	Any	TCP	Any	445	Scan_Attack	420		
3	07/01/15 13:21:49	14	200.1.1.2	Any	TCP	Any	Any	Scan_Flooding	510		

SeqNo : MDS 차단 로그 번호  
 Date Time : 최초 차단된 시간  
 Phy : 유해트래픽이 발생한 물리적 포트 번호  
 SourceIP & MAC : 출발지 IP 정보 (Spoofing 공격등은 Mac Address로 표시)  
 DestIP : 목적지 IP 정보 (Flooding, Scan등의 경우 any로 표시)  
 Proto : 프로토콜 Type  
 SPort : 출발지 서비스 포트  
 DPort : 목적지 서비스 포트  
 SigName : 차단 정책명  
 DropPkt : 총 차단된 패킷 수

## 4.5.5 MDS 차단 로그(detect-history) 세부 내역 보기

유해트래픽으로 확인되어 탐지(차단)되었던 로그(detect-history)의 세부 내역을 통해 차단된 유해트래픽의 공격 형태 등을 확인할 수 있습니다.

차단된 로그의 세부 내역을 확인하는 예제입니다.

```

SG2024#show mds detect-history log 1 → detect-history의 SeqNo.
detect code : 8
Sig Name    : Scan_Flooding
from Date   : 07/01/15 13:14:21
to Date     : 07/01/15 13:14:26 (5 Sec)
Phy. Port No: 14
Source MAC  : 0090.fb03.22db
Source IP   : 200.1.1.2
Dest IP     : Any
Protocol    : TCP
Source Port : Any
Dest Port   : Any
Drop Count  : 96

```

No.	SourceIP	DestIP	Proto	SPort	DPort
1	200.1.1.2	220.168.3.52	TCP	1158	81
2	200.1.1.2	220.168.2.52	TCP	1426	89
3	200.1.1.2	220.168.3.51	TCP	1158	80
4	200.1.1.2	220.168.2.51	TCP	1426	88
5	200.1.1.2	220.168.3.50	TCP	2492	90
6	200.1.1.2	220.168.2.50	TCP	1426	87
7	200.1.1.2	220.168.3.49	TCP	2492	89
8	200.1.1.2	220.168.2.49	TCP	1426	86

detect code : MDS 차단 로그 번호  
 Sig Name : 차단 정책명  
 from Date, to Date : 유해트래픽 차단 시간  
 Phy. Port No : 유해트래픽이 발생한 물리적 포트 번호  
 Source Mac : 공격자 Mac Address  
 SourceIP : 공격자 IP Address 정보  
 DestIP : 목적지 IP 정보 (Flooding, Scan등의 경우 any로 표시)  
 Protocol : 프로토콜 Type  
 Source Port : 출발지 서비스 포트  
 Dest Port : 목적지 서비스 포트  
 Drop Count : 차단된 패킷 수

### 4.5.6 MDS 예외처리

스위치 내부 네트워크의 트래픽 중 특정 IP, 서비스 포트로 발생하는 특정 트래픽에 대해서는 어떠한 경우에도 차단하지 않도록 설정할 수 있습니다. 예외처리에 등록된 IP 또는 서비스포트로 발생하는 특정 트래픽의 경우 DoS, Flooding 등의 공격 트래픽이 발생하여도 차단하지 않습니다.


다음은 MDS 예외 처리와 관련된 명령어입니다.

명령어	모드	기능
<b>mds permit [any   icmp   mac   raw   tcp   udp] SIP DIP DPORT</b>	Config	MDS 엔진에서 차단하지 않을 트래픽의 유형을 지정합니다.
<b>clear mds KeyNo.</b>	Top	실시간 차단내역이 동작하는 경우 강제로 차단 정책을 해제 합니다.

