

Version 1.4

SG Switch Series Command Guide

HANDREAMNET
www.handreamnet.com

저작권

이 설명서의 저작권은 (주)한드림넷에 있습니다.

이 설명서는 (주)한드림넷의 서면동의 없이 어떤 형태로도 재생산, 배포, 변경할 수 없습니다.

등록상표

이 설명서에 언급된 등록상표는 그 해당 회사 소유의 등록상표입니다.

제품을 설치 및 운용하기 전에 이 설명서를 반드시 읽고, 설명서의 내용에 따라 제품을 안전하고 올바르게 사용하여 주십시오.

이 설명서는 제품의 기능 향상, 설계 변경에 따라 내용이 수정될 수 있습니다. 수정된 설명서가 필요하거나 설명서의 내용에 대해 궁금한 사항이 있으면 아래의 주소나 홈페이지로 문의 바랍니다.

주소: 서울특별시 구로구 디지털로 30 길 28 마리오타워 1209 호

☎152-741

홈페이지: <http://www.handreamnet.com>

제품에 대한 불만 사항이나 요청 사항이 있으면 Call Center 로 문의 바랍니다.
전화: 1661-6650

목차

제1장. 관리기능 15

1.1 콘솔 연결 15

1.2 MGMT 포트 16

1.3 CLI 기본 사용법 17

1.3.1 명령어 체계 17

1.3.2 사용 가능한 명령어 보기 25

1.3.3 단축 명령어 26

1.3.4 실행된 명령어 목록 확인 26

1.3.5 이전 명령어 불러오기 27

1.3.6 TOP 모드 명령어 실행 28

1.3.7 Show 명령어 29

1.3.8 이전 모드로 전환하기 34

1.3.9 명령어 표기법 34

1.4 접속 및 관리 IP 설정 35

1.4.1 Login 35

1.4.2 Password 변경 36

1.4.3 자동 Logout 기능 38

1.4.4 사용자 추가 41

1.4.5 관리 IP 주소 설정 45

1.4.6 Telnet 및 SSH 48

1.4.7 동시 접속자 수 제한기능 53

1.4.8 Login 실패 시 접속차단기능 54

1.4.9	관리자 등급기반의 CLI 접근 통제	55
1.4.10	CPU-ACL을 통한 관리자 접근 통제	61
1.5	환경 설정	63
1.5.1	Host Name 설정	63
1.5.2	날짜 및 시간 설정	64
1.5.3	NTP / SNTP Setup	65
1.5.4	Timezone 설정	68
1.5.5	DNS 설정	70
1.5.6	Banner 설정	72
1.5.7	L3 License 등록	74
1.5.8	설정 내용 관리	76
1.6	시스템 상태 정보	80
1.6.1	Network 상태 확인(Ping Test)	80
1.6.2	Packet 경로 확인	82
1.6.3	Cable 길이 / 상태 확인	83
1.6.4	현재 접속자 확인	84
1.6.5	MAC Table / MAC-Count	85
1.6.6	ARP Table	87
1.6.7	Uptime 정보	89
1.6.8	CPU 사용량	90
1.6.9	Memory 사용량	91
1.6.10	Process 상태	92
1.6.11	FAN / 온도 Alarm 설정 및 확인	93
1.6.12	Version 정보	94
1.6.13	System 정보	95
1.6.14	SFP Mode Definition (MOD-DEF)	96

1.6.15	Scanning 기능	98
1.6.16	TFM 기능	99
1.6.17	Mode Button 설정.....	103
1.6.18	자체 검사 기능.....	104
1.7	Interface	107
1.7.1	Interface 상태 정보.....	107
1.7.2	Interface 활성화 / 비활성화.....	113
1.7.3	Interface Negotiation 설정.....	115
1.7.4	Interface MDIX 설정.....	117
1.7.5	MTU 설정	119
1.7.6	Flow Control 설정.....	121
1.7.7	Interface 사용량 확인	122
1.7.8	Port Mirroring 설정.....	123
1.7.9	Power Saving (Green IT).....	124
1.7.10	PoE 기능	127
1.7.11	UDLD 설정	134
1.8	SNMP	136
1.8.1	SNMP 설정.....	136
1.8.2	SNMP Community 설정.....	138
1.8.3	SNMP Trap 설정	140
1.8.4	SNMP Version 1/2/3 View 기반 접근 제어 설정	143
1.9	Syslog	147
1.9.1	Syslog 설정	147
1.9.2	Remote Syslog 설정	150
1.10	sFlow	152

1.11	RMON	154
1.11.1	Statistics 설정	155
1.11.2	History 설정.....	157
1.11.3	Event 설정	159
1.11.4	Alarm 설정	161

제2장. 시스템 운영 163

2.1	VLAN.....	163
2.1.1	VLAN 개요.....	163
2.1.2	VLAN 설정.....	164
2.1.3	Port VLAN 설정	165
2.1.4	802.1Q VLAN 설정	167
2.1.5	Hybrid VLAN 설정	169
2.1.6	Shared-VLAN Egress-Port 설정.....	174
2.1.7	MAC / IP / Protocol Based VLAN.....	178
2.1.8	GVRP 설정	181
2.1.9	Voice VLAN	186
2.1.10	VLAN Stacking (QinQ) 설정	189
2.2	Link Aggregation	195
2.2.1	Static Channel Group	196
2.2.2	LACP	198
2.2.3	Load Balance 설정.....	200
2.3	Redundancy.....	202
2.3.1	SPR(Smart Port Redundancy)	202
2.3.2	SSR (Smart Switch Redundancy)	203

2.4	LLDP / CDP	208
2.4.1	LLDP (Link Layer Discovery Protocol)	209
2.4.2	LLDP-MED (LLDP-Media Endpoint Discovery)	212
2.4.3	CDP (Cisco Discovery Protocol).....	217
2.5	Spanning Tree	219
2.5.1	개요	219
2.5.2	STP / RSTP / MSTP / PVSTP 동작	220
2.5.3	Spanning Tree Mode 설정	225
2.5.4	Spanning Tree 활성화	227
2.5.5	Root Switch 설정	229
2.5.6	Path-Cost.....	231
2.5.7	Port-Priority	233
2.5.8	Edgeport.....	235
2.5.9	Force-Version	237
2.5.10	Root Guard.....	239
2.5.11	Link-Type	241
2.5.12	MST Region 설정	243
2.5.13	BPDU 전송 설정	245
2.5.14	Portfast, BPDU-Guard.....	248
2.5.15	Spanning-Tree 예제	251
2.6	QoS.....	263
2.6.1	QoS 개요.....	263
2.6.2	QoS 적용 방법	263
2.6.3	QoS ACL 설정	266
2.6.4	QoS Class Map 설정	270
2.6.5	QoS 정책 설정 및 적용	272

2.6.6	QoS 스케줄링 설정	274
2.6.7	Interface 별 속도 제한	278
2.7	IGMP	280
2.7.1	IGMP Snooping	281
2.7.2	IGMP Snooping Fast-leave	283
2.7.3	IGMP Filter	286
2.8	MLD	289
2.8.1	MLD Snooping	289
2.8.2	MLD Filter	292
2.9	사용자 인증	295
2.9.1	사용자 인증 Interface 설정 (802.1x)	295
2.9.2	시스템 사용자 인증 (RADIUS / TACACS+)	302
2.9.3	802.1x Extended Authentication	304
2.9.4	Embedded RADIUS Server	310
2.10	Filtering	312
2.10.1	ACL을 이용한 Filtering	312
2.10.2	MAC Address Filtering	315
2.10.3	Interface별 접속자 수 제한	316
2.10.4	Port Security	318
2.10.5	NetBIOS Filtering	320
2.10.6	DHCP Filtering	322
2.10.7	Storm Control	324
2.10.8	MLS (Multi-Layer Switch) DoS 기능	326
2.10.9	IP Source Guard	329
2.11	MDS	332

2.11.1	MDS 개요	332
2.11.2	Network 공격의 유형	341
2.11.3	MDS 자동 차단 기능 설정 확인	347
2.11.4	MDS 실시간 차단 Log 보기.....	349
2.11.5	MDS 차단 Log(detect-history) 보기	351
2.11.6	MDS Permit.....	353
2.11.7	MDS Extended Permit / Deny	357
2.11.8	Self Loop 차단.....	358
2.11.9	ARP Spoofing 차단	361
2.11.10	ICMP Redirect 차단.....	364
2.11.11	IF-PKT-Loss 탐지	367
2.11.12	MAC Flooding 차단	369
2.11.13	MDS Web-Alert.....	373
2.11.14	IPv6 DAD Attack 차단.....	379
2.11.15	Auto-Config	381
2.11.16	DDoS Disable	383
2.11.17	MDS Policy-ACT	384
2.11.18	MDS Threshold.....	386
2.11.19	MDS Detect-Port-Range.....	388
2.11.20	MDS DHCP-Filter	389
2.11.21	MDS ARP-List Send-Port All	390
2.11.22	MDS Attack-CRC	391
2.11.23	MDS Attack-Fragment.....	392
2.11.24	MDS Attack-Smurf	393
2.11.25	MDS ARP-Only-Collection	394
2.11.26	MDS Detect-Port-Lock	395

2.11.27	MDS NetBIOS.....	396
2.11.28	MDS IP-Range-Scan.....	397
2.11.29	MDS IPM-Accept.....	398
2.11.30	MDS IPM-Collision.....	398
2.11.31	MDS IPM-Guard-To-MAC-Security	399
2.11.32	MDS IPM-Interface.....	401
2.11.33	MDS IPM-Local-DHCP	402
2.11.34	MDS IPM-Permit.....	403
2.11.35	MDS IPM-Probe	404
2.11.36	MDS IPM-Range-Over-MSG-Disable	405
2.11.37	Visual Node Manager (VNM) 연동.....	406
2.11.38	Visual IP Manager (VIPM) 연동.....	408
2.12	DHCP.....	411
2.12.1	DHCP Server 설정	411
2.12.2	DHCP Relay	416
2.12.3	DHCP Unleased-IP	418
2.12.4	DHCP Option-82 설정	420
2.12.5	DHCP Snooping.....	421
2.13	ERP	424

제3장. Routing Protocol 432

3.1	BGP Routing Protocol.....	432
3.1.1	기본설정.....	433
3.1.2	BGP Routing 활성화.....	434
3.1.3	BGP Neighbor Router 설정	435

3.1.4	Routing 정책 변경.....	436
3.1.5	BGP Weights 설정	439
3.1.6	AS 경로 무시	439
3.1.7	AS 경로 사용중지	440
3.1.8	AS 경로 필터링	441
3.1.9	Prefix List를 이용한 BGP 필터링	442
3.1.10	다음 목적지로의 정보전달차단	445
3.1.11	BGP 버전설정.....	446
3.2	BGP 고급설정	447
3.2.1	Route-Map을 이용한 경로변경	448
3.2.2	통합주소 (Aggregate Address) 설정.....	448
3.2.3	BGP Community 필터링 설정.....	449
3.2.4	Router 식별번호 설정.....	450
3.2.5	BGP에 경로 배포하기	450
3.2.6	Routing Domain 연합 설정.....	451
3.2.7	경로 반영자(Route Reflector) 설정	452
3.2.8	Neighbor 명령어를 이용한 설정.....	453
3.2.9	Neighbor 라우터 동작종료	455
3.2.10	Backdoor 경로지정.....	455
3.2.11	거리값 설정.....	456
3.2.12	BGP 시간조정.....	457
3.2.13	첫 번째 AS 설정	458
3.2.14	로컬네트워크의 우선 순위변경	458
3.2.15	외부네트워크의 우선 순위변경	458
3.2.16	MED 없는 경로를 최악의 경로로 간주	459
3.2.17	AS들이 전달한 MED 값으로 경로 선택	459

3.2.18	MED를 이용한 연합 경로선택	459
3.2.19	MED를 이용한 연합 내 경로선택	460
3.2.20	반영된 경로저장	460
3.2.21	경로 무효화(Route Dampening).....	461
3.2.22	BGP 점검과 관리.....	463
3.3	OSPF Routing Protocol	465
3.3.1	OSPF 활성화.....	466
3.3.2	ABR 유형설정.....	468
3.3.3	호환성지원	468
3.3.4	OSPF 인터페이스 설정	469
3.3.5	OSPF 네트워크 타입설정	471
3.3.6	Non-Broadcast 네트워크 설정	472
3.3.7	OSPF 영역(Area)설정.....	473
3.3.8	OSPF 영역 사이의 대표경로 설정	474
3.3.9	가상라인 (Virtual Link) 생성	475
3.3.10	경로값의 변경	475
3.3.11	경로계산 주기설정	476
3.3.12	OSPF 네트워크에 경로전달	476
3.3.13	기본경로 (Default Route) 설정	477
3.3.14	OSPF 거리값 변경	477
3.3.15	정보전달 차단	478
3.3.16	갱신된 정보 차단	478
3.3.17	OSPF 모니터링과 관리	479
3.4	RIP Routing Protocol.....	481
3.4.1	RIP 활성화	482
3.4.2	RIP Neighbor 라우터 지정	484

3.4.3	RIP Version 지정.....	485
3.4.4	RIP 에서만 유효한 Static 경로생성	486
3.4.5	Routing 정보전달	486
3.4.6	전달되는 경로의 경로값 설정.....	488
3.4.7	거리값(Administrative Distance) 설정	489
3.4.8	기본경로 (Default Route) 생성	489
3.4.9	Routing Infomation Filtering.....	490
3.4.10	시간설정.....	491
3.4.11	경로차단(Split-horizon) 활성화/비활성화.....	492
3.4.12	인증키 관리.....	493
3.4.13	RIP 모니터 및 관리.....	494
3.5	VRRP (Virtual Router Redundancy Protocol).....	495
3.5.1	VRRP 기본설정	496
3.5.2	Authentication 패스워드 설정	501
3.5.3	Preempt 기능 설정	502
3.5.4	Advertisement Time 설정	503

제4장. 부록..... 504

4.1	OS Image Upgrade	504
4.2	USB Auto Upgrade	506
4.3	OS Image 선택.....	509
4.4	FTP로 Config Backup/Restore, Syslog Backup.....	510
4.5	Reload 스케줄링	513
4.6	Packet Debug 기능	514

4.7	Boot Loader에서의 Password 및 Config Recovery	515
4.8	OS 업그레이드 Fail 시 복구 방법	516
4.9	Alarm 발생 시 확인 사항	518
4.9.1	내부 온도 확인	519
4.9.2	FAN Fail 확인	520
4.9.3	PSU Fail 확인	521
4.10	Wizard 기능을 이용한 손쉬운 설치	522
4.11	Tech-Support	528
4.12	RAW IP Protocol	530
4.13	RFC / IEEE Support	535
4.13.1	RFC Support	535
4.13.2	IEEE Support	538
4.14	Syslog Event 정의	539
4.15	MDS 엔진에서 탐지하는 공격 유형	542

그림

[그림 1-1] TFM Port 용도.....	99
[그림 1-2] Power Saving	124
[그림 1-3] PoE 연결 구성	128
[그림 2-1] Hybrid VLAN 구성도	169
[그림 2-2] shared-vlan egress-port Traffic 흐름	174
[그림 2-3] VLAN Stacking (QinQ) 구성	189
[그림 2-4] STP 구성.....	219
[그림 2-5] MSTP 구성도 및 Traffic 흐름	222
[그림 2-6] 802.1x 사용자 인증 과정.....	296
[그림 2-7] Web-based 인증 Default	306
[그림 2-8] MDS Engine	333
[그림 2-9] DoS 공격의 형태	341
[그림 2-10] DDoS 공격의 형태.....	342
[그림 2-11] The pattern(type) of SCAN 공격	343
[그림 2-12] Traffic flow when happening IP Spoofing.....	344
[그림 2-13] ARP Spoofing 발생 시 Traffic 흐름도.....	346
[그림 2-14] ICMP Redirect Attack 동작.....	364
[그림 2-15] MDS Web-Alert 동작 원리	373
[그림 2-16] MDS Web-Alert 동작 후 IE 화면	378
[그림 2-17] ERP Single Ring 연결 구성	425
[그림 2-18] ERP Multi Ring 연결 구성	425
[그림 4-1] 장비 후면 외관	521

표

[표 1-1] Non-PRIVILEGE 모드 주요 명령어	18
[표 1-2] TOP (PRIVILEGE) 모드 주요 명령어.....	19
[표 1-3] CONFIG 모드 주요 명령어.....	20
[표 1-4] VLAN 설정 모드 주요 명령어.....	21
[표 1-5] DHCP 설정 모드 주요 명령어.....	21
[표 1-6] INTERFACE 모드 주요 명령어	22
[표 1-7] LINE 설정 모드 주요 명령어.....	23
[표 1-8] QoS CLASS-MAP 모드 주요 명령어.....	23
[표 1-9] QoS POLICY-MAP 모드 주요 명령어	24
[표 1-10] Main Commands of QoS POLICY-MAP-CLASS	24
[표 1-11] 단축 명령어 형태	26
[표 1-12] 자주 사용하는 show 명령어	30
[표 1-13] Timezone (GMT 시각).....	68
[표 1-14] Interface Default 설정.....	107
[표 2-1] show gvrp machine의 state 값 (GARP 표준).....	182
[표 2-2] Load Balance 방법.....	200
[표 2-3] LLDP / CDP 비교	208
[표 2-4] LLDP / CDP 지원 내역.....	208
[표 2-5] LLDP-MED Civic Address Type (ANNEX B)	214
[표 2-6] STP와 RSTP의 Interface 상태 비교.....	223
[표 2-7] STP와 RSTP의 포트 역할.....	224
[표 2-8] path-cost 값	231
[표 2-9] QoS Default Map	265
[표 2-10] Multicast Address Range	280
[표 2-11] Multicast Routing Protocol Address	280

제1장. 관리기능

1.1 콘솔 연결

관리자는 SG Switch Series에서 제공하는 RJ-45 형태의 Console Port와 관리단말을 연결하여 관리할 수 있습니다. Console Port에 연결된 단말 모드(Terminal Mode)의 설정은 아래와 같습니다

항 목	Baud Rate	Parity	Data Bits	Stop Bits	Flow Control
설 정	9600 bps	None Parity	8 bits	1 stop bit	No Flow Control

Switch 측은 RJ-45 커넥터로 연결되며, 관리 단말 측은 9핀 RS-232 커넥터로 연결됩니다.

RS-232 커넥터의 핀 설정은 다음과 같습니다.

■ Console Port Pin-Outs

Switch측(RJ-45)	PC측 (DB-9)	Switch측 핀 기능	PC측 핀 기능
3	2	TX (Data 송신)	RX (Data 수신)
6	3	RX (Data 수신)	TX (Data 송신)
4,5	5	GND (접지)	GND (접지)

1.2 MGMT 포트

관리자는 SG Switch Series의 MGMT(RJ-45) Interface에 Cable을 연결하여 관리할 수 있습니다. MGMT Interface는 Firmware Upgrade Fail 등으로 인해 Booting 되지 않는 경우 Bootloader 모드에서 Firmware Upgrade등을 하거나 Debug용으로 사용하는 Interface이며, 일반적으로는 사용되지 않습니다.

MGMT Interface를 사용하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
interface mgmt {ip ipv6} address <i>IP_Addr/M</i>	CONFIG	Management interface 주소를 설정합니다.
interface mgmt ip route default <i>Gateway_Addr</i>	CONFIG	Management interface의 Gateway 주소를 설정합니다.

MGMT Interface를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no interface mgmt {ip ipv6} address	CONFIG	Management interface 주소를 삭제합니다.
no Interface mgmt ip route default	CONFIG	Management interface의 Gateway 주소를 삭제합니다.



참고

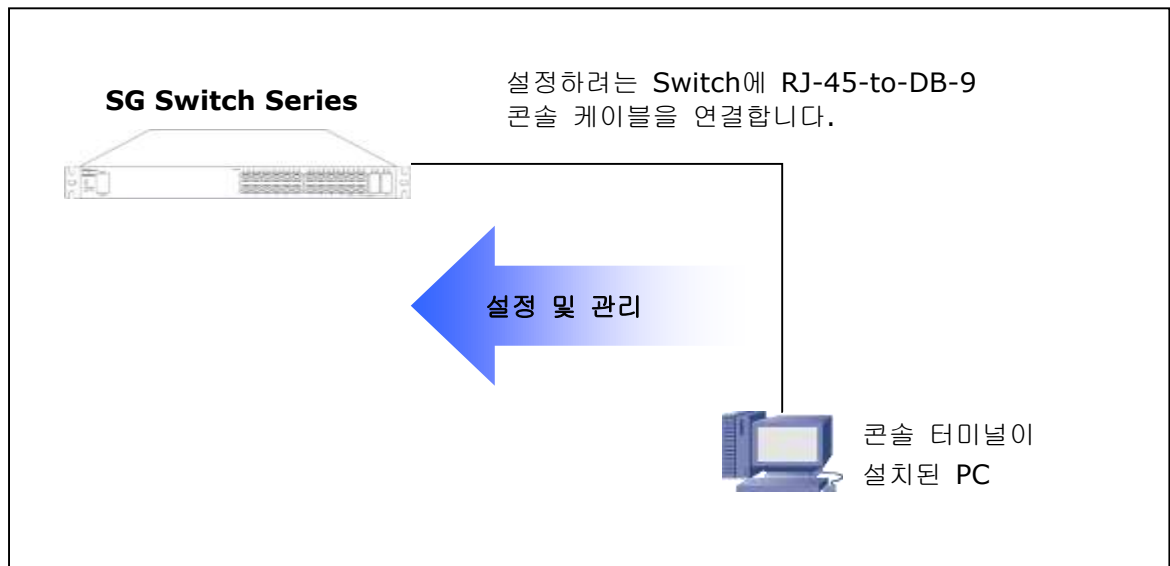
SG2128G, SG2128GX, SG2152G, SG2152GX Series 는 MGMT 포트를 지원하지 않으며, Bootloader에서의 Firmware 복구 방법은 본 설명서 "4.8 OS 업그레이드 Fail시 복구 방법"을 참고하시기 바랍니다.

1.3 CLI 기본 사용법

1.3.1 명령어 체계

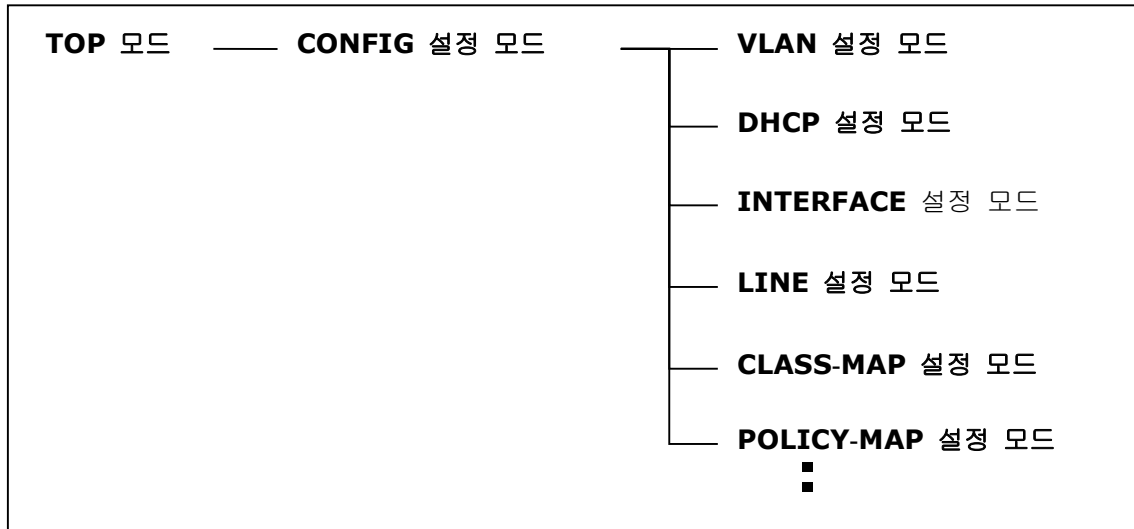
SG Switch Series Switch는 관리자의 PC에 Terminal Program을 설치하여 Console Cable을 연결하여 시스템을 설정 및 관리할 수 있습니다. 이 때 관리자는 Handreamnet에서 개발한 CLI (Command Line Interface) 명령어 체계를 사용하게 됩니다.

본 설명서에서는 SG2124G, SG2124GP의 프롬프트 상태를 기준으로 설명합니다.



CLI 입력방법

■ 명령어 체계 Tree



■ Non-PRIVILEGE 모드

콘솔 터미널을 통해 Switch에 성공적으로 Login하면 Non-PRIVILEGE 모드가 시작됩니다. Non-PRIVILEGE 모드는 접속한 모든 사용자들에게 읽기 전용 모드로 실행되는 대부분의 명령어들을 통해 장비의 설정 내용을 확인할 수 있습니다.

[표 1-1] Non-PRIVILEGE 모드 주요 명령어

명 령 어	기 능
clear	일부 기능들의 값을 초기화합니다.
clock	Switch의 시간 및 날짜를 설정합니다.
enable	TOP (PRIVILEGE) 모드로 전환합니다.
exit	Logout 합니다.
logout	Logout 합니다.
show	장비의 설정 내용을 확인합니다.
terminal	터미널 스크린에 출력되는 행 수를 설정합니다.

■ TOP (PRIVILEGE) 모드

읽기 권한만 가지는 것이 아니라 장비를 설정하는 권한까지 가지려면 TOP 모드로 전환해야 합니다. Non-PRIVILEGE모드에서 “enable” 명령어를 입력하면, 프롬프트가 **SG2124G>**에서 **SG2124G#**로 바뀌면서 TOP 모드로 전환됩니다. TOP 모드에서는 Switch 전체를 모니터링(show, ping, traceroute 등) 할 수 있습니다. TOP 모드를 통해 CONFIG 모드로 전환할 수 있습니다.

[표 1-2] TOP (PRIVILEGE) 모드 주요 명령어

명령어	기능
clear	일부 기능들의 값을 초기화합니다.
clock	Switch의 시간 및 날짜를 설정합니다.
configure terminal	CONFIG 모드로 전환됩니다.
copy	TFTP, FTP, SFTP Server, USB를 통해 startup-config 파일을 백업 및 복구합니다.
disable	Non-PRIVILEGE 모드로 전환합니다.
exec-timeout	현재 접속된 터미널에 대한 자동 Logout 시간을 설정합니다.
exit	Logout 합니다.
logout	Logout 합니다.
ping	Network 연결 상태를 확인합니다.
reload	Switch를 다시 부팅합니다.
show	장비의 설정 내용을 확인합니다.
ssh	SSH로 다른 장비에 접속합니다.
telnet	텔넷으로 다른 장비에 접속합니다.
traceroute	Packet 전송 경로를 추적합니다.
terminal	터미널 스크린에 출력되는 행 수를 설정합니다.
write	설정된 내용을 저장합니다.
wizard	IPT, MGMT, MDS 설정을 간단하게 구성할 수 있습니다.

■ CONFIG 모드

TOP 모드에서 **configure terminal** 명령어를 입력하면, 프롬프트가 **SG2124G#**에서 **SG2124G(config)#**로 바뀌면서 CONFIG 모드로 전환됩니다. CONFIG 모드는 시스템 전체를 통괄하는 전반적인 기능과 **SNMP, Syslog**등을 설정하는데 사용합니다. CONFIG 모드를 통해 **VLAN, DHCP, INTERFACE** 설정 모드 등으로 전환할 수 있습니다.

[표 1-3] CONFIG 모드 주요 명령어

명령어	기능
aaa	AAA 인증 기능을 설정합니다.
arp	ARP Table에 IP Address와 MAC Address를 등록합니다.
banner	배너를 설정합니다.
class-map	QoS CLASS_MAP 모드로 전환합니다.
dot1x	802.1x 사용자 인증을 enable 합니다.
enable password	Non-PRIVILEGE 모드에서 TOP 모드로의 전환 시 입력할 password 를 설정합니다.
end	현재 모드를 종료하고 TOP 모드로 전환합니다.
exit	현재 모드를 종료하고 이전 모드로 전환합니다.
factory-default	Config 내용을 초기화합니다.
hostname	Hostname을 변경합니다.
interface	INTERFACE 모드로 전환합니다.
ip (dhcp)	IP Protocol에 대해 설정합니다. (DHCP 설정 모드로 전환합니다)
ipv6	IPv6 Protocol에 대해 설정합니다.
line	LINE 설정 모드로 전환합니다.
log	Syslog를 설정합니다.
mds	MDS Engine에 대한 설정을 변경합니다.
ntp	NTP Server를 설정합니다.
policy-map	QoS POLICY_MAP 모드로 전환합니다.
acl	QoS Access List를 설정합니다.
snmp-server	SNMP를 설정합니다.
timezone	Timezone을 설정합니다.
update	OS Image를 Update합니다.
username	사용자 계정을 추가하거나 password를 변경합니다.
vlan	VLAN에 관한 설정을 합니다.

■ VLAN 설정 모드

CONFIG 모드에서 **vlan database** 명령어를 입력하면, 프롬프트가 **SG2124G(config)#**에서 **SG2124G(config-vlan)#**로 바뀌면서 VLAN 설정 모드로 전환됩니다. VLAN 설정 모드에서는 VLAN의 생성, 삭제 등을 설정합니다.

[표 1-4] VLAN 설정 모드 주요 명령어

명령어	기능
end	현재 모드를 종료하고 TOP 모드로 전환합니다.
exit	현재 모드를 종료하고 이전 모드로 전환합니다.
no	생성된 VLAN을 삭제합니다.
shared-vlan	shared-vlan 을 생성하기 위해 설정합니다.
vlan	VLAN을 생성합니다.

■ DHCP 설정 모드

CONFIG 모드에서 **ip dhcp pool pool-name** 명령어를 입력하여 DHCP Pool Name을 설정하면, 프롬프트가 **SG2124G(config)#**에서 **SG2124G(config-dhcp)#**로 바뀌면서 DHCP 설정 모드로 전환됩니다. DHCP 설정 모드에서는 DHCP Server에서 사용하는 IP Address 범위, Subnet 및 Group을 지정하고, Subnet의 Default Gateway 등을 설정합니다.

[표 1-5] DHCP 설정 모드 주요 명령어

명령어	기능
default-router	DHCP Pool의 Default Router IP를 설정합니다.
dns-server	DHCP Pool의 DNS Server IP를 설정합니다.
domain-name	DHCP Pool의 Domain Name을 설정합니다.
end	현재 모드를 종료하고 TOP 모드로 전환합니다.
exit	현재 모드를 종료하고 이전 모드로 전환합니다.
host	특정 MAC Address에 대해 고정된 IP를 사용하도록 설정합니다.
lease	DHCP IP를 할당 받아 사용할 수 있는 기본 시간을 설정합니다.
network	DHCP Pool의 Network 대역을 설정합니다.
no	설정된 DHCP 정보를 초기화합니다.
range	DHCP로 할당할 IP Address의 범위를 설정합니다.
shared-network	DHCP Pool을 shared network으로 설정합니다.
tftp-server	DHCP Option 150을 설정합니다.

■ INTERFACE 모드

CONFIG 모드에서 **interface interface-name** 명령어를 입력하면, 프롬프트가 **SG2124G(config)#**에서 **SG2124G(config-if)#**로 바뀌면서 INTERFACE 설정 모드로 전환됩니다. INTERFACE 설정 모드에서는 각 Interface에 대한 DHCP Filtering, NETBIOS Filtering, Negotiation 등을 설정 및 변경합니다.

[표 1-6] INTERFACE 모드 주요 명령어

명령어	기능
arp-ageing-timeout	ARP의 ageing-time을 설정합니다.
channel-group	Lacp의 Member로 설정합니다.
description	Interface 의 description 설정합니다.
dhcp filter	dhcp filter 기능을 설정합니다.
dot1x	dot1x 인증 기능을 설정합니다.
end	현재 모드를 종료하고 TOP 모드로 전환합니다.
exit	현재 모드를 종료하고 이전 모드로 전환합니다.
flowcontrol	전송 중지 신호를 보내는 기능을 설정합니다.
ip	VLAN Interface에 관리 IP를 설정합니다.
max-macs	MAC Address 수를 제한 기능을 설정합니다.
mdix	MDIX 동작 기능을 설정합니다.
mirror	Port Mirroring을 설정합니다.
mtu	MTU 값을 변경합니다.
netbios filter	NetBIOS filter 기능을 설정합니다.
port-channel	Link Aggregation의 Load Balancing 방법을 설정합니다.
rate shaping	Traffic 전송률을 Kbps 단위로 설정합니다.
redund-group	Port Redundancy 기능을 설정합니다.
service-policy	QoS Policy-Map에 생성한 정책을 적용합니다.
shutdown	Interface를 비활성화 시킵니다.
spanning-tree	edgeport, portfast등의 기능을 설정합니다.
static-channel-group	static channel group의 Member로 설정합니다.
storm-control	Storm Control 기능을 설정합니다.
switchport	Mode를 변경하거나 VLAN의 Member로 설정합니다.

■ LINE 설정 모드

CONFIG 모드에서 **line Option** 명령어를 입력하면, 프롬프트가 **SG2124G(config)#** 에서 **SG2124G(config-line)#**로 바뀌면서 LINE 설정 모드로 전환됩니다. LINE 설정 모드에서는 Console 및 Telnet 접속에 대한 설정을 변경합니다.

[표 1-7] LINE 설정 모드 주요 명령어

명령어	기능
exec-timeout	자동 Logout 시간을 설정합니다.
login	Login 시 Password를 물어보도록 설정합니다.
end	현재 모드를 종료하고 TOP 모드로 전환합니다.
exit	현재 모드를 종료하고 이전 모드로 전환합니다.

■ QoS CLASS-MAP mode

CONFIG 모드에서 **class-map name** 명령어를 입력하면, 프롬프트가 **SG2124G(config)#** 에서 **SG2124G(config-cmap)#**로 바뀌면서 QoS CLASS MAP 설정 모드로 전환됩니다. QoS CLASS MAP 설정 모드에서는 QoS 설정을 위해 acl, CoS, IP-DSCP, IP-Precedence등을 선택 및 변경합니다.

[표 1-8] QoS CLASS-MAP 모드 주요 명령어

명령어	기능
end	현재 모드를 종료하고 TOP 모드로 전환합니다.
exit	현재 모드를 종료하고 이전 모드로 전환합니다.
match	Packet의 조건을 선택하여 class-map에 설정합니다.

■ QoS POLICY-MAP 모드

CONFIG 모드에서 **policy-map name** 명령어를 입력하면, 프롬프트가 **SG2124G(config)#**에서 **SG2124G(config-pmap)#**로 바뀌면서 QoS POLICY MAP 설정 모드로 전환됩니다. QoS POLICY MAP 설정 모드에서는 QoS CLASS-MAP에서 지정한 CLASS에 대해 CoS, IP-DSCP, IP-Precedence등을 설정 및 변경합니다.

[표 1-9] QoS POLICY-MAP 모드 주요 명령어

명령어	기능
class	Packet 조건(class-map)을 선택합니다.
end	현재 모드를 종료하고 TOP 모드로 전환합니다.
exit	현재 모드를 종료하고 이전 모드로 전환합니다.

[표 1-10] Main Commands of QoS POLICY-MAP-CLASS

명령어	기능
class	Packet 조건(class-map)을 선택합니다.
end	현재 모드를 종료하고 TOP 모드로 전환합니다.
exit	현재 모드를 종료하고 이전 모드로 전환합니다.
Police	평균 Traffic 및 임계치 초과 Packet의 처리 방안을 설정합니다.
set	CoS, DSCP, ip-precedence를 변경하는 기능입니다.

1.3.2 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.



참고

물음표(?)는 입력해도 화면에는 출력되지 않으며 **Enter** 키를 누르지 않아도 명령어 리스트를 출력해줍니다.

- **more-**가 출력된 상태에서 '?'를 다시 입력하면 사용 가능한 명령어 확인이 가능합니다. **-more-** 상태에서 **space**또는 **z**를 누르면 현재 라인만큼 출력되며, **Enter**를 누르면 1라인만큼 출력됩니다. 출력되는 것을 중단하려면 **q** 또는 **Ctrl+C**를 입력합니다.

<예제> TOP 모드에서 사용 가능한 명령어

```
SG2124G#?
Exec commands:
  arping      Send ARP Request message to a neighbor host
  clear       Reset functions
  clock       set system clock
  configure   Enter configuration mode
  copy        Copy from one file to another
  debug       Debugging functions
  disable     Turn off privileged mode command
  dot1x       IEEE 802.1X Port-Based Access Control (802.1X)
  enable      Turn on privileged mode command
  exec-timeout Set timeout value
  exit        End current mode and down to previous mode
  help        Description of the interactive help system
  logout      Exit from the EXEC
  net-trace    Network Trace Tool commands
  netbios-scan NETBIOS scanning
  no          Negate a command or set its defaults
  ping        Send echo messages
  port-scan    Port scanning
  quit        Exit current mode and down to previous mode
  reload      Halt and perform a warm restart
  remove      Remove file
  show        Show running system information
  ssh         Open a ssh connection
  telnet      Open a telnet connection
  terminal     Set terminal line parameters
  traceroute   Trace route to destination
-- 이하 생략 --

SG2124G#
```

1.3.3 단축 명령어

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

[표 1-11] 단축 명령어 형태

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

1.3.4 실행된 명령어 목록 확인

콘솔 및 텔넷으로 접속하여 실행된 명령어들을 최대 50개까지 명령어 Buffer에 기록되어 있어 관리자가 어떤 명령을 사용하였는지 확인할 수 있습니다.

50개 이상의 명령어가 실행된 경우 명령어들은 **First In First Out**에 따라 먼저 실행되었던 명령어의 순서로 차례로 지워지게 되면서, 나중에 실행된 명령어가 가장 높은 순번으로 명령어 목록에 기록됩니다.

실행된 명령어 목록을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show history	Non-PRIVILEGE TOP	실행된 명령어 목록을 확인합니다.

1.3.5 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 화살표(↑)를 누르면

`exit` → `interface vlan1.1` → `configure terminal` → `show clock` 순서로 출력됩니다.

<예제> 이전 명령어 불러오기

```
SG2124G#show clock
Tue May 05 15:21:44 2009
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface vlan1.1
SG2124G(config-if)#exit
SG2124G(config)#

SG2124G(config)#exit

SG2124G(config)#interface vlan1.1

SG2124G(config)#configure terminal

SG2124G(config)#show clock
SG2124G(config)#
```



참고

이전 명령어에서 불러오는 이전 명령어 내역들은 명령어 **Buffer**에 기록되어 있는 **history** 목록을 사용합니다.

Buffer에는 최대 50개의 history 목록이 기록됩니다.

1.3.6 TOP 모드 명령어 실행

CONFIG 모드에서 TOP 모드의 명령어를 실행할 수 있습니다.

CONFIG 모드에서 TOP 모드의 명령을 실행하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
do TOP_COMMAND	CONFIG	TOP 모드의 명령어를 실행합니다.

<예제> CONFIG 모드에서 Ping 명령 사용하기

```
SG2124G(config)#do ping
Protocol [ip]:
Target IP address: 10.1.1.15
Repeat count [5]:
Datagram size [100]:
Extended commands [n]:
PING 10.1.1.15 (10.1.1.15) from 10.1.1.55 : 100(128) bytes of data.
108 bytes from 10.1.1.15: icmp_seq=1 ttl=128 time=0.783 ms
108 bytes from 10.1.1.15: icmp_seq=2 ttl=128 time=0.801 ms
108 bytes from 10.1.1.15: icmp_seq=3 ttl=128 time=0.751 ms
108 bytes from 10.1.1.15: icmp_seq=4 ttl=128 time=0.763 ms
108 bytes from 10.1.1.15: icmp_seq=5 ttl=128 time=0.755 ms

--- 10.1.1.15 ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4040ms
rtt min/avg/max/mdev = 0.751/0.770/0.801/0.035 ms
SG2124G(config)#
```

1.3.7 Show 명령어

show 명령어를 통해 설정된 내용을 확인할 수 있습니다.

또한, show 명령어는 마지막에 옵션을 추가하여 특정 정보만 선별하여 확인할 수 있습니다.

특정 정보만 선별하여 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show COMMAND <i>COMMAND</i> [begin WORD]	ALL	지정된 문자열로 시작되는 설정 내용을 확인합니다.
show COMMAND [<i>COMMAND</i>] [exclude WORD]	ALL	지정된 문자열이 포함되지 않은 설정 내용을 확인합니다.
show COMMAND [<i>COMMAND</i>] [include WORD]	ALL	지정된 문자열을 포함하는 설정 내용을 확인합니다.
show COMMAND [<i>COMMAND</i>] [tail <1-100>]	ALL	마지막 N줄의 설정 내용을 확인합니다. (Default 라인 수 : 10줄)

<예제> CONFIG Mode에서의 show 명령어의 옵션

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#show ?
cli          Show CLI tree of current mode
debugging    Debugging functions
list         Show command lists
running-config Current Operating configuration

SG2124G(config)#
```

[표 1-12] 자주 사용하는 **show** 명령어

명령어	기능
SG2124G#show running-config	현재 설정된 관리중인 Config를 출력 (SG2124G#sh run)으로 단축가능
SG2124G#show startup-config	Flash에 저장되어 있는 Config를 출력
SG2124G#show version	Firmware version을 표시
SG2124G#show system alarm	System의 FAN Temperature PSU의 Alarm 상태를 출력
SG2124G#show system cpu-load	System의 CPU 사용률을 보여주며, 5 s, 30 s, 1 min, 5 min, 15 min, 60 min, all-time으로 평균값을 출력
SG2124G#show system fan	FAN의 동작상태를 출력
SG2124G#show system memory	System의 Memory 사용현황을 출력
SG2124G#show system sfp [Port_No]	Combo Port에 SFP Module이 장착되었을 경우, SFP Module의 정보를 출력하며 sfp 21은 21번 Port(ge21)의 정보를 출력
SG2124G#show system system-info	Vendor명, 모델명, Serial No 등의 기본 정보를 출력
SG2124G#show system temperature	장비의 내부온도 및 FAN Start Stop, Alarm 발생되는 Low High 온도의 범위를 출력
SG2124G#show system uptime	system uptime 출력
SG2124G#show ip arp	ARP Table Cache된 내용을 출력
SG2124G#show ip igmp [group interface snooping]	IGMP설정 시 group별, interface별, snooping, source specific multicast mapping등의 내용을 출력
SG2124G#show ip interface [IFNAME brief]	interface의 상태를 확인 할 수 있으며 IFNAME(ge1등)을 입력 시 해당 Interface의 상태만 확인할 수 있으며 brief를 입력 시 전체 Interface의 상태를 확인가능
SG2124G#show ip route	현재 설정되어 있는 routing table을 출력
SG2124G#show acl	설정되어 있는 acl를 출력. access-list가 아닌 acl를 사용
SG2124G#show aaa	AAA 설정과 관련된 설정 값을 출력
SG2124G#show bandwidth [IFNAME]	전체 Port의 Traffic 사용량을 확인할 수 있으며, IFNAME을 설정 시 해당 Port의 Traffic 만을 확인
SG2124G#show bridge	Bridge에 연결된 host를 확인, L2 Switch로

	동작하므로 bridge 1 만 사용, show MAC-table과 동일내용이 출력
SG2124G#show cable-diag [IFNAME]	Fast Ethernet Port에 해당되며 Port에 연결된 Cable의 상태 및 거리를 확인할 수 있으며, Cable 이 Open된 상태에서만 결과치가 출력되고, 기본 Default는 Cable이 연결되어 있지 않더라도 1 Meter로 표시되며, Interface에 Link up 되어 있는 경우에는 - Meter로 출력
SG2124G#show class-map NAME	설정된 class-map을 확인
SG2124G#show clock	장비의 현재 time을 확인
SG2124G#show dot1x [all brief interface statistics web-auth]	dot1x(802.1X) 인증 관련된 내용을 확인
SG2124G#show etherchannel [<1-65535> detail load-balance summary]	LACP 관련된 설정내용을 확인
SG2124G#show lacp sys-id	LACP 설정된 system id를 확인
SG2124G#show lacp-counter	Port별 LACP BPDU 전송상태 확인
SG2124G#show interface [IFNAME media stat switchport]	interface의 status를 확인할 수 있으며, IFNAME을 설정 시 설정한 IFNAME의 상태만 확인할 수 있으며, media를 설정 시 Interface 별 연결된 Port의 media type을 확인 stat를 지정 시 Port의 Input Output Packet 및 Error Packet, Packet의 Size등을 확인할 수 있으며, switchport bridge 1을 지정 시 각 Port의 동작 Mode와 Accept Frame Type, 설정된 VLAN등의 정보를 출력
SG2124G#show gvrp [configuration machine statistics timer]	GVRP의 config와 관련된 세부사항을 확인
SG2124G#show mds config	mds 설정 내역을 확인
SG2124G#show mds arp-table [all dynamic static]	mds의 arp-table의 내용을 보여주며, 이 기능은 ARP-Spoofing기능이 설정되어 있어야 사용 가능
SG2124G#show mds detect-list log KeyNo	mds에 현재 차단된 list를 보여주며, log와 keyNo를 입력 시 해당 차단내역의 세부 Log를 확인
SG2124G#show mds detect-history [desc log KeyNO]	mds에 차단되었던 과거의 History를 확인할 수 있으며, desc를 선택 입력 시 최근 list부터 출력하며, log KeyNo를 입력하면 해당되는 List의 세부Log를 출력

SG2124G#show mds log-server	관제시스템인 VNM Server의 IP와 사용 Port No, 접속상태를 확인
SG2124G#show mds permit	Config에서 mds permit으로 설정한 예외정책의 내역을 출력
SG2124G#show mds extended permit	Config에서 mds extended permit으로 설정한 예외정책의 내역을 출력
SG2124G#show log syslog remote	remote syslog server의 설정내용을 확인
SG2124G#show max-macs [IFNAME]	Port에 설정된 최대허용 MAC Address의 개수를 출력
SG2124G#show mac-table	mac table에 등록되어 있는 내용을 출력
SG2124G#show history	Login 후 사용한 Command의 History를 출력
SG2124G#show mirror [interface IFNAME]	Port Mirroring 기능의 설정 시 적용된 Config를 확인
SG2124G#show mls qos [aggregator-policer interface maps]	QoS기능의 설정내용을 확인
SG2124G#show process	사용중인 Process의 List를 출력
SG2124G#show services dhcp	dhcp server relay 기능의 동작상태를 확인
SG2124G#show snmp-server	snmp-server의 동작상태를 확인
SG2124G#show spanning-tree [interface IFNAME mst config detail interface pvstp]	spanning-tree의 동작상태를 확인할 수 있으며, interface IFNAME을 지정 시 지정된 Interface의 Spanning-tree의 동작상태를 출력하고, mst의 설정은 MSTP protocol의 설정 및 상태확인을 하는 경우 사용
SG2124G#show static-channel-group	static-channel-group의 config 내역 출력
SG2124G#show storm-control IFNAME	storm-control기능이 설정되어 있는 경우 broadcast, multicast, DLF의 설정치를 확인하는 명령이며, IFNAME 설정 시 특정 port의 설정치만 출력
SG2124G#show ntp [associations [detail] status]	NTP Server를 설정 시 설정한 내용 및 동작상태를 출력
SG2124G#show syslog [auth backup desc dhcp igmp imi imish interface lacp lldp mds mstp nopager nsm pimpktgen pvstp rstp sflow stp tail unspec]	장비의 Event Log를 출력하며 option 설정 시 해당내용만 출력

<pre>SG2124G#show vlan [<2-4094> all brief classifier [group GROUP_ID rule Rule_ID] dynamic static vlan-stacking]</pre>	<2-4094> : VLAN ID 설정 시 해당되는 VLAN이 설정되어 있는 Interface를 출력 all bridge 1 : bridge 1에 설정된 VLAN을 출력 classifier : config의 VLAN classifier에 설정한 내용을 출력 dynamic : Dynamic으로 설정된 VLAN의 내용을 출력 static : Static으로 설정된 VLAN의 내용을 출력 vlan-stacking : VLAN Stacking으로 설정된 VLAN의 내용을 출력
--	--

1.3.8 이전 모드로 전환하기

현재 사용중인 모드에서 이전 모드로 전환하거나 TOP 모드로 전환할 수 있습니다.

명령어	모드	기능
exit	CONFIG 이후의 모든 모드	이전 모드로 전환합니다.
Ctrl + D		
end	ALL	TOP 모드로 전환합니다.
Ctrl + C		

<예제> 이전 모드로 전환하기

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge1
SG2124G(config-if)#exit
SG2124G(config)#
SG2124G(config)#
SG2124G(config)#interface ge1
SG2124G(config-if)#end
SG2124G#
```

1.3.9 명령어 표기법

- 프롬프트는 SG Switch Series 구분 없이 SG2124G로 표기합니다.
- 관리자가 입력해야 하는 변수는 이탤릭 체로 표기합니다.
li>
- 변수들 가운데 선택 사항인 것은 [대괄호]안에 표기합니다.
- 입력할 수 있는 숫자 범위는 <꺅쇠 괄호>안에 표기합니다.
- 여러 가지 변수들 가운데 반드시 선택해서 입력해야 하는 것은 {괄호}안에 표기합니다.
- 선택 가능한 변수들은 수직선(|)으로 나누어 표기합니다.

1.4 접속 및 관리 IP 설정

1.4.1 Login

Switch의 설치가 끝나면 각 Interface가 Network와 관리용 PC에 올바르게 연결되어 있는지 최종 점검하십시오. 모든 점검이 끝나면, 전원 Switch를 켜고 부팅시킵니다.

Login Prompt에 Login ID를 입력하면 Password Prompt가 출력되고, Password를 입력하면 TOP 모드로 이동합니다. Login ID와 Password의 초기값은 root / root 입니다.

Login 후 TOP 모드로 전환하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
enable	Non-PRIVILEGE	TOP 모드로 전환합니다.

<예제> Login

```
SG2124G login: root
Password: *****

SG0S version 2.2.6 SGL2-OS 05/23/14 03:51:32
SG2124G>enable
SG2124G#
```

1.4.2 Password 변경

Switch를 설정 및 관리하는 권한을 가진 관리자는 Password를 변경할 수 있습니다. 보다 안전한 보안을 위해서는 Password를 수시로 변경해 주는 것이 바람직합니다. 관리자 Password 및 Enable Password 변경은 CONFIG 모드에서 설정합니다.

초기 입력 시 기본 Password를 변경하도록 되어 있으며, 9자 이상으로 영대문자, 영소문자, 숫자, 특수문자를 최소 1자 이상씩 혼합하여 설정하여야 합니다.

사용자 password 및 enable password를 변경하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
username NAME password PASSWD	CONFIG	사용자 계정의 Password를 변경합니다.
enable password PASSWD	CONFIG	Privileged Mode 진입 Password를 설정합니다.
write	TOP	설정 내용을 저장합니다.

enable password를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no enable password	CONFIG	Enable Password를 삭제합니다.

<예제> Password 변경

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#username root password *****
% INFO: you need to save your configuration changes to NVRAM so that the changes are
applied
SG2124G(config)#enable password *****
SG2124G(config)#username hdnet password *****
SG2124G(config)#username test1 privilege 5 password *****
SG2124G(config)#end
SG2124G#write
Building configuration...
[OK]
SG2124G#show running-config |include username
username root password *****
username hdnet password *****
username test1 privilege 5 password *****
SG2124G#
```

- **Firmware Version 2.2.6 이상에서는 Password 보안이 더욱 강화되었습니다**
 Password 보안강화를 위하여 공장초기화 상태인 **Factory Default** 상태에서 부팅 후 Login 시 **Default** 관리자계정에 대한 Password를 변경하도록 유도하는 기능이 추가되었습니다.

Password 입력이나 변경 시 반드시 9자 이상으로 영대문자, 영소문자, 숫자, 특수문자를 최소 1자 이상씩 혼합하여 설정하여야 합니다.

<예제> 최초 Login 시 Default 관리자계정 Password 변경 유도

```
SG2124G login: root
Password:

SGOS version 2.2.6 SGL2-OS 05/23/14 03:51:32

Press any key to continue.

- Setting Administrator(root) password -

% Enter new root password :
% Retype new root password :
SG2124G>enable
SG2124G#
```



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



1. 설정된 password는 자동으로 암호화되어 저장되며, *****과 같은 형태로 나타납니다.
2. Password는 영문, 숫자, 특수문자를 포함하여 최대 31자 까지 설정할 수 있습니다.

1.4.3 자동 Logout 기능

관리자가 콘솔 터미널 스크린을 켜 둔 채 자리를 비우게 되는 경우 계속 Login 상태로 방치된다면, 다른 사람이 설정을 변경할 수도 있거나 Telnet 등으로 접속을 시도하는 경우에는 Login 개수 제한으로 인해 접속을 못하는 현상이 발생할 수 있습니다.

관리자가 정해 놓은 시간 동안 키보드 입력이 없으면 자동으로 Logout 되는 기능을 가지고 있으며, 그 시간은 관리자가 설정할 수 있습니다.

자동 Logout 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
exec-timeout 0	TOP	자동 Logout 기능을 해제합니다.
exec-timeout <0-35791> [<0-2147483>]	TOP	관리자가 설정한 시간 동안 콘솔 터미널에 키보드 입력이 없으면 시스템을 자동 Logout 합니다. 시간의 단위는 x분 [x초]입니다.

<예제1> 자동 Logout

```
SG2124G login: root
Password: *****

SGOS version 2.2.6 SGL2-OS 05/23/14 03:51:32
SG2124G>en
SG2124G#
Vty connection is timed out.

SG2124G login:root
Password: *****

SGOS version 2.2.6 SGL2-OS 05/23/14 03:51:32
SG2124G>en
SG2124G#exec-timeout 30
SG2124G#
```



참고

1. 자동 Logout 기능의 Logout 시간의 Default 설정 값은 10 min 입니다.
2. 현재 Login한 터미널에만 적용되며 저장되지 않습니다.

자동 Logout 시간 변경 후 저장하려면 콘솔 및 Telnet 설정 모드로 변경 후 자동 Logout 기능의 시간 설정을 x분 [x초] 단위로 설정한 후 저장하면 다음 Login 시에 변경된 내용으로 적용됩니다.

Console 및 Telnet 접속 시 자동 Logout 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
line con 0	CONFIG	콘솔 LINE 설정 모드로 전환합니다.
line vty First_NUM Last_NUM	CONFIG	Telnet LINE 설정 모드로 전환합니다.
exec-timeout 0	LINE	자동 Logout 기능을 해제합니다.
exec-timeout <0-35791> [<0-2147483>]	LINE	관리자가 설정한 시간 동안 키보드 입력이 없으면 시스템을 자동 Logout 합니다. 시간의 단위는 x분[x초]입니다.

Console 및 Telnet 접속 시 자동 Logout 기능의 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show running-config	TOP CONFIG	설정된 모든 내용을 확인합니다.

Console 및 Telnet 접속 시 자동 Logout 기능을 Default 설정으로 변경하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no exec-timeout	LINE	자동 Logout 시간을 Default 설정 값으로 변경합니다.

<예제2> Console 및 Telnet 접속 시 자동 Logout 기능을 Console은 15 min, Telnet은 5 min 30 s로 설정한 후 저장 후 설정 내용 확인.

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#line con 0
SG2124G(config-line)#exec-timeout 15
SG2124G(config-line)#exit
SG2124G(config)#line vty 0 5
SG2124G(config-line)#exec-timeout 5 30
SG2124G(config-line)#end
SG2124G#write
Building configuration...
[OK]
SG2124G#sh running-config | begin line

...skipping
line con 0
  exec-timeout 15 0
  login local
line vty 0 5
  exec-timeout 5 30
  login local
!
end

SG2124G#
```

<예제3> 자동 Logout 시간을 Default 값으로 설정한 후 저장.

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#line vty 0 5
SG2124G(config-line)#no exec-timeout
SG2124G(config-line)#end
SG2124G#write
Building configuration...
[OK]
SG2124G#
```

1.4.4 사용자 추가

Switch의 효율적인 관리를 위하여 다음과 같이 사용자를 추가하거나, 변경 및 권한등급을 설정하여 보안을 강화할 수 있습니다.

새로운 사용자 계정을 추가, 변경 및 권한을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
username <i>NAME</i> password <i>PASSWD</i>	CONFIG	사용자 계정을 생성하거나 Password를 변경합니다.
username <i>NAME</i> privilege <1-15> password <i>PASSWD</i>	CONFIG	사용자 계정을 생성하거나 Password를 변경 시 권한을 설정합니다.

추가된 사용자 계정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show running-config	TOP CONFIG	설정된 모든 내용을 확인합니다.

사용자 계정을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no username <i>NAME</i>	CONFIG	사용자 계정을 삭제합니다.



주의

1. 사용자 계정 추가 시 **password**를 입력하지 않는 경우 계정이 추가되지 않습니다.
2. **Password** 설정 시 공백이 포함된 경우 공백을 포함하여 **password**가 설정되므로 주의하시기 바랍니다.



참고

1. 사용자 계정 삭제 시 마지막으로 남은 계정은 삭제할 수 없습니다.
2. 사용자 계정의 **Password**를 잃어 버린 경우에는 부록의 “4.7 Bootloader에서의 **Password** 및 **config recovery**” 내용을 참고하셔서 사용자 계정의 **Password**를 변경하시기 바랍니다.
3. 설정된 **password**는 자동으로 암호화되어 저장됩니다.
4. **Password**는 영문, 숫자, 기호를 포함하여 최소 1자에서 31자 까지 설정할 수 있습니다. 영어는 대소문자를 구분합니다.
(**Password**는 영문.숫자 나 특수문자[!, @, #, \$, %, ^, &*, (,)]를 혼합하여 사용하여야 합니다.)
5. **privilege level**이 부여되지 않은 사용자는 **root**와 동일한 권한으로 동작합니다. (Privilege Level 15)
6. 사용자 계정은 최대 100개까지 설정할 수 있습니다. (**root** 포함)
7. **Password** 설정시 첫 글자는 8로 시작하면 안됩니다. (첫번째 8은 암호화를 뜻합니다.)

Privilege 기능에서 사용할 수 있는 MODE는 다음과 같습니다:

Mode	L2, L3 Static 장비	L3 Dynamic 장비
Non Privilege (EXEC)	O	O
TOP (EXEC)	O	O
Configure	O	O
DHCP Pool	O	O
Interface	O	O
VLAN	O	O
MSTI	O	O
Class map	O	O
Policy map	O	O
Policy Class map	O	O
Keychain		O
Keychain key		O
BGP		O
BGP IPv4		O
BGP IPV4M		O
BGP IPV6		O
BGP VPNV4		O
RIP		O
OSPF		O
VRRP		O
RMAP		O

<예제1> 사용자 계정 추가 및 설정 내용 확인.

- 사용자 계정 : HDN, TEST1, PASSWORD : SG2124G!

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#username HDN password *****
SG2124G(config)#username TEST1 privilege 5 password *****
SG2124G(config)#end
SG2124G#write
Building configuration...
[OK]
SG2124G#show running-config |include username
username root password *****
username HDN password *****
username test1 privilege 1 password *****
SG2124G#
```

<예제2> 사용자 계정 삭제

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#no username HDN
SG2124G(config)#end
SG2124G#write
Building configuration...
[OK]
SG2124G#show running-config |include username
username root password *****
username test1 privilege 1 password *****
SG2124G#
```

1.4.5 관리 IP 주소 설정

관리자는 시리얼 콘솔을 이용하여 Login 후 관리용 IP Address (IPv4, IPv6)를 설정해야 합니다. 관리용 IP Address는 Default VLAN(VLAN1.1)에 설정합니다.

Network를 이용한 정보전달(Remote Syslog, SNMP Trap, VNM 연동 등), 정보갱신(SNMP, VNM 연동 등), Telnet, OS Image Update 등을 사용하려면 관리용 IP 및 Default Gateway를 반드시 설정하셔야 합니다.

공장 출하 시 장비에 IP Address가 설정되어 있지 않습니다. 관리자는 Network 구성에 따라 원하는 IP Address로 설정하여 사용할 수 있습니다.

IP 주소를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
interface <i>IFNAME</i>	CONFIG	INTERFACE 모드로 변경합니다.
ip address <i>IP_Addr/Mask</i> [<i>label LINE</i>]	INTERFACE	IP Address를 설정 및 변경합니다.
ip address <i>IP_Addr/Mask</i> secondary [<i>label LINE</i>]	INTERFACE	Secondary IP Address를 추가로 설정합니다.
ip route <i>Network/Mask</i> <i>Gateway_Addr</i>	CONFIG	Default Gateway등을 설정합니다.

설정된 IP주소 및 Gateway 등을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show ip interface [<i>IFNAME</i>] brief	TOP	Interface에 설정된 IP를 확인합니다.
Show ip route	TOP	등록된 Routing Table을 확인합니다.

설정된 IP 주소를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no ip address [<i>IP_Addr/Mask</i>]	INTERFACE	IP Address를 삭제합니다.
no ip address <i>IP_Addr/Mask</i>	INTERFACE	Secondary IP Address를 삭제합니다.

secondary		
no ip route <i>Network/Mask</i> [<i>Gateway_Addr</i>]	CONFIG	Default Gateway등을 삭제합니다.

IPv6 주소를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
interface <i>IFNAME</i>	CONFIG	INTERFACE 모드로 변경합니다.
ipv6 address <i>X:X::X:X/M</i>	INTERFACE	IPv6 Address를 설정 및 변경합니다.
Ipv6 address <i>X:X::X:X/M</i> [<i>anycast eui-64 link-local</i>]	INTERFACE	IPv6 Address의 설정에 따른 부가 옵션을 지정합니다.
ipv6 address autoconfig	INTERFACE	Stateless Address Auto Configuration을 통하여 IP를 자동 설정합니다.

설정된 IPv6 주소 및 Gateway 등을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show ipv6 interface [<i>IFNAME</i>] brief	TOP	Interface에 설정된 IPv6 주소를 확인합니다.
Show ipv6 route	TOP	등록된 Routing Table을 확인합니다.

설정된 IPv6 주소를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no ipv6 address <i>X:X::X:X/M</i>	INTERFACE	IPv6 Address를 삭제합니다.
no ipv6 address <i>X:X::X:X/M</i> [<i>eui-64 link-local</i>]	INTERFACE	Secondary IPv6 Address를 삭제합니다.
no ipv6 address autoconfig	INTERFACE	Stateless Address Auto Configuration 설정을 삭제합니다.
no ipv6 route <i>Network/Mask</i> [<i>Interface <1-255> </i> <i>Gateway_Addr</i>]	CONFIG	IPv6 Gateway등을 삭제합니다.

<예제1> IPv4, IPv6 설정

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface vlan1.1
SG2124G(config-if)#ip address 192.168.0.1/24
SG2124G(config-if)#ipv6 address 2000::2/64
SG2124G(config-if)#exit
SG2124G(config)#ip route 0.0.0.0/0 192.168.0.254
SG2124G(config)#ipv6 route ::/0 2000::1
SG2124G(config)#

```

<예제2> IPv4, IPv6 Routing Table 확인

```

SG2124G#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       0 - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
Gateway of last resort is 192.168.100.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.254, vlan1.1
C     127.0.0.0/8 is directly connected, lo
C     192.168.0.0/24 is directly connected, vlan1.1

SG2124G#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, L - local, C - connected, S - static
       R - RIP, O - OSPF, I - IS-IS, B - BGP
Timers: Uptime

C     ::1/128 via ::, lo, 00:00:36
C     2000::/64 via ::, vlan1.1, 00:00:29
L     fe80::/64 via ::, vlan1.1, 00:00:29
SG2124G#

```



참고

1. INTERFACE 모드에서 IP Address를 변경하면, 변경된 IP Address로 즉시 적용됩니다.
2. Default Gateway 를 변경할 경우 기존의 Default Gateway 는 자동으로 삭제되지 않으므로, “no” 명령어를 입력하여 삭제하시기 바랍니다.



주의

Secondary IP 입력 시 Primary IP가 변경되지 않도록 주의하시기 바랍니다.

1.4.6 Telnet 및 SSH

관리자는 Switch로의 접속 시 Console, Telnet 또는 보안이 강화된 SSH를 이용하여 접속할 수 있으며 Telnet, SSH를 통해 다른 장비로 접속하여 Config를 확인하거나 수정할 수 있습니다.

특히 SSH를 사용하면 모든 Data가 암호화되고 Traffic은 압축되어 더 빠른 전송 효율을 얻을 수 있습니다.

SG Switch Series는 IPv4, IPv6 SSH 서버/클라이언트를 모두 지원합니다.

Telnet 및 SSH를 사용하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
telnet IP_Addr [Port]	TOP	Telnet을 이용하여 다른 장비로 원격 접속합니다.
ssh IP_Addr [Port]	TOP	SSH를 이용하여 다른 장비로 원격 접속합니다.
service telnetd	CONFIG	TELNET Server를 활성화합니다.
service sshd [regen dsa regen rsa]	CONFIG	SSH Server를 활성화합니다. (SSH 인증 키 설정)

Telnet 및 SSH를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show users	TOP	원격 접속된 사용자를 확인합니다.
show service sshd {[fingerprint private public] [dsa rsa]}	TOP	SSH Server의 인증 키를 확인합니다.

Telnet 및 SSH 서비스를 종료하거나 연결된 세션을 종료하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
clear line <i>LINEINDEX</i>	CONFIG	접속된 사용자의 연결을 강제로 종료합니다.
no service telnetd	CONFIG	TELNET Server를 비활성화합니다.
no service sshd	CONFIG	SSH Server를 비활성화합니다. (Default)



참고

1. Default 설정
Telnet Server : Enable
SSH Server : Disable
Telnet / SSH Client : Enable
2. SSHD 및 TELNETD Service가 활성화된 상태에서 접속된 사용자가 존재하면, 해당 Service를 강제 종료할 수 없습니다.
3. v2.2.8 이상에서부터는 보안적합성 요구기능을 충족하기 위하여 SSH 접속시 사용되는 key exchange algorithm의 MAC(Message Authentication Code) algorithm을 hmac-sha2-256, hmac-sha2-512 두가지로 제한하였습니다. 따라서 해당 MAC algorithm을 사용하지 않는 터미널접속 프로그램은 SSH접속이 불가능합니다.

<예제> 원격 사용자 확인 및 SSH Server 활성화

```
SG2124G#show users
  Line      User      Uptime      Host(s)
   0 con 0   root      00:07:37    local
 130 vty 0   root      00:00:13    10.1.1.15
SG2124G#show syslog desc
May  3 21:51:34 SG2124G login[348]: root login on `pts/0' from `10.1.1.15'
May  3 21:51:31 SG2124G in.telnetd[347]: connect from 10.1.1.15 (10.1.1.15)
May  3 21:50:39 SG2124G inetd[259]: pid 319: exit status 1
SG2124G#show running-config | include ssh
no service sshd
SG2124G#
SG2124G#show service sshd fingerprint dsa
Fingerprint: md5 71:38:aa:f1:cb:44:08:12:c9:fb:e4:e6:19:68:e2:fd
SG2124G#show service sshd fingerprint rsa
Fingerprint: md5 43:64:38:be:98:ff:bf:a2:be:e7:56:fa:a6:f6:1b:94
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SG2124G(config)#service sshd
SG2124G(config)#end
SG2124G#show users
  Line      User      Uptime      Host(s)
```

```

    0 con 0      root      00:01:13      local
   130 vty 0      root      00:00:26      10.1.1.15
   131 vty 1      root      00:00:04      10.1.1.15
SG2124G#
SG2124G#clear line 130
SG2124G#show users
      Line      User      Uptime      Host(s)
    0 con 0      root      00:01:13      local
   131 vty 1      root      00:00:04      10.1.1.15
SG2124G#conf t
SG2124G(config)#no service telnetd
% Telnet session is already in use.
SG2124G#
SG2124G#show syslog desc
May  3 21:45:19 SG2124G login[320]: root login on `pts/1' from `10.1.1.15'
May  3 21:45:16 SG2124G in.telnetd[319]: connect from 10.1.1.15 (10.1.1.15)
May  3 21:44:58 SG2124G sshd[314]: login OK from 10.1.1.15:4955
May  3 21:44:52 SG2124G sshd[314]: Child connection from 10.1.1.15:4955
SG2124G#
SG2124G#show running-config | include ssh
service sshd

```



show service sshd 내용 설명

- fingerprint : Host Key의 변동 여부를 확인하기 위한 값.
- private key : 공개키 암호 방식에서의 비밀키.
- public key : 공개키 암호 방식에서의 공개키.

1.4.7 동시 접속자 수 제한기능

보안 관리를 위해 관리자의 Telnet, SSH 접속과 같은 원격 접속세션 수를 제한하는 기능입니다.

동시 접속자 수 제한기능을 사용하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
line vty First_NUM Last_NUM	CONFIG	Telnet LINE 설정 모드로 전환합니다.
shutdown	LINE	VTY 세션을 비활성화 합니다.

동시 접속자 수 제한기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no shutdown	LINE	VTY 세션을 활성화 합니다.

<예제> 6개의 VTY(원격접속) 세션중 1개의 세션만 허용하고 나머지 5개 세션은 차단

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#line vty 1 5
SG2124G(config-line)#shutdown
SG2124G(config-line)#end
SG2124G#show run
- 생략 -
line con 0
 login local
line vty 0
 login local
line vty 1 5
 shutdown
 login local
!
end
SG2124G#
```

1.4.8 Login 실패 시 접속차단기능

장비의 자체 보안강화를 위하여 접속 후 3회의 Password 오류 발생시 설정한 시간 동안 장비로의 접근을 차단하는 기능입니다.

Login-fail auto-deny 기능은 기본활성화 되어 있으며, Console, Telnet, SSH 접속에 모두 해당됩니다.

Login-fail 시 접속차단 기능을 사용하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
login-fail auto-deny [1-1440]	CONFIG	Switch로의 접근이 3회 실패 시 해당 시간 동안 접속을 차단하도록 합니다. (Default: 5 min)

Login-fail 시 접속차단 기능을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show login-fail auto-deny	TOP	인증실패 한 IP와 남은 차단시간을 확인할 수 있습니다.

Login-fail 시 접속차단 기능을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no login-fail auto-deny	CONFIG	인증실패 시 접속 차단 기능을 삭제합니다.

<예제> Login-fail auto-deny 기능 활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#login-fail auto-deny 10
SG2124G(config)#end
SG2124G#show login-fail auto-deny
login-fail auto-deny is enabled
block time is 10 minutes

Blocked Host      Remaining Time(sec)
-----
192.168.254.95    291
```


1.4.9 관리자 등급기반의 CLI 접근 통제

CLI 기반의 접근통제 기능은 장비에 등록된 User 별로 Privilege 값을 가져 Privilege에 따라서 보안 스위치 장비의 CLI 기능을 제한합니다.

Privilege 값은 설정에 따라 1~15의 값을 가지며, 1이 가장 작은 값이고, 15가 가장 큰 값입니다. 슈퍼관리자 계정은 고정적으로 15의 값을 가지고 있으며 username 명령어를 통하여 Privilege 값을 명시할 수 있으며, 명시하지 않는 경우 가장 높은 15의 값을 갖습니다.

CLI 기반 접근통제 기능을 사용하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
privilege <i>MODE</i> level <1-15> [CLI]	CONFIG	각 mode별로 level을 부여하고 사용할 수 있는 CLI를 설정합니다.
show privilege users	TOP	현재 장비에 등록된 User들의 Privilege 값을 보여줍니다.

CLI 기반 접근통제 기능을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no privilege <i>MODE</i> level <1-15> [CLI]	CONFIG	등록된 level 별 CLI를 삭제합니다.
no username <i>WORD</i>	CONFIG	등록한 사용자를 삭제합니다.

Privilege에서 사용할 수 있는 MODE는 다음과 같습니다.

Privilege MODE	기능
exec	Non Privilege Mode 이거나, Non Privilege에서 enable 명령어를 통해 TOP Mode로 전환한 Mode입니다.
aaa	Radius 인증을 통한 AAA user Default Privilege Level Mode 입니다.
config	Configuration 이 가능한 Mode 입니다.
dhcp	DHCP Configuration 설정 Mode 입니다.
interface	Interface Configuration 설정 Mode 입니다.

line	Console이나 SSH Session에 관한 설정이 가능한 Mode 입니다.
qos-class	QoS Class map을 설정할 수 있는 Mode 입니다.
qos-policy	QoS 설정의 policy map을 설정할 수 있는 Mode 입니다.
qos-policy-class	QoS의 Policy map과 Class 관련 설정이 가능한 Mode 입니다.
vlan	VLAN을 설정할 수 있는 Mode 입니다



참고

설정 시 하위 Level의 Privilege의 CLI는 상위 Level에서는 설정하지 않아도 사용할 수 있으므로, CLI의 Level 설정 시 주의하여야 합니다.

<예제> Privilege 기능 설정

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#privilege ?
aaa                AAA users default privilege level
config             Configuration Mode
dhcp               DHCP Configuration Mode
exec               EXEC Mode
interface           Interface Configuration Mode
line               Line Configuration Mode
mstp               MSTP Configuration Mode
qos-class           QoS Class map Configuration Mode
qos-policy          QoS Policy map Configuration Mode
qos-policy-class    QoS Policy map Class Configuration Mode
vlan               VLAN Configuration Mode

SG2124G(config)#privilege exec level 1 show
SG2124G(config)#privilege exec level 1 enable
SG2124G(config)#privilege exec level 2 config
SG2124G(config)#privilege exec level 2 show
SG2124G(config)#privilege config level 3 show
SG2124G(config)#privilege config level 3 interface
SG2124G(config)#privilege config level 3 ip
SG2124G(config)#privilege config level 4 dhcp
SG2124G(config)#privilege config level 4 line
SG2124G(config)#privilege config level 4 threshold
SG2124G(config)#privilege config level 4 poe
SG2124G(config)#privilege config level 4 hostname
SG2124G(config)#end
SG2124G#
SG2124G#show privilege
mode                type level command
=====

```

```

exec          command      2  show
exec          command      1  enable
exec          command      2  config
config        command      3  show
config        command      3  interface
config        command      3  ip
config        command      4  dhcp
config        command      4  line
config        command      4  threshold
config        command      4  poe
config        command      4  hostname

```

SG2124G#

SG2124G#show privilege users

AAA default privilege : 15

username	level
test1	1
test2	2
test3	3
test4	4

<Username "test1"로 Login시 사용할 수 있는 CLI>

login as: **test1**

test1@192.168.11.100's password:

SG2124G>**enable**

SG2124G#?

Exec commands:

```

enable  Turn on privileged mode command
exit    End current mode and down to previous mode
help    Description of the interactive help system
quit    Exit current mode and down to previous mode
show    Show running system information

```

SG2124G#show ?

```

cli  Show CLI tree of current mode
list Show command lists

```

<Username "test2"로 Login시 사용할 수 있는 CLI>

login as: **test2**

test2@192.168.11.100's password:

SG2124G>**enable**

SG2124G#?

Exec commands:

```

configure Enter configuration mode
enable     Turn on privileged mode command

```

```

exit      End current mode and down to previous mode
help      Description of the interactive help system
quit      Exit current mode and down to previous mode
show      Show running system information

SG2124G#show ?
aaa                AAA Configuration commands
access-list        List IP access lists
acl                List QoS (MAC & IP) access lists
bandwidth          Interface bandwidth usage
bridge             bridge protocol
cable-diag         show cable diagnostic information
cdp                Cisco Discovery Protocol(CDP)
class-map          Class map entry
cli                Show CLI tree of current mode
clock              Current time
cpu-acl            show CPU access list
-- 이하 생략 --

SG2124G#configure terminal
SG2124G(config)#?
Configure commands:
  exit  End current mode and down to previous mode
  help  Description of the interactive help system
  show  Show running system information

SG2124G(config)#exit
SG2124G#show ?
cli      Show CLI tree of current mode
list     Show command lists

```

<Username "test3"으로 Login시 사용할 수 있는 CLI>

```

login as: test3

test3@192.168.11.100's password:
SG2124G>en
SG2124G#?
Exec commands:
  configure  Enter configuration mode
  enable     Turn on privileged mode command
  exit       End current mode and down to previous mode
  help       Description of the interactive help system
  quit       Exit current mode and down to previous mode
  show       Show running system information

SG2124G#show ?
aaa                AAA Configuration commands
access-list        List IP access lists
acl                List QoS (MAC & IP) access lists
bandwidth          Interface bandwidth usage
bridge             bridge protocol
cable-diag         show cable diagnostic information
cdp                Cisco Discovery Protocol(CDP)

```

```

class-map          Class map entry
cli                Show CLI tree of current mode
clock              Current time
cpu-acl            show CPU access list
-- 이하 생략 --

SG2124G(config)#?
Configure commands:
exit              End current mode and down to previous mode
help              Description of the interactive help system
interface         Select an interface to configure
ip                Internet Protocol (IP)
ipv6              Internet Protocol version 6 (IPv6)
show              Show running system information

SG2124G(config)#ip ?
acl                Setting IP and MAC access list
connection-limit  Source IP based connection limit
dhcp              DHCP Server configuration
domain-list       Add a domain to the DNS
domain-lookup     Enable Domain Name Service (DNS)
domain-name       Set default domain for DNS
igmp              Internet Group Management Protocol (IGMP)
name-server       Add a Nameserver to the DNS
radius            RADIUS configuration commands
route             Establish static routes
tacacs            TACACS+ client configuration commands

```

<Username "test4"로 Login시 사용할 수 있는 CLI>

```

login as: test4

test4@192.168.11.100's password:
SG2124G>en
SG2124G#?
Exec commands:
configure         Enter configuration mode
enable            Turn on privileged mode command
exit              End current mode and down to previous mode
help              Description of the interactive help system
quit              Exit current mode and down to previous mode
show              Show running system information

SG2124G#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#?
Configure commands:
dhcp              Configure dhcp filter
exit              End current mode and down to previous mode
help              Description of the interactive help system
hostname          Set system's network name
interface         Select an interface to configure
ip                Internet Protocol (IP)
ipv6              Internet Protocol version 6 (IPv6)
line              Configure a terminal line

```

```
poe          Power-Over-Ethernet
show         Show running system information
threshold    Threshold configuration

SG2124G(config)#dhcp ?
  filter     Enable dhcp filter
  log        DHCP log configuration

SG2124G(config)#threshold ?
  alarm      Temperature alarm
  fan        Fan setting

SG2124G(config)#line ?
  con        Primary terminal line
  vty        Virtual terminal

SG2124GP(config)#poe ?
  pm-mode    Power management mode
```

1.4.10 CPU-ACL을 통한 관리자 접근 통제

관리자가 Switch로의 접근을 허용할 IP와 차단할 IP를 설정하여 불필요한 사용자의 접근을 차단할 수 있습니다.

ACL로 접근통제를 하는 것과 동일하며, ACL 설정을 쉽게 하도록 하는 명령입니다.

SG Switch Series는 IPv4, IPv6를 모두 지원합니다.

CPU-ACL 기능을 사용하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
<code>cpu-acl [snmp ssh telnet] [deny permit] [IP_Addr IPv6_Addr any]</code>	CONFIG	Switch로 접근할 수 있는 snmp나 ssh, telnet의 IP 주소를 등록하여 접근허용이나 거부할 수 있도록 합니다.
<code>show cpu-acl</code>	TOP	설정된 내용을 확인할 수 있습니다.

CPU-ACL 기능을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
<code>no cpu-acl [snmp ssh telnet] [deny permit] [IP_Addr IPv6_Addr any]</code>	CONFIG	등록된 CPU-ACL을 삭제합니다.

<예제> CPU-ACL 기능의 활성화

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#cpu-acl ?
    snmp      SNMP access list
    ssh       SSH access list
    telnet    Telnet access list

SG2124G(config)#cpu-acl ssh ?
    deny      Specify packets to reject
    permit    Specify packets to permit

SG2124G(config)#cpu-acl ssh permit 192.168.254.99
SG2124G(config)#cpu-acl ssh permit 192.168.254.95
SG2124G(config)#cpu-acl telnet permit 192.168.254.99
SG2124G(config)#cpu-acl ssh deny any
SG2124G(config)#cpu-acl snmp permit 192.168.254.99
SG2124G(config)#cpu-acl snmp deny any
SG2124G(config)#end
SG2124G#show running-config | inc cpu-acl
cpu-acl snmp permit 192.168.254.99
cpu-acl snmp deny any
cpu-acl ssh permit 192.168.254.99
cpu-acl ssh permit 192.168.254.95
cpu-acl telnet permit 192.168.254.99
cpu-acl ssh deny any
SG2124G#show cpu-acl
  type  action          IP-Address  wildcard bits
=====
snmp    permit          192.168.254.99  0.0.0.0
snmp    deny              any             any
telnet  permit          192.168.254.99  0.0.0.0
ssh     permit          192.168.254.99  0.0.0.0
ssh     permit          192.168.254.95  0.0.0.0
ssh     deny              any             any

```



참고

1. Terminal 기능은 현재 접속된 화면에 대해서만 적용됩니다.
2. Terminal Length를 0으로 설정하면 -More- 표시 없이 출력되는 모든 내용을 한번에 보여줍니다.

1.5 환경 설정

1.5.1 Host Name 설정

관리자는 관리의 편의를 위해서 명령 프롬프트에 나타나는 **Hostname**을 변경할 수 있습니다. 공장 출하시의 초기 **Hostname**은 **"모델명(SG Switch Series)"**입니다.

Hostname을 변경하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
hostname <i>name</i>	CONFIG	Switch의 Hostname 을 변경합니다.

Hostname을 Default 값으로 변경하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no hostname	CONFIG	Switch의 Hostname 을 Default 명칭으로 변경합니다.

<예제> **Hostname** 변경 및 초기화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#
SG2124G(config)#hostname HDN-TEST
HDN-TEST(config)#
HDN-TEST(config)#no hostname
SG2124G(config)#
```

1.5.2 날짜 및 시간 설정

관리의 편의를 위해 시간을 설정 및 변경할 수 있는 기능을 제공합니다.

시스템 시간을 변경하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
clock <i>HH:MM:SS dd mm yyyy</i>	PREVIOUS TOP	현재 시간을 설정합니다.

시스템 시간을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show clock	TOP	설정된 시간을 확인합니다.

<예제> 날짜 및 시간 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G#clock 16:24:10 10 05 2015
SG2124G#show clock
Tue May 12 16:24:10 2015
SG2124G#
```



참고

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

1.5.3 NTP / SNTP Setup

NTP (Network Time Protocols)는 Network 상에서 시간을 제공하는 특정 Time Server로부터 시간을 가져옴으로써 시스템 시간을 1/1 000 s까지 정확하게 설정하는데 사용합니다.

NTP는 정확한 시간을 제공하기 위해 여러 개의 Time Server를 사용하는데, 여러 개의 Time Server 중에 시간이 틀린 Time Server를 구별하여 현재 시간이 정확한지를 확인합니다. NTP를 설정하면 Switch는 지정된 NTP Server와 지속적으로 Message (UDP Time Packet)을 주고 받으면서 시간 편차를 조정하여 동기화함으로써 현재 시간을 정확하게 맞추며, NTP를 설정하여 맞춰진 시간은 변함없이 유지됩니다.

Switch의 syslog 및 mds detect-list, detect-history 등의 시간을 정확히 확인하기 위해서는 NTP Server를 등록하여 시간을 맞추는 것이 중요합니다.

NTP Server는 공인된 NTP Server나 자체적으로 운영하는 NTP Server를 모두 사용할 수 있으며, 등록할 때는 IP Address나 Domain Name을 사용합니다.

SNTP (Simple Network Time Protocol)는 NTP와 마찬가지로 정확한 시간을 보장하기 위해 사용하지만, 복잡한 알고리즘을 사용하여 여러 개의 Server를 사용하는 NTP와는 달리 시간을 맞추기 위해 하나의 Time Server만 사용하기 때문에 더 신속하고 시스템 성능에도 영향을 덜 미치게 됩니다.

또한, SNTP는 Time Server를 통해 시간을 가져올 때마다 시간을 Update하기 때문에 시간이 갑자기 변할 수 있습니다. Client가 사용하는 Time Server에 문제가 발생한 경우 나중에 등록된 Time Server를 통해 시간을 가져옵니다.

SG Switch Series는 IPv4, IPv6를 모두 지원합니다.

NTP / SNTP를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
ntp authenticate	CONFIG	NTP 인증을 설정합니다.
ntp authentication-key <1-4294967295> md5 WORD	CONFIG	NTP 인증 key를 생성합니다.
ntp server IP_Addr [key <1-4294967295> preger verison <1-4>]	CONFIG	NTP Server의 주소를 지정하며, NTP Client로 설정합니다.
ntp trusted-key <1-4294967295>	CONFIG	NTP Key를 사용합니다.
sntp server A.B.C.D priority <1-3>	CONFIG	SNTP Server의 주소를 지정하며, SNTP Client로 설정합니다.

sntp interval <60-65535>	CONFIG	SNTP 서버에서 동기화 시 interval을 설정합니다. (Default: 720 sec)
sntp timeout <1-10>	CONFIG	SNTP 서버와의 통신 시 Timeout 시간을 설정합니다. (Default: 3 sec)

NTP / SNTP 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show clock	TOP	시스템에 설정된 시간을 확인합니다.
show ntp associations [detail]	TOP	NTP server의 설정내역을 확인합니다.
show ntp status	TOP	시스템에 설정한 NTP의 상태를 확인합니다.
show sntp	TOP	SNTP server의 설정내역을 확인합니다.

NTP / SNTP 설정 내용을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no ntp authenticate	CONFIG	NTP 인증을 초기화합니다.
no ntp authentication-key <1-4294967295> md5 WORD	CONFIG	생성된 NTP 인증 key를 초기화합니다.
no ntp server IP_Addr	CONFIG	NTP server의 주소를 삭제합니다.
no ntp trusted-key <1-4294967295>	CONFIG	설정된 NTP Key를 초기화합니다.
no sntp server WORD	CONFIG	SNTP Server의 주소를 삭제합니다.



참고

1. Network Time Server들로부터 시간을 가져와 동기화 시키기 위해서는 Management IP를 통하여 외부 Time Server와 통신이 이루어져야 합니다.

2. NTP / SNTP Server는 최대 3개까지 설정할 수 있습니다.
3. NTP / SNTP Server를 설정한 경우 TOP 모드에서 clock 명령을 이용한 시간 조정 기능은 사용할 수 없습니다.

<예제> NTP 설정 및 확인

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#ntp server 203.248.240.103
Translating "203.248.240.103"... [OK]
SG2124G(config)#ntp server 211.115.194.21
Translating "211.115.194.21"... [OK]
SG2124G(config)#ntp server 203.238.145.102
Translating "203.238.145.102"... [OK]
SG2124G(config)#end
SG2124G#show ntp associations
      address      ref clock      st when pol reach delay offset disp
--~203.248.240.103  204.123.2.5    2   -   64   377   0.0   0.1   1.0
*~211.115.194.21   192.168.18.6   2   -   64   377   0.0   0.1   1.0
--~203.238.145.102  203.248.240.103 3   52   64   377   0.0   0.0   0.9
* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured
SG2124G#
SG2124G#sh ntp status
Clock is synchronized, stratum 3, regerence is 211.115.194.21
actual frequency is 0.0000 Hz, precision is 2**-17
regerence time is cd9dc526.aaeaa63b ( 2:21:42.667 UTC Mon Apr 26 2009)
clock offset is 0.000 msec, root delay is 18.343 msec
root dispersion is 10830.000 msec,
SG2124G#
```

1. NTP Server를 새로 지정한 경우 5 min 이상 경과 후 NTP Server와의 SYNC가 진행되기 시작합니다.
2. NTP associations 설명
 - address : NTP Server로 지정된 타임 Server IP
 - ref clock : NTP Server가 동기화되는 상위의 NTP Server
 - st : stratum Number
(값이 16이 나오는 경우 해당 Server에 접속할 수 없음)
 - poll : s 단위의 Polling 간격
 - reach : 도달 가능한 레지스터
 - * : NTP Server와 SYNC되고 있음.
 - + : NTP 접속은 가능하지만 SYNC는 안 함.
 - - : NTP 접속은 가능하지만 SYNC 가능 리스트에서 제외됨.



참고

1.5.4 Timezone 설정

관리자는 Switch에 Timezone 명령을 사용하여 그리니치 표준 시간(GMT, Greenwich Mean Time) 대역을 선택할 수 있습니다. Timezone을 변경하게 되면 시스템은 현재 시간을 변경된 표준 시간대의 시간으로 변환하며, syslog등에 기록되는 새로운 event에서 변경된 시간이 적용됩니다. (Timezone을 변경하기 전에 기록된 syslog의 시간은 변경되지 않습니다.).

[표 1-13] Timezone (GMT 시각).

Timezone	국 가	Timezone	국 가
GMT+0	London, Lisbon, Dublin		
GMT+1	Berlin, Paris, Rome	GMT-1	Greenland, Portugal
GMT+2	Athens, Cairo, Jerusalem	GMT-2	South Georgia
GMT+3	Moscow, Dubai	GMT-3	Buenos Aires, Brasilia
GMT+4	Tehran, Kabul	GMT-4	Halifax, Manaus, Santiago
GMT+5	New Delhi, Karachi	GMT-5	New York, Boston, Miami
GMT+6	Yangon	GMT-6	Mexico City, Chicago
GMT+7	Bangkok, Jakarta	GMT-7	Edmonton, Denver
GMT+8	Singapore, Beijing, Taipei	GMT-8	San Francisco, LA, Seattle
GMT+9	Seoul, Tokyo	GMT-9	Anchorage
GMT+10	Melbourne, Sydney	GMT-10	Honolulu
GMT+11	Vladivostok	GMT-11	Midway Islands, Samoa
GMT+12	Auckland, Suva	GMT-12	Howland Isand



참고

1. Default로 설정되어 있는 Timezone은 GMT+9입니다.
2. Timezone의 설정은 GMT, GMT0, GMT+0~12, GMT-0~12, Greenwich, Seoul, Tokyo, UCT, UTC, Universal, Zulu 중 선택하여 변경할 수 있습니다.

Timezone의 설정을 변경하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
timezone <i>WORD</i>	CONFIG	timezone을 변경합니다.

설정된 Timezone을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show running-config include timezone	TOP	설정된 timezone을 확인합니다.

Timezone 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no timezone	CONFIG	timezone을 초기화합니다.

<예제> timezone 변경

```
SG2124G#show clock
Thu Jun 12 11:05:35 GMT+9 2014
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#timezone GMT0
SG2124G(config)#end
SG2124G#show running-config | include timezone
timezone GMT0
SG2124G#
SG2124G#show clock
Thu Jun 12 02:07:03 GMT0 2014
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#no timezone
SG2124G(config)#end
SG2124G#show running-config | include timezone
timezone GMT+9
SG2124G#
SG2124G#show clock
Thu Jun 12 11:07:33 GMT+9 2014
SG2124G#
```

1.5.5 DNS 설정

Telnet, Ping 등의 명령어를 사용할 때 IP Address 대신 Hostname이나 URL을 직접 입력하여 각각의 기능을 수행할 수 있습니다. URL등을 직접 입력하기 위해서는 DNS Server를 지정해 주어야 합니다.

DNC 클라이언트 기능은 IPv4, IPv6를 모두 지원합니다.

DNS Server를 입력하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
ip name-server [IP_Addr IPv6_Addr]	CONFIG	DNS server의 ip address를 설정합니다.
ip domain-list WORD	CONFIG	DNS client의 domain list를 추가합니다.
ip domain-lookup	CONFIG	DNS client를 활성화합니다.
ip domain-name WORD	CONFIG	DNS client의 default domain을 설정합니다.

DNS Server를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show ip name-server	TOP	DNS server의 ip address를 확인합니다.
show ip domain-list	TOP	DNS client의 domain list를 확인합니다.
show ip domain-name	TOP	DNS client의 default domain을 확인합니다.

DNS Server를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no ip name-server [IP_Addr IPv6_Addr]	CONFIG	DNS server의 ip address를 삭제합니다.

no ip domain-list <i>WORD</i>	CONFIG	DNS client의 domain list를 삭제합니다.
no ip domain-lookup	CONFIG	DNS client를 중지합니다.
no ip domain-name <i>WORD</i>	CONFIG	DNS client의 default domain을 삭제합니다.

<예제> DNS 설정 및 삭제

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
SG2124G(config)#ip domain-lookup.
SG2124G(config)#ip name-server 192.168.10.10
SG2124G(config)#exit
SG2124G#
SG2124G#show ip name-server
192.168.10.10
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#ip domain-list SGDNS
SG2124G(config)#exit
SG2124G#
SG2124G#show ip domain-list
SGDNS
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#ip domain-name SG2124DNS.net
SG2124G(config)#exit
SG2124G#
SG2124G#show ip domain-name
SG2124DNS.net
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#no ip name-server 192.168.10.10
SG2124G(config)#no ip domain-list SGDNS
SG2124G(config)#no ip domain-lookup
SG2124G(config)#no ip domain-name SG2124DNS.net
SG2124G(config)#

```

1.5.6 Banner 설정

Login 화면에 여러 가지 Message를 등록하여 콘솔 및 Telnet을 통해 접속하는 사용자에게 접속 및 Login 시 등록된 Message를 전달할 수 있습니다. 이 기능을 이용하면 관리자가 다른 사람에게 주의 사항이나 전달 사항을 등록할 수 있습니다.

Banner를 설정 하거나 변경 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
<code>banner begin word</code>	CONFIG	접속 시 출력되는 Message를 등록합니다.
<code>banner login-fail word</code>	CONFIG	Login 실패 시 출력되는 Message를 등록합니다.
<code>banner motd {word default}</code>	CONFIG	Login 성공 시 출력되는 Message를 등록 및 초기화합니다.

설정된 Banner를 삭제 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
<code>no banner begin</code>	CONFIG	접속 시 출력되는 Message를 삭제합니다.
<code>no banner login-fail</code>	CONFIG	Login 실패 시 출력되는 Message를 삭제합니다.
<code>no banner motd</code>	CONFIG	Login 성공 시 출력되는 Message를 삭제합니다.

<예제> Banner 설정

```
SG2124G(config)#banner motd Welcome to HDN Switch Hub!!
SG2124G(config)#end
SG2124G#exit
```

```
SG2124G login: root
Password: *****
```

```
Welcome to HDN Switch Hub!!
```

SG2124G>



1. **Banner**로 지정할 수 있는 문자열은 최대 **256**자까지 사용할 수 있습니다.
 2. “**banner begin**” 및 “**banner login-fail**”을 초기화하는 경우 접속 및 Login 실패 시 **Message**가 출력되지 않습니다.
-

1.5.7 L3 License 등록

SG Switch Series의 Routing 기능을 사용하려면 L3 License 등록 및 L3 Firmware update가 필요합니다.

BGP, OSPF, RIP, VRRP 등과 같은 Routing 기능은 License가 등록된 이후부터 사용가능 합니다.

License를 등록하지 않은 상태에서 L3 Firmware만 업데이트 한 경우 TOP / EXEC / CONFIG / INTERFACE Mode를 제외한 나머지 모드의 접근이 불가능 하며, 지정된 모드 외에 다른 모드로 접근을 시도하면 'L3-OS License is required' 메시지를 표시하고 Top 모드로 강제 전환 됩니다.

SG3000, SG3100, SG3200 Switch Series의 경우 License Key는 별도로 출력되지 않으며, License install 여부만 표시됩니다.

License를 등록하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
license install l3 KEYSTR	CONFIG	License Key를 등록합니다.

등록된 License를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show license	TOP	등록된 License 정보가 출력됩니다.



참고

1. L2 Firmware 상태에서 License를 등록한 경우 시스템 재시작 여부는 자율적입니다.
2. L3 Firmware로 업데이트한 이후 License를 등록한 경우 시스템 재시작이 필요하며, 재시작하지 않는 경우 License가 등록되지 않습니다.(Reboot 필수)
3. License 는 기본 제공되지 않습니다. License가 필요한 경우 제품 구매처 또는 당사 영업부로 문의하시기 바랍니다.
4. SG2008G Series 제품은 L3 License 기능을 지원하지 않습니다.

<예제> L3 Firmware update 이후 License를 등록하는 경우

```
SG2124G login: root
Password: *****

SGOS version 2.2.5 SGL3-OS 01/22/14 11:39:55
% L3-OS License is required.
% If you do not have the l3 license to upgrade your L2 OS image.

SG2124G>en
SG2124G#show license
  L3 Dynamic Routing feature : Not installed
SG2124G#con t
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#router ospf 1
% L3-OS License is required.
% If you do not have the l3 license to upgrade your L2 OS image.
SG2124G#
SG2124G#con t
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#license install l3 9bfbff98183abab-001AF4.123456-287ed2c3c7aef58a
% Reload is required. Do you want to continue? (y/n): y    → 시스템 재시작 필수
% Successfully installed

----- REBOOTING -----

SGOS version 2.2.5 SGL3-OS 01/22/14 11:39:55
SG2124G>en
SG2124G#show license
  L3 Dynamic Routing feature : Installed
  License Key                  : 9bfbff98183abab-001AF4.123456-287ed2c3c7aef58a
SG2124G#
```

1.5.8 설정 내용 관리

■ 설정 내용 확인

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

현재 설정되어 있는 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show running-config	TOP CONFIG	설정된 모든 내용을 보여줍니다.

<예제> Default-Config 내용 확인

```
SG2124G#show running-config
!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
snmp-server disable
!
bridge 1 protocol pvstp
!
bridge 1 pvstp vlan 1
no bridge 1 pvstp enable bridge-forward bpdu-flood
!
mds enable ge1-22 detect
mds uplink ge23-24
mds syslog enable
mds auto-config config-save
!
mls qos enable
!
interface ge1
!
interface ge2
!
interface ge3
!
interface ge4
!
interface ge5
!
interface ge6
!
```

```
interface ge7
!
interface ge8
!
interface ge9
!
interface ge10
!
interface ge11
!
interface ge12
!
interface ge13
!
interface ge14
!
interface ge15
!
interface ge16
!
interface ge17
!
interface ge18
!
interface ge19
!
interface ge20
!
interface ge21
!
interface ge22
!
interface ge23
!
interface ge24
!
interface lo
  ip address 127.0.0.1/8
  ipv6 address ::1/128
!
interface vlan1.1
!
timezone GMT+9
!
service dhcp
no service sshd
line con 0
  login local
line vty 0 5
  login local
!
end

SG2124G#
```

■ 설정 내용 저장

동작 모드 및 환경 설정 변경 후 재 부팅 후에도 계속하여 설정된 내용을 유지하기 위해서는 반드시 설정한 내용을 **Switch** 내의 저장영역에 저장하여야 합니다.

현재 설정되어 있는 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
write [memory]	TOP	변경된 내용을 저장영역에 저장합니다.
write terminal	TOP	현재 설정되어 있는 정보를 화면에 보여줍니다. (show running-config와 동일함)



설정 내용을 저장 중일 때 **Switch**의 전원을 **Off**하면 설정 내용을 잃어버리고, **Switch** 동작에 문제가 발생할 수 있습니다.

<예제> Hostname 변경 후 설정 저장

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#
SG2124G(config)#hostname HDN-TEST
HDN-TEST(config)#
HDN-TEST(config)#end
HDN-TEST#write
Building configuration...
[OK]
HDN-TEST#
```


■ 설정 내용 초기화

동작 모드 및 환경 설정이 변경된 **Switch**를 공장 출하 시 기본 설정 상태로 설정할 수 있습니다.

Switch를 공장 출하시의 기본 설정 상태로 초기화하고자 하는 경우에는 다음 명령어를 사용하십시오.

명령어	모드	기능
factory-default	CONFIG	설정 내용을 공장 출하시의 기본값으로 초기화합니다.



참고

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

<예제> 설정 내용 초기화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#factory-default
full reset to factory-default? (y/n): y

HDNBR-2.5.12

* OS Number   : 1
* OS Name     : SG2124G OS Image v2.2.6
* OS Size     : 13119 KiB
* Build Date  : 2014. 5.30 14:44: 5
Loading: ..... 16777216 bytes read

Initializing ..... Done

SG2124G login:
```

1.6 시스템 상태 정보

1.6.1 Network 상태 확인(Ping Test)

관리자의 Switch가 Network에 올바르게 연결되어 있는지 여부를 알기 위해서는 ping 명령어를 사용합니다. IP Network에서 ping 명령어는 ICMP (Internet Control Message Protocol) Echo Message를 전송합니다. ICMP는 오류상황을 알려 주고 IP Packet 수신지 정보를 제공하는 인터넷 Protocol입니다. ICMP Echo Message를 받은 수신지는 ICMP Echo Reply Message를 송신지로 돌려 보냅니다.

SG Switch Series는 IPv4, IPv6를 모두 지원합니다

상대방과 Network 연결 상태를 확인하기 위해 IPv4 Ping 테스트를 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
ping	TOP	옵션들을 설정하여 Network 연결 상태를 확인합니다.
ping ip-address	TOP	Network 연결 상태를 확인합니다.(3회)
ping ip-address infinite	TOP	Ctrl+C를 눌러 중지하기 전까지 지속적으로 Network 연결 상태를 확인합니다.

IPv6 Ping 테스트를 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
ping ipv6 ip-address	TOP	Network 연결 상태를 확인합니다. (3회)
ping ipv6 ip-address infinite	TOP	Ctrl+C를 눌러 중지하기 전까지 지속적으로 Network 연결 상태를 확인합니다.

<예제> Network 연결 상태 확인

```
SG2124G#ping 164.124.101.2
PING 164.124.101.2 (164.124.101.2) from 192.168.254.11 : 56(84) bytes of data.
64 bytes from 164.124.101.2: icmp_seq=1 ttl=128 time=5.44 ms
64 bytes from 164.124.101.2: icmp_seq=2 ttl=128 time=0.688 ms
64 bytes from 164.124.101.2: icmp_seq=3 ttl=128 time=0.667 ms

--- 164.124.101.2 ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 2124ms
rtt min/avg/max/mdev = 0.667/2.265/5.441/2.245 ms
SG2124G#ping
Protocol [ip]:
Target IP address: 164.124.101.2
Repeat count [5]:
Datagram size [100]:
Extended commands [n]:
PING 164.124.101.2 (164.124.101.2) from 192.168.254.11 : 100(128) bytes of data.
108 bytes from 164.124.101.2: icmp_seq=1 ttl=54 time=4.39 ms
108 bytes from 164.124.101.2: icmp_seq=2 ttl=54 time=4.73 ms
108 bytes from 164.124.101.2: icmp_seq=3 ttl=54 time=3.45 ms
108 bytes from 164.124.101.2: icmp_seq=4 ttl=54 time=4.18 ms
108 bytes from 164.124.101.2: icmp_seq=5 ttl=54 time=5.06 ms

--- 164.124.101.2 ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4040ms
rtt min/avg/max/mdev = 3.455/4.365/5.068/0.549 ms

SG2124G#ping ipv6 2000::3
PING 2000::3 (2000::3): 56 data bytes
64 bytes from 2000::3: seq=0 ttl=64 time=3.940 ms
64 bytes from 2000::3: seq=1 ttl=64 time=1.242 ms
64 bytes from 2000::3: seq=2 ttl=64 time=1.214 ms

--- 2000::3 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.214/2.132/3.940 ms
SG2124G#
```

1.6.2 Packet 경로 확인

Switch 관리자는 Packet이 목적지로 가면서 거쳐 가는 경로를 확인할 수 있습니다.

Traceroute 명령어는 검침 Packet을 보낸 후 거쳐가는 경로마다 되돌아 오는 시간을 화면에 출력합니다. 만일 검침 Packet이 되돌아오는 시간이 될 때까지 Packet의 응답이 없는 경우에는 별표(*)가 출력됩니다.

SG Switch Series는 IPv4, IPv6를 모두 지원합니다.

Packet 경로를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
traceroute	TOP	목적지의 IP Address 또는 Hostname 등의 옵션들을 설정하여 Packet 전송 경로를 추적합니다.
traceroute {IP_Addr IPv6_Addr}	TOP	목적지의 IP Address 또는 Hostname 을 입력하면 Packet 전송 경로를 추적합니다.

<예제> traceroute 확인

```
SG2124G#traceroute 192.168.2.1
traceroute to 192.168.2.1 (192.168.2.1), 30 hops max, 38 byte packets
 1 192.168.1.1 (192.168.1.1) 9.897 ms 9.599 ms 9.883 ms
 2 192.168.2.1 (192.168.2.1) 9.921 ms 9.753 ms 9.893 ms
SG2124G#traceroute
Protocol [ip]:
Target IP address: 192.168.2.1
Source address:
Numeric display [n]:
Timeout in seconds [2]:
Probe count [3]:
Maximum time to live [30]:
Port Number [33434]:
traceroute to 192.168.2.1 (192.168.2.1), 30 hops max, 38 byte packets
 1 192.168.1.1 (192.168.1.1) 9.897 ms 9.599 ms 9.883 ms
 2 192.168.2.1 (192.168.2.1) 9.921 ms 9.753 ms 9.893 ms
SG2124G#traceroute ipv6 2000::3
traceroute6
2000::3
traceroute to 2000::3 (2000::3), 30 hops max, 16 byte packets
 1 2000::3 (2000::3) 4.908 ms 0.749 ms 1.068 ms
```

1.6.3 Cable 길이 / 상태 확인

Cable-diag 기능은 이상 발생시 Cable 단절 및 Cable에서 오류가 발생한 위치 및 발생한 Cable 오류 종류에 대한 정보를 얻을 수 있어 Cable의 이상 유무 및 단절된 부분까지의 Cable의 길이를 확인할 수 있습니다.

검사에서는 시간 Domain 반사 측정법(TDR) 기술을 사용하여 Interface에 연결된 Cable의 품질 및 특성을 검사합니다. 반환된 Cable 길이는 근사치이므로 약간의 편차가 있을 수 있습니다.

Switch와 PC 및 장비간의 연결이 정상(Link up)인 경우 "ok"로 표시되며, Cable 길이를 표시하지 않습니다. Switch에만 Cable이 연결되어 있으며 사용자 PC에는 Cable이 연결되어 있지 않은(Link Down) 경우 "open"으로 표시되면서 Cable 길이가 표시됩니다.

연결된 Cable 길이를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show cable-diag [IFNAME]	TOP	Interface에 연결된 Cable 길이를 알려줍니다.

