



User Manual

V5812G

UMN : CLI NOS v3.03

이 설명서는 V5812G를 구입하신 사용자에게 제품 설정 방법을 알려 드립니다. 사용자는 본 제품 취급 전에 반드시 설명서를 잘 읽은 후 지침에 따라 제품을 바르게 설정해 주십시오. 또한, 설명서를 읽으신 후에는 잘 보관하여 관리자가 바뀔 때에는 반드시 후임 관리자에게 전달, 제품을 바르게 사용할 수 있도록 하십시오.

이 설명서는 V5812G를 설정하고 관리할 네트워크 관리자를 위한 것입니다. 따라서 이 설명서를 이용할 네트워크 관리자는 네트워크 장비에 대한 전문적인 지식과 LAN(Local Area Network) 구축 및 운영에 대한 경험이 요구됩니다.

※ 본 설명서의 내용과 그림 등은 제품의 기능 향상 및 그 밖의 이유로 별도의 공지 없이 변경될 수 있습니다.

※ 본 설명서의 내용은 저작권법으로부터 보호를 받습니다. 따라서 (주)다산네트웍스의 허가없이 안내서의 내용을 변경할 수 없습니다.

※ Copyright 2009 © DASAN Networks, Inc.

경기도 성남시 분당구 11-4번지
휴맥스빌리지 6층
Helpdesk) 1588-7080

Release for Update

Summary :

Initial release

Details :

Chapter/Section	Reasons for update
All	Initial release

Version history

Status	Date of release	Reasons for change
1	2009/01	Initial release

◆ 목 차 ◆

1.	개요	30
1.1	내용 구성	30
1.2	사용 기호	31
1.3	표기법	31
2.	제품 소개.....	33
2.1	주요 특징	34
3.	CLI 사용하기.....	38
3.1	명령어 체계.....	38
3.1.1.	Privilge Exec View 모드.....	39
3.1.2.	Privilege Exec Enable 모드	39
3.1.3.	Global 설정 모드.....	40
3.1.4.	Rule 설정 모드.....	41
3.1.5.	DHCP 설정 모드	43
3.1.6.	DHCP Option-82 설정 모드	44
3.1.7.	Rmon 설정 모드	44
3.1.8.	VRRP 설정 모드	45
3.1.9.	Bridge 설정 모드.....	45
3.1.10.	Interface 설정 모드	46
3.1.11.	Router 설정 모드	47
3.1.12.	Route-Map 설정 모드	47
3.1.13.	G-PON 설정 모드	48
3.2	명령어 기본 사용법	50
3.2.1.	사용 가능한 명령어 보기.....	50
3.2.2.	이전 명령어 불러내기	53
3.2.3.	축약된 명령어 사용하기.....	53
3.2.4.	Privilege Exec Enable 모드 명령어 사용하기.....	54
3.2.5.	다른 모드로 이동하기	54
4.	시스템 접속 및 IP 주소 설정	56
4.1	시스템 접속	56

4.1.1.	시스템 로그인.....	56
4.1.2.	시스템 로그인 패스워드 변경.....	58
4.1.3.	Privilege Exec Enable 모드 접속 패스워드 설정	59
4.1.4.	자동 로그 아웃 기능 설정	61
4.1.5.	사용자 계정 관리	62
(1)	사용자 계정 추가	63
(2)	사용자 권한 설정	63
(3)	설정 예제.....	67
4.1.6.	접속자 수 제한	69
4.1.7.	원격 접속.....	70
4.1.8.	원격 접속자 확인 및 연결 강제 해제	70
4.1.9.	시스템 재부팅.....	71
(1)	수동 시스템 재부팅.....	71
(2)	자동 시스템 재부팅.....	72
4.1.10.	시스템 로그아웃	74
4.2	IP 주소 설정	75
4.2.1.	인터페이스 활성화	75
4.2.2.	인터페이스 활성화 해제.....	76
4.2.3.	네트워크 인터페이스에 IP 주소 설정	76
4.2.4.	Static 경로 및 default gateway 지정	77
4.2.5.	FIB(Forwarding Information Base) 테이블 확인.....	78
4.2.6.	인터페이스 설명하기	79
4.2.7.	인터페이스 확인	80
4.3	SSH(Secure Shell)	81
4.3.1.	SSH 서버 운영	81
(1)	SSH 서버 활성화	81
(2)	현재 접속중인 클라이언트 확인	81
(3)	클라이언트 접속 해제	82
(4)	클라이언트 접속 History 확인	82
4.3.2.	클라이언트 사용법	83
(1)	SSH 서버 로그인	83
(2)	인증키 설정	83
4.3.3.	설정 예제	85
4.4	사용자 인증 포트 설정(802.1x).....	87
4.4.1.	802.1x 기본 설정	89
(1)	802.1x 활성화.....	89
(2)	인증 서버 설정	89

(3) 인증 모드 설정	91
(4) 인증 포트 설정	91
(5) 인증 포트 상태 설정	92
(6) Request/Identity 패킷 재전송 시간 설정	92
(7) 인증 시도 요청 횟수 설정	93
(8) 인증 시도 주기 설정	93
4.4.2. 802.1x 재인증 설정	94
(1) 802.1x 재인증 활성화	94
(2) 재인증 주기 설정	95
(3) 재인증 시도 주기 설정	95
(4) 포트 재인증 실행	95
4.4.3. 802.1x 인증 상태 초기화	96
4.4.4. 802.1x 설정 내용 초기화	96
4.4.5. 802.1x 설정 내용 확인	96
4.4.6. 802.1x 사용자 인증 통계 확인 및 삭제	97
4.5 시스템 사용자 인증	98
4.5.1. 사용자 인증 방법 설정	99
4.5.2. 사용자 인증 인터페이스 지정	100
4.5.3. 사용자 인증 방법 우선 순위 설정	100
4.5.4. 사용자 인증 방법 설정 내용 확인	101
4.5.5. RADIUS 설정	101
(1) RADIUS 서버 설정	101
(2) RADIUS 서버 우선 순위 설정	102
(3) 재전송 시도 횟수 설정	102
(4) 응답 시간 제한	103
4.5.6. TACACS+ 설정	104
(1) TACACS 서버 설정	104
(2) TACACS 서버 우선 순위 설정	105
(3) 인증 방식 설정	105
(4) 응답 시간 제한	106
(5) 사용자 권한 범위 지정	106
4.5.7. 사용자 작업 내용 기록	107
4.5.8. 시스템 사용자 인증 초기화	108
5. 포트 기본 설정	109
5.1 포트 기본 환경 설정	109
5.1.1. 포트 활성화	110

5.1.2.	포트 타입 지정	110
5.1.3.	Auto Nego 설정	111
5.1.4.	포트 속도 설정	111
5.1.5.	duplex 모드 설정	111
5.1.6.	Flow Control 설정	112
5.1.7.	포트 설명하기	112
5.1.8.	트래픽 통계 확인	113
(1)	포트 패킷 통계	113
(2)	프로토콜별 통계	114
5.2	포트 미러링 설정	115
5.2.1.	Monitor 포트와 Mirrored 포트 지정	116
5.2.2.	포트 미러링 활성화	116
5.2.3.	포트 미러링 설정 내용 확인	117

6. 시스템 환경 118

6.1	환경 설정	118
6.1.1.	Host name 설정	118
6.1.2.	날짜 및 시간 설정	119
6.1.3.	Time-zone 설정	119
6.1.4.	NTP 설정	121
6.1.5.	SNTP 설정	123
6.1.6.	NTP 메시지 주소 설정	125
6.1.7.	터미널 스크린 출력 상태 설정	125
6.1.8.	DNS 서버 설정	126
6.1.9.	로그인 배너 설정	129
6.1.10.	Fan 동작 설정	132
6.1.11.	데몬 강제 종료	134
6.1.12.	FTP 서버 활성화	134
6.1.13.	FTP 클라이언트 주소 설정	135
6.1.14.	Module DMI 정보 출력 설정	135
6.1.15.	시스템 임계값 설정	136
(1)	CPU 사용량 임계값 설정	136
(2)	포트 트래픽 임계값 설정	138
(3)	Fan 임계값 설정	139
(4)	온도 임계값 설정	140
(5)	메모리량 임계값 설정	141
(6)	SFP 모듈 상태 임계값 설정	142

6.2	설정 관리	144
6.2.1.	설정 내용 확인	144
6.2.2.	설정 내용 저장	145
6.2.3.	설정 내용 자동 저장	145
6.2.4.	설정 초기화 하기	146
6.2.5.	데이터 Backup 하기	146
(1)	일반 Backup 하기	147
(2)	SSH를 이용하여 데이터 Backup 하기	148
(3)	Backup 파일 확인	148
(4)	Backup 파일 삭제	149
6.3	시스템 확인	150
6.3.1.	네트워크 연결 상태 확인	151
6.3.2.	IP ICMP Source-routing	153
6.3.3.	패킷 경로 추적	155
6.3.4.	원격 접속자 확인	156
6.3.5.	MAC table 보기	157
6.3.6.	Aging time 설정	158
6.3.7.	장비 사용 시간 확인	158
6.3.8.	시스템 정보 확인	158
6.3.9.	CPU 평균 사용량 확인	159
6.3.10.	CPU 트래픽 제한	159
6.3.11.	CPU 프로세스 확인	160
6.3.12.	메모리 사용 정보 확인	161
6.3.13.	시스템 이미지 버전 확인	161
6.3.14.	시스템 이미지 파일 크기 확인	161
6.3.15.	설치된 NOS 확인하기	161
6.3.16.	Default OS 설정	163
6.3.17.	장비 상태 확인	164
6.3.18.	모듈 정보 확인	164
6.3.19.	Tech-support 확인	164
6.3.20.	부팅 정보 확인	165

7. 네트워크 관리 기능 설정 166

7.1	SNMP 설정	166
7.1.1.	SNMP v1의 Community 설정	168
7.1.2.	SNMP 에이전트의 관리자에 대한 연락처와 설치 위치 정보 지정	169
7.1.3.	SNMP v2c의 com2sec 설정	171

7.1.4.	SNMP v2c 및 v3의 Group 설정	172
7.1.5.	SNMP v2c 및 v3의 OID 공개 범위 제한(View 설정).....	173
7.1.6.	SNMP v2c 및 v3의 제한OID에 대한 접속권한부여(Access 설정).....	175
7.1.7.	SNMP v3의User 설정	176
7.1.8.	SNMP 트랩 설정	177
(1)	SNMP trap-host 지정.....	177
(2)	SNMP 트랩 모드 설정	179
(3)	Event 모드에서 SNMP 트랩 설정	179
(4)	Alarm-report 모드에서 SNMP 트랩 설정	182
(5)	ERP Alarm 중요도 설정 및 해제	187
(6)	Notify-Activity 활성화.....	188
(7)	SNMP 트랩 설정 확인	188
7.1.9.	SNMP 에이전트의 IP 지정	191
7.1.10.	SNMP 설정 확인	192
7.1.11.	SNMP 기능 해제.....	192
7.2	EFM OAM(Operation, Administration, Maintenance)	193
7.2.1.	OAM 활성화	194
7.2.2.	OAM Link 모니터링	195
7.2.3.	EFM OAM 모드 설정	195
7.2.4.	OAM Loopback 설정	196
7.2.5.	OAM Unidirection 설정	196
7.2.6.	OAM 설정 확인	197
7.3	LLDP 설정	198
7.3.1.	LLDP 동작 원리	198
(1)	LLDP 동작 방식	198
7.3.2.	LLDP 설정	198
(1)	LLDP 활성화	198
(2)	LLDP 동작 방식 설정	199
(3)	Basic TLV 설정	200
(4)	LLDP 메시지 송신 관련 설정.....	200
(5)	Reinitdelay 설정	201
(6)	LLDP 프레임 전송 Delay 시간 설정	201
(7)	LLDP 설정 확인	202
7.4	RMON 설정	203
7.4.1.	RMON History 설정	203
(1)	통계 데이터 발생 포트 지정	205
(2)	RMON History 사용 주체 명시	205

(3) 표본 데이터 수 설정	206
(4) 표본 조사 간격 설정	206
(5) RMON History 활성화 하기	207
(6) RMON History 삭제 및 설정 변경	208
7.4.2. RMON Alarm 설정	208
(1) RMON Alarm 사용 주체 명시	210
(2) 표본 조사에 사용될 object 설정	210
(3) 절대 비교 및 델타 비교 설정	211
(4) 상한 임계 값 설정	211
(5) 하한 임계 값 설정	212
(6) 최초 Alarm 기준 설정	213
(7) 표본 조사 간격 설정	214
(8) RMON Alarm 활성화 하기	214
(9) RMON Alarm 삭제 및 설정 변경	215
7.4.3. RMON Event 설정	216
(1) Event Community 설정	217
(2) Event 설명	217
(3) Event 사용 주체 명시	218
(4) Event 공지 형태 설정	218
(5) Evnet 활성화 하기	219
(6) RMON Event 삭제 및 설정 변경	220
7.5 Syslog	220
7.5.1. Syslog 메시지 Level 설정	221
7.5.2. System Facility 설정	222
7.5.3. Syslog Message Priority 설정	222
7.5.4. Syslog 해제	225
7.5.5. Syslog 설정 확인	225
7.5.6. Syslog 메시지 IP 주소 지정	226
7.5.7. 원격에서 Debug 메시지 확인하기	227
7.6 QoS(Quality of Service)	228
7.6.1. QoS 동작 원리	229
7.6.2. 패킷 분류(Classify) 설정	231
(1) 모드 설정	231
(2) Flow 설정	232
(3) Flow 내용 저장 및 수정	234
(4) Class 설정	235
7.6.3. 패킷 정책(Policing) 설정	235

(1) Policer 생성	236
(2) Metering	237
(3) 패킷 Counter	243
(4) 패킷 Rate-limit	244
(5) Policer 내용 저장 및 수정	244
7.6.4. Rule 동작 설정	245
(1) Policy 설정	245
(2) Policy 우선 순위 설정	246
(3) Action 설정	247
(4) CoS값 및 ToS값 설정	248
(5) Rule 적용 인터페이스 지정	249
(6) Policy 내용 저장 및 수정	250
7.6.5. Rule 설정 내용 확인	250
7.6.6. 스케줄링(Scheduling) 설정	252
(1) 스케줄링(Scheduling) 방식 설정	252
(2) Weight 설정	253
(3) Min-bandwidth 설정	254
(4) Max-bandwidth 제한	255
(5) 특정 포트의 트래픽 제한 설정	256
(6) CPU 패킷에 대한 사용자 정의	258
(7) QoS 내용 확인	258
(8) 포트별 Queue 트래픽 확인	258
7.6.7. Admin Rule 설정	258
7.6.8. Admin Rule 패킷 분류(Classify) 설정	259
(1) Admin Flow 설정	259
(2) Admin Flow 내용 저장 및 수정	261
(3) Class 설정	261
7.6.9. Admin Rule 동작 설정	262
(1) Policy 설정	262
(2) Policy 우선 순위 설정	263
(3) Admin Policy의 Action 설정	263
(4) Policy 내용 저장 및 수정	264
7.6.10. Admin Rule 설정 내용 확인	265
7.7 NetBIOS Filtering	266
7.8 DHCP 서버 패킷 필터링	268
7.9 Martian Filtering	269
7.10 MAC 필터링	271

7.10.1. MAC 필터 기본 정책 설정	271
7.10.2. MAC 필터 정책 추가	271
7.10.3. MAC 필터 정책 삭제	272
7.10.4. MAC 필터링 정책 List 불러오기	272
7.10.5. 고정 IP 사용자 차단하기	273
7.11 접속자 수 지정	273
7.12 MAC 테이블 관리	274
7.13 ARP(Address Resolution Protocol).....	276
7.13.1. ARP 테이블 설정	276
(1) ARP 테이블 등록	277
(2) ARP 테이블 확인	277
7.13.2. ARP Alias	278
(1) ARP-Alias 설정	278
(2) Gateway Aging-time 설정	279
(3) ARP-Alias 정보 확인	279
7.13.3. ARP Inspection	280
(1) ARP Inspection 활성화	281
(2) ARP ACL 설정	281
(3) ARP Inspection 필터링 설정	286
(4) 포트 상태 설정	286
(5) ARP Address-validation 검사 설정	287
(6) 불법 고정 IP 사용 가입자 리스트 확인	287
(7) 설정 내용 및 통계 확인	289
7.13.4. Proxy-ARP 설정	290
7.13.5. Gratuitous ARP 설정	291
7.14 ICMP 메시지 Control.....	292
7.14.1. Echo Reply 메시지 제한	293
7.14.2. ICMP 메시지 전송 시간 제한	293
(1) ARP Inspection 활성화	294
(2) 전송 제한 시간 설정	296
(3) 전송 제한 설정 확인	296
(4) 전송 제한 설정 초기화	296
7.15 IP TCP flag control.....	297
7.15.1. RST 설정	298
7.15.2. SYN attack 방지 기능 설정	299
7.15.3. SYN Guard 대역폭 설정	300
7.16 패킷 라우팅 테이블 사용량 확인	301

7.17	덤프 패킷 모니터링	302
7.17.1.	덤프 패킷(Dump Packet) 확인	302
(1)	프로토콜별 덤프 패킷 확인	302
(2)	호스트 덤프 패킷 확인	302
(3)	멀티캐스트 덤프 패킷 확인	303
(4)	사용자 지정 덤프 패킷 확인	304
7.17.2.	덤프 패킷 디버그	305
7.18	Port Security.....	307
7.18.1.	Port Security 활성화	307
7.18.2.	MAC 주소 개수 지정	308
7.18.3.	Port Security Aging Time 지정	308
7.18.4.	Port Security Aging Type 지정	309
7.18.5.	Port Security Aging Static 지정	309
7.18.6.	Violation Action 지정	310
7.18.7.	Secure MAC 주소 등록	310
7.18.8.	Port Security 기능 설정 확인	311

8.	시스템 주요 기능 설정.....	312
-----------	--------------------------	------------

8.1	VLAN(Virtual Local Area Network).....	312
8.1.1.	Default VLAN	315
8.1.2.	포트 기반 VLAN 설정	316
(1)	VLAN 만들기	316
(2)	PVID 지정	316
(3)	포트 할당 및 삭제	317
(4)	VLAN 기능 해제	317
8.1.3.	프로토콜 기반 VLAN 설정	318
8.1.4.	MAC 주소 기반 VLAN 설정	319
8.1.5.	Subnet 기반 VLAN 설정	319
8.1.6.	VLAN 우선 순위 지정	319
8.1.7.	QinQ 설정	320
(1)	QinQ 설정 방법	321
(2)	TPID 종류 설정	322
(3)	QinQ 해제	322
8.1.8.	Layer 2 전용 설정에서 Shared-VLAN 설정	322
8.1.9.	Protected 포트 설정	323
8.1.10.	VLAN 설명하기	324
8.1.11.	VLAN 관련 설정 내용 확인	324

8.2	Link aggregation	325
8.2.1.	포트 트렁크	327
(1)	트렁크 그룹 및 멤버 포트 설정	327
(2)	트렁크 그룹 패킷 분배 모드 지정	328
(3)	포트 트렁크 설정 확인	328
8.2.2.	LACP 설정	329
(1)	LACP 활성화	330
(2)	패킷 경로 규정 설정	330
(3)	멤버 포트 설정	331
(4)	멤버 포트의 동작 모드 설정	331
(5)	장비 우선 순위 설정	332
(6)	멤버 포트의 LACP 참가 여부 설정	333
(7)	BPDU 전송 주기 설정	334
(8)	멤버 포트의 Key 값 설정	334
(9)	포트 우선 순위 설정	336
(10)	LACP 설정 내용 확인	337
(11)	LACP 통계 확인	337
8.3	STP 설정	338
8.3.1.	STP 동작 원리	340
8.3.2.	RSTP의 동작 원리	343
(1)	포트 상태의 변화	344
(2)	BPDU 정책 변화	345
(3)	네트워크 convergence 시간 단축	346
(4)	802.1d와의 호환성	348
8.3.3.	PVSTP와 MSTP	349
(1)	동작	349
(2)	MSTP	351
8.3.4.	STP/RSTP/MSTP/PVSTP/PVRSTP 모드 설정	354
8.3.5.	STP/RSTP/MSTP 설정	354
(1)	STP/RSTP/MSTP 활성화	354
(2)	Root 설정	355
(3)	Path-cost 설정	355
(4)	Port-priority 설정	357
(5)	MST Region 설정	357
(6)	설정 내용 확인	359
8.3.6.	PVSTP/PVRSTP 설정	360
(1)	PVST/PVRSTP 활성화	360

(2) Root 설정	360
(3) Path-cost 설정	361
(4) Port-priority 설정	362
(5) PVST/PVRSTP 설정 내용 확인	362
8.3.7. BPDU 설정	363
(1) Hello time 설정	364
(2) Forward Delay 설정	364
(3) Max age 설정	365
(4) BPDU Hop 설정	366
(5) BPDU 설정 내용 확인	366
8.3.8. BPDU Filtering 설정	366
8.3.9. Point-to-Point MAC 설정	367
8.3.10. STP 모드 변경 감지	368
8.3.11. STP Guard 설정	368
(1) Edge Port 설정	368
(2) Root Guard 설정	368
8.3.12. BPDU Guard 설정	369
(1) BPDU Guard 활성화	369
(2) Edge Port 자동 활성화	370
(3) Edge Port 수동 활성화	370
8.4 Loop 감지 기능	371
8.4.1. Loop 감지 기능 활성화	371
8.4.2. Loop 감지 포트 설정	372
8.4.3. Loop 감지 패킷 전송 시간 설정	372
8.4.4. Loop 감지 패킷 전송 소스 MAC 주소 설정	373
8.4.5. Loop 감지 설정 확인	374
8.4.6. Self Loop 감지 기능	374
8.5 ERP 설정	375
8.5.1. ERP 동작 원리	376
8.5.2. LOTP (Loss of Test Packet)	379
8.5.3. Shared Link 환경	379
8.5.4. ERP 도메인 설정	380
(1) ERP ID 설정	380
(2) ERP 도메인 설명	381
(3) Node 설정	381
(4) Primary/Secondary 포트 설정	381
8.5.5. Protected Activation 설정	382

8.5.6. Manual Switch to Secondary 설정	382
8.5.7. Wait-to-Restore Time 설정	383
8.5.8. Learning Disable Time 설정	383
8.5.9. Test Packet Interval 설정	384
8.5.10. ERP Ring 우선순위 정하기	384
8.5.11. LOTP Hold Off Time 설정	385
8.5.12. ERP Port Protected.....	386
8.5.13. ERP 트랩 메시지	387
8.5.14. ERP 설정 확인.....	388
8.6 스택킹 설정	388
8.6.1. 장비 그룹 설정	389
8.6.2. Master 장비 지정	389
8.6.3. Slave 장비 설정	390
8.6.4. 스택킹 설정 해제	390
8.6.5. 스택킹 설정 내용 확인	391
8.6.6. Master에서 Slave로 접속.....	391
8.6.7. 설정 예제.....	391
8.7 Rate Limit와 Flood Guard	394
8.7.1. Rate Limit 설정	395
8.7.2. Flood Guard 설정	396
(1) MAC-Flood-Guard 설정 방법	396
(2) CPU-Flood-Guard 설정	397
(3) Port-Flood-Guard 설정	398
8.8 VRRP (Virtual Router Redundancy Protocol)	400
8.8.1. VRRP 기본 설정	401
(1) Associate IP 주소 설정하기	402
(2) Associated IP 주소 직접 액세스 설정.....	402
(3) Master Router와 Backup Router 지정하기	403
8.8.2. VRRP Track 설정	405
8.8.3. Authentication 패스워드 설정	406
8.8.4. Preempt 가능 설정	407
8.8.5. Advertisement time 설정	408
8.8.6. VRRP 통계 확인	409
8.8.7. VRRP 통계 삭제	410
8.9 대역폭 설정	410
8.10 DHCP(Dynamic Host Configuration Protocol)	412
8.10.1. DHCP 서버 설정	413

(1) IP Pool 만들기	413
(2) 서브넷 설정	414
(3) 서브넷 디폴트 게이트웨이 설정	414
(4) IP 주소 범위 설정	415
(5) IP 사용 가능 시간 설정	415
(6) DNS 등록	416
(7) IP 주소 수동 할당	417
(8) 도메인 이름 설정	417
(9) Option 설정	417
(10) Static Lease database 파일 확인	418
(11) 주소 할당 제한	418
(12) 할당 IP 주소의 사용 여부 확인	419
(13) BOOTP Request 차단	420
(14) IP 주소 할당 기준 설정	420
(15) IP 주소 1:N 할당 방지	421
(16) 고정 IP 사용자 차단	421
(17) Lease 데이터베이스 Backup	423
(18) Lease 데이터베이스 확인	423
(19) Lease 데이터베이스 초기화	424
(20) IP Pool 사이즈 설정	424
(21) IP Pool 설정 내용 확인	424
8.10.2. DHCP 릴레이 에이전트 설정	425
(1) DHCP Relay 에이전트 활성화	425
(2) DHCP server-ID 옵션 설정	426
(3) Vendor별 DHCP 서버 지정	427
(4) Smart Relay 설정	427
8.10.3. DHCP Option 설정	428
(1) DHCP Option 활성화	429
(2) DHCP Option 설정하기	429
(3) DHCP Option 삭제	430
(4) DHCP Option 확인	431
8.10.4. DHCP Option-82 설정	431
(1) DHCP Option-82 활성화	432
(2) Option-82 패킷 정책 설정	432
(3) 시스템 Remote-ID, Circuit-ID 설정	433
(4) DHCP Option82 Trust 패킷 설정	434
8.10.5. Class 설정	434

(1) Class 만들기	435
(2) Option 82 패킷 설정	435
(3) IP 주소 범위 설정	437
(4) Class 기능 활성화	437
8.10.6. DHCP 클라이언트	438
(1) DHCP 클라이언트 활성화	438
(2) Client-id 설정	438
(3) Class-id 설정	439
(4) 호스트 이름	439
(5) IP 주소 사용 시간 제한	440
(6) DHCP 서버로부터 정보 요청	440
(7) IP 주소 사용 중단	441
(8) IP 주소 재요청	441
(9) DHCP 클라이언트 설정 확인	441
8.10.7. DHCP Snooping 설정	442
(1) DHCP Snooping 활성화	442
(2) VLAN별 DHCP Snooping 설정	442
(3) Trust 포트 지정	443
(4) Trust 포트 DHCP 패킷 필터링	443
(5) DHCP 패킷 수 제한	443
(6) 바인딩 테이블에 등록되는 IP 주소 개수 제한	444
(7) 바인딩 테이블 Backup	445
(8) 바인딩 테이블 Static 등록	445
(9) MAC 주소를 통한 관리	445
(10) ARP Inspection Start Time 설정	446
(11) DHCP Snooping Option 82 설정	447
(12) DHCP Snooping Option 설정	447
(13) DHCP Snooping 설정 내용 확인	449
8.10.8. IP Source Guard	449
(1) IP Source Guard 활성화	449
(2) Static IP Source Guard	450
(3) IP Source Guard 설정 내용 확인	450
8.10.9. DHCP 디버깅	450
8.10.10. DHCP 패킷 통계 확인	451
8.11 Storm Control	452
8.12 Jumbo-frame 수용하기	453
8.13 Direct 브로드캐스트 차단	454

8.14	최대 전송 단위 (MTU) 설정	454
8.15	Access List 설정	455
8.15.1.	ACL 동작 방법	456
8.15.2.	Wildcard Bits	457
8.15.3.	Standard Access List 설정	458
8.15.4.	Extended Access List 설정	459
8.15.5.	Named Access List 설정	462
8.15.6.	Access List 설정 내용 확인	464

9.	멀티캐스트(Multicast) 설정	465
-----------	----------------------------------	------------

9.1	IGMP (Internet Group Management Protocol)	468
9.1.1.	IGMP 기본 설정	470
(1)	IGMP 버전 설정	471
(2)	QRV 설정	471
(3)	IGMP 엔트리 초기화	472
(4)	IGMP Debug	473
9.1.2.	IGMP 버전 2 설정	473
(1)	IGMP Static Join 설정	475
(2)	접속 가능한 IGMP 그룹 리스트 설정	477
(3)	IGMP Querier 설정	478
(4)	Immediate Leave 설정	483
9.1.3.	IGMP 버전 3 설정	484
9.1.4.	IGMP 설정 확인	487
9.2	멀티캐스트 부가 기능 설정	488
9.2.1.	멀티캐스트 포워딩 데이터베이스 설정	488
(1)	Unknown 멀티캐스트 트래픽 처리	488
(2)	포워딩 엔트리 설정	489
(3)	멀티캐스트 포워딩 데이터베이스 확인 및 초기화	490
9.2.2.	IGMP Snooping 기본 설정	491
(1)	IGMP Snooping 활성화	492
(2)	IGMP Snooping 버전 설정	492
(3)	Robustness Variable 설정	493
9.2.3.	IGMP 버전 2 Snooping 설정	495
(1)	IGMP Snooping Querier 설정	495
(2)	IGMP Snooping Last Member Query의 전송 주기 설정	497
(3)	IGMP Snooping Immediate-Leave 설정	498
(4)	IGMP Snooping Report Suppression 설정	499

(5) IGMP Snooping S-Query Report Agency 설정	500
(6) 호스트 트래킹 기능 설정	501
(7) 멀티캐스트 라우터 포트 설정	503
(8) 멀티캐스트 TCN Flooding 설정	506
9.2.4. IGMP 버전 3 Snooping 설정	510
9.2.5. IGMP Snooping 정보 확인	511
9.2.6. MVR (Multicast VLAN Registration)	512
(1) MVR 활성화	513
(2) MVR 그룹 설정	514
(3) Source/Receiver 포트 설정	514
(4) MVR Helper 주소 설정	515
(5) MVR 설정 확인	516
9.2.7. IGMP 필터링 기능 설정	516
(1) IGMP 필터링 설정	516
(2) 패킷 종류에 따른 IGMP 필터링 설정	519
(3) IGMP 그룹의 최대값 설정	520
(4) IGMP 필터링 확인	520
9.2.8. IGMP Proxy 설정	521
(1) 다운스트림 인터페이스 설정	522
(2) 업스트림 인터페이스 설정	522
(3) 업스트림 인터페이스 모드 설정	522
(4) IGMP Flap Discredit 설정	523
(5) IGMP 패킷의 소스 IP 확인 해제	525
(6) IGMP Report/Leave 메시지의 소스 IP 설정	526
(7) 실제 소스 IP로 Query 전송	526
(8) IGMP Proxy 설정 확인	527
9.2.9. IGMP State 제한 설정	527
9.2.10. 멀티캐스트 Source Trust 포트 설정	528
9.3 멀티캐스트 라우팅 설정	529
9.3.1. 멀티캐스트 라우팅	530
(1) 멀티캐스트 라우팅 활성화	530
(2) 멀티캐스트 TTL 임계값 설정	531
(3) Multi-Path 설정	532
(4) MRIB 엔트리 제한	534
(5) MRIB 엔트리 삭제	535
(6) MRIB 엔트리 정보 확인	536
(7) MRIB Statistics 삭제	536

(8) MRIB Statistics 정보 확인	537
(9) MRIB Debug	537
(10) MFIB 정보 확인	538
9.3.2. PIM 개요.....	539
(1) PIM-SM 동작 원리	539
(2) Rendezvous Point Tree(RPT)	540
(3) Shortest Path Tree(SPT).....	541
(4) PIM 메시지	542
9.3.3. PIM-SM 기본 설정	544
(1) PIM 모드 설정	544
(2) DR Priority 설정	545
(3) Neighbor Filtering 설정	546
(4) Hello 메시지 설정	547
(5) Join/Prune 전송 간격 설정	548
(6) VIF Flap Discredit 설정	549
(7) PIM 정보 확인	551
9.3.4. RP 설정	551
(1) Static RP 설정	551
(2) KAT (Keep Alive Time) 설정	553
(3) Candidate RP 설정	554
(4) RP Priority 사용 중지	555
(5) RP 설정 확인	555
9.3.5. BSR 설정.....	556
(1) Candidate BSR 설정	556
(2) RP-set 정보 삭제	557
(3) BSR 설정 확인.....	557
9.3.6. Source Registration	558
(1) Registration Rate Limit 설정	559
(2) Registration Suppression Time 설정	559
(3) Register 메시지 Filtering.....	560
(4) RP Reachability Validation 설정	561
(5) Register 메시지의 Source Address 설정.....	561
9.3.7. SPT 전환	562
9.3.8. Cisco 라우터와의 호환	563
(1) Register 메시지 Checksum 설정	563
(2) Candidate RP 메시지 설정	564
(3) GenID 옵션 설정	565

9.3.9.	PIM Debug	566
9.3.10.	SSM (Source Specific Multicast) 설정	567
(1)	PIM SSM 설정	568
(2)	Static SSM 맵핑 설정	569

10.	G-PON 설정	571
------------	-----------------------	------------

10.1	G-PON 개요	571
10.2	G-PON 설정	573
10.2.1.	OLT 활성화	573
10.2.2.	ONU(ONT) 등록	574
(1)	ONU(ONT) 자동 등록	574
(2)	ONU(ONT) 수동 등록	574
(3)	ONU(ONT) 등록 상태 변경	575
10.2.3.	ONU(ONT) 펌웨어 관리	575
(1)	펌웨어 업그레이드	575
(2)	펌웨어 삭제	577
(3)	펌웨어 정보 확인	577
10.2.4.	T-CONT 설정	578
10.2.5.	최대 거리 설정	579
10.2.6.	ONU(ONT) 오류 자동 감지 기능	580
10.2.7.	재부팅	581
10.2.8.	Security 설정	581
10.2.9.	FEC 설정	582
10.2.10.	Admin 트래픽 제한 설정	582
10.3	Profile 설정	583
10.3.1.	Profile의 생성 및 삭제	584
10.3.2.	Profile의 설정	585
10.3.3.	Profile 적용	587
10.3.4.	Profile 정보 확인	587
10.4	G-PON 정보 확인	587
10.4.1.	OLT MAC 정보 확인	587
10.4.2.	G-PON Slot 상태 확인	588
10.4.3.	OLT 상태 확인	588
10.4.4.	ONU(ONT) 정보 확인	588
10.4.5.	통계 정보 확인	589
10.5	G-PON 디버깅	589

11. IP 라우팅 프로토콜 설정	590
11.1 BGP 개요	591
11.1.1. 기본 설정	592
(1) BGP 라우팅 프로토콜 활성화	592
(2) Neighbor 등록	594
11.1.2. IGP와 BGP의 Synchronization	599
11.1.3. 네트워크 Aggregate	600
11.1.4. Route-Reflector	601
11.1.5. Confederation	607
11.1.6. 최적 경로 선택	609
(1) Next-Hop Address Tracking	615
(2) Next-Hop-Self	617
(3) Local Preference 설정	618
(4) As-path 비교 생략	619
(5) Confederation AS-path 비교	619
(6) 외부 AS 경로의 MED 비교 설정	620
(7) AS 그룹별 MED 비교 설정	620
(8) Missing-as-Worst	621
(9) Confederation MED 비교	621
(10) Router-ID 비교 설정	622
11.1.7. Address-Family 설정 모드	623
11.1.8. Route Dampening	623
11.1.9. BGP Session Reset	626
11.1.10. Graceful Restart	629
11.1.11. BGP Neighbor 설정	630
(1) 기본 경로 설정	630
(2) Peer Group 설정	631
(3) 강제 종료 기능	632
11.1.12. BGP 설정 내용 확인	632
11.2 OSPF(Open Shortest Path First)	634
11.2.1. OSPF 활성화	635
11.2.2. ABR 유형 설정	637
11.2.3. RFC 1583 호환성 지원	637
11.2.4. OSPF 인터페이스 설정	638
(1) 인증 관련 설정	638
(2) 인증 키 설정	639
(3) 인터페이스 Cost 설정	640

(4) 경로 정보 Database 송신 차단.....	640
(5) 라우팅 프로토콜 동작 주기 설정	641
(6) MTU 관련 설정	643
(7) 우선 순위 결정	644
(8) OSPF 네트워크 유형 설정	645
11.2.5. Non-broadcast 네트워크 설정	646
11.2.6. Area 설정	647
(1) Area 인증 설정	647
(2) Area의 기본 Cost값 설정	648
(3) Area간 경로 정보 전달 제한 설정	649
(4) NSSA 설정	650
(5) Area 경로 정보 요약 설정.....	652
(6) Shortcut Area 설정	653
(7) Stub Area 설정	653
(8) Area 최대 개수 설정	654
(9) 가상 경로 설정	654
11.2.7. 기본 경로값 변경	657
11.2.8. Graceful Restart 지원	657
11.2.9. Opaque-LSA 지원	659
11.2.10. 기본 경로 설정	660
11.2.11. 경로 계산 주기 설정	662
11.2.12. ECMP(Equal Cost Multi-Path) 설정	662
11.2.13. 외부 경로 전달	663
11.2.14. OSPF 거리값 변경	665
11.2.15. 호스트 경로 설정	666
11.2.16. 수동 인터페이스 설정	666
11.2.17. 갱신된 정보 전달 제어	667
11.2.18. 요약 경로 정보 전달	667
11.2.19. OSPF 모니터링과 관리	668
(1) OSPF 프로토콜 정보 출력	668
(2) Debugging 정보 출력	670
(3) 데이터베이스 처리 개수 제한	671
(4) 최대 처리가능 LSA값 설정	671
11.3 RIP(Routing Information Protocol)	673
11.3.1. RIP 활성화	674
11.3.2. RIP Neighbor 라우터 지정	675
11.3.3. RIP 버전 지정	675

11.3.4. RIP에서만 유효한 Static 경로 생성	676
11.3.5. 라우팅 정보 전달	677
11.3.6. 특정 라우팅 정보 전달	677
11.3.7. 전달되는 경로의 경로값 설정.....	678
11.3.8. 9.3.8 거리값(Administrative Distance) 설정	679
11.3.9. 기본 경로(Default Route) 생성.....	679
11.3.10. 라우팅 정보 필터링.....	680
(1) 특정 경로 정보에 대한 Access-list 및 Prefix-list 차단.....	680
(2) 인터페이스로 나가는 라우팅 정보 차단.....	680
(3) 경로값 증가 기능 설정	681
11.3.11. 최대 RIP 경로 개수 설정	681
11.3.12. 라우팅 프로토콜 동작 주기 설정	682
11.3.13. 경로 차단(Split-horizon) 활성화/비활성화	683
11.3.14. 인증 키 관리	683
11.3.15. RIP 재부팅	684
11.3.16. RIP 수신 버퍼 크기 조절	685
11.3.17. RIP 설정 확인	685

부록 A. 시스템 이미지 설치하기	686
---------------------------------	------------

A.1 Global 설정 모드에서 시스템 이미지 설치	686
A.1.1 FTP/TFTP 서버로 시스템 이미지 내려 받기	687
A.1.2 시스템 이미지 설치 준비	689
A.2 Boot 모드에서 시스템 이미지 설치	690
A.2.1 시스템 이미지 설치 준비	691
A.2.2 시스템 이미지 설치	693
A.3 원격으로 시스템 이미지 설치	693

◆ 그 림 ◆

【 그림 2-1 】 V5812G를 이용한 네트워크 구성	33
【 그림 4-1 】 802.1x 사용자 인증 과정	88
【 그림 4-2 】 Multi Authentication Server	89
【 그림 4-3 】 시스템 사용자 인증 과정	98
【 그림 5-1 】 포트 미러링의 예	115
【 그림 6-1 】 Domain name server	128
【 그림 6-2 】 네트워크 연결 확인을 위한 Ping 테스트	154
【 그림 6-3 】 IP ICMP Source Routing	154
【 그림 7-1 】 SNMP 구성의 예	167
【 그림 7-2 】 EFM OAM 시나리오	193
【 그림 7-3 】 QoS의 동작 구조	229
【 그림 7-4 】 Rule의 구조	230
【 그림 7-5 】 Token Bucket 방식	237
【 그림 7-6 】 Single Rate Three Color Marker의 Color Marking	238
【 그림 7-7 】 Two Rate Three Color Marker의 Color Marking	240
【 그림 7-8 】 Strict Priority Queuing에서의 패킷 처리	252
【 그림 7-9 】 WRR에서의 패킷 처리	253
【 그림 7-10 】 DRR에서의 Min-bandwidth와 Max-bandwidth	255
【 그림 7-11 】 NetBIOS Filtering의 필요성	266
【 그림 7-12 】 DHCP 필터링	268
【 그림 7-13 】 ARP-Alias의 원리	278
【 그림 7-14 】 ARP Inspection의 동작 예	280
【 그림 7-15 】 Proxy-ARP	290
【 그림 7-16 】 ICMP 메시지	292
【 그림 7-17 】 3 Way Hand Shaking	299
【 그림 8-1 】 Layer 2 환경 포트 기준 VLAN 구성도	313
【 그림 8-2 】 VLAN 기준 패킷 경로 결정 절차	314
【 그림 8-3 】 QinQ 설정 네트워크 구성의 예	320
【 그림 8-4 】 Link aggregation	325
【 그림 8-5 】 Link aggregation 구성 예 ①	326
【 그림 8-6 】 LACP의 구성 예 ①	335
【 그림 8-7 】 LACP의 구성 예 ②	336
【 그림 8-8 】 루프 현상의 예	338

【 그림 8-9 】 STP의 원리	339
【 그림 8-10 】 Root 장비	340
【 그림 8-11 】 Designated 장비 결정	341
【 그림 8-12 】 Designated 장비와 Designated 포트	342
【 그림 8-13 】 Port priority를 사용한 결정	343
【 그림 8-14 】 Alternate 포트와 Backup 포트	344
【 그림 8-15 】 낮은 BPDU를 받아들이는 경우	345
【 그림 8-16 】 802.1d의 네트워크 convergence	346
【 그림 8-17 】 802.1w의 네트워크 convergence ①	347
【 그림 8-18 】 802.1w의 네트워크 convergence ②	347
【 그림 8-19 】 802.1w의 네트워크 convergence ③	348
【 그림 8-20 】 STP와의 호환 ①	349
【 그림 8-21 】 STP와의 호환 ②	349
【 그림 8-22 】 STP	350
【 그림 8-23 】 PVSTP	350
【 그림 8-24 】 MSTP	351
【 그림 8-25 】 MSTP의 CST와 IST①	352
【 그림 8-26 】 MSTP의 CST와 IST②	353
【 그림 8-27 】 Link failure 발생	377
【 그림 8-28 】 Ring Protection	378
【 그림 8-29 】 Link Failure 복구	378
【 그림 8-30 】 Ring Recovery	379
【 그림 8-31 】 Shared Link 환경	380
【 그림 8-32 】 스택킹 설정의 예	388
【 그림 8-33 】 Rate Limit와 Flood Guard	394
【 그림 8-34 】 VRRP 구성도	400
【 그림 8-35 】 DHCP 서비스 구성의 예	412
【 그림 8-36 】 DHCP 서버와 Relay 에이전트 구성도의 예	425
【 그림 8-37 】 DHCP Option-82를 사용하는 경우의 패킷 흐름	431
【 그림 9-1 】 PIM-SM을 설정했을 경우	466
【 그림 9-2 】 PIM-SM과 IGMP Snooping을 같이 설정했을 경우	467
【 그림 9-3 】 IGMP 버전 1 메시지 형식	468
【 그림 9-4 】 IGMP 버전 2 메시지 형식	469
【 그림 9-5 】 IGMP 버전 3 Query 메시지 형식	485
【 그림 9-6 】 IGMP 버전 3 Report 메시지 형식	486
【 그림 9-7 】 IGMP Snooping을 설정했을 경우	491
【 그림 9-8 】 MVR 동작	512

【 그림 9-9 】 Equal Cost Multi-path.....	532
【 그림 9-10 】 PIM-SM의 RPT	541
【 그림 9-11 】 PIM-SM의 SPT	542
【 그림 9-12 】 멀티캐스트 Source Registration.....	558
【 그림 10-1 】 G-PON 시스템 구성도	572
【 그림 10-2 】 Profile 기능.....	583
【 그림 11-1 】 BGP의 구성원.....	591
【 그림 11-2 】 Full Mesh IBGP내의 라우팅 정보 전송.....	602
【 그림 11-3 】 Route-Reflector를 이용한 BGP 구성예①.....	602
【 그림 11-4 】 Route-Reflector를 이용한 BGP 구성예②.....	603
【 그림 11-5 】 Confederation을 이용한 BGP 구성	607
【 그림 11-6 】 Local Preference	610
【 그림 11-7 】 AS-path	611
【 그림 11-8 】 MED	612
【 그림 11-9 】 Next-Hop	613
【 그림 11-10 】 Weight	614
【 그림 11-11 】 Next-Hop	617
【 그림 11-12 】 Next-Hop-Self.....	618

◆ 표 ◆

【 표 1-1 】 콘솔 터미널 명령어 표기법	31
【 표 1-2 】 안내서 명령어 표기법	32
【 표 3-1 】 Privilege Exec View 모드 주요 명령어	39
【 표 3-2 】 Privilege Exec Enable 모드 주요 명령어	40
【 표 3-3 】 Global 설정 모드 주요 명령어	41
【 표 3-4 】 Flow 설정 모드 주요 명령어	42
【 표 3-5 】 Policer 설정 모드 주요 명령어	42
【 표 3-6 】 Policy 설정 모드 주요 명령어	43
【 표 3-7 】 DHCP 설정 모드 주요 명령어	43
【 표 3-8 】 DHCP Option-82 설정 모드 주요 명령어	44
【 표 3-9 】 RMON 설정 모드 공통 명령어	45
【 표 3-10 】 VRRP 설정 모드 주요 명령어	45
【 표 3-11 】 Bridge 설정 모드 주요 명령어	46
【 표 3-12 】 Interface 설정 모드 주요 명령어	47
【 표 3-13 】 Router 설정 모드 공통 주요 명령어	47
【 표 3-14 】 Route-Map 설정 모드 주요 명령어	48
【 표 7-1 】 V5812G의 기본 SNMP 트랩	180
【 표 7-2 】 ICMP 메시지의 15가지 Type	292
【 표 7-3 】 ICMP 메시지의 값	294
【 표 7-4 】 Default mask 계산 결과표	295
【 표 7-5 】 TCP 덤프 옵션	304
【 표 8-1 】 STP path-cost	356
【 표 8-2 】 RSTP의 path-cost	356
【 표 8-3 】 Wildcard mask의 설정 예	457
【 표 10-1 】 G-PON 표준 문서의 종류	571
【 표 10-2 】 T-CONT 타입	573

1. 개요

이 설명서는 (주)다산네트웍스의 V5812G를 구입하신 모든 사용자에게 제품에 대한 전반적인 소개와 더불어 제품 설정 방법에 대해 알려드립니다. 사용자의 이해를 돋기 위해 제품 설정에 대한 구체적인 설명과 예제가 포함되어 있습니다.

이 설명서는 V5812G를 설정하고 관리할 네트워크 관리자를 위한 것입니다. 따라서 이 안내서를 이용할 네트워크 관리자는 네트워크 장비에 대한 전문적인 지식과 LAN(Local Area Network) 구축 및 운영에 대한 경험이 요구됩니다.

1.1 내용 구성

- **제품 소개** : V5812G가 가지고 있는 기능을 소개합니다.
- **CLI 사용하기** : (주)다산네트워크에서 개발한 DSH 명령어의 체계와 명령어의 기본 사용법에 대해 간단히 소개합니다.
- **시스템 접속 및 IP 주소 설정** : 시스템 접속과 관련된 정보와 네트워크 통신에 필요한 IP 주소를 설정하는 방법을 설명합니다.
- **포트 기본 설정** : V5812G의 이더넷 포트가 가지는 기본적인 파라미터를 설정하는 방법과 포트 미러링 기능에 대한 설정 방법을 설명합니다.
- **시스템 환경** : 시스템의 기본적인 환경 설정 및 설정 관리, 시스템 내용을 확인하는 방법에 대해 설명합니다.
- **네트워크 관리 기능 설정** : SNMP, Syslog, 패킷필터링 등 네트워크 관리 기능을 설정하는 방법에 대해 설명합니다.
- **시스템 주요 기능 설정** : V5812G가 가지고 있는 VLAN, STP(Spanning Tree Protocol) 등의 주요 기능을 설정하는 방법에 대해 설명합니다.
- **멀티캐스트** : 멀티캐스팅을 설정하는 방법에 대해 설명합니다.
- **IP 라우팅 프로토콜 설정** : BGP, OSPF, RIP의 라우팅 프로토콜을 설정하는 방법을 설명합니다.
- **GPON 설정** : GPON을 설정하는 방법을 설명합니다.
- **부록 A. 시스템 이미지 내려 받기** : 사용자의 장비에 새로운 시스템 이미지를 설치하는 방법에 대해 설명합니다.

1.2 사용 기호



경고

이 표시는 사용자에게 상해를 가하거나 제품을 손상시킬 수 있는 위험한 상황을 의미합니다. 손해를 방지하기 위해 이 사항을 준수하십시오. 또한 이 내용을 바탕으로 별도의 지침서를 만들어 수시로 확인할 수 있는 곳에 보관하여 제품 설치 전후나 제품 취급 전에 참고하십시오.



주의

이 표시는 제품을 설치하고 관리하는 동안에 사용자가 주의해야 하는 사항을 의미합니다.



참고

이 표시는 제품 설정하는 명령을 사용할 때 참고해야 할 사항을 의미합니다.

1.3 표기법

◆ 콘솔 터미널의 명령어 표기

V5812G의 콘솔 터미널에서 보여지는 명령어 표기는 【 표 1-1 】과 같습니다. 각 표기의 의미를 정확히 인지하여 바르게 명령어를 사용하십시오.

【 표 1-1 】 콘솔 터미널 명령어 표기법

표기	의미
a	정해진대로 입력해야 하는 명령어는 알파벳 소문자로 표기됩니다.
A	사용자가 입력해야 하는 변수는 알파벳 대문자로 표기됩니다.
[]	사용자의 판단에 따라 선택 가능한 명령어나 변수는 대괄호 [] 안에 표기됩니다.
< >	입력할 수 있는 숫자 범위는 꺥쇠 괄호 < > 안에 표기됩니다.
()	여러가지 변수들 가운데 반드시 선택해서 입력해야 하는 것은 소괄호 () 안에 표기됩니다.
	선택할 수 있는 변수들은 수직선 으로 나누어 표기됩니다.

◆ 안내서의 명령어 표기

안내서에 설명을 위해 명령어를 표기하는 방법은 【 표 1-2 】와 같습니다. 각 표기의 의미를 정확히 인지하여 바르게 명령어를 사용하십시오.

【 표 1-2 】 안내서 명령어 표기법

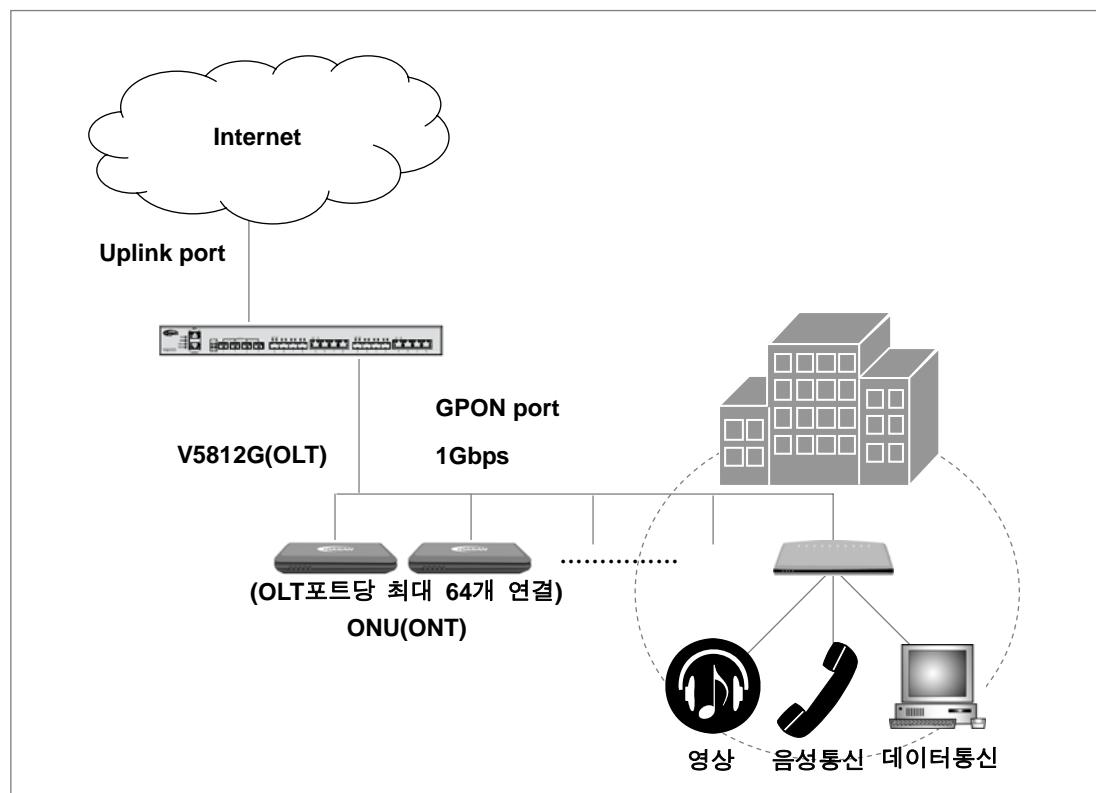
표 기	의 미
a , A	정해진대로 입력해야 하는 명령어는 굵은 글씨체의 알파벳 소문자로 표기됩니다.
a	사용자가 입력해야 하는 변수는 알파벳 소문자 이탤릭체로 표기됩니다.
[]	사용자의 판단에 따라 선택 가능한 명령어나 변수는 대괄호 [] 안에 표기됩니다.
< >	입력할 수 있는 숫자 범위는 꺽쇠 괄호 < > 안에 표기됩니다.
{ }	여러가지 변수들 가운데 반드시 선택해서 입력해야 하는 것은 중괄호 { } 안에 표기됩니다.
 	선택할 수 있는 변수들은 수직선 으로 나누어 표기됩니다.

2. 제품 소개

인터넷 서비스의 종류가 점점 다양해지면서 네트워크를 구성하는데 인터페이스의 종류도 점점 다양해지고 있습니다. 이러한 변화에 대응하여 개발된 V5812G는 4개의 G-PON 포트를 가입자 포트로 제공하고, 업링크 포트는 콤보 파입으로 100/1000BASE-X와 10/100/1000BASE-TX 중에서 사용할 수 있도록 하였습니다. 이더넷과 G-PON을 동시에 제공하는 것이 V5812G가 가지는 특징 중 하나라고 할 수 있겠습니다. 1개의 G-PON 포트에는 ONT가 최대 64대 연결 가능합니다.

V5812G를 이용하면 인구밀집도가 낮은 지역이나 서비스 대상이 비교적 적은 지역에서도 FTTH 서비스를 제공할 수 있습니다. 또한, 모듈형 전원을 지원함으로 설치 장소의 환경에 따라 AC와 DC 전원을 선택하여 사용할 수 있으며, 전원 이중화 기능을 지원하여 전원 관련 장애시에도 가입자 서비스를 지속적으로 제공할 수 있습니다.

다음은 그림은 V5812G를 이용한 네트워크 구성의 예를 나타낸 것입니다.



【 그림 2-1 】 V5812G를 이용한 네트워크 구성

2.1 주요 특징

V5812G가 제공하는 주요 기능은 다음과 같습니다.

- **VLAN(Virtual Local Area Network)**

VLAN이란 네트워크 관리자가 하나의 네트워크를 논리적으로 분리하여 만든 가상 LAN을 말합니다. VLAN은 물리적으로는 같은 네트워크 상에 있지만 사용자의 설정에 따라 같은 네트워크로 구성된 영역에서만 패킷을 주고 받을 수 있기 때문에 대역폭을 경제적으로 활용할 수 있을 뿐만 아니라 보안 효과가 뛰어납니다. V5812G는 하나의 시스템 당 최대 4K개의 VLAN을 구성할 수 있습니다.

- **QoS (Quality of Service)**

일반적인 네트워크 환경에서는 트래픽이 폭주할 경우 사용자의 데이터는 자동적으로 유실(drop)됩니다. 그러나 QoS를 지원하는 V5812G는 IEEE 802.1p CoS 표준안에 기반하여 트래픽을 여러 개의 등급으로 나누고, 각 등급의 처리 순서를 다시 정립합니다(reprioritize). QoS는 중요한 데이터의 우선 순위를 정해 놓음으로써 데이터의 유실을 막고, 패킷마다 차등화 된 대역폭을 제공하여 전송 지연을 방지합니다.

- **멀티캐스트 통신**

V5812G는 IGMP Snooping 기능과 IGMP Querier 기능을 제공하기 때문에 멀티캐스트 통신이 가능한 장비입니다. 멀티캐스트 통신은 필요로 하는 호스트들에게만 패킷을 전송하기 때문에 불필요한 패킷으로 과부하 현상이 일어나는 것을 막을 수 있습니다.

- **SNMP (Simple Network Management Protocol)/RMON (Remote Monitoring)**

SNMP 기능이 탑재된 장비는 원격에서 장비 상태를 확인하고 관리할 수 있습니다. V5812G는 SNMP 버전 1과 2과 4가지 그룹의 RMON을 지원, 관리자가 원하는 때에 원하는 통계 자료를 볼 수 있습니다.

- **IP 라우팅**

V5812G는 Layer 3 기능을 지원하기 때문에 라우터가 가지고 있는 기능인 IP 라우팅을 실현, 라우터를 별도로 설치할 필요가 없기 때문에 장비 추가에 따른 비용을 줄일 수 있습니다.

- **ARP-Alias**

V5812G는 장비에 등록되어 있지 않은 IP 주소에 대해 ARP 응답을 해줄 수 있습니다. 이러한 기능은 서로 통신이 불가능한 노드들 간의 통신을 해소해줄 수 있습니다.

- **DHCP Server 및 Relay 기능**

V5812G는 클라이언트에게 자동으로 IP 주소를 부여하는 DHCP 기능을 지원하여 한정된 네트워크 자원을 보다 효율적으로 이용하도록 합니다. 특히 DHCP 서버는 중앙에서 일괄적으로 IP 주소를 관리하여 네트워크 관리 비용을 절감시켜 줍니다.

- **패킷 필터링**

IP 패킷 필터링은 특정 장비나 사용자만이 네트워크에 접속할 수 있도록 네트워크 사용을 제한할 수 있는 기능입니다. V5812G는 이 기능을 이용하여 사용자는 불필요한 정보를 차단하고 특정 데이터가 유출되는 것을 방지하는 것은 물론 신원이 확인되지 않은 사용자를 차단함으로써 네트워크 보안을 강화할 수 있습니다. 한편, 다른 Source IP 주소를 가지고 외부로 나가는 패킷을 차단하는 Martian-filter 기능과 아파트나 특정한 지역에 LAN 서비스로 인터넷 통신이 제공되는 경우, 사용자들의 정보를 보장하는 NetBIOS 필터링도 제공합니다.

- **스택킹 (Stacking)**

장비 그룹에서 master로 지정된 장비가 하나의 IP 주소를 가지고 나머지 장비(slave 장비)를 설정 및 관리, 모니터링 할 수 있는 기능입니다. 하나의 IP 주소로 여러 대의 장비를 관리할 수 있기 때문에 IP 자원을 절약할 수 있습니다.

- **Link aggregation**

V5812G는 여러 개의 물리적인 인터페이스를 하나의 논리적인 포트로(aggregate port) 통합하는 포트 트렁크 기능을 지원합니다. 포트 트렁크는 동일한 속도, 동일한 duplex 모드, 동일한 VLAN ID를 기준으로 인터페이스를 통합합니다. V5812G는 트래픽을 줄이고 장애 복구 기능을 향상 시키기 위해 IEEE 802.3ad 표준안에 따라 최대 8개의 포트를 포괄하는 통합 포트를 6개까지 설정할 수 있습니다.

- **LACP(Link Aggregation Control Protocol)**

V5812G는 IEEE 802.3ad 표준을 기반하는 LACP를 지원하는데, 이는 LACP를 지원하는 장비간에 더 많은 전체 대역을 할당할 수 있도록 장비간 다중 연결 결합을 허용합니다.

- **대역폭 설정(Rate-limit)**

V5812G는 모든 포트에 대해 차등화된 대역폭을 제공합니다. 사용자의 요구에 따라 차등화된 대역폭을 제공함으로써 ISP 사업자는 차등화된 요금을 책정할 수 있을 뿐만 아니라 보다 효율적이고 경제적인 회선 관리가 가능합니다.

- **Flood Guard 설정**

Rate Limit는 포트 대역폭을 설정하여 패킷의 양을 조절하는 것과는 달리 1초 동안 수용할 수 있는 패킷 개수를 제한하여 패킷을 조절하는 Flood Guard 기능을 제공합니다.

- **STP(Spanning Tree Protocol)**

STP란 네트워크 상에서 루프가 계속해서 발생하는 것을 방지하기 위한 네트워크 관리 프로토콜입니다. 루프를 방지하기 때문에 트래픽 전송 속도를 유지하도록 도와줍니다. V5812G는 이러한 STP 기능을 가지고 있습니다.

- **PVST(Per VLAN Spanning Tree)**

V5812G는 VLAN마다 STP가 독립적으로 동작하는 PVST(Per VLAN Spanning Tree)를 지원합니다. PVST(Per VLAN Spanning Tree)는 VLAN 마다 STP가 하나씩 돌기 때문에 하나의 VLAN에서 루프가 발생하여 전체 네트워크가 다운되는 현상을 막을 수 있습니다.

- **RSTP(Rapid Spanning Tree Protocol) (802.1w)**

V5812G는 IEEE 802.1W 표준안에 따른 RSTP(Rapid Spanning Tree Protocol)를 지원하여 메트로 이더넷의 RING 환경이나 기존 P-to-P 환경에서 안정적이고 융통성있는 망구성이 가능합니다. RSTP는 소규모 장비 네트워크에서 STP Reconvergency 시간을 혁신적으로 감소시키기 위한 목적으로 개발된 것으로, Redundant link를 갖는 Layer 2 장비에서 Fail over 시간을 획기적으로 단축시킵니다.

- 시스템 관리

CLI 기반 DSH

사용자는 명령문 형식으로 구성된 DSH를 이용하여 하나의 장비나 장비 그룹 전체를 설정하고 모니터링할 수 있습니다. 콘솔 터미널 프로그램이 설치된 PC와 장비 콘솔을 연결하거나 텔넷 서비스를 이용하여 DSH를 이용할 수 있습니다.

- 802.1x 기반 사용자 인증

V5812G는 IEEE 802.1x를 기반으로 한 사용자 인증 정책을 포트별로 설정할 수 있습니다. 802.1x를 설정한 사용자 인증 포트는 RADIUS 서버를 통해 접속 권한 여부를 판단, 권한을 가지고 있는 접속자만 사용이 가능하기 때문에 네트워크 관리의 보안과 이동성을 높일 수 있습니다.

- RADIUS 및 TACACS+

V5812G는 사용자 인증 프로토콜로 RADIUS(Remote Authentication Dial-In User Service)와 Tacacs+(Terminal Access Controller Access Control System+)를 지원합니다. 장비에 등록되어 있는 사용자 ID와 Password 이외에도 RADIUS 서버와 TACACS+ 서버를 통하여 인증을 받아야 하기 때문에 시스템 관리 및 네트워크 관리의 보안성을 높였습니다.

- SSH 서버

V5812G는 SSH(Secure Shell) 서버를 활성화 함으로써 telnet, ftp 서비스에 보안성을 높일 수 있습니다.

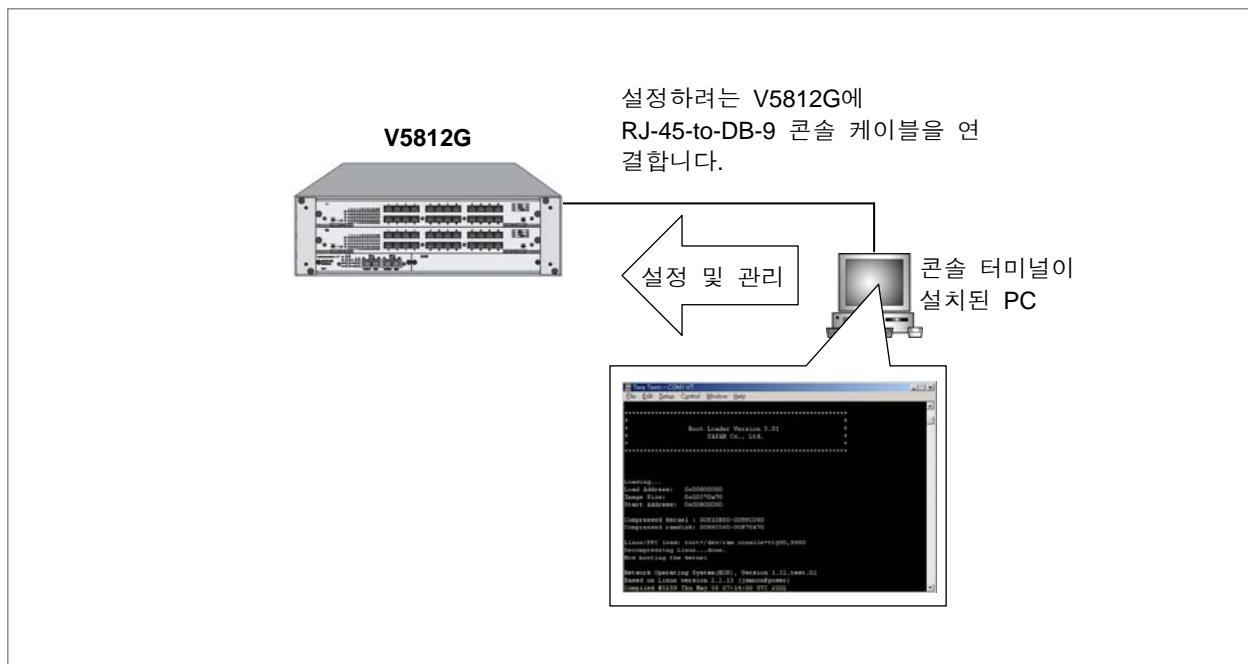
- 브로드캐스트 Storm Control

브로드캐스트 Storm이란, 다량의 브로드캐스트 패킷이 네트워크상에 전송되면서 전송 용량의 대부분을 점유함에 따라 네트워크 타임 아웃이 발생하는 현상을 말합니다. V5812G는 사용자가 설정한 시간동안 한계 값을 넘는 브로드캐스트 패킷, 멀티캐스트 패킷, 그리고 DLF 패킷을 폐기하는 브로드캐스트 Storm Control을 지원합니다.

3. CLI 사용하기

3.1 명령어 체계

V5812G는 사용자의 PC에 터미널 프로그램을 설치하여 콘솔 터미널을 통해 시스템을 설정 및 관리할 수 있습니다. 이 때 사용자는 CLI(Command Line Interface) 기반의 DSH를 사용하게 되며 이 DSH은 (주)다산네트웍스에서 개발한 명령어 체계입니다.



다음은 V5812G의 설정에서 사용하는 DSH 명령어를 구성하는 모드입니다.

- Privilege Exec View 모드
- Privilege Exec Enable 모드
- Global 설정 모드
- Rule 설정 모드
- DHCP 설정 모드
- DHCP Option-82 설정 모드
- RMON 설정 모드

- VRRP 설정 모드
- Bridge 설정 모드
- Interface 설정 모드
- Router 설정 모드
- Route-Map 설정 모드
- G-PON 설정 모드

3.1.1. Privilege Exec View 모드

사용자가 장비에 성공적으로 로그인하면 DSH 명령어의 Privilege Exec View 모드로 시작합니다.

Privilege Exec View 모드는 장비에 접속한 모든 사용자들에게 제공되는 읽기 전용 권한 모드입니다.

Privilege Exec View 모드에서는 장비의 설정 내용을 확인하는 기능의 명령어가 대부분입니다.

【 표 3-1 】은 V5812G NOS 3.03 Privilege Exec View 모드에서 사용하는 주요 명령어입니다.

【 표 3-1 】 Privilege Exec View 모드 주요 명령어

명령어	기 능
enable	Privilege Exec Enable 모드로 들어갑니다.
exit	시스템을 로그아웃 합니다.
show	장비의 설정 내용을 확인합니다.

3.1.2. Privilege Exec Enable 모드

읽기 권한만 가지는 것이 아니라 장비를 설정하는 권한까지 가질려면 Privilege Exec Enable 모드로 들어가야 합니다. Privilege Exec View 모드에서 “enable” 명령어를 사용하면, Privilege Exec Enable 모드로 들어갈 수 있습니다.

Privilege Exec Enable 모드로 들어가면 명령어 프롬프트가 SWITCH> SWITCH#로 바뀝니다.

명령어	모 드	기 능
enable	View	User Exec 모드에서 Privilege Exec Enable 모드로 들어갑니다.

또한, 좀 더 보안을 강화하려면, 관리자가 패스워드를 지정해 놓을 수도 있습니다. Privilege Exec View 모드에서는 사용자가 장비에 성공적으로 로그인하면, DSH 명령어의 Privilege Exec Enable 모드로 들어갑니다. Privilege Exec Enable 모드 명령어는 터미널 설정 변경, 네트워크 상태 및 시스템 정보 확인 등에서 사용합니다.

【 표 3-2 】은 V5812G의 NOS 3.03 Privilege Exec Enable 모드에서 사용하는 주요 명령어입니다.

【 표 3-2 】 Privilege Exec Enable 모드 주요 명령어

명령어	기능
clock	시스템에 시간 및 날짜를 입력합니다.
configure terminal	Global 설정 모드로 들어갑니다.
exit	시스템을 로그아웃 합니다.
reload	시스템을 다시 부팅합니다.
telnet	telnet으로 다른 장비에 접속합니다.
terminal line	터미널 스크린에 출력되는 행 수를 설정합니다.
traceroute	패킷 전송 경로를 추적합니다.
where	시스템에 접속한 원격 사용자를 확인합니다.

3.1.3. Global 설정 모드

Global 설정 모드는 Privilege Exec Enable 모드에서 “**configure terminal**” 명령어를 입력하면 들어갈 수 있습니다. Global 설정 모드로 들어가면 시스템 프롬프트가 SWITCH#에서 SWITCH(config)#로 바뀝니다.

명령어	모드	기능
config terminal	Enable	Privilege Exec Enable 모드에서 Global 설정 모드로 들어갑니다.

Global 설정 모드에서는 특정 프로토콜이나 특정 기능을 설정하기 이전에 시스템 전체를 통괄하는 전반적인 기능과 SNMP, RMON 기능을 설정하는데 사용합니다. 또한 사용자는 Global 설정 모드에서 DHCP, Interface, Router, Route-map 설정 모드로 들어갈 수 있습니다.

【 표 3-3 】 은 V5812G의 NOS 3.03 Global 설정 모드의 주요 명령어입니다.

【 표 3-3 】 Global 설정 모드 주요 명령어

명령어	기능
access-list	AS를 기준으로 라우팅 정보를 제한할 때 제한 정책을 설정합니다.
arp	IP 주소와 MAC 주소를 ARP 테이블에 등록합니다.
bgp	BGP 설정을 돋는 명령어입니다.
bridge	Bridge 설정 모드로 들어갑니다.
copy	설정한 내용을 Backup하거나 Backup한 설정을 불러 옵니다.
disconnect	원격 접속자의 연결을 해제합니다.
end	현재 모드를 마치고 Privilege Exec Enable 모드로 전환합니다
exec-timeout	자동 로그 아웃 기능을 설정합니다.
exit	현재 모드를 마치고 이전 모드로 전환합니다.
hostname	시스템 프롬프트의 호스트 이름을 변경합니다.
interface	Interface 설정 모드로 들어갑니다.
ip	DHCP 서버 등 인터페이스에 다양한 기능을 설정합니다.
passwd	패스워드를 변경합니다.
qos	QOS를 설정합니다.
restore factory-defaults	시스템 내용을 초기화합니다.
route-map	Route-map 설정 모드로 들어갑니다.
router	Router 설정 모드로 들어갑니다.
snmp	Snmp를 설정합니다.
syslog	Syslog를 설정합니다.
time-zone	Time-zone을 설정합니다.

3.1.4. Rule 설정 모드

Global 설정 모드에서 “**flow flow-name create**”, “**policer policer-name create**”, “**policy policy-name create**” 명령어를 사용하면, Rule을 설정할 수 있는 해당 Flow, Policer, Policy 설정 모드로 들어갑니다. Rule을 설정하기 위해 Flow, Policer, Policy 설정 모드로 들어가면 명령어의 프롬프트가 SWITCH(config)#에서 SWITCH(config-flow[name])#, SWITCH(config-policer[name])#, SWITCH(config-policy[name])#으로 바뀝니다.

새로운 Rule을 만들고 해당 설정 모드로 들어가려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
flow flow-name create	Global	Global 설정 모드에서 Flow 설정 모드로 들어갑니다.
policer policer-name create		Global 설정 모드에서 Policer 설정 모드로 들어갑니다.
policy policy-name create		Global 설정 모드에서 Policy 설정 모드로 들어갑니다.

Rule 설정 모드는 Rule 기능을 적용할 패킷의 조건과 해당 패킷의 동작 방식을 설정할 수 있습니다. 다음은 Rule을 설정하기 위한 각 모드에서 사용하는 주요 명령어입니다.

【 표 3-4 】 Flow 설정 모드 주요 명령어

명령어	기 능
apply	설정한 Rule 내용을 저장하고 장비에 적용시킵니다.
cos	해당 Rule에 CoS를 설정합니다.
dscp	패킷의 ToS 영역에 있는 DSCP값으로 정책을 설정합니다.
ethtype	Ethernet type으로 패킷 조건을 설정합니다.
ip-precedence	IP TOS precedence로 정책을 설정합니다.
length	패킷 길이로 패킷 조건을 설정합니다.
mac	MAC 주소로 패킷 조건을 설정합니다.
tos	ToS 값으로 정책을 설정합니다.

【 표 3-5 】 Policer 설정 모드 주요 명령어

명령어	기 능
apply	설정한 Rule 내용을 저장하고 장비에 적용시킵니다.
color	Metering을 설정합니다.
counter	패킷 Counter를 설정합니다.
rate-limit	패킷의 Rate Limit을 설정합니다.

【 표 3-6 】 Policy 설정 모드 주요 명령어

명령어	기능
action	패킷에 대한 동작을 설정합니다.
apply	설정한 Rule 내용을 저장하고 장비에 적용시킵니다.
include-class	Class를 Policy에 포함시킵니다.
include-flow	Flow를 Policy에 포함시킵니다.
include-policer	Policer를 Policy에 포함시킵니다. 정합니다.
interface-binding	Rule을 적용할 인터페이스를 지정합니다.
priority	우선 순위를 설정합니다.

3.1.5. DHCP 설정 모드

Global 설정 모드에서 “**ip dhcp pool pool-name**” 명령어를 입력하여 서브넷을 설정하면 시스템 프롬프트가 SWITCH(config)#에서 SWITCH(config-dhcp[pool-name])#로 바뀌면서 DHCP 설정 모드로 들어갑니다.

명령어	모드	기능
ip dhcp pool pool-name	Global	DHCP 설정을 위한 DHCP 설정 모드로 들어갑니다.

DHCP 설정 모드에서는 DHCP 서버에서 사용하는 IP 주소 범위를 설정하고, 서브넷에 그룹을 지정하고, 서브넷의 디폴트 게이트웨이를 설정합니다.

【 표 3-7 】 DHCP 설정 모드 주요 명령어

명령어	기능
default-gateway	서브넷의 디폴트 게이트웨이를 설정합니다.
dns-server	DNS 서버를 설정합니다.
exit	현재 모드를 마치고 이전 모드로 전환합니다.
range	DHCP 서버에서 사용하는 IP 주소의 범위를 설정합니다.

3.1.6. DHCP Option-82 설정 모드

Global 설정 모드에서 “**ip dhcp option82**” 명령어를 입력하여 서브넷을 설정하면 시스템 프롬프트가 SWITCH(config)#에서 SWITCH(config-dhcoption)#로 바뀌면서 DHCP 설정 모드로 들어갑니다.

명령어	모 드	기 능
ip dhcp option82	Global	DHCP 설정을 위한 DHCP 설정 모드로 들어갑니다.

DHCP 설정 모드에서는 DHCP 서버에서 사용하는 IP 주소 범위를 설정하고, 서브넷에 그룹을 지정하고, 서브넷의 디폴트 게이트웨이를 설정합니다.

【 표 3-8 】 DHCP Option-82 설정 모드 주요 명령어

명령어	기 능
exit	현재 모드를 마치고 이전 모드로 전환합니다.
lease	IP lease에 대한 조건을 설정합니다.
policy	Option-82 패킷에 대한 정책을 설정합니다.
pool	IP pool lease에 대한 조건을 설정합니다.
system-remote-id	시스템의 remote-id를 설정합니다.

3.1.7. Rmon 설정 모드

Global 설정 모드에서 “rmon-alarm <1-65534>”, “rmon-event <1-65534>”, “rmon-histoy <1-65534>” 명령어를 입력하면 각각 Rmon-alarm 설정 모드, Rmon-event 설정 모드, Rmon-history 설정 모드로 들어갑니다. 각각의 Rmon 설정 모드로 들어가면 시스템 프롬프트가 SWITCH(config)#에서 SWITCH(config-rmonalarm[n])#, SWITCH(config-rmonevent[n])#, SWITCH(config-rmonhistory[n])#로 바뀝니다.

【 표 3-9 】는 V5812G의 NOS 3.03 RMON 설정 모드에서 공통적으로 사용하는 명령어입니다.

【 표 3-9 】 RMON 설정 모드 공통 명령어

명령어	기능
active	각각의 Rmon을 활성화합니다.
exit	현재 모드를 마치고 이전 모드로 전환합니다.
owner	각각의 Rmon을 설정하고 관련 정보를 이용하는 주체를 명시합니다.

3.1.8. VRRP 설정 모드

Global 설정 모드에서 “**router vrrp interface-name group-id**” 명령어를 입력하면 시스템 프롬프트가 SWITCH(config)에서 SWITCH(config-router)#로 바뀌면서 VRRP 설정 모드로 들어갑니다.

명령어	모 드	기 능
router vrrp interface-name group-id	Global	Global 설정 모드에서 VRRP 설정 모드로 들어갑니다.

VRRP 설정 모드에서는 V5812G에 VRRP를 설정하여 그 기능을 활성화 합니다.

【 표 3-10 】 은 V5812G의 NOS 3.03 VRRP 설정 모드 주요 명령어에서 사용하는 명령어입니다.

【 표 3-10 】 VRRP 설정 모드 주요 명령어

명령어	기 능
associate	Virtual Router들이 가지는 동일한 Associated IP 주소를 설정합니다.
authentication	Virtual Router Group에 패스워드를 설정합니다.
preempt	Preempt 기능을 활성/비활성화 시킵니다.
vr_priority	Virtual Router에 우선 순위를 할당합니다.
vr_timers	Master Router가 자신의 정보를 다른 Virtual Router에 배포하는 시간 간격인 Advertisement time을 설정합니다.

3.1.9. Bridge 설정 모드

Global 설정 모드에서 “**bridge**”를 입력하면 시스템 프롬프트가 SWITCH(config)#에서 SWITCH(bridge)#로 바뀌면서 Bridge 모드로 들어갑니다.

명령어	모 드	기 능
bridge	Global	Global 설정 모드에서 Bridge 설정 모드로 들어갑니다.

Bridge 모드에서는 MAC 주소를 관리하고, VLAN, 포트 트렁킹, 스택링, 미러링 등 Layer 2 스위치로서의 기능을 설정합니다.

【 표 3-11 】은 V5812G의 NOS 3.03 Bridge 설정 모드에서 사용하는 주요 명령어입니다.

【 표 3-11 】 Bridge 설정 모드 주요 명령어

명령어	기 능
lacp	LACP 기능을 설정합니다.
mac-flood-guard	Mac-flood-guard를 설정합니다.
mirror	Mirroring 기능을 설정합니다.
rate	Rate-limit 기능을 설정합니다.
trunk	Trunk 기능을 설정합니다.
vlan	VLAN 기능을 설정합니다.

3.1.10. Interface 설정 모드

V5812G의 Interface 설정 모드에서는 각 Interface에 IP 주소를 설정하고 전송 속도 및 duplex 모드, 통신 대역폭을 지정하거나 관련 통계치를 확인할 수 있습니다. 특정 Interface 설정 모드로 들어가시려면 Global 설정 모드나 다른 Interface 설정 모드에서 **interface interface-name** 명령을 사용하십시오. Interface 설정 모드의 시스템 프롬프트는 SWITCH(config-if)# 입니다.

명령어	모 드	기 능
Interface interface-name	Global	Global 설정 모드에서 Interface 설정 모드로 들어갑니다.

【 표 3-12 】는 V5812G의 NOS 3.03 Interface 설정 모드의 주요 명령입니다.

【 표 3-12 】 Interface 설정 모드 주요 명령어

명령어	기 능
bandwidth	라우팅 정보 작성 시 필요한 대역폭을 설정합니다.
descripton	인터페이스에 대한 설명을 기록합니다.
interface interface-name	다른 인터페이스 설정 모드로 이동합니다.
ip	IP 주소를 설정합니다.
shutdown	인터페이스를 비활성화 시킵니다.

3.1.11. Router 설정 모드

Router 설정 모드는 Global 설정 모드에서 “**router ip-protocol**” 형태의 명령어를 사용하여 들어가며 시스템 프롬프트는 SWITCH(config)#에서 SWITCH(config-router)#로 바くなります.

명령어	모 드	기 능
router ip-protocol	Global	Global 설정 모드에서 Router 설정 모드로 들어갑니다.

Router 설정 모드는 라우팅 프로토콜 방식에 따라 BGP, RIP, OSPF의 세 가지가 있으며 각 종류의 IP 라우팅 프로토콜을 설정합니다. 【 표 3-13 】은 V5812G NOS 3.03 Router 설정 모드에서 공통으로 사용하는 주요 명령어입니다.

【 표 3-13 】 Router 설정 모드 공통 주요 명령어

명령어	기 능
distance	보다 효율적인 경로를 찾기 위해 거리값을 지정합니다.
exit	현재 모드를 마치고 이전 모드로 전환합니다.
neighbor	Neighbor 라우터를 지정합니다.
network	각 라우팅 프로토콜을 운영할 네트워크를 지정합니다.
redistribute	전달받은 라우팅 정보를 다른 라우터의 테이블에 등록합니다.

3.1.12. Route-Map 설정 모드

Route-Map 설정 모드는 Global 설정 모드에서 “**route-map name { permit | deny}<1-65535>**” 형태의 명령어를 사용하여 들어갑니다.

명령어	모 드	기 능
route-map name {permit deny} <1-65535>	Global	Global 설정 모드에서 Route-map 설정 모드로 들어갑니다.

Route-Map 설정 모드로 들어가면 시스템 프롬프트는 SWITCH (config)#에서 SWITCH(config-route-map)#으로 바뀝니다. Route-map 설정 모드에선 라우팅 테이블에 송신지와 목적지를 설정합니다.

【 표 3-14 】는 V5812G NOS 3.03 의 Route-Map 설정 모드 주요 명령어입니다.

【 표 3-14 】 Route-Map 설정 모드 주요 명령어

명령어	기 능
exit	현재 모드를 마치고 이전 모드로 전환합니다.
match	지정된 곳에 라우팅 정보를 전달합니다.
set	라우터 주소, 거리값 등을 설정합니다.

3.1.13. G-PON 설정 모드

Global 설정 모드에서 “**gpon**” 명령어를 입력하면 시스템 프롬프트가 SWITCH(config)#에서 SWITCH(gpon)#으로 바뀌면서 G-PON 설정 모드로 들어갑니다.

명령어	모 드	기 능
gpon	Global	Global 설정 모드에서 G-PON 설정 모드로 들어갑니다.

G-PON 설정 모드에서는 기본적인 G-PON 기능 설정 및 각종 설정내용을 확인할 수 있습니다.

【 표 3-15 】는 G-PON 설정 모드의 주요 명령어입니다.

【 표 3-15 】 G-PON 모드 주요 명령어

명령어	기 능
gpon-olt	G-PON OLT를 설정합니다.
onu-profile	G-PON ONU 프로파일을 설정합니다.

Gpon-olt 설정 모드와 Onu-profile 설정 모드는 각각 OLT와 ONU에 대한 세부 기능을 설정하고 적용하기 위해 들어가야 하는 모드입니다. 각각의 모드로 들어가려면 다음 명령어를 사용하십시오.

명령어	모드	기 능
gpon-olt <i>olt-id</i>	Gpon	G-PON OLT 설정 모드로 들어갑니다.
onu-profile <i>profile-name</i> create		ONU 프로파일 설정 모드로 들어갑니다.

G-PON 설정 모드에서 OLT 설정 모드로 들어가면 시스템 프롬프트가 SWITCH(gpon)#에서 SWITCH(config-gpon-olt[olt-id])#으로 바뀝니다. 한편, G-PON 설정 모드에서 Onu-profile 설정 모드로 들어가면 시스템 프롬프트가 SWITCH(gpon)#에서 SWITCH(config-onu-profile[profile-name])#으로 바뀝니다.

【 표 3-16 】은 Gpon-olt 설정 모드에서 사용하는 명령어입니다.

【 표 3-16 】 Gpon-olt 설정 모드 주요 명령어

명령어	기 능
olt signal-check	ONU 광신호를 체크합니다.
onu add	ONU를 등록합니다.
onu reset	ONU를 재부팅합니다.
onu upgrade	ONU 펌웨어를 업그레이드 합니다.

【 표 3-17 】은 Onu-profile을 설정할 때 사용하는 명령어입니다.

【 표 3-17 】 Onu-profile 설정 모드 주요 명령어

명령어	기 능
apply	설정한 profile을 저장합니다.
rate-limit	사용 가능한 대역폭을 설정합니다.
vlan-filter	VLAN 필터링을 설정합니다.

3.2 명령어 기본 사용법

DSH 명령어를 사용할 때 사용자가 미리 알아두면 편리한 기능이 몇 가지 있습니다. 그 기능은 다음과 같습니다.

- 사용 가능한 명령어 보기
- 이전 명령어 불러내기
- 축약된 명령어 사용하기
- Privilege Exec Enable 모두 명령어 사용하기
- 다른 모드로 이동하기

3.2.1. 사용 가능한 명령어 보기

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

다음은 V5812G의 Privilege Exec Enable 모드에서 사용할 수 있는 명령어입니다.

```
SWITCH# ?
Exec commands:
  clear      Reset functions
  clock      Manually set the system clock
  configure   Enter configuration mode
  copy       Copy from one file to another
  debug      Debugging functions
  default-os Select default OS
  disconnect Disconnect user connection
  enable     Turn on privileged mode command
  erase      Erase saved configuration
  exit       End current mode and down to previous mode
  halt       Halt process
  help       Description of the interactive help system
  no        Negate a command or set its defaults
  ping      Send echo messages
  quote     Execute external command
```

```
rcommand      Management stacking node
release       Release the acquired address of the interface
reload        reload
renew         Re-acquire an address for the interface
restart       Restart routing protocol
restore        Restore configurations
show          Show running system information
ssh           Configure secure shell
switchover    do switchover
tech-support  Technical Supporting Function for Diagnosis System
telnet        Open a telnet connection
terminal      Set terminal line parameters
traceroute   Trace route to destination
where         List active user connections
write         Write running configuration to memory, network, or terminal
```

SWITCH#

주 의

물음표(?)는 입력해도 화면에는 출력되지 않으며 Enter 키를 누르지 않아도 곧장 명령어 리스트를 출력해줍니다. 이 매뉴얼은 3.03 버전의 OS를 기준으로 작성된 것입니다. 제품에 설치된 NOS에 따라 출력된 내용이 다를 수 있으니 주의하시기 바랍니다.

현재 모드에서 사용 가능한 명령어들의 리스트를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show list	All	현재 모드에서 사용 가능한 명령어들을 확인합니다.
show cli		현재 모드에서 사용 가능한 명령어들을 트리구조로 확인합니다.

DSH이 탑재되어 있는 V5812G의 사용자는 특정 알파벳으로 시작하는 명령어를 알아볼 수 있습니다. 알고 싶은 첫 단어를 입력한 뒤 빈 칸없이 물음표를 입력하십시오.

다음은 V5812G의 Privilege Exec Enable 모드에서 s로 시작하는 명령어를 알아보는 방법입니다.

```
SWITCH# s?
show Show running system information
ssh  Configure secure shell
```

```
SWITCH# s
```

사용자는 또한 명령어 뒤에 입력해야 하는 변수 등도 알아볼 수 있습니다. 해당 명령어를 입력한 후 한 칸을 띄운 후 물음표를 입력하십시오. 다음은 **write** 명령어에 따르는 변수를 알아보는 방법입니다. 해당 명령어를 입력한 후 반드시 한 칸 띄운다는 것을 기억하시기 바랍니다.

```
SWITCH# write?
file      Write to file
memory   Write to NV memory
terminal Write to terminal
```

```
SWITCH# write
```

각 명령어 모드에서 사용할 수 있는 명령어와 입력해야 하는 변수의 리스트를 더욱 자세히 알기를 원한다면 **show list** 명령어를 사용하십시오.

다음은 Privilege Exec Enable 모드에서 사용할 수 있는 명령어를 **show list** 명령어를 사용하여 출력한 것입니다.

```
SWITCH# show list
clear arp
clear arp IFNAME
clear ip arp inspection statistics (vlan VLAN_NAME | )
clear ip bgp *
clear ip bgp * in
clear ip bgp * in prefix-filter
clear ip bgp * ipv4 (unicast|multicast) in
clear ip bgp * ipv4 (unicast|multicast) in prefix-filter
clear ip bgp * ipv4 (unicast|multicast) out
clear ip bgp * ipv4 (unicast|multicast) soft
-- more --
```



주의

이 매뉴얼은 OS 3.03 버전의 NOS를 기준으로 작성된 것입니다. 제품에 설치된 NOS에 따라 출력된 내용이 다를 수 있으니 주의하시기 바랍니다.



참고

“more”가 출력된 상태에서는 아무 키나 누르면 다음 리스트를 출력해 줍니다.



참 고

“q” 키, 또는 “Ctrl+C”를 입력하면 출력되는 것을 중단할 수 있습니다.

3.2.2. 이전 명령어 불러내기

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

다음은 여러 가지 명령어를 사용한 이후 이전 명령어를 불러오는 예입니다. **show clock**→**configure terminal**→**interface default**→**exit**의 순서로 입력한 후의 시스템 프롬프트 상태에서 위 방향 화살표를 누르면 반대로 **exit**→**interface default**→**configure terminal**→**show clock** 순서로 불러집니다.

```
SWITCH# show clock
Tue Nov 30 03:27:07 1999
SWITCH# configure terminal
SWITCH(config)# interface default
SWITCH(config-if)# exit
SWITCH(config)# exit
SWITCH# (↑키를 누름)
↓
SWITCH# exit(↑키를 누름)
↓
SWITCH# interface default(↑키를 누름)
↓
SWITCH# configure terminal(↑키를 누름)
↓
SWITCH# show clock(↑키를 누름)
```

이 부분은 동일선 상에서 출력되는 화면의 설명입니다.

사용자가 한 세션에서 사용한 모든 명령어를 확인하려면 다음 명령어를 사용하십시오.

Command	모 드	Function
show history	View/Enable	한 세션에서 사용한 모든 명령어를 확인합니다.

3.2.3. 축약된 명령어 사용하기

다른 명령어와 구분할 수 있는 최소한의 문자로 명령어를 사용할 수 있습니다. 다음 표는 축약된 형태의 명령어의 몇 가지 예입니다.

명령어	축약어
clock	cl
configure terminal	con te
show	sh
syslog	sys

3.2.4. Privilege Exec Enable 모드 명령어 사용하기

V5812G는 Privilege Exec Enable Mode의 명령어를 다른 모드에서 사용할 수 있습니다. Privilege Exec Enable Mode의 명령어를 다른 모드에서 사용하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
do command	Global/RMON/DHCP/Option-82/Bridge Interface/Rule/PIM/VRRP/Router/ Route-map	다른 모드에서 User 모드의 명령어를 사용 할 수 있습니다.

3.2.5. 다른 모드로 이동하기

V5812G는 CLI를 사용하여 설정하면서 전 단계 모드로 돌아가거나 Privilege Exec Enable 모드로 돌아갈 수 있습니다. 한편, Privilege Exec View 모드와 Privilege Exec Enable 모드에서는 전 단계 모드로 돌아갈 수 있는 명령어는 없고, 대신 시스템을 로그아웃 하는 명령어가 존재합니다.

전 단계 모드로 돌아가거나 Privilege Exec Enable Mode로 돌아가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
exit	Global/RMON/DHCP/Option-82/Bridge Interface /VRRP/Router/ Route-map	전 단계 모드로 돌아갑니다.



주의

Privilege Exec View 모드와 Privilege Exec Enable 모드에서는 두 명령어가 동일하게 시스템을 로그아웃 하는 데 사용됩니다.

다음은 Privilege Exec View 모드와 Privilege Exec Enable 모드에서 시스템을 로그아웃 하는 명령어입니다.

명령어	모 드	기 능
<code>exit</code>	View/Enable	시스템을 로그아웃 합니다.

4. 시스템 접속 및 IP 주소 설정

4.1 시스템 접속

설치가 끝난 V5812G는 각 포트가 네트워크와 관리용 PC에 올바르게 연결되어 있는지 최종 점검을 거치게 됩니다. 모든 점검이 끝나면, 사용자는 V5812G를 설정 및 관리하기 위해 시스템에 접속을 하게 됩니다.

이 장에서는 시스템 접속을 위해 필요한 패스워드를 변경하는 방법, Telnet을 사용하여 원격으로 시스템에 접속하는 방법 등을 다음의 순서로 설명합니다.

- 시스템 로그인
- 시스템 로그인 패스워드 변경
- Privilege Exec Enable 모드 접속 패스워드 설정
- 자동 로그 아웃 기능 설정
- 사용자 계정 관리
- 접속자 수 제한
- 원격 접속
- 원격 접속자 확인 및 연결 강제 해제
- 시스템 재부팅
- 시스템 로그 아웃

4.1.1. 시스템 로그인

V5812G의 설치가 끝나면 각 포트가 네트워크와 관리용 PC에 올바르게 연결되어 있는지 최종 점검하십시오. 모든 점검이 끝나면, 전원 장비를 켜고 다음과 같이 부팅 시킵니다.

1 단계 전원 장비를 켜면 자동적으로 부팅이 시작되고 로그인 프롬프트가 출력됩니다.

```
*****
*                               *
*          Boot Loader Version 4.74      *
*          DASAN Networks Inc.           *
*                               *
*****  
Press 's' key to go to Boot Mode: 0  
  
Load Address: 0x01000000  
Image Size: 0x00af5000  
Start Address: 0x01000000  
  
console=ttyS0,9600 root=/dev/ram rw  
NOS version 3.03 #1013  
CPU : Motorola [rev=1014]  
Total Memory Size : 256 MB  
Calibrating delay loop... 175.71 BogoMIPS  
INIT: version 2.85 booting  
Extracting configuration  
Fri, 13 Jan 2006 17:58:48 +0000  
INIT: Entering runlevel: 3  
  
SWITCH login:
```

2 단계 로그인 프롬프트에 로그인명을 입력하면 패스워드 프롬프트가 출력되고, 패스워드를 입력하면 Privilege Exec View 모드로 이동합니다. 제품이 공장에서 출하될 당시 기본적으로 설정된 로그인명은 “**admin**”이고, 패스워드는 없으므로 Enter 키를 입력하십시오.

```
SWITCH login: admin  
Password:  
SWITCH>
```

3 단계 Privilege Exec View 모드에서는 장비의 설정 내용을 확인하는 권한만 가지게 됩니다. 장비를 설정하고 관리하는 권한을 가지려면, Privilege Exec Enable 모드로 들어가야 합니다. 다음은 Privilege Exec Enable 모드로 들어가는 경우입니다.

```
SWITCH> enable  
SWITCH#
```

4.1.2. 시스템 로그인 패스워드 변경

장비를 설정 및 관리하는 권한을 가진 사용자는 패스워드를 변경할 수 있습니다. 확실한 보안을 위해서는 패스워드를 수시로 변경해 주는 것이 바람직합니다. 패스워드를 변경할 때에는 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
passwd	Global	사용자의 패스워드를 변경합니다.



패스워드는 5자 이상, 8자 이하의 문자와 숫자로 입력하실 수 있습니다. 로그인 ID와 유사한 패스워드는 되도록 삼가해 주십시오.

한편, “**user add**” 명령어를 사용하여 추가된 읽기 전용 사용자의 패스워드도 변경할 수 있습니다. 읽기 전용 사용자의 패스워드를 변경하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
passwd user-name	Global	읽기 전용 사용자의 패스워드를 변경합니다.

[설정 예제 1]

다음은 “dasan”이라는 이름으로 추가된 읽기 전용 사용자의 패스워드를 “networks”로 변경하는 경우의 예입니다.

```
SWITCH(config)# passwd dasan
Changing password for dasan
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password: networks
Re-enter new password: networks
Password changed.
SWITCH(config)#

```



패스워드는 입력해도 화면상에서 출력되지 않기 때문에 실수를 방지하기 위해 두 번 입력하도록 되어 있습니다.

4.1.3. Privilege Exec Enable 모드 접속 패스워드 설정

Privilege Exec View 모드에서 Privilege Exec Enable 모드로 전환할 때, 좀 더 보안성을 높이기 위해 패스워드를 설정해 둘 수 있습니다. Privilege Exec Enable 모드로 전환할 때 필요한 패스워드를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
passwd enable password	Global	Privilege Exec Enable 모드에 들어가기 위한 패스워드를 설정합니다.

사용자가 설정한 Privilege Exec Enable 모드 접속 패스워드는 **show running-config** 명령어를 사용하여 확인할 수 있습니다. 그러나, 설정된 패스워드의 보안을 위해 **show running-config** 명령어를 사용해서도 일반 사용자들이 확인할 수 없도록 설정할 수 있습니다. 다음 명령어를 사용하면, **show running-config** 명령어를 사용해도 패스워드가 암호화 되어서 보여지기 때문에 일반 사용자들은 패스워드를 알 수가 없습니다.

명령어	모 드	기 능
service password-encryption	Global	패스워드를 암호화하여 보여지게 합니다.

패스워드 보안을 위해 패스워드를 암호화하여 보여지게 했던 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no service password-encryption	Global	패스워드를 암호화하여 보여지게 했던 것을 해제합니다.

한편, 보안을 한층 더 강화하기 위해 **service password-encryption** 명령어를 사용하지 않아도 암호화된 패스워드만 공개되도록 설정할 수 있습니다. 그러나, 이 설정 방법은 사용자가 설정하려는 패스워드의 암호화된 문자열을 입력해야 합니다.

어떤 방법으로도 패스워드가 공개되지 않도록 암호화된 문자열로 패스워드를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
passwd enable 8 encrypted-password	Global	암호화된 문자열로 패스워드를 설정합니다.



참 고

사용자가 설정하려는 패스워드의 암호화된 문자열을 알고 싶을 때에는 일단 **passwd enable password** 명령어로 패스워드를 설정하고, **service password-encryption**을 활성화 시킨 상태에서 **show running-config** 명령어를 사용하여 패스워드를 확인하시면 됩니다.



참 고

위의 명령어를 사용하여 패스워드를 설정하면, **service password-encryption**을 활성화시키지 않아도 암호화된 문자열로 패스워드가 공개됩니다.

설정한 패스워드를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no passwd enable	Global	Privilege Exec Enable 모드에 들어가기 위해 설정한 패스워드를 삭제합니다.

[설정 예제 1]

다음은 Privilege Exec Enable 모드 접속 패스워드를 networks로 설정하는 경우입니다.

```
SWITCH# configure terminal
SWITCH(config)# passwd enable networks
SWITCH(config)# show running-config
!
hostname SWITCH
!
passwd enable networks
!
exec-timeout 0 0
(중략)
SWITCH(config)#

```

다음은 위와 같이 접속 패스워드를 설정한 후 접속하는 경우입니다.

```
SWITCH login: admin
Password:
SWITCH > enable
Password: networks
SWITCH #
```

다음은 **service password-encryption**을 활성화 하여 패스워드를 확인한 경우입니다.

```
SWITCH(config)# show running-config
!
hostname SWITCH
!
passwd enable 8 bJ6fc1PZ1AIRk
!
service password-encryption
exec-timeout 0 0
!
(중략)
SWITCH(config)#

```

[설정 예제 2]

다음은 암호화된 문자열을 이용하여 **networks**라는 패스워드를 설정하고 로그인 하는 경우입니다.



참 고

암호화된 문자열은 [설정 예제 1]와 같은 방법으로 확인할 수 있습니다. 사용자가 설정하려는 패스워드를 일단 **passwd enable password** 명령어로 설정하고, **service password-encryption**을 활성화 시킨 상태에서 **show running-config** 명령어를 사용하여 패스워드를 확인하시면 됩니다.

```
SWITCH# configure terminal
SWITCH(config)# passwd enable 8 bJ6fc1PZ1AIRk
SWITCH(config)# exit
SWITCH# exit

SWITCH login: admin
Password:
SWITCH > enable
Password: networks
SWITCH #
```

4.1.4. 자동 로그 아웃 기능 설정

V5812G의 관리자가 콘솔 터미널 스크린을 켜 둔 채 자리를 비우게 되는 경우, 계속 로그인 상태로 방치된다면 다른 사람이 관리자의 설정을 변경할 수도 있습니다. 따라서 V5812G에는 관리자가 정해 놓은 시간 동안 키보드 입력이 없으면 자동으로 시스템이 로그 아웃되는 기능을 가지고 있으며, 그 시간은 관리자가 설정할 수 있습니다.

다음은 자동 로그 아웃 기능을 설정하는 명령어입니다.

명령어	모 드	기 능
exec-timeout <1-35791>[0-59]	Global	사용자가 설정한 시간 동안 콘솔 터미널에 키보드 입력이 없으면 시스템을 자동 로그 아웃합니다. 시간의 단위는 초입니다.
exec-timeout 0		자동 로그 아웃 기능을 해제합니다.



<1-35791>의 시간 단위는 분이며 [0-59]의 시간 단위는 초입니다.



자동 로그 아웃 기능은 기본적으로 10분으로 설정되어 있습니다.

사용자의 장비에 자동 로그 아웃 시간이 몇 초로 설정되어 있는지 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show exec-timeout	View/Enable /Global	자동 로그 아웃 기능에 대한 설정 내용을 확인합니다.

다음은 자동 로그 아웃 시간을 60분으로 설정하고 확인한 경우의 예입니다.

```
SWITCH(config)# exec-timeout 60
SWITCH(config)# show exec-timeout
Log-out time : 60 min
SWITCH(config)#

```

4.1.5. 사용자 계정 관리

V5812G는 관리자가 관리자 이외의 사용자 계정을 추가할 수 있습니다. 또한, 관리자는 장비에 대한 보안을 강화하기 위해 관리자 이외의 사용자에 대해 Level 0부터 Level 15까지의 사용 권한 수준을 지정할 수 있습니다. Level 0부터 Level 14까지의 기본권한은 Privilege Exec View 모드에서 **exit**와 **help** 명령만 사용할 수 있기 때문에 Privilege Exec Enable 모드로 들어갈 수 없습니다. Level 15는 admin과 동일한 권한을 가지기 때문에 읽고 쓰기의 권한이 모두 주어집니다.

다음은 사용자를 추가하고, 사용자 권한을 설정하는 등 사용자 계정을 관리하는 방법에 대해 설명합니다.

(1) 사용자 계정 추가

V5812G는 관리자 이외의 사용자 계정을 추가할 수 있습니다. 사용자 계정을 추가할 때, 사용자 권한을 동시에 지정할 수 있으며, 만일 사용자 권한을 지정하지 않으면 기본적으로 Level 0의 권한이 주어집니다. 사용자 계정을 추가하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
user add name description	Global	Level0의 권한을 가진 사용자 계정을 추가합니다.
user add name level <0-15> description		사용자 권한을 지정하면서 사용자 계정을 추가합니다.



아무것도 설정하지 않은 Level 0부터 Level 14까지의 기본 권한은 Privilege Exec View Mode에서 **exit**와 **help** 명령어만 사용할 수 있고, Privilege Exec Enable Mode에 접속할 수 없게 되어 있습니다. 가장 높은 Level 15가 가지는 권한은 admin으로, 모든 읽고 쓰는 권한을 가지고 있습니다.

추가한 사용자 계정을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
user del name	Global	사용자 계정을 삭제합니다.

관리자가 추가한 사용자 계정을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show user	View/Enable/Global	추가된 사용자 계정을 확인합니다.

(2) 사용자 권한 설정

V5812G는 장비에 접속하는 사용자 권한 Level을 0부터 15까지 16단계로 구분하여 설정할 수 있습니다. 가장 높은 Level 15 모든 읽고 쓰는 권한을 가지고 있습니다. Level 0부터 Level 14까지의 권한은 관리자가 지정할 수 있습니다. 관리자는 해당 Level의 사용자가 어떤 모드에서 어떤 명령어를 사용할 수 있도록 할 것인지를 결정하여 이를 지정해줍니다. Level 0부터 Level 14까지의 기본 권한은 Privilege Exec View Mode에서 **exit**와 **help** 명령어만 사용할 수 있고, Privilege Exec Enable Mode에 접속할 수 없게 되어 있습니다.

다음은 사용자 Level에 따른 명령어 사용 권한을 설정하는 명령어입니다.

명령어	모 드	기 능
privilege bgp level <0-15> {command all}	Global	BGP 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege bridge level <0-15> {command all}		Brige 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege configure level <0-15> {command all}		Global 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege dhcp-option82 level <0-15> {command all}		DHCP Option82 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege dhcp-pool level <0-15> {command all}		DHCP Pool 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege dhcp-pool-class level <0-15> {command all}		DHCP Pool Class설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege dhcp-class level <0-15> {command all}		DHCP Class 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege enable level <0-15> {command all}		Privilege Exec Enable 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege flow level <0-15> {command all}		Flow 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege interface level <0-15> {command all}		Interface 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege ospf level <0-15> {command all}		OSPF 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege pim level <0-15> {command all}		PIM 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege policer level <0-15> {command all}		Policer 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege policy level <0-15> {command all}		Policy 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege rip level <0-15> {command all}		RIP 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.

명령어	모 드	기 능
privilege rmon-alarm level <0-15> {command all}	Global	RMON 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege rmon-event level <0-15> {command all}		Route-map 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege rmon-history level <0-15> {command all}		Privilege Exec View 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege route-map level <0-15> {command all}		VRRP 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege view level <0-15> {command all}		
privilege vrrp level <0-15> {command all}		

 주 의

낮은 Level에서 사용할 수 있도록 설정된 명령어는 그 이상의 Level에서는 모두 사용할 수 있게 됩니다. 예를 들어 Level 0에서 사용할 수 있도록 설정한 명령어는 Level 0부터 Level 14까지 모든 Level에서 사용할 수 있게 되는 것입니다.

 참고

동일하게 시작하는 명령어들은 맨 앞의 대표 명령어를 입력하면 모두 해당됩니다. 예를 들어 **show**를 입력하는 **show**로 시작하는 모든 명령어가 해당되게 되는 것입니다.

다음은 관리자가 사용자 권한으로 설정한 내용을 삭제하기 위해 사용하는 명령어입니다.

명령어	모 드	기 능
no privilege		사용자 권한으로 설정한 모든 내용을 삭제합니다.
no privilege bgp level <0-15> {command all}		
no privilege bridge level <0-15> {command all}		
no privilege configure level <0-15> {command all}		
no privilege dhcp-option82 level <0-15> {command all}		
no privilege dhcp-pool level <0-15> {command all}		
no privilege dhcp-pool-class level <0-15> {command all}		
no privilege dhcp-class level <0-15> {command all}		
no privilege enable level <0-15> {command all}		
no privilege flow level <0-15> {command all}		
no privilege interface level <0-15> {command all}	Global	각 모드의 명령어에 대해 사용자 권한으로 설정한 내용을 삭제합니다.
no privilege ospf level <0-15> {command all}		
no privilege pim level <0-15> {command all}		
no privilege policer level <0-15> {command all}		
no privilege policy level <0-15> {command all}		
no privilege rip level <0-15> {command all}		
no privilege rmon-alarm level <0-15> {command all}		
no privilege rmon-event level <0-15> {command all}		
no privilege rmon-history level <0-15> {command all}		
no privilege route-map level <0-15> {command all}		
no privilege view level <0-15> {command all}		
no privilege vrrp level <0-15> {command all}		

관리자가 설정한 Level에 따른 권한을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show privilege	Enable/Global	관리자가 설정한 Level에 따른 권한을 확인합니다.
show privilege now		현재 접속자의 Level을 확인합니다.