다음은 특정 목적지 서버의 TCP 80 Port에 대해 예외 처리하는 예제입니다.

```

SG2024(config)# mds permit tcp any 192.168.1.10 80
SG2024(config)# show running-config
...
maximum-paths 8
bridge 1 protocol ieee vlan-bridge
bridge 1 acquire
mls qos enable
no mls dos
mds enable fe detect
mds uplink ge
mds permit tcp any 192.168.1.10 80
no bridge 1 stp enable bridge-forward
!
    
```

	<p>MDS 엔진에서 유해트래픽으로 인지하여 차단 정책이 생성되어 동작중인 상태에서는 MDS 예외 정책을 생성하여도 바로 예외로 적용되지 않습니다. 현재 차단중인 트래픽에 대해 예외 정책을 적용하시려면 다음 순서로 적용하시기 바랍니다.</p> <ol style="list-style-type: none"> <li>1. show mds detect-list : 예외 처리할 트래픽의 KeyNo. 확인</li> <li>2. mds permit SIP DIP DPORT : 예외 정책 생성</li> <li>3. clear mds KeyNo. : 차단정책 강제 해제</li> </ol>
<p>참고</p>	

## 4.5.7 Self Loop 차단

내부 네트워크에 이중 경로가 존재하지 않는다고 해도 네트워크 환경이나 케이블 상태 등에 따라 자신이 송신한 패킷이 다시 자신에게 돌아오는 **Loop** 현상이 발생할 수 있습니다. 이러한 경우를 방지하기 위해 자신이 내 보낸 패킷이 되돌아 오는 현상을 감지하여 차단하는 기능이 **Self Loop** 차단 기능입니다. **Self Loop** 차단 기능을 활성화 하면, 자신이 내보낸 패킷이 되돌아왔을 때 포트를 **Blocking** 하기 때문에 네트워크를 안전하게 운영할 수 있습니다.

Self Loop 차단 기능을 활성화 하는 명령어입니다.

명령어	모드	기 능
<b>mds self-loop-detect enable</b>	Config	Self Loop 차단 기능을 설정합니다.
<b>mds self-loop-detect range <i>IFNAME</i></b>	Config	Self Loop 차단 기능을 설정 할 Interface 범위를 지정합니다.
<b>no mds self-loop-detect enable</b>	Config	Self Loop 차단 기능을 해제합니다.

다음은 Self-loop 차단 기능을 활성화하는 예제입니다.

```
SG2024(config)# mds self-loop-detect enable
SG2024(config)# mds self-loop-detect range fe
SG2024#show mds detect-list
KeyNo Phy SourceIP & MAC DestIP Proto SPort DPort SigName DropPkt TimeOut
-----
1 3 0.0.0.0 Any NONE Self_Loop 976538 5
```



주의

1. STP와 mds self-loop-detect 기능을 동시에 사용 시, self-loop-detect 기능을 사용할 interface를 분리하시기 바랍니다.
2. STP를 enable한 상태에서 self-loop-detect 기능을 fe1-24 포트로 지정하게 되면, STP에서 사용하는 interface가 self-loop-detect에서 우선 차단되어 STP가 제대로 동작하지 않을 수 있습니다.

### 4.5.8 패킷 필터링

➤ NETBIOS 필터링

특정 Interface에 NetBIOS 차단 기능을 설정할 수 있습니다. (MS Windows 공유 차단)

명령어	모드	기능
<b>netbios filter</b>	Interface	NetBIOS 필터링을 설정합니다.
<b>no netbios filter</b>	Interface	NetBIOS 필터링을 해제합니다.

➤ DHCP 필터링


내부 네트워크에 IP 공유기 등 또 다른 DHCP 서버가 연결된 경우 일부 사용자에서 통신 장애가 발생할 수 있습니다. Interface에 DHCP 필터링을 설정 한 경우 해당 Interface로부터 다른 가입자 포트로 발생하는 DHCP Reply를 차단합니다.

명령어	모드	기능
<b>dhcp filter</b>	Interface	dhcp 필터링을 설정합니다.
<b>no dhcp filter</b>	Interface	dhcp 필터링을 해제합니다.

➤ 포트별 접속자 수 제한

Interface별로 접속 가능한 MAC 개수를 설정함으로써 사용자 수를 제한할 수 있으며, ISP의 경우 접속자 수에 따른 차별화된 서비스를 운용할 수 있습니다. 또한, Mac Spoofing과 같은 Attack이 발생하여도 네트워크를 안정적으로 운용할 수 있습니다.

명령어	모드	기능
<b>max-macs &lt;0-8192&gt;</b>	Interface	포트별 Mac 수를 제한합니다.
<b>no max-macs</b>	Interface	포트별 Mac 제한 기능을 해제합니다.
<b>show max-macs</b>	Top	Mac 제한 설정 상태를 확인합니다.