<예제> Interface에 연결된 Cable 길이 확인

SG2124G#show cable-diag ge1					
Port/ Port(Pair)	Cable State/ Pair State	Pair Count	Fuzz	Length	Cable Length
ge1	Ok	4	+/-	- Meter	
ge1(A)	Ok		+/-	- Meter	- Meter
ge1(B)	Ok		+/-	- Meter	- Meter
ge1(C)	Ok		+/-	- Meter	- Meter
ge1(D)	Ok		+/-	- Meter	- Meter
SG2124G#show cable-diag ge2					
Port/ Port(Pair)	Cable State/ Pair State	Pair Count	Fuzz	Length	Cable Length
ge2	Open	4	+/-	1 Meter	
ge2(A)	Open		+/-	1 Meter	3 Meter
ge2(B)	Open		+/-	1 Meter	3 Meter
ge2(C)	Open		+/-	1 Meter	3 Meter
ge2(D)	Open		+/-	1 Meter	3 Meter



참고

cable-diag 명령을 2~3회 실행하면 더 정확한 Cable 길이를 확인할 수 있습니다.

1.6.4 현재 접속자 확인

현재 접속한 사용자들에 대해 접속한 방식, Login ID, 접속하여 사용중인 시간, 접속한 Host의 정보 등을 확인할 수 있습니다.

접속한 사용자를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show users	TOP	현재 접속되어 있는 사용자를 확인합니다.

<예제> 현재 접속자 확인

```
SG2124G#show users
  Line      User      Uptime      Host(s)
   0 con 0   root      01:40:52    local
 130 vty 0   test1     00:00:09    192.168.254.120
SG2124G#
```

1.6.5 MAC Table / MAC-Count

연결된 다른 Network 장비나 컴퓨터 등으로부터 Data Frame이 수신되면 Switch는 해당 Interface와 MAC Address를 MAC Table에 기록하며, 기록된 MAC Address 정보는 Aging Time (Default 300 s) 후 MAC Table에서 초기화됩니다.

MAC-Count 는 Interface별로 연결되어 있는 MAC Address의 수를 확인하는 기능입니다. max-history는 특정 기간 Hour (5 min 단위), Day (1 h 단위), Month (1 d 단위)로 기록되어 있는 MAC Address 수가 제일 많았던 Interface를 저장하고 지나간 Log는 자동으로 폐기하는 기능입니다.

MAC-Count History 기능을 사용하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mac-count max-history enable	CONFIG	Interface 별로 기록된 MAC Count의 History 기능을 활성화합니다.

Interface에 기록된 MAC Table을 출력할 때는 다음 명령어를 사용하십시오.

명령어	모드	기능
show mac-table [IFNAME]	TOP	MAC Address를 출력합니다.
show mac-count	TOP	Interface 별로 기록된 MAC Address를 count하여 출력합니다.
show mac-count max-history {day hour month}	TOP	일/시간/월 단위의 Max MAC Count 및 Interface 정보를 출력합니다.

MAC Table 관련 정보를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
clear mac address-table {dynamic multicast static} [address MAC_Addr interface IFNAME vlan VLAN_ID] bridge 1	TOP	MAC Table을 초기화합니다.
clear mac count-history	TOP	Max MAC Count 정보를 초기화합니다.
no mac-count max-history enable	CONFIG	MAC-Count History 기능을 중지합니다.

<예제> MAC Table 확인

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mac-count max-history enable
SG2124G(config)#exit
SG2124G#show mac-table
bridge      VLAN port      mac          fwd timeout
1           1   ge24      000d.65e6.8504 1    300
1           1   ge2       000e.0c4e.d0d5 1    300
1           1   ge24      0010.f308.4c86 1    300
1           1   ge24      00d0.cb22.1a1b 1    300
1           1   ge24      00e0.ed10.8a38 1    300
MAC Count(Dynamic) = 5
SG2124G#
SG2124G#show mac-count
port      mac-count
=====
ge2        1
ge24       4
=====
Total = 5

SG2124G#show mac-count max-history hour
Measurement Time (1 Hour) Incoming Port Max MAC Count
=====
Thu Feb 25 10:28:10 2009 ge24          23
Thu Feb 25 10:23:10 2009 ge24          20
Thu Feb 25 10:18:10 2009 ge24          21
Thu Feb 25 10:13:10 2009 ge24          21
Thu Feb 25 10:08:10 2009 ge24          24
Thu Feb 25 10:03:10 2009 ge24          19
Thu Feb 25 09:58:10 2009 ge24          21
Thu Feb 25 09:53:10 2009 ge24          24
Thu Feb 25 09:48:10 2009 ge24          20

SG2124G#

```



참고

1. MAC Table에는 8K~최대 32K까지 MAC Address가 등록될 수 있습니다. 장비별 MAC Address Entry 개수는 제품 설치가이드의 사양정보를 참고하시기 바랍니다.
2. MAC Aging Time (Default 300 s) 이 너무 높게 설정된 경우 MAC Table이 Full되어 신규 MAC Address를 등록하지 못하여 DLF가 발생할 수 있습니다. 너무 낮게 설정된 경우에는 MAC Table로부터 MAC Address가 짧은 주기로 사라지기 때문에 해당 MAC Address를 Destination으로 하는 Packet들의 DLF 발생으로 인하여 전체 Network에 잦은 Flooding이 발생하여 Network의 혼잡도가 증가할 수 있습니다.

1.6.6 ARP Table

ARP Table의 내용은 Switch 관리 IP와 동일한 Network인 경우 ARP를 통해 IP Address와 일치하는 MAC Address를 찾았을 때 자동으로 기록됩니다. Network 관리자는 특정 IP Address의 MAC Address를 직접 ARP Table에 등록하여 사용할 수도 있습니다.

특정 IP Address와 MAC Address를 일치시키려면 다음 명령어를 사용하십시오.

명령어	모드	기능
arp <i>IP_Addr</i> <i>MAC_Addr</i>	CONFIG	IP Address와 MAC Address를 ARP Table에 등록합니다.

ARP Table을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show ip arp	TOP	ARP 정보를 출력합니다.

특정 ARP Table을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no arp <i>IP_Addr</i>	CONFIG	수동으로 등록한 ARP Table을 삭제합니다.

<예제> Static ARP 추가/삭제

```
SG2124G(config)#arp 192.168.100.3 0000.0000.0007
SG2124G(config)#exit
SG2124G#show ip arp
  IP Address      MAC Address      Interface  Type
192.168.100.3    0000.0000.0007  vlan1.1    static
192.168.100.5    00d0.cb0b.e37e  vlan1.1    dynamic
192.168.100.90   00e0.8161.9e8f  vlan1.1    dynamic
192.168.100.99   00e0.4ca5.6334  vlan1.1    dynamic
192.168.100.100  001a.f400.0301  vlan1.1    dynamic
192.168.100.140  0013.2041.fbb2  vlan1.1    dynamic
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#no arp 192.168.100.3
SG2124G(config)#exit
SG2124G#show ip arp
```

IP Address	MAC Address	Interface	Type
192.168.100.3	0000.0000.0007	vlan1.1	dynamic
192.168.100.5	00d0.cb0b.e37e	vlan1.1	dynamic
192.168.100.90	00e0.8161.9e8f	vlan1.1	dynamic
192.168.100.99	00e0.4ca5.6334	vlan1.1	dynamic
192.168.100.100	001a.f400.0301	vlan1.1	dynamic
192.168.100.140	0013.2041.fbb2	vlan1.1	dynamic

SG2124G#

1.6.7 Uptime 정보

관리자는 현재 시간, Switch의 전원을 켜고 부팅한 이후부터 장비를 사용한 시간 및 1 min, 5 min, 15 min간의 Switch의 Load Average를 확인할 수 있습니다.

Switch 사용 시간을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show system uptime	TOP	Switch의 전원을 켜 이후부터 사용한 시간 등을 확인합니다.

<예제> 시스템 사용 시간 확인

```
SG2124G#show system uptime
 6:11am up 13 days, 11:29, load average: 0.06, 0.02, 0.00
SG2124G#
```

1.6.8 CPU 사용량

관리자는 Switch의 CPU 사용량에 대해 5 s, 30 s, 1 min, 5 min, 15 min, 60 min, all-time (부팅한 이후 현재까지)의 평균 사용량을 확인할 수 있습니다.

CPU 평균 사용량을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show system cpu-load	TOP	Switch의 CPU 평균 사용량을 확인할 수 있습니다.

<예제> 시스템 CPU 사용량 확인

```
SG2124G#show system cpu-load
```

Time	sum	user	system
5 sec :	0.00%	0.00%	0.00%
30 sec :	0.03%	0.03%	0.01%
1 min :	0.03%	0.00%	0.03%
5 min :	0.00%	0.00%	0.00%
15 min :	0.00%	0.00%	0.00%
60 min :	0.00%	0.00%	0.00%
all-time :	0.32%	0.01%	0.02%

```
SG2124G#
```

1.6.9 Memory 사용량

관리자는 현재 각각의 **Daemon Process**에 할당된 **Memory** 정보와 **Switch**에서 사용중인 **Memory** 정보를 확인할 수 있습니다. 관리자는 이 기능을 통해 장비에 문제가 발생하였을 때 문제를 해결할 수 있는 정보를 파악할 수 있습니다.

Memory에 대한 정보를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show system memory [detail]	TOP	Switch의 Memory 사용 정보를 확인합니다.
show memory	TOP	Switch의 Daemon process에 할당된 Memory 정보를 확인합니다.

<예제> 시스템 Memory 사용량 확인

```
SG2124G#show memory
```

```
Library memories for IMI
```

Memory type	Alloc cells	Alloc bytes
Temporary memory	7181	725296
Hash	1	80
Hash index	1	4144
Hash bucket	28	2240
Thread master	1	1072
Thread	13	1456
Link list	42	3360
Link list node	58	4640
Show	1	560
Show page	1	8240
Show server	1	112
Prefix IPv4	4	320
Route table	4	320
Route node	165	18480
Vector	3639	291120
Vector index	3639	297520
Host config	2	160
Message of The Day	1	176
Host config password	2	160
VTY if	28	15680
VTY connected	2	160
Message entry	9	720
Message handler	2	224
Host	1	176
Log information	2	224
Context	1	560

-- 이하 생략 --

1.6.10 Process 상태

관리자는 현재 구동중인 **Process**를 확인할 수 있습니다. 관리자는 이 기능을 통해 장비에 문제가 발생하였을 때 문제를 해결할 수 있는 정보를 파악할 수 있습니다.

Process를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show process	TOP	itch의 Daemon Process를 확인합니다.

<예제> Daemon Process 확인

```
SG2124G#show process
PID NAME          TIME FD
  1 nsm            1d01h56m 6
 14 authd          1d01h56m 8
 15 lacpd          1d01h56m 10
 16 stpd           1d01h56m 9
 17 rstpd          1d01h56m 11
 18 mstpd          1d01h56m 12
 24 rmon           1d01h56m 14
 26 lldpd          1d01h56m 15
 27 sflow          1d01h56m 16
 29 pvstpd        1d01h56m 13
 30 erpd           1d01h56m 16
SG2124G#
```

1.6.11 FAN / 온도 Alarm 설정 및 확인

Switch는 FAN 및 내부 온도에 따른 Alarm 기능을 제공하고 있으며, 관리자의 설정을 통해 FAN 동작 온도 및 Alarm 온도 설정을 변경할 수 있습니다.

온도 Alarm의 경우 보드 중앙에 부착된 온도센서 Chip을 통해 내부의 온도를 확인하여 내부 온도가 +70 °C 이상이거나 -20 °C 이하인 경우에 동작하며, FAN Alarm의 경우 Switch 내부에 장착된 FAN의 동작에 이상이 발생한 경우 동작합니다.

장비의 FAN, Alarm 설정 값을 변경하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
threshold alarm high {VALUE default} low {VALUE default}	CONFIG	Alarm 온도를 설정합니다.
threshold fan start {VALUE default} stop {VALUE default}	CONFIG	FAN 동작 온도를 설정합니다.

장비의 내부 온도 및 FAN, Alarm 설정 값을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show system temperature	TOP	Switch의 온도를 확인합니다.

<예제> 장비 내부 온도 확인

```
SG2124G#show system temperature
M/B Temp      : 43.0 C
Outside Temp   : 30.0 C
Fan Start      : 20 C
Fan Stop       : 15 C
Alarm Low      : -20 C
Alarm High     : 70 C
SG2124G#
```



참고

1. Temperature Alarm을 설정할 수 있는 온도의 범위는 최소 -20 °C에서 최대 80 °C입니다.

1.6.12 Version 정보

현재 구동되고 있는 OS Image의 Version 및 Build Version을 확인할 수 있습니다.

초기 설치 시 현재 구동되는 OS Image Version을 확인하여 최신 OS Image인지를 확인하시기 바랍니다.

OS Image Version을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show version	TOP	OS Image Version을 확인합니다.

<예제> OS Version 확인

```
SG2124G#show version
SG-2124G-2.2.6 05/30/14 15:36:26
Copyright (C) HanDreamNet. All rights reserved.
SG2124G#
```


1.6.13 System 정보

Switch의 Model Name, Main Memory Size, Flash Memory Size, Serial Number, MAC Address, Boot Loader Version 정보 등을 확인할 수 있습니다.

System 정보를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show system system-info	TOP	System 정보를 확인합니다.

<예제> 시스템 정보 확인

```
SG2124G#sh system system-info
Vendor       : HanDreamNet
Model        : SG2124G
Serial No    : SG12387C0018
Main Memory  : 512MB
Flash Memory : 64MB
MGMT MAC     : 00:1A:F4:BC:00:3B
SF BASE MAC  : 00:1A:F4:3C:00:3B
HW Version   : V1.2
BootLoader Version : 2.5.12
OS Version   : SG-2124G-2.2.8
L3 License Feature : Installed
SG2124G#
```

1.6.14 SFP Mode Definition (MOD-DEF)

Uplink Interface로 SFP Type과 10/100/1000Base-T Type의 COMBO Interface를 사용할 수 있으며 SFP Module을 장착한 경우 SFP Module의 정보 및 현재 동작하는 Interface Type이 어떤 것인지를 확인할 수 있으며, SFF-8472 규격을 지원하는 SFP Module을 장착한 경우 SFF-8472(Tx/Rx Power, Voltags, Bias current, Temperature등) 정보를 확인할 수 있습니다. SFF-8472규격을 지원하는 SFP에서 Alarm 또는 Warning이 발생할 경우 syslog에 Event를 기록하며, SNMP Trap을 전송하도록 설정한 경우에는 SNMP Trap-Server로 관련 Event를 전송합니다.

SFP와 10/100/1000T 모두에 Cable이 연결되어 있는 경우 우선순위가 높은 SFP가 동작하도록 되어 있으며, SFP Module 또는 Fiber Cable에 이상이 발생한 경우 자동으로 10/100/1000T로 통신을 시작합니다.

Combo Port에 대한 정보를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show system sfp Port_No	TOP	SFP Module의 정보를 확인합니다.
show interface media [IFNAME]	TOP	동작 중인 Interface Type을 확인합니다.

<예제> Combo Port의 정보 확인

- ge23에 SFP Module 장착. Fiber로 통신.

```
SG2124G#show system sfp 23
Identifier      : SFP transceiver
Connector      : LC
Encoding       : 8B10B
BR. Nominal    : 1300Mbits'sec
Rate Identifier:
Transceiver    :
  Gigabit Ethernet Compliance Codes:
    1000BASE-LX
  Fibre Channel link length:
    long distance (L)
  Fibre Channel transmitter technology:
    Longwave Laser(LC)
  Fibre Channel transmission media:
    Single Mode (SM)
  Fibre Channel speed:
    100 MBytes/Sec
Length         :
  Link length supported for 9/125mm(SMF) fiber, 15000m
VendorName     : HG GENUINE
VendorOUI      : 0x000000
VendorPN       : MXP-243S-15KM
```

```
VendorRev      :  
WaveLength     : 1310 nm  
Options        :  
    TX_DISABLE is implemented  
    TX_FAULT signal implemented  
    Loss of signal implemented  
BR. MAX        : 0%  
BR. MIN        : 0%  
VendorSN       : 0187975  
DateCode       : 2007.05.09  
Monitoring Type:  
Enhanced Opt.  :  
SG2124G#  
SG2124G#show int media ge23  
    Interface: ge23  Active medium: Fiber
```

1.6.15 Scanning 기능

SG Switch Series에서는 NETBIOS와 TCP PORT를 scanning 하는 기능을 사용할 수 있습니다.

Scanning 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
netbios-scan {IP_Addr IP_Addre/Mask} [MAX_IP_Addr]	TOP	정해진 IP 범위내의 netbios 정보를 스캔 합니다.
port-scan	TOP	입력라인에서 IP와 Port를 입력하여 TCP Port 정보를 스캔 합니다.
port-scan {IP_Addr IPv6_Addr}	TOP	정해진 IP의 TCP Port 1~1024 정보를 스캔 합니다.
port-scan {IP_Addr IPv6_Addr} <1-65535>	TOP	정해진 IP의 특정 TCP Port 정보를 스캔 합니다.
port-scan {IP_Addr IPv6_Addr} [MIN_Port_Num MAX_Port_Num]	TOP	정해진 IP의 지정한 범위의 TCP Port 정보를 스캔 합니다.

<예제> Scanning 정보 확인

```
SG2124G#netbios-scan 192.168.1.1 192.168.1.255
IP address      NetBIOS Name    Server    User          MAC address
-----
192.168.255.30  <unknown>      <unknown> <unknown>     00-21-9b-08-9a-66
192.168.255.60  COM-PC         <server>  <unknown>     60-eb-69-fe-11-ff
192.168.255.211 HDN-PC         <server>  <unknown>     00-02-b3-98-3a-22
SG2124G#
SG2124G#port-scan 192.168.1.10 23 500
Scanning 192.168.1.10 ports 23 to 500
Port  Proto  State  Service
23    tcp    open   telnet
80    tcp    open   www
179   tcp    open   bgp
474 closed, 3 open, 1 timed out (or blocked) ports
SG2124G#
```



참고

Scanning 기능은 Switch버전 2.x 이상에서만 지원합니다.

1.6.16 TFM 기능

TFM(Traffic Flow Monitoring)은 Flow기반의 모니터링을 제공하는 기능입니다.

TFM 기능을 설정하면 지정한 Port간의 Protocol 사용량을 확인 할 수 있습니다. 기능을 활성화한 입/출력 포트는 정상적으로 스위칭 기능을 사용할 수 없습니다. 또한, 입력포트에서 지정한 트래픽 이외의 패킷은 drop 처리됩니다.

최대 32개까지 설정 가능하며, 입력포트에 default로 우선순위가 낮은 all drop rule이 추가됩니다.

TFM은 ACL rule을 사용하므로 TFM rule 설정으로 ACL 설정 개수가 그만큼 감소됩니다. (TFM 3개 설정 시 ACL 설정 개수 4개가 줄어들게 됩니다.) 여러 개의 rule 사용시에는 가장 먼저 설정된 rule에 따라 동작합니다.

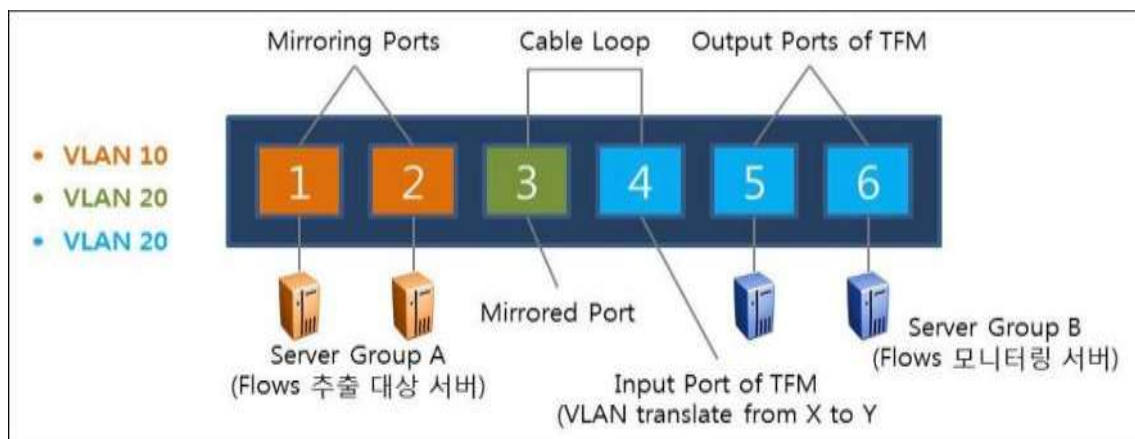
하나의 스위치에서 트래픽을 분류하여 모니터링 하기 위해서는 N:1로 mirror 시킨 트래픽을 cable loop를 통해 TFM 입력포트에 연결하여 모니터링 입/출력 포트들의 vlan을 분리시킨 후 분류하려는 프로토콜이 출력되는 포트를 1:N으로 설정하여야 합니다.

vlan으로 분리된 TFM 포트에서 egress mirror한 트래픽을 cable loop를 통해 받을 경우 vlan 변환 설정을 추가해 주어야 합니다. (vlan 10의 트래픽을 vlan 20으로 mirror 시킨 뒤 cable loop으로 vlan 30에 연결하면 vlan 30으로 지정한 포트에 vlan 10 tag가 들어가게 되고, 그 패킷은 drop 됩니다. 따라서 vlan 30 포트에 vlan 10 tag 패킷을 vlan 30 tag로 변환하도록 ip monitor vlan-translate 10 30 설정이 필요합니다.)

TFM에 사용되는 Port 용도는 아래와 같습니다.

- Mirroring Port
- Mirrored Port
- Input Port of TFM
- Output Port of TFM

[그림 1-1] TFM Port 용도



TFM을 통해 추출할 수 있는 Flow범위는 아래와 같습니다.

- Layer2 Source/Destination MACs
- Layer3 Source/Destination IPs
- Layer4 Source/Destination Service Ports

TFM 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
{ip ipv6} monitor {any icmp raw tcp udp} SRC_PORTRANGE DST_PORTRANGE {SRC_MAC SRC_MAC/Mask any} {SIP SIP/Mask any} {DST_MAC DST_MAC/Mask any} {DIP DIP/Mask any} [Comment ratelimit <64-100000> vlan VLAN_ID]	CONFIG	TFM 기능을 설정합니다.
ip monitor vlan-translate ingress_packet_VLANID New_VLANID	INTERFACE	모니터링 하는 트래픽에 붙은 VLAN tag를 mirror 트래픽을 수신하는 Interface의 VLAN tag로 변환 하도록 설정합니다.

TFM 기능을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show {ip ipv6} monitor	TOP	TFM 정보를 확인합니다.

TFM 기능을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no {ip ipv6} monitor {all any icmp raw tcp udp} SRC_PORTRANGE DST_PORTRANGE {SRC_MAC SRC_MAC/Mask any} {SIP SIP/Mask any} {DST_MAC DST_MAC/Mask any} {DIP	CONFIG	TFM 설정 내역을 삭제합니다.

<i>DIP/Mask</i> any}		
clear count {ip ipv6} monitor	TOP	수집된 TFM count 정보를 초기화 합니다.
no ip monitor vlan-translate <i>ingress_packet_VLANID</i>	INTERFACE	VLAN tag 변환을 해제합니다.

<예제> TFM(Traffic Flow Monitoring) 설정 내역

- 하나의 스위치에서 트래픽 분류 모니터링

- 1) ge1-3 : TFM 출력 포트(분리된 트래픽 수신), vlan 20 설정
- 2) ge4 : TFM 입력 포트, vlan tag 변환 설정, vlan 20, ge5와 loop 연결
- 3) ge5 : mirror 포트, ge13-14 트래픽 수신 설정, vlan 10, ge4와 loop 연결
- 4) ge13 : 네트워크 통신 포트, vlan 50 설정
- 5) ge14 : 네트워크 통신 포트, vlan 60 설정

SG2124G#show running-config

```
vlan database
vlan range 10,20,50,60 bridge 1
!
mls qos enable
mds enable ge6-22 detect
mds uplink ge23-24
ip monitor any ge4 ge1-2 any 192.1.1.2 any any

ip monitor any ge4 ge3 any any any 192.1.1.2

ip monitor any ge4 ge1 any 192.4.1.2 any any
!
interface ge1
switchport access vlan 20
!
interface ge2
switchport access vlan 20
!
interface ge3
switchport access vlan 20
!
interface ge4
switchport access vlan 20
ip monitor vlan-translate 50,60 20
!
interface ge5
mirror interface ge13-14 direction both
switchport access vlan 10
!
interface ge13
switchport mode trunk
switchport mode trunk acceptable-frame-type all
```

→ mirror 목적지 포트 및 TFM 입/출력 포트는 mds disable

→ ge4에서 수신된 패킷중 SIP가 192.1.1.2인 패킷은 ge1,ge2 포트로 복사하여 전송

→ ge4에서 수신된 패킷중 DIP가 192.1.1.2인 패킷은 ge3 포트로 전송

→ ge4에서 수신된 패킷중 SIP가 192.4.1.2인 패킷은 ge1 포트로 전송

→ ge1-4 포트는 TFM rule에 설정된 것 이외의 불필요한 트래픽을 받지 않도록 vlan 분리

→ ge13-14번의 egress mirror 트래픽은 vlan50, vlan60 tag 이므로 이들을 vlan20으로 변환

→ mirror 트래픽 이외의 불필요한 트래픽을 받지 않도록 vlan 분리

```

switchport trunk allowed vlan add 50
!
interface ge14
switchport access vlan 60
!
interface ge15
switchport access vlan 60
!
interface ge24
switchport mode trunk
switchport mode trunk acceptable-frame-type all
switchport trunk allowed vlan add 50,60
!

```

SG2124G#show ip monitor

IP monitor information.

SRC_PORTS				DST_PORTS			
IP_Protocol	Count	VLAN	Rate	Comment			
Source_MAC		Source_IP		SPort	Destination_MAC	Destination_IP	DPort
ge4				ge1-2			
any	8	any					
any		192.1.1.2		any	any		
ge4				ge3			
any	30	any					
any		any		any	any	192.1.1.2	any
ge4				ge1			
any	62	any					
any		192.4.1.2		any	any	any	any



주의

1. TFM rule과 match 되는 트래픽이 MDS에서 감지시 MDS의 우선 순위가 높기 때문에 TFM rule이 동작하지 못하므로 mirror 목적지 포트와 TFM의 입/출력 포트는 mds disable로 설정합니다.
2. 48 Port 장비에서는 Unit이 두 개로 나누어져 있기 때문에 동일 Unit상에 설정해야 합니다. (ge1-24, xe1 : Unit0 / ge25-48, xe2 : Unit1)



참고

1. SG2024 Series, SG2200 Series, SG2128G Series, SG2128GX Series, SG2152G Series, SG2152GX Series 제품은 ip monitor vlan-translate 기능을 지원하지 않습니다
2. IPv6 TFM 기능은 Switch버전 2.x 이상에서만 지원합니다.

1.6.17 Mode Button 설정

Switch 전면 부에 Mode Button을 사용하여 MDS 기능의 DETECT/DROP 설정을 변경하는 기능을 사용할 수 있습니다.

또한 Mode Button을 8초이상 길게 누르면 Switch가 Reset되는 기능을 활성화 할 수 있습니다.

Mode-button 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds mode-button enable	CONFIG	MDS 모드를 전면의 Mode-button 으로 DETECT/DROP 모드가 변경되도록 설정합니다.
reset mode-button enable	CONFIG	Mode-button을 길게 누르면 Switch가 reset하는 기능을 활성화합니다.

Mode-button 기능을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds mode-button enable	CONFIG	MDS 모드를 전면의 Mode-button 으로 DETECT/DROP 모드가 변경되도록 설정합니다.
reset mode-button enable	CONFIG	Mode-button을 길게 누르면 Switch가 reset하는 기능을 활성화합니다.



참고

SG2000 Series, SG2200 Series, SG2128G Series, SG2128GX Series, SG2152G Series, SG2152GX Series 제품은 Mode-button 기능을 지원하지 않습니다.

1.6.18 자체 검사 기능

Switch는 Config, Process, Hardware에 대한 자체 검사 기능을 제공합니다.

Switch는 주기적으로 설정파일 및 실행파일들에 대한 자체 검사를 수행하며, 무결성 검사 결과 파일이 훼손된 것으로 판단될 경우 해당 로그를 출력합니다.

자체 시험을 수행하는 대상 프로세스를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show process	TOP	자체 시험을 수행하는 시험 대상 프로세스 목록 정보를 확인합니다.

자체 시험 결과를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show self-test process	TOP	프로세스에 대한 자체검사 결과를 확인합니다.
Show self-test hardware	TOP	하드웨어에 대한 자체검사 결과를 확인합니다.

자체 무결성 검사를 수행하고 결과를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show integrity-check (process config)	TOP	자체 무결성 검사를 수행하고 결과를 출력합니다.

<예제1> 자체 시험 결과 확인

```
SG2024G#show self-test process
process self test result
  nsm daemon is running
  ripd daemon is running
  ripngd daemon is running
  ospfd daemon is running
```

```
ospf6d daemon is running
bgpd daemon is running
pimd daemon is running
pim6d daemon is running
authd daemon is running
lacpd daemon is running
stpd daemon is running
rstpd daemon is running
mstpd daemon is running
imi daemon is running
rmond daemon is running
lldpd daemon is running
sflow daemon is running
uipd daemon is running
pvstpd daemon is running
erpd daemon is running
snmpd daemon is running
inetd daemon is running
SG2024G#show self-test hardware
hardware self test result
Flash memory test success
Memory test success
Temperature is normal (37.5)
Fan status is normal
PSU status is normal
CPU load is normal
Memory usage is normal
SG2024G#
```

<예제2> 무결성 검사 결과 확인

```
SG2024G#show integrity-check config

- startup-config -
Original Hash : a9e115c742f10097933ba42011c659963c7edd5d1fe15805ec314576949919e5
Current Hash : a9e115c742f10097933ba42011c659963c7edd5d1fe15805ec314576949919e5
Compare Result : Success

SG2024G#show integrity-check process

- nsm -
Original Hash : 31eab8835236949f13a73753c4aacd0c1792d2c4fa1ae51c815d86e3c29aff7e
Current Hash : 31eab8835236949f13a73753c4aacd0c1792d2c4fa1ae51c815d86e3c29aff7e
Compare Result : Success

- lacpd -
Original Hash : 6e39655aaf76dc3d66c1259c1f4acd012af38a2ad98a0dfaacc36a662c0b68e3a
Current Hash : 6e39655aaf76dc3d66c1259c1f4acd012af38a2ad98a0dfaacc36a662c0b68e3a
Compare Result : Success

- stpd -
Original Hash : 19f78a6cc4775402aec411afdb02fd72b79f0bd858268caa42171c490c586081
Current Hash : 19f78a6cc4775402aec411afdb02fd72b79f0bd858268caa42171c490c586081
Compare Result : Success
```

```
- rstpd -
Original Hash : ed17d306b701e082e15c904f6200421aa7db71e46a20fc7c6d75e05d96deb2da
Current Hash : ed17d306b701e082e15c904f6200421aa7db71e46a20fc7c6d75e05d96deb2da
Compare Result : Success

- mstopd -
Original Hash : 52399af2660c04eb0901ce046a2eeeb85ebea4440101860353a0b7d5064a852c
Current Hash : 52399af2660c04eb0901ce046a2eeeb85ebea4440101860353a0b7d5064a852c
Compare Result : Success

- rmond -
Original Hash : 59528965a56c56db4afb3929e142c32dfe67ba47af0f33a3989a46af1dba8713
Current Hash : 59528965a56c56db4afb3929e142c32dfe67ba47af0f33a3989a46af1dba8713
Compare Result : Success

- lldpd -
Original Hash : 9fe8fee1c077f505d9372cd77aab7da6bb8ec34b6fb46a0aef900b68599bebf6
Current Hash : 9fe8fee1c077f505d9372cd77aab7da6bb8ec34b6fb46a0aef900b68599bebf6
Compare Result : Success

- sflow -
Original Hash : 990482a721903b9a8efe606836cc2e8537e91b248691f57343ab0e85894b7395
Current Hash : 990482a721903b9a8efe606836cc2e8537e91b248691f57343ab0e85894b7395
Compare Result : Success

- pvstopd -
Original Hash : 7bef03e316b063a47c09c6c7e79f329dfe86afb43530bd229a5f3568e262b159
Current Hash : 7bef03e316b063a47c09c6c7e79f329dfe86afb43530bd229a5f3568e262b159
Compare Result : Success

- erpd -
Original Hash : 593d5732ee3e370a32f212ce4f8627973ddd5154c85963fb54e855364d3952d2
Current Hash : 593d5732ee3e370a32f212ce4f8627973ddd5154c85963fb54e855364d3952d2
Compare Result : Success

- sensor -
Original Hash : 5d45169ccbfa815aee77837bc1f1c57677e10ccce84827dd202e70d4b6acdba2
Current Hash : 5d45169ccbfa815aee77837bc1f1c57677e10ccce84827dd202e70d4b6acdba2
Compare Result : Success
```

1.7 Interface

1.7.1 Interface 상태 정보

SG Switch Series에서는 Interface와 관련된 상태 정보를 확인하는 여러 가지의 명령어를 제공하고 있습니다. Interface가 Active상태인지 아닌지를 확인하는 것으로 회선의 연결 상태 등의 Interface의 Negotiation, 동작 상태를 확인하는 명령어, Interface의 Inbound / Outbound 된 사용량을 확인하는 명령어, 현재 연결되어 동작하는 Interface Type이 SFP Type인지 RJ45 Type인지를 확인하는 명령어, Interface에 관련된 Inbound / Outbound의 세부정보 및 Packet Error 발생 건수 등을 확인할 수 있는 명령어 등을 통해 확인된 결과값의 각종 Parameter 값을 이용해서 장애 처리 및 Network의 문제점 및 Interface에 사용되는 Packet의 처리량을 확인할 수 있습니다.

[표 1-14] Interface Default 설정

내용	기본설정
Interface 상태	동작 가능
Auto negotiation	Yes
Forward State	FORWARD
VLAN	VLAN1.1
Spanning Tree Protocol	RSTP Enable

Interface의 현재 설정 상태를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show port status [IFNAME]	TOP	Interface의 연결 상태 정보를 확인합니다.
show interface [IFNAME]	TOP	Interface 별 사용 정보를 확인합니다.
show interface media [IFNAME]	TOP	동작 중인 Interface Type을 확인합니다.
show interface stat [IFNAME]	TOP	Interface 별 error 등에 대한 세부 사용 정보를 확인합니다.
show interface switchport	TOP	Interface 별 switchport mode, VLAN 설정 정보 등을 확인합니다.
show interface bandwidth [IFNAME]	TOP	Interface의 Traffic 정보를 확인합니다.

Interface 세부 정보를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
clear interface stat [IFNAME]	TOP	Interface 별 error 등에 대한 세부 사용 정보를 초기화합니다.

<예제1> Interface 연결 상태 확인

```

SG2124G#show port status
ena/          auto forward learn inter      lastTime
port link  speed duplex nego   state  oper   face      linkChanged
=====
ge1    up    1g    FD   Yes   *      FA   SGMII    2012/06/04 13:30:52
ge2    up    1g    FD   Yes   *      FA   SGMII    2012/06/04 13:30:52
ge3    up    1g    FD   Yes   *      FA   SGMII    2012/06/04 13:30:52
ge4    down           HD   Yes   *      FA   SGMII
ge5    down           HD   Yes   *      FA   SGMII    2012/06/05 17:16:41
ge6    down           HD   Yes   *      FA   SGMII    2012/06/05 11:14:43
ge7    down           HD   Yes   *      FA   SGMII
ge8    down           HD   Yes   *      FA   SGMII
ge9    down           HD   Yes   *      FA   SGMII
ge10   down           HD   Yes   *      FA   SGMII
ge11   down           HD   Yes   *      FA   SGMII
ge12   down           HD   Yes   *      FA   SGMII
ge13   down           HD   Yes   *      FA   SGMII
ge14   down           HD   Yes   *      FA   SGMII
ge15   down           HD   Yes   *      FA   SGMII
ge16   down           HD   Yes   *      FA   SGMII
ge17   down           HD   Yes   *      FA   SGMII
ge18   down           HD   Yes   *      FA   SGMII
ge19   down           HD   Yes   *      FA   SGMII
ge20   down           HD   Yes   *      FA   SGMII
ge21   down           HD   Yes   *      FA   SGMII
ge22   down           HD   Yes   *      FA   SGMII
ge23   down           HD   Yes   *      FA   SGMII
ge24   down           HD   Yes   *      FA   SGMII
xe1    down           FD   No    *      FA   XGMII
xe2    down           FD   No    *      FA   XGMII
SG2124G#
SG2124G#show port status ge7
ena/          auto forward learn inter      lastTime
port link  speed duplex nego   state  oper   face      linkChanged
=====
ge1    up    1g    FD   Yes   *      FA   SGMII    2012/06/04 13:30:52
SG2124G#

```



참고

Learning operation의 상태 정보

F : SLF (Source Lookup Failure) packet 들을 forward하는 상태

A : SLF Packet 들을 Learn (L2 FDB 에 등록) 하는 상태

D : F, A 모두 설정되어 있지 않은 상태 (Disabled)

C : max-mac을 설정한 상태를 나타내며, max-mac을 지정하지 않은 경우나 max-mac으로 지정된 임계치에 도달된 경우에는 표시 안 됨.

<예제2> Interface 사용 정보 확인

SG2124G#show interface ge1

→ 특정 Interface 보기

```
Interface ge1
Hardware is Ethernet, address is 001a.f43c.000a (bia 001a.f43c.000a)
index 5001 metric 1 mtu 1500 duplex-full arp ageing timeout 0
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
Speed 1g
  input packets 2,242,185 bytes 174,305,858 dropped 0 multicast packets 379,294
  output packets 981,759 bytes 64,345,555 multicast packets 60,225 broadcast
  packets 916,556
  30 Sec  input rate 6 pkts/s, 558 bytes/s, 0.00 percent utilization
  30 Sec output rate 3 pkts/s, 373 bytes/s, 0.00 percent utilization
Linktrap Enabled
```

SG2124G#show interface

→ 전체 Interface 보기

```
Interface ge1
Hardware is Ethernet, address is 001a.f43c.000a (bia 001a.f43c.000a)
index 5001 metric 1 mtu 1500 duplex-full arp ageing timeout 0
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
Speed 1g
  input packets 2,242,715 bytes 174,353,806 dropped 0 multicast packets 379,402
  output packets 982,063 bytes 64,375,129 multicast packets 60,239 broadcast
  packets 916,696
  30 Sec  input rate 7 pkts/s, 615 bytes/s, 0.00 percent utilization
  30 Sec output rate 3 pkts/s, 420 bytes/s, 0.00 percent utilization
Linktrap Enabled

Interface ge2
Hardware is Ethernet, address is 001a.f43c.000a (bia 001a.f43c.000a)
index 5002 metric 1 mtu 1500 duplex-full arp ageing timeout 0
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
Speed 1g
  input packets 776,686 bytes 61,401,395 dropped 0 multicast packets 386,202
  output packets 2,512,995 bytes 192,436,989 multicast packets 321,913 broadcast
  packets 78,288
  30 Sec  input rate 1 pkts/s, 140 bytes/s, 0.00 percent utilization
```

```

30 Sec output rate 7 pkts/s, 659 bytes/s, 0.00 percent utilization
linktrap Enabled

-----
Interface ge3
Hardware is Ethernet, address is 001a.f43c.000a (bia 001a.f43c.000a)
index 5003 metric 1 mtu 1500 duplex-full arp ageing timeout 0
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
Speed 1g
  input packets 121,954 bytes 9,609,965 dropped 0 multicast packets 340,497
  output packets 3,095,725 bytes 229,818,539 multicast packets 275,510 broadcast
  packets 23,055
  30 Sec input rate 0 pkts/s, 114 bytes/s, 0.00 percent utilization
  30 Sec output rate 9 pkts/s, 757 bytes/s, 0.00 percent utilization
linktrap Enabled
-----
-- 이하 생략 --

```

<예제3> Interface 세부 사용 정보 확인

```

SG2124G#show interface stat ge1
=====
Interface ge1
-----
ifInOctets      : 174,374,822
ifInUcastPkts   : 1,006,997
ifInNUcastPkts  : 1,235,988
ifInDiscards    : 13,935
ifInErrors      : 0
ifInUnknownProtos : 0
-----
ifOutOctets      : 64,391,658
ifOutUcastPkts   : 865,248
ifOutNUcastPkts  : 116,966
ifOutDiscards    : 155,090
ifOutErrors      : 0
ifOutQLens       : 0
-----
EtherStatsPkts64to127Octets : 2,893,297
EtherStatsPkts128to255Octets : 213,836
EtherStatsPkts256to511Octets : 69,568
EtherStatsPkts512to1023Octets : 18,833
EtherStatsPkts1024to1518Octets : 28,510
EtherStatsPkts1519toMaxOctets : 1,155
-----
Dot1dTpPortInFrames : 2,242,985
Dot1dTpPortOutFrames : 982,214
Dot3StatsInternalMacTransmitErrors : 0
Dot3StatsExcessiveCollisions : 0
Dot3StatsInternalMacReceiveErrors : 0
Dot3StatsLateCollisions : 0
IfHCOutMulticastPkts : 60,246
IfHCInBroadcastPkts : 916,779
EtherStatsBroadcastPkts : 973,499
EtherStatsMulticastPkts : 379,455
EtherStatsDropEvents : 0

```



```

EtherStatsUndersizePkts      :      0
EtherStatsFragments          :      0
EtherStatsOversizePkts      :      0
EtherStatsJabbers            :      0
EtherStatsCRCAlignErrors     :      0
EtherStatsCollisions         :      0
SG2124G#

```



참고

1. CRC Error가 발생하는 경우 : 연결된 **Cable**이 불량인 경우
2. Collisions Error가 발생하는 경우 : 상대방 장비와 **Negotiation**이 올바르게 설정되지 않은 경우

<예제4> Interface Media Type 확인

```

SG2124G#show interface media
Interface: ge1 Active medium: -
Interface: ge2 Active medium: -
Interface: ge3 Active medium: Copper
Interface: ge4 Active medium: -
Interface: ge5 Active medium: Copper
Interface: ge6 Active medium: -
Interface: ge7 Active medium: -
Interface: ge8 Active medium: -
Interface: ge9 Active medium: -
Interface: ge10 Active medium: Copper
Interface: ge11 Active medium: -
Interface: ge12 Active medium: -
Interface: ge13 Active medium: -
Interface: ge14 Active medium: -
Interface: ge15 Active medium: Copper
Interface: ge16 Active medium: Copper
Interface: ge17 Active medium: -
Interface: ge18 Active medium: -
Interface: ge19 Active medium: -
Interface: ge20 Active medium: -
Interface: ge21 Active medium: -
Interface: ge22 Active medium: -
Interface: ge23 Active medium: Fiber
Interface: ge24 Active medium: Copper
SG2124G#

```



참고

SG2124G Series는 Combo Interface(SG2124G ge21-24, SG2148G ge45-48, SG2124GXF ge13-24)에 Copper 및 SFP Interface에 동시에 연결한 경우 SFP Interface 가 Copper Interface 보다 우선 인식됩니다.

<예제5> Interface 세부 설정 내용 확인

```

SG2124G#show interface switchport
Interface Switchport Ingress Acceptable Default Configured

```

name	mode	filter	frame type	Vlan	Vlans
ge1	access	disable	all	1	1
ge2	access	disable	all	30	30
ge3	hybrid	disable	all	1	1,20
ge4	hybrid	disable	all	1	1,20
ge5	access	disable	all	1	1
ge6	access	disable	all	1	1
ge7	access	disable	all	1	1
ge8	access	disable	all	1	1
ge9	access	disable	all	1	1
ge10	access	disable	all	1	1
ge11	access	disable	all	1	1
ge12	access	disable	all	1	1
ge13	access	disable	all	1	1
ge14	access	disable	all	1	1
ge15	access	disable	all	1	1
ge16	access	disable	all	1	1
ge17	access	disable	all	1	1
ge18	access	disable	all	1	1
ge19	access	disable	all	1	1
ge20	access	disable	all	1	1
ge21	access	disable	all	1	1
ge22	access	disable	all	1	1
ge23	access	disable	all	1	1
ge24	trunk	disable	all	1	1,2,3,4, 5,6,7,8

SG2124G#

<예제6> Interface Bandwidth 사용현황 확인

SG2124G#show interface bandwidth ge23

port name	time	receive pkts/s	receive bytes/s	receive bits/s	sent pkts/s	sent bytes/s	sent bits/s
ge23	5s	1	68	544	0	57	456
ge23	30s	0	56	448	0	87	696
ge23	1m	0	68	544	0	160	1,280
ge23	5m	0	49	392	0	128	1,024
ge23	15m	0	34	272	0	60	480
ge23	60m	0	27	216	0	20	160

SG2124G#

1.7.2 Interface 활성화 / 비활성화

Cable이 연결되어 물리적으로는 활성화 상태인 Interface를 논리적으로 비활성화 상태로 만들 수 있습니다.

활성화 상태인 Interface를 비활성화 상태로 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
shutdown	INTERFACE	Interface를 비활성화 상태로 설정합니다.

Interface가 활성화/비활성화 상태인지 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show port status <i>IFNAME</i>	TOP	연결 상태 정보를 통해 Interface의 활성화 상태를 확인합니다.
show running-config interface <i>IFNAME</i>	TOP	설정 상태를 통해 Interface의 활성화 상태를 확인합니다.

비활성화 상태로 설정했던 Interface를 다시 활성화시키려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no shutdown	INTERFACE	Interface를 활성화 상태로 설정합니다.

<예제> Interface 활성화/비활성화

```
SG2124G#configure terminal
SG2124G(config)#interface ge9
SG2124G(config-if)#shutdown
SG2124G(config-if)#end
SG2124G#show port status ge9
      ena/          auto forward learn   inter      lastTime
port link  speed duplex  nego    state   oper    face      linkChanged
=====
ge9    !ena          HD   Yes    -      FA     SGMII  2009/04/13 22:25:55
SG2124G#
SG2124G#show running-config interface ge9
!
```

```

interface ge9
shutdown
!
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge9
SG2124G(config-if)#no shutdown
SG2124G(config-if)#end
SG2124G#
SG2124G#show port status ge9
      ena/          auto forward learn inter          lastTime
port link  speed duplex  nego   state   oper    face          linkChanged
=====
ge9     up   100m     FD   Yes  FORWARD   FA   SGMII  2009/04/13 22:27:53
SG2124G#
SG2124G#show running-config interface ge9
!
interface ge9
!
SG2124G#

```



참 고

Interface의 상태가 “!ena”로 표시되면서 비활성화 상태인 경우, 물리적인 Link는 연결되나 실제 사용할 수는 없습니다.

1.7.3 Interface Negotiation 설정

Switch의 Interface는 연결된 장비의 전송 속도와 Duplex 모드에 자동으로 맞추어 동작하는 Auto Negotiation 기능이 Default로 설정되어 있습니다.

Interface의 전송 속도 및 Duplex 모드를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
speed {10m 100m 1g}	INTERFACE	Interface의 Auto Negotiation을 중지하고 전송 속도를 설정합니다.
duplex {full half}	INTERFACE	Interface의 Auto Negotiation을 중지하고 duplex 모드를 설정합니다.

Interface의 전송 속도 및 Duplex 모드를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show port status <i>IFNAME</i>	TOP	연결 상태 정보를 통해 Interface의 전송 속도 상태를 확인합니다.
show running-config interface <i>IFNAME</i>	TOP	설정 상태를 통해 Interface의 전송 속도 상태를 확인합니다.

Interface의 전송 속도 및 Duplex 모드를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
duplex auto	INTERFACE	Negotiation 상태를 Auto로 변경합니다.
speed auto	INTERFACE	Negotiation 상태를 Auto로 변경합니다.



참고

1. Speed 및 Duplex를 설정한 Interface는 Auto Negotiation 기능이 No로 설정됩니다.
2. Auto Negotiation 기능이 Yes로 설정되지 않은 Interface는 Auto MDIX를 지원하지 않으며, Auto MDIX를 이용하기 위해서는 mdix force-auto를 선택하여야 합니다. (1.7.4 Interface MDIX 설정 참조)
3. Fiber Media Ethernet의 경우 Full Duplex로만 동작하므로 Duplex 모드를 변경할 수 없습니다.

<예제> Interface에 Negotiation 설정

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge9
SG2124G(config-if)#speed 10m
SG2124G(config-if)#end
SG2124G#
SG2124G#show port status ge9
      ena/          auto forward learn inter      lastTime
port link  speed duplex nego   state oper    face      linkChanged
=====
ge9      up    10m    FD   Yes FORWARD   FA   SGMII  2009/04/13 22:34:07
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge9
SG2124G(config-if)#duplex full
SG2124G(config-if)#end
SG2124G#
SG2124G#show port status ge9
      ena/          auto forward learn inter      lastTime
port link  speed duplex nego   state oper    face      linkChanged
=====
ge9      up    10m    FD   No  FORWARD   FA   SGMII  2009/04/13 22:35:23
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge9
SG2124G(config-if)#duplex auto
SG2124G(config-if)#speed auto
SG2124G(config-if)#end
SG2124G#
SG2124G#show port status ge9
      ena/          auto forward learn inter      lastTime
port link  speed duplex nego   state oper    face      linkChanged
=====
ge9      up    100m   FD   Yes FORWARD   FA   SGMII  2009/04/13 22:36:37
SG2124G#

```

1.7.4 Interface MDIX 설정

Direct를 나타내는 MDI (Medium Dependent Interface)와 Cross를 나타내는 MDIX (MDI Cross)가 있습니다. 일반적으로 동일 기종 장비 간의 연결일 때는 Cross Cable로 연결하며 서로 다른 기종간의 연결은 Direct Cable을 사용하여 연결합니다.

Interface에는 Auto MDIX가 설정되어 있어 Switch와 연결되는 Cable Type에 상관없이 사용할 수 있도록 되어 있습니다. 그러나 Interface의 설정을 변경하여 Auto MDIX가 Disable 상태로 동작하는 경우에는 Cable Type을 관리자가 확인하여야 합니다.

관리자는 Interface의 MDIX 명령을 통해 Interface에 연결되는 Cable의 Type을 강제로 설정하여 운영할 수 있습니다.

Interface의 MDIX 동작 모드를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mdix force-auto	INTERFACE	Negotiation과 상관없이 항상 Auto MDIX로 동작하도록 설정합니다. (Default)
mdix normal	INTERFACE	Auto MDIX를 Disable 하며, 항상 MDI로 동작하도록 설정합니다.
mdix xover	INTERFACE	Auto MDIX를 Disable 하며, 항상 MDIX로 동작하도록 설정합니다.

Interface의 MDIX 동작 모드를 확인하려면 다음 명령어를 사용하십시오

명령어	모드	기능
show running-config interface <i>IFNAME</i>	TOP	Interface의 설정 상태를 통해 MDIX 설정 상태를 확인합니다.
show port mdix	TOP	MDIX 설정 상태를 확인합니다.

Interface의 MDIX 동작 모드를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mdix auto	INTERFACE	mdix 설정 모드를 초기화합니다.

**참고**

Gigabit Ethernet Interface의 MDIX 설정은 force-auto를 Default로 지원하고 있어 Negotiation을 조정하는 경우에도 MDI 및 MDIX Cable을 혼용하여 사용할 수 있습니다.

<예제> Interface에 MDIX 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge9
SG2124G(config-if)#mdix xover
SG2124G(config-if)#show running-config interface ge9
!
interface ge9
  mdix xover
!
SG2124G(config-if)#
SG2124G(config-if)#mdix normal
SG2124G(config-if)#show running-config interface ge9
!
interface ge9
  mdix normal
!
SG2124G(config-if)#
SG2124G(config-if)#mdix force-auto
SG2124G(config-if)#show running-config interface ge9
!
interface ge9
  mdix force-auto
!
SG2124G(config-if)#
SG2124G(config-if)#mdix auto
SG2124G(config-if)#show running-config interface ge9
!
interface ge9
!
SG2124G(config-if)#
```


1.7.5 MTU 설정

MTU (Maximum Transmission Unit)는 Ethernet 환경에서 허용되는 Packet의 최대 전송 단위로 Ethernet에서 허용되는 범위는 64Byte~1,518Byte입니다. Network 장비들은 해당 범위 이상이거나 이하인 Packet을 수신하는 경우 해당 Packet은 무시되며, MTU값을 설정하면 1,518Byte보다 큰 Jumbo Frame을 수신할 수 있습니다.

Interface의 MTU 값을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mtu <64-9208>	INTERFACE	MTU 값을 설정합니다.

Interface에 설정된 MTU 값을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show running-config interface <i>IFNAME</i>	TOP	Interface의 설정 상태를 통해 설정된 MTU 값을 확인합니다.

Interface에 설정된 MTU 값을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mtu	INTERFACE	MTU 값을 초기화합니다.

<예제> Interface에 MTU 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge9
SG2124G(config-if)#mtu 9208
SG2124G(config-if)#show running-config interface ge9
!
interface ge9
mtu 9208
!
SG2124G(config-if)#no mtu
SG2124G(config-if)#show running-config interface ge9
!
interface ge9
```

```
!  
SG2124G(config-if)#
```



Default MTU 값은 1500 Frame입니다.

1.7.6 Flow Control 설정

Switch의 Ethernet Interface는 수신 Buffer에 여유 공간이 없으면 일정 시간 동안 Packet 전송을 제한하기 위해 송신 Interface에게 일정 시간 동안 Packet 전송을 중단하라는 중지 Message를 보냅니다. Ethernet Interface 역시 다른 시스템으로부터 중지 Message를 받으면 일정 시간 동안 Packet 전송을 중단합니다.

Ethernet Interface에 전송 중지 신호(Flow Control)를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
flowcontrol [receive send] [on off]	INTERFACE	전송 중지 신호를 보내는 기능을 설정합니다.

Interface에 설정된 Flow Control을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show running-config interface <i>IFNAME</i>	TOP	Interface의 설정 상태를 통해 Flow Control의 설정 상태를 확인합니다.

Interface에 설정된 Flow Control을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no flowcontrol	INTERFACE	전송 중지 신호를 보내는 기능을 삭제합니다.

<예제> Flow Control 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge9
SG2124G(config-if)#flowcontrol receive on
SG2124G(config-if)#show running-config interface ge9
!
interface ge9
  flowcontrol receive on
!
SG2124G(config-if)#no flowcontrol
SG2124G(config-if)#show running-config interface ge9
!
interface ge9
!
```

1.7.7 Interface 사용량 확인

Switch의 관리자는 각 Interface의 5 s, 30 s, 1 min, 5 min, 15 min, 60 min 평균 Traffic을 확인할 수 있습니다.

각 Interface의 평균 Traffic을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show bandwidth [IFNAME]	TOP	Interface별 평균 Traffic을 확인합니다.
show [interface] bandwidth [IFNAME]	TOP	Interface별 평균 Traffic을 확인합니다.

<예제> Interface별 사용량 확인

SG2124G#show bandwidth ge24

port name	time	receive pkts/s	receive bytes/s	receive bits/s	sent pkts/s	sent bytes/s	sent bits/s
ge24	5s	116	122,738	981,904	82	12,715	101,720
ge24	30s	69	75,802	606,416	48	9,432	75,456
ge24	1m	62	73,188	585,504	41	9,142	73,136
ge24	5m	50	81,265	650,120	31	14,006	112,048
ge24	15m	46	97,117	776,936	29	19,264	154,112
ge24	60m	46	97,552	780,416	28	20,846	166,768



참고

1. receive : Switch가 받는 Traffic량
2. sent : Switch가 내보낸 Traffic량

1.7.8 Port Mirroring 설정

Port Mirroring은 지정된 하나의 Interface에서 모니터링 대상으로 지정된 하나 이상의 Interface를 통해 전송되는 모든 Packet을 복사하여 모니터링 할 수 있도록 하는 기능입니다.

Port Mirroring은 최대 4개(SG2200 Series 는 1개)까지 사용할 수 있으며, 모니터링 대상으로 지정된 Interface는 중복해서 설정할 수 없습니다.

Port Mirroring을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mirror interface <i>PORTRANGE</i> direction {both receive transmit}	INTERFACE	모니터링 할 Interface 범위 및 Packet 전송 방향을 지정합니다.

Interface에 설정된 Port Mirroring을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mirror	TOP	Port Mirroring 설정 상태를 확인합니다.
show running-config interface <i>IFNAME</i>	TOP	Interface의 설정 상태를 통해 Port Mirroring 설정 상태를 확인합니다.

Interface에 설정된 Port Mirroring을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mirror interface <i>PORTRANGE</i> [direction {receive transmit}]	INTERFACE	Port Mirroring 설정을 해제합니다.

<예제> Port Mirroring 설정

```
SG2124G(config)#interface ge9
SG2124G(config-if)#mirror interface ge1 direction both
SG2124G(config-if)#end
SG2124G#show running-config interface ge9
!
interface ge9
 mirror interface ge1 direction both
!
```

1.7.9 Power Saving (Green IT)

Power Saving은 Link Down된 Interface에 대해 Auto 또는 Schedule에 의해 Interface에 공급되는 전력을 강제로 Power Down하여 최대 70%이상의 전력 절감 효과로 Green IT를 실현할 수 있는 기능입니다.

■ Auto Mode

Interface가 Link Down되는 경우 Interface를 Power Down하며, Link Up되는 경우에는 자동으로 Power Up 해주는 기능

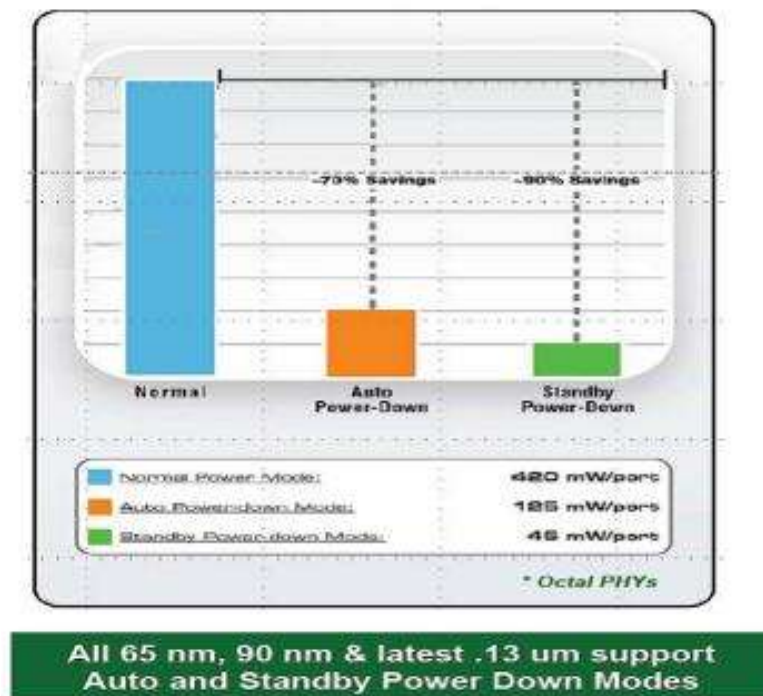
■ Schedule Mode

시간과 요일, 지속시간, Interface를 지정하여 지정된 시간에 Link Down된 Interface를 강제로 Power Down 해주는 기능

■ Recover Interval

Schedule Mode 사용 중이라도 Link Up되는 Interface에는 Power Up이 될 수 있도록 Link Up Interface가 존재하는지 주기적으로 감시하는 시간

[그림 1-2] Power Saving



Interface에 Power Saving을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
power-saving auto <i>PORTRANGE</i>	CONFIG	Power Saving Auto Mode를 설정할 Interface 범위를 선택합니다.
power-saving Rule_No Day Start_Time Duration <i>PORTRANGE</i>	CONFIG	Power Saving Schedule을 설정할 Interface 범위를 선택합니다.
power-saving recovery <i>Interval</i>	CONFIG	Power Saving Schedule 설정 시 Link-Up Check Interval을 설정합니다.

Power Saving의 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show power-saving	TOP	Port Redundancy Group을 확인합니다.

Interface에 설정된 Power Saving을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no power-saving auto <i>PORTRANGE</i>	CONFIG	Power Saving Auto Mode 설정을 초기화합니다.
no power-saving Rule_No	CONFIG	Power Saving Schedule 설정을 초기화합니다.
no power-saving recovery	CONFIG	Power Saving Link-Up Check Interval 설정을 초기화합니다.



참고

Power Saving을 Schedule mode로 설정한 후 recovery Interval을 설정하지 않은 경우에는 Schedule에 지정된 시간 내에 한 번이라도 Link-Down된 Interface는 Power-Down되어 Host가 정상 연결되어도 Power-Down 상태를 유지합니다.

<예제> Power Saving 설정

ge1-4 : 19 h부터 5 h 동안 절전 기능 사용. Link-Up Check 주기는 60 s로 설정

ge5-8 : Auto Power Saving Mode로 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#power-saving auto ge5-8
SG2124G(config)#power-saving 10 0 19:00 300 ge1-4
SG2124G(config)#power-saving recovery 60
SG2124G(config)#end
SG2124G#show power-saving
```

Recovery Inteval : 60 sec

Rule	Days	ApplyTime	Minute	PortRange
10	AllDay	19:00	300	ge1-4

Port	Static-Power-Down	Auto-Power-Down
ge1	PowerDown	Disable
ge2	PowerDown	Disable
ge3	PowerDown	Disable
ge4	PowerDown	Disable
ge5	Disable	PowerDown
ge6	Disable	PowerDown
ge7	Disable	PowerDown
ge8	Disable	PowerDown
ge9	Disable	Disable
ge10	Disable	Disable
ge11	Disable	Disable

-- 이하 생략 --

SG2124G#

Power Saving Interface Statistics



참고

Schedule Waiting : Schedule로 동작하기 위한 대기 상태의 Interface (Schedule로 지정되지 않은 시간)

Linkdown Waiting : Interface가 Link-Up인 상태

PowerDown : Interface가 Link-Down되어 Power Down된 상태

Disable : Power Saving이 설정되지 않은 상태

1.7.10 PoE 기능

PoE(Power Over Ethernet)를 지원하는 SG Switch Series는 10/100/1000Mbps Interface에 대해 IEEE802.3AF/AT 산업 표준의 PoE 기능을 제공하며 기존 Ethernet Cable을 통해 별도의 전원공급 장치 없이 전력을 공급할 수 있습니다.

따라서 추가 Power Cable과 주위의 외부 전원 장치 없이 무선 Access Point 및 IP 기반 감시용 웹 카메라, VoIP Phone 등에 Ethernet Cable 만을 연결하여 직접 전력을 공급함으로써 Network 장치를 최적의 장소(천정 또는 실외 등)에 위치시킬 수 있습니다.

다른 PoE 지원 장비와 연결 시 자동 인식하여 전원을 공급할 수 있으며 PoE 장비와의 연결이 끊어졌을 때에는 전원을 자동으로 차단합니다. 또한 Auto MDIX 기능을 통해 Speed, Cable Type, Duplex 등을 자동으로 인식하고 최적의 Network 상태로 맞추어 줍니다.

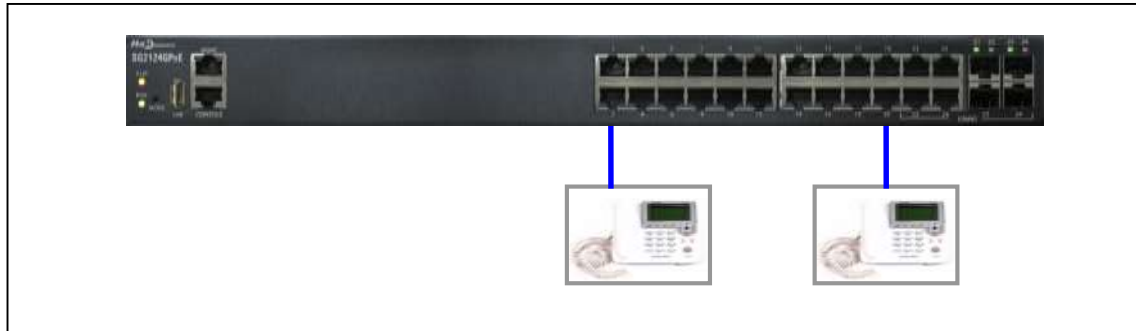
Factory Option으로 제공되는 Option SMPS를 추가 장착한 SG Switch Series/2의 경우 전원을 이중으로 구성하여 한쪽 Power Supply에 Power Cable 제거 등으로 인한 장애가 발생하여도 다른 쪽 Power Supply에서 원활하게 전원을 공급할 수 있습니다. Power Redundancy 기능은 안정적인 네트워크 서비스를 구성할 수 있어 장비의 신뢰도를 높여줍니다.

- **auto-power-up(Power Failure 시 PoE 전원 공급 자동 재시작 여부 선택)**
Default (Disable)일 때 Failure 상태가 되면 PoE LED가 계속 점등하며, Cable의 제거 여부와 상관없이 관리자가 직접 PoE 를 disable/enable 하여야만 다시 사용할 수 있음
- **classification (연결된 PD의 Class에 대한 classification type 선택)**
none일 경우 classification 수행치 않음.
- **detection-type (Point Check)**
PSE와 PD는 PoE Link 연결 시 2.8V~10V 사이에서 Negotiation을 할 때 몇 Point를 Check할 것인지를 구분하여 2-Point or 4-Point Detection을 구분.
- **disconnect-type (PSE와 PD 사이에 Disconnect 상태를 인식하기 위한 방법 선택)**
DC-Disconnect: 전류량이 5~10 mA이며 300~400 ms 지속 시 PoE Link를 끄는 방법
AC-Disconnect : PSE와 PD가 연결된 구간의 임피던스를 기준으로 |27K-ohm|이하이면 Link 를 지속시키고, |1.98K-ohm|이면 PoE Link를 끄는 방법 (SG2200 Series 지원안함)
- **limit (Interface별 전류량 제한 방법 선택)**
Class : classification 단계를 거쳐 얻어진 class값 기반으로 전류량을 제한.
User : 사용자가 설정한 값 기반으로 전류량을 제한.
- **Threshold (limit threshold값)**
limit user 상태에서 사용하는 Threshold 값. (W 단위, Default 15.4, 최대 16)

■ power-up-mode (High Power Mode)

High Power Mode 에서 사용되는 기능으로 802.1af 기반의 장비에서는 사용되지 않음.
(802.3at의 기능을 제공하기 위해 사용되는 명령어)

[그림 1-3] PoE 연결 구성



802.3at 를 지원하는 Switch는 다음과 같은 규격 중 하나를 지원해야 합니다.

1) 802.3AT PSE, PD 요약 정보

IEEE802.3AT 규격에 의하면 802.3AT PSE(Power Sourcing Equipment)는 아래 3가지 classification 방식 중 하나를 지원해야 합니다.

- 1) 2-Event PHY classification + No LLDP classification
- 2) 2-Event PHY classification + LLDP classification
- 3) 1-Event PHY classification + LLDP classification

SG2128G/SG2128GX/SG2152G/SG2152GX/SG2212G/SG2220G Series 802.3at 지원 스위치는 1~3번 방식을 모두 지원합니다. 이외 나머지 SG21xx/SG22xx Series 802.3at 지원 스위치는 3번 방식을 지원합니다.

PD(Powered Device)는 2-Event PHY classification과 LLDP classification을 모두 지원해야 합니다.

Configuration via Ethernet layer 2 (LLDP)의 구조

LLDP - MED Advanced Power Management							
TLV Header		MED Header		Extended power via MDI			
Type (7 bits)	Length (9 bits)	TIA OUI (3 octets)	Extended power via MDI subtype (1 octet)	Power type (2 bits)	Power source (2 bits)	Power priority (4 bits)	Power value (2 octets)
127	7	00-12-BB	4	PSE or PD	Nomal or Backup conservation	Critical, High, Low	0 - 102,3W in 0,1 steps

■ LLDP (link layer Discovery Protocol (링크계층 탐색 프로토콜))

보고되는 망 정보를 단순히 수집하여 활성화된 망의 현 상태를 탐색

■ MED (Media Endpoint Discovery)

미디어 종점 검색

■ MDI (Medium Dependent Interface)

이더넷에서 사용하는 Connection 종류(Straight-through or Crossover)를 검색, 즉 컨넥터와 같은 실제 접속부

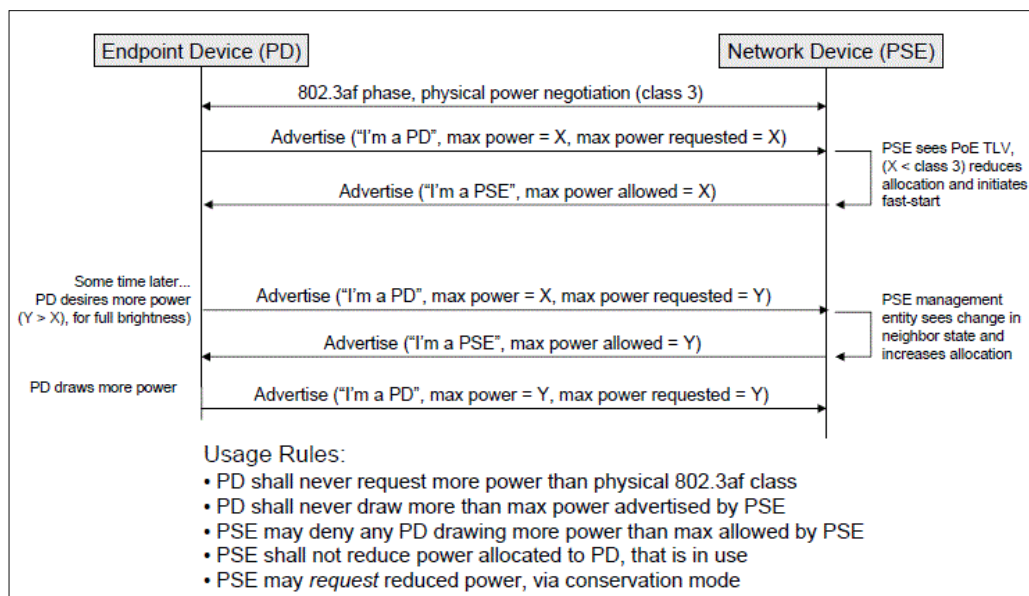
■ TLV (Type Length Value)

데이터의 타입, 데이터의 길이, 데이터의 내용

■ TIA (Telecommunications Industry Association)

■ OUI (Organizationally Unique Identifier)

IEEE에서 MAC(Media Access Control) 주소할당 받아 사용하는 제조사 주소



< LLDP 사용 시 Power Nego 과정 >

802.3at를 지원하는 SG 시리즈 PoE에서 최적의 802.3at를 사용하려면 다음과 같이 설정해 주시기 바랍니다.

<예제> 802.3at 사용을 위한 LLDP 설정

```

SG2124GP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124GP(config)#lldp enable
SG2124GP(config)#lldp port both ge1-24
SG2124GP(config)#lldp tlv dot3tlv power-via-mdi ge1-24
SG2124GP(config)#interface range ge1-24
% ge Selected
SG2124GP(config-if-range)#poe classification 8023af
SG2124GP(config-if-range)#end
SG2124GP#

```

- PoE를 지원하는 SG Switch Series는 Alternate A MDIX를 지원하며 Alternate A MDI와 Alternate B Type의 PoE는 지원되지 않습니다.
 - Alternate A Type : UTP 1,2,3,6에 Data와 전원을 함께 공급하는 방식
 - ◇ UTP 1,2포트 (Positive Vport),
UTOP 3,6 포트 (Negative Vport)
 - ◇ UTP 1,2포트 (Negative Vport),
UTOP 3,6 포트 (Positive Vport)
 - Alternate B Type : UTP 1,2,3,6에 Data, 4,5,7,8에 전원을 공급하는 방식
- POE 상태가 Other fault인 경우는 다음과 같습니다.
 - MPS absent : Cable 단선이 감지된 경우
 - Short : 425 mA 이상의 전류가 감지된 경우
 - Overload : 63 ms 이상 Interface의 전력 한계치를 초과한 경우
 - Power denied : 시스템 전력이 부족한 경우
- PoE Class에 따라 지원되는 전력량은 다음과 같습니다.
 - Class 0 : 0.44 ~ 12.94 W
 - Class 1 : 0.44 ~ 3.84 W
 - Class 2 : 3.84 ~ 6.49 W
 - Class 3 : 6.49 ~ 12.95 W
 - Class 4 : (PSE's classify as Class 0)
- PoE Classification
 - 1-Event classification: 802.3AF에서 사용하던 하나의 전압 펄스를 이용해 PD class를 확인하는 방식
 - 2-Event classification: 802.3AT에서 사용하는 두개의 전압 펄스를 이용해 PD class를 확인하는 방식
 - LLDP classification: 1-Event classification 방식으로 PSE -PD간 class 확인후, PD에서 13W 이상의 전력이 필요할 경우 LLDP nego를 통해 25.5W까지의 전력을 요청하는 방식
- LLDP nego시 LLDPDU 내에 Power-Via-MDI TLV 메시지 포맷을 사용합니다.



참고

6. SG2000 Series 제품은 IEEE802.3AF 표준 PoE만 지원합니다.

PoE와 관련된 세부 설정을 변경하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
poe pm-mode {dynamic dynamic -wop none static static-wop}	CONFIG	Power Management mode를 설정합니다. (Default: dynamic)
poe auto-recovery {enable disable}	CONFIG	Linkup시 자동으로 PoE오류를 복구시키는 기능을 사용할 것인지 설정합니다.
poe auto-power-up {disable enable}	INTERFACE	과전류 요청 등으로 인한 PoE 포트 자동 Disable시 자동 reset 여부를 선택합니다. (Default: disable)
poe classification {8023af none}	INTERFACE	PoE Class를 설정합니다. (Default: 802.3af)
poe detection-type {2-point 2-point-legacy 4-point 4-point-legacy legacy none}	INTERFACE	PoE 디바이스를 검출하는 방식을 설정합니다. (Default: 4-point)
poe disconnect-type {ac dc none}	INTERFACE	PoE 전원의 차단 방식을 설정합니다. (Default: ac)
poe {disable enable}	INTERFACE	PoE 기능을 사용여부를 설정합니다. (Default: enable)
poe limit {class none user}	INTERFACE	PoE 전력의 Limit를 설정합니다. (Default: none)
poe power-up-mode {high-power normal}	INTERFACE	High Power 모드를 설정합니다. (Default: normal)
poe priority {critical high low normal}	INTERFACE	INTERFACE별로 PoE 전력을 할당 받기 위한 우선 순위를 설정합니다. (Default: normal)

PoE Interface의 상태를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show poe [interface [IFNAME] brief detail]	TOP	PoE 설정 내용을 확인합니다.

Interface에 PoE 기능을 비활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
poe disable	INTERFACE	PoE 기능을 사용하지 않도록 설정합니다.
no poe auto-power-up	INTERFACE	PoE 포트 자동 Disable시 자동 reset 기능을 초기화 합니다.
no poe classification	INTERFACE	PoE Class를 초기화합니다.
no poe detection-type	INTERFACE	PoE 디바이스를 검출하는 방식을 초기화합니다.
no poe disconnect-type	INTERFACE	PoE 전원의 차단 방식을 초기화합니다.
no poe limit	INTERFACE	PoE 전력의 Limit 설정을 초기화합니다.
no poe power-up-mode	INTERFACE	High Power 모드 설정을 초기화합니다.
no poe priority	INTERFACE	PoE 전력을 할당 받기 위한 우선 순위를 설정을 초기화합니다.
no poe threshold	INTERFACE	PoE 전력의 지정 값을 초기화합니다.

<예제> PoE Interface 상태 보기

SG2124GP#show poe

Port	Power Enable	Limit Type	Priority	Detection Status	Power Class	Power
ge1	Yes	None	Low	Searching	N/A	0.0W
ge2	Yes	None	Low	Searching	N/A	0.0W
ge3	Yes	None	Low	Searching	N/A	0.0W
ge4	Yes	None	Low	Searching	N/A	0.0W
ge5	Yes	None	Low	Searching	N/A	0.0W
ge6	Yes	None	Low	Delivering	0	3.4W
ge7	Yes	None	Low	Searching	N/A	0.0W
ge8	Yes	None	Low	Searching	N/A	0.0W

ge9		Yes		None		Low		Searching		N/A		0.0W
ge10		Yes		None		Low		Delivering		0		3.4W
ge11		Yes		None		Low		Searching		N/A		0.0W
- 중 략 -												
ge23		Yes		None		Low		Searching		N/A		0.0W
ge24		Yes		None		Low		Searching		N/A		0.0W

Total Power											:	6.8W

SG2124GP#												

1.7.11 UDLD 설정

UDLD(UniDirectional Link Detection)기능은 CABLE 상의 전기적 Signal은 정상이나 장비 양단간에 L2 Frame을 서로 주고 받지 못하는 경우가 있어 이를 Detect 하기 위한 기능입니다.

예를 들어 SFP로 연결된 2 Core Fiber Cable중에 RX 1Core는 정상이나 다른 TX 1Core에 이상이 있는 경우 Link는 RX를 수신하였기 때문에 정상적으로 표시되나 실제 Traffic은 전송되지 못하는 경우 UDLD 기능이 enable 되어 있으면 이를 진단하여 상태를 표시합니다.

UDLD와 관련된 세부 설정을 변경하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
udld port	INTERFACE	해당 Port의 UDLD기능을 enable 합니다. (Default: normal)
udld port aggressive	INTERFACE	해당 Port의 UDLD mode를 aggressive mode로 변경합니다.

UDLD Interface의 상태를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show udld [IFNAME]	TOP	UDLD 설정 내용을 확인합니다.

UDLD 기능을 비활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no udld port	INTERFACE	UDLD기능을 사용하지 않도록 설정합니다.
no udld port aggressive	INTERFACE	aggressive mode를 해제합니다.

<예제> UDLD Interface 상태 보기

```
SG2124GP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124GP(config)#interface ge1
SG2124GP(config-if)#udld port
SG2124GP(config-if)#udld port aggressive
```



```
SG2124GP(config-if)#end
SG2124GP#show udld ge1
```

```
-----
Interface ge1
```

```
UDLD administrative configuration setting : Enabled (aggressive mode)
Current operational state : Advertisement
Current bidirectional state : Unknown
Message interval : 7
Time out interval : 5
Host device ID : SG1030500003
Host port ID : ge1
```

```
No neighbor cache information.
```

```
COM6 - PuTTY

-----
Interface ge1

UDLD administrative configuration setting : Enabled (aggressive mode)
Current operational state : Advertisement
Current bidirectional state : Bidirectional
Message interval : 7
Time out interval : 5
Host device ID : ESS2224UC2007040200013
Host port ID : ge1

  Cache Infomation
  -----
  Cache expiration time : 43
  Device ID : CAT0947Z3JT
  Port ID : Gi0/25
  Device name : Switch
  Message interval : 15
  Time out interval : 5

-----
Interface ge2

UDLD administrative configuration setting : Disabled
Current operational state : Link down
Current bidirectional state : Unknown

DUT_166#
```

- Current operation state : 현재 UDLD의 상태를 표시
- Current bidirection state : 상대 Port의 Directional 상태로 Unknown, Unidirectional, Bidirectional 의 3가지 값 중 현재의 상태를 표시합니다.
- Unknown : 상대방의 상태를 모르는 상태
- Unidirectional : 단방향 통신이 이루어지는 상태
- Bidirectional : 양방향 통신이 이루어지는 상태

1.8 SNMP

SNMP (Simple Network Management Protocol)는 SNMP 관리자와 Agent 간의 통신을 가능하게 하는 Protocol입니다. SNMP를 설정할 때 Community에 따라 읽기 권한만 부여할 수도 있고 읽기와 쓰기 권한을 모두 부여할 수도 있습니다.

SNMP Agent는 SNMP 관리자의 요청에 응답할 수 있는 MIB 변수를 가지고 있으며 SNMP 관리자는 Agent로부터 Data를 얻거나 저장할 수 있습니다. Agent는 시스템과 Network에 대한 정보를 저장하고 있는 MIB에서 Data를 얻습니다.

SG Switch Series는 IPv4, IPv6를 모두 지원합니다.

1.8.1 SNMP 설정

SNMP Agent의 시스템 관리자 정보와 Agent가 설치되어 있는 장비 위치, 장비 이름을 지정하면 해당 내용은 SNMP 설정 파일에 저장되어 Read 권한이 있는 관리자가 SNMP Query를 하는 경우 설정된 내용을 출력해 줍니다.

- Version 2.2.6부터 SNMP 기본동작이 Disable로 동작하며, 사용을 위해서는 no snmp disable을 입력 해야 합니다.

SNMP를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
snmp-server syscontact <i>WORD</i>	CONFIG	SNMP Agent의 시스템 관리자에 대한 정보를 설정합니다.
snmp-server syslocation <i>WORD</i>	CONFIG	SNMP Agent가 설치된 장비의 위치를 설정합니다.
snmp-server sysname <i>WORD</i>	CONFIG	SNMP Agent의 관리 Name을 설정합니다.

SNMP의 설정 값을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show running-config	TOP	Config 설정 내용을 통하여 snmp 설정 상태를 확인합니다.
show snmp-server	TOP	SNMP Server의 동작 상태를 확인합니다.

SNMP의 설정 내용을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no snmp-server syscontact	CONFIG	SNMP Agent의 시스템 관리자에 대한 정보를 초기화합니다.
no snmp-server syslocation	CONFIG	SNMP Agent가 설치된 장비 위치를 초기화합니다.
no snmp-server sysname	CONFIG	SNMP Agent의 관리 Name을 초기화합니다.

<예제> SNMP 설정

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#snmp-server syscontact SGcontact
SG2124G(config)#snmp-server syslocation SGlocation
SG2124G(config)#snmp-server sysname SGsysname
SG2124G(config)#end
SG2124G#show snmp-server |include sys
sysName      : SGsysname
sysContact   : SGcontact
sysLocation  : SGlocation
SG2124G#show snmp-server
enable       : enabled
state        : running operating
process id   : 167
engine id    : 80 00 1F 88 80 10 BF AD 47 4A 3C CF F6 (hex)

sysName      : SGsysname
sysContact   : SGcontact
sysLocation  : SGlocation

TrapEnable Auth : Disabled(default)
      Start : Disabled(default)
      Fan : Disabled(default)
      Psu : Disabled(default)
      Temp : Disabled(default)
      Login : Disabled(default)
-- 이하 생략 --

```



참고

1. syscontact을 지정하지 않은 경우 Default 값은 Null입니다.
2. syslocation을 지정하지 않은 경우 Default 값은 Null입니다.
3. sysname을 지정하지 않은 경우 Default 값은 Null입니다.

1.8.2 SNMP Community 설정

SNMP Protocol을 이용하여 다수의 장비를 원격으로 통합 관리할 수 있습니다. EMS로 원격 관리하기 위해서는 Switch에 IP Address가 설정되어 있어야 하며, CLI 명령어를 이용하여 환경설정을 하여야 합니다.

SNMP Community는 시스템과 원격 Network 관리자(EMS) 사이의 간단한 상호 인증 기능을 제공합니다. Switch는 두 가지 형태의 Community String을 지원합니다.

■ Read only community strings

읽기 전용 (read-only)으로 접속

■ Read-write community strings

읽기 및 쓰기(read and write)가 가능하도록 접속

SNMP Community를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
snmp-server community {ro rw} Name <A.B.C.D>	CONFIG	SNMP Community를 지정합니다.

SNMP의 설정 값을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show running-config	TOP	설정 내용을 통하여 snmp 설정 상태를 확인합니다.
show snmp-server	TOP	SNMP Server의 동작 상태를 확인합니다.

SNMP Community를 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no snmp-server community {ro rw} Name	CONFIG	SNMP Community를 삭제합니다.

<예제> snmp community 설정

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#snmp-server community ro hdnet
SG2124G(config)#snmp-server community rw HDNET
SG2124G(config)#end
SG2124G#show snmp-server |include community
trap community:
community      : ro hdnet
community      : rw HDNET
SG2124G#show snmp-server
enable          : enabled
state           : running operating
process id      : 167
engine id       : 80 00 1F 88 80 10 BF AD 47 4A 3C CF F6 (hex)

sysName         : Null
sysContact      : Null
sysLocation     : Null

TrapEnable Auth : Disabled(default)
                Start : Disabled(default)
                Fan : Disabled(default)
                Psu : Disabled(default)
                Temp : Disabled(default)
                Login : Disabled(default)

trap community:
community      : ro hdnet
community      : rw HDNET

port linktrap config status
ge1             : Enabled
ge2             : Enabled
ge3             : Enabled
ge4             : Enabled
ge5             : Enabled
ge6             : Enabled
ge7             : Enabled
-- 이하 생략 --

```



참고

1. 통합 보안 관제 시스템(Visual Node Manager)과의 연동을 위해
서 Snmp-Server Community를 rw로 설정합니다.
2. Snmp-Server Community는 Read Only, Read Write에 각각 최
대 10개까지 지정할 수 있습니다.

1.8.3 SNMP Trap 설정

하나 이상의 Network 관리 단말(PC 또는 워크스테이션)이 인증된 Trap을 수신하는 단말로 설정될 수 있으며 SNMP Agent는 Network 장비 상태에 대한 Event (Trap)가 발생한 경우 발생한 Event를 수신 단말로 전송합니다.

Trap은 잘못된 사용자 인증, Rebooting, 연결 상태 등과 같은 정보를 알려줍니다.

SNMP Trap을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
snmp-server trap-enable auth	CONFIG	Authentication Failure 시 Trap event를 전송하도록 설정합니다.
snmp-server trap-enable fan	CONFIG	FAN 이상이 있을 때 Trap event를 전송하도록 설정합니다.
snmp-server trap-enable login	CONFIG	장비 login시 Trap event를 전송하도록 설정합니다.
snmp-server trap-enable mds-detect	CONFIG	MDS event가 발생한 경우 Trap event를 전송하도록 설정합니다.
snmp-server trap-enable psu	CONFIG	PSU에 이상이 감지되면 Trap event를 전송하도록 설정합니다.
snmp-server trap-enable sfp	CONFIG	SFP8472 Warning, Alarm 발생 시 Trap event를 전송하도록 설정합니다.
snmp-server trap-enable start	CONFIG	WARM, COLD Booting 시 Trap event를 전송하도록 설정합니다. 기능의 특성상 약 2 min 정도 소요됩니다.
snmp-server trap-enable temp	CONFIG	온도 Alarm 동작 시 Trap event를 전송하도록 설정합니다.
snmp-server trapcommunity WORD	CONFIG	SNMP Trap Community를 지정합니다.
snmp-server trapsink {inform trap trap2} ip-address [Community_Name [DST_Port]]	CONFIG	SNMP Trap 수신 단말을 지정합니다.

SNMP의 설정 값을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show running-config	TOP	Config 설정 내용을 통하여 snmp 설정 상태를 확인합니다.
show snmp-server	TOP	SNMP Server의 동작 상태를 확인합니다.

SNMP Trap을 설정 상태를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no snmp-server trap-enable {auth fan login start mds-detect psu sfp start temp }	CONFIG	Event 발생 시 Trap을 전송하도록 설정한 항목을 초기화합니다.
no snmp-server trapcommunity WORD	CONFIG	SNMP Trap Community를 초기화합니다.
no snmp-server trapsink {inform trap trap2} ip- address	CONFIG	SNMP Trap 수신 단말의 지정을 초기화합니다.



참고

snmp-server trapsink 설정 시 Option 별로 10개까지 설정할 수 있습니다.

<예제> 192.168.100.10의 IP Address의 단말을 SNMP Trap 수신 단말로 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#snmp-server trap-enable auth
SG2124G(config)#snmp-server trap-enable fan
SG2124G(config)#snmp-server trap-enable login
SG2124G(config)#snmp-server trap-enable mds-detect
SG2124G(config)#snmp-server trap-enable psu
SG2124G(config)#snmp-server trap-enable sfp
SG2124G(config)#snmp-server trap-enable start
SG2124G(config)#snmp-server trap-enable temp
SG2124G(config)#snmp-server trapcommunity SGcommunity
SG2124G(config)#snmp-server trapsink inform 192.168.100.10
SG2124G(config)#end
```

```
SG2124G#show snmp-server
enable      : enabled
state       : running operating
process id  : 167
engine id   : 80 00 1F 88 80 10 BF AD 47 4A 3C CF F6 (hex)

sysName     : Null
sysContact  : Null
sysLocation : Null

TrapEnable Auth : Enabled
              Start : Enabled
              Fan : Enabled
              Psu : Enabled
              Temp : Enabled
              Login : Enabled
              Sfp : Enabled
              mds-detect : Enabled

trap community: SGcommunity
trapsink      : inform 192.168.100.10

port linktrap config status
ge1           : Enabled
ge2           : Enabled
ge3           : Enabled
ge4           : Enabled
ge5           : Enabled
ge6           : Enabled
ge7           : Enabled
ge8           : Enabled
ge9           : Enabled
ge10          : Enabled
ge11          : Enabled
ge12          : Enabled
-- 이하 생략 --
```


1.8.4 SNMP Version 1/2/3 View 기반 접근 제어 설정

SG Switch Series Switch는 SNMP v1, v2c, v3를 지원하며 OID에 접속하는 권한을 제한할 수 있는 SNMP v2c, v3를 통해 관리자는 보안 인증키와 함께 특정 User를 설정하여 특정 Group에 공개 범위를 제한한 OID를 볼 수 있도록 설정할 수 있습니다.

SNMPv1, v2c, v3 View 기반 접근 제어 설정을 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
snmp-server security <i>NAME</i> <i>IP_Addr WORD</i>	CONFIG	접근이 허용되는 관리자와 Community를 설정합니다.
snmp-server user <i>NAME</i> {md5 sha} <i>WORD</i> des <i>WORD</i>	CONFIG	SNMP v3의 User를 설정합니다.
snmp-server group <i>NAME</i> {v1 v2c v3} <i>WORD</i>	CONFIG	SNMP 관리자와 Community를 Group으로 설정합니다.
snmp-server view <i>NAME</i> {exclude include} <i>OID_VALUE</i>	CONFIG	MIB의 OID 공개 범위를 설정합니다.
snmp-server access <i>NAME</i> {v1 v2c} <i>Read_WORD</i> <i>Write_WORD Notify_WORD</i>	CONFIG	v1, v2c에서 특정 Group이 제한된 OID에 접속할 수 있도록 설정합니다.
snmp-server access <i>NAME</i> v3 {auth noauth priv} <i>Read_WORD Write_WORD</i> <i>Notify_WORD</i>	CONFIG	v3에서 특정 Group이 제한된 OID에 접속할 수 있도록 설정합니다.

SNMPv1, v2c, v3 View 기반 접근 제어 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show running-config	TOP	Config 설정 내용을 통하여 snmp 설정 상태를 확인합니다.
show snmp-server	TOP	SNMP Server의 동작 상태를 확인합니다.

SNMPv1, v2c, v3 View 기반 접근 제어 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no snmp-server security <i>NAME</i>	CONFIG	설정된 접근이 허용되는 관리자와 Community를 초기화합니다.
no snmp-server user <i>NAME</i>	CONFIG	SNMP v3의 User를 초기화합니다.
no snmp-server group <i>NAME</i> {v1 v2c v3}	CONFIG	Group으로 설정된 SNMP 관리자와 Community를 초기화합니다.
no snmp-server view <i>NAME</i> <i>OID_VALUE</i>	CONFIG	MIB의 OID 공개 범위를 초기화합니다.
no snmp-server access <i>NAME</i>	CONFIG	제한된 OID를 허가했던 Group을 초기화합니다.



주의

1. SNMP 접근 제어 설정 및 해제 시 다음의 순서대로 진행하지 않는 경우 의존성으로 인해 정상 동작하지 않을 수 있습니다.
SNMPv1/v2c 설정 순서: security -> group -> view -> access
SNMPv3 설정 순서: user -> group -> view -> access
설정 해제는 설정할 때의 역순으로 초기화를 진행합니다.
2. Group 설정과 access 설정 시 SNMP 버전은 동일해야 합니다.



참고

보안성 향상으로 인해 SNMP USER 설정 시 인증 및 암호화 비밀번호는 9자 이상으로 영대문자, 영소문자, 숫자, 특수문자를 최소 1자 이상씩 혼합하여 설정하여야 합니다

<예제> SNMPv1, v2c, v3 View 기반 접근 제어 설정

- SNMPv1 public 사용자는 system Group(1.3.6.1.2.1.1)만 ro 허용
- SNMPv1 private 사용자는 system Group(1.3.6.1.2.1.1)만 rw 허용
- SNMPv2 public 사용자는 interfaces Group(1.3.6.1.2.1.2)만 ro 허용
- SNMPv2 private 사용자는 interfaces Group(1.3.6.1.2.1.2)만 rw 허용
- SNMPv3 user1은 sha authentication (auth passphrase: Qwe123!@#)과 aes privacy (priv passphrase: Asd123!@#)를 사용하며, system Group(1.3.6.1.2.1.1)만 rw 허용
- SNMPv3 user2는 sha authentication (auth passphrase: Asd123!@#)과 aes privacy (priv passphrase: Qwe123!@#)를 사용하며, interfaces Group(1.3.6.1.2.1.2)만 rw 허용
- SNMPv3 user3는 authentication과 privacy를 사용하지 않으며, mib-2 Group (1.3.6.1.2.1)에서 interfaces Group(1.3.6.1.2.1.2)만 제외하고 모두 rw 허용

```
SG2124G(config)#snmp-server security sro1 192.168.100.169 public
SG2124G(config)#snmp-server security srw1 192.168.100.169 private
```

```

SG2124G(config)#snmp-server user user1 sha ***** aes *****
SG2124G(config)#snmp-server user user2 sha ***** aes *****
SG2124G(config)#snmp-server user user3 sha *****
SG2124G(config)#snmp-server group gro1 v1 sro1
SG2124G(config)#snmp-server group grw1 v1 srw1
SG2124G(config)#snmp-server group gro2 v2c sro1
SG2124G(config)#snmp-server group grw2 v2c srw1
SG2124G(config)#snmp-server group group3 v3 user1
SG2124G(config)#snmp-server group group4 v3 user2
SG2124G(config)#snmp-server group group5 v3 user3
SG2124G(config)#snmp-server view view1 include 1.3.6.1.2.1.1
SG2124G(config)#snmp-server view view2 include 1.3.6.1.2.1.2
SG2124G(config)#snmp-server view view3 include 1.3.6.1.2.1
SG2124G(config)#snmp-server view view3 exclude 1.3.6.1.2.1.2
SG2124G(config)#snmp-server access group3 v3 priv view1 view1 view1
SG2124G(config)#snmp-server access group4 v3 priv view2 view2 view2
SG2124G(config)#snmp-server access group5 v3 noauth view3 view3 view3
SG2124G(config)#snmp-server access gro1 v1 view1 none none
SG2124G(config)#snmp-server access gro2 v2c view2 none none
SG2124G(config)#snmp-server access grw1 v1 view1 view1 view1
SG2124G(config)#snmp-server access grw2 v2c view2 view2 view2
SG2124G(config)#end
SG2124G#show snmp-server
enable          : enabled
state           : running operating
process id      : 167
engine id       : 80 00 1F 88 80 10 BF AD 47 4A 3C CF F6 (hex)

sysName         : Null
sysContact      : Null
sysLocation     : Null

TrapEnable Auth : Disabled(default)
                Start : Disabled(default)
                Fan   : Disabled(default)
                Psu   : Disabled(default)
                Temp  : Disabled(default)
                Login : Disabled(default)
                Sfp   : Disabled(default)
                mds-detect : Disabled(default)

trap community:
security       : sro1 192.168.100.169 public
security       : srw1 192.168.100.169 private
user           : user1 sha ***** aes *****
user           : user2 sha ***** aes *****
user           : user3 sha *****
group          : gro1 v1 sro1
group          : grw1 v1 srw1
group          : gro2 v2c sro1
group          : grw2 v2c srw1
group          : group3 v3 user1
group          : group4 v3 user2
group          : group5 v3 user3
view           : view1 include 1.3.6.1.2.1.1
view           : view2 include 1.3.6.1.2.1.2

```

```
view      : view3 include 1.3.6.1.2.1
view      : view3 exclude 1.3.6.1.2.1.2
access    : group3 v3 priv view1 view1 view1
access    : group4 v3 priv view2 view2 view2
access    : group5 v3 noauth view3 view3 view3
access    : gro1 v1 view1 none none
access    : gro2 v2c view2 none none
access    : grw1 v1 view1 view1 view1
access    : grw2 v2c view2 view2 view2
```

```
port linktrap config status
```

```
ge1       : Enabled
ge2       : Enabled
ge3       : Enabled
ge4       : Enabled
ge5       : Enabled
ge6       : Enabled
ge7       : Enabled
ge8       : Enabled
ge9       : Enabled
ge10      : Enabled
ge11      : Enabled
ge12      : Enabled
ge13      : Enabled
ge14      : Enabled
ge15      : Enabled
ge16      : Enabled
ge17      : Enabled
ge18      : Enabled
ge19      : Enabled
ge20      : Enabled
ge21      : Enabled
ge22      : Enabled
ge23      : Enabled
ge24      : Enabled
vlan1.1   : Enabled
```

```
SG2124G#
```

1.9 Syslog

Syslog는 시스템에서 발생하는 경보 및 Event 등의 정보를 관리자에게 Message를 통하여 알려주는 방법입니다. 이러한 Syslog는 발생한 경보 및 Event의 등급을 분류하여 시스템 내부의 이력으로 보관하면서 관리자의 특정 시스템으로 전달할 수 있습니다.

1.9.1 Syslog 설정

Syslog Message는 그 중요성에 따라 alerts | critical | debugging | emergencies | errors | informational | notifications | warnings 의 8단계 Level로 구분되어 있으며, emergency가 가장 중요한 경보 및 Event Message를 알려줍니다.

Trap-Level등을 설정하여 시스템에서 발생하는 경보 및 Event 등의 정보를 SYSLOG 저장할 수 있습니다.

Syslog 관련 설정을 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
log record-priority	CONFIG	Syslog의 record-priority를 설정합니다.
log syslog	CONFIG	Syslog Service를 시작합니다. (Default)
log trap {alerts critical debugging emergencies errors informational notifications warnings}	CONFIG	Syslog Level을 지정합니다. (Default: Information)

Syslog 관련 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show log syslog config	TOP	Syslog 설정 상태를 확인합니다.
show syslog [module_name]	TOP	저장된 event 중 특정 Module에 관련된 정보를 확인합니다.
show syslog [desc]	TOP	저장된 event 정보를 최근 시간부터 확인합니다.
show syslog [tail num <1-100>]	TOP	저장된 event 정보의 마지막 n Line까

		지 확인합니다.
--	--	----------

Syslog 관련 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
clear syslog	TOP	Syslog event 내용을 초기화합니다.
no log record-priority	CONFIG	Syslog의 record-priority를 초기화합니다.
no log syslog	CONFIG	Syslog Service를 중지합니다.
no log trap	CONFIG	Syslog Level을 초기화합니다.

<예제> syslog 설정 및 확인

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#log record-priority
SG2124G(config)#log syslog
SG2124G(config)#log trap alerts
SG2124G(config)#exit
SG2124G#show log syslog config
-----
syslog configuration
-----
trap level : alerts
record priority : Yes
-----

SG2124G#
SG2124G#show syslog
Jan 30 21:00:12 SG2124G ntpd[116]: ntpd 4.1.2@1.892 Wed Dec 24 00:34:40 PST 2003 (1)
Jan 30 21:00:13 SG2124G ntpd[116]: precision = 6 usec
Jan 30 21:00:13 SG2124G ntpd[116]: kernel time discipline status 0040
Jan 30 21:00:13 SG2124G kernel: fan start temperature reached
Jan 30 21:00:24 SG2124G inetd[237]: Online and ready (1 sockets)
Jan 30 21:00:24 SG2124G NSM[179]: NSM: Port up notification received for port
vlan1.1
Jan 30 21:00:24 SG2124G NSM[179]: NSM: Port down notification received for port
vlan1.1
Jan 30 21:00:24 SG2124G NSM[179]: NSM: Port up notification received for port
vlan1.1
Jan 30 21:00:24 SG2124G NSM[179]: NSM: Port down notification received for port
vlan1.1
Jan 30 21:00:24 SG2124G NSM[179]: NSM: Port up notification received for port
vlan1.200
Jan 30 21:00:24 SG2124G NSM[179]: NSM: Port up notification received for port
vlan1.1
Jan 30 21:00:24 SG2124G NSM[179]: NSM: Port down notification received for port
vlan1.1
```

```
Jan 30 21:00:24 SG2124G NSM[179]: NSM: Port up notification received for port
vlan1.1
Jan 30 21:00:24 SG2124G NSM[179]: NSM: Port up notification received for port
vlan1.254
Jan 30 21:00:25 SG2124G NSM[179]: NSM: Port up notification received for port
vlan1.100
Jan 30 21:00:25 SG2124G NSM[179]: NSM: Port up notification received for port
vlan1.150
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#no log record-priority
SG2124G(config)#no log syslog
SG2124G(config)#no log trap
SG2124G(config)#exit
SG2124G#show log syslog config
-----
syslog configuration
-----
trap level : informational
record priority : No
-----

SG2124G#
SG2124G#copy syslog sftp 192.168.0.200 syslog.log test
Filename is syslog.log
Starting Transmission....
The authenticity of host '192.168.0.200 (192.168.0.200)' can't be established.
RSA key fingerprint is 09:7c:79:db:5e:26:ec:39:38:6b:ba:94:7c:58:73:f1.
Are you sure you want to continue connecting (yes/no)? yes
test@192.168.0.200's password:
Finished ....
SG2124G#
SG2124G#copy syslog sftp 192.168.0.200 syslog_backup.log test
Filename is syslog.log
Starting Transmission....
The authenticity of host '192.168.0.200 (192.168.0.200)' can't be established.
RSA key fingerprint is 09:7c:79:db:5e:26:ec:39:38:6b:ba:94:7c:58:73:f1.
Are you sure you want to continue connecting (yes/no)? yes
test@192.168.0.200's password:
Finished ....
SG2124G#
SG2124G#clear syslog
clear system log? (y/n): y
SG2124G#
```

1.9.2 Remote Syslog 설정

Syslog Message의 remote Message 전달 장소를 설정하면 Syslog Daemon이 설치되어 있는 Remote Host 시스템으로 Switch에서 발생하는 경보 및 Event Message를 전달합니다.

또한, Facilities가 만드는 Messages를 통해 Log Messages가 어디서 보내졌으며 어디에 저장되어 있는지를 결정하여 Source에 따른 서로 다른 Messages를 분리된 다른 log 파일에 보관함으로써 Syslog를 관리할 수 있습니다.

Remote Syslog 관련 설정을 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
log trap {alerts critical debugging emergencies errors informational notifications warnings}	CONFIG	Syslog Level을 지정합니다.
log syslog remote hostname	CONFIG	Syslog 수신 호스트 명이나 IP, IPv6 주소를 지정합니다.
log syslog facility {auth authpriv cron daemon ftp kern local0 local1 local2 local3 local4 local5 local6 local7 lpr mail news syslog user uucp}	CONFIG	Syslog의 Facility Keyword를 설정합니다. (Default: local7)

Remote Syslog 관련 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show log syslog {config remote}	TOP	Syslog 설정 상태를 확인합니다.

Remote Syslog 관련 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no log trap	CONFIG	Syslog Level을 초기화합니다.
no log syslog remote ip-address	CONFIG	Syslog 수신 IP를 삭제합니다.

no log syslog facility	CONFIG	Syslog의 Facility Keyword를 초기화합니다.
------------------------	--------	-----------------------------------

<예제> event 발생 시 remote syslog Server(IP 192.168.100.1)로 event 정보를 전달하도록 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#log syslog remote 192.168.100.1
SG2124G(config)#log syslog facility local7
SG2124G(config)#exit
SG2124G#
SG2124G#show log syslog config
-----
syslog configuration
-----
trap level : informational
record priority : No
-----

SG2124G#
SG2124G#show running-config | include remote
log syslog remote 192.168.100.1
SG2124G#
```

1. Remote Syslog Server는 최대 10개까지 설정할 수 있습니다.

2. The syslog source facilities



참고

auth	Login Authentication Messages
authpriv	Security/Authorization Messages
cron	Clock Daemon Messages
daemon	System Daemons Messages
ftp	FTP Daemon Messages
kern	The Kernel Messages
local0 through local7	As Defined Locally
lpr	The Line Printer Subsystem Messages
mail	Mail System Messages
news	Network News Subsystem Messages
syslog	Messages Generated Internally by Syslogd
user	User-Level Messages
uucp	The UUCP Subsystem Messages

1.10 sFlow

sFlow는 RFC3176에서 표준화되었으며 Network 장비에서 고속의 Traffic Data를 Capture 하여 분석하기 위해 실시간 Packet Sampling 방식을 사용하기 때문에 L2부터 L7 Traffic에 대해 Network의 성능 저하 없이 Monitoring 할 수 있습니다.

sFlow Agent는 Interface에서 처리되는 Packet을 분석하여 Traffic 수집서버 (Collector)로 전송하는 방식으로 동작하며, sFlow 통계 기능을 이용하여 하단 Network 및 인접한 Network의 흐름에 대한 특성이나 Interface 단위 MIB 정보 수집 등의 Event를 모니터링 합니다. 이를 위해 각 Interface에 실시간 Packet Counter 간격을 설정해 주어야 하며 Packet을 추출하는 빈도 수를 Sampling 비율(sample-rate)이라고 합니다.

SG Switch Series는 IPv4, IPv6를 모두 지원합니다.

sFlow 관련 설정을 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
sflow agent IP_Address	CONFIG	Agent IP Address를 설정합니다. (Default: 127.0.0.1)
sflow {both egress ingress} Port_Range	CONFIG	Packet을 분석할 Interface를 설정합니다.
sflow collector IP_Address [Port_No]	CONFIG	Collector IP Address 및 Service Port를 설정합니다. (Default Port: 6343)
sflow sample-rate <5000-1048576>	CONFIG	Packet을 추출하는 Sampling 비율을 설정합니다. (Default: 1 out of 10000 Packet)

sFlow 관련 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show sflow config	TOP	sFlow 설정 상태를 확인합니다.

sFlow 관련 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no sflow agent	CONFIG	Agent IP Address를 삭제합니다.
no sflow {both egress ingress} Port_Range	CONFIG	Packet을 분석할 Interface를 삭제합니다.

no sflow collector	CONFIG	Collector IP Address를 삭제합니다.
no sflow sample-rate	CONFIG	Packet을 추출하는 Sampling 비율을 삭제합니다.

<예제> Switch(IP 192.168.0.1)에서 ge1~ge10의 Interface의 Ingress / Egress Traffic에 대해 Packet 5000개당 1개를 Sampling하여 Traffic 수집서버(IP 192.168.0.100)로 전송하도록 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#sflow agent 192.168.0.1
SG2124G(config)#
SG2124G(config)#sflow both ge1-10
SG2124G(config)#
SG2124G(config)#sflow collector 192.168.0.100
SG2124G(config)#
SG2124G(config)#sflow sample-rate 5000
SG2124G(config)#end
SG2124G#
SG2124G#show sflow config
- sFlow Agent Address      : 192.168.0.1
- sFlow Collector Address  : 192.168.0.100
- sFlow Collector Port     : 6343
-----
Interface Ingress   Rate      Egress    Rate
=====
ge1       Enable    5000      Enable    5000
ge2       Enable    5000      Enable    5000
ge3       Enable    5000      Enable    5000
ge4       Enable    5000      Enable    5000
ge5       Enable    5000      Enable    5000
ge6       Enable    5000      Enable    5000
ge7       Enable    5000      Enable    5000
ge8       Enable    5000      Enable    5000
ge9       Enable    5000      Enable    5000
ge10      Enable    5000      Enable    5000
ge11
ge12
-- 이하 생략 --
SG2124G#
```



참고

sFlow Agent 및 Collector IP Address는 1개만 지정이 가능합니다. 따라서 중복하여 설정하는 경우 마지막에 등록된 IP Address가 설정됩니다.