(3) 설정 예제

[설정 예제 1]

다음은 Level0의 권한을 가진 test0과 Level15의 권한을 가진 test15라는 사용자를 패스워드 없이 추가하는 경우입니다.

```
SWITCH(config)# user add test0 test
Changing password for test0
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
Bad password: too short.

Warning: weak password (continuing).
Re-enter new password:
Password changed.

SWITCH(config)# user add test15 level 15 test
Changing password for test15
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
Bad password: too short.

Warning: weak password (continuing).
Re-enter new password:
Password changed.

SWITCH(config)# show user
=====
User name          Description      Level
=====
test0              test            0
test15             test            15

SWITCH(config)#

```

[설정 예제 2]

다음은 Level 0의 권한을 가진 test0이라는 사용자와 Level 1의 권한을 가진 test1이라는 사용자를
패스워드 없이 추가하는 경우입니다.

```
SWITCH# configure terminal
SWITCH(config)# user add test0 test
Changing password for test0
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
Bad password: too short.

Warning: weak password (continuing).
Re-enter new password:
Password changed.

SWITCH(config)# user add test1 level 1 test
Changing password for test1
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
Bad password: too short.

Warning: weak password (continuing).
Re-enter new password:
Password changed.

SWITCH(config)# show user
=====
User name          Description      Level
=====
test0              test            0
test1              test            1

SWITCH(config)#
=====
```

다음은 Level 0과 Level 1의 권한 수준을 설정하는 경우입니다.

```
SWITCH# configure terminal
SWITCH(config)# privilege view level 0 enable
SWITCH(config)# privilege enable level 0 show
SWITCH(config)# privilege enable level 1 clock
SWITCH(config)# privilege enable level 1 configure terminal
SWITCH(config)# show privilege

Command Privilege Level Configuration
-----
Node      All    Level   Command
EXEC(ENABLE)      1      clock
EXEC(ENABLE)      1      configure terminal
EXEC(VIEW)        0      enable
EXEC(ENABLE)      0      show

4 entry(s) found.

SWITCH(config)#

```

위와 같이 설정하면, Level 0은 Privilege Exec Enable 모드에 접속하여 show 명령어만 확인할 수 있으며, Level 1은 Level 0이 가지는 권한은 물론 Privilege Exec Enable 모드에서 시간 설정하는 명령어와 Global 설정 모드에 접속하는 명령어를 사용할 수 있습니다.

4.1.6. 접속자 수 제한

V5812G 관리자는 장비에 접속할 수 있는 사용자의 수를 제한할 수 있습니다. 이 때 제한되는 접속자는 Console 포트를 통해 접속하는 사용자와 원격으로 접속하는 사용자를 모두 포함합니다. 그리고, 장비가 RADIUS 서버, 또는 TACACS+ 서버로 설정되어 있을 경우, 서버에 접속하는 사용자들도 제한되는 접속자 수에 모두 포함됩니다. 장비에 접속할 수 있는 사용자 수를 제한하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
login connect <1-8>	Global	장비에 접속할 수 있는 사용자 수를 제한합니다.



V5812G는 기본적으로 접속자 수를 8명으로 제한하고 있습니다.

장비에 접속할 수 있는 사용자 수를 제한했던 설정을 삭제합니다.

명령어	모 드	기 능
no login connect	Global	장비에 접속할 수 있는 사용자 수를 제한했던 설정을 삭제합니다.

4.1.7. 원격 접속

V5812G는 다음의 명령어를 사용하여 원격으로 시스템에 접속할 수 있습니다.

명령어	모 드	기 능
telnet destination	Enable	다른 시스템의 IP 주소나 Hostname을 입력하면 원격으로 접속합니다.
telnet destination port-number		다른 시스템의 지정된 포트로 원격 접속합니다.



“**write memory**”를 사용하여 설정 내용을 저장할 때, 저장이 완료되면 **[OK]**라는 메시지가 나타납니다. Telnet으로 접속하여 설정을 변경한 후 설정 저장할 때, **[OK]** 메시지를 확인하지 않고 Telnet session을 끊으면 설정이 모두 사라져버립니다. 반드시 **[OK]** 메시지를 확인한 후 접속을 해제하시기 바랍니다.

```
SWITCH# write memory
[ OK ]
SWITCH#
```

4.1.8. 원격 접속자 확인 및 연결 강제 해제

V5812G의 관리자는 원격 접속자를 확인하고, 원하지 않는 접속자의 연결을 해제할 수 있습니다. 원격 접속자의 연결을 해제하려면 일단, 다음 명령어를 사용하여 원격 접속자의 tty를 확인하십시오.

명령어	모 드	기 능
where	Enable /Global	원격 접속자를 확인합니다.

이 정보를 이용하여 다음 명령어를 사용하면 원격 접속자의 연결을 해제할 수 있습니다.

명령어	모 드	기 능
disconnect tty	Global	원격 접속자의 연결을 해제합니다.

다음은 원격 접속자를 확인하고, tty가 “**ttyp1**”인 원격 접속자의 연결을 해제하는 경우의 예입니다.

```
SWITCH(config)# where
admin at ttyS0 from console for 23 hours 50 minutes 17.27 seconds
admin at ttyp0 from 172.16.30.2:3246 for 4 hours 31 minutes 46.65 seconds
hyun at ttyp1 from 172.16.119.201:2633 for 2 hours 31 minutes 51.61 seconds
SWITCH(config)# disconnect ttyp1
SWITCH(config)#
ID 접속자의
```

4.1.9. 시스템 재부팅

(1) 수동 시스템 재부팅

TFTP/FTP 서버에서 새로운 시스템 이미지를 내려 받은 이후에는 반드시 시스템을 재부팅해야 하고, 이 밖에도 터미널 프로그램을 통해 장비를 설정 및 관리하는 도중에 다시 시스템을 부팅시켜야 하는 경우가 발생할 수 있습니다. 시스템을 재부팅하려면 Privilege Exec Enable 모드에서 다음의 명령어를 사용하십시오.

명령어	모 드	기 능
reload	Enable	시스템을 다시 부팅시킵니다.

한편, V5812G는 장비에 설치된 Flash Memory에 따라 Dual-OS를 지원할 수 있습니다. Flash Memory가 8M+16M일 때에는 Single-OS, Flash Memory가 8M+32M일 때에는 Dual-OS가 제공됩니다. Flash Memory는 **show system**으로 확인할 수 있습니다.

명령어	모 드	기 능
reload {os1 os2}	Enable	NOS를 선택하여 시스템을 재부팅 시킵니다.



주의

시스템을 재부팅하면 저장하지 않은 설정 내용은 지워지게 됩니다. 따라서 시스템을 재부팅하기 전에는 설정 내용을 반드시 저장하십시오.

V5812G는 사용자가 설정한 내용을 저장하지 않고 재부팅하는 것을 방지하기 위해서 설정한 내용이 있는데도 “**write memory**” 명령어를 사용하여 저장하지 않았을 경우, 다시 한번 재부팅 의사를 확인합니다. 그대로 재부팅하기를 원한다면 “y”를 입력하시고, 설정 내용을 저장하시려면 “n”을 입력한 후 저장하시기 바랍니다.

다음은 시스템을 설정한 후 내용을 저장하지 않고 재부팅했을 경우 보여지는 메시지입니다.

```
SWITCH# reload
Do you want to save the system configuration? [y/n]
```

(2) 자동 시스템 재부팅

V5812G는 사용자가 설정해 놓은 조건에 따라 자동으로 시스템을 재부팅하는 기능을 가지고 있습니다. 시스템을 재부팅하는 기준이 되는 것은 CPU와 Memory 2가지가 있습니다. CPU는 CPU Load나 Interrupt Load가 주어진 시간동안 지정한 값을 지속될 때 시스템이 재부팅됩니다. Memory는 Memory low가 주어진 시간 동안 지정한 횟수만큼 발생하면 자동으로 재부팅됩니다.

다음은 자동 시스템 재부팅 기능을 설정할 때 사용하는 명령어입니다.

명령어	모 드	기 능
auto-reset cpu <i>cpu-load-average</i> <i>interrupt-load-average</i> <i>time</i>		<i>time</i> 동안 <i>cpu-load-average</i> 또는 <i>interrupt-load-average</i> 가 지속되면 자동 재부팅되도록 설정합니다.
auto-reset memory <i>time-threshold--memory-low</i> <i>count--memory-low</i>	Bridge	<i>time-threshold--memory-low</i> 동안 Memory low가 <i>count--memory-low</i> 만큼 발생하면 자동 재부팅되도록 설정합니다.
no auto-reset {cpu memory}		자동 시스템 재부팅일 해제합니다.



참 고

*cpu-load-average*는 50부터 100까지 설정할 수 있고, *interrupt-load-average*는 1부터 100까지 설정할 수 있습니다.



참 고

*time-threshold-of-memory-low*는 1부터 120까지 설정할 수 있고, *count-of-memory-low*는 1부터 10까지 설정할 수 있습니다.



참 고

*time-threshold-memory-low*는 기본적으로 10분으로 설정되어 있고, *count-memory-low*는 기본적으로 5회로 설정되어 있습니다.

자동 시스템 재부팅에 대한 설정을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show auto-reset {cpu memory}	Enable/Global/Bridge	자동 시스템 재부팅 설정을 확인합니다.

[설정 예제 1]

다음은 1분 동안 CPU Load가 70%로 지속되거나 Interrupt Load가 70%로 지속될 때 자동으로 재부팅하도록 설정한 경우입니다.

```
SWITCH(bridge)# auto-reset cpu 70 70 1
SWITCH(bridge)# show auto-reset cpu
-----
Auto-Reset Configuration(CPU)
-----
auto-reset:          on
cpu load:           70
interrupt load:     70
continuation time:  1

SWITCH(bridge)#

```

[설정 예제 2]

다음은 10분 동안 Memory low가 3번 발생하였을 때 자동으로 재부팅하도록 설정한 경우입니다.

```
SWITCH(bridge)# auto-reset memory 10 3
SWITCH(bridge)# show auto-reset memory
-----
Auto-Reset Configuration(Memory)
-----
auto-reset : enabled
time threshold : 10
admin reboot count : 3

SWITCH(bridge)#

```

4.1.10. 시스템 로그아웃

시스템을 로그아웃 하는 것은 Privilege Exec View 모드나 Privilege Exec Enable 모드에서 가능합니다. 따라서 다른 모드에서 설정하던 중이라면, Privilege Exec Enable 모드로 돌아가야 합니다. 시스템을 로그아웃 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
exit	View/Enable	시스템을 로그아웃 합니다.

4.2 IP 주소 설정

V5812G는 데이터의 MAC 주소 만을 보고 패킷이 어디로 들어 와서 어느 포트로 가는지를 결정합니다. 원래 장비는 패킷을 전달할 때 IP 주소를 필요로 하지 않지만 SNMP나 텔넷을 통해 TCP/IP로 장비에 원격 접속을 하려면 IP 주소가 필요합니다.



V5812G는 가상 인터페이스 `default(interface 1)`가 설정되어 있고, 모든 포트가 `default`에 멤버 포트로 설정되어 있습니다.

IP 주소를 설정과 관련된 내용은 다음과 같습니다.

- 인터페이스 활성화 및 해제
- 네트워크 인터페이스에 IP 주소 설정
- Static 경로 및 default gateway 지정
- FIB(Forwarding Information Base) 테이블 확인
- 인터페이스 설명하기
- 인터페이스 확인
- 설정 예제

4.2.1. 인터페이스 활성화

인터페이스에 IP 주소를 할당하기 전에, 해당 인터페이스가 통신이 가능하도록 활성화되어 있는지 확인해야 합니다. 만일 활성화 되어 있지 않다면, IP 주소를 할당하여도 통신을 할 수 없습니다. 인터페이스가 활성화되어 있는지 확인하려면, “**show running-config**” 명령어를 사용하십시오.

다음은 인터페이스가 활성화 되어 있는지 확인하는 경우입니다.

```
SWITCH# show running-config
Building configuration...
(중략)
!
interface default
no shutdown
(이하 생략)
SWITCH#
```

**참 고**

Interface 1의 VLAN 이름은 「default」 입니다.

인터페이스를 활성화하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
interface <i>interface-name</i>	Global	해당 인터페이스의 Interface 설정 모드로 들어갑니다.

Interface 설정 모드에서 인터페이스를 활성화하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no shutdown	Interface	인터페이스를 활성화합니다.

4.2.2. 인터페이스 활성화 해제

인터페이스의 활성화를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
shutdown	Interface	인터페이스 활성화를 해제합니다.

4.2.3. 네트워크 인터페이스에 IP 주소 설정

인터페이스를 활성화한 후에는 IP 주소를 할당하십시오. IP 주소를 할당하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip address <i>address/M</i>	Interface	인터페이스에 IP 주소를 설정할 때 사용합니다. Config IP 주소로 설정됩니다.
ip address <i>address/M secondary</i>		Secondary IP 주소를 설정합니다.
ip address <i>address/M [secondary]</i> description <i>ip-address-description</i>		인터페이스에 IP 주소를 설정하고 해당 IP 주소에 대한 부연설명을 추가합니다.

다음은 인터페이스 1에 IP 주소 192.168.1.10을 할당하는 경우입니다.

```
SWITCH(config-if)# ip address 192.168.1.10/16
SWITCH(config-if)# show ip
IP-Address      Scope    Status
-----
192.168.1.10/16   global

SWITCH(config-if)#

```

할당한 IP 주소를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip	Interface	인터페이스에 설정된 IP 주소를 확인합니다.
show ip interface [interface-name] brief	View/Enable/Global	IP 상태와 설정을 서머리하여 보여줍니다.

할당한 IP 주소를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip address address/M		인터페이스에 할당된 IP 주소를 삭제합니다.
no ip address address/M secondary	Interface	Secondary IP 주소를 삭제합니다.
no ip address address/M [secondary] description ip-address-description		인터페이스에 할당한 IP 주소의 설명을 삭제합니다.

4.2.4. Static 경로 및 default gateway 지정

V5812G는 Static 라우트를 설정할 수 있습니다. Static 경로는 사용자가 지정하는 경로로 패킷은 static 경로를 통해 목적지에 도달합니다. Static 경로는 목적지 주소, 패킷을 전달 받을 Neighbor 라우터, 그리고 해당 목적지에 도달하기 위해 거쳐야 하는 경로 수를 포함합니다. Static 라우트를 설정하려면, Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip route ip-address prefix-mask {ip-gateway-address null} [<1-255>]		
ip route ip-address/m {ip-gateway-address null} [<1-255>]	Global	Static 라우트를 설정합니다.
ip route ip-address/m {ip-gateway-address null} src ip-address		

Default gateway를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip route default { ip-address null} [<1-255>]	Global	Default gateway를 설정합니다.

설정된 Static 라우트를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip route {ip-address ip-address/m summary}	Enable/Global	Static 라우트를 설정합니다.
show ip route database [bgp connected kernel ospf rip static]		

설정했던 Static 라우트를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip route ip-address ip-address {ip-address null} [<1-255>]	Global	설정했던 Static 라우트를 삭제합니다.
no ip route ip-address/m {ip-address null} [<1-255>]		

설정했던 Default gateway를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip route default { ip-address null} [<1-255>]	Global	Default gateway를 삭제합니다.

여러 개의 경로가 존재하는 멀티 패스에서 사용자는 최대 몇 개까지의 경로를 거칠 수 있는지 최대 경로수를 지정할 수 있습니다. 최대 경로 수를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip maximum-paths <1-8>	Global	최대 경로 수를 지정합니다.

4.2.5. FIB(Forwarding Information Base) 테이블 확인

대용량 라우팅 장비에서 패킷 포워딩을 고속으로 분산 처리하기 위해 라우팅 프로토콜에 의해 생성된 RIB(Routing Information Base) 정보가 FIB(Forwarding information Base)의 형태로 내려지고, 이에 따라 패킷들은 FIB를 바탕으로 전달되어야 할 목적지를 결정하여 전달됩니다.

FIB 방식은 지속적으로 캐시(Cache) 테이블을 유지할 필요가 없기 때문에 CPU 부하를 줄이면서 라우팅되어야 하는 패킷을 신속하게 처리해 줄 수 있는 장점을 가지고 있습니다.

네트워크 서비스를 위한 FIB 테이블 정보를 유지시키는 시간을 설정하려면, 다음과 같은 명령어를 사용하십시오.

명령어	모 드	기 능
fib retain forever		FIB 테이블 정보를 계속 유지하도록 설정합니다.
fib retain time <1-65535>	Global	FIB 테이블 정보를 설정한 초(secound) 동안 유지하도록 설정합니다.

FIB 테이블 정보의 유지 시간과 관련하여 설정한 내용을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no fib retain forever		설정한 FIB 테이블 정보 유지 시간을 해제합니다.
no fib retain time <1-65535>		

V5812G는 이러한 FIB 테이블을 확인할 수 있습니다. FIB 테이블을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip route fib	Enable/Global/Bridge	FIB 테이블을 확인합니다.

4.2.6. 인터페이스 설명하기

V5812G는 각 인터페이스에 대한 설명을 등록하여 사용자가 관리하기 편리하게 하였습니다. 각 인터페이스에 대한 설명을 등록하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
description description		인터페이스에 대한 설명을 등록합니다.
no description	Interface	등록한 설명을 삭제합니다.

4.2.7. 인터페이스 확인

V5812G의 인터페이스에 대한 설정 및 상태를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show interface [interface-name]	View/ Enable /Interface	인터페이스에 대한 설정과 상태를 확인합니다.

4.3 SSH(Secure Shell)

네트워크가 발달하면서 사용자들 사이에서 보안의 중요성이 더해가고 있습니다. 그러나 전통적인 ftp, telnet과 같은 서비스들은 보안이 매우 취약한 단점을 가지고 있습니다. SSH(Secure Shell)는 보안 로그인 쉘입니다. SSH를 사용하면 모든 데이터가 암호화되고, 트래픽은 압축되어 더 빠른 전송 효율을 얻을 수 있습니다. 또한 기존의 ftp, pop 같은 안전하지 못한 서비스들을 위한 터널까지 지원합니다.

4.3.1. SSH 서버 운영

V5812G는 서버로 운영될 수 있습니다. SSH 서버로서 V5812G는 다음과 같은 설정을 할 수 있습니다.

- SSH 서버 활성화
- 현재 접속중인 클라이언트 확인
- 클라이언트 접속 해제
- 클라이언트 접속 History 확인

(1) SSH 서버 활성화

사용자의 V5812G에 SSH 서버를 활성화하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ssh server enable	Global	SSH 서버를 활성화합니다.

한편, V5812G에서 SSH 서버 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ssh server disable	Global	SSH 서버 기능을 해제합니다.

(2) 현재 접속중인 클라이언트 확인

SSH 서버인 사용자의 V5812G에 현재 접속해 있는 클라이언트를 확인할 수 있습니다.

현재 접속 중인 클라이언트를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ssh	Enable/Global	현재 SSH 서버에 접속한 클라이언트를 확인합니다.

다음은 SSH 서버에 연결되어 있는 클라이언트를 확인한 경우입니다.

```
SWITCH# show ssh
connected clients : 001
num      pid      ppid      srv_usr      remote_ip      Start_Time
SPrevileged_Time

001      731      96      root      100.10.14.20   Fri Mar  7 04:23:51 1980  -----
--
SWITCH#
```

(3) 클라이언트 접속 해제

SSH 서버에 접속한 클라이언트의 접속을 강제로 해제할 수 있습니다. 클라이언트의 접속을 강제로 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ssh disconnect pid	Global	SSH 서버에 접속한 클라이언트를 강제로 해제합니다.



“pid”는 SSH 클라이언트의 번호로 “**show ssh**” 명령어를 사용하면 알 수 있습니다.

(4) 클라이언트 접속 History 확인

V5812G가 SSH 서버가 된 이후부터 접속했던 클라이언트들의 History를 확인할 수 있습니다.

클라이언트의 접속 History를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ssh history	Global	지금까지 SSH 서버에 접속했던 클라이언트들의 History를 확인합니다.



참 고

“**show ssh history**”로 확인하는 접속 History는 접속을 해제한 후에 기록되는 내용입니다. 현재 접속하고 있는 클라이언트는 “**show ssh**”로 확인할 수 있습니다.

4.3.2. 클라이언트 사용법

V5812G는 SSH 서버의 클라이언트로 다음과 같이 사용될 수 있습니다.

- SSH 서버 로그인
- 인증키 설정

(1) SSH 서버 로그인

V5812G가 SSH 클라이언트가 되어 SSH 서버에 로그인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ssh login destination	Enable	SSH 서버에 접속합니다.



참 고

“destination”은 서버의 IP 주소를 입력하거나 「계정@IP주소」 또는 「호스트도메인네임(ex : abc@100.1.1.1)」을 입력하시면 됩니다.

(2) 인증키 설정

SSH 클라이언트는 인증키를 설정하고 자신의 인증키를 서버에 알려줌으로써 인증키를 사용하여 서버에 접속할 수 있습니다. 인증키를 사용하는 것은 로그인 할 때마다 암호를 직접 입력하는 것보다 더욱 안전하며, 하나의 암호로 여러 SSH서버에 접속할 수 있는 등의 장점을 가집니다.

V5812G에 인증키를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ssh keygen {dsa rsa rsa1}	Global	인증키를 설정합니다.



참 고

“rsa1”은 ssh1에서 지원하는 인증 방식이고, “rsa”와 “dsa”는 ssh2에서 지원하는 인증 방식입니다.

인증키를 설정하고 인증키를 사용하여 서버에 접속하려면 다음 방법에 따르십시오.

- 1 단계 사용자의 장비에 인증키를 설정합니다. 다음은 SWTICH A에 dsa 인증 방식으로 “networks”라는 암호로 인증키를 설정하는 경우입니다.

```
SWITCH_A(config)# ssh keygen dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/etc/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):networks
Enter same passphrase again:networks
Your identification has been saved in /etc/.ssh/id_dsa.
Your public key has been saved in /etc/.ssh/id_dsa.pub
The key fingerprint is:
d9:26:8e:3d:fa:06:31:95:f8:fe:f6:59:24:42:47:7e admin@V5812G
SWITCH_A(config)#

```

저장된 디렉토리와
파일명

- 2 단계 인증키가 저장된 파일을 SSH 서버가 되는 SWITH B에 복사합니다. 복사를 하려면 SWITCH B에 접속해야 하기 때문에 SWITCH B 계정의 암호를 입력해야 합니다. 이 때 SWITCH B의 IP 주소는 172.16.209.10입니다.

```
SWITCH_A(config)#          ssh           copy           /etc/.ssh/id_dsa.pub
root@172.16.209.10:/etc/.ssh/authorized_keys
The authenticity of host '172.16.209.10 (172.16.209.10)' can't be established.
RSA key fingerprint is ea:af:c8:e9:3f:4f:22:1c:61:2e:2b:9d:0a:f6:2b:7e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.209.10' (RSA) to the list of known hosts.
root@172.16.209.10's password:
id_dsa.pub      100%  |*****| 600
00:00
SWITCH_A(config)#

```

- 3 단계 SSH 서버에 인증키로 접속합니다.

```
SWITCH_A(config)# ssh login 172.16.209.10
Enter passphrase for key '/etc/.ssh/id_dsa': networks
SWITCH_B#
```

4.3.3. 설정 예제

[설정 예제 1] SSH 서버 활성화

다음은 SSH 서버를 활성화한 후 그 내용을 확인한 경우입니다.

```
SWTICH(config)# ssh server enable
Generating SSH public/private RSA1 key ...
Generating SSH public/private RSA key ...
Generating SSH public/private DSA key ...
SSH Server start!
SWTICH(config)# show ssh
connected clients : 000
num      pid      ppid      srv_usr      remote_ip      Start_Time
Stop_Time
SWTICH(config)#

```

[설정 예제 2] 클라이언트 접속 해제

다음은 클라이언트의 번호를 확인한 후 강제로 접속을 해제한 경우입니다.

```
SWITCH# show ssh
connected clients : 001
num      pid      ppid      srv_usr      remote_ip      Start_Time
Stop_Time
001      150      96       root     203.236.124.89   Wed Mar  5 15:40:55 1980  -----
SWITCH# config terminal
SWITCH(config)# ssh disconnect 150
SWITCH(config)# show ssh
connected clients : 000
num      pid      ppid      srv_usr      remote_ip      Start_Time
Stop_Time
SWITCH(config)#

```

[설정 예제 3] 클라이언트 접속 History 확인

다음은 클라이언트 접속 History를 확인한 경우입니다.

```
SWITCH(config)# show ssh history
history clients : 013
num    pid     ppid   srv_usr      remote_ip        Start_Time          Stop_Time
001    235     96     admin       202.26.10.29  Thu Mar 6 09:54:15 1980  Thu Mar 6 09:55:47 1980
002    269     96     admin       172.16.10.1   Thu Mar 6 09:58:30 1980  Thu Mar 6 10:00:00 1980
003    297     96     admin       172.16.10.1   Thu Mar 6 10:00:46 1980  Thu Mar 6 10:28:39 1980
004    441     96     admin       172.16.10.1   Thu Mar 6 10:46:44 1980  Thu Mar 6 10:46:46 1980
005    487     96     admin       172.16.20.10  Thu Mar 6 11:42:13 1980  Thu Mar 6 11:47:56 1980
006    500     96     admin       172.16.20.10  Thu Mar 6 11:59:06 1980  Thu Mar 6 12:00:32 1980
007    511     96     admin       172.16.9.10   Thu Mar 6 12:03:42 1980  Thu Mar 6 12:03:43 1980
008    258     96     admin       202.6.14.20   Thu Mar 6 09:56:17 1980  Thu Mar 6 12:07:52 1980
009    640     96     admin       172.16.21.55  Thu Mar 6 16:31:02 1980  Thu Mar 6 16:31:02 1980
010    646     96     admin       10.10.21.61   Thu Mar 6 16:34:27 1980  Thu Mar 6 16:35:49 1980
011    656     96     admin       100.16.21.61  Thu Mar 6 16:39:37 1980  Thu Mar 6 16:39:37 1980
012    660     96     admin       172.16.21.61  Thu Mar 6 16:39:59 1980  Thu Mar 6 16:40:06 1980
013    669     96     admin       172.16.21.61  Thu Mar 6 16:41:45 1980  Thu Mar 6 16:41:45 1980
SWITCH(config)#

```

[설정 예제 4] 클라이언트로서 서버에 접속

다음은 172.16.209.10이라는 주소를 가진 SSH 서버에 접속하는 경우입니다. 클라이언트가 되어 SSH서버에 접속하려고 하면 일단 접속 의사를 묻는 메시지가 출력됩니다.

```
SWITCH(config)# ssh login 172.16.209.10
The authenticity of host '172.16.209.10 (172.16.209.10)' can't be established.
RSA key fingerprint is ea:af:c8:e9:3f:4f:22:1c:61:2e:2b:9d:0a:f6:2b:7e.
Are you sure you want to continue connecting (yes/no)?
```

이때 서버에 계속하여 접속하려면 “yes”를 입력하십시오. 그러면 암호를 묻는 메시지가 출력됩니다. 이때, SSH 서버 계정의 암호를 입력하면 성공적으로 접속됩니다.

```
SWITCH(config)# ssh login 172.16.209.10
The authenticity of host '172.16.209.10 (172.16.209.10)' can't be established.
RSA key fingerprint is ea:af:c8:e9:3f:4f:22:1c:61:2e:2b:9d:0a:f6:2b:7e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.209.10' (RSA) to the list of known hosts.
admin@172.16.209.10's password:
SWITCH(config)#

```

위에서 설명한 경우는 서버에 처음 접속할 때에만 발생합니다. 한 번 접속한 서버는 known-host가 생성되기 때문에 간단히 암호만 묻게 됩니다. 다음은 known-host가 존재하는 서버에 접속했을 경우입니다.

```
SWITCH(config)# ssh login 172.16.209.10
admin@172.16.209.10's password:
SWITCH(config)#

```

4.4 사용자 인증 포트 설정(802.1x)

네트워크 관리의 보안과 이동성을 높이기 위해 사용자의 정보를 제한하는 방식에는 MAC 주소를 이용한 인증 방식과 포트를 기반으로 한 802.1x 인증 방식이 있습니다. 이 중에서 802.1x 인증 방식은, 간단히 설명하자면 접속을 시도하는 사용자의 정보를 가지고 RADIUS 서버에서 접속 권한 부여를 결정하는 것입니다.

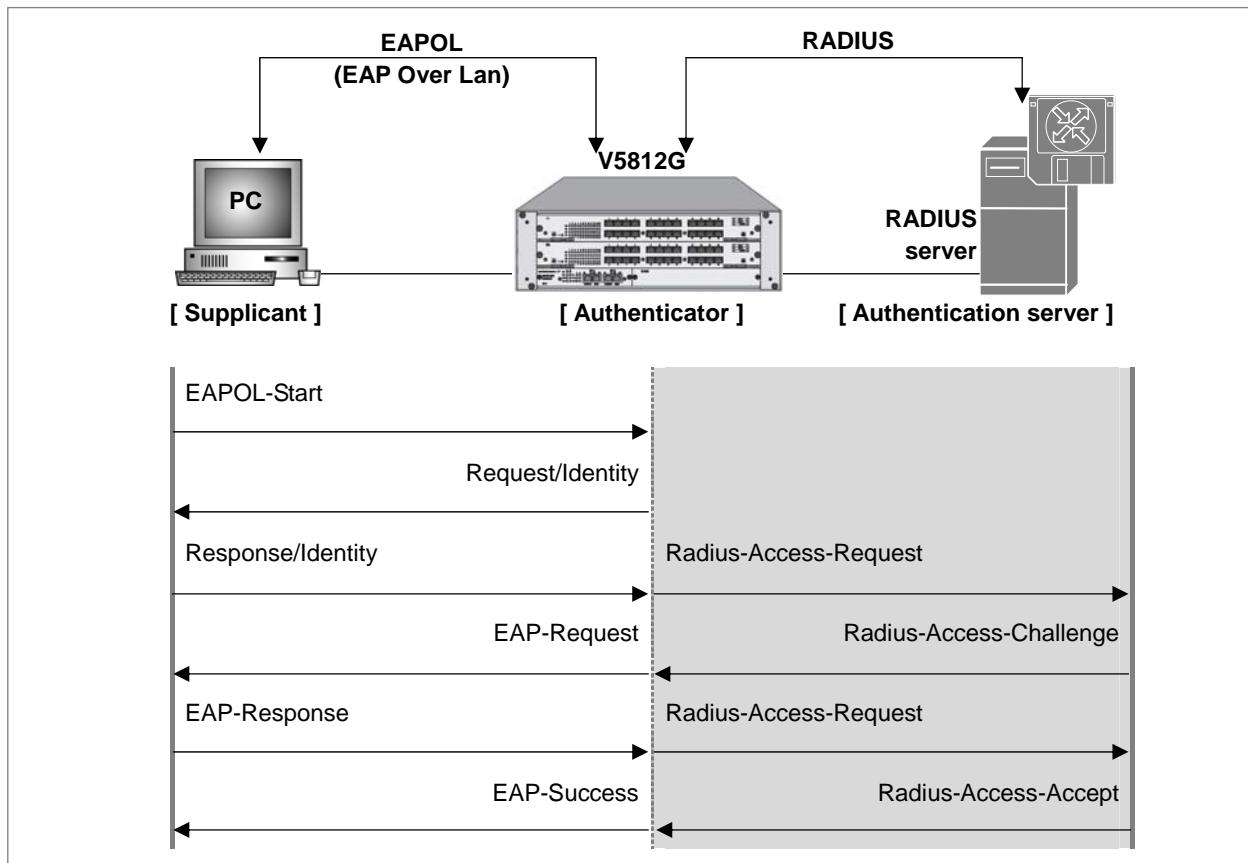
802.1x 인증은 EAP(Extensible Authentication Protocol) 구조를 채택하고 있습니다. EAP 방식에는 EAP-MD5(Message Digest 5), EAP-TLS(Transport Level Security), EAP-SRP(Secure Remote Password), EAP-TTLS(Tunneled TLS) 등이 있으며 V5812G는 EAP-MD5와 EAP-TLS 방식을 지원합니다.

EAP-MD5는 사용자의 ID와 패스워드를 이용하여 접속하는 것인데 단방향으로 이루어지는 패스워드 기반 네트워크 인증 방식입니다. EAP-TLS는 서버 인증서와 사용자 개인 인증서의 상호 인증을 통해 접속하는 방법인데, 양방향으로 이루어지는 인증서 기반 인증 방식이기 때문에 높은 보안 성능을 보장할 수 있습니다.

사용자가 접속 인증을 요청하면 사용자의 PC에서 EAPOL-Start 타입의 패킷이 Authenticator에 전송되고, Authenticator는 다시 사용자에게 신원을 요청합니다. 신원에 대한 응답을 받은 후에는 RADIUS 서버에 접속 승인을 요청하고, 사용자의 정보를 통해 접속 권한이 확인되면 인증을 받습니다.

이 때, 사용자(Supplicant)와 Authenticator는 PAE(Port Authentication entites)에 해당합니다. Authenticator는 단지 인증을 위한 브리지 역할을 할 뿐, 사용자에 대한 어떠한 정보도 가지고 있지 않습니다. 인증에 필요한 사용자 정보의 데이터베이스는 RADIUS 서버가 가지고 있습니다.

아래 그림은 802.1x 사용자 인증의 과정을 간단하게 나타낸 것입니다.



【 그림 4-1 】 802.1x 사용자 인증 과정

다음은 V5812G의 포트에 802.1x를 설정하기 위한 설정 방법입니다.

- 802.1x 기본 설정
- 802.1x 재인증 설정
- 802.1x 인증 상태 초기화
- 802.1x 설정 내용 초기화
- 802.1x 설정 내용 확인
- 802.1x 사용자 인증 통계 확인 및 삭제

주 의

논리 포트를 Private VLAN의 *primary-uplink*와 *secondary-uplink* 포트로 지정하는 경우에는 해당 포트에 대한 802.1x 인증이 불가능합니다.

4.4.1. 802.1x 기본 설정

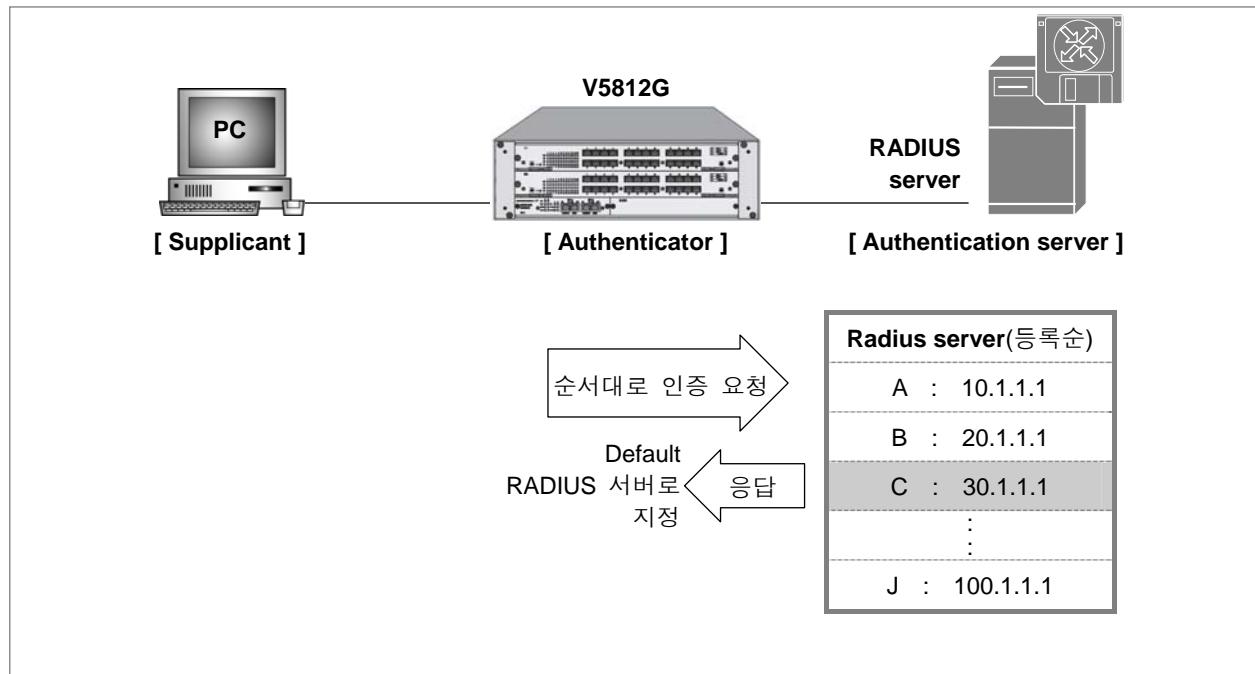
(1) 802.1x 활성화

802.1x 사용자 인증 포트를 설정하려면, 가장 먼저 사용자 장비의 802.1x 데몬을 활성화해야 합니다. 사용자 장비의 802.1x 데몬을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
dot1x system-auth-control	Global	802.1x 데몬을 활성화합니다.
no dot1x system-auth-control		802.1x 데몬을 비활성화합니다.

(2) 인증 서버 설정

포트에 802.1x 사용자 인증을 설정하였다면 접속 권한을 가지고 있는 사용자에 대한 데이터를 가지고 있는 RADIUS 서버가 존재하게 마련입니다. 사용자는 802.1x 사용자 인증 포트를 지정한 후 자신의 장비가 사용하게 될 RADIUS 서버의 IP 주소와 Key 값을 등록해야 합니다.



【 그림 4-2 】 Multi Authentication Server

여러 개의 서버를 등록해 두면, 첫 번째로 등록한 RADIUS 서버부터 인증 요청을 시작하게 되고, 응답이 없을 때에는 두 번째 지정한 RADIUS 서버에게 인증을 요청하게 됩니다. 등록한 순서에 따라 인증 요청을 시도하게 되며 응답을 한 서버는 응답을 한 시점부터 Default 서버가 됩니다.

Default 서버가 정해지면, 그 이후의 모든 인증 요청은 Default 서버가 된 RADIUS 서버에서부터 시작합니다. 다시 Default 서버로부터 응답이 없어지면 다음으로 지정된 RADIUS 서버에 인증 요청을 시도합니다.

다음은 RADIUS 서버의 IP 주소와 Key 값을 등록할 때 사용하는 명령어입니다.

명령어	모 드	기 능
dot1x radius-server host {ip-address name} auth-port <0-65535> key key	Global	암호화 키값과 인증 서버의 UDP 포트와 함께 RADIUS 서버를 등록합니다.
dot1x radius-server host {ip-address name} key key		암호화 키값과 함께 RADIUS 서버를 등록합니다.



인증 포트인 *auth-port-num*는 <0 – 65535> 사이에서 설정 가능합니다.



V5812G는 Authentication Server가 되는 RADIUS 서버를 5개까지 지정할 수 있습니다.



Authenticator에 RADIUS 서버를 등록하는 것처럼 RADIUS 서버에도 Authenticator를 등록해야 합니다. 이 때 Authenticator와 RADIUS 서버는 서로의 IP 주소를 등록하는 것 외에도 서로를 인증해줄 별도의 데이터가 필요한데 이것을 Key라고 하며 각각 동일한 값을 넣어주어야 합니다. Key 값으로는 공백이나 특수 문자를 제외한 모든 문자를 사용할 수 있습니다.

등록했던 RADIUS 서버를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no dot1x radius-server host {ip-address name}	Global	등록했던 RADIUS 서버를 삭제합니다.

한편, V5812G는 사용자가 설정한 RADIUS 서버에 대한 우선 순위를 설정할 수 있습니다.

RADIUS 서버에 우선 순위를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
dot1x radius-server move {ip-address name} priority <i>priority</i>	Global	RADIUS 서버에 대한 우선순위를 설정합니다..

(3) 인증 모드 설정

V5812G의 802.1x에서는 다음 명령어로 사용자가 포트 기반과 MAC 주소 기반 중에서 인증 모드를 선택할 수 있습니다.

명령어	모 드	기 능
dot1x auth-mode mac-base port-number	Global	MAC 주소 기반 802.1x 인증 방식을 선택합니다.
no dot1x auth-mode mac-base port-number		포트 기반 802.1x 인증 방식을 선택합니다.



주의

MAC 주소 기반의 802.1x 인증을 설정하기 전에 반드시 **mac-filter default-policy deny port-number** 명령어로 인증 포트로 들어오는 모든 패킷을 차단하도록 하십시오.

(4) 인증 포트 설정

802.1x 인증 모드를 설정하였다면, 다음 명령어로 인증 포트를 선택하십시오.

명령어	모 드	기 능
dot1x nas-port port-number	Global	802.1x 인증 포트를 지정합니다.
no dot1x nas-port port-number		802.1x 인증 포트를 해제합니다.



참 고

*port-number*는 쉼표(,)를 사용하여 여러 개를 입력하거나, 대쉬(-)를 사용하여 일련의 범위를 지정할 수 있습니다.

(5) 인증 포트 상태 설정

V5812G 802.1x에서는 다음 명령어로 인증 포트의 상태를 설정할 수 있습니다. **force-authorized**는 인증 성공, **force-unauthorized**는 인증 실패로 해당 포트의 상태를 부여하며, **auto**는 포트에서 요청이 있어야만 인증을 실시합니다.

명령어	모 드	기 능
dot1x port-control {auto force-authorized force-unauthorized} port-number	Global	인증 포트 상태를 설정합니다.
no dot1x port-control port-number		설정한 인증 포트 상태를 해제합니다.

(6) Request/Identity 패킷 재전송 시간 설정

Authenticator는 Supplicant에게 인증을 시작하는 EAPOL-Start 패킷을 보냅니다. Authenticator가 Request/Identity 패킷을 보낸 후, 일정한 시간 동안 Supplicant로부터 Response/Identity 패킷을 받지 못하면, 다시 Request/Identity 패킷을 보내 Response/Identity 패킷을 재요청합니다. V5812G는 Authenticator가 얼마동안 Supplicant로부터 응답을 못 받았을 때 Response/Identity 패킷을 재요청할 것인지, 그 시간을 설정할 수 있습니다.



참 고

여기서 말하는 과정은 위의 【그림 4-1】 802.1x 사용자 인증 과정에서 “EAP-Request/Identity”와 “EAP-Response/Identity”에 해당합니다.

Response/Identity 패킷이 얼마동안 전송되지 않으면 Request/Identity 패킷을 재전송할 것인지, 그 시간을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
dot1x timeout tx-period interval port-number	Global	Request/identity 패킷을 재전송하는 시간을 설정합니다.

설정한 시간을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no dot1x timeout tx-period port-number	Global	설정한 시간을 삭제합니다.



참 고

기본적으로 Request/Identity 패킷에 대한 응답은 30초 이내에 받도록 설정되어 있습니다. 30초 동안 응답이 없으면 다시 요청합니다.



*interval*은 <1-65535> 사이에서 설정 가능합니다.

(7) 인증 시도 요청 횟수 설정

802.1x의 인증 포트를 설정한 뒤에는 다음 명령어로 Authenticator가 되는 장비가 RADIUS 서버로 부터 인증을 받기까지 Authenticator의 인증 시도 요청 횟수를 설정하십시오. 여기서 말하는 인증 요청이란 【그림 4-1】 802.1x 사용자 인증 과정에서 **Radius-Access-Request**에 해당합니다.

인증 요청 회수를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
dot1x radius-server retries number	Global	인증 요청 횟수를 설정합니다.



참 고

V5812G는 기본적으로 인증 요청을 3번 시도하도록 설정되어 있습니다.

(8) 인증 시도 주기 설정

Authenticator가 되는 장비에서 RADIUS 서버에 접속 인증을 요청한 후 아무런 응답이 없을 경우에 위에서 설정한 횟수만큼 인증을 다시 요청하게 됩니다.

이 때, 관리자는 얼마나 기다렸다가 다시 요청을 할 것인지, 그 대기 시간을 지정해줄 필요가 있습니다. 그래서, 인증 재요청 간격을 1000ms로 설정하면, 인증 요청을 보낸 후 1000ms 동안 응답이 없을 때 다시 인증을 요청하게 되는 것입니다.

인증 요청은 재시도는 Request에 대한 Response가 전혀 없을 경우에만 시행됩니다. 예를 들어 RADIUS 서버는 다운 되고, RADIUS 패킷이 아닌 다른 패킷으로라도 응답이 있다면 인증 요청 재시도는 시행되지 않습니다.

다음 명령어로 재인증 요청 주기를 설정하십시오. 여기서 말하는 인증 요청이란, 위의 【 그림 4-1 】 802.1x 사용자 인증 과정에서 **Radius-Access-Request**에 해당합니다.

명령어	모 드	기 능
dot1x radius-server timeout <i>interval</i>	Global	인증 시도 요청 주기를 설정합니다.



참 고

*interval*은 <1~65,535> 사이에서 설정 가능하며 기본적으로 1초로 설정되어 있습니다.



주 의

서버와 거리가 멀리 있는 경우, Request 패킷이 서버에 도달하는 시간을 고려하지 않고 인증 요청 재시도 간격을 너무 짧게 설정하면 인증이 안되는 상황이 발생할 수 있을 수 있습니다. 따라서, 서버와의 거리에 따라 인증 요청 재시도 간격을 설정해주시고, 모든 설정을 마친 상태에서 인증이 제대로 이루어지지 않을 경우에는 인증 요청 재시도 간격을 확인하여 좀 더 넉넉하게 설정해보시기 바랍니다.

4.4.2. 802.1x 재인증 설정

V5812G의 dot1x에서는 인증 포트에 대해 주기적으로 인증 상태가 갱신될 수 있도록 설정할 수 있습니다. V5812G의 802.1x에서 포트 재인증을 설정하려면 다음 단계를 따르십시오.

- 1 단계 802.1x 재인증을 활성화합니다.
- 2 단계 재인증 주기를 설정합니다.
- 3 단계 재인증 실패시 인증 재시도 주기를 설정합니다.
- 4 단계 필요에 따라 특정 포트를 항상 재인증에 성공한 상태로 설정합니다.

(1) 802.1x 재인증 활성화

다음 명령어로 V5812G 802.1x의 재인증을 활성화하십시오.

명령어	모 드	기 능
dot1x reauth-enable <i>port-number</i>	Global	802.1x 재인증을 활성화합니다.
no dot1x reauth-enable <i>port-number</i>		802.1x 재인증을 비활성화합니다.

(2) 재인증 주기 설정

다음 명령어로 V5812G 802.1x의 재인증 주기를 설정하십시오. 사용자가 설정한 주기마다 각 포트의 인증 상태가 갱신됩니다.

명령어	모 드	기 능
dot1x timeout reauth-period interval port-number	Global	재인증 주기를 설정합니다.
no dot1x timeout reauth-period port-number		설정한 재인증 주기를 해제합니다.



참 고

*interval*의 단위는 ms로, <1~4,294,967,295>에서 설정 가능합니다. 디폴트 설정값은 100ms(0.1초)입니다.

(3) 재인증 시도 주기 설정

V5812G의 802.1x는 다음 명령어로 주기적인 이루어지는 재인증에 실패하였을 때, 다시 인증을 시도하는 주기를 설정할 수 있습니다.

명령어	모 드	기 능
dot1x timeout quiet-period interval port-number	Global	재인증 시도 주기를 설정합니다.
no dot1x timeout quiet-period port-number		재인증 시도 주기를 해제합니다.



참 고

*interval*의 단위는 ms로, <1~65,535>에서 설정 가능합니다. 디폴트 설정값은 100ms(0.1초)입니다.

(4) 포트 재인증 실행

(2) 재인증 주기 설정에서는 네트워크에 접속되어 있는 사용자들이 접속 권한을 잃지 않도록 하거나 RADIUS 서버와 802.1x 인증 포트를 관리하는 여러 가지 정책적인 이유로 네트워크에 접속되어 있는 사용자들은 일정한 간격을 두고 재인증을 받아야 한다고 설명하였습니다. 그리고, 관리자는 재인증을 받는 시간 간격을 설정할 수 있습니다. 그러나, 사용자가 새로 설정한 재인증 내용을 바로 실행하거나 재인증을 지금 즉시 받아야하는 경우가 발생할 수 있습니다. V5812G는 이러한 경우 즉시 재인증을 실행할 수 있습니다.

설정되어 있는 시간 간격과 무관하게 즉시 재인증을 실행하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
dot1x reauthenticate port-number	Global	설정되어 있는 시간 간격과 무관하게 재인증을 실행합니다.

4.4.3. 802.1x 인증 상태 초기화

V5812G 802.1x에서는 다음 명령어로 현재 상태에 관계없이 포트의 인증 상태를 초기화 시킬 수 있습니다. 초기화된 포트는 다시 인증을 받아야만 시스템에 접근할 수 있습니다.

명령어	모 드	기 능
dot1x initialize port-number	Global	포트의 인증 상태를 초기화합니다.

4.4.4. 802.1x 설정 내용 초기화

V5812G에서는 다음 명령어로 포트의 802.1x 설정 내용을 초기화하여, 시스템에서 지정한 디폴트 값을 적용시킬 수 있습니다.

명령어	모 드	기 능
dot1x default port-number	Global	802.1x 설정 내용을 초기화합니다.

4.4.5. 802.1x 설정 내용 확인

V5812G의 802.1x 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show dot1x [port-number]	View/Enable/Global	802.1x 사용자 인증의 설정 내용을 확인합니다.



참 고

*port-number*는 쉼표(,)를 사용하여 여러 개를 입력하거나, 대쉬(-)를 사용하여 일련의 범위를 지정할 수 있습니다.

4.4.6. 802.1x 사용자 인증 통계 확인 및 삭제

V5812G의 사용자는 802.1x 사용자 인증의 인증 과정에 대한 통계를 확인하거나 통계를 삭제하여 Reset 상태로 만들 수 있습니다. 802.1x 사용자 인증의 인증 과정에 대한 통계를 확인하려면 다음 명령어를 사용하십시오.

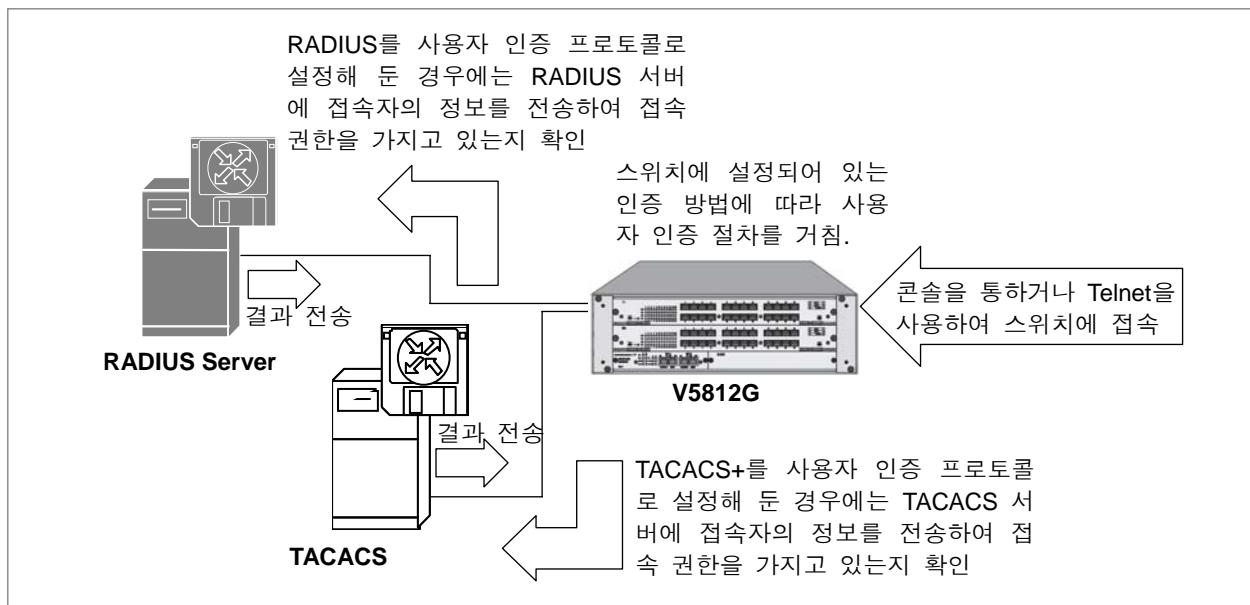
명령어	모 드	기 능
show dot1x statistics port-number	Global	해당 포트에서 발생한 802.1x 인증 과정 관련 통계를 확인합니다.

802.1x 인증 과정 관련 통계를 초기화 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
dot1x clear statistics port-number	Global	802.1x 인증 과정 관련 통계를 초기화합니다.

4.5 시스템 사용자 인증

시스템 사용자 인증에 대한 보안이 한 단계 더 높아진 V5812G는 시스템에 접속하는 사용자에 대한 인증 방법을 다양하게 설정할 수 있습니다. 일반적으로는 장비에 등록되어 있는 사용자 ID와 패스워드를 통하여 접속 권한이 주어지지만, 사용자 인증 프로토콜인 RADIUS(Remote Authentication Dial-In User Service)와 Tacacs+(Terminal Access Controller Access Control System+)등을 이용하도록 설정해 두면 각각의 서버가 가지고 있는 데이터베이스에 기록된 사용자만이 접속을 할 수 있게 됩니다.



【 그림 4-3 】 시스템 사용자 인증 과정

V5812G에 시스템 사용자 인증을 설정하기 위해 다음과 같은 설정 방법을 설명합니다.

- 사용자 인증 방법 설정
- 사용자 인증 인터페이스 지정
- 사용자 인증 방법 우선 순위 설정
- 사용자 인증 방법 설정 내용 확인
- RADIUS 설정
- TACACS+ 설정
- 사용자 작업 내용 기록 설정
- 시스템 사용자 인증 초기화



주 의

사용자 인증 프로토콜인 RADIUS나 TACACS+를 활성화 하려면 「user add」 명령어를 사용하여 「user」라는 읽기 전용 사용자를 추가하십시오. 그렇지 않으면 사용자 인증 프로토콜을 통해 접속하는 모든 사용자에게 「root」의 권한이 주어지게 됩니다. 읽기 전용 사용자 추가 방법은 「시스템 접속」 메뉴얼을 참고하십시오.

4.5.1. 사용자 인증 방법 설정

V5812G는 사용자 인증 방법으로, 기존의 장비에 등록되어 있는 사용자 ID와 패스워드를 사용하여 접속 권한 여부를 확인하는 방법과 RADIUS, 그리고 TACACS+를 사용할 수 있습니다. 이 세 가지 방법을 모두 설정하여 사용할 수도 있고, 그 중에서 선택하여 사용할 수도 있습니다.

사용자 인증 방법을 설정하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
login local {radius tacacs host all}	Global	콘솔을 통해 접속하는 사용자의 인증 방법을 설정합니다.
login remote {radius tacacs host all}		원격 접속 사용자의 인증 방법을 설정합니다.



참 고

「host」는 장비에 등록되어 있는 사용자 ID와 패스워드를 이용한 접속 방법입니다. V5812G는 기본적으로 이 방법을 사용하도록 설정되어 있습니다.

한편, 설정한 사용자 인증 방법을 해제하는 경우에는 다음 명령어를 사용합니다.

명령어	모 드	기 능
no login local {radius tacacs host all}	Global	콘솔을 통해 접속하는 사용자에 대해 설정했던 인증 방법을 해제합니다.
no login remote {radius tacacs host all}		원격 접속 사용자에 대해 설정했던 인증 방법을 해제합니다.

4.5.2. 사용자 인증 인터페이스 지정

두 개 이상의 인터페이스 또는 IP 주소가 설정된 V5812G에서 RADIUS 또는 TACACS 방식의 인증을 사용하는 경우에는 사용자가 인증 서버로 전송되는 패킷의 송신지를 특정 인터페이스 또는 IP 주소로 지정할 수 있습니다. 사용자 인증 인터페이스를 지정하시려면 다음 명령을 사용하십시오.

명령어	모 드	기 능
login {radius tacacs} interface <i>interface-name [ip-address]</i>	Global	사용자 인증 인터페이스 및 IP 주소를 지정합니다.

사용자 인증 인터페이스로 지정했던 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no login {radius tacacs} interface	Global	사용자 인증 인터페이스를 해제합니다.

4.5.3. 사용자 인증 방법 우선 순위 설정

사용자 인증 방법을 여러 가지로 설정해 두었다면, 어떤 방법부터 차례대로 인증 절차를 거칠지 그 순서를 설정할 수 있습니다. 시스템 사용자 인증 방법에 우선 순위를 설정하여 인증 절차의 순서를 정하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
login local {radius tacacs host} primary	Global	콘솔을 통해 접속하는 사용자에 대한 인증 방법의 우선 순위를 설정합니다.
login remote {radius tacacs host} primary		원격 접속 사용자에 대한 인증 방법에 우선 순위를 설정합니다.



참 고

V5812G의 사용자 인증 방법은 기본적으로 「host → radius → tacacs」의 순서로 설정되어 있습니다.

4.5.4. 사용자 인증 방법 설정 내용 확인

V5812G에 사용자 인증 방법을 설정한 후 설정 내용을 확인할 수 있습니다. 사용자 인증 방법과 관련된 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show login	Enable / Global	사용자 인증 방법과 관련된 설정 내용을 확인합니다.

4.5.5. RADIUS 설정

(1) RADIUS 서버 설정

시스템 사용자 인증 방법으로 RADIUS를 설정하였다면, 가장 먼저 사용자의 장비에서 사용할 RADIUS 서버를 설정해야 합니다. RADIUS 서버를 설정하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
login radius server ip-address key	Global	사용자의 장비에서 사용하게 될 RADIUS 서버의 IP 주소와 Key 값을 등록합니다.
login radius server ip-address key auth_port port-number acct_port port-number	Global	인증 포트와 Accounting 포트도 함께 RADIUS 서버를 등록합니다.



auth_port와 **acct_port** 다음에 입력하는 *port-number*는 UDP 포트 번호로 입력합니다.



V5812G는 RADIUS 서버를 최대 5개까지 등록할 수 있습니다.

한편, 등록했던 RADIUS 서버를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no login radius server ip-address	Global	등록했던 RADIUS 서버를 삭제합니다.

(2) RADIUS 서버 우선 순위 설정

V5812G는 최대 5개까지의 RADIUS 서버를 등록할 수 있습니다. 복수의 RADIUS 서버를 등록했을 때에는 서버의 우선 순위를 설정하여 사용할 수 있습니다. RADIUS 서버의 우선 순위를 설정해 놓으면, 우선 순위가 높은 서버를 먼저 사용하게 됩니다. 우선 순위는 숫자가 작을수록 큽니다.

RADIUS 서버에 우선 순위를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>login radius server move ip-address priority</code>	Global	RADIUS 서버의 우선 순위를 설정합니다.



우선 순위는 1부터 5까지 설정할 수 있습니다.

(3) 재전송 시도 횟수 설정

RADIUS 서버에 사용자 인증을 위해 접속자에 대한 정보를 보냈을 때 아무런 응답이 없을 경우에는 재전송을 하게 됩니다. 기본적으로는 3번의 재전송 시도를 하도록 설정되어 있지만, 사용자의 요구에 따라 재전송 시도 횟수를 지정할 수 있습니다. 재전송 시도 횟수를 설정하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>login radius retransmit count</code>	Global	사용자 인증을 위해 정보를 재전송하는 횟수를 설정합니다.



재전송 시도 횟수는 1번부터 10번까지 설정할 수 있습니다.



V5812G는 기본적으로 재전송 시도 횟수가 3번으로 설정되어 있습니다.

재전송 시도 횟수를 설정했던 것을 삭제하고 기본 설정값으로 돌아가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no login radius retransmit	Global	RADIUS 서버에 사용자 인증을 위해 정보를 재전송하는 횟수를 기본 설정값으로 되돌립니다.

(4) 응답 시간 제한

V5812G는 사용자 인증을 위해 RADIUS 서버에 접속자의 정보를 보낸 후 서버로부터의 응답을 기다리는 시간이 설정되어 있습니다. 사용자는 이 응답 시간을 사용자의 요구에 따라 설정할 수 있습니다.

서버 응답 시간을 제한하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
login radius timeout time	Global	RADIUS 서버로부터의 응답을 기다리는 시간을 설정합니다.



응답 시간은 1초부터 100초까지 설정할 수 있습니다.



V5812G는 기본적으로 응답 시간이 3초로 제한되어 있습니다.

RADIUS 서버로부터의 응답을 기다리는 시간을 기본 설정값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no login radius timeout	Global	RADIUS 서버로부터의 응답을 기다리는 시간을 기본 설정값으로 되돌립니다.

4.5.6. TACACS+ 설정

(1) TACACS 서버 설정

시스템 사용자 인증 방법으로 TACACS+를 설정하였다면, 가장 먼저 사용자의 장비에서 사용할 TACACS 서버를 설정해야 합니다.

TACACS 서버를 설정하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
login tacacs server ip-address key	Global	사용자의 장비에서 사용하게 될 TACACS 서버의 IP 주소와 Key 값을 등록합니다.



V5812G는 TACACS 서버를 최대 5개까지 등록할 수 있습니다.

한편, 장비에 등록한 TACACS 서버를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no login tacacs server [ip-address]	Global	등록했던 TACACS 서버를 삭제합니다.

사용자의 장비와 연결되어 있는 TACACS 서버의 포트를 등록하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
login tacacs socket-port port-number	Global	사용자의 장비와 연결되어 있는 TACACS 서버의 포트를 등록합니다.

사용자가 등록한 TACACS 서버의 포트를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no login tacacs socket-port	Global	사용자가 등록한 TACACS 서버의 포트를 삭제합니다.

사용자의 장비와 연결돼 있는 TACACS 서버의 인터페이스를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
login tacacs interface interface-name [ip-address]	Global	사용자의 장비와 연결되어 있는 TACACS 서버의 인터페이스를 등록합니다.
no login tacacs interface		등록된 인터페이스를 삭제합니다.

(2) TACACS 서버 우선 순위 설정

V5812G는 최대 5개까지의 TACACS 서버를 등록할 수 있습니다. 복수의 TACACS 서버를 등록했을 때에는 서버의 우선 순위를 설정하여 사용할 수 있습니다. TACACS 서버의 우선 순위를 설정해 놓으면, 우선 순위가 높은 서버를 먼저 사용하게 됩니다. 우선 순위는 숫자가 작을수록 큽니다.

명령어	모 드	기 능
login tacacs server move ip-address priority	Global	TACACS 서버의 우선 순위를 설정합니다.



우선 순위는 1부터 5까지 설정할 수 있습니다.

(3) 인증 방식 설정

V5812G의 사용자 인증 방법을 TACACS+로 설정하였다면, TACACS+의 인증 방식을 선택하십시오. PAP(Password Authentication Protocol)은 TACACS+에서 사용하는 기본적인 인증 방식이며, CHAP(Challenge Handshake Authentication Protocol)은 보안이 한 층 더 강화된 인증 방식입니다. TACACS+의 인증 방식을 설정하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
login tacacs auth-type {ascii pap chap}	Global	TACACS+의 인증 방식을 선택합니다.



V5812G는 기본적으로 TACACS+의 인증 방식이 「**ascii**」로 설정되어 있습니다.

설정한 TACACS+의 인증 방식을 기본 설정값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no login tacacs auth-type	Global	설정한 TACACS+의 인증 방식을 기본 설정값으로 되돌립니다.

(4) 응답 시간 제한

V5812G는 사용자 인증을 위해 TACACS 서버에 접속자의 정보를 보낸 후 서버로부터의 응답을 기다리는 시간이 설정되어 있습니다. 사용자는 이 응답 시간을 사용자의 요구에 따라 설정할 수 있습니다. 서버 응답 시간을 제한하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
login tacacs timeout time	Global	TACACS 서버로부터의 응답을 기다리는 시간을 설정합니다.



응답 시간은 1초부터 100초까지 설정할 수 있습니다.



V5812G는 기본적으로 응답 시간이 5초로 제한되어 있습니다.

서버 응답 시간을 기본 설정값으로 되돌리려면, Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no login tacacs timeout	Global	서버 응답 시간을 기본 설정값으로 되돌립니다.

(5) 사용자 권한 범위 지정

V5812G는 TACACS 서버의 권한 수준 설정에 따라 시스템 사용자의 권한 범위를 지정할 수 있습니다. 이 권한 설정은 V5812G에서의 설정만으로는 의미가 없으며 사용자가 접속하는 TACACS 서버에서 권한 범위 설정을 별도로 해주어야 적용됩니다.

예를 들어, 사용자의 장비에서 어떠한 사용자 ID에 「user」라는 수준의 권한 설정을 해주었다면 TACACS 서버에서는 「user」와 동일한 이름의 설정을 등록하고, 그에 대한 권한 범위를 설정해주어야 합니다. 권한 수준을 비교해보면 「max > user > min」입니다.

시스템 사용자의 권한 수준을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
login tacacs priority-level {max min root user}	Global	TACACS 서버 사용자의 권한 범위를 지정합니다.



V5812G는 기본적으로 시스템 사용자의 권한 범위가 「min」으로 설정되어 있습니다.

시스템 사용자의 범위를 기본 설정값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no login tacacs priority-level	Global	사용자의 권한 범위를 기본 설정값으로 되돌립니다.

4.5.7. 사용자 작업 내용 기록

V5812G는 사용자 인증 방법으로 RADIUS나 TACACS+를 선택하면 회선 사용자가 특정 서비스를 이용한 내용을 기록할 수 있습니다. 이러한 기능을 이용하면 특별한 경우, 특정한 서비스에 대해 과금 정책을 적용할 수도 있습니다.

사용자가 작업한 내용을 기록하는 기능을 활성화 하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
login accounting-mode {none start stop both}	Global	사용자의 장비에 과금 정책을 적용합니다.



「start」은 사용자가 어떠한 프로세스를 시작하는 시점을 로그에 기록하는 것이고, 「stop」은 사용자가 프로세스를 종료하는 시점을 로그에 기록하는 것입니다. 또한 「both」는 프로세스의 시작 시점과 종료 시점을 모두 기록하는 것이고, 「none」은 해당 기능을 해제하는 것입니다.

사용자가 작업한 내용을 기록하도록 설정한 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no login accounting-mode	Global	사용자가 작업한 내용을 기록하도록 설정한 것을 해제합니다.

4.5.8. 시스템 사용자 인증 초기화

시스템 사용자 인증에 대한 모든 설정을 초기화 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no login	Global	시스템 사용자 인증에 대한 모든 설정을 초기화합니다.

5. 포트 기본 설정

사용자는 V5812G 포트의 Auto-negotiate, 전송 속도, Flow-control 등의 기본 환경을 설정할 수 있습니다. 포트 기본 설정에서는 사용자가 V5812G 포트의 기본 환경을 설정하는 방법뿐만 아니라 포트 미러링 기능을 설정하는 방법에 대해서도 설명합니다.

5.1 포트 기본 환경 설정

사용자는 포트 상태, 속도 등의 기본 환경을 설정할 수 있습니다. 포트 설정을 위해서는 Global 설정 모드에서 **bridge** 명령어를 입력, Bridge 설정 모드로 들어가야 합니다.

다음은 V5812G의 이더넷 포트에 기본적으로 설정되어 있는 내용입니다.

내 용	기 본 설 정
포트상태	동작 가능
Auto-negotiate	ON
Duplex mode	Full duplex mode
플로우 컨트롤	On
STP	VLAN 1에 대해 설정
VLAN	default

한편, 사용자 장비 포트가 어떤 상태로 설정되어 있는지 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show port	Enable/Global/Bridge	모든 포트의 상태를 확인합니다.
show port port-number		특정 포트의 상태를 확인할 수 있습니다.

포트 기본 환경 설정과 관련하여 다음과 같은 내용을 설명합니다.

- 포트 활성화
- Auto nego 설정
- 포트 속도 설정
- duplex 모드 설정
- Flow Control 설정
- 포트 설명하기
- 포트 통계 확인

5.1.1. 포트 활성화

케이블이 연결되어 물리적으로는 활성화 상태인 포트를 논리적으로 비활성화 상태로 만들 수 있습니다. 활성화 상태인 포트를 비활성화 상태로 설정하거나 비활성화 상태로 설정했던 포트를 다시 활성화 시키려면 Bridge 설정 모드에서 다음과 같은 명령어를 사용하십시오.

명령어	모 드	기 능
port enable port-number	Bridge	포트를 활성화 상태로 설정합니다.
port disable port-number		포트를 비활성화 상태로 설정합니다.



기본적으로 V5812G는 모든 포트가 논리적으로 활성화인 상태로 설정되어 있습니다.

5.1.2. 포트 타입 지정

사용자는 다음 명령어로 네트워크 서비스가 제공될 포트의 타입을 지정할 수 있습니다.

명령어	모 드	기 능
port medium port-number {sfp rj45}	Bridge	포트의 타입을 지정합니다.
show port medium	Enable / Global / Bridge	포트의 타입을 확인합니다.

5.1.3. Auto Nego 설정

사용자는 V5812G의 포트가 연결된 장비의 전송 속도와 duplex 모드에 맞추어 동작하는 Auto nego 기능을 설정할 수 있습니다. 전송 속도와 duplex 모드를 연결 장비에 맞출 수 있도록 하는 Auto nego 기능을 설정하는 명령어는 다음과 같습니다.

명령어	모 드	기 능
port nego port-number on	Bridge	자동 조절 기능을 설정합니다.
port nego port-number off		자동 조절 기능을 해제합니다.



주의

100/1000BASE-X 포트는 Auto nego에 대한 설정이 불가능합니다.



주의

auto-nego 기능이 「on」으로 설정되지 않은 포트는 Auto MDIX를 지원하지 않습니다.

5.1.4. 포트 속도 설정

V5812G는 각 포트의 전송 속도를 설정할 수 있습니다. V5812G 포트의 전송 속도를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port speed port-number {10 100 1000}	Bridge	포트 전송 속도를 10,100, 또는 1000Mbps로 설정합니다.



주의

1000BASE-X 의 Gigabit 포트는 Speed 설정을 할 수 없습니다.

5.1.5. duplex 모드 설정

스위치는 half duplex 모드에서 단 방향 통신만 가능하고, full duplex 모드에서는 패킷을 동시에 주고 받는 쌍방향 통신이 가능합니다. 패킷을 쌍방향으로 전달하면 10Mbps는 20Mbps로 100Mbps는 200Mbps로 이더넷 대역폭이 두 배로 확장됩니다.

이더넷 포트의 duplex 모드를 설정하려면, Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port duplex port-number {full half}	Bridge	포트의 duplex 모드를 설정합니다.



주의

100BASE-FX 이더넷과 1000BASE-X 기가비트 이더넷은 Full duplex 만 가능합니다. 사용자는 100BASE-FX와 기가비트 이더넷 포트에 대해 duplex 모드를 변경할 수 없습니다.

5.1.6. Flow Control 설정

V5812G의 이더넷 포트는 일정 시간 동안 패킷 전송을 제한하기 위해 전송 중지 신호를 보냅니다. 일반적으로 수신 버퍼에 여유 공간이 없으면 포트는 송신 포트에게 일정 시간동안 패킷 전송을 중단하라는 「중지」 메시지를 보냅니다. 이더넷 포트 역시 다른 시스템으로부터 「중지」 메시지를 받으면 일정 시간 동안 패킷 전송을 중단합니다. 이더넷 포트에 전송 중지 신호를 설정 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port flow-control port-number {on off}	Bridge	전송 중지 신호를 보내는 기능을 설정합니다.



참 고

V5812G의 포트는 기본적으로 Flow-control이 “off”로 설정되어 있습니다.

5.1.7. 포트 설명하기

V5812G는 각 포트에 대한 설명을 등록하여 사용자가 관리하기 편리하게 하였습니다. 각 포트에 대한 설명을 등록하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port description port-number description	Bridge	포트에 대한 설명을 등록합니다.

각 포트에 등록된 설명을 보려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show port description port-number	Enable /Global/Bridge	포트에 등록된 설명을 확인합니다.

한편, 포트에 등록한 설명을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no port description port-number	Bridge	포트에 대한 설명을 삭제합니다.

5.1.8. 트래픽 통계 확인

(1) 포트 패킷 통계

V5812G의 사용자는 각 포트의 평균적인 트래픽이나 SNMP MIB에 정의된 interface MIB, RMON MIB 데이터를 확인할 수 있습니다.

V5812G 각 포트의 평균 트래픽, SNMP MIB에 정의된 interface MIB, RMON MIB 데이터를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show port statistics avg-pkt [port-number]	Enable	지정 포트의 평균 트래픽을 확인합니다.
show port statistics avg-pps [port-number]	Global	패킷 종류에 따른 트래픽 통계를 확인합니다.
show port statistics interface [port-number]	Bridge	지정한 포트의 인터페이스 MIB 데이터를 확인합니다.
show port statistics rmon [port-number]		지정한 포트의 RMON MIB 데이터를 확인합니다.



주의

GPON 포트가 설치된 SIU_GPON4 포트의 경우 위의 명령어를 사용하면, SFU의 내부적인 포트에 대한 정보가 보입니다. GPON 포트에 대한 정보 확인은 G-PON 설정 모드에서 할 수 있습니다.

포트에 기록된 통계를 초기화하려면 Global 설정 모드에서 clear 명령어를 사용하십시오. 모든 포트의 통계를 초기화할 수도 있고, 원하는 포트를 선택하여 초기화할 수도 있습니다. 다음은 포트 통계를 초기화할 때 사용하는 명령어입니다.

명령어	모 드	기 능
clear port statistics { port-number all}	Enable/ Global/ Bridge	포트 통계를 초기화합니다. 원하는 포트는 여러 개 선택할 수 있습니다.

(2) 프로토콜별 통계

프로토콜별로 트래픽 통계를 확인할 수 있습니다. ARP, ICMP, IP, TCP, UDP의 프로토콜별 트래픽 통계를 확인하려면, 다음 방법을 사용하십시오.

1 단계 프로토콜별로 트래픽 통계를 확인하는 기능을 활성화합니다.

명령어	모 드	기 능
protocol statistics enable [arp icmp ip tcp udp]	Global	프로토콜별 트래픽 통계를 활성화합니다.

2 단계 프로토콜별 트래픽 통계를 확인합니다. 프로토콜별 트래픽 통계를 확인하는 명령어는 다음과 같습니다.

명령어	모 드	기 능
show protocol statistics avg-pkt [port-number]	Enable/ Global/ Bridge	프로토콜별 평균 트래픽 통계를 확인합니다.
show protocol statistics total [port-number]	Bridge	프로토콜별 전체 트래픽 통계를 확인합니다.

프로토콜별 트래픽 통계를 확인하는 기능을 해제하려면, 다음 명령어를 사용하십시오.

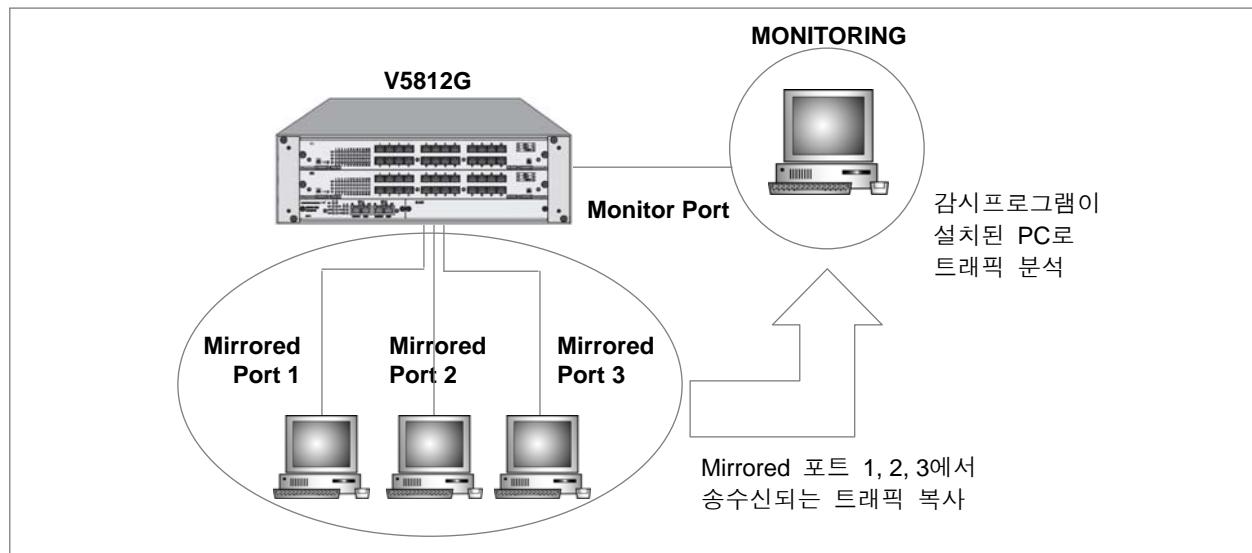
명령어	모 드	기 능
protocol statistics disable [arp icmp ip tcp udp]	Global	프로토콜별 트래픽 통계를 해제합니다.

프로토콜별 트래픽 통계를 초기화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear protocol statistics [port-number]	Global Bridge	지정 포트의 프로토콜 평균 트래픽을 삭제합니다.

5.2 포트 미러링 설정

포트 미러링(Port Mirroring)은 지정된 하나의 포트에서 모니터링 대상으로 지정된 포트를 모니터링 할 수 있는 기능입니다. 이 때, 모니터링을 하는 포트를 「Monitor 포트」라고 하고, 모니터링 대상이 되는 포트를 「Mirrored 포트」라고 합니다. 포트 미러링의 원리는 Mirrored 포트에서 송수신이 이루어지는 패킷을 Monitor 포트로 복사하여 네트워크 트래픽을 모니터링할 수 있도록 하는 것입니다. 다음 그림은 포트 미러링 기능을 설정하여 트래픽을 분석하기 위한 네트워크 연결 예입니다. Mirrored 포트와 Monitor 포트를 설정하고, Monitor 포트로 설정된 포트에 감시프로그램이 설치된 컴퓨터를 연결하여 장비의 트래픽 및 네트워크 상태를 분석합니다.



【 그림 5-1 】 포트 미러링의 예

(주)다산네트웍스 장비에 포트 미러링을 설정하려면, 모니터링 대상이 되는 Mirrored 포트와 모니터링을 담당하는 Monitor 포트를 지정하고, 포트 미러링 기능을 활성화시키십시오. 물론, Monitor 포트는 감시 프로그램이 설치된 PC와 연결해야 합니다. 동일 장비에 Monitor 포트는 오직 한 개만 지정할 수 있고, Mirrored 포트는 하나 이상 지정할 수 있습니다.

5.2.1. Monitor 포트와 Mirrored 포트 지정

포트 미러링 기능을 설정하려면 모니터링을 담당할 Monitor 포트와 모니터링 대상이 되는 Mirrored 포트를 지정해야 합니다. Monitor 포트와 Mirrored 포트를 지정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
mirror monitor port-number	Bridge	Monitor 포트를 지정합니다.
mirror monitor cpu		장비의 CPU에서 모니터링 하도록 설정합니다.
mirror add port-number [ingress egress]		Mirrored 포트를 지정합니다.



참 고

2개 이상의 Mirrored 포트를 지정할 때, port-number는 「,」나「-」기호를 사용하여 입력하실 수 있습니다.



주 의

Mirrored 포트의 트래픽을 장비의 CPU가 모니터링 하도록 설정하면 CPU에 많은 부하를 야기하게 할 수 있습니다.

한편, Monitor 포트를 해제하거나 모니터링 대상이 되었던 포트를 대상에서 삭제하려면, Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no mirror monitor	Bridge	Monitor 포트를 해제합니다.
mirror del port-number [ingress egress]		모니터링 대상 포트를 삭제합니다.

5.2.2. 포트 미러링 활성화

포트 미러링 기능을 가능하게 하기 위해서는 포트 미러링을 활성화시켜야 합니다. 포트 미러링 기능을 활성화시키기 위해서는 Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
mirror enable	Bridge	포트 미러링 기능을 활성화합니다.

한편, 포트 미러링 기능을 해제하기 위해서는 Bridge 설정 모드를 사용하여 다음 명령어를 사용하여 포트 미러링을 비활성화 시켜야 합니다.

명령어	모 드	기 능
mirror disable	Bridge	포트 미러링 기능을 해제합니다.



주의

데이터 분석이 끝나면 반드시 Mirrored 포트를 delete하거나, Mirroring 포트를 disable 해주는 것을 권장합니다. Mirroring 기능을 장시간 사용하면 CPU에 부담을 주기 때문에, 장비의 패킷 처리 속도가 늦어질 수 있습니다.

5.2.3. 포트 미러링 설정 내용 확인

사용자가 포트 미러링 기능에 대한 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show mirror	Enable/Global/Bridge	포트 미러링 설정 내용을 확인합니다.

6. 시스템 환경

시스템 환경에서는 시스템의 Host name, 시간 등을 설정하는 방법과 설정 내용을 관리하는 방법 등에 대해 설명합니다.

6.1 환경 설정

V5812G의 시스템 환경 설정에 대해 다음과 같은 내용을 설명합니다.

- Host name 설정
- 날짜 및 시간 설정
- Time-zone 설정
- NTP 설정
- SNTP 설정
- NTP 메시지 주소 설정
- 터미널 스크린 출력 상태 설정
- DNS 서버 설정
- 로그인 배너 설정
- FAN 동작 설정
- 데몬 강제 종료
- FTP 서버 활성화
- FTP 클라이언트 주소 설정
- Module DMI 정보 출력 설정
- 시스템 임계값 설정

6.1.1. Host name 설정

프롬프트(prompt) 상태에서 출력되는 Host name은 네트워크에 연결된 각 장비를 서로 구분하기 위해 필요합니다.

V5812G의 Host name을 설정하거나 변경하려면 Global 설정 모드에서 “**hostname**” 명령어를 사용하십시오.

명령어	모 드	기 능
hostname name	Global	사용자 장비의 호스트 이름을 입력한 이름으로 변경합니다.



참 고

명령어 뒤에 입력해야 하는 변수 “name”은 사용자가 부여하는 장비의 새로운 이름입니다. 이 이름은 대, 소문자를 구분합니다.



참 고

공장에서 출하된 V5812G에는 Hostname이 기본적으로 “SWITCH”로 설정되어 있습니다.

한편 설정한 호스트 이름을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no hostname name	Global	설정한 호스트 이름을 삭제합니다.

6.1.2. 날짜 및 시간 설정

V5812G는 장비에 현재 시각과 날짜를 설정하거나 변경할 수 있습니다. V5812G의 시각과 날짜를 변경하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clock datetime	Enable/Global	사용자 장비에 현재 시간과 날짜를 설정, 변경합니다.

한편, 시스템에 설정된 날짜와 시간을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show clock	Enable/Global/Bridge	사용자 장비에 설정된 현재 시간과 날짜를 확인합니다.

6.1.3. Time-zone 설정

사용자는 장비에 Time-zone을 설정할 수 있습니다. 설정하기 전에 사용자가 지정할 수 있는 Time-zone의 종류를 확인하십시오.

사용자가 지정할 수 있는 Time-zone을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show time-zone	View/Enable/Global	Time-zone의 종류를 보여줍니다.



참 고

“**show time-zone**” 명령어는 Time-zone의 종류만 알려줍니다. Time-zone에 대한 설정 내용을 확인하려면 “**show clock**” 명령어를 사용하십시오.

다음은 사용자가 설정할 수 있는 Time-zone의 종류 가운데 GMT 시각에 속하는 주요 국가 및 지역을 나타낸 표입니다.

【 GMT 시각 】

Time-zone	국 가	Time-zone	국 가	Time-zone	국 가
GMT-12	에니وي톡	GMT-3	리오네자네이로	GMT+6	랑군
GMT-11	사모아	GMT-2	메릴랜드	GMT+7	방콕, 싱가포르
GMT-10	하와이, 호놀룰루	GMT-1	아조레스	GMT+8	홍콩, 북경
GMT-9	알라스카	GMT+0	런던, 리스본	GMT+9	서울, 동경
GMT-8	LA, 시애틀	GMT+1	베를린, 로마	GMT+10	시드니, 멜버른
GMT-7	덴버	GMT+2	카이로, 아테네	GMT+11	오크לנד
GMT-6	시카고, 달拉斯	GMT+3	모스크바	GMT+12	웰링턴
GMT-5	뉴욕, 마이애미	GMT+4	테헤란		
GMT-4	조지타운	GMT+5	뉴델리		

V5812G에 Time-zone을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
time-zone time-zone	Global	장비에 Time-zone을 설정합니다.



주 의

Time-zone을 변경하면 해당하는 time-zone에 맞춰 날짜와 시간도 변경됩니다. 따라서 Time-zone을 변경한 후에는 다시 한 번 날짜와 시간을 변경하여 주십시오.



참 고

공장에서 출하된 제품에는 기본적으로 세계 협정 시간을 나타내는 UTC(Universal Coordinated Time)로 설정되어 있습니다.

설정한 Time-zone의 내용을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear time-zone	Global	설정한 Time-zone의 내용을 삭제합니다.

한편, 일시 및 Time-zone의 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show clock	Enable/Global/Bridge	사용자가 설정한 장비의 일시 및 Time-zone을 보여줍니다.

다음은 서울의 Time-zone에서 일시를 2002년 12월 13일 오후 16시 14분으로 설정하고, 그 내용을 확인하는 경우입니다.

```
SWITCH(config)# time-zone GMT+9
SWITCH(config)# clock 121316142002
Fri, 13 Dec 2002 16:14:10 GMT+0900
SWITCH(config)# show clock
Fri, 13 Dec 2002 16:14:10 GMT+0900
SWITCH(config)#

```

6.1.4. NTP 설정

NTP(Network Time Protocols)는 네트워크 상의 정확한 시간을 보장할 수 있도록 사용자 장비의 시간을 1/1000초까지 세밀하게 맞추는데 사용합니다. NTP 서버와 끊임없이 메시지를 주고 받으면서 현재 시간에 계속해서 수렴해 나감으로써 사용자 장비의 시간이 맞춰집니다.

장비가 올바르게 작동하기 위해서라도 정확한 시간을 맞추는 것은 매우 중요합니다. NTP에 대한 자세한 설명은 STD와 RFC 1119에서 볼 수 있습니다.

다음은 NTP 서버를 등록하고, 사용자의 장비에 NTP가 작동하도록 설정하고, 내용을 확인할 때 사용하는 명령어입니다.

명령어	모 드	기 능
ntp server 1 [server 2] [server 3]	Global	사용자 장비에 NTP 서버를 등록합니다.



참 고

NTP 서버는 최대 3개까지 등록할 수 있습니다.

NTP 서버는 공식적으로 사용하고 있는 NTP 서버나 자체적으로 사용하는 NTP 서버를 모두 사용할 수 있는데, NTP 서버의 IP 주소나 도메인 이름을 입력하면 됩니다. 우리나라에서 공식적으로 사용하고 있는 NTP 서버로는 「time.nuri.net」으로 IP 주소는 「203.255.112.96」입니다.

등록했던 NTP 서버를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ntp server 1 [server 2] [server 3]	Global	사용자 장비에 등록했던 NTP 서버를 삭제합니다.

NTP 기능을 해제하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ntp	Global	사용자 장비에서 NTP 기능을 해제합니다.

NTP에 대한 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ntp	Enable/Global/Bridge	NTP 설정을 확인합니다.

[설정 예제]

다음은 203.255.112.96을 NTP 서버로 설정하고 NTP 기능을 작동한 후 설정 여부를 확인하는 경우의 예입니다.

```
SWITCH(config)# ntp 203.255.112.96
SWITCH(config)# show ntp
=====
ntp is running.
=====
Time Servers
-----
1st : 203.255.112.96
=====
SWITCH(config)#

```

다음은 NTP 기능을 해제하고, 해제 여부를 확인하는 경우입니다.

```
SWITCH(config)# no ntp
SWITCH(config)# show ntp
=====
ntp isn't running.
=====
SWITCH(config)#

```

6.1.5. SNTP 설정

SNTP(Simple Network Time Protocol)는 NTP (Network Time Protocol)와 마찬가지로 정확한 시간을 보장하기 위해 사용되는 것으로, 이더넷 타임 서버의 UDP 타임 패킷을 사용하는 TCP/IP 프로토콜입니다. 그러나, 이 두 가지 프로토콜은 서버를 통해 클라이언트가 시간을 조절하는데 사용하는 알고리즘이 서로 다릅니다. NTP는 정확한 시간을 제공하기 위해 여러 개의 타임 서버를 사용하여 시간을 맞춥니다. 여러 개의 타임 서버 가운데 다른 서버와 시간이 틀린 서버를 구별해 냄으로써 현재 시간이 정확한지 아닌지를 확인합니다. 그리고 PC와 서버의 시간 편차를 조절하여 PC의 시간을 정확하게 맞춥니다. NTP를 사용하여 맞춰진 시간은 변함없이 계속 유지됩니다.

한편, SNTP는 NTP와는 달리 시간을 맞추기 위해 오직 하나의 이더넷 타임 서버를 사용합니다. 그리고, SNTP는 타임 서버를 통해 시간이 새롭게 맞춰질 때마다 시간을 업데이트하기 때문에 시간이 갑자기 변할 수 있습니다. 클라이언트가 사용하는 타임 서버에 문제가 발생하였을 때에는 Back-up 서버가 사용되는데, 이와 같이 SNTP는 Back-up 서버를 설정해 둘 수가 있고, 여러 개의 Back-up 서버는 서버의 우선 순위에 따라 순서대로 대체됩니다.

하나의 이더넷 타임 서버를 통해 시간을 조절하는 SNTP에 비해 여러 개의 서버를 사용하는 NTP는 알고리즘이 더욱 복잡합니다. 따라서, NTP를 사용하여 시간을 맞추는 것 보다 SNTP를 사용했을 때 보다 더 신속합니다.

V5812G에 SNTP를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
sntp first-server [second-server] [third-server]	Global	SNTP 서버를 등록합니다.



V5812G는 SNTP 서버를 최대 3개까지 등록할 수 있습니다.



SNTP 서버는 등록하는 순서대로 서버의 우선 순위가 결정됩니다. *second-server*는 *first-server*에 문제가 발생하였을 때 사용되는 서버이고, *third-server*는 *second-server*에도 문제가 발생하였을 때 사용되는 서버입니다.

등록했던 SNTP 서버를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no sntp server 1 [server 2] [server 3]	Global	사용자 장비에 등록했던 SNTP 서버를 삭제합니다.

SNTP 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no sntp	Global	SNTP 기능을 해제합니다.

SNTP에 대한 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show sntp	Enable/Global/Bridge	SNTP 설정을 확인합니다.

다음은 203.255.112.96의 IP 주소를 가진 SNTP 서버를 등록하고, 동작을 활성화시키는 경우입니다.

```
SWITCH(config)# sntp 203.255.112.96
SWITCH(config)# show sntp
=====
sntp is running.
=====
Time Servers
-----
1st : 203.255.112.96
=====
SWITCH(config)#

```

6.1.6. NTP 메시지 주소 설정

사용자 장비의 시간을 정확히 맞추기 위해 NTP 서버를 등록하였다면, 사용자의 장비와 NTP 서버는 끊임없이 메시지를 주고 받으면서 현재 시간에 계속하여 수렴해 나감으로써 장비의 시간이 맞춰지게 됩니다. 이 때, NTP 서버와 주고받는 메시지가 가지게 되는 임의의 IP 주소를 설정할 수 있습니다. 이 IP 주소는 NTP 서버가 사용자의 장비를 구별할 수 있도록 도와주게 됩니다. NTP 서버와 메시지를 주고받을 때 메시지가 가지게 되는 IP 주소를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ntp bind-address ip-address	Global	NTP 서버와 메시지를 주고받을 때 메시지가 가지게 되는 IP 주소를 설정합니다.

NTP 서버와 메시지를 주고받을 때 메시지가 가지게 되는 IP 주소를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ntp bind-address	Global	NTP 서버와 메시지를 주고받을 때 메시지가 가지게 되는 IP 주소를 삭제합니다.

6.1.7. 터미널 스크린 출력 상태 설정

V5812G는 기본적으로 콘솔 터미널 화면에 80자로 이루어진 행을 24개 출력합니다. 사용자는 **terminal length** 명령어를 사용하여 출력되는 행 수를 변경할 수 있습니다.

터미널 스크린에 출력할 행 수를 설정하려면 Privileged 모드에서 다음의 명령어를 사용하십시오.

명령어	모 드	기 능
terminal length<1-512>	Enable	터미널 스크린에 출력되는 행수를 설정합니다.
terminal length 0		터미널 스크린에 출력되는 행수를 무제한으로 설정합니다.

다음은 터미널 스크린에 20행을 출력하도록 설정하는 예입니다.

```
SWITCH# terminal length 20
SWITCH#
```

터미널 스크린에 출력할 수 있는 행수를 설정했던 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no terminal length	Enable	터미널 스크린에 출력되는 행 수를 설정했던 것을 해제합니다.

6.1.8. DNS 서버 설정

V5812G는 telnet, ftp, tftp, ping 명령어를 사용할 때 IP 주소를 입력하는 대신 Hostname이나 URL을 입력하여 각각의 기능을 수행할 수 있습니다. 그러기 위해서 사용자는 장비에 DNS 서버를 입력하여야 합니다. DNS 서버를 입력하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
dns server server-ip-address	Global	사용자 장비에 DNS 서버를 등록합니다.

위의 명령어를 사용하여 DNS 서버를 입력하고, DNS 서버와 네트워크 상에서 연결이 이루어지면 telnet, ftp, tftp, ping 등의 명령어에서 IP 주소를 입력하는 대신 Hostname이나 URL을 입력할 수 있습니다.



참 고

이 기능은 사용자의 장비와 DNS 서버가 네트워크 상에서 연결되어 있어야 실행 가능합니다.

DNS 서버를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no dns server server-ip-address	Global	DNS 서버를 삭제합니다.

DNS 서버로 등록한 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show dns	Enable/Global/Bridge	사용자 장비에 등록된 DNS 서버를 확인합니다.

다음은 168.126.63.1이라는 주소를 DNS 서버로 등록하고 그 내용을 확인하는 경우입니다.

```
SWITCH(config)# dns server 168.126.63.1
SWITCH(config)# show dns
nameserver 168.126.63.1
SWITCH(config)#

```



참 고

위에서 등록한 DNS 서버는 예시를 보여주기 위해 입력한 것이며 실제로는 사용자가 사용하게 될 DNS 서버를 등록하셔야 합니다.

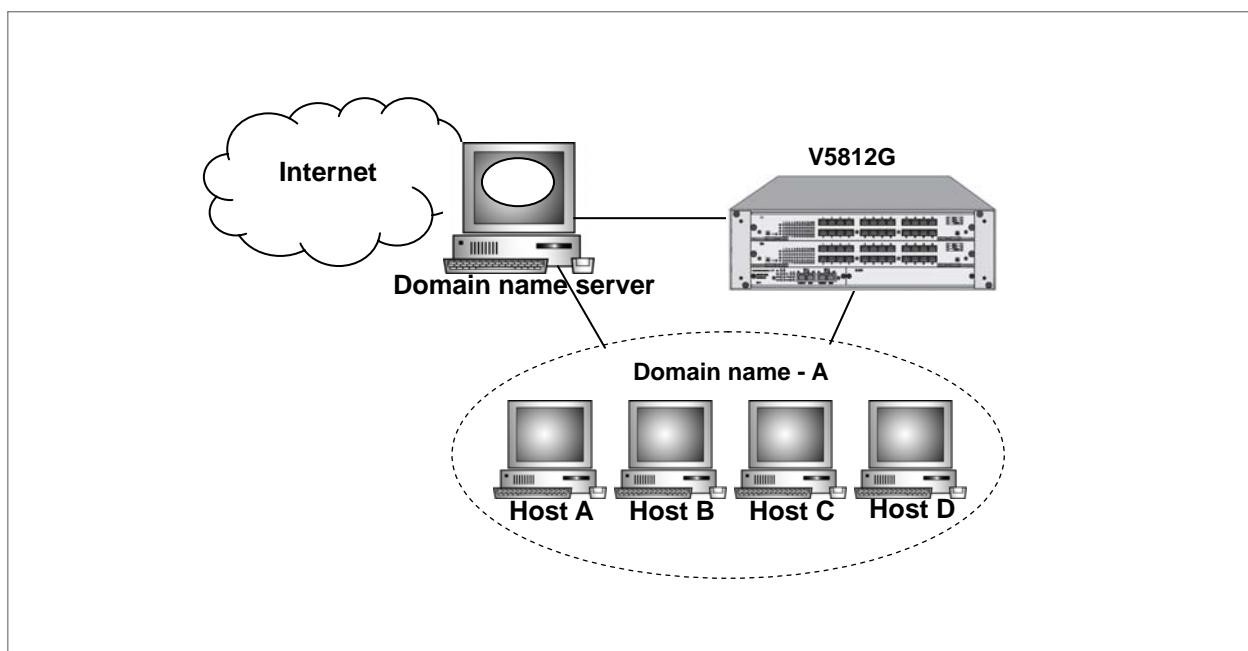
다음은 DNS 서버를 등록한 후 도메인 네임으로 Ping 테스트를 실행해 본 결과입니다.

```
SWITCH# ping da-san.com
PING da-san.com (203.236.124.3) from 203.236.124.248 : 56(84) bytes of data.
64 bytes from 203.236.124.3: icmp_seq=0 ttl=254 time=0.4 ms
64 bytes from 203.236.124.3: icmp_seq=1 ttl=254 time=0.3 ms
64 bytes from 203.236.124.3: icmp_seq=2 ttl=254 time=0.3 ms
64 bytes from 203.236.124.3: icmp_seq=3 ttl=254 time=0.3 ms
64 bytes from 203.236.124.3: icmp_seq=4 ttl=254 time=0.3 ms
64 bytes from 203.236.124.3: icmp_seq=5 ttl=254 time=0.2 ms
64 bytes from 203.236.124.3: icmp_seq=6 ttl=254 time=0.3 ms

--- da-san.com ping statistics ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.3/0.4 ms
SWITCH#
```

한편, V5812G는 특정 도메인 네임을 등록하면 해당하는 도메인 내부에 있는 호스트의 경우에는 IP 주소를 입력하지 않고 Hostname을 입력하고도 telnet, ftp, tftp, ping 명령어를 실행할 수 있습니다.

다음의 그림으로 예를 들면 V5812G에 Domain name “A”를 등록해 두면 A의 내부에 있는 Host A, B, C, D를 대상으로 telnet, ftp, tftp, ping 명령어를 실행할 때, IP 주소 대신에 Hostname을 입력할 수 있습니다.



【 그림 6-1 】 Domain name server

특정한 도메인 내부에 있는 호스트를 대상으로 telnet, ping 등을 실행시킬 때, IP 주소 대신 Hostname을 사용하도록 설정하려면 다음 명령어를 사용하여 도메인 네임을 등록하십시오.

명령어	모 드	기 능
dns search domain-name	Global	특정 도메인 네임을 등록합니다.

주 의

위의 기능은 사용자의 장비와 DNS 서버와 특정 도메인이 네트워크 상에서 연결되어 통신이 가능한 상태일 때 실행 가능합니다.

다음은 위의 그림의 도메인 “A”를 등록하고 Host “B”에 Ping 테스트를 실행할 때 IP 주소 대신 Hostname을 입력한 경우의 예입니다.

```
SWITCH(config)# dns search A
SWITCH# ping B
PING B.A (192.168.218.10) from 192.168.218.248 : 56(84) bytes of data.
 64 bytes from 192.168.218.10: icmp_seq=0 ttl=127 time=0.6 ms
 64 bytes from 192.168.218.10: icmp_seq=1 ttl=127 time=0.3 ms
 64 bytes from 192.168.218.10: icmp_seq=2 ttl=127 time=0.3 ms
 64 bytes from 192.168.218.10: icmp_seq=3 ttl=127 time=0.3 ms
 64 bytes from 192.168.218.10: icmp_seq=4 ttl=127 time=0.3 ms

--- B.A ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.4/0.6 ms
SWITCH#
```

위에서 입력한 A와 B는 하나의 예일 뿐입니다. 실제로 A에는 도메인네임, B에는 Hostname이 입력됩니다. 장비에 등록한 DNS 도메인 네임을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no dns search domain-name	Global	등록한 DNS 도메인 네임을 삭제합니다.

장비에 등록한 DNS 서버와 도메인 네임을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no dns	Global	DNS 서버와 도메인 네임을 삭제합니다.

6.1.9. 로그인 배너 설정

V5812G는 시스템 로그인 화면에 여러 가지 메시지를 등록하여 콘솔 터미널 프로그램을 통하여나 ftp, telnet을 통해 접속하는 사용자에게 로그인 하기 전이나 로그인 된 후, 그리고, 로그인에 실패했을 때 등록한 메시지를 전달할 수 있습니다. 이 기능을 이용하면 시스템 관리자가 다른 사람에게 주의 사항이나 전달 사항을 등록할 수 있게 됩니다.

시스템 로그인 화면에 메시지를 등록하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
banner	Global	시스템에 로그인 되기 전에 출력되는 메시지를 등록합니다.
banner login		시스템에 성공적으로 로그인했을 때 출력되는 메시지를 등록합니다.
banner login-fail		시스템 로그인에 실패했을 때 출력되는 메시지를 등록합니다.

시스템 로그인 화면에 등록한 메시지를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no banner	Global	시스템에 로그인 되기 전에 출력되는 메시지를 삭제합니다.
no banner login		시스템에 성공적으로 로그인했을 때 출력되는 메시지를 삭제합니다.
no banner login-fail		시스템 로그인에 실패했을 때 출력되는 메시지를 삭제합니다.

사용자가 등록한 로그인 배너를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show banner	Enable/Global	사용자가 등록한 로그인 배너를 확인합니다.

[설정 예제]

위의 명령어를 사용하여 메시지를 등록하는 방법은 다음과 같습니다.



참 고

다음은 “**banner**” 명령어의 경우를 예로 보여주고 있지만, 세 가지 명령어 모두 방법은 동일합니다.

```
SWITCH(config)# banner
```

```
Save & Exit : CTRL-D
```

Ctrl-D를 누르면 배너가 저장되면서 시스템 프롬프트로 빠져나가게 된다는 표시입니다.

사용자가 입력하고 싶은 메시지를 입력하십시오. 메시지 입력이 끝나면 Ctrl+D를 두 번 누르십시오.

```
SWITCH(config)# banner
```

```
Save & Exit : CTRL-D
```

```
V5812G
```

```
Dasan Networks Inc.SWITCH(config)#{
```

메시지를 입력하고 Ctrl-D를
누르면 시스템 프롬프트로 돌아갑니다.

위와 같이 입력하면 로그인할 때 다음과 같이 배너가 생깁니다.

```
V5812G
Dasan Networks Inc.

SWITCH login:
```

다음은 로그인에 성공했을 때와 실패했을 때의 메시지를 입력하는 경우의 예입니다.

```
SWITCH(config)# banner login
Save & Exit : CTRL-D
Success Login
SWITCH(config)# banner login-fail
Save & Exit : CTRL-D
Login Fail!!
SWITCH(config)#

```

위에서 설정한 세 가지 경우의 메시지를 모두 확인하면 다음과 같습니다.

```
SWITCH(config)# show banner
< Login banner >
V5812G
Dasan Networks Inc.

< Login success banner >
Complete!!

< Login fail banner >
Fail!!

SWITCH(config)#

```

위에서 설정한 내용을 저장한 후 다시 시스템 로그인을 시도하면 다음과 같은 화면이 출력됩니다.

```
*****
*                               *
*          Boot Loader Version 4.74      *
*          DASAN Networks Inc.           *
*                               *
*****
```

Press 's' key to go to Boot Mode: 0

```
Load Address: 0x01000000
Image Size: 0x00af5000
Start Address: 0x01000000

console=ttyS0,9600 root=/dev/ram rw
NOS version 3.03 #1013
CPU : Motorola [rev=1014]
Total Memory Size : 256 MB
Calibrating delay loop... 175.71 BogoMIPS
INIT: version 2.85 booting
Extracting configuration
Fri, 13 Jan 2006 17:58:48 +0000
INIT: Entering runlevel: 3
```

(중략)

```
V5812G
Dasan Networks Inc.

SWITCH login: root
Password:
Login incorrect
Login Fail!! ─────────── 로그인 실패
SWITCH login: admin
Password:
Success Login ─────────── 로그인 성공
SWITCH#
```

6.1.10. Fan 동작 설정

V5812G의 FAN은 임계값에 따라 자동으로 동작하도록 설정되어 있습니다.



V5812G는 기본적으로 FAN이 동작을 시작하는 온도가 20°C, 동작을 멈추는 온도가 -10°C로 설정되어 있습니다.

하지만, 사용자가 임계값과 상관없이 FAN 동작을 시작하거나 종료할 수 있습니다. FAN 동작을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
fan operation on	Global	FAN을 강제로 동작시킵니다.
fan operation off		FAN의 동작을 강제로 종료시킵니다.

사용자가 강제로 FAN 동작을 설정하였다가 다시 자동적으로 동작하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
fan operation auto	Global	임계값에 따라 자동으로 FAN을 ON/OFF 시키도록 설정합니다.

FAN 상태를 확인하고, FAN이 동작하는 온도를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show status fan	View/Enable/Global	FAN 상태와 FAN이 동작하는 온도를 확인합니다.

[설정 예제 1]

다음은 FAN이 동작하기 시작하는 온도를 25°C, FAN이 멈추는 온도를 5°C로 설정한 경우입니다.

```
SWITCH(config)# threshold fan 25 5
SWITCH# show status fan

Fan A : Installed
Fan A-1 status is RUN
Fan A-2 status is RUN
Fan A-3 status is RUN
Fan A-4 status is RUN
Fan operation : AUTO
Fan threshold : Run 25 C / Stop 5 C

SWITCH#
```

6.1.11. 데몬 강제 종료

V5812G는 불필요하게 CPU를 점유하고 있는 데몬에 대한 동작을 관리자가 강제로 끝낼 수 있습니다. 장비에서 동작하고 있는 데몬을 강제로 끝내려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
halt process-id	Enable/Global	해당 PID의 데몬을 강제로 종료시킵니다.

데몬의 PID는 Process-ID로, **show process** 명령어(**6.3.10 CPU 프로세스 확인** 참조)로 확인할 수 있습니다.

```
SWITCH# show process
USER          PID %CPU %MEM   VSZ RSS TTY      STAT START    TIME COMMAND
admin         1  0.0  0.5 1448 592 ?          S   15:56   0:03 init [3]
admin         2  0.0  0.0    0   0 ?          S   15:56   0:00 [keventd]
admin         3  0.0  0.0    0   0 ?          SN  15:56   0:00 [ksoftirqd_CPU0]
admin         4  0.0  0.0    0   0 ?          S   15:56   0:00 [kswapd]
```

6.1.12. FTP 서버 활성화

V5812G는 기본적으로 FTP 서버로서의 기능을 가지고 있습니다. 그러나, FTP 서버로서 활성화시켜 놓을 경우에는 23번 포트를 통해 접근이 쉬워지기 때문에 보안상의 문제가 발생할 수 있습니다. 따라서, FTP 서버로서의 기능이 불필요할 때에는 사용자가 FTP 서버로서의 기능을 해제함으로써 보안을 강화할 수 있습니다.

V5812G에 FTP 서버로서의 기능을 활성화하거나 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ftp server {enable disable}	Global	FTP 서버로서의 기능을 활성화하거나 해제합니다.



V5812G는 기본적으로 FTP 서버가 활성화되어 있습니다.

6.1.13. FTP 클라이언트 주소 설정

V5812G는 여러 개의 IP 주소가 설정될 수 있습니다. 그러나, FTP 서버에 클라이언트가 되어 접속할 때, 여러 개의 IP 주소 중에서 하나를 지정해 줄 수 있습니다. FTP 클라이언트로 서버에 접속할 때 Source IP 주소로 사용할 IP 주소를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ftp bind-address ip-address	Global	FTP 서버에 접속할 때 Source IP 주소로 사용할 IP 주소를 지정합니다.



FTP bind-address를 설정하면 TFTP 클라이언트가 해당 IP 주소가 Source 주소로 적용됩니다.

FTP 클라이언트로서 가지는 IP 주소를 지정했던 것을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ftp bind-address	Global	FTP 클라이언트로서 가지는 IP 주소를 지정했던 것을 삭제합니다.

6.1.14. Module DMI 정보 출력 설정

V5812G의 모든 포트에 대한 DMI 정보 수집은 I2C에 의해서 이루어집니다. 그러나, DMI 정보 수집으로 인해 CPU Load에 영향을 미칠 수 있습니다. 이러한 현상을 방지하기 위하여 V5812G는 사용자의 필요에 따라 장비의 DMI 정보를 polling 하지 않도록 설정할 수 있습니다.

사용자의 필요에 따라 장비 DMI 정보의 polling 여부를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
module dmi [enable disable]	Global	장비 DMI 정보의 polling 여부를 설정합니다.



V5812G는 기본적으로 **module dmi**가 **enable**로 설정되어 있습니다. 따라서 DMI 정보를 polling 하지 않으려면 **disable**로 설정하십시오.

**주 의**

module dmi가 **disable**로 설정되어 있는 경우, **show port module-info** 명령어로 확인할 때 해당 포트의 DMI 정보가 출력되지 않습니다.

설정한 Module DMI의 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show module dmi	Enable/Global/Bridge	장비의 Module DMI 설정 내용을 확인합니다.

다음은 V5812G의 **module dmi**를 **disable**로 설정하고 그 내용을 확인하는 경우의 예입니다.

```
SWITCH(config)# module dmi disable
SWITCH(config)# show module dmi
-----
Module Diagnostics Monitoring
-----
module diagnostics monitor(dmi) : disable
SWITCH(config)#

```

6.1.15. 시스템 임계값 설정

V5812G는 사용자가 CPU 사용량, 포트 트래픽, FAN 동작, 온도, 메모리량 등에 대한 임계값을 설정해 두면, 해당 임계값을 넘어섰을 때, 그리고 다시 임계값 아래로 떨어졌을 때 syslog 메시지를 통해 알려주는 기능을 가지고 있습니다.

(1) CPU 사용량 임계값 설정

V5812G는 사용자가 CPU 사용량에 대한 임계값을 설정해 두면, CPU 사용량이 임계값을 넘어섰을 때, 그리고 다시 임계값 아래로 떨어졌을 때 syslog 메시지를 통해 알려주는 기능을 가지고 있습니다. V5812G에 CPU 사용량 임계값을 설정하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
threshold cpu <21-100> {5 60 600}	Global	사용자 장비의 CPU 사용량에 대한 최대 임계값을 설정합니다.
threshold cpu <21-100> {5 60 600} <20-100> {5 60 600}		사용자 장비의 CPU 사용량에 대한 최대 임계값과 최소 임계값을 설정합니다.

설정된 CPU 사용량 임계값을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no threshold cpu	Global	사용자 장비의 CPU 사용량 임계값을 삭제합니다.



임계값의 단위는 "%"이며 최대 임계값은 21%부터 100%까지, 최소 임계값은 20%부터 100%까지 설정 가능합니다.



V5812G는 CPU 사용량 임계값이 기본적으로 최대값은 70%, 최소값은 30%로 설정되어 있습니다.



시간 간격은 5초, 60초, 600초로 설정할 수 있습니다.