 참고	네트워크 내에 설치되어 있는 장비(스위치 등)들의 MAC 수를 고려해서 제한 설정을 하시기 바랍니다.
---	--



### ➤ Storm Control

Broadcast Storm이란 비정상적으로 과도한 Broadcast 패킷이 발생하는 현상을 말합니다. Broadcast, Multicast, DLF (Destination Lookup Fail)에 대하여 초당 pps 단위로 한계 값을 설정할 수 있으며, 한계 값을 초과하는 패킷은 자동으로 폐기합니다.

명령어	모드	기능
<b>storm-control [broadcast   dlf   multicast] &lt;0-1953125&gt;</b>	Interface	Storm Control 기능을 설정합니다.
<b>no storm-control [broadcast   dlf   multicast]</b>	Interface	Storm Control 기능을 해제합니다.

## 4.6 Visual Node Manager 연동

SG2024 Series의 관리는 Serial Console등의 CLI 를 통해 관리할 수 있으며 하나의 터미널을 통해서는 한대의 스위치만 접속하여 관리할 수 있기 때문에 다수의 SG2024 Series를 운용하는 경우 CLI를 통해 한대씩 접속하여 모니터링 및 관리하기에는 어려운 점이 많습니다. Visual Node Manager는 한 화면에서 다수의 장비를 모니터링 및 관리할 수 있는 프로그램입니다. Visual Node Manager를 통해 SG2024 Series를 관리하기 위해서는 스위치에서 SNMP Community 및 mds log-server를 설정해 주어야 합니다.

Visual Node Manager와 연동하여 SG2024 Series를 관리하기 위해서는 다음 명령어를 사용하십시오

명령어	모드	기능
<b>mds log-server IPAddr &lt;1-65536&gt;</b>	Config	mds log-server의 IP 및 서비스포트를 설정합니다. 서비스포트를 지정하지 않은 경우 default Port(8085)로 설정됩니다.
<b>snmp-server community rw NAME</b>	Config	Snmp community명을 설정합니다.

### 4.7 포트 상태 정보 보기 및 변경

이더넷 포트의 현재 설정상태 Interface의 Negotiation 설정상태, 포트별 사용량을 확인하려면 다음 명령어를 사용하십시오

➤ 포트 별 상태 정보 보기

```

SG2024#show port status
      ena/      auto forward learn inter      lastTime
port link speed duplex nego state oper face      linkChanged
-----
fe1  down      HD Yes - FA MII
fe2  down      HD Yes - FA MII
fe3  down      HD Yes - FA MII
fe4  down      HD Yes - FA MII
fe5  down      HD Yes - FA MII
fe6  down      HD Yes - FA MII
fe7  down      HD Yes - FA MII 2009/04/25 22:03:19
fe8  down      HD Yes - FA MII
fe9  down      HD Yes - FA MII
fe10 down      HD Yes - FA MII
fe11 down      HD Yes - FA MII
fe12 down      HD Yes - FA MII
fe13 down      HD Yes - FA MII
fe14 down      HD Yes - FA MII
fe15 down      HD Yes - FA MII
fe16 down      HD Yes - FA MII
fe17 down      HD Yes - FA MII
fe18 down      HD Yes - FA MII
fe19 down      HD Yes - FA MII
fe20 down      HD Yes - FA MII
fe21 down      HD Yes - FA MII
fe22 down      HD Yes - FA MII
fe23 down      HD Yes - FA MII 2009/04/25 22:03:20
fe24 down      HD Yes - FA MII
ge1  up        1g  FD Yes FORWARD FA SGMII 2009/04/25 22:18:24
ge2  down      HD Yes - FA SGMII
xe1  down      FD No - FA XGMII
SG2024#
SG2024#show port status fe7
      ena/      auto forward learn inter      lastTime
port link speed duplex nego state oper face      linkChanged
-----
fe7  down      HD Yes - FA MII 2009/04/25 22:03:19
SG2024#
    
```

➤ 포트 Negotiation 설정

SG2024#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

SG2024(config)#**interface fe9**

SG2024(config-if)#**speed 10m**

SG2024(config-if)#**end**

SG2024#**show port status fe9**

ena/	auto	forward	learn	inter			
port	link	speed	duplex	face			
fe9	up	10m	HD	No	FORWARD	FA	SGMII

SG2024#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

SG2024(config)# **interface fe9**

SG2024(config-if)#**duplex full**

SG2024(config-if)#**end**

SG2024#**show port status fe9**

ena/	auto	forward	learn	inter			
port	link	speed	duplex	face			
fe9	up	10m	FD	No	FORWARD	FA	SGMII