1.11 RMON

RMON (Remote Monitoring)은 원격지에 있는 통신망을 관리하도록 설계된 SNMP의 확장기능으로, RFC 1757에 정의된 MIB의 일부로 정의되어 있습니다. 표준 SNMP 전송 구조와 명령을 이용하여 특정 Interface를 통해 드나드는 분산된 랜(LAN) 환경의 모든 Traffic을 수집하여 원격으로 점검하고 확인할 수 있는 기능입니다.

SNMP는 SNMP Agent 장비에 대한 정보만을 얻을 수 있지만, RMON은 장비를 포함한 세그먼트 전체에서 발생하는 정보를 파악할 수 있기 때문에 보다 효율적으로 Network를 관리할 수 있습니다.

Layer2 수준에서 Traffic 내용을 분석해주는 RMON Version 1과 Layer 2 - 7 즉 모든 계층에 대한 Traffic 분석 정보를 제공하는 Version 2가 있습니다. SG Switch Series Switch는 RMON 버전1을 지원하며, RFC 1757에 정의되어 있는 Statistics, History, Alarm, Host, Host Enable N, Matrix, Filter, Packet capture, Event의 9가지 종류의 정보 중에서 Statistics, History, Alarm, Event의 4가지 MIB그룹을 지원합니다.

RMON은 Interface의 모든 Traffic을 분석하기 때문에 CPU 점유율이 높아질 수 있습니다. RMON 사용으로 인해 시스템의 성능이 저하되거나 Network 전송에 과부하가 걸리지 않도록 설정 시 주의하셔야 합니다.

1.11.1 Statistics 설정

RMON Statistics (OID 1.3.6.1.2.1.16.1)은 장비가 측정한 각종 Network 통계에 관련된 객체를 포함하며 Network의 Traffic량, 평균 Packet 크기, Broadcast의 횟수, 발생한 오류의 수, 일정 범위의 크기를 갖는 Packet의 개수 등을 측정하여 보고합니다.

- Owner : 소유자에 대한 정보를 등록합니다

RMON Stats를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
rmon collection stats <1-65535> [owner WORD]	INTERFACE	RMON Statistic을 설정합니다.

RMON Stats 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show rmon statistics	TOP	RMON Statistic 설정을 확인합니다.

RMON Stats 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no rmon collection stats <1-65535>	INTERFACE	RMON Statistic 설정을 삭제합니다.

<예제> RMON Stats 설정 및 확인

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#
SG2124G(config)#interface ge1
SG2124G(config-if)#rmon collection stats 1
SG2124G(config-if)#end
SG2124G#
SG2124G#show rmon statistics
=====
etherStatsIndex : 1
etherStatsDataSource : 5001
etherStatsDropEvents : 0
etherStatsOctets : 545,461,731
etherStatsPkts : 8,522,273
```

```
etherStatsBroadcastPkts : 8,521,522
etherStatsMulticastPkts : 20,366
etherStatsCRCAlignErrors : 0
etherStatsUndersizePkts : 0
etherStatsOversizePkts : 0
etherStatsFragments : 0
etherStatsJabbers : 0
etherStatsCollisions : 0
etherStatsPkts64to127octets : 17,125,238
etherStatsPkts128to255octets : 893
etherStatsPkts256to511octets : 533
etherStatsPkts512to1023octets : 160
etherStatsPkts1024to1518octets : 1
etherStatsOwner :
etherStatsStatus : 1
```

SG2124G#



RMON Stats는 하나의 Interface에 중복하여 설정할 수 없습니다. 지정된 Stats Index를 다른 Interface에 중복하여 설정하는 경우 마지막에 등록한 Interface에 RMON Stats가 설정됩니다.

1.11.2 History 설정

RMON History (OID 1.3.6.1.2.1.16.2)는 Interface에서 발생하는 각종 Traffic에 대해 표본 조사할 데이터 수, 표본 조사 시간 등에 대한 통계자료를 조사하는 기능입니다. 모든 Interface의 통계 데이터는 기본적으로 1 800 s마다 한 번씩 점검되고 Interface마다 50개의 통계 데이터를 저장하도록 설정되어 있습니다.

- **Bucket** : 표본 조사할 데이터 수를 지정할 때 사용하며, **Default** 값은 50입니다.
- **Interval** : 표본 조사 시간을 초단위로 지정하며, 기본 값은 1,800입니다.
- **Owner** : 소유자에 대한 정보를 등록합니다.

RMON History를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
rmon collection history <1-65535> [buckets <1-65535>] [interval <1-3600>] [owner WORD]	INTERFACE	RMON History를 설정합니다.

RMON History 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show rmon history	TOP	RMON History 설정을 확인합니다.

RMON History 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no rmon collection history <1-65535>	INTERFACE	RMON History 설정을 삭제합니다.

<예제> RMON History 설정 및 확인

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#
SG2124G(config)#interface ge1
SG2124G(config-if)#rmon collection history 1 buckets 50 interval 5
SG2124G(config-if)#end
SG2124G#
SG2124G#show rmon history
=====
historyControlIndex : 1
historyControlDataSource : 5001
historyControlBucket Request & Granted : 50
historyControlIntervall : 5
historyControlOwner :
historyControlStatus : 1

SG2124G#
```

**참고**

RMON History는 하나의 Interface에 중복하여 설정할 수 없습니다.
지정된 History Index를 다른 Interface에 중복하여 설정하는 경우 마지막에 등록한 Interface에 RMON History가 설정됩니다.

1.11.3 Event 설정

RMON Event (OID 1.3.6.1.2.1.16.9)는 RMON Alarm 그룹에 따라 특정 경보가 발생한 경우 event가 발생하면, 발생한 event를 Syslog 서버 또는 SNMP 관리 서버로 Event 메시지나 Trap 메시지를 전송하는 기능입니다.

- Log : syslog Level이 Warning 이상인 경우 syslog를 통하여 event를 발생하게 합니다.
- Trap : snmptrap을 통하여 Trap을 발생하게 합니다.
- Description : 해당 Event에 대한 설명을 등록합니다.
- Owner : 소유자에 대한 정보를 등록합니다.
- Log만 발생하게 하려면 " log ", Trap만 발생하게 하려면 " trap 트랩명 ", Log와 Trap 모두 발생하게 하려면 " log trap 트랩명 " 과 같이 입력합니다.

RMON Event를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
rmon event <1-65535> {log trap WORD} [description WORD] [owner WORD]	CONFIG	RMON Event를 설정합니다.

RMON Event 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show rmon event	TOP	RMON Event 설정을 확인합니다.

RMON Event 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no rmon event <1-65535>	CONFIG	RMON Event 설정을 삭제합니다.

<예제> RMON Event 설정 및 확인

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#
SG2124G(config)#rmon event 1 log description SYSLOG owner USER1
SG2124G(config)#rmon event 2 trap rmontrap description RMONTRAP owner USER2
SG2124G(config)#rmon event 3 log trap rmontrap2
SG2124G(config)#exit
SG2124G#
SG2124G#show rmon event
=====
eventIndex = 1
eventDescription SYSLOG
eventType = Log
eventCommunity =
eventLastTimeSent = 0
eventOwner = USER1
eventStatus = 1

=====
eventIndex = 2
eventDescription RMONTRAP
eventType = Trap
eventCommunity = rmontrap
eventLastTimeSent = 0
eventOwner = USER2
eventStatus = 1

=====
eventIndex = 3
eventDescription TRAP
eventType = Log & Trap
eventCommunity = rmontrap2
eventLastTimeSent = 0
eventOwner = RMON_SNMP
eventStatus = 1

SG2124G#

```



RMON Event Index는 중복하여 설정할 수 없습니다. 설정되어 있는 RMON Event Index를 수정하시려면, 삭제 후 설정하시기 바랍니다.

1.11.4 Alarm 설정

RMON Alarm (OID 1.3.6.1.2.1.16.3)은 사용자가 설정한 주기에 따라 표본을 조사하여 사용자가 설정한 임계 값 또는 이전에 조사된 값을 비교한 후 임계 값에서 벗어났을 때 event가 발생되도록 하는 기능입니다. 이 때 임계 값과 비교하는 방법에는 **Absolute** 와 **Delta**의 두 가지가 있습니다.

- **EtherStatsEntry** : 표본 조사에 사용될 object를 설정해주는 것으로서 etherStatsEntry를 지원하도록 설정되어 있고, 다음 값은 OID값이며,
그 다음 값은 인덱스를 의미합니다.
- **Interval** : 표본 조사 시간을 초 단위로 지정합니다.
- **Event** : 임계 값 설정 후에는, 그 임계 값을 넘어섰을 때 해당 Index에 해당하는 Event가 발생하도록 설정합니다.
- **Owner** : 소유자에 대한 정보를 등록합니다.
- **Absolute | delta** : **Absolute**는 주기적으로 조사한 데이터의 값과 임계 값을 비교했을 때 그 이상이거나 이하이면 **Alarm**을 발생시키게 되며, **Delta**는 현재 조사된 값과 이전 조사된 값의 편차를 임계 값과 비교하여 그 이상 이거나 이하이면 **Alarm**을 발생시킵니다.
- **Rising-threshold & Falling-threshold** : 상한 임계 값과 하한 임계 값을 설정한다.

RMON Alarm을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
rmon alarm <1-65535> WORD interval <1-65535> {absolute delta} rising- threshold <1-65535> event <1-65535> falling-threshold <1-65535> event <1- 65535> [owner WORD]	CONFIG	RMON Alarm을 설정합니다.

MON Alarm 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show rmon alarm	TOP	RMON Alarm 설정을 확인합니다.

RMON Alarm 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
-----	----	----

no rmon alarm <1-65535>	CONFIG	RMON Alarm 설정을 삭제합니다.
-------------------------	--------	-----------------------

<예제> RMON Alarm 설정 및 확인.

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#
SG2124G(config)#rmon alarm 1 etherStatsEntry.5.1 interval 5 delta rising-threshold 30
event 1 falling-threshold 20 event 1
SG2124G(config)#exit
SG2124G#
SG2124G#show rmon alarm
=====
alarmIndex = 1
alarmInterval = 5
alarmVariable = etherStatsEntry.5.1
alarmSampleType = Delta
alarmValue = 0
alarmStartupAlarm = risingOrFallingAlarm(3)
alarmRisingThreshold = 30
alarmFallingThreshold = 20
alarmRisingEvent = 1
alarmFallingEvent = 1
alarmOwner =
alarmStatus = 1

SG2124G#
```



참고

RMON Alarm Index는 중복하여 설정할 수 없습니다.
설정되어 있는 RMON Alarm Index를 수정하시려면, 삭제 후 설정하시
기 바랍니다.

제2장. 시스템 운영

2.1 VLAN

2.1.1 VLAN 개요

VLAN (Virtual LAN)은 관리자의 필요에 따라 논리적으로 세분화된 Network이며, 하나의 VLAN은 하나 이상의 물리적인 Interface로 구성됩니다. 같은 VLAN에 속한 Interface들만 서로 Packet을 주고 받을 수 있으며, 다른 VLAN에 속한 Interface들은 VLAN 간의 통신을 가능하게 해주는 Routing 장비를 통해서만 Packet을 주고 받을 수 있습니다. 따라서 서로 다른 VLAN에 속한 사용자들은 불필요한 broadcast Packet 등을 수신하지 않으므로 대역폭을 더 많이 사용할 수 있으며, VLAN 단위로 Traffic을 분리 전송하므로 보안 기능도 향상됩니다.

SG Switch Series Switch는 IEEE802.1q 표준안을 충실히 실행하여, VLAN ID가 붙어 있는 tagged Packet과 VLAN ID가 붙어있지 않은 untagged Packet 모두를 전송할 수 있습니다. 모든 Interface는 설정한 VLAN ID (VID) 값을 가지고 있으며 관리자가 특정 VLAN으로 분류하지 않은 untagged Traffic에는 기본 VID (VLAN 1.1)가 부여됩니다. 그러므로 VLAN으로 구성된 Switch Interface들은 동일한 VID를 가진 VLAN 내에서만 Packet을 전송할 수 있습니다.

2.1.2 VLAN 설정

기본적으로 Switch의 초기 설정으로 `vlan1.1`이 생성되어 있고 모든 `Interface`가 `vlan1.1`에 할당되어 있습니다. `Packet`은 동일 `VLAN` 내에 있는 `Interface`에서만 통신이 가능합니다. `VLAN ID`는 `Packet`을 전송할 때 `Packet` 내에 첨부하는 `VLAN` 번호입니다.

새로운 `VLAN`을 생성하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
<code>vlan database</code>	CONFIG	<code>VLAN</code> 설정 모드로 변경합니다.
<code>vlan <2-4094> bridge 1 {name vlan-name} state {enable disable}</code>	VLAN	<code>VLAN</code> 이름과 ID를 부여하여 <code>VLAN</code> 설정합니다. (최대 256개의 <code>VLAN</code> 설정)
<code>vlan range RANGE bridge 1</code>	VLAN	다수의 <code>VLAN</code> 을 설정합니다. (최대 255개까지 동시 설정)

생성된 `VLAN` 및 `Member` 정보를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
<code>show vlan <2-4094></code>	TOP	특정 <code>VLAN</code> 정보를 확인합니다.
<code>show vlan [brief]</code>	TOP	모든 <code>VLAN</code> 정보를 확인합니다.

`VLAN`을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
<code>no vlan {<2-4094> range} [mtu] bridge 1</code>	VLAN	<code>VLAN</code> 을 삭제합니다.



참고

`VLAN`은 Default `VLAN`을 포함하여 최대 256개까지 설정할 수 있습니다. (SG2200 Series의 경우 최대 128개로 제한)

2.1.3 Port VLAN 설정

새로운 VLAN을 만든 다음에는 Interface에 해당 VLAN을 지정합니다.

Interface에 Port VLAN을 지정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
interface <i>IFNAME</i>	CONFIG	Interface를 선택합니다.
interface range <i>PORTRANGE</i>	CONFIG	Interface 범위를 선택합니다.
switchport access vlan <2-4094>	INTERFACE	Interface에 VLAN을 설정합니다.

생성된 VLAN 및 Member 정보를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show vlan <2-4094>	TOP	특정 VLAN 정보를 확인합니다.
show vlan all	TOP	모든 VLAN 정보를 확인합니다.
show vlan [brief]	TOP	모든 VLAN 정보를 확인합니다.

Interface에 설정된 VLAN을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no switchport access vlan	INTERFACE	Interface에 설정된 VLAN을 초기화합니다.

<예제> Configure Port VLAN

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#vlan database
SG2124G(config-vlan)#vlan 10 bridge 1          → Vlan1.10 생성
SG2124G(config-vlan)#exit
SG2124G(config)#
SG2124G(config)#interface range ge1-2
% ge1-2 Selected
SG2124G(config-if-range)#switchport access vlan 10 → Interface에 Vlan1.10 지정
% ge1-2 Selected
SG2124G(config-if-range)#exit
SG2124G(config)#exit
SG2124G#
SG2124G#show vlan 10          → Vlan1.10의 전체 Interface 확인
Bridge Group : 1

VLAN ID    Name           State  Member ports (u)-Untagged, (t)-Tagged
=====
10         VLAN0010       ACTIVE ge1(u) ge2(u)

SG2124G#
SG2124G#show vlan brief      → 전체 Vlan 설정 상태 확인
Bridge Group : 1

VLAN ID    Name           State  Member ports (u)-Untagged, (t)-Tagged
=====
1          default      ACTIVE ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u)
          ge9(u) ge10(u) ge11(u) ge12(u) ge13(u)
          ge14(u) ge15(u) ge16(u) ge17(u) ge18(u)
          ge19(u) ge20(u) ge21(u) ge22(u) ge23(u)
          ge24(u)
10         VLAN0010       ACTIVE ge1(u) ge2(u)

SG2124G#

```



주의

1. **Interface range** 명령어로 여러 개의 **Interface**를 지정할 때는 빈 칸 없이 **Interface** 번호를 콤마로 구분하여 입력합니다. (예: ge1,ge3)
2. **Interface range** 명령어로 일련의 **Interface** 범위를 지정할 때는 데쉬 기호(-)를 사용하여 입력합니다. (예: ge1-5)

2.1.4 802.1Q VLAN 설정

다수의 VLAN을 설정한 후 다른 Switch의 동일 VLAN과 통신을 하려면 VLAN 수만큼의 Uplink Interface가 필요하게 됩니다. 하지만, Trunk 기능을 사용하여 Uplink Interface로 전송되는 Packet에 VLAN 정보를 암호화하여 첨부하여 보내면 최소한의 Uplink Interface만을 사용하여 통신할 수 있습니다.

새로운 VLAN을 만든 다음, Interface를 tagging으로 설정한 후 VLAN을 지정하면, 해당 Interface는 VLAN ID가 첨부된 Packet들을 전송합니다.

Interface에 Trunk VLAN을 구성하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
interface range PORTRANGE	CONFIG	Interface 범위를 선택합니다.
switchport mode trunk	INTERFACE	Interface를 trunk mode로 변경합니다.
switchport trunk allowed vlan {add remove} VLAN_RANGE	INTERFACE	Interface에 VLAN을 설정합니다. (최대 256개까지 동시 설정)
switchport trunk native vlan <2-4094>	INTERFACE	Native VLAN을 설정합니다.

생성된 VLAN 및 Member 정보를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show vlan <2-4094>	TOP	특정 VLAN 정보를 확인합니다.
show vlan all bridge 1	TOP	모든 VLAN 정보를 확인합니다.
show vlan brief	TOP	모든 VLAN 정보를 확인합니다.

Interface에 Trunk VLAN을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
switchport mode access	INTERFACE	Access VLAN 설정으로 초기화합니다.
no switchport trunk native vlan	INTERFACE	Native VLAN 설정을 초기화합니다.

<예제> ge1-2를 VLAN10으로 설정하고 ge3을 trunk로 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#vlan database
SG2124G(config-vlan)#vlan 10 bridge 1
SG2124G(config-vlan)#exit
SG2124G(config)#interface range ge1-2
% ge1-2 Selected
SG2124G(config-if-range)#switchport access vlan 10
SG2124G(config-if-range)#exit
SG2124G(config)#interface ge3
SG2124G(config-if)#switchport mode trunk
SG2124G(config-if)#switchport trunk allowed vlan add 10
SG2124G(config-if)#end
SG2124G#
SG2124G#show vlan 10
```

VLAN ID	Name	State	Bridge Group : 1 Member ports (u)-Untagged, (t)-Tagged
10	VLAN0010	ACTIVE	ge1(u) ge2(u) ge3(t)

```
SG2124G#
SG2124G#show vlan brief
```

VLAN ID	Name	State	Bridge Group : 1 Member ports (u)-Untagged, (t)-Tagged
1	default	ACTIVE	ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u) ge3(u)
10	VLAN0010	ACTIVE	ge1(u) ge2(u) ge3(t)

```
SG2124G#
```



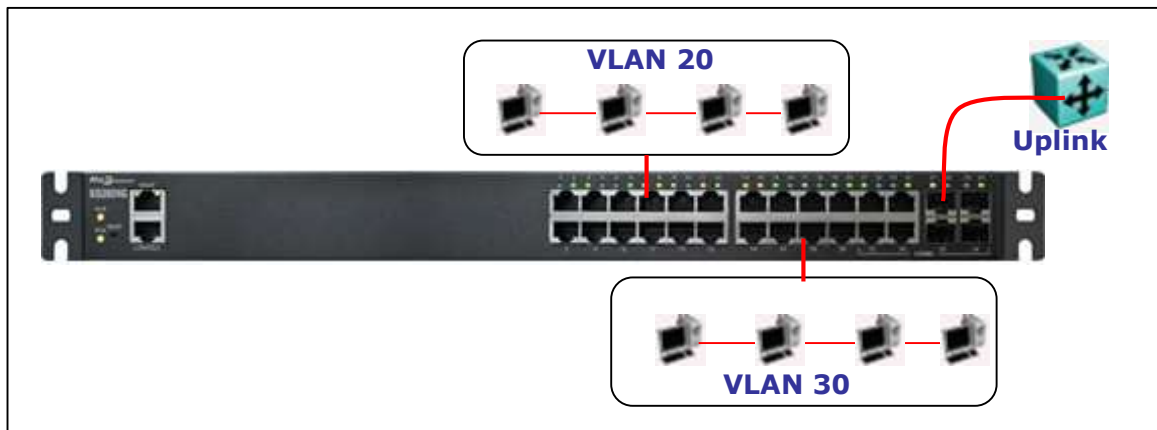
참고

Switch1의 Trunk Port로 설정된 Uplink Interface와 연결된 Switch2의 Interface의 경우 Switch1에 설정된 VLAN ID를 포함하는 Trunk Port로 연결되어야 통신이 가능합니다.

2.1.5 Hybrid VLAN 설정

SG Switch Series는 Layer2 전용 Switch로 Routing 기능이 없어 다수의 VLAN을 생성한 경우 VLAN 간의 통신이 불가능합니다. 특히, 다른 Switch와 Untagged로 연결된 Uplink Interface는 모든 VLAN으로부터 Packet을 받아야 하는데, 모든 VLAN에 속하도록 설정하지 않으면 Packet을 받을 수가 없습니다. 따라서 다수의 VLAN을 설정할 때에는 다음과 같이 Uplink Interface를 모든 VLAN에 속하도록 설정해야 합니다.

[그림 2-1] Hybrid VLAN 구성도



위의 그림과 같이 설정한 경우에서 VLAN20내의 PC에서 다른 VLAN과의 통신을 시도하면, Untagged Packet이 VLAN20으로 들어오게 됩니다. 해당 VID가 20이므로 Packet 내에 tag 20을 추가하여 전송하게 되고, Uplink Interface 역시 VLAN 20에 속하기 때문에 Packet 전송이 가능합니다. 그러나 Uplink Interface를 통해 외부로부터 들어오는 Untagged Packet은 어떤 VID를 가지고 어떤 Interface로 전송되어야 할 지를 알 수 없습니다.

외부로부터 Uplink Interface로 전송된 Untagged Packet을 다른 Interface에 전송할 수 있도록 하려면, Uplink Interface를 포함하는 모든 Interface를 구성원으로 하는 VLAN을 만들어야 Uplink Interface에서 모든 Interface의 존재를 알 수 있습니다.

따라서, 모든 VLAN에 Uplink Interface를 구성원으로 추가하고, 모든 Interface를 구성원으로 하는 VLAN을 생성하여 VLAN간의 통신이 되도록 설정해야 합니다.

Hybrid VLAN을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
shared-vlan VLAN_ID {block non-block}	VLAN	Hybrid VLAN내에 존재하는 다른 VLAN에 Broadcast Packet을 전달할 지에 대해 선택합니다.
interface range PORTRANGE	CONFIG	Interface 범위를 선택합니다.
switchport mode hybrid	INTERFACE	hybrid mode로 변경합니다.
switchport hybrid allowed vlan {add remove} VLAN_Range egress-tagged {enable disable}	INTERFACE	중첩 VLAN을 설정합니다. (최대 255개까지 동시 설정)
switchport hybrid native vlan <2-4094>	INTERFACE	Native VLAN을 설정합니다.
switchport hybrid vlan <2-4094>	INTERFACE	Interface에 VLAN을 설정합니다

생성된 VLAN 및 Member 정보를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show vlan <2-4094>	TOP	특정 VLAN 정보를 확인합니다.
show vlan all	TOP	모든 VLAN 정보를 확인합니다.
show vlan [brief]	TOP	모든 VLAN 정보를 확인합니다.

Hybrid VLAN을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no shared-vlan	VLAN	shared-vlan 설정을 초기화합니다.
switchport mode access	INTERFACE	Access VLAN 설정으로 초기화합니다.
no switchport hybrid native vlan	INTERFACE	Native VLAN 설정을 초기화합니다.
no switchport hybrid vlan	INTERFACE	설정된 VLAN을 초기화합니다.



참고

Hybrid VLAN으로 Switch를 구성한 경우, “show bridge” 명령어 실행 시 VLAN에 연결된 Interface에 보이는 MAC Address가 Uplink VLAN이 아닌 User VLAN으로 표시되어야 통신이 됩니다.

<예제1> Hybrid VLAN을 이용한 Access & Voice VLAN 설정

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#vlan database
SG2124G(config-vlan)#vlan 10 bridge 1 name Access state enable
SG2124G(config-vlan)#vlan 20 bridge 1 name Voice state enable
SG2124G(config-vlan)#exit
SG2124G(config)#
SG2124G(config)#interface range all
% all Selected
SG2124G(config-if-range)#switchport mode hybrid
% all Selected
SG2124G(config-if-range)#switchport hybrid vlan 10
% all Selected
SG2124G(config-if-range)#switchport hybrid allowed vlan add 20 egress-tagged enable
% all Selected
SG2124G(config-if-range)#end
SG2124G#
SG2124G#show vlan brief

```

VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
1	default	ACTIVE	
10	Access	ACTIVE	ge1(u) ge2(u) ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u)
20	Voice	ACTIVE	ge1(t) ge2(t) ge3(t) ge4(t) ge5(t) ge6(t) ge7(t) ge8(t) ge9(t) ge10(t) ge11(t) ge12(t) ge13(t) ge14(t) ge15(t) ge16(t) ge17(t) ge18(t) ge19(t) ge20(t) ge21(t) ge22(t) ge23(t) ge24(t)

```

SG2124G#show running-config
- 요약 -
vlan database
vlan 10 bridge 1 name access
vlan 20 bridge 1 name voice
!
interface ge1
bridge-group 1
switchport mode hybrid
switchport hybrid vlan 10
switchport mode hybrid acceptable-frame-type all
switchport hybrid allowed vlan add 20 egress-tagged enable
switchport hybrid allowed vlan add 10 egress-tagged disable
-- 이하 생략 --

```

<예제2> Hybrid VLAN 설정

ge1-11는 VLAN 10, ge12-22는 VLAN 20의 Member로 지정

ge23-24는 VLAN 30으로 지정 후 VLAN 10,20의 Hybrid VLAN으로 지정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#vlan database
SG2124G(config-vlan)#vlan range 10,20,30 bridge 1
SG2124G(config-vlan)#shared-vlan 30 block
SG2124G(config-vlan)#exit
SG2124G(config)#interface range all
% all Selected
SG2124G(config-if-range)#switchport mode hybrid
% all Selected
SG2124G(config-if-range)#switchport hybrid allowed vlan add 30 egress-tagged disable
% all Selected
SG2124G(config-if-range)#exit
SG2124G(config)#interface range ge1-11
% ge1-11 Selected
SG2124G(config-if-range)#switchport hybrid vlan 10
% ge1-11 Selected
SG2124G(config-if-range)#exit
SG2124G(config)#interface range ge12-22
% ge12-22 Selected
SG2124G(config-if-range)#switchport hybrid vlan 20
% ge12-22 Selected
SG2124G(config-if-range)#exit
SG2124G(config)#interface range ge23-24
% ge23-24 Selected
SG2124G(config-if-range)#switchport mode hybrid
% ge23-24 Selected
SG2124G(config-if-range)#switchport hybrid vlan 30
% ge23-24 Selected
SG2124G(config-if-range)#switchport hybrid allowed vlan add 10 egress-tagged disable
% ge23-24 Selected
SG2124G(config-if-range)#switchport hybrid allowed vlan add 20 egress-tagged disable
% ge23-24 Selected
SG2124G(config-if-range)#end
SG2124G#
SG2124G#show vlan brief
```

Bridge Group : 1

VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
1	default	ACTIVE	
10	VLAN0010	ACTIVE	ge1(u) ge2(u) ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge23(u) ge24(u)
20	VLAN0020	ACTIVE	ge12(u) ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u)
30	VLAN0030	ACTIVE	ge1(u) ge2(u) ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u)

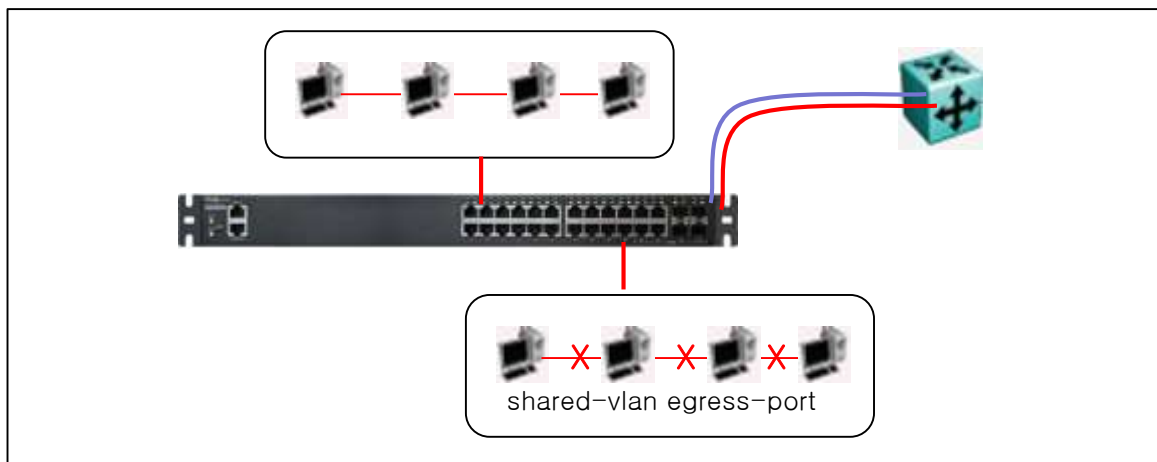
```
SG2124G#show bridge
bridge      VLAN port      mac          fwd timeout
1           10  ge3       0017.420c.d547 1    300
1           20  ge15      000c.f1c0.662b 1    300
1           30  ge24      001a.f400.0101 1    300
1           30  ge24      0002.b3af.b9fd 1    300
1           30  ge24      0002.b3e9.5fa3 1    300
SG2124G#
```

2.1.6 Shared-VLAN Egress-Port 설정

동일한 Network에 있는 사용자들이 서로의 보안(security)을 보장받으며 인터넷 통신을 가능하게 하기 위해 Uplink Interface와의 통신만 가능하게 하고 그 이외의 Interface와의 통신을 차단하는 기능입니다.

shared-vlan egress-port로 설정된 Interface는 Uplink Interface 이외의 Interface로부터 전송되는 Unicast, Multicast, Broadcast 등 모든 Traffic으로부터 보호를 받게 됩니다.

[그림 2-2] shared-vlan egress-port Traffic 흐름



shared-vlan egress-port를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
shared-vlan <i>VLAN_ID</i> {block non-block}	VLAN	Hybrid VLAN내에 존재하는 다른 VLAN에 Broadcast Packet을 전달할 지에 대해 선택합니다.
interface range <i>PORTRANGE</i>	CONFIG	Port Range를 선택합니다.
switchport shared-vlan egress-port <i>IFNAME</i>	INTERFACE	특정 Interface를 Uplink Interface로 설정합니다.

생성된 VLAN 및 Member 정보를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show vlan <2-4094>	TOP	특정 VLAN 정보를 확인합니다.
show vlan all	TOP	모든 VLAN 정보를 확인합니다.
show vlan [brief]	TOP	모든 VLAN 정보를 확인합니다.

shared-vlan egress-port를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no shared-vlan	VLAN	shared-vlan 설정을 초기화합니다.
no switchport shared-vlan egress-port	INTERFACE	설정된 VLAN egress-port를 초기화합니다.

<예제1> shared-vlan egress-port 설정

ge1-12 : Interface간 통신 제한. 모든 Traffic은 ge24 Interface를 통해서만 통신되도록 설정.

ge13-23 : Interface간 통신 허용. egress-port로 설정된 Interface와는 통신 제한

```
SG2124G#configure terminal
SG2124G(config)#interface range ge1-12
% ge1-12 Selected
SG2124G(config-if-range)#switchport shared-vlan egress-port ge24
% ge1-12 Selected
SG2124G(config-if-range)#end
SG2124G#sh run
--- 중 략 ---
!
bridge 1 protocol pvstp
!
spanning-tree mst config
!
mls qos enable
mds enable ge1-22 detect
mds uplink ge23-24
!
interface ge1
switchport shared-vlan egress-port ge24
!
interface ge2
switchport shared-vlan egress-port ge24
!
-- 이하 생략 --
```



참고

shared-vlan egress-port는 ge1-24, po1-12, sa1-12 의 Interface 중 최대 2개까지 지정할 수 있습니다.

<예제2> Hybrid VLAN과 shared-vlan egress-port를 설정

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#vlan database
SG2124G(config-vlan)#vlan range 10,20,30 bridge 1
SG2124G(config-vlan)#shared-vlan 30 block
SG2124G(config-vlan)#exit
SG2124G(config)#interface range all
% all Selected
SG2124G(config-if-range)#switchport mode hybrid
% all Selected
SG2124G(config-if-range)#switchport hybrid allowed vlan add 30 egress-tagged disable
% all Selected
SG2124G(config-if-range)#exit
SG2124G(config)#interface range ge1-12
% ge1-12 Selected
SG2124G(config-if-range)#switchport hybrid vlan 10
% ge1-12 Selected
SG2124G(config-if-range)#exit
SG2124G(config)#interface range ge13-23
% ge13-23 Selected
SG2124G(config-if-range)#switchport hybrid vlan 20
% ge13-23 Selected
SG2124G(config-if-range)#exit
SG2124G(config)#interface ge24
% ge24 Selected
SG2124G(config-if)#switchport hybrid vlan 30
% ge24 Selected
SG2124G(config-if)#switchport hybrid allowed vlan add 10 egress-tagged disable
% ge24 Selected
SG2124G(config-if)#switchport hybrid allowed vlan add 20 egress-tagged disable
% ge24 Selected
SG2124G(config-if)#exit
SG2124G(config)#interface range ge13-23
% ge13-23 Selected
SG2124G(config-if-range)#switchport shared-vlan egress-port ge24
% ge13-23 Selected
SG2124G(config-if)#end
SG2124G#
SG2124G#show vlan brief

```

Bridge Group : 1

VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
1	default	ACTIVE	
10	VLAN0010	ACTIVE	ge1(u) ge2(u) ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) ge24(u)
20	VLAN0020	ACTIVE	ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u)
30	VLAN0030	ACTIVE	ge1(u) ge2(u) ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u)

```
SG2124G#  
SG2124G#show bridge  
bridge      VLAN port      mac          fwd timeout  
1           10  ge3       0017.420c.d547 1    300  
1           20  ge15      000c.f1c0.662b 1    300  
1           30  ge24      001a.f400.0101 1    300  
1           30  ge24      0002.b3af.b9fd 1    300  
1           30  ge24      0002.b3e9.5fa3 1    300  
SG2124G#
```

2.1.7 MAC / IP / Protocol Based VLAN

관리자는 특정 Host의 MAC / IP / Protocol을 바탕으로 Interface의 이동과 관계없이 Dynamic하게 VLAN을 할당할 수 있습니다.

MAC Based VLAN은 Port Based VLAN에서 Interface별로 해당 VLAN를 지정한 것과 같이 Network Device별로 해당 VLAN를 지정하는 방식으로 Port Based VLAN 구성과 크게 차이가 나지 않습니다. Network 상에서 Computer가 추가 / 삭제되어도 연결되는 Switch Interface와는 무관하게 동일한 VLAN의 Member가 됩니다. 또한, 하나의 Interface에서 연결된 하단 Hub로 구성한 Network Segment의 Computer들도 서로 다른 VLAN의 Member가 되도록 설정할 수 있습니다.

하지만, MAC Address별로 해당되는 VLAN을 Administrator가 mapping하여 관리해야 하기 때문에, Network Device가 많이 존재하는 Network에서는 번거로운 방식입니다. 또한 NIC가 교체되어 MAC Address가 변경된다면 User의 VLAN이 변경될 수도 있습니다.

IP Based VLAN은 TCP/IP Network Environment에서 구성된 Subnet별로 VLAN을 구성할 수 있어 MAC Address 당 소속 VLAN을 표기하여 DB를 구현하는 MAC Based VLAN 보다 효율적이고, User의 NIC 교체에도 쉽게 대처할 수 있습니다. 그러나 모든 Computer들이 DHCP를 사용하는 환경에서는 사용하지 못하며 Fixed IP Address를 사용해야 하는 단점이 있습니다.

Protocol Based VLAN은 IPX와 같은 특정 Protocol을 이용하는 경우 동일 Protocol을 사용하는 장비들에 대해 어디에 연결되었는지 동일 VLAN으로 동작하도록 설정할 수 있습니다.

MAC/ IP / Protocols VLAN을 생성하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
vlan classifier rule <1-256> ipv4 <i>IP_Addr/MASK</i> vlan <i>VLAN_ID</i>	CONFIG	IP Based VLAN을 설정합니다.
vlan classifier rule <1-256> mac <i>MAC_Addr</i> vlan <i>VLAN_ID</i>	CONFIG	MAC Based VLAN을 설정합니다.
vlan classifier rule <1-256> proto <i>PROTOCOLS</i> encap {ethv2 nosnapllc snapllc} vlan <i>VLAN_ID</i>	CONFIG	Protocol Based VLAN을 설정합니다.
vlan classifier group <1-16> {add delete} rule <1-256>	CONFIG	Classifier Group ID를 생성합니다.
vlan classifier activate <1-16>	CONFIG	Classifier Group ID를 활성화합니다.

MAC / IP / Protocols VLAN 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show vlan classifier group [<1-16>]	TOP	Classifier Group에 적용된 Rule을 확인합니다.
show vlan classifier rule [<1-256>]	TOP	Classifier Rule의 내용을 확인합니다.

MAC / IP / Protocols VLAN을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no vlan classifier rule <1-256>	CONFIG	Classifier Rule의 설정 내용을 초기화합니다.
no vlan classifier group <1-16>	CONFIG	Classifier Group의 설정 내용을 초기화합니다.
no vlan classifier activate	CONFIG	Classifier Group ID를 비활성화합니다.



참고

MAC / IP / Protocol Based VLAN을 활성화하려면 Interface들은 Hybrid Mode 또는 Trunk Mode로 설정되어야 합니다.

<예제> MAC Based VLAN 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#
SG2124G(config)#vlan database
SG2124G(config-vlan)#vlan range 2-10 bridge 1
SG2124G(config-vlan)#exit
SG2124G(config)#
SG2124G(config)#interface range all
% all Selected
SG2124G(config-if-range)#switchport mode hybrid
% all Selected
SG2124G(config-if-range)#switchport hybrid allowed vlan add 2-10 egress-tagged
disable
% all Selected
SG2124G(config-if-range)#exit
SG2124G(config)#
SG2124G(config)#vlan classifier rule 1 mac 0000.4241.5678 vlan 10
SG2124G(config)#vlan classifier rule 2 mac 0000.4241.1234 vlan 10
SG2124G(config)#vlan classifier group 1 add rule 1
SG2124G(config)#vlan classifier group 1 add rule 2
SG2124G(config)#vlan classifier activate 1
SG2124G(config)#end
SG2124G#
SG2124G#show vlan classifier group
vlan classifier group 1 add rule 1
vlan classifier group 1 add rule 2
SG2124G#
SG2124G#show vlan classifier rule
vlan classifier rule 1 mac 0000.4241.5678 vlan 10
vlan classifier rule 2 mac 0000.4241.1234 vlan 10
SG2124G#
SG2124G#show bridge | include 5678
1          10   ge1          0000.4241.5678 1      300
SG2124G#
```

2.1.8 GVRP 설정

GVRP는 VLAN 기능이 있는 Switch 등이 자신의 Default VLAN을 제외한 다른 VLAN 정보를 다른 Switch 등에게 알리는데 사용되는 Protocol로서, GVRP를 수신한 Switch는 다른 Switch에게도 이 Frame을 전달하게 됩니다. GVRP에 있는 VID 값은 이것을 수신하는 측에게 VID를 가진 Member가 있다는 것을 알려주어 자신의 FDB의 Dynamic VLAN Registration Entry에 해당 VID를 등록합니다. GVRP를 사용하여 VLAN Membership을 등록하는 과정은 Multicast Group을 등록할 때 사용하는 GMRP의 동작과 유사하나, GMRP의 값으로는 Multicast용 MAC주소가 사용되지만 GVRP의 경우 12 비트의 VID 값이 사용되는 점이 다릅니다.

예를 들어, Switch 1에 연결된 단말이 GVRP(VID = 10)인 등록요청을 보내왔다면, Switch 1은 자신의 Interface 1에 VID = 10의 Member가 있으니, 이쪽으로 향하는 Packet이 다른 Switch나 다른 Interface로부터 수신되면 이 단말에게 전달하도록 동작합니다. 또한, 이 요청은 Spanning Tree에 있는 이웃 Switch에게도 전달되는데, 요청을 받은 Switch는 GVRP가 수신된 Interface 2를 VID = 10으로 설정하여 자신의 Down Stream에 VID=10인 Member가 있음을 등록합니다.

GVRP를 설정하여 Dynamic VLAN을 생성하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
set gvrp enable bridge 1	CONFIG	gvrp를 enable합니다.
set gvrp applicant state {active normal} <i>PORTRANGE</i>	CONFIG	gvrp applicant의 상태를 설정합니다.
set gvrp registration {fixed forbidden normal} <i>PORTRANGE</i>	CONFIG	gvrp registration을 설정합니다.
set gvrp timer {join leave leaveall} TIME_VALUE <i>IFNAME</i>	CONFIG	gvrp timer를 설정합니다. (Default: Join : 20 ms, Leave : 60 ms, LeaveAll : 1 000 ms)
set port gvrp enable <i>PORTRANGE</i>	CONFIG	gvrp를 설정할 Interface를 지정합니다.

GVRP를 설정하여 생성된 Dynamic VLAN을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show gvrp timer <i>IFNAME</i>	TOP	설정된 gvrp timer의 값을 확인합니다.
show gvrp statistics [<i>IFNAME</i>]	TOP	gvrp Packet의 통계 정보를 확인합니다.

show gvrp configuration	TOP	gvrp 설정 내용을 확인합니다.
show gvrp machine	TOP	gvrp 상태를 확인합니다.
show vlan {all brief classifier dynamic static vlan-stacking}	TOP	설정된 VLAN 정보를 확인합니다.

GVRP를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
set gvrp disable bridge 1	CONFIG	gvrp를 disable합니다.
set port gvrp disable <i>PORTRANGE</i>	CONFIG	interface에 설정된 gvrp를 초기화합니다.
clear gvrp statistics <i>IFNAME</i>	CONFIG	gvrp 통계 정보를 초기화합니다.



참 고

GVRP를 송수신하는 Interface는 Tagged Member이어야 합니다.

[표 2-1] show gvrp machine의 state 값 (GARP 표준)

Applicant state	Registrar state
VA : Very Anxious Active	INN : In Normal Registration
AA : Anxious Active	LV : Leave Normal Registration
QA : Quiet Active	L3 : Leave countdown3 Normal Registration
LA : Leaving Active	L2 : Leave countdown2 Normal Registration
VP : Very Anxious Passive	L1 : Leave countdown1 Normal Registration
AP : Anxious Passive	MT : Empty Normal Registration
QP : Quiet Passive	INR : In Fixed Registration
VO : Very Anxious Observer	LVR : Leave Fixed Registration
AO : Anxious Observer	L3R : Leave countdown3 Fixed Registration
QO : Quiet Observer	L2R : Leave countdown2 Fixed Registration
LO : Leaving Observer	L1R : Leave countdown1 Normal Registration
VON : Very Anxious Observer Nonparticipant	MTR : Empty Fixed Registration
AON : Anxious Observer Nonparticipant	INF : In Forbidden Registration
QON : Quiet Observer Non-Participant MAX	LVF : Leave Forbidden Registration
	L3F : Leave countdown3 Forbidden Registration
	L2F : Leave countdown2 Forbidden Registration
	L1F : Leave countdown1 Forbidden Registration
	MTF : Empty Forbidden Registration MAX

<예제1> GVRP 설정

- Switch-1 : ge24 trunk mode, vlan 10,20
- Switch-2 : ge24 trunk mode, vlan 30

-- Switch-1 --

```
SG2124G-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G-1(config)#vlan database
SG2124G-1(config-vlan)#vlan range 10,20 bridge 1
SG2124G-1(config-vlan)#exit
SG2124G-1(config)#interface ge24
SG2124G-1(config-if)#switchport mode trunk
SG2124G-1(config-if)#switchport trunk allowed vlan add 10,20
SG2124G-1(config-if)#exit
SG2124G-1(config)#set gvrp enable bridge 1
SG2124G-1(config)#set port gvrp enable ge24
SG2124G-1(config)#interface ge1
SG2124G-1(config-if)#switchport access vlan 10
SG2124G-1(config-if)#exit
SG2124G-1(config)#interface ge2
SG2124G-1(config-if)#switchport access vlan 20
SG2124G-1(config-if)#end
SG2124G-1#show vlan brief
```

→ Switch-2 에 gvrp 설정하기 전 VLAN 상태

Bridge Group : 1

VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
1	default	ACTIVE	ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u)
10	VLAN0010	ACTIVE	ge24(t) ge1(u)
20	VLAN0020	ACTIVE	ge24(t) ge2(u)

SG2124G-1#

```
SG2124G-1#show vlan brief
```

→ Switch-2 에 gvrp 설정한 후 VLAN 상태

Bridge Group : 1

VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
1	default	ACTIVE	ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u)
10	VLAN0010	ACTIVE	ge24(t) ge1(u)
20	VLAN0020	ACTIVE	ge24(t) ge2(u)
30	*VLAN0030	ACTIVE	ge24(t)

SG2124G-1#

-- Switch-2 --

```
SG2124G-2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G-2(config)#vlan database
```

```

SG2124G-2(config-vlan)#vlan range 30 bridge 1
SG2124G-2(config-vlan)#exit
SG2124G-2(config)#interface ge24
SG2124G-2(config-if)#switchport mode trunk
SG2124G-2(config-if)#switchport trunk allowed vlan add 30
SG2124G-2(config-if)#exit
SG2124G-2(config)#set gvrp enable bridge 1
SG2124G-2(config)#set port gvrp enable ge24
SG2124G-2(config)#interface ge1
SG2124G-2(config-if)#switchport access vlan 30
SG2124G-2(config-if)#end
SG2124G-2#show vlan brief   → Switch-1 에 gvrp 설정하기 전 VLAN 상태

```

Bridge Group : 1

VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
1	default	ACTIVE	ge2(u) ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u)
30	VLAN0030	ACTIVE	ge24(t) ge1(u)

SG2124G-2#

```

SG2124G-2#show vlan brief   → Switch-1 에 gvrp 설정한 후 VLAN 상태

```

Bridge Group : 1

VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
1	default	ACTIVE	ge2(u) ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u)
10	*VLAN0010	ACTIVE	ge24(t)
20	*VLAN0020	ACTIVE	ge24(t)
30	VLAN0030	ACTIVE	ge24(t) ge1(u)

SG2124G-2#

```

SG2124G-2#show vlan dynamic

```

VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
10	*VLAN0010	ACTIVE	ge24(t)
20	*VLAN0020	ACTIVE	ge24(t)

SG2124G-2#

<예제2> GVRP 설정 확인

```
SG2124G#show gvrp configuration
```

```
Global GVRP Configuration for bridge 1:
```

```
Dynamic Vlan Creation: Enabled
```

```
Port based GVRP Configuration:
```

Port	GVRP Status	Registration	Applicant	Timers(centiseconds)		
				Join	Leave	LeaveAll
ge24	Enabled	Normal	Normal	20	60	1000

```
SG2124G#
```

```
SG2124G#show gvrp machine bridge 1
```

```
port = ge24
```

```

applicant state[0] = QA registrar state[0] = INR
applicant state[1] = QA registrar state[1] = INR
applicant state[2] = QA registrar state[2] = INR
applicant state[3] = Q0 registrar state[3] = INN

```

```
SG2124G#
```

```
SG2124G#show gvrp statistics
```

```
Bridge: 1
```

Port		JoinEmpty	JoinIn	LeaveEmpty	LeaveIn	Empty
ge24	RX	0	28	0	0	6
	TX	0	420	0	0	3

```
SG2124G#
```

```
SG2124G#show gvrp timer ge24
```

```
Timer Timer Value (centiseconds)
```

Join	20
Leave	60
Leave All	1000

```
SG2124G#
```

2.1.9 Voice VLAN

Voice VLAN으로 설정하는 Voice Traffic(특정 VLAN 또는 MAC OUI)의 경우 실시간으로 전송해야 서로간에 의미를 명확하게 전달할 수 있기 때문에 Voice VLAN으로 설정한 Traffic에 대해 자동으로 우선순위를 높여 Data Traffic보다 우선 전송하도록 하는 기능입니다.

Interface가 Hybrid Mode일 때만 Voice VLAN으로 설정이 가능합니다. Interface에 Voice VLAN을 설정하면 Syslog에 해당 Interface에 LLDP-MED가 활성화되었다는 Event가 저장되면서 LLDP-MED가 자동으로 활성화되며, LLDP-MED Policy Packet 및 CDP Packet이 전송됩니다. (CDP는 자동으로 활성화되지 않으므로 CDP가 Enable되어 있는 상태에서만 CDP Packet을 전송합니다.) LLDP-MED Packet은 VLAN, Tag, Default Priority, DSCP Option등을 포함하여 전송되며, LLDP-MED Packet을 수신하도록 설정된 전화기 등에서는 설정을 자동으로 변경합니다.

Interface에 설정된 Voice vlan 을 제거하여도 활성화되어 있는 LLDP가 자동으로 비활성화되지 않습니다. (LLDP를 비활성화 시키려면 "2.4 LLDP / LLDP MED"의 명령어를 참고하여 LLDP 비활성화 명령을 실행해야 합니다.)

- vlan VID : Voice VLAN에 해당하는 Traffic은 <vlan-id> 붙인 Tagged Frame (CoS5)을 보내며, Data Traffic(CoS0)은 untagged Frame 으로 전송하여 Voice Traffic이 우선 전송됩니다.
- Untagged : Voice Traffic도 untagged Frame (vlan-id 4095)으로 전송됩니다.
- dot1p : Voice Traffic은 Priority Tagged Frame (vlan-id 0, CoS5), Data Traffic은 untagged Frame으로 전송됩니다.

Voice VLAN을 생성하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
switchport voice vlan {VLANID dot1p untagged}	INTERFACE	Interface를 Voice VLAN Member로 설정합니다.
voice-vlan oui MAC_OUI [Description]	CONFIG	특정 MAC OUI를 Voice VLAN으로 설정합니다.
voice-vlan med {dscp <0-63> priority <0-7>}	CONFIG	LLDP-MED를 통한 Voice VLAN 전송 Packet의 값을 조정합니다. (Default: dscp 46, priority 5)

Voice VLAN을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
-----	----	----

show voice-vlan oui	TOP	Voice VLAN으로 지정된 MAC OUI를 확인합니다.
---------------------	-----	----------------------------------

Voice VLAN을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no switchport voice vlan	INTERFACE	Interface를 Voice VLAN Member에서 삭제합니다.
no voice-vlan oui <i>MAC_OUI</i>	CONFIG	특정 MAC OUI를 Voice VLAN으로 삭제합니다.
no voice-vlan med {dscp priority}	CONFIG	LLDP-MED를 통한 Voice VLAN 전송 Packet의 값을 초기화합니다.



참고

voice vlan 명령어는 hybrid Mode에서만 동작합니다.

<예제> Voice VLAN 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#vlan database
SG2124G(config-vlan)#vlan 10 bridge 1
SG2124G(config-vlan)#exit
SG2124G(config)#voice-vlan oui 00-00-01
SG2124G(config)#
SG2124G(config)#interface range ge1-2
% ge1-2 Selected
SG2124G(config-if-range)#switchport mode hybrid
% ge1-2 Selected
SG2124G(config-if-range)#switchport voice vlan dot1p
% ge1-2 Selected
SG2124G(config-if-range)#end
SG2124G#show voice-vlan oui
=====
Telephony OUI(s)   Description
-----
00-00-01-00-00-00
-----
SG2124G#show vlan brief
Bridge Group : 1

VLAN ID   Name               State   Member ports (u)-Untagged, (t)-Tagged
=====
```

```

1      default      ACTIVE ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u)
                                ge9(u) ge10(u) ge11(u) ge12(u) ge13(u)
                                ge14(u) ge15(u) ge16(u) ge17(u) ge18(u)
                                ge19(u) ge20(u) ge21(u) ge22(u) ge23(u)
                                ge24(u) ge1(u) ge2(u)
10     VLAN0010     ACTIVE

```

SG2124G#

SG2124G#**configure terminal**

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

SG2124G(config)#**interface range ge1-2**

% ge1-2 Selected

SG2124G(config-if-range)#**switchport voice vlan 10**

SG2124G(config-if-range)#**end**

SG2124G#**show vlan brief**

Bridge Group : 1

VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
1	default	ACTIVE	ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u) ge1(u) ge2(u)
10	VLAN0010	ACTIVE	ge1(t) ge2(t)

2.1.10 VLAN Stacking (QinQ) 설정

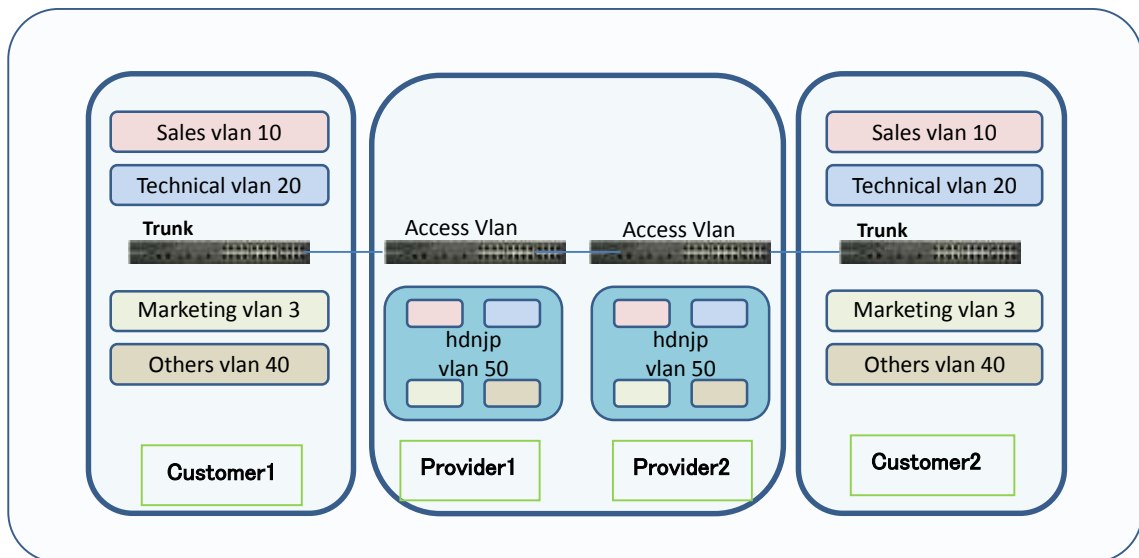
IEEE 802.1ad 표준에 따른 VLAN Stacking은 서로 다른 VLAN이 설정되어 있는 네트워크 간의 통신을 하나의 VLAN으로 가능하게 하기 위해 VLAN ID(VID)안에 또 다른 VLAN ID(Tag)를 삽입하여 논리적인 Network 구분이 가능한 VLAN으로 나누어 Packet을 전송하는 기능으로 QinQ, Provider Bridge 또는 Double Q-Tag라고도 합니다. 일반적으로 Provider와 customer로 구분하여 customer로 구분된 VID들은 대표 Vlan인 Provider Vlan ID에 포함되어 Packet이 전송되고, 해당 Packet을 전송 받은 Switch도 동일한 기능을 이용해 Provider VID 안에 Customer VID를 판독해 같은 VID의 VLAN으로 전송합니다.

VLAN Stacking는 복수의 VLAN을 Grouping한 802.1Q를 다시 802.1Q 여러 개로 나눠 Grouping하여 구성, 관리함으로써 전체적으로 관리하는 VLAN의 수를 줄여 Local Network 망을 확장할 수 있습니다.

[그림 2-3]에서 Customer1이 Customer2로 Packet을 전송하는 방법은 다음과 같습니다.

먼저 Customer1 에서 Provider1로 Packet이 전달되면, Provider1의 VLAN Stacking Interface를 통해 전송되는 Packet은 또 하나의 Tag가 추가되어 전송됩니다. 전송된 Packet은 VLAN Stacking Interface가 설정된 Provider2를 통해 목적지인 Customer2에 전달될 때에는 Provider Switch간에 추가된 Tag Packet을 제외한 Customer1에서 전송한 Packet의 Tag만 전송됩니다.

[그림 2-3] VLAN Stacking (QinQ) 구성



Interface에 VLAN Stacking을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
Interface range PORTRANGE	CONFIG	Interface 범위를 선택합니다.
switchport mode trunk	INTERFACE	Interface를 trunk mode로 설정합니다.
switchport trunk allowed vlan {add remove} VLANRANGE	INTERFACE	Interface에 VLAN을 설정합니다.
switchport vlan-stacking {customer-edge-port provider-port}	INTERFACE	VLAN Stacking의 종류를 설정합니다.

VLAN Stacking 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show vlan {VID brief}	TOP	VLAN 정보 및 Member를 확인합니다.

VLAN Stacking 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
switchport mode access	INTERFACE	Interface를 Access Mode로 설정합니다.
no switchport trunk	INTERFACE	Interface를 Access Mode로 설정합니다.
no switchport vlan-stacking	INTERFACE	VLAN Stacking 설정을 초기화합니다.



참고

1. Provider와 Customer Switch는 동일 VLAN을 사용하는 경우에도 통신이 안됩니다. Provider와 Customer Switch가 통신을 하기 위해서는 VLAN Stacking으로 구성되는 VLAN 이외의 별도 VLAN을 설정하여야 합니다.
2. Provider Switch는 Customer Switch와 연결되는 Interface를 Access Mode로 설정하여야 하며, Customer Switch는 Trunk Mode로 설정하여야 합니다.

<예제> VLAN Stacking 설정

- Customer1 : vlan10(ge1-10, sales), vlan20(ge11-15, technical), vlan30(ge16-18, Marketing), vlan40(ge19-20, Others), ge24 - Provider1과 연결(trunk)
- Provider1 : ge2 customer1과 연결(Customer1 vlan 의 대표 VID 설정)
ge1 Provider2와 연결(VLAN Stacking을 위한 Trunk VID 설정)
- Provider2 : ge2 customer2와 연결(Customer1 vlan 의 대표 VID 설정)
ge1 Provider1과 연결(VLAN Stacking을 위한 Trunk VID 설정)
- Customer2 : vlan10(ge1-10, sales), vlan20(ge11-15, technical), vlan30(ge16-18, Marketing), vlan40(ge19-20, Others), ge24 - Provider2과 연결(trunk)

```

=====
                                Customer1 설정
=====

Customer1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Customer1(config)#vlan database
Customer1(config-vlan)#vlan range 10,20,30,40,50 bridge 1
Customer1(config-vlan)#exit
Customer1(config)#interface vlan1.50
Customer1(config-if)#ip address 192.168.50.2/24
Customer1(config-if)#exit
Customer1(config)#interface ge24
Customer1(config-if)#switchport mode trunk
Customer1(config-if)#switchport trunk allowed vlan add 10,20,30,40,50
Customer1(config-if)#exit
Customer1(config)#interface range ge1-10
% ge1-10 Selected
Customer1(config-if-range)#switchport access vlan 10
% ge1-10 Selected
Customer1(config-if-range)#exit
Customer1(config)#interface range ge11-15
% ge11-15 Selected
Customer1(config-if-range)#switchport access vlan 20
% ge11-15 Selected
Customer1(config-if-range)#exit
Customer1(config)#interface range ge16-18
% ge16-18 Selected
Customer1(config-if-range)#switchport access vlan 30
% ge16-18 Selected
Customer1(config-if-range)#exit
Customer1(config)#interface range ge19-20
% ge19-20 Selected
Customer1(config-if-range)#switchport access vlan 40
% ge19-20 Selected
Customer1(config-if-range)#exit
Customer1(config)#exit
Customer1#
Customer1#show vlan brief

                                Bridge Group : 1

VLAN ID   Name                State   Member ports (u)-Untagged, (t)-Tagged
=====

```

```

1      default      ACTIVE ge21(u) ge22(u) ge23(u) ge24(u)
10     VLAN0010     ACTIVE ge24(t) ge1(u) ge2(u) ge3(u) ge4(u) ge5(u)
                                ge6(u) ge7(u) ge8(u) ge9(u) ge10(u)
20     VLAN0020     ACTIVE ge24(t) ge11(u) ge12(u) ge13(u) ge14(u)
                                ge15(u)
30     VLAN0030     ACTIVE ge24(t) ge16(u) ge17(u) ge18(u)
40     VLAN0040     ACTIVE ge24(t) ge19(u) ge20(u)
50     VLAN0050     ACTIVE ge24(t)

Customer1#

=====
                        Provider1 설정
=====

Provider1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Provider1(config)#vlan database
Provider1(config-vlan)#vlan 50 bridge 1
Provider1(config-vlan)#exit
Provider1(config)#interface vlan1.50
Provider1(config-if)#ip address 192.168.50.3/24
Provider1(config-if)#exit
Provider1(config)#interface ge2
Provider1(config-if)#switchport access vlan 50           → Customer1의 대표 VID
Provider1(config-if)#switchport vlan-stacking customer-edge-port → Customer1과
Provider1(config-if)#exit                                연결될 Port 설정
Provider1(config)#interface ge1
Provider1(config-if)#switchport mode trunk
Provider1(config-if)#switchport trunk allowed vlan add 50 → Provider1 Stacking VID
Provider1(config-if)#switchport vlan-stacking provider-port → Provider1과 연결될
Provider1(config-if)#end                                  Port 설정
Provider1#show vlan brief

                        Bridge Group : 1

VLAN ID   Name           State   Member ports (u)-Untagged, (t)-Tagged
=====
1          default      ACTIVE  ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u)
                                ge9(u) ge10(u) ge11(u) ge12(u) ge13(u)
                                ge14(u) ge15(u) ge16(u) ge17(u) ge18(u)
                                ge19(u) ge20(u) ge21(u) ge22(u) ge23(u)
                                ge24(u) ge1(u)
50         VLAN0050     ACTIVE  ge2(u) ge1(t)

Provider1#

=====
                        Provider2 설정
=====

Provider2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Provider2(config)#vlan database
Provider2(config-vlan)#vlan 50 bridge 1

```

```

Provider2(config-vlan)#exit
Provider2(config)#interface vlan1.50
Provider2(config-if)#ip address 192.168.50.4/24
Provider2(config-if)#exit
Provider2(config)#interface ge2
Provider2(config-if)#switchport access vlan 50
Provider2(config-if)#switchport vlan-stacking customer-edge-port
Provider2(config-if)#exit
Provider2(config)#interface ge1
Provider2(config-if)#switchport mode trunk
Provider2(config-if)#switchport trunk allowed vlan add 50
Provider2(config-if)#switchport vlan-stacking provider-port
Provider2(config-if)#end
Provider2#show vlan brief

```

→ Customer1의 대표 VID
→ Customer2와 연결될 Port 설정
→ Provider1 Stacking VID
→ Provider1과 연결될 Port 설정

Bridge Group : 1

VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
1	default	ACTIVE	ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u) ge11(u) ge12(u) ge13(u) ge14(u) ge15(u) ge16(u) ge17(u) ge18(u) ge19(u) ge20(u) ge21(u) ge22(u) ge23(u) ge24(u) ge1(u)
50	VLAN0050	ACTIVE	ge2(u) ge1(t)

Provider2#

Customer2 설정

```

Customer2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Customer2(config)#vlan database
Customer2(config-vlan)#vlan range 10,20,30,40,50 bridge 1
Customer2(config-vlan)#exit
Customer2(config)#interface vlan1.50
Customer2(config-if)#ip address 192.168.50.5/24
Customer2(config-if)#exit
Customer2(config)#interface ge24
Customer2(config-if)#switchport mode trunk
Customer2(config-if)#switchport trunk allowed vlan ad 10,20,30,40,50
Customer2(config-if)#exit
Customer2(config)#interface rang ge1-10
% ge1-10 Selected
Customer2(config-if-range)#switchport access vlan 10
% ge1-10 Selected
Customer2(config-if-range)#exit
Customer2(config)#interface range ge11-15
% ge11-15 Selected
Customer2(config-if-range)#switchport access vlan 20
% ge11-15 Selected
Customer2(config-if-range)#exit
Customer2(config)#interface range ge16-18
% ge16-18 Selected
Customer2(config-if-range)#switchport access vlan 30

```

```

% ge16-18 Selected
Customer2(config-if-range)#exit
Customer2(config)#interface range ge19-20
% ge19-20 Selected
Customer2(config-if-range)#switchport access vlan 40
% ge19-20 Selected
Customer2(config-if-range)#end
Customer2#show vlan brief

```

Bridge Group : 1

VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
1	default	ACTIVE	ge21(u) ge22(u) ge23(u) ge24(u)
10	VLAN0010	ACTIVE	ge24(t) ge1(u) ge2(u) ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u)
20	VLAN0020	ACTIVE	ge24(t) ge11(u) ge12(u) ge13(u) ge14(u) ge15(u)
30	VLAN0030	ACTIVE	ge24(t) ge16(u) ge17(u) ge18(u)
40	VLAN0040	ACTIVE	ge24(t) ge19(u) ge20(u)
50	VLAN0050	ACTIVE	ge24(t)

Customer2#

2.2 Link Aggregation

Link Aggregation은 여러 개의 물리적인 여러 개의 Ethernet 대역폭을 고속으로 Data를 처리할 수 있는 한 개의 논리적인 Interface로 만들어 하나의 커다란 대역폭으로 확장하는 것을 의미하며, Load balancing, redundancy 효과를 얻을 수 있습니다. Link Aggregation에 속하는 Interface들을 Link Aggregation Group이라고 부르고 Member 중 하나의 Interface를 지정해서 그 Group의 Master Interface로 간주합니다.

Link Aggregation Group의 모든 Interface는 같은 VLAN에 속해야 하고, STP 상태, Static Multicast, Traffic 제어, Traffic Segmentation, 802.1p Default Priority, Speed 및 Full Duplex 설정 등이 모두 동일하게 설정되어야 합니다.

Link Aggregation으로 생성된 가상의 Interface에는 Interface 잠금, Interface Mirroring, 802.1x 기능이 설정되어서는 안됩니다.

■ Link Aggregation의 장점

- Link 사용률을 높입니다.
 - Link Aggregation Group에 속한 Link들은 서로간에 동적으로 백업이 되어 연결된 Link 중 하나가 죽으면 나머지 Link들이 거의 순간적으로 Traffic을 접수합니다.
- Link 성능을 향상 시킵니다.
 - 연결된 두 Switch 사이의 대역폭을 향상시킵니다. 2개 이상의 Link는 연결된 Link를 모두 합한 값에 해당하는 대역폭을 지원합니다.

■ Link Aggregation의 두 가지 방법

- Static
 - Aggregated port group 의 동적인 변화를 허용하지 않습니다.
- IEEE 802.3ad(LACP)
 - Switch와 다른 Network 장비 간에 동적 aggregated link를 협상하는데 사용됩니다



참고

표준으로 타사 장비와 연동해야 할 경우 LACP로 설정합니다.

2.2.1 Static Channel Group

Static-Channel-Group은 두 개 이상의 Interface를 하나의 논리적인 Interface로 통합하여 보다 넓은 대역폭을 사용할 수 있도록 하는 기능입니다.

Static-Channel-Group의 Member로 지정된 Interface는 기존 VLAN의 Member에서 자동으로 삭제되며 생성된 통합 Interface는 자동으로 Default VLAN(VLAN1.1)의 Member로 지정됩니다. 따라서, Member Interface와 통합 Interface가 Default VLAN(VLAN1.1)이 아닌 다른 VLAN에 존재하고 있었다면 생성된 통합 Interface에 대해 VLAN 설정을 변경해 주어야 합니다.

Static-Channel-Group을 사용하여 Interface를 통합하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
interface range <i>PORTRANGE</i>	CONFIG	Interface 범위를 선택합니다.
static-channel-group <1-24>	INTERFACE	Static-channel-group을 설정합니다.

Static-Channel-Group 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show static-channel-group	TOP	설정 내용을 확인합니다.

Static-Channel-Group로 설정된 통합 Interface를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no static-channel-group	INTERFACE	Static-channel-group을 초기화합니다.

<예제> Static-Channel-Group 설정

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface range ge1-4
% ge1-4 Selected
SG2124G(config-if-range)#static-channel-group 1
% ge1-4 Selected
SG2124G(config-if-range)#exit
SG2124G(config)#exit
SG2124G#show static-channel-group
% Static Aggregator: sa1
% Member :
    ge1
    ge2
    ge3
    ge4
SG2124G#
SG2124G#configure terminal
SG2124G(config)#interface range ge1-4
% ge1-4 Selected
SG2124G(config-if-range)#no static-channel-group
% ge1-4 Selected
SG2124G(config-if-range)#exit
SG2124G(config)#exit
SG2124G#show static-channel-group
SG2124G#

```



참고

1. Static-Channel-Group으로 만들 수 있는 논리적인 Interface는 SG2124G에서 최대 12개(SG2148G는 최대 24개)까지 만들 수 있으며, 하나의 논리적인 Interface는 최대 8개의 Member Interface로 구성될 수 있습니다.
2. Static-Channel-Group을 설정하여 생성된 통합 Interface의 Interface 명칭은 sa<Number> 입니다.

2.2.2 LACP

IEEE 802.3ad 표준에 따른 LACP (Link Aggregation Control Protocol)은 Static-Channel-Group 기능과 같이 두 개 이상의 Interface를 하나의 논리적인 Interface로 통합하여 보다 더 넓은 대역폭을 사용할 수 있도록 하는 기능입니다.

Interface를 통합할 논리적인 통합 Interface (Aggregator)와 논리적인 Interface로 통합할 물리적인 Member Interface만 설정해두면 자동으로 통합된 대역폭을 형성합니다.

Channel-Group의 Member로 지정된 Interface는 기존 VLAN의 Member에서 자동으로 삭제되며 생성된 통합 Interface는 자동으로 Default VLAN(VLAN1.1)의 Member로 지정됩니다. 따라서, Member Interface와 통합 Interface가 Default VLAN(VLAN1.1)이 아닌 다른 VLAN에 존재하고 있었다면 생성된 통합 Interface에 대해 VLAN 설정을 변경해 주어야 합니다.

Switch에 LACP를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
interface range <i>PORTRANGE</i>	CONFIG	Interface 범위를 선택합니다.
channel-group <1-65535> mode { active passive }	INTERFACE	LACP를 Active 또는 Passive 모드로 설정합니다.

LACP 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show port etherchannel <i>IFNAME</i>	TOP	Interface에 설정된 LACP Mode등을 확인합니다.
show etherchannel [<1-65535> detail load-balance summary]	TOP	설정 내용을 확인합니다.
show lacp sys-id	TOP	LACP System ID와 Priority 값을 확인합니다.
show lacp-counter [<1-65535>]	TOP	LACPDUs 정보를 확인합니다.

Switch에 LACP를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no channel-group	INTERFACE	LACP로 설정된 Interface를 초기화합니다.

<예제> LACP 설정

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface range ge1-4
% ge1-4 Selected
SG2124G(config-if-range)#channel-group 1 mode active
% ge1-4 Selected
SG2124G(config-if-range)#end
SG2124G#show etherchannel
% LACP Aggregator: po1
% Member :
    ge1
    ge2
    ge3
    ge4
SG2124G#show lacp sys-id
% System 8000,00-1a-f4-00-05-41
SG2124G#show lacp-counter
% Traffic statistics
Port      LACPDUs      Marker      Pckt err
      Sent  Recv  Sent  Recv  Sent  Recv
% Aggregator po1 1000000
ge3      10    0    0    0    0    0
SG2124G#

```



참고

1. LACP로 만들 수 있는 논리적인 Interface는 SG2124G에서 최대 12개 (SG2148G는 최대 24개)까지 만들 수 있으며, 하나의 논리적인 Interface는 최대 8개의 Member Interface로 구성될 수 있습니다.
2. Channel-Group을 설정하여 생성된 통합 Interface 명칭은 po<Number> 입니다.

2.2.3 Load Balance 설정

Link Aggregation으로 설정한 통합 Interface로 들어오는 Packet들은 지정된 기준에 따라 각 Member Interface에 분산되어 처리됩니다. 이 방법은 특정 Member Interface로의 Traffic 집중을 방지하여 보다 안정적이고 효율적으로 통합 Interface를 관리할 수 있도록 합니다.

[표 2-2] Load Balance 방법

분배 방식	설 명
dst-ip	Destination IP Address를 기준으로 Packet을 분배합니다.
dst-mac	Destination MAC Address를 기준으로 Packet을 분배합니다.
src-dst-ip	Source 및 Destination IP Address를 기준으로 Packet을 분배합니다.
src-dst-mac	Source 및 Destination MAC Address를 기준으로 Packet을 분배합니다.
src-ip	Source IP Address를 기준으로 Packet을 분배합니다.
src-mac	Source MAC Address를 기준으로 Packet을 분배합니다. (Default)

통합 Interface의 Load Balance를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
port-channel load-balance { <i>dst-ip</i> <i>dst-mac</i> <i>src-dst-ip</i> <i>src-dst-mac</i> <i>src-ip</i> <i>src-mac</i> }	INTERFACE {po1 sa1}	Link Aggregation으로 설정된 통합 Interface를 경유하는 Packet의 처리 방법을 설정합니다.

통합 Interface의 Load Balance 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show etherchannel load-balance	TOP	설정 내용을 확인합니다.

통합 Interface의 Load Balance를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no port-channel load-balance	INTERFACE {po1 sa1}	Link Aggregation으로 설정된 통합 Interface를 경유하는 Packet의 처리 방법을 초기화합니다.

<예제1> static-channel-group의 Load Balance의 설정 변경

```
SG2124G#show etherchannel load-balance
% LACP Aggregator: sa1
Source Mac address
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface sa1
SG2124G(config-if)#port-channel load-balance src-dst-mac
SG2124G(config-if)#end
SG2124G#show etherchannel load-balance
% LACP Aggregator: sa1
Source and Destination Mac address
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface sa1
SG2124G(config-if)#no port-channel load-balance
SG2124G(config-if)#end
SG2124G#show etherchannel load-balance
% LACP Aggregator: sa1
Source Mac address
SG2124G#
```

<예제2> LACP의 Load Balance의 설정 변경

```
SG2124G#show etherchannel load-balance
% LACP Aggregator: po1
Source Mac address
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface po1
SG2124G(config-if)#port-channel load-balance dst-mac
SG2124G(config-if)#end
SG2124G#show etherchannel load-balance
% LACP Aggregator: po1
Destination Mac address
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface po1
SG2124G(config-if)#no port-channel load-balance
SG2124G(config-if)#end
SG2124G#show etherchannel load-balance
% LACP Aggregator: po1
Source Mac address
SG2124G#
```

2.3 Redundancy

2.3.1 SPR(Smart Port Redundancy)

SPR 기능은 STP를 지원하지 않는 Dummy Switch등과의 연결 시 Cable을 이중화하여 하나의 Interface 또는 Cable에 장애가 발생한 경우 두 번째 Interface 또는 Cable을 사용하여 Switch간 연결 구성을 유지하도록 하여 안정성을 높이고, Interface 또는 Cable의 이상으로 인한 Network 기능의 정지 등의 가능성을 낮출 수 있는 기능입니다.

Link Up인 2개의 Member Interface를 포함하는 Redundancy Group을 Auto Mode로 활성화하는 경우, 2개의 Interface 중 ifindex가 높은 Interface가 통신이 가능한 Active Mode로 동작하게 되며 다른 하나의 Interface는 통신이 불가능한 standby Mode로 동작하게 됩니다. 이 때 Standby Mode로 동작하는 Interface의 상태는 admin down(shutdown) 상태로 표시합니다. 하나의 Redundancy Group에 속한 Interface, Trunk Member Interface 혹은 Trunk 및 VLAN Interface는 다른 Redundancy Group에 포함될 수 없습니다.

Port Redundancy Group을 설정할 때 Interface를 Active Mode 또는 Standby Mode로 활성화하는 경우 Auto Mode로 활성화된 Interface보다 우선순위가 높게 설정되며, Port Redundancy Group의 Member Interface가 하나만 설정되어 있는 경우에는 해당 Member Interface는 Active Mode로 동작하게 됩니다.

Redundancy Group 내에서 Active Mode로 동작하는 Interface가 link down 될 경우, Standby Mode로 동작하던 Interface가 Active Mode로 변경되며 통신이 가능한 상태로 변경되면서 통신이 이루어집니다.

SPR 기능에 의한 Interface의 admin 제어가 Network 관리자에 의한 Interface admin 제어보다 우선순위가 더 높으며, SPR 기능에 의해 admin down되어 있는 Interface를 관리자가 강제로 admin up 시키려 할 경우에는 오류 Message가 출력되며 admin up 상태로 변경되지 않습니다.

SPR 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
interface range <i>PORTRANGE</i>	CONFIG	Interface 범위를 선택합니다.
redund-group <1-12> {active auto standby}	INTERFACE	Redundancy Group을 설정합니다.

SPR 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show redund-group	TOP	Redundancy Group을 확인합니다.

SPR 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no redund-group	INTERFACE	Redundancy Group을 설정을 초기화합니다.



참고

1. SPR의 Redundancy Group은 최대 12개를 만들 수 있으며, 하나의 Group은 최대 2개의 Interface로 구성될 수 있습니다.
2. 관리자가 admin down (shutdown) 시켜 놓은 Interface도 SPR 기능이 활성화되면 admin up 될 수 있습니다.
3. Trunk Member Interface 및 VLAN Interface에는 SPR 기능을 설정할 수 없습니다.
4. 하나의 Redundancy Group에 속한 Interface는 다른 Redundancy Group에 속할 수 없습니다
5. 두 개의 interface가 모두 Link Up인 경우에는 우선순위가 높은 interface가 항상 Active로 동작합니다.

<예제> SPR 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface range ge1-2
% ge1-2 Selected
SG2124G(config-if-range)#redund-group 1 auto
% ge1-2 Selected
SG2124G(config-if-range)#end
SG2124G#show redund-group
% Redundancy group: group1
% Member:
  ge1: config(auto), state(standby), link state(down)
  ge2: config(auto), state(active), link state(down)
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface range ge1-2
% ge1-2 Selected
SG2124G(config-if-range)#no redund-group
% ge1-2 Selected
SG2124G(config-if-range)#end
SG2124G#show redund-group
SG2124G#
```

2.3.2 SSR (Smart Switch Redundancy)

2대의 스위치간에 동일 그룹에 속한 두 포트를 이중화 하는 기능입니다. 1대의 스위치에서 하나의 그룹에는 하나의 포트만 포함됩니다.

Heartbeat 포트는 포트 이중화 상태처리를 위한 **heartbeat** 메시지를 주고 받는 전용 포트이며, 이 포트는 **access vlan** 모드입니다. 루프방지를 위해 시스템의 다른 포트들에 있는 **VLAN**과 중첩되지 않는 별도의 **VLAN**을 설정해야 합니다.

Heartbeat 포트 설정 시, 그 포트는 **STP**에서 제거됩니다. **Heartbeat** 포트 링크다운 발생 시 **master**로 전환됩니다. (두 대중 하나의 스위치가 재부팅 될 때 **Heartbeat** 포트가 링크다운 되므로 포트 절체를 위해선 **master**로 되어야만 하며, 운용 중 **heartbeat** 포트를 링크다운 시키면 이중화된 두 포트가 모두 링크업 되므로 루프가 발생할 수 있으므로 주의해야 합니다).

Redundancy 포트는 **Slave**일 경우 **shutdown**되며, **master**일 경우 **active** 상태가 되는 **downlink** 포트입니다. 두 대의 스위치에서 동일 그룹에 속한 포트끼리 **master-slave pair**가 되어 동작합니다.

스위치 내에서 포트는 하나의 포트 그룹에만 포함될 수 있으며, 각 포트 그룹은 하나의 포트만 할당됩니다. **Active** 모드와 **Standby** 모드(설정에 의해 결정됨)가 있으며, **Master role**과 **Slave role**(포트 이중화 상태에 의해 결정됨)이 있습니다. **Active** 모드로 설정한 포트가 **Master**가 되며, 모드가 같으면 **MAC** 주소가 낮은 스위치의 포트가 **Master**가 됩니다.

각 스위치는 **300 ms** 마다 **heartbeat** 메시지를 전송하며, **1 s**(**node-absent** 시간) 동안 **heartbeat** 메시지가 수신되지 않으면 상대방 스위치가 다운된 것으로 판단하고 **master**로 전환됩니다. 또한 **Heartbeat** 포트가 **link down**되면 **heartbeat-fault** 시간 경과 후 **master**로 전환됩니다.

SSR 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
sw-port-redund redundancy-port <1-48> IFNAME {active standby}	CONFIG	특정 스위치 포트에 redundancy group 넘버를 할당하고, 그 그룹에서 포트의 모드를 설정합니다.
sw-port-redund heartbeat-port IFNAME	CONFIG	이중화된 스위치들이 heartbeat 메시지를 주고 받는 포트를 설정합니다.
sw-port-redund timer master-wait <1-60>	CONFIG	slave 포트에서 master 포트로 전환 시 루프방지를 위해 대기하는 시간을 설정합니다. (default 1 s)
sw-port-redund timer node-absent <1-60>	CONFIG	heartbeat 메시지가 수신되지 않으면 상대방 스위치가 없어진 것으로 판단하는 시간을 설정합니다. (default 1 s)
sw-port-redund timer heartbeat-fault <1-60>	CONFIG	Heartbeat 포트 link down 후 모든 redundancy 포트를 master 로 전환시키는 시간을 설정합니다. (default 1 s)

SSR 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show sw-port-redund	TOP	SSR 상태를 확인합니다.

SSR 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no sw-port-redund redundancy-port <1-48>	CONFIG	SSR 설정을 초기화합니다.
no sw-port-redund heartbeat-port <i>IFNAME</i>	CONFIG	heartbeat 메시지를 주고 받는 포트를 초기화합니다.
no sw-port-redund timer master-wait	CONFIG	slave포트에서 master포트로 전환 시 루프방지를 위해 대기하는 시간을 초기화합니다.
no sw-port-redund timer node-absent	CONFIG	heartbeat 메시지가 수신되지 않으면 상대편 스위치가 없어진 것으로 판단하는 시간을 초기화합니다.
no sw-port-redund timer heartbeat-fault	CONFIG	Heartbeat 포트 link down 후 모든 redundancy 포트를 master로 전환시키는 시간을 초기화합니다. (default 1 s)



참고

1. 상위 L2 집선 혹은 L3 스위치와는 STP를 통해 이중화를 지원하며, 하위 Hub와는 SSR 기능을 이용해 이중화를 지원합니다.
2. 망 운영중 heartbeat 포트를 제거할 경우, 두 대의 스위치 redundancy 포트들이 모두 master로 전환되므로 loop가 발생할 수 있습니다.

<예제> SSR 설정

SG2124G#configure terminal → 1 번 Switch 설정

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

SG2124G(config)#sw-port-redund redundancy-port 1 ge10 active

SG2124G(config)#sw-port-redund heartbeat-port ge15

SG2124G(config)#end

SG2124G#

SG2124GP#configure terminal → 2 번 Switch 설정

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

SG2124GP(config)#sw-port-redund redundancy-port1 ge10 standby

SG2124GP(config)#sw-port-redund heartbeat-port ge15

SG2124GP(config)#end

SG2124GP#

SG2124G#sh sw-port-redund → 1 번 Switch SSR 설정내역

Switch MAC address : 001a.f400.048d

Master wait timer : 1 seconds

Node absent timer : 1 seconds

HB port fault timer : 1 seconds

Redundancy Node MAC	State	Model
001a.f400.048d	normal	SG2124G
001a.f408.1369	normal	SG2124GXP0E

Redundancy Group	Port	Local			Remote			
		Mode	Role	State	Port	Mode	Role	State
1	ge10	active	master	up	ge10	standby	slave	down

Heartbeat Port	Port State
ge15	normal

SG2124GP#show sw-port-redund → 2 번 Switch SSR 설정내역

Switch MAC address : 001a.f408.1369

Master wait timer : 1 seconds

Node absent timer : 1 seconds

HB port fault timer : 1 seconds

Redundancy Node MAC	State	Model
001a.f408.1369	normal	SG2124GXP0E
001a.f400.048d	normal	SG2124G

Redundancy Group	Port	Local			Remote			
		Mode	Role	State	Port	Mode	Role	State
1	ge10	standby	slave	down	ge10	active	master	up


```

Heartbeat Port  Port State
-----
ge15            normal

-----

SG2124G#show sw-port-redund          → 1 번 Switch redundancy-port
Switch MAC address      : 001a.f400.048d    절체 시 1 번 Switch 내역
Master wait timer       : 1 seconds
Node absent timer       : 1 seconds
HB port fault timer     : 1 seconds

Redundancy Node MAC  State  Model
-----
001a.f400.048d       normal  SG2124G
001a.f408.1369       normal  SG2124GXP0E

Redundancy          Local
Group      Port  Mode  Role  State  Port  Mode  Role  State
-----
1          ge10 active master down  ge10 standby master up

Heartbeat Port  Port State
-----
ge15            normal

SG2124GP#show sw-port-redund          → 1 번 Switch redundancy-port
Switch MAC address      : 001a.f408.1369    절체 시 2 번 Switch 내역
Master wait timer       : 1 seconds
Node absent timer       : 1 seconds
HB port fault timer     : 1 seconds

Redundancy Node MAC  State  Model
-----
001a.f408.1369       normal  SG2124GXP0E
001a.f400.048d       normal  SG2124G

Redundancy          Local
Group      Port  Mode  Role  State  Port  Mode  Role  State
-----
1          ge10 standby master up  ge10 active master down

Heartbeat Port  Port State
-----
ge15            normal

SG2124GP#

```

2.4 LLDP / CDP

Layer 2 탐색은 어떤 장비에 어떤 Interface 또는 Switch가 서로 연결되는지 등에 대한 정보까지 찾아주는 것으로 Network Service와 Application용의 Client, Switch, Router 및 Server 사이의 경로를 확인할 수 있습니다.

IEEE 802.1ab는 Layer2 계층에서의 연결성 검색(Connectivity Discovery) Protocol이며 Cisco Discovery Protocol (CDP) 와 유사합니다. CDP가 IP계층 이상에서 동작하는 것에 비하여 LLDP는 Link 계층의 여러 가지 시스템 정보를 교환하는 특징이 있습니다.

LLDP는 물리적인 망의 형상정보, 상위계층의 지원 기능 정보, 자원들의 변경상황을 알리는 Protocol로서 자신의 정보를 주기적으로 광고하는 단방향 Protocol이기 때문에 해당 장치에 대한 동작 Parameter를 변경하는 등의 제어 기능은 수행하지 않습니다. LLDP로 보고되는 정보는 단순히 수집하여 활성화된 망의 현 상태를 탐색하는데 활용되고 있습니다.

LLDP Packet이 유입되면 LLDP 활성화 여부에 관계없이 CPU로 복사가 되지만, CDP는 CDP를 활성화 시켜놓지 않으면 Flooding 됩니다.

[표 2-3] LLDP / CDP 비교

	Inbound DATA Management	Inbound Packet Forwarding	Tx Frame	Voice VLAN	SNMP
LLDP	YES	NO	YES	YES	YES (제한적)
CDP	YES	YES (Disable)	YES (제한적)	YES	NO

[표 2-4] LLDP / CDP 지원 내역

	SG Switch Series
LLDP Packet 전송	YES
LLDP Packet 수신	YES
LLDP MED Packet 전송	YES
LLDP MED Packet 수신	YES
LLDP MED Voice Vlan설정	YES
CDP Packet 전송	YES
CDP Packet 수신	YES
CDP VoiceVlan설정	YES

2.4.1 LLDP (Link Layer Discovery Protocol)

LLDP (Link Layer Discovery Protocol)은 IEEE 802.1ab 표준에 따라 LAN에 연결된 장비들 사이에 Network 관리에 필요한 자료를 송수신하도록 하는 기능입니다. 관리자는 서로 다른 Network 장비들로 구축된 환경에서 LLDP 기능을 사용하여 Network 장비를 검색하고 유지 관리함으로써 Network 관리 문제를 해결할 수 있습니다.

LLDP는 이웃한 다른 시스템에 자신의 Network 장치 정보를 전송하고 검색된 정보를 저장하는 방법을 표준화한 프로토콜이며, 이웃된 Network의 시스템 이름, 시스템 ID, 시스템 설명, 장치 기능, 장치 구성 정보를 검색할 수 있습니다.

LLDP를 전송하는 장치는 다중 통지 Message 세트를 Packet 유형 길이 값(TLV) 필드를 포함하는 단일 LAN Packet으로 전송합니다. 다중 통지 세트에는 Chassis ID, Interface ID, 시스템 이름, 시스템 ID, 시스템 설명, 시스템 기능 통지 기능을 지원합니다.

LLDP를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
lldp enable	CONFIG	LLDP를 활성화합니다.
lldp msg tx {hold <1-180> interval <1-3600>}	CONFIG	LLDP Packet을 폐기하기 전에 수신 장치가 이 Packet을 유지해야 하는 시간을 설정합니다. (Default: hold 4, interval 30 s)
lldp port {both receive transmit} <i>PORTRANGE</i>	CONFIG	LLDP를 활성화할 Interface의 상태를 설정합니다.
lldp reinit-delay <1-180>	CONFIG	LLDP가 다시 초기화할 때까지 기다리는 최소 시간을 설정합니다. (Default: 2)
lldp tlv mgmtaddr {conf <i>IP_Addr</i> enable <i>PORTRANGE</i> }	CONFIG	장비의 IP 정보를 LLDP의 TLV를 통해 전송할 수 있도록 설정합니다.
lldp tx-delay <1-180>	CONFIG	연속 LLDP Frame 전송 간 지연을 설정합니다. (Default: 2)

LLDP 설정 내용 및 결과를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show lldp config [<i>IFNAME</i>]	TOP	LLDP를 설정 상태를 확인합니다.
show lldp neighbor [<i>IFNAME</i>]	TOP	LLDP를 지원하는 근접 장비의 정보를

		확인합니다.
show lldp stat [<i>IFNAME</i>]	TOP	LLDP 관련 통계를 확인합니다.

LLDP 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no lldp enable	CONFIG	LLDP를 비활성화합니다.
no lldp msg tx {hold interval}	CONFIG	LLDP Packet을 폐기하기 전에 수신 장치가 이 Packet을 유지해야 하는 시간을 초기화합니다. (Default: hold 4, interval 30 s)
no lldp port {both receive transmit} <i>PORTRANGE</i>	CONFIG	LLDP를 활성화할 Interface의 상태를 초기화합니다.
no lldp reinit-delay	CONFIG	LLDP가 다시 초기화할 때까지 기다리는 최소 시간을 초기화합니다. (Default: 2)
no lldp tlv mgmtaddr {conf enable <i>PORTRANGE</i> }	CONFIG	장비의 IP 정보를 LLDP의 TLV를 통해 전송할 수 있도록 초기화합니다.
no lldp tx-delay	CONFIG	연속 LLDP Frame 전송 간 지연을 초기화합니다. (Default: 2)

LLDP Enable 시 Default LLDP 설정

- Global LLDP : Enabled
- Message Tx Interval : 30 s
- Message Tx HoldMultiplier : 4
- ReInit Delay : 2
- Tx Delay : 2
- Management IP Address : Invalid
- MED Device Type Value : Network Connectivity
- MED Fast Start Count : Disabled



참고

<예제> LLDP의 설정 변경

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#lldp enable
SG2124G(config)#lldp msg tx interval 20
SG2124G(config)#lldp msg tx hold 5
SG2124G(config)#lldp port transmit ge1-2
SG2124G(config)#lldp reinit-delay 3
SG2124G(config)#lldp tx-delay 3
SG2124G(config)#lldp tlv mgmtaddr conf 192.168.100.10
SG2124G(config)#lldp tlv mgmtaddr enable ge1-2
SG2124G(config)#end
SG2124G#show lldp config
  - Global LLDP           : Enabled
  - Message Tx Interval   : 20 sec
  - Message Tx HoldMultiplier : 5
  - Reinit Delay          : 3
  - Tx Delay              : 3
  - Management IP Address : 192.168.100.10
  - MED Device Type Value : Network Connectivity
  - MED Fast Start Count  : Disabled
-----
Port   Status   PortEnable tlvMgmt
=====
ge1    TxOnly    FORWARD   Enable
ge2    TxOnly           Enable
ge3    None
ge4    None
ge5    None
ge6    None
ge7    None
ge8    None
-- 이하 생략 --

SG2124G#
SG2124G#show lldp stat
-----
Port   : Tx      Frames : Rx      Frames      Drop      Err
=====
ge1    :          5 :          0          0          0
ge2    :          0 :          0          0          0
ge3    :          0 :          0          0          0
ge4    :          0 :          0          0          0
ge5    :          0 :          0          0          0
ge6    :          0 :          0          0          0
ge7    :          0 :          0          0          0
ge8    :          0 :          0          0          0
-- 이하 생략 --

SG2124G#

```

2.4.2 LLDP-MED (LLDP-Media Endpoint Discovery)

LLDP 매체 종단점 검색(ANSI/TIA-1057 LLDP-MED)은 Network에 있는 장치 및 장치의 위치를 포함하는 자세한 Network 정보를 제공하여 단일 Network LLDP에서 다양한 IP Address를 공존시켜 Network 유연성을 증가시킵니다. 예를 들어, 어떤 IP Phone이 어떤 Interface에 연결되어 있고, 어떤 Software가 어떤 Switch에서 실행 중인지, 그리고 어떤 PC에 어떤 Interface가 연결되어 있는지에 대한 정보를 제공합니다.

- fast-start : 좀 더 빠른 반응을 얻고자 할 때 사용하며, LLDP-MED 가 설정된 Interface들은 기존 lldp tx-interval을 따르지 않고, fast-start에 설정된 delay를 적용시켜 동작합니다.
- port tx-enable : LLDP-MED 정보를 포함시켜 보낼 Interface를 지정합니다.
- Policy : LLDP-MED의 Network Policy TLV를 설정합니다.
- Location : LLDP-MED의 Location TLV를 설정합니다.

LLDP-MED를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
lldp med fast-start <i>VALUE</i>	CONFIG	LLDP-MED fast-start를 설정합니다. (Default: 3)
lldp med port {tx-enable policy <1-48>} <i>PORTRANGE</i>	CONFIG	LLDP-MED 정보 / Network Policy TLV를 포함한 정보를 전송할 Interface를 지정합니다.
lldp med policy <1-48> {application-type dscp priority vlan flag} <i>VALUE</i>	CONFIG	LLDP-MED 정보에 추가할 Network Policy TLV를 설정합니다.
lldp med location enable {civic-address coordinate ecs-elin}	INTERFACE	LLDP-MED 정보에 추가할 Location TLV를 설정합니다.
lldp med location civic-address {country-code type what} <i>VALUE</i>	INTERFACE	Location civic-address(행정지구 또는 도로주소) TLV를 설정합니다. (IETF RFC 4776 참조)
lldp med location {coordinate ecs-elin} <i>VALUE</i>	INTERFACE	Location coordinate (IETF RFC 3825 참조, 지도상 좌표) 또는 ecs-elin(긴급전화) TLV를 설정합니다.

LLDP-MED 설정 내용 및 결과를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
-----	----	----

show lldp config [IFNAME]	TOP	LLDP를 설정 상태를 확인합니다.
show lldp med policy	TOP	LLDP-MED Network policy에 설정된 정책들을 확인합니다.

LLDP-MED 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no lldp med fast-start	CONFIG	LLDP-MED fast-start를 삭제합니다.
no lldp med {tx-enable policy <1-48>} PORTRANGE	CONFIG	LLDP-MED 정보 / Network Policy TLV를 포함한 정보를 전송할 Interface를 삭제합니다.
no lldp med policy <1-48> {application-type dscp priority vlan flag} VALUE	CONFIG	Network Policy TLV를 삭제합니다.
no lldp med location enable	INTERFACE	Location TLV를 삭제합니다.
no lldp med location civic-address {country-code type VALUE what}	INTERFACE	Location civic-address TLV를 삭제합니다.
no lldp med location {coordinate ecs-elin VALUE}	INTERFACE	Location coordinate 또는 ecs-elin TLV를 삭제합니다.

LLDP-MED Enable 시 Default로 전송되는 TLV

- Chassis Subtype : MAC Address
- Port Subtype : Interface Name
- Time To Live : 120 sec (Default: LLDP tx-interval * 4)
- Port Description : Interface Name or Description
- System Name : Hostname
- System Description : Hostname 및 OS Information
- System Capabilities : Bridge/Switch (enabled)
- TIA - Capabilities : 0x01 LLDP-MED Capabilities



참고

LLDP-MED Device Type = Network Connectivity

[표 2-5] LLDP-MED Civic Address Type (ANNEX B)

CAtype	Description	Sample
0	Language	i-default [3]
1	National Subdivisions (State, Canton, Region, Province, Prefecture), Do (KR), To or Fu (JP)	Bavaria
2	County, Parish, Gun (KR), Shi or Gun (JP), District (IN)	
3	City, Township, Ri (KR), Ku or Mura (JP)	Munich
4	City Division, Borough, City District, Ward, Gu (KR), Chou or Machi (JP)	
5	Neighborhood, Block, Dong (KR), Choume (JP)	
6	Group of streets below the neighborhood level, Banchi or Ban (JP)	
16	Leading Street Direction	N
17	Trailing Street Suffix	SW
18	Street Suffix or Type	Avw, Platz
19	House Number	123
20	House Number Suffix	A, 1/2
21	Landmark or Vanity Address	Columbia University
22	Additional Location Information	South Wing
23	Name (Residence and Office Occupant)	Joe's Barbershop
24	Postal/Zip Code	10027-1234
25	Building (Structure)	Low Library
26	Unit (Apartment, Suite)	Apt 42
27	Floor	4
28	Room	450F
29	Type of Place	Office
30	Postal Community Name	Leonia
31	Post Office Box (P.O. Box)	12345
32	Additional Code	13203000003
33	Seat (Desk, Cubicle, Workstation)	WS 181
34	Primary Road Name	Broadway
35	Road Section	14
36	Branch Road Name	Lane 7

37	Sub-branch Road Name	Alley 8
38	Street Name Pre-modifier	Old
39	Street Name Post-modifier	Service
128	Script	Lath
255	Reserved	

<예제> LLDP-MED의 설정

```

SG2124G(config)#lldp med port tx-enable ge1-2
SG2124G(config)#lldp med fast-start
SG2124G(config)#lldp med policy 1 application-type 5
SG2124G(config)#lldp med policy 1 dscp 46
SG2124G(config)#lldp med policy 1 flag tag
SG2124G(config)#lldp med policy 1 priority 7
SG2124G(config)#lldp med policy vl
SG2124G(config)#lldp med policy 1 vlan 10
SG2124G(config)#lldp med port policy 1 ge1-2
SG2124G(config)#interface range ge1-2
% ge1-2 Selected
SG2124G(config-if-range)#lldp med location coordinate 5453c1f7515750ba
% ge1-2 Selected
SG2124G(config-if-range)#lldp med location ecs-elin 82 2 1234 5678
% ge1-2 Selected
SG2124G(config-if-range)#lldp med location civic-address country-code KR
% ge1-2 Selected
SG2124G(config-if-range)#lldp med location civic-address what 2
% ge1-2 Selected
SG2124G(config-if-range)#lldp med location civic-address type 1 Seoul
% ge1-2 Selected
SG2124G(config-if-range)#lldp med location civic-address type 2 Gorugu
% ge1-2 Selected
SG2124G(config-if-range)#lldp med location civic-address type 3 Gorudong
% ge1-2 Selected
SG2124G(config-if-range)#lldp med location enable civic-address
% ge1-2 Selected
SG2124G(config-if-range)#end
SG2124G#
SG2124G#show lldp med policy

```

```

-----
PolicyNumber  ApplcationType      VLANID  DSCP  L2Prioty  Unknown  Tagged
=====
1              Softphone Voice          10      46    7         -        Yes

```

```

SG2124G#
SG2124G#show lldp config
- Global LLDP           : Enabled
- Message Tx Interval   : 30 sec
- Message Tx HoldMultiplier : 4
- ReInit Delay          : 2
- Tx Delay               : 2
- Management IP Address  : Invalid
- MED Device Type Value  : Network Connectivity
- MED Fast Start Count   : 3 sec

```

```

-----
Port    Status    PortEnable tlvMgmt MedTxEnable Policy
-----
ge1     RxTx      FORWARD           Enable    1
ge2     RxTx                        Enable    1
ge3     RxTx
ge4     RxTx
ge5     RxTx
-- 이하 생략 --

```

SG2124G#

```

=====
SG2124G-2
=====

```

SG2124G-2#show lldp neighbor detail

Port = ge1

```

-MSAP Identifier      : 0x001AF4100104676532
Chassis Subtype       : MAC Address - 0x 00 1a 00 00 01 04
Port Subtype          : Interface Name - ge2 - 0x 67 65 32
Time To Live          : 120 sec
Port Description      : ge2
System Name           : SG2124G
System Description    : SG2124G #7694 Fri Mar 12 14:21:43 KST 2010
System Capabilities   : 0x4, Enabled Capabilities: 0x4
                        Bridge/Switch (enabled)
TIA - Capabilities    : 0x07 LLDP-MED Capabilities
                        Network Policy
                        Location Identification
                        LLDP-MED Device Type = Network Connectivity Device
TIA - NetworkPolicy: Application Type = Softphone Voice
                        Flags = Tagged
                        VLAN ID = 10
                        L2 Priority = 7
                        DSCP Value = 46
TIA - Location ID    : Civic Address LCI
                        What = 2
                        Country = KR
                        Type = 1 Value = Seoul
                        Type = 2 Value = Gorugu
                        Type = 3 Value = Gorudong

```

SG2124G-2#

2.4.3 CDP (Cisco Discovery Protocol)

CDP (Cisco Discovery Protocol)는 Layer 2 계층에서 Cisco 장비를 찾아내는데 사용하는 Cisco 독자적인 프로토콜로 Hardware Type과 Software Version, Cisco 장비가 현재 사용하고 있는 활성화된 Interface에 대한 정보를 알려주는데 사용됩니다.

SG Switch Series에서는 CDP 전송 시 Cisco 장비에 영향을 주지 않기 위해 최소한의 정보 (Version 2, Device ID, Port ID, Capabilities, Software Version, Platform)만을 전송하며, 사용자가 따로 전송할 내역의 수정이 불가능합니다. Voice-vlan을 설정한 경우에는 VoIP VLAN Reply Field를 추가하여 CDP 정보를 전송하여 Cisco IP Phone의 설정을 자동으로 변경합니다. CDP가 활성화되지 않은 경우에 CDP Packet이 수신되면 CPU로 복사되지 않고 Flooding됩니다.

CDP를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
cdp enable	CONFIG	CDP를 활성화합니다.
cdp port {receive transmit both} <i>PORTRANGE</i>	CONFIG	CDP Packet 전송할 Interface를 설정합니다.

CDP 설정 내용 및 결과를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show cdp neighbor [<i>IFNAME</i> detail]	TOP	CDP를 지원하는 근접 장비의 정보를 확인합니다.

CDP 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no cdp enable	CONFIG	CDP를 비활성화합니다.
no cdp port {both receive transmit} <i>PORTRANGE</i>	CONFIG	CDP를 활성화할 Interface의 상태를 초기화합니다.

<예제> CDP의 설정 변경

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#cdp enable
SG2124G(config)#cdp port both ge2
SG2124G(config)#end
SG2124G#
SG2124G#show cdp neighbor

  CDP Neighbor Devices Information

  Port      | DeviceID          | PortID          | Platform
  -----+-----+-----+-----
  ge2       | SG2124G          | ge2             | SG2124G #1 Tue Jul

SG2124G#
SG2124G#show cdp neighbor detail
Port = ge2
  CDP Ver      : 2
  TTL          : 180 second
  Device ID    : SG2124G
  Port ID     : ge2
  Capabilities : Switch IGMPcapable
  ISO Version  : SG-24G-2.5.6
  PLATFORM    : SG2124G #1 Tue Jun 10 11:54:36 KST 2014

SG2124G#

```

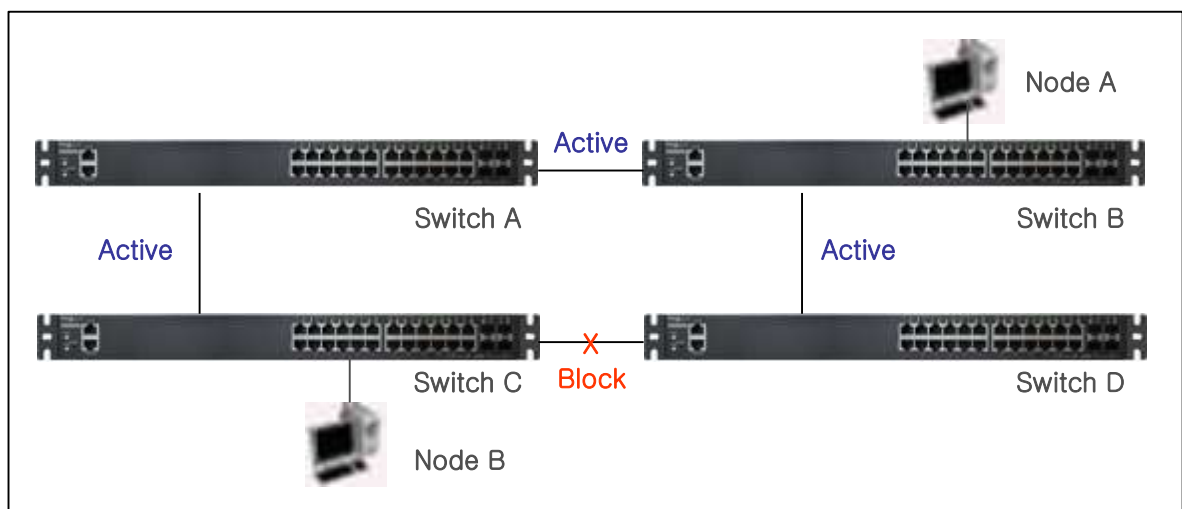
2.5 Spanning Tree

2.5.1 개요

Spanning Tree Protocol (STP)는 다중 경로를 가지는 Network 내에서 임의의 두 Switch 사이에는 하나의 활성화된 경로만 존재하도록 Loop의 생성을 방지하는 Protocol입니다. 다중 경로를 갖는 Network에서 Loop가 발생하면 Broadcast 및 Multicast Packet 전송 시 Packet이 계속 회전하면서 불필요한 Data가 계속해서 전송되어 Network가 불안정해집니다. STP (Spanning-Tree Protocol, IEEE 802.1d)는 다중 경로가 존재하는 Network에서 Loop 현상을 막고 다중 경로를 효율적으로 이용할 수 있도록 해 주는 기능으로 여러 경로 중 가장 효율적인 경로를 선택한 후 나머지 경로를 막아주기 때문에 Loop 현상이 발생하지 않습니다.