사용자가 설정한 CPU 사용량 임계값을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show cpuload	Enable/ Global	사용자 장비의 CPU 사용량 임계값과 CPU 평균 사용량을 확인합니다.

다음은 사용자 장비의 CPU 사용량 임계값을 50%로 설정하고, 그 내용을 확인하는 경우입니다.

```
SWITCH(config)# threshold cpu 50 60
SWITCH(config)# show cpuload
-----
Average CPU load
-----
5 sec: 4.60( 0.05) %
1 min: 5.09( 0.05) %
10 min: 5.03( 0.04) %

cpuload threshold (high) : 50
timer interval (high) : 60
cpuload threshold (low) : 30
timer interval (low) : 60
SWITCH(config)#

```

위와 같이 설정해 놓으면 CPU 사용량이 50%를 넘어갔을 때 다음과 같은 메시지가 출력됩니다.

```
Oct 18 17:37:24 zebra[80]: CPU Overload Warning : Threshold [50] < CPU Load [86]
```

그리고, CPU 사용량이 다시 70% 아래로 다시 떨어지면 다음과 같은 메시지가 출력됩니다

```
Oct 18 17:37:29 zebra[80]: CPU Overload Cleared : Threshold [50] > CPU Load [39]
```



참 고

위의 메시지에서 [] 안의 숫자는 부하를 나타냅니다.

(2) 포트 트래픽 임계값 설정

V5812G는 사용자가 각 포트의 트래픽량에 대한 임계값을 설정해 두면, 트래픽량이 임계값을 넘어섰을 때, 그리고 다시 임계값 아래로 떨어졌을 때 syslog 메시지를 통해 알려주는 기능을 가지고 있습니다. V5812G의 각 포트에 트래픽 임계값을 설정하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
threshold port port-number threshold {5 60 600} { rx tx }	Global	사용자 스위치의 포트 트래픽 임계값을 설정합니다. 임계값의 단위는 “kbps”입니다.
threshold port port-number block timer <10-3600>		설정된 트래픽 임계값을 초과했을 경우 해당 포트를 차단시키는 시간을 설정합니다.



참 고

포트 임계값은 기본적으로 해당 포트의 최대 속도 값으로 설정되어 있습니다. Giga 포트인 경우에는 1000000kbps, 100M 포트인 경우에는 100000kbps로 설정되어 있습니다.



참 고

시간 간격은 5초, 60초, 600초로 설정할 수 있습니다.

포트 트래픽 임계값을 설정한 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no threshold port port-number { rx tx }	Global	포트 트래픽 임계값을 해제합니다.
no threshold port port-number block		포트 트래픽을 차단하려 설정했던 시간을 해제합니다.

사용자가 설정한 포트 트래픽 임계값을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show port threshold	Enable/Global	사용자가 설정한 포트 트래픽 임계값을 확인합니다.

다음은 1번 포트에 포트 트래픽 임계값을 500Mbps로 설정한 경우입니다.

```
SWITCH(config)# threshold port 1 500 5 rx
SWITCH(config)#{
```

(3) Fan 임계값 설정

V5812G는 일정한 온도가 되면 Fan의 동작을 시작하거나 멈추도록 설정할 수 있습니다. 온도에 따라 자동적으로 Fan이 동작하도록 설정하려면, 다음 명령어를 사용하여 Fan이 동작을 시작하는 온도와 동작을 멈추는 온도를 설정하십시오.

명령어	모 드	Function
threshold fan start-temperature stop-temperature	Global	Fan이 동작을 시작하는 온도와 동작을 멈추는 온도를 설정합니다.

설정된 FAN 동작 온도 임계값을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	Function
no threshold fan	Global	설정된 Fan 동작이 시작하는 온도와 동작을 멈추는 온도를 삭제합니다.



참 고

기본적으로 Fan이 동작을 시작하는 온도는 20°C, 동작을 멈추는 온도는 -10°C로 설정되어 있습니다.

**참 고**

Fan이 동작을 시작하는 온도는 최대 100°C까지 설정할 수 있고, 동작을 멈추는 온도는 최하 -30°C까지 설정할 수 있습니다.

**참 고**

반드시 Fan이 동작을 멈추는 온도보다 동작을 시작하는 온도가 커야 합니다.

Fan 상태와 사용자가 설정한 Fan 동작 온도를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	Function
show status fan	Enable/Global	Fan의 상태와 사용자가 설정한 Fan 동작 온도를 확인합니다.

다음은 Fan이 동작을 시작하는 온도를 25°C로 설정하고, Fan이 동작을 멈추는 온도를 5°C로 설정하는 경우입니다.

```
SWITCH(config)# threshold fan 25 5
SWITCH(config)# show status fan

Fan A : Installed
Fan A-1 status is RUN
Fan A-2 status is RUN
Fan A-3 status is RUN
Fan A-4 status is RUN
Fan operation : AUTO
Fan threshold : Run 25 C / Stop 5 C

SWITCH(config)#+
```

**주 의**

show status fan에 대한 내용은 제품에 따라 상이하게 다를 수 있습니다.

(4) 온도 임계값 설정

V5812G는 사용자가 장비 온도에 대한 임계값을 설정해 두면, 장비 온도가 임계값을 넘어섰을 때, 그리고 다시 임계값 아래로 떨어졌을 때 syslog 메시지를 통해 알려주는 기능을 가지고 있습니다.

장비 온도 임계값을 설정하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
threshold temp <-40-100> <-40-100>	Global	사용자 장비의 장비 온도 임계값을 설정합니다.

설정된 장비 온도 임계값을 삭제하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no threshold temp	Global	설정된 사용자 장비의 장비 온도 임계값을 삭제합니다.



참 고

기본적으로 장비 온도 임계값은 80°C로 설정되어 있습니다.

장비 온도 상태와 장비 온도 임계값을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show status temp	Enable/Global/Bridge	사용자 장비의 장비 온도 상태와 장비 온도 임계값을 알려줍니다.



주의

show status temp에 대한 내용은 제품에 따라 상이하게 다를 수 있습니다.

(5) 메모리량 임계값 설정

V5812G는 메모리 사용량에 대한 임계값을 설정하고, 설정한 임계값 이상으로 메모리를 사용할 경우 Syslog 메시지를 통해 알려주도록 되어 있습니다. 전체 메모리 용량(100%)을 기준으로 사용하고 있는 메모리의 용량에 대한 임계값을 설정합니다. 만일 사용하는 메모리 용량이 임계값보다 작아지면, 다시 Syslog 메시지를 통해 알려줍니다.



참 고

기본적으로 장비의 메모리 사용량 임계값은 80%로 설정되어 있습니다.

장비의 메모리 사용량에 대한 임계값을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
threshold memory value	Global	메모리 사용량에 대한 임계값을 설정합니다.

설정된 메모리 사용량에 대한 임계값을 삭제하고 기본값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no threshold memory	Global	메모리 사용량 임계값을 기본값으로 되돌립니다.

(6) SFP 모듈 상태 임계값 설정

V5812G는 서비스 포트가 SFP 모듈로 구성됩니다. V5812G의 관리자는 SFP 모듈의 전압, 전력, 온도, 바이어스(Bias)에 대한 임계값을 설정해 두고, 임계값의 범위를 초과하거나, 임계값 범위 미만으로 그 값이 떨어졌을 때 Alarm이나 Warning 메시지로 알리도록 할 수 있습니다.

이러한 기능을 사용하면, 항상 SFP 모듈의 상태를 모니터링할 수 있고, SFP 모듈에 이상이 생겼을 때, 즉시 상황을 파악하고 대처할 수 있기 때문에 SFP 모듈의 문제로 인해 인터넷 서비스 가입자들이 안정된 서비스를 제공받지 못하는 상황을 막을 수 있습니다.

SFP 모듈의 전압, 전력, 온도, 바이어스에 대한 임계값을 설정하여 SFP 모듈을 모니터링 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
threshold module {rxpower txpower} {alarm warning} {port-number low-threshold high-threshold}	Global	해당 포트의 전력에 대한 임계값을 설정하여 SFP 모듈을 모니터링합니다.
threshold module temper {alarm warning} {port-number low-threshold high-threshold}	Global	해당 포트의 온도에 대한 임계값을 설정하여 SFP 모듈을 모니터링합니다.
threshold module txbias {alarm warning} {port-number low-threshold high-threshold}	Global	해당 포트의 TX 바이어스에 대한 임계값을 설정하여 SFP 모듈을 모니터링합니다.
threshold module voltage {alarm warning} {port-number low-threshold high-threshold}	Global	해당 포트의 전압에 대한 임계값을 설정하여 SFP 모듈을 모니터링합니다.

설정된 SFP 모듈의 전압, 전력, 온도, 바이어스에 대한 임계값을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no threshold module {rxpower txpower txbias voltage temper} {alarm warning} port-number	Global	해당 포트의 모듈 옵션 임계값 설정을 삭제합니다.

위에서 설정한 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show port module-info [port-number]	Enable/Global/Bridge	SFP 모듈의 상태를 확인합니다.

6.2 설정 관리

사용자는 설정한 내용이 올바른지 확인하거나 설정한 내용을 시스템에 저장할 수 있습니다. 이러한 설정 관리와 관련, 다음과 같은 내용을 설명합니다.

- 설정 내용 확인
- 설정 내용 저장
- 설정 내용 자동 저장
- 설정 초기화 하기
- 설정 내용 Backup 하기

6.2.1. 설정 내용 확인

V5812G는 장비에 대한 설정 내용을 각 모드에서 확인할 수 있습니다. 다음은 설정 내용을 확인할 때 사용하는 명령어입니다.

명령어	모 드	기 능
show running-config		설정된 내용을 보여줍니다.
show running-config { admin-flow admin-policy arp bridge dns flow full hostname interface [interface-name] login policer policy qos rmon-alarm rmon-event rmon-history snmp syslog time-zone time_out }	All	특정한 설정에 대한 내용만 보여줍니다.
show running-config router {bgp ospf rip vrrp}		

다음은 Syslog의 설정 내용을 확인한 경우입니다.

```
SWITCH# show running-config syslog
syslog start
syslog output info local volatile
syslog output info local non-volatile
!
SWITCH#
```

6.2.2. 설정 내용 저장

TFTP/FTP 서버를 통해 새로운 시스템 이미지를 내려 받은 후에는 사용자의 장비를 설정하거나 설정한 내용을 변경했을 때, 사용자는 반드시 플래시 메모리에 설정, 또는 변경된 내용을 저장해야 합니다. 만일 저장하지 않으면 장비의 전원을 껐다가 다시 키거나 재부팅시켰을 때, 이전에 설정 또는 변경된 내용이 모두 사라집니다. 설정 또는 변경한 내용을 플래시 메모리에 저장할 때는 다음 명령어를 사용하십시오.

명령어	모 드	기 능
write memory	All	사용자가 설정, 변경한 내용을 플래시 메모리에 저장합니다.

다음은 설정한 내용을 저장하는 경우의 예입니다.

```
SWITCH# write memory
[OK]
SWITCH#
```



주의

위의 명령어를 사용하여 설정 내용을 저장한 경우에는 반드시 [OK] 메시지가 나올 때까지 어떤 키도 입력하지 말아주십시오.

6.2.3. 설정 내용 자동 저장

V5812G는 사용자의 설정에 따라 일정한 간격으로 설정 내용을 자동 저장하는 것이 가능합니다. 일정한 간격으로 장비의 설정 내용을 자동 저장하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
write interval <10-1440>	Global	설정 내용을 자동 저장하는 시간 간격을 설정합니다.



참 고

자동 저장 간격을 입력하는 <10-1440>의 단위는 분입니다. 단, 값은 10의 배수로 설정되며, 그 이외의 숫자가 입력되면 일의 자리 수를 절삭합니다. 예를 들어, 사용자가 15를 입력해도 실제로 장비에 적용되는 값은 10이 되는 것입니다.



참 고

V5812G는 기본적으로 **write interval**이 설정되어 있지 않습니다.

장비의 설정 내용을 자동 저장했던 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no write interval	Global	설정 내용을 자동 저장하도록 설정한 것을 해제합니다.

6.2.4. 설정 초기화 하기

사용자는 설정한 내용을 하나씩 개별적으로 삭제할 수도 있지만, 처음 제품을 구입했던 당시의 상태로 초기화 할 수도 있습니다. 설정을 초기화 하려면 다음의 명령어를 사용하십시오.

명령어	모 드	기 능
restore factory-defaults		설정을 초기화 합니다.
restore layer2-defaults	Enable	L2 설정을 초기화 합니다.
restore layer3-defaults		L3 설정을 초기화 합니다.



주 의

“**restore factory-defaults**” 명령어를 사용하여 설정 내용을 초기화한 후에 반드시 장비를 재부팅하십시오. 재부팅하지 않으면 초기화 되지 않습니다.

다음은 장비의 설정 내용을 초기화 한 경우입니다.

```
SWITCH# restore factory-defaults
You have to restart the system to apply the changes
SWITCH#
```

6.2.5. 데이터 Backup 하기

V5812G는 사용자가 설정한 내용을 따로 저장해 두었다가 파괴된 데이터의 복원을 돋기도 하고 시스템 작동을 유지하는데 사용할 수 있습니다. 또한, 다음에서 설명하는 명령어를 사용하여 시스템 이미지를 설치할 수도 있습니다.

한편, V5812G는 보안을 위해 SSH(Secure Shell)을 사용하여 데이터를 Backup 할 수 있습니다. SSH를 사용하면 모든 데이터가 암호화되고, 트래픽은 압축되어 작업의 효율성을 높일 수 있습니다.

(1) 일반 Backup 하기

사용자가 설정한 내용을 Backup하려면 다음의 명령어를 사용하십시오. 변수인 “*file-name*”은 Backup하는 내용의 일종의 파일명으로 사용자가 편리한 이름으로 설정할 수 있습니다.

명령어	모 드	기 능
copy running-config { <i>file-name</i> startup-config}	Enable	현재 설정내용을 사용자가 지정한 파일명으로 Backup하거나 Startup의 설정 내용으로 Backup합니다.
copy startup-config <i>file-name</i>		Startup의 설정내용을 Backup합니다.
copy <i>file-name</i> startup-config		<i>file-name</i> 이라는 이름으로 Backup된 내용을 startup-config에서 사용하기 위해 불러냅니다.
copy <i>file-name1</i> <i>file-name2</i>		이미 Backup된 <i>file-name1</i> 을 <i>file-name2</i> 로 다시 Backup합니다.

FTP 서버나 TFTP 서버를 사용하여 데이터를 Backup 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
copy {ftp tftp} config upload { <i>file-name</i> startup-config}	Enable	이미 Backup된 <i>file-name</i> 을 원격지의 FTP 또는 TFTP 서버로 업로드하거나 Startup의 설정내용으로 업로드 합니다.
copy {ftp tftp} config download { <i>file-name</i> startup-config}		이미 Backup된 <i>file-name</i> 을 원격지의 FTP 또는 TFTP 서버에서 다운로드하거나 Startup의 설정내용으로 다운로드 합니다.
copy {ftp tftp} os upload {os1 os2}		FTP 또는 TFTP 서버로 os를 업로드 합니다.
copy {ftp tftp} os download {os1 os2}		FTP 또는 TFTP 서버에서 os를 다운로드 합니다.
copy {ftp tftp} fpga download		FTP 또는 TFTP 서버에서 FPGA 이미지를 다운로드 합니다.
copy {ftp tftp} dumpfile upload { <i>file-nam</i> }		덤프 파일을 FTP 또는 TFTP 서버에 업로드 합니다.
copy {ftp tftp} onu { download upload}		ONU Backup 파일을 FTP 또는 TFTP 서버에 업로드하거나 다운로드 합니다.

**주 의**

설정 내용을 백업하거나, 백업된 파일을 불러오기 위해 FTP에 접속하기 위해서는 FTP 사용자 ID와 비밀번호를 알고 있어야 합니다.

**참 고**

FTP를 통해 설정 내용을 백업하거나, 백업된 파일을 불러오는 경우에는 hash on 기능이 자동으로 활성화되기 때문에 파일 전송률을 확인할 수 있습니다.

**주 의**

Backup 해 둔 내용을 불러 낸 내용을 장비에 적용하기 위해서는 시스템을 재부팅해야 합니다.

(2) SSH를 이용하여 데이터 Backup 하기

클라이언트가 된 V5812G는 SSH를 이용하여 서버에 파일을 복사하거나 서버에 있는 파일을 가져올 수 있습니다. 또한, FTP 서비스는 매우 보안이 취약한 단점을 가지고 있는데 SSH를 이용하면 보다 안전하게 FTP 서비스를 이용할 수 있습니다. SSH를 이용하여 파일을 복사하거나 FTP 서비스를 이용하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>copy {scp sftp} config {download upload} config_file</code>	Enable	SSH를 이용하여 데이터를 업로드 또는 다운로드 합니다.
<code>copy {scp sftp} key upload config_file</code>		SSH를 이용하여 인증키를 가지고 있는 데이터를 업로드합니다.

(3) Backup 파일 확인

Startup config를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>show startup-config</code>	Enable	Startup config를 확인합니다.

Backup한 파일을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show config-list	Enable/Global	Backup된 파일을 보여줍니다.

다음은 V5812G에서 현재 설정 내용을 “V5812G”라는 파일명으로 Backup한 후 Backup 파일 리스트를 확인한 경우입니다.

```
SWITCH(config)# copy running-config V5812G
[OK]
SWITCH(config)# show config-list
=====
CONFIG-LIST
=====
V5812G
SWITCH(config)#

```

(4) Backup 파일 삭제

Backup한 파일을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
erase config filename	Enable/Global	Backup된 파일을 삭제합니다.
erase key filename	Enable	인증키를 삭제합니다.
erase startup-config filename		Startup의 설정내용을 Backup 했던 것을 삭제합니다.

6.3 시스템 확인

사용자는 장비에 문제가 발생했을 때 그 원인을 파악하고 해결책을 찾아야 하고, 문제가 발생하기 이전에도 항상 장비의 상태를 점검해야 합니다. 따라서 사용자는 문제가 발생했을 때 장비의 상태를 확인할 수 있어야 할 뿐만 아니라 설정 내용을 변경한 이후에는 올바르게 변경되었는지 여부를 확인할 수 있어야 합니다.

V5812G는 DSH 명령어를 사용하여 사용자가 다음과 같은 항목들을 확인할 수 있습니다.

- 네트워크 연결 상태 확인
- IP ICMP Source-routing
- 패킷 경로 추적
- 원격 접속자 확인
- MAC table 보기
- Aging time 설정
- 장비 사용 시간 확인
- 시스템 information 확인
- CPU 평균 사용량 확인
- CPU 트래픽 제한
- CPU 프로세스 확인
- 메모리 사용 정보 확인
- 시스템 이미지 버전 확인
- 시스템 이미지 파일 크기 확인
- 설치된 NOS 확인하기
- Default OS 설정
- 장비 상태 확인
- 모듈 정보 확인
- Tech-support 확인
- 부팅 정보 확인

6.3.1. 네트워크 연결 상태 확인

사용자의 장비가 사용자의 네트워크에 올바르게 연결되어 있는지 여부를 알기 위해서는 ping 명령어를 사용합니다. IP 네트워크에서 ping 명령어는 ICMP(Internet Control Message Protocol) 에코 메시지를 전송합니다.

ICMP는 오류상황을 알려 주고 IP 패킷 수신지 정보를 제공하는 인터넷 프로토콜입니다. 수신지에서 ICMP Echo 메시지를 받으면 수신자는 ICMP Echo 응답 메시지를 송신자로 돌려 보냅니다.

상대방과 네트워크 연결 상태를 확인하기 위해 Ping 테스트를 하려면 Privilege Exec Enable 모드에서 다음의 명령어를 사용하십시오.

명령어	모 드	기 능
ping [ip address host name]	Enable	상대방과의 네트워크 연결 상태를 확인하기 위해 Ping 테스트를 실행합니다.

다음은 Ping 테스트를 실행하기 위해 설정해야 하는 기본 정보입니다. Enable 모드에서 Ping 테스트를 실행 한 후 다음 기본 설정 내용을 입력하십시오.

내 용	기 본 설 정
Protocol [ip]	Ping test를 위해 지원되는 프로토콜입니다. 디폴트는 IP로 설정되어 있습니다.
Target IP address	상대방과의 네트워크 연결 상태를 확인하기 위해 목적지의 IP 주소나 Hostname을 입력하면 목적지로 ICMP echo 메시지를 보냅니다.
Repeat count [5]	count를 입력하면 입력된 횟수만큼 ICMP echo 메시지를 보냅니다. Default는 5 번으로 설정되어 있습니다.
Datagram size [100]	Ping 패킷의 사이즈입니다. Default는 100 bytes입니다.
Timeout in seconds [2]	Ping 패킷에 대한 reply가 정해진 시간간격 이내에 돌아와야만 성공적인 Ping test가 이루어 졌다고 간주합니다. Default는 2초로 설정되어 있습니다.
Extended commands [n]	추가적인 명령어들을 나타낼 것인지를 결정합니다. Default는 no로 설정되어 있습니다.

[설정 예제 1]

IP 주소 192.168.1.10과의 네트워크 상태를 확인하기 위해 Ping 테스트 5번 실시한 경우입니다.

```
SWITCH# ping
Protocol [ip]: ip
Target IP address: 172.16.1.254
Repeat count [5]: 5
Datagram size [100]: 100
Timeout in seconds [2]: 2
Extended commands [n]: n
PING 172.16.1.254 (172.16.1.254) 100(128) bytes of data.
Warning: time of day goes back (-394us), taking countermeasures.
108 bytes from 172.16.1.254: icmp_seq=1 ttl=255 time=0.058 ms
108 bytes from 172.16.1.254: icmp_seq=2 ttl=255 time=0.400 ms
108 bytes from 172.16.1.254: icmp_seq=3 ttl=255 time=0.403 ms
108 bytes from 172.16.1.254: icmp_seq=4 ttl=255 time=1.63 ms
108 bytes from 172.16.1.254: icmp_seq=5 ttl=255 time=0.414 ms
--- 172.16.1.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 8008ms
rtt min/avg/max/mdev = 0.058/0.581/1.632/0.542 ms
SWITCH#
```

사용자의 장비에 여러 개의 IP 주소가 설정되어 있을 때에는 특정한 IP 주소와 상대방의 네트워크 연결 상태를 확인해야 하는 경우가 있습니다. Spring을 테스트를 실시하기 위해서는 Ping 테스트 설정과 동일한 과정을 거친 다음, ‘Extended commands’ 이후부터 Spring 테스트를 위한 다음 사항들을 입력합니다. 다음 명령어를 이용하여, 장비에 설정되어 있는 특정한 IP 주소와 상대방과의 네트워크 연결 상태를 확인할 수 있습니다. 다음은 Spring을 실행하기 위해 설정해야 할 정보입니다.

내 용	기 본 설 정
Source address or interface:	상대방이 응답해야 하는 주소를 source ip address에 지정해 줍니다.
Type of service [0]:	Layer 3 어플리케이션에서 Qos (Quality Of Service) 를 구현하기 위한 서비스 필드입니다. IP Packet에 대한 priority를 지정해 줄수 있습니다.
Set DF bit in IP header? [no]	Don't Fragment (DF) bit를 Ping 패킷에 적용할지를 결정합니다. Default는 no로 설정되어 있습니다. yes를 선택할 경우에 패킷이 자신의 용량보다 더 작은 데이터 단위로 이루어진 세그먼트를 통과할 때 Fragment 되는것을 막기 때문에 여러 메시지가 전송 될 수 있습니다.
Data pattern [0xABCD]	데이터 패턴을 설정합니다. Default는 0xABCD입니다.



주 의

“sping”은 사용자의 장비에 IP 주소가 여러 개 설정되어 있을 때 사용하십시오. IP 주소가 한 개 뿐인 장비에서는 아무런 의미가 없습니다.

[설정 예제 2]

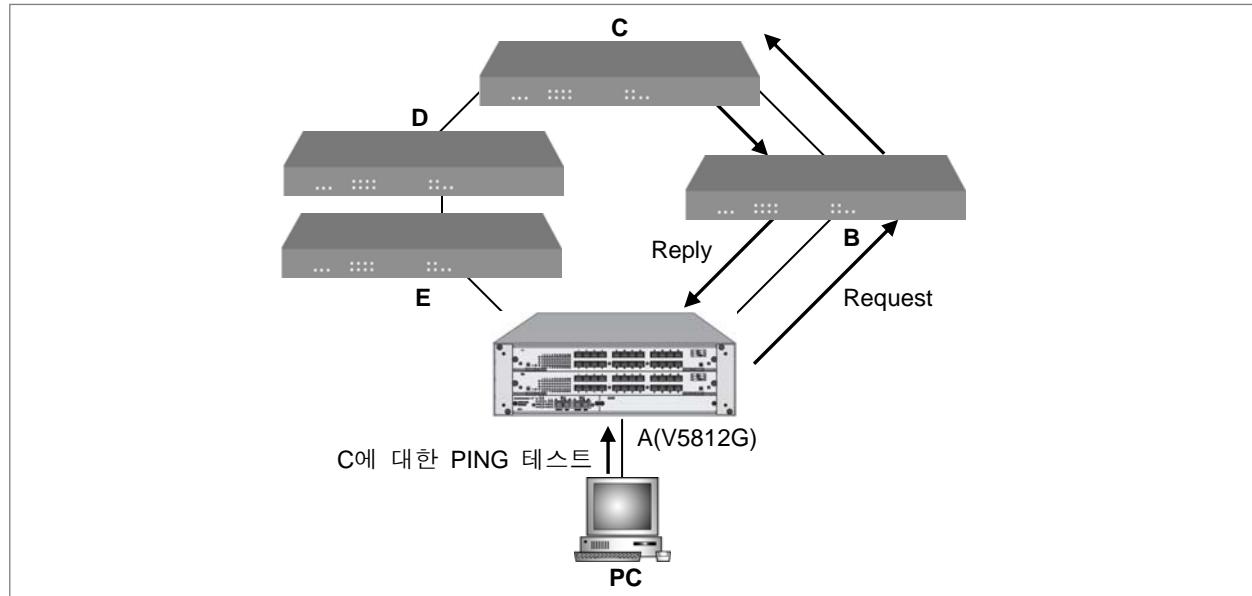
다음은 장비의 IP가 172.16.157.100으로 설정되어 있을 때, 172.16.157.100과 172.16.1.254라는 IP 주소의 네트워크 연결 상태를 확인한 경우입니다.

```
SWITCH# ping
Protocol [ip]:
Target IP address: 172.16.1.254
Repeat count [5]: 5
Datagram size [100]:100
Timeout in seconds [2]:2
Extended commands [n]: y                                         "sping"을 실행하기 위해서
Source address or interface: 172.16.157.100                         Extended commands를
Type of service [0]:0                                               선택하는 'y'를 입력합니다.
Set DF bit in IP header? [no]:no
Data pattern [0xABCD]:
PATTERN: 0xabcd
PING 172.16.1.254 (172.16.1.254) from 172.16.157.100 : 100(128) bytes of data.
108 bytes from 172.16.1.254: icmp_seq=1 ttl=255 time=30.4 ms
108 bytes from 172.16.1.254: icmp_seq=2 ttl=255 time=11.9 ms
108 bytes from 172.16.1.254: icmp_seq=3 ttl=255 time=21.9 ms
108 bytes from 172.16.1.254: icmp_seq=4 ttl=255 time=11.9 ms
108 bytes from 172.16.1.254: icmp_seq=5 ttl=255 time=30.1 ms

--- 172.16.1.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 8050ms
rtt min/avg/max/mdev = 11.972/21.301/30.411/8.200 ms
SWITCH#
```

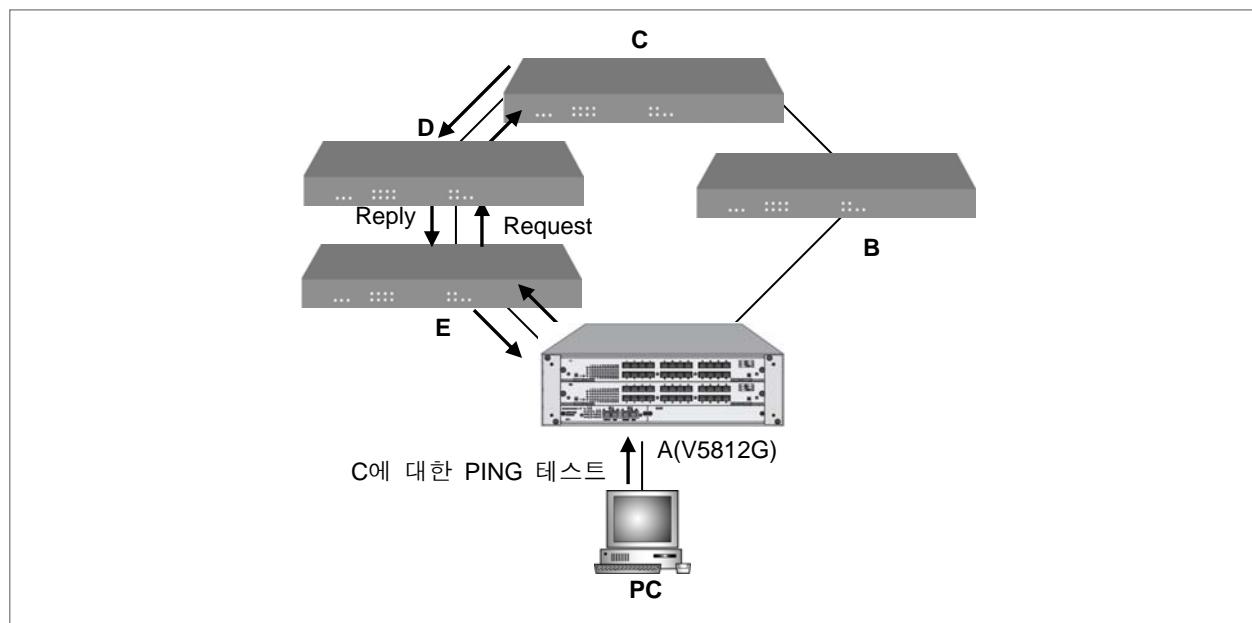
6.3.2. IP ICMP Source-routing

네트워크 연결 상태를 확인하기 위해서 Ping 테스트를 실시하면, 일반적으로 ICMP 응답은 라우팅 이론에 따라 가장 가까운 경로를 통해서 전송되게 됩니다.



【 그림 6-2 】 네트워크 연결 확인을 위한 Ping 테스트

위의 그림의 경우, PC에서 C라는 장비에 Ping 테스트를 실시한다면, 일반적으로 「A→B→C」의 경로를 따라 ICMP 응답이 전송됩니다. 그러나, V5812G는 아래와 같이 「A→E→D→C」의 경로를 따라 ICMP 응답이 전송되도록 설정할 수 있습니다.



【 그림 6-3 】 IP ICMP Source Routing

관리자가 지정한 경로를 따라 Ping 테스트를 실시하도록 설정하려면, 다음의 단계를 따르십시오.

- 1 단계 Ping 테스트를 실시할 PC에 연결된 장비에 IP ICMP source-routing 기능을 활성화합니다.
V5812G에 IP ICMP source-routing 기능을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip icmp source-route	Global	IP ICMP source-routing 기능을 활성화합니다.
no ip icmp source-route		IP ICMP source-routing 기능을 해제합니다.

- 2 단계 「**ping -k ip-address ip-address...**」 명령어를 사용하여 지정된 경로를 따라 Ping 테스트를 실시하도록 합니다.

6.3.3. 패킷 경로 추적

V5812G의 사용자는 패킷이 목적지로 가면서 거쳐 가는 경로를 확인할 수 있습니다. 이 경로를 알기 위해, **traceroute** 명령어는 검침 패킷을 보낸 후 거쳐가는 경로마다 되돌아 오는 시간을 화면에 출력합니다. 만일 검침 패킷이 되돌아오는 시간이 될 때까지 패킷의 응답이 없는 경우에는 별표(*)가 출력됩니다. 패킷 경로를 추적하려면 Privilege Exec Enable 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
traceroute [word]		
traceroute ip word	Enable	목적지의 IP 주소 또는 Hostname을 입력하면 패킷 전송 경로를 추적합니다.
traceroute icmp word		

다음은 **traceroute** 명령어를 실행하기 위해 설정해야 할 정보입니다.

내 용	기 본 설 정
Source address or interface:	상대방이 응답해야 하는 주소를 source ip address에 지정해 줍니다.
Type of service [0]:	Layer 3 어플리케이션에서 Qos (Quality Of Service) 를 구현하기 위한 서비스 필드입니다. IP Packet에 대한 priority를 지정해 줄수 있습니다.
Set DF bit in IP header? [no]	Don't Fragment (DB) bit를 Ping 패킷에 적용할지를 결정합니다. Default는 no로 설정되어 있습니다. yes를 선택할 경우에 패킷이 자신의 용량보다 더 작은 데이터 단위로 이루어진 세그먼트를 통과할 때 Fragment 되는것을 막기 때문에 에러 메시지가 전송 될 수 있습니다.
Data pattern [0xABCD]	데이터 패턴을 설정합니다. Default는 0xABCD입니다.

다음은 IP 주소가 192.168.1.10인 목적지로 보내는 패킷의 경로를 확인하는 경우입니다.

```
SWITCH# traceroute 192.168.1.10
traceroute to 192.168.1.10 (192.168.1.10), 30 hops max, 38 byte packets
 1 hmt.da-san.com (203.236.124.252)  0.528 ms  0.450 ms  0.719 ms
 2 172.16.147.49 (172.16.147.49)  141.994 ms  125.313 ms  13.171 ms
 3 168.126.228.101 (168.126.228.101)  13.600 ms  6.597 ms  6.591 ms
 4 211.193.39.1 (211.193.39.1)  6.848 ms  6.884 ms  6.691 ms
 5 211.196.155.2 (211.196.155.2)  7.215 ms  7.023 ms  6.995 ms
 6 hh-k5-ge3.kornet.net (211.192.47.15)  7.749 ms  11.795 ms  50.576 ms
 7 128.134.40.182 (128.134.40.182)  8.389 ms  34.922 ms  13.549 ms
 8 211.39.255.229 (211.39.255.229)  134.076 ms  12.646 ms  7.442 ms
 9 211.45.90.253 (211.45.90.253)  8.134 ms  13.891 ms  7.714 ms
10 * * *
11 * * *
12 * * *
SWITCH#
```

6.3.4. 원격 접속자 확인

시스템에 접속한 사용자를 확인하려면 Privilege Exec Enable 모드나 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
where	Enable	시스템에 접속한 원격 사용자를 확인합니다.

다음은 시스템 관리자 이외에 IP 주소 172.16.119.251인 사용자가 시스템에 접속하고 있음을 보여 주고 있습니다.

```
SWITCH# where
admin at ttyS0 from console for 44 minutes 18.96 seconds
admin at tttyp0 from 172.16.119.251:1847 for 31 minutes 28.73 seconds
```

6.3.5. MAC table 보기

특정한 포트에 기록된 MAC 테이블을 출력할 때는 다음과 같은 명령어를 사용합니다.

명령어	모 드	기 능
show mac bridge-name [port-number]	Enable/Global/Bridge	MAC 주소를 출력합니다.

다음은 default에 기록된 MAC 테이블을 출력한 경우입니다.

```
SWITCH# show mac 1 1/1-1/3
SWITCH(config)# show mac 1 1/1-1/3
=====
port      mac addr          permission     status      in use
=====
1/1      00:d0:cb:22:00:49    OK           dynamic     0.02
1/2      00:0b:5d:99:58:4c    OK           dynamic     4.95
1/3      00:0b:5d:51:3a:a8    OK           dynamic     6.05
SWITCH(config)#

```



위의 출력되는 내용은 장비에 따라 달라질 수 있습니다.



MAC 테이블은 천여 개 이상의 MAC 주소가 등록되어 있습니다. 따라서 한꺼번에 출력되면 필요한 정보를 찾기가 힘들기 때문에 일정한 양을 출력한 후에는 「-more-」 가 출력되면서 대기 상태가 됩니다. 그러나 필요한 정보를 얻은 후에 “q” 키를 누르면, 나머지 테이블을 출력하지 않고 곧바로 시스템 프롬프트로 돌아갈 수 있습니다.

6.3.6. Aging time 설정

MAC 주소를 사용해 패킷을 주고 받는 장비는 패킷이 전송될 때마다 브로드캐스팅하는 것을 막기 위해 MAC table을 기록합니다. 이 때 불필요한 MAC 주소를 기록에서 삭제되는데, 일정한 시간 내에 응답이 없는 MAC 주소를 삭제하도록 설정하는 시간을 Aging time이라고 합니다. 이러한 Aging time을 설정하는 명령어는 다음과 같습니다.

명령어	모 드	기 능
mac aging-time <10-2147483647>	Bridge	MAC 주소 기록 유지 여부를 가리는 Aging time을 설정합니다.



Aging time의 Default는 300초로 설정되어 있습니다.

6.3.7. 장비 사용 시간 확인

사용자는 장비의 전원을 켜고 부팅한 이후부터 장비를 얼마나 사용하였는지 확인할 수 있습니다. 장비 사용 시간을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show uptime	Enable/Global/Bridge	사용자가 장비의 전원을 켠 이후부터 사용한 시간을 확인합니다.

6.3.8. 시스템 정보 확인

사용자는 장비의 모델명, 메모리 사이즈, 하드웨어 종류, NOS 버전 등을 다음 명령어를 사용하여 확인할 수 있습니다.

명령어	모 드	기 능
show system	Enable/Global/Bridge	사용자 장비의 시스템 정보를 확인합니다.

6.3.9. CPU 평균 사용량 확인

V5812G의 사용자는 장비의 CPU 평균 사용량을 확인할 수 있습니다. CPU 평균 사용량을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show cpuload	Enable/Global/Bridge	사용자 장비의 CPU 사용량 임계값과 CPU 평균 사용량을 확인할 수 있습니다.

한편, V5812G는 사용자의 필요에 따라 CPU의 평균 사용량과 동시에 자세한 사용 내역까지 확인할 수 있습니다. 장비의 CPU 사용 내역을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show cpu-trueload	Enable/Global/Bridge	사용자 장비의 자세한 CPU 사용 내역을 확인합니다.



참 고

show cpu-trueload 명령어를 사용하면 **show cpuload** 명령어로 출력되는 CPU 평균 사용량 정보까지 함께 확인할 수 있습니다.

6.3.10. CPU 트래픽 제한

V5812G는 CPU로 유입되는 패킷의 수 설정하여 CPU의 과부하를 방지할 수 있습니다. 단, 명령어로 사용되는 패킷 단위와 실제로 설정되는 단위가 다릅니다. 이 설정을 통해 어느 포트에서 CPU로 올라오는 패킷이 많은지 확인할 수 있습니다.

사용자 장비의 CPU로 유입된 패킷의 종류에 따라 트래픽을 제한하려면, 특정 포트에 다음 명령어를 사용하십시오.

명령어	모 드	기 능
cpu statistics-limit {unicast multicast broadcast} port-number <10-100>	Global	CPU로 유입되는 패킷의 종류에 따라 패킷의 수를 설정하여 제한합니다.
no cpu statistics-limit {unicast multicast broadcast all} [port-number all]		특정 혹은 모든 패킷의 종류에 따라 패킷의 수를 제한했던 설정을 해제합니다.



참 고

설정되는 패킷의 수 범위 <10-100>의 숫자는 10은 패킷 수 1000을 의미합니다. 예를 들면 100일 경우에는 10000개의 패킷을 의미합니다.



참 고

설정한 범위보다 더 많은 패킷이 CPU로 유입될 경우 syslog 메시지를 보내 경고합니다.

한편, 특정 포트의 CPU 트래픽 통계 정보를 초기화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear cpu statistics {port-number}	Global	해당 포트의 CPU 통계정보를 초기화합니다.

V5812G의 사용자는 장비의 CPU 통계 정보를 확인할 수 있습니다. CPU 평균 혹은 전체 통계 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show cpu statistics avg-pkt {port-number}	Enable/	CPU의 평균 트래픽을 확인합니다.
show cpu statistics total {port-number}	Global/	CPU의 전체 통계 정보를 확인합니다.
show cpu statistics-limit	Bridge	CPU의 패킷 수의 제한 정보를 확인합니다.

6.3.11. CPU 프로세스 확인

V5812G의 사용자는 프로세스별로 구분된 CPU 부하량을 확인할 수 있습니다. 사용자는 이 기능을 통해 CPU를 가장 많이 점유하고 있는 데몬, 불필요한 데몬의 존재 여부, 문제가 있는 데몬이 실행된 과정 등을 알 수 있습니다. 이러한 정보는 장비에 문제가 발생하였을 때 문제를 해결할 수 있는 중요한 단서가 될 수도 있습니다.

V5812G의 CPU 프로세스를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show process	Enable/Global	사용자 장비의 CPU 프로세스를 확인합니다.

6.3.12. 메모리 사용 정보 확인

사용자 장비의 메모리에 대한 정보를 확인하려면 Enable모드나 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show memory	Enable/	사용자 장비의 메모리 사용 정보를 확인합니다.
show memory {bgp dhcp imi lib nsm ospf pim rip }	Global/	특정 기능에 대한 Memory 사용량을 확인합니다.
show memory swch	Bridge	스위치의 메모리 태입별 사용 정보를 확인합니다.

6.3.13. 시스템 이미지 버전 확인

V5812G의 사용자는 현재 구동되고 있는 시스템 이미지의 버전을 확인할 수 있습니다. 현재 구동되고 있는 시스템 이미지 버전을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show version	Enable/Global/Bridge	시스템 이미지 버전을 확인합니다.

6.3.14. 시스템 이미지 파일 크기 확인

V5812G의 사용자는 시스템 이미지 파일의 크기를 확인할 수 있습니다. 시스템 이미지의 파일 크기를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show os-size	Enable/Global/Bridge	시스템 이미지 파일의 크기를 확인한 경우입니다.

6.3.15. 설치된 NOS 확인하기

사용자 장비의 플래시 메모리에 대한 정보를 보면 어떤 NOS가 설치되어 있는지 알 수 있습니다. 플래시 메모리에 대한 정보를 보려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show flash	Enable/Global/Bridge	장비의 플래시 메모리에 대한 정보를 알 수 있습니다.



주의

V5812G는 장비에 설치된 Flash Memory에 따라 Dual-OS를 제공할 수 있습니다.

V5812G는 장비에 설치된 Flash Memory에 따라 Dual-OS를 지원할 수 있습니다. Flash Memory는 **show system**으로 확인할 수 있습니다. 다음은 Dual-OS를 지원하는 경우의 정보입니다.

```
SWITCH(config)# show system

SysInfo(System Information)
Model Name      : V5812G_SFU
Main Memory Size : 512 MB
Flash Memory Size : 8 MB(SPANSION 29GL064N), 32 MB(SPANSION 29GL256N), 32
MB(SPANSION 29GL256N)
H/W Revision    : DS-TD-07P-B0
H/W Address     : 00:d0:cb:00:26:dd
RTC Information   : M41T11
(SFU) Serial Number : N/A
S/W Compatibility : 3, 7
NOS Version      : 3.03
B/L Version       : 5.15_266_667
PLD Version       : 0x0b

SWITCH(config)#

```

다음은 Dual-OS를 지원하는 장비에서 설치된 NOS를 확인하는 경우입니다.

```
SWITCH(config)# show flash

Flash Information(Bytes)

Area          total    used(%)    free
-----
OS1(default)(running) 33554432 14717736 18836696 3.03 #0011
OS2           33554432 14717736 18836696 3.03 #0011
CONFIG        4194304   352256   3842048
CONFIG        253906944    0   253906944
-----
Total         325210112 29787728( 9%) 295422384
SWITCH(config)#

```



주의

위의 정보는 제품에 따라 다를 수 있습니다.

6.3.16. Default OS 설정

V5812G는 장비에 설치된 Flash Memory에 따라 Dual-OS를 지원할 수 있습니다. Flash Memory가 8M+16M일 때에는 Single-OS, Flash Memory가 8M+32M일 때에는 Dual-OS가 제공됩니다. Flash Memory는 **show system**으로 확인할 수 있습니다. V5812G의 사용자는 두 가지의 시스템 이미지를 설치하였을 경우에 자신이 원하는 시스템 이미지를 Default OS로 설정할 수 있습니다.



참 고

V5812G는 기본적으로 os1에 설치된 시스템 이미지가 Default OS로 지정됩니다.

Default OS를 설정할 때에는 Enable모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
default-os {os1 os2}	Enable	Default OS를 설정합니다.

다음은 os1이 Default OS였던 V5812G의 Default OS를 os2로 바꾼 후 그 내용을 확인한 경우입니다.

```
SWITCH# show flash

Flash Information(Bytes)
Area      total      used      free
-----
OS1(default) 7864320  5367868  2234398  3.11 #1012
OS2          7864320  5115586  2748734  3.03 #1013
Config       524284   92160    432124
-----
Total        167252924 10575614  5415256

SWITCH# default-os os2
SWITCH# show flash
Flash Information(Bytes)
Area      total      used      free
-----
OS1          7864320  5367868  2234398  3.11 #1012
OS2 (default) 7864320  5115586  2748734  3.03 #1013
Config       524284   92160    432124
-----
Total        167252924 10575614  5415256

SWITCH#
```

6.3.17. 장비 상태 확인

V5812G의 일부 기종은 장비의 온도, 전원 상태, FAN 상태 등을 확인할 수 있습니다. 장비의 온도, 전원 상태, FAN 상태 등을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show status fan		장비의 FAN 상태를 확인합니다.
show status power	View/Enable/Global/Bridge	장비의 전원 상태를 확인합니다.
show status temp		장비의 온도를 확인합니다.

6.3.18. 모듈 정보 확인

V5812G는 서비스 포트가 SFP 모듈로 되어있습니다. SFP 모듈의 상태 등을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show port module-info port-number	Enable/Global/Bridge	SFP 모듈의 상태를 확인합니다.



주의

module dmi가 disable로 설정되어 있는 경우, **show port module-info** 명령어로 확인할 때 해당 포트의 DMI 정보가 출력되지 않습니다.

6.3.19. Tech-support 확인

V5812G는 설정 내용, 설정 파일, 로그 정보, 레지스터 정보, 메모리, 디버깅 정보 등을 확인할 수 있습니다. 이러한 정보들을 Tech-support라고 하고, Tech-support를 사용하면, 시스템 오류를 확인하고, 문제를 해결하는데 도움이 됩니다. Tech-support를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
tech-support {all crash-info} console		Console에서 Tech-support를 확인합니다.
tech-support {all crash-info} remote ip-address file-name {ftp tftp}	Enable	Tech-support를 지정한 IP 주소에 저장합니다.



참 고

위의 옵션에서 **all**을 선택하면, 모든 Tech-support 정보를 확인하고, **crash-info**를 선택하면, [SYSTEM], [SYSINFO], [VERSION], [TAG], [SHOW RUNNING-CONFIG], [VOLATILE SYSLOG], [NON-VOLATILE SYSLOG], [SWITCHING ASIC INFO], [UPTIME INFO], [FLASHINFO]만 확인할 수 있습니다.



참 고

Console에 출력되는 Tech-support는 Terminal screen의 출력 행수에 상관없이 한 번만 출력됩니다.

6.3.20. 부팅 정보 확인

한편, V5812G는 Kernel을 재시작할 때 Time Stamp와 함께 Watch-dog Reset 및 S/W Reset 정보를 남기게 됩니다. 이러한 정보를 이용하여 Boot-info를 확인할 수 있습니다. 장비의 Boot-info를 확인 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show boot-info	Enable/Global/Bridge	장비의 Boot Information을 확인합니다.



참 고

Cold Restart(H/W Reset)시는 reset과 관련된 날짜와 시간 정보가 출력되지 않습니다. 이는 해당 기능이 시스템 메모리(RAM)을 통해 기록 및 출력되기 때문입니다.

다음은 V5812G의 전원을 껐다가 다시 켰을 경우에 확인한 부팅 정보입니다.

```
SWITCH# show boot-info
-----
Type          Date        Time
-----
POWERBOOT     ---- / -- / --
                -- : -- : --
```

다음은 V5812G의 **reload** 명령어를 사용하여 시스템을 리부팅 한 직후에 확인한 부팅 정보입니다.

```
SWITCH# show boot-info
-----
Type          Date        Time
-----
SWREBOOT      2006/10/12   10:10:21
```

7. 네트워크 관리 기능 설정

V5812G와 장비가 속해 있는 네트워크를 관리할 수 있는 기능에 대한 설정 방법을 설명합니다. 이 장은 다음과 같은 내용으로 이루어져 있습니다.

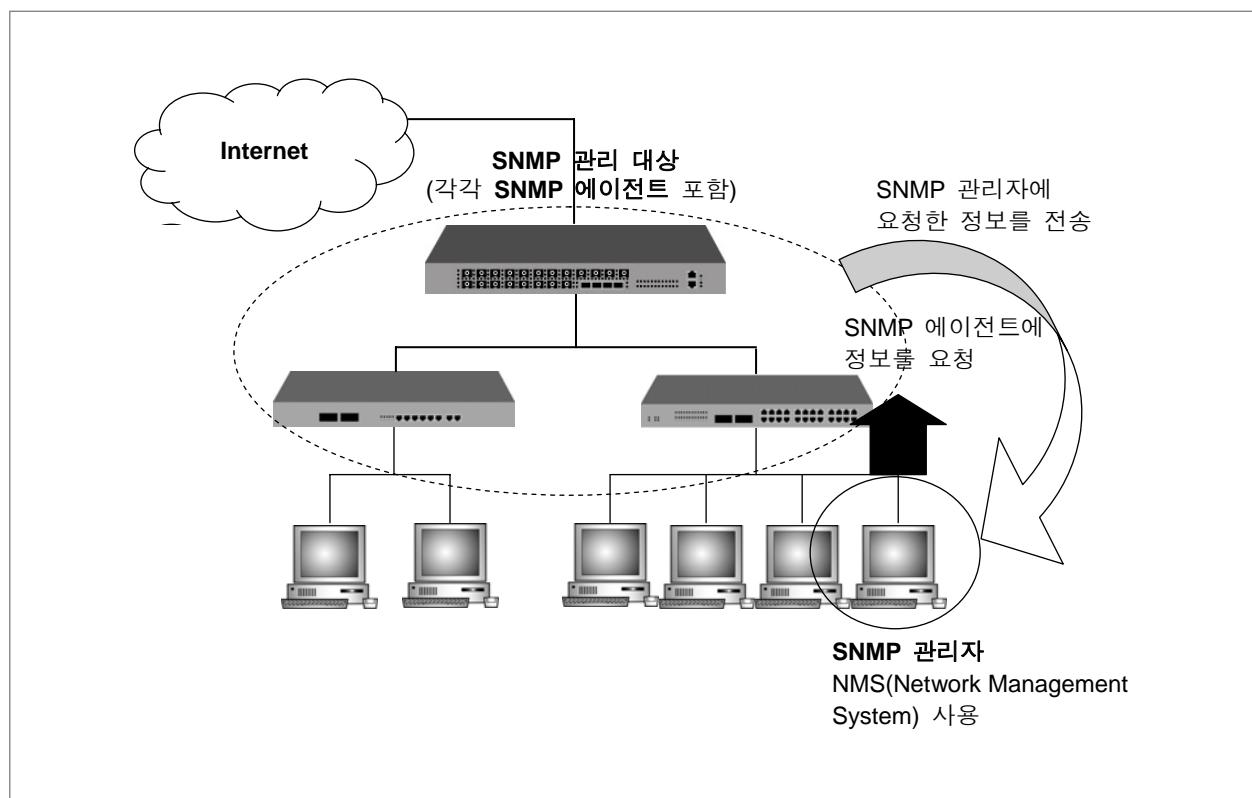
- SNMP 설정
- OAM 설정
- LLDP 설정
- RMON 설정
- Syslog 설정
- QoS 설정
- NetBIOS 필터링
- DHCP 서버 패킷 필터링
- Martion 필터링
- CPU 패킷 송신 필터링
- MAC 필터링
- 접속자 수 지정(Max Host)
- MAC 테이블 관리
- ARP(Address Resolution Protocol)
- ICMP 메시지 Control
- IP TCP flag control
- 패킷 라우팅 테이블 사용량 확인
- Dump packet
- Port Security

7.1 SNMP 설정

SNMP(Simple Network Management Protocol)는 SNMP 관리자, 관리 대상 네트워크를 구성하는 장비들, 그리고 관리 대상 장비에 설치되어 있는 SNMP 에이전트로 구성되어 있습니다. SNMP는 SNMP 관리자와 SNMP 에이전트 간의 통신을 가능하게 하는 프로토콜로 SNMP 관리자와 SNMP 에이전트가 주고 받는 정보 양식을 규정합니다.

장비에 SNMP를 설정할 때, 사용자는 SNMP 관리자와 에이전트 간의 관계를 명시하는데 Community에 따라 읽기 권한만 부여할 수도 있고 읽기와 쓰기 권한을 모두 부여할 수도 있습니다. SNMP 에이전트는 SNMP 관리자의 요청에 응답할 수 있는 MIB 변수를 가지고 있으며 SNMP 관리자는 에이전트로부터 데이터를 얻거나 에이전트에 데이터를 저장할 수 있습니다. 에이전트는 시스템과 네트워크에 대한 정보를 저장하고 있는 MIB에서 데이터를 얻습니다.

한편, SNMP 에이전트는 유사시에 발생하는 트랩(trap)을 관리자에게 전송할 수 있습니다. 트랩은 네트워크 상태를 SNMP 관리자에게 알리는 경고 메시지입니다. 트랩은 잘못된 사용자 인증, 재부팅, 연결 상태(활성화 상태 또는 비활성화 상태), TCP 연결 종료, 인접 장비와 통신 불가능 등과 같은 정보를 알려 줍니다.



【 그림 7-1 】 SNMP 구성의 예

SNMP가 지원되는 (주) 다산네트웍스의 장비는 v1을 선택하고 있습니다. 한편, V5812G는 SNMP v2c 및 v3까지도 지원하여 향상된 기능을 제공합니다. 이렇게 SNMP 기능 향상된 (주)다산네트웍스 장비는 SNMP 에이전트의 접속 관리를 더욱 강화하였고, 에이전트에게 공개하는 OID의 범위를 제한할 수 있습니다.

다음은 (주)다산네트웍스 장비에 SNMP를 설정하는 방법에 대한 목록입니다.

- SNMP v1의 Community 설정
- SNMP 에이전트의 관리자에 대한 연락처와 설치 위치 정보 지정
- SNMP v2c com2sec 설정
- SNMP v2c 및 v3의 Group 설정
- SNMP v2c 및 v3의 OID 공개 범위 제한(View 설정)
- SNMP v2c 및 v3의 제한 OID에 대한 접속권한부여(Access 설정)
- SNMP v3의 User 설정
- SNMP Trap-host 지정과 트랩 설정 및 해제
- SNMP 에이전트의 IP 지정
- SNMP 설정 확인
- SNMP 기능 해제



주의

SNMP는 그 발전도에 따라서 v1, v2c, v3가 있습니다. (주)다산네트웍스 장비는 각 제품별로 지원하는 버전이 다르므로 제품별로 설정의 적용여부가 다를 수 있습니다.

7.1.1. SNMP v1의 Community 설정

장비에 설치된 하나의 SNMP 에이전트는 한 무리의 여러 SNMP 관리자와 사이에 community라고 불리는 관계를 다수 형성할 수 있습니다. 하나의 SNMP 에이전트가 정의하는 각 community는 유일한 community name을 가지게 되는데, SNMP 관리자와 SNMP 에이전트에 동일한 community name이 설정되어 있어야 서로 간의 정보 공유가 가능합니다. 다음은 community name을 설정하는 명령어입니다.

명령어	모 드	기 능
snmp community community-name {ro rw} [ip-address] [oid]	Global	접속 권한을 부여하는 Community를 설정합니다.



참 고

(주)다산네트웍스의 장비에는 읽기 권한(ro)만 가지는 Community와 읽기/쓰기 권한(rw)을 가진 Community를 각각 최대 3개까지 설정할 수 있습니다.

Community는 일반적으로 우리가 알고 있는 패스워드의 의미를 내포하고 있습니다. 사용자는 지정하고 싶은 패스워드를 “*community-name*”라는 변수에 입력하십시오. 한편, 패스워드에 따라 SNMP 에이전트에 대한 접속 권한을 읽기로 한정하거나 읽기/쓰기의 모든 권한을 부여할 수 있습니다. 명령어 중에 제일 뒤에 오는 **ro**와 **rw**는 각각 **read-only**와 **read/write**의 약어로서 읽기 권한과 읽기/쓰기 권한을 구별해주는 명령어입니다.

한편, 설정한 Community를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no snmp community <i>community-name</i> {ro rw}	Global	Community를 삭제합니다.

설정한 Community를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show snmp community	Enable/Global	Community를 확인합니다.

[설정 예제 1]

다음은 읽기/쓰기 권한을 주는 *community name*을 *public*이라고 설정하고, 읽기 권한만 주는 *community name*을 *private*로 설정하는 예입니다.

```
SWITCH(config)# snmp community rw public
SWITCH(config)# snmp community ro private
SWITCH(config)# show snmp community

Community List
Type Community      Source      OID
-----
rw    public
ro    private

SWITCH(config)#

```

7.1.2. SNMP 에이전트의 관리자에 대한 연락처와 설치 위치 정보 지정

SNMP 에이전트의 시스템 관리자에 대한 정보와 에이전트가 설치된 장비 위치를 지정하면 해당 내용은 SNMP 설정 파일에 저장됩니다.

다음은 SNMP 에이전트의 시스템 관리자에 대한 정보 및 에이전트가 설치된 장비 위치를 지정할 때 사용하는 명령어입니다.

명령어	모 드	기 능
snmp contact name	Global	SNMP 에이전트의 시스템 관리자에 대한 정보를 입력합니다.
snmp location name		SNMP 에이전트가 설치된 장비 위치를 입력합니다.

한편, 설정한 SNMP 에이전트의 시스템 관리자에 대한 정보와 설치된 장비 위치를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no snmp contact	Global	등록했던 SNMP 에이전트의 시스템 관리자에 대한 정보를 삭제합니다.
no snmp location		등록했던 SNMP 에이전트가 설치된 장비 위치를 삭제합니다.

설정한 SNMP 에이전트의 시스템 관리자에 대한 정보와 설치된 장비 위치를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show snmp contact	Enable/Global	등록했던 SNMP 에이전트의 시스템 관리자에 대한 정보를 확인합니다.
show snmp location		등록했던 SNMP 에이전트가 설치된 장비 위치를 확인합니다.

[설정 예제 2]

다음은 SNMP 에이전트의 시스템 관리자에 대한 정보는 dasan<02.3484.6500>이며 SNMP 에이전트가 설치된 장비 위치는 Seoul,Korea 인 경우입니다.

```
SWITCH(config)# snmp contact dasan<02.3484.6500>
SWITCH(config)# show snmp contact
```

```
contact dasan<02.3484.6500>
```

```
SWITCH(config)# snmp location Seoul,Korea
SWITCH(config)# show snmp location
```

```
location Seoul,Korea
```

```
SWITCH(config)#

```

7.1.3. SNMP v2c의 com2sec 설정

SNMP v2에서는 어떤 호스트로부터의 접근을 허가할 것인가에 대한 호스트 출처와 Community Name을 관리하여 에이전트에 접근을 허가하는 방식을 택하고 있습니다. com2sec 명령어는 접근하려는 호스트의 범위와 Community Name을 Security Name이라는 형태로 정의합니다.

com2sec을 등록하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
snmp com2sec security-name {ip-address ip-address/m} community	Global	에이전트에 접근이 허용되는 Manager와 그 Community Name을 등록합니다.

등록한 com2sec을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no snmp com2sec security-name	Global	com2sec을 삭제합니다.

등록한 com2sec을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show snmp com2sec	Enable/Global	등록한 com2sec을 확인합니다.

[설정 예제 3]

다음은 com2sec을 설정하고 확인하는 경우의 예입니다.

```
SWITCH(config)# snmp com2sec dasan 100.1.1.1 public
SWITCH(config)# show snmp com2sec

Com2Sec List
SecName      Source      Community
-----
dalan        100.1.1.1    public

SWITCH(config)#

```

7.1.4. SNMP v2c 및 v3의 Group 설정

(주)다산네트웍스 장비의 운영·관리자는 SNMP의 에이전트에 접근하는 SNMP 관리자와 그 Community를 Group으로 설정할 수 있습니다. SNMP 에이전트에 접근하는 SNMP 관리자와 그 Community를 Group으로 설정하는 명령어는 다음과 같습니다.

명령어	모 드	기 능
snmp group group-name {v1 v2c v3} security-name	Global	SNMP Group을 <i>group-name</i> 으로 설정합니다.

{v1 | v2c | v3} 부분에는 설정하는 Group에 부여하고자 하는 보안 모델을 선택하면 됩니다. *security-name*은 com2sec에서 설정한 *security-name*을 사용합니다. 다만 SNMP v3 모델은 *security-name*이 SNMP의 기본 프로토콜의 일부분이므로 v2에서와 같은 com2sec에서의 설정 없이 곧바로 본 명령어에서 지정하여 사용할 수 있습니다. 한편, Group으로 설정했던 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no snmp group group-name [v1 v2c v3]	Global	Group을 해제합니다.

등록한 group을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show snmp group	Enable/Global	등록한 Group을 확인합니다.

[설정 예제 4]

다음은 Group을 설정하고 확인하는 경우의 예입니다.

```
SWITCH(config)# snmp group rogroup v1 dasan
SWITCH(config)# show snmp group

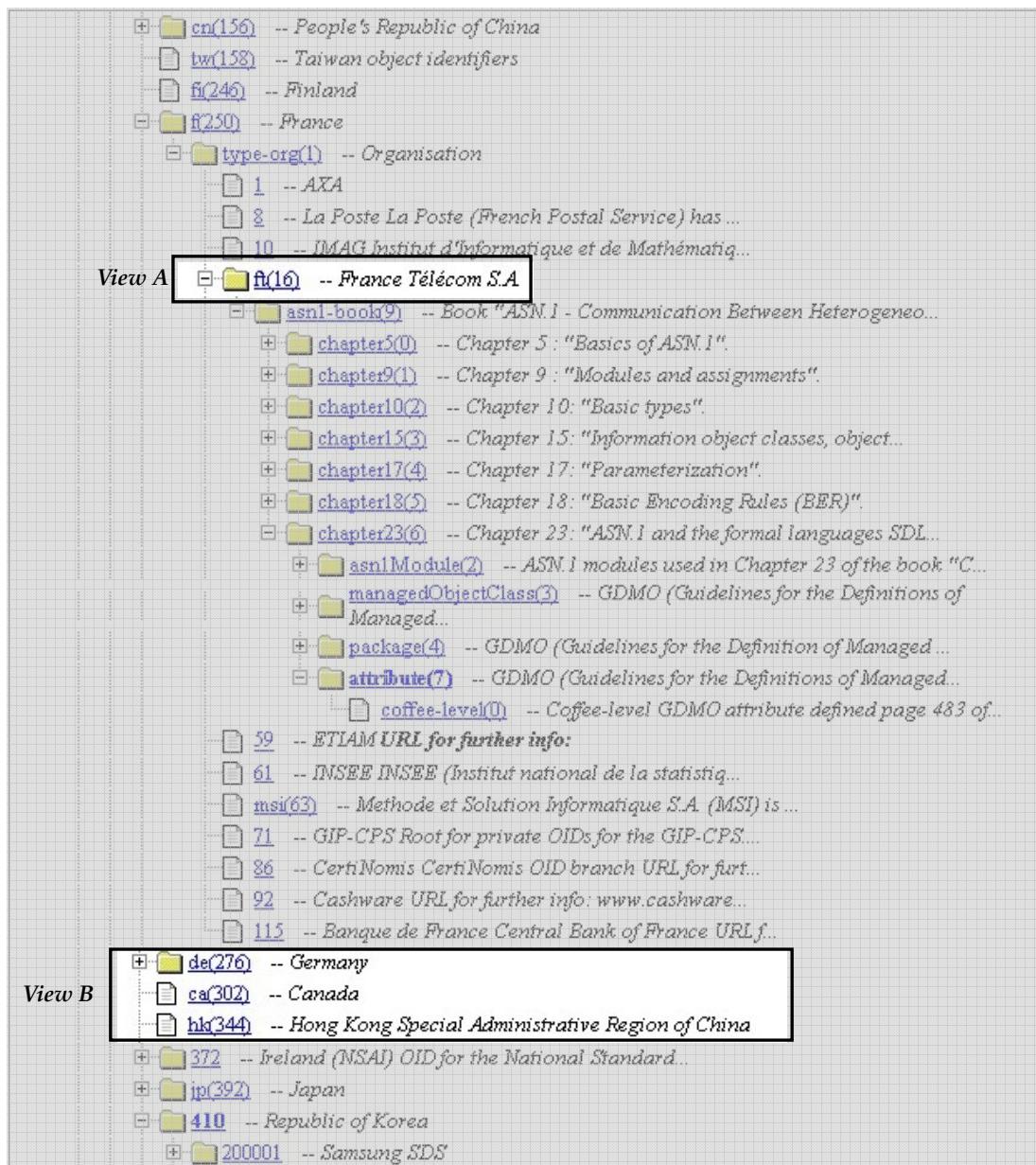
Group List
GroupName      SecModel  SecName
-----
rogroup        v1       dasan

SWITCH(config)#

```

7.1.5. SNMP v2c 및 v3의 OID 공개 범위 제한(View 설정)

SNMP v2c와 v3에서는 MIB의 열람범위를 정하는 개별 그룹을 설정할 수 있습니다. 이것을 “View”라고 합니다.



본 명령어를 사용하여 각 View마다 접근할 수 있는 MIB 계층 범위를 설정 또는 제한하는 View Name을 설정합니다.

(주)다산네트웍스 장비에 View를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
snmp view view-name included oid [mask]	Global	서브트리를 포함한 OID를 “view-name”으로 지정합니다.
snmp view view-name excluded oid [mask]		서브트리를 포함하지 않은 OID를 “view-name”으로 지정합니다.



[mask] 는 어떤 View에 OID가 속하는지 판단할 경우, 어느 OID 서브트리의 구성요소가 적절한지 통제할 때 사용될 수 있습니다. OID 전체가 포함될 때에는 생략할 수 있습니다.

설정한 View를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no snmp view view-name	Global	“view-name”라는 이름의 View를 삭제합니다.

설정한 View를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show snmp view	Enable/Global	등록한 View를 확인합니다.

[설정 예제 5]

다음은 View를 하나 등록하고, 그 내용을 확인한 경우입니다.

```
SWITCH(config)# snmp view TEST included 1.3.6
SWITCH(config)# show snmp view

View List
ViewName      Type      SubTree / Mask
-----
TEST          included  1.3.6

SWITCH(config)#

```

7.1.6. SNMP v2c 및 v3의 제한OID에 대한 접속권한부여(Access 설정)

(주)다산네트웍스 장비 중 SNMP v2c와 v3를 지원하는 장비의 관리자는 특정한 Group에게 공개 범위를 제한한 OID(=View)를 볼 수 있도록 설정할 수 있습니다.

특정 Group이 공개 제한된 OID에 접속할 수 있도록 허가하려면 다음 명령어를 사용하여 설정하십시오.

명령어	모 드	기 능
<code>snmp access group-name {v1 v2c} read-name write-name notify-name</code>	Global	SNMP v1과 SNMP v2c에서 해당 그룹에게 허가할 View를 설정합니다.
<code>snmp access group-name v3 {noauth auth priv} read-name write-name notify-name</code>		SNMP v3에서 해당 그룹에게 허가할 View를 설정합니다.

`read-name`, `write-name`, `notify-name`에는 View 설정에서 지정한 `view-name`을 사용합니다. 허가지정하지 않을 경우에는 `none`으로 입력합니다. `v1`, `v2c` 또는 `v3` 부분에는 Group 설정에서 Group에 부여한 보안 모델을 선택하면 됩니다.



참 고

{`noauth` | `auth` | `priv`} 부분은 보안 레벨을 지정합니다. `noauth`는 인증에 `username`을 사용하는 방식이고, `auth`와 `priv`는 MD5 또는 SHA알고리즘에 의한 인증방식입니다. 다만, `priv` 레벨은 DES 암호화를 사용하여 보안을 한층 강화한 것입니다.

공개가 제한된 OID에 접속을 허가하도록 설정한 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>no snmp access group-name</code>	Global	제한된 OID를 허가했던 Group을 해제합니다.

공개 제한된 OID에 접속 허가를 받은 Group을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>show snmp access</code>	Enable/Global	공개 제한된 OID에 접속 허가를 받은 Group을 확인합니다.

[설정 예제 6]

다음은 Access를 설정하고 확인하는 경우의 예입니다.

```
SWITCH(config)# snmp access rogroup v1 test none none
SWITCH(config)# show snmp access

Access List
GroupName      SecModel   SecLevel   ReadView      WriteView      NotifyView
-----
rogroup        v1          noauth     TEST          none          none

SWITCH(config)#

```

7.1.7. SNMP v3의 User 설정

SNMP v3에서는 에이전트의 보안인증 모델인 USM에 접근할 수 있는 User로 등록합니다. User를 등록하려면, 인증키를 함께 설정해야 합니다. SNMP v3를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
snmp user user-name {md5 sha} auth-passphrase [des] [private-passphrase]	Global	SNMP v3의 User를 설정합니다.



각각의 *passphrase*는 영문자 또는 숫자를 사용하여 설정할 수 있으며 최소 8자 이상이어야 합니다. 영문자는 대소문자, 특수문자 구분됩니다.

등록한 user를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no snmp user user-name	Global	User를 삭제합니다.

등록한 user를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show snmp user	Enable/Global	등록한 User를 확인합니다.

[설정 예제 7]

다음은 user를 설정하고 확인하는 경우의 예입니다.

```
SWITCH(config)# snmp user root md5 vertex25 des vertex66
SWITCH(config)# show snmp user

User List
Name          AuthMode AuthPassphrase  PrivMode PrivPassphrase
-----
root          md5      vertex25       des      vertex66

SWITCH(config)#

```

7.1.8. SNMP 트랩 설정

SNMP 트랩이란, 유사시 발생한 사건에 대해 SNMP 에이전트가 SNMP 관리자에게 보고하는 경고 메시지(alert message)입니다. SNMP 트랩 기능을 설정해 두면 특정한 사건이 발생했을 때 스위치가 네트워크 관리 프로그램에 관련 정보를 전송할 수 있습니다.

V5812G의 SNMP 트랩은 크게 Event 모드와 Alarm-report 모드로 나누어집니다. Event 모드에서는 장비에 설정되어 있는 기본적인 SNMP 트랩을 알리는 정도로 동작하고, Alarm-report 모드에서는 기본 SNMP 트랩이 동작하는 것은 물론, 좀 더 자세하게 구분된 SNMP 트랩들이 각각의 Level을 가지고 트랩 호스트에게 전달됩니다.



V5812G의 SNMP 트랩은 기본적으로 Event로 설정되어 있습니다.

(1) SNMP trap-host 지정

다음은 에이전트가 트랩 메시지를 전송하는 trap-host를 지정할 때 사용하는 명령어입니다. 이 때, *ip-address*에는 트랩을 전송받을 대상의 IP 주소를 입력하는데, 예를 들어 SNMP 관리자를 trap-host로 설정할 경우에는 SNMP 관리자의 IP 주소를 입력하시면 됩니다.

(주)다산네트웍스 장비는 SNMP v1의 trap-host와 SNMP v2c의 trap-host, 그리고 SNMP v3 inform-trap-host를 각각 설정할 수 있습니다.

명령어	모 드	기 능
snmp trap-host ip-address [community]	Global	SNMP v1의 trap 메시지의 수신자를 설정합니다.
snmp trap2-host ip-address [community]		SNMP v2c의 트랩 메시지의 수신자를 설정합니다.
snmp inform-trap-host ip-address [community]		SNMP v3 inform 통지의 수신자를 설정합니다.

[설정 예제 8]

다음은 IP 주소가 10.1.1.3인 관리자에게 트랩을 전송하도록 설정하는 경우의 예입니다.

```
SWITCH(config)# snmp trap-host 10.1.1.3
SWITCH(config)#
```



(주)다산네트웍스 장비의 SNMP trap-host는 최대 16개까지 설정할 수 있습니다.

trap-host를 복수로 지정할 경우, IP 주소를 하나씩 입력하면서 설정할 수도 있고, IP 주소를 열거하여 여러 개 씩 설정할 수도 있습니다.

[설정 예제 9]

다음은 IP 주소 10.1.1.3, 20.1.1.5, 30.1.1.2를 trap-host로 지정할 때 사용할 수 있는 두 가지 방법을 설명한 것입니다.

```
SWITCH(config)# snmp trap-host 10.1.1.3
SWITCH(config)# snmp trap-host 20.1.1.5
SWITCH(config)# snmp trap-host 30.1.1.2
SWITCH(config)#
SWITCH(config)# snmp trap-host 10.1.1.3 20.1.1.5 30.1.1.2
SWITCH(config)#

```

다음은 위에서 설정한 trap-host를 확인한 경우의 예입니다.

```
SWITCH# show running-config
(총략)
snmp trap-host 10.1.1.3 20.1.1.5 30.1.1.2
!
SWITCH#
```

한편, SNMP 트랩을 전송하도록 설정했던 내용을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no snmp trap-host ip-address	Global	해당 IP 주소로 트랩 메시지를 송신하도록 설정했던 것을 해제합니다.
no snmp trap2-host ip-address		해당 IP 주소로 SNMP v2c의 트랩 메시지를 송신하도록 설정했던 것을 해제합니다.
no snmp inform-trap-host ip-address		해당 IP 주소로 SNMP v3 inform 통지메시지를 송신하도록 설정했던 것을 해제합니다.

(2) SNMP 트랩 모드 설정

위에서 설명한 바와 같이 V5812G SNMP 트랩은 Event 모드와 Alarm-report 모드의 2종류가 있습니다. 기본적으로는 Alarm-report 모드로 설정되어 있지만, 사용자의 필요에 따라 SNMP 트랩 모드를 변경할 수 있습니다.

SNMP 트랩 모드를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
snmp trap-mode {event alarm-report}	Global	SNMP 트랩 모드를 설정합니다.

(3) Event 모드에서 SNMP 트랩 설정

위에서 설명한 바와 같이 V5812G의 SNMP 트랩은 크게 Event 모드와 Alarm-report 모드의 2종류로 나눠집니다. Event 모드로 설정되어 있을 때에는 다음과 같은 종류의 기본 트랩 가운데 관리자가 트랩 메시지를 송신하도록 설정해 놓은 것만 동작하게 됩니다.

【 표 7-1 】 V5812G의 기본 SNMP 트랩

SNMP 트랩	기 능 설 명
authentication-failure	SNMP에 접속하려는 사용자가 잘못된 Community를 입력하였을 때, Community가 잘못되었음을 알려주는 트랩 메시지입니다.
cold-start	SNMP 에이전트가 꺼졌다가 다시 재부팅 되었을 때 전송되는 트랩 메시지입니다.
cpu-threshold	CPU 사용량이 사용자가 본 매뉴얼 Syslog의 「CPU 사용량 임계값 설정」에서 설정한 CPU 사용량 임계값을 초과했음을 알려주는 트랩 메시지입니다. 또한, CPU 사용량이 다시 임계값 아래로 떨어지면 트랩 메시지로 떨어졌음을 알려줍니다.
dhcp-lease	DHCP 서버의 Subnet에서 더 이상 할당할 수 있는 IP 주소가 없는 상황임을 알리는 트랩 메시지입니다. Subnet이 여러 개 있을 때는 하나만 더 이상 할당할 수 있는 IP 주소가 없는 상황이면 트랩 메시지가 전송됩니다.
fan	장비의 Fan에 이상이 있을 때 트랩 메시지를 전송합니다.
link-up/down	사용자가 지정한 해당 포트의 네트워크 연결이 꺼졌을 때, 혹은 다시 네트워크 연결이 이루어졌을 때 전송되는 트랩 메시지입니다.
mem-threshold	본 매뉴얼 Syslog의 「사용 가능한 메모리 임계값 설정」에서 설정한 사용 가능한 메모리 임계값보다 남은 메모리량이 적을 때 알려주는 트랩 메시지입니다. 또한, 임계값보다 남은 메모리량이 다시 많아 졌을 때 알려주는 트랩 메시지입니다.
module	장비의 Module에 이상이 있을 때 트랩 메시지를 전송합니다.
port-threshold	포트 트래픽이 사용자가 본 매뉴얼 Syslog의 「포트 트래픽 임계값 설정」에서 설정한 임계값을 초과했음을 알려주는 트랩 메시지입니다. 또한, 포트 트래픽이 다시 임계값 아래로 떨어졌을 때도 트랩 메시지를 통해 알려줍니다.
power	장비의 Power에 이상이 있을 때 트랩 메시지를 전송합니다.
temp-threshold	장비 온도가 본 매뉴얼 Syslog의 「온도 임계값 설정」에서 설정한 임계값을 초과했음을 알려주는 트랩 메시지입니다.



V5812G는 기본적으로 위에서 설명한 트랩 메시지가 모두 송신되도록 설정되어 있습니다.

V5812G의 기본 SNMP 트랩은 기본적으로 각 상황에서 트랩 메시지를 송신하도록 설정되어 있습니다. 그러나 이 모든 트랩 메시지가 전달될 경우, 불필요한 트랩 메시지가 빈번하게 트랩 호스트에게 송신된다면 비효율적일 수 있습니다. 이러한 점을 고려하여 V5812G의 관리자는 트랩 호스트에게 전달되는 트랩 메시지의 종류를 선택할 수 있습니다.



참 고

V5812G의 SNMP는 기본적으로 모든 종류의 트랩이 송신되도록 설정되어 있습니다.

일단, Event 모드에서 동작하는 기본 SNMP 트랩 메시지의 동작을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no snmp trap auth-fail		
no snmp trap cold-start		
no snmp trap cpu-threshold		
no snmp trap dhcp-lease		
no snmp trap fan		
no snmp trap link-down port-number [node-number]	Global	해당 트랩 메시지의 동작을 해제합니다.
no snmp trap link-up port-number [node-number]		
no snmp trap mem-threshold		
no snmp trap module		
no snmp trap port-threshold		
no snmp trap power		
no snmp trap temp-threshold		

트랩 메시지가 송신되는 것을 해제했던 것을 다시 동작하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
snmp trap auth-fail	Global	auth-fail 트랩 메시지를 전송하도록 설정입니다.
snmp trap cold-start		cold-Start 트랩 메시지를 전송하도록 설정합니다.
snmp trap cpu-threshold		cpu-threshold 트랩 메시지를 전송하도록 설정합니다.
snmp trap dhcp-lease		dhcp-lease 트랩 메시지를 전송하도록 설정합니다.
snmp trap fan		fan 트랩 메시지를 전송하도록 설정합니다.
snmp trap link-down		link-down 트랩 메시지를 전송하도록 설정합니다.
<i>port-number [node-number]</i>		
snmp trap link-up		link-up 트랩 메시지를 전송하도록 설정합니다.
<i>port-number [node-number]</i>		
snmp trap mem-threshold		mem-threshold 트랩 메시지를 전송하도록 설정합니다.
snmp trap module		module 트랩 메시지를 전송하도록 설정합니다.
snmp trap port-threshold		port-threshold 트랩 메시지를 전송하도록 설정합니다.
snmp trap power		power 트랩 메시지를 전송하도록 설정합니다.
snmp trap temp-threshold		temp-threshold 트랩 메시지를 전송하도록 설정합니다.

(4) Alarm-report 모드에서 SNMP 트랩 설정

Alarm-report 모드에서 SNMP 트랩은 보다 자세하게 구분된 SNMP 트랩으로 장비의 상태를 알리게 됩니다. Alarm-report 모드에서 송신되는 세부 SNMP 트랩은 각각의 중요도를 설정할 수 있습니다. 중요도 순서는 중요도가 높은 순으로 critical > major > minor > warning > intermediate입니다. 관리자가 별도로 중요도를 설정하지 않았을 경우에는 장비에 설정되어 있는 기본 중요도로 적용되며, 기본 중요도는 minor입니다. 또한, 기본 중요도는 사용자가 변경할 수 있습니다. 별도로 중요도를 설정하지 않은 세부 SNMP 트랩에 기본적으로 적용되는 중요도를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
snmp alarm-severity default {critical major minor warning intermediate}	Global	기본적으로 적용되는 중요도를 설정합니다.



참 고

기본 중요도는 **minor**로 설정되어 있습니다.

Alarm-report 모드에서 사용되는 세부 SNMP 트랩은 중요도에 따라 송신 여부를 컨트롤 할 수 있습니다. 이 때 송신 여부를 판단하게 되는 기준이 되는 중요도를 Criteria라고 하며, SNMP 트랩의 중요도가 Criteria로 설정해 놓은 중요도와 같거나 작으면 SNMP 트랩은 송신되지 않습니다. SNMP 트랩의 송신을 결정하는 기준이 되는 Criteria를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
snmp alarm-severity criteria {critical major minor warning intermediate}	Global	SNMP 트랩 송신을 결정하는 기준이 되는 Criteria를 설정합니다.

Alarm-report 모드에서 사용되는 세부 SNMP 트랩의 중요도를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
snmp alarm-severity cold-start {critical major minor warning intermediate}	Global	Cold-start Alarm에 중요도를 설정합니다.
snmp alarm-severity broadcast-over {critical major minor warning intermediate}		Broadcast-over Alarm에 중요도를 설정합니다.
snmp alarm-severity cpu-load-over {critical major minor warning intermediate}		Cpu-load-over Alarm에 중요도를 설정합니다.
snmp alarm-severity dhcp-lease {critical major minor warning intermediate}		DHCP-Lease Alarm에 중요도를 설정합니다.
snmp alarm-severity dhcp-illegal {critical major minor warning intermediate}		DHCP-illegal Alarm에 중요도를 설정합니다.
snmp alarm-severity fan-fail {critical major minor warning intermediate}		Fan-fail Alarm에 중요도를 설정합니다.
snmp alarm-severity fan-remove {critical major minor warning intermediate}		Fan-remove Alarm에 중요도를 설정합니다.

명령어	모 드	기 능
snmp alarm-severity ipconflict {critical major minor warning intermediate}		Ipconflict Alarm에 중요도를 설정합니다.
snmp alarm-severity memory-over {critical major minor warning intermediate}		Memory-over Alarm에 중요도를 설정합니다.
snmp alarm-severity mfgd-block {critical major minor warning intermediate}		Mfgd-block Alarm에 중요도를 설정합니다.
snmp alarm-severity port-link-down {critical major minor warning intermediate}		Port-link-down Alarm에 중요도를 설정합니다.
snmp alarm-severity port-remove {critical major minor warning intermediate}		Port-remove Alarm에 중요도를 설정합니다.
snmp alarm-severity port-thread-over {critical major minor warning intermediate}		Port-thread-over Alarm에 중요도를 설정합니다.
snmp alarm-severity power-fail {critical major minor warning intermediate}		Power-fail Alarm에 중요도를 설정합니다.
snmp alarm-severity power-remove {critical major minor warning intermediate}	Global	Power-remove Alarm에 중요도를 설정합니다.
snmp alarm-severity rmon-alarm-rising {critical major minor warning intermediate}		Rmon-alarm-rising Alarm에 중요도를 설정합니다.
snmp alarm-severity rmon-alarm-falling {critical major minor warning intermediate}		Rmon-alarm-falling Alarm에 중요도를 설정합니다.
snmp alarm-severity stp-bpdu-guard {critical major minor warning intermediate}		STP BPDU Guard Alarm에 중요도를 설정합니다.
snmp alarm-severity stp-root-guard {critical major minor warning intermediate}		STP Root Guard Alarm에 중요도를 설정합니다.
snmp alarm-severity system-restart {critical major minor warning intermediate}		System-restart Alarm에 중요도를 설정합니다.
snmp alarm-severity module-remove {critical major minor warning intermediate}		Module-remove Alarm에 중요도를 설정합니다.
snmp alarm-severity temperature-high {critical major minor warning intermediate}		Temperature-high Alarm에 중요도를 설정합니다.

사용자의 설정을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no snmp alarm-severity cold-start		
no snmp alarm-severity broadcast-over		
no snmp alarm-severity cpu-load-over		
no snmp alarm-severity dhcp-lease		
no snmp alarm-severity dhcp-illegal		
no snmp alarm-severity fan-remove		
no snmp alarm-severity ipconflict		
no snmp alarm-severity memory-over		
no snmp alarm-severity mfgd-block		
no snmp alarm-severity port-link-down		
no snmp alarm-severity port-remove	Global	트랩의 중요도가 기본값으로 설정됩니다.
no snmp alarm-severity port-thread-over		
no snmp alarm-severity power-fail		
no snmp alarm-severity power-remove		
no snmp alarm-severity rmon-alarm-rising		
no snmp alarm-severity rmon-alarm-falling		
no snmp alarm-severity stp-bpdu-guard		
no snmp alarm-severity stp-root-guard		
no snmp alarm-severity system-restart		
no snmp alarm-severity module-remove		
no snmp alarm-severity temperature-high		

ADVA Alarm에 대한 중요도를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
snmp alarm-severity adva-fan-fail {critical major minor warning intermediate}	Global	adva-fan-fail Alarm에 대한 중요도를 설정합니다.
snmp alarm-severity adva-if-misconfig {critical major minor warning intermediate}		adva-if-misconfig Alarm에 대한 중요도를 설정합니다.
snmp alarm-severity adva-if-opt-thres {critical major minor warning intermediate}		adva-if-opt-thres Alarm에 대한 중요도를 설정합니다.
snmp alarm-severity adva-if-rcv-fail {critical major minor warning intermediate}		adva-if-rcv-fail Alarm에 대한 중요도를 설정합니다.
snmp alarm-severity adva-if-sfp-mismatch {critical major minor warning intermediate}		adva-if-sfp-mismatch Alarm에 대한 중요도를 설정합니다.
snmp alarm-severity adva-if-trans-fault {critical major minor warning intermediate}		adva-if-trans-fault Alarm에 대한 중요도를 설정합니다.
snmp alarm-severity adva-psu-fail {critical major minor warning intermediate}		adva-psu-fail Alarm에 대한 중요도를 설정합니다.
snmp alarm-severity adva-temperature {critical major minor warning intermediate}		adva-temperature Alarm에 대한 중요도를 설정합니다.
snmp alarm-severity adva-voltage-high {critical major minor warning intermediate}		adva-voltage-high Alarm에 대한 중요도를 설정합니다.
snmp alarm-severity adva-voltage-low {critical major minor warning intermediate}		adva-voltage-low Alarm에 대한 중요도를 설정합니다.

위의 명령어를 사용하여 설정한 내용을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no snmp alarm-severity adva-fan-fail	Global	사용자가 설정한 내용을 해제합니다.
no snmp alarm-severity adva-if-misconfig		
no snmp alarm-severity adva-if-opt-thres		
no snmp alarm-severity adva-if-rcv-fail		
no snmp alarm-severity adva-if-sfp-mismatch		
no snmp alarm-severity adva-if-trans-fault		
no snmp alarm-severity adva-psu-fail		
no snmp alarm-severity adva-temperature		
no snmp alarm-severity adva-voltage-high		
no snmp alarm-severity adva-voltage-low		

(5) ERP Alarm 중요도 설정 및 해제

ERP에 대한 Alarm의 중요도를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
snmp alarm-severity erp-domain-lotp {critical major minor warning intermediate}	Global	테스트 패킷을 3번 보내고, 응답이 없으면 전송하는 Alarm의 중요도를 설정합니다.
snmp alarm-severity erp-domain-multi-rm {critical major minor warning intermediate}		Multiple RM node가 생성되었을 때 전송되는 Alarm의 중요도를 설정합니다.
snmp alarm-severity erp-domain-reach-fail {critical major minor warning intermediate}		ERP Link Failurer가 감지되었을 때 전송하는 Alarm의 중요도를 설정합니다.
snmp alarm-severity erp-domain-ulotp {critical major minor warning intermediate}		테스트 패킷이 특정한 포트에서만 응답이 있을 때 전송하는 Alarm의 중요도를 설정합니다.

위에서 설정한 내용을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no snmp alarm-severity erp-domain-lotp	Global	ERP에 대한 Alarm 설정을 해제합니다.
no snmp alarm-severity erp-domain-multi-rm		
no snmp alarm-severity erp-domain-reach-fail		
no snmp alarm-severity erp-domain-ulotp		

(6) Notify-Activity 활성화

V5812G는 SNMP 트랩이 Alarm-report로 지정되어 있을 때, 관리자가 장비에 특정 기능을 설정하였을 때, 설정이 이루어졌음을 Notification으로 알리도록 되어 있습니다. 이러한 기능을 Notify-Activity라고 하며, Notification은 각 기능마다 내부적으로 정해져 있습니다. Notify-Activity를 활성화하여 장비에 특정 기능이 설정되었음을 알리도록 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
snmp notify-activity enable	Global	장비에 특정 기능이 설정되었음을 알리도록 합니다.



Notify-Activity 기능은 기본적으로 동작하지 않도록 설정되어 있습니다.

Notify-Activity를 다시 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
snmp notify-activity disable	Global	Notify-Activity를 해제합니다.

(7) SNMP 트랩 설정 확인

Event 모드에서 사용되는 기본 SNMP 트랩 관련 설정을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show snmp trap	Global	기본적인 SNMP 트랩 설정을 확인합니다.

[설정 예제 10]

다음은 auth-fail 트랩 메시지를 해제하고 그 내용을 확인한 경우입니다.

```
SWITCH(config)# no snmp trap auth-fail
SWITCH(config)# show snmp trap
```

```
Trap-Host List
      Host          Community
-----
inform-trap-host 30.1.1.1
trap2-host       20.1.1.1
trap-host        10.1.1.1

Trap List
Trap-type      Status
-----
auth-fail      disable
cold-start     enable
cpu-threshold enable
port-threshold enable
dhcp-lease     enable
power         enable
module        enable
fan            enable
temp-threshold enable
mem-threshold enable

SWITCH(config)#

```

사용자가 설정한 세부 SNMP 트랩의 중요도를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show snmp alarm-severity	Enable/Global	사용자가 설정한 Alarm의 중요도를 확인합니다.

[설정 예제 11]

다음은 alarm-severity에 대한 설정을 한 예입니다.

```
SWITCH(config)# snmp notify-activity enable
SWITCH(config)# snmp alarm-severity criteria critical
SWITCH(config)# snmp alarm-severity cpu-load-over warning
SWITCH(config)# show snmp alarm-severity
notify activity : enable
default severity : minor
severity criteria : critical
cpu-load-over : warning
SWITCH(config)#

```

한편, 장비에 전송된 alarm이 어떤 것이 있는지 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show snmp alarm-report	Global	장비에 전송된 alarm이 어떤 것이 있는지 확인합니다.
show snmp alarm-history		장비에 전송된 alarm의 기록을 확인합니다.

장비에 전송되어 기록된 alarm을 모두 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
snmp clear alarm-report	Global	장비에 전송된 alarm-report를 삭제합니다.
snmp clear alarm-history		장비에 전송된 alarm-history를 삭제합니다.



snmp clear alarm-report 명령어는 Trap-mode가 alarm-report 일 때만 사용 가능합니다..

다음은 장비에 전송된 alarm의 기록을 확인하고, 그 기록을 모두 지운 경우입니다.

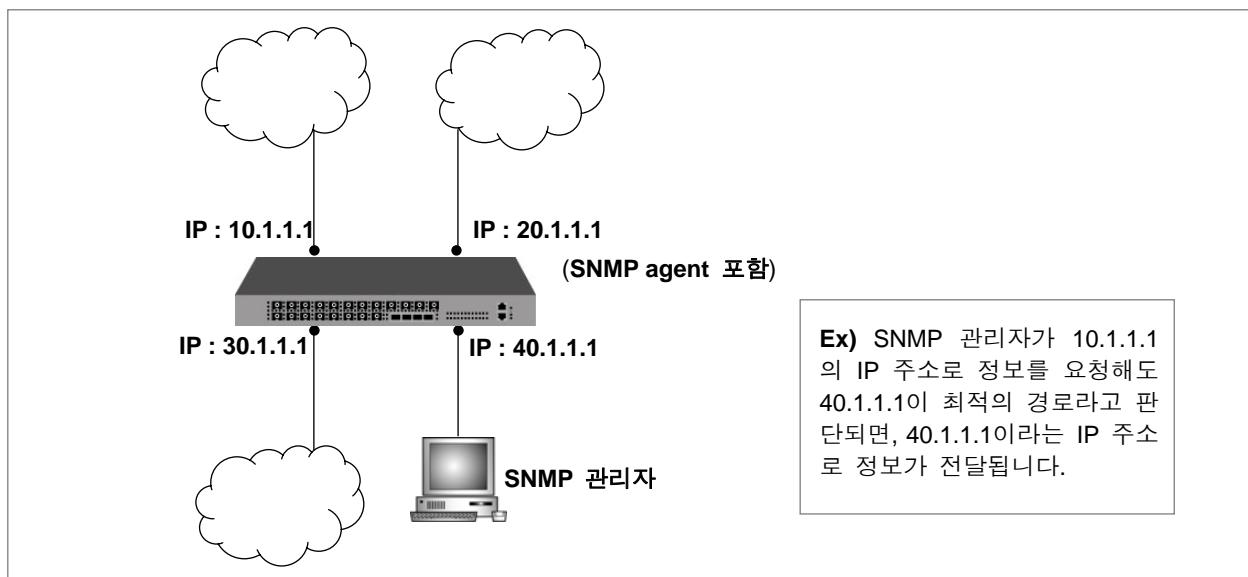
```
SWITCH(config)# show snmp alarm-history
cold-start minor Fri Mar 25 15:30:56 2005 System booted.
SWITCH(config)# snmp clear alarm-history
SWITCH(config)# show snmp alarm-history
SWITCH(config)#

```

7.1.9. SNMP 에이전트의 IP 지정

SNMP 에이전트가 여러 개의 IP 주소를 가지고 있을 경우, SNMP 관리자가 정보를 요청하면, SNMP는 최적의 경로를 통해 정보를 전달하도록 되어 있습니다. 따라서 관리자가 정보를 요청할 때 명기한 IP 주소와는 다른 주소를 가진 정보가 전달될 수 있습니다.

아래의 그림을 참조하시기 바랍니다.



그러나, V5812G는 관리자가 정보를 요청할 때 명기한 IP 주소로 다시 정보를 받을 수 있도록 SNMP 에이전트의 IP 주소를 지정할 수 있습니다. 위의 그림으로 설명하자면, SNMP 관리자가 에이전트의 IP 주소를 10.1.1.1로 지정하면, SNMP 정보는 늘 10.1.1.1이라는 IP 주소로 받게 되는 것입니다. SNMP 에이전트의 IP 주소를 지정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
snmp agent-address ip-address	Global	SNMP 에이전트의 IP 주소를 지정합니다.
no snmp agent-address ip-address		SNMP 에이전트의 IP 주소를 삭제합니다.



주의

SNMP 에이전트의 IP 주소로 지정되어 있는 IP를 장비에서 삭제하면, SNMP가 응답하지 않을 수 있습니다.

SNMP 에이전트의 IP 주소로 지정한 IP를 장비에서 삭제하려고 하면, 다음과 같이 SNMP가 응답하지 않을 수 있다고 알려줍니다.

```
SWITCH(config)# snmp agent-address 10.1.1.1
SWTICH(config)# interface default
SWITCH(config-if)# no ip address 10.1.1.1/8
Warning : 172.16.209.100/16 is specified to the SNMP agent address.
SNMP agent may not reply.
SWITCH(config-if)#

```

SNMP 에이전트의 IP 주소를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show snmp agent-address	Enable/Global	SNMP 에이전트의 IP 주소를 확인합니다.

7.1.10. SNMP 설정 확인

사용자가 설정한 SNMP에 대한 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show snmp	Enable/Global	SNMP 설정 내용을 확인합니다.

7.1.11. SNMP 기능 해제

SNMP 기능을 중단시키려면, Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no snmp	Global	SNMP 기능을 해제합니다.



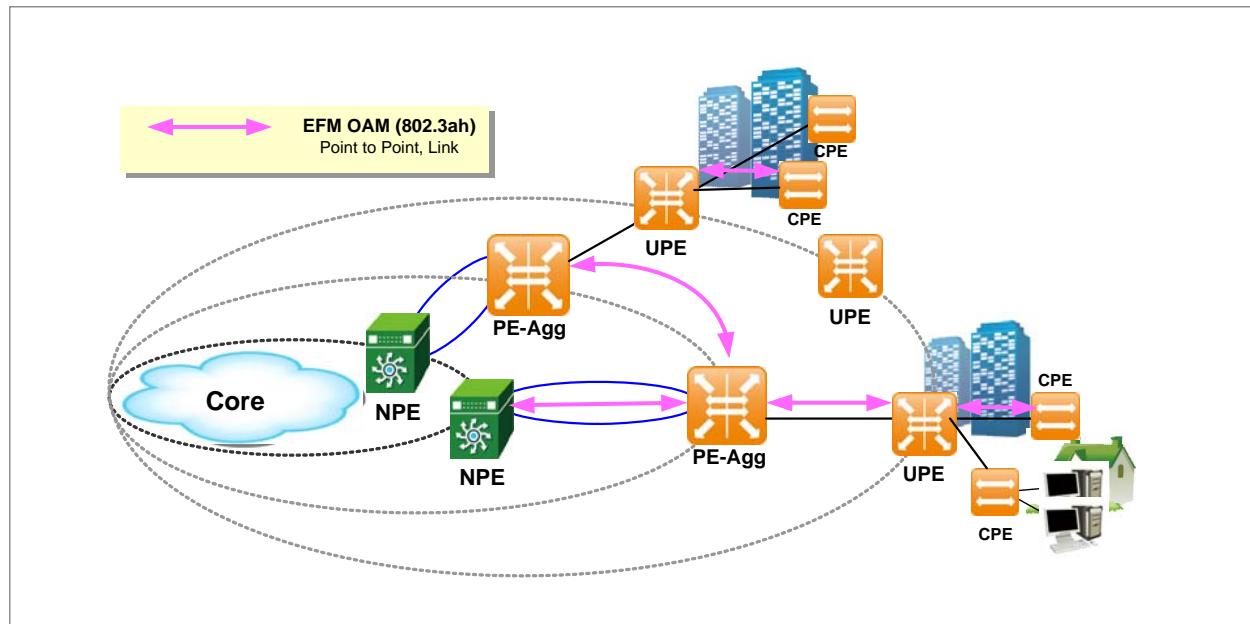
주의

위의 명령어를 사용하면 SNMP와 관련된 모든 설정 내용이 삭제됩니다.

7.2 EFM OAM(Operation, Administration, Maintenance)

일반적으로 네트워크를 관리할 때에는 SNMP(Simple Network Management Protocol)을 사용해 왔습니다. SNMP는 널리 사용하고 있는 만큼 유연성 있는 기능이긴 하지만, 관리 대상이 되는 장비에 IP 주소가 할당되어 있을 때에만 가능합니다. 따라서, Layer 2 환경에서는 적합하지 않습니다.

이러한 이유로 모든 네트워크에서 관리가 가능한 기능이 필요하게 되었고, OAM(Operation, Administration, Maintenance)라는 기능이 만들어지게 되었습니다. OAM은 이더넷 링크를 모니터링을 하거나 Troubleshooting 함으로써 SNMP를 보완하는 기능이며, SNMP의 모든 관리 기능을 대신하여 사용할 수는 없습니다. 따라서 Layer 2가 아닌 Layer 3에서는 IP 기반의 SNMP가 요구됩니다.



【 그림 7-2 】 EFM OAM 시나리오

EFM OAM은 Link 상태와 장애 위치, 장애 원인 등을 신속하게 감지하고, 이를 관리자에게 알려줌으로써 Link를 관리하도록 합니다. 이러한 정보들은 OAMPDU(OAM Protocol Data Unit)을 통해 전달됩니다. 관리자가 되는 장비를 Local DTE(Data Terminal Equipment), 관리 대상이 되는 장비를 Remote DTE라고 합니다.

다시 말하면, Local DTE는 Remote DTE로부터 전달받은 OAMPDU에서 Link 장애 등의 정보를 얻어 Remote DTE를 관리하는 것입니다.

EFM OAM은 다음과 같이 동작합니다.

◊ OAM Discovery

Local DTE와 Remote DTE가 OAMPDU를 통해 OAM 정보를 교환합니다.

◊ Remote Loopback

Remote DTE가 정상적으로 연결되어 있는지 확인하는 단계입니다.

- Local DTE에서 OAMPDU를 사용하여 Remote DTE의 Loopback을 활성화합니다.
- Loopback 기능을 사용하여 Link 상태를 모니터링 합니다.

◊ Link 모니터링

Link의 장애를 모니터링하고, 장애가 발생했을 경우에는 해당 Event 통보 OAMPDU를 Remote DTE에게 전송합니다.

◊ Remote DTE 장애 알림

Local DTE는 Remote DTE의 Loss of Signal(Link 장애), 복구가 불가능한 에러(Dying Gasp), 치명적 에러(Critical Event) 상태를 알려줍니다.

◊ 다양한 정보 습득

Local DTE는 Request OAMPDU를 보내 그에 대한 답으로 Remote OAM 포트에 있는 다양한 MIB 정보를 얻어냅니다.

7.2.1. OAM 활성화

EFM OAM 기능을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam efm enable port-number	Global	EFM OAM 기능을 활성화 합니다.

EFM OAM 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam efm disable port-number	Global	EFM OAM 기능을 해제 합니다.

7.2.2. OAM Link 모니터링

OAM Link 모니터링 기능을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam efm link-monitor enable port-number	Global	Link 모니터링 기능을 활성화 합니다.
oam efm link-monitor disable port-number		Link 모니터링 기능을 해제 합니다.

Event의 종류에 따라 Window의 크기와 임계값을 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam efm link-monitor frame window <10-65535> threshold <0-65535> port-number	Global	특정 시간 동안의 errored 프레임의 개수의 임계값을 지정합니다. (Window 기본값: 30초)
oam efm link-monitor frame-period window <1000-200000000> threshold <0-65535> port-number	Global	특정 프레임의 개수에서 errored 프레임의 개수 임계값을 지정합니다. (Window 기본값: 1000000)

OAMPDU를 통해 Event를 인지한 후 관리자에게 알리는 정책을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam efm link-monitor action syslog port-number	Global	Link 모니터링 정보를 syslog로 출력합니다.
oam efm link-monitor action snmp-trap port-number		Link 모니터링 정보를 SNMP Trap 메시지로 출력합니다.

7.2.3. EFM OAM 모드 설정

EFM OAM의 모드를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam efm mode {active passive} port-number	Global	EFM OAM의 모드를 설정합니다.



참 고

EFM OAM 모드 중 **active**는 Request와 Loopback이 모두 가능한 상태입니다. 반대로 **passive**는 Request와 Loopback을 요청할 수 없는 상태를 나타냅니다.

7.2.4. OAM Loopback 설정

OAM Loopback 기능은 사용자의 장비와 상대방 장비가 모두 OAM 프로토콜을 지원해야 합니다.

OAM Loopback 기능은 사용자가 상대방 장비까지 Loopback 기능을 활성화하고, Loopback을 실행합니다.

Remote DTE의 Loopback 기능을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam efm remote-loopback enable port-number	Global	Remote DTE의 Loopback 기능을 활성화합니다.

Remote DTE의 Loopback 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam efm remote-loopback disable port-number	Global	Remote DTE의 Loopback 기능을 해제합니다.

Loopback을 실행하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam efm remote-loopback test port-number	Global	Loopback을 실행합니다.

7.2.5. OAM Unidirection 설정

Local DTE에서 RX가 불가능할 때, TX를 이용해서 자신의 정보를 전송할 수 있습니다. 이러한 기능을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam efm undir enable port-number	Global	RX가 불가능할 때, TX를 이용해서 자신의 정보를 전송하도록 설정합니다.

다음은 RX가 불가능할 때 TX를 사용하여 자신의 정보를 전송하도록 설정한 것을 해제할 때 사용하는 명령어입니다.

명령어	모 드	기 능
oam efm unidir disable port-number	Global	RX가 불가능할 때, TX를 이용해서 자신의 정보를 전송하도록 설정한 것을 해제합니다.

7.2.6. OAM 설정 확인

OAM 설정 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show oam efm	Enable/ Global/ Bridge	EFM OAM 활성화 여부를 확인합니다.
show oam efm link-monitor port-number		포트 별 Link 모니터링 정보 및 포트에 수신된 Remote 통계를 확인합니다.
show oam efm remote port-number		Remote DTE 상태 및 기능에 대한 정보를 확인합니다.
show oam efm local port-number		Local DTE 상태 및 기능에 대한 정보를 확인합니다.

Local DTE가 Variable Request OAMPDU를 전송하여 수신된 Variable Response OAMPDU 값을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show oam efm variable branch-number leaf-number port-number	Enable/ Global/ Bridge	MIB를 Remote DTE에게 요청하여 수신된 값을 확인합니다.



*branch number*는 상대편 OAM 정보의 확인을 위해 사용되는 MIB 변수를 의미하며 0-255에서 설정 가능합니다. *leaf number*는 0에서 65535까지 설정할 수 있습니다.

7.3 LLDP 설정

LLDP(Link Layer Discovery Protocol)은 IEEE 802.1ab 표준에 따라 LAN에 연결된 장비들 사이에 네트워크 관리에 필요한 자료를 송수신하도록 하는 기능입니다.

7.3.1. LLDP 동작 원리

LLDP를 지원하는 V5812G는 서로 근접한 장비들 사이에서 관리 정보를 주고 받습니다. 이 관리 정보에는 각 장비들을 식별할 수 있는 고유 관리 정보와 해당 기능을 나타내기 위한 것들이 포함되며 이러한 정보들은 내부 MIB(Management Information Base)에 저장됩니다.

(1) LLDP 동작 방식

LLDP가 동작하기 시작하면, 장비들은 자신의 정보를 근접한 장비들에게 보냅니다. 그리고, Local의 상태가 변화되면, 이를 알리기 위해 또 다시 자신의 바뀐 정보를 근접한 장비들에게 보냅니다. 예를 들어 포트 상태가 disable로 바뀌면, 근접한 장비들에게 포트가 비활성화 되었음을 알려줍니다. 한편, 근접한 장비들로부터 정보를 받은 장비들은 LLDP 프레임을 수신 처리하여 다른 장비들의 정보를 보관하게 됩니다. 다른 장비들로부터 수신된 정보들은 Ageing됩니다.

7.3.2. LLDP 설정

LLDP를 설정하는 방법은 다음과 같습니다.

(1) LLDP 활성화

LLDP를 동작하도록 하려면, LLDP를 활성화시켜야 합니다. LLDP를 활성화시키려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lldp port-number	Bridge	해당 포트에서 LLDP를 활성화
lldp port-number mgmtaddr mgmt-ip-address		해당 포트에서 LLDP를 활성화시키고 LLDP 프레임에 할당할 IP를 설정합니다.



참 고

*mgmt-ip-address*는 LLDP 프레임이 전송될 때 가지는 IP 주소입니다.

LLDP를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no lldp port-number	Bridge	해당 포트에서 LLDP를 해제합니다.
no lldp port-number mgmtaddr mgmt-ip-address		해당 포트에서 LLDP를 해제합니다.

(2) LLDP 동작 방식 설정

포트에서 LLDP를 활성화시켰다면, LLDP의 동작 방식을 설정해야 합니다.



V5812G의 LLDP 동작 방식은 기본적으로 프레임에 대한 처리를 진행하지 않도록 설정되어 있습니다.

LLDP의 동작 방식을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lldp adminstatus port-number {both tx_only rx_only}	Bridge	포트의 LLDP 동작방식을 설정합니다.

LLDP 동작 방식 가운데 **tx_only**는 LLDP 프레임을 수신하는 동작만 진행하는 것이고, **rx_only**는 LLDP 프레임을 송신하는 동작만 진행하는 것입니다. 마지막으로 **both**는 TX와 RX를 동시에 진행하는 것으로, LLDP 프레임을 송수신하는 동작을 모두 진행하는 것입니다.

한편, LLDP 동작 방식을 프레임을 처리하지 않도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lldp adminstatus port-number disable	Bridge	LLDP 프레임에 대한 처리를 진행하지 않는다.

(3) Basic TLV 설정

LLDC는 TLV를 통해 정보를 전달합니다. TLV에는 반드시 보내야 하는 필수(Mandatory) TLV와 선택할 수 있는(Optional) TLV가 있습니다. 선택 TLV는 Basic TLV와 기타(organizationally specific) TLV가 있는데, Basic TLV는 LLDP가 구현된 장비들에 반드시 존재하는 것이고, 기타 TLV는 그 밖의 장비 특성에 따라 추가될 수 있는 것입니다.

V5812G는 관리자가 Basic TLV의 전송을 선택하여 활성화하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lldp port-number {portdescription sysname sysdescription syscap}	Bridge	해당 포트에서 송신할 Basic TLV를 선택합니다.

송신하도록 설정했던 Basic TLV를 송신하지 않도록 하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no lldp port-number {portdescription sysname sysdescription syscap}	Bridge	해당 포트에서 송신하도록 설정했던 Basic TLV를 송신하지 않도록 합니다.

(4) LLDP 메시지 송신 관련 설정

V5812G는 LLDP 메시지 송신 간격 및 회수를 설정할 수 있습니다. LLDP 메시지 송신 간격과 송신 회수를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lldp msg txinterval <5-32768>	Bridge	LLDP 메시지의 주기적인 송신 간격을 지정합니다. 단위는 초입니다.
lldp msg txhold <2-10>		LLDP 메시지의 주기적인 송신 회수를 지정합니다.



V5812G는 기본적으로 LLDP 메시지를 30초 마다 4번 송신하도록 설정되어 있습니다.

(5) Reinitdelay 설정

V5812G의 관리자는 LLDP 프레임을 처리하지 않도록 설정한 때로부터 다시 이를 활성화하기까지의 시간을 설정할 수 있습니다.

LLDP 프레임을 처리하지 않도록 설정한 후 이를 다시 활성화하기까지의 시간을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lldp reinitdelay <1-10>	Bridge	LLDP 프레임을 처리하지 않도록 설정한 때로부터 다시 이를 활성화하기까지의 시간을 설정합니다.