SG2024#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

SG2024(config)# **interface fe9**

SG2024(config-if)#**speed auto**

SG2024(config-if)#**end**

SG2024#**show port status fe9**

ena/	auto	forward	learn	inter			
port	link	speed	duplex	face			
fe9	up	1g	FD	Yes	FORWARD	FA	SGMII



참고

1. Auto Negotiation 기능이 Yes로 설정되지 않은 포트는 Auto MDIX를 지원하지 않습니다.
2. Fiber Media 이더넷의 경우 Full Duplex로만 동작하므로 Duplex 모드를 변경 할 수 없습니다.

➤ 포트별 사용량 확인

SG2024#**show bandwidth fe24**

port name	time	receive pkts/s	receive bytes/s	receive bits/s	sent pkts/s	sent bytes/s	sent bits/s
fe24	5s	116	122,738	981,904	82	12,715	101,720
fe24	30s	69	75,802	606,416	48	9,432	75,456
fe24	1m	62	73,188	585,504	41	9,142	73,136
fe24	5m	50	81,265	650,120	31	14,006	112,048
fe24	15m	46	97,117	776,936	29	19,264	154,112
fe24	60m	46	97,552	780,416	28	20,846	166,768



참고

1. receive : 스위치가 받는 트래픽량

2. sent : 스위치가 내보낸 트래픽량

## ➤ 포트별 사용 정보 확인

SG2024#**show interface fe1**

## ← 특정 포트 보기

## Interface fe1

Hardware is Ethernet, address is 001a.f400.0001 (bia 001a.f400.0001)  
index 5001 metric 1 mtu 1500 duplex-full arp ageing timeout 0  
<UP,BROADCAST,RUNNING,MULTICAST>  
VRF Binding: Not bound  
Speed 100m  
input packets 0343709, bytes 0161325487, dropped 00, multicast packets 04092763  
output packets 0144183418, bytes 4752536031, multicast packets 04092763 broadcast packets 0759  
linktrap Enabled

SG2024#**show interface**

## ← 전체 포트 보기

## Interface fe1

Hardware is Ethernet, address is 001a.f400.0001 (bia 001a.f400.0001)  
index 5001 metric 1 mtu 1500 duplex-full arp ageing timeout 0  
<UP,BROADCAST,RUNNING,MULTICAST>  
VRF Binding: Not bound  
Speed 100m  
input packets 0343715, bytes 0161325883, dropped 00, multicast packets 04092767  
output packets 0144183429, bytes 4752537017, multicast packets 04092767 broadcast packets 0759  
linktrap Enabled

## Interface fe2

Hardware is Ethernet, address is 001a.f400.0001 (bia 001a.f400.0001)  
index 5002 metric 1 mtu 1500 duplex-full arp ageing timeout 0  
<UP,BROADCAST,RUNNING,MULTICAST>  
VRF Binding: Not bound  
Speed 100m  
input packets 03867558, bytes 02877030475, dropped 00, multicast packets 04097257  
output packets 0147486037, bytes 42877006582, multicast packets 04097257 broadcast packets 02692  
linktrap Enabled

➤ 포트별 상태 정보 확인

SG2024#**show interface stat fe1**
← 특정 포트 보기

```

Interface fe1
-----
ifInOctets           :                0
ifInUcastPkts       :                0
ifInNUcastPkts      :                0
ifInDiscards        :                0
ifInErrors           :                0
ifInUnknownProtos   :                0
-----
ifOutOctets          :            40,256
ifOutUcastPkts       :                0
ifOutNUcastPkts     :                629
ifOutDiscards       :                0
ifOutErrors          :                0
ifOutQLens           :                0
-----
EtherStatsPkts640ctets :                629
EtherStatsPkts65to1270ctets :                0
EtherStatsPkts128to2550ctets :                0
EtherStatsPkts256to5110ctets :                0
EtherStatsPkts512to10230ctets :                0
EtherStatsPkts1024to15180ctets :                0
-----
Dot1dTpPortInFrames :                0
Dot1dTpPortOutFrames :                629
Dot3StatsInternalMacTransmitErrors :                0
Dot3StatsExcessiveCollisions :                0
Dot3StatsInternalMacReceiveErrors :                0
Dot3StatsLateCollisions :                0
IfHCOutMulticastPkts :                629
IfHCInBroadcastPkts :                0
EtherStatsBroadcastPkts :                0
EtherStatsMulticastPkts :                629
EtherStatsDropEvents :                0
EtherStatsUndersizePkts :                0
EtherStatsFragments :                0
EtherStatsOversizePkts :                0
EtherStatsJabbers :                0
EtherStatsCRCAlignErrors :                0
EtherStatsCollisions :                0
            
```