STP보다 Network convergence 시간을 단축한 RSTP (Rapid Spanning-Tree Protocol, IEEE 802.1w)는 STP에서 사용하는 용어와 대부분의 설정 값들을 그대로 사용하기 때문에 새로운 Protocol을 쉽고 빠르게 설정할 수 있습니다. 또한, RSTP는 STP를 내부적으로 포함하고 있어 호환이 가능합니다.

[그림 2-4] STP 구성



STP는 모든 Switch에 대해 Root Switch와 Loop가 없는 경로들로 구성된 tree를 정의하며, 중복된 Data 경로는 대기(block) 상태에 놓이게 됩니다. 만약 대체 경로가 존재하는 STP로 구성된 Network에서 Active Line에 장애가 발생하면 STP는 자동으로 대체경로를 활성화 시킵니다.

2.5.2 STP / RSTP / MSTP / PVSTP 동작

■ STP 동작

802.1d의 STP에서는 Interface 상태를 Blocking, Listening, Learning, Forwarding의 네 가지로 정의합니다.

다중 경로를 가지고 있는 Network에 STP를 설정하면 Switch들은 Bridge ID를 포함한 자신의 정보를 교환하게 되는데 이를 BPDU (Bridge Protocol Data Unit)라고 하며, BPDU를 바탕으로 Interface의 상태 및 Switch간의 최적의 경로를 자동적으로 결정합니다.

Root Switch를 결정하는 중요한 정보는 바로 Bridge ID입니다. Bridge ID는 2Bytes로 된 Priority와 6Bytes로 된 MAC Address로 구성됩니다. 이 때 Bridge ID가 가장 작은 것이 Root Switch로 결정되며, BPDU를 비교하여 Designated Switch까지 어떤 경로를 선택하여 사용할 지를 결정합니다.

Designated Switch는 Root Switch까지의 Interface 전송속도에 따라 정해지는 path-cost 값을 합산한 Root path-cost 값이 가장 적은 경로로 선택됩니다. 이 때 Root Switch와 연결되는 Interface를 Root Port라고 하며, Root Port는 한 장비에 한 개만 존재할 수 있습니다.

각 장비에서 Root Port를 제외하고 다른 Switch와 연결되는 Interface는 Designated Port, Root Port와 Designated Port를 제외한 모든 Interface는 Blocked Port라고 합니다. Path-cost가 동일한 두 개의 경로가 존재하는 경우에는 port-priority값이 작은 Interface가 root Port로 선택되어 Packet을 전송합니다.

이러한 설정들은 이미 각 Switch가 가지고 있는 BPDU를 통해 자동적으로 결정되며, Root Switch나 Designated Switch의 경로를 변경하려면 BPDU의 값을 변경해야 합니다.

■ RSTP 동작

Loop가 발생할 수 있는 다중 경로를 가진 Network에서 STP 또는 RSTP를 설정했을 때 RSTP는 STP보다 빠르게 진행됩니다. RSTP는 802.1d의 Blocking과 Listening을 Discarding으로 통합하여 Interface 상태를 Discarding, Learning, Forwarding의 세 가지로 정의하며, Root Port와 Designated Port의 결정 과정은 STP와 같습니다.

RSTP에서 Blocked Port는 Alternate Port와 Backup Port로 나뉘어집니다. Alternate Port는 다른 장비로부터 우선 순위가 높은 BPDU를 받음으로써 Blocked 된 Port로 Root Switch와 다른 SWITCH 사이에 문제가 발생하였을 때 Packet의 경로를 대체해줄 수 있지만, Backup Port는 같은 장비의 다른 Port로부터 우선 순위가 높은 BPDU를 받음으로써 Blocked된 Port로 Root Switch와 다른 SWITCH 사이에 문제가 발생하여도 끊임없는 접속을 보장할 수는 없습니다.

STP는 Root Switch의 Hello-time에 따라 전송되는 BPDU를 받았을 때에만 Designated Switch의 BPDU를 전송하나, RSTP는 모든 Switch가 BPDU를 전송합니다. BPDU는 실제로 Root Switch에 의해 주고받는 시간 간격보다 더 자주 변할 수 있기 때문에 RSTP에서는 STP보다 변화하는 Network 환경에 더욱 빨리 대응할 수 있게 되었습니다. 또한, BPDU의 Forward-delay 시간 때문에 발생하는 통신 단절 시간을 단축하기 위해 Designated Switch와 Root Switch 사이에 새로운 Link가 연결되면 SWITCH와 Root 사이에는 Packet을 주고받을 수 없지만 BPDU는 전송할 수 있는 상태가 됩니다.

BPDU를 통해 Link를 Forwarding 상태로 만들기 위해 non-edge designate Port를 Blocking 상태로 변경하나, edge designated Port는 Listening과 Learning이 필요하지 않기 때문에 관리자가 설정해 놓은 어떤 시간 기준도 사용되지 않아 매우 빠르게 진행됩니다.

RSTP는 내부적으로 STP를 포함하고 있기 때문에 호환성을 가지고 있어 STP의 BPDU를 인식할 수 있습니다. 그러나, STP는 RSTP의 BPDU는 판독할 수 없습니다.

■ MSTP 동작

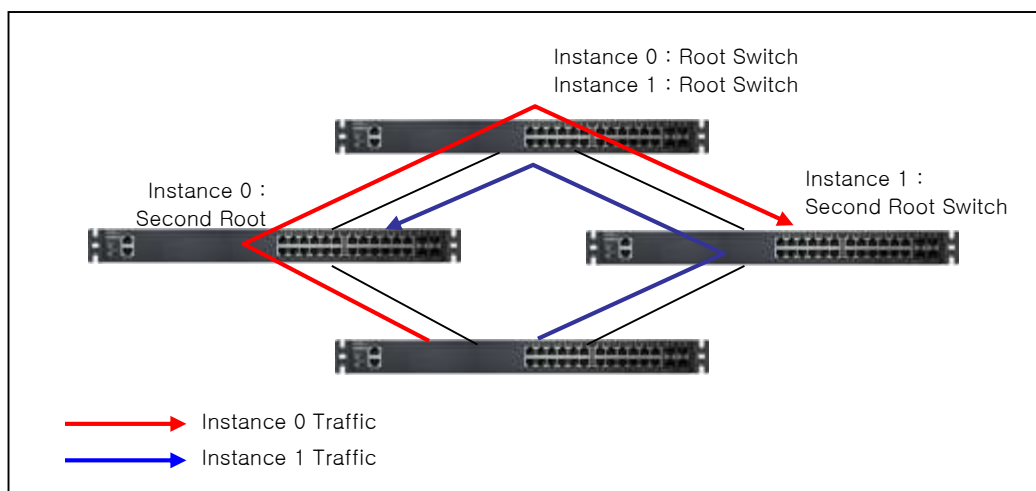
VLAN으로 Network를 구축한 경우 Loop 방지를 위하여 VLAN 별로 또는 VLAN Group 별로 경로를 설정할 수 있는 MSTP (Multiple Spanning Tree Protocol)를 사용합니다. MSTP를 사용하면 RSTP를 구현하지 않고도 트리 재구성 시간을 최소화 할 수 있습니다. Multiple Spanning Tree Protocol (MSTP)는 IEEE 802.1s 에서 규정되었으며 MST를 규정하고 있는 802.1s는 802.1Q에 대한 수정입니다.

기존의 Spanning Tree Protocol은 통신선로 단절에 대비한 예비선로를 정상시에는 전혀 사용하지 않고 Traffic들이 유일한 경로를 통과하게 되어 있어 통신선로의 낭비를 초래하였습니다. MSTP는 RSTP 알고리즘을 여러 개의 Spanning Tree까지 확장하여 VLAN환경에서 고속 수렴성과 부하분산 양쪽을 실현하였습니다. 매개의 토폴로지에서 MST의 수렴속도는 PVST+ 및 MISTP보다 고속이며 MSTP는 802.1D STP, 802.1w RSTP 및 PVST 와 하위호환성을 가집니다.

STP/RSTP의 경우 모든 VLAN들은 하나의 STP만 사용하며 다중 Instance를 지원하지 않습니다. Network 트리 재구성을 빠르게 하기 위해 RSTP를 사용하는 IEEE 802.1s MSTP는 VLAN Trunk를 매체로 VLAN을 여러 개의 Group으로 나누어 Instance 단위로 분류하며, 각 Instance는 다른 Spanning Tree의 Instance와는 관계가 없는 토폴로지를 설정할 수 있습니다. 때문에 Traffic에 여러 개의 전송경로가 주어져 부하분산이 가능해졌으며 1개의 Instance(전송경로)에서 장애가 발생해도 다른 Instance(전송경로)는 영향을 받지 않기 때문에 Network내의 안정성이 향상되었으며 대규모 Network에서는 서로 다른 VLAN Spanning Tree Instance를 모두 계산할 필요가 없기 때문에 불필요한 Switch의 부하를 줄일 수 있습니다.

MSTP의 Region에는 하나의 STP가 구동 되기 때문에 STP 수가 적어 BPDU Traffic을 줄일 수 있습니다. Region에 설정하는 Instance는 최대 15개까지 생성 할 수 있습니다.

[그림 2-5] MSTP 구성도 및 Traffic 흐름



■ PVSTP 동작

일반적으로 Switch 장비 간의 Loop를 방지하는 Spanning Tree Protocol은 Switch간에 Link로 연결된 물리적인 Tree를 바탕으로 Loop를 방지하기 때문에 하나의 Tree만을 만들어 사용하는 단점이 있습니다. 이 때 물리적 Tree 구조에서 일부분을 차지하는 VLAN은 하나로 이루어진 전체 Tree를 바탕으로 운용되기 때문에 어느 한 곳은 지속적으로 차단되어 있어 모든 트래픽이 한 곳으로 집중되어 효율적이지 못합니다. 하나의 Tree를 사용하여 발생하는 문제점을 보완하기 위해 VLAN 마다 서로 다른 경로로 Spanning Tree Algorithm을 수행하여 로드를 분산하는 방식을 PVST (Per VLAN Spanning Tree)라고 합니다.

PVST는 CST (하나의 Tree를 사용하는 형식. Common Spanning Tree)를 사용하는 장비와는 서로의 STP BPDU를 이해하지 못하기 때문에 같이 사용할 수 없는 단점이 있습니다.

PVST를 보완하기 위해 만들어진 PVSTP는 PVCST에서 수신한 BPDU 정보를 PVST로 전송할 때 VLAN마다 반복해서 전송하는 작업을 하거나, Tunneling을 해서 이웃하지 않은 PVST 간에 연결을 허락하게 됩니다.

PVSTP는 Spanning Tree Protocol로 STP BPDU를 전송하며, PVSTP Mode에서 RSTP BPDU를 전송하는 방식을 PVSTP+ 또는 PVRSTP라고 합니다. Switch에서는 PVSTP로 설정 시 Default로 RSTP BPDU를 전송하고 있으며, PVSTP로 활성화할 수 있는 최대 트리(VLAN)의 구성 개수는 64개입니다.

[표 2-6] STP와 RSTP의 Interface 상태 비교

STP	RSTP	BPDU 수신	BPDU 송신	MAC Address 학습	Data Frame 전달
차단 (Blocking)	폐기 (Discarding)	가능	송신 못함	학습 안됨	전달 안됨
청취 (Listening)	폐기 (Discarding)	가능	송신 못함 (*)	학습 안됨	전달 안됨
학습 (Learning)	학습 (Learning)	가능	가능	학습 가능	전달 안됨
전송 (Forwarding)	전송 (Forwarding)	가능	가능	학습 가능	전달 가능
비활성 (Disabled)	폐기 (Discarding)	수신 못함	송신 못함	학습 안됨	전달 안됨

(*) STP는 청취 상태부터 BPDU 송신이 가능함



참 고

Spanning-Tree 사용 시 Interface 상태 요약 정의

- Blocking - Frame을 전달하지 않는 상태
 Listening - BPDU Data를 수신하는 상태
 Learning - Frame 전달을 위한 준비를 하는 단계, MAC learning 수행
 Forwarding - Frame을 전달하는 상태

[표 2-7] STP와 RSTP의 포트 역할

STP	RSTP	설 명
루트 포트 (RP)	루트 포트 (RP)	Switch에서 Root Bridge 방향으로 Data Frame이 전송되는 유일한 Port입니다. Root Switch가 아닌 Switch는 한 개의 RP가 선택되며 이 Port를 통해서 수신된 BPDU 중 최상의 BPDU를 청취합니다.
지정 포트 (DP)	지정 포트 (DP)	Segment에서 Root Bridge 방향으로 Data Frame이 전송되는 유일한 Port이며 최상의 BPDU를 광고합니다.
-	대체 포트 (AP)	차선의 BPDU를 광고하는 Port로 RP Down 시 그 역할을 이어받는 Port입니다. AP는 RSTP에서 비활성 Port이므로 차단 상태에 있습니다.
-	백업 포트 (BP)	DP가 아닌 Port 중에서 동일한 Segment에 연결되어 있는 또 다른 Port입니다. DP가 Down되면 그 역할을 이어받습니다. BP는 허브와 복수의 Link로 접속할 때 생기며 비활성 Port이므로 차단 상태에 있습니다.
비활성 (disabled)	비활성 (disabled)	관리자에 의해 Down되거나 다른 이유로 작동 불가능 상태인 Port입니다.

2.5.3 Spanning Tree Mode 설정

STP를 설정하려면 우선 STP / RSTP / MSTP / PSTP 중 어떤 모드를 선택할 것인지 설정해야 합니다.

Switch에 STP Mode를 설정 및 변경하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
bridge 1 protocol ieee vlan-bridge	CONFIG	STP 모드로 설정합니다.
bridge 1 protocol rstp vlan-bridge	CONFIG	RSTP 모드로 설정합니다. (Default)
bridge 1 protocol mstp	CONFIG	MSTP 모드로 설정합니다.
bridge 1 protocol pvstp	CONFIG	PVSTP 모드로 설정합니다.

STP 기능을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show spanning-tree [detail interface IFNAME]	TOP	Spanning-tree 설정 내용을 확인합니다.
show spanning-tree mst <config detail instance interface>	TOP	MSTP 설정 내용을 확인합니다.
show spanning-tree pvstp <detail interface summary vlan>	TOP	PVSTP 설정 내용을 확인합니다.

<예제> STP Mode로 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#bridge 1 protocol ieee vlan-bridge → STP 로 설정
SG2124G(config)#end
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#bridge 1 protocol rstp vlan-bridge → RSTP 로 설정
SG2124G(config)#end
SG2124G#
SG2124G#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.  
SG2124G(config)#bridge 1 protocol mstp           → MSTP 로 설정  
SG2124G(config)#end  
SG2124G#  
SG2124G#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
SG2124G(config)#bridge 1 protocol pvstp          → PVSTP 로 설정  
SG2124G(config)#end  
SG2124G#
```

2.5.4 Spanning Tree 활성화

STP 기능을 설정하려면 STP를 활성화시켜야 합니다.

STP 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
bridge 1 {stp rstp mstp pvstp} enable	CONFIG	STP / RSTP / MSTP / PVSTP를 활성화합니다.
bridge 1 mstp cisco-interoperability {enable disable}	CONFIG	VLAN별로 STP가 동작하도록 설정합니다.

STP 기능을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show spanning-tree [detail interface IFNAME]	TOP	Spanning-tree 설정 내용을 확인합니다.
show spanning-tree mst <config detail instance interface>	TOP	MSTP 설정 내용을 확인합니다.
show spanning-tree pvstp <detail interface summary vlan>	TOP	PVSTP 설정 내용을 확인합니다.

STP 기능을 비활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no bridge 1 {stp rstp mstp pvstp} enable bridge-forward	CONFIG	STP / RSTP / MSTP / PVSTP를 비활성화합니다.
no bridge 1 {stp rstp mstp pvstp} enable bridge-forward bpdu-flood	CONFIG	STP / RSTP / MSTP / PVSTP를 비활성화하지만, BPDU 수신 시 Flooding 합니다.

<예제> STP 활성화 설정

=====

STP 활성화

```
=====
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#bridge 1 stp enable
SG2124G(config)#end
SG2124G#
```

=====

RSTP 활성화

```
=====
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#bridge 1 rstp enable
SG2124G(config)#end
SG2124G#
```

=====

MSTP 활성화

```
=====
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#bridge 1 mstp enable
SG2124G(config)#end
SG2124G#
```

=====

PVSTP 활성화

```
=====
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#bridge 1 pvstp enable
SG2124G(config)#end
SG2124G#
```

2.5.5 Root Switch 설정

Spanning-Tree 기능이 동작하기 위해서는 Root Switch가 정해져야 합니다. STP나 RSTP에서는 Root Switch, MSTP에서는 IST Root Switch가 됩니다. 각 Switch는 자신의 Bridge ID를 가지고 있으며 동일한 LAN에 존재하는 Switch의 Bridge ID를 비교하여 Root Switch를 결정합니다.

특정 Switch의 Priority를 설정하면 인위적으로 Root Switch를 변경할 수 있습니다. Priority가 변경되면 가장 작은 Priority를 가진 Switch가 Root Switch로 결정되도록 재설정됩니다.

Switch에 Priority를 설정하여 Root Switch를 변경하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
bridge 1 {stp rstp mstp} priority <0-61440>	CONFIG	STP / RSTP / MSTP의 CIST Priority를 변경합니다.
bridge 1 mstp instance <1-15> priority <0-61440>	INTERFACE	Interface에 MSTP Instance MSTI의 Priority를 변경합니다.
bridge 1 pvstp vlan <i>VLANID</i> priority <0-61440>	CONFIG	PVSTP의 특정 VLAN의 Priority를 변경합니다.

Switch의 Priority 값을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show spanning-tree [detail interface <i>IFNAME</i>]	TOP	Spanning-tree 설정 내용을 확인합니다.
show spanning-tree mst <config detail instance interface>	TOP	MSTP 설정 내용을 확인합니다.
show spanning-tree pvstp <detail interface summary vlan>	TOP	PVSTP 설정 내용을 확인합니다.

Switch의 Priority 값을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no bridge 1 {stp rstp mstp pvstp vlan <i>VLANID</i> } priority	CONFIG	STP / RSTP / MSTP / PVSTP의 CIST Priority를 초기화합니다.
no bridge 1 mstp instance <1-15> priority	INTERFACE	Interface에 MSTP Instance MSTI의 Priority를 초기화합니다.

<예제> Spanning Tree의 Switch Priority 설정

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#bridge 1 stp priority 4096
SG2124G(config)#bridge 1 rstp priority 8192
SG2124G(config)#bridge 1 mstp priority 16384
SG2124G(config)#end
SG2124G#show spanning-tree

1: Spanning Tree Enabled protocol RSTP
  Ageing Time 300 - Root Path Cost 0 - Priority 32768
  Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
  Root Id 8000001af40f0400
  Bridge Id 8000001af40f0400

  interface Role      State          Path-cost  Priority  Rcv  Send
  -----
  ge1       Designated Forwarding  200000    128      None RSTP

SG2124G#
SG2124G#show spanning-tree detail
% 1: Spanning Tree Enabled
% 1: Ageing Time 300 - Root Path Cost 0 - Priority 8192
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
% 1: Root Id 2000001af4000541
% 1: Bridge Id 2000001af4000541
% 1: 1 topology changes - last topology change Thu May 7 20:29:26 2009
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%
% ge24: Port 5024- Id 83a2 - Role Disabled - State Discarding
% ge24: Configured path cost 20000 - Designated path cost 0
% ge24: Designated port id 0 - Priority 128
% ge24: Designated Root 0000000000000000
% ge24: Designated Bridge 0000000000000000
% ge24: Message Age 0 - Max Age 0
% ge24: Hello Time 0 - Forward Delay 0
% ge24: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
% ge24: Version Rapid Spanning Tree Protocol - Received None - Send STP
% ge24: No portfast configured - Current portfast off
% ge24: portfast bpdu-guard default - Current portfast bpdu-guard off
% ge24: portfast bpdu-filter default - Current portfast bpdu-filter off
% ge24: no root guard configured - Current root guard off
% ge24: Configured Link Type point-to-point - Current shared
% ge24: forward-transitions 0
%
-- 이하 생략 --
SG2124G#

```



참고

Priority 값은 4096의 배수로 입력합니다.

2.5.6 Path-Cost

Root Switch가 결정된 후에는 path-cost를 기준으로 Designated Switch에 대한 Packet 전송 경로가 결정되는데 기본적으로 path-cost는 Switch의 Interface 전송 속도로 값이 정해집니다. 관리자는 Root Port의 path-cost의 설정을 변경할 수 있으며 path-cost를 기준으로 선택된 경로가 과부하 상태에 빠졌을 경우 다른 경로를 선택하는 것이 좋습니다.

[표 2-8] path-cost 값

전송 속도	STP	RSTP
4M	250	20,000,000
10M	100	2,000,000
100M	19	200,000
1G	4	20,000
10G	2	2,000

Path-cost를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
bridge-group 1 path-cost <1-200000000>	INTERFACE	path-cost 값을 변경합니다.

Path-cost 값을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show spanning-tree [detail interface <i>IFNAME</i>]	TOP	Spanning-tree 설정 내용을 확인합니다.
show spanning-tree mst <config detail instace interface>	TOP	MSTP 설정 내용을 확인합니다.
show spanning-tree pvstp <detail interface summary vlan>	TOP	PVSTP 설정 내용을 확인합니다.

Path-cost 값을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no bridge-group 1 path-cost	INTERFACE	path-cost 값을 초기화합니다.

<예제> Spanning Tree의 path-cost 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge1
SG2124G(config-if)#bridge-group 1 path-cost 10000
SG2124G(config-if)#end
SG2124G#show spanning-tree interface ge1
% 1: Spanning Tree Enabled
% 1: Ageing Time 300 - Root Path Cost 0 - Priority 8192
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
% 1: Root Id 20000001af4000541
% 1: Bridge Id 20000001af4000541
% 1: 1 topology changes - last topology change Thu May 7 20:29:26 2009
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% ge1: Port 5001 - Id 8389 - Role Disabled - State Discarding
% ge1: Configured path cost 10000 - Designated path cost 0
% ge1: Designated port id 0 - Priority 128
% ge1: Designated Root 00000001af4000541
% ge1: Designated Bridge 00000001af4000541
% ge1: Message Age 0 - Max Age 0
% ge1: Hello Time 0 - Forward Delay 0
% ge1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
% ge1: Version Rapid Spanning Tree Protocol - Received None - Send STP
% ge1: No portfast configured - Current portfast off
% ge1: portfast bpdu-guard default - Current portfast bpdu-guard off
% ge1: portfast bpdu-filter default - Current portfast bpdu-filter off
% ge1: no root guard configured - Current root guard off
% ge1: Configured Link Type point-to-point - Current shared
% ge1: forward-transitions 0
-- 이하 생략 --

SG2124G#
```

2.5.7 Port-Priority

두 경로의 **path-cost**를 비롯한 모든 기준이 동일할 경우 최종적으로 경로를 선택하는 기준은 **port-priority**이며, 관리자는 **port-priority**의 설정을 변경할 수 있습니다.

Port-priority를 변경하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
bridge-group 1 priority <0-240>	INTERFACE	port-priority 값을 변경합니다.

Port-priority 값을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show spanning-tree [detail interface <i>IFNAME</i>]	TOP	Spanning-tree 설정 내용을 확인합니다.
show spanning-tree mst <config detail instance interface>	TOP	MSTP 설정 내용을 확인합니다.
show spanning-tree pvstp <detail interface summary vlan>	TOP	PVSTP 설정 내용을 확인합니다.

Port-priority 값을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no bridge-group 1 priority	INTERFACE	port-priority 값을 초기화합니다.

<예제> Spanning Tree의 port-priority 설정

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge1
SG2124G(config-if)#bridge-group 1 priority 32
SG2124G(config-if)#end
SG2124G#show spanning-tree interface ge1
% 1: Spanning Tree Enabled
% 1: Ageing Time 300 - Root Path Cost 0 - Priority 8192
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
% 1: Root Id 2000001af4000541
% 1: Bridge Id 2000001af4000541
% 1: 1 topology changes - last topology change Thu May  7 20:29:26 2009
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% ge1: Port 5001 - Id 2389 - Role Disabled - State Discarding
% ge1: Configured path cost 20000000 - Designated path cost 0
% ge1: Designated port id 0 - Priority 32
% ge1: Designated Root 0000001af4000541
% ge1: Designated Bridge 0000001af4000541
% ge1: Message Age 0 - Max Age 0
% ge1: Hello Time 0 - Forward Delay 0
% ge1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
% ge1: Version Rapid Spanning Tree Protocol - Received None - Send STP
% ge1: No portfast configured - Current portfast off
% ge1: portfast bpdu-guard default - Current portfast bpdu-guard off
% ge1: portfast bpdu-filter default - Current portfast bpdu-filter off
% ge1: no root guard configured - Current root guard off
% ge1: Configured Link Type point-to-point - Current shared
% ge1: forward-transitions 0
-- 이하 생략 --

SG2124G#

```



참고

port-priority 값은 16의 배수로 입력합니다.

2.5.8 Edgeport

Edgeport는 STP가 활성화 될 필요가 없는 Bridge Port입니다. 해당 Interface와 연결된 하단의 장비들이 STP Loop 감지 기능이 필요하지 않는 PC등이 직접 연결되어 있거나 STP Neighbor가 해당 Interface 하단에 존재하는 않는 경우에 설정합니다. Interface에 edgeport를 설정한 후 Link를 연결하면 바로 Forwarding 상태로 전환됩니다.

Edgeport를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
spanning-tree edgeport	INTERFACE	Interface를 edgeport로 설정합니다.

Edgeport 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show spanning-tree [detail interface <i>IFNAME</i>]	TOP	Spanning-tree 설정 내용을 확인합니다.
show spanning-tree mst <config detail instance interface>	TOP	MSTP 설정 내용을 확인합니다.
show spanning-tree pvstp <detail interface summary vlan>	TOP	PVSTP 설정 내용을 확인합니다.

Edgeport 설정 내용을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no spanning-tree edgeport	INTERFACE	edgeport로 설정된 Interface를 초기화합니다.



참고

Interface에 edgeport 설정과 portfast 설정은 중복하여 설정할 수 없습니다.

<예제> Spanning Tree의 edgeport 설정

```

SG2124G(config)#interface ge1
SG2124G(config-if)#spanning-tree edgeport
SG2124G(config-if)#end
SG2124G#show spanning-tree interface ge1
% 1: Spanning Tree Enabled
% 1: Ageing Time 300 - Root Path Cost 0 - Priority 8192
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
% 1: Root Id 2000001af4000541
% 1: Bridge Id 2000001af4000541
% 1: 1 topology changes - last topology change Thu May  7 20:29:26 2009
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% ge1: Port 5001 - Id 8389 - Role Disabled - State Discarding
% ge1: Configured path cost 20000000 - Designated path cost 0
% ge1: Designated port id 0 - Priority 128
% ge1: Designated Root 0000001af4000541
% ge1: Designated Bridge 0000001af4000541
% ge1: Message Age 0 - Max Age 0
% ge1: Hello Time 0 - Forward Delay 0
% ge1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
% ge1: Version Rapid Spanning Tree Protocol - Received None - Send STP
% ge1: Edgeport configured - Current edgeport on
% ge1: portfast bpdu-guard default - Current portfast bpdu-guard off
% ge1: portfast bpdu-filter default - Current portfast bpdu-filter off
% ge1: no root guard configured - Current root guard off
% ge1: Configured Link Type point-to-point - Current shared
% ge1: forward-transitions 0
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge1
SG2124G(config-if)#no spanning-tree edgeport
SG2124G(config-if)#end
SG2124G#show spanning-tree interface ge1
% 1: Spanning Tree Enabled
% 1: Ageing Time 300 - Root Path Cost 0 - Priority 8192
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
% 1: Root Id 2000001af4000541
% 1: Bridge Id 2000001af4000541
% 1: 1 topology changes - last topology change Thu May  7 20:29:26 2009
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% ge1: Port 5001 - Id 8389 - Role Disabled - State Discarding
% ge1: Configured path cost 20000000 - Designated path cost 0
% ge1: Designated port id 0 - Priority 128
% ge1: Designated Root 0000001af4000541
% ge1: Designated Bridge 0000001af4000541
% ge1: Message Age 0 - Max Age 0
% ge1: Hello Time 0 - Forward Delay 0
% ge1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
% ge1: Version Rapid Spanning Tree Protocol - Received None - Send STP
% ge1: No portfast configured - Current portfast off
% ge1: portfast bpdu-guard default - Current portfast bpdu-guard off
% ge1: portfast bpdu-filter default - Current portfast bpdu-filter off
% ge1: no root guard configured - Current root guard off
% ge1: Configured Link Type point-to-point - Current shared
% ge1: forward-transitions 0
SG2124G#

```

2.5.9 Force-Version

활성화되어 있는 Spanning-tree 모드와 상관없이 802.1w 기반의 STP에 참여하는 특정 Interface를 통해 전송하는 BPDU 정보를 강제로 STP / RSTP / MSTP BPDU 정보를 전송하도록 설정할 수 있습니다. (0 - STP, 1 - Not Support, 2 - RSTP, 3 - MSTP를 의미합니다.)

Default 설정에서는 설정되어 있지 않으며, 이 경우 Interface의 파트너가 Legacy 장비로서 802.1D BPDU를 보내게 됩니다. BPDU를 수신한 이후 Migration Timer가 시작되고, 이후 3 s 이내에 RSTP BPDU가 수신되지 않으면, 해당 Port는 802.1D에 맞추어 운영되게 됩니다.

force-versions을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
spanning-tree force-version <0-3>	INTERFACE	force-versions을 설정합니다. Set up force-versions

force-versions값을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show spanning-tree [detail interface IFNAME]	TOP	Spanning-tree 설정 내용을 확인합니다.
show spanning-tree mst <config detail instance interface>	TOP	MSTP 설정 내용을 확인합니다.
show spanning-tree pvstp <detail interface summary vlan>	TOP	PVSTP 설정 내용을 확인합니다.

force-versions을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no spanning-tree force-version	INTERFACE	force-versions을 초기화합니다. Initialize force-versions

<예제> force-version 설정

```

SG2124G#show spanning-tree interface ge3
% 1: Spanning Tree Enabled
% 1: Ageing Time 300 - Root Path Cost 200000 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 5024
% 1: Root Id 8000000c2c030481
% 1: Bridge Id 8000001af40f0400
% 1: 159 topology changes - last topology change Fri May 1 10:52:38 2009
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% ge3: Port 5003 - Id 838b - Role Designated - State Forwarding
% ge3: Configured path cost 200000 - Designated path cost 200000
% ge3: Designated port id 838b - Priority 128
% ge3: Designated Root 8000000c2c030481
% ge3: Designated Bridge 8000001af40f0400
% ge3: Message Age 1 - Max Age 20
% ge3: Hello Time 2 - Forward Delay 15
% ge3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
% ge3: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% ge3: No portfast configured - Current portfast off
% ge3: portfast bpdu-guard default - Current portfast bpdu-guard off
% ge3: portfast bpdu-filter default - Current portfast bpdu-filter off
% ge3: no root guard configured - Current root guard off
% ge3: Configured Link Type point-to-point - Current point-to-point
% ge3: forward-transitions 1
SG2124G#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge3
SG2124G(config-if)#spanning-tree force-version 0
SG2124G(config-if)#end
SG2124G#show spanning-tree interface ge3
% 1: Spanning Tree Enabled
% 1: Ageing Time 300 - Root Path Cost 200000 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 5024
% 1: Root Id 8000000c2c030481
% 1: Bridge Id 8000001af40f0400
% 1: 159 topology changes - last topology change Fri May 1 10:52:38 2009
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% ge3: Port 5003 - Id 838b - Role Designated - State Discarding
% ge3: Configured path cost 200000 - Designated path cost 200000
% ge3: Designated port id 838b - Priority 128
% ge3: Designated Root 8000000c2c030481
% ge3: Designated Bridge 8000001af40f0400
% ge3: Message Age 1 - Max Age 20
% ge3: Hello Time 2 - Forward Delay 15
% ge3: Forward Timer 8 - Msg Age Timer 0 - Hello Timer 1
% ge3: Version Spanning Tree Protocol - Received None - Send STP
% ge3: No portfast configured - Current portfast off
% ge3: portfast bpdu-guard default - Current portfast bpdu-guard off
% ge3: portfast bpdu-filter default - Current portfast bpdu-filter off
% ge3: no root guard configured - Current root guard off
% ge3: Configured Link Type point-to-point - Current point-to-point
% ge3: forward-transitions 1
SG2124G#

```


2.5.10 Root Guard

STP가 활성화되어 관리중인 Network 내에서는 Bridge ID가 가장 작은 Switch가 Root가 됩니다. 그러나 전원중단, Switch 추가 설치, 기존 Switch 제거 등 기존 Network를 구성하던 Switch들이 발생시키는 문제들로 인해 STP 토폴로지가 자주 변경되는 경우 Network가 불안정해질 수 있습니다.

관리자가 Root Switch를 직접 설치한 후 guard 설정을 통해 STP에 의해 변경되지 않도록 설정하여 보다 안정적인 STP를 관리할 수 있습니다.

관리자에 의해 Root로 설정된 Switch에 Root Bridge ID가 수신되면 Message를 보낸 Switch는 Blocking 상태로 바뀌며, Forward Delay 시간 동안 BPDU가 수신되지 않으면 자동으로 Blocking 상태가 해제됩니다.

Root Guard를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
spanning-tree guard root	INTERFACE	spanning-tree guard를 설정합니다.

Root Guard 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show spanning-tree [detail interface <i>IFNAME</i>]	TOP	Spanning-tree 설정 내용을 확인합니다.
show spanning-tree mst <config detail instance interface>	TOP	MSTP 설정 내용을 확인합니다.
show spanning-tree pvstp <detail interface summary vlan>	TOP	PVSTP 설정 내용을 확인합니다.

Root Guard를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no spanning-tree guard root	INTERFACE	spanning-tree guard를 초기화합니다.

<예제> Spanning Tree의 root guard 설정

```

SG2124G(config)#interface ge1
SG2124G(config-if)#spanning-tree guard root
SG2124G(config-if)#end
SG2124G#show spanning-tree interface ge1
% 1: Spanning Tree Enabled
% 1: Ageing Time 300 - Root Path Cost 0 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
% 1: Root Id 8000001af4000541
% 1: Bridge Id 8000001af4000541
% 1: 3 topology changes - last topology change Thu May  7 22:50:28 2009
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% ge1: Port 5001 - Id 8389 - Role Designated - State Forwarding
% ge1: Configured path cost 200000 - Designated path cost 0
% ge1: Designated port id 8389 - Priority 128
% ge1: Designated Root 8000001af4000541
% ge1: Designated Bridge 8000001af4000541
% ge1: Message Age 0 - Max Age 20
% ge1: Hello Time 2 - Forward Delay 15
% ge1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
% ge1: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% ge1: No portfast configured - Current portfast off
% ge1: portfast bpdu-guard default - Current portfast bpdu-guard off
% ge1: portfast bpdu-filter default - Current portfast bpdu-filter off
% ge1: root guard configured - Current root guard on
% ge1: Configured Link Type point-to-point - Current point-to-point
% ge1: forward-transitions 1
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge1
SG2124G(config-if)#no spanning-tree guard root
SG2124G(config-if)#end
SG2124G#show spanning-tree interface ge1
% 1: Spanning Tree Enabled
% 1: Ageing Time 300 - Root Path Cost 0 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
% 1: Root Id 8000001af4000541
% 1: Bridge Id 8000001af4000541
% 1: 3 topology changes - last topology change Thu May  7 22:50:28 2009
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% ge1: Port 5001 - Id 8389 - Role Designated - State Forwarding
% ge1: Configured path cost 200000 - Designated path cost 0
% ge1: Designated port id 8389 - Priority 128
% ge1: Designated Root 8000001af4000541
% ge1: Designated Bridge 8000001af4000541
% ge1: Message Age 0 - Max Age 20
% ge1: Hello Time 2 - Forward Delay 15
% ge1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
% ge1: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% ge1: No portfast configured - Current portfast off
% ge1: portfast bpdu-guard default - Current portfast bpdu-guard off
% ge1: portfast bpdu-filter default - Current portfast bpdu-filter off
% ge1: no root guard configured - Current root guard off
% ge1: Configured Link Type point-to-point - Current point-to-point
% ge1: forward-transitions 1
SG2124G#

```

2.5.11 Link-Type

Switch Interface간의 연결 유형을 link-type 명령을 통해 point-to-point인지 shared edge Interface인지를 설정합니다. Link-type Default 값은 point-to-point Link이며, point-to-point Link는 Rapid Transition을 지원합니다.

link-type을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
spanning-tree link-type {point-to-point shared}	INTERFACE	link-type의 설정을 변경합니다.

link-type의 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show spanning-tree [detail interface <i>IFNAME</i>]	TOP	Spanning-tree 설정 내용을 확인합니다.
show spanning-tree mst <config detail instance interface>	TOP	MSTP 설정 내용을 확인합니다.
show spanning-tree pvstp <detail interface summary vlan>	TOP	PVSTP 설정 내용을 확인합니다.

설정된 link-type 값을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no spanning-tree link-type	INTERFACE	link-type의 설정을 초기화합니다.

<예제> Spanning Tree의 Interface Link Type 설정

```

SG2124G(config)#interface ge1
SG2124G(config-if)#spanning-tree link-type
SG2124G(config-if)#end
SG2124G#show spanning-tree interface ge1
% 1: Spanning Tree Enabled
% 1: Ageing Time 300 - Root Path Cost 0 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
% 1: Root Id 8000001af4000541
% 1: Bridge Id 8000001af4000541
% 1: 3 topology changes - last topology change Thu May  7 22:50:28 2009
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% ge1: Port 5001 - Id 8389 - Role Designated - State Forwarding
% ge1: Configured path cost 200000 - Designated path cost 0
% ge1: Designated port id 8389 - Priority 128
% ge1: Designated Root 8000001af4000541
% ge1: Designated Bridge 8000001af4000541
% ge1: Message Age 0 - Max Age 20
% ge1: Hello Time 2 - Forward Delay 15
% ge1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
% ge1: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% ge1: No portfast configured - Current portfast off
% ge1: portfast bpdu-guard default - Current portfast bpdu-guard off
% ge1: portfast bpdu-filter default - Current portfast bpdu-filter off
% ge1: no root guard configured - Current root guard off
% ge1: Configured Link Type shared - Current shared
% ge1: forward-transitions 1
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge1
SG2124G(config-if)#no spanning-tree link-type
SG2124G(config-if)#end
SG2124G#show spanning-tree interface ge1
% 1: Spanning Tree Enabled
% 1: Ageing Time 300 - Root Path Cost 0 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
% 1: Root Id 8000001af4000541
% 1: Bridge Id 8000001af4000541
% 1: 3 topology changes - last topology change Thu May  7 22:50:28 2009
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% ge1: Port 5001 - Id 8389 - Role Designated - State Forwarding
% ge1: Configured path cost 200000 - Designated path cost 0
% ge1: Designated port id 8389 - Priority 128
% ge1: Designated Root 8000001af4000541
% ge1: Designated Bridge 8000001af4000541
% ge1: Message Age 0 - Max Age 20
% ge1: Hello Time 2 - Forward Delay 15
% ge1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
% ge1: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% ge1: No portfast configured - Current portfast off
% ge1: portfast bpdu-guard default - Current portfast bpdu-guard off
% ge1: portfast bpdu-filter default - Current portfast bpdu-filter off
% ge1: no root guard configured - Current root guard off
% ge1: Configured Link Type point-to-point - Current point-to-point
% ge1: forward-transitions 1
SG2124G#

```

2.5.12 MST Region 설정

MSTP를 설정한 Switch들은 MST Configuration ID를 설정하여 Switch가 어떤 MST Region에 속하게 되는지 결정합니다. Region name, Revision, Instance Map의 값이 일치해야 같은 MST Region에 속하게 됩니다.

MST Region을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
spanning-tree mst configuration	CONFIG	MST 설정 모드로 변경합니다.
bridge 1 region <i>NAME</i>	MST	MST Region Name을 설정합니다.
bridge 1 revision <0-255>	MST	MST Revision을 설정합니다.
bridge 1 instance <1-15> vlan <1-4094>	MST	MSTP Instance에 VLAN을 Mapping 합니다.
bridge-group 1 instance <1-15> [path-cost <1-200000000> priority <0-240>]	INTERFACE	Interface에 MSTP Instance를 설정합니다. (priority 낮은 값이 우선)

MST Region의 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
Show spanning-tree mst	TOP	MSTP의 정보를 확인합니다.
show spanning-tree mst config	TOP	MSTP의 구성 정보를 확인합니다.
show spanning-tree mst detail [state [<i>IFNAME</i>] interface <i>IFNAME</i>]	TOP	Interface 별 MSTP의 세부 정보를 확인합니다.
show spanning-tree mst instance <1-15> [interface <i>IFNAME</i>]	TOP	MSTP의 instance 정보를 확인합니다.
show spanning-tree mst interface <i>IFNAME</i>	TOP	Interface 별 MSTP의 정보를 확인합니다.

설정된 MST Region을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no bridge 1 region	MST	MST Region Name을 초기화합니다.
no bridge 1 instance <1-15> vlan <1-4094>	MST	MSTP Instance에 VLAN을 Mapping 을 초기화합니다.
no bridge-group 1 instance <1-15> path-cost	INTERFACE	Interface에 설정된 MSTP Instance를 초기화합니다.

2.5.13 BPDU 전송 설정

BPDU (Bridge Protocol Data Unit)란 STP / RSTP / MSTP / PVSTP를 설정, 유지 및 최적의 경로를 파악하기 위해 자신의 정보를 서로 교환하는 Message입니다.

■ Hello Time

Hello time은 BPDU를 전송하는 간격으로 Default 설정은 2 s입니다.

■ 유효 시간 (Max Age)

Root Switch는 Switch들에 대한 새로운 정보를 계속해서 송신합니다. 많은 Switch들이 있는 Network에서는 BPDU를 전달 시간이 상당히 걸리게 되며, BPDU를 전달하는 동안에 Network 상태가 변경되면 해당 정보는 더 이상 효력이 없게 됩니다. BPDU에 의해 전달된 STP 정보의 유효시간을 Max Age라고 하며, 유효 시간 동안 수신된 BPDU Packet이 없는 경우 STP를 재구성하게 됩니다.

■ Packet 전송 시간 (Forward Delay)

BPDU에는 Listening과 Learning 상태에서 Forwarding의 상태에 이르기까지 걸리는 시간을 명기할 수 있습니다. 이 때, Interface 상태를 변화시키는데 걸리는 시간 간격을 Forward Delay라고 하며, Listening - Learning - Forwarding의 상태가 변화될 때마다 Forward Delay 시간 동안 기다리기 때문에 실제 Blocking에서 Forwarding으로 변화되기까지의 시간은 Forward Delay 시간의 두 배가 됩니다.

BPDU의 설정을 변경하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
bridge 1 {stp rstp mstp pvstp vlan <i>VLANID</i> } hello-time <1-10>	CONFIG	Hello Time 설정을 변경합니다.
bridge 1 {stp rstp mstp pvstp vlan <i>VLANID</i> } max-age <6-40>	CONFIG	BPDU 유효 시간을 변경합니다.
bridge 1 {stp rstp mstp pvstp vlan <i>VLANID</i> } forward-time <4-30>	CONFIG	Packet 전송 시간을 변경합니다.

BPDU의 설정 값을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show spanning-tree [detail interface <i>IFNAME</i>]	TOP	Spanning-tree 설정 내용을 확인합니다.
show spanning-tree mst <config detail instance interface>	TOP	MSTP 설정 내용을 확인합니다.
show spanning-tree pvstp <detail interface summary vlan>	TOP	PVSTP 설정 내용을 확인합니다.

설정된 BPDU값을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no bridge 1 {stp rstp mstp pvstp vlan <i>VLANID</i> } {hello-time max-age forward-time}	CONFIG	BPDU의 설정을 초기화합니다.

<예제> Spanning Tree의 BPDU 전송 설정 변경 및 확인

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#bridge 1 rstp max-age 10
SG2124G(config)#bridge 1 rstp forward-time 10
SG2124G(config)#bridge 1 rstp hello-time 1
SG2124G(config)#end
SG2124G#show spanning-tree interface ge1
% 1: Spanning Tree Enabled
% 1: Ageing Time 300 - Root Path Cost 0 - Priority 32768
% 1: Forward Delay 10 - Hello Time 1 - Max Age 10 - Root Port 0
% 1: Root Id 8000001af40f0400
% 1: Bridge Id 8000001af40f0400
% 1: 60 topology changes - last topology change Sat May 16 03:36:59 2009
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
-- 이하 생략 --

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#no bridge 1 rstp forward-time
SG2124G(config)#no bridge 1 rstp hello-time
SG2124G(config)#no bridge 1 rstp max-age

```



```
SG2124G(config)#end
SG2124G#show spanning-tree interface ge1
% 1: Spanning Tree Enabled
% 1: Ageing Time 300 - Root Path Cost 0 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
% 1: Root Id 8000001af40f0400
% 1: Bridge Id 8000001af40f0400
% 1: 60 topology changes - last topology change Sat May 16 03:36:59 2009
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
-- 이하 생략 --

SG2124G#
```

2.5.14 Portfast, BPDU-Guard

STP는 Loop가 발생하는 Ring형 또는 mesh형 토폴로지를 Loop가 없는 구조로 바뀌게 하는 역할을 수행합니다. Interface가 살아나게 되면 해당 Interface에서 STP 계산이 수행되는데, 이때 STP 계산을 통해 Blocking 또는 Forwarding 상태로 바뀌게 됩니다. 일반적인 STP 환경에서 Interface에 Link가 연결된 후 이러한 계산을 수행하고 Interface를 Forwarding하는데 소요되는 시간은 대략 30 ~ 50 s로서 이 시간 동안에는 해당 Interface를 통한 Data 송수신이 중단됩니다.

Portfast는 Interface가 Link-Up 되었을 때 Blocking -> Listening -> Learning -> Forwarding의 STP 순서 중에서 Listening -> Learning을 무시하고 Blocking -> Forwarding로 바뀌도록 해 줍니다. 하지만 Interface는 여전히 STP 계산을 수행하는 것이고 따라서 계산 결과에 따라서는 STP Blocking 모드도 될 수 있습니다.

Interface는 여전히 STP 계산에 참여하기 때문에 Root Bridge보다 더 낮은 BPDU 값을 갖는 새로운 장비가 연결되는 경우 전체 STP가 교란되는 현상이 발생하여 문제가 발생할 수 있으므로 portfast가 설정된 Interface에는 PC 또는 Server가 연결되어야 합니다.

Network 관리자는 STP BPDU Guard를 통해서 STP Domain의 경계와 토폴로지를 예측할 수 있습니다. portfast bpdu-guard가 설정되어 있는 Interface 하단에서 BPDU 정보가 들어오면, interface가 disable되면서 해당 Interface 너머 영역의 STP 토폴로지에 영향을 주지 않습니다.

특정 Interface에 대해 STP를 이용한 loop 방지 기능이 필요하지 않거나 해당 Interface 하단에 STP Neighbor가 존재하지 않는 경우 portfast 설정을 통해 STP를 활성화할 필요가 없는 Interface를 지정합니다. (Host가 직접 연결된 Port에 대해 Portfast를 설정하면 Port 상태가 Forwarding 상태로 바로 전환됩니다.)

Interface에 BPDU filter 및 bpdu-guard가 동작하게 하려면 portfast가 설정되어 있어야 합니다. 만약 BPDU guard가 설정된 Interface로 BPDU 정보가 수신하면 해당 Interface의 Link를 Admin Down 시키며 errdisable-timeout이 활성화되어 있으면 설정된 interval후에 다시 Admin UP 됩니다.

Portfast 및 BPDU-Guard를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
bridge 1 {stp rstp mstp pvstp} portfast bpdu-filter	CONFIG	bpdu-filter 기능을 활성화합니다.
bridge 1 {stp rstp mstp pvstp} portfast bpdu-guard	CONFIG	bpdu-guard 기능을 활성화합니다.
bridge 1 {stp rstp mstp pvstp} errdisable-timeout enable	CONFIG	errdisable-timeout 기능을 활성화합니다.

bridge 1 {stp rstp mstp pvstp} errdisable-timeout interval <10-1000000>	CONFIG	errdisable-timeout 기능의 Interval 시간을 설정합니다. (Default 300 s)
bridge 1 pvstp rapid-transitions	CONFIG	pvstp의 rapid-transitions 기능을 활성화 합니다.
spanning-tree portfast	INTERFACE	Portfast 기능을 활성화합니다.
spanning-tree portfast bpdu-filter	INTERFACE	Interface에 bpdu-filter 기능을 활성화 합니다.
spanning-tree portfast bpdu-guard	INTERFACE	Interface에 bpdu-guard 기능을 활성화 합니다.

설정된 Portfast 및 BPDU-Guard를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show spanning-tree [detail interface <i>IFNAME</i>]	TOP	Spanning-tree 설정 내용을 확인합니다.
show spanning-tree mst <config detail instance interface>	TOP	MSTP 설정 내용을 확인합니다.
show spanning-tree pvstp <detail interface summary vlan>	TOP	PVSTP 설정 내용을 확인합니다.

Portfast 및 BPDU-Guard 를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no bridge 1 {stp rstp mstp pvstp} portfast bpdu-filter	CONFIG	bpdu-filter 기능을 초기화합니다.
no bridge 1 {stp rstp mstp pvstp} portfast bpdu-guard	CONFIG	bpdu-guard 기능을 초기화합니다.
no bridge 1 {stp rstp mstp pvstp} errdisable-timeout enable	CONFIG	errdisable-timeout 기능을 초기화합니다.
no bridge 1 {stp rstp mstp pvstp} errdisable-timeout interval	CONFIG	errdisable-timeout 기능의 Interval 시간을 초기화합니다.

no bridge 1 pvstp rapid-transitions	CONFIG	pvstp의 rapid-transitions 기능을 초기화 합니다.
no spanning-tree portfast	INTERFACE	Portfast 기능을 초기화합니다.
no spanning-tree portfast bpdu-filter	INTERFACE	Interface에 bpdu-filter 기능을 초기화합니다.
no spanning-tree portfast bpdu-guard	INTERFACE	Interface에 bpdu-guard 기능을 초기화합니다.



참 고

1. portfast 설정은 edgeport와 중복하여 설정할 수 없습니다.
2. bpdu-filter : BPDU 송수신 불가.
송신되는 BPDU를 차단 하는 기능
3. bpdu-guard : BPDU 송신만 가능.
BPDU 수신 시 Interface를 Down시키는 기능

2.5.15 Spanning-Tree 예제

<예제1> RSTP 및 portfast, priority 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#
SG2124G(config)#bridge 1 protocol rstp vlan-bridge
SG2124G(config)#bridge 1 rstp enable
SG2124G(config)#end
SG2124G#
SG2124G#show spanning-tree detail
% 1: Spanning Tree Enabled
% 1: Ageing Time 300 - Root Path Cost 0 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
% 1: Root Id 8000001af40006d5
% 1: Bridge Id 8000001af40006d5
% 1: 3 topology changes - last topology change Sat Mar 25 09:34:10 2000
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
%
% ge24: Port 5024 - Id 83a2 - Role Designated - State Forwarding
% ge24: Configured path cost 20000 - Designated path cost 0
% ge24: Designated port id 83a2 - Priority 128
% ge24: Designated Root 8000001af40006d5
% ge24: Designated Bridge 8000001af40006d5
% ge24: Message Age 0 - Max Age 20
% ge24: Hello Time 2 - Forward Delay 15
% ge24: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
% ge24: Version Rapid Spanning Tree Protocol - Received None - Send STP
% ge24: No portfast configured - Current portfast off
% ge24: portfast bpdu-guard enabled - Current portfast bpdu-guard on
% ge24: portfast bpdu-filter enabled - Current portfast bpdu-filter on
% ge24: no root guard configured - Current root guard off
% ge24: Configured Link Type point-to-point - Current point-to-point
% ge24: forward-transitions 1
-- 이하 생략 --
```

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#bridge 1 rstp portfast bpdu-filter
SG2124G(config)#bridge 1 rstp portfast bpdu-guard
SG2124G(config)#bridge 1 rstp priority 16384
SG2124G(config)#interface range ge1-22
% ge1-22 Selected
SG2124G(config-if-range)#spanning-tree portfast
% ge1-22 Selected
SG2124G(config-if-range)#spanning-tree portfast bpdu-filter enable
% ge1-22 Selected
SG2124G(config-if-range)#spanning-tree portfast bpdu-guard enable
% ge1-22 Selected
SG2124G(config-if-range)#end
SG2124G#show spanning-tree interface ge22
```

```
% 1: Spanning Tree Enabled
% 1: Ageing Time 300 - Root Path Cost 0 - Priority 16384
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
% 1: Root Id 4000001af40006d5
% 1: Bridge Id 4000001af40006d5
% 1: 3 topology changes - last topology change Sat Mar 25 09:34:10 2000
% 1: portfast bpdu-filter enabled
% 1: portfast bpdu-guard enabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
%
% ge22: Port 5022 - Id 83a0 - Role Disabled - State Discarding
% ge22: Configured path cost 20000000 - Designated path cost 0
% ge22: Designated port id 0 - Priority 128
% ge22: Designated Root 0000000000000000
% ge22: Designated Bridge 0000000000000000
% ge22: Message Age 0 - Max Age 0
% ge22: Hello Time 0 - Forward Delay 0
% ge22: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
% ge22: Version Rapid Spanning Tree Protocol - Received None - Send STP
% ge22: Portfast configured - Current portfast on
% ge22: portfast bpdu-guard enabled - Current portfast bpdu-guard on
% ge22: portfast bpdu-filter enabled - Current portfast bpdu-filter on
% ge22: no root guard configured - Current root guard off
% ge22: Configured Link Type point-to-point - Current shared
% ge22: forward-transitions 0
```

<예제2> STP 및 portfast, priority 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#bridge 1 protocol ieee vlan-bridge
SG2124G(config)#bridge 1 stp enable
SG2124G(config)#end
SG2124G#show spanning-tree detail
% 1: spanning tree enabled - topology change - topology change detected
% 1: root path cost 0 - priority 32768
% 1: forward-time 15 - hello-time 2 - max-age 20 - root port 0
% 1: root id 8000001af40006d5
% 1: bridge id 8000001af40006d5
% 1: hello timer 1 - tcn timer 0 - topo change timer 28
% 1: 0 topology changes - last topology change Thu Jan 1 09:00:00 1970
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
% ge24: port 5024 - id 83a2 - path cost 4 - designated cost 0
% ge24: designated port id 83a2 - state Forwarding - priority 128
% ge24: designated root 8000001af40006d5
% ge24: designated bridge 8000001af40006d5
% ge24: forward-timer 0 - hold-timer 0 - msg age timer 0
% ge24: forward-transitions 2
% ge24: portfast disabled
-- 이하 생략 --
```

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#bridge 1 stp priority 16384
SG2124G#show spanning-tree detail
% 1: spanning tree enabled
% 1: root path cost 0 - priority 16384
% 1: forward-time 15 - hello-time 2 - max-age 20 - root port 0
% 1: root id 4000001af40006d5
% 1: bridge id 4000001af40006d5
% 1: hello timer 0 - tcn timer 0 - topo change timer 0
% 1: 0 topology changes - last topology change Thu Jan  1 09:00:00 1970
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
-- 이하 생략 --

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#bridge 1 stp portfast bpdu-guard
SG2124G(config)#bridge 1 stp portfast bpdu-filter
SG2124G(config)#interface range ge1-22
% ge1-22 Selected
SG2124G(config-if-range)#spanning-tree portfast
% ge1-22 Selected
SG2124G(config-if-range)#spanning-tree portfast bpdu-guard enable
% ge1-22 Selected
SG2124G(config-if-range)#spanning-tree portfast bpdu-filter enable
% ge1-22 Selected
SG2124G(config-if-range)#end
SG2124G#sh spanning-tree interface ge22
% 1: spanning tree enabled
% 1: root path cost 0 - priority 16384
% 1: forward-time 15 - hello-time 2 - max-age 20 - root port 0
% 1: root id 4000001af40006d5
% 1: bridge id 4000001af40006d5
% 1: hello timer 0 - tcn timer 0 - topo change timer 0
% 1: 0 topology changes - last topology change Thu Jan  1 09:00:00 1970
% 1: portfast bpdu-filter enabled
% 1: portfast bpdu-guard enabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
%
% ge22: port 5022 - id 83a0 - path cost 20000000 - designated cost 0
% ge22: designated port id 83a0 - state Forwarding - priority 128
% ge22: designated root 4000001af40006d5
% ge22: designated bridge 4000001af40006d5
% ge22: forward-timer 0 - hold-timer 0 - msg age timer 0
% ge22: forward-transitions 2
% ge22: portfast enabled
% ge22: portfast bpdu-guard enabled - Current portfast bpdu-guard on
% ge22: portfast bpdu-filter enabled - Current portfast bpdu-filter on
% ge22: no root guard configured - Current root guard off

```

<예제3> MSTP 설정

ge1-24는 trunk, VLAN 10,40은 instance 1, VLAN 20,50은 instance 2, VLAN 30,60은 instance 3

우선 순위 설정 : ge1-8은 instance 1, ge9-16은 instance 2, ge17-24은 instance 3

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#bridge 1 protocol mstp
SG2124G(config)#vlan database
SG2124G(config-vlan)#vlan range 10,20,30,40,50,60 bridge 1
SG2124G(config-vlan)#exit
SG2124G(config)#spanning-tree mst configuration
SG2124G(config-mst)#bridge 1 revision 1
SG2124G(config-mst)#bridge 1 region test
SG2124G(config-mst)#bridge 1 instance 1
SG2124G(config-mst)#bridge 1 instance 2
SG2124G(config-mst)#bridge 1 instance 3
SG2124G(config-mst)#bridge 1 instance 1 vlan 10
SG2124G(config-mst)#bridge 1 instance 1 vlan 40
SG2124G(config-mst)#bridge 1 instance 2 vlan 20
SG2124G(config-mst)#bridge 1 instance 2 vlan 50
SG2124G(config-mst)#bridge 1 instance 3 vlan 30
SG2124G(config-mst)#bridge 1 instance 3 vlan 60
SG2124G(config-mst)#exit
SG2124G(config)#interface range ge
% ge Selected
SG2124G(config-if-range)#switchport mode trunk
% ge Selected
SG2124G(config-if-range)#switchport trunk allowed vlan add 10,20,30,40,50,60
% ge Selected
SG2124G(config-if-range)#exit
SG2124G(config)#interface range ge1-8
% ge1-8 Selected
SG2124G(config-if-range)#bridge-group 1 instance 1
% ge1-8 Selected
SG2124G(config-if-range)#bridge-group 1 instance 2
% ge1-8 Selected
SG2124G(config-if-range)#bridge-group 1 instance 3
% ge1-8 Selected
SG2124G(config-if-range)#bridge-group 1 instance 1 priority 16
% ge1-8 Selected
SG2124G(config-if-range)#bridge-group 1 instance 2 priority 32
% ge1-8 Selected
SG2124G(config-if-range)#bridge-group 1 instance 3 priority 32
% ge1-8 Selected
SG2124G(config-if-range)#exit
SG2124G(config)#interface range ge9-16
% ge9-16 Selected
SG2124G(config-if-range)#bridge-group 1 instance 1
% ge9-16 Selected
SG2124G(config-if-range)#bridge-group 1 instance 2
% ge9-16 Selected
SG2124G(config-if-range)#bridge-group 1 instance 3
% ge9-16 Selected
SG2124G(config-if-range)#bridge-group 1 instance 1 priority 32
% ge9-16 Selected
SG2124G(config-if-range)#bridge-group 1 instance 2 priority 16
```



```

% ge9-16 Selected
SG2124G(config-if-range)#bridge-group 1 instance 3 priority 32
% ge9-16 Selected
SG2124G(config-if-range)#exit
SG2124G(config)#interface range ge17-24
% ge17-24 Selected
SG2124G(config-if-range)#bridge-group 1 instance 1
% ge17-24 Selected
SG2124G(config-if-range)#bridge-group 1 instance 2
% ge17-24 Selected
SG2124G(config-if-range)#bridge-group 1 instance 3
% ge17-24 Selected
SG2124G(config-if-range)#bridge-group 1 instance 1 priority 32
% ge17-24 Selected
SG2124G(config-if-range)#bridge-group 1 instance 2 priority 32
% ge17-24 Selected
SG2124G(config-if-range)#bridge-group 1 instance 3 priority 16
% ge17-24 Selected
SG2124G(config-if-range)#end
SG2124G#show spanning-tree mst
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 8000001af40006d5
% 1: CIST Reg Root Id 8000001af40006d5
% 1: CST Bridge Id 8000001af40006d5
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
%
% Instance      VLAN
% 0:            1
% 1:            10, 40
% 2:            20, 50
% 3:            30, 60
SG2124G#show spanning-tree mst detail interface ge1
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 8000001af40006d5
% 1: CIST Reg Root Id 8000001af40006d5
% 1: CST Bridge Id 8000001af40006d5
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
% ge1: Port 5001 - Id 8389 - Role Designated - State Forwarding
% ge1: Designated External Path Cost 0 - Internal Path Cost 0
% ge1: Configured Path Cost 200000 - Add type Explicit ref count 4
% ge1: Designated Port Id 8389 - CST Priority 128 -
% ge1: CIST Root 8000001af40006d5
% ge1: Regional Root 8000001af40006d5
% ge1: Designated Bridge 8000001af40006d5
% ge1: Message Age 0 - Max Age 20
% ge1: CIST Hello Time 2 - Forward Delay 15

```

```

% ge1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
% ge1: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
% ge1: No portfast configured - Current portfast off
% ge1: portfast bpdu-guard default - Current portfast bpdu-guard off
% ge1: portfast bpdu-filter default - Current portfast bpdu-filter off
% ge1: no root guard configured - Current root guard off
% ge1: Configured Link Type point-to-point - Current point-to-point
%

% Instance 1: Vlans: 10, 40
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8001001af40006d5
% 1: MSTI Bridge Id 8001001af40006d5
% ge1: Port 5001 - Id 8389 - Role Designated - State Forwarding
% ge1: Designated Internal Path Cost 0 - Designated Port Id 1389
% ge1: Configured Internal Path Cost 200000
% ge1: Configured CST External Path cost 200000
% ge1: CST Priority 128 - MSTI Priority 16
% ge1: Designated Root 8001001af40006d5
% ge1: Designated Bridge 8001001af40006d5
% ge1: Message Age 0 - Max Age 0
% ge1: Hello Time 2 - Forward Delay 15
% ge1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%

% Instance 2: Vlans: 20, 50
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8002001af40006d5
% 1: MSTI Bridge Id 8002001af40006d5
% ge1: Port 5001 - Id 8389 - Role Designated - State Forwarding
% ge1: Designated Internal Path Cost 0 - Designated Port Id 2389
% ge1: Configured Internal Path Cost 200000
% ge1: Configured CST External Path cost 200000
% ge1: CST Priority 128 - MSTI Priority 32
% ge1: Designated Root 8002001af40006d5
% ge1: Designated Bridge 8002001af40006d5
% ge1: Message Age 0 - Max Age 0
% ge1: Hello Time 2 - Forward Delay 15
% ge1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%

% Instance 3: Vlans: 30, 60
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8003001af40006d5
% 1: MSTI Bridge Id 8003001af40006d5
% ge1: Port 5001 - Id 8389 - Role Designated - State Forwarding
% ge1: Designated Internal Path Cost 0 - Designated Port Id 2389
% ge1: Configured Internal Path Cost 200000
% ge1: Configured CST External Path cost 200000
% ge1: CST Priority 128 - MSTI Priority 32
% ge1: Designated Root 8003001af40006d5
% ge1: Designated Bridge 8003001af40006d5
% ge1: Message Age 0 - Max Age 0
% ge1: Hello Time 2 - Forward Delay 15
% ge1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%

SG2124G#show spanning-tree mst detail interface ge9

```

```

% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 8000001af40006d5
% 1: CIST Reg Root Id 8000001af40006d5
% 1: CST Bridge Id 8000001af40006d5
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
%
% ge9: Port 5009 - Id 8391 - Role Disabled - State Discarding
% ge9: Designated External Path Cost 0 - Internal Path Cost 0
% ge9: Configured Path Cost 20000000 - Add type Explicit ref count 4
% ge9: Designated Port Id 0 - CST Priority 128 -
% ge9: CIST Root 0000000000000000
% ge9: Regional Root 0000000000000000
% ge9: Designated Bridge 0000000000000000
% ge9: Message Age 0 - Max Age 0
% ge9: CIST Hello Time 0 - Forward Delay 0
% ge9: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
% ge9: Version Multiple Spanning Tree Protocol - Received None - Send STP
% ge9: No portfast configured - Current portfast off
% ge9: portfast bpdu-guard default - Current portfast bpdu-guard off
% ge9: portfast bpdu-filter default - Current portfast bpdu-filter off
% ge9: no root guard configured - Current root guard off
% ge9: Configured Link Type point-to-point - Current shared
%
% Instance 1: Vlans: 10, 40
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8001001af40006d5
% 1: MSTI Bridge Id 8001001af40006d5
% ge9: Port 5009 - Id 8391 - Role Disabled - State Discarding
% ge9: Designated Internal Path Cost 0 - Designated Port Id 0
% ge9: Configured Internal Path Cost 20000000
% ge9: Configured CST External Path cost 20000000
% ge9: CST Priority 128 - MSTI Priority 32
% ge9: Designated Root 0000000000000000
% ge9: Designated Bridge 0000000000000000
% ge9: Message Age 0 - Max Age 0
% ge9: Hello Time 0 - Forward Delay 0
% ge9: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
% Instance 2: Vlans: 20, 50
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8002001af40006d5
% 1: MSTI Bridge Id 8002001af40006d5
% ge9: Port 5009 - Id 8391 - Role Disabled - State Discarding
% ge9: Designated Internal Path Cost 0 - Designated Port Id 0
% ge9: Configured Internal Path Cost 20000000
% ge9: Configured CST External Path cost 20000000
% ge9: CST Priority 128 - MSTI Priority 16
% ge9: Designated Root 0000000000000000
% ge9: Designated Bridge 0000000000000000
% ge9: Message Age 0 - Max Age 0
% ge9: Hello Time 0 - Forward Delay 0

```

```

% ge9: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
% Instance 3: Vlans: 30, 60
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8003001af40006d5
% 1: MSTI Bridge Id 8003001af40006d5
% ge9: Port 5009 - Id 8391 - Role Disabled - State Discarding
% ge9: Designated Internal Path Cost 0 - Designated Port Id 0
% ge9: Configured Internal Path Cost 20000000
% ge9: Configured CST External Path cost 20000000
% ge9: CST Priority 128 - MSTI Priority 32
% ge9: Designated Root 0000000000000000
% ge9: Designated Bridge 0000000000000000
% ge9: Message Age 0 - Max Age 0
% ge9: Hello Time 0 - Forward Delay 0
% ge9: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
SG2124G#show spanning-tree mst detail interface ge17
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 8000001af40006d5
% 1: CIST Reg Root Id 8000001af40006d5
% 1: CST Bridge Id 8000001af40006d5
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
% ge17: Port 5017 - Id 8399 - Role Disabled - State Discarding
% ge17: Designated External Path Cost 0 - Internal Path Cost 0
% ge17: Configured Path Cost 20000000 - Add type Explicit ref count 4
% ge17: Designated Port Id 0 - CST Priority 128 -
% ge17: CIST Root 0000000000000000
% ge17: Regional Root 0000000000000000
% ge17: Designated Bridge 0000000000000000
% ge17: Message Age 0 - Max Age 0
% ge17: CIST Hello Time 0 - Forward Delay 0
% ge17: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
% ge17: Version Multiple Spanning Tree Protocol - Received None - Send STP
% ge17: No portfast configured - Current portfast off
% ge17: portfast bpdu-guard default - Current portfast bpdu-guard off
% ge17: portfast bpdu-filter default - Current portfast bpdu-filter off
% ge17: no root guard configured - Current root guard off
% ge17: Configured Link Type point-to-point - Current shared
%
% Instance 1: Vlans: 10, 40
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8001001af40006d5
% 1: MSTI Bridge Id 8001001af40006d5
% ge17: Port 5017 - Id 8399 - Role Disabled - State Discarding
% ge17: Designated Internal Path Cost 0 - Designated Port Id 0
% ge17: Configured Internal Path Cost 20000000
% ge17: Configured CST External Path cost 20000000
% ge17: CST Priority 128 - MSTI Priority 32
% ge17: Designated Root 0000000000000000
% ge17: Designated Bridge 0000000000000000

```

```
% ge17: Message Age 0 - Max Age 0
% ge17: Hello Time 0 - Forward Delay 0
% ge17: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
% Instance 2: Vlans: 20, 50
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8002001af40006d5
% 1: MSTI Bridge Id 8002001af40006d5
% ge17: Port 5017 - Id 8399 - Role Disabled - State Discarding
% ge17: Designated Internal Path Cost 0 - Designated Port Id 0
% ge17: Configured Internal Path Cost 20000000
% ge17: Configured CST External Path cost 20000000
% ge17: CST Priority 128 - MSTI Priority 32
% ge17: Designated Root 0000000000000000
% ge17: Designated Bridge 0000000000000000
% ge17: Message Age 0 - Max Age 0
% ge17: Hello Time 0 - Forward Delay 0
% ge17: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
% Instance 3: Vlans: 30, 60
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8003001af40006d5
% 1: MSTI Bridge Id 8003001af40006d5
% ge17: Port 5017 - Id 8399 - Role Disabled - State Discarding
% ge17: Designated Internal Path Cost 0 - Designated Port Id 0
% ge17: Configured Internal Path Cost 20000000
% ge17: Configured CST External Path cost 20000000
% ge17: CST Priority 128 - MSTI Priority 16
% ge17: Designated Root 0000000000000000
% ge17: Designated Bridge 0000000000000000
% ge17: Message Age 0 - Max Age 0
% ge17: Hello Time 0 - Forward Delay 0
% ge17: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```

<예제4> PVSTP 설정

SG2124G-1 Switch, SG2124G-2 Switch의 ge23-24를 연결 후 PVSTP 설정

SG2124G-2 Switch의 VLAN 5의 Priority 값을 4096으로 변경설정

```
=====
SG2124G-1
=====
SG2124G-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G-1(config)#vlan database
SG2124G-1(config-vlan)#vlan range 4-5 bridge 1
SG2124G-1(config-vlan)#exit
SG2124G-1(config)#bridge 1 protocol pvstp
SG2124G-1(config)#bridge 1 pvstp enable
SG2124G-1(config)#bridge 1 pvstp vlan 4-5
SG2124G-1(config)#interface range ge23-24
% ge23-24 Selected
SG2124G-1(config-if-range)#switchport mode trunk
% ge23-24 Selected
SG2124G-1(config-if-range)#switchport trunk allowed vlan add 4-5
% ge23-24 Selected
```

```

SG2124G-1(config-if-range)#exit
SG2124G-1(config)#interface range ge1-12
% ge1-12 Selected
SG2124G-1(config-if-range)#switchport access vlan 4
% ge1-12 Selected
SG2124G-1(config-if-range)#exit
SG2124G-1(config)#interface range ge13-22
% ge13-22 Selected
SG2124G-1(config-if-range)#switchport access vlan 5
% ge13-22 Selected
SG2124G-1(config-if-range)#end
SG2124G-1#show spanning-tree pvstp summary

```

```

portfast bpdu-filter disabled
portfast bpdu-guard disabled
portfast errdisable timeout enabled
portfast errdisable timeout interval 300 sec

```

Name	Blocking	Listening	Learning	Forwarding	STP Active
-----	-----	-----	-----	-----	-----
VLAN1	0	0	0	2	2
VLAN4	0	0	0	2	2
VLAN5	1	0	0	1	2
-----	-----	-----	-----	-----	-----
3 vlans	1	0	0	5	6

```

SG2124G-1#
SG2124G-1#show spanning-tree pvstp

```

VLAN1

```

Spanning Tree Enabled protocol PVSTP
Root Path Cost 0 - Priority 32769 (priority 32768 sys-id-ext 1)
Root Id 8001001af4000300
Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
Bridge Id 8001001af4000300
Forward Delay 15 - Hello Time 2 - Max Age 20

```

Interface	Role	State	Path-cost	Priority	Rcv	Send
-----	-----	-----	-----	-----	-----	-----
ge24	Designated	Forwarding	4	128	RSTP	RSTP
ge23	Designated	Forwarding	4	128	RSTP	RSTP

VLAN4

```

Spanning Tree Enabled protocol PVSTP
Root Path Cost 0 - Priority 32772 (priority 32768 sys-id-ext 4)
Root Id 8004001af4000300
Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0
Bridge Id 8004001af4000300
Forward Delay 15 - Hello Time 2 - Max Age 20

```

Interface	Role	State	Path-cost	Priority	Rcv	Send
-----	-----	-----	-----	-----	-----	-----
ge24	Designated	Forwarding	4	128	RSTP	RSTP
ge23	Designated	Forwarding	4	128	RSTP	RSTP

VLAN5

```

Spanning Tree Enabled protocol PVSTP

```

```

Root Path Cost 4 - Priority 32773 (priority 32768 sys-id-ext 5)
Root Id 1005001af40003aa
  Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 5025
Bridge Id 8005001af4000300
  Forward Delay 15 - Hello Time 2 - Max Age 20

```

Interface	Role	State	Path-cost	Priority	Rcv	Send
ge24	Alternate	Discarding	4	128	RSTP	RSTP
ge23	Rootport	Forwarding	4	128	RSTP	RSTP

SG2124G#

SG2124G-2

```

SG2124G-2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G-2(config)#vlan database
SG2124G-2(config-vlan)#vlan range 4-5 bridge 1
SG2124G-2(config-vlan)#exit
SG2124G-2(config)#bridge 1 protocol pvstp
SG2124G-2(config)#bridge 1 pvstp enable
SG2124G-2(config)#bridge 1 pvstp vlan 4-5
SG2124G-2(config)#bridge 1 pvstp vlan 5 priority 4096
SG2124G-2(config)#
SG2124G-2(config)#interface range ge23-24
% ge23-24 Selected
SG2124G-2(config-if-range)#switchport mode trunk
% ge23-24 Selected
SG2124G-2(config-if-range)#switchport trunk allowed vlan add 4-5
% ge23-24 Selected
SG2124G-2(config-if-range)#exit
SG2124G-2(config)#interface range ge1-12
% ge1-12 Selected
SG2124G-2(config-if-range)#switchport access vlan 4
% ge1-12 Selected
SG2124G-2(config-if-range)#exit
SG2124G-2(config)#interface range ge13-22
% ge13-22 Selected
SG2124G-2(config-if-range)#switchport access vlan 5
% ge13-22 Selected
SG2124G-2(config-if-range)#end
SG2124G-2#show spanning-tree pvstp summary

```

```

portfast bpd-filter disabled
portfast bpd-guard disabled
portfast errdisable timeout enabled
portfast errdisable timeout interval 300 sec

```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN1	1	0	0	1	2
VLAN4	1	0	0	1	2
VLAN5	0	0	0	2	2
3 vlans	2	0	0	4	6

SG2124G-2#

SG2124G-2#show spanning-tree pvstp

VLAN1

Spanning Tree Enabled protocol PVSTP

Root Path Cost 4 - Priority 32769 (priority 32768 sys-id-ext 1)

Root Id 8001001af4000300

Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 5025

Bridge Id 8001001af40003aa

Forward Delay 15 - Hello Time 2 - Max Age 20

Interface	Role	State	Path-cost	Priority	Rcv	Send
ge24	Alternate	Discarding	4	128	RSTP	RSTP
ge23	Rootport	Forwarding	4	128	RSTP	RSTP

VLAN4

Spanning Tree Enabled protocol PVSTP

Root Path Cost 4 - Priority 32772 (priority 32768 sys-id-ext 4)

Root Id 8004001af4000300

Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 5025

Bridge Id 8004001af40003aa

Forward Delay 15 - Hello Time 2 - Max Age 20

Interface	Role	State	Path-cost	Priority	Rcv	Send
ge24	Alternate	Discarding	4	128	RSTP	RSTP
ge23	Rootport	Forwarding	4	128	RSTP	RSTP

VLAN5

Spanning Tree Enabled protocol PVSTP

Root Path Cost 0 - Priority 4101 (priority 4096 sys-id-ext 5)

Root Id 1005001af40003aa

Forward Delay 15 - Hello Time 2 - Max Age 20 - Root Port 0

Bridge Id 1005001af40003aa

Forward Delay 15 - Hello Time 2 - Max Age 20

Interface	Role	State	Path-cost	Priority	Rcv	Send
ge24	Designated	Forwarding	4	128	RSTP	RSTP
ge23	Designated	Forwarding	4	128	RSTP	RSTP

SG2124G-2#

2.6 QoS

2.6.1 QoS 개요

QoS (Quality of Service)는 Traffic 과부하 시 Traffic에 우선 순위를 설정함으로써 중요 Traffic의 전송 실패나 지연을 방지하도록 설정하여 Traffic의 손실을 최소화하는데 효과적입니다. 특정한 Traffic에 우선권을 부여하거나 특정한 Traffic을 제외한 나머지 Traffic을 제한함으로써 우선권을 부여할 수 있습니다.

일반적으로 Network에서 Data를 처리할 때는 먼저 입력된 Data를 먼저 처리하는데 모든 Data를 시간 순서대로 처리하는 이 방식은 Traffic이 한꺼번에 몰렸을 때 Data를 잃어버리는 단점이 있습니다. QoS는 Traffic이 과부하일 때 상대적인 중요도에 따라 우선 순위를 재조정하여 처리 순서를 다르게 적용합니다. QoS를 이용하여 Network 성능을 미리 예측하고 보다 효율적으로 대역폭을 관리할 수 있습니다.

2.6.2 QoS 적용 방법

입력되는 Packet에 대해 Packet을 분류하는 규칙을 적용하여 IEEE802.1p에서 정의한 CoS (Class of Service) 값으로 우선 순위를 설정한 후 QoS를 적용시킵니다. 입력되는 Packet에 대해 Packet 분류를 수행한 후 Packet 처리 정책(policy)을 정하는 방법은 다음과 같습니다.

■ Packet 분류(packet classification)

Traffic을 특정한 속성에 따라 분류합니다. 이러한 분류에 사용되는 기준 속성은 MAC Address, VLAN ID, IP Address, IP Protocol, L4 Service Port Number, IP precedence, DiffServ의 DSCP 값 등입니다.

■ 정책 적용 (Policy)

Packet을 분류된 후에 분류된 Packet에 대해 특정한 정책을 수행할 수 있습니다.

Packet 차단, Packet 허용, 대역폭 제한, CoS값 설정, DSCP 값 설정, IP precedence 값 설정 등의 정책을 수행할 수 있습니다.

■ QoS Mapping

Interface 별로 8개의 Queue를 지원하며, 이들 Queue는 Traffic 처리에 대한 각기 다른 우선순위를 가집니다. Packet의 CoS값에 따라 특정한 Queue로 Traffic을 전달하도록 Mapping 할 수 있습니다. QoS Mapping 설정한 후에는 Traffic 과부하 시에 Traffic 처리에 대한 우선순위가 결정됩니다.

■ 스케줄링(Scheduling)

Traffic 과부하가 발생했을 경우 이를 조정하는 방안은 scheduling 알고리즘을 사용하여 Traffic 처리 순서를 다르게 지정하는 것입니다.

■ 우선 순위 알고리즘 (SPQ : Strict Priority Queuing)

이 정책에서는 높은 우선순위 Queue에 위치한 Packet이 먼저 전송됩니다. 높은 우선순위의 Queue에 Packet이 없는 경우에만 다음 낮은 순위의 Queue에 있는 Packet이 전송될 수 있습니다. 낮은 우선순위의 Queue에 있는 Packet은 처리 순서가 밀리면서 대기 상태 (Starvation)로 있는 단점이 있습니다.

■ 비율 기반 알고리즘 (WRR : Weighted Round Robin)

일정 비율을 기반으로 Data를 처리하는 이 알고리즘은 Queue에 Packet을 처리하는 비율 (Weight: 처리 Packet 수)을 관리자가 지정함으로써 Packet의 우선 순위에 따른 Packet 처리 비율을 지정할 수 있습니다.

■ 가중치 기반 알고리즘 (DRR : Deficit Round Robin)

Packet의 개수가 아닌 Packet의 Size를 기준으로 Data를 처리하는 알고리즘입니다. 간단히 살펴 보면, 초기 값이 0인 Deficit Counter 는 각각의 입력 Interface에 해당하는 출력 Queue마다 유지 되고 있는 변수입니다. 그리고 Packet을 받으면 Packet을 받은 Queue가 활성화 되어 있다는 것을 Active queue 에 넣고 Packet을 Enqueue 를 합니다. Dequeue 할 때 Active List 에 활성화된 Queue가 존재하면 현재 Queue가 유지하고 있는 Deficit Counter 에 Quantum size를 더한 후 Deficit counter 의 값과 Queue에 있는 Packet의 Size를 비교 하여 Packet Size가 Deficit counter 값보다 작을 경우 Packet을 Dequeue 하게 됩니다.

이 때 Deficit counter 값은 전송된 Packet의 길이만큼의 값을 빼게 되는데, Deficit Counter 의 값이 보내려는 Packet Size보다 작아질 때까지 계속 Dequeue 를 반복합니다. 만약 Deficit Counter의 값이 Packet Size 보다 작은 경우엔 Round Robin 스케줄링이 한Cycle 돈 후 다시 Quantum size 만큼의 Count 값을 더하여 Packet을 보내게 됩니다.

■ 공정 비율 알고리즘 (WFQ : weighted fair queuing)

모든 Queue에 최소 대역폭을 제공함으로써 낮은 우선순위 Queue에 있는 Packet이 계속적으로 처리되지 못할 수 있는 단점을 제거합니다. 보장된 대역폭이 Queue 별로 먼저 공급되고, 설정된 최대 대역폭까지 남아있는 대역폭이 우선 순위나 Round Robin 방식으로 분배됩니다. 이 방식은 낮은 우선순위의 Queue가 처리되지 않는 문제를 해결하면서 제어 가능한 CoS 동작을 제공합니다.

[표 2-9] QoS Default Map

	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
CoS	0	1	2	3	4	5	6	7
DSCP	0~7	8~15	16~23	24~31	32~39	40~47	48~55	56~63
우선순위	Low ←-----→ High							

2.6.3 QoS ACL 설정

Network 관리자는 Network을 통해 전송되는 Traffic에 대해 ACL를 사용함으로써 상당히 세밀하게 통제할 수 있습니다. 관리자는 Packet의 전송 상태에 대한 기본적인 통계자료를 통해 보안 정책을 수립할 수 있습니다. 또한 인증되지 않은 Packet의 접속으로부터 시스템을 보호할 수 있으며, 특정 Packet에 대한 허용 및 거부 정책을 사용하거나 QoS를 적용하는데 사용할 수 있습니다.

ACL에는 리스트의 구분을 위해 access list 번호가 할당됩니다. Packet의 조건과 조건에 해당하는 Packet을 어떻게 처리할 것인지 그 처리 방법으로 이루어집니다. 다양한 기준으로 관리자가 원하는 조건을 설정합니다.

Access List 넘버 200-299는 IPv6 Standard access list에 할당되어 있으며, 300-399는 IPv6 Extended access list에 할당되어 있습니다.

ACL에 매치된 패킷 로그를 출력하려면 ACL 설정시 log 옵션을 활성화해야 하며, ACL 로그 출력 주기는 ACL log interval에 따라 변경됩니다. 기본 log 출력 주기는 10분입니다.

ACL 로그는 패킷이 매치된 ACL rule 번호, deny 혹은 permit 액션, 매치된 조건, 매치 카운터 정보를 출력합니다. ACL 로그는 ACL을 포트에 적용한 후부터 동작하며, ACL을 포트에 적용하는 방법은 "2.10 Filtering"메뉴 참고하시기 바랍니다.

ACL을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
acl <1-99> {permit deny} {any IP_Addr Wildcard } [log time-range NAME]	CONFIG	IP Standard Access List를 설정합니다.
acl <100-199> {permit deny} {icmp ip tcp udp} {any SRC_IP_Addr Wildcard host SRC_host} {any DST_IP_Addr Wildcard host DST_host} {dp sp} eq <0-65535> [log time-range NAME]	CONFIG	IP Extended Access List 를 설정합니다.
acl <700-799> {permit deny} {any SRC_MAC_Addr Wildcard } {any DST_MAC_Addr Wildcard } <1-4> [log time-range NAME]	CONFIG	MAC Extended Access List를 설정합니다. <1-4> : 1:Ethernet II/ 2:802.3 / 3:SNAP/ 4:LLC
acl <1100-1199> {permit deny} {any SRC_MAC_Addr Wildcard } {any DST_MAC_Addr Wildcard } <1-4> [log time-range NAME]	CONFIG	MAC Extended Access List 를 설정합니다. (Expanded Range) <1-4> : 1:Ethernet II/ 2:802.3 / 3:SNAP/ 4:LLC

acl <1300-1999> {permit deny} {any <i>IP_Addr</i> Wildcard} [log time-range <i>NAME</i>]	CONFIG	IP Standard Access List 를 설정합니다. (Expanded Range)
acl <2000-2699> {permit deny} {icmp ip tcp udp} {any <i>SRC_IP_Addr</i> Wildcard host <i>SRC_host</i> {any <i>DST_IP_Addr</i> Wildcard host <i>DST_host</i> {dp sp} eq <0-65535> [log time-range <i>NAME</i>]	CONFIG	IP Extended Access List를 설정합니다. (Expanded Range)
acl <200-299> {permit deny} {any <i>SRC_IPv6_Addr/Mask</i> } {any <i>DST_IPv6_Addr/Mask</i> } [log time-range <i>NAME</i>]	CONFIG	IPv6 Standard Access List를 설정합니다.
acl <300-399> {permit deny} {any <i>SRC_IPv6_Addr/Mask</i> } {any <i>DST_IPv6_Addr/Mask</i> } [log time-range <i>NAME</i>]	CONFIG	IPv6 Extended Access List 를 설정합니다.
acl <500-599> {permit deny} { <i>sender_IP_Addr</i> } [Wildcard] [log time-range <i>NAME</i>]	CONFIG	ARP standard access list를 설정합니다.
acl <i>acl_name</i> {permit deny} {icmp ip tcp udp} <i>SIP_Addr</i> Wildcard <i>DIP_Addr</i> Wildcard_bits {dp sp} eq {<0-65535> Port_Name}	CONFIG	Name Access List를 설정합니다. (<i>acl_name</i> : Max 19글자.)
acl log interval <1-1440>	CONFIG	Access List 내역이 log에 기록되도록 설정합니다. (단위 : min)



참고

1. 동일한 ACL 번호에는 IPv4 최대 128개, IPv6는 최대 64개까지의 Entry를 설정할 수 있습니다.
2. SG2024, SG2024P, SG2200 Series 제품은 IPv6 ACL/QoS를 지원하지 않습니다.
3. IPv6 ACL기능은 Switch버전 2.x 이상에서만 지원합니다.

설정된 ACL을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show acl	TOP	설정된 ACL 전체의 설정 내용 및 QoS에 적용된 Packet의 Count 값을 확인합니다.
show ip acl [IFNAME]	TOP	특정 Interface에 적용된 ACL을 확인합니다.
show acl [<1-99> <100-199> <1100-1199> <1300-1999> <2000-2699> <700-799>]	TOP	특정 ACL의 설정 내용을 확인합니다.

ACL을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no acl <1-99> {permit deny} {any IP_Addr Wildcard}	CONFIG	IP Standard Access List를 초기화합니다.
no acl <100-199> {permit deny} {icmp ip tcp udp} {any SRC_IP_Addr Wildcard host SRC_host} {any DST_IP_Addr Wildcard host DST_host} {dp sp} eq <0-65535>	CONFIG	IP Extended Access List를 초기화합니다.
no acl <700-799> {permit deny} {any SRC_MAC_Addr} {any DST_MAC_Addr} <1-4>	CONFIG	MAC Extended Access List를 초기화합니다. <1-4> : 1:Ethernet II/ 2:802.3 / 3:SNAP/ 4:LLC
no acl <1100-1199> {permit deny} {any SRC_MAC_Addr Wildcard} {any DST_MAC_Addr Wildcard} <1-4>	CONFIG	MAC Extended Access List를 초기화합니다. (Expanded Range) <1-4> : 1:Ethernet II/ 2:802.3 / 3:SNAP/ 4:LLC
no acl <1300-1999> {permit deny} {any IP_Addr Wildcard}	CONFIG	IP Standard Access List를 초기화합니다. (Expanded Range)
no acl <2000-2699> {permit deny} {icmp ip tcp udp} {any SRC_IP_Addr Wildcard host SRC_host} {any DST_IP_Addr Wildcard host DST_host} {dp sp} eq <0-65535>	CONFIG	IP Extended Access List를 초기화합니다. (Expanded Range)

no acl <200-299> {permit deny} {any SRC_IPv6_Addr/Mask } {any DST_IPv6_Addr/Mask }	CONFIG	IPv6 Standard Access List를 초기화합니다.
no acl <300-399> {permit deny} {any SRC_IPv6_Addr/Mask } {any DST_IPv6_Addr/Mask }	CONFIG	IPv6 Extended Access List 를 초기화 합니다.
no acl <500-599> {permit deny} {sender_IP_Addr} [Wildcard]	CONFIG	ARP standard access list를 초기화합니다.
no acl acl_name {permit deny} {icmp ip tcp udp} SIP_Addr Wildcard DIP_Addr Wildcard_bits <0-63>	CONFIG	Name Access List를 초기화합니다.
no acl log interval	CONFIG	Access List 내역이 log에 기록되는 설정을 해제합니다.

2.6.4 QoS Class Map 설정

Packet의 조건을 설정하였다면, 조건에 맞는 Packet을 어떻게 처리하도록 할 것인지를 설정해야 합니다.

Class Map을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
class-map NAME	CONFIG	Class map을 생성합니다.
match cos <0-7>	CONFIG-CMAP	COS 값으로 Class-Map을 설정합니다.
match ip-dscp <0-63>	CONFIG-CMAP	DSCP 값으로 Class-Map을 설정합니다.
match ip-precedence <0-7>	CONFIG-CMAP	ip-precedence 값으로 Class-Map을 설정합니다.
match acl NAME	CONFIG-CMAP	acl으로 Class-Map을 설정합니다.
match vlan <1-4094>	CONFIG-CMAP	VLAN 값으로 Class-Map을 설정합니다.
match vlan-range <1-4094> to <1-4094>	CONFIG-CMAP	VLAN 범위를 이용하여 Class-Map을 설정합니다.

설정된 Class-Map을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show class-map	TOP	설정된 class-map 전체의 설정 내용을 확인합니다.
show class-map NAME	TOP	특정 class-map의 설정 내용을 확인합니다.

설정된 Class-Map을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no class-map NAME	CONFIG	Class map을 초기화합니다.
no match cos	CONFIG-CMAP	COS 값으로 Class-Map을 초기화합니다.

no match ip-dscp	CONFIG-CMAP	DSCP 값으로 Class-Map을 초기화합니다.
no match ip-precedence <0-7>	CONFIG-CMAP	ip-precedence 값으로 Class-Map을 초기화합니다.
no match acl <i>NAME</i>	CONFIG-CMAP	acl으로 Class-Map을 초기화합니다.
no match vlan	CONFIG-CMAP	VLAN 값으로 Class-Map을 초기화합니다.



참고

1. class-map으로 설정된 acl는 다른 class-map으로 지정될 수 없습니다.
2. cos, ip-dscp, ip-precedence, acl는 중복되어 설정될 수 없습니다.

2.6.5 QoS 정책 설정 및 적용

Interface 별로 8개의 Queue를 지원하며, Packet의 DSCP, CoS, ip-precedence 값에 따라 특정한 Queue로 Traffic을 전달하도록 Mapping 할 수 있습니다. 이러한 QoS Mapping을 설정한 후에는 Traffic 과부하 시의 Traffic 처리방법에 대해 설정할 수 있습니다

QoS 정책을 설정 및 적용하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
policy-map <i>NAME</i>	CONFIG	Policy map을 생성합니다.
class <i>NAME</i>	CONFIG-PMAP	생성된 Packet 조건(class-map)을 선택합니다.
police <1-1000000> <1-1000000> exceed-action drop	CONFIG-PMAP-C	평균 Traffic (kbps), Burst Traffic (kbps) 및 임계치 초과 Packet을 Drop 하도록 설정합니다.
set cos <0-7>	CONFIG-PMAP-C	CoS 값으로 정책을 설정합니다.
set ip-dscp <0-63>	CONFIG-PMAP-C	Packet의 TOS 영역의 DSCP값으로 정책을 설정합니다.
set ip-precedence <0-7>	CONFIG-PMAP-C	ip-precedence로 정책을 설정합니다.
service-policy input <i>NAME</i>	INTERFACE	INTERFACE에 생성된 Policy를 선택하여 적용한다.

설정된 policy-map을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show policy-map	TOP	설정된 policy-map 전체의 설정 내용을 확인합니다.
show policy-map <i>NAME</i>	TOP	특정 policy-map의 설정 내용 및 QoS에 적용된 Packet의 Count 값을 확인합니다.
show running-config interface <i>IFNAME</i>	TOP	Interface에 설정된 QoS 설정 내용을 확인합니다.

적용된 QoS 정책을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no service-policy input <i>NAME</i>	INTERFACE	Interface에 적용된 Policy를 초기화합니다.
no police <1-1000000> <1-1000000> exceed-action drop	CONFIG-PMAP-C	평균 Traffic (kbps), Burst Traffic (kbps) 및 임계치 초과 Packet에 대한 정책을 초기화합니다.
no set cos	CONFIG-PMAP-C	CoS 값 정책을 초기화합니다.
no set ip-dscp	CONFIG-PMAP-C	Packet의 TOS 영역의 DSCP값 정책을 초기화합니다.
no set ip-precedence	CONFIG-PMAP-C	ip-precedence 정책을 초기화합니다.
no class <i>NAME</i>	CONFIG-PMAP	Packet 조건(class-map)을 초기화합니다.
no policy-map <i>NAME</i>	CONFIG	Policy map을 초기화합니다.



참고

1. policy-map이 Interface에 적용된 후에는 policy-map을 수정할 수 없습니다.
2. policy-map을 수정하기 위해서는 Interface에 지정된 QoS 설정 내용을 먼저 초기화하시기 바랍니다.

2.6.6 QoS 스케줄링 설정

QoS 스케줄링은 WRR, SPQ, DRR, RR등을 지원하며, Default 상태는 Round Robin에 QoS 동작은 Off 상태입니다. 이러한 QoS 스케줄링을 설정한 후에는 Traffic 과부하 시에 QoS 정책의 CoS, DSCP 값 등을 이용한 우선 순위 정책을 설정할 수 있습니다.

QoS 스케줄링을 설정 및 적용하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
queue sched drr <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>	CONFIG	DRR COSQ 0~7 의 값을 통해 QoS를 설정합니다.
queue sched rr	CONFIG	Round Robin 형태로 QoS를 설정합니다.
queue sched wrr <0-15> <0-15> <0-15> <0-15> <0-15> <0-15> <0-15>	CONFIG	WRR COSQ 0~7 의 값을 통해 QoS를 설정합니다.
queue sched spq	CONFIG	SPQ 의 값을 통해 QoS를 설정합니다.
mls qos enable	CONFIG	QoS Service를 실행합니다. (default)

설정된 qos 스케줄을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mls qos	TOP	QoS 동작 상태를 확인합니다.
show running-config include queue	TOP	적용된 QoS 스케줄 정책을 확인합니다.
show mls qos interface IFNAME	TOP	Interface에 설정된 QoS 정책을 확인합니다.

qos 스케줄을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no queue sched-weight	TOP	QoS 스케줄을 초기화합니다.
no mls qos	TOP	QoS Service를 중지합니다.

<예제1> SPQ 스케줄을 이용한 QoS 설정

IP 192.168.10.1, 192.168.20.1에서 발생한 Traffic 중 IP 192.168.10.1이고 DSCP 46으로 Marking 된 Traffic을 최우선 순위 QoS 정책으로 적용하고자 할 때

```
SG2124G(config)#acl 100 permit ip host 192.168.10.1 any 46
SG2124G(config)#acl 101 permit ip host 192.168.20.1 any
SG2124G(config)#class-map c1
SG2124G(config-cmap)#match acl 100
SG2124G(config-cmap)#exit
SG2124G(config)#class-map c2
SG2124G(config-cmap)#match acl 101
SG2124G(config-cmap)#exit
SG2124G(config)#policy-map p1
SG2124G(config-pmap)#class c1
SG2124G(config-pmap-c)#set cos 7
SG2124G(config-pmap-c)#exit
SG2124G(config-pmap)#class c2
SG2124G(config-pmap-c)#set cos 1
SG2124G(config-pmap-c)#exit
SG2124G(config-pmap)#exit
SG2124G(config)#queue sched spq
SG2124G(config)#interface range ge1-2
% ge1-2 Selected
SG2124G(config-if-range)#service-policy input p1
SG2124G(config-if-range)#exit
SG2124G(config)#exit
SG2124G#show mls qos
    Enable
SG2124G#
SG2124G#show acl
```

```
Extended IP acl: 100
    permit ip host 192.168.10.1 any
```

```
Extended IP acl: 101
    permit ip host 192.168.20.1 any
```

```
SG2124G#
```

```
SG2124G#show mls qos interface ge1
```

```
INPUT-POLICY-MAP-NAME: p1
CLASS-MAP-NAME: c1
ACCESS-LIST-NAME: 100
Set CoS: 7
CLASS-MAP-NAME: c2
ACCESS-LIST-NAME: 101
Set CoS: 1
```

```
SG2124G#
```

```
SG2124G#show mls qos interface ge2
```

```
INPUT-POLICY-MAP-NAME: p1
CLASS-MAP-NAME: c1
ACCESS-LIST-NAME: 100
Set CoS: 7
CLASS-MAP-NAME: c2
ACCESS-LIST-NAME: 101
```

```
Set CoS: 1

SG2124G#
SG2124G#show policy-map

POLICY-MAP-NAME: p1
State: attached

CLASS-MAP-NAME: c1
ACCESS-LIST-NAME: 100
Set CoS: 7
  Port: ge1
    Count: 11206
  Port: ge2
    Count: 26796

CLASS-MAP-NAME: c2
ACCESS-LIST-NAME: 101
Set CoS: 1
  Port: ge1
    Count: 1512
  Port: ge2
    Count: 2452

SG2124G#
```

<예제2> WRR 스케줄을 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 Traffic에 대해 QoS 정책을 설정하여 4:3:2:1 비율로 Forwarding 할 때

```
SG2124G(config)#acl 100 permit ip host 192.168.10.1 any 46
SG2124G(config)#acl 101 permit ip host 192.168.20.1 any 40
SG2124G(config)#acl 102 permit ip host 192.168.30.1 any 26
SG2124G(config)#acl 103 permit ip host 192.168.40.1 any
SG2124G(config)#
SG2124G(config)#class-map c1
SG2124G(config-cmap)#match acl 100
SG2124G(config-cmap)#exit
SG2124G(config)#class-map c2
SG2124G(config-cmap)#match acl 101
SG2124G(config-cmap)#exit
SG2124G(config)#class-map c3
SG2124G(config-cmap)#match acl 102
SG2124G(config-cmap)#exit
SG2124G(config)#class-map c4
SG2124G(config-cmap)#match acl 103
SG2124G(config-cmap)#exit
SG2124G(config)#
SG2124G(config)#policy-map p1
SG2124G(config-pmap)#class c1
SG2124G(config-pmap-c)#set cos 4
SG2124G(config-pmap-c)#class c2
SG2124G(config-pmap-c)#set cos 3
SG2124G(config-pmap-c)#class c3
SG2124G(config-pmap-c)#set cos 2
SG2124G(config-pmap-c)#class c4
SG2124G(config-pmap-c)#set cos 1
SG2124G(config-pmap-c)#exit
SG2124G(config-pmap)#exit
SG2124G(config)#
SG2124G(config)#queue sched wrr 0 1 2 3 4 5 6 7
SG2124G(config)#interface range all
% all Selected
SG2124G(config-if-range)#service-policy input p1
SG2124G(config-if-range)#exit
SG2124G(config)#
```

2.6.7 Interface 별 속도 제한

Interface 별 Ingress와 Egress에 대하여 대역폭을 제한할 수 있는 기능입니다. 이 기능은 서비스 사업자가 제공 속도에 따른 다양한 서비스 상품을 제공할 수 있게 합니다. 속도 제한은 Interface의 Ingress와 Egress에 대해 1 Kbps 단위로 적용시킬 수 있습니다.

Interface 별 속도 제한 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
rate shaping in <64-1000000> <64-1000000> [enhanced]	INTERFACE	해당Interface의 Ingress에 대해 Limit와 Burst 값을 kbps 단위로 설정합니다.
rate shaping out <64-1000000> <64-1000000>	INTERFACE	해당Interface의 Egress에 대해 Limit와 Burst 값을 kbps 단위로 설정합니다.

Interface 별 속도 제한 기능을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show running-config interface [IFNAME]	INTERFACE	해당Interface의 Rate Shaping 설정 값을 확인합니다.

Interface 별 속도 제한 기능을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no rate shaping in	INTERFACE	해당Interface의 Ingress에 대해 Limit와 Burst 값을 초기화합니다.
no rate shaping out	INTERFACE	해당Interface의 Egress에 대해 Limit와 Burst 값을 초기화합니다.



참고

rate shaping과 storm-control은 하나의 Interface에 동시에 설정할 수 없습니다.

<예제> rate shaping 설정


```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge1
SG2124G(config-if)#rate shaping in 1000 2000
SG2124G(config-if)#rate shaping out 3000 4000
SG2124G(config-if)#end
SG2124G#
SG2124G#show running-config interface ge1
!
interface ge1
  rate shaping in 1000 2000
  rate shaping out 3000 4000
!
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge1
SG2124G(config-if)#no rate shaping in
SG2124G(config-if)#no rate shaping out
SG2124G(config-if)#end
SG2124G#
SG2124G#show running-config interface ge1
!
interface ge1
!
SG2124G#
```

2.7 IGMP

Multicast란 Packet을 받고자 하는 특정 Group에게만 Data를 송신하는 Packet 전송 방식입니다. Multicast Packet 전송을 도와주는 IGMP (Internet Group Management Protocol)는 Multicast Group을 인근의 Multicast Router들에게 알리는 수단을 제공하는 인터넷 Protocol입니다.

Multicast Router는 Multicast Data가 들어오면 해당 Multicast Data를 받고자 하는 Group이 등록되어 있는지를 확인하기 위하여 IGMP Query Message를 계속해서 전송합니다. 이때 Multicast Packet 수신을 요청하기 위하여 Join Message를 보내는 Switch가 있다면 해당 Switch를 Multicast Group으로 등록하고 Data를 전송합니다. 그리고 계속해서 해당 Multicast Packet을 수신하고자 하는 Switch가 해당 Multicast Group에 참가하기를 원하는지 또는 Group에서 빠져나가기 원하는지를 Message (IGMP query, join, leave) 전달을 통하여 확인합니다.

[표 2-10] Multicast Address Range

범 위	용 도	설 명
224.0.0.0 ~ 224.0.0.255	Reserved Link Local Address	Routing Protocol
224.0.1.0 ~ 238.255.255.255	Globally Scoped Addresses	Internet
232.0.0.0 ~ 232.255.255.255	Source Specific Multicast	SSM
233.0.0.0 ~ 233.255.255.255	GLOP Address	AS에 배정
239.0.0.0 ~ 239.255.255.255	Limited Scope Addresses	사설 IP Multicast

[표 2-11] Multicast Routing Protocol Address

구 분	용 도
224.0.0.1	Sunet의 모든 Multicast System
224.0.0.2	Subnet의 모든 Router
224.0.0.4	DVMRP Routers
224.0.0.5	OSPF Routers
224.0.0.6	OSPF DR, BDR Routers
224.0.0.9	RIPv2 Routers
224.0.0.10	EIGRP Routers
224.0.0.13	PIM Routers
224.0.0.18	VRRP
224.0.0.102	HSRP

2.7.1 IGMP Snooping

IGMP snooping은 Multicast Packet을 수신 받기 위해서 Multicast Group에 참가하기를 원하는 "Join Message"나 Multicast Packet 수신을 거부하기 위해 해당 Multicast Group에서 빠져 나오기를 원하는 "leave Message"를 보내는 Interface를 파악해 주는 기능을 수행합니다. 이렇게 해당 Multicast Group에 등록된 Interface로만 Multicast Packet을 전송하게 됩니다.

IGMP Snooping 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
ip igmp snooping	INTERFACE VLAN_ID	IGMP Snooping을 설정합니다.

IGMP Snooping 기능을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show ip igmp groups [IP_Addr [detail] VLAN_ID [[IP_Addr] detail] detail]	TOP	Multicast Group Membership 정보를 확인합니다.
show ip igmp interface [VLAN_ID]	TOP	Interface에 설정된 IGMP 내용을 확인합니다.
show ip igmp snooping mrouter VLAN_ID	TOP	IGMP Snooping Mrouter 정보를 확인합니다.

IGMP Snooping 기능을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no ip igmp snooping	INTERFACE VLAN_ID	IGMP Snooping을 초기화합니다.

<예제> igmp snooping 설정

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface vlan1.1
SG2124G(config-if)#ip igmp snooping
SG2124G(config-if)#end
SG2124G#
SG2124G#show ip igmp interface vlan1.1
Interface vlan1.1 (Index 3)
  Interface vlan1.1 (Index 3)
  IGMP Enabled, Active, Non-Querier, Version 2 (default)
  Internet address is 192.168.1.1
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP querying router is 0.0.0.0
  IGMP query interval is 125 seconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 260 seconds
  IGMP Snooping is enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface vlan1.1
SG2124G(config-if)#no ip igmp snooping
SG2124G(config-if)#end
SG2124G#
SG2124G#show ip igmp interface vlan1.1
Interface vlan1.1 (Index 3)
  IGMP Inactive, Version 2 (default)
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP query interval is 125 seconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 260 seconds
  IGMP Snooping is not enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
SG2124G#

```



참고

ip igmp snooping 명령어는 VLAN Interface에서만 설정이 가능합니다.