V5812G는 기본적으로 LLDP 프레임을 처리하지 않도록 설정한 때로부터 다시 이를 활성화하기까지의 시간을 2초로 설정하고 있습니다.

(6) LLDP 프레임 전송 Delay 시간 설정

V5812G 관리자는 LLDP 프레임을 주고받는 장비간에서 프레임 전송 Delay 시간을 설정할 수 있습니다. LLDP 프레임 송수신 Delay 시간을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lldp txdelay <1-8192>	Bridge	LLDP 프레임을 주고받는 장비간에서 프레임 전송 Delay 시간을 설정합니다.



V5812G는 기본적으로 LLDP 프레임을 주고 받는 프레임 전송 Delay 시간을 2초로 설정하고 있습니다.

(7) LLDP 설정 확인

LLDP 관련 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show lldp config [port-number]	Enable/Global/Bridge	LLDP 관련 설정내용을 확인합니다.
show lldp remote [port-number]		Remote 엔트리들의 Statistics 내용을 확인합니다.

LLDP 관련 동작 상태 및 통계 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show lldp statistics port-number	Enable/Global/Bridge	LLDP 관련 동작 상태 및 통계를 확인합니다.

한편, 포트에 누적된 통계량을 초기화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear lldp statistics port-number	Bridge	포트에 누적된 통계량을 초기화합니다.

7.4 RMON 설정

RMON(Rmote Monitoring)은 이더넷에 연결된 각 장비들의 통신 상태를 원격으로 점검하고 확인할 수 있는 기능입니다. SNMP는 SNMP 에이전트가 탑재된 장비 자신에 대한 정보만을 얻을 수 있는 반면, RMON은 장비를 포함한 세그먼트 전체에서 발생하는 정보를 파악할 수 있기 때문에 보다 효율적으로 네트워크를 관리할 수 있습니다. 예를 들면, SNMP는 특정 포트에서 발생하는 트래픽에 대해서만 알 수 있지만, RMON은 네트워크 전체에서 발생한 트래픽, 세그먼트에 연결된 각 호스트의 트래픽, 호스틀간의 트래픽 발생 현황 등도 알 수 있습니다.

RMON은 상당히 많은 양의 데이터를 처리하기 때문에 프로세서(processor) 점유율이 높습니다. 따라서 RMON 사용으로 인해 시스템의 성능이 저하되거나 네트워크 전송에 과부하가 걸리지 않도록 관리자가 각별히 신경을 써야 합니다. RFC 1757에는 Statistics, History, Alarm, Host, Host Top N, Matrix, Filter, Packet capture, Event의 9가지의 RMON MIB그룹이 정의되어 있습니다. (주)다산네트웍스의 V5812G는 이 가운데 가장 기본적인 Statistics, History, Alarm, Event의 4가지 MIB그룹을 지원합니다.

7.4.1. RMON History 설정

RMON History는 이더넷 포트에서 발생하는 각종 트래픽에 대한 통계 데이터를 주기적으로 표본 조사하는 기능입니다. 모든 포트의 통계 데이터는 기본적으로 30분마다 한 번씩 점검되고 한 포트 당 50개의 통계 데이터를 저장하도록 설정되어 있습니다. 사용자는 포트를 주기적으로 점검하는 시간과 저장 가능한 통계 데이터 수를 변경할 수 있습니다.

다음은 History의 기본 설정 내용입니다.

```
SWITCH(config)# show running-config
(중략)
rmon-history 1
  owner monitor
  data-source ifIndex.n1/port1
  interval 30
  requested-buckets 50
(중략)
SWITCH(config)#

```

RMON History를 설정하기 위해서는 일단 History 설정 모드로 들어가야 합니다. History 설정 모드로 들어가려면 다음과 같은 명령어를 사용하십시오.

명령어	모 드	기 능
rmon-history number	Global	RMON 히스토리를 구별할 수 있도록 번호를 설정합니다. 1부터 65,534까지 쓸 수 있습니다.

History 설정 모드로 들어가면 시스템 프롬프트가 SWITCH(config)#에서 SWITCH(config-rmonhistory[n])#로 바뀝니다. 이 때 변수 “n”은 서로 다른 History를 구별하기 위해 설정하는 번호입니다.

다음은 5번 History에 대해 설정하기 위한 History 설정 모드로 들어간 경우의 예입니다.

```
SWITCH(config)# rmon-history 1
SWITCH(config-rmonhistory[1])#
```

History 설정 모드에서 RMON History와 관련, 설정할 수 있는 명령어를 알아보려면 History 설정 모드의 시스템 프롬프트에서 물음표를 입력하십시오. 다음은 History 설정 모드에서 사용할 수 있는 명령어를 출력한 것입니다.

```
SWITCH(config-rmonhistory[1])# ?
active          Activate the history
data-source     Define the data source object for the ethernet port
exit            Exit current mode and down to previous mode
interval        Define the time interval for the history
list             Print command list
owner           Assign the owner who define and is using the history resources
requested-buckets Define the bucket count for the interval
show            Show running system information
SWITCH(config-rmonhistory[1])#
```



주의

실제로 물음표는 출력되지 않고, 물음표를 입력하면 곧장 명령어가 출력됩니다.

한편, History 설정 모드에서 빠져나와 Global 설정 모드로 돌아가거나 Privilege Exec Enable 설정 모드로 곧장 돌아가려면 다음의 명령어를 사용하십시오.

명령어	모 드	기 능
exit	RMON	Global 설정 모드로 돌아갑니다.

다음은 각각 History 설정 모드에서 Global 설정 모드로 돌아가는 경우와 Privilege Exec Enable 설정 모드로 돌아가는 경우의 예입니다.

```
SWITCH(config-rmonhistory[1])# exit  
SWITCH(config)#
```

```
SWITCH(config-rmonhistory[1])# end  
SWITCH#
```

(1) 통계 데이터 발생 포트 지정

RMON History를 설정할 때에는 반드시 통계 데이터가 발생하는 포트를 지정해야 합니다. 특정 포트에서 발생한 통계 데이터를 표본 조사하려면 다음 명령어를 사용하여 특정 포트를 지정하십시오.

명령어	모 드	기 능
data-source data-object-id	RMON	통계 데이터가 발생하는 포트를 지정합니다. <i>object</i> 변수는 “ ifIndex .number ”의 형태로 입력하십시오.

다음은 포트 1번을 데이터 발생지로 설정하는 경우입니다.

```
SWITCH(config-rmonhistory[1])# data-source ifindex.default  
SWITCH(config-rmonhistory[1])#
```

(2) RMON History 사용 주체 명시

사용자는 RMON 히스토리를 설정하고 히스토리가 제공하는 여러 가지 정보를 이용하는 주체를 명시할 수 있습니다.

History를 사용하는 주체를 명시하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
owner name	RMON	History를 설정하고 관련 정보를 이용하는 주체를 명시합니다.

다음은 History 주체를 “dasan”으로 설정한 경우입니다.

```
SWITCH(config-rmonhistory[1])# owner dasan
SWITCH(config-rmonhistory[1])#
```



History를 설정하는 주체를 입력할 때에는 최대 32자까지만 입력이 가능합니다. 32자를 넘는 이름이 입력될 경우 “%Too long owner name”이라는 에러 메시지를 보여줍니다.

(3) 표본 데이터 수 설정

사용자는 RMON History에서 표본 조사할 데이터 수를 지정할 수 있습니다. 표본 조사할 데이터 수를 지정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
requested-buckets count	RMON	표본 조사에 사용할 데이터 수를 지정합니다.

다음은 History에서 표본 조사할 데이터 수를 25개로 설정하는 경우의 예입니다.

```
SWITCH(config-rmonhistory[1])# requested-buckets 25
SWITCH(config-rmonhistory[1])#
```



표본 조사할 데이터 수는 65535개까지 가능합니다.

(4) 표본 조사 간격 설정

사용자는 RMON History가 표본 조사를 하는 주기적인 시간 간격을 초 단위로 설정할 수 있습니다.

표본 조사 시간 간격을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
interval time	RMON	표본 조사 시간을 지정합니다. 기본 설정 시간은 30초입니다.

다음은 표본 조사 시간을 60초로 지정한 예입니다.

```
SWITCH(config-rmonhistory[1])# interval 60  
SWITCH(config-rmonhistory[1])#
```



표본 조사를 하는 시간 간격을 설정할 때, 3600초까지 설정이 가능합니다.

(5) RMON History 활성화 하기

모든 설정이 끝난 RMON History를 활성화하려면 반드시 다음 명령어를 사용하여 활성화 설정을 해 주어야 합니다. History를 활성화 시키려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
active	RMON	History를 활성화 시킵니다.

다음은 RMON History를 활성화시키고, 위에서 설정한 내용들을 확인한 경우의 예입니다.

```
SWITCH(config-rmonhistory[1])# active  
SWITCH(config-rmonhistory[1])# show running-config  
Building configuration...  
(중략)  
rmon-history 5  
owner dasan  
data-source ifindex.hdlcl  
interval 60  
requested-buckets 25  
active  
(중략)  
SWITCH(config-rmonhistory[1])#
```



참 고

RMON History를 활성화 시키기 전에 설정 내용을 확인하고 해당 내용이 맞는지 반드시 확인하십시오. RMON History가 활성화 된 후에도 특정 항목의 내용을 바꾸고, 그 내용은 **active** 명령어를 사용하여 적용할 수는 있습니다. 그러나 보다 관리자의 실수에 대비하고 보다 확실한 적용을 위해서는 해당 RMON History를 삭제하고 처음부터 다시 설정하는 방법을 권장합니다.

(6) RMON History 삭제 및 설정 변경

RMON History와 관련하여 설정 내용을 변경하려면, 해당 번호의 RMON History를 삭제한 후 모든 내용을 다시 변경해야 합니다. RMON History를 삭제하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no rmon-history number	Global	해당 번호의 RMON History를 삭제합니다.

다음은 5번 RMON History를 삭제하는 경우의 예입니다.

```
SWITCH(config)# no rmon-history 1
SWITCH(config)#
```

7.4.2. RMON Alarm 설정

RMON Alarm은 사용자가 설정한 주기에 따라 표본을 조사하고, 사용자가 설정한 임계 값에서 벗어났을 때 전달됩니다. 이 때 임계 값과 비교하는 방법에는 절대 비교와 델타 비교의 두 가지가 있습니다.

- **절대 비교** : 주기적으로 표본 조사한 데이터 값과 임계 값을 비교했을 때, 데이터 값이 임계 값의 이상이거나 이하이면 Alarm을 발생시킵니다.
- **델타 비교** : 현재 조사된 데이터 값과 바로 이전에 조사된 데이터 값의 편차를 임계 값과 비교해서 편차가 임계 값 이상이거나 이하가 되면 Alarm을 발생시킵니다.

RMON Alarm을 설정하기 위해서는 일단 RMON Alarm 설정 모드로 들어가야 합니다. RMON Alarm 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
rmon-alarm <1-65534>	Global	RMON Alarm 설정 모드로 들어갑니다.

RMON Alarm 설정 모드로 들어가면, 시스템 프롬프트가 SWITCH(config)#에서 SWITCH(config-rmonalarm[n])#으로 바뀝니다. 이 때 변수 “n”은 서로 다른 RMON Alarm을 구별하기 위한 번호입니다.

다음은 1번 RMON Alarm 설정을 위한 Alarm 설정 모드로 들어가는 경우의 예입니다.

```
SWITCH(config)# rmon-alarm 1
SWITCH(config-rmonalarm[1])#
```

Alarm 설정 모드에서 RMON Alarm과 관련, 설정할 수 있는 명령어를 알아보려면 Alarm 설정 모드의 시스템 프롬프트에서 물음표를 입력하십시오. 다음은 Alarm 설정 모드에서 사용할 수 있는 명령어를 출력한 것입니다.

```
SWITCH(config-rmonalarm[1])# ?
active          Activate the event
exit            Exit current mode and down to previous mode
falling-event   Associate the falling threshold with an existing RMON event
falling-threshold Define the falling threshold
list            Print command list
owner           Assign the owner who define and is using the history resources
rising-event    Associate the rising threshold with an existing RMON event
rising-threshold Define the rising threshold
sample-interval Specify the sampling interval for RMON alarm
sample-type     Define the sampling type
sample-variable Define the MIB Object for sample variable
show            Show running system information
startup-type   Define startup alarm type
SWITCH(config-rmonalarm[1])#
```



주의

실제로 물음표는 출력되지 않고, 물음표를 입력하면 곧장 명령어가 출력됩니다.

한편, Alarm 설정 모드에서 빠져나와 Global 설정 모드로 돌아가거나 Privilege Exec Enable 설정 모드로 곧장 돌아가려면 다음의 명령어를 사용하십시오.

명령어	모 드	기 능
exit	RMON	Global 설정 모드로 돌아갑니다.

다음은 각각 Alarm 설정 모드에서 Global 설정 모드로 돌아가는 경우의 예입니다.

```
SWITCH(config-rmonalarm[1])# exit
SWITCH(config)#
```

(1) RMON Alarm 사용 주체 명시

사용자는 RMON Alarm을 설정하고 Alarm이 제공하는 여러 가지 정보를 이용하는 주체를 명시해야 합니다. Alarm 이용 주체를 명시하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
owner name	RMON	Alarm을 설정하고 관련 정보를 이용하는 주체를 명시합니다.

다음은 Alarm 주체를 dasan으로 설정한 경우입니다.

```
SWITCH(config-rmonalarm[1])# owner dasan
SWITCH(config-rmonalarm[1])#
```



Alarm을 설정하고 관련 정보를 이용하는 주체를 입력할 때에는 최대 32자까지 입력 가능합니다. 32자를 넘는 이름이 입력될 경우 "%Too long owner name" 이라는 에러 메시지를 보여줍니다.

(2) 표본 조사에 사용될 object 설정

사용자는 RMON Alarm을 제공하기 위해 표본 조사에 사용되는 object의 변수값이 필요합니다. 표본으로 사용될 object에 대한 규정은 다음과 같은 것들이 있습니다.

- svcExt.mib은 표본으로 사용되는 object를 규정하고 있습니다.
- CntExt.mib은 object 값을 표기하는 방식을 규정하고 있습니다.

표본 조사에 사용 할 object를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
sample-variable <i>mib-object</i>	RMON	표본 조사에 사용될 MIB object를 지정합니다.

다음은 MIB object apSvcConnections 값을 표본 조사에 사용할 수 있도록 설정한 경우입니다.

```
SWITCH(config-rmonalarm[1])# sample-variable apSvcConnections
SWITCH(config-rmonalarm[1])#
```

(3) 절대 비교 및 델타 비교 설정

사용자는 RMON Alarm을 설정할 때 표본 조사에 사용될 MIB object 값을 비교하는 방법을 설정할 수 있습니다. 절대 비교는 표본으로 선택한 object 변수값과 임계값을 직접 비교합니다. 예를 들어 표본 조사가 30,000 번에 이르는 시점을 알고 싶을 때 apSvcConnections의 값을 30,000번으로 설정하면 이는 절대 비교를 위한 것 입니다.

표본으로 선택한 object 값을 임계 값과 절대 비교하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
sample-type absolute	RMON	변수값을 임계값과 절대 비교로 비교합니다.

델타 비교는 현재 표본 조사하는 object 값과 바로 이전에 조사한 object 값의 편차를 임계 값과 비교합니다. 예를 들어 변수 표기 방식 규정이 이전에 지정한 규정 보다 100,000개 더 많은 시점을 알려면, apCntHits 변수를 델타 비교로 설정합니다.

델타 비교를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
sample-type delta	RMON	변수값의 편차를 임계값과 비교합니다.

(4) 상한 임계 값 설정

표본 조사에 사용한 object 값이 상한 임계 값 이상일 때 알람을 발생시키도록 하려면, 먼저 상한 임계 값을 설정해야 합니다. 상한 임계 값을 정할 때에는 다음 명령어를 사용하십시오.

명령어	모 드	기 능
rising-threshold number	RMON	상한 임계값을 설정합니다.

다음은 상한 임계값을 100으로 설정한 경우입니다.

```
SWITCH(config-rmonalarm[1])# rising-threshold 100
SWITCH(config-rmonalarm[1])#
```



상한 임계값은 2,147,483,647까지 입력 가능하며 “0”을 입력하면 Alarm은 발생하지 않습니다.

상한 임계값을 정한 후에는 다음 명령어를 사용하여 조사된 object 값이 설정한 상한 임계값 이상일 때 RMON Event를 발생시키도록 설정하십시오.

명령어	모 드	기 능
rising-event <1-65535>	RMON	상한 임계값 이상일 때 RMON Event가 발생하도록 합니다.

다음은 상한 임계값 이상일 때 RMON 이벤트 1이 발생하도록 설정한 경우입니다.

```
SWITCH(config-rmonalarm[1])# rising-event 1
SWITCH(config-rmonalarm[1])#
```

(5) 하한 임계 값 설정

표본 조사에 사용한 object 값이 하한 임계 값 이하일 때 알람을 발생시키려면, 먼저 하한 임계 값을 설정해야 합니다. 하한 임계 값을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
falling-threshold number	RMON	하한 임계값을 설정합니다.

다음은 하한 임계값을 90으로 설정한 경우입니다.

```
SWTICH(config-rmonalarm[1]))# falling-threshold 90
SWTICH(config-rmonalarm[1]))#
```



참 고

하한 임계값은 2,147,483,647까지 입력 가능하며 “0”을 입력하면 Alarm은 발생하지 않습니다.

하한 임계 값을 설정한 후에는 다음 명령어를 사용하여 조사된 object 값이 하한 임계 값 이하일 때 RMON Event가 발생하도록 설정하십시오.

명령어	모 드	기 능
falling-event <1-65535>	RMON	하한 임계값 이하가 될때 RMON 알람 이벤트를 발생시킵니다.

(6) 최초 Alarm 기준 설정

사용자는 최초로 Alarm이 발생하는 기준을 설정할 수 있습니다. 표본으로 선택한 object 값이 처음으로 상한 임계 값 이상이 될 때로 정할 수도 있고, 하한 임계 값 이하가 될 때로 정할 수도 있으며 상한 임계 값 이상이 되거나 하한 임계 값 이상이 됐을 때로 정할 수 도 있습니다.

다음은 하한 임계 값 이하일 때 최초로 RMON Alarm을 발생시키도록 하는 명령어입니다.

명령어	모 드	기 능
startup-type falling	RMON	처음으로 하한 임계값 이하가 됐을 때 최초로 Alarm이 발생하도록 설정합니다.

표본으로 선택한 object 값이 처음으로 상한 임계값 이상이 될 때 첫 RMON Alarm을 발생시키려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
startup-type rising	RMON	처음으로 상한 임계값 이상이 됐을 때 최초로 Alarm이 발생하도록 설정합니다.

한편, 표본으로 선택한 object 값이 처음으로 상한 임계값 이상이 되거나 하한 임계값 이하가 될 때 Alarm을 발생시키려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
startup-type rising-and-falling	RMON	처음으로 상한 임계값 이상이 되거나 하한 임계값 이하가 될 때 첫 Alarm이 발생하도록 설정합니다.

(7) 표본 조사 간격 설정

표본 조사 간격은 표본을 추출해서 상한 임계값이나 하한 임계값과 비교하는데 초 단위의 시간 간격을 말합니다.

RMON Alarm을 발생시키기 위해 표본 조사 간격을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
sample-interval <0-65535>	RMON	표본 조사 간격을 설정합니다.

다음은 표본 조사를 60초 마다 한번씩 수행하도록 설정한 경우입니다.

```
SWITCH(config-rmonalarm[1])# sample-interval 60
SWITCH(config-rmonalarm[1])#
```

(8) RMON Alarm 활성화 하기

모든 설정이 끝난 RMON Alarm을 활성화하려면 반드시 다음 명령어를 사용하여 활성화 설정을 해주어야 합니다. Alarm을 활성화 시키려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
active	RMON	Alarm을 활성화 시킵니다.

다음은 RMON Alarm을 활성화시키고, 위에서 설정한 내용들을 확인한 경우의 예입니다.

```
SWITCH(config-rmonalarm[1])# active
SWITCH(config-rmonalarm[1])# show running-config
Building configuration...
(중략)
rmon-alarm 1
  owner dasan
  sample-variable apSvcConnections
  sample-type absolute
  startup-type rising
  rising-threshold 100
  falling-threshold 90
  rising-event 1
  falling-event 2
  sample-interval 60
  active
(중략)
SWITCH(config-rmonalarm[1])#
```



참 고

RMON Alarm을 활성화 시키기 전에 설정 내용을 확인하고 해당 내용이 맞는지 반드시 확인하십시오. RMON Alarm이 활성화 된 후에도 특정 항목의 내용을 바꾸고, 그 내용은 **active** 명령어를 사용하여 적용할 수는 있습니다. 그러나 보다 관리자의 실수에 대비하고 보다 확실한 적용을 위해서는 해당 RMON Alarm을 삭제하고 처음부터 다시 설정하는 방법을 권장합니다.

(9) RMON Alarm 삭제 및 설정 변경

RMON Alarm과 관련하여 설정 내용을 변경하려면, 해당 번호의 RMON Alarm을 삭제한 후 모든 내용을 다시 변경해야 합니다. RMON Alarm을 삭제하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no rmon-alarm number	Global	해당 번호의 RMON Alarm을 삭제합니다.

다음은 1번 RMON Alarm을 삭제하는 경우의 예입니다.

```
SWITCH(config)# no rmon-alarm 1
SWITCH(config)#
```

7.4.3. RMON Event 설정

RMON Event는 RMON Alarm을 비롯하여 장비에서 발생하는 모든 동작을 나타냅니다. 사용자는 RMON이 Alarm을 보낼 때 SNMP 관리 서버로 Event 메시지나 Trap 메시지를 전송하도록 설정할 수 있습니다. RMON Event를 설정하려면 우선 Event 설정 모드로 들어가야 합니다.

RMON Event 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
rmon-event <1~65534>	Global	RMON Event 설정 모드로 들어갑니다.

RMON Event 설정 모드로 들어가면, 시스템 프롬프트가 SWITCH(config)#에서 SWITCH(config-rmonevent[n])#로 변경됩니다. 변수 “n”은 서로 다른 Event를 구별하기 위한 번호입니다.

다음은 1번 RMON Event를 설정하기 위한 Event 설정 모드로 들어가는 경우의 예입니다.

```
SWITCH(config)# rmon-event 1
SWITCH(config-rmonevent[1])#
```

Event 설정 모드에서 RMON Event와 관련, 설정할 수 있는 명령어를 알아보려면 Event 설정 모드의 시스템 프롬프트에서 물음표를 입력하십시오. 다음은 Event 설정 모드에서 사용할 수 있는 명령어를 출력한 것입니다.

```
SWITCH(config-rmonevent[1])# ?
active      Activate the event
community   Define a community to an unactivated event
description Define description of RMON event
exit        Exit current mode and down to previous mode
list         Print command list
owner       Assign the owner who define and is using the history resources
show        Show running system information
type        Define the event type determines where send the event notification
SWITCH(config-rmonevent[1])#
```



주의

실제로 물음표는 출력되지 않고, 물음표를 입력하면 곧장 명령어가 출력됩니다.

한편, Event 설정 모드에서 빠져나와 Global 설정 모드로 돌아가거나 Privilege Exec Enable 설정 모드로 곧장 돌아가려면 다음의 명령어를 사용하십시오.

명령어	모 드	기 능
exit	RMON	Global 설정 모드로 돌아갑니다.

(1) Event Community 설정

RMON Event가 발생했을 때 호스트로 SNMP 트랩(trap) 메시지를 전송하려면 **community**를 입력해야 합니다. **community**란 메시지 전송 권한을 부여하는 패스워드를 의미합니다. 트랩 메시지 전송에 필요한 **community**를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
community password	RMON	해당 이벤트 전송 권한을 부여하는 패스워드를 설정합니다.

다음은 RMON 이벤트 전송 권한을 부여하는 **community**를 “password”으로 설정하는 경우입니다.

```
SWITCH(config-rmonevent[1])# community password  
SWITCH(config-rmonevent[1])#
```

(2) Event 설명

V5812G는 Event가 발생했을 때, Event에 대해 간략하게 설명할 수 있습니다. 그러나, Event에 대한 설명이 자동으로 생성되는 것이 아니므로 관리자는 직접 해당 내용을 기술해야 합니다. Event에 대한 설명을 기술하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
description description	RMON	Event에 대해 설명합니다.

다음은 이벤트에 대해 설명하는 방법입니다.

```
SWITCH(config-rmonevent[1])# description This event ..  
SWITCH(config-rmonevent[1])#
```



참 고

Event에 대한 설명은 최대 126자까지 입력 가능합니다.

(3) Event 사용 주체 명시

사용자는 Event를 설정하고 Event가 제공하는 여러 가지 정보를 이용하는 주체를 명시해야 합니다.

다음은 Event 이용 주체를 명시할 때 사용하는 명령어입니다.

명령어	모 드	기 능
owner name	RMON	이벤트를 이용하는 주체를 명시합니다. 최대 126자까지 쓸 수 있으며 이벤트 주체는 반드시 알람 주체와 일치해야 합니다.

다음은 Event 이용 주체를 dasan으로 명시한 경우의 예입니다.

```
SWITCH(config-rmonevent[1])# owner dasan
SWITCH(config-rmonevent[1])#
```



참 고

Event 사용 주체를 설명할 때에는 최대 32자까지 입력 가능합니다. 32자를 넘는 이름이 입력될 경우 "%Too long owner name"이라는 에러 메시지를 보여줍니다.

(4) Event 공지 형태 설정

RMON Event가 발생했을 경우, Event의 형태를 지정함으로써 Event가 어디로 전송될지 결정됩니다. Event 타입을 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
type log		Event 공지 형태를 로그 타입으로 설정합니다. 로그 타입 Event는 로그 파일이 생성된 지점에 공지됩니다.
type trap	RMON	Event 공지 형태를 트랩 타입의 Event를 지정합니다. 트랩 타입의 Event는 SNMP 관리자 PC로 전달됩니다.
type log-and-trap		로그와 트랩 타입의 Event 둘 다 지정합니다.
type none		Event 공지 형태를 지정하지 않습니다.



참 고

Event 공지 형태는 기본적으로 **none**으로 설정되어 있습니다.

(5) Evnet 활성화 하기

모든 설정이 끝난 RMON Event를 활성화하려면 반드시 다음 명령어를 사용하여 활성화 설정을 해주어야 합니다. Event를 활성화 시키려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
active	RMON	Event를 활성화 시킵니다.

다음은 RMON Event를 활성화시키고, 위에서 설정한 내용들을 확인한 경우의 예입니다.

```
SWITCH(config-rmonevent[1])# active
SWITCH(config-rmonevent[1])# show running-config
Building configuration...
(중략)
!
rmon-event 1
  owner dasan
  community password
  description This event ...
  type log-and-trap
  active
(중략)
SWITCH(config-rmonevent[1])#
```



참 고

RMON Event를 활성화 시키기 전에 설정 내용을 확인하고 해당 내용이 맞는지 반드시 확인하십시오. RMON Event가 활성화 된 후에도 특정 항목의 내용을 바꾸고, 그 내용은 '**active**' 명령을 사용하여 적용할 수는 있습니다. 그러나 보다 관리자의 실수에 대비하고 보다 확실한 적용을 위해서는 해당 RMON Event를 삭제하고 처음부터 다시 설정하는 방법을 권장합니다.

(6) RMON Event 삭제 및 설정 변경

RMON Event와 관련하여 설정 내용을 변경하려면, 해당 번호의 RMON Event을 삭제한 후 모든 내용을 다시 변경해야 합니다. RMON Event를 삭제하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no rmon-event number	Global	해당 번호의 RMON Event를 삭제합니다.

다음은 5번 RMON Event를 삭제하는 경우의 예입니다.

```
SWITCH(config)# no rmon-event 1
SWITCH(config)#
```

7.5 Syslog

Syslog는 사용자의 장비에서 발생하는 오류 등의 정보를 관리자에게 메시지를 통해 알려주는 역할을 합니다. V5812G에는 기본적으로 System logger(syslog) 기능이 설정되어 있습니다. 따라서 이 기능을 해제한다고 해도 장비를 다시 부팅하면 다시 설정된 상태로 되돌아가게 됩니다.



참 고

V5812G는 기본적으로 syslog 기능이 설정되어 있습니다.

Syslog와 관련하여 다음과 같은 내용을 설명합니다.

- Syslog 메시지 Level 설정
- System Facility 설정
- Syslog Message Priority 설정
- Syslog 해제
- Syslog 설정 확인
- Syslog 메시지 IP 주소 설정
- 원격에서 Debug 메시지 확인하기

7.5.1. Syslog 메시지 Level 설정

V5812G의 Syslog 메시지는 Level과 Priority가 표시되어 전송됩니다. Priority는 상관없이 전송되는 모든 Syslog 메시지에 Level을 표시하려면, 다음 명령어를 사용하십시오. 이 때, 관리자가 Syslog 메시지를 전송하려는 장소도 함께 설정할 수 있습니다.

Syslog 메시지의 종류와 메시지 전송 장소를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>syslog output {emerg alert crit err warning notice info} console</code>	Global	사용자가 설정한 level의 syslog 메시지를 콘솔로 전송합니다.
<code>syslog output {emerg alert crit err warning notice info} local {volatile non-volatile}</code>	Global	사용자가 설정한 level의 syslog 메시지를 system 내부로 전송합니다.
<code>syslog output {emerg alert crit err warning notice info} remote ip-address</code>	Global	사용자가 설정한 level의 syslog 메시지를 내부 호스트로 전송합니다.

syslog 메시지는 중요도 우선 순위에 따라 emergency | alert | critical | error | warning | notice | info의 7단계 level로 나눌 수 있습니다. emergency가 중요도에서 가장 상위에 속하며 info가 중요도에서 가장 하위에 속하게 됩니다.

사용자는 syslog 메시지의 level을 설정할 수 있는데, 선택한 level을 기준으로 하위 level의 syslog 메시지는 받을 수 없습니다. 즉, info level을 선택해야 모든 level의 syslog 메시지를 얻을 수 있고, error level을 선택하면 error level과 error보다 상위 level의 syslog 메시지를 얻을 수 있습니다.

한편, 사용자는 syslog 메시지를 받는 위치도 설정할 수 있습니다. 사용자의 PC에 있는 콘솔을 통해 syslog 메시지를 받으려면 console, system 내부로 받으려면 local, 내부 호스트에서 받으려면 remote를 입력하십시오.

Syslog 메시지의 종류와 메시지 전송 장소를 설정한 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no syslog output {emerg alert crit err warning notice info} console	Global	Syslog 메시지의 종류와 메시지 전송 장소를 설정한 것을 해제합니다.
no syslog output {emerg alert crit err warning notice info} local {volatile non-volatile}		
no syslog output {emerg alert crit err warning notice info} remote ip-address		

7.5.2. System Facility 설정

다음 명령어로 V5812G Syslog 메시지의 Facility에 Local-code를 부여하십시오. 사용자가 설정한 Facility Local-code에 따라 각 시스템 또는, 시스템 그룹별 Syslog 메시지 관리가 가능합니다.

명령어	모 드	기 능
syslog local-code <0 – 7>	Global	System Facility를 설정합니다.
no syslog local-code		System Facility를 해제합니다.
show syslog		System Facility를 확인합니다.

다음은 System Facility를 3으로 설정하고 그 내용을 확인하는 예입니다.

```
SWITCH(config)# syslog local-code 3
SWITCH(config)# show syslog
System logger on running!
info          local volatile
info          local non-volatile
local_code    3
SWITCH(config)#

```

7.5.3. Syslog Message Priority 설정

V5812G는 Syslog Message의 Priority를 선택할 수 있습니다. 다음 명령어를 사용하면, 사용자가 선택한 Priority에 해당하는 Syslog 메시지만 전송할 수 있습니다. 이 때, Level과 전송 장소는 동시에 설정합니다.

명령어	모 드	기 능
<code>syslog output priority {auth authpriv cron deamon kern lpr mail news syslog user uucp} {emerg alert crit err warning notice info debug} console</code>		사용자가 선택한 Priority에 해당하는 Syslog 메시지만 콘솔로 전송합니다.
<code>syslog output priority {auth authpriv cron deamon kern lpr mail news syslog user uucp} {emerg alert crit err warning notice info debug} local {volatile non-volatile}</code>	Global	사용자가 선택한 Priority에 해당하는 Syslog 메시지만 시스템 내부로 전송합니다.
<code>syslog output priority {auth authpriv cron deamon kern lpr mail news syslog user uucp} {emerg alert crit err warning notice info debug} } remote ip-address</code>		사용자가 선택한 Priority에 해당하는 Syslog 메시지만 원격으로 전송합니다.

V5812G에서 선택할 수 있는 priority는 **auth, authpriv, cron, deamon, kern, lpr, mail, news, syslog, user, uucp**가 있습니다.

한편, V5812G는 local0부터 local7까지 사용자가 정의할 수 있는 Priority가 있습니다. 이 Priority는 Syslog 서버에서 여러 장비로부터 Syslog 메시지를 받을 때, 각 장비로부터의 Syslog 메시지를 구분하거나 할 때 사용될 수 있습니다. 다음은 사용자 정의의 Priority를 설정하여 Syslog 메시지를 전송하도록 할 때 사용하는 명령어입니다.

명령어	모 드	기 능
<code>syslog output priority {local0 local1 local2 local3 local4 local5 local6 local7} {emerg alert crit err warning notice info debug} console</code>		
<code>syslog output priority {local0 local1 local2 local3 local4 local5 local6 local7} {emerg alert crit err warning notice info debug} local {volatile non-volatile}</code>	Global	사용자 정의의 Priority를 설정하여 Syslog 메시지를 전송하도록 합니다.
<code>syslog output priority {local0 local1 local2 local3 local4 local5 local6 local7} {emerg alert crit err warning notice info debug} } remote ip-address</code>		

한편 사용자가 선택한 Syslog 메시지가 전송되도록 설정한 것을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>no syslog output priority {auth authpriv cron deamon kern lpr mail news syslog user uucp} {emerg alert crit err warning notice info debug} console</code>		
<code>no syslog output priority {auth authpriv cron deamon kern lpr mail news syslog user uucp} {emerg alert crit err warning notice info debug} local {volatile non-volatile}</code>	Global	사용자가 선택한 Syslog 메시지를 전송하도록 설정한 것을 해제합니다.
<code>no syslog output priority {auth authpriv cron deamon kern lpr mail news syslog user uucp} {emerg alert crit err warning notice info debug } remote ip-address</code>		

[설정 예제 1]

다음은 local1.info라는 Syslog 메시지를 console로 전달하도록 설정하는 경우입니다.

```
SWITCH(config)# syslog output notice remote 10.1.1.1
SWITCH(config)# syslog output priority local1 info console
SWITCH(config)# show syslog
System logger on running!

info          local volatile
info          local non-volatile
notice        remote 10.1.1.1
local1.info    console
SWITCH(config)#

```

7.5.4. Syslog 해제

Syslog를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	Function
no syslog	Global	Syslog를 해제합니다.

다음은 “**no syslog**”로 syslog를 해제한 이후, 다시 이를 복귀할 때 사용하는 명령어입니다.

System logger의 기능은 장비를 부팅하면 기본적으로 활성화 상태이기 때문에 이 명령어는 syslog를 해제하지 않은 상태에서는 의미가 없습니다.

명령어	모 드	기 능
syslog start	Global	해제했던 system logger를 다시 시작합니다.

7.5.5. Syslog 설정 확인

syslog와 관련된 설정된 내용을 확인하거나 syslog 메시지를 확인하고 싶을 때는 다음 명령어를 사용합니다.

명령어	모 드	기 능
show syslog		현재의 syslog 설정을 보여줍니다.
show syslog local {volatile non-volatile}		syslog 메시지를 보여줍니다.
show syslog local {volatile non-volatile} number	Enable /Global	사용자가 입력한 <i>number</i> 에 해당하는 수만큼의 최신 메시지를 보여줍니다. 예를 들어 “2”를 입력하면 최신 메시지를 2줄 보여줍니다.
show syslog {volatile non-volatile} information		Syslog 상태를 보여줍니다.



주의

syslog 설정 내용은 “**show running-config**” 명령어로 확인할 수 없습니다.

다음은 info level 이상은 volatile 파일에 저장하고, emergency level 이상은 콘솔에 저장하도록 설정된 상태입니다.

```
SWITCH(config)# show syslog
System logger on running!

info          local volatile
emerg         console
SWITCH(config)#

```

syslog 파일에 저장된 log 메시지를 삭제하려면 다음의 명령어를 사용하십시오.

명령어	모 드	기 능
clear syslog local {volatile non-volatile}	Global	Syslog 파일에 저장된 로그 메시지를 삭제합니다.

7.5.6. Syslog 메시지 IP 주소 지정

V5812G는 원격으로 전송되는 Syslog 메시지의 IP 주소를 지정할 수 있습니다. Syslog 메시지에 IP 주소를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
syslog bind-address ip-address		원격으로 내보내는 Syslog 메시지에 IP 주소를 지정합니다.
no syslog bind-address	Global	원격으로 내보내는 Syslog 메시지에 설정될 IP 주소를 해제합니다.
show syslog		Syslog 메시지에 할당된 IP 주소를 확인합니다.

다음은 Syslog 메시지에 IP 주소 192.168.253.0가 할당되도록 설정한 후, 그 내용을 확인하는 예입니다.

```
SWITCH(config)# syslog bind-address 192.168.253.0
SWITCH(config)# show syslog
System logger on running!
info          local volatile
info          local non-volatile
kern.=err      console
alert         console
=====
agent address 192.168.253.0
SWITCH(config)#

```

7.5.7. 원격에서 Debug 메시지 확인하기

원격에서 접속하는 사용자들은 원격에 있는 서버로 Syslog 메시지를 전송하면 서버를 통해 Syslog 메시지를 확인할 수 있습니다. 그러나 V5812G는 원격에서도 자신의 Console 창에서 Syslog 메시지 가운데 Debug 메시지를 확인할 수 있습니다.

원격 접속자가 자신의 Console 창에서 Debug 메시지를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	Function
terminal monitor	Enable	원격 접속자가 자신의 Console 창에서 Debug 메시지를 확인할 수 있도록 합니다.

다음은 원격 접속자가 자신의 Console 창에서 Debug 메시지를 확인하도록 설정하는 경우입니다.

```
SWITCH# terminal monitor
SWITCH# show syslog
System logger on running!

info          local volatile
info          local non-volatile
user.debug    /dev/ttyP1      Telnet으로 접속한
              사용자에 해당됨
SWITCH#
```

원격 접속자가 자신의 Console 창에서 Debug 메시지를 확인하는 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	Function
no terminal monitor	Enable	원격 접속자가 자신의 Console 창에서 Debug 메시지를 확인할 수 있도록 하는 것을 해제합니다.

7.6 QoS(Quality of Service)

일반적으로 네트워크에서 데이터를 처리할 때는 시간 순서대로 먼저 들어 온 데이터를 먼저 내보냅니다. 특정 데이터를 우선적으로 처리하지 않고 모든 데이터를 시간 순서대로 처리하는 이 방식은 패킷이 한꺼번에 몰렸을 때 데이터를 전부 잃어버리는 단점이 있습니다.

그러나, QoS를 사용하면 트래픽이 과부하 상태일 때 상대적인 중요도에 따라 각 패킷들의 우선 순위를 재조정, 처리 순서를 다르게 적용함으로써 사용자가 선택한 네트워크 트래픽에 대해 더욱 향상된 서비스를 제공할 수 있습니다.

◆ QoS의 장점

- 네트워크 자원 제어

대역폭, 장비, IP 주소 등 다양한 자원을 제어할 수 있습니다. 네트워크 관리자는 FTP 전송을 위한 대역폭을 제한하거나 중요 데이터를 우선적으로 처리할 수 있습니다.

- 효율적인 자원 사용

사용자의 네트워크가 어떤 데이터를 처리하는지 파악한 후 중요도가 가장 높은 데이터를 우선적으로 받아 볼 수 있습니다.

- 맞춤형 서비스

QoS 기능을 이용하여 망 사업 관리자는 사용자에게 차등화 된 서비스를 제공할 수 있습니다.

- 중요 데이터 우선 처리

다산이 제공하는 QoS는 중요도가 가장 높은 데이터나 음성 데이터가 우선 처리되도록 대역폭을 보장하고 지연 시간을 최소화 시킵니다. 나머지 일반 데이터는 우선 순위가 높은 데이터를 먼저 처리하고 난 후 시간 순서대로 차례로 처리합니다.

한편, QoS 설정에서 주의해야 할 것은 사용자가 설정한 우선 순위가 높은 패킷으로 인해 다른 패킷들의 전송이 실패하는 일이 없어야 한다는 점입니다.

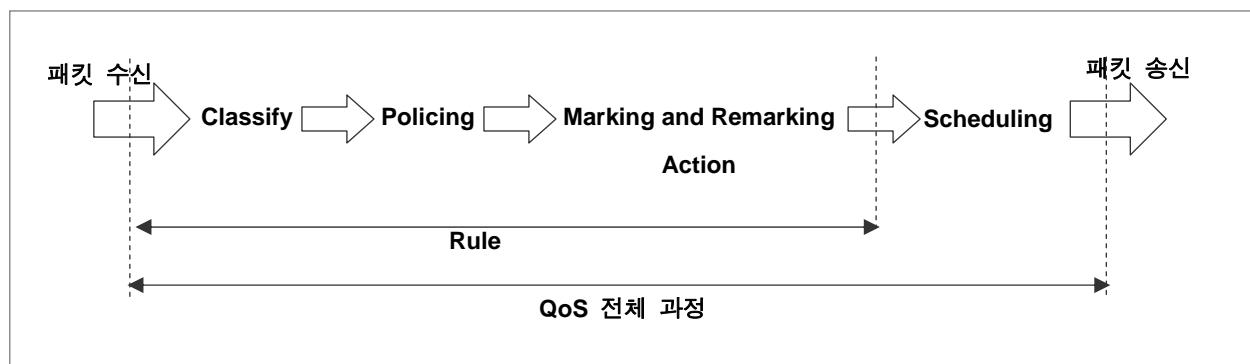
여기에서는 V5812G에서 제공하는 QoS 기능을 다음과 같이 설명합니다.

- QoS 동작 원리
- 패킷 분류(Classify) 설정
- 패킷 정책(Policing) 설정
- Rule 동작 설정
- Rule 설정 내용 확인
- 스케줄링(Scheduling) 설정
- Admin Rule 설정
- Admin Rule Classify 설정
- Admin Rule 동작 설정
- Admin Rule 설정 내용 확인

7.6.1. QoS 동작 원리

V5812G의 QoS가 이루어지는 과정을 간단히 설명하면, 일단, 전송된 패킷을 분류(Classify)할 수 있는 조건과 패킷에 대한 정책(Policing)을 설정한 후, 사용자가 필요로 하는 Classify와 Policing을 Policy에 포함시켜 해당 패킷에 대한 Rule을 실행합니다. Rule을 실행할 때에는 Classify와 Policing이 이루어진 패킷의 Action을 결정하는 것은 물론, CoS나 DSCP 등 패킷의 우선 순위를 결정하는 다양한 값을 설정 또는 재조정(Marking/Remarketing) 할 수 있습니다. 이와 같이 Rule에 따라 처리된 패킷은 사용자가 설정한 스케줄링(Scheduling) 방법에 따라 외부에 전송되게 되는 것입니다.

다음은 QoS 동작구조를 간단히 나타낸 그림입니다.



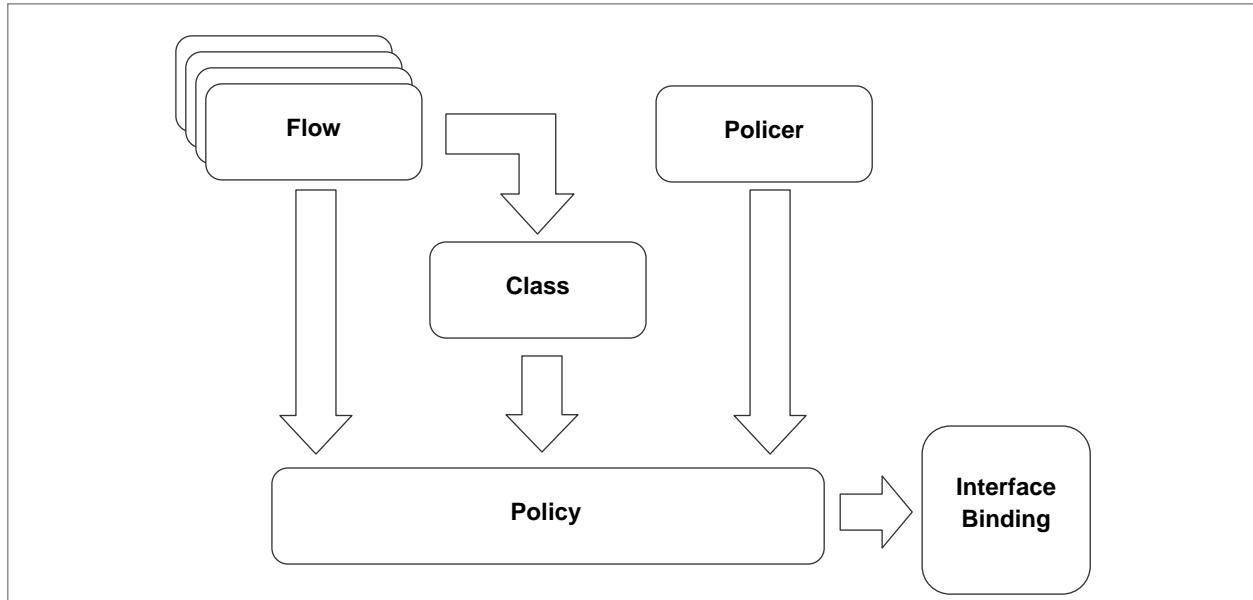
【 그림 7-3 】 QoS의 동작 구조

QoS 기능을 통해 외부로 전송할 패킷을 스케줄링 하기 전까지는 Rule을 이용하여 패킷을 처리하게 됩니다. V5812G Rule의 구조를 보다 세분화하여 패킷 분류 및 정책에 대한 설정을 다양하게 적용할 수 있도록 하였습니다.

기본적인 Rule의 구조는 Flow, Class, Policer, Policy의 4가지로 분류되고, 각각은 다음과 같은 역할을 합니다.

- **Flow** : 패킷을 분류(Classify)하기 위한 조건을 정의합니다. 분류 조건으로 지정되는 값들에는 MAC 주소, IP 주소, DSCP, Ether 타입 등이 있습니다.
- **Class** : 패킷 분류 조건이 되는 Flow에 정책을 적용하는데 있어서 보다 효율적인 관리를 위해 도입된 것으로 Flow의 집합체라고 할 수 있습니다.
- **Policer** : Flow 및 Class에 적용하게 될 정책(Policing)을 정의합니다. 해당 Flow 및 Class에 Metering이나 Counting 등을 설정하게 됩니다.
- **Policy** : 사용자가 설정한 Flow 또는 Class, 그리고 Policer를 필요에 따라 선택하여 하나의 Rule으로 동작하도록 실행합니다.

Rule의 기본 구조를 이루는 Flow, Class, Policer, Policy의 관계는 아래 그림과 같습니다.



【 그림 7-4 】 Rule의 구조

2개 이상의 Flow는 하나의 Class로 관리할 수 있습니다. Flow나 Class, Policer는 하나의 Policy로 구성됨으로써 실행을 하게 됩니다. Policy에 포함되지 않은 Flow, Class, Policer는 아무런 동작이 이루어지지 않으며 단순히 Rule을 실행하기 위해 장비가 가지고 있는 데이터 정도에 불과합니다.

하나의 Policy에 Flow와 Class는 동시에 속할 수 없으므로 Flow를 포함한 Policy에는 Class를 포함시킬 수 없고, Class를 포함한 Policy에는 Flow를 포함시킬 수 없습니다. 그리고, 동일한 Flow나 Class는 복수의 Policy에 중복 포함될 수 있으나, 하나의 Policier는 하나의 Policy에만 포함이 가능합니다. V5812G에서 Policy를 설정하여 실제로 동작하게 되는 Rule은 약 1천 개 정도가 지원됩니다.

7.6.2. 패킷 분류(Classify) 설정

V5812G은 Rule을 적용할 패킷을 분류하는 조건을 Flow로 만들어 설정하고, 복수의 Flow를 관리할 때에는 Class를 활용하도록 되어 있습니다.

(1) 모드 설정

V5812G의 Flow는 default와 extension의 2가지 모드를 지원합니다. 각 모드는 다음과 같은 특성을 가지고 있으니, 사용자는 알맞게 설정하시기 바랍니다.

- 1) Default 모드는 Admin-access-flow를 포함하여 최대 1024개의 Flow를 만들 수 있습니다.
- 2) Default 모드에서는 NetBIOS 필터링을 설정할 수 없습니다.
- 3) Default 모드에서는 ICMP나 패킷 길이로 패킷을 분류할 수 없습니다.
- 4) Extension 모드는 Admin-access-flow를 포함하여 최대 512개의 Flow를 만들 수 있습니다.

사용자 장비에서 사용할 Flow 모드를 설정하려면, Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
flow default	Global	Flow를 Default 모드로 설정합니다.
flow extension		Flow를 Extension 모드로 설정합니다.



Default 모드에서 Extension 모드로 변경할 때, 생성된 Flow 개수가 Extension 모드에서 제한된 개수를 초과하고 있을 경우에는 변경이 불가능합니다. 또한 ICMP나 패킷 길이를 사용하여 패킷을 구분한 Flow가 존재하거나, NetBIOS 필터링이 활성화되어 있을 경우에는 Default 모드로 변경이 불가능합니다.

(2) Flow 설정

Flow를 설정하려면, 가장 먼저 Flow를 생성해야 하고, Flow를 생성하면 Flow 설정 모드로 들어가면서 세부적인 패킷 분류 조건을 설정할 수 있게 됩니다.

패킷 분류 조건을 설정하기 위해 Flow를 생성하고 Flow 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
flow flow-name create	Global	Flow를 생성하고 Flow 설정 모드로 들어갑니다.

한편, 설정했던 Flow를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no flow flow-name	Global	생성했던 해당 Flow를 삭제합니다.
no flow all		모든 Flow를 삭제합니다.

Flow에는 패킷을 분류하는 조건이 지정되며, 패킷 분류 조건의 기준으로는 MAC 주소, IP 주소, Ethtype, CoS, DSCP 등이 있습니다.

MAC 주소를 기준으로 패킷을 분류하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
mac {src-mac-address any} {dst-mac-address any}	Flow	Source MAC 주소와 Destination MAC 주소를 패킷 분류 조건으로 설정합니다.

IP 주소 및 프로토콜을 기준으로 패킷을 분류하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any}		설정한 Source IP 주소와 Destination IP 주소 기준으로 패킷을 분류합니다.
ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} <0-255>		
ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} {icmp tcp udp}	Flow	설정한 IP 주소와 해당 프로토콜을 기준으로 패킷을 분류합니다.
ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} icmp <0-255> any} <0-255> any}		설정한 IP 주소와 ICMP의 Message type, Code 값을 기준으로 패킷을 분류합니다.
ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} tcp <1-65535> any} <1-65535> any} [tcp-flag any]		설정한 IP 주소와 TCP 포트를 기준으로 패킷을 분류합니다.
ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} udp <1-65535> any} <1-65535> any}		설정한 IP 주소와 UDP 포트를 기준으로 패킷을 분류합니다.

IP ToS precedence, CoS, ToS, DSCP, Ethtype, 패킷 길이, IP-Header 등을 기준으로 패킷을 분류하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip-precedence {<0-7> any}		설정한 IP TOS precedence에 해당하는 패킷을 분류합니다.
cos {<0-7> any}		설정한 CoS 값에 해당하는 패킷을 분류합니다.
tos {<0-255> any}	Flow	설정한 ToS 값에 해당하는 패킷을 분류합니다.
dscp {<0-63> any}		설정한 DSCP 값에 해당하는 패킷을 분류합니다.
ethertype {ether-type arp any}		설정한 Ethtype에 해당하는 패킷을 분류합니다.
length {<21-65535> any}		설정한 패킷 길이에 해당하는 패킷을 분류합니다.



참 고

하나의 Flow에 여러 개의 패킷 분류 조건을 설정할 수 있습니다.

한편, Flow에 설정한 패킷 분류 조건을 삭제하려면, Flow 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no cos		
no dscp		
no ethtype		
no ip	Flow	Flow에 설정한 패킷 분류 조건을 삭제합니다.
no ip-precedence		
no length		
no mac		
no tos		

(3) Flow 내용 저장 및 수정

패킷 분류 조건에 대한 설정이 끝난 Flow는 반드시 장비에 저장해야 합니다. 설정이 끝난 Flow를 장비에 저장하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
apply	Flow	Flow의 설정을 장비에 저장합니다.



참 고

Flow 설정을 저장하지 않고 Flow 설정 모드에서 Global 모드로 돌아가면, 설정한 내용은 모두 사라지게 됩니다.

한편, 기존의 Flow의 내용을 수정하려면, 일단 수정하려는 특정 Flow의 설정 모드로 들어가야 합니다.

Flow의 내용 수정을 위해 Flow 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
flow flow-name modify	Global	내용을 수정하려는 특정 Flow의 설정 모드로 들어갑니다.



Flow의 내용을 수정한 후에도 반드시 **apply** 명령어를 사용하여 내용을 저장해야 합니다.

(4) Class 설정

여러 가지 조건을 가지고 패킷을 분류하게 될 경우, 2개 이상의 Flow가 필요로 할 경우가 있습니다. 이러한 경우 여러 개의 Flow를 Class로 묶어서 사용하면 관리하기도 쉽고, 설정도 간편해집니다. 2 개 이상의 Flow를 하나의 Class로 묶어서 사용하려면, 다음 명령어를 사용하여 Class를 설정하십시오.

명령어	모 드	기 능
class class-name flow flow-name [flow-name] [flow-name] ...	Global	Flow를 모아 Class를 설정합니다.

한편, Class 설정을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no class all	Global	설정되어 있는 모든 Class를 삭제합니다.
no class name		해당 Class를 삭제합니다.
no class name flow flow-name [flow-name] [flow-name] ...		해당 Class에서 특정 Flow를 삭제합니다.

7.6.3. 패킷 정책(Policing) 설정

Classify로 분류된 패킷에 여러 가지 정책(Policing)을 설정하는 것은 Policer에서 행해집니다. Policer에서 적용할 수 있는 패킷 정책에는 Metering과 Rate-limit 등이 있습니다. 또한, 사용자가 설정한 Rule에 따라 처리된 패킷의 수를 파악할 수 있도록 해주는 Counter도 설정할 수 있습니다.

(1) Policer 생성

분류된 패킷의 정책을 설정하려면, 일단 Policer를 생성하여 Policer 설정 모드로 들어가야 합니다. 패킷 정책을 설정하기 위해 Policer를 생성하고, Policer 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
policer policer-name create	Global	Flow를 생성하고 Flow 설정 모드로 들어갑니다.



Policer에 설정하는 패킷 정책들의 내용은 **Metering**과 **Rate-limit, Counter** 등이 있습니다.

한편, 설정했던 Policer를 삭제하려면, 다음 명령어를 사용하십시오.

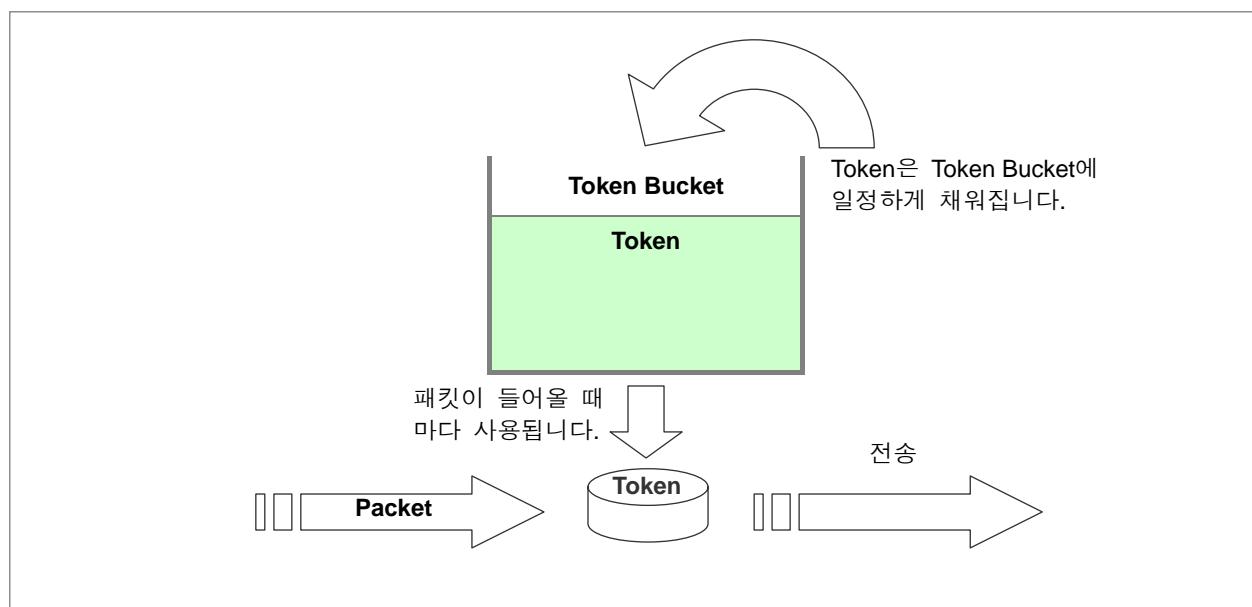
명령어	모 드	기 능
no policer policer-name	Global	생성했던 해당 Policer를 삭제합니다.
no policer all		모든 Policer를 삭제합니다.

(2) Metering

V5812G 스위치가 지원하는 Metering의 방법에는 SRTCM(Single Rate Three Color Marker)과 TRTCM(Two Rate Three Color Marker)의 2가지가 있습니다. 이 2가지 방법은 모두 Token Bucket 방식으로 동작하게 됩니다.

Token Bucket 방식

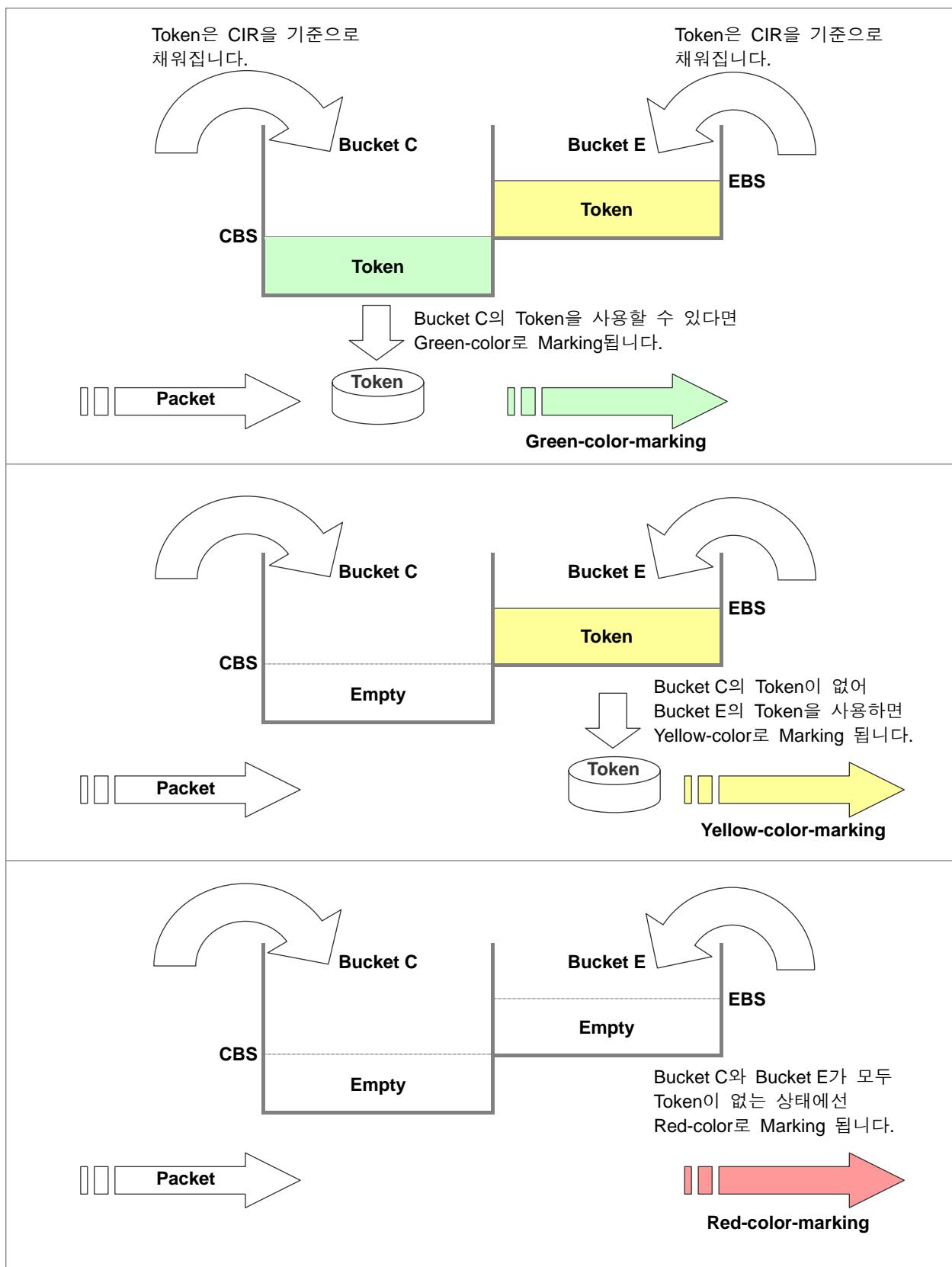
Token Bucket 방식이란, 우리가 일상 생활에서 특정한 목적지에 도착하기 위해 대중 교통을 이용할 때 요금을 내듯이, Token이 있어야만 패킷 전송이 가능하도록 하는 것입니다. Token Bucket에 Token은 일정하게 계속해서 채워지고, 패킷이 들어올 때마다 Token이 사용되기 때문에 패킷이 폭주하여 Token이 바닥나면 다시 Token이 채워질 때까지 패킷을 전송할 수 없게 됩니다.



【 그림 7-5 】 Token Bucket 방식

SRTCM(Single Rate Three Color Marker)

SRTCM은 RFC2697에서 정의하고 있는 것으로 CIR(Committed Information Rate)와 CBS(Committed Burst Size), EBS(Excess Burst Size)를 기준으로 Green, Yellow, Red의 3가지 Color를 Marking하게 됩니다. CIR은 Bucket에 Token을 채우는 속도가 되고, Token을 채우는 Bucket의 크기를 CBS와 EBS 두 단계로 나눠 Color를 다르게 Marking하는 기준으로 사용하게 됩니다.



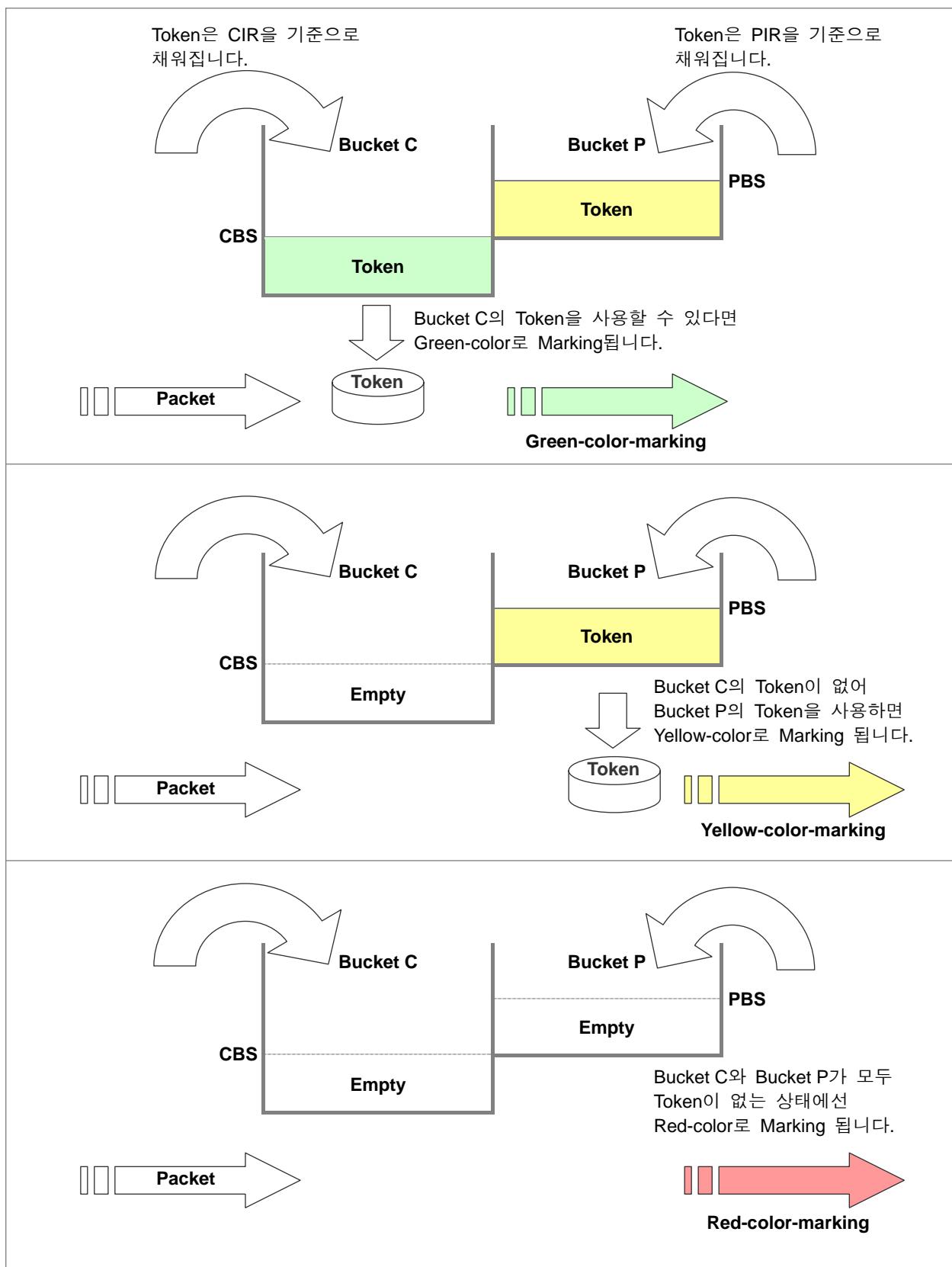
【 그림 7-6 】 Single Rate Three Color Marker의 Color Marking

장비에 패킷이 전송되었을 때 CBS 기준의 Bucket C에 있는 Token을 사용할 수 있다면 Green-color가 Marking 되고, Bucket C에 있는 Token가 고갈되어 EBS 기준의 Bucket E에 있는 Token을 사용한다면 Yellow-color가 Marking 됩니다. 그러나, 패킷 전송률이 높아 Bucket C와 Bucket E가 모두 고갈된 상태라면 Red-color로 Marking되게 됩니다.

RFC2697에서는 CBS와 EBS 중 하나는 반드시 0보다 큰 값으로 설정되어야 하며, 둘 중 하나를 0보다 큰 값으로 설정할 경우에는 장비에 들어오게 될 패킷의 최대 사이즈를 고려하여 최대 패킷 사이즈보다 크거나 같은 값으로 설정할 것을 권하고 있습니다. 이는 최소 1개의 패킷이라도 통과하도록 하기 위한 것입니다.

TRTCM(Two Rate Three Color Marker)

TRTCM은 RFC2698에서 정의하고 있는 것으로 CIR(Committed Information Rate)와 PIR(Peak Information Rate), CBS(Committed Burst Size), PBS(Peak Burst Size)를 기준으로 Green, Yellow, Red의 3가지 Color를 Marking하게 됩니다. SRTCM은 CBS 기준의 Bucket C에 Token을 채우는 속도와 EBS 기준의 Bucket E에 Token을 채우는 속도가 CIR로 동일하게 적용되지만, TRTCM은 CBS를 기준으로 하는 Bucket C에 Token을 채우는 속도와 PBS를 기준으로 하는 Bucket P를 채우는 속도가 각각 CIR과 PIR로 다르게 적용됩니다.



【 그림 7-7 】 Two Rate Three Color Marker의 Color Marking

장비에 패킷이 전송되었을 때 CBS 기준의 Bucket C에 있는 Token을 사용할 수 있다면 Green-color가 Marking 되고, Bucket C에 있는 Token가 고갈되어 PBS 기준의 Bucket P에 있는 Token을 사용한다면 Yellow-color가 Marking 됩니다. 그러나, 패킷 전송률이 높아 Bucket C와 Bucket P가 모두 고갈된 상태라면 Red-color로 Marking되게 됩니다.

RFC2698에서는 CBS와 PBS 중 하나는 반드시 0보다 큰 값으로 설정되어야 하며, 둘 중 하나를 0보다 큰 값으로 설정할 경우에는 장비에 들어오게 될 패킷의 최대 사이즈를 고려하여 최대 패킷 사이즈보다 크거나 같은 값으로 설정할 것을 권하고 있습니다. 이는 최소 1개의 패킷이라도 통과하도록 하기 위한 것입니다.

분류된 패킷들에 대해 Metering을 실행하려면, 먼저 사용자가 사용할 모드를 설정하십시오. Metering 모드를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
color mode {srtcm trtcn} blind	Policer	Metering 모드를 Color-Blind 모드로 설정합니다.

Blind 모드는 패킷에 이미 Marking된 Color를 무시하고 Metering을 실행하는 것이고, Aware는 이미 Marking된 Color도 고려하면서 Metering을 실행하는 것입니다.

Metering에서 사용할 모드를 설정하였으면, Metering의 각 기준 값을 설정해 놓아야 합니다. SRTCM을 선택하였다면, CIR, CBS, EBS를 설정해야 하고, TRTCM을 선택하였다면, CIR, PIR, CBS, PBS를 설정해야 합니다.

설정된 Metering 모드를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no color mode	Policer	설정한 Metering 모드를 해제하고 기본 모드로 설정합니다.

Metering에서 사용되는 각 기준 값을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
color cir bandwidth cbs burst	Policer	CIR과 CBS 값을 설정합니다.
color ebs burst		EBS 값을 설정합니다.
color pir bandwidth pbs burst		PIR과 PBS 값을 설정합니다.



참 고

CIR과 PIR의 설정 단위는 Kbps이며 64의 배수로 설정하십시오. EBS와 CBS, PBS의 설정 단위는 bytes입니다.



Metering의 기준을 설정하지 않으면 모든 패킷이 Green-color로 분류됩니다.

Metering 기준에 따라 각 Color-marking된 패킷에 따라 DSCP 값을 변경하여 설정해 주려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
color dscp <0-63> {green yellow red}	Policer	각 color-marking 된 패킷에 따라 DSCP 값을 변경하여 설정합니다.

Blind 모드의 경우, Red-color 또는 Yellow-color가 marking된 패킷은 받아들이지 않고 Drop 하도록 설정할 수 있습니다. Red-color 또는 Yellow-color의 패킷을 Drop 하도록 설정하거나 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
color red action drop	Policer	Red-color가 marking된 패킷을 Drop 하도록 설정합니다.
color yellow action drop		Yellow-color가 marking된 패킷을 Drop 하도록 설정합니다.
no color {red yellow} action		Red/Yellow-color가 marking된 패킷을 Drop하도록 한 설정을 해제합니다.

Aware 모드의 경우에는 Red-color 또는 Yellow-color의 패킷을 DSCP를 remarking 하도록 설정하거나 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
color {red yellow} action marking [drop-precedence {red yellow green}]	Rule	Red 또는 yellow-color가 marking된 패킷을 remarking 하도록 설정합니다.

(3) 패킷 Counter

V5812G는 Rule에 의해 처리된 패킷이 얼마나 되는지 그 개수를 세도록 설정할 수 있습니다. 이러한 기능은 관리자가 설정한 Rule의 내용에 따라 장비에 전송되는 패킷의 성격을 파악하는데 도움이 됩니다. 사용자가 설정해 놓은 Rule에 해당하는 패킷이 몇 번 들어왔는지 파악하려면 Policer 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
counter	Policer	사용자가 설정한 Rule에 해당하는 패킷이 몇 번 들어왔는지 파악합니다.



V5812G는 패킷을 Drop 하도록 설정한 Rule은 Count 할 수 없습니다.

사용자가 설정해 놓은 Rule에 해당하는 패킷이 몇 번 들어왔는지 파악하도록 설정한 것을 해제하려면 Policer 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no counter	Policer	사용자가 설정해 놓은 Rule에 해당하는 패킷이 몇 번 들어왔는지 파악하도록 설정한 것을 해제합니다.

V5812G의 Policy Counter를 초기화 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear policy counter {policer-name all}	Global/Bridge	Policy Counter를 초기화합니다.

Rule의 Count 개수를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show flow statistics	Enable/Global	Flow의 Count 개수를 확인합니다.
show class statistics		Class의 Count 개수를 확인합니다.
show policer statistics		Policer의 Count 개수를 확인합니다.
show policy statistics		Policy의 Count 개수를 확인합니다.

(4) 패킷 Rate-limit

V5812G는 Classify로 분류한 패킷에 대한 대역폭을 조절할 수 있습니다. Classify로 분류한 패킷에 대한 Rate-limit을 설정하려면 Policer 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
rate-limit bandwidth	Policer	Classify로 분류한 패킷에 대한 대역폭을 설정합니다.

Classify로 분류한 패킷에 대한 Rate-limit을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no rate-limit	Policer	Classify로 분류한 패킷에 대한 대역폭을 해제합니다.



참 고

Classify로 분류한 패킷에 대한 Rate-limit의 설정 단위는 **Kbps**입니다.

(5) Policer 내용 저장 및 수정

Classify로 분류된 패킷에 적용할 정책에 대한 설정을 마친 후에는 반드시 Policer의 내용을 저장해야 합니다.

설정이 끝난 Policer를 장비에 저장하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
apply	Policer	Policer의 설정을 장비에 저장합니다.



참 고

Policer 설정을 저장하지 않고 Policer 설정 모드에서 Global 모드로 돌아가면, 설정한 내용은 모두 사라지게 됩니다.

한편, 기존의 Policer의 내용을 수정하려면, 일단 수정하려는 Policer의 설정 모드로 들어가야 합니다. Policer의 내용을 수정하기 위해 특정 Policer의 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
policer <i>policer-name</i> modify	Global	내용을 수정하려는 특정 Policer의 설정 모드로 들어갑니다.



참 고

Policer의 내용을 수정한 후에도 반드시 **apply** 명령어를 사용하여 내용을 저장해야 합니다.

7.6.4. Rule 동작 설정

패킷을 분류하도록 Flow 및 Class를 설정하고, 분류된 패킷에 적용할 Policer를 설정하였다면, 사용자가 필요로 하는 Flow 또는 Class와 Policer를 선택적으로 구성하여 Policy를 설정하고 Rule의 동작을 실행해야 합니다.

(1) Policy 설정

Policy를 설정하려면, 먼저 Policy를 생성하여 Policy 설정 모드로 들어가야 합니다. Policy를 생성하고 Policy 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
policy <i>policy-name</i> create	Global	Policy를 생성하고 Policy 설정 모드로 들어갑니다.

한편, 설정했던 Policy를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no policy <i>policy-name</i>	Global	생성했던 해당 Policy를 삭제합니다.
no policy all		모든 Policy를 삭제합니다.

Policy를 생성하였다면, Rule로 실행할 Flow 또는 Class, 그리고, Policer를 Policy에 포함시킵니다. Policy에 Flow, Class, Policer를 포함시키려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
include-flow flow-name	Policy	해당 Flow를 Policy에 포함시킵니다.
include-class class-name		해당 Class를 Policy에 포함시킵니다.
include-policer policer-name		해당 Policer를 Policy에 포함시킵니다.



하나의 Policy에 Flow와 Class는 동시에 속할 수 없습니다.



동일한 Flow나 Class는 복수의 Policy에 중복 포함될 수 있지만, 하나의 Policer는 하나의 Policy에만 포함될 수 있습니다.

Policy에 포함시켰던 Flow 또는 Class, Policer를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no include-flow	Policy	해당 Flow를 삭제합니다.
no include-class		해당 Class를 삭제합니다.
no include-policer		해당 Policer를 삭제합니다.

(2) Policy 우선 순위 설정

사용자가 생성한 Policy에 대해 우선 순위를 설정할 수 있습니다. Policy에 우선 순위를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
priority { low medium high highest }	Policy	Policy에 우선 순위를 설정합니다.



모든 Policy는 기본적으로 우선 순위가 **low**로 설정되어 있습니다.

(3) Action 설정

패킷을 처리할 Rule의 동작을 설정하려면 Policy 모드에서 다음 명령어를 사용하십시오.

명령어	모드	기능
action match copy-to-cpu	Policy	분류된 패킷을 CPU로 올려보냅니다.
action match deny		분류된 패킷을 받아 들이지 않습니다.
action match mirror		분류된 패킷의 사본을 미러링 포트로 전송합니다.
action match dmac dst-mac-address		Rule에 해당하는 패킷의 Destination MAC 주소를 지정합니다.
action match dscp <0-63>		Rule에 해당하는 패킷의 ToS 영역에 있는 DSCP값을 지정합니다.
action match egress filter port-number		Rule에 해당하는 패킷의 Egress 포트에서 해당 포트를 제외합니다.
action match egress port port-number		Rule에 해당하는 패킷의 Egress 포트에서 해당 포트로 대체합니다.
action match permit		분류된 패킷을 받아 들입니다.
action match redirect port-number		분류된 패킷을 지정된 포트로 내보냅니다.
action match vlan <1-4094>		분류된 패킷의 VID를 지정합니다.



주의

redirect는 MAC 필터링과 같이 사용될 수 없습니다.

분류된 패킷에 대한 Rule의 동작을 설정한 것을 해제하려면, Policy 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no action match copy-to-cpu	Policy	Rule에 해당하는 패킷의 처리 방법을 설정했던 것을 해제합니다.
no action match deny		
no action match mirror		
no action match dmac		
no action match dscp		
no action match egress		
no action match permit		
no action match redirect		
no action match vlan		

(4) CoS값 및 ToS값 설정

사용자가 설정한 Rule을 사용하여 스케줄링 값을 적용하려면 먼저 각 규칙에 스케줄링 값을 적용할 수 있는 등급을 적용해야 합니다. CoS값은 총 8등급으로 구분됩니다. 한편, **overwrite** 변수는 사용자의 장비 내부에서만 패킷이 CoS 등급을 가지고 처리될 것인지, 아니면 외부 네트워크로 나갈 때에도 지정한 CoS값을 가지고 나갈 것 인지를 결정합니다. 즉, **overwrite**를 명령어에 포함하면 외부와 통신할 때에도 패킷에 CoS값이 적용되는 것이고 명령어에 포함하지 않으면 내부에서만 사용되도록 설정하는 것입니다.

Rule에 해당하는 패킷에 등급을 적용할 때에는 다음 명령어를 사용하십시오.

명령어	모 드	기 능
action match cos <0-7> [overwrite]	Policy	Rule에 해당하는 패킷에 CoS 값을 부여합니다.
action match cos same-as-tos		Rule에 해당하는 패킷에 CoS 값을 IP ToS precedence 값으로 지정합니다.
overwrite		
action match ip-precedence <0-7>		Rule에 해당하는 패킷에 IP ToS precedence 값을 지정합니다.
action match ip-precedence same-as-cos		Rule에 해당하는 패킷에 IP ToS precedence 값을 CoS 값을 지정합니다.

위에서 설정한 것을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no action match cos [overwrite]	Policy	Rule에 해당하는 패킷에 CoS 또는 IP ToS precedence 값을 부여했던 것을 해제합니다.
no action match cos same-as-tos overwrite		
no action match ip-precedence		
no action match ip-precedence same-as-cos		

(5) Rule 적용 인터페이스 지정

V5812G에서 Classify와 Policing, Rule 동작에 대한 설정이 끝났다면, 해당 Rule을 적용할 인터페이스를 지정해야 합니다. 앞에서 설명한 모든 설정을 마쳐도 적용할 인터페이스를 지정하지 않으면 Rule은 동작하지 않습니다.

Rule을 적용할 인터페이스를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
interface-binding port ingress {port-number cpu any}	Policy	해당 포트로 들어오는 패킷을 기준으로 Rule을 적용하도록 합니다.
interface-binding port egress {port-number cpu any}		해당 포트에서 나가는 패킷을 기준으로 Rule을 적용하도록 합니다.
interface-binding vlan {<1-4094> any}		해당 VLAN ID를 가지고 들어오는 패킷을 기준으로 Rule을 적용하도록 합니다.

Rule을 적용할 인터페이스를 지정했던 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no interface-binding port ingress port-number	Policy	Rule을 적용할 인터페이스를 지정했던 것을 해제합니다.
no interface-binding port egress {port-number cpu}		
no interface-binding vlan		

(6) Policy 내용 저장 및 수정

Rule의 동작을 실행하기 위해 Policy를 설정한 후에는 반드시 Policy의 내용을 저장해야 합니다. 설정이 끝난 Policy를 장비에 저장하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
apply	Policy	Policy의 설정을 장비에 저장합니다.



Policy 설정을 저장하지 않고 Policy 설정 모드에서 Global 모드로 돌아가면, 설정한 내용은 모두 사라지게 됩니다.

한편, 기존의 Policy의 내용을 수정하려면, 일단 수정하려는 Policy의 설정 모드로 들어가야 합니다. Policy의 내용을 수정하기 위해 특정 Policy의 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
policy policy-name modify	Global	내용을 수정하려는 특정 Policy의 설정 모드로 들어갑니다.



Policy의 내용을 수정한 후에도 반드시 **apply** 명령어를 사용하여 내용을 저장해야 합니다.

7.6.5. Rule 설정 내용 확인

사용자가 설정한 Rule Profile을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show flow-profile	Flow	해당 Flow의 Profile을 확인합니다.
show policer-profile	Policer	해당 Policer의 Profile을 확인합니다.
show policy-profile	Policy	해당 Policy의 Profile을 확인합니다.

사용자가 설정한 Rule의 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show {flow class policer policy} [name]	Veiw/Enable/ Global/Bridge	설정한 Rule의 내용을 확인합니다.
show {flow class policer policy} detail [name]		
show running-config {flow policer policy}	All	Flow, Clas 및 Policy의 모든 설정을 확인합니다.

Policy-based-routing을 설정한 Rule의 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip route pbs	Enable/Global/Bridge	Policy를 기반으로 설정된 Rule의 이름 및 Next-hop 주소 등을 확인합니다.

7.6.6. 스케줄링(Scheduling) 설정

(1) 스케줄링(Scheduling) 방식 설정

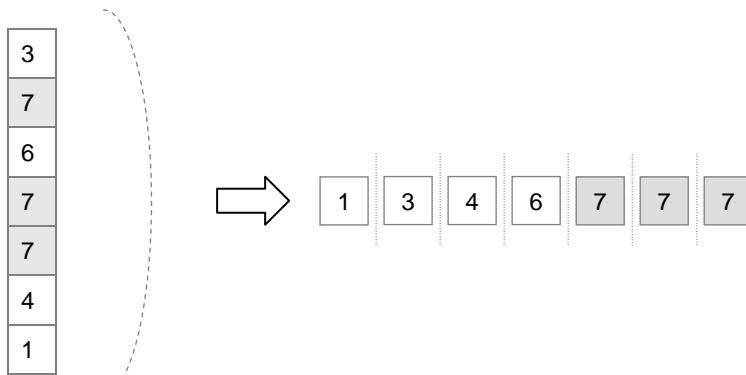
V5812G는 큐를 처리하는데 Strict Priority Queuing, WRR, DRR 방식을 이용할 수 있습니다.

- **Strict Priority Queuing**

Strict Priority Queuing은 우선 순위가 높은 큐의 패킷을 우선적으로 처리하는 방식으로, 다시 말하자면, 우선 순위가 낮은 큐의 패킷은 우선 순위가 높은 큐의 패킷이 모두 처리된 이후에나 처리됩니다. 만약, 우선 순위가 낮은 큐의 패킷이 처리되고 있는 도중이라도 우선 순위가 높은 큐의 패킷이 입력되면 우선 순위가 낮은 큐의 패킷에 대한 처리는 잠시 멈추게 됩니다.

이 방식은 간단한 방식으로 차별화된 서비스를 제공할 수 있다는 장점을 가지고 있습니다. 그러나 우선 순위가 높은 큐의 패킷이 계속해서 입력되는 경우에는 우선 순위가 낮은 큐의 패킷은 처리되지 않는다는 문제점이 있습니다.

아래와 같은 큐 번호를 가진 패킷들이 들어왔을 때 Strict Priority Queuing에서 처리되는 순서

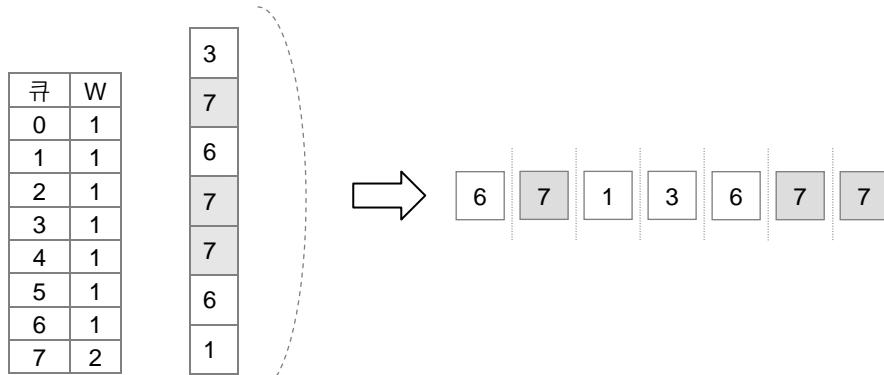


【 그림 7-8 】 Strict Priority Queuing에서의 패킷 처리

- **WRR(Weighted Round Robin)**

WRR은 주어진 Weight 값만큼 차례대로 패킷을 처리하는 방법입니다. 우선 순위가 높은 큐의 패킷을 먼저 처리하는 것은 Strict Priority Queuing과 마찬가지이지만, 주어진 Weight 값만큼만 처리하고 다음 단계로 넘어가기 때문에 패킷 처리가 우선 순위가 높은 큐의 패킷에 치우치지 않게 설정할 수 있습니다. 그러나, 서비스의 공정성을 생각한 만큼 차별화된 서비스를 제공하는 것에 한계가 있습니다.

아래와 같은 큐 번호를 가진 패킷들이 들어왔을 때 WRR에서 처리되는 순서



【 그림 7-9 】 WRR에서의 패킷 처리

- DRR(Deficit Round Robin)

DRR은 큐에 할당된 수신 포트 대역폭의 %값, scheduler가 매회 큐에서 내보낼 수 있는 bytes의 전체량, weight에 대한 bytes의 비율을 파라미터로 사용하여 패킷 처리 순서를 결정합니다. 클래스 별로 할당된 대역폭이 패킷 사이즈에 관계없이 정확하게 보장되는 장점을 가지고 있습니다.

이 세 가지 스케줄링 방식 가운데 어떤 방식을 사용할지 선택하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>qos scheduling-mode {sp wrr drr} port-number</code>	Global	스케줄링 방식을 선택합니다.



V5812G는 기본적으로 “WRR”을 기본 방식으로 사용하고 있습니다.

(2) Weight 설정

스케줄링 방식 중 WRR 방식은 Weight 값에 따라 패킷을 처리하는 방식입니다. 따라서 Weight 값이 필요한데, 사용자가 이를 설정할 수 있습니다.

WRR 방식을 사용할 경우, Weight 값을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
qos weight port-number queue-number weight-value	Global	지정한 포트의 해당 큐에 Weight 값을 설정합니다.
qos weight port-number queue-number unlimited		지정한 포트의 해당 큐를 Strict Priority Queuing으로 진행합니다.



queue-number 는 <0-3>, *weight-value*는<1-127> 범위 내에서 입력합니다.



V5812G는 기본적으로 모든 큐의 Weight가 “1”로 설정되어 있습니다.

DRR 방식을 사용하기 위한 Quantum을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
qos quantum port-number queue-number quantum-value	Global	지정한 포트의 해당 큐에 Quantum 값을 설정합니다.
qos quantum port-number queue-number unlimited		지정한 포트의 해당 큐를 Strict Priority Queuing으로 진행합니다.



queue-number 는 <0-7>, *quantum-value*는<1-255> 범위 내에서 입력합니다.



V5812G는 기본적으로 모든 큐의 *quantum-value*가 “1”로 설정되어 있습니다.

(3) Min-bandwidth 설정

스케줄링 방식 중 DRR은 대역폭으로 해당 큐의 패킷을 처리량을 제한합니다. 따라서 DRR 방식을 이용할 때에는 큐마다 보장 대역폭을 설정해야 합니다. 이러한 보장 대역폭을 **Min-bandwidth**라고 합니다.



참 고

V5812G는 기본적으로 모든 큐의 최소 보장 대역폭이 “0”으로 설정되어 있습니다.

보장 대역폭을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
qos min-bandwidth port-number <0-7> <1-100>	Global	보장 대역폭을 설정합니다.
qos min-bandwidth port-number <0-7> unlimited		보장 대역폭을 제한하지 않습니다.

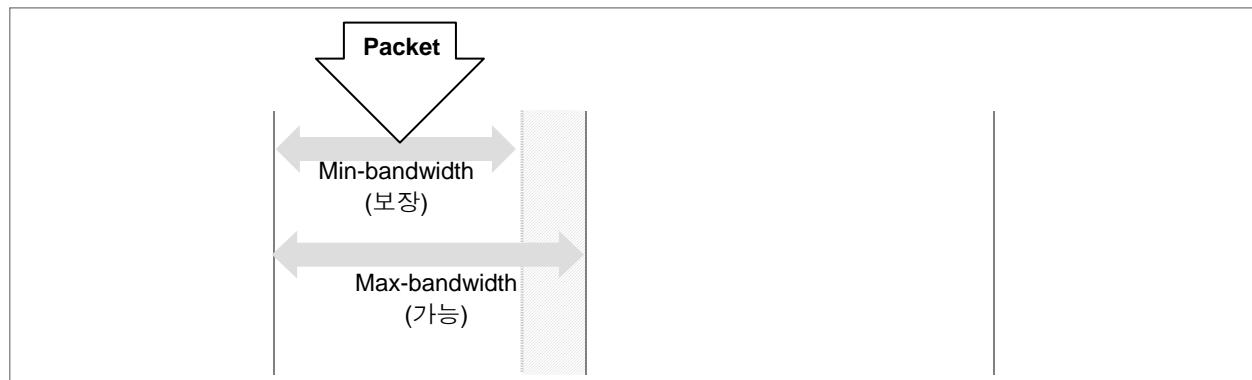


참 고

SP 방식이나 WRR 방식을 선택한 상태에서는 보장 대역폭을 설정할 수 없습니다.

(4) Max-bandwidth 제한

Strict Priority Queuing 방식으로 스케줄링을 처리하더라도 한 가지 등급의 패킷만 집중되어 처리될 수도 있습니다. 이런 것을 방지하기 위해 사용자는 대역폭에 제한을 둘 수 있습니다. 이러한 역할을 하는 것이 바로 Max-bandwidth입니다.



【 그림 7-10 】 DRR에서의 Min-bandwidth와 Max-bandwidth

해당 큐가 사용할 수 있는 최대 대역폭을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
qos max-bandwidth port-number <0-7> <1-100>	Global	최대 사용 가능한 대역폭을 설정합니다.
qos max-bandwidth port-number unlimited		최대 사용 가능한 대역폭에 제한을 없앱니다.



참 고

V5812G는 기본적으로 사용 가능한 대역폭에 제한을 두고 있지 않습니다.



참 고

SP 방식이나 WRR 방식을 선택한 상태에서는 가능 대역폭을 설정할 수 없습니다.

(5) 특정 포트의 트래픽 제한 설정

V5812G에서는 QoS 기능을 이용하여 사용자의 필요에 따라 특정 포트로 들어오거나 나가는 패킷의 트래픽을 제한할 수 있습니다. 사용자의 장비로 패킷이 들어오는 수신 포트(Ingress Port)의 버퍼 크기를 제한하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
qos ibp port-number <1-8191>	Global	수신 포트로 지정된 특정 포트에서 사용하는 버퍼 크기를 제한합니다.



참 고

버퍼 크기를 제한하는 단위는 Kbit입니다.



참 고

V5812G에는 기본값이 81Kbit로 설정되어 있습니다.

설정한 수신 포트의 버퍼 크기 제한을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no qos ibp port-number	Global	수신 포트로 지정된 특정 포트에서 사용하는 버퍼 크기 제한 설정을 해제합니다.

한편, 사용자 장비에서 패킷이 나가는 송신 포트(Egress Port)는 Queue에서 사용하는 패킷 개수와 버퍼 크기를 동시에 제한할 수 있습니다.

송신 포트의 트래픽을 제한하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
qos pktlimit port-number queue-number <4-1023>	Global	송신 포트로 지정된 특정 포트의 Queue에서 사용하는 패킷 개수를 제한합니다. 장비의 기본값은 256개로 설정되어 있습니다.
qos seglimit port-number queue-number <1-8191>		송신 포트로 지정된 특정 포트의 Queue에서 사용하는 버퍼 크기를 제한합니다. 장비의 기본값은 24Kbit로 설정되어 있습니다.



*queue-number*는 <0-3> 범위 내에서 입력하십시오.

설정한 송신 포트의 Queue에서 사용하는 패킷 개수와 버퍼 크기의 제한을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no qos pktlimit port-number <0-3>	Global	송신 포트로 지정된 특정 포트의 Queue에서 사용하는 패킷 개수의 제한을 해제합니다.
no qos seglimit port-number <0-3>		송신 포트로 지정된 특정 포트의 Queue에서 사용하는 버퍼 크기의 제한을 해제합니다.

한편, 위에서 설정한 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show qos buffer port-number	Global	송신 포트 및 수신 포트의 트래픽 제한 정보를 확인합니다.

(6) CPU 패킷에 대한 사용자 정의

V5812G는 CPU 패킷의 큐를 처리하는데 Strict Priority Queuing 방식을 이용할 수 있습니다. CPU 패킷의 큐를 처리하는데 Strict Priority Queuing 방식을 이용하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
qos cpu scheduling-mode sp	Global	Strict Priority Queuing 방식으로 CPU 패킷을 스케줄링 합니다.

(7) QoS 내용 확인

QoS에 대한 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show qos	Enable/ Global/ Bridge	QoS 스케줄링에 대한 설정 내용을 확인합니다.
show qos port-number		포트별로 QoS 스케줄링에 대한 설정 내용을 확인합니다.
show qos buffer port-number		포트별로 할당된 버퍼에 대한 설정 내용을 확인합니다.
show qos cpu		QoS 스케줄링 모드와 CoS-Queue map을 확인합니다.

(8) 포트별 Queue 트래픽 확인

V5812G는 포트별 Queue의 트래픽 양을 확인할 수 있습니다. 포트별로 각각의 Queue에 해당하는 트래픽이 얼마나 되는지 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show queue status port-number [<0-3>]	Enable /Global	포트별로 각각의 Queue에 해당하는 트래픽 양을 확인합니다.

7.6.7. Admin Rule 설정

위에서 설명한 Rule을 이용하여 스위치 자체로 들어오는 telnet, ftp, icmp, snmp 등의 서비스 접속을 막도록 설정할 때에는 수많은 Rule을 적용해야 하기 때문에 복잡하고 Rule 소모량이 많은 단점이 있습니다. 이러한 불편함을 해결하기 위하여 V5812G에서는 스위치에 연결된 장비에 패킷이 포워딩 되기 전에 필터링을 수행할 수 있는 기능을 지원합니다. 스위치 자체로 들어오는 Telnet, FTP, ICMP, SNMP 등의 서비스 접속을 막을 때에는 Admin Rule이라는 기능이 사용됩니다.

7.6.8. Admin Rule 패킷 분류(Classify) 설정

V5812G는 Admin Rule을 적용할 패킷을 분류하는 조건을 Flow로 만들어 설정하고, 복수의 Flow를 관리할 때에는 Class를 활용하도록 되어 있습니다.

(1) Admin Flow 설정

V5812G는 Admin Rule을 설정하려면 가장 먼저 Admin Flow를 생성하여 Admin Flow 설정 모드로 들어가야 합니다. 그래야 세부적인 패킷 조건을 설정할 수 있게 됩니다.

패킷의 세부적인 조건을 정해 분류하려면 먼저 Admin Flow 설정 모드로 들어가려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
flow admin name create	Global	Admin Flow를 생성하고 Admin Flow 설정 모드로 들어갑니다.

Admin Flow 설정 모드로 들어가면 명령어의 프롬프트가 SWITCH(config)#에서 SWITCH(config-admin-flow[name])#로 바뀝니다.



하나의 Admin Flow에 여러 가지 정책을 설정할 수 있습니다.

한편, 설정했던 Admin Flow를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no flow admin flow-name	Global	생성했던 해당 Flow를 삭제합니다.
no flow admin all		모든 Flow를 삭제합니다.

Admin Flow 설정 모드로 들어간 후에는 사용자가 원하는 Admin Flow를 알맞게 설정하십시오. Admin Flow에는 Admin Flow에 적용시킬 패킷의 조건과 조건에 맞는 패킷을 어떻게 처리할 것인가 하는 패킷 처리 방법을 설정합니다. Admin Flow에는 패킷을 분류하는 조건이 지정되며, IP 주소, ICMP, TCP, UDP 등 다양한 기준으로 사용자가 원하는 조건의 Admin Flow를 설정할 수 있습니다.

IP 주소를 기준으로 패킷을 분류하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any}	Admin Flow	Source IP 주소와 Destination IP 주소 기준으로 정책을 설정합니다.
ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} <0-255>		Source IP 주소, Destination IP 주소, 그리고 프로토콜을 기준으로 정책을 설정합니다.
ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} {icmp tcp udp}		ICMP의 Message type과 Code 값도 정책 기준으로 설정합니다.
ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} icmp <0-255> any} <0-255> any}		TCP Source 포트와 Destination 포트까지 정책 기준으로 설정합니다.
ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} tcp <1-65535> any} <1-65535> any} [tcp-flag any]		UDP Source 포트와 Destination 포트까지 정책 기준으로 설정합니다.
ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} udp <1-65535> any} <1-65535> any}		Source IP 주소와 Destination IP 주소 기준으로 정책을 설정합니다.
ip header-length <1-15>		설정한 IP Header 길이에 해당하는 패킷을 분류합니다.



하나의 Admin Flow에 여러 가지 정책을 설정할 수 있습니다.

한편, Admin Flow에 설정한 패킷 분류 조건을 삭제하려면, Admin Flow 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip	Admin Flow	Admin Flow에 설정한 패킷 분류 조건을 삭제합니다.
no ip header-length		

(2) Admin Flow 내용 저장 및 수정

패킷 분류 조건에 대한 설정이 끝난 Flow는 반드시 장비에 저장해야 합니다. 설정이 끝난 Flow를 장비에 저장하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
apply	Admin Flow	Flow의 설정을 장비에 저장합니다.



Admin Flow 설정을 저장하지 않고 Admin Flow 설정 모드에서 Global 모드로 돌아가면, 설정한 내용은 모두 사라지게 됩니다.

한편, 기존의 Admin Flow의 내용을 수정하려면, 일단 수정하려는 특정 Admin Flow의 설정 모드로 들어가야 합니다. Flow의 내용 수정을 위해 Admin Flow 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
flow admin flow-name modify	Global	내용을 수정하려는 특정 Admin Flow의 설정 모드로 들어갑니다.



Admin Flow의 내용을 수정한 후에도 반드시 **apply** 명령어를 사용하여 내용을 저장해야 합니다.

(3) Class 설정

여러 가지 조건을 가지고 패킷을 분류하게 될 경우, 2개 이상의 Flow가 필요로 할 경우가 있습니다. 이러한 경우 여러 개의 Flow를 Class로 묶어서 사용하면 관리하기도 쉽고, 설정도 간편해집니다. 2개 이상의 Admin Flow를 하나의 Class로 묶어서 사용하려면, 다음 명령어를 사용하여 Class를 설정하십시오.

명령어	모 드	기 능
class admin class-name flow flow-name [flow-name] [flow-name]…	Global	Admin Flow를 모아 Admin Class를 설정합니다.

한편, Admin Class 설정을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no class admin all	Global	설정되어 있는 모든 Admin Class를 삭제합니다.
no class admin class-name		해당 Class를 삭제합니다.
no class admin class-name flow flow-name [flow-name] [flow-name] ...		해당 Class에서 특정 Flow를 삭제합니다.

7.6.9. Admin Rule 동작 설정

패킷을 분류하도록 Flow 및 Class를 설정하였다면, 사용자가 필요로 하는 Flow 또는 Class와 Policer를 선택적으로 구성하여 Policy를 설정하고 Rule의 동작을 실행해야 합니다.

(1) Policy 설정

Admin Policy를 설정하려면, 먼저 Admin Policy를 생성하여 해당 설정 모드로 들어가야 합니다. Admin Policy 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
policy admin policy-name create	Global	Admin Policy를 생성하여 해당 설정 모드로 들어갑니다.

한편, 설정했던 Admin Policy를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no policy admin policy-name	Global	생성했던 해당 Admin Policy를 삭제합니다.
no policy admin all		모든 Admin Policy를 삭제합니다.

Admin Policy를 생성하였다면, Admin Rule로 실행할 Flow 또는 Class 를 해당 Policy에 포함시킬 수 있습니다. 이를 통해 Policy 단위로 action 설정이 가능합니다.

Admin Policy에 특정한 Class나 Flow를 포함시키려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
include-class class-name	Admin Policy	해당 Admin Class를 해당 Policy에 포함시킵니다.
include-flow flow-name		해당 Admin Flow를 해당 Policy에 포함시킵니다.



주의

하나의 Admin Policy에 Admin Flow와 Admin Class는 동시에 속할 수 없습니다.

포함시켰던 Flow 또는 Class를 해당 Policy로부터 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no include-class	Admin Policy	설정한 Admin Class를 삭제합니다.
no include-flow		설정한 Admin Flow를 삭제합니다.

(2) Policy 우선 순위 설정

우선 순위가 높은 Admin Policy 일수록 빠르게 처리됩니다. 사용자가 설정할 Admin Policy의 우선 순위를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
priority {low medium high highest}	Admin Policy	새로운 Admin Policy에 대한 우선 순위를 설정합니다.



참 고

모든 Admin Policy는 기본적으로 우선 순위가 **low**로 설정되어 있습니다.

(3) Admin Policy의 Action 설정

Admin Policy에 적용할 패킷의 조건을 설정하였다면, 조건에 맞는 패킷을 어떻게 처리하도록 할 것 인지를 설정해야 합니다.

Admin Policy에 해당하는 패킷을 어떻게 처리할 것인지 Policy의 동작을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
action match deny	Admin Policy	Admin Policy에 해당하는 패킷을 받아 들이지 않습니다.
action match permit		Admin Policy에 해당하는 패킷을 받아 들입니다.

위에서 설정한 것을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no action match deny	Admin Policy	Admin Policy에 해당하는 패킷의 처리 방법을 설정했던 것을 해제합니다.
no action match permit		

한편, 다음은 Admin Policy에 해당하지 않는 패킷을 처리하는 방법을 설정하는 명령어입니다.

명령어	모 드	기 능
action no-match deny	Admin Policy	Admin Policy에 해당하지 않는 패킷을 받아 들이지 않습니다.
action no-match permit		Admin Policy에 해당하지 않는 패킷을 받아 들입니다.

위에서 설정한 것을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no action no-match deny	Admin Policy	Admin Policy에 해당하지 않는 패킷에 대한 처리 방법을 설정했던 것을 해제합니다.
no action no-match permit		

(4) Policy 내용 저장 및 수정

위에서 설명한 명령어를 이용하여 Admin Rule을 모두 설정하였다면, Admin Rule을 저장하여 장비에 적용시켜야 합니다. Admin Rule의 내용을 저장하고 장비에 적용하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
apply	Admin Policy	Policy의 설정을 장비에 저장합니다.



참 고

Admin Policy 설정을 저장하지 않고 Admin Policy 설정 모드에서 Global 모드로 돌아가면, 설정한 내용은 모두 사라지게 됩니다.

한편, 기존의 Policy의 내용을 수정하려면, 일단 수정하려는 Policy의 설정 모드로 들어가야 합니다. Policy의 내용을 수정하기 위해 특정 Policy의 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
policy admin policy-name modify	Global	내용을 수정하려는 특정 Policy의 설정 모드로 들어갑니다.



참 고

Policy의 내용을 수정한 후에도 반드시 **apply** 명령어를 사용하여 내용을 저장해야 합니다.

7.6.10. Admin Rule 설정 내용 확인

사용자가 설정한 Admin Rule Profile을 확인하려면 다음 명령어를 사용하십시오.

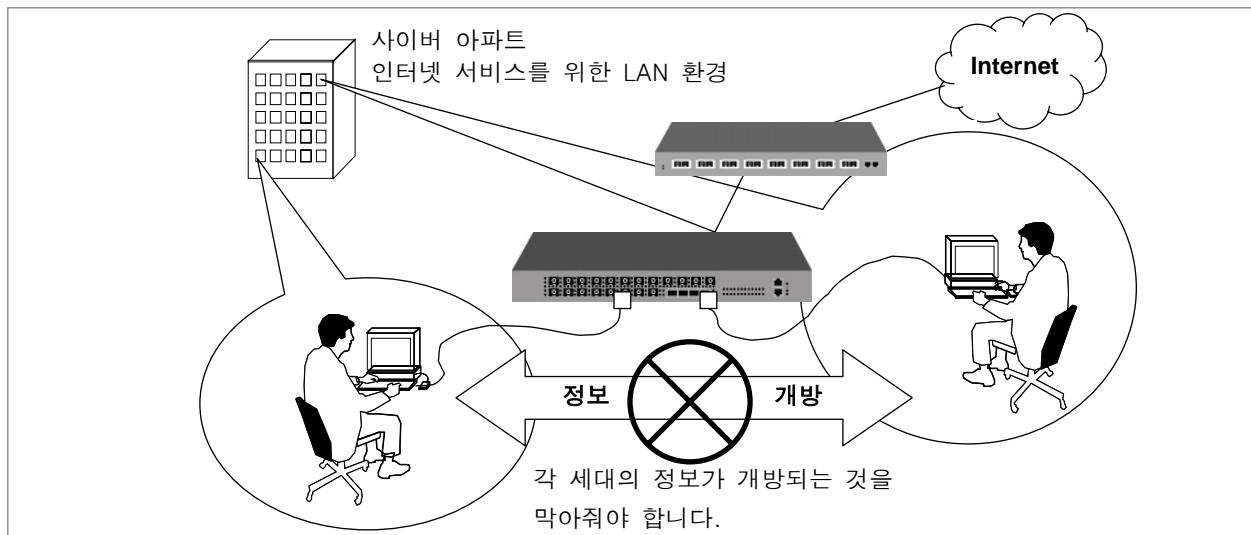
명령어	모 드	기 능
show flow-profile admin	Admin Flow	해당 Flow의 Profile을 확인합니다.
show policy-profile admin	Admin Policy	해당 Policy의 Profile을 확인합니다.

사용자가 설정한 Admin Rule의 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show {flow class policy} admin [name]	View/Enable/ Global/Bridge	설정한 Admin Rule의 내용을 확인합니다.
show {flow class policy} admin detail [name]		
show running-config {admin-flow admin-policy}	All	Admin Flow나 Policy의 모든 설정을 확인합니다.

7.7 NetBIOS Filtering

서로 정보를 공유해야 하는 LAN(Local Area Network) 환경에서는 컴퓨터간에 통신이 가능하도록 NetBIOS를 사용합니다. 그러나 ISP(Internet Service Provider) 사업자들이 아파트나 특정한 지역에 LAN 서비스로 인터넷 통신을 제공하는 경우에는 고객들의 정보가 보장되어야 합니다. 이 때, NetBIOS 필터링 기능이 없다면 정보를 공유해서는 안되는 상황에서 서로의 정보가 공개될 수 도 있습니다.



【 그림 7-11 】 NetBIOS Filtering의 필요성



NetBIOS 필터링 기능은 Flow를 Extension 모드로 설정해야 설정할 수 있습니다.

사용자의 요구에 따라 특정 포트에 NetBIOS 필터링 기능을 설정하려면 필터링 기능을 활성화 시킨 후 다음 명령어를 사용하여 NetBIOS 필터링 기능이 필요한 포트를 지정하십시오.

명령어	모 드	기 능
<code>netbios-filter port-number</code>	Bridge	해당 포트에 NetBIOS 필터링 기능을 설정합니다.

한편, 사용자의 요구에 따라 특정 포트에서 NetBIOS 필터링 기능을 해제하려면 다음 명령어를 사용하십시오.