SG2024#**show interface stat**
← 전체 포트 상태 정보 보기

SG2024#**clear interface stat [IFNAME]**
← 포트별 상태 정보 초기화

## 4.8 Link Aggregation

### ▶ Link Aggregation의 두가지 방법

- ▷ **Static** – 직접 설정해야 하고 **aggregated port group**의 동작인 변화를 허용하지 않습니다.
- ▷ **IEEE 802.3ad(LACP)** – 스위치와 다른 네트워크 장비 간에 동적 **aggregated link**를 협상하는데 사용됩니다.



참고

표준으로 타사 장비와 연동해야 할 경우, LACP를 설정합니다.

### 4.8.1 Static Channel Group

Static-channel-group는 두 개 이상의 포트를 하나의 논리적인 포트로 통합하여 보다 넓은 대역폭을 사용할 수 있도록 하는 기능입니다.

명령어	모드	기능
<b>interface range <i>port-range</i></b>	Config	포트 범위를 선택합니다.
<b>static-channel-group &lt;1-12&gt;</b>	Interface	Static-channel-group을 설정합니다.
<b>show static-channel-group</b>	Top	설정 내용을 확인합니다.

```

SG2024(config)#interface range fe19-24
% fe19-24 Sected
SG2024(config-if-range)#static-channel-group 1
% fe19-24 Selected
SG2024(config-if)#end
SG2024#show static-channel-group
% Static Aggregator: sa1
% Member:
  fe19
  fe20
  fe21
  fe22
  fe23
  fe24
  
```

## 4.8.2 LACP

두 개 이상의 포트를 하나의 논리적인 포트로 통합하여 보다 넓은 대역폭을 사용할 수 있도록 하는 기능입니다. 포트를 통합할 논리적인 통합 포트(Aggregator)와 논리적인 포트로 통합할 물리적인 멤버 포트만 설정해두면 자동적으로 통합된 대역폭을 형성합니다.

명령어	모드	기능
<code>interface range <i>port-range</i></code>	Config	포트 범위를 선택합니다.
<code>channel-group &lt;1-65535&gt; mode { active   passive }</code>	Interface	Lacp를 active 또는 passive 모드로 설정합니다.
<code>port-channel load-balance { dst-ip   dst-mac   src-dst-ip   src-dst-mac   src-ip   src-mac }</code>	Interface po1	LACP를 경유하는 패킷의 처리 방법을 설정합니다.
<code>show etherchannel</code>	Top	설정 내용을 확인합니다.



```
SG2024(config)#interface range fe19-24
```

```
% fe19-24 Selected
```

```
SG2024(config-if-range)#channel-group 1 mode active
```

```
% fe19-24 Selected
```

```
SG2024(config-if-range)#end
```

```
SG2024#show etherchannel
```

```
% LACP Aggregator: po1
```

```
% Member:
```

```
fe19
```

```
fe20
```

```
fe21
```

```
fe22
```

```
fe23
```

```
fe24
```

```
SG2024#show etherchannel detail
```

```
% Aggregator po1 1000000
```

```
% Mac address: 00:1a:f4:00:10:14
```

```
% Admin Key: 0001 - Oper Key 0001
```

```
% Receive link count: 1 - Transmit link count: 0
```

```
% Individual: 0 - Ready: 1
```

```
% Partner LAG: 0x8000,00-d0-cb-2a-52-be
```

```
% Link: fe19 (5019) sync: 1
```

```
% Link: fe21 (5021) sync: 1
```

```
% Link: fe23 (5023) sync: 1
```

```
% Link: fe20 (5020) sync: 1
```

```
% Link: fe22 (5022) sync: 1
```

```
% Link: fe24 (5024) sync: 1
```

```
SG2024#show etherchannel load-balance
```

```
% LACP Aggregator: po1
```

```
Source Mac address
```

```
SG2024#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
SG2024(config)#interface po1
```

```
SG2024(config-if)#port-channel load-balance src-dst-mac
```

```
SG2024(config-if)#end
```

```
SG2024#show etherchannel load-balance
```

```
% LACP Aggregator: po1
```

```
Source and Destination Mac address
```