2.7.2 IGMP Snooping Fast-leave

Multicast Group에 속해 있는 Client가 Multicast Group에서 빠져 나가기 위해 leave Message를 내보내면 Multicast Router는 다시 한 번 IGMP Query Message를 보내고, 그에 대한 응답이 없을 경우에 해당 Host를 Multicast Group에서 삭제하기 때문에 어느 정도 시간이 소요됩니다.

IGMP Snooping Fast-leave는 Leave Message를 보낸 Client를 곧바로 Multicast Group에서 삭제하는 기능입니다.

IGMP Snooping Fast-leave 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
ip igmp snooping fast-leave	INTERFACE VLAN_ID	IGMP Snooping fast leave를 설정합니다.

IGMP Snooping Fast-leave 기능을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show ip igmp groups [IP_Addr [detail]] VLAN_ID [[IP_Addr] detail] detail	TOP	Multicast Group Membership 정보를 확인합니다.
show ip igmp interface [VLAN_ID]	TOP	Interface에 설정된 IGMP 내용을 확인합니다.
show ip igmp snooping mrouter VLAN_ID	TOP	IGMP Snooping Mrouter 정보를 확인합니다.

IGMP Snooping Fast-leave 기능을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no ip igmp snooping fast-leave	INTERFACE VLAN_ID	IGMP Snooping fast leave 설정을 삭제합니다.



참고

ip igmp snooping fast-leave 명령어는 VLAN Interface에서만 설정이 가능합니다.

<예제> IGMP Snooping, IGMP Snooping Fast-leave 설정 및 확인

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface vlan1.1
SG2124G(config-if)#ip igmp snooping
SG2124G(config-if)#ip igmp snooping fast-leave
SG2124G(config-if)#end
SG2124G#
SG2124G#show ip igmp interface vlan1.1
Interface vlan1.1 (Index 3)
  IGMP Enabled, Active, Non-Querier, Version 2 (default)
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP querying router is 0.0.0.0
  IGMP query interval is 125 seconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 260 seconds
  IGMP Snooping is enabled on this interface
  IGMP Snooping fast-leave is enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
SG2124G#
SG2124G#show ip igmp groups
IGMP Connected Group Membership
Group Address      Interface      Uptime    Expires    Last Reporter
225.10.10.1        fe9            00:01:47  00:02:40  10.100.100.123
225.10.10.2        fe9            00:01:47  00:02:36  10.100.100.123
225.10.10.3        fe9            00:01:45  00:02:36  10.100.100.123
225.10.10.4        fe9            00:01:45  00:02:39  10.100.100.123
225.10.10.5        fe9            00:01:45  00:02:39  10.100.100.123

--- 중 략 ---

225.10.10.6        fe2            00:01:47  00:02:41  10.100.100.123
225.10.10.7        fe2            00:01:47  00:02:38  10.100.100.123
225.10.10.8        fe2            00:01:47  00:02:41  10.100.100.123
225.10.10.9        fe2            00:01:47  00:02:38  10.100.100.123
225.10.10.10       fe2            00:01:47  00:02:39  10.100.100.123
Total Groups: 200
SG2124G#
SG2124G#show ip igmp groups detail

Interface:      ge9
Group:          225.10.10.1
Uptime:         00:02:14
Group mode:     Exclude (Expires: 00:03:51)
Last reporter:  10.100.100.123
Source list is empty

Interface:      ge9
Group:          225.10.10.2
Uptime:         00:02:14
Group mode:     Exclude (Expires: 00:03:51)
Last reporter:  10.100.100.123

```

```
Source list is empty

Interface:      ge9
Group:          225.10.10.3
Uptime:         00:02:14
Group mode:     Exclude (Expires: 00:03:53)
Last reporter:  10.100.100.123
Source list is empty
```

```
Interface:      ge9
Group:          225.10.10.4
Uptime:         00:02:14
Group mode:     Exclude (Expires: 00:03:53)
Last reporter:  10.100.100.123
Source list is empty
```

```
-- 이하 생략 --
SG2124G#
```

2.7.3 IGMP Filter

IGMP Filter는 Multicast Group 중 Interface로부터 특정 IGMP Membership Report들을 Filter하는 용도로 사용되며, VLAN Interface에 적용하여 구현할 수 있습니다.

IGMP Filter를 설정하는 방법은 먼저 Filter하기 원하는 Multicast Group에 대한 Address를 범위로 설정하는 Access List을 생성하고, 그 후에 이를 VLAN Interface에 적용하면 됩니다.

IGMP Filter가 설정된 Multicast Group에 대해서는 Join / Leave Message를 수신하지 않으며, Expires Time 경과 후 Multicast Group에서 자동으로 삭제되게 됩니다.

IGMP Filter 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
access-list {<1-99> <1300-1999>} {deny permit} {IP_Addr [Wildcards] any host IP_Addr}	CONFIG	IGMP Filter를 설정할 Access List를 생성합니다.
ip igmp access-group {<1-99> <1300-1999>}	INTERFACE VLAN_ID	VLAN Interface에 IGMP Filter를 설정합니다.

IGMP Filter 기능을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show access-list	TOP	설정된 Access List를 확인합니다.
show ip igmp groups [IP_Addr [detail] VLAN_ID [[IP_Addr] detail] detail]	TOP	Multicast Group Membership 정보를 확인합니다.
show ip igmp interface [VLAN_ID]	TOP	Interface에 설정된 IGMP 내용을 확인합니다.
show ip igmp snooping mrouter VLAN_ID	TOP	IGMP Snooping Mrouter 정보를 확인합니다.

IGMP Filter 기능을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no ip igmp access-group {<1-99> <1300-1999>}	INTERFACE VLAN_ID	VLAN Interface에 설정된 IGMP Filter를 삭제합니다.
no access-list {<1-99> <1300-1999>} {deny permit} {IP_Addr [Wildcards] any host IP_Addr}	CONFIG	Access List를 삭제합니다.



참 고

ip igmp filter 명령어는 VLAN Interface에서만 설정이 가능합니다

<예제> IGMP Filter 설정 및 확인

```
SG2124G#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface      Uptime    Expires    Last Reporter
225.10.10.1      fe9            00:01:47  00:02:40  10.100.100.123
225.10.10.2      fe9            00:01:47  00:02:36  10.100.100.123
225.10.10.3      fe9            00:01:45  00:02:36  10.100.100.123
225.10.10.4      fe9            00:01:45  00:02:39  10.100.100.123
225.10.10.5      fe9            00:01:45  00:02:39  10.100.100.123
225.10.10.6      fe9            00:01:47  00:02:40  10.100.100.123
225.10.10.7      fe9            00:01:47  00:02:36  10.100.100.123
225.10.10.8      fe9            00:01:45  00:02:36  10.100.100.123
225.10.10.9      fe9            00:01:45  00:02:39  10.100.100.123
225.10.10.10     fe9            00:01:45  00:02:39  10.100.100.123
Total Groups: 10
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#access-list 10 deny 225.10.10.1
SG2124G(config)#access-list 10 deny 225.10.10.2
SG2124G(config)#
SG2124G(config)#interface vlan1.1
SG2124G(config-if)#ip igmp access-group 10
SG2124G(config-if)#end
SG2124G#
SG2124G#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface      Uptime    Expires    Last Reporter
225.10.10.1      fe9            00:08:47  00:00:37  10.100.100.123
225.10.10.2      fe9            00:08:47  00:00:33  10.100.100.123
225.10.10.3      fe9            00:08:45  00:03:33  10.100.100.123
225.10.10.4      fe9            00:08:45  00:03:36  10.100.100.123
225.10.10.5      fe9            00:08:45  00:03:36  10.100.100.123
225.10.10.6      fe9            00:08:47  00:03:37  10.100.100.123
225.10.10.7      fe9            00:08:47  00:03:33  10.100.100.123
225.10.10.8      fe9            00:08:45  00:03:33  10.100.100.123
225.10.10.9      fe9            00:08:45  00:03:36  10.100.100.123
225.10.10.10     fe9            00:08:45  00:03:36  10.100.100.123
Total Groups: 10
SG2124G#
SG2124G#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface      Uptime    Expires    Last Reporter
225.10.10.3      fe9            00:09:35  00:03:23  10.100.100.123
```

```
225.10.10.4      fe9          00:09:35 00:03:26 10.100.100.123
225.10.10.5      fe9          00:09:35 00:03:26 10.100.100.123
225.10.10.6      fe9          00:09:37 00:03:27 10.100.100.123
225.10.10.7      fe9          00:09:37 00:03:23 10.100.100.123
225.10.10.8      fe9          00:09:35 00:03:23 10.100.100.123
225.10.10.9      fe9          00:09:35 00:03:26 10.100.100.123
225.10.10.10     fe9          00:09:35 00:03:26 10.100.100.123
Total Groups: 10
SG2124G#
```

2.8 MLD

MLD(Multicast Listener Discovery)란 IPv6에서 Multicast 라우터가 Multicast 호스트들을 관리하는 프로토콜로서, IPv4에서 IGMP와 동일한 기능을 수행합니다. MLDv1과 MLDv2가 있으며 이들은 각각 IGMPv2와 IGMPv3에 상응하는 기능을 수행합니다. IGMP에서는 Multicast 라우터와 Multicast 호스트간 주고 받는 control 메시지는 IP 프로토콜 넘버 2인 IGMP 메시지를 사용했지만, MLD에서는 ICMPv6 메시지 통합되었습니다.

IPv6 Multicast Router는 Multicast Data가 들어오면 해당 Multicast Data를 받고자 하는 IPv6 Multicast Group이 등록되어 있는지를 확인하기 위하여 MLD Query Message를 주기적으로 전송합니다. 이때 Multicast Packet 수신을 요청하기 위하여 MLD Join Message를 보내는 호스트 혹은 Switch가 있다면 해당 호스트 혹은 Switch를 IPv6 Multicast Group으로 등록하고 Multicast Data를 전송합니다. 그리고 계속해서 해당 Multicast Packet을 수신하고자 하는 호스트 혹은 Switch가 해당 Multicast Group에 참가하기를 원하는지 또는 Group에서 빠져나가기 원하는지를 Message MLD query, join, leave) 전달을 통하여 확인합니다.

2.8.1 MLD Snooping

MLD snooping은 IPv6 Multicast Packet을 수신 받기 위해서 IPv6 Multicast Group에 참가하기를 원하는 "Join Message"나 IPv6 Multicast Packet 수신을 거부하기 위해 해당 IPv6 Multicast Group에서 빠져 나오기를 원하는 "leave Message"를 보내는 Interface를 파악해주는 기능을 수행합니다. 이렇게 해당 IPv6 Multicast Group에 등록된 Interface로만 Multicast Packet을 전송하게 됩니다.

MLD Snooping 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
ipv6 mld snooping fast-leave	INTERFACE VLAN_ID	MLD Snooping fast leave를 설정합니다.

MLD Snooping Fast-leave 기능을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show ipv6 mld groups [IP_Addr [detail]] VLAN_ID [[IP_Addr] detail] detail	TOP	IPv6 Multicast Group Membership 정보를 확인합니다.

show ipv6 mld interface [VLAN_ID]	TOP	Interface에 설정된 MLD 내용을 확인합니다.
show ipv6 mld snooping mrouter VLAN_ID	TOP	MLD Snooping Mrouter 정보를 확인합니다.

MLD Snooping Fast-leave 기능을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no ipv6 mld snooping fast-leave	INTERFACE VLAN_ID	MLD Snooping fast leave 설정을 삭제합니다.



참고

1. IPv6 MLD Snooping fast-leave 명령어는 VLAN Interface에서만 설정이 가능합니다.
2. SG2024, SG2024P, SG2200 Series 제품은 MLD Snooping 기능을 지원하지 않습니다.
3. MLD Snooping 기능은 Switch버전 2.x 이상에서만 지원합니다.

<예제> MLD Snooping, MLD Snooping Fast-leave 설정 및 확인

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface vlan1.1
SG2124G(config-if)#ipv6 mld snooping
SG2124G(config-if)#ipv6 mld snooping fast-leave
SG2124G(config-if)#end
SG2124G#
SG2124G#show ipv6 mld interface vlan1.1
Interface vlan1.1 (Index 4)
  MLD Enabled, Active, Non-Querier, Version 2 (default)
  Internet address is fe80::21a:f4ff:fe1c:3d9
  MLD interface has 0 group-record states
  MLD activity: 0 joins, 0 leaves
  MLD querying router is ::
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
  MLD max query response time is 10 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 260 seconds
  MLD Snooping is globally enabled
  MLD Snooping is enabled on this interface
  MLD Snooping fast-leave is enabled
  MLD Snooping querier is not enabled
  MLD Snooping report suppression is enabled
SG2124G#
```

```

SG2124G#show ipv6 mld groups
MLD Connected Group Membership
Group Address                               Interface      Uptime    Expires    Last
Reporter
ff05::e108:d001                             ge21           00:00:08  00:04:12
fe80::200:65ff:fe02:102
ff05::e108:d006                             ge21           00:00:04  00:04:15
fe80::200:65ff:fe02:102
ff05::e108:d101                             ge21           00:00:08  00:04:12
fe80::200:65ff:fe02:102
ff05::e108:d106                             ge21           00:00:04  00:04:15
fe80::200:65ff:fe02:102
ff05::e108:d201                             ge21           00:00:08  00:04:12
fe80::200:65ff:fe02:102
ff05::e108:d206                             ge21           00:00:04  00:04:15
fe80::200:65ff:fe02:102
ff05::e108:d301                             ge21           00:00:08  00:04:12
fe80::200:65ff:fe02:102
ff05::e108:d306                             ge21           00:00:04  00:04:15
fe80::200:65ff:fe02:102
ff05::e108:d401                             ge21           00:00:08  00:04:12
fe80::200:65ff:fe02:102
ff05::e108:d406                             ge21           00:00:04  00:04:15
fe80::200:65ff:fe02:102
Total Groups: 10
SG2124G#
SG2124G#show ipv6 mld groups detail

Interface:      ge21
Group:          ff05::e108:d001
Uptime:         00:00:20
Group mode:     Exclude ( (Expires: 00:04:10))
Last reporter:  fe80::200:65ff:fe02:102
Source list is empty

Interface:      ge21
Group:          ff05::e108:d006
Uptime:         00:00:16
Group mode:     Exclude ( (Expires: 00:04:13))
Last reporter:  fe80::200:65ff:fe02:102
Source list is empty

Interface:      ge21
Group:          ff05::e108:d101
Uptime:         00:00:20
Group mode:     Exclude ( (Expires: 00:04:10))
Last reporter:  fe80::200:65ff:fe02:102
Source list is empty

Interface:      ge21
Group:          ff05::e108:d106
Uptime:         00:00:16
Group mode:     Exclude ( (Expires: 00:04:13))
Last reporter:  fe80::200:65ff:fe02:102
Source list is empty

-- 이하 생략 --

```

2.8.2 MLD Filter

MLD Filter는 IPv6 Multicast Group 중 Interface로부터 특정 MLD Membership Report들을 Filter하는 용도로 사용되며, VLAN Interface에 적용하여 구현할 수 있습니다.

MLD Filter를 설정하는 방법은 먼저 Filter하기 원하는 IPv6 Multicast Group에 대한 Address를 범위로 설정하는 Access List을 생성하고, 그후에 이를 VLAN Interface에 적용하면 됩니다.

MLD Filter가 설정된 IPv6 Multicast Group에 대해서는 Join / Leave Message를 수신하지 않으며, Expires Time 경과 후 Multicast Group에서 자동으로 삭제되게 됩니다.

MLD Filter 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
ipv6 access-list <i>WORD</i> {deny permit} { <i>X:X::X:X/M</i> any}	CONFIG	MLD Filter를 설정할 IPv6 Access List를 생성합니다.
ipv6 mld access-group <i>WORD</i>	INTERFACE VLAN_ID	VLAN Interface에 MLD Filter를 설정합니다.

MLD Filter 기능을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show ipv6 access-list	TOP	설정된 IPv6 Access List를 인합니다.
show ipv6 mld groups [<i>IP_Addr</i> [detail] <i>VLAN_ID</i> [[<i>IP_Addr</i>] detail] detail]	TOP	IPv6 Multicast Group Membership 정보를 확인합니다.
show ipv6 mld interface [<i>VLAN_ID</i>]	TOP	Interface에 설정된 MLD 내용을 확인합니다.
show ipv6 mld snooping mrouter <i>VLAN_ID</i>	TOP	MLD Snooping Mrouter 정보를 확인합니다.

MLD Snooping Fast-leave 기능을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no ipv6 mld access-group	INTERFACE VLAN_ID	VLAN Interface에 설정된 MLD Filter를 삭제합니다.
no ipv6 access-list <i>WORD</i> {deny permit} { <i>X:X::X:X/M</i> any}	CONFIG	IPv6 Access List를 삭제합니다.



참고

1. IPv6 MLD Filter 명령어는 VLAN Interface에서만 설정이 가능합니다.
2. SG2024, SG2024P, SG2200 Series 제품은 MLD Snooping 기능을 지원하지 않습니다.
3. MLD Snooping 기능은 Switch버전 2.x 이상에서만 지원합니다.

<예제> MLD Filter 설정 및 확인

```
SG2124G#show ipv6 mld groups
MLD Connected Group Membership
Group Address                                Interface      Uptime    Expires    Last
Reporter
ff05::e108:d001                             ge21          00:05:05  00:03:54
fe80::200:65ff:fe02:102
ff05::e108:d006                             ge21          00:05:01  00:03:47
fe80::200:65ff:fe02:102
ff05::e108:d101                             ge21          00:05:05  00:03:49
fe80::200:65ff:fe02:102
ff05::e108:d106                             ge21          00:05:01  00:03:50
fe80::200:65ff:fe02:102
ff05::e108:d201                             ge21          00:05:05  00:04:16
fe80::200:65ff:fe02:102
ff05::e108:d206                             ge21          00:05:01  00:03:52
fe80::200:65ff:fe02:102
ff05::e108:d301                             ge21          00:05:05  00:03:47
fe80::200:65ff:fe02:102
ff05::e108:d306                             ge21          00:05:01  00:04:16
fe80::200:65ff:fe02:102
ff05::e108:d401                             ge21          00:05:05  00:03:53
fe80::200:65ff:fe02:102
ff05::e108:d406                             ge21          00:05:01  00:04:17
fe80::200:65ff:fe02:102
Total Groups: 10
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#ipv6 access-list mld deny ff05::e108:d001/128
SG2124G(config)#
SG2124G(config)#interface vlan1.1
SG2124G(config-if)#ipv6 mld access-group mld
SG2124G(config-if)#end
SG2124G#
SG2124G#show ipv6 mld groups
MLD Connected Group Membership
Group Address                                Interface      Uptime    Expires    Last
Reporter
ff05::e108:d006                             ge21          00:00:02  00:04:17
fe80::200:65ff:fe02:102
ff05::e108:d101                             ge21          00:00:02  00:04:17
fe80::200:65ff:fe02:102
```

ff05::e108:d106	ge21	00:00:02 00:04:17
fe80::200:65ff:fe02:102		
ff05::e108:d201	ge21	00:00:02 00:04:17
fe80::200:65ff:fe02:102		
ff05::e108:d206	ge21	00:00:02 00:04:17
fe80::200:65ff:fe02:102		
ff05::e108:d301	ge21	00:00:02 00:04:17
fe80::200:65ff:fe02:102		
ff05::e108:d306	ge21	00:00:02 00:04:17
fe80::200:65ff:fe02:102		
ff05::e108:d401	ge21	00:00:02 00:04:17
fe80::200:65ff:fe02:102		
ff05::e108:d406	ge21	00:00:02 00:04:17
fe80::200:65ff:fe02:102		
Total Groups: 9		
SG2124G#		

2.9 사용자 인증

2.9.1 사용자 인증 Interface 설정 (802.1x)

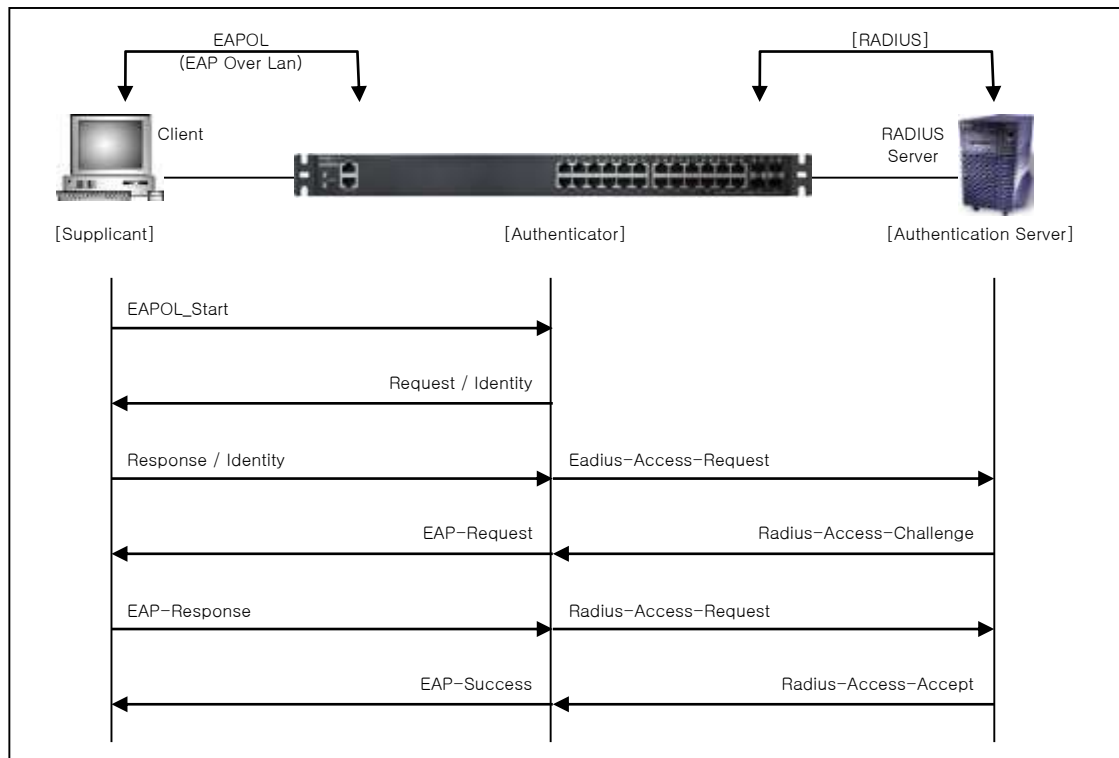
Switch는 IEEE 802.1x를 기반으로 한 사용자 인증 정책을 Interface 별로 설정할 수 있습니다. 802.1x를 설정한 사용자 인증 Interface는 RADIUS Server를 통해 접속 권한 여부를 판단하여 권한을 가지고 있는 접속자만 사용이 가능하기 때문에 Network 관리의 보안과 이동을 높일 수 있습니다.

사용자의 정보를 제한하는 방식에는 MAC Address를 이용한 인증 방식과 Interface를 기반으로 한 802.1x 인증 방식이 있습니다. 이 중에서 802.1x 인증 방식은 접속을 시도하는 사용자의 정보를 가지고 RADIUS Server에서 접속 권한부여를 결정하는 것으로 EAP (Extensible Authentication Protocol) 구조를 채택하고 있습니다. EAP 방식에는 EAP-MD5(Message Digest 5), EAP-TLS (Transport Level Security), EAP-SRP (Secure Remote Password), EAP-TTLS (Tunneled TLS) 등이 있습니다.

Switch는 사용자의 ID와 Password를 이용하여 단방향으로 이루어지는 Password 기반 Network 인증 방식을 통하여 접속하는 EAP-MD5 방식을 지원합니다.

사용자 (Supplicant)가 접속 인증을 요청하면 사용자 (Supplicant)의 PC에서 EAPOL-Start Type의 Packet이 Switch (Authenticator)에 전송되고, Switch (Authenticator)는 다시 사용자에게 신원을 요청합니다. 신원에 대한 응답을 받은 후에는 RADIUS Server에 접속 승인을 요청하고, 사용자의 정보를 통해 접속 권한이 확인되면 인증을 받습니다.

이 때, 사용자 (Supplicant)와 Switch (Authenticator)는 PAE (Port Authentication Entities)에 해당합니다. Switch (Authenticator)는 단지 인증을 위한 브리지 역할을 할 뿐, 사용자에게 어떠한 정보도 가지고 있지 않습니다. 인증에 필요한 사용자 정보의 Database는 RADIUS Server가 가지고 있습니다.

[그림 2-6] 802.1x 사용자 인증 과정

■ Client (Supplicant)

Switch는 LAN에 접근하는 Client (Supplicant)의 요청에 대한 응답을 해줍니다. Client는 반드시 802.1x 표준에서 정의한 Client 소프트웨어를 실행해야 합니다.

■ 인증 Server (RADIUS)

인증 Server는 Client로부터 ID, Password 정보를 받아서 Client에 대한 인증을 하며 인증 결과를 RADIUS (RFC 2865) Protocol에 의해 Switch에 알려 줍니다.

■ Switch (Authenticator)

Switch는 Client로부터 인증 정보를 받아서 인증 Server로 전달해 주는 중개자 역할을 하며 인증 Server로부터 인증에 대한 결과 정보를 받아서 이것을 Client에게 전달하는데 인증 결과에 따라서 Client의 접근을 물리적으로 제어합니다. (Client는 EAPOL Protocol, 인증 Server와는 RADIUS Protocol을 이용하여 통신)

■ 802.1x의 동작 절차는 다음과 같습니다.

1. Client는 부팅 시 EAPOL-Start Message를 자신의 Interface로 전송합니다.
2. Switch는 EAPOL-Start Message를 수신하면 Client에게 ID 요구하는 Message를 전송합니다.
3. Client는 ID 요구하는 Message를 수신하면 Switch에게 Client ID 정보를 포함한 Message를 전송합니다.
4. Switch는 Client ID 정보를 포함한 Message를 RADIUS Protocol에 맞게 변환하여 RADIUS Server로 전송합니다.
5. RADIUS Server는 Message에 포함되어 있는 ID가 자신의 Database와 비교하여 존재하는 ID일 경우 Switch에 RADIUS Access-Challenge Message를 전송합니다.
6. RADIUS Access-Challenge Message를 수신한 Switch는 MD-5 Password를 요구하는 Message를 Client에게 보냅니다.
7. Client는 Password 정보를 담은 EAPOL Message를 Switch로 전송합니다.
8. Switch는 Client로부터 수신한 EAPOL Message를 RADIUS Protocol Packet으로 변환하여 인증 Server로 전송합니다.
9. 인증 Server는 Message의 내용을 이용해 인증을 실행하고 성공할 경우 Switch로 RADIUS Access-Accept로 Message를 전송합니다.
10. Switch는 RADIUS Access-Accept Message를 수신하면 Client에게 EAP-Success Message를 전송하면서 Client가 연결되어 있는 Interface에 대해 Port Authorized 상태로 설정합니다.
11. Client는 EAP Success Message를 받으면 인증이 성공하였음을 인지합니다. Client에서 통신을 중단할 때에는 EAPOL Logoff Message를 Switch에 보냅니다.

802.1x 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
aaa system-aaa-ctrl	CONFIG	aaa 인증을 활성화합니다.
dot1x system-auth-ctrl	CONFIG	802.1x 인증을 활성화합니다.
mac-based-dynamic-vlan	CONFIG	MAC Based Dynamic VLAN 기능을 활성화합니다.
vlan-notification vlanid	CONFIG	VLAN Notification 기능을 활성화 합니다. (Default: VLAN Name)
dot1x port-control {auto force-authorized force-unauthorized}	INTERFACE	Interface를 인증 모드로 설정합니다.
dot1x max-req <1-10>	INTERFACE	최대 재전송 회수를 설정합니다. (Default: 2회)
dot1x quiet-period <1-65535>	INTERFACE	인증 실패 시 인증 재시도 주기를 설정합니다. (Default: 60 s)
dot1x reauthMax <1-10>	INTERFACE	인증 상태를 갱신할 수 있도록 재인증 회수를 설정합니다. (Default: 2회)
dot1x reauthentication	INTERFACE	인증 상태를 갱신할 수 있도록 Interface에 재인증 절차를 활성화합니다.
dot1x timeout {re-authperiod <1-4294967295> server-timeout <1-65535> supp-timeout <1-65535> tx-period <1-65535>}	INTERFACE	Timeout 주기를 설정합니다.
dot1x attribute framed-mtu <64-9208>	INTERFACE	RADIUS Server로 전송하는 Framed-MTU Attribute 값을 변경합니다. (Default: 1000)

802.1x 기능을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show dot1x [all brief]	TOP	802.1x 설정 내용 및 인증 결과를 확인합니다.
show dot1x interface <i>IFNAME</i>	TOP	Interface 관련 802.1x 설정을 확인함

		니다.
show dot1x statistics interface <i>IFNAME</i>	TOP	802.1x에 대한 통계를 확인합니다.

802.1x 기능을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no dot1x max-req	INTERFACE	최대 재전송 회수를 초기화합니다.
no dot1x quiet-period	INTERFACE	인증 재시도 주기를 초기화합니다.
no dot1x reauthMax	INTERFACE	재인증 회수를 초기화합니다.
no dot1x reauthentication	INTERFACE	재인증 절차를 비활성화합니다.
no dot1x timeout {re-authperiod server-timeout supp-timeout tx-period}	INTERFACE	Timeout 주기를 초기화합니다.
no dot1x port-control	INTERFACE	인증 모드로 설정된 해당 Interface를 초기화합니다.
no dot1x system-auth-ctrl	CONFIG	802.1x 인증을 비활성화합니다.
no aaa system-aaa-ctrl	CONFIG	aaa 인증을 비활성화합니다.
no mac-based-dynamic-vlan	CONFIG	MAC Based Dynamic VLAN 기능을 비활성화합니다.
no vlan-notification	CONFIG	VLAN Notification 기능을 비활성화합니다.



참고

1. dot1x port-control

- AUTO
 - : RADIUS Server 인증을 통해 Network에 접근 가능/불허
- FORCE_AUTHORIZED/FORCE_UNAUTHORIZED
 - : RADIUS Server의 인증절차를 생략하고 Network에 접근 허락/불허
- 기본적으로 FORCE_AUTHORIZED 모드로 설정됩니다.

2. dot1x timeout

- re-authperiod
 - : Radius-Access-Request. 재인증 주기 설정 (Default: 3 600 s)
- server-timeout
 - : Radius-Access-Request. 인증 Server의 response 주기 설정 (Default: 30 s)

-
- supp-timeout
: EAP_Request / Identify. Supplicant (Client)의 response 주기 설정 (Default: 30 s)
 - tx-period
: EAP_Request / Identify. 재전송 주기 설정 (Default: 30 s)
-

<예제1> 802.1x 기본 설정

- RADIUS Server의 IP : 192.168.100.110

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#dot1x system-auth-ctrl
SG2124G(config)#radius-server host 192.168.100.110 key *****
SG2124G(config)#interface ge1
SG2124G(config-if)#dot1x port-control auto
SG2124G(config-if)#exit
SG2124G(config)#interface vlan1.1
SG2124G(config-if)#ip address 192.168.100.118/24
SG2124G(config-if)#end
SG2124G#
```

<예제2> 802.1x 연동 설정

- RADIUS 및 TACACS+ Server의 IP : 192.168.254.30
- ge1-22를 사용자 인증 Interface로 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#aaa system-aaa-ctrl
SG2124G(config)#radius-server host 192.168.254.30 auth-port 1812 timeout 5 retransmit 3 key *****
SG2124G(config)#tacacs-server host 192.168.254.30 auth-port 1812 timeout 5 retransmit 3 key *****
SG2124G(config)#dot1x system-auth-ctrl
SG2124G(config)#interface range ge1-22
% ge1-22 Selected
SG2124G(config-if-range)#dot1x port-control auto
% ge1-22 Selected
SG2124G(config-if-range)#end
SG2124G#show dot1x all
802.1X Port-Based Authentication Enabled
  RADIUS server address: 192.168.254.30:1812
  Next radius message id: 0
  RADIUS client address: not configured
802.1X info for interface ge24
  portEnabled: false - portControl: Auto
  portStatus: Unauthorized - currentId: 1
  reAuthenticate: disabled
  reAuthPeriod: 3600
abort:F fail:F start:F timeout:F success:F
PAE: state: Connected - portMode: Auto
```

```
PAE: reAuthCount: 0 - rxRespld: 0
PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
BE: state: Idle - reqCount: 0 - idFromServer: 0
BE: suppTimeout: 30 - serverTimeout: 30 - maxReq: 2
CD: adminControlledDirections: in - operControlledDirections: both
CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false
802.1X info for interface ge8
portEnabled: false - portControl: Auto
portStatus: Unauthorized - currentId: 1
reAuthenticate: disabled
reAuthPeriod: 3600
abort:F fail:F start:F timeout:F success:F
PAE: state: Connected - portMode: Auto
PAE: reAuthCount: 0 - rxRespld: 0
PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
BE: state: Idle - reqCount: 0 - idFromServer: 0
BE: suppTimeout: 30 - serverTimeout: 30 - maxReq: 2
CD: adminControlledDirections: in - operControlledDirections: both
CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false
802.1X info for interface ge17
portEnabled: false - portControl: Auto
portStatus: Unauthorized - currentId: 1
reAuthenticate: disabled
reAuthPeriod: 3600
abort:F fail:F start:F timeout:F success:F
PAE: state: Connected - portMode: Auto
PAE: reAuthCount: 0 - rxRespld: 0
PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
BE: state: Idle - reqCount: 0 - idFromServer: 0
BE: suppTimeout: 30 - serverTimeout: 30 - maxReq: 2
CD: adminControlledDirections: in - operControlledDirections: both
CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false
-- 이하 생략 --
```

2.9.2 시스템 사용자 인증 (RADIUS / TACACS+)

SG Switch Series는 사용자 인증 Protocol로 RADIUS (Remote Authentication Dial-In User Service)와 TACACS+ (Terminal Access Controller Access Control System+)를 지원합니다. Switch에 등록되어 있는 사용자 ID와 Password 이외에도 RADIUS Server와 TACACS+ Server를 통하여 인증을 받아야 하기 때문에 시스템 관리 및 Network 관리의 보안을 강화할 수 있습니다.

여러 대의 Server를 등록한 경우 등록된 순서에 따라 첫 번째 Server에 인증 요청을 시도하였으나 응답이 없는 경우 두 번째 지정된 Server에 인증을 요청하게 되며 응답을 한 Server는 응답한 때부터 Default Server로 동작합니다.

RADIUS Server 등록 시 추가 명령인 `mode aaa` or `mode dot1x` 를 사용하면 AAA 인증과 Dot1x-User 인증용 Server를 분리하여 등록할 수 있습니다.

Authenticator (Switch)와 RADIUS Server는 서로의 IP Address를 등록하는 것 외에도 서로를 인증해 줄 별도의 Key 값이 있어야 하며, Key 값은 서로 동일해야 합니다.

RADIUS 또는 TACACS 서버를 등록하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
<code>radius-server host IP_Addr</code> <code>[auth-port PORT_NO eap-method WORD key WORD</code> <code> retransmit <1-100> </code> <code>timeout <1-1000>] mode</code> <code>[aaa dot1x]</code>	CONFIG	RADIUS Server를 등록합니다. (Default: auth-port 1812, retransmit 3회, timeout 5 s) Mode를 설정하지 않은 경우 AAA, Dot1x-User 동시 사용
<code>tacacs-server host IP_Addr</code> <code>[auth-port PORT_NO key</code> <code>WORD retransmit <1-100></code> <code> timeout <1-1000>]</code>	CONFIG	TACACS+ Server를 등록합니다. (Default: auth-port 1812, retransmit 3회, timeout 5 s)

802.1x 기능을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
<code>show dot1x [all brief]</code>	TOP	802.1x 설정 내용 및 인증 결과를 확인합니다.

RADIUS 또는 TACACS Server를 제거하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no radius-server host <i>IP_Addr</i> [auth-port <i>PORT_NO</i>]	CONFIG	RADIUS Server를 제거합니다. (Default: auth-port 1812)
no tacacs-server host <i>IP_Addr</i> [auth-port <i>PORT_NO</i>]	CONFIG	TACACS+ Server를 제거합니다. (Default: auth-port 1812)



참고

1. RADIUS-Server 및 TACACS-Server는 최대 5개까지 설정 가능합니다.
2. 보안성 향상을 위해 SNMP USER 설정 시 인증 및 암호화 비밀번호는 9자 이상으로 영대문자, 영소문자, 숫자, 특수문자를 최소 1자 이상씩 혼합하여 설정하여야 합니다

<예제1> AAA 인증 및 Dot1x-User 인증 Server 분리 설정

- AAA인증용 RADIUS Server IP: 192.168.100.110
- Dot1x-User 인증용 RADIUS Server IP: 192.168.100.220

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#radius-server host 192.168.100.110 key ***** mode aaa
SG2124G(config)#radius-server host 192.168.100.220 key ***** mode dot1x
```

<예제2> 시스템 관리자 RADIUS 인증 설정

- RADIUS Server IP : 192.168.100.110

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#aaa system-aaa-ctrl
SG2124G(config)#radius-server host 192.168.100.110 key *****
SG2124G(config)#ip radius source-interface 192.168.100.118 1023
SG2124G(config)#aaa group server radius test server 192.168.100.110
SG2124G(config)#aaa authentication login default radius test
SG2124G(config)#interface vlan1.1
SG2124G(config-if)#ip address 192.168.100.118/24
SG2124G(config-if)#exit
SG2124G(config)#line vty 0 5
SG2124G(config-line)#login authentication default
SG2124G(config-line)#end
SG2124G#
```

2.9.3 802.1x Extended Authentication

SG Switch Series는 IEEE 802.1x 표준을 준수한 인증 외에도 사용자 기반(Multi User)의 인증 방식, MAC Address 기반의 인증, Guest-VLAN 기반의 인증, Web-based 인증 및 dot1x가 비활성화된 상태에서도 EAPOL Frame 을 drop 하지 않고 switching 할 수 있는 기능을 지원합니다.

■ 사용자 기반(Multi User)의 인증

기존 dot1x 인증은 Interfaced가 통신을 하지 못하도록 하였으나, 사용자 기반의 인증은 허가된 MAC address는 통신이 가능하도록 하여 최대 32개의 사용자가 동시에 하나의 Interface를 통해 인증을 수행할 수 있습니다.

User 기반 인증을 활성화하면 Switch에서 전송되는 EAPOL은 Link-Local (EAPOL) 인 Destination MAC Address를 지니고 전송되지 않고, Unicast 형태로 전송됩니다.

하나의 Interface에 Guest VLAN과 동시에 설정할 수 없습니다.

■ EAPOL-Switching

EAPOL-Switching은 EAPOL Frame 을 Drop 하지 않고 switching 하도록 설정하는 방법입니다. 사용자 기반의 인증을 사용하는 Interface를 이용해 Multi 인증을 사용하는 경우 Switch에서 전송되는 EAPOL은 Link-Local (EAPOL) 인 Destination MAC Address를 포함하여 전송되지 않고, Unicast 형태로 전송되는데 PC에서 전송되는 EAP Message들은 Link-Local로 전송되기 때문에 하단의 Switch에서 eapol-switching 기능을 활성화 하여야 PC의 EAPOL Frame이 multi-user 인증 사용 Interface에 전달되어 정상적으로 Multi User 인증이 가능합니다.

■ MAC Address 기반의 인증 (MAC Authentication Bypass)

사용자의 MAC address에 기반하여 인증을 수행하는 방법으로 MAC address 발견 시 즉시 인증을 시도하는 것이 아니라 Authentication Time(최대 60 s)이 되었을 때 인증을 수행하며 인증 대상 Interface에서 Broadcast Packet이 발생되지 않을 경우에는 MAC Address를 확인할 수 없어 인증을 수행할 수 없습니다. dot1x의 Timeout, Quiet Timeout 값을 감소하면 MAC Address 기반의 인증 시간을 단축할 수 있습니다.

MAC Address 기반의 인증을 위해서는RADIUS Server에 인증 할 MAC Address가 User ID 및 Password에 (알파벳은 소문자)로 등록되어 있어야 합니다.

■ Guest VLAN 기반의 인증

인증되지 않은 사용자의 경우 통신을 차단하지 않고, 별도로 설정된 Guest VLAN으로 자동으로 할당하여 통신을 허가하는 방식입니다. 인증되지 않은 사용자가 Guest VLAN을 통해 통신하는 중이라도 EAPOL을 이용한 인증은 계속 시도하기 때문에 dot1x Supplicant를 지니고 있는 Client에서는 반복적인 인증 실패 메시지를 볼 수 있습니다.

Guest VLAN으로 설정하기 위해서는 vlan database에 해당 VLAN이 존재해야 하나의 Interface에서 사용자 기반의 인증 및 Web-based 인증을 동시에 설정할 수 없습니다.

■ Dynamic VLAN Assignment 기능

RADIUS Server를 통한 802.1x 인증 시 RADIUS Server에 설정되어 있는 User의 Attribute로 지정되어 있는 값을 이용하여, 인증이 성공한 Interface의 VLAN을 Attribute에 지정되어 있는 값으로 변경해주는 기능입니다.

Dynamic VLAN Assignment 기능은 Guest VLAN의 확장기능, MAC Based Dynamic VLAN, 일반 Dynamic VLAN의 3가지 설정으로 지원합니다.

RADIUS Server에 지정하는 Attribute는 표준 RFC3580를 따르며, 상세 내역은 다음과 같습니다.

- Tunnel-Type = VLAN
- Tunnel-Medium-Type = IEEE-802
- Tunnel-Private-Group-ID = <VLAN_ID>

Guest VLAN기반의 인증기능을 이용한 경우 인증이 성공된 사용자라 하더라도 RADIUS Server의 User Attribute의 Tunnel-Type과 TunnelMedium-Type이 위와 같이 설정되어 있지 않을 경우 동작하지 않으며, VLAN_ID가 vlan database 내에 없는 Invalid한 VLAN일 경우 Interface의 default vlan으로 인증을 성공합니다. (단순 guest-vlan 처럼 동작함)

■ Web-based 기반의 인증

DHCP를 사용하는 환경에서 사용자의 PC에서 인터넷 사용시 WEB 기반의 인증을 유도하여 ID, Password를 입력 받아 RADIUS Server를 통해 인증을 수행합니다. 별도의 Userspace TCP/IP Stack에 ARP Spoofer, DNS Spoofer, Modified TCP/IP Stack, DHCPD, HTTPD 등이 적재되어 있기 때문에 별도의 IP 설정도 필요 없고 무조건 사용 가능하며, authd와 통신하여 RADIUS Server를 통한 dot1x 인증을 수행합니다. Userspace TCP/IP Stack은 관리 IP/IPv4 Link Local Address (Zero-configuration에 이용되는 169.254.x.x)를 제외한 모든 IP를 자신이라 여기고 응답하며 Userspace TCP/IP Stack의 관리 IP는 192.168.174.20~254 (DHCP를 통한 자동 할당 범위, DHCPD의 Lease Time은 5 s)까지입니다.

WEB 인증이 완료되어도 PC의 DNS Cache 문제로 인하여 즉시 WEB의 초기화면이 나타나

지 않을 수 있으며 이 경우 IE, Firefox등의 browser를 종료한 후 IP 갱신을 위한 약 10 s 정도의 시간이 지난 후에 시작하면 DNS Cache가 삭제되면서 WEB의 초기 화면이 나타납니다.

DNS Record에 대한 Spoofed Reply의 TTL (Time-To-Live)의 값은 1 s로 설정되어있으나, 이 TTL을 무시한 Application Level에서 DNS Cache를 사용하는 일부 프로그램 (Firefox)에서는 인증 후 프로그램을 다시 시작해야 정상 동작합니다.

[그림 2-7] Web-based 인증 Default

The diagram illustrates the default web-based authentication process with three screens:

- login.html**: A login form with fields for Username and Password, and a Login button.
- login_fail.html**: A screen showing "Login failed" in red text, with the Username and Password fields and a Login button.
- page_redirect.html**: A screen showing "login success" and a message: "you need to restart web browser if your web browser have internal DNS cache feature (ie. firefox) please click here if nothing changes within 10 second".

802.1x Extended 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
dot1x extension multi-user	INTERFACE	Multi User 인증 방식을 활성화합니다.
dot1x extension multi-user client-limit <0-32>	INTERFACE	Multi User 인증 방식 사용 시 최대 사용자 수를 설정합니다. (Default: 32)
dot1x extension mac-auth-bypass	INTERFACE	MAC Bypass 인증을 활성화합니다.
dot1x extension mac-auth-bypass first-bypass <1-30 >	INTERFACE	처음 인증 시도 시 MAC 인증을 우선하며, 인증 시 Delay time을 1~30 s 사이로 설정합니다.
dot1x extension guest-vlan VLANID dynamic-vlan	INTERFACE	Guest VLAN 기능 및 Dynamic VLAN Assignment 기능을 활성화합니다.
dot1x extension dynamic-	INTERFACE	Dynamic VLAN Assignment 기능을 활

vlan		성화합니다.
dot1x extension web-auth	INTERFACE	WEB 기반 인증을 활성화합니다.
dot1x web-auth user-template	CONFIG	web-auth 인증 시 사용자가 작성한 HTML을 보여주도록 합니다.
dot1x extension required-auth [mac port web]	INTERFACE	Multi-Step 인증 기능을 활성화 합니다.
copy tftp IP_Address WORD dot1x web-auth flash	TOP	TFTP를 통하여 web-auth를 위한 Flash에 HTML을 Upload 합니다.
copy ftp IP_Address FILENAME FTP_ID PASSWORD [<1-65535>] dot1x web-auth flash	TOP	FTP를 통하여 web-auth를 위한 Flash에 HTML을 Upload 합니다.
copy usb FILENAME dot1x web-auth flash	TOP	usb를 통하여 web-auth를 위한 Flash에 HTML을 Upload 합니다.

dot1x 관련 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show dot1x web-auth flash	TOP	web-auth HTML이 저장된 Flash 의 자료 및 용량을 확인합니다.
show dot1x [all brief]	TOP	802.1x 설정 내용 및 인증 결과를 확인합니다.
show dot1x interface IFNAME	TOP	Interface 관련 802.1x 설정을 확인합니다.
show dot1x statistics interface IFNAME	TOP	802.1x에 대한 통계를 확인합니다.

802.1x Extended 기능을 제거하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no dot1x system-auth-ctrl eapol-switching	CONFIG	dot1x를 사용하지 않는 Switch에서 EAPOL frame 이 multi-user 인증 사용 포트에 전달될 수 있도록 합니다.
no dot1x extension multi-user	INTERFACE	Interface 기반의 인증 방식을 사용합니다. (Default)
no dot1x extension multi-user client-limit	INTERFACE	Multi User 인증의 최대 사용자를 기본값인 32로 복구합니다.
no dot1x extension mac-	INTERFACE	MAC authentication bypass 비활성화

auth-bypass		합니다.
no dot1x extension guest-vlan <i>VLANID</i>	INTERFACE	Guest VLAN 설정 및 Dynamic VLAN Assignment 기능을 비활성화합니다..
no dot1x extension dynamic-vlan	INTERFACE	Dynamic VLAN Assignment 기능을 비활성화합니다.
no dot1x extension web-auth	INTERFACE	WEB 기반 인증을 비활성화합니다.
remove dot1x web-auth flash <i>FILENAME</i>	INTERFACE	web-auth를 위해 Flash에 저장된 HTML 파일을 제거합니다. (<i>FILENAME</i> 에 * 입력 시 모든 자료 삭제)
no dot1x extension required-auth	INTERFACE	Multi-Step 인증 기능을 제거 합니다.



참고

1. Guest-VLAN과 Multi User 인증 또는 WEB 기반 인증은 동일한 Interface에 중복하여 설정할 수 없습니다.
2. Multi-Step 인증 기능을 활성화 한 경우 설정된 인증항목 (Port+MAC 또는 Port+WEB 또는 MAC+WEB 또는 Port+MAC+WEB)이 모두 인증되어야 네트워크사용이 가능합니다.

<예제1> Dot1x Extended 인증 설정

- RADIUS Server IP : 192.168.130.20

- ge3 : multi-user, mac-auth-bypass, web-auth 인증 설정

```

SG2124G#configure terminal
SG2124G(config)#dot1x system-auth-ctrl
SG2124G(config)#radius-server host 192.168.130.20 key *****
SG2124G(config)#int ge3
SG2124G(config-if)#dot1x port-control auto
SG2124G(config-if)#dot1x extension multi-user
SG2124G(config-if)#dot1x extension mac-auth-bypass
SG2124G(config-if)#dot1x extension web-auth
SG2124G(config-if)#end
SG2124G#show bridge
bridge          VLAN port      mac          fwd timeout
MAC Count = 0
SG2124G#
SG2124G#show dot1x brief
port  instance  port-status  auth      supplicant      supplicant  successful
      type     type         address        name          auth-Type
ge3   Master    Unauthorized User
ge3   1          Unauthorized User  001a.f40f.0400  001af40f0400
ge3   2          Authorized   User  0017.4241.5189  hdn70
SG2124G#
SG2124G#show bridge
bridge          VLAN port      mac          fwd timeout

```

```

1          1    ge3      0017.4241.5189 1    300
1          1    ge3      001a.f40f.0400 1    300
MAC Count = 2
SG2124G#

```

<예제 2> Dot1x Extended 인증 설정

- RADIUS Server IP : 192.168.130.20
- ge3 : guest-vlan 인증 설정

```

SG2124G#configure terminal
SG2124G(config)#dot1x system-auth-ctrl
SG2124G(config)#radius-server host 192.168.130.20 key *****
SG2124G(config)#interface ge3
SG2124G(config-if)#dot1x port-control auto
SG2124G(config-if)#dot1x extension guest-vlan 10
SG2124G(config-if)#end
SG2124G#show bridge
bridge      VLAN port      mac          fwd timeout
1           1    ge5      001a.f400.0300 1    300
1           10   ge3      0017.4241.5189 1    300      → 인증 전
MAC Count = 2
SG2124G#
SG2124G#show bridge
bridge      VLAN port      mac          fwd timeout
1           1    ge3      0017.4241.5189 1    300      → 인증 후
1           1    ge5      001a.f400.0300 1    300
MAC Count = 2
SG2124G#

```

<예제3> Multi-Step 인증 설정

- RADIUS Server IP : 192.168.130.20
- ge3 : port+mac+web 인증 설정

```

SG2124G#configure terminal
SG2124G(config)#dot1x system-auth-ctrl
SG2124G(config)#radius-server host 192.168.130.20 key *****
SG2124G(config)#interface ge3
SG2124G(config-if)#dot1x port-control auto
SG2124G(config-if)#dot1x extension web-auth
SG2124G(config-if)#dot1x extension mac-auth-bypass first-bypass 20
SG2124G(config-if)#dot1x extension required-auth port mac web
SG2124G(config-if)#end
SG2124G#sh dot1x brief
port  instance  port-status  auth      supplicant  supplicant  successful
              type      address      name      auth-Type
=====
ge3    Master    Authorized  Port     14da.e917.d44a  us2          P M W
SG2124G#

```

인증 완료 조건: Successful Auth-Type항목에 설정한 인증항목이 모두 표시되어야 함
(Port=P, MAC=M, WEB=W)

2.9.4 Embedded RADIUS Server

Embedded RADIUS Server를 내장되어 있어 간편하게 CLI 제어를 통해 EAPOL 인증, WEB 기반 인증, Guest VLAN 등의 dot1x 관련 인증에 이용할 수 있으며, Client는 MD5-Challenge를 이용한 인증과 PAP (Password authentication protocol)를 이용한 인증을 사용하여 인증을 수행할 수 있습니다. 내장된 RADIUS Server 는 localhost(127.0.0.1) 의 요청에만 응답합니다.

Embedded RADIUS Server에는 최대 512개의 User를 설정할 수 있으며, Password는 최대 23자까지 입력 가능하며, plain-text 형태의 Password를 요구하는 인증 방식 때문에 DES (Data Encryption Standard)를 이용한 Private Key 기반 암호화 사용하고 있습니다.

원격지의 RADIUS Server 와 내장된 Embedded RADIUS Server는 동시에 사용할 수 없으며, 사용자 추가 시 RADIUS Server는 5 s에 1번 이하로 Reload 하기 때문에 사용자 추가 후 최대 5 s 이후에 RADIUS Server에 반영될 수 있습니다.

Embedded RADIUS Server 기능을 활성화하려면 다음 명령어를 사용하십시오

명령어	모드	기능
dot1x embedded enable	CONFIG	Embedded RADIUS Server를 활성화합니다.
dot1x embedded username <USERNAME> password <PASSWORD>	CONFIG	Embedded RADIUS Server의 사용자를 추가합니다.

Embedded RADIUS Server 관련 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show dot1x [all brief]	TOP	802.1x 설정 내용 및 인증 결과를 확인합니다.
show running-config {include grep} embedded	TOP	Embedded RADIUS Server의 User 설정 내역을 확인합니다.

Embedded RADIUS Server 기능을 제거하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no dot1x embedded enable	CONFIG	Embedded RADIUS Server 기능을 비활성화합니다.

no dot1x embedded username <USERNAME>	CONFIG	Embedded RADIUS Server의 사용자를 삭제합니다.
--	--------	-------------------------------------

<예제> Embedded RADIUS Server 설정

- Embedded RADIUS Server 설정 및 User 생성한 후 ge2에서 test1 계정으로 인증

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#dot1x system-auth-ctrl
SG2124G(config)#dot1x embedded enable
SG2124G(config)#dot1x embedded username test1 password test1
SG2124G(config)#dot1x embedded username test2 password test2
SG2124G(config)#dot1x embedded username test3 password test3
SG2124G(config)#interface range ge1-10
% ge1-10 Selected
SG2124G(config-if-range)#dot1x port-control auto
% ge1-10 Selected
SG2124G(config-if-range)#dot1x extension multi-user
% ge1-10 Selected
SG2124G(config-if-range)#dot1x extension mac-auth-bypass
% ge1-10 Selected
SG2124G(config-if-range)#dot1x extension web-auth
% ge1-10 Selected
SG2124G(config-if-range)#end
SG2124G#
SG2124G#show dot1x brief
```

port	instance	port-status	auth type	supplicant address	supplicant name
ge1	Master	Unauthorized	User		
ge2	Master	Unauthorized	User		
ge2	1	Authorized	User	0000.a0b1.7de6	test1
ge3	Master	Unauthorized	User		
ge4	Master	Unauthorized	User		
ge5	Master	Unauthorized	User		
ge6	Master	Unauthorized	User		
ge7	Master	Unauthorized	User		
ge8	Master	Unauthorized	User		
ge9	Master	Unauthorized	User		
ge10	Master	Unauthorized	User		

```
SG2124G#
```



참고

1. 원격지의 RADIUS Server 와 내장 RADIUS Server는 동시에 사용할 수 없습니다.
2. RADIUS Server에 127.0.0.1 과 같은 localhost는 추가할 수 없습니다.

2.10 Filtering

2.10.1 ACL을 이용한 Filtering

Switch로 전송되어 들어오는 Telnet, FTP, ICMP, SNMP 등 특정 서비스 또는 특정 IP의 접속을 막도록 설정할 수 있습니다. Switch 자체로 들어오는 Telnet, FTP, ICMP, SNMP 등의 서비스 접속을 막을 때에는 ACL을 사용합니다.

ACL 지정 시 time-range 정책을 사용하여 time-based ACL을 사용할 수 있습니다.

Packet의 방향은 Inbound/outbound를 선택하여 설정할 수 있으며, Portrange 단위로 적용 시에 포트그룹은 중첩이 불가능합니다. 독립된 포트 그룹은 최대 15개까지 사용이 가능합니다.

ACL의 자세한 설정 방법은 "2.6.3 QoS ACL 설정" 메뉴를 참고하시기 바랍니다.

ACL을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
acl Rule_No {permit deny} Protocol Source Destination [DSCP Dport EtherType] {log time-range}	CONFIG	Access List 정책을 설정합니다.
{ip ipv6} acl Rule_No {in out} PORTRANGE [vlan VLAN_ID]	CONFIG	Interface에 Access List를 적용합니다.
{ip ipv6} acl Rule_No {in out} [vlan VLAN_ID]	INTERFACE	Interface에 Access List를 적용합니다.
acl log interval <1-1440>	CONFIG	Access List의 로그 기록 간격을 설정합니다. (단위: min)
acl time-range Name absolute {start stop} HH:MM	CONFIG	Access List의 time-range absolute 정책을 설정합니다.
acl time-range Name periodic {daily monday tuesday wednesday thursday friday saturday weekday weekend} HH:MM	CONFIG	Access List의 time-range periodic 정책을 설정합니다.

설정된 ACL을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show acl [Rule_No]	TOP	설정된 ACL 전체의 설정 내용 및 QoS에 적용된 Packet의 Count 값을 확인합니다.
show ip acl [IFNAME]	TOP	특정 Interface에 적용된 ACL을 확인합니다.

ACL을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no acl Rule_No {permit deny} Protocol Source Destination [DSCP Dport EtherType]	CONFIG	Access List 정책을 삭제합니다.
no {ip ipv6} acl Rule_No {in out} PORTRANGE	CONFIG	Interface에서 Access List를 삭제합니다.
no {ip ipv6} acl Rule_No {in out}	INTERFACE	Interface에서 Access List를 삭제합니다.
no acl time-range Name	CONFIG	Access List의 time-range 정책을 삭제합니다.

<예제1> 특정 IP로의 WEB 접근을 특정 IP에서만 허용하도록 하는 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#acl 100 permit tcp host 192.168.100.2 host 192.168.100.252 dp eq www
SG2124G(config)#acl 100 deny tcp any host 192.168.100.252 dp eq www
SG2124G(config)#ip acl 100 in ge15
SG2124G#end
SG2124G#
SG2124G#show acl

Extended IP acl: 100
  permit tcp host 192.168.100.2 host 192.168.100.252 dp eq 80
    Ports: ge15
    Counter: 1265
  deny tcp any host 192.168.100.252 dp eq 80
    Ports: ge15
    Counter: 24254
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#no ip acl 100 in ge15
```

```
SG2124G(config)#exit
SG2124G(config)#
```

<예제2> 특정 IP로의 WEB Traffic을 차단하는 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#acl 100 deny tcp any host 192.168.100.252 dp eq www
SG2124G(config)#ip acl 100 in ge15
SG2124G(config)#
SG2124G(config)#no ip acl 100 in ge15
SG2124G(config)#
```



참고

1. 동일한 ACL 번호에는 최대 128개까지의 Entry를 설정할 수 있습니다.
2. Interface에 ACL이 적용된 상태에서 설정된 ACL 정책을 변경한 경우에는 적용된 ACL 해제 후 다시 적용해야 합니다.
3. Interface 내에서 ACL을 지정한 경우에도 Config Mode에서 설정한 것과 동일하게 설정 및 표시됩니다.
4. ARP ACL은 Out Bound 설정을 할 수 없습니다.
5. SG2024, SG2024P, SG2200 Series 제품은 IPv6 ACL/QoS를 지원하지 않습니다.
6. IPv6 ACL기능은 Switch버전 2.x 이상에서만 지원합니다.

2.10.2 MAC Address Filtering

Interface에 전송되는 특정한 MAC Address를 가진 Packet에 대해 설정할 때에는 모든 MAC Address의 Packet을 차단하도록 설정한 후, 특정 MAC Address의 Packet을 받아들이도록 설정을 추가해 나가는 것이 편리합니다. 특정한 MAC Address를 가진 Packet을 차단 또는 허용하도록 정책을 만들 때에는 ACL을 사용합니다.

ACL의 자세한 설정 방법은 "2.6.3 QoS ACL 설정" 메뉴를 참고하시기 바랍니다.

<예제> MAC Address Filtering을 통한 특정 MAC 차단/허용 설정

MAC Address 1 개 차단

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#acl 1100 deny 0001.0000.0001 0000.0000.0000 any 1
SG2124G(config)#interface ge1
SG2124G(config-if)#ip acl 1100 in
SG2124G(config-if)#exit
```

MAC Address 1 개만 허용하고 나머지 모두 차단

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#acl 1100 permit 0001.0000.0001 0000.0000.0000 any 1
SG2124G(config)#acl 1100 deny any any 1
SG2124G(config)#interface ge1
SG2124G(config-if)#ip acl 1100 in
SG2124G(config-if)#exit
```



참고

MAC Address의 Mask 설정 (wildcard Bit)

- 단일 MAC Address ; 0000.0000.0000
- 모든 MAC Address : ffff.ffff.ffff

2.10.3 Interface별 접속자 수 제한

Interface 별로 접속 가능한 MAC 개수를 설정함으로써 사용자 수를 제한할 수 있습니다. 이때, 사용자는 단순히 Network 내에 있는 PC의 개수만 생각하고 접속자 수를 제한하면 Network 내에 있는 Switch 등의 장비들로 인해 제한한 MAC 수보다 접속할 MAC 수가 많은 상태가 되어 일부 장비의 통신에 장애가 발생할 수 있으므로 MAC 개수를 잘 고려하여 설정해야 합니다. Interface 별로 접속 가능한 MAC 수를 제한하면 MAC Flooding과 같은 Attack이 발생하여도 Network를 안정적으로 관리할 수 있습니다.

인터넷 서비스 사업자의 경우 이 설정을 이용하여 접속자 수에 따른 차별화된 서비스를 관리할 수 있습니다.

Interface에 Max-MACs 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
max-macs <0-32768>	INTERFACE	Interface별 MAC 수를 제한합니다.

설정된 Max-MACs 기능을 확인 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show max-macs	TOP	MAC 제한 설정 상태를 확인합니다.

설정된 Max-MACs 기능을 초기화 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no max-macs	INTERFACE	Interface별 MAC 제한 기능을 해제합니다.

<예제> max-macs 설정

```

SG2124G#show bridge
bridge      VLAN port      mac          fwd timeout
1           1    ge1       0000.0000.000e 1    300
1           1    ge1       0000.0000.0014 1    300
1           1    ge1       0000.0000.0019 1    300
1           1    ge2       0000.1100.0000 1    300
1           1    ge2       0000.1200.0000 1    300
1           1    ge2       0000.1300.0000 1    300
1           1    ge2       0000.1400.0000 1    300
1           1    ge2       0000.1500.0000 1    300
1           1    ge2       0000.1600.0000 1    300
MAC Count = 9
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge2
SG2124G(config-if)#max-macs 4
SG2124G(config-if)#end
SG2124G#show bridge
bridge      VLAN port      mac          fwd timeout
1           1    ge1       0000.0000.000e 1    300
1           1    ge1       0000.0000.0014 1    300
1           1    ge1       0000.0000.0019 1    300
1           1    ge2       0000.1200.0000 1    300
1           1    ge2       0000.1300.0000 1    300
1           1    ge2       0000.1400.0000 1    300
1           1    ge2       0000.1600.0000 1    300
MAC Count = 7
SG2124G#show max-macs
ge2      :      4/4      (current/max macs)
SG2124G#

```



참고

1. 설정된 Max-MACs 개수를 변경하려면, 기존에 제한되어 있던 Max-MACs 기능을 해제한 후 다시 설정해야 합니다.
2. Network 내에 설치되어 있는 장비(Switch 등)들의 MAC 수를 고려해서 제한 설정을 하시기 바랍니다.

2.10.4 Port Security

Port Security 기능은 특정 Interface에 접속 가능한 MAC 개수를 설정한 후 특정 MAC Address에 대해서만 사용 가능하도록 하는 기능이며, Port Security를 적용한 Interface는 max-mac으로 제한된 MAC 개수 범위 내에서 우선 등록되어 동작합니다. Port Security 설정 시 VLAN ID를 입력하지 않았을 경우에는 PVID 값이 자동으로 설정되며 Default VLAN 인 경우에는 표시하지 않습니다.

Port Security를 설정하게 되면 FDB를 Flush 한 후 Static으로 L2 Table에 들어가게 되어 해당 Interface에 Static으로 설정되므로 등록된 MAC Address를 사용하는 장비를 다른 Interface로 옮기는 경우 해당 MAC Address는 통신이 되지 않으며, Port Security 명령을 삭제하면 L2 Table에 등록된 Static 설정을 제거합니다.

Port Security 기능은 Interface에 max-macs 명령이 먼저 설정되어 있어야 하며, 기능을 사용하는 중에 max-macs 설정을 제거하면 해당 명령도 모두 제거됩니다.

Port Security를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
max-macs <0-32768>	INTERFACE	Interface별 MAC 수를 제한합니다.
max-macs mac-address MAC_Address [VLANID]	INTERFACE	Interface에 Port Security를 설정합니다.

Port Security 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show max-macs	TOP	MAC 제한 설정 상태를 확인합니다.

Port Security 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no max-macs	INTERFACE	Interface별 MAC 제한 기능을 해제합니다.
no max-macs mac-address MAC_Address	INTERFACE	Port Security 기능을 해제합니다.

<예제> Port Security 설정

```

SG2124G#show bridge
bridge      VLAN port      mac          fwd timeout
1           1    ge1      0000.0000.000e 1    300
1           1    ge1      0000.0000.0014 1    300
1           1    ge1      0000.0000.0019 1    300
1           1    ge2      0000.1200.0000 1    300
1           1    ge2      0000.1300.0000 1    300
1           1    ge2      0000.1400.0000 1    300
1           1    ge2      0000.1600.0000 1    300
MAC Count = 7
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge1
SG2124G(config-if)#max-macs 2
SG2124G(config-if)#max-macs mac-address 0000.0000.0001
SG2124G(config-if)#max-macs mac-address 0000.0000.0002 10
SG2124G(config-if)#end
SG2124G#
SG2124G#show bridge
bridge      VLAN port      mac          fwd timeout
1           1    ge1      0000.0000.0001 1    0
1           10   ge1      0000.0000.0002 1    0
1           1    ge2      0000.1200.0000 1    300
1           1    ge2      0000.1300.0000 1    300
1           1    ge2      0000.1400.0000 1    300
1           1    ge2      0000.1600.0000 1    300
MAC Count = 6
SG2124G#
SG2124G#show max-macs
ge2      :      2/2      (current/max macs)
SG2124G#

```

**참고**

설정된 Max-MACs 개수를 변경하는 경우, Port Security에 설정한 내용이 삭제되므로 Max-MACs 개수를 변경한 경우에는 Port Security 기능을 다시 설정해야 합니다.

2.10.5 NetBIOS Filtering

NetBIOS는 별개의 컴퓨터 상에 있는 Application들이 Local Network 내에서 서로 통신 할 수 있게 해주는 Protocol이며, 특정 Interface에 NetBIOS 차단 기능을 설정할 수 있습니다. (MS Windows 공유 차단)

NetBIOS의 Session Mode는 두 개의 컴퓨터들이 서로 연결을 맺을 수 있도록 해주며, Datagram Mode는 LAN의 모든 컴퓨터들에게 Message를 보내는 기능을 지원합니다. 서로 정보를 공유해야 하는 LAN 환경에서는 컴퓨터간에 통신이 가능하도록 NetBIOS를 사용할 수 있도록 해야 하지만 ISP 사업자들이 아파트나 특정한 지역에 LAN 서비스로 인터넷 통신을 제공하는 경우에는 고객들의 정보를 공유해서는 안 되는 상황에서 서로의 정보가 공개될 수 도 있습니다.

NetBIOS Filtering 기능은 IPv4, IPv6 NetBIOS 차단기능을 한번에 제공합니다.

Interface에 NetBIOS Filtering 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
netbios filter <i>PORTRANGE</i>	CONFIG	NetBIOS Filtering을 설정합니다.
netbios filter	INTERFACE	NetBIOS Filtering을 설정합니다.

NetBIOS Filtering 설정 내역을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show filter	TOP	NetBIOS Filtering 설정내역을 확인합니다.

Interface에 설정된 NetBIOS Filtering 기능을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no netbios filter <i>PORTRANGE</i>	CONFIG	NetBIOS Filtering을 해제합니다.
no netbios filter	INTERFACE	NetBIOS Filtering을 해제합니다.



참고

1. Interface Mode에서 NetBIOS Filter를 설정한 경우에도 설정 값은 Config Mode의 설정으로 통합되어 표시됩니다.
2. SG2024, SG2024P, SG2200 Series 제품은 IPv6 NetBIOS

Filter 기능을 지원하지 않습니다.

3. IPv6 NetBIOS Filter 기능은 Switch버전 2.x 이상에서만 지원합니다.
-

<예제> Interface ge1-4에 netbios filter 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface range ge1-4
% ge1-4 Selected
SG2124G(config-if-range)#netbios filter
% ge1-4 Selected
SG2124G(config-if-range)#end
SG2124G#
SG2124G#show running-config
!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
bridge 1 protocol pvstp
!
spanning-tree mst config
!
mls qos enable
mds enable ge1-22 detect
mds uplink ge23-24
netbios filter ge1-4
!
interface ge1
!
-- 이하 생략 --

SG2124G#
SG2124G#show filter
Port          Netbios Filter  DHCP Filter
=====
ge1           Enable         -
ge2           Enable         -
ge3           Enable         -
ge4           Enable         -
ge5           -              -
ge6           -              -
--생략--
ge22          -              -
ge23          -              -
ge24          -              -
=====
Counter information
Netbios Filter : 12
```

2.10.6 DHCP Filtering

DHCP (Dynamic Host Control Protocol)는 DHCP Server가 DHCP Client에게 자동적으로 IP Address를 할당하고 IP Address를 관리할 수 있도록 하는 Protocol로서 대부분의 ISP 사업자는 이와 같은 방법으로 서비스를 제공하고 있습니다.

이 때, 어떤 DHCP Client가 IP 공유기 등 또 다른 DHCP Server가 될 수 있는 장비를 연결해 버린다면, 일부 사용자의 경우 사설 DHCP를 할당 받아 인터넷 통신에 장애가 발생할 수 있습니다.

DHCP Filtering이 설정된 Interface 하단으로부터의 DHCP Reply를 차단하여 DHCP Service가 올바르게 이루어지도록 도와주는 기능입니다.

DHCP Filtering 기능은 IPv4, IPv6 DHCP Server 차단기능을 한번에 제공합니다.

Interface에 DHCP Filtering 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
dhcp filter <i>PORTRANGE</i>	CONFIG	DHCP Filtering을 설정합니다.
dhcp filter	INTERFACE	DHCP Filtering을 설정합니다.

DHCP Filtering 설정 내역을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show filter	TOP	DHCP Filtering을 설정합니다.

Interface에 설정된 DHCP Filtering 기능을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no dhcp filter <i>PORTRANGE</i>	CONFIG	DHCP Filtering을 해제합니다.
no dhcp filter	INTERFACE	DHCP Filtering을 해제합니다.



참고

1. Interface Mode에서 DHCP Filter를 설정한 경우에도 설정 값은 Config Mode의 설정으로 통합되어 표시됩니다.
2. SG2024, SG2024P, SG2200 Series 제품은 IPv6 DHCP Filter 기능을 지원하지 않습니다.
3. IPv6 DHCP Filter 기능은 Switch버전 2.x 이상에서만 지원합니다.

<예제> Interface ge1-4에 DHCP Filtering 적용

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface range ge1-4
% ge1-4 Selected
SG2124G(config-if-range)#dhcp filter
% ge1-4 Selected
SG2124G(config-if-range)#end
SG2124G#
SG2124G#show running-config
!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
bridge 1 protocol pvstp
!
spanning-tree mst config
!
mls qos enable
mds enable ge1-22 detect
mds uplink ge23-24
dhcp filter ge1-4
!
interface ge1
!
-- 이하 생략 --

SG2124G#
SG2124G#show filter
Port          Netbios Filter  DHCP Filter
=====
ge1            -               Enable
ge2            -               Enable
ge3            -               Enable
ge4            -               Enable
ge5            -               -
ge6            -               -
--생략--
ge22           -               -
ge23           -               -
ge24           -               -
=====

Counter information
    DHCP      Filter : 0

```

2.10.7 Storm Control

Broadcast Storm이란, 비정상적으로 과도한 Broadcast Packet이 발생하는 현상을 말합니다. 비정상적으로 과도하게 발생한 Broadcast Packet은 회선 용량의 대부분을 차지하여 시스템 및 Network에 과도한 부하를 줌으로써 Network를 마비시킬 수 있습니다.

Broadcast Storm Control 기능은 1 s 동안 Broadcast Packet의 전송률을 설정하여 pps 단위로 설정된 한계 값을 넘는 Packet이 발생한 경우 해당 Packet을 폐기하는 방법으로 구현되고 있습니다. 관리자는 Storm control을 사용하여 제한하는 Packet의 전송률을 변경할 수 있습니다.

Broadcast Storm 뿐만 아니라 Multicast나 DLF (Destination Lookup Fail) Storm에 대한 조절도 가능합니다.

Storm Control을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
storm-control {broadcast dlf multicast} <0-1488000>]	INTERFACE	Storm Control 기능을 설정합니다.

Storm Control을 설정 값을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show storm-control [IFNAME]	TOP	Storm Control 설정 값을 확인합니다.

Storm Control 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no storm-control {broadcast dlf multicast}	INTERFACE	Storm Control 기능을 해제합니다.



참고

rate shaping과 storm-control은 하나의 Interface에 동시에 설정할 수 없습니다.

<예제> Storm Control 설정

Broadcast Packet 이 10000 개 이상인 경우 제한

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge1
SG2124G(config-if)#storm-control broadcast 10000
SG2124G(config-if)#exit
SG2124G(config)#
```

Multicast Packet 이 20000 개 이상인 경우 제한

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge2
SG2124G(config-if)#storm-control multicast 20000
SG2124G(config-if)#exit
SG2124G(config)#
```

dif Packet 이 30000 개 이상인 경우 제한

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#interface ge3
SG2124G(config-if)#storm-control dif 30000
SG2124G(config-if)#exit
SG2124G(config)#
```

Storm-control 설정 내역 확인

```
SG2124G#show storm-control
Storm control ratelimit (pps frames)
ge1      : bcast( 10000) mcast(      0) dif(      0)
ge2      : bcast(      0) mcast( 20000) dif(      0)
ge3      : bcast(      0) mcast(      0) dif( 30000)
ge4      : bcast(      0) mcast(      0) dif(      0)
ge5      : bcast(      0) mcast(      0) dif(      0)
ge6      : bcast(      0) mcast(      0) dif(      0)
ge7      : bcast(      0) mcast(      0) dif(      0)
ge8      : bcast(      0) mcast(      0) dif(      0)
ge9      : bcast(      0) mcast(      0) dif(      0)
ge10     : bcast(      0) mcast(      0) dif(      0)
ge11     : bcast(      0) mcast(      0) dif(      0)
ge12     : bcast(      0) mcast(      0) dif(      0)
ge13     : bcast(      0) mcast(      0) dif(      0)
ge14     : bcast(      0) mcast(      0) dif(      0)
--- 중 략 ---
ge23     : bcast(      0) mcast(      0) dif(      0)
ge24     : bcast(      0) mcast(      0) dif(      0)
SG2124G#
```

2.10.8 MLS (Multi-Layer Switch) DoS 기능

MLS (Multi-Layer Switch) DoS 차단 기능은 Switching Fabric에서 Packet Header를 분석하여 특정 유형의 Traffic에 대해서는 Forwarding하지 않고 Chip에서 차단하도록 하는 기능입니다. MLS DoS로 차단이 가능한 Traffic의 유형은 아래 옵션 중 선택하여 지정해야 활성화되며, 차단된 Packet들은 Switching Fabric에서부터 차단되기 때문에 별도의 차단 로그를 기록하지는 않습니다.

mls dos 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mls dos	CONFIG	mls dos 기능을 활성화합니다.
mls dos-option {l4port sipequaldip tcpflags}	CONFIG	mls dos로 차단가능 항목 중 SG2124, SG2124PoE에서 사용 가능한 명령입니다.
mls dos-option {icmpfragments sipequaldip macsaequalmacda tcpflagsfup tcpflagssf tcpportsequal udpportsequal}	CONFIG	mls dos로 차단가능 항목 중 SG2124G/SG2124GPoE/SG2148G/SG2148GPoE에서 사용 가능한 명령입니다.

mls dos-option 차단 조건은 아래와 같습니다.

- Icmpfragments : ICMP Fragmented 인 패킷
- Macsaequalmacda : SRC MAC Address와 DST MAC Address가 동일한 패킷
- Sipequaldip : SRC IP Address와 DST IP Address가 동일한 패킷
- tcpflagsfup : TCP FIN, URG, PSH Flag 설정 및 Sequence Number가 0 인 패킷
- tcpflagssf : TCP SYN, FIN Flag가 동시에 활성화되어 있는 패킷
- tcpportsequal : TCP SRC Port와 DST Port가 동일한 패킷
- Udpportsequal : UDP SRC Port와 DST Port가 동일한 패킷

mls dos 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show running-config include mls	TOP	mls dos 설정 값을 확인합니다.

mls dos 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mls dos	CONFIG	mls dos 기능을 비활성화합니다. (Default)
no mls dos-option {icmpfragments macsaequalmacda sipequaldip tcpflagsfup tcpflagssf l4port tcpportsequal udpportsequal}	CONFIG	mls dos에서 차단할 항목을 삭제합니다.



참고

10/100 모델과 10/100/1000모델의 Chip 사양에 따라 사용할 수 있는 명령이 제한 됩니다.

<예제> mls dos 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mls dos-option icmpfragments
SG2124G(config)#mls dos-option macsaequalmacda
SG2124G(config)#mls dos-option sipequaldip
SG2124G(config)#mls dos-option tcpflagsfup
SG2124G(config)#mls dos-option tcpflagssf
SG2124G(config)#mls dos-option tcpportsequal
SG2124G(config)#mls dos-option udpportsequal
SG2124G(config)#mls dos
SG2124G(config)#
SG2124G(config)#show running-config | include mls
mls qos enable
mls dos
mls dos-option sipequaldip
mls dos-option macsaequalmacda
mls dos-option icmpfragments
mls dos-option udpportsequal
mls dos-option tcpportsequal
mls dos-option tcpflagssf
mls dos-option tcpflagsfup
```

```
SG2124G(config)#
```



1. **mls dos** 기능을 활성화하는 경우 차단된 트래픽에 대한 로그는 기록되지 않기 때문에 차단되는 **Packet**에 대해 **Monitoring**할 수 있는 방법이 없습니다.
2. 활성화할 수 있는 **Option**에 포함되는 특정 **Application**들을 사용하는 경우 사용에 문제가 발생할 수 있으니 설정 시 주의하시기 바랍니다.

2.10.9 IP Source Guard

IP Source Guard 는 IP Spoofing 공격을 차단하는 기능입니다. DHCP 서버에 의해 IP 주소를 할당 받지 않은 장비는 통신을 막기 때문에 DHCP Snooping 기능과 함께 동작합니다. 우선순위는 ACL 보다 높으며, etherchannel은 지원되지 않습니다. 최대 IP 120개까지 지정 가능합니다.

IP Source guard를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
ip verify source <i>PORTRANGE</i>	CONFIG	ip source guard를 설정합니다. (Untrust interface에 설정)
ip source binding <i>IP_Addr</i> interface <i>IFNAME</i>	CONFIG	IP 주소를 수동으로 바인딩 합니다.

설정된 IP Source guard를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show ip verify source	TOP	ip 주소 바인딩 인터페이스를 확인합니다.
show ip source binding [dhcp-snooping static]	TOP	ip 주소 바인딩 내역을 확인합니다.

IP Source guard를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no ip verify source <i>PORTRANGE</i>	CONFIG	ip source guard를 해제합니다.
ip source binding <i>IP_Addr</i> interface <i>IFNAME</i>	CONFIG	바인딩된 IP 주소를 삭제합니다.

<예제> IP Source guard 설정

```
SG2124G(config)#ip verify source ge5-6
SG2124G(config)#ip source binding 192.168.1.10 interface ge5
SG2124G(config)#end

SG2124G#show ip verify source
```

Interface	Filter-Type
-----	-----
ge1	none
ge2	none
ge3	none
ge4	none
ge5	ip filter
ge6	ip filter
ge7	none
ge8	none
ge9	none
ge10	none
ge11	none
ge12	none
ge13	none
ge14	none
ge15	none
ge16	none
ge17	none
ge18	none
ge19	none
ge20	none
ge21	none
ge22	none
ge23	none
ge24	none
xe1	none
xe2	none

SG2124G#show ip source binding

Total binding entry count : 2

IpAddress	MacAddress	Lease(Sec)	Type	VLAN	Interface
-----	-----	-----	-----	-----	-----
192.168.1.10	-	infinite	static	-	ge5
192.168.1.11	0021.9b08.9a66	3516	dhcp-snooping	1	ge6

SG2124G#show running-config

```
!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
mls qos enable
mds enable ge1-20 detect
mds uplink ge21-24,xe
mds self-loop-detect ge1-20
bridge 1 pvstp vlan 1
no bridge 1 pvstp enable bridge-forward bpdu-flood
!
ip dhcp snooping
ip dhcp snooping vlan 1
```

```

ip verify source ge5-6
ip source binding 192.168.1.10 interface ge5
!
interface ge1
!
interface ge2
!
interface ge3
!
interface ge4
!
interface ge5
!
interface ge6
!
-- 이하 생략 --

```



참고

1. PC가 직접 연결되는 최종단 **Access** 스위치에서만 **IP Source Guard** 기능을 활성화 하시기 바랍니다.
2. **IP Source Guard**가 활성화된 상태에서 재부팅할 경우, DHCP를 통해 할당받지 않은 IP주소는 모든 통신이 차단됩니다.
3. 최종단 **Access** 스위치가 아닐경우, 스위치가 리부팅되어도 PC에서 DHCP 요청을 하지 않으므로 통신이 차단될 수 있습니다.
4. SG2024 Series, SG2200 Series, SG2128G Series, SG2128GX Series, SG2152G Series, SG2152GX Series 제품은 **IP Source Guard** 기능을 지원하지 않습니다.(해당 제품은 DHCP Unleased-ip 기능을 이용하시기 바랍니다)
5. **IP Source Guard** 기능은 **Switch버전 2.x** 이상에서만 지원합니다.

2.11 MDS

2.11.1 MDS 개요

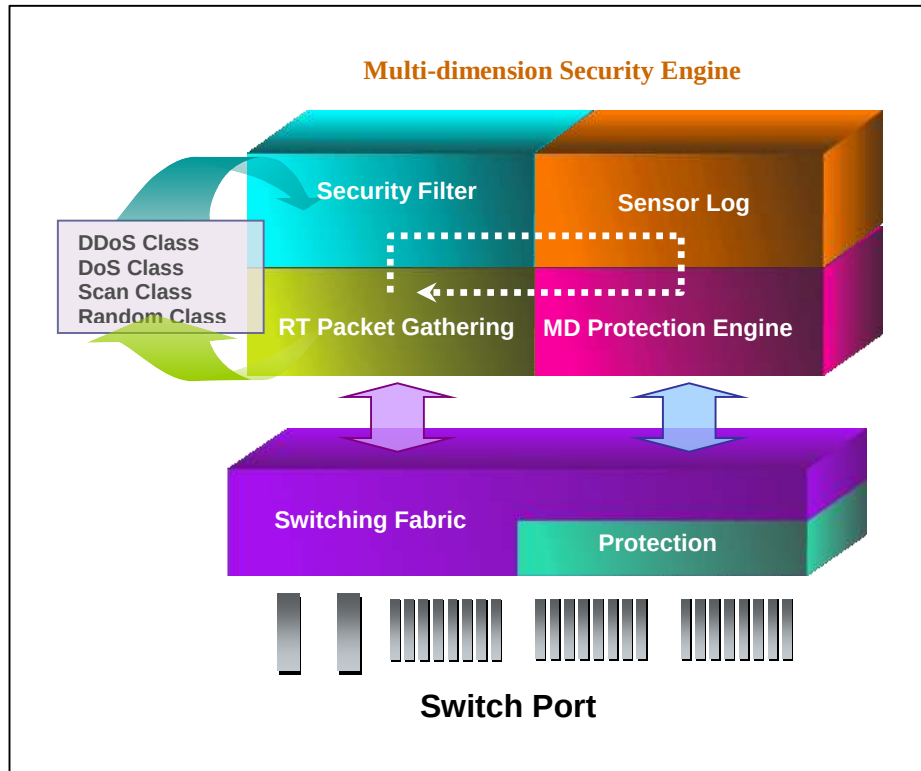
Switching Fabric을 통해 전송되는 Traffic은 동시에 MDS Engine에 전달되고, MDS Engine은 Traffic의 양과 시간을 한 축으로 하고 Host와 TCP/UDP Port별 보안 상황 정보를 한 축으로 하여 Traffic을 분석합니다.

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

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

DoS, DDoS, Flooding등의 유해Traffic이 발생하는 경우 실시간으로 공격을 차단하나, SCAN 유형의 경우에는 Traffic의 변화 추이를 확인한 후 차단합니다. MDS Engine에서 생성된 보안 필터로 인해 차단된 Traffic은 공격자로부터 같은 유형의 공격이 더 이상 발생하지 않으면 생성됐던 보안 필터를 자동으로 해제합니다.

[그림 2-8] MDS Engine



MDS 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds uplink <i>IFNAME</i>	CONFIG	mds를 enable하기 위해 Uplink Interface를 지정합니다. (Default: ge1-4,)
mds enable <i>IFNAME</i> {drop detect}	CONFIG	mds를 enable하기 위해 User Interface를 지정합니다. (Default: SG2124 : ge1-24 detect, SG2148G : ge1-48 detect)
mds mode-button enable	CONFIG	전면 Mode 버튼을 사용하여 MDS Mode를 변경할 수 있도록 합니다.
mds ddos [disable router-safe disable]	CONFIG	ddos disable 시 IP Spoofing을 차단하지 않습니다. router-safe disable 시 Router (Gateway) 차단 방지 기능을 사용하지 않습니다.
mds log-server <i>IP-Addr</i> [<i>Port_No</i>]	CONFIG	VNM Server의 IP Address를 설정합니다.
mds syslog enable	CONFIG	mds를 통해 차단된 event를 syslog에 기록합니다.

mds dad-attack <i>PORTRANGE</i> {detect drop} <10-180>	CONFIG	mds IPv6 DAD attack 탐지를 enable 합니다.
mds policy-act {host-drop icmp tcp udp} { <i>DST_IP_Addr</i> any fixed} { <i>SRC_PORT</i> any fixed} { <i>DST_PORT</i> any fixed} {cancel detect drop pps qos ratelimit <64-1000000>}	CONFIG	mds를 통해 탐지된 내역의 처리를 설정 합니다.
mds threshold {icmp <50- 100000> tcp <100-1000000> udp <100-100000>} <5- 3600>	CONFIG	mds threshold를 설정합니다.
mds self-loop-detect [<i>PORTRANGE</i> timeout <5- 300>]	CONFIG	Self-Loop 차단 기능을 사용할 Port Range와 Loop 해제 시 Timeout 을 설정합니다. (Default Timeout : 30 Sec)
mds arp-spoofing [detect drop] <i>PORTRANGE</i>	CONFIG	mds arp-spoofing 차단기능을 설정합니다.
mds arp-spoofing-detect <i>PORTRANGE</i>	CONFIG	mds arp-spoofing 을 Detect할 Interface를 지정합니다.
mds arp-spoofing-mac-safe [<i>MAC</i> <i>MAC**</i> any oui]	CONFIG	arp-spoofing기능 탐지 시 지정한 MAC 주소나 OUI를 더 세밀하게 확인합니다.
mds arp-spoofing-permit-mask <1-24>	CONFIG	arp-spoofing 기능 사용 시 동일한 IP 대역 내에서만 동작하도록 Permit MASK를 설정합니다.
mds detect-port-range disable	CONFIG	MDS Detect시 탐지된 Service Port 범위만 차단하도록 하는 기능을 해제합니다.
mds arp-table <i>MAC A.B.C.D</i>	CONFIG	mds 에서 arp 탐지 시 신뢰할 수 있는 MAC 과 IP를 고정할 경우 사용합니다
mds arp-list send-port all	CONFIG	모든 up/down 포트에서 수집되는 ip 정보를 log-server와 vipm-server에 전송하도록 설정합니다.
mds attack-crc disable	CONFIG	Packet의 check sum이 동일하게 반복적으로 검출 시 DoS Attack으로 차단하는 기능으로 Default Enable 상태로 기능 해제 시 사용합니다.
mds attack-fragment enable	CONFIG	IP Protocol의 Fragment 조작에 대한 공격 방어기능을 활성화 합니다. (Default: Disable)
mds attack-smurt enable	CONFIG	ICMP Protocol이며, 목적지 MAC 주소

		가 Broadcast일 경우 차단합니다.
mds dhcp-filter disable	CONFIG	dhcp filter 기능을 활성화 하였을 때, Log를 mds log로 표시합니다. (Default: Enable)
mds icmp-redirect	CONFIG	ICMP Redirect 공격을 탐지합니다.
mds if-pkt-loss <i>PORTRANGE</i> threshold	CONFIG	Interface에서 설정한 threshold 값보다 많은 Packet Loss가 발생 시 mds log로 표시합니다.
mds mac-flooding [enable <i>PORTRANGE</i> <1-8192> <1-8192> <1-1000> maximum <1-8192> trust [<i>IFNAME</i> any] <MAC MAC*> MAC/MASK>]	CONFIG	MAC Flooding 차단 시 사용할 Port Range와 Port당 허용할 MAC 개수, Port당 최대 허용할 MAC 개수, Port당 허용할 MAC개수가 초과한 경우 최대 허용할 MAC 개수까지 도달할 때 초당 Learning을 허용할 MAC 개수 및 신뢰할 수 있는 Interface와 MAC을 지정합니다.
mds web-alert attacker [<i>SIP</i> <i>SMAC</i>]	CONFIG	mds에서 web-alert을 사용할 기준을 설정합니다 (Default: Source MAC)
mds web-alert domain-match <i>DOMAIN</i>	CONFIG	DNS를 Match할 Domain Address를 지정합니다.
mds web-alert enable [alert-per-attack alert-per-day <i>A.B.C.D</i> < 1-65535> localhost [auto en ja ko]]	CONFIG	WEB-Alert 기능을 설정합니다 (주기 및 언어 등을 설정합니다. 주기의 Default는 alert-per-day 입니다)
mds web-alert except-port <i>PORTRANGE</i>	CONFIG	경고창을 보여주지 않을 Interface를 설정합니다.
mds web-alert [test-ip <i>A.B.C.D</i> test-mac <i>MAC</i>]	CONFIG	경고창이 정상으로 동작하는 지 확인할 수 있습니다.
mds update web-alert [<i>A.B.C.D</i> <i>IPv6_Addr</i>] <i>FILENAME</i> <i>ID</i> <i>Passwd</i> [port <i>Port_Num</i>]	CONFIG	FTP를 이용하여 MDS WEB-Alert page를 변경할 수 있습니다. (MAX : 32Kbyte)
mds ipm-server <i>A.B.C.D</i> bootmode [last-flash server]	CONFIG	VIPM Server 의 IP와 동작 mode를 설정합니다.
mds ipm-port <i>PORTRANGE</i>	CONFIG	VIPM에서 관리한 Interface를 지정합니다.
mds ipm-collision [disable stress <1-10>]	CONFIG	VIPM Solution과 연동 시에 사용하며 미인증 IP 차단 후 해당 IP로 ARP 충돌 Message를 보낼 때 사용합니다.
mds ipm-guard-to-mac-security disable	CONFIG	VIPM Solution 연동기능으로 IP고정(탐

		지전용)으로 IP 등록 시 Router IP 보호 기능을 사용하지 않을 경우 사용합니다.
mds ipm-interface [<i>IFNAME</i> <i>mgmt</i>]	CONFIG	VIPM Server와 연결 시 다수의 VLAN 이 존재할 경우 불특정 VLAN 정보로 접속하는 것을 막고 지정한 Interface로 통신을 하도록 할 때 사용합니다.
mds ipm-local-dhcp	CONFIG	미인증 사용자 차단 시 DHCP로 운용되는 환경에서 임시 IP를 대여하여 WEB 을 이용한 사용자 인증신청이나 Message 출력기능을 사용할 수 있습니다. (Default: disable)
mds ipm-range-over-msg-disable	CONFIG	VIPM 에서 등록되지 않은 IP 대역 사용 시 차단 Message 기능을 Disable 합니다.
mds ipm-permit [IP IP-Address/M vlan < VLAN-ID range VLAN_RANGE>]	CONFIG	VIPM Server와 연동하여 사용하는 기능으로 특정 조건에서 IP대역 혹은 VLAN 정보를 이용하여 IP관리를 제외하는 경우 사용합니다.
mds permit cpu [icmp tcp udp] [A.B.C.D A.B.C.D/M any] <1-1000 pps>	CONFIG	CPU로 들어오는 Attack성 Traffic을 Permit하는 기능으로 지정한 PPS 만큼 허용합니다.
mds permit sender-arp [Sender_MAC Sender_MAC_MASK OUI]	CONFIG	ARP 탐지 시 Sender MAC을 보호하는 기능으로 Sender_MAC 지정 시 탐지되는 ARP Packet은 Skip 하는 기능입니다.
mds permit mac PORTRANGE [MAC MAC/MASK any] [MAC MAC/MASK any] [MSG ratelimit <64-100000 kbps> vlan <1-4094> [MSG ratelimit <64-100000 kbps>		MDS의 예외정책을 MAC 주소를 기준으로 설정합니다.
mds permit log-server	CONFIG	VNM Log Server의 IP 를 예외 처리합니다.
mds permit arp PORTRANGE [MAC MAC/MASK any] [A.B.C.D A.B.C.D/M any] [MAC MAC/MASK any] [A.B.C.D A.B.C.D/M any] [MSG]	CONFIG	지정한 Interface들에서 들어오는 arp를 설정한 정책에 따라 예외처리 합니다.
mds permit icmp PORTRANGE [A.B.C.D A.B.C.D/M any] [A.B.C.D A.B.C.D/M any] [MSG ratelimit <64-100000	CONFIG	ICMP Protocol에 대하여 예외정책을 설정합니다.

kbps> vlan <1-4094> [MSG ratelimit <64-100000 kbps>]]		
mds permit [tcp tcp-syn udp] <i>PORTRANGE</i> [A.B.C.D A.B.C.D/M any] [A.B.C.D A.B.C.D/M any] [<0-65535> any] [MSG ratelimit <64-100000 kbps> vlan <1-4094> [MSG ratelimit <64-100000 kbps>]]	CONFIG	TCP, TCP-SYN, UDP Protocol에 대하여 예외정책을 설정합니다.
mds permit raw <0-255> [A.B.C.D A.B.C.D/M any] [A.B.C.D A.B.C.D/M any] [MSG ratelimit <64-100000 kbps> vlan <1-4094> [MSG ratelimit <64-100000 kbps>]]	CONFIG	IP Protocol Number로 예외정책을 설정합니다.
mds permit any <i>PORTRANGE</i> [A.B.C.D A.B.C.D/M any] [A.B.C.D A.B.C.D/M any] [MSG ratelimit <64-100000 kbps> vlan <1-4094> [MSG ratelimit <64-100000 kbps>]]	CONFIG	특정 IP나 대역으로 예외정책을 설정합니다.
mds permit other	CONFIG	TCP/UDP/ICMP Protocol이 아닌 타 Protocol에 대하여 예외정책을 설정합니다.
mds extended [deny permit] [any icmp raw <0-255> tcp udp] <i>PORTRANGE</i> [SMAC SMAC/MASK any] [SIP SIP/M any] [DMAC DMAC/MASK any] [DIP DIP/M any] [MSG vlan <1-4094> MSG]	CONFIG	mds permit을 세밀하게 적용 시 사용합니다.
mds auto-config [conifg-save]	CONFIG	Auto-Config 기능을 활성화 합니다.

MDS설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mds config	TOP	mds 설정 내역을 확인합니다.
show mds detect-list	TOP	실시간 차단현황을 확인합니다.
show mds detect-list log <i>log_num</i>	TOP	실시간 차단 세부 내역을 확인합니다.
show mds detect-history	TOP	유해Traffic 차단 History Log를 확인합니다.

show mds detect-history log log_num	TOP	유해Traffic 차단 History Log의 세부 내역을 확인합니다.
show mds policy-act	TOP	mds policy-act 내역을 확인합니다.
show mds arp-spoofing-mac- safe	TOP	mds arp-spoofing-mac-safe 내역을 확인합니다.
show mds arp-table	TOP	MDS엔진의 ARP Table을 확인합니다.
show mds extended	TOP	mds extended 설정을 확인합니다.
show mds ipm-safeguard-list	TOP	mds ipm-guard-to-mac-security기능 을 확인합니다.
show mds log-server	TOP	VNM Server의 연결상태를 확인합니다.
show mds mac-block-list	TOP	차단된 MAC Address를 확인합니다.
show mds mac-flooding-trust	TOP	Trust로 지정한 MAC Address를 확인합 니다.
show mds permit	TOP	mds permit으로 지정한 내역을 확인합 니다.
show mds policy-act	TOP	mds policy-act로 설정한 내역을 확인 합니다.
show mds version	TOP	mds version을 확인합니다.
show mds web-alert [domain- list flash list]	TOP	mds web-alert의 세부 Log를 확인합니 다.

MDS설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds uplink IFNAME	CONFIG	Uplink Interface를 삭제합니다.
no mds enable [IFNAME [drop detect]]	CONFIG	유해Traffic 자동 차단 기능을 해제합니 다.
no mds mode-button enable	CONFIG	전면부의 Mode 버튼을 사용하여 MDS Mode를 변경하는 기능을 삭제합니다.
no mds ddos disable	CONFIG	mds ddos 차단 기능을 enable 합니다. (Default)
no mds syslog enable	CONFIG	mds를 통해 차단된 event를 syslog에 기록하지 않습니다. (Default)
no mds dad-attack PORTRANGE {detect drop}	CONFIG	mds DAD attack 탐지를 삭제합니다.

no mds policy-act {host-drop icmp tcp udp} { <i>DST_IP_Addr</i> any fixed} { <i>SRC_PORT</i> any fixed} { <i>DST_PORT</i> any fixed} {cancel detect drop pps qos ratelimit}	CONFIG	mds를 통해 탐지된 내역의 처리를 초기화 합니다.
no mds threshold {icmp tcp udp}	CONFIG	mds threshold 설정을 삭제합니다
no mds arp-list send-port all	CONFIG	모든 up/down 포트에서 수집되는 ip 정보를 전송하는 기능을 해제합니다
no mds arp-spoofing [detect drop] <i>PORTRANGE</i>	CONFIG	ARP-Spoofing 기능의 설정을 해제합니다
no mds arp-spoofing-detect <i>PORTRANGE</i>	CONFIG	arp-spoofing-detect Port를 해제합니다
no mds arp-spoofing-mac-safe [<i>MAC</i> <i>MAC/MASK</i> any oui [<i>OUI</i>]]	CONFIG	arp-spoofing-mac-safe 기능을 해제합니다
no mds arp-spoofing-permit-mask	CONFIG	arp-spoofing-permit-mask 기능을 해제합니다
no mds arp-table [<i>MAC</i>] [<i>A.B.C.D</i>]	CONFIG	arp-table 지정을 해제합니다
no mds [attack-crc disable attack-fragment enable attack-smurf enable]	CONFIG	attack-crc, attack-fragment, attack-smurf 설정을 해제합니다
no mds detect-port-range disable	CONFIG	detect-port-range 명령을 해제합니다
no mds dhcp-filter disable	CONFIG	dhcp-filter 설정을 해제합니다
no mds extended [all comment MSG]	CONFIG	extended 정책설정을 모두 해제합니다.
no mds extended [deny permit] [any icmp tcp udp raw <0-255>] <i>PORTRANGE</i> [<i>MAC</i> <i>MAC/MASK</i> any] [<i>A.B.C.D</i> <i>A.B.C.D/M</i> any] [<0-65535> any] [<i>MAC</i> <i>MAC/MASK</i> any] [<i>A.B.C.D</i> <i>A.B.C.D/M</i> any]] [<0-65535> any] vlan <1-4094>	CONFIG	extended로 설정한 deny, permit 정책을 해제합니다
no mds icmp-redirect	CONFIG	icmp-redirect 기능을 해제합니다
no mds if-pkt-loss [<i>PORTRANGE</i> threshold]	CONFIG	if-pkt-loss 설정을 해제합니다
no mds ipm-server	CONFIG	ipm-server 설정을 해제합니다

no mds ipm-port <i>PORTRANGE</i>	CONFIG	ipm-port 설정을 해제합니다
no mds ipm-range-over-msg-disable <i>PORTRANGE</i>	CONFIG	ipm-range-over-msg-disable 기능을 해제합니다.
no mds ipm-collision [disable stress]	CONFIG	ipm-collision 기능의 설정을 해제합니다
no mds ipm-guard-to-mac-security disable	CONFIG	ipm-guard-to-mac-security 설정을 해제합니다
no mds ipm-interface	CONFIG	ipm-interface 설정을 해제합니다
no mds ipm-permit [ip [<i>A.B.C.D</i> <i>A.B.C.D/M</i>] <i>A.B.C.D</i> vlan [<i><1-4094></i> range <i>RANGE</i>]	CONFIG	ipm-permit 설정을 해제합니다
no mds ipm-local-dhcp	CONFIG	ipm-local-dhcp 설정을 해제합니다
no mds log-server <i>A.B.C.D</i> <i><1-65535></i>	CONFIG	log-server 설정을 해제합니다
no mds mac-flooding [enable <i>PORTRANGE</i> maximum trust [<i>IFNAME</i> <i>MAC MAC/M</i> any]]	CONFIG	mac-flooding 기능을 해제합니다.
no mds self-loop-detect [<i>PORTRANGE</i> timeout]	CONFIG	self-loop-detect 기능을 해제합니다.
no mds web-alert [attacker domain-match <i>DOMAIN</i> enable except-port <i>PORTRANGE</i> test-ip <i>A.B.C.D</i> test-mac <i>MAC</i>]	CONFIG	web-alert 기능을 해제합니다



참고

1. Uplink Interface 및 User Interface에 대한 설정은 내/외부 Network를 구분하여 유해Traffic을 차단하기 위해 설정합니다.
2. Uplink Interface를 User Interface 쪽에 설정한 경우 외부로부터의 공격 발생 시 공격의 유형에 따라 상단에 설치되어 있는 Network 장비의 MAC을 차단 할 수 있으므로, 반드시 Uplink Interface를 User Interface와 구분하여 설정하시기 바랍니다.

2.11.2 Network 공격의 유형

■ DoS (Denial of Service)

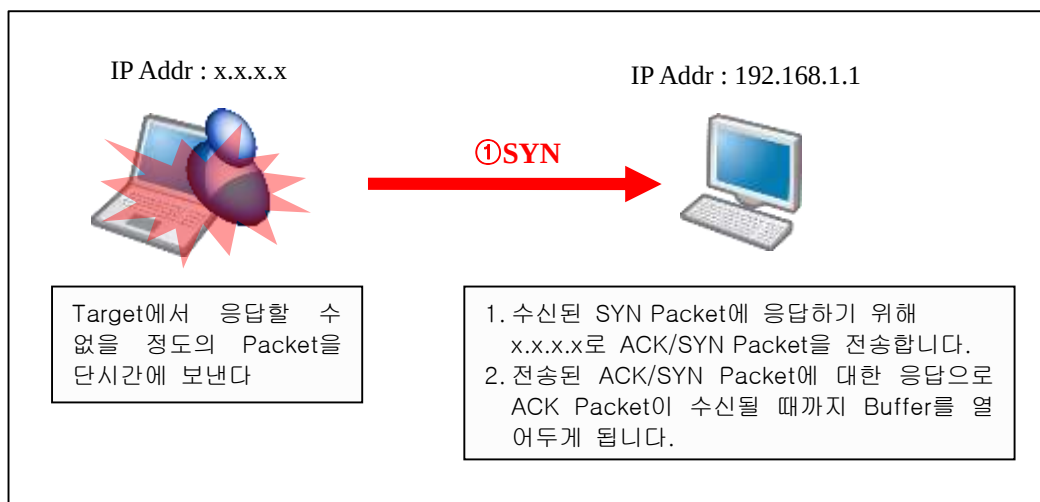
DoS는 한 사용자가 특정 시스템의 리소스를 독점하거나 모두 사용해버리거나 파괴함으로써 다른 사용자들이 이 시스템의 서비스를 올바르게 사용할 수 없도록 만드는 것을 말합니다. 그러므로 시스템의 정상적인 수행에 문제를 일으키는 모든 행위를 **DoS**라 할 수 있으며, 웹 Server나 Router, Network 기반 시설이 공격 대상인 경우가 대부분입니다.

DoS 공격이 발생하는 방법은 매우 다양하기 때문에 고의적으로 발생할 수 있지만 사용자의 의도와는 무관하게 발생할 수도 있습니다. DoS 공격은 Root 권한 획득, 시스템 사용자 Data의 파괴 및 변조 등을 시도함으로써 시스템에 치명적인 문제를 일으키지는 않지만 Network나 서비스 등이 마비되는 등의 문제를 일으킵니다.

공격자는 과다한 서비스 요구를 통해 대상 장비의 중요 서비스의 중단을 초래할 수 있습니다. 예를 들어 공격자가 1 s당 10개의 Mail을 받을 수 있는 Server에 초당 20개의 Mail을 보내면 공격 대상이 된 Mail Server는 제대로 전송하지 못할 것이며 20개보다 훨씬 많은 Mail을 보낼 경우엔 Server가 Down될 수도 있는 것입니다.

DoS/DDoS 공격자는 서비스 제공만을 방해할 뿐 Data를 직접적으로 파괴하지는 않지만, 이 공격을 바람잡이처럼 사용해 Server 침입이라는 실질적인 공격을 숨기는 경우도 있습니다.

[그림 2-9] DoS 공격의 형태



■ 분산 서비스 거부 공격 (DDoS, Distributed Denial of Service)

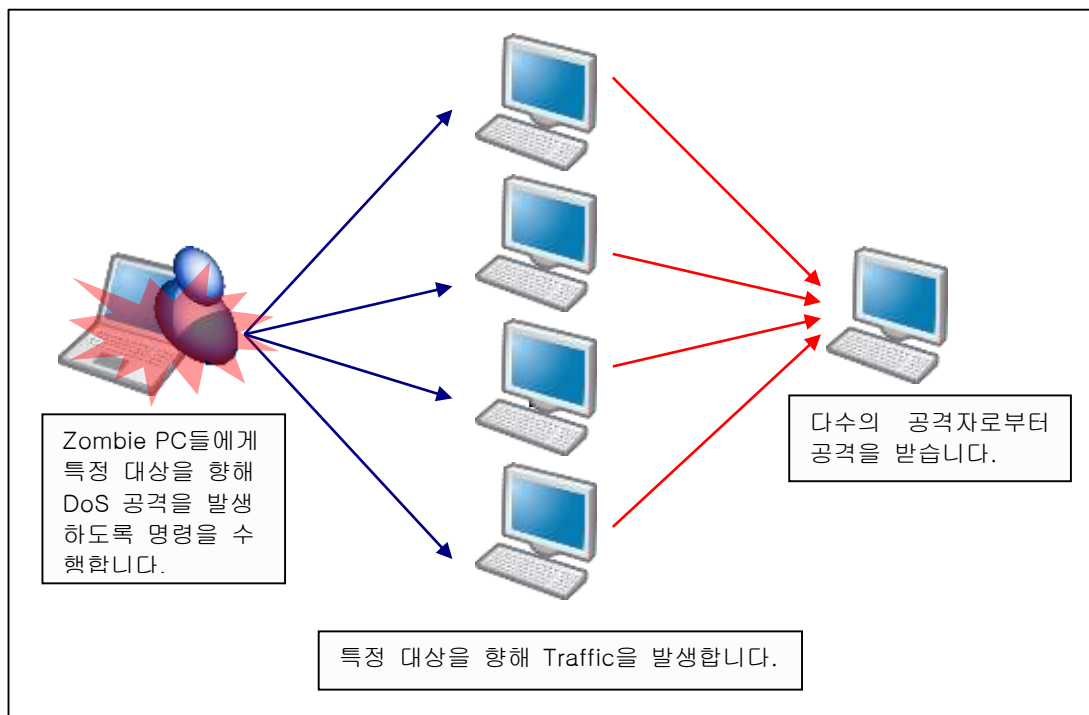
DDoS (Distributed Denial of Service)는 한 대의 컴퓨터가 아니라 100대 또는 1000대의 컴퓨터가 공격하는 것, 즉 공격자(attacker)가 하나가 아닌 다수인 것이 특징입니다.

BotNet의 경우 각 PC에 Bot이라는 악성 코드를 설치해 은폐한 후, 감염된 PC들에게 원격의 공격자가 특정 공격 대상에 대해 특정 시간에 특정 패턴으로 공격 명령을 내리면 감염된 PC들은 자신이 공격을 하는지도 알지 못한 채 Spam Mail을 발송하거나 유해Traffic을 발생하게 됩니다.

DDoS 공격의 명령을 내리는 공격자가 Zombie PC들에게 유해Traffic 발생량을 높이도록 명령을 내리면 Zombie PC 사용자의 컴퓨터가 느려지면서 이상을 감지하여 백신 등으로 치료할 가능성이 있으므로, 공격자는 유해Traffic 발생량은 낮은 상태로 많은 Zombie PC들에게 명령을 내리는 경우가 많습니다.

자신의 PC가 Network 사용을 별로 하지도 않는데 Network 점유율이 증가(Traffic 공격)하거나, Memory 사용률이 90%이상이며 CPU 사용률이 90~100%를 사용 중(웹 부하 공격)이라면 Virus에 감염되어 Zombie PC로 동작하는 경우일 가능성이 높으니 보안 Patch를 적용하거나 백신 치료를 하시기 바랍니다.

[그림 2-10] DDoS 공격의 형태



■ SCAN 공격

Scan 공격은 주로 대상 컴퓨터를 찾아 내어 어떤 **Service Port**가 **Open**되어 있는지 등을 파악하여 컴퓨터를 해킹하기 위해서 사용하는 공격입니다. **Worm Virus**에 감염된 컴퓨터에서 발생하는 **Traffic**의 전형적인 패턴은 동일한 발신지 **IP** 주소에서 초당 수 만개의 서로 다른 목적지 **IP** 주소로, 동일한 서비스 번호로 전송하는 것이며, 이러한 패턴은 전형적인 **SCAN Traffic** 패턴(즉, 어떤 서비스를 **OPEN**하고 있는 **Host**를 찾는 행위)로 볼 수 있습니다.

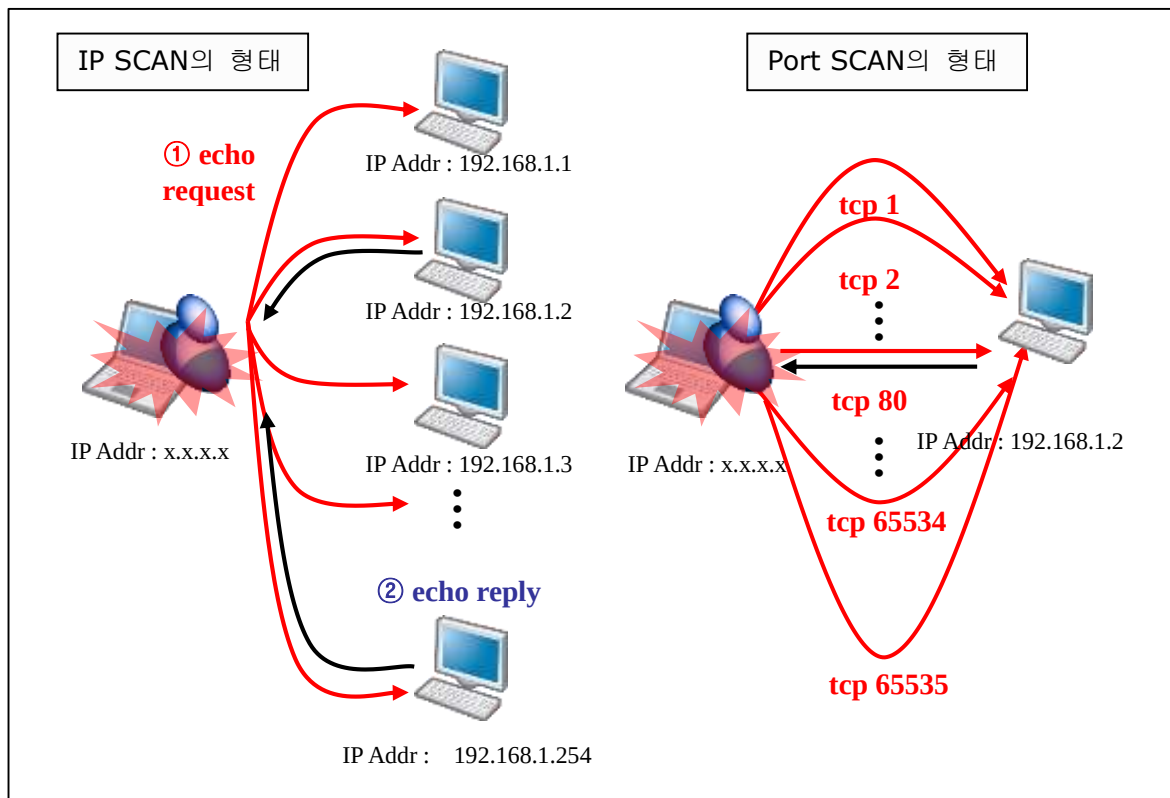
▪ IP Scan 공격

특정 **Network IP** 대역에 대해 어떤 컴퓨터가 현재 동작 중인지를 파악하기 위해 사용됩니다. **ICMP**를 이용하는 경우 특정 **IP** 대역의 모든 **IP**로 **ICMP echo request Packet**를 전송한 후 **ICMP echo reply Packet**이 수신되는지의 여부를 통해 확인할 수 있으나, 내부 **Network**에서 **ICMP**를 사용하지 못하게 설정되어 있는 경우에는 사용할 수 없습니다. **TCP/UDP**를 사용하는 경우에는 특정 **Service Port**를 고정한 **Packet**을 전체 **Network**에 전송하여 해당 **Service Port**가 **Open**되어 있는 컴퓨터를 찾아내는 방법도 있습니다.

▪ Port Scan

특정 대상 컴퓨터를 해킹하기 위해 현재 대상 컴퓨터에서 어떤 **Service**가 **Open**되어 서비스를 하고 있는지 알아내기 위해 하는 방법으로 **Service Port** 번호 0번부터 65535번까지 순차적 또는 무순위로 **Data**를 보내어 **Server**가 **ICMP**로 응답하는 것을 확인합니다.

[그림 2-11] The pattern(type) of SCAN 공격



■ IP Spoofing 공격

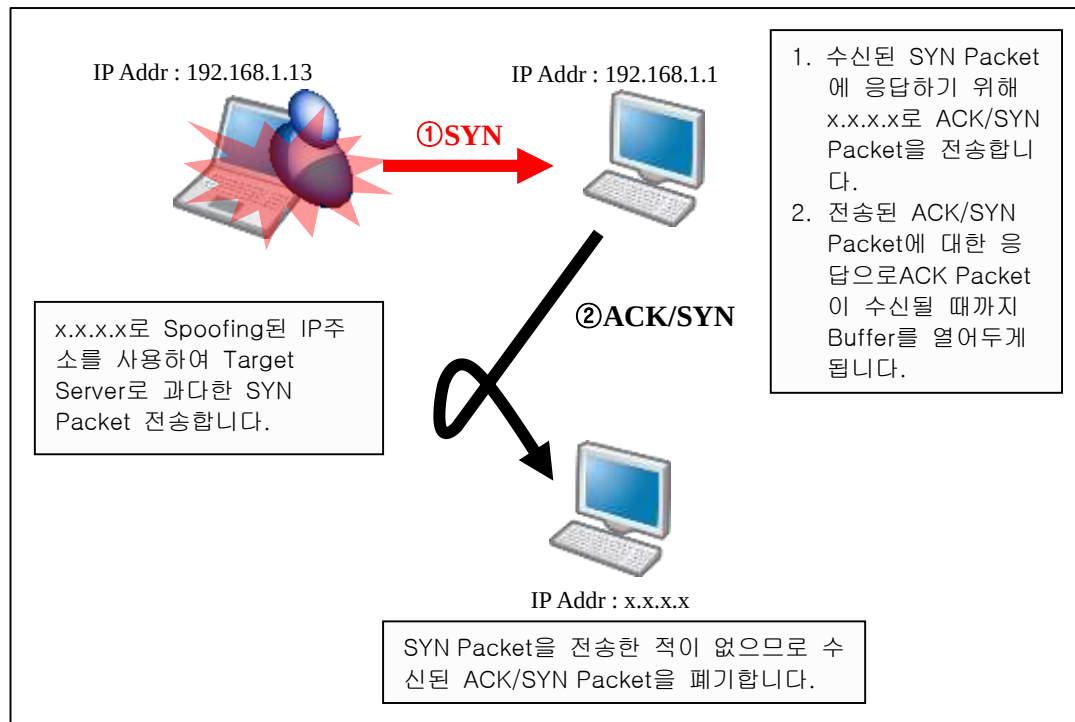
IP Spoofing은 말 그대로 IP 정보를 속여서 다른 시스템을 공격하는 것입니다. IP Spoofing을 통해 공격 대상 장비에 서비스 거부 공격(TCP Syn flooding, UDP flooding, ICMP flooding)을 수행할 수도 있으며, 공격대상 장비와 Server 사이의 연결된 세션에 대해서 세션 끊기도 가능합니다.

TCP/IP 상의 Protocol 취약성인 TCP Sequence Number의 생성이 매초당 일정하게 증가한다는 것과 Host에 대한 인증 시 IP의 소스 주소만을 사용한다는 것을 이용하여 TCP Syn flooding + TCP Sequence Number Guessing + IP Spoofing을 연동한 공격을 할 수 있습니다. Sequence Number는 연결 지향형 Protocol인 TCP Protocol에서 두 Host 간의 Packet 전달이 손실 없이 이루어졌는지 체크하기 위한 일종의 Packet 번호표입니다.

공격자는 클라이언트와 Server와의 통신 사이에 끼어들어 클라이언트를 TCP Syn flooding 서비스 거부 공격으로 반응하지 못하게 한 후, Server의 순서번호를 예측하여 IP Spoofing된 위조 Packet을 발송함으로써 공격자가 이 클라이언트인 것으로 가장하여 Server와 통신하는 기법입니다.

IP 기반의 인증만을 제공하는 서비스들은 이러한 IP Spoofing 공격에 취약합니다.

[그림 2-12] Traffic flow when happening IP Spoofing



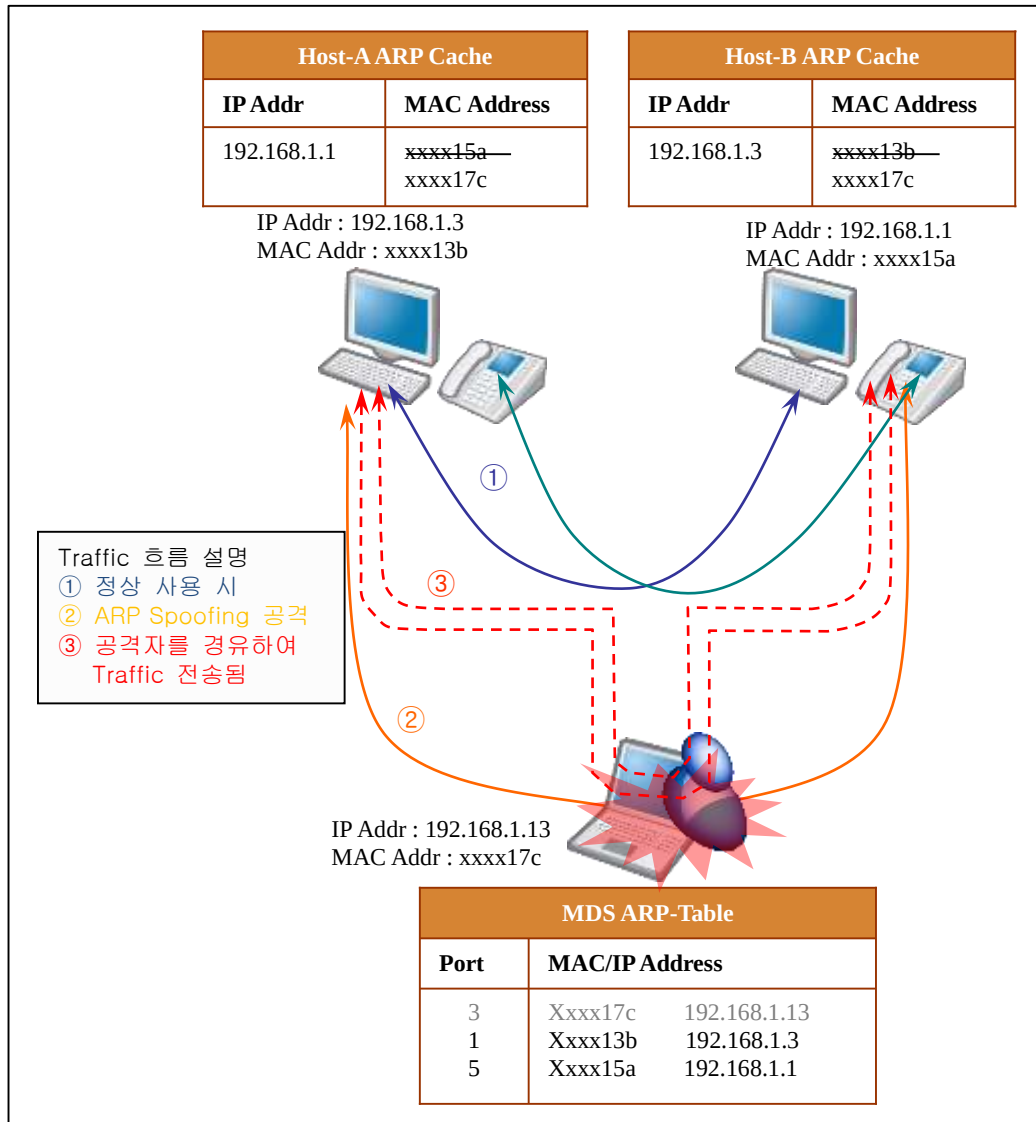
■ ARP Spoofing 공격

ARP란 Layer 2 환경에서 서로의 IP Address를 아는 장치들이 서로의 MAC Address를 알기 위해 사용하는 Protocol로 32bit IP Address를 48bit의 Network 카드 주소(MAC Address)로 대응시켜 주는 Protocol입니다. Layer 2 환경에서는 실제로 장비간의 통신을 위해 서로의 IP Address를 통해 Network 연결을 시도하면 TCP/IP에서는 해당 IP에 해당하는 MAC Address를 찾아 연결하고 Switch는 이 MAC Address를 기반으로 해당 MAC Address를 Learning한 Interface에만 Packet을 전달하게 됩니다. 이러한 IP Address와 MAC Address의 대응되는 정보는 Switch나 기타 Network 장비 및 사용자 컴퓨터에서 ARP Cache Table이라는 곳에 위치하게 됩니다.

예를 들어, PC-A와 PC-B가 통신을 하려면 먼저 PC-A에서 PC-B의 IP Address를 이용해 ARP Request를 전체 Network에 보내고 PC-B는 자신의 MAC Address를 포함한 ARP Reply Packet을 PC-A에게 보낸 후 서로간의 통신이 이루어지게 됩니다.

ARP Spoofing 공격은 로컬 Network(LAN)에서 공격자의 MAC Address를 다른 장비의 MAC Address인 것처럼 속여 공격 대상 장비의 ARP Table 정보를 위조하여 공격 대상 장비와 Server 사이의 Traffic을 공격자 자신의 장비로 우회시킬 수 있습니다. 공격자는 우회된 Traffic으로부터 도청, ID/Password 정보 등 개인 정보를 획득할 수 있습니다.

[그림 2-13] ARP Spoofing 발생 시 Traffic 흐름도



■ DAD 공격

DAD(Duplicated Address Detection)란 IPv6 환경에서 자동적으로 생성하는 link local 주소 혹은 관리자가 설정하는 IPv6 주소에 대해 이 주소를 이미 사용하고 있는 장비가 존재하는지 확인하는 기능입니다. IPv6 주소를 사용하려는 장비가 사용하려는 주소에 대해 DAD NS 메시지를 보내면 이미 그 주소를 사용하고 있는 장비가 있다면 NA 메시지로 응답하며, 아무도 사용하고 있지 않는 주소일 경우에는 응답이 없습니다. DAD NS 메시지를 보냈을 때 그 주소에 대한 NA 응답을 받은 장비는 IP 충돌로 인식하고 해당 IPv6 주소를 사용할 수 없게 됩니다.

DAD 공격은 네트워크 내의 모든 IPv6 주소에 대한 DAD NS 메시지에 대해서 NA 응답을 보냄으로써 네트워크 내의 모든 장비들이 IPv6 주소를 사용할 수 없도록 만듭니다.

2.11.3 MDS 자동 차단 기능 설정 확인

MDS 설정은 Default로 detect Mode가 enable되어 있습니다. MDS 설정상태는 CONFIG 모드에서 확인할 수 있으며, default 설정은 ge23~24를 Uplink Interface, ge1~22를 User Interface로 사용하도록 설정되어 있습니다.

<예제1> Default Config 중 MDS 관련 설정