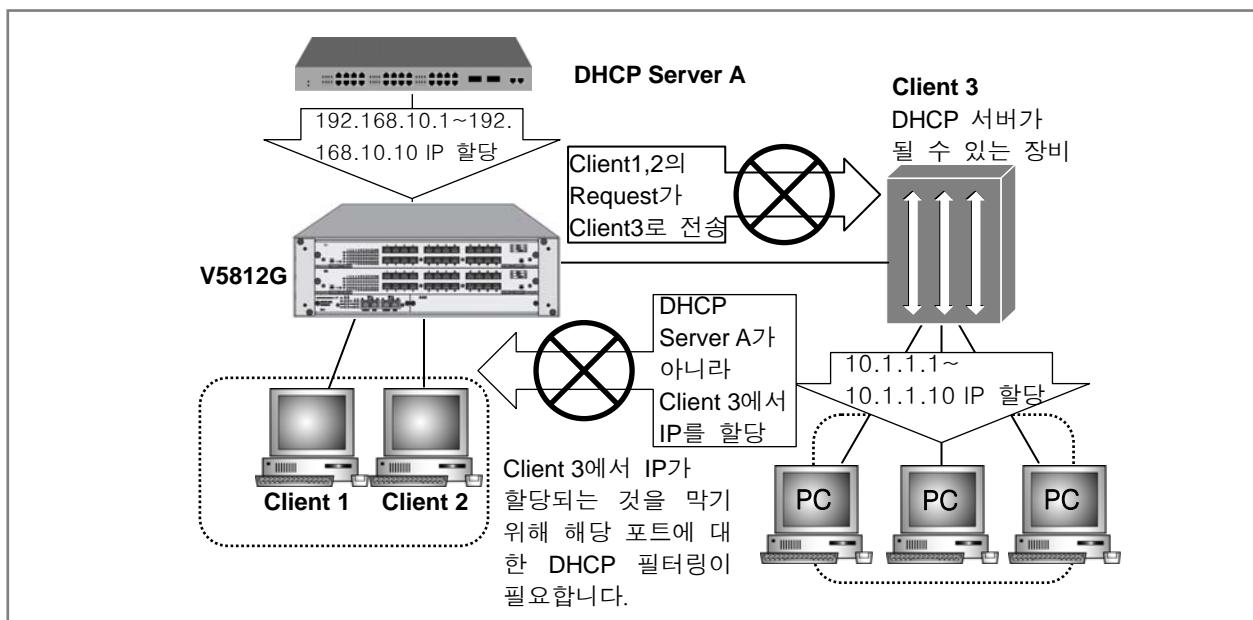
명령어	모 드	기 능
no netbios-filter port-number	Bridge	해당 포트에서 NetBIOS 필터링 기능을 해제합니다.

NetBIOS 필터링 기능의 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show netbios-filter	Enable/Global/Bridge	NetBIOS 필터링 설정을 확인합니다.

7.8 DHCP 서버 패킷 필터링

DHCP(Dynamic Host Control Protocol)는 DHCP 서버가 DHCP 클라이언트에게 자동적으로 IP 주소를 할당하고 IP 주소를 관리할 수 있도록 하는 프로토콜로서 대부분의 ISP 사업자는 이와 같은 방법으로 서비스를 제공하고 있습니다. 이 때, 어떤 DHCP 클라이언트가 IP 공유기 등 또 다른 DHCP 서버가 될 수 있는 장비를 연결해 버린다면, 통신 장애가 발생할 수 있습니다. DHCP 필터링은 가입자포트를 통해 들어왔다가 업링크포트나 다른 가입자포트로 나가는 Request와 가입자포트로 들어오는 Reply를 막아줌으로써 DHCP 서비스가 올바르게 이루어지도록 도와주는 것입니다.



【 그림 7-12 】 DHCP 필터링

위의 그림을 예로 들어보면, DHCP 서버가 192.168.10.1부터 192.168.10.10까지의 IP 주소 영역을 가지고 있는 서버 A에 어떤 사용자가 DHCP 서버가 될 수 있는 장비인 Client 3을 연결, 10.1.1.1부터 10.1.1.10까지의 IP를 공유한다고 가정해 봅시다. 이러한 상황에서 Client 1과 Client 2를 각각 DHCP 서버가 되어버린 Client 3와 차단하지 않으면, Client 1과 Client 2가 Client 3에게 IP를 요청하고, IP를 받아와서 통신이 불가능하게 되는 경우가 발생하게 됩니다.

따라서, Client 1과 Client 3의 사이에 필터링 기능을 설정하고, Client 2와 Client 3 사이에 필터링 기능을 설정하여 Client 1과 Client 2는 DHCP 서버 A로부터 IP를 무리없이 받아 올 수 있도록 해야 합니다.

사용자의 요구에 따라 특정 포트에 DHCP 필터링 기능을 설정하려면 필터링 기능을 활성화 시킨 후 다음 명령어를 사용하여 DHCP 필터링 기능이 필요한 포트를 지정하십시오.

명령어	모 드	기 능
dhcp-server-filter port-number	Bridge	DHCP 서버 패킷 필터링을 설정합니다.
no dhcp-server-filter port-number		DHCP 서버 패킷 필터링을 해제합니다.

DHCP 서버 필터링 기능에 대한 설정을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show dhcp-server-filter	Enable/Global/Bridge	DHCP 서버 필터링 기능에 대한 설정을 확인합니다.

7.9 Martian Filtering

V5812G는 같은 네트워크 안에서 다른 Source IP 주소를 가지고 외부로 나가려는 패킷을 막을 수 있습니다. 자신의 Source IP 주소가 아닌 다른 주소를 가지고 외부로 나가면 패킷 경로 추적이 불가능하기 때문에 문제를 일으키고도 발각되지 않을 수 있습니다. 따라서 자신의 네트워크에서 이러한 패킷이 나가도록 미리 방지하는 것이 좋습니다.

같은 네트워크 안에서 다른 Source IP 주소를 가지고 외부로 나가는 패킷을 막으려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip martian-filter interface-name	Global	해당 인터페이스에서 다른 Source IP 주소를 가지고 외부로 나가는 패킷을 막습니다.



QoS와 Martian Filtering은 동시에 설정할 수 없습니다.

한편, 같은 네트워크 안에서 다른 Source IP 주소를 가지고 외부로 나가는 패킷을 막도록 설정한 것을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip martian-filter interface-name	Global	해당 인터페이스에서 다른 Source IP 주소를 가지고 외부로 나가는 패킷을 막도록 설정한 것을 해제합니다.

Martian-filter의 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show running-config	View/Enable/Global/Bridge/Interface	장비 설정 내용을 확인합니다.

7.10 MAC 필터링

사용자의 장비는 별다른 성능 저하 없이 최대 8,192개의 MAC 주소를 등록하여 프레임 전송 제한에 참고합니다.

7.10.1. MAC 필터 기본 정책 설정

포트에 전송되는 특정한 MAC 주소를 가진 패킷에 대한 필터 정책을 설정하기 전에 모든 패킷에 대한 기본적인 필터링 정책을 설정하려면, Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
mac-filter default-policy {deny permit} port-number	Bridge	해당 포트에 기본 정책을 설정합니다.



참 고

MAC 필터링을 설정할 때에는 모든 MAC 주소의 패킷을 차단하도록 설정한 후, 특정 MAC 주소의 패킷을 받아들이도록 설정을 추가해 나가는 것이 편리합니다.

한편, 모든 패킷에 대한 기본적인 필터링 정책을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show mac-filter default-policy	Enable/Global/Bridge	필터링 기본 정책을 확인합니다.



참 고

시스템에서 제공하는 기본적인 필터링 정책은 각 포트마다 모든 패킷을 허용하는 것으로 설정되어 있습니다.

7.10.2. MAC 필터 정책 추가

MAC 필터링에 대한 기본 정책을 설정한 후 특정한 MAC 주소를 가진 패킷을 차단, 또는 허용하도록 정책을 추가할 수 있습니다. 이러한 정책을 추가할 때에는 다음 명령어를 사용하십시오.

명령어	모 드	기 능
mac-filter add mac-address {deny permit} [vlan-id any] [port-number]	Bridge	해당 MAC 주소의 패킷을 허용 또는 차단합니다.



참 고

변수 MAC-ADDRESS는 12개의 16 진수로 이루어졌는데 **show mac** 명령어로 확인할 수 있습니다. 00:d0:cb:06:01:32 는 MAC 주소의 한 예입니다.

사용자가 설정한 필터 정책을 확인할 때에는 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show mac-filter	Enable Global/Bridge	MAC 필터 정책 테이블을 보여줍니다.



참 고

MAC 필터 정책은 사용자가 최근에 설정한 것이 1번으로 기록됩니다. 지정한 개수 만큼의 필터 정책을 보여줄 때에는 테이블의 기록된 순서를 기준으로 보여줍니다.

7.10.3. MAC 필터 정책 삭제

사용자 장비에 설정한 필터링 정책을 삭제하려면, 다음 명령어를 사용하십시오. 필터링 정책을 삭제할 때에는 특정 MAC 필터 또는 모든 MAC 필터를 삭제하도록 선택할 수 있습니다.

명령어	모 드	기 능
mac-filter del mac-address	Bridge	특정 MAC 필터를 삭제합니다.
no mac-filter		모든 MAC 필터를 삭제합니다.

7.10.4. MAC 필터링 정책 List 불러오기

많은 MAC 필터링 정책을 한꺼번에 만들어야 할 때에는 하나하나 명령어를 입력하기가 힘들 수 있습니다. 이러한 경우에 사용자는 MAC 필터링 정책을 간편한 방법으로 만들어서 “/etc/mfdb.conf”에 저장시키면 다음 명령어를 사용하여 MAC 필터링 정책 List를 불러 올 수 있습니다.

명령어	모 드	기 능
mac-filter list	Bridge	/etc/mfdb.conf 에 있는 MAC 필터 정책 List를 불러옵니다.

7.10.5. 고정 IP 사용자 차단하기

V5812G는 MAC 필터링 기능을 이용하여 DHCP 서버로부터 IP 주소를 할당 받지 않고 강제로 IP 주소를 설정하여 사용하는 사용자를 차단할 수 있습니다. 고정 IP 사용자를 차단하는 방법은 다음과 같습니다.

- 1 단계 고정 IP 사용자를 차단할 포트에 MAC 필터의 기본 정책을 “**deny**”로 설정합니다.
- 2 단계 DHCP 서버로부터 IP 주소를 받아가는 MAC 주소에 대해서만 “**permit**”으로 설정해줍니다.

7.11 접속자 수 지정

사용자는 포트 별로 접속 가능한 MAC 갯수를 설정함으로써 사용자 수를 제한할 수 있습니다. 이 때, 사용자는 단순히 네트워크 내에 있는 PC의 개수만 생각하고 접속자 수를 제한하면 안 되며, 네트워크 내에 있는 스위치 등의 장비들도 고려하여 설정해야 합니다. ISP 사업자의 경우, 이 설정을 이용하여 접속한 사용자 단위로 가격 책정을 진행할 수 있습니다.

Max-new-hosts는 1초 동안 시스템에 Learning될 수 있는 MAC의 갯수와 1초동안 포트에 Learning될 수 있는 MAC의 갯수를 설정하여 접속자 수를 제한하는 방법입니다. 이 두 가지 기준을 설정해 두면, 1초 동안 시스템에 Learning되는 MAC 갯수와 1초 동안 포트에 Learning되는 MAC 갯수를 각각 카운트 하다가 제한할 때에는 시스템에 Learning될 수 있는 MAC의 갯수가 우선적으로 적용됩니다.

Max-new-hosts를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
max-new-hosts port-number max-mac-number	Bridge	1초동안 포트에 Learning될 수 있는 MAC 개수를 설정합니다.
max-new-hosts system port-number max-mac-number		1초동안 시스템에 Learning될 수 있는 MAC 개수를 설정합니다.

설정한 Max-new-hosts를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no max-new-hosts port-number	Bridge	1초동안 포트에 Learning될 수 있는 MAC 개수를 삭제합니다.
no max-new-hosts system		1초동안 시스템에 Learning될 수 있는 MAC 개수를 삭제합니다.

설정한 Max-new-hosts를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show max-new-hosts	Enable/Global/Bridge	설정한 Max-new-hosts를 확인합니다.



주의

카운트되었던 MAC이 1초가 지나기 전에 사라졌다가 다시 Learning될 때에는 카운트 하지 않습니다.



주의

같은 MAC이 포트를 이동한 경우에는, 다시 카운트 하지 않습니다. 다시말해, 1/1번 포트에서 Learning된 MAC이 1/2번 포트에서 Learning되는 경우에는, 포트를 이동했다고 간주하여 1/1번 포트에서는 삭제하고 1/2번 포트에서 Learning하지만, 카운트는 하지 않습니다.

7.12 MAC 테이블 관리

MAC 테이블에는 dynamic 주소와 static 주소, 두 가지 형태의 주소가 등록됩니다. Dynamic 주소는 장비 자신이 테이블에 등록했다가 사용하지 않으면 삭제하는 주소이고 static 주소는 사용자가 설정 한 주소로 장비가 재부팅해도 테이블에 그대로 남아 있는 주소입니다. MAC 테이블에 static 주소를 입력하려면, Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
mac brdge-name port-number mac-address	Bridge	MAC 주소, Bridge 이름, 그리고 포트 번호를 입력한다.
show mac brdge-name port-number	Enable /Global/Bridge	사용자가 등록한 MAC 주소를 확인한다.

MAC 테이블에서 static 주소를 삭제하려면, Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no mac bridge-name port-number mac-address	Bridge	포트에 등록된 static MAC 주소를 삭제합니다.

MAC 테이블에 등록된 주소를 초기화하려면, Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear mac bridge-name port-number mac-address	Bridge	MAC 테이블을 초기화합니다.

7.13 ARP(Address Resolution Protocol)

IP 네트워크에 연결된 장비들은 LAN 주소와 네트워크 주소 두 가지를 지니고 있습니다. 일반적으로 LAN 주소는 Layer 2 계층에서 사용되기 때문에 data link 주소라고 하는데 이 보다는 MAC 주소로 널리 알려져 있습니다.

이더넷에 위치한 스위치가 패킷을 전송하려면 우선 48 비트로 된 MAC 주소를 알아야 합니다. 이 때 IP 주소와 일치하는 MAC 주소를 찾아내는 과정을 주소 산출(address resolution) 이라 하고 역으로 MAC 주소에서 IP 주소를 찾아내는 것을 역 주소 산출(reverse address resolution)이라고 합니다. 그리고, IP 주소와 일치하는 MAC 주소를 찾아낼 때 사용하는 프로토콜이 바로 ARP(Address Resolution Protocol)입니다.

ARP는 Request 패킷과 Reply 패킷으로 나뉘어집니다. Request 패킷은 동일한 이더넷 상에 있는 모든 노드들에게만 전송되고, Router에 의해서는 전송되지 않습니다. Reply 패킷은 Request 패킷의 대상이 되는 노드가 MAC 주소를 알려주는 것입니다.

IP 주소와 일치하는 MAC 주소를 찾을 때마다 ARP Request 패킷이 브로드캐스팅되는 것을 막고, 한번 찾아낸 정보를 다음에 빨리 찾아내기 위해 ARP를 통해 얻어진 정보는 ARP 테이블에 기록하여 관리합니다. 그러나, ARP 테이블을 효율적으로 관리하기 위해 테이블에 기록된 내용은 일정한 시간이 지나면 소멸됩니다.

여기에서는 V5812G의 ARP 설정 방법을 다음 순서로 설명합니다.

- ARP 테이블 설정
- ARP Alias
- ARP Inspection
- Proxy-ARP 설정
- Gratuitous ARP 설정

7.13.1. ARP 테이블 설정

V5812G는 ARP 테이블을 등록하고 설정 정보를 확인할 수 있습니다.

(1) ARP 테이블 등록

특정 IP 주소와 MAC 주소를 일치시키려면 Global 설정 모드에서 다음 명령어를 이용 하십시오.

명령어	모 드	기 능
arp ip-address mac-address [interface-name]	Global	IP 주소와 MAC 주소를 ARP 테이블에 등록합니다.

등록했던 IP 주소와 MAC 주소를 삭제하거나 ARP 테이블의 내용을 모두 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no arp ip-address [interface-name]	Global	IP 주소와 MAC 주소를 삭제합니다.
clear arp [interface-name]		ARP 테이블의 내용을 모두 삭제합니다.

(2) ARP 테이블 확인

장비에 등록되어 있는 ARP 테이블을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show arp [ip-address interface-name]	View/Enable/Global	ARP 테이블을 확인합니다.

다음은 IP 주소 10.1.1.1 을 MAC 주소 00:d0:cb:00:00:01 로 등록하는 경우입니다.

```
SWITCH(config)# arp 10.1.1.1 00:d0:cb:00:00:01
```

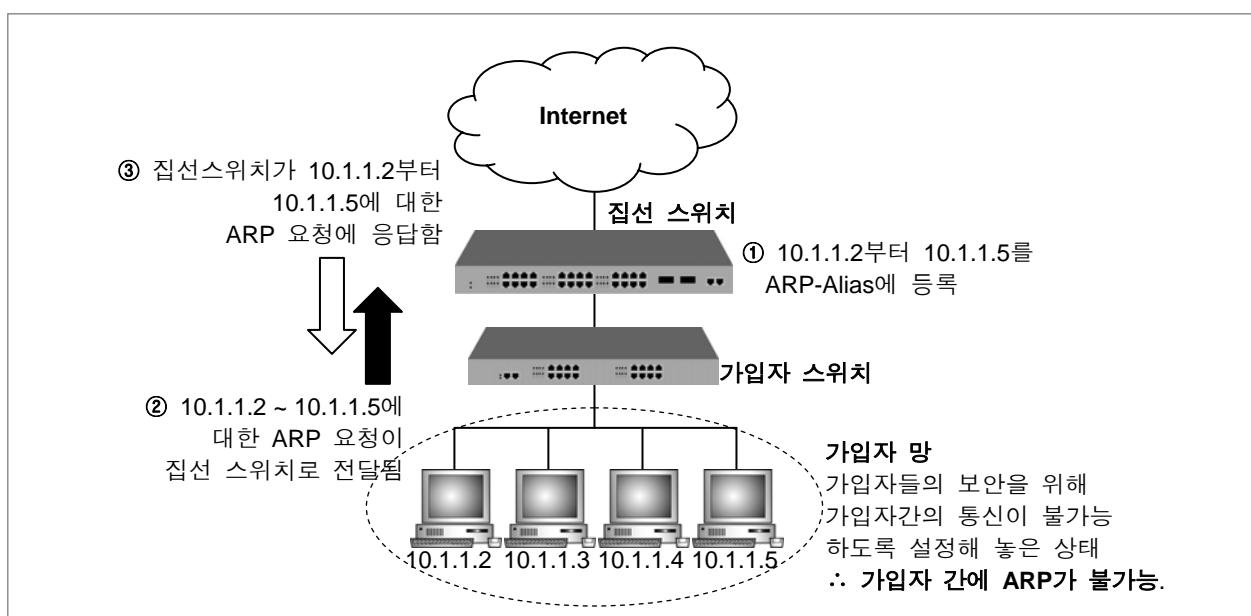
다음 명령어는 ARP 테이블을 출력합니다.

```
SWITCH(config)# show arp
Address      HWtype  HWaddress          Flags Mask   Iface  Port
10.1.1.1     ether    00:11:09:7b:da:19   C      mgmt   0/2
10.22.1.254   ether    00:d0:cb:0a:be:6b   C      mgmt   0/2
50.0.200.4    ether    00:d0:cb:00:00:01   CH     default 1/1
```

7.13.2. ARP Alias

V5812G는 장비에 등록된 IP 주소가 아니더라도 ARP 응답을 할 수 있습니다. 아래의 그림을 예로 들어보겠습니다.

아래의 그림은 가입자들의 보안 유지를 위해 가입자 간의 통신이 불가능하도록 설정된 상태의 가입자 망입니다. 그러나, 이러한 상태에서 집선 스위치에 ARP-Alias를 등록하게 되면, 가입자 간의 ARP 통신을 집선 스위치에서 대신하게 되어 마치 가입자들끼리 통신이 가능한 것처럼 보입니다.



【 그림 7-13 】 ARP-Alias의 원리

(1) ARP-Alias 설정

ARP-Alias를 등록하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
arp alias start-ip-address end-ip-address [mac-address]	Global	사용자의 장비가 ARP 응답을 하도록 IP 주소 범위 및 MAC 주소를 입력합니다.
arp alias start-ip-address end-ip-address vlan <1-4094> gateway gateway-ip-address		사용자의 장비가 ARP 응답하는데 사용할 VLAN 및 Gateway를 지정합니다.



참 고

MAC 주소를 입력하지 않으면 사용자 장비의 MAC 주소를 가지고 ARP 응답을 하게 됩니다.

등록한 ARP-Alias를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no arp alias start-ip-address end-ip-address	Global	사용자의 장비가 ARP 응답을 하도록 등록한 IP 주소 범위를 삭제합니다.

(2) Gateway Aging-time 설정

V5812G에서는 Gateway IP 주소와 관련된 ARP 테이블 기록 가운데 일정 시간 동안 사용되지 않는 것을 삭제하도록 설정할 수 있습니다.

ARP-Alias Aging-time을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
arp alias aging-time <5-2147483647>	Global	ARP-Alias Aging-time을 설정합니다.
no arp alias aging-time		설정한 ARP-Alias Aging-time을 삭제합니다.



참 고

장비의 기본값은 300초로 설정되어 있습니다.

(3) ARP-Alias 정보 확인

등록되어 있는 ARP-Alias를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show arp alias	View / Enable / Global	등록한 모든 ARP-Alias를 확인합니다.



참 고

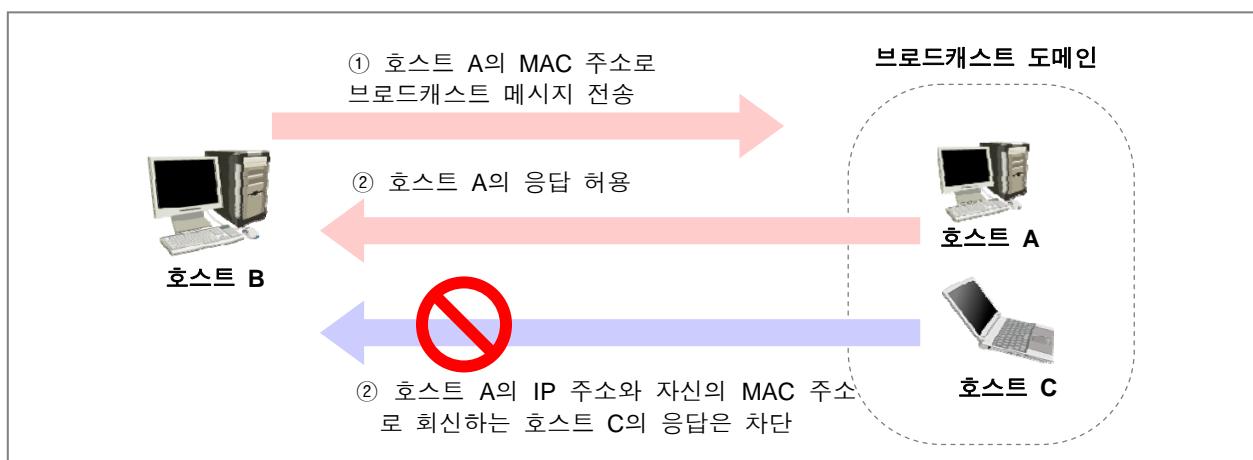
MAC 주소를 입력하지 않는다면, V5812G의 MAC 주소를 가지고 통신을 하게 됩니다.

7.13.3. ARP Inspection

ARP 패킷은 IP 주소를 통해 MAC 주소를 찾기 위한 것이기 때문에 네트워크의 모든 호스트를 신뢰하고 있다고 볼 수 있습니다. 이러한 점에서 보안성이 낮기 때문에 네트워크 통신을 방해하기 위한 목적으로 사용되기도 쉽습니다.

예를 들어, 호스트 B가 호스트 A의 IP 주소와 연결되는 MAC 주소를 가지고 브로드캐스트 도메인에 속해 있는 모든 호스트에게 브로드캐스트 메시지를 전송한 경우를 생각해봅시다. 만일 호스트 B의 브로드캐스트 메시지에 대해 호스트 C가 호스트 A의 IP 주소와 자신의 MAC 주소로 응답했다면, 호스트 B는 호스트 A에게 전달해야 하는 트래픽의 목적지로 호스트 C의 MAC 주소를 사용할 수 있습니다.

V5812G는 이러한 ARP 패킷에 대한 보안성을 높이기 위해서 ARP 패킷은 모두 CPU로 보내 검사하도록 하고, 네트워크 통신을 방해하기 위한 목적으로 전송된 ARP 패킷을 제거하도록 할 수 있습니다. 따라서 아래 그림과 같이 호스트 A가 아닌 호스트 C가 호스트 A의 IP 주소와 자신의 MAC 주소로 응답한 것을 차단할 수 있습니다.



【 그림 7-14 】 ARP Inspection의 동작 예

이러한 기능을 ARP Inspection 이라고 합니다. ARP Inspection 기능을 설정하려면, 이 기능을 활성화시키고 ARP 패킷에 대한 정책을 설정해야 합니다.



참 고

단순히 ARP Inspection을 활성화하는 것만으로는 제대로 동작하지 않습니다. ARP Access-list를 만들고, ARP Inspection 필터링을 설정해야 ARP 패킷을 차단하는 동작이 올바르게 실행됩니다.

(1) ARP Inspection 활성화

특정 VLAN에 ARP Inspection을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip arp inspection vlan <i>vlan-name</i>	Global	특정 VLAN에서 ARP Inspection을 활성화합니다.

특정 VLAN에 ARP Inspection을 활성화한 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip arp inspection vlan <i>vlan-name</i>	Global	특정 VLAN에 ARP Inspection을 활성화한 것을 해제합니다.



주 의

ARP Inspection 기능을 활성화한 것만으로는 ARP 패킷을 차단할 수 없습니다. 반드시 뒤에 나오는 ARP ACL 및 필터링 기능을 이용하여 ARP 패킷을 차단하도록 설정하십시오.



참 고

일반적으로 ARP Inspection은 Static ARP 테이블을 참조합니다. 그러나 DHCP Snooping이 동작하고 있다면 ARP Inspection은 DHCP Snooping 바인딩 테이블을 참조하여 해당 테이블에 등록되어 있는 IP 주소를 ARP 엔트리에 추가할 수 있습니다.

(2) ARP ACL 설정

ARP Inspection 기능을 이용하여 ARP 패킷을 차단하려면 먼저 ARP ACL(ARP Access List)를 생성하여야 합니다. ARP ACL 설정을 통해 특정 범위의 IP 주소를 차단하거나 고정 IP 사용자를 허용하는 등 ARP 패킷에 대한 정책을 설정합니다.

ARP ACL을 설정하려면, Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
arp access-list arp-acl-name	Global	ARP ACL을 설정합니다.
no arp access-list arp-acl-name		설정한 ARP ACL을 삭제합니다.
arp access-list delete all		모든 ARP ACL을 삭제합니다.



ARP ACL은 기본적으로 모든 IP 주소와 MAC 주소를 차단하도록 설정되어 있습니다.

ARP ACL을 생성하면 시스템 프롬프트가 SWITCH(config)#에서 SWITCH(config-arp-acl[arp-acl-name])#로 바뀌면서 ARP ACL 설정 모드로 들어갑니다. ARP ACL 설정 모드에서는 ARP Inspection 을 적용할 IP 주소의 범위를 설정할 수 있습니다.

특정 IP 주소 범위에 대하여 ARP 패킷을 차단하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
deny ip any mac { any host mac-address }	Arp-acl	모든 MAC 주소 또는 특정 호스트 MAC 주소에 대해 ARP 패킷을 차단합니다.
deny ip host ip-address mac { any host mac-address }		특정 호스트 IP 주소 또는 특정 호스트의 IP주소와 MAC 주소에 대해 ARP 패킷을 차단합니다.
deny ip A.B.C.D/M mac { any host mac-address }		특정 서브넷 IP 주소 또는 특정 서브넷 IP 주소와 특정 호스트 MAC 주소에 대해 ARP 패킷을 차단합니다.
deny ip range start-ip-address end-ip-address mac any		특정 범위에 포함되는 IP 주소에 대해 ARP 패킷을 차단합니다.



ARP ACL의 설정 후 반드시 필터링을 설정하여야 ARP ACL의 설정 내용이 적용됩니다.

특정 IP 주소 범위에 대하여 ARP 패킷을 허용하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
permit ip any mac { any host mac-address }	Arp-acl	모든 MAC 주소 또는 특정 호스트 MAC 주소에 대해 ARP 패킷을 허용합니다.
permit ip host ip-address mac { any host mac-address }		특정 호스트 IP 주소 또는 특정 호스트의 IP주소와 MAC 주소에 대해 ARP 패킷을 허용합니다.
permit ip A.B.C.D/M mac { any host mac-address }		특정 서브넷 IP 주소 또는 특정 서브넷 IP 주소와 특정 호스트 MAC 주소에 대해 ARP 패킷을 허용합니다.
permit ip range start-ip-address <i>end-ip-address mac any</i>		특정 범위에 포함되는 IP 주소에 대해 ARP 패킷을 허용합니다.



참 고

ARP ACL의 설정 후 반드시 필터링을 설정하여야 ARP ACL의 설정 내용이 적용됩니다.

특정 IP 주소 범위에 대하여 ARP 패킷을 차단 또는 허용하도록 설정한 것을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no deny ip any mac { any host mac-address }	Arp-acl	
no deny ip host ip-address		
mac { any host mac-address }		특정 범위의 IP 주소에 대하여 ARP 패킷을 차단하도록 설정한 것을 삭제합니다.
no deny ip A.B.C.D/M		
mac { any host mac-address }		
no deny ip range start-ip-address <i>end-ip-address mac any</i>		
no permit ip any mac { any host mac-address }	Arp-acl	
no permit ip host ip-address		
mac { any host mac-address }		특정 범위의 IP 주소에 대하여 ARP 패킷을 허용하도록 설정한 것을 삭제합니다.
no permit ip A.B.C.D/M		
mac { any host mac-address }		
no permit ip range start-ip-address <i>end-ip-address mac any</i>		

**주 의**

필터링을 적용한 ARP ACL을 삭제하면 해당 필터링까지 동시에 삭제됩니다.

한편, V5812G는 DHCP Snooping을 이용하여 고정 IP 사용자에 대한 제한설정을 할 수 있습니다. 이 기능을 설정하면 DHCP 사용자에 대해서는 ARP 패킷을 차단하지 않습니다. DHCP 사용자에 대해 ARP 패킷을 허용하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
permit dhcp-snoop-inspection	Arp-acl	DHCP 사용자에 대해 ARP 패킷을 허용하도록 설정합니다.
no permit dhcp-snoop-inspection		DHCP 사용자에 대해 ARP 패킷을 허용하도록 설정한 것을 해제합니다.

**참 고**

ARP ACL의 설정 후 반드시 필터링을 설정하여야 ARP ACL의 설정 내용이 적용됩니다.

한편, 특정 MAC 패턴에 따라 ARP 패킷을 차단하도록 설정하여 ARP Inspection 필터링을 강화할 수 있습니다. MAC 패턴 필터링은 ARP 패킷을 수신하면 Pattern(Length)과 Offset 정보를 참조하여 Sender MAC 주소와 비교한 후 사용자가 설정한 필터링 정책(Action)에 따라 패킷 처리를 실행합니다. 여기에서 Pattern은 필터링을 적용할 특정 MAC 주소의 패턴을 나타내며, Offset은 Sender MAC 주소와 비교할 Pattern의 위치를 뜻합니다.

**참 고**

설정 가능한 MAC 주소의 패턴은 다음과 같습니다.

* MAC Address Pattern(1~5byte)

- | | |
|----------------|------------|
| XX | (length 1) |
| XX:XX | (length 2) |
| XX:XX:XX | (length 3) |
| XX:XX:XX:XX | (length 4) |
| XX:XX:XX:XX:XX | (length 5) |

예를 들어, 사용자가 Length 3에 해당하는 Pattern XX:XX:XX 과 Offset 2를 만족하는 패킷을 차단하도록 설정했다고 합니다. ARP 패킷이 수신되면 V5812G는 Sender MAC 주소와 Pattern을 다음 과정처럼 비교하여 조건을 만족하면 해당 패킷을 차단합니다.

- Sender MAC XX:XX:**XX:XX:XX:XX**
- MAC Pattern **XX:XX:XX** ← Offset만큼 떨어진 위치에서 Length만큼을 비교

MAC Pattern 필터링을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
permit ip any	Arp-acl	모든 MAC 주소 또는 특정 호스트 MAC 주소에 대해 MAC Pattern에 일치하는 ARP 패킷을 허용합니다.
mac pattern mac-pattern offset <0-5>		
permit ip host ip-address		특정 호스트 IP 주소에 대해 MAC Pattern에 일치하는 ARP 패킷을 허용합니다.
mac pattern mac-pattern offset <0-5>		
permit ip A.B.C.D/M		특정 서브넷 IP 주소에 대해 MAC Pattern에 일치하는 ARP 패킷을 허용합니다.
mac pattern mac-pattern offset <0-5>		
deny ip any		모든 MAC 주소 또는 특정 호스트 MAC 주소에 대해 MAC Pattern에 일치하는 ARP 패킷을 차단합니다.
mac pattern mac-pattern offset <0-5>		
deny ip host ip-address		특정 호스트 IP 주소에 대해 MAC Pattern에 일치하는 ARP 패킷을 차단합니다.
mac pattern mac-pattern offset <0-5>		
deny ip A.B.C.D/M		특정 서브넷 IP 주소에 대해 MAC Pattern에 일치하는 ARP 패킷을 차단합니다.
mac pattern mac-pattern offset <0-5>		

설정한 MAC Pattern 필터링을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no permit ip {any host ip-address A.B.C.D/M} mac pattern mac-pattern offset <0-5>	Arp-acl	각각의 조건에 대해 MAC Pattern에 일치하는 ARP 패킷을 허용하도록 설정한 것을 해제합니다.
no deny ip {any host ip-address A.B.C.D/M} mac pattern mac-pattern offset <0-5>		각각의 조건에 대해 MAC Pattern에 일치하는 ARP 패킷을 차단하도록 설정한 것을 해제합니다.

(3) ARP Inspection 필터링 설정

V5812G는 ARP Inspection 기능을 활성화하면 기본적으로 모든 MAC 주소를 허용하도록 되어 있습니다. 따라서 허용 또는 차단할 IP 주소 범위를 ARP ACL로 지정한 후에 이를 적용하도록 설정하여 야만 ARP Inspection에 의한 ARP 패킷 차단 기능이 동작합니다.

ARP ACL에서 설정한 ARP 패킷 차단 기능이 동작하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip arp inspection filter <i>arp-acl-name vlan vlan-name</i>	Global	ARP 패킷 차단 기능이 동작하도록 설정합니다.
no ip arp inspection filter <i>arp-acl-name vlan vlan-name</i>		ARP 패킷 차단 기능이 동작하도록 설정한 것을 해제합니다.



참 고

V5812G는 ARP Inspection 기능을 설정하면 기본적으로 모든 MAC 주소를 허용하도록 되어 있습니다. 따라서 ARP 패킷을 차단하려면 위의 명령어를 이용하여 ARP ACL을 적용하십시오.



참 고

위의 명령어로 필터링을 적용한 ARP ACL이 삭제될 경우 필터링 설정도 동시에 삭제됩니다.

(4) 포트 상태 설정

ARP Inspection에서 포트의 상태는 Trusted 상태와 Untrusted 상태가 있습니다. Trust 포트로 수신된 ARP 패킷은 ARP Inspection을 거치지 않고 바로 통과하며, Untrust 포트로 수신된 ARP 패킷은 ARP Inspection에서 검사하여 적합할 경우에 통과합니다. 따라서, 일반적으로 가입자들과 연결된 포트는 Untrust 포트로 설정하고 상위 장비와 연결된 포트는 Trust 포트로 설정합니다.

ARP Inspection에서 포트의 상태를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip arp inspection trust port <i>port-number</i>	Global	해당 포트를 Trust 포트로 설정합니다.
no ip arp inspection trust port <i>port-number</i>		해당 포트를 Untrust 포트로 설정합니다.

ARP Inspection에서 포트 상태를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip arp inspection trust	Enable/	
show ip arp inspection trust port <i>port-number</i>	Global/ Bridge	ARP Inspection에서 포트 상태를 확인합니다.

(5) ARP Address-validation 검사 설정

ARP Address-validation 검사는 ARP 패킷의 IP 주소 및 MAC 주소의 유효성을 검사하여 다음과 같이 패킷을 처리하는 기능입니다.

- ARP 패킷 송신자의 MAC 주소와 이더넷 헤더의 Source MAC 주소가 일치하지 않을 경우 해당 ARP 패킷을 Drop 합니다.
- ARP Reply 패킷의 Target MAC 주소와 이더넷 헤더의 Destination MAC 주소가 일치하지 않을 경우 해당 ARP Reply 패킷을 Drop 합니다.
- ARP 패킷 송신자의 IP 주소 또는 ARP Reply 패킷의 Target IP 주소가 0.0.0.0 혹은 255.255.255.255이거나 멀티캐스트 IP 주소일 경우 해당 ARP 패킷을 Drop 합니다.

ARP Address-validation 검사를 실행하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip arp inspection validate {src-mac dst-mac ip}	Global	ARP Address-validation 검사를 설정합니다.
no ip arp inspection validate {src-mac dst-mac ip}		ARP Address-validation 검사를 해제합니다.



참 고

src-mac, dst-mac, ip 옵션은 중복 설정이 가능합니다.

(6) 불법 고정 IP 사용 가입자 리스트 확인

V5812G는 Log-buffer 기능을 이용하여 불법으로 고정 IP를 사용하는 가입자 리스트를 확인할 수 있습니다. Log-buffer는 ARP Inspection에 의해 차단되거나 유효하지 않은 가입자 정보를 저장하여 주기적으로 Syslog 메시지를 발생하는 기능입니다.

Log-buffer 기능은 ARP Inspection이 활성화되면 자동적으로 실행되며, 수신한 ARP 패킷이 ARP Inspection에 의한 Invalid 또는 Deny에 해당할 경우, Drop된 순서대로 가입자 정보 엔트리를 생성하여 저장합니다. Log-buffer에 저장되는 엔트리에는 포트 번호, VLAN ID, 패킷 발생지의 IP 주소 및 MAC 주소, 패킷 개수, Drop된 이유, 수신 시간 등의 정보가 포함됩니다. 또한, 사용자는 저장할 엔트리의 최대 개수를 지정할 수 있습니다.

이렇게 저장된 정보는 Log-buffer에 저장된 순서에 따라 주기적으로 Syslog 메시지로 출력된 후 Log-buffer에서 삭제됩니다. 만약, 사용자가 지정한 엔트리 최대 개수를 초과하는 ARP 패킷을 수신한 경우, 초과 패킷은 하나의 엔트리로 저장되며 이에 대한 Syslog 메시지는 Special Log Entry 형태로 가장 마지막에 출력됩니다. 한편, 이미 Log-buffer에 저장된 가입자로부터 동일한 ARP 패킷을 수신한 경우에는 패킷 개수와 최종 수신 시간만 바뀌고 저장된 엔트리의 순서는 변경되지 않습니다. 그리고, 사용자가 엔트리 개수를 현재 저장되어 있는 값보다 작은 값으로 변경할 경우 Log-buffer에 저장된 순서대로 삭제되고 Syslog 메시지는 출력되지 않습니다.

Log-buffer 기능에 필요한 옵션값을 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip arp inspection log-buffer { entries <0-1024> logs <0-1024> interval <0-86400> }	Global	Log-buffer 기능에 필요한 옵션값을 변경합니다.



참 고

entries는 Log-buffer에 저장할 수 있는 엔트리의 최대 개수를 나타냅니다. <0-1024> 범위에서 설정할 수 있으며 기본값은 32개입니다.



참 고

logs는 출력할 Syslog 메시지의 개수를 나타냅니다. <0-1024> 범위에서 설정할 수 있으며 기본값은 5개입니다. 0으로 설정하면 Log-buffer에 저장된 엔트리가 남아있는 경우에도 Syslog 메시지는 출력되지 않습니다.



참 고

interval은 Syslog 메시지를 출력할 시간 간격을 나타냅니다. <0-86400> 범위에서 설정할 수 있으며 기본값은 1초입니다. 0으로 설정하면 Log-buffer에 저장된 엔트리와 새로 수신되는 모든 엔트리가 즉시 Syslog 메시지로 출력됩니다.



참 고

Syslog 메시지 출력시간은 위에서 설정한 **interval**에서 **logs**를 나눈 값입니다. (**Syslog rate = interval / logs**) 단, 최초 Syslog 메시지 출력시간은 Syslog rate 이내에서 랜덤으로 결정됩니다.

사용자가 설정한 Log-buffer 기능의 옵션값을 해제하고 기본값으로 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip arp inspection log-buffer {entries logs}	Global	사용자가 설정한 Log-buffer 기능의 옵션값을 해제하고 기본값으로 변경합니다.

Log-buffer에 저장된 모든 엔트리를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip arp inspection log	Enable/Global/ Bridge	Log-buffer에 저장된 모든 엔트리를 삭제합니다.

Log-buffer의 설정내용과 저장된 엔트리 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip arp inspection log	Enable/Global/ Bridge	Log-buffer의 설정내용과 저장된 엔트리 정보를 확인합니다.

(7) 설정 내용 및 통계 확인

ARP Inspection의 설정 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip arp inspection	Enable/	ARP Inspection의 설정 내용을 확인합니다.
show ip arp inspection vlan <i>vlan-name</i>	Global/	
show ip arp inspection statistics	Bridge	ARP Inspection의 통계 내용을 확인합니다.
show ip arp inspection statistics vlan <i>vlan-name</i>		

ARP Inspection의 통계를 초기화하려면, 다음 명령어를 사용하십시오.

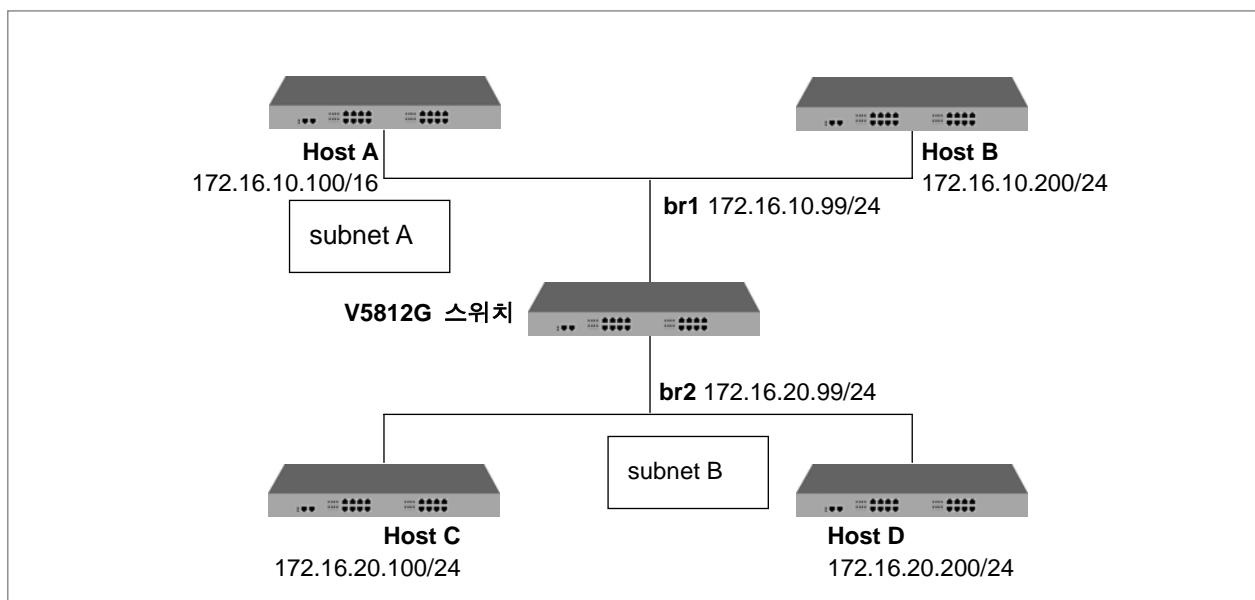
명령어	모 드	기 능
clear ip arp inspection statistics	Enable/	ARP Inspection의 통계를 초기화합니다.
clear ip arp inspection statistics vlan <i>vlan-name</i>	Global/Bridge	

7.13.4. Proxy-ARP 설정

V5812G는 Proxy-ARP 기능을 가지고 있습니다. Proxy-ARP는 간단히 말해서 다른 장비의 ARP 요청에 대한 응답을 대신 실시하는 것입니다. 아래 그림에서 Host A는 IP 주소가 172.16.10.100으로 설정되어 있고, subnet mask가 /16으로 설정되어 있습니다.

따라서, 자신이 172.16.0.0이라는 네트워크에 연결되어 있다고 생각합니다. 만일, Host A에서 Host D로 패킷을 보내야 한다면, Host A는 Host D가 같은 네트워크에 있을 것이라고 생각하고 ARP 요청을 합니다. ARP 요청은 브로드캐스트로 전송되기 때문에 Host A가 보낸 ARP 요청은 V5812G의 br1에 해당하는 인터페이스와 subnet A에 속해 있는 노드들에게만 전달되고, Host D에게는 전달되지 않습니다.

하지만, V5812G는 Host D가 다른 subnet에 속해 있음을 알고 있으며 Host D에 패킷을 전송할 수도 있습니다. 따라서, Host A로부터 ARP 요청에 대해 자신의 MAC 주소를 응답을 해 줍니다.



【 그림 7-15 】 Proxy-ARP

이러한 방법으로 subnet A로부터 들어오는 subnet B에 대한 ARP 요청은 모두 V5812G의 MAC 주소로 응답하게 되고, Host A로부터 Host D로 전송되어야 하는 패킷은 V5812G를 통해 무사히 전달하게 됩니다.

Proxy-ARP를 설정하려면 해당 Interface의 Interface 설정 모드로 들어가서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip proxy-arp	Interface	해당 Interface에 Proxy-ARP를 설정합니다.

설정했던 Proxy-ARP를 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip proxy-arp	Interface	해당 Interface에 설정한 Proxy-ARP를 해제합니다.

7.13.5. Gratuitous ARP 설정

V5812G는 게이트웨이의 IP 주소와 MAC 주소를 포함한 Gratuitous ARP를 브로드캐스팅되도록 하여, 네트워크의 특정 호스트에 게이트웨이의 IP 주소가 중복 할당되어 있는 경우에도 통신이 지속되도록 합니다.

다음 명령을 사용하여 Gratuitous ARP 전송 간격(*interval*)과 전송 횟수(*count*)를 설정하십시오. ARP Reply 후에 Gratuitous ARP 전송을 하려는 경우에는 전송 시작 시간(*delivery-start*) 또한 설정하십시오. ARP Reply가 전송된 후 지정된 시간이 경과하고 나서 Gratuitous ARP가 전송됩니다.

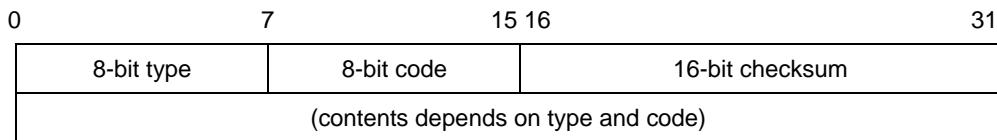
명령어	모 드	기 능
arp patrol interval count {delivery-start}	Global	Gratuitous ARP를 설정합니다.
no arp patrol		Gratuitous ARP를 해제합니다.
show running-config		Gratuitous ARP 설정 내용을 확인합니다.

7.14 ICMP 메시지 Control

ICMP(Internet Control Message Protocol)는 인터넷 제어 메시지 프로토콜입니다. ICMP는 데이터를 전달할 수 없는 경우가 발생하거나 데이터에 대한 경로 설정을 할 수 없을 때 호스트에게 에러 메시지를 통하여 알려주는 기능을 합니다.

ICMP 메시지의 처음 4byte는 모든 메시지가 동일한 형태로 이루어지지만, 나머지는 해당 메시지의 type 필드 값과 code 필드 값에 따라 달라집니다. type 필드는 각각 다른 ICMP 메시지를 나타내기 위해 15가지의 값으로 구별되고, code 필드의 값은 각 type을 더욱 자세하게 구분하게 해 주는 역할을 합니다.

다음은 ICMP 메시지의 형태를 간단히 나타낸 것입니다.



【 그림 7-16 】 ICMP 메시지

다음은 ICMP 메시지의 15가지 type 값을 설명한 표입니다.

【 표 7-2 】 ICMP 메시지의 15가지 Type

type	내 용	type	내 용
0	echo reply	12	parameter problem
3	destination unreachable	13	timestamp request
4	source quench	14	timestamp reply
5	redirect	15	information request
8	echo request	16	information reply
9	router advertisement	17	address mask request
10	router solicitation	18	address mask reply
11	time exceeded		

V5812G는 ICMP 메시지를 설정에 따라 조절할 수 있는 기능을 가지고 있습니다. 사용자의 장비에 Ping 테스트를 실시하는 상대에게 echo reply 메시지를 보내지 않을 수도 있고, ICMP 메시지 전송 시간 간격을 지정할 수 있습니다.

다음은 V5812G에서 가능한 ICMP 메시지 조절 기능입니다.

- Echo reply 메시지 제한
- ICMP 메시지 전송 시간 제한

7.14.1. Echo Reply 메시지 제한

V5812G는 사용자의 장비에 Ping 테스트를 실시하는 상대에게 Echo Reply 메시지를 보내지 않도록 제한할 수 있습니다.

Echo Reply 메시지를 제한하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip icmp ignore echo all	Global	사용자의 장비에 Ping 테스트를 실시하는 모든 상대에게 echo reply 메시지를 보내지 않도록 합니다.
ip icmp ignore echo broadcast		사용자의 장비에 Broadcast ping 테스트를 실시하는 상대에게 echo reply 메시지를 보내지 않도록 합니다.

echo reply 메시지를 제한하는 것을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip icmp ignore echo all	Global	사용자의 장비에 Ping 테스트를 실시하는 모든 상대에게 echo reply 메시지를 보내지 않도록 설정한 것을 해제합니다.
no ip icmp ignore echo broadcast		사용자의 장비에 Broadcast ping 테스트를 실시하는 상대에게 echo reply 메시지를 보내지 않도록 설정한 것을 해제합니다.

7.14.2. ICMP 메시지 전송 시간 제한

V5812G는 사용자가 지정한 ICMP 메시지의 전송 시간을 제한할 수 있습니다. 전송 시간을 제한하게 되면, 마지막으로 ICMP 메시지를 보낸 시간을 기준으로 제한된 시간이 지나기 전까지는 ICMP 메시지를 내보내지 않습니다.

예를 들어, 전송 시간을 1초로 제한하면, 마지막으로 ICMP 메시지를 보낸 후 1초 이내에는 응답을 하지 않게 됩니다. ICMP 메시지의 전송 시간을 제한하기 위해 V5812G 관리자는 전송 시간을 제한할 메시지 종류와 제한 전송 시간을 설정해야 합니다.

(1) ARP Inspection 활성화

일단, ICMP 메시지 가운데 전송 시간을 제한할 메시지를 선택하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip icmp interval rate-mask mask	Global	ICMP 메시지 중에서 전송 시간을 제한할 메시지를 설정합니다.



ip icmp interval rate-mask mask 명령어에서 *mask*는 16진수로 입력됩니다.

각 ICMP 메시지는 아래 표와 같은 값을 가지고 있습니다.

【 표 7-3 】 ICMP 메시지의 값

TYPE	VALUE	TYPE	VALUE
ICMP_ECHOREPLY	0	ICMP_DEST_UNREACH	3
ICMP_SOURCE_QUENCH	4	ICMP_REDIRECT	5
ICMP_ECHO	8	ICMP_TIME_EXCEEDED	11
ICMP_PARAMETERPROB	12	ICMP_TIMESTAMP	13
ICMP_TIMESTAMPREPLY	14	ICMP_INFO_REQUEST	15
ICMP_INFO_REPLY	16	ICMP_ADDRESS	17
ICMP_ADDRESSREPLY	18		

Mask의 풀이 방법은 다음과 같습니다. 사용자가 입력한 16진수의 mask를 2진수로 풀었을 때, “1”은 “Status ON”, “0”은 “Status OFF”를 나타냅니다. 2진수에서 “1”로 나타내지는 자리수가 ICMP 메시지의 값과 일치하면, 해당 ICMP 메시지는 “Status ON”으로 전송 시간을 제한하는 메시지로 선택된 것입니다. 자리수는 0부터 시작됩니다.



2진수에서 자리수를 계산할 때에는 0부터 시작됩니다.

위에서 설명한 것으로 예를 들어, 16진수 “8”을 2진수로 바꾸면 “1000”이 됩니다. “1000”은 0자리수가 “0”, 1자리수가 “0”, 2자리수도 “0”, 3자리수는 “1”입니다. “1”로 나타내어지는 자리수는 “3”이고, ICMP 메시지 값이 “3”인 것은 ICMP_DEST_UNREACH입니다. 그러면, ICMP_DEST_UNREACH 메시지는 전송 시간을 제한하는 메시지로 선택된 것입니다.

참 고

*mask*는 기본적으로 0x1818으로 설정되어 있습니다.

참 고

*mask*는 0xFFFFFFFF까지 입력 가능합니다.

Default 값은 0x1818입니다. 16진수 1818은 2진수로 바꾸면 1100000011000입니다. 0자리수부터 계산하면, 3자리, 4자리, 11자리, 12자리가 “1”로 “STATUS ON”입니다. 따라서 ICMP 메시지 값이 3,4,11,12에 해당하는 메시지가 전송 속도 제한 메시지로 선택되는 것입니다.

다음은 Default 값의 mask 계산 결과를 표로 나타낸 것입니다.

【 표 7-4 】 Default mask 계산 결과표

TYPE	STATUS
ICMP_ECHOREPLY(0)	OFF
ICMP_DEST_UNREACH(3)	ON
ICMP_SOURCE_QUENCH(4)	ON
ICMP_REDIRECT(5)	OFF
ICMP_ECHO(8)	OFF
ICMP_TIME_EXCEEDED(11)	ON
ICMP_PARAMETERPROB(12)	ON
ICMP_TIMESTAMP(13)	OFF
ICMP_TIMESTAMPREPLY(14)	OFF
ICMP_INFO_REQUEST(15)	OFF
ICMP_INFO_REPLY(16)	OFF
ICMP_ADDRESS(17)	OFF
ICMP_ADDRESSREPLY(18)	OFF

(2) 전송 제한 시간 설정

사용자가 선택한 ICMP 메시지의 전송 시간을 얼마나 제한할 것인지를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip icmp interval rate-limit <i>interval</i>	Global	ICMP 메시지 가운데 선택된 메시지의 전송 시간을 얼마나 제한할 것인지를 설정합니다.



“*interval*”의 단위는 10ms(1/100s)입니다.



V5812G는 기본적으로 전송 시간을 20ms로 제한하고 있습니다.



“*interval*”에 “0”을 입력하면 시간 제한을 두지 않고 항상 메시지를 내보내는 것입니다.

(3) 전송 제한 설정 확인

사용자가 선택한 ICMP 메시지의 전송 시간을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip icmp interval	View/Enable/Global	ICMP 메시지 가운데 선택된 메시지의 전송 시간 확인합니다.

(4) 전송 제한 설정 초기화

전송을 제한한 ICMP 메시지와 해당 메시지의 전송 시간을 초기화하시려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip icmp interval default	Global	ICMP 메시지 전송 제한을 초기화합니다.

[설정 예제 1]

다음은 ICMP_ECHO, ICMP_INFO_REQUEST, ICMP_INFO_REPLY에 대한 메시지의 전송 속도를 제한하도록 설정하는 경우의 예입니다.

ICMP_ECHO는 8, ICMP_INFO_REQUEST는 15, ICMP_INFO_REPLY는 16이기 때문에 8자리, 15자리, 16자리가 “1”인 2진수를 16진수로 바꿔서 mask를 입력해야합니다. 다시 숫자로 나타내면 2진수 110000001000000000이기 때문에 16진수로 나타내면 18100입니다.

```
SWITCH(config)# ip icmp interval rate-mask 0x18100
SWITCH(config)# show ip icmp interval
-----
RATE-LIMIT : 20 (default:20)
-----
RATE-MASK  : 0x1818 (default:0x1818)
-----
TYPE          | STATUS
-----
ICMP_ECHOREPLY(0)   | OFF
ICMP_DEST_UNREACH(3) | ON
ICMP_SOURCE_QUENCH(4) | ON
ICMP_REDIRECT(5)    | OFF
ICMP_ECHO(8)        | OFF
ICMP_TIME_EXCEEDED(11) | ON
ICMP_PARAMETERPROB(12) | ON
ICMP_TIMESTAMP(13)   | OFF
ICMP_TIMESTAMPREPLY(14) | OFF
ICMP_INFO_REQUEST(15) | OFF
ICMP_INFO_REPLY(16)   | OFF
ICMP_ADDRESS(17)     | OFF
ICMP_ADDRESSREPLY(18) | OFF
-----
SWITCH(config)#

```

7.15 IP TCP flag control

TCP(Transmission Control Protocol)의 TCP header에는 URG, ACK, PSH, RST, SYN, FIN의 6가지 flag를 포함하고 있습니다. V5812G는 이 가운데 RST와 SYN에 대해 다음과 같은 설정을 할 수 있습니다.

- RST 설정
- SYN attack 방지 기능 설정

7.15.1. RST 설정

RST는 TCP connection을 시도하는 상대에게 접속이 불가능함을 응답해 주는 기능을 가지고 있습니다. 그러나, V5812G의 사용자는 RST가 TCP connection을 시도하는 상대에게 접속이 불가능한 상황을 알리지 않도록 설정할 수 있습니다. 이러한 기능은 해커들이 접속 대상을 찾을 때 접속이 불가능함을 알려주지 않아 해킹이 어려워질 수 있도록 도와줄 수 있습니다.

다음 명령어를 사용하면 TCP connection을 시도하는 상대에게 접속이 불가능함을 응답하지 않습니다.

명령어	모 드	기 능
ip tcp ignore rst-unknown	Global	TCP connection을 시도하는 상대에게 접속이 불가능함을 응답하지 않습니다.



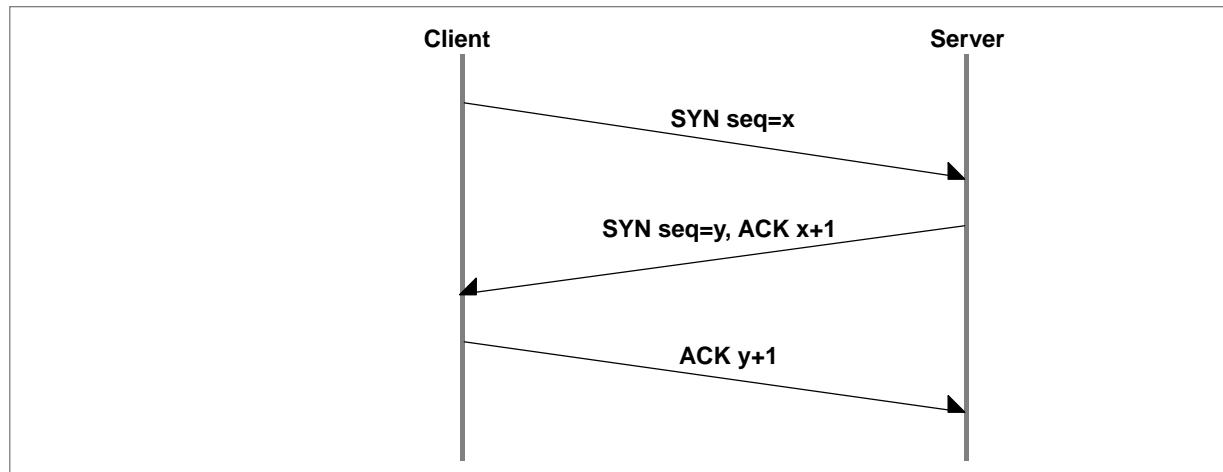
V5812G는 기본적으로 TCP connection을 시도하는 상대에게 접속이 불가능함을 응답하도록 설정되어 있습니다.

TCP connection을 시도하는 상대에게 접속이 불가능함을 다시 알리도록 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip tcp ignore rst-unknown	Global	TCP connection을 시도하는 상대에게 접속이 불가능함을 응답하도록 설정합니다.

7.15.2. SYN attack 방지 기능 설정

TCP에서 Client와 Server의 connection은 다음과 같이 세 방향(3 Way Hand Shaking)으로 이루어집니다.



【 그림 7-17 】 3 Way Hand Shaking

일단, Client는 connection을 시도하기 위해 1bit의 SYN 비트를 설정하고, sequence number=x와 함께 보냅니다. 그러면, Server는 Hand Shaking이 계속 이루어지고 있다는 것 뿐만 아니라 SYN에 대한 응답을 SYN와 ACK 비트 집합으로 보냅니다. 이 때 ACK 비트에는 Client가 보낸 sequence number에 1을 더해 “x+1”의 sequence number가 포함되고, SYN에는 새로운 sequence number=y가 포함됩니다. 마지막으로 Client는 Server에게 보내는 응답으로 ACK 비트와 “y+1”의 sequence number를 보내면서 서로 연결이 이루어졌음을 알립니다.

3 Way Hand Shaking에서 connection을 맺기 위해 전송된 SYN은 Server의 Incomplete connection queue에 entry로 추가되고, TCP connection이 완료되면 이 connection은 Completed connection queue에 추가됩니다.

그리고, 이러한 queue들의 합은 일정한 값을 넘을 수 없습니다. 이 때, 어떤 Client가 무작위로 선출된 Source IP를 가진 SYN를 전송하면 Server는 SYN을 Incomplete connection queue에 추가하고, SYN에 대한 응답을 보냅니다.

그러나, Server에 대한 응답은 오지 않고, Incomplete connection queue만 쌓아가게 되고 결국에는 queue가 생성될 수 있는 한계 값에 이르게 됩니다. 이러한 상태가 되면 정상적으로 패킷을 처리할 수 없고, 통신이 불가능하게 됩니다. V5812G는 이러한 SYN flooding을 막기 위해 sequence number 대신에 cookies를 SYN과 함께 전송하고, 전송했던 cookies에 대한 응답이 되돌아오는 경우에만 연결을 승인하도록 하는 기능을 가지고 있습니다.

SYN에 cookies를 함께 전송하여 cookies가 되돌아왔을 때만 접속을 승인하도록 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip tcp syncookies	Global	SYN에 cookies를 함께 전송하여 cookies가 되돌아왔을 때만 접속을 승인하도록 설정합니다.

SYN에 cookies를 함께 전송하여 cookies가 되돌아왔을 때만 접속을 승인하도록 설정한 것을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip tcp syncookies	Global	SYN에 cookies를 함께 전송하여 cookies가 되돌아왔을 때만 접속을 승인하도록 설정한 것을 해제합니다.

7.15.3. SYN Guard 대역폭 설정

많은 양의 SYN 패킷으로 인한 공격으로부터 서버를 보호하려면 불필요한 트래픽이 해당 스위치의 CPU로 유입되는 것을 방지하기 위해, 특정 대역폭을 지정해 줄 수 있습니다.

SYN 패킷에 대한 대역폭을 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip tcp syn-guard bandwidth	Global	SYN 패킷이 CPU로 유입되는 수신 대역폭을 지정합니다.



참 고

대역폭의 단위는 Kbps입니다. 대역폭은 최소 64Kbps 이상으로 입력하십시오. 또한, 64단위로, 즉 64의 배수로 입력할 수 있습니다..

지정된 SYN 패킷에 대한 대역폭을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip tcp syn-guard	Global	지정된 SYN 패킷에 대한 대역폭을 삭제합니다.

7.16 패킷 라우팅 테이블 사용량 확인

호스트 기준의 패킷 라우팅 과정은 L3 테이블이라고 하는 메모리를 사용합니다. L3 테이블에서 destination 주소의 정보를 검색하여 Nexthop에 대한 정보를 얻고 이를 기준으로 Rewriting 과정을 거쳐 패킷을 전송합니다. 만약 L3 테이블에 destination 주소에 대한 정보를 찾지 못하면 CPU의 라우팅 테이블을 참조하여 Nexthop에 대한 정보를 얻어서 L3에 적어주고 Rewriting 과정을 거치고 패킷을 전송합니다.

네트워크 기준의 패킷 라우팅은 각각의 패킷 단위로 검색, 기록하는 과정의 비효율성을 보완하여 네트워크 단위로 이를 처리하는 방식입니다. V5812G는 이를 위해 LPT 테이블이라고 하는 메모리를 사용합니다.

패킷 라우팅에서 사용되는 L3 테이블, LPM 테이블 혹은 인터페이스의 사용량을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip tables summary	Enable	L3 테이블 또는 LPM 테이블 혹은 인터페이스의 사용량을 보여줍니다.

7.17 덤프 패킷 모니터링

V5812G은 덤프 패킷 모니터링 기능을 통해 그때그때 네트워크에서 일어나는 모든 트래픽 동향을 분석함으로써 바이러스 피해나 네트워크 이상 징후 등에 대해서 파악할 수 있습니다. 예를 들면, 네트워크에서 평상시 보이지 않던 UDP 혹은 TCP 포트의 비정상적 증가 등을 통해 새로운 바이러스의 움직임을 한눈에 알 수 있습니다.

- 덤프 패킷(Dump Packet) 확인
- 덤프 패킷 디버그

7.17.1. 덤프 패킷(Dump Packet) 확인

V5812G에서는 TCP 덤프를 사용하여 원하는 패킷 정보를 확인할 수 있습니다.

(1) 프로토콜별 덤프 패킷 확인

BOOTPS, DHCP, ARP, ICMP와 관련된 덤프 패킷을 확인하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
debug packet {interface interface-name port port-number} protocol {bootps dhcp arp icmp}		
debug packet {interface interface-name port port-number} protocol {bootps dhcp arp icmp} src-ip src-ip-address	Enable	프로토콜별 덤프 패킷을 확인합니다.
debug packet {interface interface-name port port-number} protocol {bootps dhcp arp icmp} src-ip src-ip-address dest-ip dest-ip-address		

(2) 호스트 덤프 패킷 확인

호스트 덤프 패킷을 확인하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
debug packet {interface interface-name port port-number}		
host		
debug packet {interface interface-name port port-number}		
host src-ip src-ip-address		
debug packet {interface interface-name port port-number}		
host src-ip src-ip-address dest-ip dest-ip-address	Enable	호스트 덤프 패킷을 확인합니다.
debug packet {interface interface-name port port-number}		
host src-ip src-ip-address dest-ip dest-ip-address		
src-port src-port-number		
debug packet {interface interface-name port port-number}		
host src-ip src-ip-address dest-ip dest-ip-address		
src-port src-port-number dest-port dest-port-number		



참 고

*src-port-number*와 *dest-port-number*는 <1 – 65,535> 사이에서 설정 가능합니다.

(3) 멀티캐스트 덤프 패킷 확인

멀티캐스트 덤프 패킷을 확인하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
debug packet {interface interface-name port port-number}		
multicast		
debug packet {interface interface-name port port-number}		
multicast src-ip src-ip-address	Enable	멀티캐스트 덤프 패킷을 확인합니다.
debug packet {interface interface-name port port-number}		
multicast src-ip src-ip-address dest-ip dest-ip-address		

(4) 사용자 지정 덤프 패킷 확인

V5812G에서는 사용자가 다음 명령어로 덤프 패킷 출력 형식을 *option*으로 지정하여 결과를 확인할 수 있습니다.

*option*은 TCP 덤프에서 사용하는 것을 모두 사용할 수 있으며 그 내용은 【 표 7-4 】와 같습니다.

명령어	모 드	기 능
debug packet option	Enable	주어진 조건에 해당하는 패킷을 확인합니다.

【 표 7-5 】 TCP 덤프 옵션

Option	내 용
-a	Network & Broadcast 주소들을 이름들로 바꿉니다.
-d	compile된 packet-matching code를 사람이 읽을 수 있도록 바꾸어 표준 출력으로 출력하고, 종료합니다.
-e	출력되는 각각의 행에 대해서 link-level 헤더를 출력합니다.
-f	외부의 internet address를 가급적 심볼로 출력합니다.
-l	표준 출력으로 나가는 데이터들을 line buffering합니다. 다른 프로그램에서 tcpdump로부터 데이터를 받고자 할 때 유용합니다.
-n	모든 주소들을 번역하지 않습니다.(port,host address 등등)
-N	호스트 이름을 출력할 때, 도메인을 찍지 않습니다.
-O	packet-matching code optimizer를 실행하지 않습니다. 이 옵션은 optimizer에 있는 버그를 찾을 때나 쓰입니다.
-p	인터페이스를 promiscuous mode로 두지 않습니다.
-q	프로토콜에 대한 정보를 덜 출력합니다. 따라서 출력되는 라인이 좀 더 짧아집니다.
-S	TCP sequence 번호를 상대적인 번호가 아닌 절대적인 번호로 출력합니다.
-t	출력되는 각각의 라인에 시간을 출력하지 않습니다.
-v	좀 더 많은 정보들을 출력합니다.
-w	캡처한 패킷들을 분석해서 출력하는 대신에 그대로 파일에 저장합니다.
-x	각각의 패킷을 핸스(hex)코드로 출력합니다.
-c number	제시된 수의 패킷을 받은 후 종료합니다.
-F file	filter 표현의 입력으로 파일을 받아들입니다. 커맨드라인에 주어진 추가의 표현들은 모두 무시됩니다.

Option	내 용
-i interface	어느 인터페이스를 경유하는 패킷들을 잡을지 지정합니다. 지정되지 않으면 시스템의 인터페이스 리스트를 뒤져서 가장 낮은 번호를 가진 인터페이스를 선택합니다.(이 때 loopback은 제외됩니다).
-r file	패킷들을 '-w'옵션으로 만들어진 파일로 부터 읽어 들인다. 파일에 "-" 가 사용되면 표준 입력을 통해서 받아들입니다.
-s snaplen	패킷들로부터 추출하는 샘플을 default값인 68Byte외의 값으로 설정할 때 사용합니다. 68Byte는 IP, ICMP, TCP, UDP등에 적절한 값이지만 Name Server나 NFS 패킷들의 경우에는 프로토콜의 정보들을 Truncation할 우려가 있습니다. 샘플 사이즈를 크게 잡으면 곧 패킷 하나하나를 처리하는데 시간이 더 걸릴 뿐만아니라 패킷 버퍼의 사이즈도 자연히 작아지게 되어 손실되는 패킷들이 발생할 수 있기 때문에 이 옵션을 수정할 때에는 신중해야 합니다. 또, 작게 잡으면 그만큼의 정보를 잃게되는 것이므로 가급적 캡처하고자 하는 프로토콜의 헤더 사이즈에 가깝게 잡아주어야 합니다.
-T type	조건식에 의해 선택된 패킷들을 명시된 형식으로 표시한다. type에는 다음과 같은 것들이 올 수 있다. rpc(Remote Procedure Call), rtp(Real-Time Applications protocol), rtcp(Real-Time Application control protocol), vat(Visual Audio Tool), wb(distributed White Board)
Express	조건식입니다.

7.17.2. 덤프 패킷 디버그

V5812G에서는 다양한 이상 패킷 유입으로 인한 시스템 과부하를 방지하기 위해 네트워크 디버깅 기능을 제공합니다. 이 기능은 모니터링 프로세스가 5초마다 CPU의 과부하 상태를 측정하여 사용자가 설정한 임계 이상의 트래픽이 발생하면, Tcpdump를 이용하여 패킷을 캡처하고, 캡처된 상황을 파일로 저장합니다.

이름이 **file-number.dump**로 저장된 덤프 파일은 사용자 장비로 FTP 접속하여 파일 다운로드 후 확인 가능합니다. FTP 프로그램으로 다운로드한 덤프 파일을 패킷 분석 프로그램을 통해 내용을 확인하십시오.

Dump 패킷을 디버깅하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
debug packets log <i>packet-counting cpu-threshold time [file-number]</i>	Enable	조건에 해당되는 덤프 패킷들을 디버깅합니다.
no debug log		디버깅 설정을 해제합니다.

 참 고

*file-number*의 기본 설정은 1로, <1 – 10> 사이에서 설정 가능합니다.

 주 의

*file-number*에 설정된 수보다 더 많은 덤프 파일이 생성되는 경우에는, 낮은 번호의 파일에서부터 덮어 쓰기 됩니다.

 주 의

write memory 명령어로 현재 설정 내용을 저장하는 경우에도, 덤프 파일은 저장되지 않습니다.

한편, 이미 생성된 덤프 파일을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
delete dumpfile {dumpfile-name}	Enable	덤프 파일을 삭제합니다.

7.18 Port Security

V5812G는 MAC 주소를 변조하거나 패킷 Flooding을 막기 위해 Port Security 기능을 구현하고 있습니다. 특정 포트에 Learning 될 수 있는 MAC 주소의 개수를 지정하고, 지정된 개수가 넘었을 때에는 사용자가 설정한 대로 포트가 관리되게 됩니다.

여기에서는 Port Security에 대해 다음과 같이 설명합니다.

- Port Security 활성화
- MAC 주소 개수 지정
- Port Security Aging Time 지정
- Port Security Aging Type 지정
- Port Security Aging Static 지정
- Violation Action 지정
- Secure MAC 주소 등록
- Port Security 기능 설정 확인

7.18.1. Port Security 활성화

Port Security를 활성화하거나 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port security port-number	Bridge	Port Security를 활성화합니다.
no port security port-number		Port Security를 해제합니다.

Port Security를 활성화하면, 해당 포트와 연결된 모든 MAC 주소를 삭제되면서 해당 기능이 동작하기 시작합니다.



Port Security 기능은 기본적으로 활성화되어 있지 않습니다.

7.18.2. MAC 주소 개수 지정

특정 포트에 최대로 Learning 될 수 있는 MAC 주소 개수를 설정해야 합니다. 최대로 Learning 되는 MAC 주소 개수를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port security port-number maximum <1-16384>	Bridge	특정 포트에 최대로 Learning 될 수 있는 MAC 주소 개수를 설정합니다.
no port security port-number maximum		최대로 Learning 될 수 있는 MAC 주소 개수를 초기값으로 되돌립니다.

최대 MAC 주소의 개수를 변경하면 해당 포트의 MAC 주소들을 모두 삭제되고 등록된 MAC 주소들도 전부 삭제됩니다.



참 고

Learning 될 수 있는 MAC 주소는 기본적으로 1개로 설정되어 있습니다.

7.18.3. Port Security Aging Time 지정

Aging time을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port security port-number aging time <1-1440>	Bridge	Aging time을 설정합니다.
no port security port-number aging time		Aging time 을 삭제합니다.

Aging time은 포트로 MAC 주소가 처음 들어올 때 시작되고, MAC 주소에 대하여 Aging time이 만료되면 포트상에서 그 MAC 주소에 대한 entry가 삭제됩니다. Aging time을 삭제하는 경우 등록된 secure MAC에 대한 Aging-out 처리를 진행하지 않습니다.

7.18.4. Port Security Aging Type 지정

Aging-out 형식을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port security port-number aging type {absolute inactivity}	Bridge	Aging-out 형식을 결정합니다.
no port security port-number aging type		Aging-out 형식을 초기화합니다.



Aging-out 형식은 기본적으로 absolute로 설정되어 있습니다.

Absolute는 설정된 aging time이 만료되면 secure MAC을 삭제합니다. Inactivity는 해당 secure MAC을 가진 패킷이 들어오지 않은때부터 aging time이 경과하면 해당 MAC을 삭제합니다.

7.18.5. Port Security Aging Static 지정

Static으로 등록된 MAC 주소에 Aging-out을 적용시키려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port security port-number aging static	Enable	Static으로 등록된 secure MAC들의 Aging-out이 가능하게 합니다.
no security port-number aging static		Static으로 등록된 secure MAC들의 Aging-out이 진행되지 않게 합니다.



Static으로 등록된 secure MAC들의 Aging-out은 기본적으로 진행되지 않게 설정되어 있습니다

7.18.6. Violation Action 지정

Security violation이 발생하였을때의 동작을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port security port-number violation {shutdown protect restrict}	Bridge	Security violation이 발생하였을때의 동작을 설정합니다.
no port security port-number violation		Security violation이 발생하였을때의 동작을 초기화합니다.

■ **shutdown** – 포트를 disable 상태로 합니다. Port enable 명령으로 다시 enable 시킬수 있습니다. Syslog 메시지가 표시됩니다.

■ **restrict** – 들어오는 패킷을 모두 drop 시키지만 포트는 enable 상태로 합니다. Syslog 메시지가 표시됩니다.

■ **protect** – 들어오는 패킷을 모두 drop 시키지만 포트는 enable 상태로 합니다. Syslog 메시지가 표시되지 않습니다.

7.18.7. Secure MAC 주소 등록

해당 포트에 secure MAC 주소를 static으로 등록하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port security port-number mac-address mac-address [vlan vlan-name]	Bridge	해당 포트에 secure MAC 주소를 static으로 등록합니다.
clear port security port-number mac-address [mac-address]	Bridge	해당 포트에 dynamic 으로 등록된 secure MAC 주소를 삭제합니다.
clear port security port-number mac-address mac-address [vlan vlan-name]		

Mac 주소를 지정하지 않는 경우는 전체 MAC을 삭제하고, vlan 지정을 하지 않는 경우에는 전체 vlan에 대해서 적용합니다.

7.18.8. Port Security 기능 설정 확인

Port Security 관련 설정을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show port security [port-number]	Bridge	Port 별 security 설정 상태를 보여줍니다.

8. 시스템 주요 기능 설정

시스템 주요 기능 설정에서는 VLAN, 포트 트렁킹, STP 등 V5812G가 가지고 있는 주요 기능에 대해 설명합니다. 이 장은 다음과 같은 내용으로 이루어집니다.

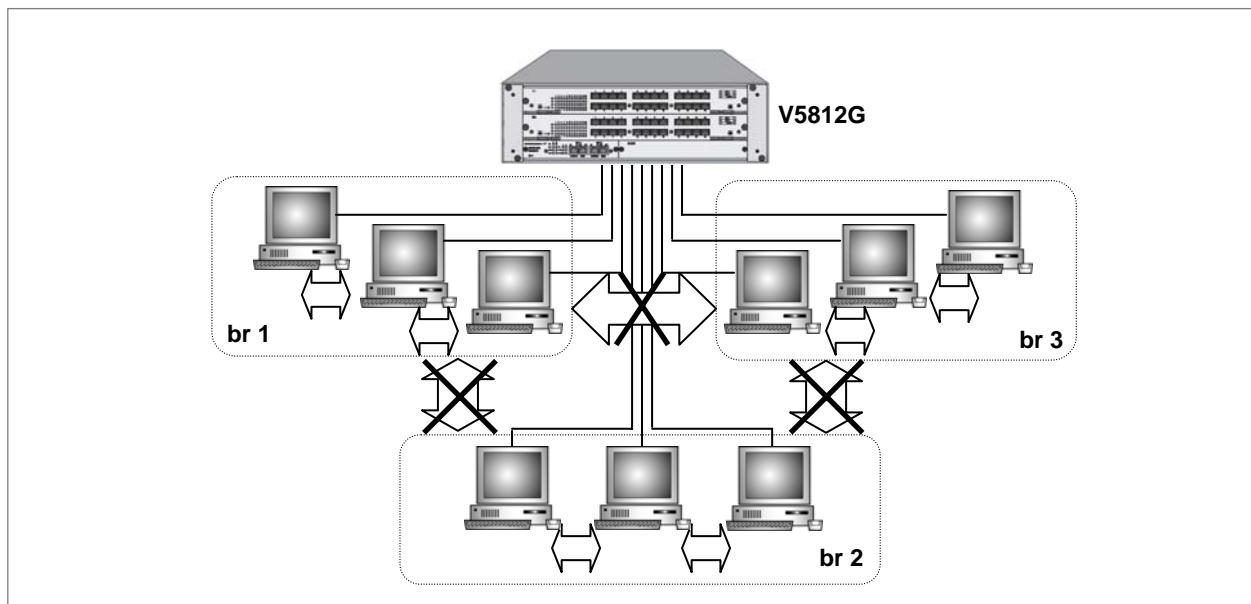
- VLAN(Virtual Local Area Network)
- Link aggregation
- STP 설정
- Loop 감지 기능 설정
- ERP 설정
- 스택킹 설정
- Rate Limit
- Flood Guard
- VRRP (Virtual Router Redundancy Protocol)
- 대역폭 설정
- DHCP(Dynamic Host Configuration Protocol)
- 브로드캐스트 Storm Control
- Jumbo Frame 수용하기
- Direct 브로드캐스트 차단

8.1 VLAN(Virtual Local Area Network)

동일한 LAN에 속해 있는 노드들은 하나의 노드에서 Broadcast를 이용하여 정보를 보내면 모두 이 정보를 받아 볼 수 있습니다. 그러나, 이러한 Broadcast는 불필요한 정보라도 어쩔 수 없이 받아야 하는 불편함이 있습니다. 이 때, LAN을 논리적인 LAN으로 또 다시 구분하면, 서로 같은 논리적인 LAN에 존재하는 노드들만 Broadcast로 보내진 정보를 받을 수 있게 됩니다.

이렇게 논리적으로 구분된 LAN을 VLAN, 즉 가상 LAN(Virtual LAN)이라고 합니다. VLAN은 사용자의 필요에 따라 논리적으로 세분화된 네트워크이며 하나의 VLAN은 여러 개의 포트를 포함하고 있습니다. VLAN으로 구성된 네트워크는 라우팅 기능이 없는 한 동일한 VLAN에 속한 포트끼리만 패킷을 주고 받을 수 있습니다.

다음은 Layer 2 환경에서의 포트 기반 VLAN 구성을 그림으로 나타낸 예입니다.

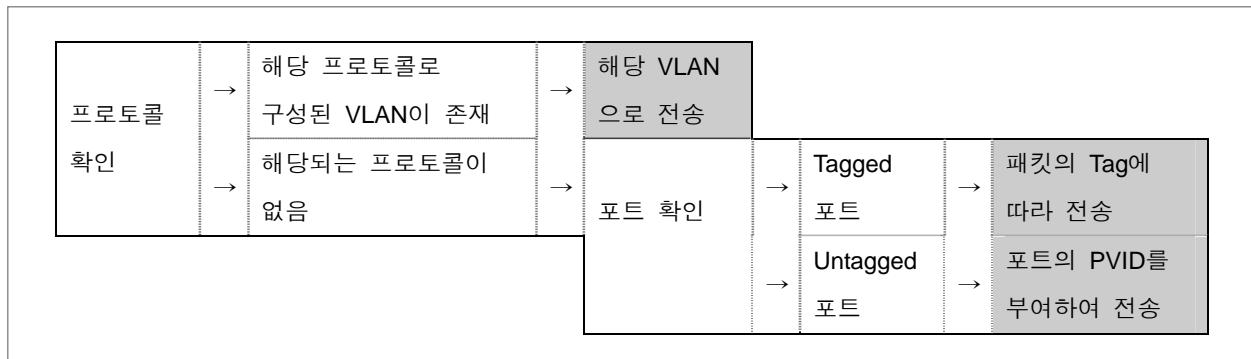


【 그림 8-1 】 Layer 2 환경 포트 기준 VLAN 구성도

위의 그림에서 VLAN으로 설정된 default, br2, br3는 논리적으로 설정된 가상 네트워크입니다. Layer 2 스위치로 동작할 경우, 가상 네트워크 내에서는 통신이 가능하지만, 서로 다른 가상 네트워크간에는 통신이 불가능합니다. 그러나, V5812G는 Layer 3 스위칭이 지원되기 때문에 Layer 3 스위치로 동작할 때에는 각기 다른 VLAN에 속한 포트들간의 통신이 가능합니다. VLAN은 이더넷 트래픽을 줄여 전송 속도를 향상시키고 VLAN 단위로 트래픽을 분리 전송하여 보안을 강화합니다. VLAN을 구성하는 방법에는 포트 단위 VLAN 구성, MAC 주소를 기반으로 한 VLAN, 그리고 프로토콜 기반 VLAN 등이 있습니다. 포트 단위 VLAN은 포트별로 VLAN을 지정하는 것으로, 하나의 포트가 여러 개의 VLAN에 속할 수 있습니다. MAC 주소 기반 VLAN은 구성원이 가지는 MAC 주소를 기준으로 VLAN의 구성원을 설정합니다. 이 방법은 구성원이 가진 고유한 MAC 주소를 사용하기 때문에 구성원이 연결 포트를 변경해도 VLAN은 변하지 않습니다. 또한, 프로토콜 기반 VLAN은 프로토콜별로 서로 다른 VLAN을 구성할 수 있도록 설정하는 방법입니다.

V5812G는 포트 기반 VLAN과 프로토콜 기반 VLAN을 지원합니다. V5812G에서 만들 수 있는 VLAN의 개수는 총 4096개이고, 그 중 프로토콜 기반 VLAN은 최대 8개까지 만들 수 있습니다. 패킷의 경로를 결정할 때에는 우선적으로 프로토콜 기반 VLAN을 기준으로 사용합니다. V5812G의 사용자가 VLAN으로 구성하도록 설정해 놓은 프로토콜에 해당하는 패킷이 전송되면 확인 후 해당 VLAN으로 전달합니다. 그러나, 사용자가 VLAN으로 구성해 놓은 프로토콜에 해당하지 않은 패킷이 전송되면, 포트 기반 VLAN을 기준으로 경로를 정해줍니다.

IEEE 802.1q 표준안을 따르는 V5812G는 모든 포트에 시스템에서 설정한 VLAN ID(PVID)를 가지고 있습니다. Tagged 포트로 들어오는 패킷에게는 자신의 VLAN ID를 유지시켜 주고, Untagged 포트로 전송되는 패킷에게는 시스템에서 설정한 포트의 PVID를 부여하게 됩니다. 다시 설명하자면, V5812G의 A번 포트를 Untagged 포트로 설정해 놓았다면, 패킷이 전송되었을 때에는 A번이 가지고 있는 PVID를 패킷에 부여하게 되는 것입니다. 따라서, VLAN 네트워크를 구성하고 있는 장비 포트들은 PVID를 통해 해당 번호와 일치하는 VLAN으로 패킷을 전송할 수 있습니다. 다음은 V5812G에 설정되어 있는 VLAN을 기준으로 패킷 경로를 결정하는 방법입니다.



【 그림 8-2 】 VLAN 기준 패킷 경로 결정 절차

VLAN은 다음과 같은 특징을 가집니다.

◆ 넓은 네트워크 대역폭

서로 다른 VLAN에 속한 사용자들은 불필요한 Broadcast 정보를 받지 않기 때문에 VLAN으로 구성되지 않았을 때보다 더 넓은 대역폭을 사용할 수 있습니다.

◆ 비용 절감

Broadcast로 인해 불필요한 트래픽이 부하되는 것을 막기 위해 LAN을 분리할 때, 서로 다른 LAN에 각각 다른 장비를 설치하는 등 여러 대의 다른 장비를 이용하지 않고 하나의 장비로 VLAN을 이용하면 저렴한 가격으로 네트워크를 구성할 수 있습니다.

◆ 보안 강화

일반 장비에서는 모든 노드가 Broadcast되는 정보를 공유하게 되는데, 이 Broadcast되는 정보 중에는 보안이 필요한 경우도 있을 수 있으며 이러한 정보를 인증되지 않은 사람이 사용할 수도 있습니다. VLAN은 인증된 사람들만으로 VLAN 멤버를 구성하는 방법을 제공함으로써 보안을 강화할 수 있습니다.

VLAN의 설정과 관련하여 다음과 같은 순서로 설명합니다.

- Default VLAN
- 포트 기반 VLAN 설정
- 프로토콜 기반 VLAN 설정
- MAC 주소 기반 VLAN 설정
- Subnet 기반 VLAN 설정
- VLAN 우선 순위 지정
- QinQ 설정
- Layer2 전용 설정에서 Shared-VLAN 설정
- Protected 포트 설정
- VLAN 설명하기
- VLAN 관련 설정 내용 확인
- 설정 예제



주의

V5812G를 SIU_GPON4와 NIU_GE12로 구성한 경우, GPON 포트에 대한 설정은 t1~t16을 사용하고, NIU에 대한 설정은 5/1, 5/2, 6/1, 6/2를 사용합니다.

8.1.1. Default VLAN

V5812G는 기본적으로 모든 포트가 Default VLAN으로 설정되어 있습니다. Default VLAN은 PVID를 1로 가지고 있으며, 절대 삭제할 수 없습니다. 사용자가 새롭게 만든 VLAN에 종복 없이 포트를 포함시키려면 반드시 Default VLAN에서 포트를 삭제해야 합니다. 다른 VLAN에서 삭제된 포트는 자동으로 Default에 포함됩니다. 또한, Trunk 포트의 멤버 포트였다가 해제된 포트도 자동적으로 Default VLAN에 포함됩니다.

8.1.2. 포트 기반 VLAN 설정

V5812G에 포트 기반 VLAN을 설정하려면, 일단 VLAN을 새롭게 만들고, 구성원을 지정하고, PVID를 할당하면 됩니다.

(1) VLAN 만들기

V5812G는 VLAN을 만들 때 VLAN명이 **N**으로 만들어지고, 이때 각 VLAN이 가지는 VID는 자동적으로 “**N**”으로 정해집니다. 다시 말하자면, VLAN 2의 VID는 2이고, VLAN 100의 VID는 100입니다. VID가 1인 VLAN은 Default VLAN으로 정해져 있습니다. 따라서 사용자는 VLAN 1이라는 이름의 VLAN은 만들 수 없습니다.

사용자 네트워크에 새로운 VLAN을 설정하기 위해 새로운 VLAN을 만들려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
vlan create vlan-name	Bridge	VLAN 이름을 지정하여 새로운 VLAN을 만듭니다.



참 고

*vlan-name*은 N=정수의 형태로 입력할 수 있습니다. 이런 형태가 아닌 다른 문자를 입력하면 다음과 같은 메시지가 출력됩니다.

```
SWITCH(bridge)# vlan create A
%invalid input parameter: A
SWITCH(bridge)#

```



*vlan-name*은 정수 “**N**”을 사용할 때, “-” 기호를 이용하여 넓은 범위를 입력하거나 “,” 기호를 사용하여 나열할 수 있습니다.

(2) PVID 지정

V5812G는 *vlan-name*에 입력되는 정수, **N**을 VID로 자동적으로 부여됩니다. 예를 들어 *vlan-name*을 “**2**”로 설정하면 VID도 “**2**”가 됩니다.

한편, PVID는 사용자가 임의로 설정할 수도 있습니다. 포트에 PVID를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
vlan pvid port-number <1-4094>	Bridge	사용자가 임의로 PVID를 설정합니다. PVID는 1~4094까지 설정이 가능합니다.

(3) 포트 할당 및 삭제

새롭게 VLAN을 만든 후에는 VLAN의 구성원이 되는 포트를 할당해야 합니다. V5812G는 기본적으로 모든 포트가 “**default**”라는 인터페이스에 통합되어 있기 때문에 중복 없이 다른 VLAN에 포트를 할당하려면 “**default**”로 부터 포트를 삭제해야 합니다.



V5812G의 모든 포트는 기본적으로 “**default**”에 속해 있습니다. 중복되지 않게 다른 VLAN에 포트를 할당하려면 제일 먼저 “**default**”에서 포트를 삭제해야 합니다.

다음은 VLAN에서 포트를 삭제, 할당할 때 사용하는 명령어입니다.

명령어	모 드	기 능
vlan add vlan-name port-number {tagged untagged}	Bridge	VLAN에 속하는 포트를 지정하고 해당 포트의 속성을 tagged나 untagged로 설정합니다.
vlan del vlan-name port-number		VLAN에 속해 있는 포트를 삭제합니다.



VLAN에 여러 개의 포트를 지정할 때는 빈 칸 없이 포트 번호를 “,” 기호로 구분하여 입력합니다. 일련의 포트 범위를 지정할 때는 “-” 기호를 사용하여 입력합니다.

(4) VLAN 기능 해제

V5812G에 설정되어 있는 VLAN을 삭제하려면 일단 해당 VLAN에 속해 있는 포트들을 삭제하고, 해당 VLAN 인터페이스를 비활성화 한 후, VLAN을 삭제해야 합니다.

다음은 설정된 VLAN을 삭제하는 방법입니다.

1 단계 bridge 모드에서 다음 명령어를 사용하여 VLAN에 속하는 모든 포트를 삭제 하십시오.

명령어	모 드	기 능
vlan del <i>vlan-name port-number</i>	Bridge	VLAN 에 속하는 포트를 삭제합니다.

2 단계 Global 설정 모드에서 삭제하려는 VLAN의 interface 설정 모드로 들어가 가상 인터페이스를 비활성화 시키십시오.

명령어	모 드	기 능
interface <i>vlan-name</i>	Global	삭제하려는 VLAN 이름을 입력하고 인터페이스 모드로 들어갑니다.
shutdown	Interface	가상 인터페이스를 비활성화 시킵니다.

3 단계 bridge 모드에서 다음 명령어를 사용하여 VLAN 을 삭제하십시오.

명령어	모 드	기 능
no vlan <i>vlan-name</i>	Bridge	VLAN을 삭제합니다.



주의

VLAN을 삭제하면 해당 VLAN에 속해있던 모든 포트가 비활성화 상태로 됩니다. 이 포트들은 새로운 VLAN에 할당할 때까지 비활성화 상태를 유지합니다.

8.1.3. 프로토콜 기반 VLAN 설정

프로토콜 기반 VLAN을 설정할 때에는 포트, 프로토콜, PVID를 지정합니다. 그러면, 사용자가 지정한 포트로 들어오는 패킷이 VLAN을 구성하고 있는 프로토콜에 해당될 때 설정된 PVID에 따라 VLAN으로 전송됩니다.

프로토콜 기반 VLAN을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
vlan pvid <i>port-number ethertype ethertype <1-4094></i>	Bridge	패킷 타입을 지정하여 프로토콜 기반 VLAN을 설정합니다.

한편, 프로토콜 기반 VLAN을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no vlan pvid port-number ethertype ethertype	Bridge	설정한 프로토콜 기반 VLAN을 해제합니다.

8.1.4. MAC 주소 기반 VLAN 설정

MAC 주소 기반 VLAN은 사용자가 입력한 MAC 주소를 기반으로 VLAN을 구성합니다. MAC 주소 기반 VLAN을 설정하시려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
vlan macbase mac-address vlan-name	Bridge	MAC 주소 기반 VLAN을 설정합니다.
no vlan macbase [mac-address]		MAC 주소 기반 VLAN을 해제합니다.
show vlan macbase	Enable / Global / Bridge	MAC 주소 기반 VLAN을 확인합니다.

8.1.5. Subnet 기반 VLAN 설정

Subnet 기반 VLAN은 사용자가 입력한 Subnet을 기반으로 VLAN을 구성합니다. Subnet 기반 VLAN을 설정하시려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
vlan subnet ip-address/m vlan-name	Bridge	Subnet 기반 VLAN을 설정합니다.
no vlan subnet [ip-address/m]		Subnet 기반 VLAN을 해제합니다.
show vlan subnet	Enable / Global / Bridge	Subnet 기반 VLAN을 확인합니다.

8.1.6. VLAN 우선 순위 지정

V5812G 스위치에 MAC 주소 기반 VLAN과 Subnet 기반 VLAN이 동시에 설정되어 있는 경우에, 사용자가 시스템에서 처리할 VLAN 우선 순위를 지정할 수 있습니다.

VLAN 우선 순위를 지정하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
vlan precedence {mac subnet}	Bridge	VLAN 우선 순위를 지정합니다.



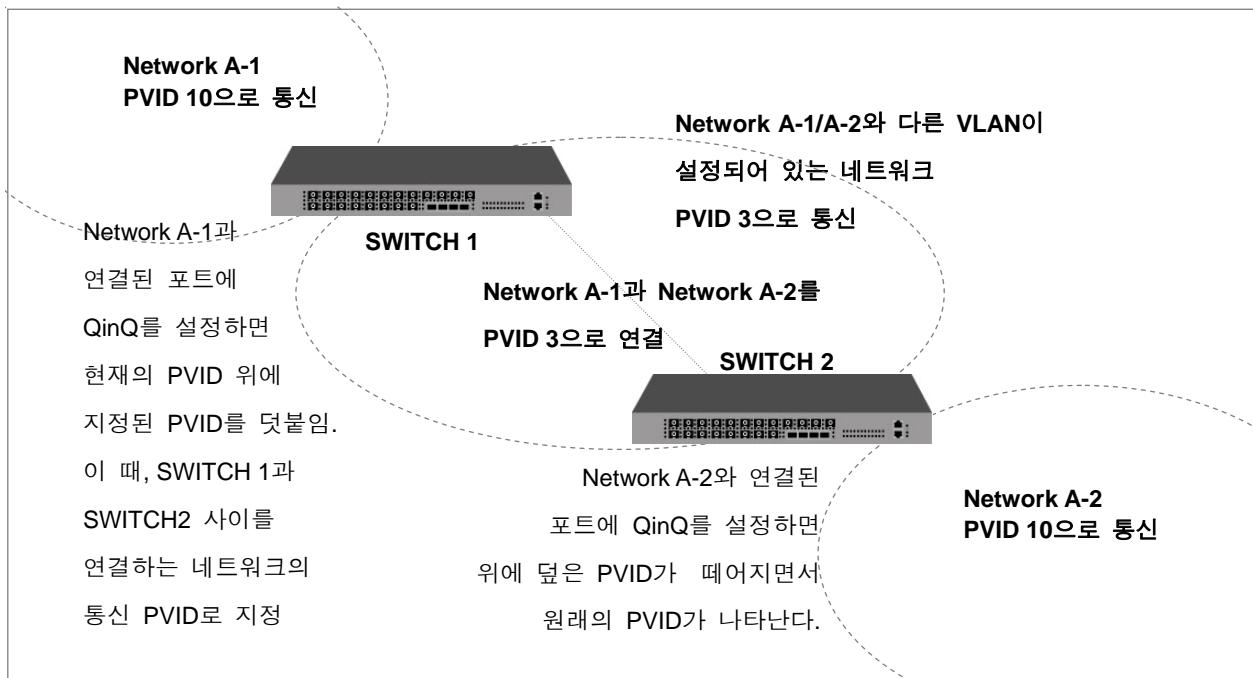
참 고

V5812G에 기본적으로 설정되어 있는 우선 순위는 **MAC 주소 기반 VLAN > Subnet 주소 기반 VLAN**입니다.

8.1.7. QinQ 설정

QinQ는 환경에서 여러 개의 서로 다른 VLAN이 설정되어 있는 네트워크간의 통신을 하나의 VLAN으로 가능하게 해 주는 기능입니다. 패킷을 전달하기 위해 또 하나의 Tag를 붙이기 때문에 Double Q-tag라고도 합니다. 기존의 일반 네트워크 환경에서 다른 VLAN으로 이루어진 네트워크와 연결되어 있는 두 장비가 있다면, 두 장비를 연결하는 모든 장비도 두 장비와 동일하게 VLAN이 설정되어 있어야 하기 때문에 설정의 번거로움이 있었습니다.

그러나, V5812G가 가지고 있는 QinQ 기능을 이용하면 번거롭게 모든 장비에 여러 개의 VLAN을 설정할 필요가 없습니다.



【 그림 8-3 】 QinQ 설정 네트워크 구성의 예

위의 그림에서 Network A-1이 Network A-2로 패킷을 보낼 때, 패킷은 SWITCH 1의 QinQ 포트로 전달되고, 전달된 패킷은 QinQ 포트가 설정된 SWITCH 2를 거쳐 Network A-2로 전달됩니다. 이 때, Network A-1에서 SWITCH 1로 패킷이 전달되면, QinQ 포트를 통해 나가는 패킷은 또 하나의 Tag를 달게 되고, 이 Tag는 여러 개의 VLAN이 설정되어 있는 네트워크 내부에서 패킷이 전송될 때 사용되는 것으로, SWITCH 2의 QinQ 포트를 통해 최종 목적지인 Network A-2에 전달될 때에는 QinQ 포트에 전달되면서 붙었던 Tag는 떼고, 본래 패킷이 가지고 있는 Tag만 가지고 전송됩니다.



주의

QinQ 포트를 제외한 다른 포트는 Tagged 포트로 설정하십시오.

한편, QinQ 포트를 설정하는 장비에서 QinQ 포트가 아닌 다른 포트들은 Tagged 패킷을 전송해야 하므로 반드시 Tagged 포트로 설정되어 있어야 합니다.

(1) QinQ 설정 방법

QinQ를 설정하려면, 다른 VLAN이 설정되어 있는 네트워크와 연결된 포트를 QinQ로 설정하고, 그 포트에는 다른 VLAN의 네트워크에서 통신에 사용하는 PVID를 설정해주어야 합니다. 【그림 8-3】 QinQ 설정 네트워크 구성의 예의 경우, PVID를 “3”으로 설정해주어야 합니다.

다음은 QinQ를 설정하는 순서입니다.

1 단계 QinQ를 설정할 포트를 다음과 같이 지정합니다.

명령어	모 드	기 능
vlan dot1q-tunnel enable port-number	Bridge	지정한 포트에 QinQ를 설정합니다.



참 고

QinQ를 설정한 포트는 VLAN의 구성원으로서 동작하지 않습니다.

2 단계 QinQ를 설정한 포트에 다른 VLAN으로 통신하는 네트워크와 동일한 PVID를 설정합니다.

명령어	모 드	기 능
vlan pvid port-number <1-4094>	Bridge	사용자가 임의로 PVID를 설정합니다. PVID는 1~4094까지 설정이 가능합니다.

(2) TPID 종류 설정

TPID(Tag Protocol Identifier)는 Tag의 프로토콜 종류를 나타내는 것으로, 현재 사용하고 있는 Tag가 어떤 프로토콜인지를 알 수 있도록 해 줍니다. 사용자는 이러한 TPID를 변경할 수도 있습니다.



TPID는 기본적으로 802.1q(0x8100)를 설정한 포트는 VLAN의 구성원으로서 동작하지 않습니다.

QinQ 포트의 TPID를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
vlan dot1q-tunnel tpid <i>tpid</i>	Bridge	QinQ 포트의 TPID를 설정합니다.

(3) QinQ 해제

QinQ 포트로 설정했던 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
vlan dot1q-tunnel disable <i>port-number</i>	Bridge	QinQ 포트로 설정한 것을 해제합니다.

8.1.8. Layer 2 전용 설정에서 Shared-VLAN 설정



주의

이 설정은 V5812G를 Layer 2 전용 스위치로 사용할 때에만 적용됩니다.

V5812G는 Layer 3 장비이지만, Layer 2 전용 장비로도 사용할 수 있습니다. 사용자가 V5812G를 Layer 2 장비로 사용할 경우에는 라우팅의 기능이 없기 때문에 VLAN 간의 통신이 불가능합니다.

특히, Uplink 포트로 지정한 포트는 모든 VLAN으로부터 패킷을 받아야 하는데, Layer 2 장비로 사용할 때에는 Uplink 포트가 모든 VLAN에 속하도록 설정하지 않으면 패킷을 받을 수가 없습니다. 따라서 Layer 2 Switch에서 VLAN을 설정할 때에는 다음과 같이 Uplink 포트를 모든 VLAN에 속하도록 설정해야 합니다.

한편, 문제는 Uplink 포트로 들어오는 Untagged 패킷입니다. Uplink 포트로 내려오는 Untagged 패킷은 어떤 PVID를 가지고 어떤 포트로 전송되어야 할지를 알 수 없습니다.

Uplink 포트로 전송된 Untagged 패킷을 다른 포트에 전송할 수 있도록 하려면, Uplink 포트를 포함한 모든 포트를 구성원으로 하는 VLAN을 또 하나 만들어줘야 합니다. 그렇게 설정하면 Uplink 포트는 모든 포트의 존재를 알 수 있습니다. 이 때 패킷 전송을 도와주는 것이 FID입니다.

FID는 MAC 테이블을 관리하는데 사용되는 ID로 동일한 FID끼리는 동일한 MAC 테이블로 관리하기 때문에 패킷 처리를 어떻게 할지를 알려줄 수 있습니다. 만일 FID를 동일하게 설정해주지 않으면 MAC 테이블을 통해 정보를 알 수 없기 때문에 패킷을 Flooding 해 버립니다.

따라서 Layer 2 전용으로 설정한 장비에서는 모든 VLAN에 Uplink 포트를 구성원으로 추가시키고, 모든 포트를 구성원으로 하는 VLAN을 하나 더 만드는 것은 물론 VLAN간의 통신이 필요한 경우에는 FID를 동일하게 설정해야 합니다.

FID를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
vlan fid vlan-name FID value	Bridge	VLAN의 FID를 설정합니다.

8.1.9. Protected 포트 설정

동일한 네트워크에 있는 사용자들이 서로의 보안(security)를 보장받으며 인터넷 통신을 가능하게 하기 위해서는 오직 업링크 포트와의 통신만 가능하게 하고 그 이외의 포트와의 통신을 막는 방법이 있습니다. V5812G가 가지고 있는 기능 가운데 Protected 포트는, 업링크 포트 이외의 포트로부터 들어오는 패킷을 막아 서비스 포트가 오직 업링크 포트와의 통신만 가능하도록 함으로써 사용자의 보안을 보장하면서 인터넷 통신이 가능하도록 해주는 기능입니다. Protected 포트로 설정된 포트는 업링크 포트 이외의 포트로부터 전송되는 유니캐스트, 멀티캐스트, 브로드캐스트 등 모든 트래픽으로부터 보호를 받게 됩니다.

Protected 포트를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port protected port-number	Bridge	Protected 포트를 설정합니다.

Protected 포트를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no port protected port-number	Bridge	Protected 포트를 해제합니다.

설정된 Protected 포트를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show port protected	Enable/Global	설정된 Protected 포트를 확인합니다.

8.1.10. VLAN 설명하기

V5812G는 각 VLAN에 대한 설명을 등록하여 사용자가 관리하기 편리하게 하였습니다. 각 VLAN에 대한 설명을 등록하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
vlan description vlan-name description	Bridge	vlan에 대한 설명을 등록합니다.

각 VLAN에 등록된 설명을 보려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show vlan description	Enable /Global/Bridge	vlan에 등록된 설명을 확인합니다.

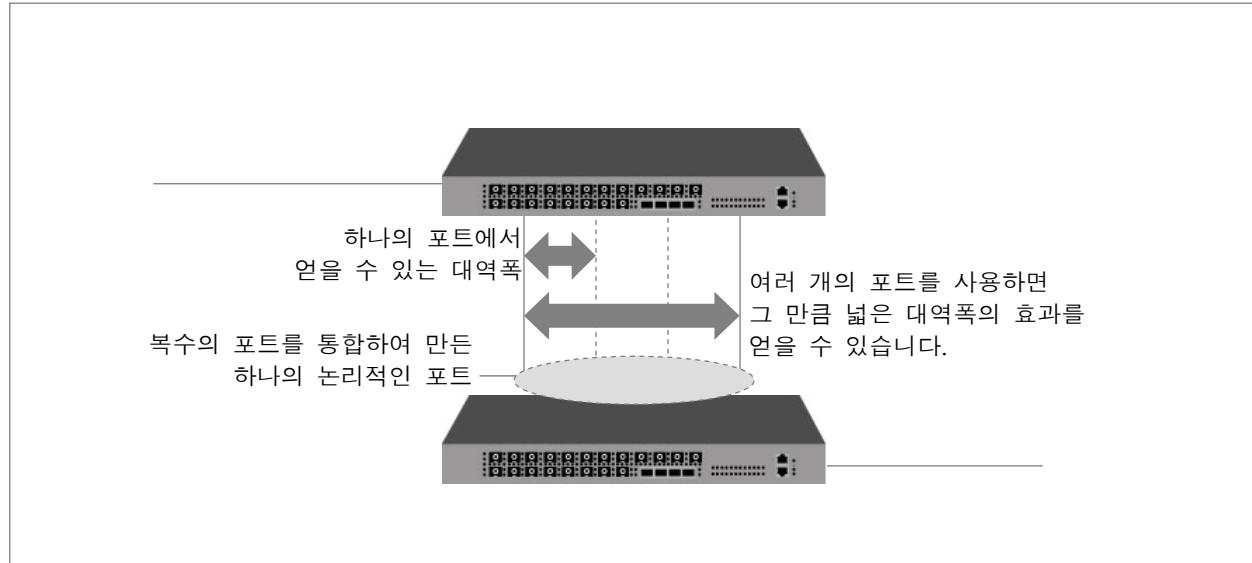
8.1.11. VLAN 관련 설정 내용 확인

V5812G는 사용자가 설정해 놓은 포트 기반 VLAN, 프로토콜 기반 VLAN, QinQ 등의 설정을 각각 확인할 수 있습니다. 각각의 설정 내용을 확인하는 방법은 다음과 같습니다.

명령어	모 드	기 능
show vlan	Enable/Global/Bridge	모든 VLAN 설정을 확인합니다.
show vlan vlan-name		특정한 VLAN에 대한 설정을 확인합니다.
show vlan dot1q-tunnel		QinQ 설정을 확인합니다.
show vlan protocol		프로토콜 기반 VLAN을 확인합니다.

8.2 Link aggregation

IEEE 802.3ad 표준에 따른 Link aggregation은 두 개 이상의 포트를 하나의 논리적인 포트로 통합하여 보다 더 넓은 대역폭을 사용할 수 있도록 하는 기능입니다.

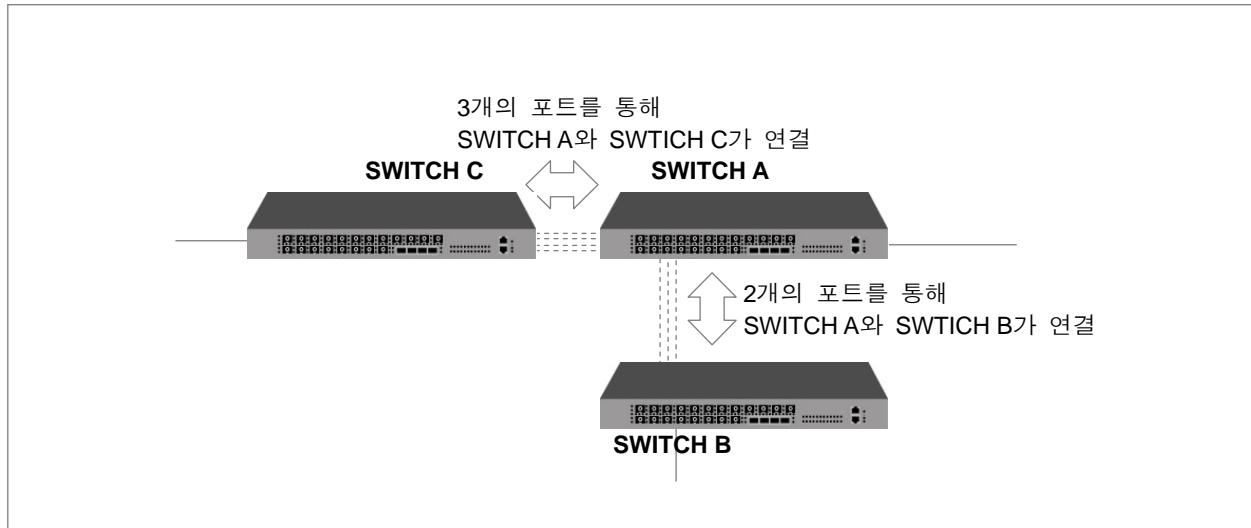


【 그림 8-4 】 Link aggregation



V5812G는 Link aggregation으로 설정한 논리적인 포트를 최대 24개까지 만들 수 있고, 하나의 논리적인 포트에는 물리적인 포트를 8개까지 포함시킬 수 있습니다.