→ lACP 설정

→ lACP로 동작중인 member interface 확인

→ lACP load-balance 정책확인

→ lACP load-balance 정책변경

## 5. Sample Config

### 5.1 Port Vlan 설정

fe1, fe2를 vlan 10으로 설정

```

SG2024(config)#vlan database
SG2024(config-vlan)#vlan 10 bridge 1 state enable
SG2024(config-vlan)#exit
SG2024(config)#interface range fe1-2
% fe1-2 Selected
SG2024(config-if-range)#switchport access vlan 10
SG2024(config-if-range)#end

```

→ Vlan1.10 생성

→ Vlan1.10 에 interface 지정

```

SG2024#show vlan 10
                Bridge Group : 1

```

Bridge	VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
1	10	VLAN0010	ACTIVE	fe1(u) fe2(u)

→ Vlan1.10 의 전체 interface 확인

```

SG2024#show vlan brief
                Bridge Group : 1

```

Bridge	VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
1	1	default	ACTIVE	fe3(u) fe4(u) fe5(u) fe6(u) fe7(u) fe8(u) fe9(u) fe10(u) fe11(u) fe12(u) fe13(u) fe14(u) fe15(u) fe16(u) fe17(u) fe18(u) fe19(u) fe20(u) fe21(u) fe22(u) fe23(u) fe24(u) ge1(u) ge2(u)
1	10	VLAN0010	ACTIVE	fe1(u) fe2(u)

→ 전체 Vlan 설정 상태 확인

## 5.2 802.1Q VLAN 설정

fe1, fe2를 vlan 10으로 설정, fe3을 trunk로 설정

```

SG2024(config)#vlan database
SG2024(config-vlan)#vlan 10 bridge 1 state enable
SG2024(config-vlan)#exit
SG2024(config)#interface range fe1-2
% fe1-2 Selected
SG2024(config-if-range)#switchport access vlan 10
SG2024(config-if-range)#exit
SG2024(config)#interface fe3
SG2024(config-if)#switchport mode trunk
SG2024(config-if)#switchport trunk allowed vlan add 10
SG2024(config-if)#end

SG2024#show vlan 10
                Bridge Group : 1

Bridge          VLAN ID  Name                State  Member ports
                (u)-Untagged, (t)-Tagged
=====
1                10      VLAN0010           ACTIVE fe1(u) fe2(u) fe3(t)

SG2024#show vlan brief
                Bridge Group : 1

Bridge          VLAN ID  Name                State  Member ports
                (u)-Untagged, (t)-Tagged
=====
1                1        default            ACTIVE fe4(u) fe5(u) fe6(u) fe7(u)
                fe8(u) fe9(u) fe10(u) fe11(u)
                fe12(u) fe13(u) fe14(u)
                fe15(u) fe16(u) fe17(u)
                fe18(u) fe19(u) fe20(u)
                fe21(u) fe22(u) fe23(u)
                fe24(u) ge1(u) ge2(u) fe3(t)
1                10      VLAN0010           ACTIVE fe1(u) fe2(u) fe3(t)

```

### 5.3 Shared VLAN 설정

fe1~11를 vlan 10, fe12~22를 vlan 20, fe23~24, ge를 vlan 30 (Uplink)으로 설정

```

SG2024(config)#vlan database
SG2024(config-vlan)#vlan 10 bridge 1 state enable
SG2024(config-vlan)#vlan 20 bridge 1 state enable
SG2024(config-vlan)#vlan 30 bridge 1 state enable
SG2024(config-vlan)#shared-vlan 30 block
SG2024(config-vlan)#exit
SG2024(config)#interface range all
% all Selected
SG2024(config-if-range)#switchport mode hybrid
% all Selected
SG2024(config-if-range)#switchport hybrid allowed vlan add 30 egress-tagged disable
% all Selected
SG2024(config-if-range)#exit
SG2024(config)#interface range fe1-11
% fe1-11 Selected
SG2024(config-if-range)#switchport hybrid vlan 10
% fe1-11 Selected
SG2024(config-if-range)#exit
SG2024(config)#interface range fe12-22
% fe12-22 Selected
SG2024(config-if-range)#switchport hybrid vlan 20
% fe12-22 Selected
SG2024(config-if-range)#exit
SG2024(config)#interface range fe23-24
% fe23-24 Selected
SG2024(config-if-range)#switchport hybrid vlan 30
% fe23-24 Selected
SG2024(config-if-range)#switchport hybrid allowed vlan add 10 egress-tagged disable
% fe23-24 Selected
SG2024(config-if-range)#switchport hybrid allowed vlan add 20 egress-tagged disable
% fe23-24 Selected
SG2024(config-if-range)#end
SG2024#show vlan brief