```
SG2124G#show running-config
!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
bridge 1 protocol pvstp
!
spanning-tree mst config
!
mls qos enable
mds enable ge1-22 detect    → ge1-22 를 User Interface 로 설정 및 detect mode enable
mds uplink ge23-24        → ge23-24 를 Uplink Interface 로 설정
!
-- 이하 생략 --

SG2124G#
```



참고

Uplink Interface를 Default Interface가 아닌 다른 Interface에 연결한 경우, 해당 Interface를 Uplink Interface로 지정해야 합니다.

<예제2> MDS 설정 변경

- ge24 Interface 만 Uplink Interface로 사용
- ge1-23 Interface를 User Interface로 사용
- mds는 차단 모드로 동작하도록 설정

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#no mds enable ge1-22 detect
SG2124G(config)#no mds uplink ge23-24
SG2124G(config)#mds uplink ge24           → ge24 를 Uplink Interface 로 설정
SG2124G(config)#mds enable ge1-23 drop   → ge1-23 을 User Interface 로 설정 및
                                           mds drop mode enable
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
bridge 1 protocol pvstp
!
spanning-tree mst config
!
mls qos enable
mds enable ge1-23 drop
mds uplink ge24
!
-- 이하 생략 --

SG2124G#

```

2.11.4 MDS 실시간 차단 Log 보기

공격자로부터 DoS, DDoS 등의 유해Traffic이 발생하여 MDS Engine에서 유해Traffic으로 탐지되면 Packet Header를 분석하여 공격자와 피해자의 L3, L4 세부정보를 확인한 후 해당 유해Traffic만을 차단하는 보안 필터를 자동으로 생성하여 실시간으로 차단하며, 실시간으로 차단된 유해Traffic의 세부 내역을 확인하여 유해Traffic의 공격 형태 등을 확인할 수 있습니다.

자동 보안 필터의 경우 공격자로부터 유해Traffic과 정상 Traffic이 동시에 발생하는 경우, 발생한 Traffic 중 유해Traffic만을 선별하여 차단(Smart Protection)하며 정상 서비스 Traffic은 차단하지 않고 안전하게 통과시켜 줍니다.

예를 들어, AA IP를 사용하는 컴퓨터가 Virus 감염 등으로 인해 BB IP를 사용하는 컴퓨터에 유해Traffic을 발생시키면서 인터넷을 사용하고 있다면, MDS Engine에서는 AA IP로부터 BB IP로 향하는 DoS 공격은 차단하지만 AA IP로부터 인터넷으로 향하는 Traffic은 차단하지 않고 정상 Forwarding합니다.

생성된 보안 필터의 경우, 일정 시간 동안 공격자로부터 동일한 형태의 유해Traffic이 더 이상 발생하지 않는 경우 보안 필터를 자동으로 해제하여 줍니다.

MDS 실시간 차단 현황을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mds detect-list [log KeyNO]	CONFIG	실시간 차단 내역을 확인합니다.

<예제1> mds detect-list 확인

```
SG2124G#show mds detect-list
```

KeyNo	Phy	SourceIP & MAC	DestIP	Proto	SPort	DPort	SigName	Packet	Action	TimeOut
1	3	100.111.1.2	192.168.254.241	TCP	Any	445	DoS_Attack	51375	DROP	98
2	3	10.21.115.200	Any	TCP	Any	22	Scan_Attack	54290	DROP	174

- KeyNo : MDS 차단 필터 번호
- Phy : 유해Traffic이 발생한 물리적 Interface 번호
- SourceIP & MAC : 출발지 IP 정보 (Spoofing 공격등은 MAC Address로 표시)
- DestIP : 목적지 IP 정보 (Flooding, Scan등의 경우 any로 표시)
- Proto : Protocol Type
- Sport : 출발지 Service 포트
- Dport : 목적지 Service 포트
- SigName : 차단 정책명
- Packet : 탐지/차단된 Packet 수
- Action : 탐지/차단 동작 표시
- TimeOut : 차단 해제를 위해 대기 중인 시간

<예제2> mds detect-list 세부 내역 확인

```

SG2124G#show mds detect-list log 4 → Detect-List 의 KeyNo.
detect code : 4
Sig Name    : (103)Scan_Attack
from Date   : 09/04/15 16:18:28
to  Date    : 09/04/15 16:18:31 (3 Sec)
Phy. Port No: 3
Source MAC   : 0000.0101.0abc
Source IP    : 10.21.115.200
Dest IP      : Any
Protocol     : TCP
Source Port  : Any
Dest Port    : 22
Drop Count   : 13935

  No. SourceIP      DestIP      Proto  SPort  DPort
-----
  1  10.21.115.200  10.134.0.200  TCP    1025   22 6 dup
  2  10.21.115.200  10.134.0.199  TCP    1025   22 6 dup
  3  10.21.115.200  10.134.0.198  TCP    1025   22 6 dup
  4  10.21.115.200  10.134.0.197  TCP    1025   22 6 dup
  5  10.21.115.200  10.134.0.196  TCP    1025   22 6 dup
  6  10.21.115.200  10.134.0.195  TCP    1025   22 6 dup
  7  10.21.115.200  10.134.0.194  TCP    1025   22 6 dup
  8  10.21.115.200  10.134.0.193  TCP    1025   22 6 dup
  9  10.21.115.200  10.134.0.192  TCP    1025   22 6 dup
 10  10.21.115.200  10.134.0.191  TCP    1025   22 6 dup
 11  10.21.115.200  10.134.0.190  TCP    1025   22 6 dup
 12  10.21.115.200  10.134.0.189  TCP    1025   22 6 dup
 13  10.21.115.200  10.134.0.188  TCP    1025   22 6 dup
-- 이하 생략 --

SG2124G#

```

- detect code : 실시간 차단 Log 번호
- Sig Name : 차단 정책명
- from Date, to Date: 유해Traffic 차단 시작 시간 및 현재 시간
- Phy. Port No : 유해Traffic이 발생한 물리적 Interface 번호
- Source MAC : 공격자 MAC Address
- Source IP : 공격자 IP 및 MAC Address 정보
- Dest IP : 목적지 IP 정보 (Flooding, Scan등의 경우 any로 표시)
- Protocol : Protocol Type
- Source Port : 출발지 Service Port
- Dest Port : 목적지 Service Port
- Drop Count : 탐지/차단된 Packet 수

2.11.5 MDS 차단 Log(detect-history) 보기

유해Traffic이 차단된 후 더 이상의 유해Traffic이 발생하지 않으면 일정 시간 후 생성되었던 차단정책이 자동으로 해제됩니다. 자동으로 해제된 Log는 탐지 및 차단(detect-history) Log에 기록되며, Log (detect-history)의 세부 내역을 통해 차단된 유해Traffic의 공격 형태 등을 확인할 수 있습니다.

내부에서 유해Traffic이 지속적으로 발생하는 경우 근원지에 대한 후속 조치(Virus 검사 및 치료, Windows 보안 Update, 악성코드 검사 및 치료) 및 별도 관리가 필요합니다.

MDS 차단 Log history를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mds detect-history [desc]	TOP	차단 history Log를 [최근 Log부터] 확인합니다.
show mds detect-history [/log KeyNO]	TOP	차단 history [세부]Log를 확인합니다.

<예제1> mds detect-history 확인

```
SG2124G#show mds detect-list
```

KeyNo	Phy	SourceIP & MAC	DestIP	Proto	SPort	DPort	SigName	Packet	Action
TimeOut									
1	3	100.111.1.2	192.168.254.241	TCP	Any	445	DoS_Attack	51375	DROP 98
2	3	10.21.115.200	Any	TCP	Any	22	Scan_Attack	54290	DROP 174

- SeqNo : MDS 차단 Log 번호
- Date Time : 최초 차단된 시간
- Phy : 유해Traffic이 발생한 물리적 Interface 번호
- SourceIP & MAC : 출발지 IP 정보 (Spoofing 공격등은 MAC Address로 표시)
- DestIP : 목적지 IP 정보 (Flooding, Scan등의 경우 any로 표시)
- Proto : Protocol Type
- Sport : 출발지 Service Port
- Dport : 목적지 Service Port
- SigName : 차단 정책명
- Packet : 총 차단된 Packet 수
- Action : 탐지/차단 동작 표시

<예제2> mds detect-history 세부 내역 확인

```

SG2124G#show mds detect-history log 4 → Detect-History 의 SeqNo.
detect code : 4
Sig Name    : (103)Scan_Attack
from Date   : 09/04/15 16:18:28
to Date     : 09/04/15 16:23:13 (285 Sec)
Phy. Port No : 3
Source MAC   : 0000.0a01.a1b2
Source IP    : 10.21.115.19
Dest IP      : Any
Protocol     : TCP
Source Port  : Any
Dest Port    : 25
Drop Count   : 1208342

  No. SourceIP      DestIP      Proto  SPort  DPort
  ---
  1  10.21.115.19    10.134.0.200 TCP     1025   25 6 dup
  2  10.21.115.19    10.134.0.199 TCP     1025   25 6 dup
  3  10.21.115.19    10.134.0.198 TCP     1025   25 6 dup
  4  10.21.115.19    10.134.0.197 TCP     1025   25 6 dup
  5  10.21.115.19    10.134.0.196 TCP     1025   25 6 dup
  6  10.21.115.19    10.134.0.195 TCP     1025   25 6 dup
  7  10.21.115.19    10.134.0.194 TCP     1025   25 6 dup
  8  10.21.115.19    10.134.0.193 TCP     1025   25 6 dup
  9  10.21.115.19    10.134.0.192 TCP     1025   25 6 dup
 10  10.21.115.19    10.134.0.191 TCP     1025   25 6 dup
-- 이하 생략 --

SG2124G#

```

- detect code : 실시간 차단 Log 번호
- Sig Name : 차단 정책명
- from Date, to Date: 유해Traffic 차단 시작 시간 및 종료 시간
- Phy. Port No : 유해Traffic이 발생한 물리적 Interface 번호
- Source MAC : 공격자 MAC Address
- Source IP : 공격자 IP 및 MAC Address 정보
- Dest IP : 목적지 IP 정보 (Flooding, Scan등의 경우 any로 표시)
- Protocol : Protocol Type
- Source Port : 출발지 Service Port
- Dest Port : 목적지 Service Port
- Drop Count : 탐지/차단된 Packet 수

2.11.6 MDS Permit

Switch 내부 Network의 Traffic 중 특정 IP, Service Port로 발생하는 특정 Traffic에 대해서는 어떠한 경우에도 차단하지 않도록 설정할 수 있습니다. 예외처리에 등록된 IP 또는 Service Port로 발생하는 특정 Traffic의 경우 DoS, Flooding 등의 공격 Traffic이 발생하여도 차단하지 않습니다.

특정 Traffic에 대해서 MDS Engine에서 차단하지 않도록 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds permit {any arp icmp log-server mac other raw tcp tcp-syn udp} PORTRANGE {any SIP SIP/mask} {any DIP DIP/mask } {any <0-65535>} [Comment ratelimit <64-100000> vlan VLANID]	CONFIG	MDS Engine에서 차단하지 않을 Traffic의 유형을 지정합니다
mdsv6 permit {any icmp mac raw tcp udp} PORTRANGE {any SIP SIP/mask} {any DIP DIP/mask } Comment	CONFIG	MDSv6 Engine에서 차단하지 않을 Traffic의 유형을 지정합니다
mds permit cpu {icmp tcp udp} [SIP SIP/mask any] <1-1000>	CONFIG	CPU로 들어오는 공격성 Traffic을 Permit 하는 기능으로 설정한 PPS 만큼 허용합니다 (Default: Disable)
mds permit sender-arp [Sender_MAC Sender_MAC_Mask OUT]	CONFIG	ARP 탐지 시 Sender MAC을 보호하는 기능으로 Sender MAC 지정시 해당 MAC에서 탐지되는 ARP Packet을 Skip 합니다
mds log-server	CONFIG	VNM Server의 IP 주소를 예외 처리합니다.

MDS Engine에서 permit으로 설정된 내역을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mds permit	CONFIG	MDS Engine에서 차단하지 않도록 설정된 Traffic 유형 및 Counter를 확인합니다.
show mdsv6 permit	CONFIG	MDS Engine에서 IPv6 주소로 차단하지 않도록 설정된 Traffic 유형 및 Counter를 확인합니다

MDS Engine에서 항상 차단하지 않도록 설정된 내역을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds permit {any arp icmp log-server mac other raw tcp tcp-syn udp} <i>PORTRANGE</i> {any <i>SIP</i> <i>SIP/mask</i> } {any <i>DIP</i> <i>DIP/mask</i> } {any <0-65535>} [vlan <i>VLANID</i>]	CONFIG	MDS Engine에서 차단하지 않도록 설정된 Traffic 유형을 초기화합니다.
no mds permit cpu {icmp igmp tcp udp} {any <i>SIP/Mask</i> } <1-1000>	CONFIG	MDS Engine에서 CPU로 들어오는 packet의 예외처리를 초기화 합니다.
no mdsv6 permit {any icmp mac raw tcp udp} <i>PORTRANGE</i> {any <i>SIP</i> <i>SIP/mask</i> } {any <i>DIP</i> <i>DIP/mask</i> }	CONFIG	MDS Engine에서 IPv6 주소를 기준으로 차단하지 않도록 설정된 Traffic 유형을 초기화합니다.
no mdsv6 permit {any icmp mac raw tcp udp} <i>PORTRANGE</i> {any <i>SIP/mask</i> } {any <i>DIP/mask</i> }	CONFIG	MDSv6 Engine에서 차단하지 않도록 설정된 Traffic 유형을 초기화합니다.
clear mds {all KeyNo.}	TOP	실시간 차단내역이 동작하는 경우 강제로 차단 정책을 해제 합니다.



참고

1. 내부 DNS Server의 경우 외부 DNS Server와 DNS 정보 Update를 위한 통신이 이루어질 때 Flooding 공격의 형태로 Update를 진행하는 경우가 있습니다. 이런 경우, 내부 DNS Server로부터 발생하는 DNS Query에 대해 차단하지 않도록 설정할 수 있습니다.
2. MDS Engine에서 유해Traffic으로 인지하여 차단 정책이 생성되어 동작중인 상태에서는 MDS 예외 정책을 생성하여도 바로 예외로 적용되지 않습니다.
3. 현재 차단중인 Traffic에 대해 예외 정책을 적용하려면 다음 순서로 적용하시기 바랍니다.
 - show mds detect-list : 예외 처리할 Traffic의 KeyNo. 확인
 - mds permit Proto SIP DIP DPORT : 예외 정책 생성
 - clear mds KeyNo. : 차단정책 강제 해제

<예제> 목적지 IP 192.168.1.10 Server의 TCP 80 Port에 대한 MDS 예외 설정

```
SG2124G(config)#mds permit tcp any 192.168.1.10 80
```

```
SG2124G(config)#end
```

```
SG2124G#
```

```
SG2124G#show running-config
```

```
!
```

```
service password-encryption
```

```
!
```

```
username root password *****
```

```
!
```

```
ip domain-lookup
```

```
!
```

```
bridge 1 protocol pvstp
```

```
!
```

```
spanning-tree mst config
```

```
!
```

```
mls qos enable
```

```
mds enable ge1-22 detect
```

```
mds uplink ge23-24
```

```
mds permit tcp any 192.168.1.10 80
```

```
!
```

```
-- 이하 생략 --
```

```
SG2124G#
```

```
SG2124G#show mds permit
```

```
MDS permit information.
```

```
=====
```

```
Src_Ports
```

```
Protocol      Source ip/mac Destination ip/mac Dport Vlan Count      Comment      Rate
```

```
=====
```

```
tcp           any          192.168.1.10    80  12542
```

```
SG2124G#
```

<예제> 목적지 IP 2001::1 Server의 TCP 80 Port에 대한 MDS 예외 설정을 ge1-ge10 포트에 적용하는 예

```
SG2124G(config)#mdsv6 permit tcp ge1-10 any 2001::1/128 80
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
bridge 1 protocol pvstp
!
spanning-tree mst config
!
mls qos enable
mds enable ge1-22 drop
mds uplink ge23-24
mdsv6 permit tcp ge1-10 any 2001::1/128 80
!
-- 이하 생략 --
```

```
SG2124G#
SG2124G#show mds permit
MDS permit information.
=====
Src_Ports
Protocol      Source ip/mac Destination ip/mac Dport Vlan Count   Comment      Rate
=====
ge1-10
  tcp  any      2001::1/128      80  0
SG2124G#
```



참고

1. 특정 유형의 Traffic에 대해 유해Traffic 예외 처리로 등록하게 되면 예외 처리된 유형의 공격이 발생하는 경우에도 차단하지 않습니다.
2. 예외 처리할 Traffic의 유형을 세분화해서 설정하지 않으면 전체 Network에 심각한 위협이 될 수 있으니, 꼭 필요한 Network만 등록하여 사용하시기 바랍니다.

2.11.7 MDS Extended Permit / Deny

Switch 내부 Network의 Traffic 중 특정 Source MAC, IP, Service Port에서 특정 Destination MAC, IP, Service Port로 발생하는 Traffic에 대해서 MDS 엔진을 통해 어떠한 경우에도 허용 또는 차단하도록 설정할 수 있습니다.

특정 Traffic에 대해서 MDS Engine에서 허용 또는 차단하도록 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds extended {deny permit} {any icmp raw tcp udp} {any SMAC} {any SIP} {any SPort} {any DMAC} {any DIP} {any DPort} [Comment]	CONFIG	MDS Engine에서 허용 또는 차단할 Traffic의 유형을 지정합니다.
clear mds {all KeyNo.}	TOP	실시간 차단내역이 동작하는 경우 강제로 차단 정책을 해제 합니다.

MDS Engine에서 extended로 설정된 내역을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mds extended permit	CONFIG	MDS Engine에서 차단하지 않도록 설정된 Traffic 유형 및 Counter를 확인 합니다.

MDS Engine에서 허용 또는 차단하도록 설정된 내역을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds extended comment MSG	CONFIG	MDS Engine에서 허용 또는 차단하도록 설정된 Traffic 유형을 초기화합니다.
no mds extended {all deny permit} {any icmp raw tcp udp} {any SMAC} {any SIP} {any SPort} {any DMAC} {any DIP} {any DPort}	CONFIG	MDS Engine에서 허용 또는 차단하도록 설정된 Traffic 유형을 초기화합니다.

<예제> 목적지 IP 192.168.1.10 Server의 TCP 80 Port에 대한 MDS 예외 설정.

출발지 MAC/IP(0000.0000.0011/192.168.1.5)에서 발생하는 목적지 TCP 80 Port에 대해 MDS 차단 설정

```
SG2124G(config)#mds permit tcp any 192.168.1.10 80
SG2124G(config)#mds extended deny tcp 0000.0000.0011 192.168.1.5 any any any 80
SG2124G(config)#end
SG2124G#
SG2124G#show mds extended
```

MDS extended permit/deny information.

Permit/Deny	IP_Protocol	Count	Comment			
Source_MAC	Source_IP		SPort	Destination_MAC	Destination_IP	DPort
std permit	tcp	5642				
any	any		any	any	192.168.1.10	80
deny	tcp	87561				
0000.0000.0011	192.168.1.5		any	any	any	80

```
SG2124G#
SG2124G#show running-config | include mds
mds enable ge1-22 detect
mds uplink ge23-24
mds permit tcp any 192.168.1.10 80
mds extended deny tcp 0000.0000.0011 192.168.1.5 any any any 80
SG2124G#
```



참고

1. 특정 유형의 Traffic에 대해 유해Traffic 예외 처리로 등록하게 되면 예외 처리된 유형의 공격이 발생하는 경우에도 차단하지 않습니다.
2. 예외 처리할 Traffic의 유형을 세분화해서 설정하지 않으면 전체 Network에 심각한 위협이 될 수 있으니, 꼭 필요한 Network만 등록하여 사용하시기 바랍니다.
3. MDS Engine에서 유해Traffic으로 인지하여 차단 정책이 생성 후에는 MDS Extended Permit 정책을 생성하여도 바로 예외로 적용되지 않습니다.
4. 현재 차단중인 Traffic에 대해 예외 정책을 적용하시려면 다음 순서로 적용하시기 바랍니다.
 - show mds detect-list : 예외 처리할 Traffic의 KeyNo. 확인
 - mds extended permit PROTO SMAC SIP SPORT DMAC DIP DPORT : Extended 예외 정책 생성
 - clear mds KeyNo. : 차단정책 강제 해제

2.11.8 Self Loop 차단

내부 Network에 이중 경로가 존재하지 않는다고 해도 Network 환경이나 Cable 상태 등에

따라 자신이 송신한 **Packet**이 다시 자신에게 돌아오는 **Loop** 현상이 발생할 수 있습니다.

이러한 경우를 방지하기 위해 자신이 내 보낸 **Packet**이 되돌아 오는 현상을 감지하여 차단하는 기능이 **Self Loop** 차단 기능입니다. **Self Loop** 차단 기능을 활성화 하면, 자신이 내보낸 **Packet**이 되돌아왔을 때 **Interface**를 **Blocking** 하기 때문에 **Packet**의 폭주로부터 **Network**를 안전하게 운영할 수 있습니다.

Self Loop 차단 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds self-loop-detect <i>IFNAME</i>	CONFIG	Interface 범위를 지정하여 Self Loop 차단 기능을 설정합니다.
mds self-loop-detect timeout <5-300>	CONFIG	Self Loop 차단 기능의 timeout 시간을 설정합니다. (단위 : s)

Self Loop 차단 현황을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mds config	TOP	mds 설정 내역을 확인합니다.
show mds {detect-list detect-history} [<i>log no</i>]	TOP	실시간 차단 현황 및 차단 History Log 를 확인합니다.

Self Loop 차단 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds self-loop-detect <i>IFNAME</i>	CONFIG	Interface 범위를 지정하여 Self Loop 차단 기능을 해제합니다.

<예제> Self Loop 차단 기능 활성화

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds self-loop-detect ge1-22
SG2124G(config)#end
SG2124G#show running-config
!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
bridge 1 protocol pvstp
!
spanning-tree mst config
!
mls qos enable
mds enable ge1-22 detect
mds uplink ge23-24
mds self-loop-detect ge1-22
!
-- 이하 생략 --

SG2124G#
SG2124G#show mds detect-list

```

KeyNo	Phy	SourceIP & MAC	DestIP	Proto	SPort	DPort	SigName	Packet	Action	TimeOut
6	9	Any	Any	NONE			Self_Loop	3	DROP	3



참고

1. STP와 self-loop-detect 기능을 동시에 사용하는 경우, self-loop-detect의 range 지정 시 BPDU를 전송하는 Uplink Interface는 제외하시기 바랍니다.
2. STP를 enable한 상태에서 self-loop-detect 기능을 ge1-24 Interface로 지정하게 되면, BPDU가 전송되는 Uplink interface가 self-loop-detect에서 우선 차단되어 STP가 정상 동작하지 않을 수 있습니다.

2.11.9 ARP Spoofing 차단

ARP란 Layer 2 환경에서 서로의 IP Address만을 아는 장치들이 서로의 MAC Address를 알기 위해 사용하는 Protocol이며, ARP Spoofing 공격은 Local Network에서 사용하는 ARP Protocol의 허점을 이용하여 자신의 MAC (Media Access Control) 주소를 다른 컴퓨터의 MAC인 것처럼 속여 공격 대상 컴퓨터와 Server 또는 Gateway 사이의 Traffic을 공격자 자신의 컴퓨터로 우회하여 Password 정보 등 유용한 정보를 획득할 수 있는 공격입니다.

ARP Spoofing을 방지하기 위해 MDS Engine에서는 ARP Packet을 감지하여 ARP Table에 등록하고 있으면서 등록된 ARP Table과 다른 ARP Packet이 발생하는 경우 차단하는 기능을 가지고 있습니다. ARP Spoofing 차단 기능을 활성화 하면, LAN 환경에서 ARP Spoofing이 발생한 경우에도 공격자의 Spoofing된 ARP Packet만을 차단하며 LAN 사용자들에게는 정상 ARP Table을 재전송하여 사용자 컴퓨터는 정상 ARP Table을 재등록 하도록 동작합니다.

특정 벤더(Apple사의 매킨토시)의 PC는 설치되어 있는 유.무선 Interface가 1개의 IP를 동시에 활성화하여 사용할 수 있는 기능이 있으며, 이 기능을 사용하는 경우 Switch에서는 하나의 IP에 동시에 두 개의 MAC이 감지되기 때문에 arp-spoofing으로 차단되어 특정 벤더에서 제공하는 기능을 사용할 수 없는 현상이 발생합니다. (윈도우 계열의 OS에서는 동일한 환경인 경우 유.무선 Interface 중 한쪽의 interface만 사용합니다.) 이러한 경우에는 등록되어 있는 ARP Table에서 특정 MAC에 대해서 Owner IP가 있는지 여부를 확인한 후 차단하도록 설정하여 특정 벤더에서 제공하는 기능을 사용할 수 있습니다.

ARP Spoofing 차단 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds arp-spoofing {detect drop} <i>PORTRANGE</i>	CONFIG	Interface 범위를 지정하여 ARP Spoofing 차단 기능(detect, drop 지정)을 설정합니다.
mds arp-spoofing-detect <i>PORTRANGE</i>	CONFIG	Interface 범위를 지정하여 ARP Spoofing 차단 기능(drop)을 설정합니다.
mds arp-spoofing-mac-safe { <i>MAC_Addr</i> Wildcard any oui <i>OUI</i> }	CONFIG	ARP Spoofing으로 차단하기 전에 특정 또는 전체 MAC Address에 대해 ARP-Table에 Owner의 IP가 존재하는지를 한번 더 확인하여 차단합니다.
mds arp-table <i>MAC_Addr IP_Addr</i>	CONFIG	mds arp-table을 Static으로 설정합니다.
mds arp-spoofing-permit-mask <1-24>	CONFIG	CIRD포맷을 통해 허용되지 않은 IP 관리 대역을 차단합니다.

ARP Spoofing 차단 현황 및 mds arp-table을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mds config	TOP	mds 설정 내역을 확인합니다.
show mds {detect-list detect-history} [log no]	TOP	실시간 차단 현황 및 차단 History Log를 확인합니다.
show mds arp-table [all dynamic nms static]	TOP	mds arp-table을 확인합니다.
show mds arp-spoofing-mac-safe	CONFIG	arp-spoofing-mac-safe로 설정된 내역을 확인합니다.

ARP Spoofing 차단 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
clear mds arp-table	TOP	mds arp-table을 초기화합니다.
no mds arp-spoofing-detect <i>IFNAME</i>	CONFIG	Interface 범위를 지정하여 ARP Spoofing 차단 기능을 해제합니다.
no mds arp-table <i>MAC_Addr IP_Addr</i>	CONFIG	Static으로 지정된 mds arp-table을 삭제합니다.
no mds arp-spoofing-mac-safe { <i>MAC_Addr Wildcard</i> any oui <i>OUI</i> }	CONFIG	arp-spoofing-mac-safe로 설정된 내역을 삭제합니다.



참고

1. MDS Engine에서 유해Traffic으로 인지하여 차단 정책이 생성 후에는 MDS Extended Permit 정책을 생성하여도 바로 예외로 적용되지 않습니다.
2. 현재 차단중인 Traffic에 대해 예외 정책을 적용하시려면 다음 순서로 적용하시기 바랍니다.
 - show mds detect-list : 예외 처리할 Traffic의 KeyNo. 확인
 - mds extended permit PROTO SMAC SIP SPORT DMAC DIP DPORT : Extended 예외 정책 생성
 - clear mds KeyNo. : 차단정책 강제 해제
3. 특정 유형의 Traffic에 대해 유해Traffic 예외 처리로 등록하게 되면 예외 처리된 유형의 공격이 발생하는 경우에도 차단하지 않습니다.
4. Extended Permit / Deny Traffic의 유형을 세분화해서 설정하지 않으면 전체 Network에 심각한 위험이 될 수 있으니, 꼭 필요한 Network만 등록하여 사용하시기 바랍니다.

<예제> ARP Spoofing 기능 활성화

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds arp-spoofing detect ge1-20
SG2124G(config)#mds arp-spoofing-mac-safe any
SG2124G(config)#end
SG2124G#show running-config
!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
bridge 1 protocol pvstp
!
spanning-tree mst config
!
mls qos enable
mds enable ge1-20 detect
mds uplink ge21-24
mds arp-spoofing detect ge1-20
mds arp-spoofing-mac-safe any
!
-- 이하 생략 --

SG2124G#
SG2124G#show mds detect-list

KeyNo Phy SourceIP & MAC DestIP Proto SPort DPort SigName
Packet Action TimeOut
-----
7 3 0017.42ab.0001 =192.168.50.5 NONE ARP_Spoofing 17 DROP 180

SG2124G#show mds arp-table

No MAC Address IP Address GW Port=Lock VLAN tag Static LastSEC
-----
1 001a.f400.0004 192.168.50.2 * 1 Local 0
2 0017.42ab.0001 192.168.50.5 3 1 101
3 0017.4241.010a 192.168.50.200 11 1 115
4 00e0.ed0a.3a5a 192.168.50.254 23 1 224

SG2124G#
SG2124G#clear mds arp-table
SG2124G#
SG2124G#show mds arp-table

No MAC Address IP Address GW Port=Lock VLAN tag Static LastSEC
-----
SG2124G#

```

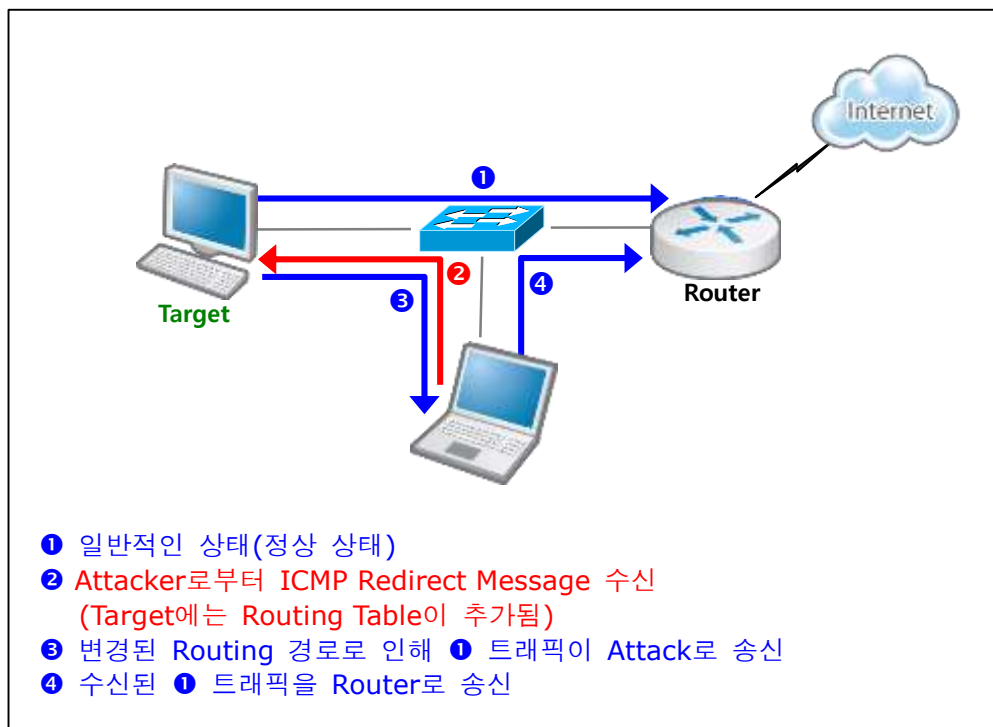
2.11.10 ICMP Redirect 차단

ICMP(Internet Control Message Protocol)는 Network Error Message를 전송하거나 Network 흐름을 통제하기 위한 Protocol이지만 보안에 취약한 부분이 있으며 대표적인 취약점이 ICMP Redirect Message입니다. ICMP Redirect Message는 하나의 Network에 여러 개의 Router가 존재할 때, Host에게 설정되어 있는 Gateway에서 특정 대역에 대해서는 다른 경로를 사용하도록 Host에게 Routing Table을 변경하도록 알려주는 역할을 합니다. ICMP Redirect Message를 수신한 Host는 자신의 Routing Table을 변경하며, 이 후 특정대역으로 발생하는 트래픽은 변경된 자신의 Routing Table을 참고하여 송신하게 됩니다.

예를 들어 어떤 Host가 Gateway의 IP로 목적지 Host에 ICMP Redirect Message를 보내어 Gateway를 변경하도록 하면 해당 Host는 Gateway로부터 수신된 ICMP Redirect Message로 인식하고 자신의 Routing Table을 변경합니다. 이렇게 동작하기 위해서는 역시 IP를 속여서 연결을 취하는 방법을 사용해야 하기 때문에 주로 내부 Network 대역에서 이용되고 있습니다.

일부 Application의 경우 ICMP Redirect의 특징을 이용하여 IP 사용자에게 대한 차단정책 설정, WEB메시지 알림 등으로 이용하며, 이런 경우에는 SIP + ICMP Protocol을 MDS Permit 정책에 등록하여 해당 Application이 차단되지 않도록 설정할 수 있습니다.

[그림 2-14] ICMP Redirect Attack 동작



ICMP Redirect 차단 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds icmp-redirect	CONFIG	ICMP Redirect 기능을 활성화합니다. (Default)

ICMP Redirect 차단 기능을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mds {detect-list detect-history} [log no]	TOP	실시간 차단 현황 및 차단 History Log를 확인합니다.

ICMP Redirect 차단 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds icmp-redirect	CONFIG	ICMP Redirect 기능을 비활성화합니다.



참고

일부 Application의 경우 ICMP Redirect의 특징을 이용하여 IP 사용자에게 대한 차단정책 설정, WEB메시지 알람 등으로 이용하며, 이런 경우에는 SIP + ICMP Protocol을 MDS Permit 정책에 등록하여 해당 Application이 차단되지 않도록 설정할 수 있습니다.

<예제> icmp redirect 차단된 예제 및 비활성화

SG2124G#show mds detect-list

KeyNo	Phy	SourceIP & MAC	DestIP	Proto	SPort	DPort	SigName	Packet	Action	TimeOut
3	2	192.168.11.1	192.168.11.10	ICMP			ICMP_Redir_Attac	40	DROP	179

SG2124G#show mds detect-list log 3

```

detect code : 3
Sig Name    : (351)ICMP_Redir_Attack
from Date   : 10/12/06 21:39:56
to  Date    : 10/12/06 21:40:00 (4 Sec)
Phy. Port No: 2
Source MAC   : 0017.4293.0ea5
Source IP    : 192.168.11.1
Dest IP      : 192.168.11.10
Protocol     : ICMP
Drop Count   : 40

```

No.	SourceIP	DestIP	Proto	SPort	DPort
1	192.168.11.50	192.168.11.20	ICMP		
2	192.168.11.50	192.168.11.20	ICMP		
3	192.168.11.50	192.168.11.20	ICMP		
4	192.168.11.50	192.168.11.20	ICMP		
5	192.168.11.50	192.168.11.20	ICMP		
6	192.168.11.50	192.168.11.20	ICMP		
7	192.168.11.50	192.168.11.20	ICMP		

-- 이하 생략 --

SG2124G#

SG2124G#configure terminal

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

SG2124G(config)#no mds icmp-redirect

SG2124G(config)#end

SG2124G#show running-config | inc mds

mds enable ge1-22 drop

mds uplink ge23-24

no mds icmp-redirect

SG2124G#

2.11.11 IF-PKT-Loss 탐지

Interface 설정이 잘못되어 Packet 송/수신에 문제가 발생하는 경우 또는 케이블등의 노후화로 인한 Packet Loss 등이 발생한 경우 Interface 상태를 확인하여 보아야 상태를 확인할 수 있습니다. 하지만 mds if-pkt-loss 기능을 사용하면 Interface에서 물리적으로 발생된 오류에 대해서 MDS 엔진에서 감시하여 빠르게 확인할 수 있습니다.

- PKT_Errors : CABLE의 Noise나 감쇄현상에 의해 상대방과 통신하는 과정에서 Packet의 Checksum이 틀릴 경우 자동으로 탐지하는 기능으로 Cable 교체 및 점점 구간의 점검 해야 합니다.
- PKT_Collisions : 주로 10M-Half로 연결된 Interface에서 발생하며, 상대방과의 Speed 또는 Duplex 설정이 다르게 설정되어 Packet의 전송/수신시 충돌에 의한 오류를 탐지하는 기능으로 양단의 설정을 동일하게 조정 해야 합니다.

IF-PKT-Loss 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds if-pkt-loss [PORTRANGE]	CONFIG	if-pkt-loss 기능을 활성화합니다.
mds if-pkt-loss threshold <1-1000>	CONFIG	Packet Loss 기준점을 설정합니다. (pkts/10 s)

IF-PKT-Loss 기능을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mds {detect-list detect-history} [log no]	TOP	실시간 차단 현황 및 차단 History Log를 확인합니다.

IF-PKT-Loss 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds if-pkt-loss [PORTRANGE]	CONFIG	if-pkt-loss 기능을 비활성화합니다.
no mds if-pkt-loss threshold	CONFIG	Packet Loss 기준점을 초기화합니다.

<예제> if-pkt-loss 기능 활성화

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds if-pkt-loss ge1-22
SG2124G(config)#mds if-pkt-loss threshold 100
SG2124G(config)#end
SG2124G#show running-config | inc mds
mds enable ge1-22 drop
mds uplink ge23-24
mds if-pkt-loss ge1-22
mds if-pkt-loss threshold 10
SG2124G#
SG2124G#show mds detect-list      → Interface Status 에 Collision 이 발생한 경우

```

KeyNo	Phy	SourceIP & MAC	DestIP	Proto	SPort	DPort	SigName	Packet	Action	TimeOut
1	1	Any	Any	NONE			PKT_Collisions	1	DR0P	160

```

SG2124G#
SG2124G#show mds detect-list      → Interface Status 에 CRC Error 가 발생한 경우

```

KeyNo	Phy	SourceIP & MAC	DestIP	Proto	SPort	DPort	SigName	Packet	Action	TimeOut
3	3	Any	Any	NONE			PKT_Errors	2	DR0P	156

```

SG2124G#

```

2.11.12 MAC Flooding 차단

스위칭 허브와 같은 공유된 이더넷 방식을 사용하는 경우 불필요한 트래픽의 발생 및 모든 정보를 Sniffing 할 수 있는등의 문제점을 해결하기 위해 스위치에서는 MAC Address 정보를 저장하여 고성능을 제공하는 기능을 사용하고 있지만, 스위치에 저장할 수 있는 물리적 공간의 제약으로 스위치마다 저장 가능한 최대 MAC Address가 제한될 수 밖에 없으며, 이런 취약점을 이용해 스니핑이 가능하도록 하는 공격 방법이 MAC Flooding 공격입니다.

MAC Flooding 공격은 공격 Host에서 변조된 MAC Address 정보를 발생하여 특정 Interface에 수천 개 이상의 Host가 연결되어 있는 것으로 보이도록 하는 공격으로, 짧은 시간 내에 대량의 위장된 MAC Address를 특정 Interface에서 발생시키면 스위치는 MAC Address Table에 변조된 MAC Address를 저장할 수 있는 최대치까지 저장하게 되며, 이때 스위치에서는 모든 Data Traffic이 전체 Interface로 Flooding되어 정상인 상태에서 불가능 하였던 Sniffing을 통한 개인 정보 유출이 가능하므로 스위칭 허브로 구성된 네트워크의 Packet Sniffing의 보안위협과 동일한 형태의 네트워크 위험이 존재하게 됩니다.

스위치에서는 아래와 같은 경우에 전체 Interface로 Packet Flooding이 발생하게 됩니다.

- 1) MAC Address Table이 완전히 비어 있어 MAC Address Table을 통해 지정된 경로가 없는 경우
- 2) 공격을 통해 MAC Address Table이 가득 차게 되는 경우
- 3) 프레임의 목적지 MAC Address가 MAC Address Table에 없는 경우나 다른 경우
- 4) 보내고자 하는 프레임의 목적지 MAC Address가 Broadcast MAC Address인 경우

MAC Flooding 공격은 특정 Host가 대량의 변조된 MAC Address를 생성하므로 이를 차단하기 위해서는 다음과 같은 방법을 사용할 수 있습니다.

- 1) Interface별로 사용하는 MAC Address를 설정 (2.10.4 Port Security 참조)
- 2) Interface별로 수용할 수 있는 최대 MAC Address의 수를 제한(2.10.3 Interface별 접속자 수 제한 참조)
- 3) MDS 엔진을 통한 MAC Flooding 공격 차단

MDS엔진을 통한 MAC Flooding 공격을 방어하기 위해서는 MAC Address 학습개수의 최소 임계치와 최대 임계치를 설정하고, 설정된 시간당 허용할 MAC Address Count를 설정하여, 이 규칙에 따라 MAC Learning을 허용하면서 사용자의 통신 장애를 최소화하고 시스템의 안정성을 보장하며, 관리자에게 현재 비정상적으로 MAC주소가 학습되고 있음을 통지하게 됩니다.

MDS Mac-flooding이 enable된 Interface는 CPU MAC Learning Mode로 변경되면서 FDB를 초기화합니다. 이때 MDS가 Enable되지 않은 Interface는 Mac-flooding 기능을 적용해도 MAC Learning Mode만 CPU MAC Learning일 뿐 실제로는 동작하지 않습니다.

MDS Mac-flooding을 enable 하기 위해서는 먼저 스위치의 MAC Table에 저장할 maximum 값을 설정해야 하며, maximum 값 설정을 제거하기 위해서는 먼저 Mac-flooding 기능을 Disable해야 합니다. 모든 설정이 완료된 후 MAC Counter가 Min 값에 도달하게 되면 mac-flooding 공격으로 인식하여 mds detect-list에 관련 Log를 표시하게 되며, MIN 값을 넘어서 mac-flooding 공격이 지속될 경우 PER_MAC에서 설정한 MAC Address 개수만큼 초당 MAC Learning이 되며 초과된 MAC Address는 자동 폐기됩니다. 이 때 Interface MAC Counter는 MAX 값을 초과할 수 없으며, 기능이 활성화된 Interface의 MAC Counter의 합계는 전체 maximum 값을 초과할 수 없습니다.

관리자가 신뢰할 수 있는 MAC Address의 경우 Trust로 등록할 수 있으며, 등록된 MAC Address는 MAC Learning이 제한되지 않습니다. 현재 Trust로 인식된 MAC Address 정보를 확인하면 MDS 엔진에서 MAC Address 학습을 통해 오랫동안 정상적으로 사용되어 자동으로 신뢰할 수 있다고 판단된 MAC Address 정보(Dynamic)와 관리자가 등록한 MAC Address(Static)로 구분되어 표시되며, Dynamic Trust MAC Address의 경우 Clear 명령을 통해 삭제할 수 있습니다. (시스템에 오랜 시간 학습되어 Trust로 인식된 Dynamic MAC Address인 경우 Reboot 후에도 제거되지 않습니다.)

MAC Flooding 차단 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds mac-flooding maximum <1-32768>	CONFIG	최대 Learning 가능한 MAC 주소의 값을 지정합니다.
mds mac-flooding enable PORTRANGE <MIN_VALUE> <MAX_VALUE> <PER_MAC>	CONFIG	MAC Flooding으로 인식하는 MIN 값과 최대허용 MAC 값 및 초당 최대 학습 가능한 MAC 주소의 값을 설정합니다.
mds mac-flooding trust {IFNAME any} MAC_Address Wildcard	CONFIG	신뢰할 수 있는 MAC주소로 등록하여 MAC Learning에 제한을 하지 않습니다.

MAC Flooding 차단 현황 및 설정내역을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mds config	TOP	mds 설정 내역을 확인합니다.
show mds {detect-list detect-history} [log no]	TOP	실시간 차단 현황 및 차단 History Log를 확인합니다.
show mds mac-flooding-trust	TOP	설정된 mac-flooding trust MAC 값을 확인합니다.

MAC Flooding 차단 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
clear mds mac-flooding-trust dynamic	CONFIG	mac-flooding 기능에서 해당 Port범위를 제외합니다.
no mds mac-flooding enable <i>PORTRANGE</i>	CONFIG	mac-flooding 기능에서 해당 Port범위를 제외합니다.
no mds mac-flooding maximum	CONFIG	최대로 등록할 수 있는 MAC 주소값을 해제합니다.
no mds mac-flooding trust { <i>IFNAME</i> any} <i>MAC_Address</i> Wildcard	CONFIG	등록된 trust MAC 주소값을 삭제합니다.



참고

1. MDS mac-flooding 기능은 dot1x-port-control 과 같이 사용할 수 없습니다.
2. MDS mac-flooding 기능은 max-macs 기능과 같이 사용할 수 없습니다.

<예제> MAC Flooding 차단 기능 활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#
SG2124G(config)#mds mac-flooding maximum 20000
SG2124G(config)#mds mac-flooding enable ge1-22 500 700 10
SG2124G(config)#mds mac-flooding trust any 0017.4293.0ea5
SG2124G(config)#end
SG2124G#
SG2124G#show running-config | inc mds
mds enable ge1-22 drop
mds uplink ge23-24
mds mac-flooding maximum 20000
mds mac-flooding enable ge1-22 500 700 10
mds mac-flooding trust any 0017.4293.0ea5
SG2124G#
SG2124G#show mds mac-flooding-trust
No      Trust MAC                Port  Remark      Last Date
-----
1       0017.4293.0ea5           2     Static
2       0011.a968.a0c4           5     Dynamic    2010/12/06 22:05:26
3       0011.a968.a18c           7     Dynamic    2010/12/06 22:05:26
SG2124G#
SG2124G#show mds detect-list
```

KeyNo	Phy	SourceIP & MAC	DestIP	Proto	SPort	DPort	SigName	Packet	Action	TimeOut
4	2	Any	Any	NONE			MAC_Flooding	1091919	DROP	59

SG2124G#

SG2124G#show mds detect-list log 4

detect code : 4

Sig Name : (11)MAC_Flooding

from Date : 10/12/06 21:56:55

to Date : 10/12/06 22:06:30 (575 Sec)

Phy. Port No: 2

No.	Attack MAC	IP
1	0017.27ba.f0fe	0.0.0.0
2	0017.8a72.1ea7	0.0.0.0
3	0017.efc1.b81a	0.0.0.0
4	0017.5f1f.e005	0.0.0.0
5	0017.9dde.bc04	0.0.0.0
6	0017.02e0.c27f	0.0.0.0
7	0017.c33f.7a16	0.0.0.0
8	0017.8995.bbe4	0.0.0.0
9	0017.e25c.94e7	0.0.0.0
10	0017.57fb.9038	0.0.0.0
11	0017.7d45.9482	0.0.0.0
12	0017.6712.7493	0.0.0.0
13	0017.34f9.a00e	0.0.0.0
14	0017.8c84.091a	0.0.0.0
15	0017.68f3.2bec	0.0.0.0

--- 이하생략 ---

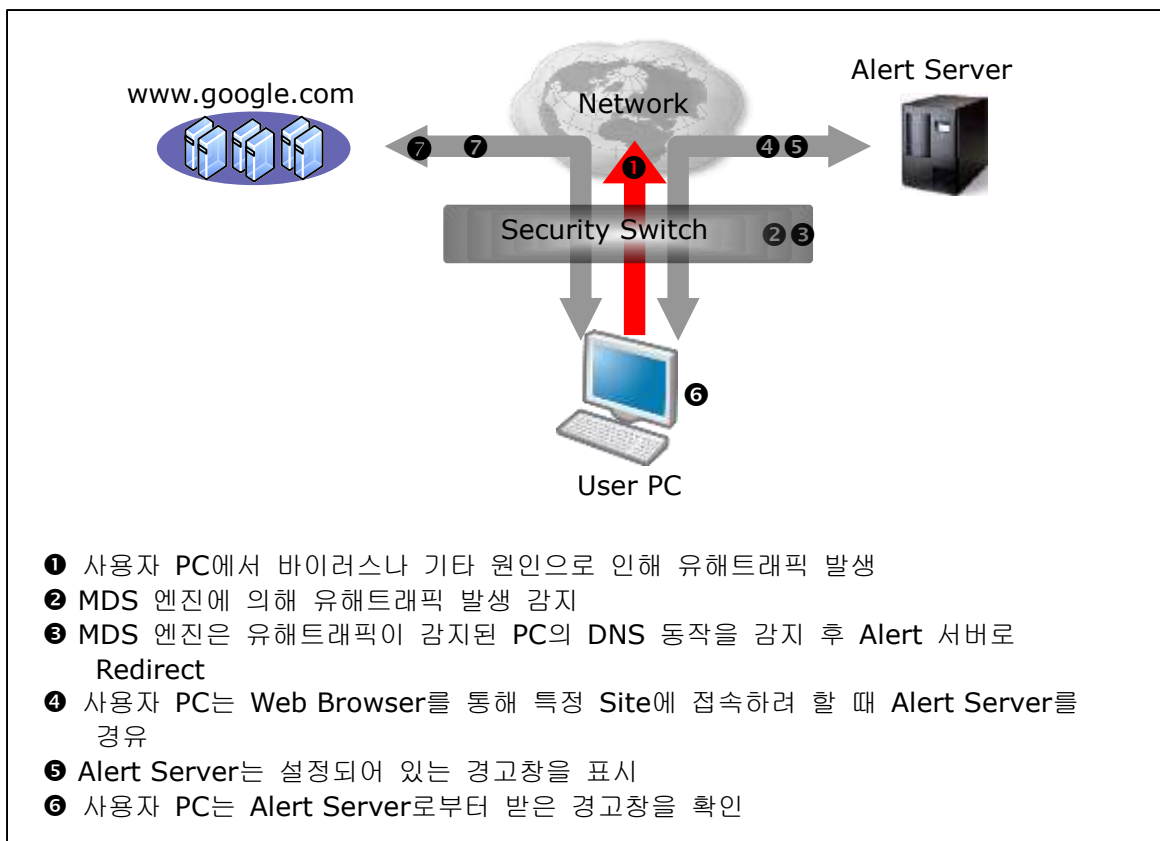
SG2124G#

2.11.13 MDS Web-Alert

MDS 엔진에 의해 유해 트래픽 발생이 감지된 사용자에게 관리자의 통보 없이 사용자가 Internet에 접속을 시도하는 경우 유해트래픽이 발생된 내역을 확인하여 바이러스등의 감염 여부를 신속히 파악할 수 있도록 웹 브라우저를 통해 경고창으로 알려주는 기능입니다.

MDS Web-Alert 기능을 사용하기 위해서는 Web Page를 Redirect할 Server의 IP와 Service Port를 MDS에 설정한 후 Redirect 할 Domain을 등록하여 사용할 수 있습니다.

[그림 2-15] MDS Web-Alert 동작 원리



사용자 PC에서 바이러스나 기타 원인으로 인해 유해트래픽이 발생하여 MDS엔진에서 유해트래픽으로 감지된 경우, MDS 엔진에서는 감지된 PC로부터 Web Browser를 통해 Internet을 사용하려 할 때 발생하는 DNS Query 동작 상태를 감지하여 Alert 서버로 해당 패킷을 Redirect하여 Alert 서버에 설정되어 있는 경고창을 표시하게 됩니다. Alert 서버로부터 경고창을 받은 사용자 PC에서는 경고창을 확인한 후 Web Browser를 재 가동하여 정상적인 Internet을 사용할 수 있습니다.

MDS Web-Alert 기능을 설정하여 사용자에게 경고창을 보여주기 위해서는 다음과 같은 내용을 설정해야 합니다.

■ mds web-alert enable {alert-per-attack | alert-per-day} IP_Addr SVC_Port

alert-per : 공격이 발생할 때마다(attack) / 하루에 한번만 경고창을 보여주도록 설정
(생략 시 alert-per-day로 설정됨)

IP_Addr : 경고 Web Page를 보여줄 서버를 설정 (서버가 없는 경우 Localhost로
설정됨) SVC_Port 대신 ko/en/jp/auto 등 언어를 설정)

SVC_Port : 서버의 Service Port 설정 (미지정시 81로 자동 설정)
web-alert 설정 시 기존에 domain-match 설정이 없는 경우 www.*으로 설정
되어 동작함. 언어 설정의 Default는 Auto로 설정되며, 이때는 사용자의 Web
Browser의 정보로 언어를 자동 판단함.

■ mds web-alert domain-match DOMAIN

DNS를 Match할 Domain Address를 지정하는 명령으로 '*'는 한번만 사용할 수 있습니다.

Domain을 지정한 경우 내부적으로 동작하던 www.*은 자동으로 삭제됩니다.

Domain에는 * 또는 http:// 와 같은 Protocol 명은 사용할 수 없습니다

■ mds web-alert {test-mac MAC_Addr | test-ip IP_Addr}

경고창의 작동 여부를 테스트하기 위한 명령으로 실행해도 running-config에는 남지 않으며,
공격이 감지되지 않아도 사용자에게 경고창을 보여주며, 경고창을 보여준 이후에는 더 이상
명령이 유효하지 않습니다. (MAC/IP 설정은 Attacker의 Type에 맞게 설정됩니다)

■ mds web-alert except-port PORTRANGE

Web-Alert을 설정한 후 경고창을 보여주지 않을 Interface를 설정합니다

■ mds web-alert attacker {src-mac | src-ip}

src-mac : Default이므로 running-config에 표시되지 않습니다.

src-ip : 하단에 L3 장비가 연결된 경우 설정하며, 공격자 IP가 잘못된 IP일 때
경고창 발생에 제약이 발생합니다.

■ show mds web-alert list

경고창을 보내기 위해 관리중인 src-mac / src-ip 목록으로 현재 감시중인 항목을 'Install
OK'로 표시하며, Test를 위해 등록한 MAC / IP인 경우 Service Port가 생략됩니다.

Alert Type : 실제 공격 / Test를 위해 추가된 항목인지 구분합니다.
 Alert Starting Time : 관리를 시작한 시간이 기록합니다

■ show mds web-alert domain-list

Web Alert : 설정된 Domain을 통해 Web Page가 Redirect된 Counter
 DNS Redirect : 설정된 Domain을 통해 DNS Query가 요청된 Counter

Web-Alert 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds web-alert attacker {src-ip src-mac}	CONFIG	공격 발생 시 공격자 분류기준을 설정합니다. (Default: src-mac)
mds web-alert domain-match DOMAIN	CONFIG	DNS을 match할 Domain Address를 지정합니다.
mds web-alert enable {alert-per-attack alert-per-day IP_Addr <1-65535> localhost [auto en ja ko]}	CONFIG	Web-Alert 기능을 설정합니다. (Default: alert-per-day)
mds web-alert except-port PORTRANGE	CONFIG	경고창을 보여주지 않을 Interface를 설정합니다.
mds web-alert {test-ip IP_Addr test-mac MAC_Addr}	CONFIG	경고창이 정상인지 Test 할 수 있도록 IP / MAC을 설정합니다.
mds update web-alert {IP_Addr IPv6_Addr} FILENAME ID PASSWD [port PORT_Num]	CONFIG	FTP를 통해 MDS Web-alert 페이지를 업로드 합니다. (Max : 32Kbyte)

Web-Alert 기능을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mds {detect-list detect-history} [log no]	TOP	실시간 차단 현황 및 차단 History Log를 확인합니다.
show mds web-alert list {list domain-list}	CONFIG	경고창을 보내기 위해 관리중인 MAC/IP 또는 지정된 Domain 목록을 확인합니다.
show mds web-alert flash	TOP	HTML 파일을 콘솔상에서 보여줍니다.

Web-Alert 차단 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
clear mds web-alert	TOP	경고창을 보내기 위해 관리중인 MAC/IP 를 초기화합니다.
no mds web-alert attacker	CONFIG	공격자 분류기준을 Default 로 초기화합니다. (Default: src-mac)
no mds web-alert domain-match [DOMAIN]	CONFIG	설정된 Domain 정보를 삭제합니다. (Domain 미 지정시 모두 삭제)
no mds web-alert enable	CONFIG	Web-Alert 기능을 비활성화합니다.
no mds web-alert except-port PORTRANGE	CONFIG	경고창을 보여주지 않을 Interface 의 설정을 초기화합니다.
no mds web-alert {test-ip [IP_Addr] test-mac [MAC_Addr]}	CONFIG	경고창이 정상인지 Test 할 수 있도록 설정된 IP / MAC 을 초기화합니다.
remove mds web-alert flash	TOP	플래시에 저장된 html 파일을 제거하여 default 문구로 초기화합니다.



참고

1. MDS Engine에서 차단된 유해Traffic 중 self-loop로 차단된 내역은 Web-Alert에 해당되지 않습니다.
2. 하단에 NAT를 사용하는 장비나 L3 장비가 설치된 경우, attacker src-ip 방식을 권장합니다.
3. 사용자 PC에서 경고창이 Popup된 후 Web Browser의 DNS Cache로 인해 목적지 Domain에 일시적으로 접속이 되지 않는 경우 Web Browser를 재 실행해야 정상 동작합니다.
4. MDS Engine에서 TCP/UDP 53(DNS) Service Port 또는 TCP Any 또는 TCP 80 Service Port가 차단중일 경우에는 Web-Alert 기능이 정상 동작하지 않을 수 있습니다.
5. ARP-Spoofing으로 차단된 내역은 Web-Alert 기능이 정상 동작하지 않을 수 있습니다.

<예제> Web-Alert 기능 설정

```

SG2124G(config)#mds web-alert enable 192.168.100.2
SG2124G(config)#show running-config | include web-alert
mds web-alert enable alert-per-day 192.168.100.2 81 find-url www.*
SG2124G(config)#mds web-alert test-mac 0000.0011.0011
SG2124G(config)#end
SG2124G#
SG2124G#show mds web-alert list

Port MAC-Address      IP-Address      Install AlertType Alert Starting Time
-----
-      0000.0011.0011 -      OK      Test      Fri Jun 25 23:35:43 2010
fe3    0000.4241.0089 -      OK      Attacker  Fri Jun 25 23:35:59 2010
SG2124G#
SG2124G#show mds web-alert domain-list

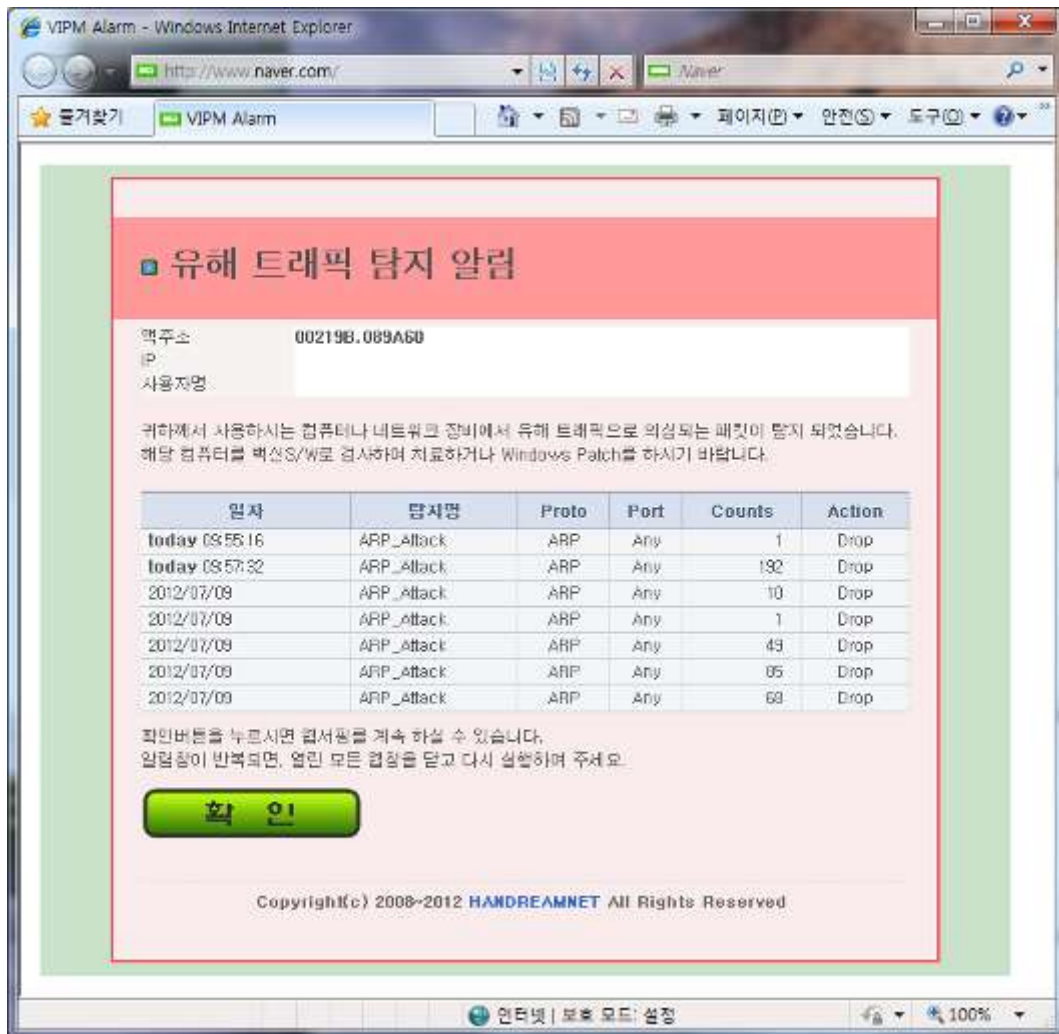
Web Alert DNS Redirect Domain Name
-----
0      0      www.*
SG2124G#
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#no mds web-alert enable
SG2124G(config)#mds web-alert domain-match www.naver.*
SG2124G(config)#mds web-alert enable localhost
SG2124G(config)#show running-config | include web-alert
mds web-alert enable alert-per-day localhost auto
mds web-alert domain-match www.naver.*
SG2124G(config)#mds web-alert test-mac 0000.0011.0011
SG2124G(config)#end
SG2124G#
SG2124G#show mds web-alert list

Port MAC-Address      IP-Address      Install AlertType Alert Starting Time
-----
-      0000.0011.0011 -      OK      Test      Fri Jun 25 23:29:42 2010
fe3    0000.4241.0089 -      OK      Attacker  Fri Jun 25 23:31:02 2010
SG2124G#
SG2124G#show mds web-alert domain-list

Web Alert DNS Redirect Domain Name
-----
0      0      www.naver.*
SG2124G#

```

[그림 2-16] MDS Web-Alert 동작 후 IE 화면



2.11.14 IPv6 DAD Attack 차단

DAD 공격은 link local IPv6 주소 혹은 global IPv6 주소가 할당되거나 설정될 때 중복된 IP가 존재하는지 확인하기 위해 보내는 NS 메시지에 대해 공격자가 자신이 사용하는 IP 주소인 것처럼 NA를 보냄으로써 IP 주소를 사용할 수 없도록 만드는 공격입니다.

네트워크 내에 DAD 공격자 있을 경우 PC의 IPv6 주소를 변경하거나 재시작 하면 IPv6 주소가 IP 충돌상태(Tentative)에 빠져 IP를 사용할 수 없게 됩니다.

DAD 공격 차단 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds dad-attack <i>PORTRANGE</i> {drop detect} <10-180>	CONFIG	mds DAD 공격 차단 기능을 enable 합니다. DAD 기능이 enable되면 활성화된 포트로 매 10 s(default)마다 DAD 공격자 탐지 패킷을 보냅니다.

DAD 공격 차단 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds dad-attack [<i>PORTRANGE</i>]	CONFIG	mds DAD 공격 차단 기능을 disable 합니다.

<예제> DAD 공격 차단 기능 활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds dad-attack ge1-22 drop
SG2124G(config)#end
SG2124G#show running-config
!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
bridge 1 protocol pvstp
!
spanning-tree mst config
!
mls qos enable
mds enable ge1-22 drop
```

```

mds uplink ge23-24
mds dad-attack ge1-22 drop
!
-- 이하 생략 --

```

```

SG2124G#
SG2124G#show mds detect-list

```

KeyNo	Phy	Source IP, MAC Destination IP	Proto	SPort DPort	SigName	Packet	Action	TimeOut
11	2	Any Any	ICMP6		DAD_Attack	1	Drop	179



참 고

1. DAD 공격 탐지를 위해 스위치 MAC 주소를 가지고 생성하는 IPv6 link local 주소를 사용하므로, 네트워크 내에 있는 PC와 장비들의 link local 주소를 스위치의 link local 주소와 동일하게 설정하지 마십시오. 만일 동일하게 설정할 경우 DAD 공격자로 탐지될 수 있습니다.
2. SG2024, SG2024P, SG2200 Series 제품은 DAD 공격 차단 기능을 지원하지 않습니다.
3. DAD 공격 차단 기능은 Switch버전 2.x 이상에서만 지원합니다.

2.11.15 Auto-Config

MDS Auto-Config 기능은 SG Switch Series 하단에 신규 SG Switch Series가 종단에 연결된 경우 관리 용 IP 설정 및 MDS 설정을 관리자가 VNM 혹은 VIPM을 통해 원격설정이 가능하도록 하는 기능입니다. 이 때 신규로 추가된 SG Switch Series는 IP Address가 없는 상태이기 때문에 원격 IP 설정 요청 및 설정 응답은 MAC Address를 이용해 통신하게 됩니다.

Auto-Config 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds auto-config [config-save]	CONFIG	Auto-Config 기능을 활성화 합니다.

Auto-Config 현황을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mds auto-config status	TOP	mds auto0config 상태를 확인합니다.
show mds auto-config relay	TOP	Auto-config가 enable 되어 있는 신규 Switch 정보를 확인합니다.

Auto-Config 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds auto-config	CONFIG	Auto-Config 기능을 비활성화 합니다.

<예제> Auto-Config 기능 활성화

```

=====
                        신규 SG Series Switch
=====

SG2124G#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SG2124G(config)#mds auto-config config-save
SG2124G#
SG2124G#show mds auto-config status
Admin Status : enable
Oper Status: Request
Model: SG2124G
Mac Addr : 001a.f400.0011
Relay Mac Addr : 001a.f400.0004
  
```

```
Relay Model : SG2124G
Discover Sent : 1
Offer Received : 1
Request Sent : 1
Reply Received : 0
SG2124G#
```

```
=====
                         중계 SG Series Switch
=====
```

```
SG2124G#show mds auto-config status
```

```
Admin Status : enable
Oper Status : Complete
Model : SG2124G
Mac Addr : 001a.f410.0004
Relay Mac Addr :
Relay Model :
Discover Sent : 0
Offer Received : 0
Request Sent : 0
Reply Received : 0
SG2124G#
```

```
SG2124G#show mds auto-config relay
```

```
No   Phy MAC Address VLAN Model Number
-----
```

```
1    21 001a.f400.0011   1 SG2124G
SG2124G#
```



참고

1. **mds auto-config**가 활성화 되어 있어도 **IP Address**가 이미 설정되어 있는 경우에는 **VNM / VIPM**을 통해 **IP Address**를 설정할 수 없습니다.
2. **mds auto-config**가 설정되어 있는 **Switch**의 정보를 **VNM / VIPM**으로 전송하는 중계 **Switch**의 경우 **SG OS 1.5.1** 이상을 사용하여야 합니다.

2.11.16 DDoS Disable

IP Spoofing(DDoS)공격이 발생되면 MDS Engine은 IP가 변조된 공격 패킷을 일일이 대응하지 않고 공격의 근원지인 MAC 주소를 차단하게 됩니다.

MDS DDoS disable 기능은 하단에 L3 장비와 같이 1개의 MAC 주소에서 다수의 IP 주소를 보내는 형태의 패킷이 IP Spoofing(DDoS)로 분류되어 MAC 주소가 차단되는 것을 방지하는 경우 사용됩니다. DDoS Disable기능이 적용되면 MAC이 아닌 IP기준으로 만 차단됩니다.

기능 사용 시 주의할 사항은 하단에서 IP Spoofing(DDoS)형태의 공격이 발생하면 차단되지 않습니다. 따라서 꼭 필요한 경우 이외에는 사용하지 않는 것을 권장합니다.

만일 특정 Port에 L3 장비 등이 연결되어 있는 경우 해당 Port를 탐지 Port에서 제외하도록 합니다.

DDoS 차단 기능을 비활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds ddos [disable router-safe disable]	CONFIG	mds ddos 차단 기능을 Disable 합니다.

<예제> ddos 차단 기능 비활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds ddos disable
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds ddos disable
```



참고

기능 설정 시 하단에서 발생하는 IP Spoofing (DDoS) 형태의 Attack 이 차단되지 않습니다

2.11.17 MDS Policy-ACT

MDS에서 탐지된 Rule을 Detect 나 Drop 모드 외에 여러 가지 정책을 부여할 수 있는 기능입니다.

이 기능은 탐지된 Rule에 대하여 Cancel, PPS 제한, QoS 설정, Ratelimit 설정을 할 수 있습니다.

만일 특정 MDS에 차단된 Rule에 대하여 CoS 값을 설정하거나, 지정한 PPS 만큼 허용하는 등 유연한 정책설정이 가능합니다.

Policy-ACT 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
<pre>mds policy-act {host-drop icmp tcp udp} {DST_IP_Addr any fixed} {SRC_PORT any fixed} {DST_PORT any fixed} {cancel detect drop qos ratelimit <64-1000000>}</pre>	CONFIG	mds를 통해 탐지된 내역의 처리를 설정합니다.

■ mds policy-act [option]

hostdrop : MDS에서 동일한 IP에서 10개 이상의 Attack이 탐지되는 경우 해당 IP의 MAC 을 차단하며, 이 때 기존 탐지된 Attack들은 해제되며 HOSTDROP 이라고 표시

icmp : 탐지된 Protocol이 ICMP 인 경우 적용

tcp : 탐지된 Protocol이 TCP 인 경우 적용

udp : 탐지된 Protocol이 UDP 인 경우 적용

■ mds policy-act [option] . . . [policy]

cancel : 설정한 기준에 의하여 탐지된 Rule에 대하여 차단하지 않습니다.

detect : 설정한 기준에 의하여 탐지된 Rule에 대하여 Detect만 합니다.

drop : 설정한 기준에 의하여 탐지된 Rule에 대하여 Drop 합니다.

qos : 설정한 기준에 의하여 탐지된 Rule에 대하여 지정한 QoS를 적용합니다.

(CoS 0~7)

ratelimit : 설정한 기준에 의하여 탐지된 Rule에 대하여 지정한 대역폭 만큼 허용합니다.
(64~1000000 Kbps)

<예제> mds policy-act 기능 설정

- HOSTDROP 발생 시 1Mbps 로 해당 트래픽 제한.
- TCP protocol이며, 목적지 IP 주소가 10.10.10.10~10.10.10.20까지 이고, 목적지 Port 가 80인 패킷이 탐지되면 10Mbps 로 Traffic 제한

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds policy-act ?
  host-drop  Host drop
  icmp       ICMP (Internet Control Message Protocol)
  tcp        TCP (Transmission Control Protocol)
  udp        UDP (User Datagram Protocol)

SG2124G(config)#mds policy-act host-drop ?
  cancel     Cancel Action
  detect     Detect Action
  drop       Drop Action
  qos        QOS Action
  ratelimit  Rate Limit Action

SG2124G(config)#mds policy-act host-drop ratelimit ?
  <64-1000000> Specify kbps Value

SG2124G(config)#mds policy-act host-drop ratelimit 1000
SG2124G(config)#mds policy-act tcp 10.10.10.10 10.10.10.20 any 80 ratelimit 10000
SG2124G(config)#
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds policy-act host-drop ratelimit 1000
mds policy-act tcp 10.10.10.10 10.10.10.20 any 80 ratelimit 10000
!
```

2.11.18 MDS Threshold

MDS에서 탐지 시 Threshold로 설정한 값 이상인 경우 탐지하도록 사용자가 설정을 할 수 있도록 하는 기능입니다.

이 기능은 기본 MDS의 탐지기능 외에 관리자의 정책에 따라 변동할 수 있습니다.

MDS Threshold 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds threshold [icmp <50`100000> tcp <100-100000> udp <100-100000>] [5-3600]	CONFIG	mds에서 탐지 시 threshold 값과 Time을 설정 할 수 있습니다..

MDS Threshold 현황을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mds threshold	TOP	mds threshold 상태를 확인합니다.

MDS Threshold 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds threshold [icmp tcp udp]	CONFIG	mds threshold 기능을 비활성화 합니다.

■ mds threshold [option]

icmp : ICMP 인 경우 적용

tcp : TCP 인 경우 적용

udp : UDP 인 경우 적용

■ mds policy-act [option] . . . [time]

관리자가 설정한 Threshold 값을 초과한 Packet이 설정한 Time 만큼 지속되는 경우 동작 합니다. 5~3600 Count 사이의 값을 설정할 수 있습니다. (MDS의 동작 Cycle 횟수)

<예제> mds threshold 기능 설정

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds threshold ?
    icmp  ICMP
    tcp    TCP
    udp    UDP

SG2124G(config)#mds threshold icmp 100 ?
    <5-3600> Detect count

SG2124G(config)#mds threshold icmp 100 10 ?
    <cr>

SG2124G(config)#mds threshold icmp 100 10
SG2124G(config)#mds threshold tcp ?
    <100-100000> PPS (packet/sec)

SG2124G(config)#mds threshold tcp 500 5
SG2124G(config)#mds threshold udp 2000 10
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds threshold tcp 500 5      → tcp syn packet 이 500 개 이상 5 회이상 지속되면 탐지
mds threshold udp 2000 10   → udp packet 이 2000 개 이상 10 회이상 지속되면 탐지
mds threshold icmp 100 10   → icmp packet 이 100 개 이상 10 회이상 지속되면 탐지
!

```



참고

MDS Threshold 기능은 Switch버전 2.x 이상에서만 지원합니다.

2.11.19 MDS Detect-Port-Range

MDS에서는 특정 Attack(Port Scan, Port Random Attack)의 분산도가 크더라도 어느 한곳에 집중되거나 편향적이라면, 해당 Service port 대역을 계산하여 차단하도록 설계되어 있습니다.

해당 기능은 Attack Port의 분산도에 따른 차단 범위를 줄여 전체 Service Port에 대한 차단을 방지해주는 기능이며 Default는 Enable상태입니다.

만약 탐지된 공격이 Port 범위 10000~20000 사이에서 변화되고 있다면 해당 Port 범위 (10000~20000)의 Packet만 차단시키고, 해당되는 않는 범위의 Packet은 통과 시키게 됩니다. 그러나 탐지된 Attack의 세부적인 Port 범위를 고려하지 않고 모두 차단시키려는 경우 detect-port-range 기능을 비활성화 하여 처리할 수 있습니다

Detect-Port-Range 기능을 비활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds detect-port-range disable	CONFIG	MDS Detect시 탐지된 Service Port 범위만 차단하도록 하는 기능을 해제합니다.

Detect-Port-Range 기능을 초기화 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds detect-port-range disable	CONFIG	Detect-Port-Range 기능을 활성화 합니다.

<예제> mds detect-port-range 기능 비활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds detect-port-range disable
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds detect-port-range disable
!
```

2.11.20 MDS DHCP-Filter

일반적인 경우 DHCP Filter 기능을 활성화 해도 Filtering Log를 확인 할 수 없으나, MDS DHCP-Filter 기능을 이용하는 경우 Filtering Log를 출력할 수 있습니다.

Default Enable 되어 있는 상태이며, 관리자가 Disable 할 경우 mds dhcp filter disable 기능을 사용하십시오.

MDS DHCP-Filter 기능을 비활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds dhcp-filter disable	CONFIG	MDS 의 Detect-List로 DHCP Filter Log를 출력하던 기능을 Disable 합니다

MDS DHCP-Filter 기능을 초기화 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds dhcp-filter disable	CONFIG	MDS 의 Detect-List로 DHCP Filter Log를 출력하는 기능을 Enable 합니다

<예제> mds dhcp-filter 기능 비활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds dhcp-filter disable
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds dhcp-filter disable
!
```

2.11.21 MDS ARP-List Send-Port All

MDS ARP-List Send-Port All 기능은 보안스위치의 전 Port (Uplink 포함)에서 수집된 Arp-Table 정보를 VNM 및 VIPM으로 보내는 기능입니다.

기본적으로 보안스위치는 Uplink에서 수집된 ARP 정보는 VNM 및 VIPM으로 전송하지 않지만, 해당 기능을 이용하면 전체 PORT대한 ARP-Table정보를 VNM 및 VIPM에 전송하도록 동작합니다.

ARP-List Send-Port All 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds arp-list send--port all	CONFIG	MDS에서 수집되는 IP정보를 VNM Server와 VIPM Server로 전송합니다.

ARP-List Send-Port All 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds arp-list send-port all	CONFIG	arp-list send 기능을 비 활성화 합니다.

<예제> mds arp-list send-port all 기능 활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds arp-list send-port all
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds arp-list send-port all
!
```


2.11.22 MDS Attack-CRC

MDS는 관리자의 편이를 위하여 Interface에서 CRC Error가 발생 시 VNM Server나 VIPM Server에 Event를 발생합니다.

기본 Default로 Enable 되어 있는 상태이며 관리자가 Disable 할 경우 MDS Attack-CRC Disable 기능을 사용하십시오.

Attack-CRC 기능을 비활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds attack-crc disable	CONFIG	MDS 의 Log로 Interface에서 CRC 발생 시 출력하던 Event 기능을 Disable 합니다

Attack-CRC 기능을 초기화 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds attack-crc disable	CONFIG	CRC 감지 기능을 활성화 합니다.

<예제> attack-crc 기능 비활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds attack-crc disable
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds attack-crc disable
!
```

2.11.23 MDS Attack-Fragment

Fragment Attack은 Ping of Death, teardrop 등의 공격은 비정상적인 fragment들을 재조합(reassemble)하는 과정에서 시스템이 정지되거나 재부팅 될 수 있습니다.

IP Fragmentation을 이용한 서비스거부공격 외에 이를 이용하여 패킷 필터링 장비나 네트워크 기반의 침입탐지시스템을 우회할 수 있는 문제점이 있을 수 있으며, 일부 구형의 라우터나 침입차단시스템 그리고 네트워크 기반의 침입탐지시스템들은 패킷 재조합 기능을 제공하고 있지 않아 공격자가 공격 패킷을 다수의 데이터그램으로 쪼개서 공격할 경우 이를 탐지하거나 차단하지 못하는 경우가 있습니다.

MDS에서 IP Protocol의 Fragment 조작에 대한 방어기능을 사용할 수 있습니다.

Attack-Fragment 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds attack-fragment enable	CONFIG	MDS 에서 Fragment Packet을 탐지하도록 설정합니다.

Attack-Fragment 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds attack-fragment enable	CONFIG	Fragment 탐지기능을 비 활성화 합니다.

<예제> mds attack-fragment 기능 활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds attack-fragment enable
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds attack-fragment enable
!
```

2.11.24 MDS Attack-Smurf

Smurf Attack은 여러 Host가 특정 대상에 다량의 ICMP Request Packet을 보내게 하여 해당 Host의 Service를 마비시키는 Attack입니다.

이는 공격대상인 Server나 단말을 마비시킬 목적으로 해당 단말의 Source IP 주소를 위조한 ICMP Request Packet을 Broadcast 주소를 목적지주소로 하여 보내, 같은 Network에 연결된 단말들이 Echo Reply로 응답을 하게 만듭니다.

공격 대상 단말은 다량의 ICMP Reply Packet이 유입되어 해당 단말이 Service 가 마비되도록 하는 공격 입니다.

MDS에서 Smurf Attack에 대한 방어기능을 사용할 수 있습니다.

Attack-Smurf 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds attack-smurf enable	CONFIG	MDS 에서 Smurf Attack을 탐지하도록 설정합니다.

Attack-Smurf 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds attack-smurf enable	CONFIG	Smurf 탐지기능을 비 활성화 합니다.

<예제> attack-smurf 기능 활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds attack-smurf enable
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds attack-smurf enable
!
```

2.11.25 MDS ARP-Only-Collection

MDS ARP-Only-Collection 은 VIPM과 연동하여 보안스위치를 Probe모드로 사용할 때 적용하는 기능입니다.

VIPM과 연동하여 보안스위치를 Probe 모드로 운영할 경우 스위치로 유입되는 모든 ARP 패킷(Uplink 포함)에 대해 MDS ARP-Table에 기록하는 옵션 기능입니다.

ARP-Only-Collection 기능을 활성화 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds arp-only-collection	CONFIG	MDS 에서 모든 ARP 패킷에 대해 MDS ARP-Table에 기록하도록 합니다.

ARP-Only-Collection 기능을 해제 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds arp-only-collection	CONFIG	Arp-only-collection 기능을 비활성화 합니다.

<예제> Arp-only-collection 기능 활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds arp-only-collection
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds arp-only-collection
!
```

2.11.26 MDS Detect-Port-Lock

MDS Detect-Port-Lock 기능은 Multicast Attack등 전체 Port에 영향을 줄 수 있는 Attack을 문제가 발생하는 Port에만 filter를 적용하여 다른 포트에 영향이 없도록 하는 기능입니다.

특정 Service Port를 이용한 서비스(Multicast streaming) 이용 중, 특정 Port에서의 해당 Service Port로의 유해 트래픽 발생으로 인해 전체 사용자에게 대해서 해당 Service Port가 차단되는 문제를 발생시키는 경우가 있는데, 해당 옵션을 사용하여 문제가 발생한 Port에만 filter를 적용하여 다른 Port에 영향이 없도록 하는 옵션 기능입니다.

Detect-Port-Lock 기능을 활성화 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds detect-port-lock	CONFIG	MDS 에서 Detect-port-lock 기능을 동작하도록 설정 합니다.

Detect-Port-Lock 기능을 해제 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds detect-port-lock	CONFIG	Detect-port-lock 기능을 비활성화합니다.

<예제> mds detect-port-lock 기능 활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds detect-port-lock
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds detect-port-lock
!
```

2.11.27 MDS NetBIOS

NetBIOS-Filter에 의한 NetBIOS 패킷차단 시에도 NetBIOS 정보를 VIPM에서 확인 할 수 있도록 하는 기능입니다.

해당 기능을 설정하면 NetBIOS Filter 에 의해 NetBIOS Protocol 패킷이 차단되어도, 스위치에서 탐지되는 IP를 기준으로 NetBIOS 정보를 수집하여 VIPM에 전달 하도록 하는 기능입니다.

기본 설정은 Disable이며, VIPM으로 NetBIOS 정보 전달 시간은 60초 ~ 86400초까지 조절할 수 있습니다.

MDS NetBIOS 기능을 활성화 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds netbios enable <60-86400>	CONFIG	NetBIOS Filter 적용 시, VIPM으로 NetBIOS정보를 전달하도록 설정 합니다.

MDS NetBIOS 기능을 해제 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds netbios enable	CONFIG	NetBIOS filter 적용 시, VIPM으로 NetBIOS 정보를 전달하지 않도록 설정 합니다.

<예제> mds netbios 기능 활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds netbios enable 60
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds netbios enable 60
!
```

2.11.28 MDS IP-Range-Scan

VIPM과 연동하여 Switch에 IP Probe 기능을 사용할 때 설정하는 옵션입니다.

이는 VIPM에서 설정된 대역을 기준으로 ARP Scan 기능을 빠르게 수행하기 위하여 만들어진 기능이며, pps 및 repeat min 값을 설정하여 사용합니다.

MDS IPM-Probe 기능과 함께 사용합니다.

MDS IP-Range-Scan 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds ip-range-scan <10-100> <1-3600>	CONFIG	IP Probe 사용 시, IP 대역을 검사합니다.

MDS IP-Range-Scan 기능을 해제하려면 다음명령어를 사용하십시오.

명령어	모드	기능
no mds ip-range-scan	CONFIG	ip-range-scan을 해제합니다.

<예제> mds ip-range-scan 기능 활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds ip-range-scan 10 60
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds ipm-probe
mds ip-range-scan 10 60
!
```

2.11.29 MDS IPM-Accept

VIPM과 연동하여 Switch에 IP Probe 기능을 사용할 때 설정하는 옵션입니다.

이는 지정된 Port에서 수집되는 정보 중, 설정한 IP 대역 및 Vlan에 대한 정보만 수집할 경우에 사용됩니다. 해당 명령어는 `mds arp-list send port` 명령어와 동반하여 사용해야 합니다.

MDS IPM-Probe 기능과 함께 사용합니다.

MDS IPM_Accept 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
<code>mds ipm-accept <ip vlan></code>	CONFIG	특정 IP 대역이나 Vlan에 대한 정보만 수집합니다.

MDS IPM-Accept 기능을 해제하려면 다음명령어를 사용하십시오.

명령어	모드	기능
<code>no mds ipm-accept <ip vlan></code>	CONFIG	Ipm-accept 기능을 해제합니다.

<예제> mds imp-accept 기능 활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds ipm-accept ip 192.168.200.0/24
SG2124G(config)#mds ipm-accept vlan 10
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds ipm-probe
mds ip-range-scan 10 60
mds ipm-accept vlan range 10
mds ipm-accept ip 192.168.200.0/24
mds arp-list send-port ge1-6
!
```

2.11.30 MDS IPM-Collision

MDS IPM-Collision 기능은 VIPM 솔루션과 보안스위치를 연동하여 사용하는 기능입니다.

VIPM에서 IP관리 모드를 접속제어 모드로 사용할 경우, 미 인증 IP에 대한 차단 강도를 설정할 수 있습니다.

미 설정 시 Collision Stress 는 초당 1개의 충돌 패킷을 보내며, 해당 기능 설정 시 충돌 강도를 1-10까지 조정할 수 있습니다.

MDS IPM-Collision 기능을 활성화하려면 다음명령어를 사용하십시오.

명령어	모드	기능
mds ipm-collision stress <1-10>	CONFIG	VIPM솔루션과 연동된 보안스위치에서 ARP 충돌 강도를 제어합니다. (Default: 1)

IPM-Collision 기능을 해제하려면 다음명령어를 사용하십시오.

명령어	모드	기능
no mds ipm-collision stress	CONFIG	VIPM솔루션과 연동된 보안스위치에서 설정한 stress 수치를 원래대로 변경합니다. (Default: 1)
mds ipm-collision disable	CONFIG	VIPM솔루션과 연동된 보안스위치에서 ARP 충돌 패킷을 보내지 않습니다. (Default: enable)

<예제> mds ipm-collision 기능 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds ipm-collision stress 10
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds ipm-collision stress 10
!
```

2.11.31 MDS IPM-Guard-To-MAC-Security

MDS IPM-Guard-To-MAC-Security 기능은 VIPM 솔루션과 보안스위치가 연동하여 사용하는 기능으로, VIPM에서 라우터 IP 보호 옵션을 적용한 IP에 대한 보호 기능입니다.

IP고정(탐지전용)으로 사용자나 장비등록 시 설정되는 Gateway MAC 및 IP충돌방지 기능을

사용하지 않을 경우 설정합니다.