V5812G는 포트 트렁크와 LACP의 두 가지 방식의 Link aggregation을 지원하는데, 두 방식에는 약간의 차이가 있습니다. 포트 트렁크는 논리적인 포트를 사용하여 장비를 연결할 때, 장비 간의 설정을 수동으로 다 맞춰줘야 하기 때문에 번거롭고, 네트워크 환경 변화에 대응하는 속도가 느릴 수 있습니다. 그러나, LACP는 각 장비에 논리적인 포트와 통합되는 물리적인 포트만 설정해주면 주어진 설정에 맞게 장비들이 연결됩니다. 따라서 포트 트렁크에 비해 설정이 간편하고, 환경 변화에 따라 신속하게 대응할 수 있습니다.



【 그림 8-5 】 Link aggregation 구성예 ①

위의 그림을 SWITCH A 기준에서 살펴보면, SWITCH B와는 2개의 물리적인 포트를 연결하여 1개의 논리적인 포트로 통합하였고, SWITCH C와는 3개의 물리적인 포트를 연결하여 1개의 논리적인 포트로 통합하였습니다. 이와 같은 설정은 Link aggregation 기능을 사용해야 합니다. 이 때, 포트 트렁크를 사용하여 설정한다면, 우선 SWITCH A에는 3개의 물리적인 포트로 통합한 논리적인 포트와 2개의 물리적인 포트로 통합한 논리적인 포트를 설정해야 합니다. 그리고, SWITCH B에는 2개의 물리적인 포트로 통합한 논리적인 포트 1개를 설정하고, SWITCH C에는 3개의 물리적인 포트로 통합한 논리적인 포트 1개를 설정합니다. 그리고 각각의 포트를 알맞게 케이블로 연결해주면, 위의 그림과 같은 Link aggregation 상태로 동작합니다.

그러나, LACP를 사용하는 경우라면, 그 설정은 더욱 간편해집니다. LACP는 논리적인 포트와 논리적인 포트로 통합할 물리적인 포트만 설정해 놓으면 자동적으로 링크가 형성됩니다. SWITCH A에는 논리적인 포트를 2개 만든 후, 그 논리적인 포트에 포함될 물리적인 포트를 5개 지정하십시오. 그리고, SWITCH B에는 논리적인 포트 1개와 물리적인 포트 2개, SWITCH C에는 논리적인 포트 1개와 물리적인 포트 3개를 지정하십시오, 그러면, SWITCH A에서 1개의 논리적인 포트에 포트 2개를 포함시키고, 또 다른 논리적인 포트에는 포트 3개를 포함시키는 설정을 하지 않아도 케이블만 연결하면 위와 같은 Link aggregation 상태로 동작하게 됩니다.

다음은 포트 트렁크와 LACP를 설정하는 방법입니다.

8.2.1. 포트 트렁크

포트 트렁킹은 두 개 이상의 포트를 하나의 논리적인 포트로 통합함으로써 보다 넓은 대역폭을 사용할 수 있도록 하는 기능입니다. V5812G 스위치에서는 총 24개의 트렁크 그룹이 제공되며, 이 그룹들은 <0 – 23> 사이의 ID를 가질 수 있습니다. 또한, 하나의 트렁크 구룹은 최대 8개의 멤버 포트로 구성될 수 있습니다.



주의

포트 트렁크의 그룹 ID와 LACP의 통합 포트에는 같은 ID가 할당 될 수 없습니다. 각 ID를 설정 하실 때 주의하십시오.

(1) 트렁크 그룹 및 멤버 포트 설정

포트 트렁크 그룹과 멤버 포트를 설정하시려면 다음 명령어를 사용하십시오. 지정된 포트가 해당 트렁크 그룹에 추가되거나 삭제됩니다. 포트 트렁크의 멤버 포트로 지정된 포트는 기존 VLAN으로부터 자동으로 삭제됩니다. 따라서, 멤버 포트와 통합 포트가 다른 VLAN에 존재하고 있었다면, 통합 포트에 대한 VLAN 설정을 변경해주어야 합니다.

명령어	모드	기능
trunk group-id port-number	Bridge	포트 트렁크 그룹에 멤버를 추가합니다.
no trunk group-id port-number		포트 트렁크 그룹의 멤버를 삭제합니다.



group-id는 <0-17> 사이에서 입력 가능합니다.



port-number는 한번에 여러 개를 입력할 수 있습니다. 각 입력값 사이를 빈칸 없이 쉼표(,)로 구분하거나, 입력 범위의 처음과 마지막 값을 빈칸 없이 이음표(~)로 연결하여 복수의 port-number를 입력하십시오.



주의

포트 트렁크의 그룹 ID와 LACP의 통합 포트에는 같은 ID가 할당 될 수 없습니다. ID를 설정하실 때 주의하십시오.

**주 의**

SIU_GPON4를 설치한 경우, GPON 포트가 SFU 내부적으로 t/1~t/16까지 설정되어 있습니다.

(2) 트렁크 그룹 패킷 분배 모드 지정

V5812G 스위치의 트렁크 그룹으로 들어오는 패킷들은 지정된 기준에 따라 각 멤버 포트에 분산되어 처리됩니다. 이 방법은 특정 멤버 포트로의 트래픽 집중을 방지하여 보다 안정적이고 효율적인 트렁크 그룹 운용이 가능하도록 합니다.

포트 트렁크 그룹의 패킷 분배 모드를 지정하시려면 다음 명령어를 사용하십시오.

패킷 분배의 기준이 되는 각 모드의 의미는 다음과 같습니다. 기본으로 지정되어 있는 모드는 **srcdstmac**입니다.

- **srcmac** : Source MAC 주소를 참조합니다.
- **dstmac** : Destination MAC 주소를 참조합니다.
- **srcdstmac** : Source MAC 주소와 Destination MAC 주소를 동시에 참조합니다.
- **srcip** : Source IP 주소를 참조합니다.
- **dstip** : Destination IP 주소를 참조합니다.
- **srcdstip** : Source IP 주소와 Destination IP 주소를 동시에 참조합니다.

명령어	모 드	기 능
trunk distmode group-id {srcmac dstmac srcdstmac srcip dstip srcdstip}	Bridge	패킷 분배 모드를 지정합니다.
no trunk distmode group-id		지정된 패킷 분배 모드를 삭제합니다.

(3) 포트 트렁크 설정 확인

포트 트렁크 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show trunk	Enable/Global/Bridge	트렁크 설정 내용을 확인합니다.

8.2.2. LACP 설정

LACP(Link Aggregation Control Protocol)는 앞에서 설명한 포트 트렁크 기능과 같이 두 개 이상의 포트를 하나의 논리적인 포트로 통합하여 보다 더 넓은 대역폭을 사용할 수 있도록 하는 기능입니다.

그러나, 포트 트렁크 기능과 구별되는 특징은 포트를 통합할 논리적인 통합 포트(Aggregator)와 논리적인 포트로 통합할 물리적인 멤버 포트만 설정해두면 자동적으로 통합된 대역폭을 형성한다는 점입니다. 또한, 포트 트렁크로 설정하여 생성된 통합 포트는 기존 멤버 포트가 속해있던 VLAN과 다른 VLAN에 속해 있었을 경우, 사용자가 명령어를 사용하여 통합 포트를 기존 멤버 포트가 속해 있던 VLAN으로 옮겨 줘야 하지만, LACP으로 설정한 통합 포트는 자동으로 해당 VLAN에 추가됩니다.



참 고

V5812G는 LACP를 통한 통합 포트는 24개 지원되기 때문에 Aggregator-number는 “0”부터 “23”까지 입력 가능합니다.



주 의

포트 트렁크의 Group-id와 LACP의 Aggregator-number는 중복 설정될 수 없습니다.

사용자가 LACP를 설정할 수 있도록 다음의 내용으로 설정 방법을 설명합니다.

- LACP 활성화
- 패킷 경로 규정 설정
- 멤버 포트 설정
- 멤버 포트의 동작 모드 설정
- 장비의 우선 순위 설정
- 멤버 포트의 LACP 참가 여부 설정
- BPDU 전송 주기 설정
- 멤버 포트의 Key 값 설정
- 포트 우선 순위 설정
- LACP 설정 내용 확인
- LACP 통계 확인

(1) LACP 활성화

V5812G에 LACP 기능을 설정하려면 제일 먼저 LACP 기능을 활성화시켜야 합니다. LACP 기능을 활성화 시키려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lacp aggregator aggregator-name	Bridge	지정된 Aggregator-number의 LACP를 활성화시킵니다.

한편, LACP 기능을 해제하고, LACP에 대한 설정을 모두 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no lacp aggregator aggregator-number	Bridge	지정한 Aggregator-number에 해당하는 LACP의 기능을 해제합니다.

(2) 패킷 경로 규정 설정

여러 개의 포트를 통합하고 있는 논리적인 포트에 패킷이 들어왔을 때, 패킷의 경로를 규정하는 방법이 없다면 특정 멤버 포트로만 패킷이 집중되어 효율적으로 논리적인 포트를 사용하지 못 할 수 있습니다.

따라서 V5812G는 패킷이 들어왔을 때 멤버 포트에 효율적으로 배분되도록 할 수 있는 패킷 경로 규정 방법이 정해져 있습니다. 이 패킷 경로 규정 방법은 패킷이 가지고 있는 Source IP 주소, Destination IP 주소, Source MAC 주소, Destination MAC 주소 등을 사용해 패킷 경로를 결정하는데, 사용자는 패킷 경로를 결정할 때 사용할 패킷의 정보를 정할 수 있습니다.

dstip는 Destination IP 주소를, **dstmac**는 Destination MAC 주소를 의미합니다. **srcdstip**는 Source Destination IP 주소를 의미하고, **srcdstmac**는 Source Destination MAC 주소를 의미합니다. **srcip**,는 Source IP 주소를 의미하며, **srcmac**는 Source MAC 주소를 의미합니다.



참 고

V5812G는 기본적으로 패킷 경로 결정 방법에 Source Destination MAC 주소를 이용합니다.

통합 포트를 설정하였다면 통합 포트를 경유하는 패킷을 규정해 주어야 합니다.

다음은 통합 포트를 경유하는 패킷을 규정할 때 사용하는 명령어입니다.

명령어	모 드	기 능
lacp aggregator distmode aggregator-number {dstip dstmac srcdstip srcdstmac srcip srcmac }	Bridge	논리적인 통합 포트인 Aggregator를 경유하는 패킷을 규정합니다.

(3) 멤버 포트 설정

통합 포트가 되는 Aggregator에 대한 설정이 끝나면 통합 포트의 멤버가 되는 물리적인 포트를 설정해야 합니다.

통합 포트의 멤버 포트를 설정하려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lacp port port-number	Bridge	Aggregator의 멤버 포트가 되는 물리적인 포트를 설정합니다.



*port-number*는 ","나 ":" 기호를 사용하여 복수로 설정할 수 있습니다.

멤버 포트로 설정했던 것을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no lacp port port-number	Bridge	Aggregator의 멤버 포트로 설정했던 것을 해제합니다.

(4) 멤버 포트의 동작 모드 설정

멤버 포트를 설정한 후에는 멤버 포트의 모드를 설정해야 합니다. 멤버 포트는 “**Active 모드**”와 “**Passive 모드**”의 두 가지 모드로 설정할 수 있습니다.

Passive 모드로 설정된 포트는 **Active** 모드로 설정된 상대 장비의 포트가 존재해야만 LACP 동작을 시작합니다. **Active** 모드 포트는 **Passive** 모드 포트보다 우선 순위가 높기 때문에 기준이 되고, 따라서 **Passive** 모드 포트가 **Active** 모드 포트의 설정을 따라가게 됩니다.



주의

서로 연결된 두 장비의 멤버 포트가 각각 “**active 모드**”와 “**passive 모드**”로 설정되면 “**active 모드**”로 설정된 장비가 기준이 됩니다. 두 장비가 모두 “**passive 모드**”로 설정되어 있으면 두 장비의 멤버 포트는 Link가 이루어지지 않습니다.

멤버 포트의 모드를 설정하려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lacp port activity port-number {active passive}	Bridge	멤버 포트의 모드를 설정합니다.



참 고

기본적으로 멤버 포트의 동작 모드는 “**active 모드**”로 설정되어 있습니다.

한편, 설정했던 멤버 포트의 동작 모드를 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no lacp port activity port-number	Bridge	설정했던 멤버 포트의 동작 모드를 해제합니다.



참 고

설정했던 멤버 포트의 동작 모드를 해제하면, 기본 설정값으로 돌아갑니다.

(5) 장비 우선 순위 설정

서로 연결된 두 장비의 멤버 포트가 모두 Active 모드로 설정되어 있는 경우에는 어떤 장비를 기준으로 정할 것인지에 대한 우선 순위를 정해야 할 필요가 있습니다. 이러한 경우를 대비해서 사용자는 장비에 우선 순위를 설정할 수 있도록 되어 있습니다. 다음은 LACP 기능에서 장비의 우선 순위 값을 설정할 때 사용하는 명령어입니다.

명령어	모 드	기 능
lacp system priority <1-65535>	Bridge	LACP 기능에서 장비의 우선 순위 값을 설정합니다.



참 고

V5812G는 기본적으로 장비의 우선 순위 값이 “32768(=0x8000)”으로 설정되어 있습니다.



주 의

서로 연결된 두 장비의 멤버 포트가 각각 “**active 모드**”와 “**passive 모드**”로 설정되면 “**active 모드**”로 설정된 장비가 기준이 되고, 모두 “**active 모드**”로 설정되어 있으면 우선 순위 값이 높은 장비가 기준이 됩니다.

설정했던 장비의 우선 순위 값을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no lacp system priority	Bridge	설정했던 장비의 우선 순위 값을 해제합니다.



참 고

설정했던 장비의 우선 순위 값을 해제하면, 기본 설정값으로 돌아갑니다.

(6) 멤버 포트의 LACP 참가 여부 설정

멤버 포트로 설정된 포트는 기본적으로 LACP에 참가하도록 설정되어 있습니다. 그러나, 멤버 포트로 설정한 것을 해제하지 않더라도 LACP에 참가하지 않고 독립된 포트로 동작하도록 할 수 있습니다. 이렇게 독립시킨 포트는 일단 멤버 포트로 설정된 상태에서 LACP 참가에서만 독립되었기 때문에 트렁크 포트 등으로 설정할 수 없습니다.

멤버 포트의 LACP 참가 여부를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lacp port aggregation port-number{ aggregatable individual}	Bridge	LACP 참가 여부를 설정합니다.



참 고

V5812G는 기본적으로 멤버 포트가 LACP에 참가하도록 설정되어 있습니다.

설정한 멤버 포트의 LACP 참가 여부를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no lacp port aggregation port-number	Bridge	설정한 멤버 포트의 LACP 참가 여부를 해제합니다.



참 고

설정했던 멤버 포트의 LACP 참가 여부를 해제하면, 기본 설정값으로 돌아갑니다.

(7) BPDU 전송 주기 설정

멤버 포트는 일정한 주기로 자신의 정보를 담은 BPDU를 전송합니다.

V5812G는 BPDU 전송 주기를 설정할 수 있는데, BPDU 전송 주기를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lacp port timeout port-number { long short }	Bridge	멤버 포트의 BPDU 전송 주기를 설정합니다.



참 고

V5812G는 기본적으로 멤버 포트의 BPDU 전송 주기가 “long”입니다.



참 고

“long”的 전송 주기는 30초이고, “short”的 전송 주기는 1초 입니다.

설정했던 멤버 포트의 BPDU 전송 주기를 해제합니다.

명령어	모 드	기 능
no lacp port timeout port-number	Bridge	설정했던 멤버 포트의 BPDU 전송 주기를 해제합니다.

(8) 멤버 포트의 Key 값 설정

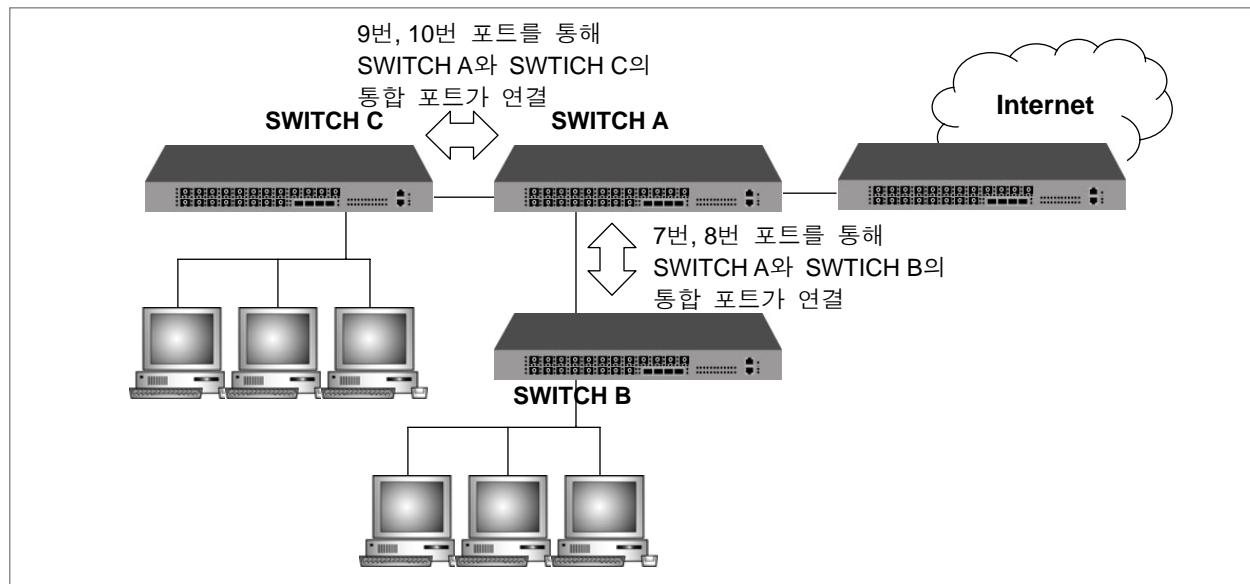
LACP의 멤버 포트는 Key 값을 가지고 있습니다. 동일한 통합 포트에 속해 있는 멤버 포트들은 모두 동일한 Key 값을 가지고 있습니다. 따라서 특정한 멤버 포트로만 이루어진 하나의 통합 포트를 만들려면 다른 통합 포트에 속한 멤버 포트와 구별되는 Key 값을 설정해주면 됩니다.

명령어	모 드	기 능
lacp port admin-key port-number <1-15>	Bridge	멤버 포트의 Key 값을 설정합니다.

▶ 참 고

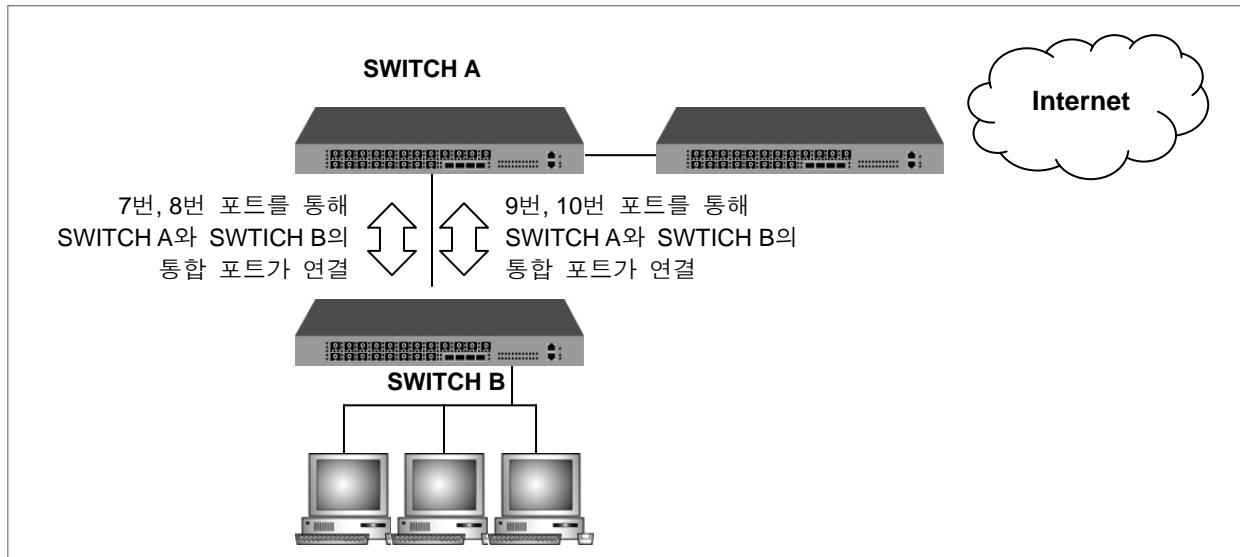
V5812G의 모든 포트는 기본적으로 Key 값이 “1”로 설정되어 있습니다.

예를 들어, 아래의 그림은 SWITCH A가 SWITCH B와 SWITCH C에 각각 연결되어 있습니다. SWITCH A에 두 개의 통합 포트를 설정하고, 7번부터 10번 포트를 멤버 포트로 설정합니다. SWITCH B에는 통합 포트를 한 개 설정하고, 7번, 8번 포트를 멤버 포트로 설정합니다. 그리고, SWITCH C에 통합 포트를 한 개 설정하고 9번, 10번 포트를 멤버 포트로 설정합니다. 이와 같이 설정이 끝나고 SWITCH A와 SWITCH B의 7번, 8번 포트, SWITCH A와 SWITCH C의 9번, 10번 포트가 케이블로 연결되어 있으면 SWITCH A는 각각 SWITCH B, SWITCH C와 통합 포트로 연결됩니다.



【 그림 8-6 】 LACP의 구성예 ①

한편, 아래 그림은 SWITCH A와 SWITCH B가 서로 연결되어 있습니다. SWITCH A와 SWITCH B에 통합 포트를 각각 2개씩 설정하고, 7번부터 10번 포트를 각각 멤버 포트로 설정합니다. 이 상태에서 7번부터 10번 포트가 케이블로 연결되어 있다면 7번부터 10번 포트를 포함한 하나의 통합 포트가 생성됩니다. 그러나, 7번, 8번 포트와 9번, 10번 포트의 Key 값을 다르게 설정한다면 두 개의 통합 포트가 생성됩니다.



【 그림 8-7 】 LACP의 구성예 ②

한편, 설정한 멤버 포트의 Key 값을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no lacp port admin-key port-number	Bridge	멤버 포트의 Key 값을 삭제합니다.



설정했던 멤버 포트의 Key 값을 해제하면, 기본 설정값으로 돌아갑니다.

(9) 포트 우선 순위 설정

하나의 통합 포트(Aggregator)에는 최대 8개 포트까지만 멤버가 될 수 있습니다. 만일 멤버 포트가 10개가 설정되어 있다면 포트가 가지고 있는 우선 순위 값에 따라 8개의 포트가 정해지게 됩니다. 그러나, 포트가 가지고 있는 우선 순위 값과 상관없이 멤버 포트로 지정하고 싶은 포트가 있다면 사용자가 우선 순위 값을 설정할 수 있습니다.

LACP의 멤버 포트에 우선 순위를 설정하려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lacp port priority port-number <1-65535>	Bridge	멤버 포트의 우선 순위 값을 설정합니다.



참 고

V5812G는 기본적으로 멤버 포트의 우선 순위 값이 “32768(=0x8000)”으로 설정되어 있습니다.

설정했던 멤버 포트의 우선 순위 값을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no lacp port priority <i>port-number</i>	Bridge	멤버 포트의 우선 순위 값을 설정합니다.



참 고

설정했던 멤버 포트의 우선 순위를 해제하면, 기본 설정값으로 돌아갑니다.

(10) LACP 설정 내용 확인

V5812G의 사용자는 LACP의 설정 내용을 확인할 수 있습니다. LACP의 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show lacp aggregator		통합 포트의 정보를 보여줍니다.
show lacp aggregator <i>aggregator-number</i>	Enable/ Global/	해당 통합 포트의 정보를 보여줍니다.
show lacp port	Bridge	멤버 포트의 정보를 보여줍니다.
show lacp port <i>port-number</i>		해당 멤버 포트의 정보를 보여줍니다.

(11) LACP 통계 확인

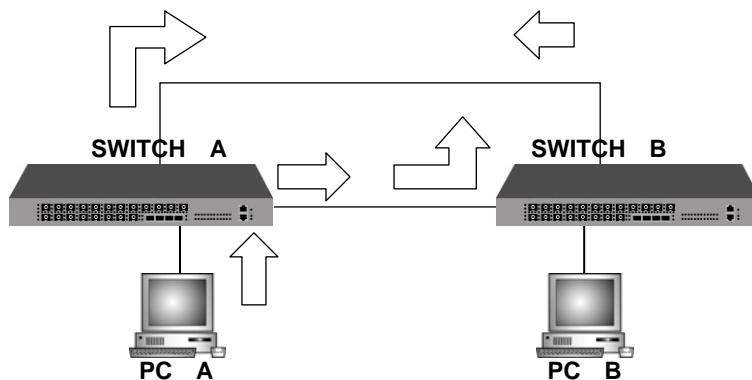
V5812G의 LACP 관련 통계를 확인 및 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show lacp statistic	Enable / Global / Bridge	LACP 관련 통계를 확인합니다.
clear lacp statistic		LACP 관련 통계를 삭제합니다.

8.3 STP 설정

토კن 링 방식과 같이 이중 경로로 구성된 LAN은 하나의 경로가 끊어지더라도 또 다른 경로를 통하여 통신이 가능하다는 장점을 가집니다. 그러나, 항상 두 가지 경로를 사용하다보면 루프 현상이라고 하는 또 다른 문제가 발생하게 됩니다.

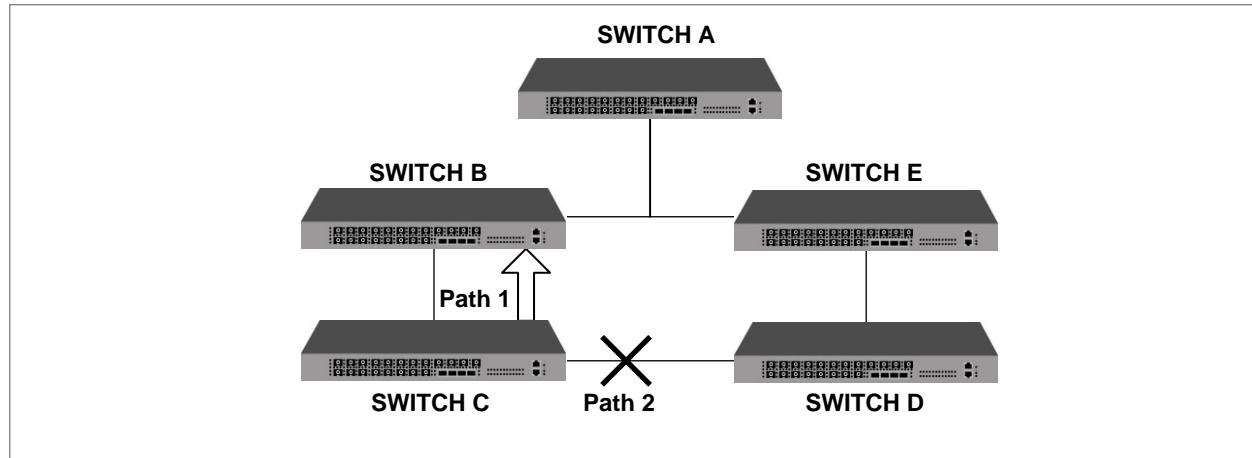
루프(Loop) 현상이란, 아래의 그림과 같이 SWITCH A와 SWITCH B 사이에 두 개 이상의 경로가 존재할 때 PC A에서 브로드캐스트나 멀티캐스트로 패킷이 전송되면 패킷이 계속 회전하게 되는 것을 말하며 이러한 현상이 발생하면 불필요한 데이터가 계속해서 전송되기 때문에 네트워크가 불안정해집니다.



【 그림 8-8 】 루프 현상의 예

STP(Spanning-Tree Protocol)는 이중 경로가 존재하는 LAN에서 루프 현상을 막고 이중 경로를 효율적으로 이용할 수 있도록 해 주는 기능으로 IEEE 802.1d 표준안에 명기되어 있습니다. STP 기능을 설정하면 두 가지 경로 중에서 효율적인 경로를 선택, 나머지 경로를 막아주기 때문에 루프 현상이 발생하지 않습니다.

말하자면, 아래 그림의 SWITCH C에서 SWITCH A로 패킷을 보낼 때, Path 1을 선택하게 되면 Path 2로는 패킷이 나갈 수 없게 되는 것입니다.



【 그림 8-9 】 STP의 원리

한편, IEEE 802.1w 표준안에 정의되어 있는 RSTP(Rapid Spanning-Tree Protocol)은 기존의 STP에서 네트워크 convergence 시간을 혁신적으로 단축하였습니다. 802.1d에서 사용한 전문적인 용어와 대부분의 설정 파라미터를 그대로 사용하기 때문에 새로운 프로토콜을 쉽고 빠르게 설정할 수 있습니다. 또한, 802.1w는 802.1d를 내부적으로 포함하고 있어 호환이 가능합니다.

이 장에서는 STP와 RSTP에 대하여 다음의 순서로 보다 자세히 설명합니다.

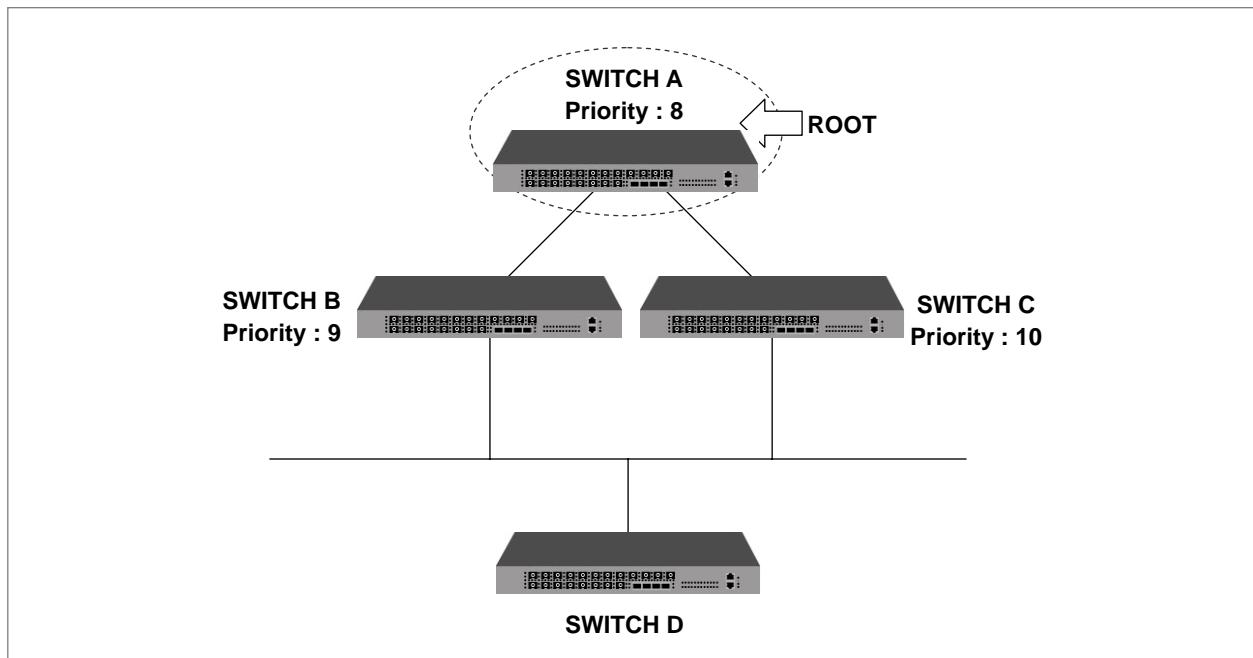
- STP 동작 원리
- RSTP 동작 원리
- PVSTP와 MSTP
- STP/RSTP/MSTP/PVSTP/PVRSTP 모드 설정
- STP/RSTP/MSTP 설정
- PVSTP/PVRSTP 설정
- BPDU(Bridge Protocol Data Unit) 설정
- BPDU 필터링 설정
- Point-to-Point MAC 설정
- STP 모드 변경 감지
- STP Guard 설정
- BPDU Guard 설정
- 설정 예제

8.3.1. STP 동작 원리

802.1d의 STP에서는 포트 상태를 Blocking, Listening, Learning, Forwarding의 네 가지로 정의합니다. 이중 경로를 가지고 있는 LAN에 STP를 설정하면 장비들은 Bridge ID를 포함한 자신의 정보를 교환하게 되는데 이를 BPDU(Bridge Protocol Data Unit)라고 합니다. 장비들은 서로 주고 받은 BPDU를 바탕으로 포트의 상태를 결정하고, Spanning-Tree의 기준이 되는 Root 장비와 Root 장비와 통신할 때의 최적 경로를 자동적으로 결정합니다.

◆ Root 장비

Root 장비를 결정하는 중요한 정보는 바로 Bridge ID입니다. Bridge ID는 2Bytes로 된 Priority와 6Bytes로 된 MAC 주소로 구성되는데, Bridge ID가 가장 작은 것을 Root 장비로 결정합니다.

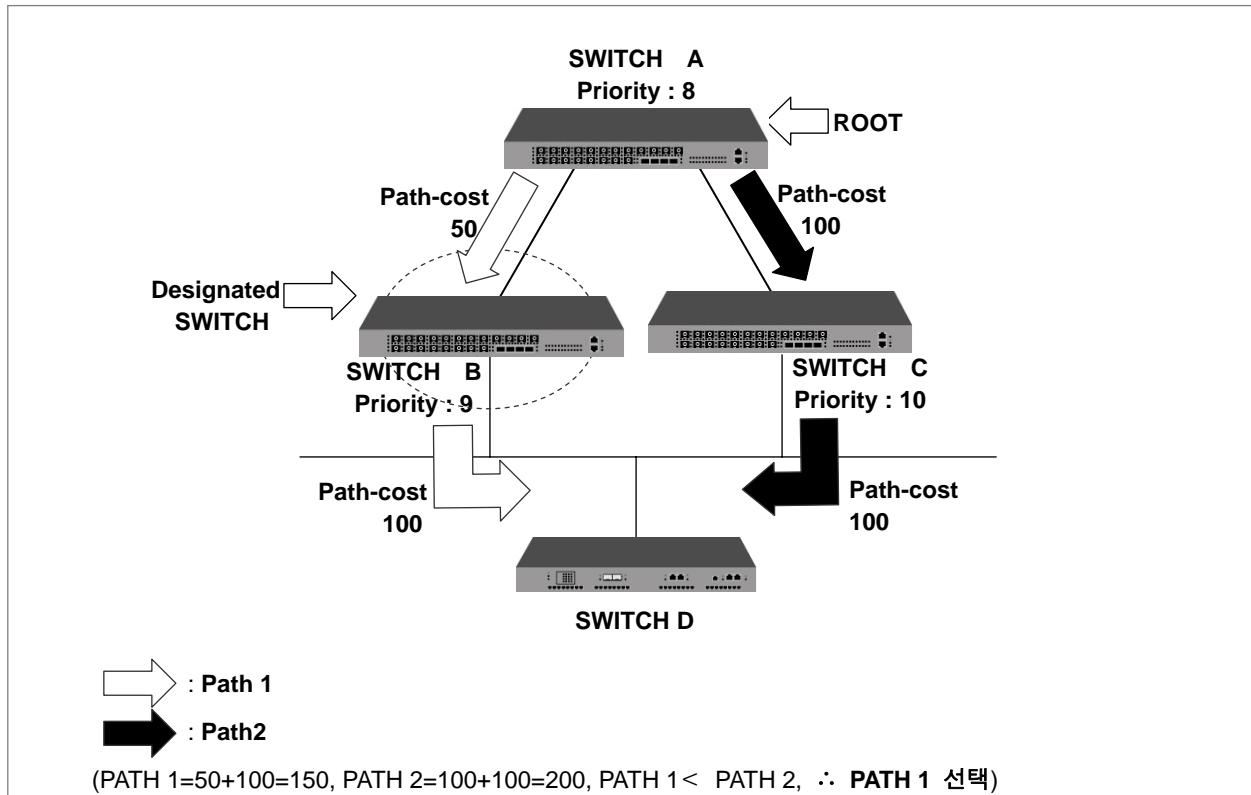


【 그림 8-10 】 Root 장비

예를 들어 위의 그림과 같이 장비 3개가 연결되어 있다고 가정합니다. STP 기능을 설정하면 장비들은 서로 자신의 정보를 교환합니다. 이 때 SWITCH A의 Priority가 8, SWITCH B의 Priority가 9, SWITCH C의 Priority가 10이라고 하면, 자동적으로 SWITCH A가 Root 장비로 설정됩니다.

◆ Designated 장비

Root 장비가 결정된 후 SWITCH A에서 패킷을 전송해야 하는 상황이 되었을 때, SWITCH A는 서로 주고 받은 BPDU를 비교하여 Designated 장비를 선택, 어떤 경로를 사용할지를 결정합니다. Designated 장비는 하나의 세그먼트 안에서 통신이 이루어질 수 있도록 선택된 장비입니다. Designated 장비를 선택할 때 기준이 되는 것은 Root 장비까지의 path-cost를 합산한 Root path-cost입니다. Path-cost는 장비의 LAN 인터페이스 전송 속도에 따라 정해지며 path-cost 값이 작은 경로에 있는 장비가 Designated 장비가 됩니다.



【 그림 8-11 】 Designated 장비 결정

위의 경우, SWITCH A에서 패킷이 나가야 하는 상황에서 PATH 1의 path-cost는 총 150이되고 PATH 2의 path-cost는 총 200이 됩니다. 따라서 path-cost가 작은 PATH 1이 선택되는 것입니다. 한편, path-cost가 동일한 경우에는 Bridge ID를 사용하여 Bridge ID가 작은 장비가 Designated 장비로 선택됩니다.

참 고

Designated 장비를 선택할 때에는 Root 까지의 path-cost를 합산한 Root path-cost를 비교합니다.

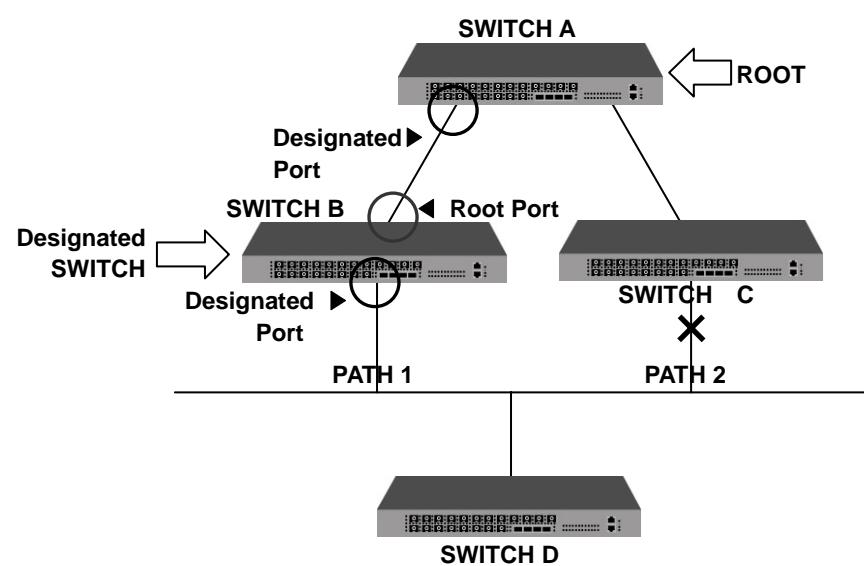
Root path-cost가 작은 쪽이 Designated 장비로 결정됩니다. Root path-cost가 동일할 경우에는 Bridge ID를 비교합니다.

◆ Designated 포트와 Root 포트

아래의 그림에서 Root 장비에서 SWITCH D로 패킷이 전송된다고 가정을 합니다. 일단 SWITCH B 와 SWITCH C는 모두 선택될 가능성을 가지고 있습니다.

그러나 SWITCH D로 패킷이 전송되면서 Loop 현상이 발생되기 때문에 위에서 설명한 바와 같이 BPDU가 가지고 있는 정보를 비교하여 둘 중 하나를 선택해야 합니다. 결과적으로 PATH 1이 선택되었다고 하면 SWITCH D로 전송되는 세그먼트에 대한 Designated 장비는 SWITCH B가 됩니다.

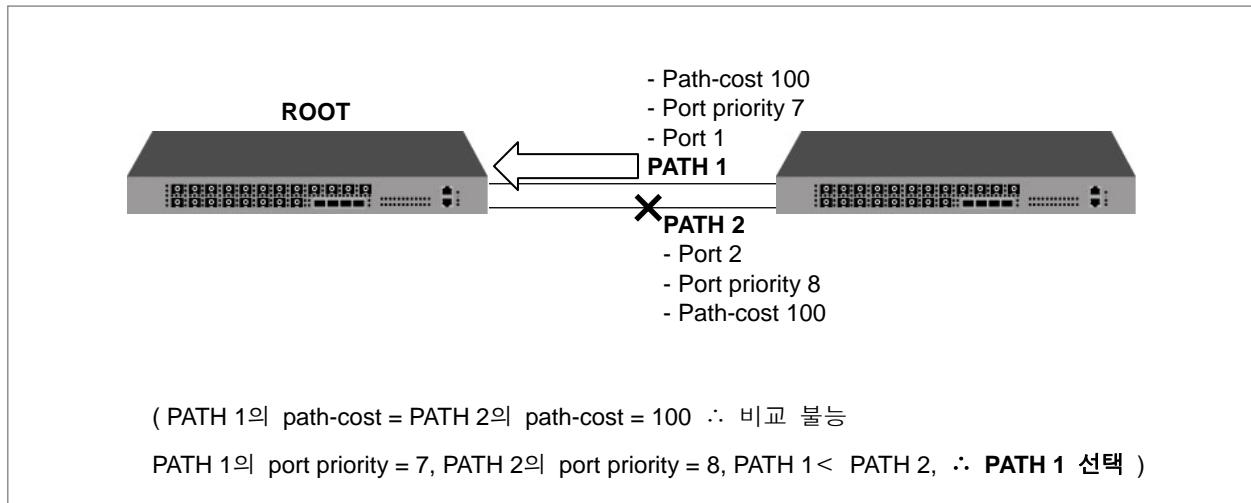
이 때 Root 장비에 연결되는 포트를 Root 포트라고 합니다. 아래의 그림과 같은 경우에는 Root 장비인 SWITCH A와 연결되는 SWITCH B의 포트가 Root 포트가 됩니다. 하나의 장비에 Root 포트는 한 개만 존재할 수 있습니다. 각 장비에서 Root 포트를 제외하고, 통신이 이루어지도록 선택된 포트는 Designated 포트입니다. 또한, Root 포트와 Designated 포트를 제외한 통신이 이루어지지 않는 포트는 Blocked 포트라고 합니다.



【 그림 8-12 】 Designated 장비와 Designated 포트

◆ Port-priority

한편, 두 경로의 path-cost가 동일한 경우에는 port-priority가 경로를 결정하는 기준이 됩니다. 다음과 같이 2개의 장비가 연결되어 있다고 가정합니다. 두 경로의 path-cost가 100으로 똑같을 때에는 port-priority를 비교, 값이 작은 포트가 root 포트로 선택되어 패킷을 전송합니다.



【 그림 8-13 】 Port priority를 사용한 결정

이 모든 동작 원리는 이미 각 장비가 가지고 있는 정보인 BPDU를 통해 자동적으로 결정되지만, V5812G의 사용자는 Root 장비나 경로를 인위적으로 변경하기 위해 BPDU의 값을 설정해 줄 수 있습니다. 설정 방법은 ‘**8.4.7 BPDU (Bridge Protocol Data Unit) 전송 설정**’에 나와 있습니다.

8.3.2. RSTP의 동작 원리

Loop가 발생할 수 있는 네트워크에서 STP 또는 RSTP를 설정했을 때, 마지막 토플로지의 결과는 동일합니다. 그러나 마지막 토플로지에 도달하기까지의 과정에서 RSTP는 STP보다 빠르게 진행됩니다.

STP에서 진화된 RSTP에 대해서 다음과 같이 설명합니다.

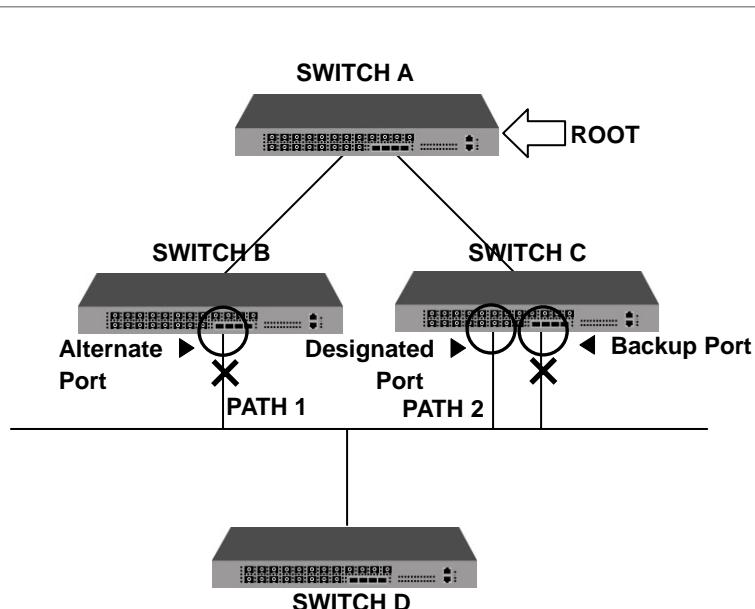
- 포트 상태의 변화
- BPDU 정책 변화
- 네트워크 convergence 시간 단축
- 802.1d와의 호환성

(1) 포트 상태의 변화

RSTP에서는 포트 상태를 Discarding, Learning, Forwarding의 세 가지로 정의합니다. 802.1d의 Blocking과 Listening을 Discarding으로 통합하였습니다. STP의 원리와 같이 포트 상태에 따라 Root 포트와 Designated 포트가 결정됩니다.

그러나 이전의 Blocked 포트는 Alternate 포트와 Backup 포트로 나뉘어집니다. Alternate 포트는 다른 장비로부터 우선 순위가 높은 BPDU를 받음으로써 Blocked 된 포트를 의미하고, Backup 포트는 같은 장비의 다른 포트로부터 우선 순위가 높은 BPDU를 받음으로써 Blocked된 포트를 의미합니다.

아래의 그림은 Alternate 포트와 Backup 포트를 설명한 것입니다.



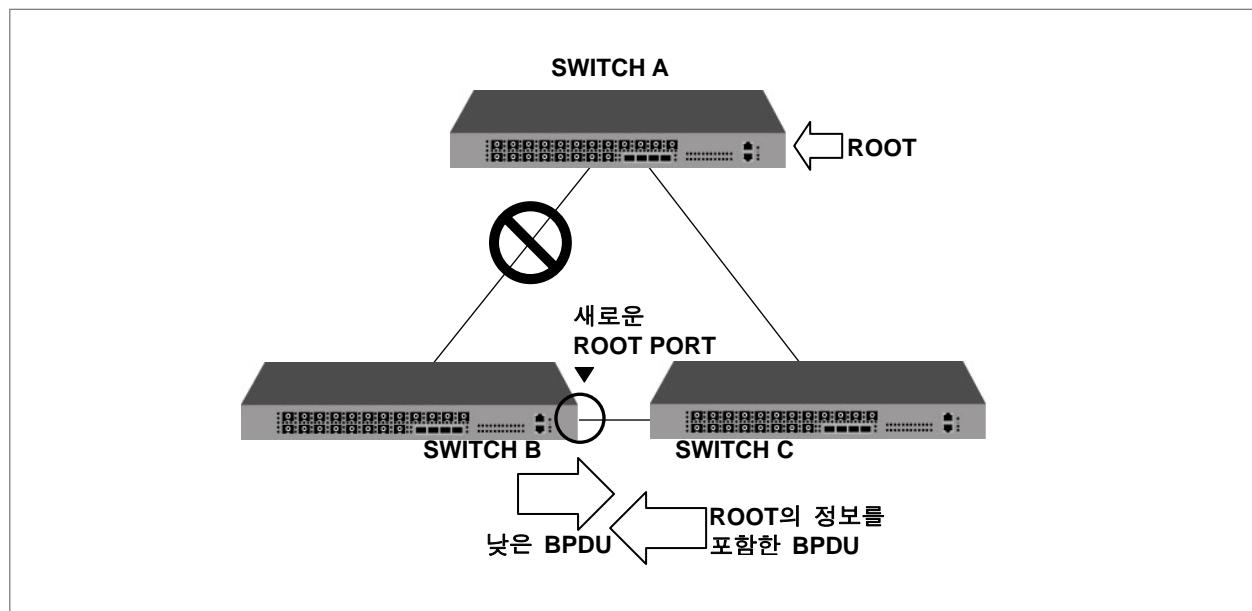
【 그림 8-14 】 Alternate 포트와 Backup 포트

Alternate 포트와 Backup 포트의 차이점은 위의 그림에서 Root 장비와 SWITCH C 사이에 문제가 발생하였을 때 패킷의 경로를 대체해줄 수 있지만, Backup 포트는 Root 장비와 SWITCH C 사이에 문제가 발생하여도 끊임없는 접속을 보장할 수는 없다는 것입니다.

(2) BPDU 정책 변화

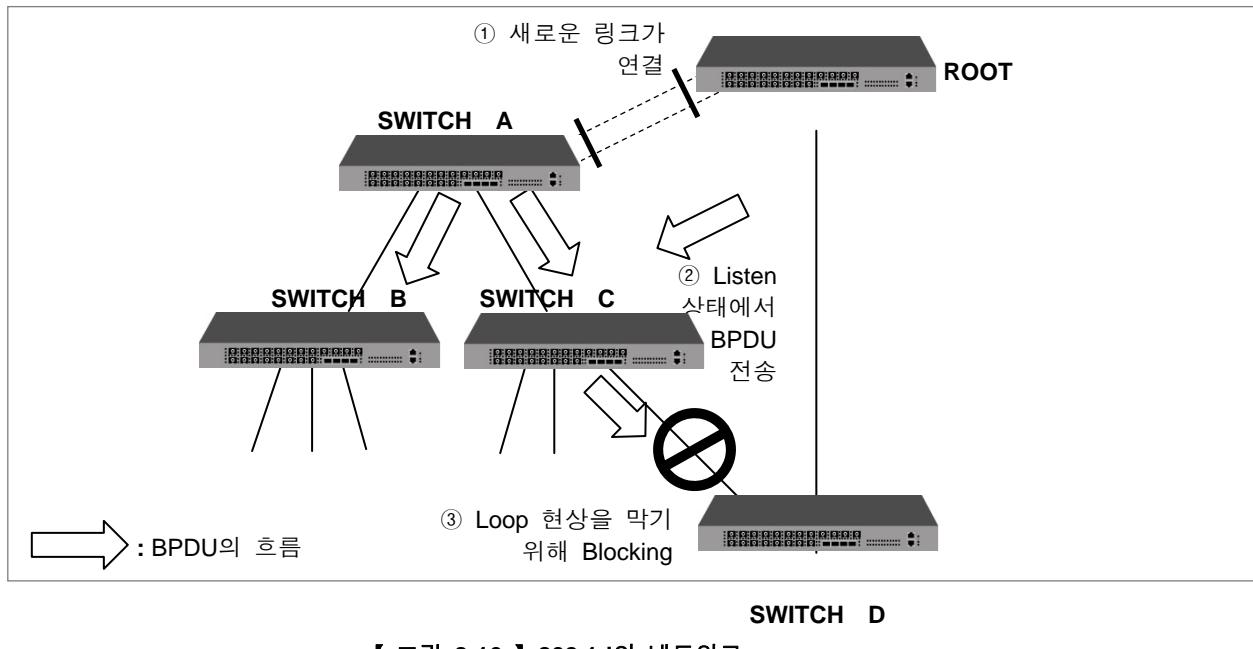
802.1d는 Root 장비만 설정된 Hello-time에 따라 BPDU를 전송하고, Root 장비를 제외한 다른 장비는 Root 장비로부터 BPDU를 받았을 때에만 자신의 BPDU를 전송하였습니다. 그러나 802.1w는 Root 장비가 아닌 모든 장비도 Hello-time에 따라 BPDU를 전송합니다. BPDU는 실제로 Root 장비에 의해 주고받는 시간 간격보다 더 자주 변화하는데 802.1w에서는 변화하는 네트워크 환경에 더욱 빨리 대응할 수 있게 되었습니다.

한편, Root 장비나 Designated 장비로부터 낮은 BPDU를 받았을 경우에는 이를 즉시 받아들입니다. 예를 들어, 아래의 그림과 같이 Root 장비와 SWITCH B 사이에 링크가 끊어졌다고 가정합니다. 그러면, SWITCH B는 Root와의 링크가 끊어졌기 때문에 Root가 사라지고 자신이 Root가 되었다고 생각하고 BPDU를 내보냅니다. 그러나 SWITCH C는 Root의 존재를 알고 있기 때문에 Root에 대한 정보를 포함한 BPDU를 브리지 B에 전송합니다. 그러면, SWITCH B는 SWITCH C와 연결된 포트를 새로운 Root 포트로 설정합니다.



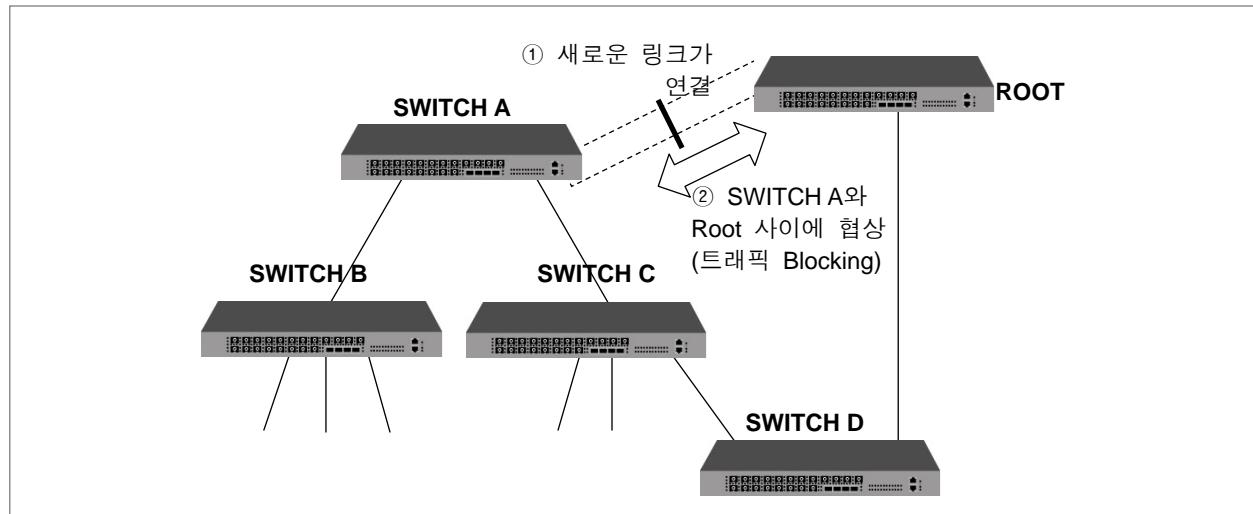
【 그림 8-15 】 낮은 BPDU를 받아들이는 경우

(3) 네트워크 convergence 시간 단축



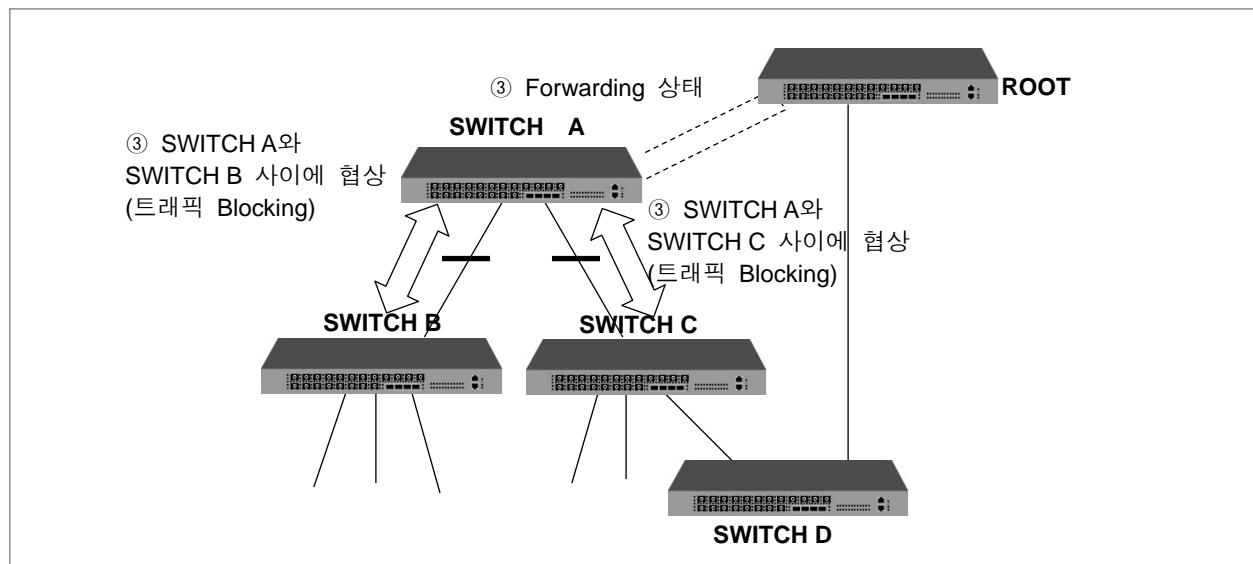
【 그림 8-16 】 802.1d의 네트워크 convergence

위의 그림과 같이 SWITCH A와 Root 사이에 새로운 링크가 연결되었다고 가정합니다. Root와 SWITCH A는 직접은 연결되어 있지 않지만 SWITCH D를 통해 간접적으로 연결되어 있는 상태입니다. SWITCH A와 Root가 새롭게 연결되면 두 장비는 일단 두 장비는 listening 상태가 되기 때문에 포트간에 패킷은 주고 받을 수 없고, 따라서 Loop도 발생하지 않습니다. 이 상태에서 Root가 SWITCH A에 BPDU를 보내면, SWITCH A는 SWITCH B와 SWITCH C에 새로운 BPDU를 보내고, SWITCH C도 SWITCH D에 새로운 BPDU를 보내게 됩니다. SWITCH C로부터 BPDU를 받은 SWITCH D는 새로운 링크 연결에 따라 Loop가 발생하는 것을 막기 위해 SWITCH C와 연결된 포트를 Blocking 상태로 만듭니다. 이러한 방법으로 Loop 현상을 막는 것은 매우 획기적인 방법이지만, 문제는 SWITCH D가 SWITCH C와 연결된 포트를 막기까지 BPDU의 Forward-delay 시간을 두 번 거치는 동안 통신이 단절된다는 점입니다. 802.1w에서는 통신이 단절되는 시간을 단축하기 위해 다음과 같은 과정을 거칩니다. SWITCH A와 Root 사이에 새로운 링크가 연결됩니다. 그러면, 연결되자마자 SWITCH A와 Root 사이는 패킷을 주고받을 수 없지만, BPDU는 전송할 수 있는 상태가 됩니다.



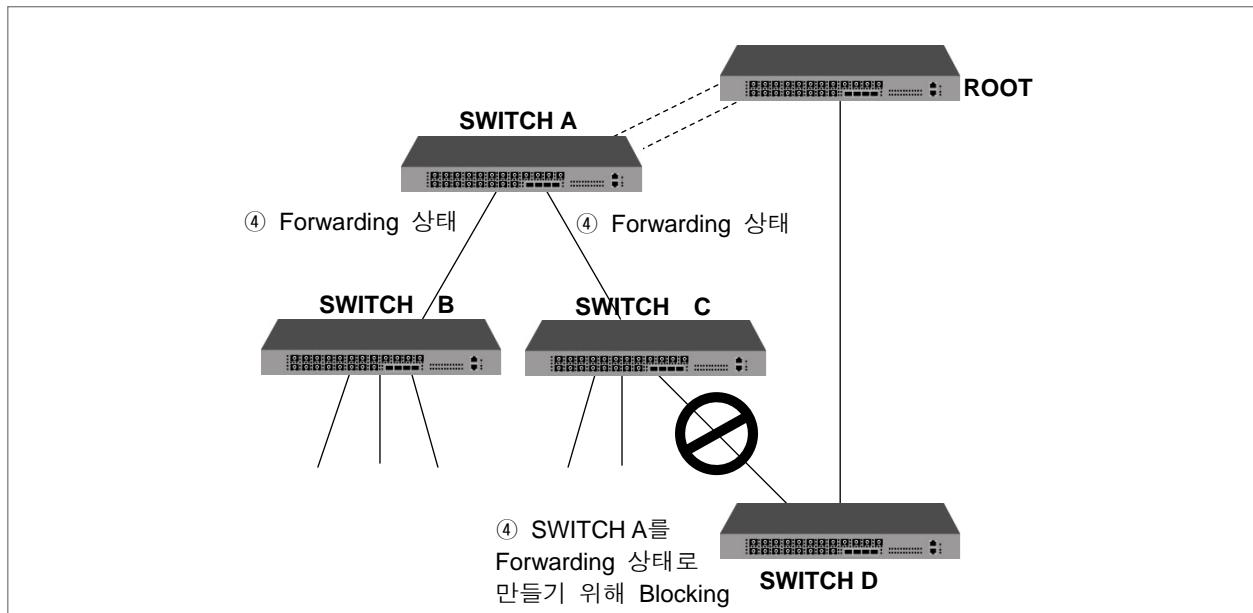
【 그림 8-17 】 802.1w의 네트워크 convergence ①

BPDU를 통해 Root와 SWITCH A는 협상이 이루어지고 Root와 SWITCH A 사이의 링크를 Forwarding 상태로 만들기 위해 SWITCH A의 non-edge designate 포트를 Blocking 상태로 변경합니다. SWITCH A와 Root가 연결되었지만, SWITCH A와 SWITCH B, C의 연결을 막았기 때문에 Loop는 발생하지 않습니다. 이 상태에서 Root의 BPDU는 SWITCH A를 통해 SWITCH B와 SWITCH C로 전송됩니다. SWITCH A를 Forwarding 상태로 만들기 위해 다시 SWITCH A와 SWITCH B, SWITCH A와 SWITCH C 간에 협상이 이루어지게 됩니다.



【 그림 8-18 】 802.1w의 네트워크 convergence ②

SWITCH B는 edge designated 포트만 가지고 있습니다. edge designated 포트는 Loop를 발생시키지 않기 때문에 802.1w에서는 Forwarding 상태로 변환할 수 있도록 정의하고 있습니다. 따라서, SWITCH B는 SWITCH A를 Forwarding 상태로 만들기 위해 특별히 Blocking 할 포트가 없습니다. 그러나, SWITCH C는 SWITCH D와 연결된 포트가 있기 때문에 SWITCH A를 Forwarding 상태로 변환시키려면 해당 포트를 Blocking 상태로 만들어야 합니다.

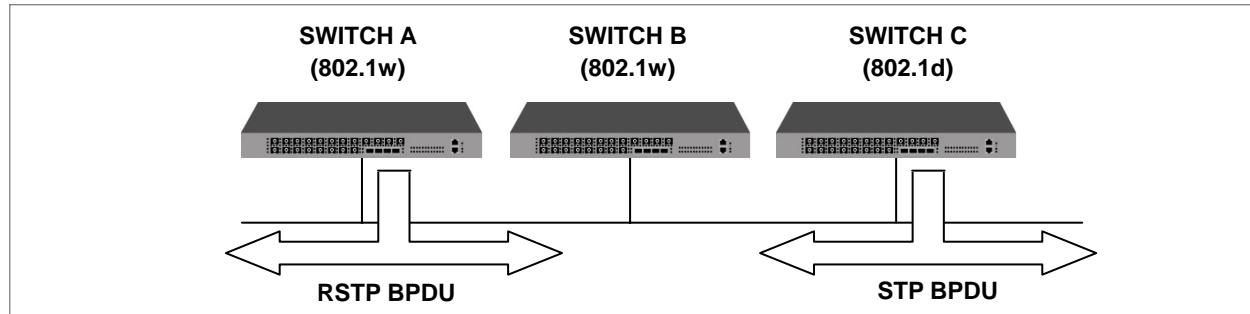


【 그림 8-19 】 802.1w의 네트워크 convergence ③

결과적으로 SWITCH D와 SWITCH C의 연결을 Blocking 하는 것은 802.1d와 동일합니다. 그러나, 802.1w는 특정 포트를 Forwarding 상태를 만들기 위해 장비간에 이루어지는 협상에 사용자가 설정해 놓은 어떤 시간 기준도 사용되지 않기 때문에 매우 빠르게 진행됩니다. 포트가 Forwarding 상태로 진행되는 과정에서 Listening과 Learning이 필요하지도 않습니다. 이러한 협상은 BPDU를 이용합니다.

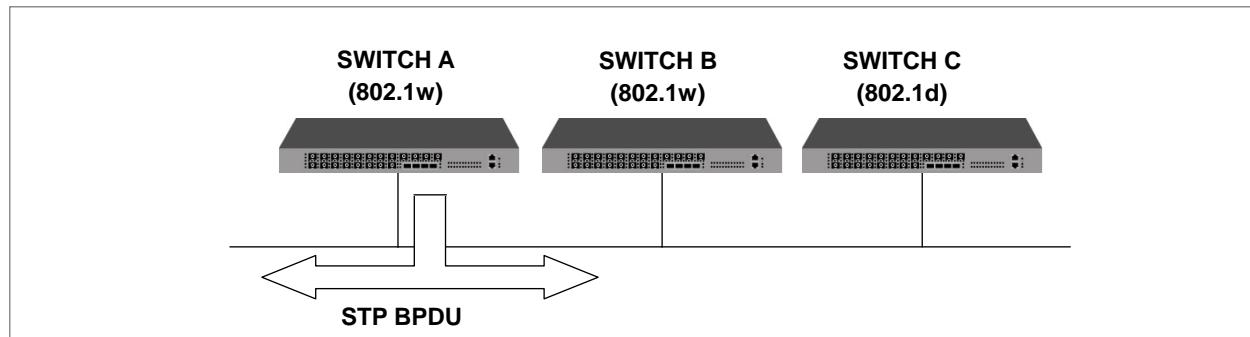
(4) 802.1d와의 호환성

RSTP는 내부적으로 STP를 포함하고 있기 때문에 호환성을 가지고 있습니다. 따라서 RSTP는 STP의 BPDU를 인식할 수 있습니다. 그러나, STP는 RSTP의 BPDU는 판독할 수 없습니다. 예를 들어 아래의 그림과 같이 SWITCH A와 SWITCH B가 RSTP로 동작하고 SWITCH A가 Designated 장비로 SWITCH C와 연결이 이루어졌다고 가정합시다. 802.1d인 SWITCH C는 RSTP BPDU를 무시하고 버리기 때문에 SWITCH C는 어떤 장비나 세그먼트와도 연결되어 있지 않다고 판단합니다.



【 그림 8-20 】 STP와의 호환 ①

그러나 SWITCH A는 SWITCH C의 BPDU를 판독할 수 있기 때문에 BPDU를 받은 포트를 802.1d의 STP로 변환시킵니다. 그러면, SWITCH C는 SWITCH A의 BPDU를 판독할 수 있게 되고, SWITCH A를 Designated 장비로 받아들입니다.



【 그림 8-21 】 STP와의 호환 ②

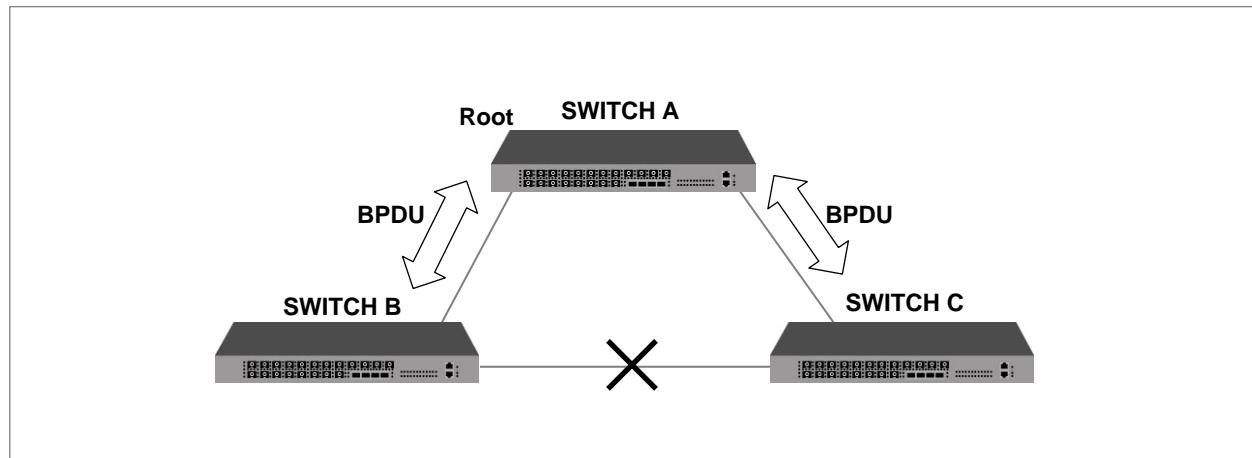
8.3.3. PVSTP와 MSTP

좀 더 효율적으로 망을 운영하기 위하여 V5812G는 기존의 LAN 도메인을 논리적으로 세분화 한 VLAN 개념을 도입하여 망을 구성하고, 경로 설정을 위하여 기존의 라우팅 프로토콜의 사용 대신 VLAN 별로 또는 VLAN 그룹 별로 경로를 설정할 수 있는 PVSTP(Per VLAN Spanning Tree Protocol) 또는 MSTP(Multiple Spanning Tree Protocol)을 사용합니다. MSTP를 사용하면, 별도의 RSTP를 구현하지 않고도 토플로지 변경시 트리 재구성 시간을 최소화 할 수 있습니다.

(1) 동작

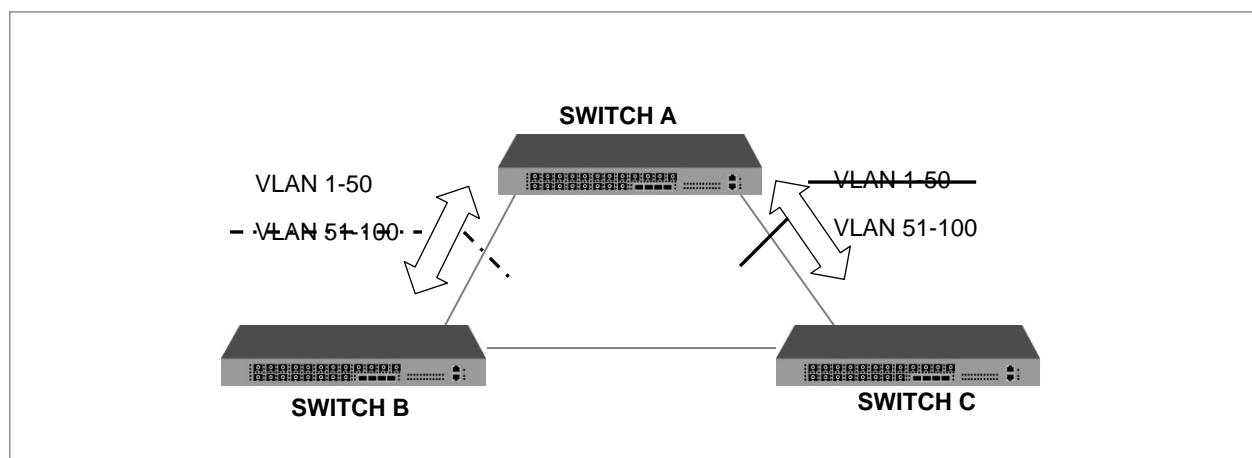
다음 그림은 STP/PVSTP/MSTP가 LAN에서 어떠한 차이점을 가지고 동작하는지에 대한 설명입니다.

Switch A로부터 B, C로 VLAN을 100개 설정했을 경우를 가정합니다. STP/RSTP의 경우 모든 VLAN들은 하나의 STP만 사용하며 다중 Instance를 지원하지 않습니다.



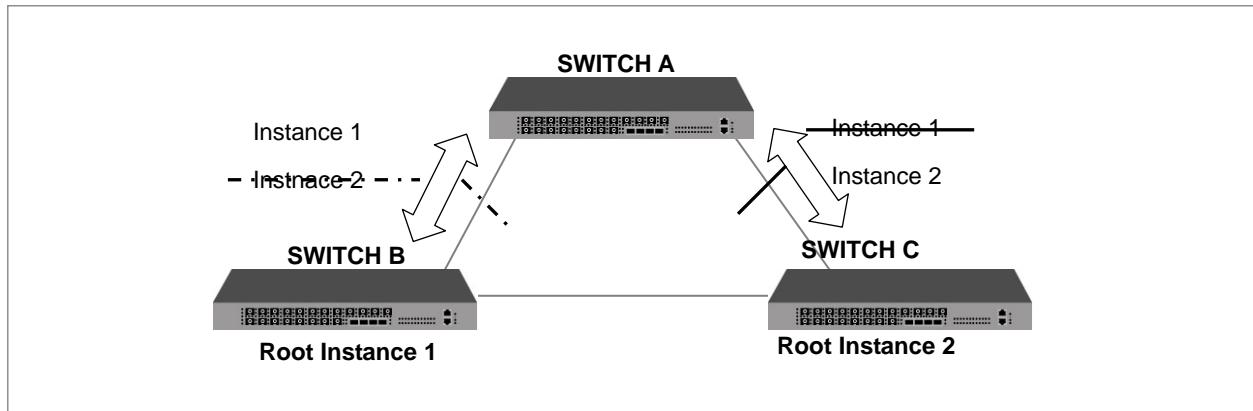
【 그림 8-22 】 STP

기존의 STP가 하나의 LAN 도메인에서 Loop를 방지하기 위해 사용된 프로토콜 이라면 PVSTP(Per VLAN Spanning Tree Protocol)은 VLAN 별로 STP를 구성함으로써 VLAN 환경에 맞는 경로 설정을 위해 보완된 프로토콜입니다. PVSTP/PVRSTP의 경우 VLAN 하나에 하나의 STP를 지원합니다. 100 개의 VLAN으로부터 나오는 100개의 STP를 각각 계산해야 하므로 장비의 부하가 걸리는 단점이 있습니다.



【 그림 8-23 】 PVSTP

고속 convergence를 위해 RSTP를 사용하는 IEEE 802.1s MSTP는 여러 개의 VLAN을 Instance 단위로 분류할 수 있으며, 각 Instance는 서로 다른 Spanning Tree Topology를 가지고 동작합니다. 여러 개의 VLAN에 대한 STP를 모두 계산할 필요가 없기 때문에 PVSTP에서 발생하는 트래픽 부하를 줄일 수 있습니다. 불필요한 부하를 줄이고 데이터 전송을 위한 다중 전송 경로를 제공하여 장비의 로드 밸런싱을 실현하는 것은 물론, Instance를 통해 많은 양의 VLAN을 지원할 수 있습니다.

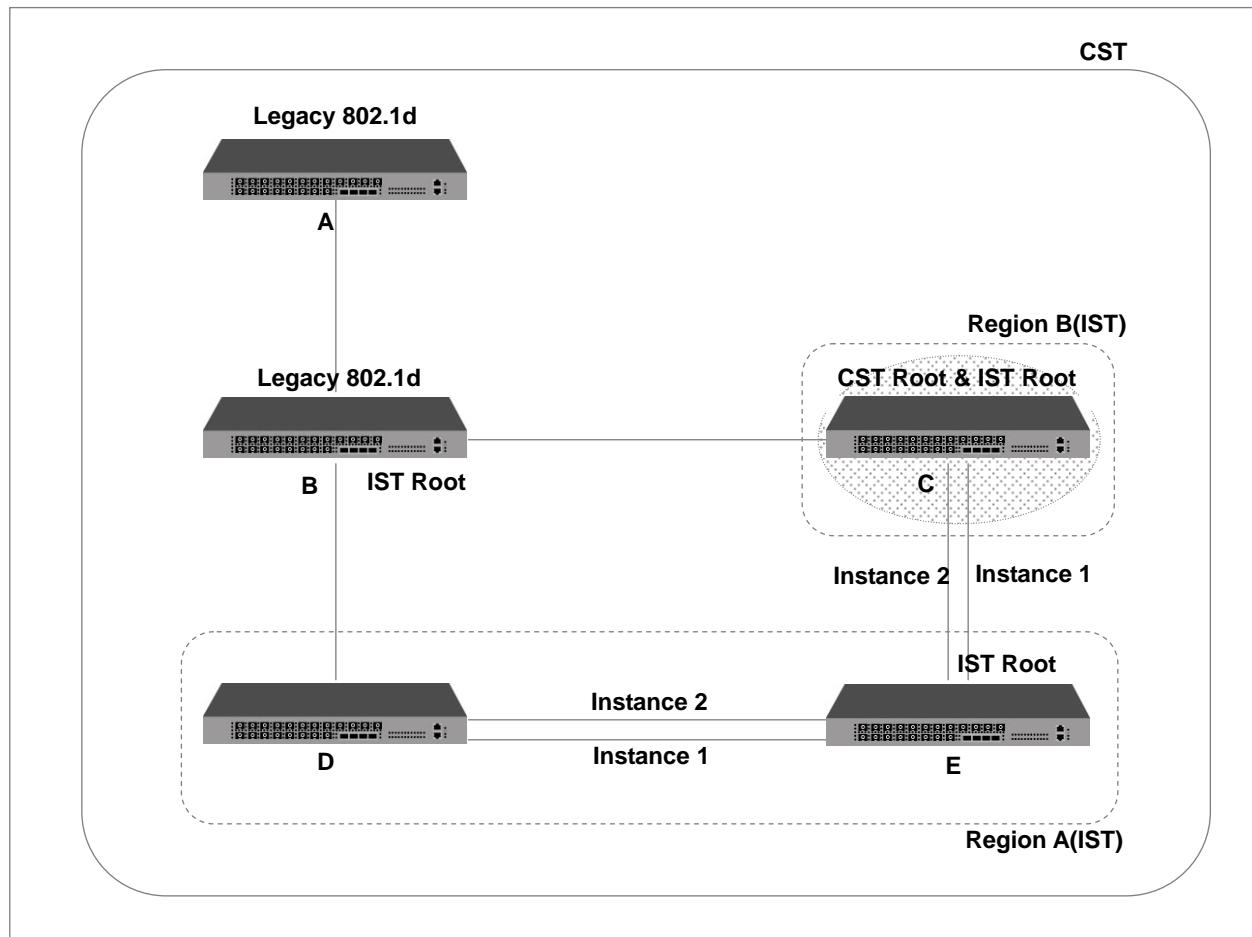


【 그림 8-24 】 MSTP

(2) MSTP

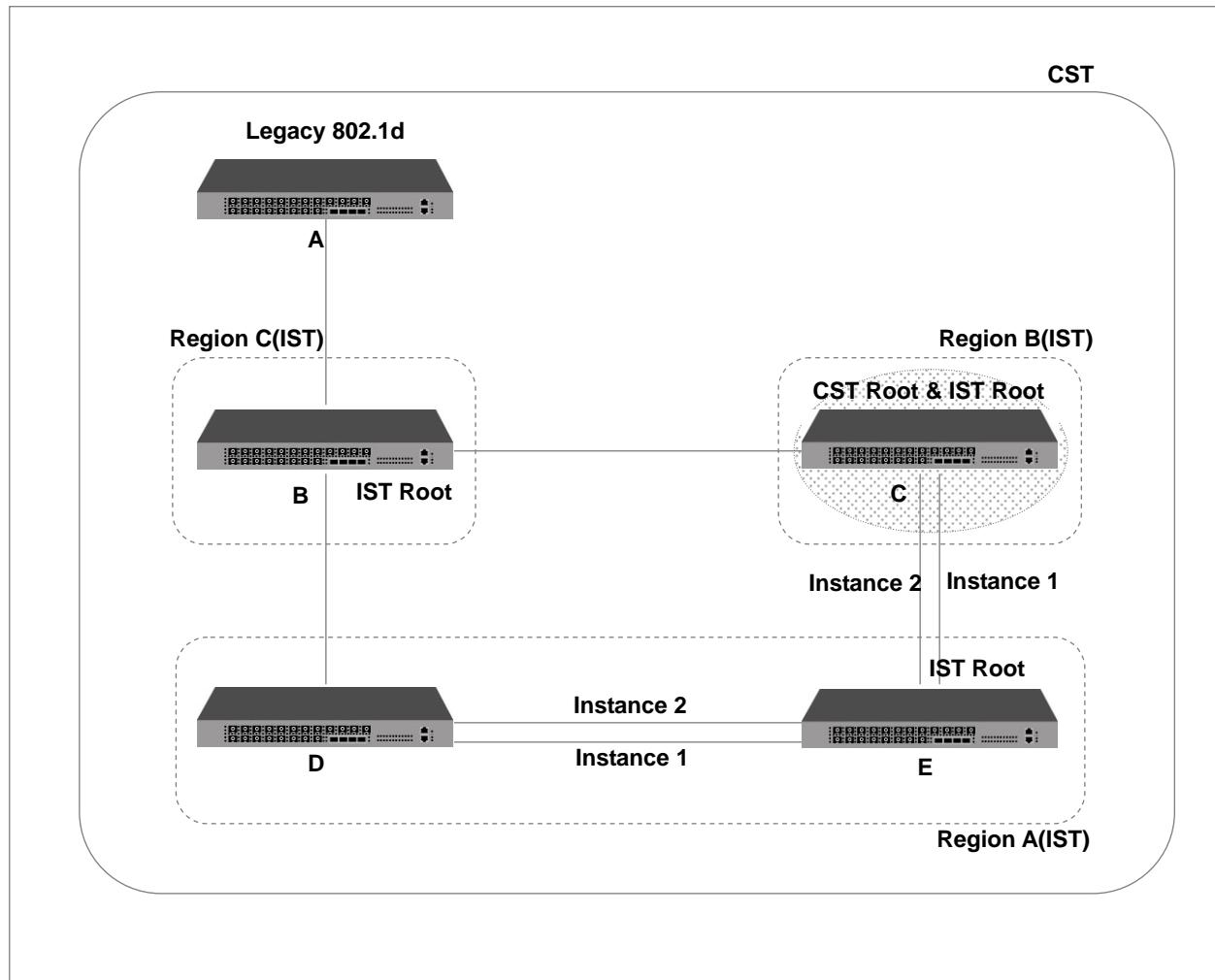
MSTP에서는 동일한 Configuration ID를 가진 그룹으로 VLAN을 나눕니다. Configuration ID는 Revision name, Revision, VLAN map으로 구성됩니다. 따라서 Configuration ID가 동일하기 위해서는 이 세가지가 모두 동일해야 합니다. 이와 같이 동일한 Configuration ID를 가진 그룹으로 나눈 VLAN을 MST Region이라고 합니다.

각 Region에는 오직 하나의 STP가 구동 되기 때문에 PVSTP에 비해 STP수를 줄일 수 있고, 이에 따라 BPDU 트래픽을 줄일 수 있습니다. 하나의 네트워크 환경에서 설정할 수 있는 Region 수는 제한이 없지만, Instance는 최대 64개까지만 생성 할 수 있습니다. 따라서 Instance는 1부터 64까지 설정할 수 있습니다. 각 Region에서 동작하는 Spanning-Tree를 IST(Internal Spanning-Tree)라고 합니다. 그리고, Region의 Spanning-Tree를 각각 연계했을 때 적용되는 Spanning-Tree를 CST라고 합니다. 한편, Instance 0은 VLAN을 그룹으로 묶은 Instance가 존재하지 않는 상태, 즉 MSTP로 동작하지 않는 상태를 의미합니다. 따라서 모든 장비의 포트는 Instance 0이 존재한다고 할 수 있습니다. MSTP 동작이 시작되면, CST 내부에 있는 모든 장비는 BPDU를 주고 받게 되고, 서로의 BPDU를 비교하여 CST Root 장비가 정해집니다. 이 때, MSTP로 동작하지 않는 장비들도 Instance 0을 가지고 있기 때문에 MSTP로 동작하지 않는 장비들도 BPDU 교환에 동참할 수 있습니다. 이와 같이 CST Root 장비를 정하기 위한 동작을 CIST(Common & Internal Spanning-Tree)라고 합니다.



【 그림 8-25 】 MSTP의 CST와 IST①

위의 그림을 살펴보면, 어떤 CST 안에서 A와 B는 기존 STP로 동작하는 장비이고, C,D,E는 MSTP로 동작하는 장비입니다. 일단 CST에서는 CST Root를 정하기 위한 CIST가 이루어지고, CST Root가 결정되면, CST Root와 가장 가까운 장비들이 Region의 IST Root로 결정됩니다. 이 때, CST Root가 속해있는 IST 내에서는 CST Root가 곧 IST Root가 됩니다.



【 그림 8-26 】 MSTP의 CST와 IST②

위와 같은 상황에서 B가 MSTP로 동작하기 시작한다면, B는 자신이 CST Root가 될 것을 요청하기 위해 자신의 BPDU를 CST Root 와 IST Root로 보냅니다. 그러나, 만약 B보다 우선 순위가 높은 BPDU가 전달된다면, B는 CST Root이 될 수 없습니다.

V5812G는 MSTP를 설정하는 명령어를 STP와 RSTP를 설정할 때도 공통적으로 사용하고 있고, PVSPT를 설정하는 명령어는 PVRSTP를 설정할 때에도 사용하고 있습니다.

8.3.4. STP/RSTP/MSTP/PVSTP/PVRSTP 모드 설정

V5812G에 STP를 설정하시려면 우선 어떤 모드를 선택할 것인지 Force-version을 설정해야 합니다. 사용자의 장비에서 Force-version을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp force-version {stp rstp mstp pvstp pvrstp }	Bridge	해당 Bridge에 Force-version을 설정합니다.

사용자의 장비에서 STP 설정을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no stp force-version	Bridge	STP 설정을 해제합니다.

8.3.5. STP/RSTP/MSTP 설정

(1) STP/RSTP/MSTP 활성화

사용자가 Force-version에서 선택한 기능 중 STP, RSTP, MSTP를 활성화하려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp mst enable	Bridge	STP, RSTP, 또는 MSTP 기능을 활성화 시킵니다.



사용자가 Force-version에서 STP를 선택한 후에 위의 명령어를 사용하면 STP가 활성화되고, RSTP를 선택한 후에 위의 명령어를 사용하면 RSTP가 활성화 됩니다. 마찬가지로 MSTP를 설정 하면 MSTP가 활성화 되는 것입니다.

이중 경로가 존재하지 않는 LAN에 속해 있는 장비에는 굳이 STP 기능을 설정하지 않아도 루프 현상은 발생하지 않습니다. 사용자의 장비에서 설정했던 STP, RSTP, 또는 MSTP를 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp mst disable	Bridge	VLAN에서 STP, RSTP, 또는 MSTP를 비활성화 시킵니다.

(2) Root 설정

STP, RSTP, 또는 MSTP 기능을 실행시키기 위해서는 우선, Root 장비가 정해져야 합니다. STP나 RSTP에서는 Root 장비가 되는 것이고, MSTP에서는 IST Root 장비가 되는 것입니다. 각 장비는 자신의 Bridge ID를 가지고 있으며 동일한 LAN에 존재하는 장비의 Bridge ID를 비교하여 Root 장비를 결정합니다. 그러나, V5812G는 사용자의 요구에 따라 Priority를 설정하면 인위적으로 Root 장비를 변경할 수도 있습니다. Priority가 변경되면 가장 작은 Priority가 Root 장비로 결정되도록 재설정됩니다.

장비에 Priority를 설정하여 인위적으로 Root 장비를 변경하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp mst priority mstid_range <0-61440>	Bridge	장비의 Priority를 설정합니다.
no stp mst priority mstid_range		장비의 설정된 Priority를 해제합니다.



참 고

*mstid_range*는 Instance의 번호를 입력합니다. 따라서 0부터 64까지 입력 가능합니다.



주 의

STP와 RSTP의 Priority를 설정할 경우에는 *mstid_range*가 「0」이 됩니다.



주 의

Priority는 4096의 배수로 입력해야 합니다.



참 고

V5812G는 기본적으로 Priority가 32768로 설정되어 있습니다.

(3) Path-cost 설정

Root 장비가 결정된 후에는 어떤 경로로 패킷을 전송할지를 정해야 합니다. 이 때 path-cost를 기준으로 경로가 결정되는데 기본적으로 path-cost는 장비의 LAN 인터페이스 전송 속도로 값이 정해지게 되어 있습니다. 다음은 LAN 인터페이스의 전송 속도에 따라 정해진 path-cost 값입니다.

**주 의**

STP와 RSTP의 설정 방법은 동일하지만 각 전송 속도에 따른 path-cost 값은 완전히 다릅니다. 따라서 주의하시기 바랍니다.

【 표 8-1 】 STP path-cost

전송 속도	Path-cost
4M	250
10M	100
100M	19
1G	4
10G	2

【 표 8-2 】 RSTP의 path-cost

전송 속도	Path-cost
4M	20,000,000
10M	2,000,000
100M	200,000
1G	20,000
10G	2,000

path-cost를 기준으로 선택된 경로가 과부하 상태에 빠졌을 경우, 사용자는 다른 경로를 선택하는 것이 좋습니다. 이러한 여러 상황을 고려하여 V5812G는 사용자가 필요에 따라 인위적으로 경로를 지정할 수 있도록 Root 포트의 path-cost를 마음대로 설정할 수 있습니다.

Path-cost를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp mst path-cost mstid_range port-number <1-200000000>	Bridge	인위적으로 경로를 설정할 수 있도록 Path-cost를 설정합니다.
no stp mst path-cost mstid_range port-number		설정한 Path-cost 를 해제합니다.



참 고

*mstid_range*는 Instance의 번호를 입력합니다. 따라서 0부터 64까지 입력 가능합니다.



주 의

STP와 RSTP의 Priority를 설정할 경우에는 *mstid_range*가 「0」이 됩니다.

(4) Port-priority 설정

두 경로의 path-cost를 비롯한 모든 기준이 동일할 경우 최종적으로 경로를 선택하는 기준은 port-priority입니다. 이 때 port-priority도 사용자의 요구에 따라 설정, 경로를 인위적으로 선택할 수 있습니다. Port-priority를 설정하려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp mst port-priority <i>mstid_range port-number <0-240></i>	Bridge	포트의 우선 순위 값을 설정합니다.
no stp mst port-priority <i>mstid_range port-number</i>		설정된 우선 순위값을 해제합니다.



참 고

*mstid_range*는 Instance의 번호를 입력합니다. 따라서 0부터 64까지 입력 가능합니다.



주 의

STP와 RSTP의 Priority를 설정할 경우에는 *mstid_range*가 「0」이 됩니다.



주 의

Priority는 16의 배수로 입력해야 합니다.



참 고

V5812G는 기본적으로 Priority가 128로 설정되어 있습니다.

(5) MST Region 설정

V5812G에 만일 MSTP를 설정하였다면, MST Configuration ID를 설정하여 장비가 어떤 MST Region에 속하게 될 것인지를 결정합니다.

이 때, Configuration ID에는 Revision name, Revision, VLAN map이 속하게 됩니다. Configuration ID를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp mst config-id name name	Bridge	해당 Region의 이름을 지정합니다.
stp mst config-id map <1-64> vlan-range		하나의 Region으로 그룹화할 VLAN의 범위를 설정합니다.
stp mst config-id revision <0-65535>		같은 MST boundary 안의 장비들은 모두 같은 revision number로 설정합니다.

참 고

한 네트워크 환경에서 MST Region의 수를 설정 하는 데는 제한이 없으나, instance는 최대 64개까지만 생성 할 수 있습니다.

참 고

STP와 RSTP로 설정할 경우에는 Configuration ID를 설정할 필요가 없습니다. 설정하면, 오류 메시지가 출력됩니다.

한편, 설정한 Configuration ID를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no stp mst config-id	Bridge	설정했던 Configuration ID를 모두 삭제합니다.
no stp mst config-id name		Region의 이름을 삭제합니다.
no stp mst config-id map <1-64> [vlan-range]		VLAN-map의 전체 또는 특정 부분을 삭제합니다.
no stp mst config-id revision		설정된 revision number를 삭제합니다.

V5812G는 Configuration ID를 설정한 후에 장비에 설정한 내용을 적용시켜야 합니다. 설정한 내용을 변경하거나 설정한 내용을 삭제한 후에도 그 내용을 적용하지 않으면 변경된 내용이 장비에 반영되지 않습니다. Configuration ID를 설정한 후 그 내용을 장비에 적용하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp mst config-id commit	Bridge	해당 Region의 설정내용을 실행합니다.



주 의

설정한 Configuration ID를 삭제한 후에도 위의 명령어를 사용하여 장비에 삭제한 내용을 적용해야 합니다.

(6) 설정 내용 확인

STP, RSTP 또는 MSTP를 설정하고, 설정한 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show stp	Enable/ Bridge	STP/RSTP/MSTP 관련 설정을 확인합니다.
show stp mst		MSTP로 설정했을 때의 설정을 확인합니다.
show stp mst mstid_range		특정 Instance의 설정을 확인합니다.
show stp mst mstid_range all [detail]		모든 포트에 대한 특정 Instance의 설정을 확인합니다.
show stp mst mstid_range port-number [detail]		특정 포트에 대한 특정 Instance의 설정을 확인합니다.



참 고

「**show stp**」 명령어는 STP/ RSTP/MSTP에 대한 정보를 모두 확인할 수 있습니다. 구별하는 방법은 「**mode**」에 어떤 것이 명시되어 있는지 확인하시면 됩니다.



주 의

V5812G가 STP나 RSTP로 설정되어 있을 경우에는 *mstid_range*를 「0」으로 설정해야 합니다.

한편, 장비에 MSTP를 설정하였을 경우, Configuration ID를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show stp mst config-id current	Bridge	현재 적용되어 있는 Configuration ID를 확인합니다.
show stp mst config-id pending		장비에서 가장 최근에 설정한 Configuration ID를 확인합니다.

예를 들어, 사용자가 Configuration ID를 설정한 후 **stp mst config-di commit**라는 명령어로 장비에 적용시켰다면 해당 Configuration ID는 **show stp mst config-id current**와 **show stp mst config-id pending**에서 모두 확인됩니다. 그러나, 설정 후 **stp mst config-di commit**라는 명령어로 장비에 적용하지 않았다면 해당 설정은 **show stp mst config-id pending**으로만 확인할 수 있고, **show stp mst config-id current**에서는 이전에 설정하여 적용한 설정 내용이 확인됩니다.

8.3.6. PVSTP/PVRSTP 설정

(1) PVST/PVRSTP 활성화

사용자가 Force-version에서 선택한 기능 중 PVSTP나 PVRSTP를 활성화하려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp pvst enable <i>vlan-range</i>	Bridge	PVSTP 또는 PVRSTP 기능을 활성화 시킵니다.



사용자가 Force-version에서 PVSTP를 선택한 후에 위의 명령어를 사용하면 PVSTP가 활성화되고, PVRSTP를 선택한 후에 위의 명령어를 사용하면 PVRSTP가 활성화 됩니다.



*vlan-range*는 VLAN 이름이나 정수로 입력할 수 있습니다. 정수를 입력할 때에는 「-」 기호를 사용하여 연속적으로 입력할 수 있습니다.



PVSTP와 PVRSTP는 현재 존재하는 VLAN에 대해서만 설정할 수 있습니다. 존재하지 않은 VLAN을 입력하면 오류 메시지가 출력됩니다.

이중 경로가 존재하지 않는 LAN에 속해 있는 장비에는 굳이 STP 기능을 설정하지 않아도 루프 현상은 발생하지 않습니다. 사용자의 장비에서 설정했던 PVSTP 또는 PVRSTP를 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp pvst disable	Bridge	VLAN에서 STP, RSTP, 또는 MSTP를 비활성화 시킵니다.

(2) Root 설정

PVSTP 또는 PVRSTP 기능을 실행시키기 위해서는 우선, Root 장비가 정해져야 합니다. 각 장비는 자신의 Bridge ID를 가지고 있으며 동일한 LAN에 존재하는 장비의 Bridge ID를 비교하여 Root 장비를 결정합니다.

그러나, V5812G는 사용자의 요구에 따라 Priority를 설정하면 인위적으로 Root 장비를 변경할 수도 있습니다. Priority가 변경되면 가장 작은 Priority가 Root 장비로 결정되도록 재설정됩니다. 장비에 Priority를 설정하여 인위적으로 Root 장비를 변경하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp pvst priority <i>vlan_range <0-61440></i>	Bridge	장비의 Priority를 설정합니다.



*mstid_range*는 Instance의 번호를 입력합니다. 따라서 0부터 64까지 입력 가능합니다.



Priority는 4096의 배수로 입력해야 합니다.



V5812G는 기본적으로 Priority가 32768로 설정되어 있습니다.

(3) Path-cost 설정

Root 장비가 결정된 후에는 어떤 경로로 패킷을 전송할지를 정해야 합니다. 이 때 Path-cost를 기준으로 경로가 결정되는데 기본적으로 Path-cost는 장비의 LAN 인터페이스 전송 속도로 값이 정해지게 되어 있습니다.

Path-cost를 기준으로 선택된 경로가 과부하 상태에 빠졌을 경우, 사용자는 다른 경로를 선택하는 것이 좋습니다. 이러한 여러 상황을 고려하여 V5812G는 사용자가 필요에 따라 인위적으로 경로를 지정할 수 있도록 Root 포트의 Path-cost를 마음대로 설정할 수 있습니다. Path-cost를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp pvst path-cost <i>vlan_range port-number <1-200000000></i>	Bridge	인위적으로 경로를 설정할 수 있도록 Path-cost를 설정합니다.



*mstid_range*는 Instance의 번호를 입력합니다. 따라서 0부터 64까지 입력 가능합니다.

(4) Port-priority 설정

두 경로의 path-cost를 비롯한 모든 기준이 동일할 경우 최종적으로 경로를 선택하는 기준은 port-priority입니다. 이 때 port-priority도 사용자의 요구에 따라 설정, 경로를 인위적으로 선택할 수 있습니다. Port-priority를 설정하려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp pvst port-priority <i>vlan_range port-number <0-240></i>	Bridge	포트의 우선 순위 값을 설정합니다.



*mstid_range*는 Instance의 번호를 입력합니다. 따라서 0부터 64까지 입력 가능합니다.



Priority는 16의 배수로 입력해야 합니다.



V5812G는 기본적으로 Priority가 128로 설정되어 있습니다.

(5) PVST/PVRSTP 설정 내용 확인

PVSTP나 PVRSTP를 설정하고, 설정한 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show stp	Bridge	STP/RSTP/MSTP 관련 설정을 확인합니다.
show stp pvst <i>vlan_range</i>		MSTP로 설정했을 때의 설정을 확인합니다.
show stp pvst <i>vlan_range all [detail]</i>		모든 포트에 대한 특정 Instance의 설정을 확인합니다.
show stp pvst <i>vlan_range port-number [detail]</i>		특정 포트에 대한 특정 Instance의 설정을 확인합니다.



「**show stp**」 명령어는 PVSTP/PVRSTP에 대한 정보를 모두 확인할 수 있습니다. 구별하는 방법은 「**mode**」에 어떤 것이 명시되어 있는지 확인하시면 됩니다.

8.3.7. BPDU 설정

BPDU란 STP/RSTP/MSTP를 설정, 유지하기 위해서 LAN에 이용되는 전송 메시지입니다. STP 기능이 설정된 장비들은 최적의 경로를 파악하기 위해 BPDU라는 자신의 정보를 서로 교환합니다. 이 때 사용자는 정보를 주고 받는 시간 간격 등 다음과 같은 내용들을 설정할 수 있습니다. MSTP BPDU는 일반적인 STP BPDU와 그것의 끝에 추가적인 MST 데이터를 지닌 것 입니다. BPUD의 MSTP 부분은 Region의 영역을 벗어날 경우 남아있지 않습니다.

◆ Hello time

Hello time은 장비가 BPDU를 전송하는 간격을 나타내는 시간으로 1초부터 10초까지 설정할 수 있습니다. 기본적으로 설정되어 있는 Hello Time은 2초 입니다.

◆ 유효 시간 (Max Age)

Root 장비는 다른 장비들이 보내주는 정보를 토대로 매번 새로운 정보를 송신합니다. 그러나 네트워크에 많은 장비들이 연결되어 있다면 BPDU를 전달하는데 상당한 시간이 걸립니다. 그리고 BPDU를 전달하는 동안에 네트워크 연결 상태가 변경되면 해당 정보는 더 이상 효력이 없게 됩니다. BPDU에 의해 전달된 STP 정보의 유효시간을 Max Age라고 합니다.

◆ 패킷 전송 시간 (Forward Delay)

STP에서는 포트 상태는 Blocking, Listening, Learning, Forwarding의 네 가지로 정의된다고 앞에서 말한 바 있습니다. BPDU에는 Listening과 Learning 상태에서 Forwarding의 상태에 이르기까지 걸리는 시간을 명기할 수 있습니다. 이 때, 포트 상태를 변화시키는데 걸리는 시간 간격을 Forward Delay라고 합니다.



참 고

BPDU 설정은 Force-version에서 선택한 기능에 대한 것으로 적용됩니다. STP, RSTP 그리고 MSTP가 동일한 명령어를 사용하고, PVSTP와 PVRSTP가 동일한 명령어를 사용합니다.

여기에서는 BPDU 설정에 대하여 다음과 같이 설명합니다.

- Hello Time 설정
- Forward Delay 설정

- Max Age 설정
- BPDU Hop 설정
- BPDU 설정 내용 확인

(1) Hello time 설정

Hello 타임은 장비가 경로 메시지를 전송하는 시간 간격을 결정합니다. Hello time을 설정하려면, Bridge 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp mst hello-time <1 – 10>	Bridge	STP, RSTP 또는 MSTP에서 장비가 경로 메시지를 전송하는 시간을 설정합니다.
stp pvst hello-time vlan-range <1 – 10>		PVST 또는 PVRSTP에서 장비가 경로 메시지를 전송하는 시간을 설정합니다.



기본적으로 Hello Time이 2초로 설정되어 있습니다.

설정된 hello-time을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no stp mst hello-time	Bridge	장비가 경로 메시지를 전송하는 시간을 설정을 해제합니다.
no stp pvst hello-time vlan-range		

(2) Forward Delay 설정

포트 상태가 Listening에서 Forwarding의 상태에 이르기 까지 걸리는 시간인 Forward Delay를 설정할 수 있습니다. Forward Delay를 설정하려면, Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp mst forward-delay <4-30>	Bridge	STP, RSTP 또는 MSTP에서 Forward-delay 지정합니다.
stp pvst forward-delay vlan-range <4-30>		PVST 또는 PVRSTP에서 Forward-delay 지정합니다.



참 고

기본적으로 Forward-delay가 15초로 설정되어 있습니다.

사용자가 설정한 forward-delay를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no stp mst forward-delay		설정된 Forward-delay 해제합니다.
no stp pvst forward-delay <i>vlan-range</i>	Bridge	

(3) Max age 설정

Max age는 경로 메시지가 얼마동안 유효한지를 나타냅니다. 효력을 잃은 메시지들을 처리하기 위해 Max age를 설정 합니다.

명령어	모 드	기 능
stp mst max-age <6~40>		STP, RSTP 또는 MSTP에서 경로 메시지의 Max age를 설정합니다.
stp pvst max-age <i>vlan-range</i> <6~40>	Bridge	PVST 또는 PVRSTP에서 Max age를 설정합니다.



기본적으로 Max age가 20초로 설정되어 있습니다.



주 의

Max Age는 Forward delay의 두배 보다 작게, Hello Time의 두 배보다 크도록 설정할 것을 권장합니다.

사용자가 설정한 Max age를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no stp mst max-age		설정한 경로 메시지의 Max age를 해제합니다.
no stp pvst max-age <i>vlan-range</i>	Bridge	

(4) BPDU Hop 설정

MSTP를 사용할 때에는 BPDU가 한 없이 떠도는 것을 방지하기 위해 BPDU가 갈 수 있는 Hop 수를 지정할 수 있습니다. 이 기능을 설정하면 MSTP의 BPDU는 지정된 Hop 수 만큼의 장비만 거쳐 갑니다.

MSTP에서 BPDU의 Hop 수를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp mst max-hops <1-40>	Bridge	MSTP에서 BPDU의 Hop 수를 설정합니다.

MSTP에서 BPDU의 Hop 수를 설정했던 것을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no stp mst max-hops	Bridge	MSTP에서 설정했던 BPDU의 Hop 수를 삭제합니다.

(5) BPDU 설정 내용 확인

BPDU 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show stp mst	Enable /Global	STP, RSTP 또는 MSTP의 BPDU 설정내용을 확인할 수 있습니다.
show stp pvst vlan-range	/Bridge	PVSTP나 PVRSTP의 BPDU 설정내용을 확인할 수 있습니다.

8.3.8. BPDU Filtering 설정

BPDU Filtering은 STP가 활성화되어 있는 포트에서의 BPDU 패킷 전송을 제한합니다. BPDU Filtering이 활성화되어 있는 포트는 STP가 비활성화 되어 있는 것처럼 동작하기 때문에, 수신된 BPDU를 인식하지 않으며, 다른 포트로 이 패킷을 전송하지도 않습니다.



주의

업링크 포트에는 BPDU Filtering을 활성화하지 마십시오. 네트워크 서비스가 중단될 수 있습니다.

BPDU Filtering을 설정하시려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp bpdu-filter enable port-number	Bridge	BPDU Filtering을 활성화합니다.
stp bpdu-filter disable port-number		BPDU Filtering을 비활성화합니다.
show running-config include bpdu-filter	Enable / Global / Bridge	BPDU Filtering 설정을 확인합니다.



BPDU Filtering은 기본적으로 비활성화 되어 있습니다.



*port-number*는 한번에 여러 개를 입력할 수 있습니다. 각 입력값 사이를 빈칸 없이 쉼표(,)로 구분하거나, 입력 범위의 처음과 마지막 값을 빈칸 없이 이음표(~)로 연결하여 복수의 *port-number*를 입력하십시오.

8.3.9. Point-to-Point MAC 설정

STP 운영상 1:1 연결이 아닌 shared edge 포트로 연결이 되어 있는 경우 한 장비에서 보낸 BPDU가 두 장비에서 받게 될 수 있으며 그로 인해 STP 운영의 Rapid transition이 가능한지에 대한 확신을 가질 수 없게 될 것이다. 링크 타입을 결정하기 위해서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp point-to-point-mac port-number {auto force-false force-true}	Bridge	링크 타입을 결정합니다.
no stp point-to-point-mac port-number		링크 타입을 해제합니다.



“auto”는 장비가 자동으로 링크 타입이 point-to-point인지 shared 링크 타입 인지를 결정하는 것입니다. Full-duplex로 포트 링크가 성립되어 있을 경우 point-to-point 링크 타입으로 간주하며 half-duplex로 성립되어 있는 경우 shared 링크 타입으로 간주합니다.

“force-false”는 한 개의 인터페이스가 두개 또는 그 이상의 브릿지로 연결되어 있을 때 사용하는 것으로 관리자가 강제적으로 링크 타입을 shared 링크로 설정 할 때 사용하며 항상 shared 링크로 연결되어 있다고 간주합니다.

8.3.10. STP 모드 변경 감지

사용자는 다음 명령어로 트리 내의 다른 노드들의 STP 모드 변경 여부를 확인하고, 그에 따라 해당 포트의 BPDU 버전이 조정되도록 할 수 있습니다. 명령어가 실행되고 나서 두번째로 수신된 BPDU를 참조하여 STP 모드 변경 여부가 감지됩니다.

명령어	모 드	기 능
stp clear-detected-protocol port-number	Bridge	STP 모드 변경 여부를 확인합니다.

8.3.11. STP Guard 설정

(1) Edge Port 설정

STP Edge Port는 STP가 활성화될 필요가 없는 Bridge Port입니다. 그것은 Loop 방지가 해당 포트와 연결된 하단의 장비들에게 필요하지 않거나 STP Neighbor가 해당 포트의 하단에 존재하지 않는 것입니다. RSTP의 경우 Edge Port에 STP를 비활성화 하는 것이 중요합니다.

만약 Edge Port에 대해 RSTP가 비활성화 되어있지 않을 경우, 그러한 포트를 통과하는 패킷으로 인해 Convergence 시간이 초과될 것입니다. 한 포트가 Edge Port로 설정되자 마자, 그것은 즉시 Forwarding상태로 전환됩니다.

RSP에서, Edge Port를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp edge-port port-number	Bridge	해당 포트를 Edge Port로 설정합니다.
no stp edge-port port-number		Edge Port로 설정되었던 것을 해제합니다.