```

```

          Bridge Group : 1

```

Bridge	VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
1	1	default	ACTIVE	
1	10	VLAN0010	ACTIVE	fe1(u) fe2(u) fe3(u) fe4(u) fe5(u) fe6(u) fe7(u) fe8(u) fe9(u) fe10(u) fe11(u) fe23(u) fe24(u)
1	20	VLAN0020	ACTIVE	fe12(u) fe13(u) fe14(u) fe15(u) fe16(u) fe17(u) fe18(u) fe19(u) fe20(u) fe21(u) fe22(u) fe23(u) fe24(u)
1	30	VLAN0030	ACTIVE	fe1(u) fe2(u) fe3(u) fe4(u) fe5(u) fe6(u) fe7(u) fe8(u) fe9(u) fe10(u) fe11(u) fe12(u) fe13(u) fe14(u) fe15(u) fe16(u) fe17(u) fe18(u) fe19(u) fe20(u) fe21(u) fe22(u) fe23(u) fe24(u) ge1(u) ge2(u)

```

SG2024#show bridge

```

bridge	VLAN	port	mac	fwd	timeout
1	10	fe3	0017.420c.d547	1	300
1	20	fe15	000c.f1c0.662b	1	300
1	30	fe24	001a.f400.0101	1	300
1	30	fe24	0002.b3af.b9fd	1	300
1	30	fe24	0002.b3e9.5fa3	1	300

## 5.4 Shared VLAN egress-port 설정

fe1~11를 vlan 10, fe12~22를 vlan 20, fe23~24,ge를 vlan 30 (Uplink) Vlan으로 설정.  
vlan10 내에서 통신 허용, vlan20은 fe24으로만 통신이 가능하도록 설정

```
SG2024(config)#vlan database
SG2024(config-vlan)#vlan 10 bridge 1 state enable
SG2024(config-vlan)#vlan 20 bridge 1 state enable
SG2024(config-vlan)#vlan 30 bridge 1 state enable
SG2024(config-vlan)#shared-vlan 30 block
SG2024(config-vlan)#exit
SG2024(config)#interface range all
% all Selected
SG2024(config-if-range)#switchport mode hybrid
% all Selected
SG2024(config-if-range)#switchport hybrid allowed vlan add 30 egress-tagged disable
% all Selected
SG2024(config-if-range)#exit
SG2024(config)#interface range fe1-11
% fe1-11 Selected
SG2024(config-if-range)#switchport hybrid vlan 10
% fe1-11 Selected
SG2024(config-if-range)#exit
SG2024(config)#interface range fe12-22
% fe12-22 Selected
SG2024(config-if-range)#switchport hybrid vlan 20
% fe12-22 Selected
SG2024(config-if-range)#exit
SG2024(config)#interface range fe23-24
% fe23-24 Selected
SG2024(config-if-range)#switchport hybrid vlan 30
% fe23-24 Selected
SG2024(config-if-range)#switchport hybrid allowed vlan add 10 egress-tagged disable
% fe23-24 Selected
SG2024(config-if-range)#switchport hybrid allowed vlan add 20 egress-tagged disable
% fe23-24 Selected
SG2024(config-if-range)#end
SG2024(config)#interface range fe12-22
% fe12-22 Selected
SG2024(config-if-range)#switchport shared-vlan egress-port fe24
% fe12-22 Selected
SG2024(config-if)#exit
```

```
SG2024(config-if)#end
SG2024#show vlan brief
```

```
Bridge Group : 1
```