MDS IPM-Guard-To-MAC-Security 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds ipm-guard-to-mac-security disable	CONFIG	VIPM솔루션과 연동된 보안스위치에서 라우터 MAC 및 IP 충돌방지 기능을 비 활성화 합니다.

MDS IPM-Guard-To-MAC-Security 기능을 초기화 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds ipm-guard-to-mac-security disable	CONFIG	VIPM솔루션과 연동된 보안스위치에서 라우터 MAC 및 IP 충돌방지 기능을 활성화 합니다. (Default enable)

<예제> mds ipm-guard-to-mac-security 기능 비활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds ipm-guard-to-mac-security disable
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds ipm-guard-to-mac-security disable
!
```

2.11.32 MDS IPM-Interface

다수의 Vlan을 사용중인 환경에서는 기본적으로 대표 VLAN(Vlan1.1)에 설정된 IP를 이용하여 VIPM과 통신을 하게 되며, 다른 Interface는 VIPM과의 연동에 사용되지 않습니다. IPM-Interface 기능은 vlan1.1과 VIPM 서버간 통신을 할 수 없는 환경일 때 vlan1.1이 아닌 다른 Interface(vlan or ge1-24 or MGMT)로 VIPM솔루션과 연동할 수 있게 하는 기능입니다.

VIPM과 통신을 하도록 지정할 수 있는 방법은 interface, IP Address, MGMT port 등을 선택하여 설정할 수 있으며, 중복 설정은 불가능 합니다

MDS IPM-Interface 기능을 활성화 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds ipm-interface [<i>IFNAME</i> <i>A.B.C.D</i> <i>X:X::X:X</i> mgmt]	CONFIG	VIPM솔루션과 보안스위치간 통신 전용interface를 선택하고 활성화 합니다.

MDS IPM-Interface 기능을 해제 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds ipm-interface	CONFIG	VIPM솔루션과 보안스위치간 통신 전용interface를 비 활성화 합니다.

<예제> mds ipm-interface 기능 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds ipm-interface 192.168.255.170
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds ipm-interface 192.168.255.170
!
```

2.11.33 MDS IPM-Local-DHCP

MDS IPM-Local-DHCP 기능은 VIPM 솔루션과 보안스위치를 연동하여 사용하는 기능입니다.

DHCP환경에서 사용하던 미등록 신규 사용자가 차단될 때 기본 네트워크 환경이 DHCP가 아니라면 차단된 사용자는 IP를 할당 받지 못하고 모든 네트워크 활동이 제약되며, VIPM은 해당 사용자에 대해 웹메시지 처리기능(사용자 인증신청 및 메시지 출력)을 수행할 수 없게 됩니다.

따라서 기본 환경이 Static 이고, 미인증 신규 사용자가 DHCP 상태로 연결 시 보안스위치가 웹 메시지 처리를 위한 임시 IP 할당을 하고, 임시로 할당된 IP를 이용하여 웹 메시지 처리 기능을 수행 하고자 할 때 적용하는 기능입니다.

해당 기능을 위한 DHCP Pool을 설정 할 필요는 없습니다.

MDS IPM-Local-DHCP 기능을 활성화 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds ipm-local-dhcp	CONFIG	Local dhcp 기능을 사용하도록 합니다.

MDS IPM-Local-DHCP 기능을 해제 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds ipm-local-dhcp	CONFIG	Local dhcp 기능을 비 활성화 합니다.

<예제> mds ipm-local-dhcp 기능 활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds ipm-local-dhcp
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds ipm-local-dhcp
!
```

2.11.34 MDS IPM-Permit

MDS IPM-Permit 기능은 VIPM 솔루션과 보안스위치가 연동하여 사용하는 기능으로, IP 제어를 사용하는 환경에서 IP 대역 혹은 VLAN 정보를 이용하여 IP관리에서 제외할 때 사용하는 기능입니다.

Server Farm, 관리용 장비IP대역 등 특정 솔루션이나 사용자에게 IP정보 수집 및 차단 기능을 수행하지 않을 때 사용하는 기능으로 신뢰할 수 있는 IP 및 VLAN에 대해서 IP관리를 제외합니다.

MDS IPM-Permit 기능을 활성화 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds ipm-permit [ip [A.B.C.D A.B.C.D/M] A.B.C.D vlan [<1-4094> range RANGE]	CONFIG	ipm-permit 기능을 사용할 수 있도록 설정 합니다.

MDS IPM-Permit 기능을 해제 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds ipm-permit [ip [A.B.C.D A.B.C.D/M] A.B.C.D vlan [<1-4094> range RANGE]	CONFIG	ipm-permit 기능을 해제합니다.

<예제> mds ipm-permit 기능 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds ipm-permit ip 192.168.255.0/24
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds ipm-permit ip 192.168.255.0/24
!
```

2.11.35 MDS IPM-Probe

MDS IPM-Probe 기능은 VIPM 솔루션과 연동하여 사용하는 기능으로, SG Switch Series Switch를 네트워크에 연결하여 Probe 방식으로 모든 사용자정보(MAC, IP)를 수집하고, 제어합니다.

수집된 IP를 대상으로 비인가 사용자 인증 및 강제 차단, MGMT등 기능을 동일하게 사용할 수 있습니다. (Traffic정보 제외)

- 해당 기능을 사용하기 위해서는 보안스위치가 관리하고자 하는 IP대역과 같은 네트워크가 되도록 B/B Switch에서 해당되는 모든 Vlan에 대해서 Trunk Port로 구성하여 SG Switch Series Switch와 연결해야 합니다.

MDS IPM-Probe 기능을 활성화 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds ipm-probe	CONFIG	ipm-probe 기능을 사용할 수 있도록 설정 합니다.

MDS IPM-Probe 기능을 해제 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds ipm-probe	CONFIG	ipm-probe 기능을 해제 하려면 설정 합니다.

<예제> mds ipm-probe 기능 활성화

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds ipm-probe
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds ipm-probe
!
```

2.11.36 MDS IPM-Range-Over-MSG-Disable

MDS IPM-Range-Over-MSG-Disable 기능은 VIPM 솔루션과 보안스위치가 연동하여 사용하는 기능으로, IP 제어를 사용하는 환경에서 IP사용 인증 및 인증요청 웹페이지를 사용하지 않을 때 설정합니다.

VIPM 에서 IP관리시 기존 설정된 IP대역을 초과할 경우 인증관련 웹 페이지를 표시해 주는 기능이 있습니다. 해당 기능을 이용하면, 해당 Interface에 대해서는 미인증 IP가 설정된 IP대역이 아닌 다른 대역을 설정하여 접속하는 경우 인증관련 웹페이지를 표시하지 않습니다.

MDS IPM-Range-Over-MSG-Disable 기능을 활성화 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
<code>mds ipm-range-over-msg-disable PORTRANGE</code>	CONFIG	ipm-range-over-msg-disable 기능을 사용 하려면 설정 합니다.

MDS IPM-Range-Over-MSG-Disable 기능을 해제 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
<code>no mds ipm-range-over-msg-disable PORTRANGE</code>	CONFIG	ipm-range-over-msg-disable 기능을 해제 하려면 설정 합니다..

<예제> mds ipm-range-over-msg-disable 기능 설정

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#mds ipm-range-over-msg-disable ge1-4
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
mds enable ge1-22 detect
mds uplink ge23-24
mds ipm-range-over-msg-disable ge1-4
!
```

2.11.37 Visual Node Manager (VNM) 연동

Switch의 관리는 Serial Console등을 이용하여 접속한 CLI 를 통해 관리할 수 있으며 하나의 터미널을 통해서만 한대의 Switch만 접속하여 관리할 수 있기 때문에 다수의 Switch를 운용하는 경우 CLI를 통해 한대씩 접속하여 모니터링 및 관리하기에는 어려운 점이 많습니다.

Visual Node Manager는 한 화면에서 다수의 장비를 모니터링 및 관리할 수 있는 Program입니다. Visual Node Manager를 통해 Switch를 관리하기 위해서는 Switch에 SNMP Community 및 mds log-server를 설정해 주어야 합니다. (자세한 내용은 VNM Manual을 참고하시기 바랍니다.)

VNM Server와 연동하여 Switch를 관리하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds log-server <i>IP_Addr</i> [<1-65535>]	CONFIG	log-server (VNM Server)의 IP 및 Service Port를 설정합니다. Service Port를 지정하지 않은 경우 default Port (TCP 8085)로 설정됩니다.
mds log-server <i>IP_Addr</i> discard {both ip none traffic}	CONFIG	특정 정보(Traffic, mds arp-table)을 log-server로 전송하지 않도록 설정합니다. (Default: None)
snmp-server community {ro rw} <i>NAME</i>	CONFIG	Snmp community명을 설정합니다.
mds log-server <i>IP_Addr</i> discard {both ip none traffic}	CONFIG	log-server 지정과 동시에 log-server에서 받지 않을 정보를 설정합니다.

VNM Server와의 연동상태를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mds log-server	TOP	log-server (VNM Server)의 상태 정보를 확인합니다.

VNM Server와 연동 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds log-server <i>IP_Addr</i> [<1-65535>]	CONFIG	log-server (VNM Server)의 설정을 초기화합니다.
no snmp-server community	CONFIG	Snmp community명을 초기화합니다.

[ro rw] NAME		
----------------	--	--

<예제> VNM 연동 설정

- SNMP Community : hdnet

- mds log-server (VNM Server) : 192.168.0.100, 192.168.0.200

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
SG2124G(config)#mds log-server 192.168.0.100
SG2124G(config)#mds log-server 192.168.0.200
SG2124G(config)#snmp-server community rw hdnet
SG2124G(config)#end
SG2124G#
SG2124G#show mds log-server
```

No.	Server IP	Port	Proto	IP MGMT	Sock.ID	Status	T P reConnect
1	192.168.0.100	8085	TCP		0	Fail	50
2	192.168.0.200	8085	TCP		5	OK	

```
** T : Discard traffic information data
** P : Discard IP information data
SG2124G#
```



참고

1. MDS Log-Server는 최대 10개까지 설정할 수 있습니다.
2. VNM을 통해 특정 Interface를 shutdown 시키려면 snmp community가 Read / Write 권한으로 설정되어야 합니다.
3. Visual Node Manager와 SG Switch Series 사이에 방화벽 등의 보안 장비가 설치되어 있거나, VNM Server에 방화벽을 사용하는 경우에는 다음의 Service Port는 통과 될 수 있도록 방화벽 설정을 변경하셔야 합니다.
 - VNM Server → SG Switch Series
: UDP 161 (SNMP Query), UDP 162 (SNMP Set)
 - SG Switch Series → VNM Server
: TCP 8085 (VNM Port)
4. “show mds log-server” 실행 시 Status가 Fail 인 경우에는 VNM의 Default Service Port인 TCP 8085를 이용한 통신에 이상이 발생한 것이므로 원인을 찾아 수정하시기 바랍니다.
5. mds detect-list등에서 event 발생 시 실시간으로 Visual Node Manager Server로 전송되며, VNM Server가 동작 중이지 않은 상태에서 발생한 event 내역은 VNM Server에는 저장되지 않습니다.

2.11.38 Visual IP Manager (VIPM) 연동

Visual IP Manager는 다수의 장비를 모니터링 및 관리할 수 있으며, IP/MAC 제어가 가능한 솔루션입니다. Visual IP Manager를 통해 Switch를 관리하기 위해서는 Switch에 SNMP Community 및 mds ipm-server를 설정해 주어야 합니다. (자세한 내용은 VIPM Manual을 참고하시기 바랍니다.)

VIPM Server와 연동하여 Switch를 관리하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
mds ipm-server [A.B.C.D X:X::X:X] bootmode {last-flash server} <1-65535>	CONFIG	VIPM Server의 IP 주소를 설정하고, Reboot 시 IP관리 동작기능을 Switch의 Flash에 보관하고 있는 Data로 할 것인지 Server와 연동 후 Server의 DATA를 수신 후 동작할 것 인지 설정합니다.
mds ipm-port <i>PORTRANGE</i>	CONFIG	vipm-server의 제어 기능을 사용할 포트를 지정합니다.
snmp-server community {ro rw} <i>NAME</i>	CONFIG	Snmp community명을 설정합니다.
mds ipm-collision {disable stress <1-10>}	CONFIG	Switch의 Interface에서 Collision의 발생 시 설정한 값 이상이면 VIPM으로 해당Event를 전송합니다.
mds ipm-guard-to-mac-security disable	CONFIG	router ip 보호 기능 사용시에 ipm-port 에서 mac-address를 위조하는 경우 방어하는 기능을 해제합니다. (Default: enable)
mds ipm-interface { <i>IFNAME</i> mgmt}	CONFIG	VIPM 연동 시 다수의 VLAN이 존재할 경우 불특정 IP로 VIPM과 접속하는 것을 차단하고, 지정한 Interface를 통해 VIPM과 통신하도록 할 때 설정합니다
md ipm-local-dhcp	CONFIG	VIPM에서 비인증된 사용자에게 local dhcp를 사용할 수 있게 설정합니다.
mds ipm-range-over-msg-disable	CONFIG	VIPM에서 등록되지 않은 IP 대역 사용 시 차단 Message 출력기능을 비활성화합니다
mds ipm-permit {ip [A.B.C.D A.B.C.D/M] High_A.B.C.D}	CONFIG	VIPM과 연동하여 사용하는 기능으로 특정조건에서 IP대역 혹은 VLAN 정보

vlan [<1-4094> range VLAN_RANGE]}		를 이용하여 IP관리를 제외하는 경우 설정합니다.
--	--	--------------------------------

VIPM Server와의 연동상태를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show mds log-server	TOP	ipm-server (VIPM Server)의 상태 정 보를 확인합니다.

VIPM Server 연동 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no mds ipm-server	CONFIG	VIPM Server와의 연동기능을 비 활성화 합니다.
no mds ipm-port PORTRANGE	CONFIG	VIPM에서 관리할 Interface를 해제합 니다.
no snmp-server community [ro rw] NAME	CONFIG	Snmp community명을 초기화합니다.
no mds ipm-collision {disable stress}	CONFIG	Collision 발생시의 Event 전송을 비 활성화 합니다.
no mds ipm-guard-to-mac- security disable	CONFIG	VIPM 연동 시 Router 보호기능을 활 성화 합니다.
no mds ipm-interface	CONFIG	VIPM과 연동설정 시 사용할 Interface의 지정을 해제합니다.
no mds ipm-local-dhcp	CONFIG	DHCP 환경에서 미인증 사용자 차단시 Message 출력기능을 비 활성화합니다
no mds ipm-range-over- msg-disable	CONFIG	VIPM 사용 시 IP대역 차단 Message 출력기능을 활성화 합니다.
no mds ipm-permit {ip [A.B.C.D A.B.C.D/M} High_A.B.C.D} vlan [<1- 4094> range VLAN_RANGE]}	CONFIG	IP관리 대상에서 제외로 설정한 내역 을 해제합니다.

<예제> VIPM 연동 설정

- SNMP Community : hdnet
- mds log-server (VNM Server) : 192.168.0.100, 192.168.0.200
- mds ipm-server (VIPM Server) : 192.168.0.250

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
SG2124G(config)#mds log-server 192.168.0.100
SG2124G(config)#mds log-server 192.168.0.200
SG2124G(config)#mds ipm-server 192.168.0.250 bootmode server
SG2124G(config)#snmp-server community rw hdnet
SG2124G(config)#end
SG2124G#
SG2124G#show mds log-server
```

No.	Server IP	Port	Proto	IP MGMT	Sock.ID	Status	T P reConnect
1	192.168.0.100	8085	TCP		0	Fail	50
2	192.168.0.200	8085	TCP		5	OK	
3	192.168.0.250	8085	TCP	YES	7	OK	

```
** T : Discard traffic information data
** P : Discard IP information data
SG2124G#
```



참고

1. MDS IPM-Server는 1개만 설정할 수 있습니다.
2. VIPM을 통해 특정 Interface를 shutdown 시키려면 snmp community가 Read/ Write 권한으로 설정되어야 합니다.
3. IP/MAC 제어를 하기 위해서는 ipm-port를 설정해 주어야 합니다.
4. Visual IP Manager와 SG Switch Series 사이에 방화벽 등의 보안 장비가 설치되어 있거나, VNM Server에 방화벽을 사용하는 경우에는 다음의 Service Port는 통과 될 수 있도록 방화벽 설정을 변경하셔야 합니다.
 - VIPM Server → SG Switch Series
: UDP 161 (SNMP Query), UDP 162 (SNMP Set)
 - SG Switch Series → VIPM Server
: TCP 8085 (VIPM Port)
5. “show mds log-server” 실행 시 Status가 Fail 인 경우에는 VIPM의 Default Service Port인 TCP 8085를 이용한 통신에 이상이 발생한 것이므로 원인을 찾아 수정하시기 바랍니다.

2.12 DHCP

2.12.1 DHCP Server 설정

DHCP (Dynamic Host Configuration Protocol)란 Network 관리자들이 조직내의 Network 상에서 IP주소를 중앙에서 관리하고 할당해 줄 수 있도록 해주는 Protocol 입니다.

TCP/IP Protocol에서는 컴퓨터 사용자들이 인터넷에 접속할 때 컴퓨터마다 고유한 IP Address를 가져야만 인터넷에 접속할 수 있습니다. DHCP를 사용하지 않는 경우에는 컴퓨터마다 IP Address를 직접 입력해야 하며, 컴퓨터를 다른 Network의 장소로 이동하면 해당 Network의 IP Address로 변경해야 합니다. DHCP는 Network 관리자가 중앙에서 IP주소를 관리하고 할당하며, 컴퓨터가 Network의 어느 장소에 접속되더라도 자동으로 IP주소를 보내 줄 수 있게 해 줍니다.

DHCP는 주어진 IP주소가 일정한 시간 동안 컴퓨터에 유효하도록 하는 "임대" 개념을 사용합니다. 임대 시간은 사용자가 특정한 장소에서 얼마나 오랫동안 인터넷 접속이 필요할 것인지에 따라 달라질 수 있으며, 사용 가능한 IP Address의 개수보다 더 많은 컴퓨터가 있는 경우에도 IP Address의 임대시간을 짧게 함으로써 Network를 동적으로 재구성할 수 있습니다. 또한 DHCP는 영구적인 IP Address를 필요로 하는 Server에 대해서는 고정 IP Address를 할당할 수 있습니다.

DHCP Server Pool 설정 시 TFTP Server의 IP Address (Option-150)를 등록하여 Option-150을 지원하는 VoIP Phone에서 DHCP를 할당 받으면서 Configuration을 TFTP Server로부터 받은 후 VoIP Phone의 현재 Firmware와 일치하지 않으면 Firmware를 Download 하게 할 수 있습니다. TFTP Server는 최대 5개까지 등록할 수 있습니다.

DHCP Server로 설정하여 DHCP Client에게 DHCP Service를 제공하기 위해서는 다음과 같은 내용을 설정해야 합니다.

■ DHCP Pool 설정

DHCP를 설정하기 위해서는 우선 DHCP Pool을 지정하여 DHCP 설정 모드로 전환합니다. DHCP 설정 모드로 전환하면, 프롬프트가 SG2124G(config)#에서 SG2124G(config-dhcp)#로 변경됩니다.

■ DHCP Subnet 설정

DHCP Server의 개별 Network인 Subnet을 지정합니다.

■ IP Address 범위 설정

DHCP Subnet을 설정하였으면 Subnet에서 사용할 IP Address의 범위를 설정합니다.

■ Default Gateway 설정

DHCP Client에서 할당 받을 IP에 대한 Default Gateway를 설정합니다.

■ IP 사용 가능 시간 설정

DHCP Client에 할당하는 IP Address의 사용 일:시간:분 단위로 지정할 수 있으며 정해진 시간이 끝나면 Client는 다시 Server에서 IP를 할당 받아야 합니다.

■ DNS Server 등록

DHCP Client에서 사용할 수 있는 DNS Server를 등록합니다. DNS Server는 2 개까지 등록할 수 있습니다.

■ Domain Name 등록

Client가 IP를 요청할 때 할당하는 IP와 함께 전달될 Domain Name을 설정합니다.

■ 고정 IP 할당 활성화

특정 MAC Address에서 DHCP를 요청할 경우 고정된 IP Address를 할당합니다.

■ Option-150 설정

TFTP Server의 IP Address를 설정합니다.

DHCP Server로 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
service dhcp	CONFIG	DHCP Service를 구동합니다.
ip dhcp server interface <i>VLAN_NAME</i>	CONFIG	DHCP Server를 구동할 Interface를 선택합니다.
dhcp log mode verbose	CONFIG	DHCP Information Level Message를 Syslog에 기록합니다.
ip dhcp pool <i>NAME</i>	DHCP	Pool Name을 설정합니다.
network <i>IP_Addr/mask</i>	DHCP	Subnet을 설정합니다.
range <i>Low_Addr High_Addr</i>	DHCP	IP Address 범위를 설정합니다.
default-router <i>IP_Addr</i>	DHCP	Default router IP를 설정합니다.
lease {<0-30> <0-24> <0-60> infinite}	DHCP	IP 사용 가능 시간을 설정합니다.
dns-server <i>IP_Addr</i>	DHCP	DNS Server를 설정합니다.
domain-name <i>IP_Addr</i>	DHCP	Domain Name을 설정합니다.
host <i>MAC_Addr</i> static-ip <i>IP_Addr</i>	DHCP	특정 Host에게 고정 IP Address를 설정합니다.
tftp-server <i>IP_Addr</i>	DHCP	TFTP Server의 IP Address를 설정합니다.

DHCP Server 동작 상태를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show ip dhcp	CONFIG	DHCP 설정 상태를 확인합니다.
show ip dhcp commit-list	CONFIG	DHCP Client에게 할당된 IP 내역을 확인합니다.
show ip dhcp pool [<i>WORD</i>]	CONFIG	DHCP Pool의 설정 내역을 확인합니다.
show ip dhcp pool-status	DHCP	DHCP Pool에 통계 정보를 확인합니다.
show ip dhcp statistics [detail]	DHCP	DHCP Packet 통계를 확인합니다.

DHCP Server를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no network	DHCP	Subnet을 삭제합니다.
no range <i>Low_Addr</i> <i>High_Addr</i>	DHCP	IP Address 범위를 삭제합니다.
no default-router <i>IP_Addr</i>	DHCP	Default router IP를 삭제합니다.
no lease	DHCP	IP 사용 가능 시간을 초기화합니다.
no dns-server <i>IP_Addr</i>	DHCP	DNS Server를 삭제합니다.
no domain-name <i>IP_Addr</i>	DHCP	Domain Name을 삭제합니다.
no host static-ip <i>MAC_Addr</i>	DHCP	특정 Host에게 할당된 고정 주소를 삭제합니다.
no tftp-server <i>IP_Addr</i>	DHCP	TFTP Server의 IP Address를 삭제합니다.
no ip dhcp pool <i>NAME</i>	DHCP	Pool Name을 삭제합니다.
no dhcp log mode verbose	CONFIG	DHCP Information Level Message를 Syslog에 기록하지 않습니다.
no ip dhcp server interface <i>VLAN_NAME</i>	CONFIG	DHCP Server를 구동할 Interface를 삭제합니다.
no service dhcp	CONFIG	DHCP Service를 중지합니다.



참고

1. DHCP Server를 구동할 Interface는 최대 5개까지 설정할 수 있습니다.
2. DHCP Server Pool은 최대 5개, Pool당 IP Range는 최대 500개까지 설정할 수 있습니다.(L3의 경우 최대 30개 까지 Pool 설정 가능)
3. TFTP Server 등록은 최대 5개까지 설정할 수 있습니다.
4. static-ip 는 최대 64개까지 설정할 수 있습니다.

<예제> DHCP Server 설정

```

SG2124G(config)#interface vlan1.1
SG2124G(config-if)#ip address 172.1.1.254/24
SG2124G(config-if)#exit
SG2124G(config)#ip dhcp server interface vlan1.1
SG2124G(config)#ip dhcp pool pool1
SG2124G(config-dhcp)#network 172.1.1.0/24
SG2124G(config-dhcp)#range 172.1.1.10 172.1.1.100
SG2124G(config-dhcp)#default-router 172.1.1.254
SG2124G(config-dhcp)#lease 0 1 0
SG2124G(config-dhcp)#dns-server 10.10.10.1
SG2124G(config-dhcp)#domain-name test.domain.com
SG2124G(config-dhcp)#tftp-server 172.1.1.252
SG2124G(config-dhcp)#host 0000.1111.2222 static-ip 172.1.1.101
SG2124G(config-dhcp)#end
SG2124G#

```

```

SG2124G#show ip dhcp
dhcp server/relay enabled
dhcp pool list: pool1
vlan1.1 dhcp server active
SG2124G#
SG2124G#show ip dhcp pool

```

```

Pool pool1 :
  network: 172.1.1.0/24
  address range(s):
    add: 172.1.1.10 to 172.1.1.100
  lease <days:hours:minutes> <0:1:0>
  domain: test.domain.com
  dns-server(s): 10.10.10.1
  tftp-server(s): 172.1.1.252
  default-router(s): 172.1.1.254
  host static ip rease config
  host entry #1
    Mac address      : 0000.1111.2222
    static ip address : 172.1.1.101

```

```

SG2124G#show ip dhcp pool-status

```

Network	prefixlen	Total	Used	Available
172.1.1.0	24	91	1	90

```

SG2124G#

```

```

SG2124G#show ip dhcp commit-list

```

IP Address	MAC Address	Interface	Committer	Expire time
172.1.1.100	0012.7957.f081	vlan1.1	server	Sun Jan 21 19:21:35 2009

```

SG2124G#

```

2.12.2 DHCP Relay

DHCP Relay 설정은 Client에서 IP Address를 요청할 때 다른 Network에 있는 DHCP Server로부터 할당된 IP Address를 DHCP Client에 전달해 주는 역할을 해 줍니다. DHCP Server에서 IP를 할당 받기 위해서는 DHCP Server와 동일한 VLAN에 Client가 존재해야 하나, DHCP Relay를 사용하면 DHCP Server가 관리할 수 있는 영역 이상의 Subnet을 관리할 수 있으므로 보다 효과적 DHCP Server를 관리할 수 있습니다.

Relay Agent로 설정된 Router는 DHCP Server가 아니며 단지 DHCP Server와 DHCP Client를 연결하는 역할을 할 뿐입니다.

DHCP Relay를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
service dhcp	CONFIG	DHCP Service를 구동합니다.
ip dhcp relay helper-address <i>IP_Addr</i>	CONFIG	DHCP Server의 IP를 지정하여 DHCP Relay를 설정합니다.
ip dhcp relay interface <i>VLAN_NAME</i>	CONFIG	DHCP Relay를 구동할 Interface를 선택합니다.

DHCP Relay 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show ip dhcp	TOP	DHCP 설정 상태를 확인합니다.

DHCP Relay 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no service dhcp	CONFIG	DHCP Service를 초기화합니다.
no ip dhcp relay interface <i>VLAN_NAME</i>	CONFIG	설정된 DHCP Relay를 초기화합니다.
no ip dhcp relay helper-address [<i>IP_Addr</i>]	CONFIG	설정된 DHCP Relay의 DHCP Server IP를 초기화합니다.



참 고

1. DHCP Relay를 구동할 Interface는 최대 5개까지 설정할 수 있습니다.
2. DHCP Relay Helper Address는 최대 2개까지 설정할 수 있습니다.

<예제> DHCP Relay 설정

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#ip dhcp relay interface vlan1.1
At least one helper-address need,when relay interface exist.
SG2124G(config)#ip dhcp relay helper-address 1.1.1.1
SG2124G(config)#show running-config
!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
ip dhcp relay helper-address 1.1.1.1
ip dhcp relay interface vlan1.1
bridge 1 protocol pvstp
!
-- 이하 생략 --

SG2124G(config)#end
SG2124G#
SG2124G#show ip dhcp
dhcp server/relay enabled
dhcp pool list: <none>
vlan1.1 dhcp relay active
SG2124G#

```

2.12.3 DHCP Unleased-IP

DHCP Client에서 DHCP를 통해 IP Address를 할당 받지 않고 Static IP Address를 이용하여 인터넷을 사용함으로써 IP자원을 지속적으로 사용하는 것을 막기 위한 기능입니다.

DHCP Unleased-ip를 설정하면 DHCP Server에서 host로 보내는 DHCP ACK Packet을 Snoop하여 DHCP ACK Packet에서 Host에서 전달하는 IP Address 이외에 모든 Source IP Address는 Block하는 기능으로 Interface는 Any Packet에 대하여 Block상태에 있다가 DHCP Packet에 의해서 Open되도록 동작합니다. 이 때 DHCP ACK Packet의 Lease Time에 의해서 ACL이 생성되고 Timer가 Update되며 Dynamic과 Static으로 구분하여 설정 가능합니다.

DHCP Unleased-ip를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
ip dhcp unleased-ip acl	CONFIG	DHCP Unleased-ip 기능을 활성화합니다.
ip dhcp unleased-ip permit {IP_Addr range Low_IP_Addr High_IP_Addr}	CONFIG	DHCP Unleased-ip 중 허용할 Static IP Address를 설정합니다.

DHCP Unleased-ip를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show ip dhcp unleased-ip block-list	TOP	DHCP Unleased-ip를 통해 Block된 IP Address List를 확인합니다.
show ip dhcp unleased-ip permit [IP_Addr IP_Range]	TOP	DHCP Unleased-ip에서 허용한 Static IP Address List를 확인합니다.

DHCP Unleased-ip 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no ip dhcp unleased-ip acl	CONFIG	DHCP Unleased-ip 기능을 초기화합니다.
no ip dhcp unleased-ip permit {IP_Addr range Low_IP_Addr High_IP_Addr}	CONFIG	DHCP Unleased-ip 중 허용한 Static IP Address를 초기화합니다.

<예제> DHCP Unleased-ip 설정

- ip dhcp unleased-ip 설정.
- ip address 192.168.1.200는 고정 IP 통신 허용

```

SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#ip dhcp unleased-ip acl
SG2124G(config)#ip dhcp unleased-ip permit 192.168.1.200
SG2124G(config)#end
SG2124G#
SG2124G#show running-config
!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
ip dhcp pool 1
network 192.168.1.0 255.255.255.0
range 192.168.1.10 192.168.1.200
dns-server 192.168.10.11
default-router 192.168.1.254
lease 0 1 0
!
ip dhcp server interface vlan1.1
bridge 1 protocol pvstp
!
ip dhcp unleased-ip acl
ip dhcp unleased-ip permit 192.168.1.200
mls qos enable
mds enable ge1-22 detect
mds uplink ge23-24
!
-- 이하 생략 --

SG2124G#
SG2124G#show ip dhcp unleased-ip block-list
  IP Address      MAC Address      Interface      Index      Block-time
192.168.1.74      0021.00ab.ed7a   vlan1.1        0x59000187  Fri Apr 17 12:21:31 2009
192.168.1.78      0021.00ab.da43   vlan1.1        0x59000193  Fri Apr 17 12:25:01 2009

SG2124G#
SG2124G#show ip dhcp unleased-ip permit
  IP Address      Type
192.168.1.200     manual

SG2124G#

```

2.12.4 DHCP Option-82 설정

DHCP Server에서 다수의 DHCP Client에게 IP Address를 할당해야 할 때 DHCP Option-82를 사용하면 효율적으로 가입자들을 관리할 수 있습니다.

DHCP Option-82는 DHCP Relay Agent가 DHCP Request Packet에 Interface 번호와 Remote ID를 가진 Option-82라고 하는 정보를 덧붙여 보냄으로써 가입자를 인증하는 것입니다. 이 때 Interface 번호가 Remote ID 보다 우선 순위가 더 높습니다.

Option-82 정보가 없는 Request Packet을 받았을 때에는 자신의 정보를 첨부하며, Option-82에 기록된 Remote ID가 자신의 시스템 MAC Address와 동일할 경우에는 Option-82에서 지정한 Interface 번호로 Option-82를 제거한 후 전송합니다

DHCP Option-82에 대한 정책을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
ip dhcp relay information policy {append drop keep}	CONFIG	Option-82 Packet에 대한 정책을 설정합니다. (Packet의 정보 변경, 삭제, 전송)
ip dhcp relay information option	CONFIG	DHCP Relay를 설정한 경우 Option-82 사용 여부를 지정합니다.

DHCP Option-82에 대한 정책을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no ip dhcp relay information policy	CONFIG	Option-82 Packet에 대한 정책을 초기화합니다.
no ip dhcp relay information option	CONFIG	Option-82 사용 여부를 초기화합니다.

<예제> DHCP Option-82 및 정책 설정

```
SG2124G(config)#ip dhcp relay information policy keep
SG2124G(config)#ip dhcp relay information option
SG2124G(config)#exit
```

2.12.5 DHCP Snooping

DHCP Snooping 기능은 신뢰(Trust)할 수 있는 Interface에 DHCP Server가 존재하는 것으로 인식하여 신뢰할 수 없는 (Untrust) Interface로부터의 DHCP Offer, Ack Packet이 수신되는 경우와 Client Source MAC Address와 DHCP Packet내의 Client MAC Address가 다를 경우 Drop 하는 기능입니다.

VLAN에 DHCP Snooping을 Enable하면 모든 DHCP Packet은 CPU에서 Forwarding 하게 되며 VLAN은 최대 32개, DHCP Snooping Binding Entry는 최대 1024개까지 지원됩니다. DHCP Snooping Binding Entry의 최대 수치를 넘을 경우에는 Binding Table에 저장되지 않으며, 모든 Binding Entry는 30 s에 한번씩 Update하고 이 때 Lease Time 정보도 30 s씩 감소됩니다. DHCP Snooping Option-82 는 2단 구성 이상에서도 동작해야 하며, 수신된 DHCP Packet에 option-82가 없을 경우 삽입하여 Server로 전송하고 Server로부터 수신된 option-82 정보가 자신이 삽입한 것일 경우만 삭제하는 기능입니다.

DHCP Snooping의 과정은 다음과 같습니다.

1. DHCP Server가 연결되어 있는 Interface등에 대해서는 Trust Interface로 설정하면 설정되지 않은 나머지 Interface들은 모두 Untrust Interface로 설정됩니다.
2. Trust Interface로부터의 DHCP Reply를 정상으로 인정하고, Untrust Interface로부터의 DHCP Reply은 Drop 처리하거나 해당 Interface를 Disable 처리합니다.
3. 정상으로 수신되는 DHCP Reply Packet의 정보를 기반으로 Client의 MAC Address, Server로부터 부여된 IP Address, Lease 기간 등을 Binding Entry에 Update합니다.
4. DHCP Packet 정보 중 Client가 Request도 하지 않았는데 Server로부터 Reply Packet이 발생한 경우 또는 Request와 Reply 상호간의 Source IP Address가 다른 경우가 발생하면 경고 및 해당 Interface의 Disable처리될 수 있습니다.



참고

1. DHCP Snooping을 설정할 수 있는 VLAN은 최대 32개까지입니다.
2. DHCP Snooping Binding Entry로 저장되는 개수는 1024개이며 초과되는 Entry는 저장되지 않습니다.

DHCP Snooping을 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
ip dhcp snooping	CONFIG	DHCP Snooping 기능을 활성화합니다.
ip dhcp snooping vlan <i>RANGE</i>	CONFIG	특정 VLAN에 DHCP Snooping 기능을 활성화합니다.
ip dhcp snooping information option 82	CONFIG	DHCP Snooping에서 Option-82 정보를 추가합니다.
ip dhcp snooping trust	INTERFACE	Interface를 Trust로 설정합니다.

DHCP Snooping을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show ip dhcp snooping	TOP	DHCP Snooping 설정 상태를 확인합니다.
show ip dhcp snooping { binding statistics [interface <i>IFNAME</i>] }	TOP	DHCP Binding Table / Counter 정보를 확인합니다.

DHCP Snooping 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no ip dhcp snooping	CONFIG	DHCP Snooping 기능을 비활성화합니다.
no ip dhcp snooping vlan <i>RANGE</i>	CONFIG	특정 VLAN에 DHCP Snooping 기능을 비활성화합니다.
no ip dhcp snooping information option 82	CONFIG	DHCP Snooping에 추가된 Option -82 정보를 초기화합니다.
no ip dhcp snooping trust	INTERFACE	Trust로 설정된 Interface를 초기화합니다.
clear ip dhcp snooping binding [interface <i>IFNAME</i> vlan <1-4094>]	CONFIG	DHCP snooping binding entry들을 초기화합니다.
clear ip dhcp snooping statistics [interface <i>IFNAME</i>]	CONFIG	DHCP snooping counter들을 초기화합니다.

<예제> DHCP Snooping 설정

- ip dhcp Snooping 설정.
- DHCP Server를 ge1, ge2에 연결 후 ge1만 Trust Interface로 설정

```
SG2124G(config)#ip dhcp snooping
SG2124G(config)#ip dhcp snooping vlan 1
SG2124G(config)#ip dhcp snooping information option 82
SG2124G(config)#interface ge1
SG2124G(config-if)#ip dhcp snooping trust
SG2124G(config-if)#end
SG2124G#sh ip dhcp snooping statistics interface ge2
```

DHCP snooping statistic counters for interface ge2

Discover	: 0
Discover dropped	: 0
Offer	: 0
Offer dropped	: 8
Request	: 0
Request dropped	: 0
Ack	: 0
Ack dropped	: 0
Nack	: 0
Nack dropped	: 0
Release	: 0
Release dropped	: 0
Inform	: 0
Inform dropped	: 0
Decline	: 0
Decline dropped	: 0

```
SG2124G#sh ip dhcp snooping statistics interface ge1
```

DHCP snooping statistic counters for interface ge1

Discover	: 0
Discover dropped	: 0
Offer	: 3
Offer dropped	: 0
Request	: 0
Request dropped	: 0
Ack	: 2
Ack dropped	: 0
Nack	: 0
Nack dropped	: 0
Release	: 0
Release dropped	: 0
Inform	: 0
Inform dropped	: 0
Decline	: 0
Decline dropped	: 0

2.13 ERP

ERP(Ethernet Ring Protection)란 Layer2 상에서 loop 없이 Ethernet Ring 구성을 할 수 있도록 해주는 Protocol 입니다. Ethernet 으로 ring을 구성 시 Ethernet 특성상 loop가 발생하나, G.8032 에서는 Ring Protection Link 라 불리는 링크를 block 시켜서 loop를 방지합니다. 정상 링크 단절 시 signal fail R-APS frame 을 다른 노드에 전달함으로써, Ring Protection Link 를 다시 unblock 하여 ring 이 정상동작 할 수 있도록 합니다.

RPL(Ring Protection Link)을 가지고 제어하는 노드를 RPL Owner, RPL 과 연결된 노드를 RPL Neighbor라 하며, 링 구성을 위하여 RPL owner와 RPL neighbor가 요구됩니다. RPL Owner와 RPL Neighbor로 설정할 노드에 각각 rpl 포트를 지정하고, RPL Owner는 rpl-owner 명령어로 지정합니다. rpl-owner로 지정되지 않은 노드는 자동으로 rpl neighbor로 인식됩니다.

ERP는 총 16개의 인스턴스 생성이 가능합니다. 버전은 V1과 V2 선택 설정이 가능합니다.

■ Version 1 에서 지원 가능한 기능

Signal Fail

Signal Fail recovery

■ Version 2 에서 지원 가능한 기능

Signal Fail

Signal Fail recovery

Manual Switch

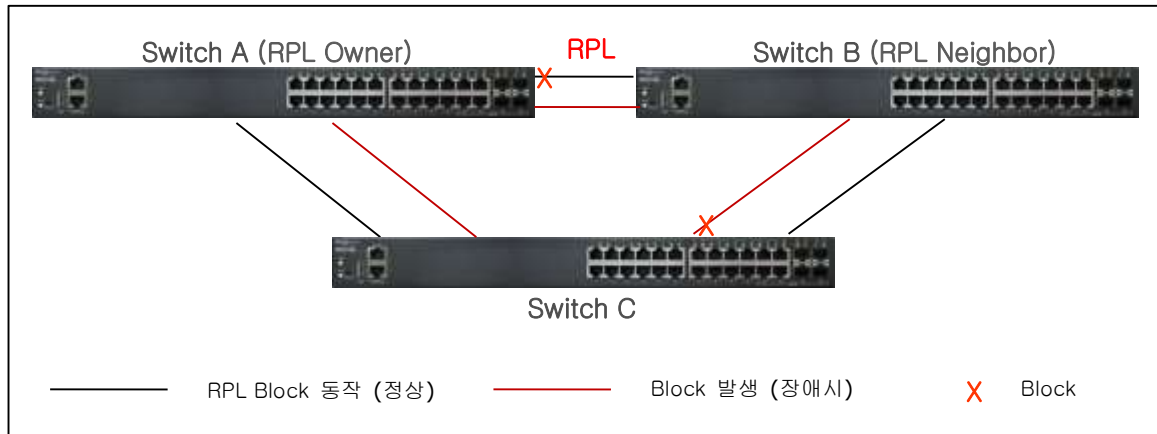
Forced Switch

Non-revertive

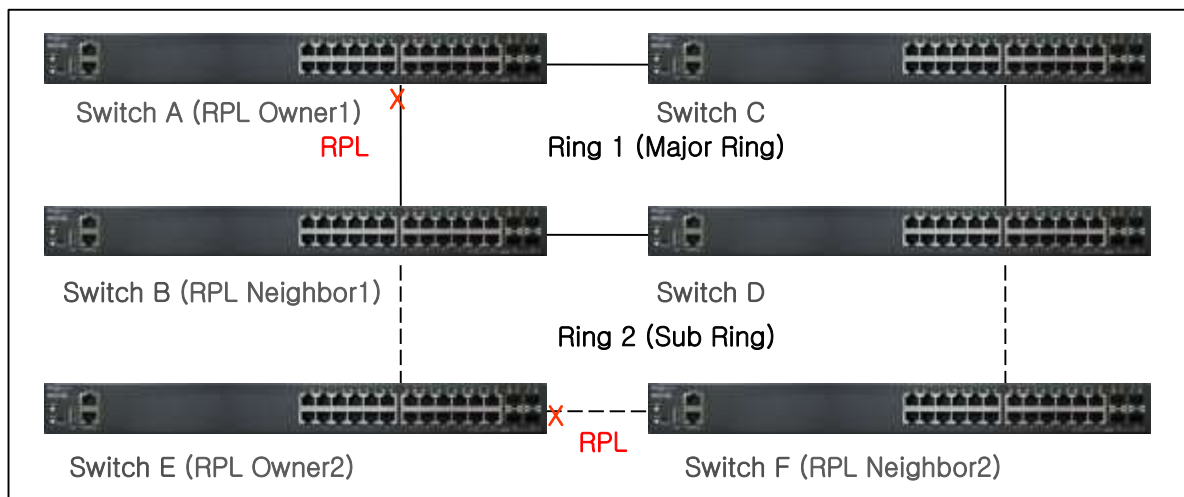
Interconnected rings

RPL Neighbor

[그림 2-17] ERP Single Ring 연결 구성



[그림 2-18] ERP Multi Ring 연결 구성



ERP를 설정하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
erp NAME	CONFIG	ERP Name을 설정합니다.
port0 interface IFNAME	ERP	ERP port0을 설정합니다.
port1 interface IFNAME	ERP	ERP port1을 설정합니다.
rpl {port0 port1}	ERP	rpl 포트를 설정합니다.
rpl-owner	ERP	rpl owner를 설정합니다.

enable-erp	ERP	ERP를 활성화 합니다
version {v1 v2}	ERP	호환 버전을 설정합니다.
sub-ring	ERP	Subring을 설정합니다.
propagate-tc	ERP	다른 링에서 발생한 topology 변경을 전달하는 기능을 활성화합니다.
non-revertive-mode	ERP	Node가 Protection으로 전환 후 복구를 자동으로 수행하도록 설정합니다.
forced-switch [port0 port1]	ERP	지정된 포트가 Signal Fail 여부와 상관없이 block을 수행하도록 설정합니다.
manual-switch [port0 port1]	ERP	지정된 포트가 Signal Fail이 없을 경우에만 block을 수행하도록 설정합니다.
timer wtr <5-12>	ERP	Signal Fail 시 복구 시간을 설정합니다. (단위 : min)
timer wtb <5000-7000>	ERP	block이 동작하는 시간을 설정합니다.

ERP 상태를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show erp [NAME detail]	TOP	ERP 설정 상태를 확인합니다.

ERP 설정을 초기화하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
clear erp { timer NAME timer } { wtr wtb guard holdoff }	Top	ERP 설정을 복구합니다.
no erp NAME	CONFIG	ERP 설정을 삭제 합니다.
no port0	ERP	ERP port0 설정을 초기화 합니다.
no port1	ERP	ERP port1 설정을 초기화 합니다.
no rpl	ERP	rpl 포트 설정을 초기화 합니다.
no rpl-owner	ERP	rpl owner 설정을 초기화 합니다.
no enable-erp	ERP	ERP를 비활성화 합니다

no version	ERP	Version 설정을 초기화 합니다.
no sub-ring	ERP	Subring 설정을 초기화 합니다.
no propagate-tc	ERP	다른 링에서 발생한 topology 변경을 전달하는 기능을 비활성화합니다.
no non-revertive-mode	ERP	Node가 Protection 으로 전환 후 복구를 자동으로 수행하는 기능을 해제합니다.
no forced-switch	ERP	Signal Fail 여부와 상관없이 block 을 수행하는 기능을 해제합니다.
no manual-switch	ERP	Signal Fail 이 없을 경우에만 block 을 수행하는 기능을 해제합니다.
no timer wtr	ERP	Signal Fail 시 복구 시간을 초기화 합니다.
no timer wtb	ERP	block 이 동작하는 시간을 초기화 합니다.



참고

1. Ring 을 구성하는 모든 스위치에는 ERP 설정이 되어 있어야 합니다.
2. Ring 에는 최소 하나의 RPL과 RPL Owner node, RPL Neighbor node 가 있어야 합니다.
3. ERP node 에는 두개의 포트가 요구됩니다. (단, sub-ring 이용시에는 링크가 하나만 있어도 됩니다.)
4. Subring 이용시, subring 소속 노드 전체에 sub-ring 설정이 되어 있어야 합니다.
5. ERP 기능은 Switch버전 2.x 이상에서만 지원합니다.

<예제1> ERP- Single Ring 설정

< ERP Single Ring >

1. A(RPL Owner)

```
SG2124G#configure terminal
SG2124G(config)#erp erp1
SG2124G(config-erp)#port0 interface ge1
SG2124G(config-erp)#port1 interface ge2
SG2124G(config-erp)#rpl port1
SG2124G(config-erp)#rpl-owner
SG2124G(config-erp)#enable-erp
SG2124G(config-erp)#end
```

2. B(RPL Neighbor)

```

SG2124G#configure terminal
SG2124G(config)#erp erp1
SG2124G(config-erp)#port0 interface ge1
SG2124G(config-erp)#port1 interface ge2
SG2124G(config-erp)#rpl port0
SG2124G(config-erp)#enable-erp
SG2124G(config-erp)#end

```

3. C

```

SG2124G#configure terminal
SG2124G(config)#erp erp1
SG2124G(config-erp)#port0 interface ge1
SG2124G(config-erp)#port1 interface ge2
SG2124G(config-erp)#enable-erp
SG2124G(config-erp)#end

```

SG2124G#show erp erp1 → A Switch

Name	Node State	Ring Link	Link State
erp1		port0(ge1)	Forwarding
Idle		port1(ge2)	Blocked

SG2124G#show erp erp1 → B Switch

Name	Node State	Ring Link	Link State
erp1		port0(ge1)	Blocked
Idle		port1(ge2)	Forwarding

SG2124G#show erp erp1 → C Switch

Name	Node State	Ring Link	Link State
erp1		port0(ge1)	Forwarding
Idle		port1(ge2)	Forwarding

<예제2> ERP – Multi Ring 설정

< ERP Multi Ring >

1. A(RPL Owner)

erp1SG2124G#**configure terminal**

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

SG2124G(config)#**erp erp1**SG2124G(config-erp)#**port0 interface ge1**SG2124G(config-erp)#**port1 interface ge2**SG2124G(config-erp)#**rpl port1**SG2124G(config-erp)#**rpl-owner**SG2124G(config-erp)#**enable-erp**SG2124G(config-erp)#**end**

2. B(RPL Neighbor)

erp1SG2124G#**configure terminal**

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

SG2124G(config)#**erp erp1**SG2124G(config-erp)#**port0 interface ge1**SG2124G(config-erp)#**port1 interface ge2**SG2124G(config-erp)#**rpl port0**SG2124G(config-erp)#**enable-erp**SG2124G(config-erp)#**end****erp2**SG2124G#**configure terminal**

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

SG2124G(config)#**erp erp2**SG2124G(config-erp)#**port0 interface ge3**SG2124G(config-erp)#**sub-ring**SG2124G(config-erp)#**enable-erp**SG2124G(config-erp)#**end**

3. C

erp1SG2124G#**configure terminal**

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

SG2124G(config)#**erp erp1**SG2124G(config-erp)#**port0 interface ge1**SG2124G(config-erp)#**port1 interface ge2**SG2124G(config-erp)#**enable-erp**SG2124G(config-erp)#**end**

4. D

erp1SG2124G#**configure terminal**

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

SG2124G(config)#**erp erp1**SG2124G(config-erp)#**port0 interface ge1**SG2124G(config-erp)#**port1 interface ge2**SG2124G(config-erp)#**enable-erp**SG2124G(config-erp)#**end****erp2**SG2124G#**configure terminal**

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

```

SG2124G(config)#erp erp2
SG2124G(config-erp)#port0 interface ge3
SG2124G(config-erp)#sub-ring
SG2124G(config-erp)#enable-erp
SG2124G(config-erp)#end

```

5. E(RPL Owner)

```

erp2
SG2124GP#configure terminal
SG2124GP(config)#erp erp2
SG2124GP(config-erp)#port0 interface ge1
SG2124GP(config-erp)#port1 interface ge2
SG2124GP(config-erp)#rpl port1
SG2124GP(config-erp)#rpl-owner
SG2124GP(config-erp)#sub-ring
SG2124GP(config-erp)#enable-erp
SG2124GP(config-erp)#end

```

6. F(RPL Neighbor)

```

erp2
SG2124GP#configure terminal
SG2124GP(config)#erp erp2
SG2124GP(config-erp)#port0 interface ge1
SG2124GP(config-erp)#port1 interface ge2
SG2124GP(config-erp)#rpl port0
SG2124GP(config-erp)#sub-ring
SG2124GP(config-erp)#enable-erp
SG2124GP(config-erp)#end

```

SG2124G#show erp → A Switch

Name			
Node	State	Ring Link	Link State
=====			
erp1		port0(ge1)	Forwarding
Idle		port1(ge2)	Blocked

SG2124G#show erp → B Switch

Name			
Node	State	Ring Link	Link State
=====			
erp1		port0(ge1)	Blocked
Idle		port1(ge2)	Forwarding

Name			
Node	State	Ring Link	Link State
=====			
erp2		port0(ge3)	Forwarding
Idle		port1(N/A)	N/A

SG2124G#show erp → C Switch

Name			
Node	State	Ring Link	Link State
=====			
erp1		port0(ge15)	Forwarding
Idle		port1(ge16)	Forwarding

SG2124G#show erp → D Switch

Name	Node State	Ring Link	Link State
erp1	Idle	port0(ge1)	Forwarding
		port1(ge2)	Forwarding
Name	Node State	Ring Link	Link State
erp2	Idle	port0(ge3)	Forwarding
		port1(N/A)	N/A

SG2124GP#show erp → E Switch

Name	Node State	Ring Link	Link State
erp2	Idle	port0(ge1)	Forwarding
		port1(ge2)	Blocked

SG2124GP#show erp → F Switch

Name	Node State	Ring Link	Link State
erp2	Idle	port0(ge1)	Blocked
		port1(ge2)	Forwarding

제3장. Routing Protocol

3.1 BGP Routing Protocol

Border Gateway Protocol(BGP)은 외부 네트워크와 연결하는 EGP(Exterior Gateway Protocol)입니다.

BGP는 서로 다른 관리도메인(Autonomous System) 간에 정보를 주고 받을 수 있도록 라우팅 정보를 관리합니다. BGP 경로는 패킷이 경유하는 네트워크 번호와 관리 도메인 번호 등으로 이루어져 있습니다.

BGP는 RFC 문서 1163, 1267에 정의되어 있으며, SG Series Switch는 RFC 1771에 정의된 BGP 버전 4를 지원합니다.

BGP버전 4는 라우팅 테이블의 크기를 줄이기 위해 네트워크에서 IP주소대신 IP Prefix를 경로로 제공합니다. CIDR (Classless Inter-Domain Routing)을 이용하여 통합경로(Aggregate Route)를 제공하며, OSPF와 RIP도 CIDR 경로로 전달할 수 있습니다. BGP를 사용하는 주된 목적은 BGP 장비사이의 AS와 AS에 도달하는 경로를 교환하여 라우팅 루프를 방지하고 가장 효율적인 AS 정보를 채택하도록 하기 위함입니다.

사용자는 Route-Map을 이용하여 MED(Multi Exit Discriminator) 값을 설정할 수 있습니다. 새로운 라우팅 정보가 Neighbor BGP 라우터에 전달 될 때, MED값은 변하지 않습니다. 따라서 동일한 AS 내에 위치한 BGP 라우터들은 동일한 기준으로 경로를 선택할 수 있습니다.

3.1.1 기본설정

BGP 설정은 크게 기본 설정과 고급 설정으로 나눌 수 있습니다. 다음은 BGP 기본 설정내용입니다.

- BGP 라우팅 활성화
- BGP Neighbor 라우터 설정
- 라우팅 정책 변경
- BGP Weights 설정
- AS 경로 사용 중지
- BGP 경로 필터링
- AS 경로 필터링
- Prefix 리스트를 이용한 BGP 필터링
- 다음 목적지로 정보 전달 차단
- BGP 버전 설정

3.1.2 BGP Routing 활성화

AS 번호는 관리 도메인(Autonomous System) 번호로 BGP 네트워크를 구분하기 위해 사용하며, 1부터 65535까지 사용할 수 있으며 65512에서 65535까지는 사설 AS 번호로 정의되어 있습니다. 사설 AS는 로컬 네트워크에서만 사용할 수 있으며, 외부로 연결될 수 없습니다.

Ethernet Ring Protection 상태를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
router bgp <1-65535>	CONFIG	AS 번호를 지정, BGP 라우팅을 설정합니다.

<예제> BGP Routing 활성화

```
SG2124GX#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124GX(config)#router bgp 32
SG2124GX(config-router)#
```

3.1.3 BGP Neighbor Router 설정

BGP는 Neighbor 라우터를 설정해야 합니다. BGP Neighbor 라우터에는 동일한 AS에 위치한 내부 Neighbor 라우터와 다른 AS에 속한 외부 Neighbor 라우터가 있으며, 보통 동일한 AS안에 있는 내부 Neighbor 라우터는 직접 연결되어 있지 않지만 외부 Neighbor 라우터들은 직접 연결되어 상대방의 서브 네트워크를 공유합니다.

BGP에 사용할 네트워크를 지정하고, BGP 라우팅 테이블에 등록합니다.

명령어	모드	기능
neighbor ip-address remote-as number	ROUTER (BGP)	BGP Neighbor 라우터를 설정합니다.

<예제> BGP Neighbor와 대항측 AS Number를 설정합니다.

```
SG2124GX#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124GX(config)#router bgp 32
SG2124GX(config-router)#neighbor 192.168.254.254 remote-as 10
```

3.1.4 Routing 정책 변경

라우팅 정책은 Neighbor 라우터와 라우팅 정보를 주고 받을 때 route-map, distribute-list, prefix-list, filter-list 등을 이용하여 어떤 정보를 받아 들이고 어떤 정보를 제공할 것인지 결정합니다. BGP 라우터는 라우팅 정책이 변경되면, 기존 정책을 따르는 라우팅 정보를 삭제하거나 원래 경로를 복구(route reset)하여 새로운 정책에 맞춰 라우팅 정보를 수정해야 합니다. BGP 라우터가 새로운 정책과 부합하는 정보를 받아 들이도록 하려면 Inbound reset을 설정하고 새로운 정보를 제공하도록 하려면 Outbound reset을 설정합니다.

BGP 라우터가 새로운 정책에 맞추어 새로운 정보를 제공하면 Neighbor 라우터들도 새로운 정보를 받아 들이게 됩니다.

만약 사용자의 네트워크에 위치한 BGP 라우터와 Neighbor 라우터가 모두 Route Refresh Capability 기능을 지원한다면 Inbound Reset을 이용하여 라우팅 정보를 갱신할 수 있습니다. 이 방법을 이용한 라우터 재설정은 다음과 같은 장점이 있습니다.

- 관리자가 따로 설정할 필요 없음
- 라우팅 정보 변경에 따른 추가 메모리 필요 없음

Neighbor 라우터가 route refresh capability 기능을 지원하는지 확인하려면 라우터 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
neighbor ip-address capability route-refresh	ROUTER (BGP)	Route Refresh Capability 기능을 Neighbor 라우터에게 알립니다. Neighbor 라우터도 이 기능을 지원한다면, 다음과 같은 메시지가 출력됩니다 : Received Route Refresh Capability From Peer.

만약 모든 BGP 라우터가 route refresh capability를 지원한다면, 사용자는 soft reset 기능을 이용하여 이전에 보낸 경로 정보를 받아 볼 수 있습니다.

새로운 정책에 부합하는 라우팅 정보를 설정하려면 다음과 같은 명령어를 사용하십시오.

명령어	모드	기능
<code>clear ip bgp [* AS address] soft in</code>	TOP	새로운 정보를 반영합니다. 새로운 정보를 받는 네트워크 주소나 AS를 지정할 수 있는데 변수로 Wildcard(*)를 사용하면 모든 곳에서 새로운 정보를 반영합니다.

Outbound Reset 기능은 별도의 사전 설정을 필요로 하지 않습니다. **soft** 라는 명령어를 사용하여 라우팅 정보를 다시 전송합니다. 라우팅 정보를 다시 제공하려면, TOP 모드에서 다음과 같은 명령어를 사용하십시오.

명령어	모드	기능
<code>clear ip bgp [* AS address] soft out</code>	TOP	라우팅 정보를 제공하는 곳에서 Route Refresh Capability를 수행합니다. 정보를 전하는 곳으로 네트워크 주소나 AS를 지정합니다. 변수 별표(*)는 모든 곳에서 라우팅 정보를 전달합니다.

관리자가 변경된 라우팅 정책을 초기 상태로 복구할 때에는 **Route Refresh Capability** 기능을 사용합니다. 이 기능을 사용하면 각각의 변경된 내용을 하나씩 삭제하지 않아도 되는 편리함이 있습니다.

한편, **Route Refresh Capability**를 지원하지 못하는 장비의 경우에는 **neighbor x.x.x.x soft-reconfiguration** 명령어를 사용하여 기존에 주고 받던 라우팅 정보를 삭제해야 합니다. 그러나 이것은 네트워크에 문제점이 발생하는 원인이 될 수 있으므로 가급적 피하는 것이 좋습니다.

BGP 정보를 재 설정하지 않고 새로운 정보를 생성하려면 BGP 라우터는 라우팅 정보를 선별적으로 처리하지 말고 BGP 네트워크로 들어 오는 모든 정보를 저장해야 합니다. 이 방법은 메모리 부하를 야기 시키기 때문에 가능한 사용하지 않는 것이 좋습니다. 반면에 변경된 정보를 제공하는 것은 메모리를 요구하지 않습니다. BGP 라우터가 새로 변경된 정보를 전달하면 연쇄적으로 Neighbor 라우터는 변경된 정보를 받아 들이게 됩니다.

저장된 라우팅 정책을 이용하여 **BGP** 설정을 바꾸려면, **Router** 설정 모드에서 다음 명령어를 사용하십시오.

1 단계 **BGP** 라우터를 재 설정한 후 **Neighbor** 라우터가 보내온 정보를 저장하도록 설정합니다. 이 시점부터 **BGP** 라우터에 들어 오는 모든 정보는 저장됩니다.

명령어	모드	기능
neighbor ip-address soft-reconfiguration inbound	ROUTER (BGP)	BGP 라우터를 재 설정한 후 Neighbor 라우터가 보내온 정보를 저장합니다.

2 단계 저장된 정보를 이용하여 새롭게 변경된 정보를 테이블에 등록하도록 합니다.

명령어	모드	기능
clear ip bgp [* as-number] soft in	TOP	저장된 정보를 이용하여 새롭게 변경된 정보를 테이블에 등록합니다. 이때 정보가 들어 오는 곳으로 네트워크 주소나 AS, 모든 곳 (*)을 지정할 수 있습니다.

라우팅 테이블과 **BGP Neighbor** 라우터를 통해 라우팅 정보가 제대로 변경되었는지 확인하려면 **Top** 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
show ip bgp neighbors ip-address [advertised-routes received-routes routes]	TOP	Neighbor 라우터로 전달하거나 전달 받은 정보를 출력합니다.

3.1.5 BGP Weights 설정

Weight는 경로에 할당하는 숫자 값으로 경로 선택 시 선택 기준이 됩니다. Weight는 BGP 내부 망에서만 유효한 값으로 0~65535까지 사용 가능합니다. 만약 특정 라우터가 보내주는 정보를 우선시하려면 해당 라우터에서 전송한 정보에 높은 weight를 부여하면 됩니다. BGP weight를 설정하려면 Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
neighbor ip-address weight <0-65535>	Router (BGP)	Router Neighbor 라우터가 보내 주는 정보에 Weight를 부여합니다.

3.1.6 AS 경로 무시

기본적으로 SG Series Switch는 경로를 결정하는 기준의 하나로 AS 경로를 사용합니다. 그러나 IETF 표준 안을 따르면, AS 경로를 고려하지 않아야 합니다.

경로를 선택할 때 AS에 도착하기 위해 필요한 경로 길이를 무시하려면, Router 설정 모드에서 다음과 같은 명령어를 사용하십시오.

명령어	모드	기능
bgp bestpath as-path ignore	Router (BGP)	경로를 선택할 때 AS까지 가는 경로 길이를 무시 합니다.

3.1.7 AS 경로 사용중지

만일 시스템이 특정 라우팅 정보를 제한하고 싶다면 **Neighbor** 라우터와 주고 받는 정보를 선별 처리해서 받아 들일 수 있습니다. 이때 사용자는 **Access List** 나 **Prefix List**를 설정하고 설정한 기준에 맞추어 라우팅 정보를 걸러냅니다.

BGP 라우팅 정보를 선별하려면, **Router** 설정 모드에서 다음과 같은 명령어를 사용 하십시오.

명령어	모드	기능
neighbor ip-address distribute-list access-list-name {in out}	Router (BGP)	Access List를 적용하여 특정 네트워크를 통해 나가거나 들어오는 정보를 선별 처리합니다.



참고

Distribute List 는 BGP 내부 네트워크에서만 사용 가능합니다.

3.1.8 AS 경로 필터링

BGP 망에서 네트워크 주소를 기준으로 정보를 제한했듯이 AS를 경유하는 정보에 대해서도 선별적인 처리가 가능합니다. 경로를 선별하기 위해 적용되는 정책들은 Access List 에 등록됩니다. AS를 기준으로 라우팅 정보를 제한하려면 Access List 에 제한 정책을 설정한 후 이 정책들을 Neighbor 라우터에 적용 하십시오.

다음은 AS가 전달하는 경로를 제한하는 방법입니다.

1 단계 특정 AS를 access list에 정의한다.

명령어	모드	기능
ip as-path access-list access-list-number {permit deny} expression	CONFIG	특정 AS를 Access List에 정의합니다.

2 단계 Router 설정 모드로 들어갑니다.

3 단계 앞서 정의한 Access List를 적용하여 해당 AS가 전달하거나 전달 받는 정보를 제한한다.

명령어	모드	기능
neighbor ip-address filter-list access-list-number {in out}	Router (BGP)	앞서 정의한 Access List를 적용하여 해당 AS가 전달 하거나 전달 받는 정보를 제한합니다.

3.1.9 Prefix List를 이용한 BGP 필터링

BGP 경로를 제한할 때에는 다음과 같은 이유로 Access List 대신 Prefix List를 많이 사용합니다.

- 필터 목록이 방대할 경우 등록된 내용을 검색하고 적용하는 시간이 절약됩니다.
- 필터 목록에 무한대로 정책을 등록할 수 있습니다.
- 사용법이 간편합니다.

Prefix List를 적용하려면, 사용자는 반드시 사전에 Prefix List를 설정해야 합니다. 사용자는 Prefix List에 등록되는 정책마다 번호를 부여할 수 있습니다

■ Prefix List를 이용한 트래픽 필터링 동작 방식

prefix list를 이용한 필터링은 필터 리스트에 정의한 정책을 네트워크에 적용하여 라우팅 정보를 선별 처리합니다. 필터 리스트에 정의한 정책대로 경로를 선별 처리하는 것은 access list 와 유사하지만 다음과 같은 좀 더 세부적인 규제 사항이 있습니다.

- Prefix List에 정의된 정책이 없으면 모든 네트워크 정보를 허용합니다.
- 네트워크에 적용한 정책이 Prefix List에 정의되어 있지 않다면 해당하는 네트워크 정보는 거부 합니다.
- 하나의 네트워크에 적용되는 정책들이 여러 개 존재할 때 번호로 각 정책을 식별하고 가장 작은 번호를 갖는 정책이 실제 적용되는 정책입니다.

라우터는 Prefix List의 맨 위부터 차례로 정책을 검색 합니다. 만일 해당하는 정책을 찾으면, 남아있는 나머지 정책은 검색할 필요가 없습니다. 검색의 효율성을 위해 사용자는 ip prefix-list 명령어에서 제공하는 seq를 사용하여 가장 자주 사용하는 정책들을 목록 상단에 배치할 수도 있습니다.

show ip prefix-list 명령어는 정책에 부여된 일련 번호를 출력해 줍니다. 사용자가 설정한 정책에는 일련 번호가 자동적으로 부여됩니다. 만약 사용자가 자동적으로 번호가 지정되지 못하도록 설정했다면 반드시 ip prefix-list 명령어를 사용하여 각 정책에 번호를 지정해야 합니다.

◇ Prefix list 생성

prefix list를 생성하려면, CONFIG 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
ip prefix-list name {deny permit} [description description] [seq value] prefix [ge value] [le value]	CONFIG	Prefix List를 생성할 때 목록 이름을 지정합니다.
ip prefix-list name {deny permit} [description description] [seq value] any		모든 네트워크에 적용되는 Prefix List를 생성합니다.
ip prefix-list name description description		Prefix List에 추가 설명을 입력합니다.



참고

Prefix list를 생성하려면 사용자는 반드시 permit이나 deny 항목을 입력해야 합니다.

◇ Prefix List 정책 설정

Prefix List에 정책을 하나씩 추가할 수 있습니다.

Prefix List에 정책을 추가하려면 CONFIG 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
ip prefix-list name seq value {deny permit} {any prefix} [ge value] [le value]	CONFIG	Prefix List에 정책을 설정하고 정책에 번호를 부여합니다.

선택적으로 입력할 수 있는 ge와 le 속성은 여러 개의 네트워크를 지정할 때 사용합니다. ge와 le속성 둘 다 사용하지 않으면 네트워크 범위가 좀 더 명확하게 설정됩니다. 만일 ge 속성만 설정되어 있으면 ge-value 에서 32 비트까지, le 속성만 설정되어 있으면 넷마스크에서 le-value까지가 네트워크 범위로 설정됩니다.

◇ **Prefix List**에 등록된 정책 출력

Prefix 테이블과 관련된 정보를 출력하려면, 다음 명령어들을 사용하십시오.

명령어	모드	기능
show ip prefix-list [detail summary]	TOP	사용자가 설정한 모든 Prefix List를 출력합니다. Prefix List를 생성할 때 목록 이름을 지정합니다
show ip prefix-list [detail summary] name		지정한 Prefix List에 들어 있는 정책들을 출력합니다
show ip prefix-list name [seq number]		지정한 번호에 해당하는 정책을 출력합니다.
show ip prefix-list name [prefix]		지정한 네트워크에 적용하는 정책을 출력합니다.
show ip prefix-list name [prefix] longer		지정한 네트워크에 적용하는 Prefix List의 모든 정책을 출력합니다.
show ip prefix-list name [prefix] first-match		지정한 네트워크에 적용되는 첫 번째 정책을 출력합니다.

◇ **Prefix** 테이블 조회 수 삭제

Prefix List의 조회 수를 삭제하려면 CONFIG 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
clear ip prefix-list name [prefix]	TOP	Prefix List 조회 수를 삭제한다. 기본적으로 시스템은 Prefix List의 조회 수를 기록합니다.

3.1.10 다음 목적지로의 정보전달차단

새롭게 변경된 라우팅 정보가 다음 목적지로 전달되지 못하게 막을 수 있습니다.

이 기능은 **FrameRelay**처럼 시스템들이 동일한 **IP** 네트워크에 연결되어 있지 않을 때 유용합니다. 라우팅 정보가 다음 목적지로 전달되는 것을 막는 방법에는 다음이 두 가지가 있습니다.

- **Neighbor** 라우터 주소 대신 다른 주소 설정
 - **Route-map**을 사용하여 **Neighbor** 라우터로부터 정보를 전달 받고, 로컬 **BGP** 라우터가 정보를 배포하도록 설정
- ◇ 다른 주소를 이용한 라우팅 정보 차단

다음 목적지 주소 대신에 다른 주소를 지정하여 라우팅 정보가 다음 목적지로 전달되지 않게 하려면, **Router** 설정 모드에서 다음 명령어를 사용하십시오

명령어	모드	기능
neighbor ip-address next-hop-self.	Router (BGP)	다음 목적지로 라우팅 정보가 전달되는 것을 막습니다.

이 명령어는 **Neighbor** 라우터 주소 대신에 라우터 자신의 주소를 알려서 다른 **BGP** 라우터들이 주소로 정보를 전달하게 합니다. 이는 라우팅 정보를 전달 받을 특정 주소를 지정하는 것보다 보다 효율적입니다.

◇ **Route-map**을 이용한 라우팅 정보 차단

BGP 경로를 전달 받는 다음 지점이 **Neighbor** 라우터가 되도록 하려면 **set ip next-hop** 명령어를 사용하십시오.

BGP 정보를 전달 받을 다음 지점으로 **Neighbor** 라우터를 설정하려면 **Route Map** 설정 명령어를 사용하십시오.

명령어	모드	기능
set ip next-hop ip-address	Route-map	BGP 정보를 전달할 다음 목적지로 Neighbor 라우터와 연결된 사용자의 BGP 라우터를 지정하고 BGP 정보를 전달할 다음 목적지로 Neighbor 라우터 주소를 설정합니다

3.1.11 BGP 버전설정

시스템은 기본적으로 BGP 버전 4를 합니다. 지정한 BGP 버전으로 Neighbor 라우터와 통신하려면 Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
neighbor ip-address version 4	Router (BGP)	Neighbor 라우터와 통신할 때 사용할 BGP 버전을 지정합니다.

3.2 BGP 고급설정

기본 설정이 끝나면 보다 자세한 고급 설정으로 들어갈 수 있습니다. 다음은 BGP 고급 설정에서

설명할 내용입니다.

- Route-map을 이용한 경로 변경
- 통합 주소(Aggregate Address) 설정
- BGP Community 필터링 설정
- 라우터 식별 번호 설정
- BGP에 경로 배포하기
- 라우팅 도메인 연합 설정
- 경로 반영자 (Route Reflector) 설정
- Neighbor 명령어를 이용한 설정
- Neighbor 라우터 동작 종료
- Backdoor 경로 지정
- NLRI 유형 결정
- 거리값 설정
- BGP 시간 조정
- 전달 받은 정보 (Import Network) 점검
- 첫 번째 AS 설정
- 로컬 네트워크의 우선 순위 변경
- 라우터 ID에 기준한 경로 선택
- MED 없는 경로를 최악의 경로로 간주
- AS들이 전달한 MED 값으로 AS 경로 선택
- MED를 이용한 연합 경로 선택
- MED를 이용한 연합 내 경로 선택
- 반영된 경로 저장
- 경로 무효화 (Route Dampening)
- BGP 점검과 관리

3.2.1 Route-Map을 이용한 경로변경

Route-map을 사용하여 경로를 선별 처리하거나 다양한 속성들을 변경할 수 있습니다. Route-map은 전달 받는 정보나 배포하는 정보 둘 다 적용 가능합니다.

Route-map을 정의하면 Route-map에 부합하는 경로만 전달 받거나 배포할 수 있습니다. 라우팅 정보는 AS 경로, Community, 네트워크 번호를 기준으로 선별 처리됩니다.

AS 경로는 as-path access-list 명령어로, Community 는 community-list 명령어로, 네트워크는 ip access-list 명령어를 사용하여 처리 조건을 규정합니다.

Route-map을 정의하려면 Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
neighbor ip-address route-map route-map -name {in out}	Router (BGP)	전달 받거나 배포하는 경로에 Route-map을 적용합니다

3.2.2 통합주소 (Aggregate Address) 설정

CIDR(Classless Inter-Domain Routing)은 라우팅 테이블 크기를 최소화 할 수 있도록 사용자가 통합경로(또는 Supernet)를 생성할 수 있게 합니다. 사용자는 통합 경로를 BGP 라우터에 전달하거나 통합 기능을 이용하여 통합 경로를 설정할 수 있습니다. BGP 테이블에 최소한 하나 이상의 경로가 등록되어 있다면, BGP 테이블에 통합 주소가 추가됩니다.

라우팅 테이블에 통합 주소를 생성하려면, Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
aggregate-address prefix	Router (BGP)	BGP 라우팅 테이블에 통합 주소를 생성합니다.
aggregate-address prefix as-set summary-only		기존 BGP광고와 요약광고를 함께 광고합니다.
aggregate-address prefix summary-only		일괄 주소만 배포합니다.

3.2.3 BGP Community 필터링 설정

BGP는 라우팅 정보를 배포하면서 전송 정책을 지원합니다. 라우팅 정보 배포는 Community 목록뿐만 아니라 IP 주소, AS 경로를 기준으로 진행됩니다. Community 목록은 목적지 별로 Community를 만들고 Community를 기준으로 라우팅 정책을 적용하는데 사용합니다. 이 목록은 라우팅 정보를 배포하는 BGP Speaker 설정을 보다 간편하게 해 줍니다. Community는 몇 가지 공통된 속성을 공유하는 목적지 그룹입니다. 하나의 목적지는 여러 개의 Community에 포함될 수 있습니다. AS 관리자는 목적지가 속할 Community를 지정할 수 있습니다. 기본적으로 모든 목적지는 인터넷 Community에 속하는 것으로 설정되어 있습니다. 그 밖에 미리 정의되고 잘 알려진 Community로 no-export, no-advertise, local-as가 있고 각각의 특성은 아래와 같습니다.

- no-export : 외부에 있는 BGP Neighbor 라우터에 이 경로를 배포하지 마십시오.
- no-advertise : (내부든 외부든) Neighbor 라우터에 이 경로를 배포하지 마십시오.
- local-as : BGP 연합 네트워크에 위치한 하위 AS의 Neighbor 라우터들에게 이 정보를 배포하십시오. 외부 라우터에는 이 경로를 배포하지 마십시오.

Community List를 생성하려면, CONFIG 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
ip community-list name {permit deny} {community local-AS no-advertise no-export}	CONFIG	Community List를 생성한다.

Community는 RFC 에서 정의한 대로 2 바이트 길이의 숫자 두 개를 AA:NN 형태로 나타냅니다.

첫 번째 부분은 AS 번호이고 두 번째 부분은 2 바이트 숫자입니다.

Router 설정 모드에서 다음 명령어를 사용하여 Community Name을 Neighbor 라우터의 IP 주소로 전달할 수 있습니다.

명령어	모드	기능
neighbor ip-address send-community [both standard extended]	Router (BGP)	지정한 IP 주소를 지닌 Neighbor 라우터에게 Community Name을 전송한다.

3.2.4 Router 식별번호 설정

사용자는 BGP 경로를 전달하는 라우터에 라우터 식별 번호를 설정할 수 있습니다. 이 기능을 삭제하고 시스템이 부여한 라우터 식별 번호로 바꾸려면 **no** 형태의 명령어를 사용합니다.

명령어	모드	기능
bgp router-id address	Router (BGP)	BGP 라우터에 라우터 식별 번호를 부여한다.

3.2.5 BGP에 경로 배포하기

다른 곳에서 생성한 경로를 BGP 라우팅 테이블에 등록할 수 있습니다. 예를 들면 Connected 경로, Kernel 경로, Static 경로, 라우팅 프로토콜이 생성한 경로 등을 BGP에 전달할 수 있습니다. 이 기능은 모든 IP 라우팅 프로토콜에 적용됩니다.

다른 곳에서 생성한 경로를 BGP에 전달하려면, Router 설정 모드에서 다음 명령어를 수행하십시오.

명령어	모드	기능
redistribute {connected kernel static ospf rip}	Router (BGP)	BGP 테이블에 라우팅 정보를 배포합니다.

3.2.6 Routing Domain 연합 설정

BGP 망의 복잡한 다중 연결을 줄이는 한 방법은 하나의 AS를 몇 개의 작은 AS로 나눈 후 이를 몇 개씩 묶어서 하나의 연합 조직을 만드는 것입니다. 밖에서 볼 때 연합은 하나의 AS처럼 보입니다. 각 AS 내부에 있는 모든 시스템은 서로 직접 연결되어 있지만, 같은 연합에 속하는 다른 AS와는 전부 직접 연결되어 있지 않습니다.

이때 연합에 있는 다른 AS에 속하는 Neighbor 라우터와 통신하는 것은 내부에 있는 BGP 라우터와 통신하는 것으로 간주 됩니다. 특히 다음 목적지, MED, 네트워크 내 우선 순위 값은 그대로 적용됩니다. BGP 연합을 설정하려면, 연합 식별 번호를 반드시 설정해야 합니다. 외부에서는 일련의 AS그룹이 서로 다른 연합 번호를 지닌 단일한 AS로 보입니다.

BGP 연합 식별자를 설정하려면, Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
bgp confederation identifier as	Router (BGP)	BGP 연합을 설정합니다.

연합 내에서 Neighbor AS를 설정하려면, Router 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
bgp confederation peers as [as...]	Router (BGP)	연합에서 Neighbor AS를 지정한다.

3.2.7 경로 반영자(Route Reflector) 설정

BGP는 내부 망에 위치한 모든 대변인 라우터(Speaker Router) 들이 서로 연결되어있기를 바라지만 대변인 라우터가 많을 때는 불가능 합니다. 연합을 설정하는 대신에 내부 BGP 망의 복잡한 연결을 줄이는 다른 방법은 경로 반영 라우터를 설정하는 것 입니다.

경로 반영 라우터를 이용해서, 전달 받은 경로를 Neighbor 라우터에게 배포할 수 있기 때문에 모든 BGP 대변인 라우터가 완벽하게 서로 연결되어 있을 필요는 없습니다. 여기에서는 내부에 있는 Neighbor 라우터 가 다음 목적지로 경로를 배포합니다.

경로 반영자와 이 경로를 전달 받을 라우터를 설정하려면, Router 설정 모드에서 다음 명령어를 사용 하십시오.

명령어	모드	기능
neighbor ip-address route-reflector-client	Router (BGP)	로컬 라우터를 BGP 경로 라우터로 설정하고 Neighbor 라우터를 수신자로 설정한다.

3.2.8 Neighbor 명령어를 이용한 설정

수많은 Neighbor 라우터에게 BGP 정보를 제공하려면 Access List를 이용하여 Neighbor에서 보내는 정보를 전달 받도록 설정할 수 있습니다.

Neighbor를 이용하여 BGP 경로를 설정하려면, Router 설정 모드에서 IP 주소를 이용하여 다음 명령어를 사용하십시오.

명령어	모드	기능
neighbor <i>ip-address</i> activate	Router (BGP)	BGP Neighbor 라우터와 정보를 교환할 수 있게 합니다.
neighbor <i>ip-address</i> remote <i>NUMBER</i> passive		지정한 Neighbor 라우터에서 라우팅 정보를 전달하지 못하도록 합니다.
neighbor <i>ip-address</i> description <i>text</i>		Neighbor 라우터의 관계를 설명합니다.
neighbor <i>ip-address</i> default-originate		BGP 라우터가 기본 경로 0.0.0.0을 Neighbor 라우터에 전달합니다.
neighbor <i>ip-address</i> send-community		지정한 Neighbor 라우터로 Community 속성을 전합니다.
neighbor <i>ip-address</i> update-source interface		내부 BGP 정보를 TCP 통신이 가능한 인터페이스에 전달합니다.
neighbor <i>ip-address</i> ebgp-multihop		Neighbor 라우터가 BGP 네트워크에 연결되어 있지 않아도 BGP 통신을 허용합니다.
neighbor <i>ip-address</i> maximum-prefix maximum		Neighbor 라우터에서 접속할 수 있는 BGP 네트워크 수를 설정합니다.
neighbor <i>ip-address</i> weight weight		모든 경로에 Weight 을 지정합니다.
neighbor <i>ip-address</i> distribute-list <i>access-list-name</i> {in out}		Access List 에 정의한 정책에 준해서 Neighbor 라우터와 주고 받는 정보를 선별 처리합니다.
neighbor <i>ip-address</i> filter-list <i>access-list-name</i> {in out}		BGP 필터를 설정합니다.
neighbor <i>ip-address</i> next-hop-self		다음 목적지로 BGP 정보가 전달되지 않게 차단합니다.
neighbor <i>ip-address</i> version <i>VALUE</i>		Neighbor 라우터와 통신을 위해

		BGP버전을 지정합니다.
<code>neighbor ip-address route-map name {in out}</code>		주고 받는 정보에 Route-map 을 적용합니다.
<code>neighbor ip-address soft-reconfiguration inbound</code>		전달 받은 정보를 저장하게 합니다.
<code>neighbor ip-address dont-capability-negotiate</code>		Peer 가 변경된 경로를 반영할 수 없도록 합니다.
<code>neighbor ip-address strict-capability-match</code>		Neighbor 라우터가 변경된 경로를 반영할 수 있는 기능이 없다면 강제 설정을 통해 변경된 경로를 반영하도록 합니다. 만약 사용자가 override capability 를 설정하면 strict capability match 는 사용 불가능 합니다.
<code>neighbor ip-address transparent-as</code>		Neighbor 라우터가 외부 BGP 네트워크이더라도 Neighbor 라우터의 AS 번호를 설정하지 않습니다.
<code>neighbor ip-address transparent-nexthop</code>		Peer 가 외부 BGP 네트워크이라 할지라도 다음 목적지를 명시하지 않습니다.
<code>neighbor ip-address override-capability</code>		Peer 가 새로 전달 받은 경로 위에 다른 경로를 덮어 쓸 수 있도록 합니다.
<code>neighbor ip-address port</code>		BGP 네트워크에 TCP 포트 번호를 지정합니다.
<code>neighbor ip-address interface interface-name</code>		Neighbor 라우터의 인터페이스를 지정합니다.
<code>neighbor ip-address route-server-client</code>		Neighbor 라우터가 경로 서버가 되도록 합니다.

3.2.9 Neighbor 라우터 동작종료

존재하는 BGP Neighbor 라우터의 동작을 중단 시키려면, Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
neighbor ip-address shutdown	Router (BGP)	BGP Neighbor 시스템의 동작을 종료시킵니다.

neighbor shutdown 명령어를 사용하여 동작이 종료된 시스템을 다시 활성화하려면, Router 설정모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
no neighbor ip-address shutdown	Router (BGP)	BGP Neighbor 라우터를 재 가동시킨다.

3.2.10 Backdoor 경로지정

경계 라우터 (Backdoor Router) 가 사용할 수 있는 backdoor 경로를 사용해서 어떤 네트워크와 통신가능한지를 나타낼 수 있습니다. Backdoor 네트워크는 배포되지 않는다는 점만 빼고 사용자 자신의 네트워크와 똑 같습니다.

Backdoor 경로를 설정하려면, Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
network ip-address backdoor	Router (BGP)	Backdoor 경로를 통해 연결 가능한 네트워크를 지정한다.

3.2.11 거리값 설정

거리 값은 각 라우팅 프로토콜의 우선 순위를 나타내는 지표입니다. BGP는 외부, 내부, 로컬 세 종류의 거리 값을 사용합니다. 외부 BGP 가 전달한 경로는 외부 거리 값을 가지고 내부 BGP 가 전달한 경로는 내부 거리값, 로컬에서 전달한 경로는 로컬 거리 값을 갖습니다.

BGP 거리 값을 설정하려면, Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
distance bgp external internal local	Router (BGP)	BGP 경로의 거리 값을 변경하는 것은 위험하기 때문에 권장하지 않습니다. 외부 경로의 거리 값은 다른 라우팅 프로토콜보다 작아야 하고 내부와 로컬 거리 값은 다른 동적 라우팅 프로토콜보다 커야 합니다.

3.2.12 BGP 시간조정

BGP가 **keepalive** 메시지를 주기적으로 전송하고 일정 시간 동안 **keepalive** 메시지를 받지 못하면 다음 동작을 취하도록 관련시간을 설정합니다. 시스템이 설정한 **keepalive** 시간은 60초이고 **holdtimer**는 180초 입니다. 모든 **Neighbor** 라우터에 대해서 모니터 시간을 설정할 수 있습니다.

모든 **Neighbor** 라우터에 대해 **BGP** 시간을 설정하려면, **Router** 설정 모드에서 다음 명령어를 사용 하십시오.

명령어	모드	기능
bgp scan-time seconds	Router (BGP)	라우팅 정보를 전달하는 시간을 줄이기 위해 주기적으로 BGP 라우터를 검사하는 시간을 설정 합니다.

Neighbor 라우터에 대하여 **BGP** 시간을 조정하려면, **Router** 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
neighbor ip-address timers keepalive holdtimer	Router (BGP)	특정 Peer 에 대해 keepalive 와 holdtimer 시간을 설정 합니다.
neighbor ip-address timers connect time		Neighbor 라우터와의 연결 시간을 설정합니다.
no neighbor timers		BGP Neighbor 라우터에 설정한 시간 값을 삭제합니다.

3.2.13 첫 번째 AS 설정

Neighbor 라우터를 첫 번째 AS로 설정하려면, Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
bgp enforce-first-as number	Router (BGP)	Neighbor 라우터에 첫 번째 AS 번호를 할당한다. BGP 네트워크에서 원격 네트워크가 전달한 정보를 점검합니다.

3.2.14 로컬네트워크의 우선 순위변경

로컬 네트워크의 우선 순위 값을 변경하여 선호도를 높이거나 낮출 수 있습니다. 시스템이 설정한 우선 순위 값은 100 입니다. 로컬 네트워크의 우선 순위 값을 변경하려면, Router 설정모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
bgp default local-preference value	Router (BGP)	로컬 네트워크의 기본 우선 순위 값을 변경합니다.

3.2.15 외부네트워크의 우선 순위변경

외부에 위치한 BGP Neighbor 라우터가 전달한 유사 경로 가운데 라우터 식별 번호가 가장 작은 경로를 최적의 경로를 선택하려면 Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
bgp bestpath compare-routerid	Router (BGP)	AS 가 다른 Neighbor 라우터가 보낸 정보 가운데 최적의 경로를 선택하기 위해 라우터 식별 번호를 비교합니다.

3.2.16 MED 없는 경로를 최악의 경로로 간주

MED속성이 없는 경로를 최악의 경로로 간주하려면, Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
bgp bestpath med missing-as-worst confed	Router (BGP)	연합 경로 중에서 최적의 경로를 선택할 때 MED가 무한대 값을 갖는 것으로 설정합니다.

3.2.17 AS들이 전달한 MED 값으로 경로 선택

MED는 여러 개의 경로 중에서 최상의 경로를 선택할 때 고려되는 항목입니다. MED 값이 낮은 경로는 MED가 높은 경로에 비해 우선시 됩니다. 최상의 경로를 선택 때, 기본적으로 MED 값의 비교는 동일한 AS 내에서만 가능하도록 되어 있습니다.

AS에 상관 없이 MED 값을 비교할 수 있도록 설정 하려면, Router설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
bgp always-compare-med	Router (BGP)	다른 AS 가 제공하는 MED 값을 비교합니다.

3.2.18 MED를 이용한 연합 경로선택

서로 다른 연합 경로 중에서 최적의 경로를 선택할 때 MED 값을 비교하도록 설정하려면, Router 모드에서 다음과 같은 명령어를 사용하십시오.

명령어	모드	기능
bgp bestpath med [confed missing-as-worst]	Router (BGP)	MED를 이용하여 서로 다른 연합이 제공한 경로 가운데 최적의 경로를 선택하도록 합니다.

3.2.19 MED를 이용한 연합 내 경로선택

같은 연합에 속한 하위 AS 가 전달한 경로 가운데 최적의 경로를 선택하기 위해 MED 값을 비교하도록 설정하려면, Router 모드에서 다음 명령어를 수행하십시오.

명령어	모드	기능
bgp deterministic-med	Router (BGP)	연합 내에 위치한 AS가 전달하는 경로 가운데 최적의 경로를 선택하기 위해 MED 값을 비교 하도록 합니다.

3.2.20 반영된 경로저장

BGP 경로 반영 라우터가 인접한 다른 라우터에게 배포한 경로를 저장하려면, Router 모드에서 다음 명령어를 수행하십시오.

명령어	모드	기능
bgp client-to-client reflection	Router (BGP)	BGP 경로 반영자가 인접 라우터들에게 전송한 경로를 저장합니다.

3.2.21 경로 무효화(Route Dampening)

경로 무효화는 어떤 경로가 사용 가능과 불가능을 반복할 때 가능한 이 경로가 배포되지 않도록 고안된 기능입니다. 경로가 반복적으로 사용 가능했다가 불가능 해지고 불가능 했다가 다시 사용 가능한 상태로 되는 것을 **Flapping** 된다고 합니다.

다음은 경로 무효화 기능과 관련된 용어입니다.

- **Flap** - 경로가 사용 가능과 불가능 상태를 반복하는 것을 나타냅니다.
- **History State** - 경로 **Flap**이 발생할 때마다, 벌점을 부여하고 이 기록을 토대로 해당 라우터가 최상의 경로를 제공하지 못한다는 것을 나타내는 **History State**로 설정합니다.
- **Penalty** - 경로 **Flap**이 발생할 때마다, 무효화 되는 경로를 제공한 라우터에 벌점 1000 점이 부과됩니다. 벌점은 누적됩니다. 벌점은 한도 점수를 초과할 때까지 라우팅 테이블에 누적되었다가 한도점수를 초과하면 경로 상태가 **History**에서 **Damp**로 바뀝니다.
- **Damp State** - 이 상태에서 있는 경로는 빈번히 상태가 바뀌기 때문에 라우터는 **BGP Neighbor** 라우터에게 이 경로를 제공하지 않습니다.
- **Suppress Limit** - 경로에 부과된 벌점이 일정 한도를 넘기면 해당 경로는 삭제됩니다. 벌점 한도의 기본값은 2000입니다.
- **Half-life** - 경로에 벌점이 부과된 후 **Half-life** 타임이 지나면 벌점은 반으로 줄어듭니다. 시스템이 설정한 **Half Life** 타임은 15분이고 벌점 감소는 매 5초마다 한번씩 진행됩니다.
- **Reuse Limit - Flapping** 경로에 부과된 벌점이 줄어 들어서 재 사용 기준치를 밑돌게 되면 무효화된 경로는 다시 살아 납니다. 해당 경로는 다시 **BGP** 테이블에 추가되고 배포됩니다. 시스템이 설정한 재 사용 기준 값은 750 입니다. 경로 무효화 해제 절차는 10초마다 한 번씩 행해집니다. 매10초마다, 라우터는 재 사용할 수 있는 경로를 찾아서 다시 배포합니다.
- **Maximum Suppress Limit** - 이 값은 경로가 무효화 상태에 있을 수 있는 최대 시간입니다. 기본값은 **Half-life**의 4배입니다.

BGP 경로 무효화 기능을 설정하려면 **Router** 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
bgp dampening	Router (BGP)	BGP 경로를 무효화 기능을 활성화 합니다.

경로 무효화 기능에 필요한 다양한 항목들을 변경하려면, **Router** 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
bgp dampening half-life-time [reuse-limit -value]	Router (BGP)	경로 무효화 기능에 필요한 다양한 항목을 설정한다. half-life-time은 1초부터 45초까지 가능하며 reuse-limit -value는 1부터 2,000까지 가능합니다.

3.2.22 BGP 점검과 관리

사용자는 캐시, 테이블, 데이터베이스의 모든 항목을 제거할 수 있습니다. 또한, 특정한 통계를 출력할 수 있습니다. 다음 절은 이 작업에 대해 설명합니다.

1) 캐시, 테이블, 데이터베이스 삭제

특정 캐시나, 테이블, 데이터베이스의 모든 항목을 제거할 수 있습니다. 캐시나 테이블, 데이터베이스를 제거하는 것은 어떤 항목이 무효화 되었거나 신뢰할 수 없을 때 입니다.

다음은 BGP에 대한 캐시, 테이블, 데이터베이스 삭제와 관련된 작업을 출력합니다. 다음 명령어를 Top 모드에서 사용하십시오.

명령어	모드	기능
clear ip bgp { * ip-address as- number } [in out soft [in out]]	TOP	BGP Neighbor 라우터, AS 그룹, 모든 BGP(*) 연결에 대한 정보를 재 설정합니다.

2) 시스템과 네트워크 통계 표시

사용자는 BGP 라우팅 테이블, 캐시, 그리고 데이터베이스와 같은 특정 통계를 출력할 수 있습니다.

제공되는 정보는 보다 효율적으로 네트워크 자원을 운영하고 발생한 문제를 해결하는데 사용 됩니다.

그리고 네트워크 연결 상태나 사용자가 전달한 패킷이 거쳐가는 경로도 확인할 수 있습니다.

여러 가지 라우팅 통계를 출력하려면, Top 모드 또는 CONFIG 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
show ip bgp prefix-list name	TOP	BGP 네트워크정보가 전달된 Neighbor라우터를 출력합니다.
show ip bgp cidr-only		서브 네트워크와 상위 네트워크를 포함한 모든 BGP 경로를 출력합니다.
show ip bgp community [number local-AS no- advertise no-export]		특정 Community에 속하는 경로를 출력합니다. Community Number는 AA:NN의 형태입니다.
show ip bgp community-list		Community List에 가 허용하는 경

community- list-name [exact-match]		로를 출력합니다.
show ip bgp community-info		모든 BGP Community 정보를 출력합니다.
show ip bgp filter-list access-list-name		AS 경로를 정의한 Access List 의 정책과 일치하는 경로를 출력합니다.
show ip bgp regexp regular-expression		명령어에 입력된 내용과 일치하는 경로를 출력합니다.
show ip bgp attribute-info		모든 BGP 속성 정보를 출력합니다
show ip bgp network		BGP 라우팅 테이블을 출력합니다.
show ip bgp [network] [network -mask [longer-prefix]]		BGP 라우팅 테이블을 출력합니다. Longer-prefix는 보다 상세한 경로를 출력합니다.
show ip bgp neighbors [ip-address]		Neighbor 라우터와 TCP로 BGP 정보를 교환하는 과정에 대해 상세하게 알려줍니다.
show ip bgp neighbors ip-address [advertised-routes received prefix-filter received-routes routes]		Neighbor 라우터와 TCP로 BGP정보를 교환하는 과정에 대해 상세하게 알려줍니다. Advertised-routes 는 Neighbor 라우터에 배포한 모든 경로 정보를 출력하고 Received-routes 는 전달 받은 정보, Routes 는 주고 받은 모든 정보를 출력합니다.
show ip bgp paths		데이터베이스에 있는 모든 BGP 경로를 출력합니다.
show ip bgp summary		모든 BGP 연결 상태를 출력합니다.

3.3 OSPF Routing Protocol

OSPF(Open Shortest Path First)는 IETF(Internet Engineering Task Force)의 OSPF 분과가 개발한 프로토콜입니다. IP 네트워크를 위해 고안된 OSPF는 IP Subnetting 를 지원하고 외부 네트워크에서 들어온 라우팅 정보에는 표시를 합니다. 이외에도 OSPF는 패킷 인증을 지원하고 IP 멀티캐스트로 라우팅 정보를 주고 받습니다.

OSPF는 계층화된 네트워크 환경에서 가장 용이하게 동작합니다. OSPF 네트워크에서 가장 먼저 해야 하는 일은 **Border** 라우터 (여러 영역과 접하는 라우터) 와 **AS** 경계 라우터를 설정하는 것입니다.

그리고 OSPF 라우터가 구동하는데 필요한 최소한의 기본 설정을 하고 영역(**Area**)에 인터페이스를 지정합니다. 사용자의 환경에 맞게 OSFP 라우터를 설정할 때는 각 라우터에 설정한 내용들이 서로 일치 하는지 확인해야 합니다.

3.3.1 OSPF 활성화

다른 라우팅 프로토콜과 마찬가지로 **OSPF** 라우팅 프로토콜을 사용하려면, 해당 프로토콜을 활성화 시킨 후, **OSPF** 로 운영할 네트워크 주소와 네트워크 번호 (**ID**) 를 설정합니다. 다음은 **OSPF**를 활성화하는 방법입니다.

1 단계 **CONFIG** 설정 모드에서 **Router** 설정모드로 들어갑니다.

명령어	모드	기능
router ospf	CONFIG	Router 모드로 들어갑니다.

2 단계 **OSPF**의 네트워크 **ID**를 지정합니다. 네트워크 **ID**는 네트워크의 **IPv4** 주소를 설정합니다.

명령어	모드	기능
router-id router-id	Router (OSPF)	OSPF의 네트워크 ID를 지정합니다.

3 단계 **OSPF**로 동작하는 인터페이스와 해당 인터페이스의 **ID** 또는 **IP** 주소를 설정합니다.

명령어	모드	기능
network ip-address /m area {<0-4294967295> ip-address}	Router (OSPF)	OSPF Area-ID를 지정합니다. OSPF Area-ID는 <0- 4294967295> 사이의 십진수나 IPv4 Address 중 한 가지를 선택하여 사용할 수 있습니다.

OSPF를 활성화 시킨 후에는 사용자가 다음과 같은 항목들을 선택하여 설정할 수 있습니다.

- ABR 유형 설정
- 호환성 지원
- OSPF 인터페이스 설정
- OSPF 네트워크 유형 설정
- Non-broadcast 네트워크 설정

- 영역(Area) 설정
- OSPF 영역 사이에 대표 경로 설정
- 가상 라인 설정
- 기본 경로 값 설정
- 경로 계산 주기 설정
- 경로 전달 주기 설정
- OSPF 네트워크에 경로 전달
- 기본 경로 생성
- OSPF 거리값 변경
- 정보 전달 차단
- 갱신된 정보 유입 차단
- OSPF 모니터 및 관리

3.3.2 ABR 유형설정

OSPF 버전들이 다양한 만큼, OSPF 설정도 장비마다 다릅니다. 장비에 OSPF 프로토콜을 설정하려면, 장비 유형을 지정하십시오. 참고로 SG Series Switch는 RFC 2328에서 정의한 표준안을 따릅니다.

명령어	모드	기능
ospf abr-type {cisco ibm shortcut standard}	Router (OSPF)	장비 유형을 지정합니다.

3.3.3 호환성지원

호환성 지원 기능은 OSPF 를 정의한 여러 가지 RFC 표준안과 호환 가능하도록 합니다. OSPF 프로토콜의 여러 가지 다른 기능을 지원하도록 하려면 다음 명령어를 수행하십시오.

명령어	모드	기능
compatible rfc1583	Router (OSPF)	RFC 1583 표준안에 정의된 기능을 지원합니다.

3.3.4 OSPF 인터페이스 설정

사용자의 필요에 따라 OSPF 인터페이스 설정을 변경할 수 있습니다. OSPF 인터페이스 설정과 관련된 항목을 전부 변경할 필요는 없지만 그 중 몇 가지는 동일한 네트워크에 위치한 다른 라우터 설정과 일치해야 합니다.

이 가운데 다른 모든 라우터와 동일하게 설정 해야 하는 명령어는 `ip ospf hello-interval`, `ip ospf dead-count`, `ip ospf authentication-key` 입니다.

사용자는 이 명령어를 사용할 때 사용자의 네트워크에 위치한 다른 모든 라우터도 동일하게 설정되었는지 확인하십시오.

Interface 설정 모드에서 제공되는 다음과 같은 명령어 중에서 사용자 환경 설정에 필요한 명령어를 수행 하십시오.

명령어	모드	기능
<code>ip ospf cost cost</code>	INTERFACE	OSPF 인터페이스에서 패킷을 전송하는 cost 를 설정 합니다. 이는 LSA의 경로값(Metic Value)으로 기록되고 SPF 계산 시 사용됩니다.
<code>ip ospf retransmit-interval second</code>		OSPF 인터페이스와 연결된 라우터에게 경로 정보를 전달하는 시간을 지정합니다. 시스템이 제공하는 기본값은 5초입니다.
<code>ip ospf transmit-delay second</code>		OSPF 인터페이스에서 경로정보를 제공하는데 걸리는 시간을 설정합니다. LSA의 유효 시간은 정보 전달에 필요한 시간과 비례합니다. 시스템이 제공하는 기본값은 1초입니다.
<code>ip ospf priority number</code>		OSPF 라우터의 우선 순위를 설정합니다. 우선 순위가 높은값이 설정되면, 해당 라우터는 네트워크의 목적지 라우터가 됩니다. 시스템이 제공하는 기본값은 1입니다.
<code>ip ospf hello-interval second</code>		OSPF 인터페이스에서 전송하는 Hello 패킷의 시간 간격을 설정합니다. 동일한 네트워크에 위치한 모든 라우터는 반드시 동일한 값을 가져야 합니다. 시스템이 제공하는 기본값은 10초입니다.
<code>ip ospf dead-interval second</code>		Neighbor 라우터들이 Hello 패킷을 몇 초 동안 전달 받지 못하면 OSPF

		라우터가 다운된 것으로 간주할 지의 해당 시간을 설정합니다.
ip ospf authentication-key key		동일한 네트워크에 위치한 OSPF 라우터들이 인증에 사용할 비밀 번호를 지정합니다. 일반 문자로 인증할 비밀 번호는 최대 8 자입니다
ip ospf message-digest-key keyed md5 key		OSPF 라우터들이 MD5 로 암호화 해서 사용할 비밀 번호를 지정합니다. 암호화 인증에 사용되는 비밀 번호는 최대 16 자입니다.

3.3.5 OSPF 네트워크 타입설정

OSPF 는 네트워크를 다음과 같은 세 가지 타입으로 분류합니다.

- Broadcast 네트워크
- Non-Broadcast Multi-Access (NBMA) 네트워크
- Point-to-Point 네트워크

사용자는 OSPF 네트워크를 Broadcast 타입이나 Non-broadcast 타입으로 설정할 수 있습니다. 예를 들어 사용자의 네트워크가 Multicasting을 지원하지 않는다면 Broadcast 네트워크를 Non-broadcast타입으로 설정할 수도 있고 역으로 Frame Relay 같은 NBMA 네트워크를 Broadcast 타입으로 설정 할 수도 있습니다.

NBMA 타입으로 네트워크를 운영하려면 라우터와 라우터를 가상 회로(Virtual Circuit) 로 전부 연결해야 합니다. 그러나 OSPF는 네트워크 관리 비용을 절감하기 위해 네트워크의 일부분만 가상회로로 연결한 Point-to-Multipoint 방식을 설정할 수 있습니다. 직접 연결 되어 있지 않은 두 라우터는 서로를 연결하는 중간 라우터를 통하여 라우팅 정보를 주고 받게 되는데 이로 인해 반드시 Neighbor 라우터를 설정해야 하는 번거로움이 사라집니다.

다음은 OSPF Point-to-Multipoint 타입의 특징입니다.

- 반드시 Neighbor 라우터를 지정할 필요가 없기 때문에 IP 자원이 절약되고 목적지 라우터를 설정하기 위한 별도의 절차가 필요 없습니다.
- 네트워크에 위치한 모든 라우터와 거미줄처럼 연결되어 있을 필요가 없기 때문에 관리 비용이 절감됩니다.
- 가상 회로가 단절될 경우에도 통신이 가능하기 때문에 더욱 안정된 네트워크 서비스를 제공할 수 있습니다.

OSPF 네트워크 타입을 설정하려면, interface 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
ip ospf network {broadcast non-broadcast (point-to-multipoint point-to-point)}	Interface	OSFP 인터페이스에 네트워크 타입을 명시한다.

3.3.6 Non-Broadcast 네트워크 설정

OSPF 네트워크에 많은 라우터가 연결되어 있다면, 해당 네트워크와 통신하기 위해 “목적지 라우터”를 선정합니다. **Broadcast** 되지 않는 네트워크이라면, 라우팅 정보를 전달하기 위해 목적지 라우터를 선정해야 합니다. **Non-broadcast** 타입으로 통신하는 라우터를 설정하려면, **Router** 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
neighbor ip-address [priority <0-255> poll interval <1-65535>]	Router (OSPF)	Non-broadcast 타입으로 통신하는 라우터를 설정한다.

3.3.7 OSPF 영역(Area)설정

사용자는 OSPF Area를 설정할 때 인증이나, Stub 영역 정의, 기본 경로값 등을 지정할 수 있습니다.

인증이란 비밀 번호로 상대방 라우터를 확인한 후 접근 권한이 없는 장비는 OSPF 영역에 접속할 수 없도록 하는 것입니다.

Stub 영역은 외부 경로가 전달되지 않는 영역입니다. 대신에, 영역 경계 (Area Border) 라우터가 생성한 외부 경로를 전달 받아 외부에 있는 AS 와 통신 합니다. stub 영역에 전달하는 경로 정보(Link State Advertisement) 수를 줄이려면, ABR 에 no-summary 를 설정하여 Stub 영역에 요약 경로 정보(Summary Link Advertisement)가 전달되는 것을 차단합니다.

Router 설정 모드에서, 사용자의 필요에 따라 다음 명령어를 사용하십시오. 변수인 area-id 는 IP 주소 형태로 입력하거나 0부터 4,294,967,295까지의 값으로 표현할 수 있습니다.

명령어	모드	기능
area area-id authentication	Router (OSPF)	OSPF 영역에서 비밀 번호를 이용한 상호 인증이 가능하다.
area area-id authentication message-digest		OSPF 영역에서 MD5로 암호화한 비밀 번호를 이용하여 상호 인증을 할 수 있다.
area area-id stub [no-summary]		Stub 영역으로 정의한다.
area area-id default-cost cost		Stub 영역에서 사용하는 기본 요약 경로(Default Summary Route) 의 경로 값을 설정한다.
area area-id filter-list access access-list [in out]		다른 영역으로의 전달할 정책을 설정한다.
area area-id shortcut {default disable enable}		영역을 통과하는 최단 경로를 설정한다.

3.3.8 OSPF 영역 사이의 대표경로 설정

경로 요약(Route Summarization) 기능을 이용하여 ABR 이 하나로 요약된 경로를 다른 영역에 전달하도록 설정합니다. OSPF 에서 ABR 은 한 영역에 속한 네트워크 정보를 다른 영역에 전달하는데, 해당 네트워크들의 주소가 연속적인 대역을 차지하면, 각각의 네트워크를 포괄하는 하나의 대표 주소로 네트워크 경로를 지정할 수 있습니다.

네트워크의 주소를 지정하려면, Router 설정 모드에서 다음 명령어를 수행하십시오.

명령어	모드	기능
area area-id range {ip-address ip- address/m} not-advertised	Router (OSPF)	나의 대표 경로로 나타낼 수 있는 네트워크 대역을 설정한다. area-id는 0부터4,294,967,295까지의 값 입니다.
area area-id range ip-address {suppress substitute ip-address}		경로 정보를 전달하지 않을 네트워크 대역을 지정 한다.

3.3.9 가상라인 (Virtual Link) 생성

OSPF에서, 모든 영역은 반드시 백본 영역과 연결되어야 합니다. 만약 백본 영역과 통신이 끊어지거나 백본 영역을 분리 운영하게 되면, 사용자는 가상 라인을 이용하여 백본 영역과 연결할 수 있습니다. 가상 라인은 반드시 라인을 통해 연결되어 있는 두 라우터 모두에 설정되어야 합니다. 가상라인을 설정할 때 상대방 라우터를 연결 지점으로 등록하고 두 라우터는 모두 비 백본 영역(Transit Area)으로 설정 합니다. 단 가상 라인은 stub 영역을 통과할 수 없습니다.

가상 라인을 생성하려면, Router 설정 모드에서 다음 명령어를 수행하십시오. 변수인 area-id는 IP 주소 형태로 입력하거나 0부터 4,294,967,295까지의 값으로 표현할 수 있습니다.

명령어	모드	기능
area area-id virtual-link router-id-address hello- interval time retransmit- interval time transmit-delay time dead-interval time	Router (OSPF)	가상 라인을 생성합니다. Hello- interval 시간은 1초부터 65535초, Retransmit-interval 시간은 3초부 터 65535초, Transmit-delay 시간 은 1초부터 65535초, Dead- interval 시간은 1초부터255초를 지 정할 수 있습니다.

3.3.10 경로값의 변경

기본 경로값 (Default Metric) 변경

OSPF는 인터페이스의 대역폭을 기준으로 경로 값을 산정합니다. 예를 들어, T1 라인의 기본 값은 64이지만 64K 라인의 기본값은 1562 입니다.

만약 대역폭이 다른 여러 개의 라인이 있다면, 각 라인에 경로 값을 할당하여 라인 사용에 필요한 경비를 확인할 수 있습니다.

라인 사용에 소요되는 Cost를 구분하려면 Router 설정 모드에서 다음 명령어를 수행하십시오.

명령어	모드	기능
auto-cost reference-bandwidth reference-bandwidth	Router (OSPF)	각 라인이 제공하는 대역폭을 구분한 다. 1Mbit/s부터 4,294,967Mbit/s 까지 설정할 수 있습니다.

3.3.11 경로계산 주기설정

사용자는 OSPF 네트워크 구성이 변경 되었음을 통지 받고 최단 경로 (shortest path first) 를 계산하기 시작하는 경로 계산 주기를 설정할 수 있습니다.

경로를 계산하는 주기를 설정 하려면, Router설정 모드에서 다음 명령어를 수행하십시오.

명령어	모드	기능
timers spf spf-delay spf-hold	Router (OSPF)	경로 계산 주기를 설정한다. Delay Time과 Hold Time은 0-4294967295 사이에서 설정 가능합니다.

3.3.12 OSPF 네트워크에 경로전달

OSPF 네트워크에 다른 라우팅 프로토콜이 작성한 경로, Static 경로, 커널 경로, 인접한 시스템에 도달하는 경로 등을 전달하면 이 경로들은 OSPF 외부 경로가 됩니다.

OSPF 네트워크에 외부에서 생성한 라우팅 정보를 전달하려면, Router 설정 모드에서 다음 명령어를 수행하십시오.

명령어	모드	기능
redistribute {kernel connected static rip bgp} [metric value] [metric-type (1 2)]	Router (OSPF)	OSPF 네트워크에 외부 경로를 전달합니다.
default-metric number		OSPF로 전달된 모든 외부 경로에 대해 동일한 경로 값을 <0-16777214> 사이에서 설정합니다.

3.3.13 기본경로 (Default Route) 설정

사용자는 관리 도메인 경계(Autonomous System Boundary) 라우터가 OSPF 네트워크에 기본경로를 전달하도록 설정할 수 있습니다. OSPF 네트워크에 외부에서 생성한 경로를 전달하는 라우터가 바로 AS 경계 라우터입니다. 그러나 AS 경계 라우터는 시스템 기본 경로를 생성하지 않습니다.

관리 도메인 경계 라우터가 시스템 기본 경로를 생성하게 하려면, **Router** 설정 모드에서 다음 명령어를 수행하십시오.

명령어	모드	기능
default-information originate [always metric value metric-type (1 2) route- map]	Router (OSPF)	관리 도메인 경계 라우터가 OSPF 에서 시스템 기본 경로를 작성하도록 합니다.

3.3.14 OSPF 거리값 변경

거리 값은 라우터가 생성하는 라우팅 정보에 대한 신뢰도를 나타냅니다. 거리 값을 나타내기 위해 0부터 255까지의 숫자를 사용할 수 있는데 거리 값이 높을수록 낮은 신뢰도를 의미합니다. 거리값 255인 라우팅 정보는 전혀 신뢰할 수 없기 때문에 사용할 수 없는 정보를 의미합니다.

OSPF는 Intra-area, Inter-area, External, 이 세 가지 종류의 거리 값을 사용합니다. 다른 네트워크를 통해 전달 받은 외부 경로는 External 경로, OSPF 도메인 안에 있는 다른 영역들이 전달한 경로는 Inter-area 경로, 한 영역 내에서 주고 받는 경로는 Intra-area 경로라고 합니다. 세 가지 타입의 경로에 대해 시스템이 설정한 기본 거리 값은 110입니다.

OSPF 거리 값을 변경하려면, **Router** 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
distance ospf {external distance1 inter-area distance2 intra-area distance3}	Router (OSPF)	Router OSPF의 거리 값을 변경합니다.

3.3.15 정보전달 차단

OSPF 네트워크에서 **Passive**로 설정한 인터페이스는 **Stub** 네트워크처럼 동작합니다. 따라서 **Passive** 인터페이스에서는 OSPF 라우팅 정보를 주고 받을 수 없습니다.

인터페이스가 라우팅 정보를 전달하지 않도록 하려면, **Router** 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
passive-interface interface-name	Router (OSPF)	지정한 인터페이스는 라우팅 정보를 전달하지 않습니다.

3.3.16 갱신된 정보 차단

다른 라우터들이 OSPF 경로 정보를 받지 못하도록 하려면, 갱신된 라우팅 정보가 전달하지 않도록 설정합니다. 단 이 기능은 외부 경로에 대해서만 적용될 수 있습니다.

새로 변경된 라우팅 정보가 배포되는 것을 차단하려면, **Router** 설정 모드에서 다음 명령어를 실행 하십시오.

명령어	모드	기능
distribute-list name out {bgp connected kernel rip static}	Router (OSPF)	Access List 에 설정한 정책에 따라 갱신된 라우팅 정보를 배포하거나 차단한다.

3.3.17 OSPF 모니터링과 관리

사용자는 IP 라우팅 테이블에 기재된 여러 가지 통계나 데이터베이스를 확인할 수 있습니다. 이들 정보는 시스템의 효율성을 높이고 장애 발생시 문제 해결을 위해 유용하게 사용됩니다. 이 밖에도 네트워크의 연결 상태나 데이터 전송시 데이터가 거쳐간 경로도 확인할 수 있습니다.

여러 가지 라우팅 통계를 출력하려면, Top 모드 또는 CONFIG 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
show ip ospf	TOP	OSPF 라우팅 구동에 대한 전반적인 정보를 출력 합니다.
show ip ospf database option		OSPF 데이터베이스와 관련된 정보를 출력합니다.
show ip ospf border-routers		ABR(Area Border Router)과 ASBR (Autonomous System Boundary Router)에게 OSPF 라우팅 테이블 정보를 출력합니다
show ip ospf route		OSPF 라우팅 테이블에 등록된 경로 정보를 출력합니다.
show ip ospf interface interface-name		OSPF 인터페이스 정보를 출력합니다.
show ip ospf neighbor [neighbor id interface-name]		OSPF 라우터와 통신하는 Neighbor 라우터 정보를 출력합니다.

네트워크 장애가 발생했을 경우 사용자는 Debugging 명령어를 사용하여 문제의 원인을 파악할 수 있습니다.

CONFIG 모드에서 OSPF 정보를 출력하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
debug ospf packet {hello dd ls-ack ls-request ls-update all} [send rcv [detail]]	TOP	각 패킷에 대한 정보를 출력한다. 출력되는 정보에는 OSPF 패킷과 관련된 정보가 들어 있다.
debug ospf event		OSPF Neighbor에, 전달한 정보, 목적지 라우터 선출, 최단 경로 계산 등 OSPF 동작 관련된 정보를 출력한다.

debug ospf ifsm [events status timers]		OSPF 내부 영역에서 전달한 정보와 최단 경로 계산 등을 출력한다.
debug ospf lsa [flooding generate refresh]		OSPF가 전달한 정보와 최단 경로 계산 등을 출력 한다.
debug ospf nsm [events status timers]		OSPF Neighbor의 정보를 출력한다.
debug ospf route		OSPF route 정보를 출력한다.
show debugging ospf		OSPF와 관련된 디버깅 메시지를 출력한다.

3.4 RIP Routing Protocol

RIP(Routing Information Protocol)는 상대적으로 오래된 프로토콜이지만 규모가 작고 단일한 프로토콜로 운영되는 네트워크에서는 여전히 많이 쓰이고 있습니다. RFC 1058 에 정의된 RIP 는 경로 수(Hop Count) 로 패킷 경로를 결정하는 라우팅 프로토콜 입니다.

RIP는 라우팅 정보를 교환하기 위해 UDP(User Datagram Protocol) 패킷을 사용합니다. SG시리즈 라우터는 매 30초마다 라우팅 정보를 전달 합니다. 180 초가 지났는데도 다른 라우터로부터 새로운 정보를 받지 못하면 라우팅 테이블에 올라 간 정보를 사용할 수 없는 정보라고 표시합니다. 그리고 나서 120 초가 지나면 그 정보는 라우팅 테이블에서 삭제 됩니다.

RIP는 서로 다른 경로들을 비교하기 위해 경로 수 (Hop Count)를 비교 단위로 사용합니다. 경로 수는 네트워크에서 거쳐가야 하는 라우터 수 입니다. 직접 연결된 네트워크의 경로 수는 0 이고 도달할 수 없는 네트워크는 경로 수가 16 입니다. 이처럼 경로 수의 범위가 작기 때문에 RIP 는 규모가 큰 네트워크에서 사용하기에 적합한 프로토콜이 아닙니다.

RIP 라우터는 다른 RIP 라우터로부터 Default Network 정보를 전달 받거나 스스로 Default Network 정보를 생성합니다. Default Network 정보를 생성한 RIP 라우터는 이를 다른 RIP 라우터로 전달합니다. RIP 는 구체적으로 명시된 네트워크의 인터페이스로 라우팅 정보를 전달합니다. 라우팅 정보를 전달할 인터페이스의 네트워크가 명시되어 있지 않으면, RIP 정보는 Neighbor 라우터로 전달 되지 않습니다. SG Series 라우터는 RIP 버전 1/2 를 지원합니다.

3.4.1 RIP 활성화

RIP 프로토콜을 사용하려면 반드시 RIP를 활성화 시켜야 합니다.

RIP를 구동 시키려면, CONFIG 설정 모드에서 다음 명령어를 사용하여 Router 설정 모드로 들어가십시오.

명령어	모드	기능
router rip	CONFIG	RIP 라우팅 프로토콜을 구동시키고 Router 설정모드로 들어갑니다.

RIP로 운영할 네트워크를 지정합니다.

명령어	모드	기능
network {ip-address interface-name}	Router (RIP)	RIP으로 운영할 네트워크를 지정합니다.

network ip-address 명령어를 이용하여 RIP 가 동작하는 특정 네트워크 대역을 지정 할 수 있습니다.

예를 들어, 10.0.0.0/24 네트워크에 RIP 가 설정되어 있다면 10.0.0.0 에서 10.0.0.255 사이의 모든 주소는 RIP 로 동작하게 됩니다. RIP 패킷은 network interface-name 명령어에서 지정한 포트로 주고 받게 됩니다. RIP를 활성화 시킨 후에는 사용자의 요구에 따라 다음과 같은 항목을 선택하여 설정 할 수 있습니다.

- RIP Neighbor 라우터 지정
- RIP 버전 지정
- RIP 에서만 유효한 Static 경로 생성
- 라우팅 정보 전달
- 전달되는 경로의 경로값 설정
- 거리값(Administrative Distance) 설정
- 기본 경로(Default Route) 생성
- 라우팅 정보 필터링
- 시간 설정

- 경로 차단(Split-horizon) 활성화/비활성화
- 인증 키 관리
- RIP 확인 및 관리

3.4.2 RIP Neighbor 라우터 지정

RIP 는 브로드캐스트 프로토콜이기 때문에, RIP 의 라우팅 정보가 브로드캐스트 되지 않는 네트워크에 전달되기 위해서는 라우터끼리 서로 연결되어 있어야 합니다.

RIP 정보를 전달할 Neighbor 라우터를 설정하려면, Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
neighbor ip-address	Router (RIP)	라우팅 정보를 교환할 Neighbor 라우터를 지정합니다.

사용자는 **passive-interface** 명령어를 사용하여 특정 인터페이스에 라우팅 정보가 전달 되지 않도록 설정할 수 있습니다.

3.4.3 RIP Version 지정

기본적으로 SG시리즈 스위치는 **RIP 버전 1**과 **버전 2**를 지원합니다. 그러나 **버전 1** 타입 패킷이나 **버전 2** 타입 패킷만 주고 받을 수 있도록 버전을 지정할 수 있습니다.

버전을 바꾸려면, **Router** 설정 모드에서 다음 명령어를 수행하십시오

명령어	모드	기능
version {1 2}	Router (RIP)	RIP 1 타입 패킷이나 RIP 2 타입 패킷만 전송하기 위해 버전을 지정합니다.

사용자는 시스템이 지원하는 **RIP** 버전을 지정할 수도 있고 특정한 인터페이스에서 지정한 **RIP** 버전으로 패킷을 전달하도록 설정할 수도 있습니다.

특정 인터페이스에서 보내는 **RIP** 패킷의 버전을 지정하려면, **Interface** 설정 모드에서 다음 명령어를 수행 하십시오.

명령어	모드	기능
ip rip send version 1	interface	해당 인터페이스에서 RIP 버전 1 타입 패킷만을 보냅니다.
ip rip send version 2		해당 인터페이스에서 RIP 버전 2 타입 패킷만을 보냅니다.
ip rip send version 1 2		해당 인터페이스에서 RIP 버전 1, 버전 2 타입 패킷을 보냅니다.

마찬가지로 특정 인터페이스가 특정 버전의 **RIP** 패킷만을 수신하도록 하려면 **interface** 설정 모드에서 다음 명령어를 수행하십시오.

명령어	모드	기능
ip rip receive version 1	Interface	해당 인터페이스에서 RIP 버전 1 타입 패킷만을 받습니다.
ip rip receive version 2		해당 인터페이스에서 RIP 버전 2 타입 패킷만을 받습니다.
ip rip receive version 1 2		해당 인터페이스에서 RIP 버전 1, 버전 2 타입 패킷을 받습니다.

3.4.4 RIP 에서만 유효한 Static 경로생성

route 명령어는 RIP 내에서만 유효한 Static 경로를 생성합니다. 만일 RIP 프로토콜을 많이 다루어 본 고급 사용자가 아니라면, 이 명령어 대신에 redistribute static 명령어를 사용하여 static 경로를 배포하십시오.

명령어	모드	기능
route ip-address/m	Router (RIP)	RIP 내에서만 사용되는 Static 경로를 만듭니다.

3.4.5 Routing 정보전달

SG Series Switch는 전달 받은 라우팅 정보를 다른 RIP 라우터로 전달할 수 있습니다. 라우터와 직접 연결된(Connected) 장비에 이르는 경로, 커널 경로, static 경로, 라우팅 프로토콜이 생성한 경로 등을 다른 라우터에 알려 주고 이 내용을 전달 받은 라우터는 라우팅 테이블에 해당 정보를 등록합니다.

라우팅 정보를 다른 장비 RIP 테이블에 등록하려면, Router 설정모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
redistribute {connected kernel static ospf bgp} [metric value route-map tag]	Router (RIP)	전달 받은 라우팅 정보를 다른 라우터의 RIP 테이블에 등록합니다.

사용자는 필요에 따라 route-map 명령어를 사용하여 두 네트워크끼리 주고 받는 라우팅 정보를 제한할 수 있습니다. Route map을 이용하여 특정 정보만을 전달하려면, CONFIG 모드에서 다음 명령어를 사용해 Route-map 설정 모드로 들어가십시오.

명령어	모드	기능
route-map tag {deny permit} sequence-number	CONFIG	Route-map을 생성합니다.

route-map 명령어 뒤에는 반드시 match 나 set 명령어가 따릅니다. 만약 match 명령어가 없다면, 모든 것을 허용하고 set 명령어가 없으면, 아무것도 수행되지 않습니다. 그러므로,

사용자는 반드시 **match** 나 **set** 명령어를 사용해야 합니다.

다른 라우터로 전달할 라우팅 정보를 제한하려면, **Route-map** 설정 모드에서 다음 명령어 가운데 하나를 수행하십시오.

명령어	모드	기능
match interface interface-name	Route-map	지정한 인터페이스로만 정보를 전달합니다.
match ip address {access-list-name prefix-list ip-address-name}		지정한 Access-list나 Prefix-list에 부합된 정보만 전달합니다.
match ip next-hop {access-list-name prefix-list ip-address-name}		Access-list나 Prefix-list에 있는 Neighbor 라우터에만 정보를 전달합니다.
match metric metric-value		지정한 거리 값과 일치하는 정보만 전달합니다.
set ip next-hop ip-address Neighbor		라우터 주소를 설정합니다.
set metric value		거리 값을 설정합니다.

3.4.6 전달되는 경로의 경로값 설정

라우팅 프로토콜이 각 경로를 비교하기 위해 사용하는 경로 값이 다른 라우팅 프로토콜에서 사용하는 경로 값으로 자동으로 변환하지 않습니다.

예를 들면, **RIP** 는 경로 수를 기준 값으로 사용하지만 **OSPF** 는 다섯 가지 수치를 조합해서 경로값을 산출합니다. 라우팅 프로토콜은 전달 받은 경로의 경로 값을 자신이 사용하는 경로 값으로 바꾸기 때문에 서로 다른 라우팅 프로토콜들이 아무런 규약 없이 라우팅 정보를 주고 받게 되면 라우팅 정보가 공전하면서 네트워크 성능이 현격히 떨어질 수 있습니다. 이런 경우를 방지하기 위해 사용자는 다른 라우터로 배포되는 경로의 경로 값을 인위적으로 지정합니다.

배포되는 경로의 경로 값을 설정하려면, **Router** 설정 모드에서 다음 명령어를 수행 하십시오.

명령어	모드	기능
default-metric value	Router (RIP)	라우팅 프로토콜이 전달하는 모든 경로에 동일한 경로 값을 지정합니다



참고

모든 프로토콜에서 사용 가능한 경로값 범위는 **0-4294967295** 입니다. **RIP** 에서 유효한 값은 **1에서 16**입니다.

3.4.7 거리값(Administrative Distance) 설정

거리 값은 라우터가 생성하는 라우팅 정보에 대한 신뢰도를 나타냅니다. 규모가 큰 네트워크에서는 몇몇 라우팅 프로토콜이나 라우터 정보가 다른 프로토콜이나 라우터 보다 더 신뢰성이 클 수 있습니다. 따라서 하나의 라우터에 여러 개의 라우팅 프로토콜을 사용하더라도 가장 신뢰성이 있는 하나의 경로만 전달될 수 있습니다. 사용자가 거리 값을 설정함으로써 라우터는 어디에서 라우팅 정보가 생성 되었는지 명백히 알게 됩니다. 라우터는 항상 거리 값이 가장 작은 라우팅 프로토콜이 생성한 경로를 선택합니다. 각 네트워크마다 네트워크 자체의 특성이 다르기 때문에 거리값 설정에 대한 일반적인 지침은 없습니다. 사용자는 전체 네트워크 관점에서 합리적인 거리 값을 지정해야 합니다.

Router 설정 모드에서 다음 명령어를 사용하여 거리 값을 설정하십시오.

명령어	모드	기능
distance value [ip-address/M [access-list- name]]	Router (RIP)	거리 값을 지정합니다.

3.4.8 기본경로 (Default Route) 생성

사용자는 RIP 경계 라우터가 RIP 네트워크에 기본 경로를 배포하도록 설정할 수 있습니다. 사용자가 RIP 네트워크에 라우팅 정보를 배포하도록 설정하면, 해당 라우터는 AS 경계 라우터가 됩니다.

그러나, AS 경계 라우터가 자동으로 기본 경로를 생성해서 RIP 네트워크에 배포하지 않습니다.

AS경계 라우터가 기본경로를 생성하도록 하려면, Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
default-information originate	Router (RIP)	AS 경계 라우터가 RIP 네트워크에 기본 경로를 배포 하도록 합니다.

3.4.9 Routing Information Filtering

다음 항목을 수행하여 라우팅 프로토콜이 전달하는 정보를 제한할 수 있습니다.

- 특정 인터페이스로 전달되는 라우팅 정보를 차단합니다. 이것은 해당 인터페이스와 연결된 시스템으로 라우팅 정보가 전달되는 것을 방지하기 위한 것입니다.
- 라우팅 정보의 경로 값이 자동으로 증가 되도록 합니다.

◇ 인터페이스로 나가는 라우팅 정보 차단

특정 라우터의 인터페이스로 전달되는 라우팅 정보를 차단하여 같은 네트워크 영역에 속하는 다른 라우터들이 라우팅 정보를 받지 못하도록 할 수 있습니다. 이 기능은 **BGP**를 제외한 모든 **IP** 기반 라우팅 프로토콜에 적용됩니다.

명령어	모드	기능
passive-interface interface-name	Router (RIP)	라우터의 인터페이스가 라우팅 정보를 전달하지 못하도록 합니다.

◇ 경로값 증가 기능 설정

Offset List 는 **RIP**를 이용해서 주고 받는 라우팅 정보의 경로 값을 증가시키는 메커니즘입니다. 사용자는 **Access List**에 **Offset List**를 설정할 수 있습니다.

전달되는 경로의 경로 값을 증가시키려면, **Router** 설정 모드에서 다음 명령어를 수행하십시오.

명령어	모드	기능
offset-list access-list-name {in out} metric [interface]	Router (RIP)	전달되는 경로의 경로 값을 증가시킵니다.

3.4.10 시간설정

라우팅 프로토콜은 일정한 간격으로 새로운 라우팅 정보를 전달하고 일정 시간이 경과한 라우팅 정보는 폐기합니다. 사용자는 자신의 네트워크 환경에서 라우팅 프로토콜이 최대한 효율적으로 동작하도록 라우팅 프로토콜의 주기를 설정할 수 있습니다. 시스템에서 제공하는 기본 시간 단위는 다음과 같습니다.

- 라우팅 정보는 30초 단위로 전달됩니다. 30초마다 RIP 는 자신의 라우팅 테이블을 연결된 다른 RIP 라우터에게 전달 합니다.
- 라우팅 정보의 유효 시간은 180초입니다. 유효 시간이 경과하면, 그 정보는 더 이상 유효하지 않지만 **Neighbor** 라우터들이 그 경로가 삭제되었다는 것을 통보 받을 때까지 잠시 라우팅 테이블에 남아 있습니다.
- 유효하지 않은 정보는 120초마다 한 번씩 수거됩니다. 유효하지 않은 정보로 분류된 정보들은 120 초가 지나면 라우팅 테이블에서 완전히 삭제됩니다.

시간 단위를 변경하려면, **Router** 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
timers basic update timeout garbage	Router (RIP)	라우팅 프로토콜의 동작 주기를 조절합니다.

3.4.11 경로차단(Split-horizon) 활성화/비활성화

일반적으로 브로드캐스트 타입의 IP 네트워크에 연결되어 각기 다른 거리값(신뢰도)을 지닌 라우팅 프로토콜을 사용하는 라우터들은 라우팅 정보가 무한 루프에 빠지지 않도록 Split Horizon 메커니즘을 사용합니다. Split Horizon은 라우팅 정보가 배포될 때 해당 정보를 생성한 라우터에게는 라우팅 정보가 배포되지 않도록 합니다.

이 기능은 특히 여러 대의 라우터가 서로 연결되어 있을 때 정상적인 통신을 가능하게 합니다. 그러나 Frame Relay처럼 브로드캐스트를 하지 않는 네트워크에서는 사용할 수 없습니다. 따라서 이런 경우에는 Split Horizon 을 비활성화 시켜야 합니다.

하나의 인터페이스에 두 개의 IP 주소가 설정되어 있고 Split Horizon이 활성화 되어 있다면, 라우팅 정보는 두 번째 IP 주소로 배포되지 않습니다. 그러나 Split Horizon이 활성화 되면 동일한 라우팅 정보가 서로 네트워크에서 전달된 것으로 간주되어 무한 루프가 발생합니다.

Split Horizon을 활성화 시키거나 비활성화 시키려면 Interface 설정 모드에서 다음 명령어를 수행하십시오.

명령어	모드	기능
ip rip split-horizon	Interface	Split Horizon을 활성화 시킵니다.
no ip rip split-horizon		Split Horizon을 비활성화 시킵니다.

3.4.12 인증키 관리

RIP 버전 1은 인증을 지원하지 않습니다. 만약 RIP 버전 2 타입의 패킷을 보내고 전달 받는다면, 인터페이스에서 RIP 인증을 가동할 수 있습니다. 키 체인은 인터페이스에서 사용할 수 있는 키를 결정합니다. 키 체인을 설정하지 않으면, 일반 문자열을 이용하여 인증을 수행합니다.

RIP 인증을 위해 일반 문자열 인증과 MD5 인증, 두 가지 모드를 지원합니다. RIP 버전 2타입의 패킷에서 제공하는 기본 인증은 일반 문자열 인증입니다.

RIP 인증을 설정하려면 인터페이스 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
ip rip authentication key-chain name	Interface	RIP 인증을 활성화 시킵니다.
ip rip authentication mode {text md5}		MD5 인증과 일반 문자열을 이용한 인증 가운데 인터페이스가 사용할 인증 모드를 지정합니다.
ip rip authentication string string		Key Chain을 사용하지 않고 일반 문자열 인증에 사용할 문자열을 설정한다. 이 때 사용하는 문자열은 16자를 넘지 않아야 합니다.



참고

암호화 되지 않은 인증 키는 RIP 버전 2 타입의 패킷 안에 넣어 전달되기 때문에 보안이 필요한 경우에는 일반 문자열 인증을 사용하지 마십시오. 문자열을 이용한 인증은 보안이 필요 없는 경우에 한해서 사용하십시오.

3.4.13 RIP 모니터 및 관리

사용자는 IP 라우팅 테이블이나 데이터 베이스 같은 통계 데이터를 출력할 수 있습니다. 이런 정보를 이용하여 사용자는 시스템을 보다 효율적으로 이용하고 발생하는 문제들을 해결할 수 있습니다. 이 밖에 패킷이 전달되는 경로도 확인할 수 있습니다.

여러 가지 다양한 통계를 출력하려면, **Top** 모드 또는 **CONFIG** 설정 모드에서 다음 명령어를 수행하십시오.

명령어	모드	기능
show ip rip	TOP	라우터에서 사용 중인 RIP 정보를 출력합니다.
show ip route rip		RIP 와 관련된 라우팅 테이블 정보를 출력합니다.
show ip protocols		사용 중인 RIP 프로토콜의 현재 상태와 관련 정보를 출력합니다.

장애가 발생했을 경우 사용자는 **debugging** 명령어를 이용하여 문제의 원인을 보다 빨리 파악할 수 있습니다.

RIP 라우터가 주고 받은 정보를 확인하려면, **CONFIG** 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
debug rip events	TOP	패킷 송, 수신과 같은 RIP 이벤트와 변경된 RIP 정보를 출력합니다.
debug rip packet [recv send] detail		RIP 패킷에 대해 보다 상세한 정보를 출력한다. 이 정보에는 패킷을 전송한 주소와 포트 번호가 들어 있습니다.
show debugging rip		RIP 디버깅 용으로 설정된 모든 정보를 출력합니다.

3.5 VRRP (Virtual Router Redundancy Protocol)

VRRP(Virtual Router Redundancy Protocol)는 Virtual Router로 이루어진 VRRP Group을 지정하여 단일 라우터를 사용시 발생할 수 있는 장애를 예방할 수 있습니다.

VRRP는 최대 255개의 가상 라우터들을 생성할 수 있으며, 1개의 VRRP ID에서 여러대의 가상라우터를 운용할 수 있습니다. 이 경우 가상라우터의 우선순위를 지정하여 가장 높은 Priority를 가진 가상라우터가 Master가 되며, 그 외의 가상라우터는 Priority가 높은 순서에 따라 차례대로 Backup으로 동작하게 됩니다.

VRRP Group에서 Master가 장애가 발생한 경우, Priority가 높은 다른 가상라우터가 Master가 됩니다.

VRRP를 설정할 때에는 VRRP Group에 속하게 될 라우터에 동일한 VRRP-ID로 VRRP Group을 설정한 후, 동일한 Virtual-IP를 할당합니다.

가상라우터의 Priority가 동일한 경우 IP 주소를 비교하여 가장 작은 IP를 가지고 있는 가상라우터가 Master로 동작하게 됩니다.

<예제> 192.168.1.1/24, 192.168.1.2/24, 192.168.1.3/24의 주소를 갖고 있는 3대의 라우터에 192.168.1.254/32 라는 Virtual-IP 주소로 Virtual Router를 설정한 예제입니다.

각 라우터의 Priority 값이 동일하다고 가정할 때, 192.168.1.1/24라는 IP 주소를 가진 라우터가 가장 작은 IP 주소를 가지고 있기 때문에 Master Router로 결정됩니다. 한편, 이 Virtual Router에 연결된 스위치나 PC들은 Virtual Router의 IP 주소인 192.168.1.254를 Default Gateway로 가지게 됩니다.

Internet

Virtual Router

Virtual-IP : 192.168.1.254/32

Master Router

IP : 192.168.1.3/24

Backup Router 2

IP : 192.168.1.2/24

Backup Router 1

IP : 192.168.1.1/24

Default Gateway : 192.168.1.254

3.5.1 VRRP 기본설정

스위치를 Virtual Router Group에 속하는 장비로 설정하려면, 우선 CONFIG 설정 모드에서 다음 명령어를 사용하십시오.

VRRP가 활성화됨과 동시에 VRRP와 관련된 여러 가지 설정을 할 수 있는 VRRP 설정 모드로 들어갈 수 있습니다.

명령어	모드	기능
router vrrp <i>vrrp-id</i>	CONFIG	Virtual Router 와 VRRP-ID를 설정합니다. VRRP ID는 (1~255) 까지 지정할 수 있습니다.

다음은 위의 명령어를 사용하여 VRRP 설정 모드로 들어간 경우입니다. VRRP 설정 모드로 들어가면, 시스템 프롬프트가 SG2124GX(config)#에서 SG2124GX(config-vrrp)#로 변경됩니다.

<예제> vrrp 설정 모드 진입