(2) Root Guard 설정

STP 표준에서는 네트워크 내의 Bridge ID가 가장 작은 스위치가 Root가 되도록 규정하고 있습니다. 그렇지만 전원 공급 중단, 새로운 스위치의 추가나 기존 스위치의 제거 등, 네트워크를 구성하고 있는 스위치들이 발생시키는 문제들은 STP 토플로지(Topology)에 영향을 미칩니다. 이러한 현상이 자주 발생하는 경우에는 잣은 STP 토플로지 변경으로 네트워크가 불안정해집니다.

V5812G에서는 Root를 스위치를 사용자가 직접 설정한 후, STP에 의해 변경되지 않도록 함으로써, 보다 안정적으로 STP가 운영될 수 있도록 합니다. 사용자에 의해 Root로 설정된 스위치에 Superior 메시지가 수신되면, 메시지를 보낸 스위치는 Blocking 상태로 바くなります. Forward Delay동안 이 스위치에 BPDU가 수신되지 않으면, 자동으로 Blocking 상태가 해제됩니다.

Root-Guard로 고정 Root 스위치를 설정하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp mst root-guard mstid_range port-number <1-200000000>	Bridge	MST Root Guard를 활성화합니다.
stp pvst root-guard vlan-range port-number		PVST Root Guard를 활성화합니다.
no stp mst root-guard mstid_range port-number		MST Root Guard를 비활성화합니다.
no stp pvst root-guard vlan-range port-number		PVST Root Guard를 비활성화합니다.

8.3.12. BPDU Guard 설정

네트워크와의 연결이 필요하지만, STP 토플로지(Topology)를 바꿀 가능성이 있는 장비 또는 시스템이 연결되어 있는 포트에 BPDU Guard를 설정하십시오. V5812G는 BPDU Guard를 설정하려는 포트가 Edge Port로 지정되어 있어야 합니다.

Edge Port는 Listening과 Learning을 거치지 않고 바로 Forwarding 상태로 바くなります. Edge Port는 Forwarding 상태로 바뀌자마자 BPDU를 수신합니다. Edge 포트에 BPDU 메시지가 수신되면, 포트가 비활성화되어 현재의 STP 토플로지가 유지될 수 있습니다.

(1) BPDU Guard 활성화

V5812G에 BPDU Guard를 설정하시려면 다음 단계를 따르십시오.

1 단계 BPDU Guard를 적용할 STP Edge Port를 지정하십시오.

명령어	모 드	기 능
stp edge-port port-number	Bridge	해당 포트를 Edge Port로 설정합니다.
no stp edge-port port-number		해당 포트의 Edge Port 설정을 해제합니다.

2 단계 STP Edge Port에 BPDU Guard를 활성화합니다.

명령어	모 드	기 능
stp bpdu-guard	Bridge	BPDU Guard를 활성화합니다.
no stp bpdu-guard		BPDU Guard를 비활성화합니다.

(2) Edge Port 자동 활성화

BPDU Guard에 의해 비활성화된 Edge Port를 일정 시간이 지난 후 자동으로 활성화 시키려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp bpdu-guard auto-recovery	Bridge	Edge Port 자동 활성화를 설정합니다.
no stp bpdu-guard auto-recovery		Edge Port 자동 활성화를 해제합니다.

사용자가 Edge Port 자동 활성화 시간을 지정하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp bpdu-guard auto-recovery-time time	Bridge	Edge Port 자동 활성화 시간을 설정합니다.
no stp bpdu-guard auto-recovery-time		Edge Port 자동 활성화 시간을 해제합니다.



참 고

*time*은 초 단위로 <10 – 1, 000, 000> 사이에서 설정 가능합니다. 기본으로 설정되어 있는 시간은 300초입니다.

(3) Edge Port 수동 활성화

BPDU Guard에 의해 비활성화된 Edge Port를 수동으로 활성화 시키려면, 다음 명령어를 사용하십시오. 명령어가 실행되면서 포트가 활성화됩니다.

명령어	모 드	기 능
stp bpdu-guard err-recovery port-number	Bridge	Edge Port를 수동으로 활성화합니다.



주 의

BPDU Guard에 의해 비활성화된 포트는 Edge 포트 설정을 해제해도 자동으로 활성화되지 않습니다. **port enable port-number** 명령어로 직접 Edge 포트를 활성화 시키십시오.

8.4 Loop 감지 기능

사용자의 장비에 이중 경로가 존재하지 않는다고 해도 네트워크 환경이나 장비에 연결되어 있는 케이블 상태 등에 따라 Loop 현상이 발생할 수 있습니다. 이러한 경우를 방지하기 위해 V5812G는 하단에 연결된 네트워크가 Looping 상태인지 확인하기 위해 주기적으로 Loop 감지 패킷을 전송합니다. 만일 Loop 상태라면 전송된 패킷이 해당 포트에 수신되므로 그에 따른 적절한 조치를 취하게 됩니다.

사용자는 이에 따른 정책들을 설정할 수 있는데 감지 패킷이 수신되는 경우 해당 포트는 Looping 된 것으로 판단하고 Loop 감지 리스트에 해당 객체를 옮기게 됩니다. 이후 사용자의 설정(block) 여부에 따라 해당 포트의 상태를 변경합니다. 만일 해당 포트가 속한 VLAN의 STP 설정이 활성화되어 있다면 blocking 하지 않고 로그만 남깁니다.

여기에서는 Loop 감지 기능에 대해 다음과 같이 설명합니다.

- Loop 감지 기능 활성화
- Loop 감지 포트 설정
- Loop 감지 패킷 전송 시간 설정
- Loop 감지 패킷 전송 소스 MAC 주소 설정
- Loop 감지 설정 확인
- Self-Loop 감지 기능

8.4.1. Loop 감지 기능 활성화

장비에 Loop 감지 기능을 활성화 하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
loop-detect enable	Bridge	Loop 감지 기능을 활성화합니다.
loop-detect disable		Loop 감지 기능을 비활성화합니다.



참조

STP 기능을 비활성화한 후 Loop-detect 기능을 활성화 할 수 있습니다.

8.4.2. Loop 감지 포트 설정

특정한 포트에 Loop 감지 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
loop-detect port-number	Bridge	포트에 Loop 감지 기능을 활성화합니다.
no loop-detect port-number		포트에 Loop 감지 기능을 해제합니다.

Loop 현상이 발생하였을 때, 해당 포트의 트래픽을 blocking 시키고자 한다면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
loop-detect port-number block	Bridge	Looping이 발생했을 때 해당 포트를 차단합니다.
no loop-detect port-number block		Looping이 발생했을 때 해당 포트를 허용하고 로그만 남깁니다.



참조

장비는 기본적으로 Looping이 발생하더라도 트래픽을 허용하도록 설정되어 있으면 로그는 기록에 남깁니다.

8.4.3. Loop 감지 패킷 전송 시간 설정

장비에서 Loop 감지 패킷을 전송하는 간격을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
loop-detect port-number period <1-60>	Bridge	장비에서 보내는 Loop 감지 패킷의 전송 간격을 설정합니다. 장비에 설정되어 있는 기본값은 30초입니다.

Looping이 발생한 후 해당 포트를 Loop 감지 리스트로 옮긴 이후 특정 시간이 지난 후에 다시 리스트로 옮겨 다시 looping 검사를 실시합니다.

이 만료시간을 설정하고자 하면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
loop-detect port-number timer <1-86400>	Bridge	Block된 포트가 풀리고, Looping 상태를 다시 감지하는 시간을 설정합니다.
loop-detect port-number timer 0		해당 포트에 Looping 재감지 시간을 해제합니다.



장비는 timer가 기본적으로 600초(10분)으로 설정되어 있습니다.

한편, V5812G의 사용자는 timer가 동작하기 전에 임의로 Blocking 상태를 해지 할 수 있습니다. 예를 들어 Loop 현상이 발생하여 해당 포트를 Blocking 하였으나, 발생했던 Loop 현상이 복원되어 다시 통신을 시켜야 할 경우가 발생할 수도 있습니다. 이러한 경우 timer에서 설정한 시간 동안 기다릴 필요 없이 사용자가 임의로 Blocking 하도록 설정했던 것을 해지할 수 있습니다.

사용자가 임의로 Loop 상태 및 Blocking 하도록 설정했던 것을 해지하는 경우, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
loop-detect port-number unblock	Bridge	사용자가 임의로 Blocking 하도록 설정했던 것을 해지합니다.

8.4.4. Loop 감지 패킷 전송 소스 MAC 주소 설정

V5812G는 Loop Detection 기능을 설정한 후 주기적으로 전송하는 Detection 패킷의 소스 MAC 주소를 시스템 MAC 주소 또는 일종의 사설 MAC 주소인 LAA(Locally Administered Address) MAC 주소로 설정 할 수 있습니다.

시스템 MAC 주소로 지정한 경우, 장비는 자기 자신의 MAC 주소를 소스 MAC 주소로 하여 Detection 패킷을 전송하고 LAA MAC 주소로 지정하면, 첫 번째 byte의 두 번째 bit를 1로 설정하여 (무조건 02로 시작하게 됨) 전송 합니다. 예를 들어, 장비의 MAC 주소가 00:D0:cb:00:00:01인 경우, LAA MAC 주소로 지정을 하면 소스 MAC 주소는 02:D0:cb:00:00:01로 변경되어 전송 됩니다.

사용자 정의의 소스 MAC 주소로 Detection 패킷을 전송하려는 경우, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
loop-detect srcmac laa	Bridge	Detection 패킷을 전송 할 경우, LAA MAC 주소를 소스 MAC 주소로 사용합니다.
loop-detect srcmac system	Bridge	Detection 패킷을 전송 할 경우, System MAC 주소를 소스 MAC 주소로 사용합니다.



참 고

V5812G는 Detection 패킷을 전송할 경우, 기본적으로 System MAC 주소를 소스 MAC 주소 사용하도록 설정되어 있습니다.



참 고

Detection 패킷의 소스 MAC 주소를 변경하기 위해서는 먼저 **loop-detect disable** 명령어를 사용하여, Loop Detection 기능을 해제해 주십시오.

8.4.5. Loop 감지 설정 확인

Loop 감지 설정을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show loop-detect	Enable/ Global/	Loop 감지에 대한 활성화/ 비활성화 설정 내용을 확인합니다.
show loop-detect {port-number all}	Bridge	개별 포트 또는 모든 포트의 Loop 감지 설정 내용을 확인합니다.

8.4.6. Self Loop 감지 기능

사용자의 장비에 이중 경로가 존재하지 않는다고 해도 네트워크 환경이나 장비에 연결되어 있는 케이블 상태 등에 따라 Loop 현상이 발생할 수 있습니다. 이러한 경우를 방지하기 위해 V5812G는 자신이 내 보낸 패킷이 되돌아 오는 현상을 감지하는 Self Loop 감지 기능을 가지고 있습니다. Self Loop 감지 기능을 활성화 하면, 자신이 내 보낸 패킷이 되돌아올 때 포트를 Blocking 하기 때문에 패킷이 들어오는 것을 막을 수 있습니다.

장비에 Self Loop 감지 기능을 활성화 하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
self-loop-detect enable	Bridge	Self Loop 감지 기능을 활성화합니다.

한편, Self Loop 감지 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
self-loop-detect disable	Bridge	Self Loop 감지 기능을 해제합니다.

Self Loop 감지 기능의 상태를 확인하거나 Loop 현상이 발생한 포트를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show self-loop-detect		Self Loop 감지 기능 상태 및 Loop 현상 발생 여부를 확인합니다.
show self-loop-detect {port-number all}	Bridge	특정 포트 또는 모든 포트에 대해 Self Loop 감지 기능 상태 및 Loop 현상 발생 여부를 확인합니다.

8.5 ERP 설정

ERP(Ethernet Ring Protection)는 메트로 이더넷망에서 발생하는 Loop를 방지하고 빠른 시간 내에 망의 복구를 위해 개발된 프로토콜입니다. V5812G는 이러한 ERP를 구현하여 트래픽 양이 많은 메트로 이더넷 망에서 Loop를 제거하는데 걸리는 시간을 50ms 이하로 단축하였습니다.



주의

ERP와 STP는 동시에 구현될 수 없습니다. STP가 이미 활성화되어 있는 상태에서 ERP를 설정하면, STP는 자동적으로 해제됩니다.

8.5.1. ERP 동작 원리

V5812G에서 동작하는 ERP는 이더넷 Ring에서 발생하는 Link Failure를 검출하고, 이를 다시 복구시키는 동작으로 Loop를 신속하게 방지합니다. 하나의 이더넷 Ring은 두 대 이상의 장비로 구성되며, 각 장비는 RM Node 또는 일반 Node로 설정할 수 있습니다. RM Node는 Link Failure를 검출하고 이를 복구하는 Protection 동작을 관리합니다. 각 이더넷 Ring은 ERP 메커니즘을 이용하여 관리되는 ERP 도메인으로 구별됩니다.

RM Node와 일반 Node는 각자 Primary 포트와 Secondary 포트를 지정해야 하며, 이 포트는 이더넷 Ring 내에서 ERP 메시지를 서로 송수신하는 하나의 통로가 됩니다.

◆ ERP 메시지

ERP 도메인 내에서 RM Node와 일반 Node 사이 송수신되는 ERP 메시지는 5가지로 나눌 수 있습니다.

◊ 일반 Node 메시지

일반 Node가 RM Node에게 전송하는 메시지로 자신의 Link 상태를 알리기 위해 사용합니다.

- **Link Down** : 일반 Node가 자신의 포트의 Link failure를 감지했을 때 전송합니다.
- **Link Up** : 일반 Node가 Link Failure 되었던 포트 상태가 복구되었을 때 전송합니다.

◊ RM Node 메시지

RM Node로 설정된 스위치는 ERP 도메인으로 연결된 이더넷 Ring의 Link를 모니터링하고 보호하는 역할을 합니다. RM Node는 주기적으로 일반 Node들에게 TP(Test Packet)를 보내고, Link Up/Down 메시지를 수신하여 이더넷 Ring안에서의 Link Failure 또는 복구상태를 감지합니다.

- **Test Packets** : 이더넷 Ring에서 Loop 발생 여부를 확인하기 위해 주기적으로 전송합니다.
- **RM Link Down** : 이더넷 Ring의 Link Failure로 인해서 RM Node의 Secondary 포트를 Unblocking하고 이 정보를 일반 Node에게 알리기 위해 전송합니다.
- **RM Link Up** : Link 상태가 정상적으로 복구되었을 때, Secondary 포트를 다시 Blocking 상태로 바꾸고 이 정보를 일반 Node에게 알리기 위해 전송합니다.

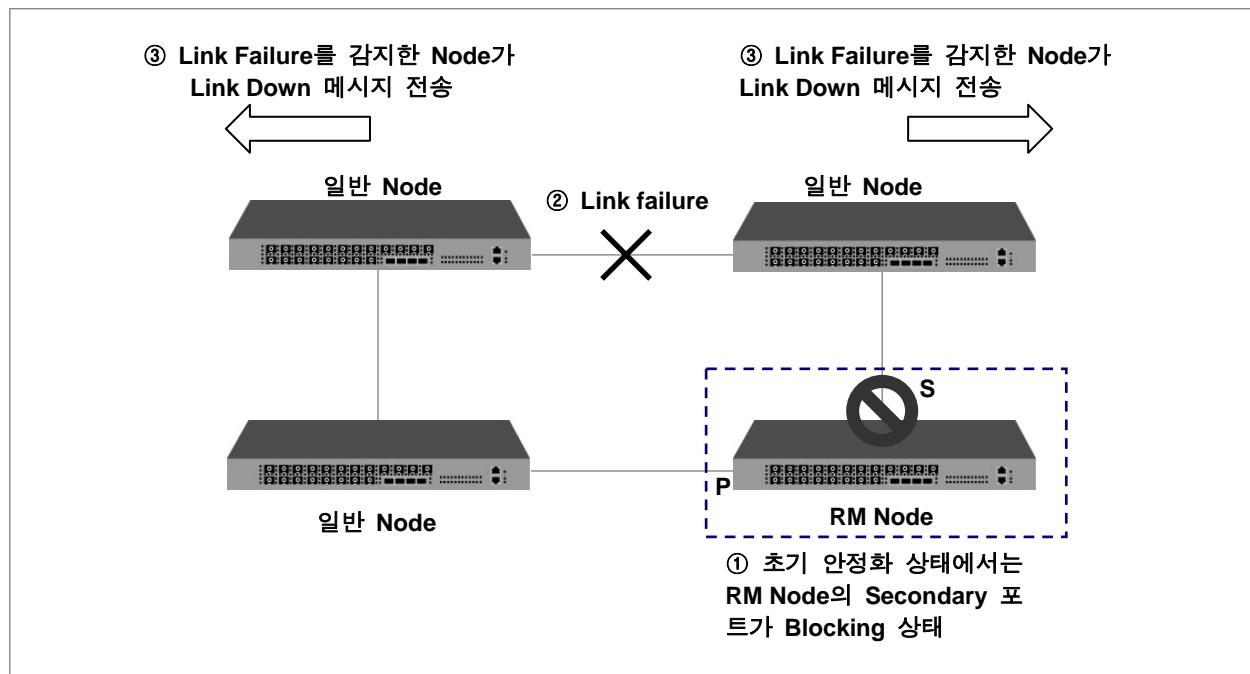


주의

ERP는 이더넷 Ring 토플로지에서만 구현할 수 있습니다..

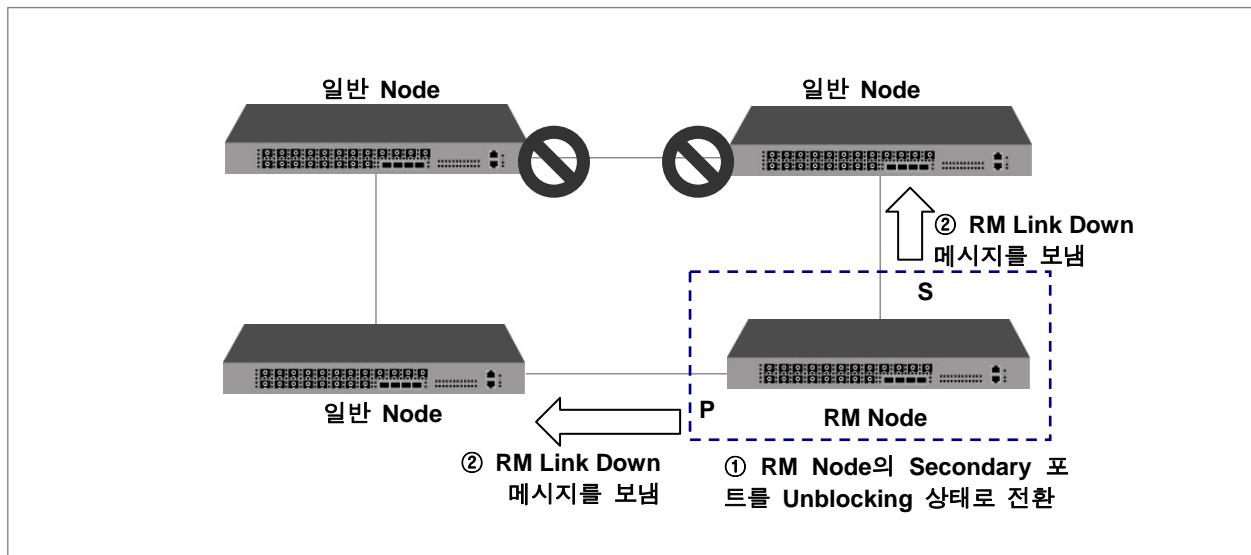
일반적으로 ERP가 동작하고 있는 Ethernet Ring이 안정화된 상태에서는 RM Node의 Secondary 포트가 Blocking 상태를 유지합니다. 이 때, 임의의 곳에서 Link Failure가 발생하게 되면, Link Failure를 감지한 일반 Node들은 Link Down 메시지를 RM Node로 발송하고, Link Failure 상태가 된 포트는 Blocking 상태가 됩니다.

다음 그림은 Link Failure가 발생했을 때의 ERP의 동작 원리를 나타낸 것입니다.



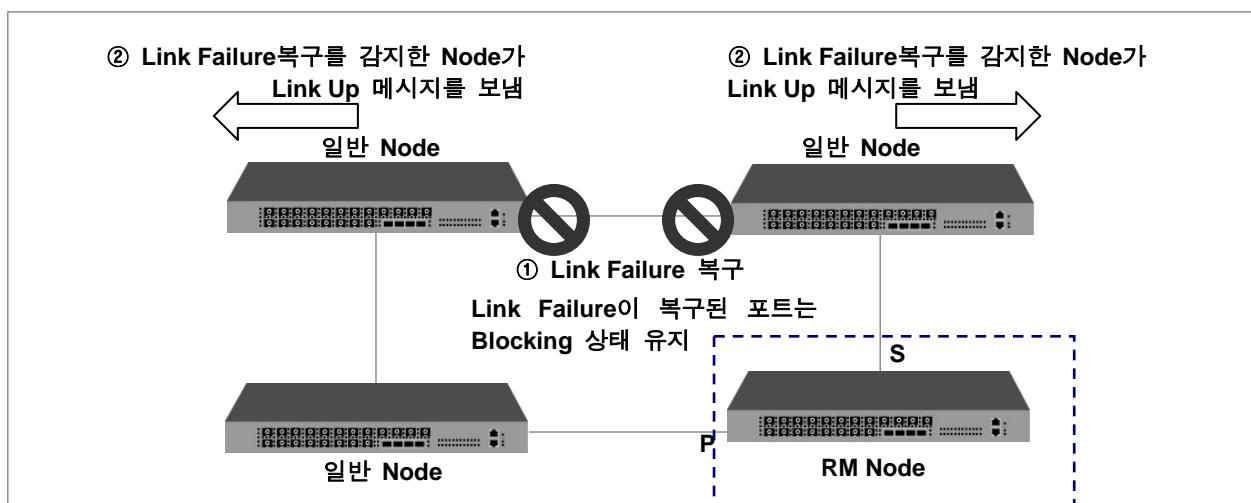
【 그림 8-27 】 Link failure 발생

일반 Node들이 발송한 Link Down 메시지가 RM Node에 전달되면, RM Node는 Blocking 상태였던 Secondary 포트를 Unblocking 상태로 전환시키고, RM Link Down 메시지로 응답하여 Secondary 포트를 통해 통신이 가능함을 알립니다. 그러면, Ethernet Ring은 다시 통신을 재개합니다.



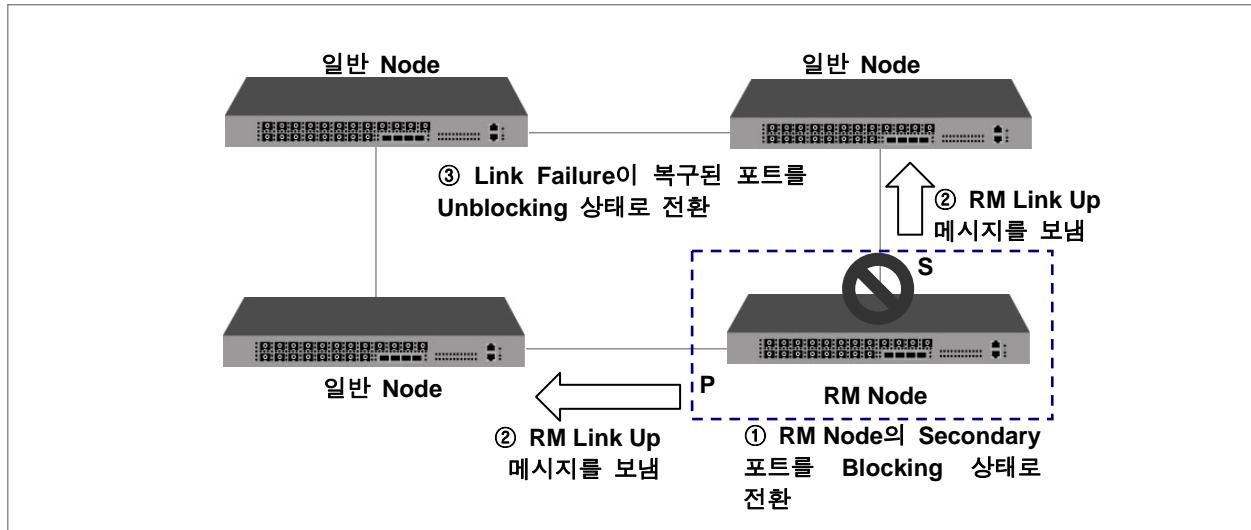
【 그림 8-28 】 Ring Protection

한편, RM Node의 Secondary 포트가 Unblockung 상태가 유지되고 있는 상태에서 Link Failure 상태가 복구되면 Loop가 발생하게 됩니다. Link Failure 상태가 복구되어 해당 포트를 통해 통신이 가능해지면, 이를 감지한 일반 Node들이 RM Node에게 Link Up 메시지를 발송하게 됩니다. 이 때, Link Failure가 복구된 포트는 Blocking 상태는 계속 유지합니다.



【 그림 8-29 】 Link Failure 복구

Link Up 메시지가 RM Node에 수신되면, RM Node는 자신의 Secondary 포트를 다시 Blocking시키고 RM Link Up 메시지를 응답으로 발송합니다. Link Up 메시지를 발송하였던 Node에서 RM Link Up 메시지를 받으면, Link Failure로 복구된 포트를 Unblockung 상태로 전환하여 통신을 재개합니다. 이러한 방법으로 Ethernet Ring은 다시 안정화 상태로 돌아가게 되는 것입니다.



【 그림 8-30 】 Ring Recovery

8.5.2. LOTP (Loss of Test Packet)

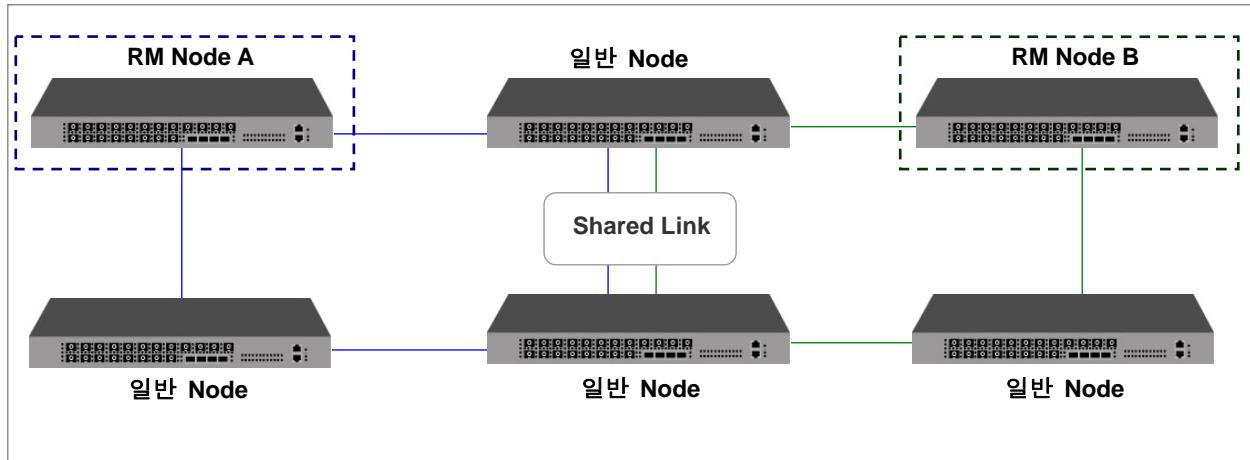
RM Node는 일반 Node의 Link Up/Down 메시지의 정보만으로는 전체 토플로지 상태를 알 수 없기 때문에 주기적으로 TP (Test Packet)을 전송하여 ERP Ring의 Loop 상태를 검출 합니다. RM Node의 두 ERP 포트에서 3번 이상 연속으로 TP가 손실되어 자기 자신으로 되돌아 오지 않은 경우에는 Loop 가 형성되지 않은 것으로 판단하고 이러한 경우는 LOTP(Loss of Test Packet) 상태라고 합니다. 따라서 이러한 경우에는 RM Node가 자신의 Secondary 포트를 Blocking 상태에서 해제합니다.

한편, RM Node가 Ethernet Ring을 통하여 RM Node에게 재수신 되었다면, 이는 Loop가 발생할 수 있는 상태임을 나타냅니다. 따라서 이러한 경우에 RM Node는 Secondary 포트를 Blocking시키게 됩니다.

8.5.3. Shared Link 환경

ERP의 Shared Link 환경이란, 두 개의 도메인이 하나의 Link를 공유하는 환경 즉, 하나의 포트를 두 도메인이 공유하는 것입니다. 만약 두 개의 ERP 도메인이 공유하는 Shared Link Failure가 일어난다면, 심각한 Loop 상태가 야기될 수 있습니다. 이러한 Loop를 방지하기 위해서, Shared link로 서로 연결된 두 개 이상의 ERP Ring은 반드시 서로 다른 우선순위를 가져야 합니다.

가장 높은 우선순위를 가진 도메인은 Shared Link의 상태와 포트들을 관리하게 되며, TP의 흐름은 반드시 낮은 우선순위 도메인에서 높은 도메인으로만 전송될 수 있습니다.



【 그림 8-31 】 Shared Link 환경

8.5.4. ERP 도메인 설정

다음은 ERP를 설정하는 방법에 대해 설명한 것입니다.

(1) ERP ID 설정

ERP를 구현하려면, ERP를 구현할 도메인 아이디를 설정해야 합니다. ERP를 구현할 도메인 ID를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	Function
erp domain domain-id	Bridge	ERP 도메인을 생성합니다.



*domain-id*는 Domain의 Control Vlan ID를 지정하며 1-4094의 범위를 가집니다.

설정한 도메인을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no erp domain {all domain-id}	Bridge	ERP 도메인을 삭제합니다.

(2) ERP 도메인 설명

사용자가 설정한 ERP 도메인에 대한 설명을 입력해 두려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
erp description domain-id description	Bridge	ERP 도메인에 대한 설명을 입력합니다
no erp description domain-id		ERP 도메인에 대한 설명을 삭제합니다

(3) Node 설정

도메인 ID를 설정하였다면, RM Node를 설정하십시오. RM Node를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
erp rmnode domain-id	Bridge	특정 도메인 ID를 RM Node로 설정합니다.

다음 명령어는 RM Node 설정을 해제하고, 일반 Node로 변경할 때 사용하는 명령어입니다.

명령어	모 드	기 능
no erp rmnode domain-id	Bridge	특정 도메인 ID를 일반 Node로 설정합니다.

(4) Primary/Secondary 포트 설정

각 Node의 Primary 포트와 Secondary 포트를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
erp port domain-id primary port-number secondary port-number	Bridge	ERP 도메인의 Primary 포트와 Secondary 포트를 설정합니다.

**주 의**

Primary 포트와 Secondary 포트는 장비의 같은 포트 번호로 사용할 수 없습니다.

8.5.5. Protected Activation 설정

해당 ERP 도메인에 도메인 ID, Primary 포트와 Secondary 포트 등을 설정했다면, 장비 시스템에 이 설정을 적용시키기 위해서는 ERP 도메인을 활성화 시켜야 합니다.

ERP 도메인의 설정을 시스템에 적용시켜 활성화하는 Protected Activation을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
erp activation domain-id	Bridge	특정 ERP 도메인 설정을 활성화합니다.

특정한 ERP 도메인의 Protected Activation 설정을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no erp activation domain-id	Bridge	특정 ERP 도메인 설정을 해제합니다.

8.5.6. Manual Switch to Secondary 설정

한 ERP 도메인에서 장비가 RM Node로 동작할 경우, 설정된 Secondary 포트는 Link Failure가 없는 망에서는 트래픽 흐름을 위해서 Blocking 되어 있습니다. 반면 Primary 포트는 다른 Node로 트래픽을 Forwarding 합니다. 하지만 사용자는 Primary 포트의 역할을 바꿔서 Secondary 포트처럼 동작하게 설정할 수 있습니다.

수동으로 RM Node의 Secondary 포트와 Primary 포트 역할을 서로 바꿔 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
erp ms-s domain-id	Bridge	RM Node의 Secondary 포트와 Primary 포트의 역할을 서로 바꿔 설정합니다.

서로 바뀐 Primary 포트와 Secondary 포트의 역할을 기본 설정으로 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no erp ms-s domain-id	Bridge	Primary 포트와 Secondary 포트의 역할 변경을 해제합니다.

8.5.7. Wait-to-Restore Time 설정

만약 일반 Node의 한 포트가 Link Failure 상태에서 벗어나 망이 복구되었다면, Blocking 상태였던 포트는 트래픽이 Forwarding되는 상태로 바뀌어야 합니다. 그러나, 해당 포트가 RM Node의 Secondary 포트가 Blocking 상태로 변경되기 전에 트래픽 Forwarding을 시작한다면, 망은 Loop 상태가 될 수 있습니다.

Loop를 방지하기 위해서 일반 Node는 RM Link UP 메시지를 받을 때까지 Forwarding을 하지 않고 Blocking 상태를 유지합니다. 이러한 시간을 Wait-to-Restore Time 이라 부르며, 만약 RM Link UP 메시지를 받지 못한다고 하더라도, 결국 Wait-to-Restore Time + (3 x Test Packet 전송 주기) 시간이 지나면 Forwarding을 시작합니다.

Wait-to-Restore Time을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
erp wait-to-restore domain-id <1-720>	Bridge	ERP Wait-to-Restore Time을 설정합니다.

설정한 Wait-to-Restore Time을 Default 값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no erp wait-to-restore domain-id	Bridge	ERP Wait-to-Restore Time을 Default 값으로 설정합니다.

8.5.8. Learning Disable Time 설정

장비에 남겨진 버퍼 정보를 참조하여, 잘못된 MAC Learning 을 방지하기 위해, 설정된 Learning Disable Time 동안 해당 Node는 MAC 주소를 Learning 하지 않습니다.

Learning Disable Time을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
erp learn-dis-time domain-id <0-500>	Bridge	ERP Learning Disable Time을 설정합니다.

설정한 Learning Disable Time을 Default 값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no erp learn-dis-time domain-id	Bridge	ERP Learning Disable Time을 default값으로 변경합니다.

8.5.9. Test Packet Interval 설정

RM Node는 Loop를 확인하기 위해 주기적으로 “Test Packet”을 보냅니다. Test Packet 전송 주기를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
erp test-packet-interval domain-id <10-500>	Bridge	Test Packet 전송 주기를 설정합니다.

설정한 Test Packet Interval을 Default 값으로 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no erp test-packet-interval domain-id	Bridge	설정된 Test Packet 전송 주기를 default 값으로 설정합니다.

8.5.10. ERP Ring 우선순위 정하기

Shared link로 서로 연결된 두 개 이상의 ERP Ring은 반드시 서로 다른 우선순위를 가져야 합니다. 그 이유는 서로 연결된 Shared Link Fail 될 경우 Loop 현상이 나타나기 때문입니다.

가장 높은 우선순위를 가진 도메인은 Shared Link의 포트들을 모니터하게 되며, control packet의 흐름은 반드시 낮은 우선순위 도메인에서 높은 도메인으로만 전송될 수 있습니다.

ERP Ring의 우선순위를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
erp ring-priority domain-id <0-255>	Bridge	ERP Ring의 우선순위를 설정합니다.

ERP Ring의 우선순위를 Default 값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no erp ring-priority domain-id	Bridge	ERP Ring의 우선순위를 default값으로 변경합니다.

8.5.11. LOTP Hold Off Time 설정

ERP ring A와 ERP ring B 사이 Shared Link 가 존재하고 ERP Ring A가 더 높은 우선순위를 가졌다 고 가정해봅시다. 만약 Shared Link가 failure가 된 경우에는 RM Node A 는 Link Down 메시지를 받고 Blocking 상태였던 Secondary 포트를 열어 트래픽을 Forwarding 합니다. 이 때, RM Node B는 RM A를 거쳐 돌아오는 Test packet을 수신하여 LOTP 상태가 발생하지 않아 Secondary 포트의 blocking 상태를 유지하게 됩니다. 그러나 RM Node A가 Secondary 포트를 여는 과정이 3* Test Packet 전송 주기 보다 늦어서, 결국 RM Node B도 LOTP를 감지하여 Secondary 포트를 열게 되면, Loop 가 생기므로 이를 방지하기 위해서 낮은 우선순위를 가진 RM Node B에 Hold Off Time을 설정해야 합니다.

Hold Off Time을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
erp hold-off-time domain-id <1-20000>	Bridge	Hold Off Time을 설정합니다.

설정한 Hold Off Time을 Default 값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no erp hold-off-time domain-id	Bridge	Hold Off Time을 default값으로 변경합니다.

8.5.12. ERP Port Protected

Protected 포트는, 업링크 포트 이외의 포트로부터 들어오는 패킷을 막아 서비스 포트가 오직 업링크 포트와의 통신만 가능하도록 함으로써 사용자의 보안을 보장하면서 인터넷 통신이 가능하도록 해 주는 기능입니다. V5812G는 ERP를 이용하여 Protected Port를 자동으로 설정할 수 있습니다.

즉, ERP가 적용된 네트워크에서 V5812G가 RM Node일 경우에는 사용자가 지정한 포트가 Promiscuous 포트가 되고 나머지 포트는 모두 Protected 포트로 동작합니다. 반면에, Normal Node 일 경우에는 ERP 프로토콜에 의해 지정되는 포트가 Promiscuous 포트가 되고 나머지 모든 포트가 Protected 포트로 동작합니다. 여기에서 Promiscuous 포트는 업링크 포트와 같은 역할을 하며 Protected 포트에서 전송한 트래픽이 Flooding 됩니다. Protected끼리는 트래픽이 Flooding 되지 않으며 오직 Promiscuous 포트로만 트래픽을 전달합니다. 한편, ERP가 동작하지 않는 포트는 모두 Promiscuous 포트로 설정됩니다.

ERP Port Protected를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port protected erp [promiscuous port-number]	Bridge	ERP Port Protected를 설정합니다.



promiscuous 포트를 지정하지 않으면 모든 포트가 Protected 포트로 설정됩니다.



ERP가 활성화되어 있지 않으면 사용자가 설정한 내용에 관계 없이 모든 포트가 Promiscuous 포트로 동작합니다. 따라서, 위의 기능을 사용하려면 먼저 ERP를 활성화하십시오.

ERP Port Protected를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no port protected erp		ERP Port Protected를 해제합니다.
no port protected erp [promiscuous port-number]	Bridge	ERP Port Protected에서 Promiscuous 포트를 삭제합니다.



참 고

Promiscuous 포트만 삭제할 경우 ERP Port Protected가 해제되지 않고, **port protected erp** 명령어를 사용했을 때와 동일하게 모든 포트가 Protected 포트로 설정됩니다.

8.5.13. ERP 트랩 메시지

ERP 트랩 메시지에는 LOTP, ULOTP, Multiple RM, RM node reachability 가 있습니다. 각 트랩 메시지는 다음과 같은 상황에서 전달됩니다.

- (1) **LOTP**는 장비가 RM Node로 설정되어 있을 경우 이 설정이 활성화 되어 있으면, Loss of Test Packet 상태를 알리는 트랩 메시지를 전송합니다.
- (2) **ULOTP**는 장비가 RM Node로 설정되어 있을 경우 이 설정이 활성화 되어 있으면, Unidirectional Loss of Test Packets 상태로 한 방향에서만 LOTP가 발생할 때 트랩 메시지를 전송합니다.
- (3) **Multiple RM**은 장비가 RM Node로 설정되어 있을 경우 이 설정이 활성화 되어 있으면, 하나의 ERP Ring 도메인에 여러 개의 RM Node가 존재할 때 트랩 메시지를 전송합니다.
- (4) **RM Node Reachability** 장비가 일반 Node로 설정되어 있을 경우 이 설정이 활성화 되어 있으면. 동시에 여러 포트가 Link Down되어 RM Node와의 연결이 끊어졌을 때 트랩 메시지를 전송합니다.

ERP Trap 메시지 전송을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
erp trap domain-id { lotp ulotp multiple-rm rmnode-reachability }	Bridge	ERP 트랩 메시지 전송을 활성화합니다

ERP Trap 메시지 전송을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no erp trap domain-id { lotp ulotp multiple-rm rmnode-reachability }	Bridge	ERP 트랩 메시지 전송을 해제합니다

8.5.14. ERP 설정 확인

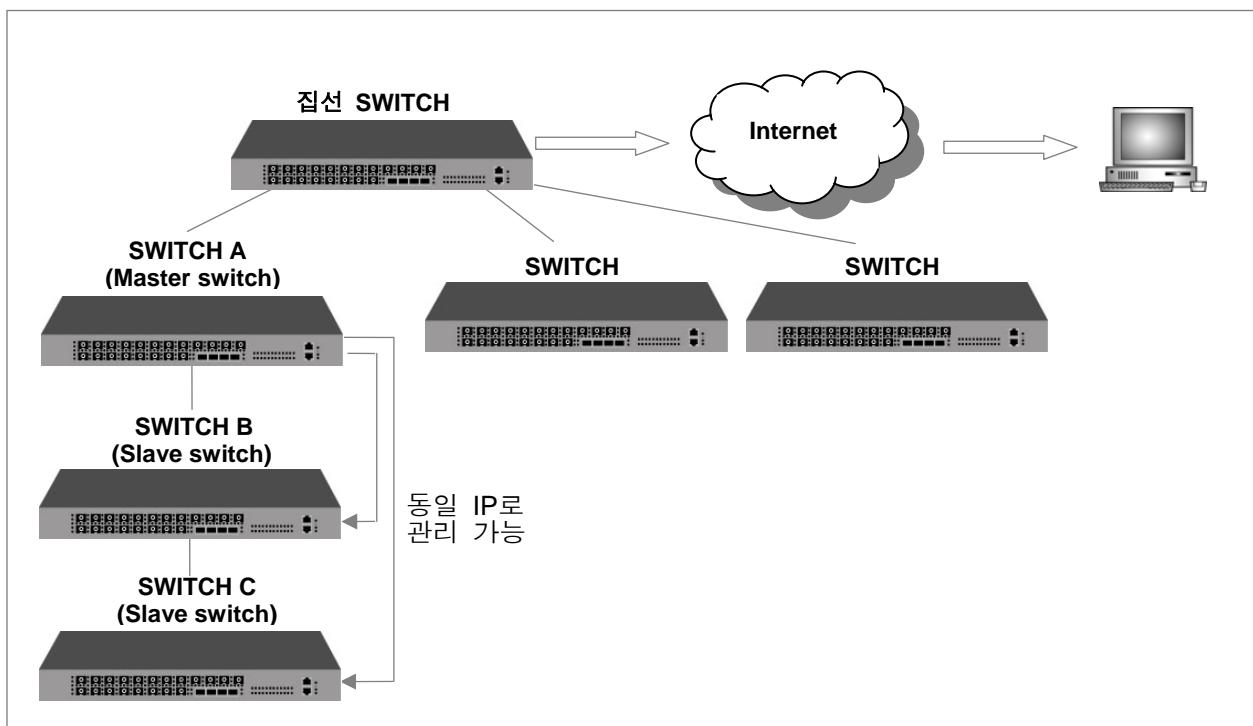
ERP에 관련된 설정 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show erp {all domain-id}	Enable/Global/Bridge	ERP에 대한 정보를 보여줍니다.

8.6 스택킹 설정

스택킹이란 하나의 IP 주소로 여러 대의 장비를 관리 할 수 있는 기능입니다. 사용 가능한 IP는 한 정 되어 있고 관리해야 할 장비는 많은 상황에서 이러한 스택킹 기능을 사용하면, 하나의 IP를 이용하여 여러 대의 장비를 관리할 수 있습니다. 스택킹은 하나의 IP 주소로 여러 대의 장비와 장비에 연결되어 있는 가입자까지 쉽게 관리 할 수 있기 때문에 One IP Management 라고도 합니다.
 (주)다산네트워크스의 장비는 이러한 스택킹 기능을 지원합니다.

다음은 스택킹을 설정한 네트워크의 예를 나타낸 것입니다.



【 그림 8-32 】 스택킹 설정의 예



참 고

V5812G는 2대부터 16대까지 스택킹 설정이 가능합니다.

위의 그림과 같이 스택킹 되어 있는 장비 그룹에서 관리를 담당하도록 설정된 한 대의 장비 A를 Master 장비라고 하고, Master 장비에게 관리되는 장비 B와 C를 Slave 장비라고 합니다. Master 장비 A는 설치된 위치나 연결 방식에 관계없이 Slave 장비 B와 C를 점검하고 관리할 수 있습니다.

다음은 스택킹을 설정하는 방법입니다.

- 장비 그룹 설정
- Master 장비 지정
- Slave 장비 지정
- 스택킹 설정 해제
- 스택킹 설정 내용 확인
- Master에서 Slave로 접속
- 설정 예제

8.6.1. 장비 그룹 설정

스택킹 기능으로 설정할 모든 장비는 동일한 VLAN에 속하도록 설정해야 합니다. 동일한 VLAN에 속하는 장비 그룹으로 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stack device bridge-name	Global	스택킹으로 설정할 모든 장비를 동일한 장비 그룹으로 설정합니다.



참 고

스택킹을 설정하여 관리하려면, Master 장비와 Slave 장비를 연결한 포트는 반드시 같은 VLAN에 속해야 합니다.

8.6.2. Master 장비 지정

Master가 되는 장비는 다음 명령어를 사용하여 Master 장비로 설정하십시오.

명령어	모 드	기 능
stack master	Global	Master 장비를 설정합니다.

8.6.3. Slave 장비 설정

Master 장비를 정하셨다면, Master 장비에 Slave 장비를 등록해야 합니다.

Slave 장비를 등록하거나, 등록했던 Slave 장비를 삭제하려면, Master 장비 상에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stack add mac-address	Global	Slave 장비를 등록합니다.
stack del mac-address		Slave 장비를 삭제합니다.



참 고

스택킹이 제대로 동작하도록 하려면, 반드시 Slave 장비의 인터페이스를 활성화 시켜야 합니다.



참 고

서로 다른 VLAN에 속하는 장비는 같은 장비 그룹에 추가되지 않습니다.

Master 장비에 등록된 Slave 장비는 Slave 장비로 지정해야 합니다. Slave 장비로 지정하려면, Slave 장비 상에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stack slave	Global	Slave 장비로 지정합니다.

8.6.4. 스택킹 설정 해제

스택킹 기능을 해제하려면 다음과 같은 명령어를 사용하십시오.

명령어	모 드	기 능
no stack	Global	Stack 기능 설정이 해제됩니다.

8.6.5. 스택킹 설정 내용 확인

스택킹에 대한 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show stack	Enable/Global/Bridge	스택킹에 대한 설정 내용을 확인합니다.

Master 장비는 등록되어 있는 Slave 장비의 정보를 알 수 있고, Slave 장비는 자신의 Node ID를 알 수 있습니다.

8.6.6. Master에서 Slave로 접속

모든 스택킹 설정을 마치고 나면 Master에서 Slave로 접속하여 설정 및 관리를 할 수 있습니다.

Master에서 Slave로 접속하려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
rcommand node-number	Bridge	Slave로 접속한다.

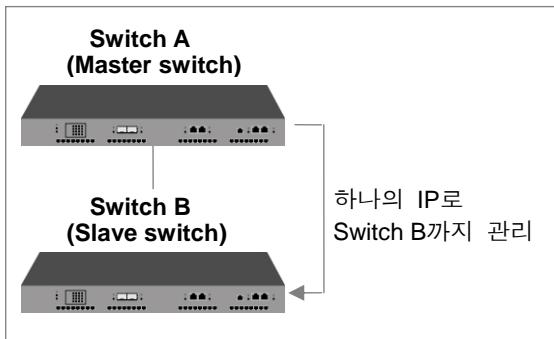
위의 명령어에서 입력하는 *node-number*는 Slave 장비에서 스택킹 설정 내용을 확인하면 얻어지는 정보 중 “**node ID**”에 해당합니다.

Master 장비에서 위의 명령어를 입력하면 Slave 장비와 연결된 Telnet 창이 나타나고, DSH command를 이용하여 Slave 장비를 설정할 수 있습니다. Telnet 창에서 “**exit**” 명령어를 사용하면 Slave 장비와의 접속이 끊어집니다.

8.6.7. 설정 예제

[설정 예제 1] 스택킹 설정

다음은 위의 방법에 따라 SWITCH A를 master로 지정하고 SWITCH B를 slave로 지정하여 스택킹을 설정한 경우의 예입니다.



1 단계 Master 장비가 되는 Switch A의 Interface 설정 모드에서 IP 주소를 부여하고, “no shutdown” 명령어를 사용하여 인터페이스를 활성화 시킵니다. 이 때 Interface 설정 모드로 들어갈 때에는 스택킹을 위한 장비 그룹으로 등록할 VLAN의 Interface 설정 모드로 들어가셔야 합니다.

다음은 장비 그룹으로 설정할 Interface가 default일 경우의 예입니다.

```
SWITCH_A# configure terminal
SWITCH_A(config)# interface 1
SWITCH_A(Interface)# ip address 192.168.10.1/16
SWITCH_A(Interface)# no shutdown
SWITCH_A(Interface)#
```



참 고

장비가 여러 대 연결되어 있으면 나머지 장비들은 Master 장비의 IP 주소를 통해 관리됩니다. 따라서 Slave 장비에 따로 주소를 설정할 필요는 없습니다.

2 단계 Switch A를 Master 장비로 설정합니다. 동일한 장비 그룹에 속하도록 VLAN을 설정하고, Slave 장비를 등록한 후 Master 장비로 설정합니다.

<Switch A – Master Switch>

```
SWITCH_A(config)# stack master
SWITCH_A(config)# stack device default
SWITCH_A(config)# stack add 00:d0:cb:22:00:11
```

3 단계 Slave 장비로 Master 장비에 등록된 Switch B에서 동일한 장비 그룹에 속하도록 VLAN을 설정하고, Slave 장비로 설정합니다.

<Switch B – Slave Switch>

```
SWITCH_B(Global)# stack slave
SWITCH_B(Global)# stack device default
```

4 단계 설정한 내용을 확인하십시오. Master 장비와 Slave 장비에서 확인할 수 있는 정보는 다음과 같이 달라집니다.

<Switch A – Master Switch>

```
SWITCH_A(bridge)# show stack
device  : default
node ID : 1
node   MAC address          status   type      name       port
1      00:d0:cb:0a:00:aa    active   V5812G   SWITCH_A    24
2      00:d0:cb:22:00:11    active   V5812G   SWITCH_B    24
SWITCH_A(bridge)#

```

<Switch B – Slave Switch>

```
SWITCH_B(bridge)# show stack
device  : default
node ID : 2
SWITCH_B(bridge)#

```

[설정 예제 2] Master 장비에서 Slave 장비로 접속

다음은 [설정 예제 1]에서 설정한 Master 장비에서 Slave 장비에 접속하는 예 입니다. 위의 [설정 예제 1]에서 Slave 장비의 설정 내용을 확인하면 node-number가 2번임을 알 수 있습니다.

```
SWITCH(bridge)# rcommand 2
Trying 127.1.0.1(23)...
Connected to 127.1.0.1.
Escape character is '^].
SWITCH login: admin
Password:

SWITCH#
```

접속을 끊으려면 다음과 같이 입력하십시오.

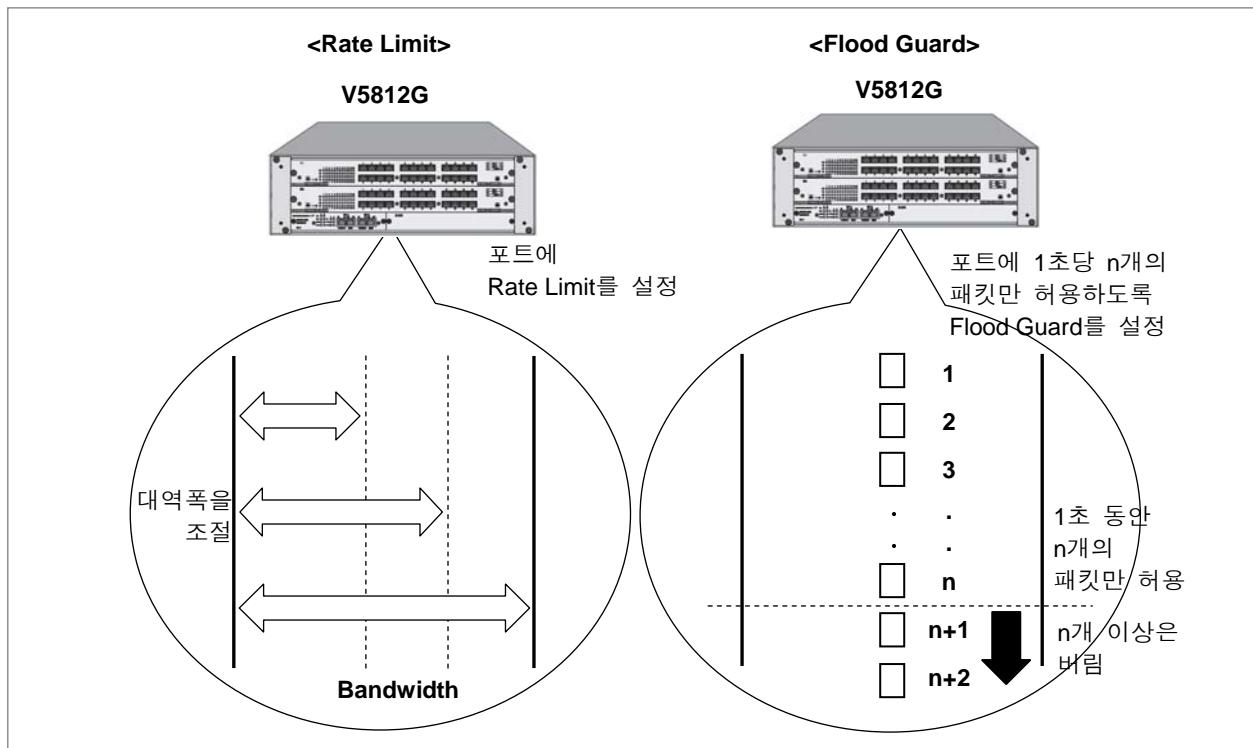
```
SWITCH# exit
Connection closed by foreign host.
SWITCH(bridge)#

```

8.7 Rate Limit와 Flood Guard

Rate Limit은 사용자가 환경에 따라 포트의 사용 가능한 대역폭을 설정할 수 있는 기능입니다. 이 설정은 특정한 포트가 모든 대역폭을 독점하게 되는 상황을 방지하고 모든 포트가 균등한 대역폭을 사용할 수 있게 할 수 있습니다. 이 때, 송신 대역폭과 수신 대역폭을 동일하게 설정할 수 있고, 다르게 설정할 수도 있습니다.

한편, 위에서 설명한 Rate Limit 기능은 패킷이 오고 가는 길 역할을 하는 대역폭의 너비로 패킷을 제한하는 기능이라면, Flood Guard란, 정해진 대역폭 안으로 들어올 수 있는 패킷의 개수를 제한하여 패킷을 조절하는 기능입니다.



【 그림 8-33 】 Rate Limit와 Flood Guard

이러한 기능은 대역폭은 일정하게 유지한 채 한꺼번에 많이 전달되는 이상 패킷이 수신되는 것을 막을 수 있습니다.

8.7.1. Rate Limit 설정

V5812G는 포트의 송신 대역폭(egress)과 수신 대역폭(ingress)을 각각 설정할 수 있습니다. 수신 대역폭(ingress)은 장비의 입장에서 수신되는 것이기 때문에 포트에 물려있는 PC 사용자의 입장에선 업로드에 해당됩니다. 그런데, 두 대역폭을 설정하는 방법이 약간 다르므로 설정할 때 주의해야 합니다.

먼저 포트의 송신 대역폭을 설정하려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
rate-limit port port-number rate rate egress	Bridge	포트에 일정한 송신 대역폭을 지정합니다.

한편, 지금까지의 ingress 측의 Rate limit는 사용자가 설정해 놓은 대역폭 이상의 패킷이 왔을 때, 이를 무조건 drop 하는 방식을 썼습니다. 그러나, 새로워진 V5812G는 ingress 측에 사용자가 설정해 놓은 대역폭 이상의 패킷이 왔을 때, 일단 상대에게 pause 패킷을 보내고, 그래도 패킷이 올 때에는 drop 하는 방식을 사용할 수 있게 하였습니다.

이러한 방식으로 ingress 측의 Rate limit를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
rate-limit port port-number rate rate ingress dotx3	Bridge	Pause 패킷을 사용하는 방식으로 포트에 일정한 수신 대역폭을 지정합니다.



참 고

대역폭의 단위는 Kbps입니다. 대역폭은 최소 64Kbps 이상으로 입력하십시오. 또한, 64단위로, 즉 64의 배수로 입력할 수 있습니다..



참 고

V5812G는 물리적인 포트는 물론 논리적인 트렁크 포트까지 Rate Limit를 설정할 수 있습니다.

한편, 포트에 설정한 대역폭을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show rate-limit	Enable /Global/Bridge	포트에 설정했던 대역폭을 해제합니다.

사용자가 지정한 대역폭을 삭제하려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no rate-limit port port-number egress	Bridge	포트에 설정했던 대역폭을 해제합니다.
no rate-limit port port-number ingress dot1x		

8.7.2. Flood Guard 설정

(1) MAC-Flood-Guard 설정 방법

1초당 수신될 수 있는 패킷의 개수를 제한하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
mac-flood-guard port-number <1-6000>	Bridge	해당 포트에 1초 동안 수신될 수 있는 패킷 개수를 제한합니다.

설정한 Flood Guard를 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no mac-flood-guard port-number	Bridge	설정했던 Flood Guard를 해제합니다.

설정한 Flood Guard의 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show mac-flood-guard [macs]	Enable / Global / Bridge	Flood Guard 설정 내용을 확인합니다.

(2) CPU-Flood-Guard 설정

V5812G는 CPU로 올라오는 브로드캐스트 트래픽이 flooding 되는 것을 차단하는 기능을 지원합니다. 이러한 기능을 특정한 포트를 통해서 들어오는 트래픽을 사용자가 원하는 대로 차단 또는 허용하여 통신을 더욱 원활하게 할 수 있습니다. CPU에 올라오는 브로드캐스트 트래픽에 cpu-flood-guard를 활성화시키고자 한다면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
cpu-flood-guard enable	Bridge	CPU에 올라오는 트래픽의 flooding을 차단하는 기능을 활성화합니다.
cpu-flood-guard disable		CPU에 올라오는 트래픽의 flooding을 차단하는 기능을 비활성화합니다.

특정한 포트를 통해 CPU에 수신되는 트래픽의 1초당 패킷 수를 제한하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
cpu-flood-guard port-number <1-6000>	Bridge	해당 포트에 1초 동안 수신될 수 있는 패킷 개수를 제한합니다.
no cpu-flood-guard [port-number]		해당 포트에 cpu-flood-guard 관련 설정 내용을 삭제합니다.

CPU에 수신되는 트래픽에 대해 Flooding을 차단하는 시간을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
cpu-flood-guard port-number timer <10-3600>	Bridge	특정한 포트를 통해 CPU에 수신되는 패킷을 차단하는 시간을 설정합니다.



참 고

Timer는 기본적으로 장비에 60초로 설정되어 있습니다.

특정한 포트만 CPU에 수신되는 트래픽에 대해 Flooding을 허용하고자 하면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
cpu-flood-guard port-number unblock	Bridge	해당 포트를 통해 CPU에 수신되는 트래픽의 flooding을 허용합니다.

CPU-flood-guard 설정을 확인하고자 하면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show cpu-flood-guard	Enable/Global/Bridge	Cpu-flood-guard 설정을 확인합니다.

(3) Port-Flood-Guard 설정

V5812G는 포트로 들어오는 패킷의 개수를 주기적으로 검사하여 특정 pps 이상 수신 될 경우 해당 포트를 Block 시켜 트래픽 유입을 차단할 수 있습니다. 이 기능은 특정한 포트를 통해서 들어오는 트래픽을 사용자가 원하는 시간만큼만 차단하여 통신을 더욱 원활하게 할 수 있습니다.

갑작스러운 트래픽 폭주로 인해 특정한 포트로 유입되는 패킷 수 임계값을 주기적으로 검사하여 포트를 Block 시키는 pps-control 기능을 활성화시키고자 한다면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
pps-control port port-number threshold { 5 60 600 }	Global	주기적으로 해당 포트에 1초 동안 수신될 수 있는 패킷 개수를 검사하여 그 값을 초과했을 경우 포트를 Block시킵니다.
no pps-control port port-number		해당 포트에 pps-control 관련 설정을 해제합니다.



시간 간격은 5초, 60초, 600초로 설정할 수 있습니다.

특정한 포트로부터 수신되는 트래픽에 대해 Flooding을 차단하는 시간을 설정하면 그 시간동안만 해당 포트로 들어오는 패킷을 차단하고 후에는 다시 패킷을 받을 수 있습니다. 만약 10초로 설정했을 경우 10초 이후부터는 해당 포트에 패킷이 유입됩니다.

포트를 Block 시키는 시간을 설정하려면, Global 모드에서 다음 명령어를 사용하십시오.

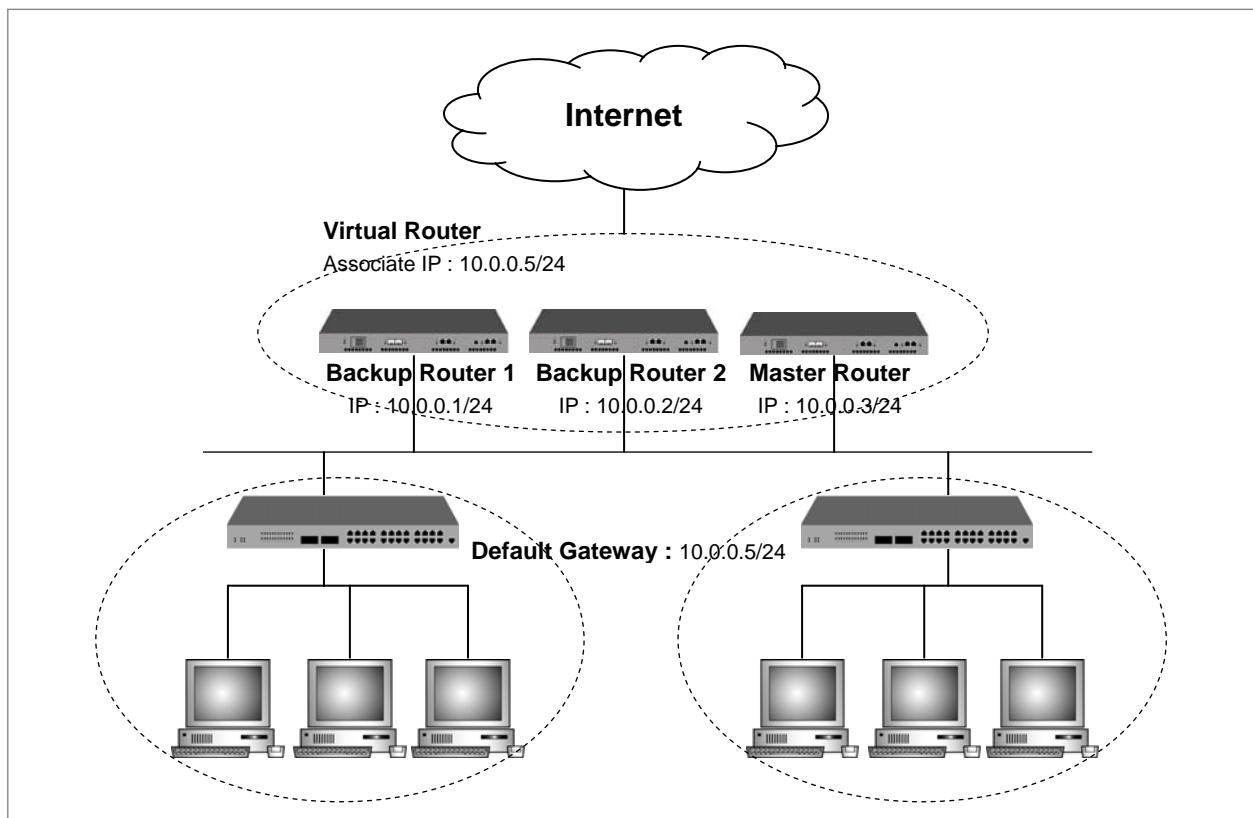
명령어	모 드	기 능
pps-control port port-number block timer <10-3600>	Global	특정한 포트를 통해 수신되는 패킷을 차단하는 시간을 설정합니다.
no pps-control port port-number block		해당 포트에 설정했던 패킷을 차단하는 시간을 해제합니다.

PPS-control 설정내용을 확인하고자 하면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show pps-control port [port-number]	Enable/Global/Bridge	pps-control 기능을 확인합니다.

8.8 VRRP (Virtual Router Redundancy Protocol)

VRRP(Virtual Router Redundancy Protocol)는 가상 라우터들로 이루어진 VRRP Group을 설정하여 고정된 단일 라우터를 사용할 때 발생할 수 있는 네트워크 장애를 막을 수 있습니다. V5812G에서는 최대 255개의 가상 라우터들을 VRRP Group에 올릴 수 있습니다. 먼저 VRRP Group의 가상 라우터 중 어떤 것이 Master Virtual Router 역할을 할지 결정하십시오. 나머지 가상 라우터들은 Backup Virtual Router가 됩니다. 이 백업 라우터들에게 우선 순위를 지정하면 마스터 라우터에 문제가 있을 때 백업 라우터들이 그 역할을 대신하게 됩니다. VRRP를 설정할 때에는 VRRP Group에 속하게 될 라우터에 동일한 Group ID로 VRRP Group을 설정한 후, 동일한 Associated IP를 할당합니다. Associated IP를 할당한 후에는 Master Virtual Router와 Backup Virtual Router를 정해야하는데, Priority가 가장 높은 라우터가 Master가 됩니다. Priority는 그 값이 클수록 우선 순위가 높게 지정되어 Backup Virtual Router들 가운데서도 이 값에 따라 순서가 정해지게 되고, Priority 값이 같을 경우에는 IP 주소에 의해 우선 순위가 정해지는데, IP 주소가 높을수록 우선 순위가 높습니다. 다음은 각각 IP 주소가 10.0.0.1/24, 10.0.0.2/24, 10.0.0.3/24인 라우터를 10.0.0.5/24라는 Associate IP 주소로 Virtual Router를 설정한 그림입니다.



【 그림 8-34 】 VRRP 구성도

세 라우터의 Priority 값이 동일하다고 가정할 때, 10.0.0.3/24라는 IP 주소를 가진 라우터가 가장 큰 IP 주소를 가지고 있기 때문에 Master Router로 결정됩니다. 한편, 이 Virtual Router에 연결된 장비나 PC들은 Virtual Router의 IP 주소인 10.0.0.5/24를 Default Gateway로 가지게 됩니다.

8.8.1. VRRP 기본 설정

V5812G를 Virtual Router Group에 속하는 장비로 설정하려면, 우선 Global 설정 모드에서 다음 명령어를 사용하십시오. 그러면, VRRP가 활성화됨과 동시에 VRRP와 관련된 여러가지 설정을 할 수 있는 VRRP 설정 모드로 들어갈 수 있습니다.

명령어	모 드	기 능
router vrrp <i>interface-name group-id</i>	Global	Virtual Router Group을 설정합니다.



참 고

*group-id*는 1부터 255까지 설정 가능합니다.

설정한 내용을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no router vrrp [<i>group-id / all</i>]	Global	Virtual Router의 특정 그룹 또는 모든 그룹을 삭제합니다.

다음은 위의 명령어를 사용하여 VRRP 설정 모드로 들어간 경우입니다. VRRP 설정 모드로 들어가면, 시스템 프롬프트가 SWITCH(config)#에서 SWITCH(config-router)#로 변경됩니다.

```
SWITCH(config)# router vrrp 1 1
SWITCH(config-router)#{
```

한편, VRRP 설정 내용을 확인하려면 다음 명령어들을 사용하십시오.

명령어	모 드	기 능
show vrrp	Enable /Global/Bridge	현재 VRRP 설정을 보여줍니다.
show vrrp stat		VRRP 패킷 통계를 확인합니다
show vrrp interface [interface-name all]		특정 인터페이스 또는 모든 인터페이스의 현재 VRRP 설정을 보여줍니다.
show vrrp [group-id all]		특정 그룹의 VRRP 설정을 확인합니다.
show running-config	Enable /Global/Bridge /Interface/VRRP	장비의 설정 내용을 확인합니다.

(1) Associate IP 주소 설정하기

Virtual Router Group을 설정한 후에는 Virtual Router의 Associate IP 주소를 설정해야 합니다. 동일한 Group에 속하는 라우터에 동일하게 IP 주소를 설정하십시오. 다음은 Virtual Router Group에 속하는 라우터들에게 IP 주소를 설정하거나, 설정했전 Associate IP 주소를 삭제할 때 사용하는 명령어입니다.

명령어	모 드	기 능
associate ip-address	VRRP	Virtual Router들이 가지는 동일한 Associated IP 주소를 설정합니다.
no associate [ip-address all]		Virtual Router들에게 할당한 특정 Associated IP 주소 또는 모든 Associated IP 주소를 삭제합니다.

다음은 V5812G에 Virtual Router Gruopd의 IP 주소를 10.0.0.5로 설정한 경우입니다.

```
SWITCH(config-router)# associate 10.0.0.5
SWITCH(config-router)#
`
```

(2) Associated IP 주소 직접 액세스 설정

V5812G는 Associated IP 주소 직접 액세스 기능을 통해 ping과 같은 통신 명령어로 Associated IP 주소를 직접 액세스 할 수 있습니다. Associated IP 주소 직접 액세스 기능을 설정하려면 다음 명령어를 참고하십시오.

명령어	모 드	기 능
vip_access [enable disable]	Global	Associated IP 주소 직접 액세스 기능을 설정합니다.

(3) Master Router와 Backup Router 지정하기

(주)다산네트웍스의 장비는 Virtual Router 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 같은 경우에는 IP 주소를 비교하여 IP 주소는 그 값이 높은 것이 우선 순위가 높게 됩니다.

V5812G의 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 Router 도 2개 이상일 때 우선 순위에 따라 사용 순서가 결정됩니다.

Virtual Router에 Priority 값을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
vr-priority priority	VRP	Virtual Router에 우선 순위를 할당합니다.
no vr-priority		Virtual Router에 할당된 우선 순위를 삭제합니다.



참 고

V5812G는 기본적으로 Priority 값이 “100”으로 설정되어 있습니다.



참 고

Priority 값은 1부터 254까지 입력할 수 있습니다.

다음은 Virtual Router Group으로 설정되어 있는 Layer 3 SWITCH 1과 Layer 3 SWITCH 2에 Priority 값을 각각 101, 102로 설정하여 Master와 Backup Router가 정하는 경우입니다. 그러면, IP 주소와 상관없이 Priority 값이 큰 Layer 3 SWITCH 2가 Master가 됩니다.

<Layer 3 SWITCH1 : IP 주소 - 10.0.0.1/24>

```
SWITCH1(config)# router vrrp 1 1
SWITCH1(config-router)# associate 10.0.0.5
SWITCH1(config-router)# vr_priority 101
SWITCH1(config-router)# exit
SWITCH1(config)# show vrrp
```

```
default - virtual router 1
-----
state          backup
virtual mac address 00:00:5E:00:01:01
advertisement interval 1 sec
preemption      enabled
priority        101
master down interval 3.624 sec
[1] associate address : 10.0.0.5
```

<Layer 3 SWITCH 2 : IP 주소 - 10.0.0.2/24>

```
SWITCH2(config)# vrrp 1 1
SWITCH2(config-router)# associate 10.0.0.5
SWITCH1(config-router)# vr_priority 102
SWITCH2(config-router)# exit
SWITCH2(config)# show vrrp
```

```
default - virtual router 1
-----
state          master
virtual mac address 00:00:5E:00:01:01
advertisement interval 1 sec
preemption      enabled
priority        102
master down interval 3.620 sec
[1] associate address : 10.0.0.5
```

Priority 값이 높은 Layer 3 SWITCH 2가 Master로 정해집니다.

한편, V5812G는 기본적으로 Priority 값이 “100”으로 정해져 있는데, 이 때 특정한 Priority 값을 할당하지 않으면 IP 주소가 작은 장비가 우선 순위가 높기 때문에 Master Router가 됩니다. 또한, Backup Router가 2개 이상일 때도 IP 주소를 기준으로 우선 순위를 결정하여 사용 순서를 적용하게 됩니다.

다음은 IP 주소가 각각 10.0.0.1, 10.0.0.2인 Layer 3 SWITCH 1과 Layer 3 SWITCH2를 Virtual Router Group으로 설정했을 때 Master와 Backup Router가 정해지는 예입니다.

<Layer 3 SWITCH1 : IP 주소 - 10.0.0.1/24>

```
SWTICH1(config)# router vrrp 1 1
SWTICH1(config-router)# associate 10.0.0.5
SWTICH1(config-router)# exit
SWTICH1(config)# show vrrp

default - virtual router 1
-----
state          master
virtual mac address 00:00:5E:00:01:01
advertisement interval 1 sec
preemption      enabled
priority        100
master down interval 3.624 sec
[1] associate address : 10.0.0.5
```

<Layer 3 SWITCH 2 : IP 주소 - 10.0.0.2/24>

```
SWTICH2(config)# router vrrp 1 1
SWTICH2(config-router)# associate 10.0.0.5
SWTICH2(config-router)# exit
SWTICH2(config)# show vrrp

default - virtual router 1
-----
state          backup
virtual mac address 00:00:5E:00:01:01
advertisement interval 1 sec
preemption      enabled
priority        100
master down interval 3.620 sec
[1] associate address : 10.0.0.5
```

Priority 값이 같기 때문에 IP 주
소가 작은 Layer 3 SWITCH1이
Master로 정해집니다.

8.8.2. VRRP Track 설정

V5812G 사용자는 Master Router와 연결되어 있는 업링크 인터페이스의 다운이나 링크 불량으로 인해 지속적인 네트워크 서비스가 불가능 할 때, VRRP Track으로 상위단과 통신 가능한 Backup Router를 Master Router로 변경할 수 있습니다.

V5812G의 VRRP Track은 Master Router의 통신 장애 시에, 사용자가 설정해 놓은 값만큼 우선 순위를 낮춤으로써 상대적으로 우선 순위가 높아진 Backup Router가 Master Router가 되도록 합니다.

VRRP Track을 설정하려면 다음 명령을 사용하십시오.

명령어	모 드	기 능
track interface <i>interface-name</i> priority <i>priority</i>	VRRP	VRRP Track을 설정합니다.
no track interface <i>interface-name</i>		VRRP Track을 해제합니다.



*priority*는 <1 – 254> 사이에서 설정 가능합니다.



낮아진 우선 순위 값이 1보다 작을 경우에는, 최소값인 1로 설정됩니다.



특정 인터페이스 IP 주소가 VIP로 설정되어 있는 경우에는 VRRP Track이 적용되지 않습니다.

8.8.3. Authentication 패스워드 설정

사용자가 Virtual Router Group을 설정한 상태에서 Group ID와 Associate 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 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
authentication clear_text password	VRRP	다른 장비가 Virtual Router Group에 소속되는 것을 막기 위해 패스워드를 설정합니다.
no authentication		다른 장비가 Virtual Router Group에 소속되는 것을 막기 위해 설정한 패스워드를 삭제합니다.



참고

Authentication 패스워드는 최대 7자리의 문자로 설정할 수 있습니다.

다음은 Virtual Router Group의 Authentication 패스워드를 network로 설정하고 그 내용을 확인한 경우의 예입니다.

```
SWITCH(config-router)# authentication clear_text network
SWITCH(config-router)# show running-config
Building configuration...
(종략)
vrrp default
authentication clear_text network
associate 10.0.0.5
!
!
!
!
no snmp
!
!
!
!
!
!
!
!
SWITCH(config-router)#

```

8.8.4. Preempt 기능 설정

Preempt는 Virtual Router Group이 설정된 상태에서 또 다른 장비를 추가했을 때, 추가한 장비에 Priority 값을 가장 높게 설정하면 장비를 재부팅하거나 별도의 설정 없이 추가된 장비가 자동으로 Master Router가 되도록 하는 기능입니다.

Preempt 기능을 설정하려면 VRRP 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
preempt {enable disable}	VRRP	Preempt 기능을 활성/비활성화 시킵니다.



참 고

V5812G는 기본적으로 Preempt 기능이 “enable”로 설정되어 있습니다.

```

SWITCH(config-router)# preempt disable
SWITCH(config-router)# exit
SWITCH(config)# show vrrp

default - virtual router 1
-----
state          master
virtual mac address      00:00:5E:00:01:01
advertisement interval    1 sec
preemption        disabled
priority         100
master down interval   3.624 sec
[1] associate address : 10.0.0.5

SWITCH(config)#

```

한편, Preempt 기능을 기본값으로 되돌리려면 VRRP 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no preempt	VRRP	Preempt 기능을 기본값으로 되돌립니다.

8.8.5. Advertisement time 설정

Virtual Router Group에서 Master Router는 일정한 간격으로 VRRP 그룹 내의 다른 Virtual Router들에게 자신의 정보를 내는데 이를 Advertisement time이라고 합니다.

V5812G의 사용자는 이러한 Advertisement time을 설정할 수 있습니다. Advertisement time을 설정하면서, VRRP 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
vr_timers advertisement time	VRRP	Master Router가 자신의 정보를 다른 Virtual Router에게 배포하는 시간 간격인 Advertisement time 을 설정합니다.



참 고

V5812G는 기본적으로 Advertisement time이 1초로 설정되어 있습니다.



참 고

V5812G의 설정 가능한 Advertisement time은 1초부터 10초까지입니다.

다음은 Advertisement time을 10초로 설정하고 그 내용을 확인한 경우입니다.

```
SWITCH(config-router)# vr_timers advertisement 10
SWITCH(config-router)# exit
SWITCH(config)# show vrrp

default - virtual router 1
-----
state                         master
virtual mac address           00:00:5E:00:01:01
advertisment interval         10 sec
preemption                     disabled
priority                       100
master down interval          30.624 sec
[1] associate address : 10.0.0.5

SWITCH(config)#

```

한편, Advertisement time을 기본값으로 되돌리려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no vr_timers advertisement	VRRP	Advertisement time을 기본값으로 되돌립니다.

8.8.6. VRRP 통계 확인

Virtual Router Group에서 주고 받은 패킷에 대한 통계를 확인하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show vrrp stat	View/Global/VRRP	Virtual Router Group에서 주고 받은 패킷에 대한 통계를 확인합니다.

다음은 Virtual Router Group에서 주고 받은 패킷에 대한 통계를 확인한 경우의 예입니다.

```
SWITCH(config)# show vrrp stat

VRRP statistics :
    VRRP packets rcvd with invalid TTL      0
    VRRP packets rcvd with invalid version   0
    VRRP packets rcvd with invalid VRID       0
    VRRP packets rcvd with invalid size       0
    VRRP packets rcvd with invalid checksum   0
    VRRP packets rcvd with invalid auth-type  0
    VRRP packets rcvd with interval mismatch  0

SWITCH(config)#

```

8.8.7. VRRP 통계 삭제

Virtual Router Group에서 주고 받은 패킷의 통계를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear vrrp stat	Global/ VRRP	Virtual Router Group에서 주고 받은 패킷의 통계를 삭제합니다.

8.9 대역폭 설정

라우팅 프로토콜은 대역폭 정보를 이용하여 라우팅 거리값을 측정합니다. 인터페이스의 대역폭을 설정하려면, Interface 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bandwidth kilobits	Interface	인터페이스의 대역폭을 설정합니다.



주의

사용자가 설정할 수 있는 대역폭은 1부터 10,000,000Kbits입니다. 여기서 설정하는 대역폭은 라우팅 정보 작성 시 필요한 것이며 물리적인 대역폭에는 영향을 주지는 않습니다.

다음은 대역폭을 1000Kbits로 설정하고, 설정 내용을 확인한 경우의 예입니다.

```
SWITCH(config-if)# bandwidth 1000
SWITCH(config-if)# show running-config
(종략)
interface default
no shutdown
bandwidth 1000
(이하 생략)
```

한편, 대역폭 정보를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no bandwidth [kilobits]	Interface	설정했던 인터페이스의 대역폭을 해제합니다.

8.10 DHCP(Dynamic Host Configuration Protocol)

DHCP(Dynamic Host Configuration Protocol)는 네트워크 관리자들이 조직 내의 네트워크 상에서 IP 주소를 중앙에서 관리하고 할당해 줄 수 있도록 해 주는 프로토콜입니다. 예를 들어 네트워크 상에 있는 모든 PC가 항상 동일한 시간에 접속하지 않을 확률이 큰 환경에서는 모든 PC가 IP 주소를 가지고 있을 필요가 없으며 IP 주소를 필요로 할 경우에만 할당 받는 구조를 생각할 수 있습니다. 이 때 IP 주소를 필요로 하는 PC에 자동적으로 IP 주소를 배분하는 것이 DHCP 서버이고, IP 주소를 배분 받는 PC들은 DHCP 클라이언트가 됩니다.

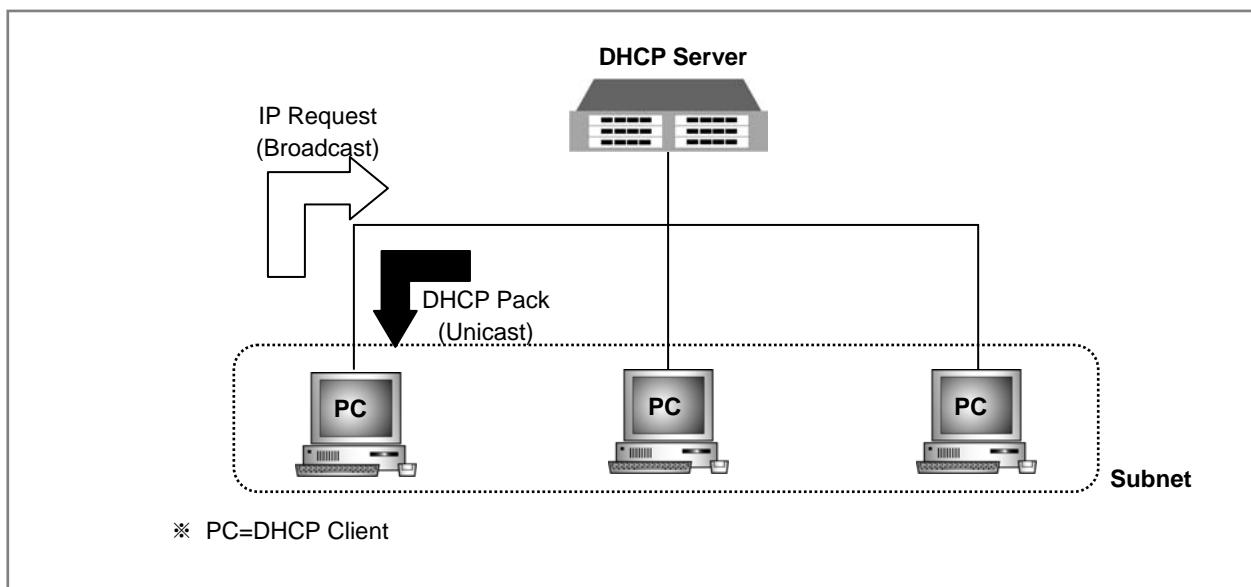
DHCP 기능은 다음과 같은 장점을 가지고 있습니다.

◆ COST 절약

DHCP 기능은 한정된 IP 자원을 가지고 많은 사용자들이 인터넷에 접속할 수 있으므로 비용도 절감하고 IP 자원도 절약할 수 있습니다.

◆ 효율적인 네트워크 관리

DHCP 서버는 누구나 쉽게 설정하고 관리할 수 있고, DHCP 서버가 관리하는 네트워크에 속해 있는 DHCP 클라이언트도 역시 네트워크 환경의 TCP/IP 설정 등의 전문 지식을 전혀 몰라도 문제없이 네트워크에 접근할 수 있습니다.



【 그림 8-35 】 DHCP 서비스 구성의 예

V5812G는 사용자의 설정에 따라 DHCP 서버로서의 기능을 제공할 수도 있고, DHCP 서버와 DHCP 클라이언트를 연결하는 Relay 에이전트의 기능을 제공할 수도 있습니다. 이 장에서는 DHCP 설정과 관련하여 다음과 같은 내용을 설명합니다.

- DHCP 서버 설정
- DHCP 릴레이 에이전트 설정
- DHCP Option-82 설정
- Class 설정
- DHCP 클라이언트
- DHCP Snooping
- IP Source Guard
- DHCP 디버깅
- DHCP 패킷 통계 확인

8.10.1. DHCP 서버 설정

V5812G 스위치를 DHCP 서버로 설정하여 DHCP 클라이언트에게 DHCP 서비스를 제공하려면, 장비를 DHCP 서버 모드로 선택해야 합니다. 사용자의 스위치를 DHCP 서버로 설정하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
service dhcp	Global	사용자 장비를 DHCP 서버로 설정합니다.
no service dhcp		사용자 장비의 DHCP 서버 설정을 해제합니다.

(1) IP Pool 만들기

DHCP 서버가 클라이언트에게 할당해 줄 수 있는 IP 주소의 집합소를 IP Pool이라고 합니다. 관리자는 자신이 관리할 IP Pool에 각각 이름을 설정할 수 있습니다. IP Pool에 이름을 설정하면, 해당 IP Pool에 대한 설정이 가능한 DHCP IP Pool 설정 모드로 들어가게 됩니다. IP Pool 설정 모드로 들어가면, 시스템 프롬프트가 SWITCH(config)#에서 SWITCH(config-dhcp [pool-name])#으로 변경됩니다. IP Pool 설정 모드에서는 서브넷, 서브넷에서 사용하게 될 IP 주소 범위, 서브넷의 디폴트 게이트웨이 등을 설정할 수 있습니다.

다음은 DHCP IP Pool의 이름을 설정하여 IP Pool 설정 모드로 들어갈 때 사용하는 명령어입니다.

명령어	모 드	기 능
ip dhcp pool pool-name	Global	DHCP IP Pool의 이름을 설정하여 IP Pool 설정 모드로 들어갑니다.
no ip dhcp pool-name		IP Pool을 삭제합니다.

(2) 서브넷 설정

IP Pool을 만들었다면, IP Pool에 DHCP 서버의 개별 네트워크인 서브넷을 지정하십시오. 서브넷을 지정하려면, IP Pool 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
network ip-address/m	IP Pool	IP Pool에 서브넷을 지정합니다.



참 고

V5812G는 하나의 IP Pool에 여러 개의 서브넷을 지정할 수 있습니다.

다음은 서브넷을 삭제할 때 사용하는 명령어입니다.

명령어	모 드	기 능
no network ip-address/m	IP Pool	서브넷을 삭제합니다.

(3) 서브넷 디폴트 게이트웨이 설정

DHCP 서버가 알지 못하는 IP 주소와 통신을 하기위해서는 모든 IP 주소가 통하는 디폴트 게이트웨이를 설정해야 합니다. 다음은 서브넷의 디폴트 게이트웨이를 설정할 때 사용하는 명령어입니다.

명령어	모 드	기 능
default-router		서브넷의 디폴트 게이트웨이를 설정합니다.
gateway-address [gateway-address]		
no default-router gateway-address [gateway-address]	IP Pool	서브넷의 디폴트 게이트웨이를 해제합니다.
no default-router all		서브넷의 디폴트 게이트웨이를 모두 해제합니다.



참 고

서브넷의 디폴트 게이트웨이는 최대 8개까지 설정 가능합니다.

(4) IP 주소 범위 설정

DHCP 서브넷을 설정하였으면 서브넷에서 사용할 IP 주소의 범위를 설정하여 주십시오. IP 주소의 범위를 설정하려면 DHCP 설정 모드에서 다음 명령어를 사용하십시오.

V5812G는 같은 IP 주소 영역에서 비연속적인 복수의 서브넷을 설정할 수 있습니다. 예를 들면, 192.168.1.0/24에서 192.168.1.10부터 192.168.1.20까지의 서브넷과 192.168.1.30부터 192.168.1.40 까지의 서브넷을 설정할 수 있습니다.

명령어	모 드	기 능
range start-address end-address	IP Pool	사용할 IP 주소의 범위를 설정합니다.

설정한 IP 주소 범위를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no range start-address end-address	IP Pool	설정한 IP 주소의 범위를 삭제합니다.

(5) IP 사용 가능 시간 설정

DHCP 서버 관리자는 해당 IP Pool에서 DHCP 클라이언트에게 할당된 IP 주소의 사용 시간을 정할 수 있습니다. 1시간이 기본으로 정해져 있으며 정해진 시간이 끝나기 전에 DHCP 클라이언트에게 연장할 것인지 의사를 물어봅니다.

IP 사용 가능 시간을 설정하려면, IP Pool 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lease-time default seconds	IP Pool	IP 주소 기본 사용 시간을 설정합니다.
no lease-time default		IP 주소 기본 사용 시간을 해제합니다.

다음 명령어를 사용하여 IP 최대 사용 시간을 설정하십시오.

명령어	모 드	기 능
lease-time max seconds	IP Pool	IP 주소 최대 사용 시간을 설정합니다.
no lease-time max		IP 주소 최대 사용 시간을 해제합니다.



IP 사용 시간은 초단위로 <120 - 2147483637> 사이에서 설정 가능합니다.



V5812G는 기본적으로 IP 주소 기본 사용 시간이 1시간(3600초), 최대한으로 사용할 수 있는 시간은 1시간(3600초)으로 설정되어 있습니다.

(6) DNS 등록

DHCP 서버는 DHCP 클라이언트가 접속을 하면, 기본적으로 IP 주소와 함께 디폴트 게이트웨이, IP 사용 가능 시간, 그리고 사용할 수 있는 DNS 서버를 알려줍니다. 따라서 DHCP 서버에 사용할 수 있는 DNS 서버를 등록해야 합니다.

해당 IP Pool에 DHCP 클라이언트에게 알려줄 DNS 서버를 등록하려면, IP Pool 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
dns-server ip-address1 [ip-address2]…[ip-address8]		DNS 서버를 등록합니다.
no dns-server ip-address1 [ip-address2]…[ip-address8]	IP Pool	DNS 서버를 삭제합니다.
no dns-server all		DNS 서버를 모두 삭제합니다.



DNS 서버는 8개까지 등록할 수 있습니다.

(7) IP 주소 수동 할당

V5812G의 관리자는 수동으로 IP 주소를 할당하도록 설정할 수 있습니다. 특정한 MAC 주소를 가진 DHCP 클라이언트에게 특정한 IP 주소를 사용자가 직접 할당하는 것입니다.

수동으로 IP 주소를 할당하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
fixed-address ip-address mac-address	IP Pool	DHCP 클라이언트에게 고정 IP 주소를 할당합니다.
no fixed-address ip-address		DHCP 클라이언트에게 할당한 IP 주소를 해제합니다.

(8) 도메인 이름 설정

IP Pool에 사용될 도메인 이름을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
domain-name domain-name	IP Pool	IP Pool에 대한 도메인 이름을 설정합니다.
no domain-name		IP Pool에 대한 도메인 이름을 해제합니다.

(9) Option 설정

V5812G는 DHCP 메시지의 Option 필드에 저장되는 내용을 설정할 수 있습니다. DHCP 패킷에 적용될 특정 Option code 와 format을 지정할 수 있습니다. 각 DHCP option code와 format 관련 설정은 DHCP option 모드를 통해 가능합니다.

DHCP 패킷에 맵핑 될 특정 Option code와 format을 지정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
option code <1-254> format format-name	IP-Pool	DHCP 패킷에 설정될 Option을 지정합니다.

설정한 Option 를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no option code <1-254>	IP-Pool	설정된 Option을 삭제합니다.

DHCP Pool에 설정된 Option이 없거나, Option의 데이터가 유효한 값이 아닐 경우, 시스템은 Default Option의 설정 여부를 확인하게 됩니다. Default Option이 설정되어 있으면, 각 Option의 데이터가 유효한 값인지 검사하고 DHCP Reply 패킷(Offer/ACK)에 Option을 설정합니다.

Default Option을 설정하거나 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp default-option code <1-254>	Global	DHCP 패킷에 Default Option 설정합니다.
no ip dhcp default-option code <1-254>		설정된 Default Option 삭제합니다.

(10) Static Lease database 파일 확인

V5812G는 TFTP 서버에 백업된 Lease database 중에서 Static으로 등록된 내용을 파일 형태로 불러서 확인할 수 있습니다.

Lease database 중 Static으로 등록된 내용을 파일 형태로 불러오려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
origin file tftp-server-address file-name	IP Pool	TFTP 서버로부터 Lease database 중 Static으로 등록된 내용을 파일 형태로 불러옵니다.
no origin file		TFTP 서버로부터 불러온 Lease database 중 Static으로 등록된 내용을 삭제합니다.



Lease database 파일은 ip dhcp database 명령어로 백업했을 때, **dhcpdb.mac-address** 형태로 저장됩니다. 따라서 *file-name*은 **dhcpdb.mac-address** 형태로 입력하십시오.

(11) 주소 할당 제한

DHCP 서버 모드의 V5812G는, DHCP Request 메시지를 수신했을 때 응답하지 않음으로써 클라이언트에게 IP 주소를 할당하지 않을 수 있습니다. 이러한 DHCP 패킷 필터링 대상 클라이언트는 MAC 주소를 확인하거나 장비의 특정 포트를 거치는지의 여부를 통해 결정됩니다.

특정 클라이언트에게 IP 주소를 할당하지 않도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp filter-address client-mac-address	Global	해당 클라이언트에게 IP 주소를 할당하지 않습니다.
ip dhcp filter-port client-ports		



*client-ports*는 여러 개 입력 가능합니다. 빈칸 없이 콤마(,)로 각 포트를 구별하여 입력하거나 대쉬(-)로 일련의 포트 범위를 지정하십시오.

특정 클라이언트에게 IP 주소를 할당하지 않도록 설정했던 것을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip dhcp filter-address client-mac-address	Global	특정 클라이언트에게 IP 주소를 할당하지 않도록 설정했던 것을 해제합니다.
no ip dhcp filter-port clients-ports		

(12) 할당 IP 주소의 사용 여부 확인

DHCP 서버는 클라이언트에게 IP 주소를 할당하기 전에 해당 IP 주소를 다른 클라이언트가 사용하고 있는지 확인하기 위해 Ping 테스트나 ARP 테스트를 실행합니다. Ping 테스트나 ARP 테스트를 실행하여 응답이 없다면, DHCP 서버는 현재 사용되고 있는 IP 주소가 아니라고 판단하여 클라이언트에게 해당 IP 주소를 할당하게 됩니다. V5812G는 DHCP 서버가 할당하려는 IP 주소의 사용여부를 확인하는데 Ping 테스트와 ARP 테스트를 모두 사용할 수 있고, 이 중 한가지 방법을 선택하면 됩니다. 다음 명령어를 사용하여 DHCP 서버가 할당할 IP 주소의 사용 여부를 확인할 테스트 방법을 선택하십시오.

명령어	모 드	기 능
ip dhcp validate {arp ping}	Global	할당 IP 주소의 사용 여부를 확인하기 위한 테스트 방법을 선택합니다.

한편, V5812G는 DHCP 서버에서 할당할 IP 주소의 사용 여부를 확인할 때, 응답 패킷을 몇 개를 받아서 확인할 것인지, Ping이나 ARP에 대한 응답을 얼마나 기다릴지 그 시간을 설정할 수 있습니다.

Ping 테스트나 ARP 테스트를 실행할 때, 응답 패킷을 몇 개 받아서 확인할 것인지, 테스트에 대한 응답을 얼마나 기다릴 것인지 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp {arp ping} packet <0-20>	Global	응답 받을 패킷 수를 설정합니다.
ip dhcp {arp ping} timeout <100-5000>		응답을 기다릴 시간을 설정합니다. .



응답 패킷의 횟수는 기본적으로 2번으로 설정되어 있습니다.



응답을 기다리는 시간의 설정 단위는 ms이며, 기본적으로 500ms으로 설정되어 있습니다.

(13) BOOTP Request 차단

DHCP 서버는 선택적으로 BOOTP(Bootstrap Protocol) request 패킷에 대한 응답을 하지 않을 수 있습니다. BOOTP request 패킷에 대한 응답을 하지 않으려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp bootp ignore	Global	BOOTP request 패킷을 무시하도록 설정합니다.
no ip dhcp bootp ignore		BOOTP request 패킷에 대한 설정을 해제합니다.

(14) IP 주소 할당 기준 설정

V5812G는 IP 주소를 할당하는 기준이 기본적으로 Client-id로 설정되어 있습니다. 그러나 Client-id 가 없는 장비도 있기 때문에 이러한 경우를 위해 IP 주소를 할당하는 기준을 Hardware-address로 바꿀 수 있습니다. IP 주소 할당 기준을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp database-key {client-id hardware-address}	Global	IP 주소 할당 기준을 설정합니다.



IP 주소 할당 기준은 기본적으로 **client-id**로 설정되어 있습니다.

(15) IP 주소 1:N 할당 방지

V5812G는 하나의 장비가 여러 개의 IP 주소를 요청해도 계속해서 IP 주소를 제공합니다. 물론, IP 주소가 여러 개가 필요한 장비도 존재하기 때문에 이러한 기능은 필요합니다. 그러나, 개인 PC는 IP 주소를 여러 개 할당 받을 필요가 없는데도 불구하고, IP 주소를 여러 개 받아가는 경우가 발생할 수 있습니다. 이러한 경우를 막기 위해 사용자는 하나의 장비에 하나 이상의 IP 주소를 할당하지 못하도록 설정할 수 있습니다.

MAC 주소가 동일한 장비로부터 IP 주소 요청이 두 번 이상 들어왔을 때, 두 번째부터는 요청을 무시하고 IP 주소를 할당하지 않도록 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp check client-hardware-address	Global	하나의 장비에 여러 개의 IP 주소를 할당하지 못하도록 설정합니다.

1:1 IP 할당 기능을 해제할 때에는 다음의 명령어를 사용하십시오.

명령어	모 드	기 능
no ip dhcp check client-hardware-address	Global	1:1 IP 할당 기능을 해제합니다.

(16) 고정 IP 사용자 차단

특정 DHCP 클라이언트가 할당 받은 IP 주소를 갱신하지 않고 계속 사용하려고 하여 IP Pool 자원을 낭비하는 경우가 있습니다. V5812G는 이러한 현상을 막기 위한 기능을 제공합니다. DHCP 서버가 30초 간격으로 IP 주소를 할당한 DHCP 클라이언트에게 해당 IP 주소를 사용하고 있는지 확인하고, 일정시간(Expire-time) 동안 응답이 없으면 할당한 IP 주소를 Pool로 복귀시키도록 하는 것입니다. 이는 IP Pool 자원의 낭비를 막는 것은 물론 DHCP 서버에서 권한이 없는 사용자로부터 ARP 응답을 차단함으로써 보안을 한층 더 강화할 수 있습니다.

고정 IP 사용을 차단하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp authorized-arp expire-time		고정 IP 사용자 차단 기능을 활성화하고 <i>expire-time</i> 까지 응답이 없을 때 IP 주소를 IP Pool로 복귀시킵니다.
ip dhcp authorized-arp start <i>start-time</i> timeout <i>expire-time</i>	Global	<i>start-time</i> 이후부터 고정 IP 사용자 차단 기능을 활성화하고 <i>expire-time</i> 까지 응답이 없을 때 IP 주소를 IP Pool로 복귀시킵니다.
no ip dhcp authorized-arp		고정 IP 사용자 차단 기능을 해제합니다.



참 고

*start-time*과 *expire-time*은 각각 <120-2147483637> 범위 내에서 설정할 수 있으며, 단위는 초(sec)입니다.



참 고

장비에 설정된 *start-time*의 기본값은 3600초(sec)입니다.

IP 주소 고정 사용으로 차단된 DHCP 클라이언트 목록을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip dhcp authorized-arp invalid	Enable/Global/	DHCP 클라이언트에게 할당되지 않은 IP 목록을 확인합니다.
show ip dhcp authorized-arp valid	Bridge	정상적으로 클라이언트에게 할당되어 사용되고 있는 IP 목록을 확인합니다.

IP 주소 고정 사용으로 차단된 DHCP 클라이언트 목록을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip dhcp authorized-arp invalid	Enable/Global/Bridge	DHCP 클라이언트에게 할당되지 않은 IP 목록을 삭제합니다.



참 고

위 기능은 DHCP 서버에서만 동작합니다. DHCP 릴레이 에이전트에서도 사용하려면 ARP Inspection 기능을 사용하십시오.

(17) Lease 데이터베이스 Backup

V5812G는 다음 명령어로 Lease 데이터베이스를 TFTP 서버에 저장할 수 있습니다. Backup 파일은 **leasedb.mac-address**의 형태로 저장됩니다. 명령어를 입력하는 순간 처음으로 저장되고, 그 시점을 기준으로 사용자가 설정한 주기로 업데이트 합니다. 따라서 이미 저장되고 있는 Lease 데이터베이스도 다시 명령어를 입력하면, 그 순간 다시 Backup되고, 설정한 주기 간격으로 업데이트 됩니다.

Lease 데이터베이스를 Backup 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp database ip-address Interval	Global	Lease 데이터베이스 Backup을 설정합니다.
no ip dhcp database		Lease 데이터베이스 Backup 설정을 해제합니다.



*interval*은 초 단위로, <120 - 2147483637> 사이에서 설정 가능합니다.

(18) Lease 데이터베이스 확인

DHCP 클라이언트에게 할당된 IP 주소에 대한 목록인 Lease 데이터베이스를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip dhcp lease {all free bound abandon offer fixed} [pool-name]	Enable/ Global/	Lease 데이터베이스를 확인합니다.
show ip dhcp lease detail [ip-address]	Bridge	

각 옵션으로 확인할 수 있는 내용은 다음과 같습니다.

- **all** : 모든 IP의 사용 현황을 보여줍니다.
- **free** : DHCP 클라이언트에게 할당 가능한 IP 현황을 보여줍니다.
- **bound** : DHCP 클라이언트에게 할당되어 있는 IP 현황을 보여줍니다.
- **abandon** : DHCP 서버에서 할당되지 않았는데도 DHCP 클라이언트에 의해 사용되고 있는 IP 현황을 보여줍니다.
- **offer** : DHCP 클라이언트의 요청으로 할당 대기 상태에 있는 IP 현황을 보여줍니다.
- **fixed** : DHCP 관리자가 수동으로 할당한 IP 현황을 보여줍니다.

(19) Lease 데이터베이스 초기화

V5812G는 다음 명령어로 Lease 데이터베이스를 초기화할 수 있습니다. DHCP 서브넷별로 초기화 하시려면 **ip-address/M** 옵션을, 각 IP Pool별로 초기화 하시려면 **pool pool-name** 옵션을, Lease 데이터베이스 전체를 초기화 하시려면 **all** 옵션을 사용하십시오.

명령어	모 드	기 능
clear ip dhcp leasedb ip-address/m	Enable/	
clear ip dhcp leasedb pool pool-name	Global/	Lease 데이터베이스를 초기화합니다.
clear ip dhcp leasedb all	Bridge	

(20) IP Pool 사이즈 설정

IP Pool의 최대 사이즈를 제한하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp max-pool-size <1-8>	Global	IP Pool 설정 내용을 확인합니다.

(21) IP Pool 설정 내용 확인

IP Pool 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

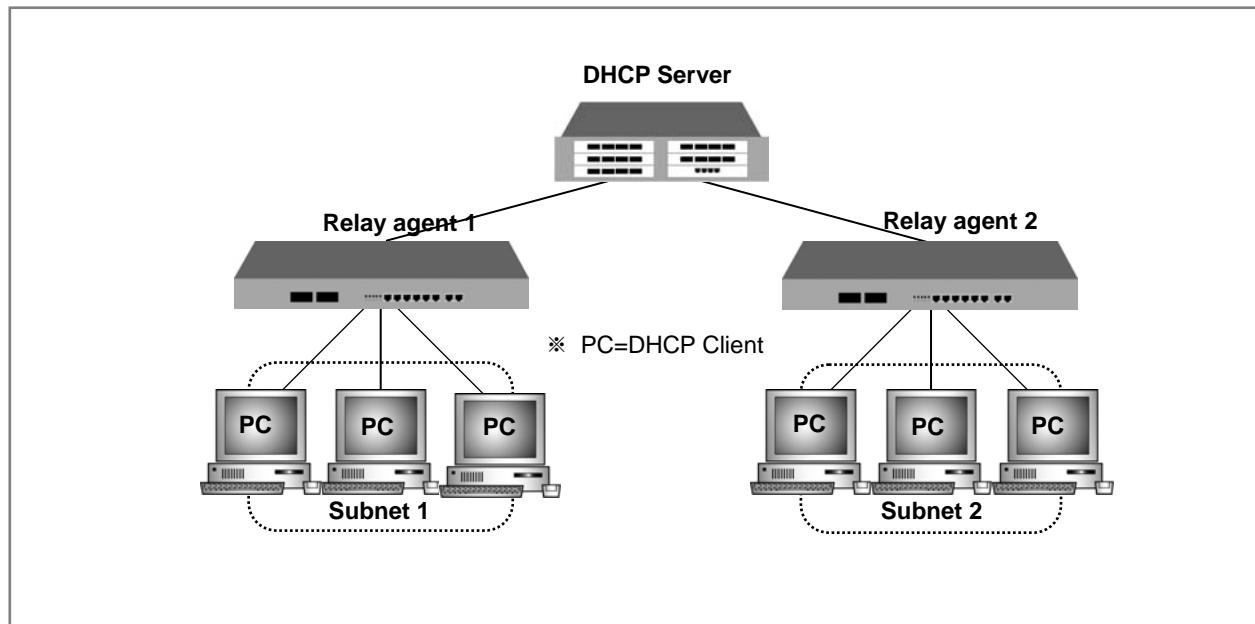
명령어	모 드	기 능
show ip dhcp pool [pool-name]	Enable/Global/	
show ip dhcp pool summary [pool-name]	Bridge	IP Pool 설정 내용을 확인합니다.

다음은 DHCP를 활성화하고, IP Pool을 설정한 후 할당 IP 주소 범위, 서브넷, IP 사용 시간, DNS 서버 등을 설정한 경우입니다.

```
SWITCH(config)# service dhcp
SWITCH(config)# ip dhcp pool test
SWITCH(config-dhcp[test])# network 100.1.1.0/24
SWITCH(config-dhcp[test])# range 100.1.1.1 100.1.1.100
SWITCH(config-dhcp[test])# lease-time default 5000
SWITCH(config-dhcp[test])# dns-server 200.1.1.1 200.1.1.2 200.1.1.3
SWITCH(config-dhcp[test])#
```

8.10.2. DHCP 릴레이 에이전트 설정

DHCP Relay 에이전트는 DHCP 클라이언트가 IP 주소를 요청할 때 DHCP 서버로 연결해 주고, 할당된 IP 주소를 DHCP 클라이언트에 전달해 주는 역할을 해 줍니다. Relay 에이전트를 사용하면 DHCP 서버가 관리할 수 있는 영역 이상의 서브넷을 관리할 수 있으므로 효과적입니다. Relay 에이전트로 설정된 장비는 DHCP 서버가 아니며 단지 DHCP 서버와 DHCP 클라이언트를 연결하는 다리 역할을 해 줄 뿐입니다.



【 그림 8-36 】 DHCP 서버와 Relay 에이전트 구성도의 예

복수의 DHCP 서버가 존재할 때, DHCP 클라이언트는 각 서버에서 할당된 여러 개의 IP 주소 중에서 가장 적합한 것을 선택하여 사용할 수 있습니다.

(1) DHCP Relay 에이전트 활성화

V5812G를 DHCP Relay 에이전트로 설정하시려면, 먼저 DHCP 서버로서 활성화 한 다음 DHCP Relay 에이전트로 설정하시면 됩니다.

1 단계 DHCP 서버로서 V5812G를 활성화합니다. 다음은 DHCP 서버로서 설정할 때 사용하는 명령어입니다.

명령어	모 드	기 능
service dhcp	Global	장비에 DHCP Relay 에이전트를 설정합니다.
no service dhcp		장비의 DHCP Relay 에이전트 설정을 해제합니다.

2 단계 DHCP Relay 에이전트로 설정합니다. DHCP Relay 에이전트로 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp helper-address helper-ip-address	Interface	장비를 DHCP Relay 에이전트로 설정합니다.



*helper-ip-address*는 DHCP 서버 주소나 DHCP 서버로 갈 수 있는 게이트웨이의 IP 주소를 입력합니다.

한편, DHCP Relay 에이전트로 등록할 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip dhcp helper-address ip-address	Interface	해당 주소로 등록한 DHCP Relay 에이전트를 해제합니다.
no ip dhcp helper-address all		설정된 DHCP Relay 에이전트 모두 삭제합니다.

(2) DHCP server-ID 옵션 설정

DHCP 클라이언트가 DHCP_Discover 메시지를 DHCP 릴레이 에이전트를 통해 복수의 DHCP 서버에 보낼 경우, 이 메시지는 모든 서버에 Broadcasting 됩니다. 그러나 오직 하나의 서버만이 해당 클라이언트에게 DHCP_Offer 메시지로 응답합니다. 이 특정 서버로 클라이언트가 DHCP_Request 메시지를 보낼 수 있도록 사용자는 릴레이 에이전트에 DHCP server-id 를 인지할 수 있게 설정할 수 있습니다.

클라이언트로부터 받은 DHCP_Request 메시지가 특정 서버에 전송될 수 있도록 DHCP 릴레이 에이전트에 DHCP server-id 옵션을 활성화하거나 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp relay aware-server-id	Global	DHCP server-id 옵션을 활성화합니다.
no ip dhcp relay aware-server-id		DHCP server-id 옵션을 해제합니다.

(3) Vendor별 DHCP 서버 지정

V5812G는 DHCP Relay 에이전트로 설정할 때, Vendor별로 DHCP 서버를 지정하도록 설정할 수 있습니다. 일반적으로 장비의 MAC 주소의 앞자리 6자리(XX:XX:XX)를 OUI(Vendor-id)라고 하는데, IP 주소를 요청하는 클라이언트의 OUI를 확인하여 OUI에 따라 지정된 DHCP 서버로부터 IP 주소를 할당 받을 수 있도록 하는 것입니다.