Bridge	VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
1	1	default	ACTIVE	
1	10	VLAN0010	ACTIVE	fe1(u) fe2(u) fe3(u) fe4(u) fe5(u) fe6(u) fe7(u) fe8(u) fe9(u) fe10(u) fe11(u) fe23(u) fe24(u)
1	20	VLAN0020	ACTIVE	fe12(u) fe13(u) fe14(u) fe15(u) fe16(u) fe17(u) fe18(u) fe19(u) fe20(u) fe21(u) fe22(u) fe23(u) fe24(u)
1	30	VLAN0030	ACTIVE	fe1(u) fe2(u) fe3(u) fe4(u) fe5(u) fe6(u) fe7(u) fe8(u) fe9(u) fe10(u) fe11(u) fe12(u) fe13(u) fe14(u) fe15(u) fe16(u) fe17(u) fe18(u) fe19(u) fe20(u) fe21(u) fe22(u) fe23(u) fe24(u) ge1(u) ge2(u)

```
SG2024#show bridge
```

bridge	VLAN	port	mac	fwd	timeout
1	10	fe3	0017.420c.d547	1	300
1	20	fe15	000c.f1c0.662b	1	300
1	30	fe24	001a.f400.0101	1	300
1	30	fe24	0002.b3af.b9fd	1	300
1	30	fe24	0002.b3e9.5fa3	1	300

## 5.5 QoS 설정

(qos-access-list → class → police → mapping)

### 5.5.1 SPQ를 이용한 QoS 설정

IP 192.168.10.1, 192.168.20.1에서 발생된 트래픽 중 IP 192.168.10.1이고 DSCP 46으로 Marking 된 트래픽을 최우선 순위 QoS 정책으로 적용하고자 할 때

```
SG2024(config)#qos-access-list 100 permit ip host 192.168.10.1 any 46
SG2024(config)#qos-access-list 101 permit ip host 192.168.20.1 any
SG2024(config)#class-map c1
SG2024(config-cmap)#match qos-access-group 100
SG2024(config-cmap)#exit
SG2024(config)#class-map c2
SG2024(config-cmap)#match qos-access-group 101
SG2024(config-cmap)#exit
SG2024(config)#policy-map p1
SG2024(config-pmap)#class c1
SG2024(config-pmap-c)#set cos 7
SG2024(config-pmap-c)#exit
SG2024(config-pmap)#class c2
SG2024(config-pmap-c)#set cos 1
SG2024(config-pmap-c)#exit
SG2024(config-pmap)#exit
SG2024(config)#queue sched spq
SG2024(config)#interface range fe1-5
% fe1-5 Selected
SG2024(config-if-range)#service-policy input p1
```

## 5.5.2 WRR을 이용한 QoS 설정

IP 192.168.10.1(DSCP 46), 192.168.20.1(DSCP 40), 192.168.30.1(DSCP 26), 192.168.40.1의 트래픽에 대해 QoS 정책을 설정하여 4:3:2:1 비율로 Forwarding 할 때

```
SG2024(config)#qos-access-list 100 permit ip host 192.168.10.1 any 46
SG2024(config)#qos-access-list 101 permit ip host 192.168.20.1 any 40
SG2024(config)#qos-access-list 102 permit ip host 192.168.30.1 any 26
SG2024(config)#qos-access-list 103 permit ip host 192.168.40.1 any
SG2024(config)#class-map c1
SG2024(config-cmap)#match qos-access-group 100
SG2024(config-cmap)#exit
SG2024(config)#class-map c2
SG2024(config-cmap)#match qos-access-group 101
SG2024(config-cmap)#exit
SG2024(config)#class-map c3
SG2024(config-cmap)#match qos-access-group 102
SG2024(config-cmap)#exit
SG2024(config)#class-map c4
SG2024(config-cmap)#match qos-access-group 103
SG2024(config-cmap)#exit
SG2024(config)#policy-map p1
SG2024(config-pmap)#class c1
SG2024(config-pmap-c)#set cos 4
SG2024(config-pmap-c)#class c2
SG2024(config-pmap-c)#set cos 3
SG2024(config-pmap-c)#class c3
SG2024(config-pmap-c)#set cos 2
SG2024(config-pmap-c)#class c4
SG2024(config-pmap-c)#set cos 1
SG2024(config-pmap-c)#exit
SG2024(config-pmap)#exit
SG2024(config)#queue sched wrr 0 1 2 3 4 5 6 7
SG2024(config)#interface range fe1-5
% fe1-5 Selected
SG2024(config-if-range)#service-policy input p1
```