```
SG2124GX#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124GX(config)#router vrrp 1
SG2124GX(config-router)#
```

VRRP를 해제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no router vrrp <i>vrrp-id</i>	CONFIG	VRRP를 해제합니다.

VRRP 설정 내용을 확인하려면 다음 명령어들을 사용하십시오.

명령어	모드	기능
show vrrp <vrrp-id>	TOP	vrrp 설정 및 동작상태를 출력합니다.
show vrrp brief		요약된 vrrp 설정 및 동작 상태를 출력합니다.
show running-config		스위치의 설정 내용을 확인합니다.

<예제> vrrp 동작상태 확인

```

SG2124GX#show vrrp
Vrld <2>
State is Master
Virtual IP is 10.10.2.10 (Not IP owner)
Interface is vlan1.2
Configured priority is 120, Current priority is 120
Advertisement interval is 2 sec
Master down interval is 15 sec
Preempt mode is TRUE
Circuit failover interface vlan1.51, Priority Delta 30, Status UP
SG2124GX#show vrrp brief
VRID State Interface VIP Prio(conf/curr) Adv-interval Master-down Preempt Circuit-failover
-----
Vr2 Master vlan1.2 10.10.2.10 120/120 2 15 True vlan1.51(30)

```

➤ Virtual IP 주소 설정

Virtual Router Group을 설정한 후에는 Virtual Router의 Virtual IP 주소를 설정해야 합니다. 동일한 Group에 속하는 라우터에 동일하게 IP 주소를 설정하십시오.

다음은 Virtual Router Group에 속하는 라우터들에게 IP 주소를 설정하거나, 설정했던 Virtual IP 주소를 삭제할 때 사용하는 명령어입니다.

명령어	모드	기능
virtual-ip <i>ip-address</i> [master/backup]	Router (vrrp)	Virtual Router들이 가지는 동일한 Virtual IP 주소를 설정합니다. master로 설정하는 경우는 현재 Interface 에 있는 IP를 그대로 Virtual-IP로 사용하는 경우이며, 다른 IP를 Virtual-IP로 사용시에는 backup으로 설정합니다.
no virtual-ip <i>ip-address</i>		Virtual Router들에게 할당한 Virtual IP 주소를 삭제합니다.



참고

1개의 vrrp-id에서 10개까지의 virtual-ip를 설정할 수 있습니다.

다음은 SG Series Switch에 Virtual Router Group의 IP 주소를 192.168.1.254로 설정한

경우입니다.

<예제> vrrp virtual ip 설정

```
SG2124GX#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124GX(config)#router vrrp 1
SG2124GX(config-router)#virtual-ip 192.168.1.254 backup
```

➤ VRRP Interface 설정

Virtual Router Group을 설정한 후에는 Virtual Router의 Virtual d IP 주소를 설정해야 합니다. 동일한 Group에 속하는 라우터에 동일하게 IP 주소를 설정하십시오.

다음은 Virtual Router Group에 속하는 라우터들에게 IP 주소를 설정하거나, 설정했던 Virtual IP 주소를 삭제할 때 사용하는 명령어입니다.

명령어	모드	기능
interface <i>ifname</i>	Router (vrrp)	VRRP를 설정할 Interface를 지정합니다.

➤ Master Router와 Backup Router 지정

SG 시리즈 Switch는 가상라우터 Group에 속한 장비들의 Priority 값과 IP 주소를 비교하여 Master Router와 Backup Router를 정합니다. 우선적으로 Priority 값을 비교하는데, Priority 값이 큰 장비가 우선 순위가 높고, Priority 값이 동일한 경우에는 IP 주소를 비교하게 되는데 IP 주소의 값이 작은 것이 우선 순위가 높습니다.

SG Series Switch의 사용자는 Priority 값을 설정하여 Master Router와 Backup Router를 정할 수 있습니다. IP 주소에 상관없이 Priority 값이 높을수록 우선 순위도 높아져서 Priority 값이 가장 높은 장비가 Master Router로 정해집니다. 한편, Master Router에 문제가 발생하였을 때 사용되는 Backup Router도 2개 이상일 때 동일한 우선 순위에 따라 사용 순서가 결정됩니다.

다음은 Virtual Router에 Priority 값을 설정할 때 사용하는 명령어입니다.

명령어	모드	기능
priority <i>priority</i>	Router (vrrp)	Virtual Router에 우선 순위를 할당합니다. Priority는 1~255 사이에

		서 지정할 수 있습니다.
no priority		Virtual Router에 할당된 우선 순위를 삭제합니다.



참 고

SG Series Switch는 기본적으로 Priority 값이 "100"으로 설정되어 있습니다.

Priority 값은 1부터 255까지 입력할 수 있습니다.

다음은 Virtual Router Group으로 설정되어 있는 Layer 3 SG2124GX_1과 Layer 3 SG2124GX_2에 Priority 값을 각각 101, 102로 설정하여 Master와 Backup Router가 정하는 경우입니다. 그러면, IP 주소와 상관없이 Priority 값이 큰 Layer 3 SG2124GX_2가 Master가 됩니다.

<예제> vrrp priority 설정

SG2124GX_1 : IP 주소 - 192.168.1.1/24, virtual-ip - 192.168.1.254

SG2124GX_2 : IP 주소 - 192.168.1.2/24, virtual-ip - 192.168.1.254

```
SG2124GX_1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124GX_1(config)#router vrrp 1
SG2124GX_1(config-router)#virtual-ip 192.168.1.254 backup
SG2124GX_1(config-router)#priority 120
SG2124GX_1(config-router)#interface vlan1.10
SG2124GX_1(config-router)#enable
SG2124GX_1(config-router)#end
SG2124GX_1#show vrrp
VrId <1>
State is Master
Virtual IP is 192.168.1.254 (Not IP owner)
Interface is vlan1.10
Priority is 120
Advertisement interval is 1 sec
Preempt mode is TRUE
```

```
SG2124GX_2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124GX_2(config)#router vrrp 1
SG2124GX_2(config-router)#virtual-ip 192.168.1.254 backup
SG2124GX_2(config-router)#priority 100
SG2124GX_2(config-router)#interface vlan1.10
SG2124GX_2(config-router)#enable
SG2124GX_2(config-router)#end
SG2124GX_2#show vrrp
VrId <1>
State is Backup
Virtual IP is 192.168.1.254 (Not IP owner)
Interface is vlan1.10
Priority is 100
Advertisement interval is 1 sec
Preempt mode is TRUE
```

3.5.2 Authentication 패스워드 설정

사용자가 Virtual Router Group을 설정한 상태에서 Group ID와 Virtual IP 주소를 알면, 다른 장비도 Virtual Router Group에 속할 수 있습니다. 이 때, 사용자가 설정한 Virtual Router Group 내에서만 패킷을 주고 받을 수 있도록 패스워드를 설정하면 다른 장비가 Group으로 설정되는 것을 막을 수 있습니다.

사용자가 설정한 Virtual Router Group의 보안을 유지하기 위해 패스워드를 설정하려면 VRRP 설정모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
authentication string password	Router (vrrp)	다른 장비가 Virtual Router Group에 소속되는 것을 막기 위해 패스워드를 설정합니다
no authentication string		다른 장비가 Virtual Router Group에 소속되는 것을 막기 위해 설정한 패스워드를 삭제합니다.



참고

Authentication 패스워드는 최대 16자리의 문자로 설정할 수 있습니다.

다음은 Virtual Router Group의 Authentication 패스워드를 설정하고 그 내용을 확인한 경우의 예입니다.

<예제> vrrp authentication 패스워드 설정

```
SG2124GX#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124GX(config)#router vrrp 1
SG2124GX(config-router)#authentication string handreamnet123456
% VRRPv2 authentication must be shorter than 16
SG2124GX(config-router)#show running-config

router vrrp 1
virtual-ip 192.168.1.254 backup
interface vlan1.10
authentication string handreamnet123456
enable
!
```

3.5.3 Preempt 기능 설정

Preempt는 VRRP Group이 설정된 상태에서 또 다른 장비를 추가했을 때, 추가한 장비에 Priority 값을 가장 높게 설정하면 장비의 재부팅이나 설정 없이 새로 추가된 장비가 자동으로 Master Router가 되도록 하는 기능입니다.

Preempt 기능을 설정하려면 VRRP 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
preempt-mode {true false}	Router (vrrp)	Preempt 기능을 활성화/비활성화 시킵니다.



참고

SG Series Switch는 기본적으로 Preempt 기능이 “enable”로 설정되어 있습니다.

다음은 Virtual Router Group의 Preempt 기능을 사용하지 않도록 설정한 경우의 예입니다.

<예제> vrrp preempt 비활성화

```
SG2124GX#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124GX(config)#router vrrp 1
SG2124GX(config-router)#preempt false
SG2124GX(config-router)#end
SG2124GX#show vrrp
Vrld <1>
State is Master
Virtual IP is 192.168.1.254 (Not IP owner)
Interface is vlan1.6
Priority is 100
Advertisement interval is 1 sec
Preempt mode is FALSE
```

Preempt 기능을 기본값으로 되돌리려면 Router 모드의 VRRP 설정에서 다음 명령어를 사용하십시오.

명령어	모드	기능
preempt-mode true	CONFIG	Preempt 기능을 기본값(true)으로 되돌립니다.

3.5.4 Advertisement Time 설정

Virtual Router Group에서 Master Router는 일정한 간격으로 VRRP 그룹 내의 다른 Virtual Router들에게 자신의 정보를 보내는데 이를 Advertisement time이라고 합니다.

SG Series Switch의 사용자는 이러한 Advertisement Time을 설정할 수 있습니다.

Advertisement Time을 설정하려면, VRRP 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
advertisement-interval time	Router (vrrp)	Master Router가 자신의 정보를 다른 Virtual Router에 배포하는 시간 간격인 Advertisement Time 을 설정 합니다.

다음은 Virtual Router Group의 Advertisemen Time을 설정하고 그 내용을 확인한 경우의 예입니다.

<예제> vrrp advertisemen time 설정

```
SG2124GX#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124GX(config)#router vrrp 1
SG2124GX(config-router)#advertisement-interval 10
SG2124GX(config-router)#end
SG2124GX#show vrrp
Vrid <1>
State is Master
Virtual IP is 192.168.1.254 (Not IP owner)
Interface is vlan1.6
Priority is 100
Advertisement interval is 10 sec
Preempt mode is FALSE
```

Advertisement Time을 기본값으로 되돌리려면 다음 명령어를 사용하십시오.

명령어	모드	기능
no advertisement-interval	Router (vrrp)	(vrrp)Advertisement Time을 기본값으로 되돌립니다.

제4장. 부록

4.1 OS Image Upgrade

FTP Server를 설치한 관리자의 PC에 새로운 OS Image를 내려 받은 후 Switch에 New OS Image를 설치하는 절차입니다. SG Switch Series에는 OS Image를 3개까지 설치 가능합니다.

- 1 단계 : PC에 FTP Server Program을 설치 후 새로운 이미지 파일을 내려 받습니다.
- 2 단계 : Switch에 IP Address를 설정한 후 FTP Server와 Network로 연결합니다.
- 3 단계 : Update 명령을 이용하여 FTP Server에 접속하여 새로운 이미지 파일을 Download 하여 OS Image를 Upgrade 한 후 reboot 합니다.

Switch 이미지를 Upgrade하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
update system {IP_Addr IPv6_Addr} IMAGEFILENAME ID PASSWD [port <1-65535>] flash {primary secondary third}	CONFIG	FTP Server를 이용하여 OS Image를 Upgrade 합니다.
update system sftp {IP_Addr IPv6_Addr} IMAGEFILENAME ID [port PORT_Num] flash {primary secondary third}	CONFIG	SFTP Server를 이용하여 OS Image를 Upgrade 합니다.
update system tftp {IP_Addr IPv6_Addr} IMAGEFILENAME flash {primary secondary third}	CONFIG	TFTP Server를 이용하여 OS Image를 Upgrade 합니다.
update system usb IMAGEFILENAME flash {primary secondary third}	CONFIG	USB 저장매체의 파일을 이용하여 OS Image를 Upgrade 합니다.
update system {IP_Addr	CONFIG	OS Image를 Upgrade 하기 전 현재

<i>IPv6_Addr</i> } <i>IMAGEFILENAME</i> <i>ID</i> <i>PASSWD</i> recovery [port <i>PORT_Num</i>]		의 Image를 Memory에 임시로 Backup합니다.
update system {xmodem ymodem zmodem} flash {primary secondary third}	CONFIG	xmodem, ymodem, zmodem을 이용 하여 OS Image를 Upgrade 합니다.



참 고

1. 업그레이드 완료 후 **reload** 명령을 통해 다시 **Booting**을 하여야 업그레이드된 새로운 이미지로 적용됩니다.
2. 이미지 업그레이드 시 **FTP**의 **passive mode**를 지원하지 않기 때문에 **Firewall** 외부에 있는 **FTP Server**로 접속이 안될 수 있습니다.

<예제> OS Image Upgrade

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#update system 192.168.1.1 system.bin userid passwd
SG2124G(config)#exit
SG2124G#reload
reboot system? (y/n): y
INIT: Switching to runlevel: 6

Broadcast message from root Sat May 16 21:43:15 2009...

The system is going down for reboot NOW !!
INIT: Sending processes the TERM signal

% Connection is closed by administrator!
Restarting system.
RESET...

HDNBR-2.4.0

* OS Number   : 1
* OS Name     : SG2124G OS Image ver. 2.0.7
* OS Size     : 9964 KiB
* Build Date  : 2012. 6.21 9:51:35
Loading: ..... 16777216 bytes read
Initializing ..... Done

SG2124G login:
```

4.2 USB Auto Upgrade

SG Switch Series는 USB를 이용하여 자동으로 OS Image의 Upgrade나 Config를 update/backup하는 기능을 사용할 수 있습니다. Keyvalue 값 미설정시에는 MAC 주소가 내부적으로 설정되어 동작하게 됩니다. USB 루트 디렉토리의 sg_usb_upgrade.conf 파일을 검사하여 파일이 존재하면 자동 Upgrade 기능을 수행합니다. ('sg_usb_upgrade.conf' 파일명은 모두 소문자입니다.)

OS Image Upgrade는 현재 boot flash로 설정된 파티션에서 동작합니다. 현재 flash에 저장된 OS의 버전이 동일하면 OS Image Upgrade는 진행되지 않습니다.

sg_usb_upgrade.conf 파일의 구성은 다음과 같습니다.

한 파일에 여러 개의 key 추가가 가능하지만, Key 값과 Hostname이 매치가 되면 매치된 key 동작만 수행하고 종료됩니다. `;(첨표) 이후에는 반드시 다음 엔트리('reload=', 혹은 'filename=')가 들어가야 합니다. 엔트리명은 소문자로 입력해야 합니다.

- 키 값 : 문자나 MAC 주소로 지정합니다. MAC 주소는 대소문자 구분이 없습니다.

(MAC 주소는 00:00:00:00:00:00 혹은 0000.0000.0000 형식)

- model 명 : Hostname과 동일해야 합니다. (대소문자 구분함)
- reload : USB 자동 Upgrade 기능 동작 완료후 재시작 시간을 설정할 수 있습니다.

(필수 요소 아님) +min, now, HH:MM 의 형태로 지정 가능합니다.

- action : 수행 순서는 설정과 관계없이 항상 syslog > startup_config > update_startup_config > update_os 순서대로 동작합니다.

- 1) syslog (syslog backup)
- 2) startup_config (startup config backup)
- 3) update_startup_config (외부파일에서 장비로 Startup-config 업데이트)
- 4) update_os (OS Image Upgrade)

- filename : 경로를 포함시킬 수 있으며 디렉토리는 '/'로 구분합니다.

'''(따옴표) 이용시 띄어쓰기 할 수 있습니다.

- 1) 업그레이드할 파일명 (action : update_os)
- 2) 저장할 파일명 지정 혹은 default 지정 (default시 syslog는 <Serial>.log, startup_config는 <Serial>.conf로 자동 저장)

usb 연결 시 자동으로 Upgrade하는 기능을 사용하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
usb auto-upgrade <i>KEYVALUE</i>	CONFIG	usb 연결시 자동으로 Upgrade 하는 기능을 설정합니다.
no usb auto-upgrade	CONFIG	usb 연결시 자동으로 Upgrade 하는 기능을 해제합니다.

usb 장비의 리스트를 확인/삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show usb dir	TOP	usb 장비의 파일 리스트를 확인합니다.
remove usb <i>FILENAME</i>	TOP	usb 장비내의 파일을 삭제합니다.

<예제> sg_usb_upgrade.conf 예제

```

-----
                                sg_usb_upgrade.conf
-----
aa.bb.cc.dd.ee.ff                                → Key 값 지정(MAC 사용 가능)
{
model=SG2124G,                                    → 장비의 Hostname(대소문자 구분)
reload=now                                         → Upgrade 후 재시작 지정
(action=update_os,filename ="/update/system.sg2124g.bin.encrypted" )
(action=syslog,filename=default)                 → action, filename 지정
(action=startup_config,filename=default)
}
-----

SG2124G(config)#usb auto-upgrade aa.bb.cc.dd.ee.ff
SG2124G#
SG2124G#show running-config
!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
bridge 1 protocol pvstp
!
vlan database
vlan range 10 bridge 1
!
mls qos enable
usb auto-upgrade aa.bb.cc.dd.ee.ff
mes enable ge23-24 detect

```

```
-- 이하 생략 --
SG2124G#
SG2124G#show syslog
-- 생략 --
Jun 22 14:47:41 SG2124G USB[989]: "/usb/ua1/sg_usb_upgrade.conf" file exist. active
usb auto-config.
Jun 22 14:47:41 SG2124G USB[989]: USB Auto-Upgrade - excute backup syslog
Jun 22 14:47:43 SG2124G USB[989]: Success syslog backup
Jun 22 14:47:43 SG2124G USB[989]: USB Auto-Upgrade - excute backup startup-config
Jun 22 14:47:43 SG2124G USB[989]: Success startup-config backup
Jun 22 14:47:43 SG2124G USB[989]: USB Auto-Upgrade - excute update system
Jun 22 14:48:42 SG2124G USB[989]: Success update system
system.sg2124g.bin.encrypted
Jun 22 14:48:42 SG2124G USB[989]: Ends usb auto-upgarde. Rebooting Schedule
2012/06/22 14:48:42
-- 이하 생략 --
```



참고

SG2000 Series, SG2128G Series, SG2152G Series 제품은 USB 관련 기능을 지원하지 않습니다.

4.3 OS Image 선택

SG Switch Series는 OS를 3개까지 저장할 수 있으며, 부팅 이미지를 선택하거나 삭제하는 기능을 사용할 수 있습니다.

부팅시 사용할 OS를 선택하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
boot flash {primary secondary third}	CONFIG	부팅할 OS Image를 설정합니다.

저장되어 있는 OS Image를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show flash	TOP	OS Image를 확인합니다.

저장되어 있는 OS Image를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
remove flash {primary secondary third}	TOP	설치된 OS Image를 삭제합니다.

<예제> OS Image 설정 및 확인

```
SG2124G#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SG2124G(config)#boot flash primary
SG2124G(config)#
SG2124G#show flash

Default Boot : Primary

-----+-----+-----+-----
|          | Size | Build Date | Image Name |
-----+-----+-----+-----
Primary   | 9957 KiB | 2012. 5. 7 | SG2124G OS Image ver. 2.0.7
Secondary | 9957 KiB | 2012. 5. 7 | SG2124G OS Image ver. 2.0.7
Third     | 9966 KiB | 2012. 4.23 | SG2124G OS Image ver. 2.0.7
```



참고

Flash Memory 용량 64MB이하의 제품은(SG2024, SG2024P) Multi-OS 기능을 지원하지 않습니다. (OS Image 1개만 지원)

4.4 FTP로 Config Backup/Restore, Syslog Backup

Switch CONFIG 내용을 별도로 저장해 두었다가 CONFIG가 손상된 경우 이전 CONFIG로 복원하여 Switch의 작동을 유지하는데 사용할 수 있습니다. (변수인 name은 Backup하는 내용의 일종의 파일명으로 관리자가 편리한 이름으로 설정할 수 있습니다.)

CONFIG 내용을 Backup 및 Restore하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
copy running-config startup-config	TOP	running-config를 startup-config로 copy합니다.
copy startup-config ftp IP_Address {FILENAME default} ID PASSWORD [port PORT_Num]	TOP	startup-config을 ftp server에 저장합니다. (default 선택 시 <Serial>.conf로 저장됩니다.)
copy ftp IP_Address FILENAME ID PASSWORD {dot1x web-auth flash port PORT_Num startup-config}	TOP	ftp server에 저장되어 있던 startup-config 파일(<Serial>.conf)을 다시 startup-config 에 restore합니다.
copy startup-config sftp IP_Address {FILENAME default} ID [port PORT_Num]	TOP	startup-config을 sftp server에 저장합니다. (default 선택 시 <Serial>.conf로 저장됩니다.)
copy sftp IP_Address FILENAME {dot1x web-auth flash port PORT_Num startup-config}	TOP	sftp server에 저장되어 있던 startup-config 파일(<Serial>.conf)을 다시 startup-config 에 restore합니다.
copy startup-config tftp IP_Address {FILENAME default}	TOP	startup-config을 tftp server에 저장합니다. (default 선택 시 <Serial>.conf로 저장됩니다.)
copy tftp IP_Address FILENAME startup-config	TOP	tftp server에 저장되어 있던 startup-config 파일(<Serial>.conf)을 다시 startup-config 에 restore합니다.
copy startup-config {xmodem ymodem zmodem}	TOP	startup-config을 x, y, zmodem을 사용하여 저장합니다.
copy {xmodem ymodem zmodem} startup-config	TOP	x, y, zmodem을 사용하여 startup-config 파일을 다시 startup-config 에 restore합니다.

copy startup-config usb [FILENAME default]	TOP	startup-config을 usb에 copy합니다. (default 선택 시 <Serial>.conf로 저장됩니다.)
copy usb FILENAME {dot1x web-auth flash startup- config}	TOP	usb에 저장되어 있던 startup-config 파일(<Serial>.conf)을 다시 startup- config 에 restore합니다.

<예제> 설정 내용을 파일로 Backup

```
SG2124G#copy startup-config ftp 192.168.1.1 default user password
Filename is SG1149780001.conf
Starting Transmission....
Finished ....
SG2124G#

SG2124G#copy ftp 192.168.1.1 SG1149780001.conf user password startup-config
Filename is SG1149780001.conf
Starting Transmission....
Finished ....
```

Syslog를 백업하여 로그내역을 저장하여 관리할 수 있습니다.

Syslog의 사이즈가 2MB가 초과되면 Syslog-backup 파일이 생성되면서 기존의 Syslog는 모두 삭제됩니다. Syslog-backup 파일이 생성되면, Syslog에 "syslogd Because syslog exceeds the size of 2MB, It has been back-up." 로그를 남깁니다.

Syslog Backup 설정을 하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
copy {syslog syslog-backup} ftp IP_Address {FILENAME default} ID PASSWORD [port PORT_Num]	TOP	Syslog를 ftp server에 저장합니다. (default 선택 시 <Serial>.log로 저장됩니다.)
copy {syslog syslog-backup} sftp IP_Address {FILENAME default} ID [port PORT_Num]	TOP	Syslog를 sftp server에 저장합니다. (default 선택 시 <Serial>.log로 저장됩니다.)
copy {syslog syslog-backup} tftp IP_Address {FILENAME default}	TOP	Syslog를 tftp server에 저장합니다. (default 선택 시 <Serial>.log로 저장됩니다.)
copy {syslog syslog-	TOP	Syslog를 x, y, zmodem을 사용하여

backup} {xmodem ymodem zmodem}		저장합니다. (default 선택 시 <Serial>.log로 저장됩니다.)
copy {syslog syslog- backup} usb {FILENAME default}	TOP	Syslog를 usb에 copy합니다.(default 선택시 <Serial>.log로 저장됩니다.)

<예제> Syslog를 파일로 Backup

```
SG2124G#copy syslog tftp 192.168.1.1 default
Filename is SG1149780001.log
Starting Transmission....
Finished ....
SG2124G#
SG2124G#copy syslog-backup tftp 192.168.1.1 default
Filename is SG1203800001.backup.log
Starting Transmission....
Finished ....
```

**참고**

Copy 명령을 이용한 Config 백업 및 복구 시 User ID/Password, Enable Password를 제외한 나머지 비밀번호(SNMP User Password, Dot1x shared key)는 복원되지 않습니다.

4.5 Reload 스케줄링

Switch를 스케줄링으로 시간을 지정 하여 재시작 할 수 있는 기능입니다. 현재 시각 이후로 설정하는 **after**와 정해진 시간에 재시작 할 수 있는 **at** 명령어와 재시작을 취소하는 **cancel** 명령어가 있습니다.

정해진 시간 없이 시스템이 **hang-up** 되면 10 s 후에 자동으로 **reboot** 하는 **watchdog** 명령어가 있습니다.

Reload 스케줄링 기능을 사용하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
reload after {HH:MM <1-31> MM}	TOP	reload를 현재시각 이후로 언제 실행할지 지정합니다.
reload at HH:MM <1-31> <1-12>	TOP	reload 할 시각을 시간/일/월로 지정합니다.
reload cancel	TOP	reload 지정을 해제합니다.
show reload	TOP	설정된 reload 기능을 확인합니다.
watchdog	CONFIG	시스템이 hang-up 된 후 10 s 이후 자동 reboot 합니다.

<예제> reload 스케줄 설정

```
SG2124G#reload at 10:10 ?
<1-31> set day
<cr>

SG2124G#reload at 10:10 15 ?
<1-12> Set month

SG2124G#reload at 10:10 15 6
Reload scheduled at 2012/06/15 10:10:00
                in 3 days, 23 hours, 6 minutes
System will be rebooted at the scheduled time from Primary image.
Do you want to continue? (y/n): y

SG2124G#show reload
Reload scheduled at 2012/06/15 10:10:00
                in 3 days, 23 hours, 8 minutes
SG2124G#reload cancel
SG2124G#show reload
SG2124G#
```

4.6 Packet Debug 기능

스위치의 CPU로 유입되는 모든 트래픽을 보여주는 기능입니다. 트래픽은 연결된 콘솔이나 telnet 화면에 실시간으로 나타나며, 중단하려면 **Ctrl+C**를 입력합니다.

Packet Debug 기능을 사용하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
debug pkt [dest-ip { <i>IP_Addr/M</i> <i>network/m</i> }]	TOP	네트워크상의 패킷 내역을 확인합니다.
debug pkt src-ip <i>IP_Addr/M</i> dest-ip <i>IP_Addr/M</i>	TOP	네트워크상의 패킷 내역을 확인합니다.
debug pkt interface <i>VLAN</i>	TOP	네트워크상의 패킷 내역을 확인합니다.
debug pkt protocol {arp icmp tcp udp} {src-ip <i>IP_Addr/M</i> dest-ip <i>IP_Addr/M</i> dest-ip <i>IP_Addr/M</i> }	TOP	네트워크상의 패킷 내역을 확인합니다.

<예제> Packet debug 화면

```
SG2124G#debug pkt ?
dest-ip      Destination IP address or network
interface    Select a vlan interface to dump packet
protocol     Protocol
src-ip       Source IP address or network
<cr>
```

```
SG2124G#debug pkt
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vlan1.1, link-type EN10MB (Ethernet), capture size 68 bytes
15:17:49.231367 IP 192.168.255.201.51021 > 192.168.255.32.telnet: Flags [.], ack
1258236707, win 16088, length 0
15:17:49.231568 IP 192.168.255.32.telnet > 192.168.255.201.51021: Flags [P.], ack 0,
win 183, length 150
15:17:49.449570 IP 192.168.255.201.51021 > 192.168.255.32.telnet: Flags [.], ack
151, win 16425, length 0
15:17:49.449801 IP 192.168.255.32.telnet > 192.168.255.201.51021: Flags [P.], ack 0,
win 183, length 220
15:17:49.644595 ARP, Request who-has 192.168.200.122 (Broadcast) tell
192.168.255.50, length 46
15:17:49.652344 IP 192.168.255.201.51021 > 192.168.255.32.telnet: Flags [.], ack
371, win 16370, length 0
15:17:49.652540 IP 192.168.255.32.telnet > 192.168.255.201.51021: Flags [P.], ack 0,
win 183, length 310

-- 이하 생략 --
```

4.7 Boot Loader에서의 Password 및 Config Recovery

관리자 Password를 잊어버렸을 경우 Boot Loader 모드에서 **recover** 명령어를 이용하여 관리자 Password를 입력하지 않고 Login하여 관리자 Password를 재설정하거나 Switch의 설정 내용을 초기화할 수 있습니다. (전원 On 시 **Ctrl+C**를 누르시면 Boot Loader 모드로 전환할 수 있습니다.)

<예제> Boot Loader 모드에서의 도움말 사용법

```
HDNBR-2.4.0

Automatic startup canceled via Ctrl-C
HDNBR> help
Available commands:

reset                Reset the system.
recover             recover administrator password, or reset configuration.
flash               Update a flash memory device
boot                System bootstrap.
os                  Multi-OS feature
ping                Ping a remote IP host.
arp                 Display or modify the ARP Table
ifconfig            Configure the Ethernet interface
help                Obtain help for CFE commands

For more information about a command, enter 'help command-name'
*** command status = 0

HDNBR> help recover

SUMMARY

    recover administrator password, or reset configuration.

USAGE

    recover -password|-config

    system recover from missing password or configuration problem

OPTIONS

    -password      override administrator password
    -config        reset configuration to the factory default

*** command status = 0
HDNBR>
```



참고

-password 는 관리자 Login 비밀번호를 입력하지 않아도 Login 할 수 있도록 하는 기능이며, **-config** 은 **configuration file**을 기본값으로 변경하는 기능입니다.

4.8 OS 업그레이드 Fail 시 복구 방법

OS Image 업그레이드 중에 전원이 Off 되었거나, 잘못된 OS Image로 업그레이드를 진행하여, OS Image가 손상되어 정상 Booting을 하지 못하는 경우 Boot Loader 모드에서 OS Image를 업그레이드 할 수 있습니다. (전원 On 시 **Ctrl+C**를 누르시면 Boot Loader 모드로 전환할 수 있습니다.) 업그레이드시에는 TFTP Server와 MGMT 포트를 연결하여 진행합니다.

<예제1> Boot Loader 모드에서 OS 확인/변경

```
HDNBR> os
O/N | Image Name | Build Date | Size
-----+-----+-----+-----
* 1 | SG2124G OS Image ver. 2.0.7 | 2012. 6.21 9:51:35 | 9964 KiB
  2 | SG2124G OS Image ver. 2.0.7 | 2012. 6.21 9:51:35 | 9964 KiB
  3 | No OS | ----.---.--- --:--:-- | - KiB
*** command status = 0
HDNBR> os 2 → Boot OS를 2번으로 변경

** DO NOT TURN OFF YOUR MACHINE UNTIL THE FLASH UPDATE COMPLETES!! **
*** Completed
O/N | Image Name | Build Date | Size
-----+-----+-----+-----
  1 | SG2124G OS Image ver. 2.0.7 | 2012. 6.21 9:51:35 | 9964 KiB
* 2 | SG2124G OS Image ver. 2.0.7 | 2012. 6.21 9:51:35 | 9964 KiB
  3 | No OS | ----.---.--- --:--:-- | - KiB
*** command status = 0
```

<예제2> Boot Loader 모드의 flash 명령어 Help

```
HDNBR> help flash

flash filename os1|os2|os3

Copies data from a source file name or device to a flash memory device.
The source device can be a remote file(TFTP) or a flash device
The destination device may be a flash.

os1      os image #1
os2      os image #2
os3      os image #3

*** command status = -2
```

<예제3> Boot Loader 모드에서의 OS 업그레이드 방법

```

HDNBR > ifconfig eth0 -addr=192.168.100.1 -mask=255.255.255.0
Device eth0: hwaddr 00-1A-F4-80-04-00, ipaddr 192.168.100.1, mask 255.255.255.0
          gateway not set, nameserver not set
*** command status = 0
HDNBR >
HDNBR > flash 192.168.100.10:/system.bin.encrypted os1
Reading 192.168.100.10:/system.bin.encrypted: Done. 12065479 bytes read
Verify OS Image...Done
Programming...done. 12065479 bytes written
*** command status = 0

```

<예제4> SG2128G, SG2128GX, SG2152G, SG2152GX Series의 경우 Boot Loader 모드에서의 OS 업그레이드 방법

- PC와 Switch interface Ge1 번 포트를 UTP Cable로 연결하여 사용

```

HDNBR > HDRMGMT netboot
HDNBR > ifconfig eth2 -addr=192.168.100.1 -mask=255.255.255.0
Device eth2: hwaddr 00-1A-F4-80-04-00, ipaddr 192.168.100.1, mask 255.255.255.0
          gateway not set, nameserver not set
*** command status = 0
HDNBR >
HDNBR > flash 192.168.100.10:/system.bin.encrypted os1
Reading 192.168.100.10:/system.bin.encrypted: Done. 12065479 bytes read
Verify OS Image...Done
Programming...done. 12065479 bytes written
*** command status = 0

```



1. 업그레이드 완료 후 **reload** 명령을 통해 다시 **Booting**을 하여야 업그레이드된 새로운 이미지로 적용됩니다.
2. Multi-OS 기능이 지원되지 않는 제품은(SG2024, SG2024P)는 Boot OS를 선택할 수 없으므로 CLI 사용 시 **os1, os2** 가 아닌 '**flash 192.168.100.10:/system.bin.encrypted os**' 와 같이 사용해야 합니다.

4.9 Alarm 발생 시 확인 사항

Switch의 Alarm LED는 Switch의 성능에 영향을 줄 수 있는 환경이거나 하드웨어의 장애가 발생한 경우 점멸하며 동작합니다.

Alarm LED가 점멸하는 경우에는 Switch 내부의 온도가 너무 높거나 낮은 경우, 내장되어 FAN의 동작에 이상이 발생한 경우에 동작하며, Alarm이 발생되지 않을시에는 내용이 출력되지 않습니다. 하드웨어의 Fail로 인한 Alarm 발생 시 고객 센터에 연락하여 주십시오.

Switch의 Alarm 상태를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show system alarm	TOP	FAN / Temperature / PSU의 Alarm 상태를 확인합니다.

<예제> Alarm 상태 확인

```
SG2124G#show system alarm
Temperature Sensor : Too high temperature detected (42.250) → 과열 Alarm
                                                             (설정온도 보다 높음)

SG2124G#show system alarm
system Status : OK → 동작상태 양호
SG2124G#
```


4.9.1 내부 온도 확인

Switch의 보드 중앙에 부착된 온도센서 Chip을 통해 내부의 온도 확인 시 +70 °C 이상이거나 -20 °C 이하인 경우에 Alarm LED가 점멸합니다.

온도로 인한 Alarm LED 점멸 시 FAN Fail로 인해 내부 온도가 상승한 경우에는 지정된 고객센터로 연락하여 점검을 받으시기 바랍니다. Switch 장애로 인한 내부 온도 상승이 아닌 경우 항온항습기, 에어컨, 히터 등을 통해 사용 환경을 적절하게 조절하시기 바랍니다.

Switch의 내부 온도를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show system temperature	TOP	내부의 온도를 확인합니다.

<예제> 내부 온도 확인

```
SG2124G#show system temperature → 시스템 온도 정보 확인
M/B Temp      : 42.4 C
Outside Temp   : 19.6 C
Fan Start      : 20 C
Fan Stop       : 15 C
Alarm Low      : -20 C
Alarm High     : 70 C
SG2124G#
```



참고

내장되어 있는 FAN에 대한 동작 온도를 변경하지 않은 경우 Default 설정은 내부 온도가 +20 °C 이상일 때 FAN이 작동을 시작하며, +15 °C 이하일 때 FAN 작동을 멈춥니다.

4.9.2 FAN Fail 확인

Switch에 내장되어 있는 FAN의 동작에 이상이 발생한 경우 Alarm LED가 점멸합니다.

FAN Fail이 발생하여 Alarm LED 점멸하는 경우에는 고객 센터로 연락하여 점검을 받으시기 바랍니다.

FAN 동작 상태를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show system fan	TOP	내장된 FAN의 동작 상태를 확인합니다.

<예제> FAN 동작 상태를 확인

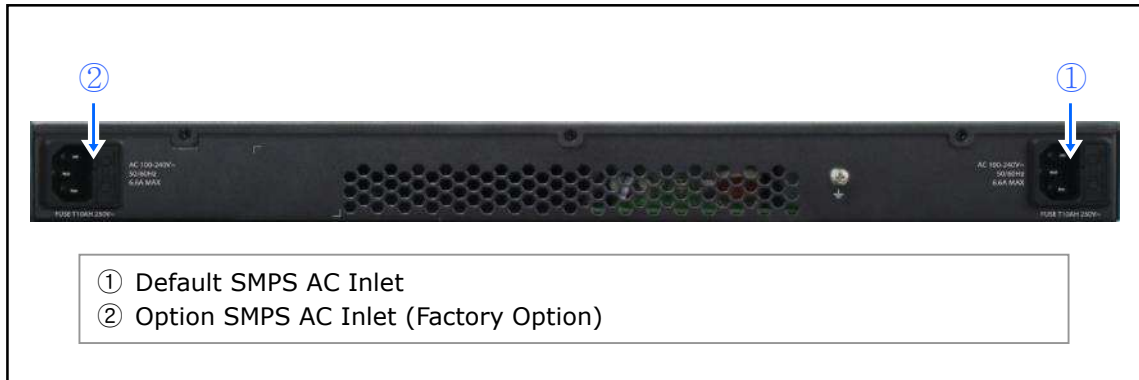
```
SG2124GP#show system fan      → FAN 정상 동작 상태
System Fan : OK

SG2124GP#show system fan
Board Fan #1 : OK
Board Fan #2 : OK
Board Fan #3 : OK
PSU1 Fan #1 : OK
PSU1 Fan #2 : Failed          → FAN 동작 상태 Fail
PSU1 Fan #3 : Failed
PSU1 Fan #4 : OK
PSU2 Fan #1 : OK
PSU2 Fan #2 : OK
PSU2 Fan #3 : OK
PSU2 Fan #4 : OK
SG2124GP#
```

4.9.3 PSU Fail 확인

Dual PSU가 장착된 SG Switch Series에서 PSU의 동작에 이상이 발생한 경우 Alarm LED가 점멸합니다.

[그림 4-1] 장비 후면 외관



PSU Fail로 인하여 Alarm LED 점멸 시, 전원 케이블이 전원 콘센트에 불완전하게 연결된 상태인 지를 먼저 확인하시기 바라며, 확인 후에도 동일 증상이 계속 발생하는 경우에는 고객센터로 연락하여 점검을 받으시기 바랍니다.

PSU 동작 상태를 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show system psu	TOP	PSU의 동작 상태를 확인합니다.

<예제> PSU 동작 상태 확인

```
SG2124G#show system psu
Number of PSU      : 2
```

```
PSU #1 Installed   : ON          → PSU 장착여부
PSU #1 Board Power : OK          → Board Power 정상동작 여부
PSU #1 Fan Power   : OK          → FAN Power 정상동작 여부
PSU #1 AC Power    : ON          → 전원 ON/OFF 상태
PSU #2 Installed   : ON
PSU #2 Board Power : OK
PSU #2 Fan Power   : OK
PSU #2 AC Power    : ON
```

4.10 Wizard 기능을 이용한 손쉬운 설치

Wizard 기능은 스위치에 익숙하지 않는 사용자를 위한 Easy Config 기능입니다.

Wizard 기능은 `ipt`, `mgmt`, `security`의 세가지로 분류되며, 각각 IPT 환경 구축을 위해 `voice-vlan` 설정을 쉽게 할 수 있는 `wizard ipt`, ip configuration 이나 `gateway` 설정 등 기본 management 설정을 위한 `wizard mgmt`, DSS 와 관련된 `uplink` 포트나 `downlink` 포트, 정책 등을 설정하는 `wizard security`가 지원됩니다.

Wizard 기능을 사용하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
<code>wizard {ipt mgmt security}</code>	TOP	Wizard (ipt, mgmt, security) 기능을 실행합니다.



참고

Wizard 기능은 `factory-default` 환경에서 설정하는 것을 권장하며, `mgmt` 와 `ipt`는 `console` 환경이 아닌, `vty(ssh, telnet)` 환경에서는 사용할 수 없습니다.

<예제1> Wizard기능을 이용한 IPT 환경 설정

```
SG2124GP#wizard ipt
```

```
-----
Configuration Wizard
-----
```

```
* It is recommended to run in the factory-default state.
* If you press Ctrl+C will be terminated at any time.
* Want to continue? (y/n) y
```

```
- IP Telephony configuration
```

```
- Voice VLAN ID : (200) → 기본값으로 설정하는 경우 Enter
```

```
- Data VLAN ID : (100)
```

```
- Uplink Port-Range : (ge23-24)
```

```
- User Port-Range : (ge1-22)
```

```
- Auto Voice-vlan & QOS (y/n) : (n) y
```

```

- Voice-vlan Telephony OUI : (ex 00-11-22)

- Queue scheduling : Strictly Priority Queue (SPQ) (y/n) : (y)

* queue sched spq
* vlan add 100
* vlan add 200
* ge23-24 switchport mode trunk
* ge23-24 switchport trunk allowed vlan add 200,100
* ge1-22 switchport mode hybrid
* ge1-22 switchport hybrid vlan 100
* ge1-22 switchport voice vlan 200
* ge1-22 switchport hybrid allowed vlan add 100 egress-tagged disable

- Apply configuration? (y/n): y

- Write memory (y/n): (y) y
Building configuration...
[OK]

SG2124GP#show vlan
                                Bridge Group : 1

VLAN ID   Name                State   Member ports (u)-Untagged, (t)-Tagged
=====
1          default              ACTIVE  ge23(u) ge24(u)
100        VLAN0100              ACTIVE  ge23(t) ge24(t) ge1(u) ge2(u) ge3(u) ge4(u)
                                         ge5(u) ge6(u) ge7(u) ge8(u) ge9(u) ge10(u)
                                         ge11(u) ge12(u) ge13(u) ge14(u) ge15(u)
                                         ge16(u) ge17(u) ge18(u) ge19(u) ge20(u)
                                         ge21(u) ge22(u)
200        VLAN0200              ACTIVE  ge23(t) ge24(t) ge1(t) ge2(t) ge3(t) ge4(t)
                                         ge5(t) ge6(t) ge7(t) ge8(t) ge9(t) ge10(t)
                                         ge11(t) ge12(t) ge13(t) ge14(t) ge15(t)
                                         ge16(t) ge17(t) ge18(t) ge19(t) ge20(t)
                                         ge21(t) ge22(t)

SG2124GP#show lldp config
- Global LLDP                : Enabled
- Message Tx Interval        : 30 sec
- Message Tx HoldMultiplier : 4
- ReInit Delay               : 2
- Tx Delay                   : 2
- MED Device Type Value      : Network Connectivity
- MED Fast Start Count       : Disabled

-----
Port      Status   PortEnable tlvMgmt MedTxEnable Policy
=====
ge1       RxTx                Enable    Voice
ge2       RxTx                Enable    Voice
ge3       RxTx                Enable    Voice
ge4       RxTx                Enable    Voice
ge5       RxTx                Enable    Voice
- 요약 -

```

```

SG2124GP#show running-config
!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
!
snmp-server disable
!
bridge 1 protocol pvstp
!
vlan database
  vlan range 100,200 bridge 1
!
bridge 1 pvstp vlan 1
no bridge 1 pvstp enable bridge-forward bpdu-flood
!
mds enable ge1-22 detect
mds uplink ge23-24
mds syslog enable
mds auto-config config-save
!
mls qos enable
  queue sched spq
!
lldp enable
lldp port both all
lldp tlv dot3tlv power-via-mdi all
lldp med port tx-enable ge1-22
!
interface ge1
  switchport mode hybrid
  switchport hybrid vlan 100
  switchport mode hybrid acceptable-frame-type all
  switchport voice vlan 200
  switchport hybrid allowed vlan add 100 egress-tagged disable
  switchport hybrid native vlan 100
!
-- 이하 생략 --

```

<예제2> Wizard기능을 이용한 MGMT 환경 설정

```

SG2124GP#wizard mgmt

-----
Configuration Wizard
-----

* It is recommended to run in the factory-default state.
* If you press Ctrl+C will be terminated at any time.

```

```

* Want to continue? (y/n) y

- Management configuration

- IP Address of Vlan 1 : 192.168.255.205

- Subnet mask of Vlan 1 : (255.255.255.0)

- Default Gateway : 192.168.255.254

- SNMP ReadOnly Community String : (public) sg2124g

- SNMP ReadWrite Community String : (private) sg2124gp

- VNM(Visual Node Manager) IP Address : 192.168.255.135

* ip address 192.168.255.205/24
* ip route 0.0.0.0/0 192.168.255.254
* snmp-server community ro sg2124g
* snmp-server community rw sg2124gp
* mds log-server 192.168.255.135

- Apply configuration? (y/n) : y
% Config not enabled
% Config not enabled
→ SNMP-Server 가 Disable 되어 있기 때문
  Wizard 설정 완료 후 SNMP 활성화 필요

- Write memory (y/n): (y) y
Building configuration...
[OK]

SG2124GP#show running-config
!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
!
snmp-server disable
snmp-server community ro sg2124g
snmp-server community rw sg2124gp
!
-- 이하 생략 --

```

<예제3> Wizard기능을 이용한 Security 환경 설정

SG2124GP#wizard security

```

-----
Configuration Wizard
-----

```

```

* It is recommended to run in the factory-default state.
* If you press Ctrl+C will be terminated at any time.
* Want to continue? (y/n) y

```

```

- Security configuration

- MDS Uplink Port-Range : (ge23-24)

- MDS Downlink Port-Range : (ge1-22)

- MDS Mode configuration (detect/drop): (detect)

- MDS ARP Spoofing Attack (y/n) : (y)

- MDS ARP Spoofing Port-Range : (ge1-22)

- MDS ARP Spoofing Mode (detect/drop) : (drop)

- MDS Self-loop Detect Enable (y/n) : (y)

- MDS Self-loop Detect Port-Range : (ge1-22)

- MDS WEB-Alert Enable (y/n) : (n)

```

```

* mds uplink ge23-24
* mds enable ge1-22 detect
* mds arp-spoofing drop ge1-22
* mds self-loop-detect ge1-22

```

```

- Apply configuration? (y/n): y

```

```

- Write memory (y/n): (y) y

```

```

Building configuration...

```

```

[OK]

```

SG2124GP#show running-config

```

!
service password-encryption
!
username root password *****
!
ip domain-lookup
!
snmp-server disable
!
bridge 1 protocol pvstp
!

```



```

bridge 1 pvstp vlan 1
no bridge 1 pvstp enable bridge-forward bpdu-flood
!
mds enable ge1-22 detect
mds uplink ge23-24
mds self-loop-detect ge1-22
mds syslog enable
mds auto-config config-save
mds arp-spoofing drop ge1-22
!

```

- 요약 -

SG2124GP#show mds config

```

- Syslog                : Enable
- Mode Button           : Disable
- Detect Service Port Range : Enable
- Detect port lock      : Disable
- DDOS                  : Enable
- DHCP-Filter           : Enable
- Bandwidth-Monitor     : Enable
- ICMP Redirect         : Enable
- Fragment Attack       : Disable
- Smurf Attack          : Disable
- Crc Attack            : Enable
- IPV6 DAD Attack       : Disable
- Smart-Phone Filter    : Disable
- AUTO Config           : Enable
- AUTO Config Relay     : Disable
- IPM Collision Check   : Enable
- IPM Guard To Mac Security : Enable
- IPM Local DHCP        : Disable

```

* Downlink Mode : Drop "0", Detect "-"

* Arp-Spoofing Mode : Drop "0", Detect "-"

```

=====
Port | UP |Down | ARP |Self | Mac | DAD | IfPkt| IPM |Smart
      |Link|Link |Spoof|Loop |Flood|      |Loss |Port |Phone
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
ge1  |   | -   | 0   | 0   |   |   |   |   |   |
ge2  |   | -   | 0   | 0   |   |   |   |   |   |
ge3  |   | -   | 0   | 0   |   |   |   |   |   |
ge4  |   | -   | 0   | 0   |   |   |   |   |   |
ge5  |   | -   | 0   | 0   |   |   |   |   |   |
-- 이하 생략 --

```

4.11 Tech-Support

Tech-support는 장비 점검 시 확인해야 할 주요 설정내역과 상태를 출력합니다.

Version 정보, cpu-load, memory, system alarm 외에도 interface 정보, mds 내역 등을 모두 출력해 보여줍니다. ftp/sftp/tftp 서버와 usb로 내역을 저장할 수 있습니다.

Tech-Support 정보를 출력하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
show tech-support [terminal]	TOP	Tech-support 내역을 화면에 출력합니다.
show tech-support ftp {IP_Addr IPv6_Addr} FILENAME ID PASSWORD [port <1-65535>]	TOP	Tech-support 내역을 ftp server에 저장합니다.
show tech-support sftp {IP_Addr IPv6_Addr} FILENAME ID [port <1-65535>]	TOP	Tech-support 내역을 sftp server에 저장합니다.
show tech-support tftp {IP_Addr IPv6_Addr} FILENAME	TOP	Tech-support 내역을 tftp server에 저장합니다.
show tech-support usb FILENAME	TOP	Tech-support 내역을 usb 저장매체에 저장합니다.

<예제> FTP Server로 tech-support 저장 및 화면 출력

```
SG2124G#show tech-support ftp 192.168.1.1 tech_support.log user password
Filename is tech_support.log
Starting Transmission....
Finished ....
SG2124G#
SG2124G#show tech-support

**** show version ****

SG-24GX-2.0.7 04/23/12 16:38:41
Copyright (C) HanDreamNet. All rights reserved.

**** show clock ****

Mon Jun 11 11:22:33 GMT+9 2012
```

**** show system system-info ****

```
Vendor       : HanDreamNet
Model        : SG2124G
Serial No    : SG1149780001
Main Memory  : 512MB
Flash Memory : 64MB
MGMT MAC     : 00:1A:F4:BC:00:0A
SF BASE MAC  : 00:1A:F4:3C:00:0A
HW Version   : V1.1
BootLoader Version : 2.4.0
```

**** show system uptime ****

11:22:33 up 6 days, 22:00, 0 users, load average: 1.05, 1.20, 1.17

**** show system cpu-load ****

Time	sum	user	system
5 sec :	10.88%	3.45%	7.42%
30 sec :	12.82%	4.71%	8.08%
1 min :	13.59%	5.17%	8.34%
5 min :	13.97%	5.25%	8.43%
15 min :	13.19%	4.41%	7.68%
60 min :	9.99%	0.91%	5.51%
all-time :	12.64%	4.58%	8.05%

**** show system memory detail ****

```
MemTotal:    498324 kB
MemFree:     334340 kB
Buffers:      0 kB
Cached:      48516 kB
SwapCached:   0 kB
Active:      67396 kB
-More-
```

-- 이하 생략 --



참고

'show tech-support' 사용 전 'terminal length 0' 명령을 실행하면 show tech-support 출력 시 '-more-' 표시 없이 한꺼번에 모든 내용이 출력됩니다.

4.12 RAW IP Protocol

	Keyword	Protocol	References
0	HOPOPT	IPv6 Hop-by-Hop Option	[RFC1883]
1	ICMP	Internet Control Message	[RFC792]
2	IGMP	Internet Group Management	[RFC1112]
3	GGP	Gateway-to-Gateway	[RFC823]
4	IP	IP in IP (encapsulation)	[RFC2003]
5	ST	Stream	[RFC1190][RFC1819]
6	TCP	Transmission Control	[RFC793]
7	CBT	CBT	[Ballardie]
8	EGP	Exterior Gateway Protocol	[RFC888][DLM1]
9	IGP	any private interior gateway (used by Cisco for their IGRP)	[IANA]
10	BBN-RCC-MON	BBN RCC Monitoring	[SGC]
11	NVP-II	Network Voice Protocol	[RFC741][SC3]
12	PUP	PUP	[PUP][XEROX]
13	ARGUS	ARGUS	[RWS4]
14	EMCON	EMCON	[BN7]
15	XNET	Cross Net Debugger	[IEN158][JFH2]
16	CHAOS	Chaos	[NC3]
17	UDP	User Datagram	[RFC768][JBP]
18	MUX	Multiplexing	[IEN90][JBP]
19	DCN-MEAS	DCN Measurement Subsystems	[DLM1]
20	HMP	Host Monitoring	[RFC869][RH6]
21	PRM	Packet Radio Measurement	[ZSU]
22	XNS-IDP	XEROX NS IDP	[ETHERNET][XEROX]
23	TRUNK-1	Trunk-1	[BWB6]
24	TRUNK-2	Trunk-2	[BWB6]
25	LEAF-1	Leaf-1	[BWB6]
26	LEAF-2	Leaf-2	[BWB6]

27	RDP	Reliable Data Protocol	[RFC908][RH6]
28	IRTP	Internet Reliable Transaction	[RFC938][TXM]
29	ISO-TP4	ISO Transport Protocol Class 4	[RFC905][RC77]
30	NETBLT	Bulk Data Transfer Protocol	[RFC969][DDC1]
31	MFE-NSP	MFE Network Services Protocol	[MFENET][BCH2]
32	MERIT-INP	MERIT Internodal Protocol	[HWB]
33	DCCP	Datagram Congestion Control Protocol	[RFC4340]
34	3PC	Third Party Connect Protocol	[SAF3]
35	IDPR	Inter-Domain Policy Routing Protocol	[MXS1]
36	XTP	XTP	[GXC]
37	DDP	Datagram Delivery Protocol	[WXC]
38	IDPR-CMTP	IDPR Control Message Transport Proto	[MXS1]
39	TP++	TP++ Transport Protocol	[DXF]
40	IL	IL Transport Protocol	[Presotto]
41	IPv6	Ipv6	[Deering]
42	SDRP	Source Demand Routing Protocol	[DXE1]
43	IPv6-Route	Routing Header for IPv6	[Deering]
44	IPv6-Frag	Fragment Header for IPv6	[Deering]
45	IDRP	Inter-Domain Routing Protocol	[Hares]
46	RSVP	Reservation Protocol	[Braden]
47	GRE	General Routing Encapsulation	[Li]
48	DSR	Dynamic Source Routing Protocol	[RFC4728]
49	BNA	BNA	[Salamon]
50	ESP	Encap Security Payload	[RFC2406]
51	AH	Authentication Header	[RFC2402]
52	I-NLSP	Integrated Net Layer Security TUBA	[GLENN]
53	SWIPE	IP with Encryption	[JI6]
54	NARP	NBMA Address Resolution Protocol	[RFC1735]
55	MOBILE	IP Mobility	[Perkins]
56	TLSP	Transport Layer Security Protocol using Kryptonet key management	[Oberg]

57	SKIP	SKIP	[Markson]
58	IPv6-ICMP	ICMP for IPv6	[RFC1883]
59	IPv6-NoNxt	No Next Header for IPv6	[RFC1883]
60	IPv6-Opts	Destination Options for IPv6	[RFC1883]
61		any host internal protocol	[IANA]
62	CFTP	CFTP	[CFTP][HCF2]
63		any local network	[IANA]
64	SAT-EXPAK	SATNET and Backroom EXPAK	[SHB]
65	KRYPTOLAN	Kryptolan	[PXL1]
66	RVD	MIT Remote Virtual Disk Protocol	[MBG]
67	IPPC	Internet Pluribus Packet Core	[SHB]
68		any distributed file system	[IANA]
69	SAT-MON	SATNET Monitoring	[SHB]
70	VISA	VISA Protocol	[GXT1]
71	IPCV	Internet Packet Core Utility	[SHB]
72	CPNX	Computer Protocol Network Executive	[DXM2]
73	CPHB	Computer Protocol Heart Beat	[DXM2]
74	WSN	Wang Span Network	[VXD]
75	PVP	Packet Video Protocol	[SC3]
76	BR-SAT-MON	Backroom SATNET Monitoring	[SHB]
77	SUN-ND	SUN ND PROTOCOL-Temporary	[WM3]
78	WB-MON	WIDEBAND Monitoring	[SHB]
79	WB-EXPAK	WIDEBAND EXPAK	[SHB]
80	ISO-IP	ISO Internet Protocol	[MTR]
81	VMTP	VMTP	[DRC3]
82	SECURE-VMTP	SECURE-VMTP	[DRC3]
83	VINES	VINES	[BXH]
84	TTP	TTP	[JXS]
85	NSFNET-IGP	NSFNET-IGP	[HWB]
86	DGP	Dissimilar Gateway Protocol	[DGP][ML109]
87	TCF	TCF	[GAL5]
88	EIGRP	EIGRP	[CISCO][GXS]

89	OSPFIGP	OSPFIGP	[RFC1583][JTM4]
90	Sprite-RPC	Sprite RPC Protocol	[SPRITE][BXW]
91	LARP	Locus Address Resolution Protocol	[BXH]
92	MTP	Multicast Transport Protocol	[SXA]
93	AX.25	AX.25 Frames	[BK29]
94	IPIP	IP-within-IP Encapsulation Protocol	[JI6]
95	MICP	Mobile Internetworking Control Pro.	[JI6]
96	SCC-SP	Semaphore Communications Sec. Pro.	[HXH]
97	ETHERIP	Ethernet-within-IP Encapsulation	[RFC3378]
98	ENCAP	Encapsulation Header	[RFC1241,RXB3]
99		any private encryption scheme	[IANA]
100	GMTP	GMTP	[RXB5]
101	IFMP	Ipsilon Flow Management Protocol	[Hinden]
102	PNNI	PNNI over IP	[Callon]
103	PIM	Protocol Independent Multicast	[Farinacci]
104	ARIS	ARIS	[Feldman]
105	SCPS	SCPS	[Durst]
106	QNX	QNX	[Hunter]
107	A/N	Active Networks	[Braden]
108	IPComp	IP Payload Compression Protocol	[RFC2393]
109	SNP	Sitara Networks Protocol	[Sridhar]
110	Compaq-Peer	Compaq Peer Protocol	[Volpe]
111	IPX-in-IP	IPX in IP	[Lee]
112	VRRP	Virtual Router Redundancy Protocol	[RFC3768]
113	PGM	PGM Reliable Transport Protocol	[Speakman]
114		any 0-hop protocol	[IANA]
115	L2TP	Layer Two Tunneling Protocol	[Aboba]
116	DDX	D-II Data Exchange (DDX)	[Worley]
117	IATP	Interactive Agent Transfer Protocol	[Murphy]
118	STP	Schedule Transfer Protocol	[JMP]
119	SRP	SpectraLink Radio Protocol	[Hamilton]
120	UTI	UTI	[Lothberg]

121	SMP	Simple Message Protocol	[Ekblad]
122	SM	SM	[Crowcroft]
123	PTP	Performance Transparency Protocol	[Welzl]
124	ISIS over IPv4		[Przygienda]
125	FIRE		[Partridge]
126	CRTP	Combat Radio Transport Protocol	[Sautter]
127	CRUDP	Combat Radio User Datagram	[Sautter]
128	SSCOPMCE		[Waber]
129	IPLT		[Hollbach]
130	SPS	Secure Packet Shield	[McIntosh]
131	PIPE	Private IP Encapsulation within IP	[Petri]
132	SCTP	Stream Control Transmission Protocol	[Stewart]
133	FC	Fibre Channel	[Rajagopal]
134	RSVP-E2E-IGNORE		[RFC3175]
135	Mobility Header		[RFC3775]
136	UDPLite		[RFC3828]
137	MPLS-in-IP		[RFC4023]
138	manet	MANET Protocols	[RFC-ietf-manet-iana-07.txt]
139	HIP	Host Identity Protocol	[RFC5201]
140-252		Unassigned	[IANA]
253		Use for experimentation and testing	[RFC3692]
254		Use for experimentation and testing	[RFC3692]
255	Reserved		[IANA]

4.13 RFC / IEEE Support

4.13.1 RFC Support

RFC 768	User Datagram Protocol
RFC 783	Trivial File Transfer Protocol (TFTP)
RFC 791/950	Internet Protocol (IP)
RFC 792	Internet Control Message Protocol (ICMP)
RFC 793	Transmission Control Protocol
RFC 826	Address Resolution Protocol (ARP)
RFC 854	Telnet Server and Client
RFC 894	IP Datagrams over Ethernet Networks
RFC 951/1542	BOOTP
RFC 1112	Internet Group Management Protocol v1
RFC 1157	Simple Network Management Protocol (SNMP)
RFC 1213	Management Information Base for Network Management of TCP/IP-based Internets (MIB II)
RFC 1215	SNMP Traps Definition
RFC 1271/ 1757/ 2819	Remote Network Monitoring Management Information Base
RFC 1350	TFTP Protocol
RFC 1354	IP Forwarding Table MIB
RFC 1361/1769	Simple Network Time Protocol (SNTP)
RFC 1442	Simple Network Management Protocol (SNMPv2)
RFC 1450	MIBv2 for SNMPv2
RFC 1492	Access Control Protocol aka TACACS
RFC 1493/4188	Bridge MIB
RFC 1519	Classless Inter-Domain Routing (CIDR)
RFC 1541	Dynamic Host Configuration Protocol
RFC 1542	Bootstrap Protocol (Clarifications and Extensions)
RFC 1573/2863	Interface MIB

RFC 1591	Domain Name System
RFC 1643/2665	Ethernet Interface MIB
RFC 1901	Introduction to Community-based SNMPv2
RFC 1905/3416	SNMP
RFC 1906/3417	SNMP Transport Mappings
RFC 1907/3418	SNMP MIB
RFC 2011	SNMP v2 MIB for IP
RFC 2012	SNMP v2 MIB for TCP
RFC 2013	SNMP v2 MIB for UDP
RFC 2131	DHCP
RFC 2138/2865	RADIUS Authentication
RFC 2139/2866	RADIUS Accounting
RFC 2030	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
RFC 2096	IP Forwarding Table MIB
RFC 2236/3376	Internet Group Management Protocol v2/ v3
RFC 2328	Open Shortest Path First v2
RFC 2452	IPv6 TCP MIB
RFC 2454	IPv6 UDP MIB
RFC 2460	IPv6 (for switch management only)
RFC 2463	ICMPv6
RFC 2464	Transmission of IPv6 over Ethernet
RFC 2465	IPv6 MIB
RFC 2466	ICMPv6 MIB
RFC 2474	Differentiated Services Support
RFC 2475	An Architecture for Differentiated Service
RFC 2526	Reserved IPv6 Subnet Anycast Addresses
RFC 2570/3410	SNMPv3
RFC 2571/3411	SNMP Frameworks
RFC 2572/3412	SNMP Message Processing
RFC 2573/3413	SNMPv3 Applications
RFC 2574/3414	SNMPv3 USM

RFC 2575/3415	SNMPv3 VACM
RFC 2576/3584	Co-existence of SNMP v1/v2/v3
RFC 2665	Ethernet MIB
RFC 2674/4363	Q-Bridge MIB
RFC 2737	Entity MIBv2
RFC 2819	RMON MIB (group 1, 2, 3, 9)
RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2925	Managed objects for Ping, Traceroute & Lookup
RFC 2992	ECMP Algorithm
RFC 3046	DHCP Relay agent
RFC 3176	sFlow
RFC 3576	IEEE 802.1X Security Extensions
RFC 3621	Power Ethernet MIB
RFC 3748	Extensible Authentication Protocol (EAP)
RFC 3826	Advanced Encryption Standard (AES) Cipher Algorithm in SNMP
RFC 4251	SSH Protocol architecture
RFC 4252	SSH Authentication Protocol
RFC 4253	SSH Transport protocol
RFC 4254	SSH Connection protocol

4.13.2 IEEE Support

IEEE 802.1D	Spanning Tree Protocol
IEEE 802.1p	Priority Queues, Class of Service (CoS)
IEEE 802.1Q	VLANs
IEEE 802.1s	Multiple Spanning Tree Protocol
IEEE 802.1v	VLAN Classification
IEEE 802.1w	Rapid Spanning Tree Protocol
IEEE 802.1X	Port Based Network Access Control (Extensible Authentication Protocol)
IEEE 802.1AB	Link Layer Discovery Protocol
IEEE 802.1AB	LLDP MED & Location TLV
IEEE 802.1ad	VLAN Stacking (QinQ, Provider Bridges)
IEEE 802.3	10BASE-T Ethernet
IEEE 802.3ab	1000Base-T Ethernet
IEEE 802.3ad	Static or Dynamic Link Aggregation (LACP)
IEEE 802.3i	10BASE-T Auto-negotiation
IEEE 802.3u	100BASE-TX Fast Ethernet
IEEE 802.3u	Auto-Negotiation on Twisted Pair (ISO/IEC 8802-3, Clause 28)
IEEE 802.3x	Full-duplex Flow Control
IEEE 802.3z	Gigabit Ethernet (1000BASE-X)

4.14 Syslog Event 정의

No	Syslog Messages	Description	Level
1	NSM: Bridge Port add failed on aggregator member	Link Aggregator를 Bridge에 추가할 때 멤버포트들도 Bridge에 추가하는데 멤버포트 추가 오류가 발생한 경우	error
2	NSM: Bridge Port delete failed on aggregator member	Link Aggregator를 Bridge에서 삭제할 때 멤버포트들도 Bridge에서 삭제하는데 멤버포트 삭제 오류가 발생한 경우	error
3	NSM: To and From interface is the same	Mirror 설정 시 Mirror 포트와 Mirrored-to 포트가 같을 경우	error
4	NSM: Can't enable vlan stacking	VLAN Stacking을 활성화할 수 없는 경우	error
5	NSM: Can't disable vlan stacking	VLAN Stacking을 비활성화할 수 없는 경우	error
6	NSM message send error socket	NSM 데몬이 NSM Client 데몬에 메시지를 보내 수 없는 경우	error
7	NSM: Can't set interface's address	Interface IP Address를 Kernel에 설정할 수 없을 경우	warning
8	NSM: Cannot initialize routing socket. Exiting!!!	Kernel과 Switch Chip 초기화에 실패한 경우	warning
9	NSM: Port up notification received for port	Interface Link-Up Event	informational
10	NSM: Port down notification received for port	Interface Link-Down Event	informational
11	NSM: NSM client disconnect	NSM Client가 NSM으로부터 Disconnect 된 경우	informational
12	802.1X: BE[]: State IDLE	802.1X Authenticator 상태가 Idle인 경우	informational
13	802.1X: BE[]: State REQUEST	802.1X Authenticator 상태가 Request인 경우	informational
14	802.1X: BE[]: State RESPONSE	802.1X Authenticator 상태가 Response인 경우	informational
15	802.1X: BE[]: State SUCCESS	802.1X Authenticator 상태가 Success인 경우	informational
16	802.1X: BE[]: State FAIL	802.1X Authenticator 상태가 Fail인 경우	informational
17	802.1X: BE[]: State TIMEOUT	802.1X Authenticator 상태가 Timeout인 경우	informational
18	802.1X: BE[]: State INITIALIZE	802.1X Authenticator 상태가	informational

		Initialize인 경우	
19	802.1X: No Current RADIUS server	802.1X 인증용 RADIUS 서버가 지정되어 있지 않을 경우	warning
20	802.1X: [EAPOL]: Wrong destination MAC address	802.1X EAPOL 프레임의 DST MAC 이 잘못된 경우	informational
21	802.1X: [EAPOL-Unknown]: Wrong packet type	802.1X EAPOL 프레임의 Packet Type이 잘못된 경우	informational
22	802.1X: [EAPOL]: Wrong EAP length	802.1X EAPOL 프레임의 길이가 잘못된 경우	informational
23	802.1X: PORT[]: Up the port	Interface Link-Up Event를 수신하고 802.1X 인증을 시작	informational
24	802.1X: PORT[]: Down the port	Interface Link-Down Event를 수신하고 802.1X 인증을 중지	informational
25	802.1X: PORT[]: 802.1Xorize the port	802.1X에 의해 Interface가 Authorize될 경우	informational
26	802.1X: PORT[]: Un802.1Xorize the port	802.1X에 의해 Interface가 Unauthorize될 경우	informational
27	802.1X: PORT[]: Add the port	Interface에 802.1X 활성화	informational
28	802.1X: PORT[]: Delete the port	Interface에 802.1X 비활성화	informational
29	STP: stp_handle_bpdu: Invalid BPDU received on port	STP 모드로 동작 중에 RSTP BPDU를 수신한 경우	warning
30	STP: stp_handle_bpdu: Config BPDU on port failed message age check	수신한 STP BPDU의 Message Age가 Max Age를 초과한 경우	warning
31	STP: stp_handle_bpdu: Invalid BPDU type received on port	Config 혹은 TCN BPDU가 아닌 경우	warning
32	STP: 2 * (Forward delay - 1) must be >= Max age	STP max-age 설정 값이 Forward Delay 설정 값에 비해 너무 큰 경우	warning
33	STP: Max age must be greater than 2 * (Hello time + 1)	STP max-age 설정 값이 hello-time 설정 값에 비해 너무 작은 경우	warning
34	STP: Hello time must be greater than Hold time	STP hello-time 설정 값이 hold-time 값보다 작은 경우	warning
35	STP: Unable to set ageing time for bridge	STP가 MAC Table Aging-time을 변경할 수 없는 경우	warning
36	STP: Received BPDU on PortFast enable port. shutting down	STP bpdu-guard가 설정된 Interface에서 BPDU가 수신된 경우	warning
37	in.telnetd[]: connect from 192.168.100.194	192.168.100.194 Host가 Switch에 Telnet 접속할 경우	informational
38	inetd[]: pid 2084: exit status 1	Host가 Telnet 접속을 종료할 경우	informational
39	telnetd[]: ttloop: peer died: EOF	Host의 Telnet 접속이 비정상적으로 종료된 경우	informational
40	kernel: too high temperature	현재 Switch의 온도가 지정된 온도	warning

	detected	의 High값보다 높은 경우	
41	kernel: too low temperature detected	현재 Switch의 온도가 지정된 온도 의 Low값보다 낮은 경우	warning
42	kernel: system fan malfunction detected	FAN 동작이 정지된 경우	warning
43	kernel: system fan malfunction recoverd	FAN 동작이 다시 실행된 경우	warning
44	sensor_comm: sensor_event_entry no:Rule- number name:DoS_Attack attacker:Attacker-IP proto:TCP dest_ip:Destination-IP svc_port:Attack Port	MDS엔진에서 Attack을 감지하여 Detect-list에 생성된 EVENT Message	informational
45	sensor_comm: sensor_event_leave no:Rule- number name:DoS_Attack attacker:Attacker-IP proto:TCP dest_ip:Destination-IP svc_port:Attack port drop_count:count conn_sec:lease-time	MDS엔진에서 Detect-list에 감지되 었던 Attack이 해제된 Event Message	Informational
46	CPU ACL drop, src_ip:IP주소, service_type:ssh 혹은 snmp	CPU-ACL에 의해 차단된 경우	informational
47	acl match - Rule_No Deny 혹은 Permit 매치된조건 (Count: 매치 카운터)	ACL rule에 매치된 경우	informational
48	Because syslog exceeds the size of 2MB, It has been back- up	Syslog가 포화되어 backup 된 경 우	informational
49	MDS Logfile remove	MDS 로그가 포화된 경우	Informational
50	Starting system log daemon	로그 데몬 구동	Informational
51	Sensor start	MDS 구동	Informational
52	Bad magic number	이미지 헤더의 매직 넘버가 정해진 값과 다를 경우	Informational
53	Invalid image size	이미지 크기가 이미지 헤더에 명시 된 크기와 다를 경우	Informational
54	Bad header checksum	이미지 헤더에 대한 CRC32 checksum 값이 이미지 헤더에 명 시된 헤더 checksum 값과 다를 경 우	Informational
55	Bad data checksum	이미지 데이터에 대한 CRC32 checksum 값이 이미지 헤더에 명 시된 데이터 checksum 값과 다를 경우	informational
56	Invalid image name	이미지 헤더에 있는 이미지 이름과 현재 시스템의 모델 이름이 다를 경 우	Informational

4.15 MDS 엔진에서 탐지하는 공격 유형

MDS엔진에서 탐지하는 공격유형은 다음과 같습니다.

공격 유형	설명
IPv4/IPv6 DoS Attack	공격자가 공격대상 호스트의 Well Known 포트로 Packet을 빠른 속도로 전송하는 형태. TCP DoS 공격에 대해선 TCP SYN 플러딩 공격만 탐지함
IPv4/IPv6 IP Spoofing Attack	공격자가 출발지 IP를 변조하여 Packet을 전송하는 형태
IPv4 ARP Spoofing Attack	공격자가 ARP를 위조하여 공격대상에게 전송하여 통신하는 Packet을 가로채는 형태
IPv4/IPv6 Host Scan Attack IPv4/IPv6 Host Scan Flooding Attack	공격자가 대상 네트워크내에 있는 모든 호스트에게 TCP, UDP, ICMP Request Packet을 IP를 증가하며, SCANNING 하는 형태
IPv4/IPv6 Port Scan Attack	공격자가 공격대상 호스트의 TCP, UDP 포트에 순차적으로 접근하는 형태
IPv4/IPv6 Host Random Attack IPv4/IPv6 Host Random Flooding Attack	공격자가 공격할 TCP, UDP 포트로 임의의 목적지 IP 주소로 Packet을 Flooding하는 형태
IPv4/IPv6 MAC Flooding Attack	공격자가 스위치의 MAC Address Table을 모두 소진하도록 Random하게 위조된 MAC 주소 Packet을 전송하는 형태
IPv4 ARP Attack	공격자가 ARP Packet을 빠른 속도로 전송하는 형태
IPv4/IPv6 Broadcast Attack	공격자가 Broadcast Packet을 빠른 속도로 전송하여 네트워크의 속도저하를 발생하는 형태
IPv4 IGMP DoS	공격자가 특정 IPv4 멀티캐스트 주소로 IGMP query, report 메시지를 빠른 속도로 전송하는 형태
IPv6 MLD DoS	공격자가 특정 IPv6 멀티캐스트 주소로 MLD query, report, done 메시지를 빠른 속도로 전송하는 형태
IPv6 DAD Attack	IPv6 link local 주소 혹은 global 주소가 할당되거나 설정될 때 중복된 IP가 존재하는지 확인하기 위해 보내는 NS 메시지에 대해 공격자가 자신이 사용하는 IP 주소인 것처럼 NA를 보냄으로써 IP 주소를 사용할 수 없도록 만드는 공격

SG Switch Series Command Guide

© 2015 HANDREAMNET Co., Ltd. All rights reserved

이 설명서의 저작권은 (주)한드림넷에 있습니다.

이 설명서는 (주)한드림넷의 서면동의 없이 어떤 형태로도 재
생산 배포 변경할 수 없습니다.