Vendor별로 DHCP 서버를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp oui vendor-id helper-address helper-ip-address	Interface	Vendor별로 DHCP 서버를 지정하여 DHCP Relay 에이전트로 설정합니다.



vendor-id는 MAC 주소의 앞자리 6자리수를 말하며 XX:XX:XX의 형태입니다.

Vendor별로 DHCP 서버를 설정한 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip dhcp oui vendor-id helper-address helper-ip-address	Interface	Vendor별로 DHCP 서버를 지정하여 DHCP Relay 에이전트로 설정한 것을 해제합니다.

(4) Smart Relay 설정

V5812G는 복수의 IP 주소를 설정할 수 있기 때문에 DHCP Relay 에이전트가 여러 개의 IP 주소를 가지고 있을 수 있습니다. 이러한 경우 일반적인 DHCP Relay 에이전트는 무조건 Primary IP 주소를 가지고 DHCP 서버에게 IP 주소를 요청하게 됩니다.

Smart Relay는, 여러 개의 IP 주소를 가진 DHCP Relay 에이전트가 클라이언트로부터 IP 주소 요청을 받았을 때, 일단은 Primary IP 주소를 가지고 IP 주소를 요청하지만, 이에 대한 서버의 응답이 없을 때에는 Secondary IP 주소를 가지고 DHCP 서버에 다시 IP 주소를 요청하는 기능입니다. 2개 이상의 IP 주소가 설정되어 있다면, 그 이후의 동작은 처음과 동일합니다. Smart relay 기능을 설정 하려면, 다음 명령어를 사용하십시오.

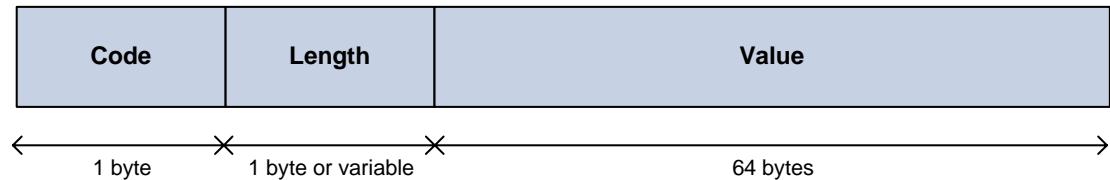
명령어	모 드	기 능
ip dhcp smart-relay	Global	Smart relay 기능을 설정합니다.
no ip dhcp smart-relay		Smart relay 기능을 해제합니다.

8.10.3. DHCP Option 설정

새롭게 구현된 DHCP Option 설정은 다양한 Option을 선택할 수 있을 뿐 아니라 Format의 설정에 따라 Option을 지정할 수 있어서 각각 네트워크 상황에 유연하게 대처할 수 있는 이점이 있습니다.

DHCP Option Format의 종류는 다음과 같이 구별됩니다.

DHCP Option Format



Code는 각각의 DHCP Option을 정의해주는 역할을 하며, 0에서 255 값 중에서 선택이 가능합니다. 또한 Option에 대한 Code 값은 표준에 일부 정의되어 있습니다. (128-254는 특정 사이트를 뜻함)

Length는 Option 값에 따라 가변적으로 변하기도 하며, 고정된 값으로 사용하기도 합니다.

Option Value는 실제 해당 정보를 담고 있는 필드로 IP 주소, String, Index 등 여러가지 종류의 값을 설정할 수 있습니다.

관리자는 먼저 DHCP Option 설정 모드에 들어가서 DHCP Option Format을 설정해야 합니다. DHCP Option Format은 DHCP 서버 Option, DHCP Snooping Option, DHCP Option82 Sub-option에 적용됩니다.

(1) DHCP Option 활성화

DHCP Option가 활성화되면서 DHCP Option 설정 모드로 들어갑니다. DHCP Option 설정 모드에서는 Option Format 관련 설정을 할 수 있습니다.

DHCP Option 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp option format format-name	Global	DHCP Option을 설정하기 위해 DHCP Option 설정 모드로 들어갑니다.

(2) DHCP Option 설정하기

특정 DHCP Option 설정 모드로 들어간 후에 Option Format 관련 세부 설정을 할 수 있습니다.

해당 Option에 대한 설정을 위해 특정 Attribute를 정의하여 종류(Type), 필드 길이(Length), 설정값(Value)를 지정하게 됩니다. 각 필드의 정의는 다음과 같습니다.

- **attr** : Option에 들어갈 각각의 Attribute를 정의합니다. 복수로 설정 가능하며 1에서 32까지 입력할 수 있고, 해당 ID에 따라 Option에 설정되는 순서가 결정됩니다.
- **type** : Option의 실제 값인 Value의 종류를 설정합니다. 0에서 255까지 설정 가능합니다.
- **length** : Option 필드의 길이를 나타내며, value의 길이를 고정으로 1에서 64 중 지정하거나 variable 옵션을 선택하여 value에 따라 바뀌게 할 수도 있습니다.
- **value** : Option의 실제 값으로 **hex**, **index**, **ip**, **string**, **if_ip** 형태로 설정 가능합니다.

해당 DHCP Option Format을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
attr <1-32> type <0-255> length {<1-64> variable} value {hex index ip string if_ip} value		DHCP Option을 정의하는 Attribute 값의 Type, Length, Value를 설정합니다.
attr <1-32> type <0-255> length-hidden {<1-64> variable} value {hex index ip string if_ip} value		
attr <1-32> length variable value {hex index ip string if_ip} value	DHCP Option	DHCP Option을 정의하는 Attribute 값의 Length와 Value를 설정합니다.
attr <1-32> length <1-64> value {hex index ip string if_ip} value		
attr <1-32> length-hidden variable value {hex index ip string if_ip} value		DHCP Option을 정의하는 Attribute 값의 Value를 설정합니다.
attr <1-32> length-hidden <1-64> value {hex index ip string if_ip} value		



참 고

value는 %VALUE(특수문자 % + 대문자)로 입력해야 합니다. 예를 들면 %PORT의 경우에는 포트 번호를 Option 값으로 설정하는 것입니다. Option 실행 시 시스템 내부에서 동적으로 설정되는 값은 다음과 같이 5가지로 나뉘어 집니다. %PORT(포트 번호), %FRAME(프레임 개수), %SLOT(슬롯 번호), %VID(VLAN ID), %CPU-MAC(시스템 MAC 주소)

DHCP Option의 특정 Attribute 설정을 모두 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no attr <1-32>	DHCP Option	특정 Attribute 관련 설정값을 모두 삭제합니다.

(3) DHCP Option 삭제

설정된 특정 DHCP Option Format을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip dhcp option format format-name	Global	설정된 DHCP Option Format을 삭제합니다.

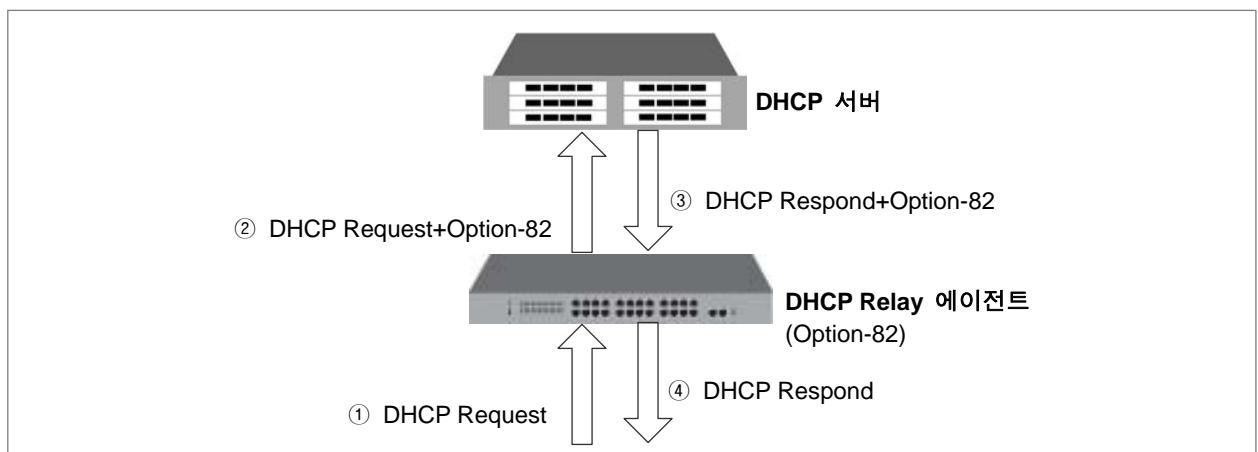
(4) DHCP Option 확인

시스템에 정의된 DHCP Option 설정을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>show ip dhcp option format format-name</code>	Enable/ Global/ DHCP Option	DHCP Option 설정을 확인합니다.
<code>show ip dhcp option format format-name port port-number vlan vid</code>		포트와 VLAN에 따른 DHCP Option 설정을 확인합니다.

8.10.4. DHCP Option-82 설정

가입자 망의 규모가 날로 거대해지고 있는 환경에서 DHCP 서버는 많은 가입자들에게 IP 주소를 할당해야 합니다. 이 때 DHCP Option-82를 사용하여 효율적으로 가입자들을 관리할 수 있습니다. DHCP Option-82는 DHCP Relay 에이전트가 DHCP Request 패킷에 Option-82라고 하는 정보를 덧붙여 보냄으로써, 이 정보를 통해서 가입자를 인증하는 것입니다. DHCP 서버는 Option-82를 사용하여 IP 주소를 할당하고, 서버의 접속을 제한함은 물론, 가입자들에게 차별화된 서비스를 제공하고, 보안성도 한층 높이게 되었습니다. V5812G는 Option-82의 내용으로 포트 번호와 Remote ID를 DHCP 서버에 전송합니다. 그리고, 포트 번호가 Remote ID보다 우선 순위가 더 높습니다. Option-82 정보가 없는 Request 패킷을 받았을 때에는 자신의 정보를 첨부하며, Option-82에 기록된 Remote ID가 자신의 시스템 MAC 주소와 동일할 경우에는 Option-82에서 지정한 포트 번호로 Option-82를 제거한 후 전송합니다. 다음은 DHCP Option-82를 사용하는 경우에서 패킷의 흐름을 간단하게 나타낸 것입니다.



【 그림 8-37 】 DHCP Option-82를 사용하는 경우의 패킷 흐름

(1) DHCP Option-82 활성화

V5812G에 DHCP Option-82를 활성화하려면, 다음 명령어를 사용하십시오. DHCP Option-82가 활성화되면서 Option-82 설정 모드로 들어갑니다. Option-82 설정 모드에서는 Remote-ID 관련 설정을 할 수 있습니다.

명령어	모 드	기 능
ip dhcp option82	Global	DHCP Option-82를 활성화합니다.
no ip dhcp option82		DHCP Option-82를 비활성화합니다.

(2) Option-82 패킷 정책 설정

V5812G의 관리자는 DHCP 서버 또는 Relay 에이전트에 DHCP Option-82 패킷이 들어왔을 때, 이 패킷을 어떻게 처리할 것인지에 대한 정책을 설정할 수 있습니다.

Option-82 패킷에 대한 정책을 설정하려면 Option-82 설정 모드에서 다음 명령어를 사용하십시오. 각 옵션의 패킷 정책은 다음과 같습니다.

- **drop** : 패킷에 Option-82 정보 있으면 버립니다.
- **keep** : Option-82 정보 조작을 하지 않고 그대로 목적지로 전송합니다.
- **replace** : 수신된 패킷의 Option-82 정보를 사용자 장비 시스템의 Option-82 설정 내용으로 바꾼 뒤, 목적지로 전송합니다.

명령어	모 드	기 능
policy {keep replace}	Option-82	패킷의 Option-82 정보에 대한 정책을 설정합니다.
policy drop {normal option82 all}		



기본적으로 Option-82 패킷에 대한 정책은 **keep**으로 설정되어 있습니다.

(3) 시스템 Remote-ID, Circuit-ID 설정

Option-82 환경에서 전송되는 패킷은 Remote-ID와 Circuit-ID를 포함하고 있습니다. V5812G 스위치는 기본적으로 MAC 주소가 Remote-ID가 되고, 포트 번호가 Circuit-ID가 됩니다. 그러나, 다음 명령어를 사용하면, 관리자는 Remote-ID와 Circuit-ID의 형식을 변경할 수 있습니다. 이 때, 설정하는 장비가 서버일 경우에는 서버에 들어온 패킷의 Remote-ID와 Circuit-ID를 변경하게 되고, 설정한 장비가 Relay일 경우에는 서버와 동일하게 Remote-ID와 Circuit-ID 형식을 맞추기 위해 변경하도록 설정하면 됩니다. Remote-ID의 형식을 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
system-remote-id hex hexstring		
system-remote-id ip ip-address	Option-82	Remote-ID의 형식을 변경합니다.
system-remote-id text remote-id		
system-remote-id option format format-name		

Circuit-ID의 형식을 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
system-circuit-id port-number hex hexstring		
system-circuit-id port-number index <0-65535>	Option-82	
system-circuit-id port-number text remote-id		Circuit-ID의 형식을 변경합니다.
system-circuit-id port-number option format format-name		
system-circuit-id port-type physical		

Remote-ID와 Circuit-ID의 형식을 변경한 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no system-remote-id		
no system-remote-id option format	Option-82	Remote-ID와 Circuit-ID의 형식을 변경한 것을 해제합니다.
no system-circuit-id port-number		
no system-circuit-id port-number option format		
no system-circuit-id port-type physical		

(4) DHCP Option82 Trust 패킷 설정

Option82 패킷의 기본 정책을 설정하려면 다음 명령어를 사용하십시오. 기본적으로는 Option82 정보 중 remote-id, circuit-id만을 고려하도록 되어 있습니다.

명령어	모 드	기 능
trust default {deny permit}	Option-82	Option-82 패킷에 대한 정책을 설정합니다.

Remote-ID의 형식을 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
trust remote-id hex hexstring	Option-82	Remote-ID의 형식을 변경합니다.
trust remote-id ip ip-address		
trust remote-id text remote-id		
no trust remote-id hex hexstring		Remote-ID의 형식을 해제합니다.
no trust remote-id ip ip-address		
no trust remote-id text remote-id		

포트에 대한 Option82 패킷의 정책을 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
trust port port-number {normal option82 all}	Option-82	포트에 대한 패킷의 정책을 설정합니다.

포트에 대한 Option82 패킷의 정책을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no trust port port-number {normal option82 all}	Option-82	포트에 대한 패킷의 정책을 해제합니다.

8.10.5. Class 설정

DHCP 서버는 Option 82 패킷이 전해주는 두 가지 정보, 포트 번호와 Remote-ID를 가지고, IP 주소 할당 여부를 결정합니다. 따라서 DHCP 서버 관리자는 이 두 가지 정보 가운데 어떤 정보를 가지고 패킷에게 IP 주소를 할당 할 것인지 그 조건을 설정해야 합니다.

V5812G는 IP 주소 할당 여부를 결정하는 Option 82 패킷의 조건을 Class별로 설정하고, 설정된 Class에 해당하는 Option 82 패킷을 가진 클라이언트에게만 IP 주소를 할당하도록 할 수 있습니다. 이때, Class에 따라 정해진 범위 내에서의 IP 주소를 할당하도록 할 수 있습니다.

Class를 설정하여 IP 주소를 할당하는 방법은 다음과 같습니다.

- 1 단계 Class를 만듭니다.
- 2 단계 해당 Class에 Option 82 패킷의 조건을 설정합니다.
- 3 단계 해당 Class에 할당할 수 있는 IP 주소 대역을 설정합니다.

(1) Class 만들기

Class 기능을 사용하기 위해 먼저 Class를 만들어야 합니다. Class를 만들면, Option 82 패킷의 정보를 설정할 수 있는 DHCP Class 설정 모드로 들어가게 됩니다. DHCP Class 설정 모드로 들어가면, 시스템 프롬프트가 SWITCH(config)#에서 SWITCH(config-dhcp-class[class-name])#으로 변경됩니다.

다음은 Class를 만들어 DHCP Class 설정 모드로 들어갈 때 사용하는 명령어입니다.

명령어	모 드	기 능
ip dhcp class class-name	Global	Class를 만들고 DHCP Class 설정 모드로 들어갑니다.
no ip dhcp class class-name		Class를 삭제합니다.



참 고

위의 명령어를 사용하여 Class를 삭제하면 Option 82 패킷의 정보에 대해 설정한 값도 모두 사라집니다.

(2) Option 82 패킷 설정

Class를 만들었다면, 해당 Class에 적용되는 Option 82 패킷의 정보를 설정해야 합니다. Option 82 패킷의 정보를 설정해야 그 정보를 보고 IP 주소 할당 여부를 결정할 수 있습니다.

Class에 Option 82 패킷의 정보를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
relay-information remote-id ip ip address [circuit-id hex hexstring]	DHCP Class	Option 82 패킷의 정보가 되는 Remote-ID와 Circuit-ID를 설정합니다.
relay-information remote-id ip ip address [circuit-id text string]		
relay-information remote-id ip ip address [circuit-id index index]		
relay-information remote-id hex hexstring [circuit-id hex hexstring]		
relay-information remote-id hex hexstring [circuit-id text string]		
relay-information remote-id hex hexstring [circuit-id index index]		
relay-information remote-id text string [circuit-id hex hexstring]		
relay-information remote-id text string [circuit-id text string]		
relay-information remote-id text string [circuit-id index index]		

Class에 설정한 Option 82 패킷의 정보를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no relay-information remote-id ip ip address circuit-id hex hexstring	DHCP Class	Option 82 패킷의 정보가 되는 Remote-ID와 Circuit-ID의 설정을 삭제합니다.
no relay-information remote-id ip ip address circuit-id text string		
no relay-information remote-id ip ip address circuit-id index index		
no relay-information remote-id hex hexstring circuit-id hex hexstring		
no relay-information remote-id hex hexstring circuit-id text string		
no relay-information remote-id hex hexstring circuit-id index index		
no relay-information remote-id text string circuit-id hex hexstring		
no relay-information remote-id text string circuit-id text string		
no relay-information remote-id text string circuit-id index index		

설정 내용을 한꺼번에 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no relay-information remote-id all	DHCP Class	Remote-id에 대한 설정 값을 모두 삭제합니다.
no relay-information all		모든 설정 내용을 삭제합니다.

(3) IP 주소 범위 설정

위에서 설정한 Class에 IP 주소를 할당하도록 하려면, IP Pool 모드에서 해당 Class를 불러내어 할당할 IP 주소의 대역폭을 설정하십시오. IP Pool 모드에서 해당 Class를 불러내면, IP Pool Class 모드로 들어가게 됩니다.

할당 IP 주소 범위를 설정하기 위해 IP Pool 모드에서 Class를 불러내려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
class class-name	IP Pool	IP Pool 모드에서 해당 Class를 불러냅니다.
no class class-name		IP Pool 모드에서 불러낸 Class를 삭제합니다.



위의 명령어에서 입력하는 *class-name*은 이미 만들어진 Class 이름입니다.



위의 명령어를 사용하여 Class를 삭제하면 할당 IP 주소의 범위에 대해 설정한 값도 자동으로 사라집니다.

IP Pool 모드에서 Class를 불러내어 Class 모드에 들어갔다면, 다음 명령어를 사용하여 할당 IP 주소의 범위를 설정할 수 있습니다.

명령어	모 드	기 능
address range start-ip-address end-ip-address	IP Pool Class	할당할 IP 주소의 범위를 설정합니다.

(4) Class 기능 활성화

Class를 만들고, Class에 해당하는 Option 82 패킷의 값과 할당할 IP 주소의 범위를 모두 설정해도, Class 기능을 활성화하지 않으면 이 기능을 동작하지 않습니다.

Class 기능을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp use class	Global	Class 기능을 활성화합니다.
no ip dhcp use class		Class 기능을 해제합니다.

8.10.6. DHCP 클라이언트

V5812G는 DHCP 클라이언트로 설정하여 DHCP 서버로부터 자동으로 IP 주소를 할당 받도록 할 수 있습니다. V5812G가 DHCP 클라이언트로 지정되었을 경우, L2 네트워크 환경에서의 일반적인 스위치로서 동작하게 되고, DHCP 클라이언트 환경에서는 DHCP 서버와 DHCP Relay 에이전트로 설정될 수 없습니다.

(1) DHCP 클라이언트 활성화

DHCP 클라이언트로 동작하려면, Interface 설정 모드에서 자동으로 IP 주소를 할당 받을 수 있도록 설정해야 합니다. IP 주소를 DHCP 서버로부터 자동으로 할당 받으려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip address dhcp	Interface	해당 Interface의 IP 주소를 자동으로 할당 받도록 설정합니다.
no ip address dhcp		자동으로 IP 주소를 할당 받도록 설정한 것을 해제합니다.

(2) Client-id 설정

DHCP 클라이언트로 설정된 상태에서 IP 주소를 할당 받으려면 Client-id를 가지고 있어야 합니다. DHCP 클라이언트가 된 V5812G에 Client-id를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp client client-id hex hexstring	Interface	DHCP 클라이언트로서의 Client-id를 설정합니다.
ip dhcp client client-id text string		



참 고

DHCP 클라이언트의 Client-id는 기본적으로 hardware-address 01:00:XX:XX:XX:XX 로 설정되어 있습니다.

Client-id를 기본값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip dhcp client client-id	Interface	Client-id를 기본값으로 되돌립니다.

(3) Class-id 설정

Class-id는 IP 주소를 요청하는 클라이언트를 Vendor 별로 분류하기 위해 이용됩니다. V5812G에 Class-id를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp client class-id hex hexstring	Interface	Class-id를 할당합니다.
ip dhcp client class-id text string		



참 고

DHCP 클라이언트의 Class-id는 기본적으로 “DASAN Networks”로 설정되어 있습니다.

Class-id를 기본값으로 돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip dhcp client class-id	Interface	Class-id를 기본값으로 되돌립니다.

(4) 호스트 이름

사용자는 DHCP 클라이언트로서 V5812G가 사용할 호스트 이름을 설정할 수 있습니다. 클라이언트가된 V5812G가 사용할 호스트 이름을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp client host-name hostname	Interface	클라이언트에 호스트 이름을 설정합니다.
no ip dhcp client host-name		설정했던 호스트 이름을 삭제합니다.



참 고

DHCP 클라이언트의 호스트 이름은 기본적으로 “switch”로 설정되어 있습니다.

(5) IP 주소 사용 시간 제한

V5812G는 DHCP 클라이언트로서 할당 받은 IP 주소를 얼마나 사용할 것인지, 그 사용 시간을 정할 수 있습니다. IP 주소의 사용 시간을 설정하면, 정해진 시간이 끝나기 전에 DHCP 서버가 IP 주소 사용 연장 의사를 물어보게 되어 있습니다. 할당 받은 IP 주소의 사용 시간을 설정하려면, Interface 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp client lease-time <120-2147483637>	Interface	클라이언트에 할당하는 IP 주소의 사용시간을 설정합니다.



참 고

IP 주소 사용 시간의 설정 단위는 초이며 기본적으로 3600초로 설정되어 있습니다.

설정을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip dhcp client lease-time	Interface	설정했던 IP 주소의 사용시간을 삭제합니다.

(6) DHCP 서버로부터 정보 요청

DHCP 서버는 DHCP 클라이언트가 접속을 하면, 기본적으로 IP 주소와 함께 디폴트 게이트웨이, IP 사용 가능 시간, 그리고 사용할 수 있는 DNS 서버와 도메인 이름 등을 자동으로 알려줍니다. V5812G는 클라이언트로 설정되었을 때, DHCP 서버가 자동으로 알려주는 정보 가운데 도메인 이름과 DNS 서버에 대한 것은 받지 않도록 설정할 수 있습니다. DHCP 서버로부터 자동으로 전달되는 도메인 이름과 DNS 서버에 대한 정보를 차단하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip dhcp client request {domain-name dns}	Interface	DHCP 서버가 자동으로 도메인 이름과 DNS 서버에 대한 정보를 전달하지 않도록 합니다.



참 고

DHCP 서버는 자동적으로 도메인 이름과 DNS 서버에 대한 정보를 보내도록 되어 있습니다. 따라서 이 정보를 자동으로 전달하는 것을 막기 위해서는 no 명령어를 사용하셔야 합니다.

DHCP 서버로부터 도메인 이름과 DNS 서버에 대한 정보가 다시 자동적으로 전달 되도록 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp client request {domain-name dns}	Interface	DHCP 서버에서 필요한 정보를 요청합니다.

(7) IP 주소 사용 중단

자동으로 할당 받은 IP 주소의 사용을 중단하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
release dhcp interface-name	Enable	할당 받은 IP의 사용을 중단합니다.

(8) IP 주소 재요청

IP 주소의 사용을 중단하였다가 다시 IP 주소를 할당 받기 원한다면, 다음 명령어를 IP 주소를 재요청 해야 합니다.

명령어	모 드	기 능
renew dhcp interface-name	Enable	IP 주소를 재요청합니다.

(9) DHCP 클라이언트 설정 확인

다음 명령어를 사용하면 DHCP 클라이언트로 설정된 V5812G의 DHCP 클라이언트 관련 설정 내용을 확인할 수 있습니다.

명령어	모 드	기 능
show ip dhcp client interface-name	Interface	클라이언트 설정을 확인합니다.

8.10.7. DHCP Snooping 설정

DHCP Snooping은 untrust 상태인 인터페이스로 전달되는 DHCP 메시지를 필터링하고, DHCP binding 테이블을 관리하면서 DHCP의 보안을 보장하는 기능입니다.

DHCP Snooping 기능은 DHCP Relay 에이전트에 설정되는데, DHCP 서버와 연결된 포트를 Trust 포트라고 하고 그 이외에 포트들을 Untrust 포트라고 합니다. DHCP Snooping이 동작하면, DHCP Relay 에이전트는 Trust 포트를 통해 할당되는 IP 주소만 제대로 된 서버로부터 할당된 IP 주소라고 인식하여 받아들이게 됩니다. 그리고 DHCP Snooping가 설정된 인터페이스에서 일어나는 IP 주소 할당에 대한 기록은 DHCP binding 테이블에서 관리가 되는데, 이 때 기록되는 내용은 해당 인터페이스가 속한 VLAN의 vlan-id, IP 주소를 할당 받은 포트 번호, 할당 받은 IP 주소, 할당 받은 클라이언트의 MAC 주소 등이 있습니다.

V5812G는 DHCP Snooping을 시스템 전체에 설정할 수도 있고, VLAN 별로 설정할 수도 있습니다.



DHCP Snooping은 DHCP Relay 에이전트로서 활성화되어야만 정상적으로 동작합니다.

(1) DHCP Snooping 활성화

V5812G는 DHCP Snooping을 시스템 전체에 활성화시킬 수 있습니다. 시스템 전체에 DHCP Snooping 기능을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping	Global	시스템 전체에 DHCP Snooping을 활성화합니다.
no ip dhcp snooping		시스템 전체에 활성화시켰던 DHCP Snooping을 해제합니다.



DHCP Snooping은 기본적으로 비활성화 되어 있습니다.

(2) VLAN별 DHCP Snooping 설정

V5812G는 VLAN 별로 DHCP Snooping 기능을 설정할 수도 있습니다. VLAN별로 DHCP Snooping 을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping vlan <i>vlan-id</i>	Global	VLAN별로 DHCP Snooping을 설정합니다.
no ip dhcp snooping vlan <i>vlan-id</i>		VLAN별로 설정한 DHCP Snooping을 해제합니다.

(3) Trust 포트 지정

Trust 포트란, DHCP 서버와 연결되어 있는 포트를 말합니다. DHCP Snooping이 활성화되는 상태에서는 Untrust 포트로부터 할당되는 DHCP 메시지는 Drop 처리 하도록 되어 있습니다. Trust 포트를 지정하려면,, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping trust <i>port-number</i>	Global	Trust 포트를 지정합니다.
no ip dhcp snooping trust <i>port-number</i>		Untrust 포트를 지정합니다.

(4) Trust 포트 DHCP 패킷 필터링

지정된 Trust 포트로부터 나가는 브로드캐스트 요청 패킷을 필터링하려면,, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping trust <i>port-number</i> filter egress bcast-req	Global	지정된 Trust 포트의 Egress 브로드캐스트 요청 패킷을 필터링합니다.
no ip dhcp snooping trust <i>port-number</i> filter egress bcast-req		설정된 Egress 브로드캐스트 요청 패킷 필터링 기능을 해제합니다.

(5) DHCP 패킷 수 제한

V5812G는 포트로 전송되는 DHCP 패킷을 제한하여 CPU의 과부하를 막을 수 있습니다. 포트로 전송되는 DHCP 패킷을 제한하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping limit-rate <i>port-number <1-255></i>	Global	포트에 전송되는 초당 DHCP 패킷 수를 설정합니다.
no ip dhcp snooping limit-rate <i>port-number</i>		설정한 초당 DHCP 패킷 수를 삭제합니다.



참 고

untrusted 클라이언트에 대한 limit rate는 초당 15로 설정하길 권고합니다. 일반적으로 limit rate는 untrusted 인터페이스에 적용하지만 limit rate를 trusted 인터페이스에 설정하고 싶다면, trusted 인터페이스는 스위치로 들어오는 모든 DHCP 트래픽을 받아들이는 것을 기억하여야 합니다. 따라서 limit rate를 상당히 높게 설정해 주어야 합니다. 이 임계치(threshold)는 네트워크 설정에 따라 달라져야 하며 CPU는 DHCP 패킷이 초당 1000 패킷 이상이 지속적으로 유입되면 수신하지 못합니다.

DHCP 서버를 악의적으로 공격하는 것을 방지하기 위해 동일한 MAC 주소에 대한 DHCP 클라이언트의 DHCP discover 메시지를 초당 1개씩만 처리하도록 설정할 수 있습니다.

같은 DHCP 클라이언트 MAC 주소로 한정하여, 초당 한 개의 DHCP discover 메시지를 처리하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping limit-rate discover	Global	포트에 전송되는 1 초당 한 개의 DHCP discover 패킷을 수신하도록 설정합니다.
no ip dhcp snooping limit-rate discover		1초당 DHCP discover 패킷 수 제한하는 기능을 해제합니다.



주 의

이 기능을 사용하려면 반드시 DHCP Snooping이 활성화되어야 합니다.

(6) 바인딩 테이블에 등록되는 IP 주소 개수 제한

바인딩 테이블에 등록되는 IP 주소 개수를 제한할 수 있습니다. 바인딩 테이블에 등록되는 IP 주소를 제한하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping limit-lease port-number <1-2147483637>	Global	바인딩 테이블에 등록되는 IP 주소 개수를 제한합니다.
no ip dhcp snooping limit-lease port-number		바인딩 테이블에 등록되는 IP 주소 개수를 제한했던 것을 해제합니다.

(7) 바인딩 테이블 Backup

V5812G는 바인딩 테이블을 Backup할 곳과 자동 업데이트 시간 간격을 설정할 수 있습니다. 바인딩 테이블을 Backup 할 곳과 업데이트 시간 간격을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping database ip-address <120-2147483637>	Global	바인딩 테이블을 Backup할 곳과 자동 업데이트 시간 간격을 설정합니다.
no ip dhcp snooping database		바인딩 테이블 Backup 관련 설정을 삭제합니다.

한편, 바인딩 테이블을 다른 곳에 다시 Backup하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping database renew ip-address	Global	설정한 곳에 바인딩 테이블을 Backup 합니다.

(8) 바인딩 테이블 Static 등록

V5812G는 DHCP snooping 바인딩 테이블을 Static으로 등록할 수 있습니다. 바인딩 테이블을 Static으로 등록하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping binding <1-4094> port-number ip-address client-mac-address <120-2147483637>	Global	Snooping 바인딩 테이블에 Static으로 내용을 등록합니다.
clear ip dhcp snooping binding port-number {ip-address all}		Static으로 등록한 내용을 삭제합니다.

(9) MAC 주소를 통한 관리

DHCP Snooping 바인딩 테이블의 MAC 주소 정보를 기준으로 바인딩 테이블에 맞지 않는 패킷이 접근했을 때 이를 받아들이지 않도록 할 수 있습니다.

MAC 주소를 기반으로 DHCP 패킷을 관리하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping verify mac-address	Global	Snooping 바인딩 테이블의 MAC 주소를 기반으로 DHCP 패킷을 관리하도록 설정합니다.
no ip dhcp snooping verify mac-address		Snooping 바인딩 테이블의 MAC 주소를 기반으로 DHCP 패킷을 관리하도록 설정한 것을 해제합니다.

(10) ARP Inspection Start Time 설정

V5812G는 ARP Inspection이 동작을 시작하는 시간을 설정할 수 있습니다. ARP Inspection은 DHCP Snooping 바인딩 테이블 정보를 이용하여 ARP 패킷의 유효성을 검사하고, 유효하지 않는 패킷은 허용하지 않는 기능입니다.



주의

이 기능을 사용하려면 반드시 ARP Inspection을 활성화 시켜야 합니다.

하지만, 사용자의 장비가 어떠한 이유로든 재부팅 된다면 DHCP Snooping 바인딩 테이블 정보는 손실되고, ARP Inspection 기능이 제대로 동작하지 않을 수 있습니다. 따라서, 장비가 재부팅 된다면 DHCP Snooping 바인딩 테이블이 생성될 때까지 ARP Inspection이 동작하지 않아야 합니다. 만약, 장비가 재부팅 된 후에 아무런 대기 시간도 없이 ARP Inspection이 동작한다면, DHCP Snooping 바인딩 테이블 정보가 생성되기 전까지 모든 ARP 패킷이 폐기됩니다. 이러한 현상을 방지하기 위해 V5812G는 장비가 재부팅 되었을 때 ARP Inspection이 곧바로 시작되지 않고 일정한 시간이 지난 후에 시작되도록 설정할 수 있습니다. ARP Inspection 시작 대기 시간을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping arp-inspection start <1-2147483637>	Global	장비가 재부팅되었을 때를 위한 ARP Inspection 시작 대기 시간을 설정합니다.
no ip dhcp snooping arp-inspection start		설정한 ARP Inspection 시작 대기 시간을 삭제합니다.



참 고

위 설정 중 <1-2147483637> 값의 단위는 초(second)입니다. 기본값은 1800초로 설정되어 있습니다.

(11) DHCP Snooping Option 82 설정

L2 네트워크 환경에서 DHCP 서버로 DHCP 메시지들을 Forwarding 할때, 스위치는 Client가 보낸 메시지에서 DHCP option 82 데이터를 추가하거나, 삭제할 수 있습니다. 장비가 DHCP Snooping이 활성화되어 있다면, 기본적으로 DHCP 패킷에 DHCP Option 82 필드를 포함하고 서버에 전송합니다. 이 기능은 L2 네트워크 환경에서 IP 할당의 효율성과 보안성을 유지할 수 있게 합니다.

L2 환경에서 DHCP Snooping 스위치로부터 Forwarding되는 DHCP 패킷에 Option 82 필드를 추가하거나 제거하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping information option	Global	Forwarding 하는 DHCP 패킷에 Option 82 필드를 추가합니다.
no ip dhcp snooping information option		Forwarding 하는 DHCP 패킷에 Option 82 필드를 삭제합니다.

(12) DHCP Snooping Option 설정

가입자마다 전송하는 DHCP 패킷의 Option 종류는 매우 다양합니다. 그러나 DHCP 서버는 DHCP 클라이언트가 보내는 각각의 다른 DHCP 패킷 Option에 따라 정보를 제공하고, 클라이언트를 관리하는 것이 어렵기 때문에 가입자에게 반드시 제공해야할 정보를 전하지 못하는 경우가 생기게 됩니다.

이러한 문제를 해결하기 위해 DHCP 클라이언트가 전송한 DHCP 패킷(DISCOVER/REQUEST)의 Option을 DHCP Snooping에서 변경 또는 추가할 수 있습니다. 시스템이나 포트별로 DHCP Snooping Option을 설정하고, 해당 DHCP 패킷에 대한 정책을 결정해야 합니다. 각 옵션의 패킷 정책은 다음과 같습니다.

- **keep** : Option 정보 조작을 하지 않고 그대로 목적지로 전송합니다.
- **replace** : 수신된 패킷의 Option 정보를 사용자 장비 시스템의 Option 설정 내용으로 바꾼 뒤, 목적지로 전송합니다.

DHCP 패킷을 수신하는 포트별로 DHCP Snooping Option을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping port port-number opt-code <1-254> format format-name	Global	포트별로 DHCP Snooping Option을 설정합니다.
ip dhcp snooping port port-number opt-code <1-254> policy {keep replace}		포트별로 설정된 Option을 가진 패킷에 대한 정책을 설정합니다.

포트별로 설정된 DHCP Snooping Option을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip dhcp snooping port port-number opt-code <1-254>	Global	포트별로 설정된 DHCP Snooping Option을 삭제합니다.

포트별로 설정된 DHCP Snooping Option이 없을 경우, 시스템은 디폴트 DHCP Snooping Option의 설정 여부를 확인하여 DHCP 클라이언트로부터 수신한 패킷에 Option을 설정합니다.

시스템에 디폴트 DHCP Snooping Option을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping default-option code <1-254> format format-name	Global	시스템에 디폴트 DHCP Snooping Option을 설정합니다.
ip dhcp snooping default-option code <1-254> policy { keep replace }		패킷의 기존 Option을 디폴트 DHCP Snooping Option으로 변경 여부를 결정하는 정책을 설정합니다.

시스템에 설정된 디폴트 DHCP Snooping Option을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip dhcp snooping default-option code <1-254>	Global	시스템에 설정된 디폴트 DHCP Snooping Option을 삭제합니다.

(13) DHCP Snooping 설정 내용 확인

DHCP Snooping 설정 내용을 확인하시려면, 다음 명령어를 사용하십시오. 할당된 IP 주소 및 관련 정보를 담은 DHCP Snooping 바인딩 테이블을 확인할 수 있습니다.

명령어	모 드	기 능
show ip dhcp snooping	Global	DHCP Snooping 설정 내용을 확인합니다.
show ip dhcp snooping binding		DHCP Snooping 바인딩 테이블을 확인합니다.

8.10.8. IP Source Guard

IP Source Guard는 DHCP 패킷이 들어왔을 때, DHCP Snooping 바인딩 테이블에 등록된 정보에서 IP 주소, 또는 IP 주소와 MAC 주소를 비교하여 테이블에 등록된 내용과 일치할 경우에만 해당 패킷을 허용합니다. DHCP Snooping 바인딩 테이블을 사용하기 때문에 DHCP Snooping 기능을 활성화하였을 때 사용이 가능합니다.



주의

IP Source Guard 기능은 DHCP Snooping을 활성화해야 사용할 수 있습니다.

(1) IP Source Guard 활성화

DHCP snooping 설정된 상태에서 IP Source Guard를 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp verify source port-number	Global	IP 주소를 이용하여 IP Source Guard를 동작시킵니다.
ip dhcp verify source port-security port-number		IP 주소와 MAC 주소를 이용하여 IP Source Guard를 동작시킵니다.



주의

위의 두 기능을 동시에 설정할 수 없습니다. 둘 중 하나를 선택하여 설정하십시오.

위의 명령어를 사용하여 IP Source Guard를 활성화 시키면, 바인딩 테이블이 내용과 일치하는 IP 주소 및 IP 주소와 MAC 주소를 가진 패킷만을 포워딩 합니다.

IP Source Guard를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip dhcp verify source port-number	Global	IP Source Guard를 해제합니다.
no ip dhcp verify source port-security port-number		

(2) Static IP Source Guard

서버로부터 IP 주소를 할당 받지 않아서 DHCP Snooping 바인딩 테이블에는 등록되어 있지 않지만, 관리자가 포워딩 시키고자 하는 DHCP 패킷을 Static으로 등록할 수 있습니다.

DHCP Snooping 바인딩 테이블에 등록되어 있지 않지만, 등록 여부와 상관없이 포워딩 하려는 DHCP 패킷을 Static으로 등록하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp verify source binding <1-4094> <i>port-number ip-address mac-address</i>	Global	포워딩 시키려는 DHCP 패킷을 Static으로 등록합니다.
no ip dhcp verify source binding <i>{ip-address all}</i>		Static으로 등록한 내용을 삭제합니다.

(3) IP Source Guard 설정 내용 확인

IP 소스 guard 정보를 확인하려면 다음의 명령어를 확인해 보아야 합니다.

명령어	모 드	기 능
show ip dhcp verify source binding	Global	고정된 IP 소스 바인딩을 확인합니다.

8.10.9. DHCP 디버깅

DHCP 기능을 효율적으로 디버깅하거나 그 설정을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
debug dhcp {filter lease service all}	Privileged	DHCP 기능을 디버깅 합니다.
no debug dhcp {filter lease service all}		디버깅 설정을 해제합니다.

8.10.10. DHCP 패킷 통계 확인

V5812G에서는 다음 명령어로 다른 네트워크 장비와 주고 받은 DHCP 패킷 통계를 확인하거나 삭제할 수 있습니다.

명령어	모 드	기 능
show ip dhcp server statistics	Global	DHCP 패킷 통계를 확인합니다.
clear ip dhcp statistics		DHCP 패킷 통계를 삭제합니다.

8.11 Storm Control

V5812G는 브로드캐스트 패킷에 대하여 브로드캐스트 Storm Control을 지원합니다. 브로드캐스트 Storm이란, 다량의 브로드캐스트 패킷이 네트워크상에 전송되면서 전송 용량의 대부분을 점유함에 따라 네트워크 타임 아웃이 발생하는 현상을 말합니다. 브로드캐스트 Storm은 프로토콜의 버전 차이에 의해서 발생하는 경우가 많습니다.

예를 들면, TCP/IP에서는 4.3 BSD와 4.2 BSD가 혼재하거나 Appletalk Phase I과 Phase II가 혼재하면 브로드캐스트 Storm이 발생할 수 있습니다. 또한 라우터가 정기적으로 송신하는 라우팅 프로토콜의 정보가 해당 프로토콜을 지원하지 않는 시스템에 의해 잘못 인식되면 브로드캐스트 Storm이 발생할 수도 있습니다.

V5812G에서 브로드캐스트 Storm Control 기능은 1초 동안 브로드캐스트 패킷의 전송률을 설정하여 미리 설정된 한계 값을 넘는 경우 해당 패킷을 폐기하는 방법으로 구현되고 있습니다. 사용자는 Storm control을 사용하여 제한하는 패킷의 전송률을 변경할 수 있습니다.

V5812G는 브로드캐스트 Storm 뿐만 아니라 멀티캐스트나 DLF(Destination Lookup Fail) Storm에 대한 조절도 가능하게 되었습니다. 멀티캐스트와 DLF Storm control 기능을 추가하려면 다음 명령어를 사용하십시오. 브로드 캐스트 Storm Constrol을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
storm-control {broadcast multicast dlf} rate [port-number]	Bridge	DLF storm control, broadcast, multicast 기능을 추가하고 Flooding되는 패킷의 전송률을 1초당 rate만큼 제한합니다. FE의 경우 전송률은 1에서 262142이며 GE의 경우 1에서 2097150입니다.



참 고

V5812G는 기본적으로 Storm control이 동작하지 않도록 설정되어 있습니다.

Storm Control 설정을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no storm-control {broadcast multicast dlf} rate [port-number]	Bridge	Storm Control 설정을 해제합니다.

Storm Control 설정을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show storm-control	Enable/Bridge	Storm Control 설정을 확인합니다.

8.12 Jumbo-frame 수용하기

이더넷 환경에서 수용이 가능한 패킷의 범위는 64Byte부터 1,518Byte까지입니다. 따라서 장비들은 이 범위의 이하가 되거나 이상이 되는 패킷은 취급하지 않습니다. 그러나, V5812G는 1,518Byte보다 크기가 큰 Jumbo-frame을 받을 수 있도록 설정할 수 있습니다.

1,518Byte보다 큰 Jumbo-frame을 받을 수 있도록 설정하려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
jumbo-frame port-number <1518-9216>	Bridge	선택한 포트에서 지정한 범위 내의 Jumbo-frame을 받을 수 있도록 설정합니다.



참 고

V5812G는 최대 10,000Byte까지의 Jumbo-frame을 받을 수 있습니다.

Jumbo-frame을 받을 수 있도록 설정했던 것을 해제하려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no jumbo-frame port-number	Bridge	해당 포트에서 Jumbo-frame을 받을 수 있도록 설정한 것을 해제합니다.

Jumbo-frame에 대한 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show jumbo-frame	Enable/Global/Bridge	Jumbo-frame에 대한 설정 내용을 확인합니다.

8.13 Direct 브로드캐스트 차단

RFC 2644에서는 장비의 인터페이스에 설정된 네트워크 대역과 같은 대역의 브로드캐스트 패킷, 즉 Direct 브로드캐스트 패킷이 들어오면 이것을 막도록 권장하고 있습니다. 이에 따라 (주)다산네트웍스의 장비들은 기본적으로 이러한 Direct 브로드캐스트 패킷을 막도록 설정되어 있습니다.

그러나, V5812G는 Direct 브로드캐스트 패킷을 차단하는 기능을 사용자가 설정할 수 있도록 하였습니다. Direct 브로드캐스트 패킷을 차단하는 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip forward direct-broadcast	Global	Direct 브로드캐스트 패킷을 차단하는 기능을 활성화합니다.



참 고

기본적으로 V5812G는 Direct 브로드캐스트 패킷 차단 기능이 활성화되어 있습니다.

Direct 브로드캐스트 패킷을 차단하는 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip forward direct-broadcast	Global	Direct 브로드캐스트 패킷을 차단하는 기능을 해제합니다.

Direct 브로드캐스트 패킷을 차단하는 기능에 대한 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show running-config	Enable /Global/Bridge/Interface	장비에 설정된 내용을 확인합니다.

8.14 최대 전송 단위 (MTU) 설정

데이터 링크의 경우 각각의 서로 다른 최대 전송 단위(MTU: Maximum Transmission Unit)를 가지고 있습니다. 이 최대 전송 단위는 이더넷의 경우에는 1500옥텟, FDDI에서는 4353옥텟, ATM에서는 9180옥텟으로 되어 있습니다. IP 상위층은 이 MTU보다 큰 패킷의 송신을 요구할지도 모르고, 경로 도중 패킷 길이보다 작은 MTU 네트워크를 통과해야 할지도 모릅니다.,

최대 전송 단위를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>mtu <68-1500></code>	Interface	인터페이스의 최대 전송 단위 MTU 를 설정합니다. 단위는 “byte” 입니다.
<code>no mtu</code>		최대 전송 단위 MTU 설정을 해제합니다.

8.15 Access List 설정

네트워크 규모가 점점 더 광대해짐에 따라 보다 효율적이고 안정적인 네트워크 서비스를 제공하기 위해 네트워크 관리자는 장비에 다양한 설정을 하게 됩니다. 이때 필요에 따라서 특정 IP 주소를 여러 가지 기능에서 반복적으로 입력하여 사용해야 하는 경우가 빈번하게 발생합니다.

Access List(ACL)는 특정 IP 주소를 미리 지정해두는 일종의 주소록과 같은 것입니다. 사용자는 장비를 설정할 때 특정 범위의 IP 주소를 직접 입력하는 대신, 이미 지정해 놓은 ACL을 하나만 선택하여 입력해줌으로써 각종 기능을 간편하게 설정할 수 있습니다.

예를 들어, 사용자가 특정 범위에 해당하는 IP 주소를 가진 호스트에게만 멀티캐스트 서비스를 제공하고자 한다면, 먼저 해당 IP 주소 범위를 ACL 1로 설정합니다. 그리고 IGMP 등의 멀티캐스트 설정에서 ACL 1에 해당하는 IP 주소를 가진 호스트만 멀티캐스트 서비스가 되고 있는 인터페이스에 접속하도록 허용한다면, 사용자가 필요한 IP 주소를 일일이 입력하는 수고를 덜게 됩니다.

또한, ACL을 이용하여 특정 패킷의 경로를 차단하거나 제한할 수 있습니다. 예를 들어, OSPF 라우팅 프로토콜을 설정할 때 차단하고자 하는 IP 주소를 미리 ACL 2로 등록해두고, 특정 Area에서 해당 ACL 2에 속하는 패킷을 차단하도록 설정합니다.

V5812G는 다음과 같이 세 가지 유형의 ACL을 설정할 수 있습니다.

- **Standard access-list:** 해당 트래픽의 IP 주소를 참조하여 허용 여부를 결정하도록 설정합니다.
- **Extended access-list:** 해당 트래픽의 Source IP, Destination IP를 참조하여 허용 여부를 결정하도록 설정합니다.
- **Named access-list:** Character string으로 고유의 이름을 부여한 access-list를 설정합니다. Named access-list의 이름은 영문자, 영문자와 숫자의 조합 또는 Standard access-list와 Extended access-list 범위에 포함되지 않는 번호로 부여할 수 있습니다.



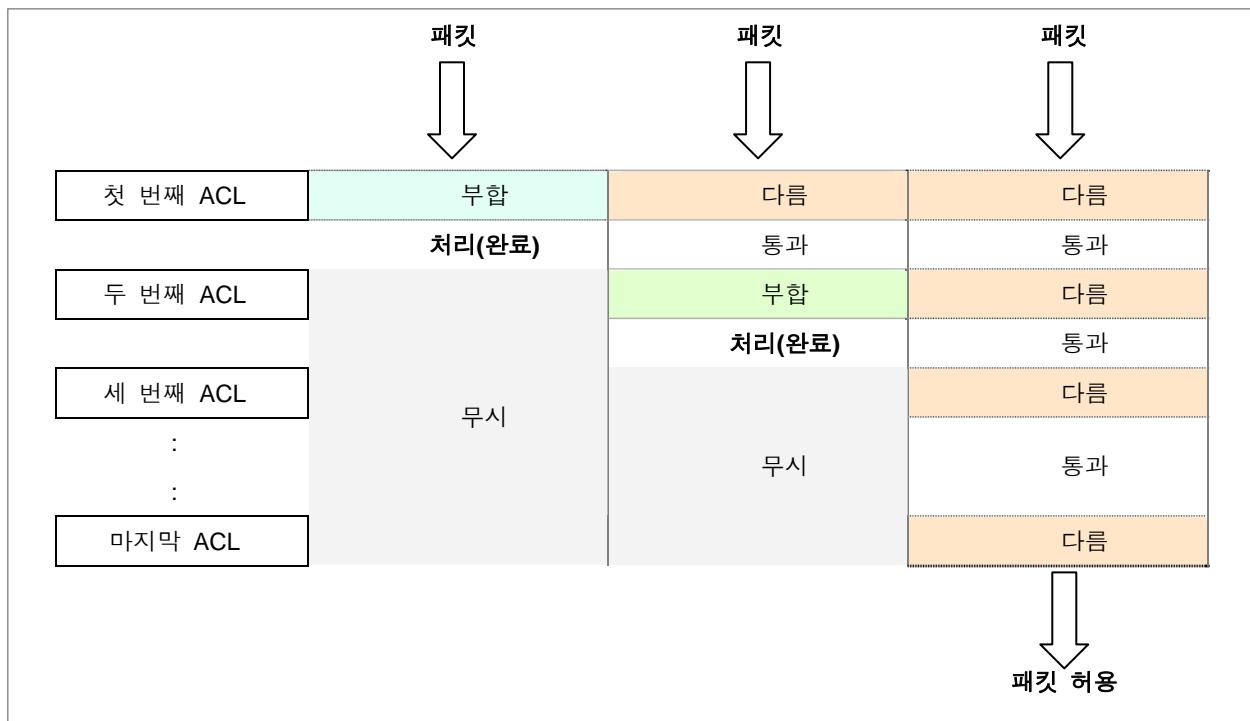
참 고

일반적으로 ACL을 지정할 때는 Global 설정 모드에서 사용자가 원하는 list를 생성한 후에 실제로 트래픽을 제어하고자 하는 위치의 인터페이스나 프로토콜에 해당 ACL을 적용합니다. 그러나, ARP Inspection에서 사용하는 access-list는 해당 기능에서 별도로 생성해야 합니다. ARP access-list의 자세한 설정 방법은 「ARP Inspection」을 참조하십시오.

8.15.1. ACL 동작 방법

하나의 인터페이스에 여러 개의 ACL이 설정되어있을 경우에는 순차적으로 적용됩니다. 먼저 설정한 ACL이 높은 우선 순위를 가지고, 사용자가 추가한 ACL 엔트리는 항상 제일 마지막에 위치하게 됩니다. 따라서 ACL 엔트리의 순서를 바꾸거나 ACL의 설정 내용을 수정할 수 없기 때문에 ACL을 전체적으로 다시 설정해야 합니다.

또한, 설정된 ACL을 적용할 때, 만일 가장 먼저 설정한 ACL에 부합하는 패킷이라면, 설정에 따라 처리하고 다른 ACL은 무시합니다. 그러나, 패킷이 설정된 ACL에 부합되지 않는다면 해당 ACL은 통과하고 다음 ACL을 적용합니다. 이와 같이 사용자가 설정한 ACL을 순차적으로 적용하게 되고, 마지막 ACL까지 통과한다면 해당 패킷은 허용되는 것입니다.



【 그림 9-33 】 ACL의 적용 순서

따라서, ACL의 설정 순서는 매우 중요합니다. 예를 들어, 192.168.10.1의 호스트를 제외한 모든 트래픽을 허용하도록 설정할 경우에는 다음과 같이 설정해야 합니다.

```
SWITCH# configure terminal
SWITCH(config)# access-list 1 deny host 192.168.10.1
SWITCH(config)# access-list 1 permit any
SWITCH(config)#

```

만일 **access-list 1 permit any**를 먼저 설정했다면 일단 모든 트래픽을 허용하기 때문에 192.168.10.1에 대한 패킷을 거부하는 것이 실패할 수 있습니다.

위에서도 설명한 것과 같이 ACL이 적용된 인터페이스에서는 IP 패킷이 ACL의 조건에 부합할 때까지 모든 ACL 엔트리를 검사하기 때문에, 너무 많은 ACL 엔트리를 설정하면 사용자 장비에 과부하가 걸릴 수 있습니다. 따라서 ACL을 설정할 때에는 되도록 간결하게 하고, 사용빈도가 높은 조건을 먼저 설정하는 것이 좋습니다.

8.15.2. Wildcard Bits

IP ACL에서는 특정 IP 주소의 범위를 지정할 때 IP 주소와 Wildcard mask가 사용됩니다. 서브넷 마스크와 달리 Wildcard mask의 mask bit는 정반대의 의미를 갖습니다. 즉, mask bit 0은 '체크'를 의미하고, mask bit 1은 '무시'를 의미합니다. 때문에, Wildcard mask를 Inverse mask라고도 합니다. 예를 들어, Wildcard mask가 0.0.0.255로 설정되어 있다면 이는 서브넷 마스크의 255.255.255.0과 같습니다.

다음 표는 Wildcard mask의 설정값에 따라 실제로 ACL에서 제어하게 될 IP 주소의 범위를 나타낸 것입니다.

【 표 8-3 】 Wildcard mask의 설정 예

IP 주소	Wildcard Bits	ACL 제어 적용 범위
10.55.10.2	0.0.0.255	10.55.10.1-10.55.10.255
10.55.10.2	0.0.0.0	10.55.10.2
0.0.0.0	255.255.255.255	모든 IP 주소(any)

만약 사용자가 어떤 ACL 엔트리에 IP 주소 10.55.10.2와 Wildcard mask 0.0.0.255를 허용하도록 설정했다면 실제로 10.55.10.1~10.55.10.255(10.55.10.0/24)에 해당하는 패킷이 허용됩니다. 한편, 특정 IP 주소와 Wildcard mask 0.0.0.0을 설정하면 해당 IP 주소를 가진 특정 호스트를 가리킵니다. 반면에, IP 주소 0.0.0.0과 Wildcard mask 255.255.255.255 설정하면 호스트의 IP 주소에 따른 제약이 없어집니다.

8.15.3. Standard Access List 설정

Standard access-list는 지정한 IP 주소를 참조하여 IP 패킷을 허용 또는 거부하도록 설정합니다.

V5812G는 사용자의 필요에 따라 여러 가지 조건을 설정하여 Standard access-list를 설정할 수 있습니다. 사용자가 설정한 조건에 부합하는 패킷을 허용하려면 **permit** 옵션을, 차단하려면 **deny** 옵션을 사용합니다.

Standard access-list를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
access-list {<1-99> <1300-1999>} {deny permit} ip-address [wildcard-mask]	Global	지정한 IP 주소 혹은 IP 주소 범위에 해당하는 패킷을 허용 또는 거부하도록 설정합니다.
access-list {<1-99> <1300-1999>} {deny permit} any	Global	모든 Source IP 주소를 가진 패킷을 허용 또는 거부하도록 설정합니다.
access-list {<1-99> <1300-1999>} {deny permit} host ip-address	Global	특정 호스트 IP 주소를 가진 패킷을 허용 또는 거부하도록 설정합니다.



참 고

<1-99>는 Standard access-list의 식별번호로 설정할 수 있는 범위입니다. <1300-1900> 이내의 값을 입력하면 확장된 범위의 Standard access-list를 이용할 수 있습니다.



참 고

서로 다른 IP 주소에 사용될 ACL 엔트리를 추가할 때에는 위의 명령어를 반복적으로 입력하십시오.



참 고

사용자 장비의 부하를 줄이기 위해서 사용빈도가 가장 높은 조건을 먼저 설정할 것을 권장합니다.

설정한 Standard access-list를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no access-list {<1-99> <1300-1999>} {deny permit} ip-address [wildcard-mask]		설정한 Standard
no access-list {<1-99> <1300-1999>} {deny permit} any	Global	access-list를
no access-list {<1-99> <1300-1999>} {deny permit} host ip-address		삭제합니다.

한편, V5812G는 사용자의 편의를 위해 설정한 ACL 엔트리에 간단한 설명을 부가할 수 있습니다.

설정한 ACL 엔트리에 설명을 입력하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
access-list {<1-99> <1300-1999>}		특정 ACL 엔트리에 부가설명을 저장합니다.
remark <i>description</i>	Global	
no access-list {<1-99> <1300-1999>}		설정한 ACL 엔트리의 부가설명을 삭제합니다.
remark <i>description</i>		



참 고

*description*은 100자까지 입력할 수 있습니다.

다음은 Standard access-list를 설정한 경우의 예입니다.

```
SWITCH(config)# access-list 5 permit 10.55.10.2 0.0.0.255
SWITCH(config)# access-list 5 deny 10.55.1.1 0.0.0.255
SWITCH(config)#{
```

8.15.4. Extended Access List 설정

Extended access-list는 필터링 조건으로 Source IP 주소와 Destination IP 주소를 지정하고, 이 조건에 일치하는 IP 패킷을 허용 또는 거부하도록 설정합니다.

V5812G는 사용자의 필요에 따라 여러 가지 조건을 설정하여 Extended access-list를 설정할 수 있습니다. 사용자가 설정한 조건에 부합하는 패킷을 허용하려면 **permit** 옵션을, 차단하려면 **deny** 옵션을 사용합니다.

Extended access-list를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
access-list {<100-199> <2000-2699>} {deny permit} ip source-ip-address wildcard-mask destination-ip-address wildcard-mask	Global	Source IP와 Destination IP가 지정한 IP 주소 혹은 IP 주소 범위에 해당하는 패킷을 허용 또는 거부하도록 설정합니다.
access-list {<100-199> <2000-2699>} {deny permit} ip source-ip-address wildcard-mask any		Source IP가 지정한 IP 주소 혹은 IP 주소 범위에 해당하는 패킷을 허용 또는 거부하도록 설정합니다.
access-list {<100-199> <2000-2699>} {deny permit} ip source-ip-address wildcard-mask host destination-ip-address		Source IP가 지정한 IP 주소 혹은 IP 주소 범위에 해당하고 특정 호스트 Destination IP 주소를 가진 패킷을 허용 또는 거부하도록 설정합니다.
access-list {<100-199> <2000-2699>} {deny permit} ip host source-ip-address destination-ip-address wildcard-mask		특정 호스트 Source IP를 가진 패킷이 지정한 IP 주소 혹은 IP 주소 범위에 해당하는 경우에 허용 또는 거부하도록 설정합니다.
access-list {<100-199> <2000-2699>} {deny permit} ip host source-ip-address any		특정 호스트 Source IP 주소를 가진 패킷을 허용 또는 거부하도록 설정합니다.
access-list {<100-199> <2000-2699>} {deny permit} ip host source-ip-address host destination-ip-address		특정 호스트 Source IP와 특정 호스트 Destination IP 주소를 가진 패킷을 허용 또는 거부하도록 설정합니다.
access-list {<100-199> <2000-2699>} {deny permit} ip any destination-ip-address wildcard-mask		특정 범위의 Destination IP 주소를 가진 패킷을 허용 또는 거부하도록 설정합니다.
access-list {<100-199> <2000-2699>} {deny permit} ip any host destination-ip-address		특정 호스트 Destination IP 주소를 가진 패킷을 허용 또는 거부하도록 설정합니다.
access-list {<100-199> <2000-2699>} {deny permit} ip any any		모든 패킷을 허용 또는 거부하도록 설정합니다.



참 고

<100-199> 는 Extended access-list의 식별번호로 설정할 수 있는 범위입니다. <2,000-2,699> 이내의 값을 입력하면 확장된 범위의 Extended access-list를 이용할 수 있습니다.



참 고

서로 다른 IP 주소에 사용될 ACL 엔트리를 추가할 때에는 위의 명령어를 반복적으로 입력하십시오.



참 고

사용자 장비의 부하를 줄이기 위해서 사용빈도가 가장 높은 조건을 먼저 설정할 것을 권장합니다.

설정한 Extended access-list를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no access-list {<100-199> <2000-2699>} {deny permit} ip source-ip-address wildcard-mask destination-ip-address wildcard-mask		
no access-list {<100-199> <2000-2699>} {deny permit} ip source-ip-address wildcard-mask any		
no access-list {<100-199> <2000-2699>} {deny permit} ip source-ip-address wildcard-mask host destination-ip-address		
no access-list {<100-199> <2000-2699>} {deny permit} ip host source-ip-address destination-ip-address wildcard-mask		
no access-list {<100-199> <2000-2699>} {deny permit} ip host source-ip-address any	Global	설정한 Extended access-list를 삭제합니다.
no access-list {<100-199> <2000-2699>} {deny permit} ip host source-ip-address host destination-ip-address		
no access-list {<100-199> <2000-2699>} {deny permit} ip any destination-ip-address wildcard-mask		
no access-list {<100-199> <2000-2699>} {deny permit} ip any host destination-ip-address		
no access-list {<100-199> <2000-2699>} {deny permit} ip any any		

한편, V5812G는 사용자의 편의를 위해 설정한 ACL 엔트리에 간단한 설명을 부가할 수 있습니다. 설정한 ACL 엔트리에 설명을 입력하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
access-list {<100-199> <2000-2699>} remark <i>description</i>	Global	특정 ACL 엔트리에 부가설명을 저장합니다.
no access-list {<100-199> <2000-2699>} remark <i>description</i>		설정한 ACL 엔트리의 부가설명을 삭제합니다.



참 고

*description*은 100자까지 입력할 수 있습니다.

다음은 Extended access-list를 설정한 경우의 예입니다.

```
SWITCH(config)# access-list 100 permit ip 10.55.10.2 0.0.0.255 10.55.193.5 0.0.0.255
SWITCH(config)# access-list 100 deny ip 10.12.154.1 0.0.0.255 10.12.202.1 0.0.0.255
SWITCH(config)#+
```

8.15.5. Named Access List 설정

Named access-list는 사용자의 편의를 위해 Character string으로 고유의 이름을 부여한 ACL입니다.

Named access-list의 이름은 영문자, 영문자와 숫자의 조합 또는 Standard access-list와 Extended access-list 범위에 포함되지 않는 번호로 부여할 수 있습니다. 또한, Named access-list는 동일한 이름을 중복해서 사용할 수 없습니다.

Named access-list를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
access-list <i>access-list-name</i> {deny permit} A.B.C.D/M [exact-match]	Global	특정 Prefix에 해당하는 패킷을 허용 또는 거부하도록 Named access-list를 설정합니다.
access-list <i>access-list-name</i> {deny permit} any		Destination IP 주소에 상관 없이 모든 패킷을 허용 또는 거부하도록 Named access-list를 설정합니다.



참 고

exact-match 옵션을 사용하면 사용자가 지정한 Prefix에 정확히 일치하는 패킷에 대해 허용 또는 거부하도록 설정합니다.



참 고

서로 다른 IP 주소에 사용될 ACL 엔트리를 추가할 때에는 위의 명령어를 반복적으로 입력하십시오.



참 고

사용자 장비의 부하를 줄이기 위해서 사용빈도가 가장 높은 조건을 먼저 설정할 것을 권장합니다.

설정한 Named access-list를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no access-list access-list-name {deny permit} A.B.C.D/M [exact-match]	Global	설정한 Named access-list를 삭제합니다.
no access-list access-list-name {deny permit} any		

한편, V5812G는 사용자의 편의를 위해 설정한 ACL 엔트리에 간단한 설명을 부가할 수 있습니다.

설정한 ACL 엔트리에 설명을 입력하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
access-list access-list-name remark description	Global	특정 ACL 엔트리에 부가설명을 저장합니다.
no access-list access-list-name remark description		설정한 ACL 엔트리의 부가설명을 삭제합니다.



참 고

*description*은 100자까지 입력할 수 있습니다.

다음은 Named access-list를 설정한 경우의 예입니다.

```
SWITCH(config)# access-list aaa permit 10.55.193.109/24
SWITCH(config)#{
```

8.15.6. Access List 설정 내용 확인

ACL의 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip access-list	Enable/ Global/ Bridge	모든 ACL 엔트리의 설정 내용을 확인합니다.
show ip access-list [<1-99> <1300-1999>]		Standard access-list의 설정 내용을 확인합니다.
show ip access-list [<100-199> <2000-2699>]		Extended access-list의 설정 내용을 확인합니다.
show ip access-list access-list-name		Named access-list의 설정 내용을 확인합니다.

다음은 모든 ACL 엔트리의 설정 내용을 확인한 경우의 예입니다.

```
SWITCH(config)# show ip access-list
Standard IP access list 5
    permit 10.55.10.0, wildcard bits 0.0.0.255
    deny 10.55.1.0, wildcard bits 0.0.0.255
Extended IP access list 100
    permit ip 10.55.10.0 0.0.0.255 10.55.193.0 0.0.0.255
    deny ip 10.12.154.0 0.0.0.255 10.12.202.0 0.0.0.255
ZebOS IP access list aaa
    permit 10.55.193.109/24
SWITCH(config)#

```

9. 멀티캐스트(Multicast) 설정

멀티캐스트란, 특정 데이터를 필요로 하는 하나 이상의 특정 수신자들에게 해당 데이터를 송신하는 패킷 전송 방식 중 하나입니다. 특정 수신자에게만 데이터를 전송한다는 점에서 유니캐스트(Unicast)와 매우 흡사하지만, 데이터를 원하는 수신자에게 일대일 방식으로 데이터를 전송하여 수신자 숫자만큼 동일한 데이터가 내보내지는 것이 아니라 단 한번의 데이터 전송으로 여러 수신자에게 전달된다는 점이 유니캐스트와 다른 점입니다.

이러한 특징 때문에 멀티캐스트는 데이터의 중복 전송으로 인한 네트워크 자원 낭비를 최소화하고, 해당 트래픽을 특정한 목적지로 네트워크 대역폭 낭비없이 효율적으로 전달하게 됩니다.

멀티캐스트의 전송 방식은 크게 하나의 소스가 여러 수신자들에게 데이터를 전달하는 방식과, 복수의 소스가 여러 수신자들에게 데이터를 전송하는 방식으로 나뉘어집니다.

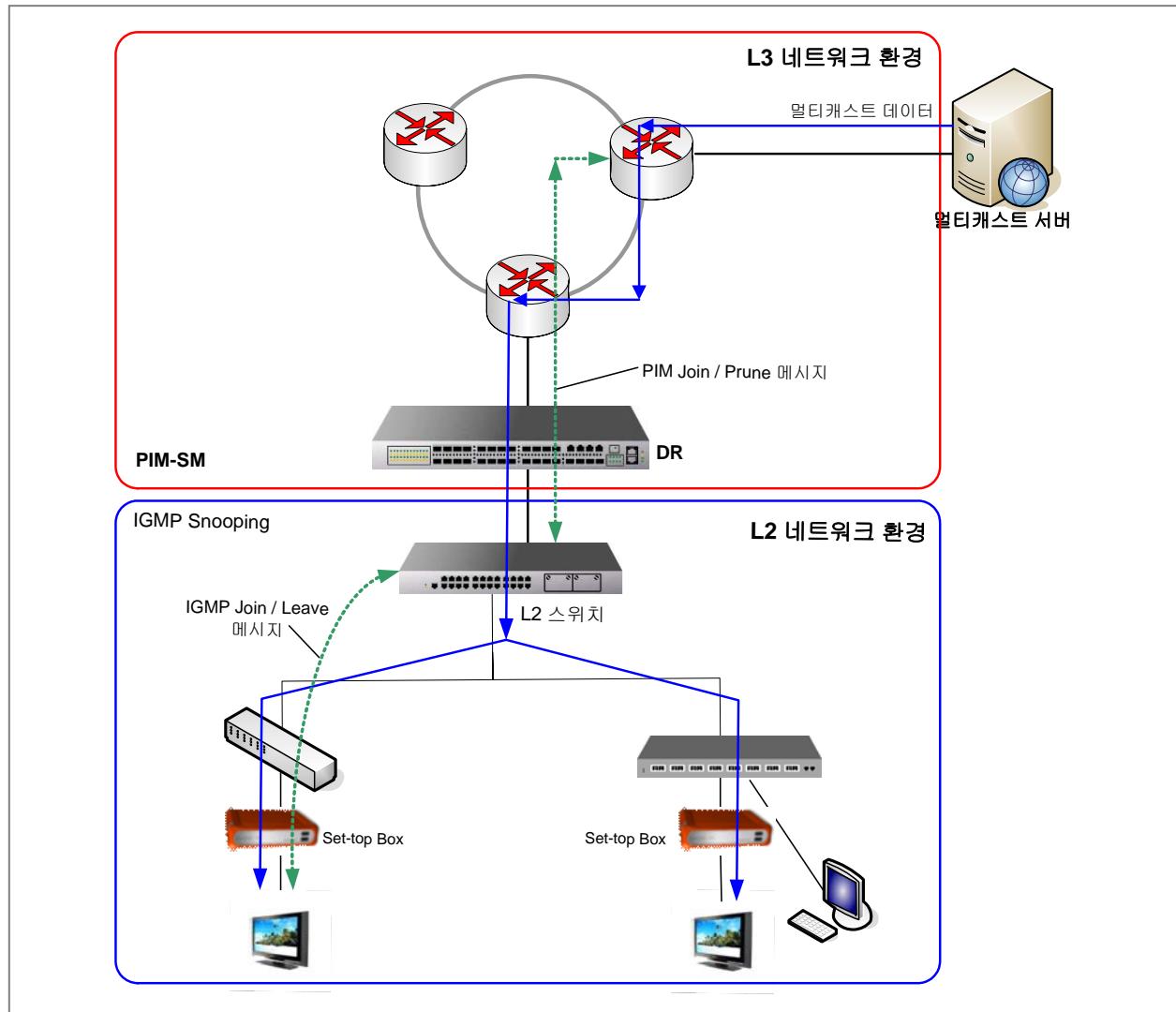
하나의 Source가 여러 수신자들(Receiver)에게 데이터를 전달하는 경우에는 PIM-SM 또는 PIM-SSM 등이 사용됩니다. 이러한 전송 방식은 오디오 및 동영상 강의, TV 프로그램, 라디오, 뉴스 헤드라인, 날씨 업데이트 등의 서비스를 제공합니다.

복수의 Source로부터 여러 수신자들(Receiver)에게 데이터를 전달하는 경우에는 PIM-DM/SM, PIM-Bidir, CBT 등을 사용합니다. 이러한 전송 방식의 응용분야로는 송신자와 수신자 서로가 실시간으로 데이터를 송수신할 수 있는 원격 교육, 인터넷 화상회의, 인터넷 컴퓨터 게임 등이 있습니다.

V5812G는 IP 멀티캐스트 기능을 제공하여 신속하고 효율적인 트래픽 전송을 보장하는데, 보다 원활한 멀티캐스트 통신 서비스를 위해 PIM-SM, PIM-SSM, IGMP 버전 3, IGMP Snooping, MVR 등의 기능을 지원합니다.

V5812G를 L3 네트워크 환경에 라우터로 구성하고자 할 때, V5812G는 멀티캐스트 라우팅 프로토콜(PIM-SM, PIM-SSM)로 설정되어야 합니다. L2 네트워크 환경에서는 IGMP Snooping으로 동작하는 스위치를 통해서 호스트의 멀티캐스트 통신을 지원할 수 있습니다.

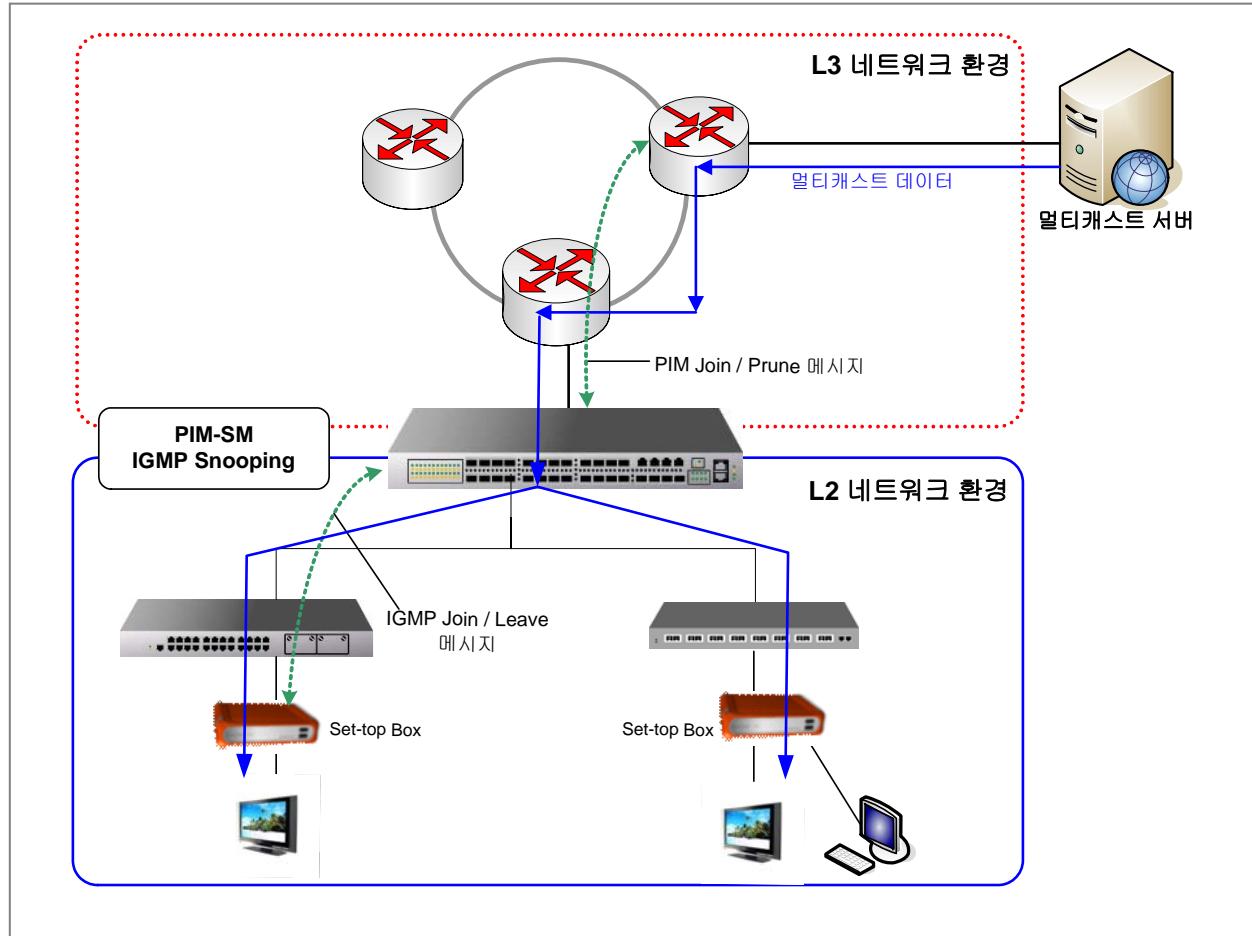
다음 그림은 V5812G를 L3 네트워크 환경에서, 멀티캐스트 라우팅 프로토콜인 PIM-SM을 활성화하여 구성한 모습입니다.



【 그림 9-1 】 PIM-SM을 설정했을 경우

만약 V5812G가 L3 네트워크 환경에서 Border 라우터로 동작하고, 2개 이상의 포트가 같은 L2 인터페이스에 있다면, 사용자는 V5812G에 IGMP Snooping과 PIM-SM 이라는 두 기능을 동시에 활성화해야합니다.

다음은 V5812G에 IGMP Snooping과 PIM-SM을 동시에 설정한 멀티캐스트 네트워크 구성도의 예입니다.



【 그림 9-2 】 PIM-SM과 IGMP Snooping을 같이 설정했을 경우

이 장은 다음과 같은 내용으로 이루어집니다.

- IGMP (Internet Group Management Protocol)
- 멀티캐스트 부가 기능 설정
- 멀티캐스트 라우팅 설정

9.1 IGMP (Internet Group Management Protocol)

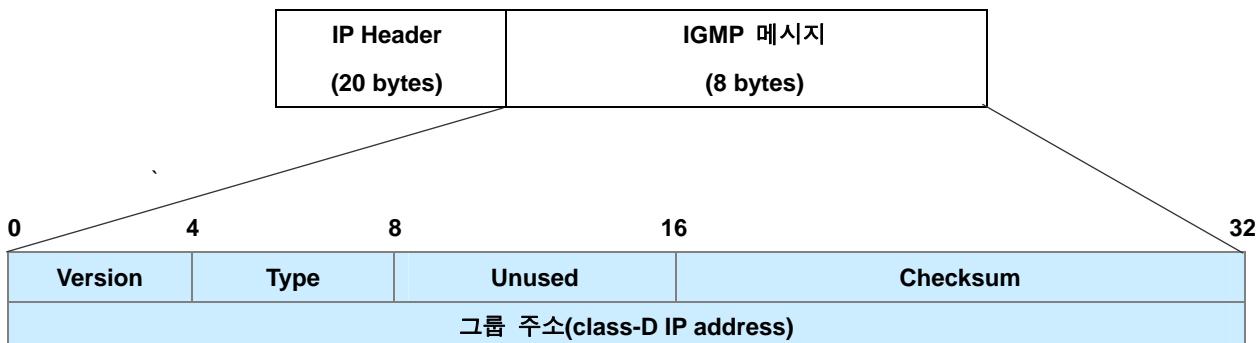
멀티캐스트 전송 방식의 핵심은 멀티캐스트 그룹 관리에 있습니다. 이러한 그룹 멤버쉽을 통하여 라우터는 어떠한 호스트가 멀티캐스트 패킷을 요청하는지 판단하여 해당 그룹에만 트래픽을 보내 줍니다.

IGMP(Internet Group Management Protocol)란 멀티캐스트 패킷을 수신하고자 하는 호스트와 멀티캐스트 패킷을 전송하는 라우터 간의 통신을 위한 프로토콜로, 호스트가 멀티캐스트 그룹으로 Join 하면 인접한 라우터는 이 정보를 기반으로 멀티캐스트 그룹 멤버쉽을 관리하게 됩니다.

현재 IGMP는 버전 1, 버전 2, 버전 3까지 정의되어 있으며, 각 버전의 IGMP 메시지는 기본적으로 Query와 Report 두 가지 형태의 메시지가 있습니다.

◆ IGMP 버전 1

다음 그림은 IP 패킷의 데이터 영역에 IGMP 메시지를 실어 전송하는 모습으로 IGMP 버전 1 메시지 형식은 다음 그림과 같습니다.



【 그림 9-3 】 IGMP 버전 1 메시지 형식

위의 그림에서 Version은 IGMP 버전을 나타냅니다. Type은 메시지의 형태를 나타내는데, 0x11이면 멀티캐스트 라우터가 보내는 Query(Membership Query)를 나타내고, 0x12이면 호스트가 그룹에 Join 하는 Report(Membership Report)입니다. 그룹 주소는 가입하고자 하는 멀티캐스트 주소를 가리키는데, Query 메시지를 송신할 때는 0이 되고, 수신 할 때는 무시됩니다. 호스트가 보내는 Report 메시지의 경우에는 응답하는 호스트의 멀티캐스트 그룹 주소로 채워지게 됩니다.

◆ IGMP 버전 2

IGMP 버전 2가 IGMP 버전 1과 다른 점은 호스트가 멀티캐스트 그룹에서 탈퇴할 때, 멀티캐스트 라우터에게 Leave 메시지를 전송하는 것입니다. 또한 Leave 메시지를 수신한 멀티캐스트 라우터는 해당 멀티캐스트 그룹 멤버쉽을 삭제하기 전에 서브넷 상에 다른 멀티캐스트 그룹 멤버가 남아 있을 수 있으므로, 이를 확인하는 절차가 추가되었습니다.

주기적으로 보내는 Query 메시지에 대한 응답 유무로만 멤버 가입 여부를 결정했던 버전 1에서는 호스트가 그룹에서 실제로 탈퇴했음에도 불구하고 라우터는 Query 메시지에 대한 응답이 오지 않는 것을 확인하기 전까지는 그룹 멤버로 남아있다고 인식하기 때문에 불필요한 멀티캐스트 트래픽이 전송되는 경우가 있었습니다. 그러나, 버전 2에서 이러한 과정이 추가됨에 따라 호스트가 그룹에서 탈퇴하는 시점을 바로 인식할 수 있기 때문에 불필요하게 멀티캐스트 트래픽이 전송되는 대역폭 낭비를 줄일 수 있게 되었습니다.

IGMP 버전 2의 메시지 형식은 다음 그림과 같습니다.

0	4	8	16	32
Version	Type	Max Response Time	Checksum	
그룹 주소(class-D IP address)				

【 그림 9-4 】 IGMP 버전 2 메시지 형식

위의 그림에서 Type은 그 목적에 따라 호스트가 자신의 그룹 가입 및 탈퇴유무를 알리는 Report 메시지와 Leave 메시지 또는 멀티캐스트 라우터가 송신하는 Query 메시지가 될 수 있습니다. Query 메시지는 General Query 메시지와 Group-specific Query 메시지 두 종류로 나누어 지며, General Query는 IGMP 버전 1에서의 Query와 동일합니다. Group-specific Query 메시지는 라우터가 Leave 메시지를 수신 후 특정 그룹에 다른 멤버가 남아있는지를 재확인하기 위해 보내게 됩니다.

Max Response Time(MRT)은 Query 메시지에 대한 응답을 기다리는 최대 시간을 뜻하며, 이 메시지를 수신한 호스트는 이 시간 이내에 IGMP 버전 2 멤버쉽 Report 메시지로 응답해야 합니다.

◆ IGMP 버전 3

IGMP 버전 3은 IGMP 버전 2와 동일한 방법으로 멀티캐스트 그룹 멤버의 Join과 Leave가 이루어지지만, Source 필터링 기능이 지원된다는 차이점을 가지고 있습니다.

Source 필터링 기능을 통해 특정 Source 주소로부터 오는 패킷만 수신하거나 혹은 그 패킷만을 제외하는 설정이 가능합니다. 이러한 설정은 그 전에 Learning 된 적이 없는 멀티캐스트 Source로부터 오는 트래픽을 Flooding 하는데 발생하는 문제점을 방지하고 네트워크 보안 기능을 향상시킬 수 있습니다. IGMP 버전 3은 하나의 메시지에 호스트의 Join과 Leave 관련 정보를 모두 포함하기 때문에 멀티캐스트 그룹 멤버쉽을 보다 신속하고 정확하게 관리 할 수 있습니다.

이 장에서는 IP IGMP 설정과 관련하여 다음과 같은 내용으로 구성됩니다.

- IGMP 기본 설정
- IGMP 버전 2 설정
- IGMP 버전 3 설정
- IGMP 설정 확인

9.1.1. IGMP 기본 설정

IGMP(Internet Group Management Protocol)는 멀티캐스트 그룹으로 등록된 호스트를 관리하기 위해 IGMP 그룹 멤버쉽 테이블을 관리 및 유지합니다. 호스트 또는 스위치는 인접한 멀티캐스트 라우터에게 멤버쉽 Join (Report) 메시지를 보내서 멀티캐스트 트래픽을 요청하게 됩니다. 이 메시지를 수신한 라우터는 멀티캐스트 트래픽을 해당 포트 또는 그룹 호스트들에게 전송합니다.

IGMP Querier란 멀티캐스트 그룹에 Query 메시지를 보내는 멀티캐스트 라우터를 명칭합니다. Querier는 멀티캐스트 그룹에 속한 호스트들에게 주기적으로 Query 메시지를 전송하고 호스트가 어느 멀티캐스트 그룹에 가입하고 있는지 응답하는 Report 메시지를 통해 그룹 호스트를 관리합니다. 만약 Query 메시지에 설정된 일정 시간동안 호스트의 응답이 없을 경우 라우터는 전송하던 트래픽을 차단합니다.

이 그룹 멤버의 변화 즉, 그룹 멤버인 호스트의 가입과 탈퇴를 멀티캐스트 라우터가 파악하도록 하는 것이 IGMP를 사용하는 목적입니다. 따라서, 멀티캐스트 라우터는 이를 바탕으로 멀티캐스트 멤버쉽 테이블을 관리하여 호스트들에게 멀티캐스트 통신 서비스를 제공합니다.

V5812G 스위치는 IGMP 버전 1, 버전 2, 버전 3을 지원합니다.

(1) IGMP 버전 설정

V5812G 스위치는 기본적으로 IGMP 버전 3으로 동작하지만 사용자의 필요에 따라 동작하는 IGMP 버전을 변경할 수 있습니다. 해당 인터페이스의 IGMP 버전을 변경하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp version <1-3>	Interface	해당 인터페이스의 IGMP 버전을 지정합니다.

설정한 IGMP 버전을 해제하고 기본 설정인 IGMP 버전3으로 동작하도록 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp version	Interface	설정한 IGMP 버전을 해제하고 IGMP 버전 3으로 설정합니다.

(2) QRV 설정

QRV(Querier's Robustness Variable)는 네트워크 상태가 불안정하여 패킷 손실이 예상되는 환경에서 Query 메시지에 대한 응답이 전달되지 않는 상황을 막기 위해 사용되는 것으로 IGMP 버전 2와 버전 3에서 지원됩니다. 이 값은 Query 메시지에 설정되는데, 호스트는 Query 메시지에 설정된 QRV 값의 횟수만큼 Query에 대한 응답을 전송해야 하고, 그 중 하나만이라도 라우터에게 정상적으로 전송되면 호스트가 응답한 것으로 인식됩니다. 네트워크의 패킷 손실이 많을 경우에는 QRV값을 크게 설정하여 응답을 여러 번 보내도록하여 패킷 수신 확률을 높여야 합니다.



네트워크 상태가 좋지 않을수록 QRV값은 크게 설정하십시오. 단, QRV값을 크게 설정하여 Query 메시지에 대한 응답 횟수가 늘어나면 Leave Latency도 증가합니다.

V5812G의 해당 인터페이스에 QRV의 값을 설정하기 위해서는 다음과 같은 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp robustness-variable <2-7>	Interface	QRV 값을 인터페이스에 설정합니다.

**참 고**

V5812G 스위치에 설정된 QRV 설정값은 기본적으로 2회 입니다. QRV는 2회부터 7회까지 설정 가능합니다.

설정된 QRV 값을 삭제하고 기본 설정값으로 지정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp robustness-variable	Interface	설정된 QRV를 삭제하고 기본 설정값으로 변경합니다.

(3) IGMP 엔트리 초기화

V5812G 스위치는 IGMP 데이터베이스를 초기화할 수 있는 명령어를 제공합니다. IGMP 인터페이스 별로 초기화 하시려면 *interface-name* 옵션을, 각 그룹 IP별로 초기화 하시려면 *group address* 옵션을, IGMP 데이터베이스 전체를 초기화 하시려면 * 옵션을 사용하십시오.

IGMP 엔트리 데이터베이스를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip igmp	Enable	모든 IGMP 엔트리 데이터베이스를 초기화합니다.
clear ip igmp interface <i>interface-name</i>		해당 인터페이스의 IGMP 엔트리 데이터베이스를 초기화합니다.
clear ip igmp group *		모든 IGMP 그룹 캐쉬 엔트리 데이터베이스를 초기화합니다.
clear ip igmp group <i>group-address [interface-name]</i>		해당 IGMP 그룹의 IGMP 엔트리 데이터베이스를 초기화합니다.

각 인터페이스에 송수신된 IGMP 패킷에 대한 통계값을 초기화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp clear-statistics	Interface	모든 IGMP 엔트리 통계를 초기화합니다.

(4) IGMP Debug

네트워크 장애가 발생했을 경우 사용자는 debug 명령어를 사용하여 IGMP 정보를 출력하도록 설정하면 문제의 원인을 신속하게 파악할 수 있습니다.

모든 IGMP 정보를 출력하거나 사용자가 설정한 특정 IGMP 정보를 출력하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
debug igmp all	Enable	IGMP 패킷에 대한 모든 정보를 출력합니다. 출력되는 정보에는 IGMP 패킷과 관련된 정보가 들어 있습니다.
debug igmp decode		IGMP decoding 관련된 정보를 출력합니다.
debug igmp encode		IGMP encoding 관련된 정보를 출력합니다.
debug igmp fsm		IGMP FSM(Finite State Machine) 관련된 정보를 출력합니다.
debug igmp tib		IGMP TIB(Tree Information Base) 관련된 정보를 출력합니다.
debug igmp events		IGMP event 관련된 정보를 출력합니다.

IGMP debug 설정을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no debug igmp {all decode encode fsm tib events}	Enable	IGMP debug 설정을 해제합니다.

9.1.2. IGMP 버전 2 설정

IGMP 버전 2의 특징으로는 IGMP Querier를 선출하고, Report Suppression 기능이 추가된 것 등을 들 수 있습니다. 또한 버전 2에서는 Leave 메시지와 Group-specific Query 메시지를 사용하여 호스트의 그룹 멤버 탈퇴 처리 과정 시간을 최소화할 수 있게 되었습니다.

◆ IGMP 버전 2 메시지

호스트와 라우터 사이 송수신되는 IGMP 버전 2 메시지는 3가지로 나눌 수 있습니다.

◇ 멤버쉽 Query 메시지

IGMP Querier인 멀티캐스트 라우터는 호스트의 그룹 가입 여부를 확인하기 위해 **Query** 메시지를 사용합니다. IGMP 버전 2의 **Query** 메시지는 두가지 종류가 존재합니다. 하나는 **General Query** 메시지로 Querier가 호스트 그룹 전체에 주기적으로 보내 그룹 가입 여부를 확인하는 것이고, 다른 하나는 **Group-specific Query** 메시지로 Querier가 호스트로부터 **Leave** 메시지를 수신한 후 해당 그룹으로 메시지를 보내 그룹에 멀티캐스트 트래픽 전송을 원하는 다른 호스트는 없는지 재확인하는 **Query** 메시지입니다.

◇ 멤버쉽 Report 메시지

IGMP 버전 2 **Report** 메시지는 호스트가 보내는 것으로 그룹에 새로 가입하여 멀티캐스트 패킷을 요청하는 **Join** 메시지(Unsolicited)와 IGMP Querier로부터 **Query** 메시지를 수신한 후 응답 제한 시간(Max Response Time)이내에 응답해야하는 **Report** 메시지(Solicited)가 있습니다.

◇ Leave 메시지

호스트가 특정 멀티캐스트 그룹에서 탈퇴 시 멀티캐스트 라우터에게 **Leave** 메시지를 전송합니다.

◆ IGMP 버전 2 동작원리

IGMP Querier가 되는 멀티캐스트 라우터는 동일 네트워크에 있는 모든 호스트들에게 **Query** 메시지를 전송합니다. IGMP 버전 2에서는 동일한 네트워크에 2대 이상의 라우터가 존재할 경우, 서로 주고 받은 **Query** 메시지의 정보를 가지고 Querier를 결정하게 되는데, 낮은 IP 주소를 가진 라우터가 Querier가 됩니다. 자신보다 더 낮은 주소를 가진 라우터로부터 **Query** 메시지를 받은 라우터들은 Querier 불능 상태(Non-Querier State)로 바뀌며 타이머가 동작하기 시작합니다. 이 타이머는 선출된 Querier로부터 **Query** 메시지를 수신할 때마다 초기화됩니다. 만약 Querier 라우터가 작동을 하지 않는 경우가 발생하면, Querier 불능 상태의 타이머가 만료된 후까지 **Query** 메시지를 받지 못하게 되므로 다시 **Query** 메시지를 주고 받아 그 다음으로 낮은 IP의 라우터가 Querier로 선출됩니다.

호스트는 멀티캐스트 패킷을 요청하는 멤버쉽 **Report**(Join)메시지를 전송하여 멀티캐스트 그룹에 가입합니다.

General Query 메시지는 멀티캐스트 그룹의 모든 호스트들에게 전송되기 때문에 이때 메시지가 가지는 그룹 주소는 224.0.0.1입니다. 만약 응답 제한 시간(MRT)이내에 호스트들의 응답이 없을 경우에 멀티캐스트 라우터는 해당 그룹에 있는 호스트가 없다고 판단하여 멀티캐스트 패킷을 더 이상 전송하지 않습니다.

한편, General Query 메시지를 수신한 호스트는 그룹의 멤버로 등록된 것을 알리기 위하여 Report 메시지로 응답하게 됩니다. 만약 호스트가 Query 메시지를 받음과 동시에 Join 메시지를 전송하거나, 그룹 안에 여러 호스트가 동시에 Report 메시지를 보내려고 시도하면 네트워크 부하가 생기고 패킷 손실이 발생할 수 있습니다. 이러한 상황을 방지하기 위해 IGMP 버전 2는 Report Suppression이라는 기능을 지원합니다. Report Suppression이란 호스트마다 Report 메시지를 보내는 시각의 차가 발생한다는 사실을 이용하여 동일한 그룹의 멤버인 호스트들로부터 최소한의 Report 메시지만 네트워크에 전송되도록 하는 것입니다. IGMP 버전 2에서 호스트는 멀티캐스트 라우터를 포함한 그룹 내의 모든 호스트들에게 Report 메시지를 전송합니다. 호스트마다 시스템 환경이 다르기 때문에 Report 메시지를 보내는 시각의 차가 발생하게 되고, Report 메시지를 먼저 전송한 호스트에 의해 자신이 보내려는 Report 메시지를 받은 호스트는 다른 호스트가 자신의 Report 메시지를 대신 보냈다고 판단하여 전송을 멈춥니다. 따라서, 최소한의 Report 메시지만 전송될 수 있는 것입니다.

IGMP 버전 2에서 호스트가 더 이상 해당 그룹의 멀티캐스트 트래픽 전송을 원하지 않으면 Leave 메시지를 라우터에게 전송합니다. Leave 메시지를 받은 라우터는 그룹에 남아있는 다른 호스트를 확인하기 위해 해당 그룹에게만 Group-specific Query 메시지를 보냅니다. 이러한 확인 절차가 끝나면, 멀티캐스트 라우터는 해당 그룹에 더 이상 트래픽을 보내지 않습니다.

(1) IGMP Static Join 설정

만약 멀티캐스트 그룹 멤버가 존재하지 않고 호스트가 그룹 멤버쉽을 요청하는 Report 메시지를 보내지 않으면, 더 이상 멀티캐스트 패킷은 전달되지 않게 됩니다. 그러나 V5812G는 IGMP Static Join 기능을 제공합니다. 이 기능은 만약 실제 호스트가 자주 요청하거나, 일반적으로 많이 사용되는 멀티캐스트 트래픽이 있다면, 가상 호스트를 만들어 마치 그룹에 Join 한 것처럼 설정해서 지속적으로 해당 트래픽을 수신할 수 있습니다. 그러나 이 트래픽은 실제 호스트가 연결되어 있는 다른 포트로는 전송되지 않으며, 요청이 올 경우에만 바로 해당 포트로 전송하게 됩니다. 이러한 기능은 호스트가 Join 메시지로 멀티캐스트 트래픽을 최초로 요청하는 시점과 요청된 트래픽이 호스트에 도착하는 시점 사이에 낭비되는 시간을 절약하도록 도와줍니다.

IGMP Static Join 기능을 설정하면 고정적으로 하나의 가상 호스트를 만들어서 마치 해당 포트에 실제로 그룹 멤버가 연결되어 있는 것처럼 하여, 멀티캐스트 트래픽을 받을 수 있게 됩니다. 결과적으로 멀티캐스트 라우터는 해당 그룹에 호스트가 늘 존재한다고 판단합니다.

IGMP Static Join 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp static-group group-address vlan vlan-id port port-number [reporter reporter-ip-address]	Global	IGMP Static Join 기능을 설정하여 해당 포트에 호스트를 멤버로 추가합니다.



참 고

위의 명령어에서 입력하는 “group-address”는 멀티캐스트 그룹의 IP 주소입니다. “reporter-ip-address”는 가상 호스트의 IP 주소입니다.

IGMP Static Join 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp static-group [vlan vlan-id]		
no ip igmp static-group group-address [vlan vlan-id]		
no ip igmp static-group group-address vlan vlan-id [port port-number]	Global	설정했던 IGMP Static Join 기능을 해제합니다.
no ip igmp static-group group-address vlan vlan-id port port-number [reporter reporter-ip-address *]		

Access-list를 지정하여 해당 IGMP 그룹들에게 IGMP Static Join 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp static-group list {<1-99> <1300-1999> access-list-name } vlan vlan-id port port-number [reporter reporter-ip-address]	Global	Access-list를 지정하여 해당 IGMP 그룹들을 IGMP Static Join 기능으로 설정합니다.

Access-list를 지정하여 해당 IGMP 그룹들의 IGMP Static Join 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp static-group list {<1-99> <1300-1999> access-list-name } [vlan vlan-id]		
no ip igmp static-group list {<1-99> <1300-1999> access-list-name } vlan vlan-id port port-number	Global	Access-list의 해당 IGMP 그룹들에게 설정한 IGMP Static Join 기능을 해제합니다.
no ip igmp static-group list {<1-99> <1300-1999> access-list-name } vlan vlan-id port port-number [reporter reporter-ip-address *]		

IGMP Static Join 기능이 설정된 그룹 리스트를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip igmp static-group	Enable / Global / Bridge	IGMP Static Join이 설정된 IGMP 그룹 리스트를 확인합니다.
show ip igmp static-group list {<1-99> <1300-1999> access-list-name } [vlan vlan-id]		해당 Access-list의 IGMP Static Join이 설정된 IGMP 그룹 리스트를 확인합니다.



참 고

IGMP Static Join 기능은 IGMP 버전 2 호스트만 지원합니다. IGMP 버전 3 호스트는 지원하지 않습니다.

(2) 접속 가능한 IGMP 그룹 리스트 설정

사용자는 특정한 Access-list에 존재하는 멀티캐스트 그룹에게만 호스트들이 접근할 수 있도록 제한할 수 있습니다.

각 인터페이스당 특정 Access-list에 포함된 멀티캐스트 그룹들의 접속 리스트를 관리하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp access-group {<1-99> access-list}	Interface	해당 인터페이스의 특정 Access-list의 멀티캐스트 그룹 리스트들을 관리할 수 있도록 설정합니다.

각 인터페이스당 특정 Access-list에 포함된 멀티캐스트 그룹들의 접속 리스트를 관리하는 설정을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp access-group	Interface	해당 인터페이스의 특정 Access-list의 멀티캐스트 그룹 리스트들을 관리하는 설정을 해제합니다.

(3) IGMP Querier 설정

IGMP Querier는 주기적으로 General Query 메시지를 보내서 멀티캐스트 그룹을 관리하는 역할을 합니다. IGMP 버전 2에서는 동일한 네트워크에 2대 이상의 멀티캐스트 라우터가 존재할 경우 서로 주고 받은 Query 메시지를 확인하여 가장 낮은 IP 주소를 가진 라우터가 IGMP Querier가 됩니다.

IGMP Query 메시지 전송 주기 설정

사용자는 IGMP Querier가 멀티캐스트 그룹에 속하는 호스트를 확인하기 위해 보내는 IGMP Query 메시지의 전송 주기를 설정할 수 있습니다.

IGMP Query 메시지의 전송 주기를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp query-interval <1-18000>	Interface	IGMP Query 메시지 전송 주기를 설정합니다.



참 고

IGMP Query 메시지 전송 주기의 단위는 초이며, 기본적으로 125초에 한번씩 주기적으로 IGMP Query 메시지를 전송합니다.

설정된 IGMP Query 메시지 전송 주기를 삭제하고 기본 설정값으로 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp query-interval	Interface	설정된 IGMP Query 메시지 전송 주기를 삭제하고 기본 설정값으로 변경합니다.

IGMP Startup Query 메시지 전송 주기 설정

만약 V5812G가 특정한 IGMP 인터페이스 안에서 IGMP Querier로 선출되었다면, 해당 인터페이스의 멀티캐스트 멤버쉽 정보를 얻기 위해 General Query 메시지를 주기적으로 보내게 됩니다. 장비가 Querier로 선출된 후, 보내는 IGMP Startup Query 메시지의 전송 주기를 설정합니다. V5812G는 그 시간 간격으로 QRV 횟수 만큼 General Query 메시지를 보냅니다.

IGMP Startup Query 메시지의 전송 주기를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp startup-query-interval <1-18000>	Interface	IGMP Startup Query 메시지 전송 주기를 설정합니다.



참 고

IGMP Query 메시지 전송 주기의 단위는 초이며, 기본적으로 32초에 한번씩 주기적으로 IGMP Startup Query 메시지를 전송합니다.

설정된 IGMP Startup Query 메시지 전송 주기를 삭제하고 기본 설정값으로 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp startup-query-interval	Interface	설정된 IGMP Startup Query 메시지 전송 주기를 삭제하고 기본 설정값으로 변경합니다.

IGMP Query 응답 제한 시간 설정

IGMP 버전 2와 버전 3은 멤버쉽 Query 메시지에 응답 제한 시간(Maximum Response Time:MRT)이 추가됩니다. 호스트는 Query 를 수신한 후 이 응답 제한 시간 이내에 Report 메시지를 전송해야 합니다.

멤버쉽 Query 메시지에 대한 호스트의 응답 제한 시간을 지정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp query-max-response-time <1-240>	Interface	멤버쉽 Query 메시지에 대한 응답 제한 시간을 설정합니다.



참 고

응답 제한 시간의 단위는 초이며, 1초부터 240초 범위 안에서 지정할 수 있습니다. 기본값은 10초입니다.

설정한 멤버쉽 Query 메시지에 대한 응답 제한 시간을 삭제하고 기본값으로 변경하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp query-max-response-time	Interface	설정한 멤버쉽 Query 메시지에 대한 응답 제한 시간을 삭제하고 기본 설정값으로 변경합니다.

IGMP Querier 자선출 주기 설정

만약 여러 멀티캐스트 라우터가 Querier로 동작할 경우 연결되어 있는 모든 호스트들에게 중복된 Query 메시지를 보내기 때문에 네트워크 대역폭 낭비를 심화시킬 수 있습니다. 그러므로 동일한 네트워크 망에 Query 메시지를 주기적으로 전송하는 IGMP Querier는 단 하나만 존재해야합니다.

앞에서 설명한 바와 같이 2대 이상의 멀티캐스트 라우터가 존재하는 상황에서는 가장 낮은 IP 주소를 가진 라우터가 Querier로 선출되며 나머지 라우터들은 이때부터 Querier 불능상태 타이머를 작동하기 시작하여 주기적으로 수신되는 Query 메시지를 검사합니다. 만약 가장 낮은 IP 주소를 가진 Querier로부터 Query 메시지가 더 이상 수신되지 않을 경우, 그 다음으로 낮은 IP 주소의 라우터가 이 타이머가 만료된 이후 Querier가 됩니다.

자신보다 낮은 IP 주소를 가진 Query 메시지를 수신한 직후 동작하는 타이머의 시간을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp querier-timeout <60-300>	Interface	Querier를 재선출하는 주기를 설정합니다.



참 고

Querier를 재선출하는 타이머 작동 주기는 60초부터 300초 범위에서 지정하며, 기본값은 255초입니다.

다시 Querier가 선출되는 타이머 시간 설정을 삭제하고 기본값으로 변경하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp querier-timeout	Interface	설정한 타이머 시간을 삭제하고 기본 설정값으로 변경합니다.

IGMP Last Member Query의 전송 횟수와 주기 설정

IGMP Querier가 호스트로부터 Leave 메시지를 받으면 그 해당 그룹에 아직 다른 멤버가 남아있는지를 확인하기 위해 Group-specific Query 메시지(IGMP 버전2)를 보내거나 Group-source-specific Query 메시지(IGMP 버전3)를 정해진 횟수만큼 전송합니다. 그 설정된 횟수만큼 전송한 이후에도 만약 해당 그룹내에 어떠한 멤버도 아무 응답을 하지 않는다면, Querier는 멤버가 없다고 간주하고 더 이상 멀티캐스트 트래픽을 보내지 않습니다.

그러나 IGMP 메시지는 여러가지 변수로 인하여 목적지에 도착하기 전에 없어질 수도 있습니다. 그래서 이러한 경우를 대비하여 Query 메시지를 보내는 횟수나 주기를 설정할 수 있습니다.

Group-specific이나 Group-source-specific Query 메시지의 전송 횟수를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp last-member-query-count <2-7>	Interface	Group-specific과 Group-source-specific Query 메시지의 전송 횟수를 설정합니다.



참 고

Group-specific과 Group-source-specific Query 메시지의 전송 횟수는 2회부터 7회의 범위에서 지정하며, 기본 설정값은 2회입니다..

Group-specific과 Group-source-specific Query 메시지의 전송 횟수의 설정을 삭제하고 기본 설정값으로 변경하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp last-member-query-count	Interface	설정된 Group-specific과 Group-source-specific Query 메시지의 전송 횟수를 삭제하고 기본 설정값으로 변경합니다.

Group-specific과 Group-source-specific Query 메시지의 전송 간격시간을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp last-member-query-interval <1000-25500>	Interface	Group-specific과 Group-source-specific Query 메시지의 전송 주기를 설정합니다.



참 고

Group-specific과 Group-source-specific Query 메시지의 전송 주기 단위는 millisecond이며, 기본 값은 1000 millisecond입니다.

설정한 Group-specific과 Group-source-specific Query 메시지의 전송 간격 시간을 삭제하고 기본 설정값으로 변경하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp last-member-query-interval	Interface	설정한 Group-specific과 Group-source-specific Query 메시지의 전송 주기를 삭제하고 기본 설정값으로 변경합니다.

IGMP Unsolicited Report 메시지의 전송 주기 설정

IGMP 버전 2 Report 메시지는 두가지로 구분됩니다. 호스트가 보내는 것으로 그룹에 새로 가입하여 멀티캐스트 패킷을 요청하는 Join 메시지인 Unsolicited Report 메시지와 IGMP Querier로부터 Query 메시지를 수신한 후 응답 제한 시간(Max Response Time)이내에 응답해야하는 Solicited Report 메시지가 있습니다.

해당 인터페이스가 IGMP Proxy Service가 설정되어 있고, 멤버쉽 내용이 변경되면, 스위치는 상위 라우터 또는 스위치로 IGMP Unsolicited Report 메시지를 보냅니다. 이 Report 메시지 전송 주기를 설정하면, 그 시간 간격으로 QRV 횟수 만큼 메시지를 보내게 됩니다.

Unsolicited Report 메시지의 전송 주기를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp unsolicited-report-interval <1-18000>	Interface	Unsolicited Report 메시지의 전송 주기를 설정합니다.



참 고

IGMP Unsolicited Report 메시지 전송 주기의 단위는 초이며, 기본적으로 10초에 한번씩 주기적으로 메시지를 전송합니다.

설정된 IGMP Unsolicited Report 메시지 전송 주기를 삭제하고 기본 설정값으로 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp unsolicited-report-interval	Interface	설정한 Unsolicited Report 메시지의 전송 주기를 삭제하고 기본 설정값으로 변경합니다.

(4) Immediate Leave 설정

일반적으로 Querier는 호스트가 멀티캐스트 그룹에서 탈퇴하고자 할 때, IGMP 버전 2와 버전 3에서는 호스트로부터 Leave 메시지를 수신하면, Group-specific과 Group-source-specific Query 메시지를 전송하여 해당 멀티캐스트 그룹의 탈퇴여부를 재확인 합니다.

V5812G는 특정한 멀티캐스트 그룹으로부터 Leave 메시지를 수신한 후 Group-specific 과 Group-source-specific Query 메시지를 보내는 절차를 생략하는 설정을 할 수 있습니다. 이러한 Immediate-Leave 설정을 통해 Leave 메시지로 인하여 서브넷에서 마지막 호스트가 그룹을 이탈하는 시점과 Query 시간이 만료되어 멀티캐스트 라우터가 더 이상 그룹에 남아있는 멤버가 없다고 결정하는 시점 사이의 대역폭 낭비를 줄이고 지연 시간을 최소화 할 수 있습니다.

해당 인터페이스에 IGMP Immediate-Leave 기능을 설정하여 관련 access-list의 멀티캐스트 그룹 주소에는 Group-specific 과 Group-source-specific Query 메시지를 보내는 것을 생략하려면, 다음 명령어를 사용하십시오.

IGMP Immediate-Leave 기능을 활성화하려면, Interface 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp immediate-leave group-list {<1 - 99> <1300 – 1999> access list number-ip}	Interface	IGMP Immediate-Leave 기능을 활성화합니다.

IGMP Immediate-Leave 기능을 해제하려면 Interface 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp immediate-leave	Interface	IGMP Immediate-Leave 기능을 해제합니다.



주의

Immediate-leave 기능은 IGMP 버전2 와 IGMP 버전3을 지원하는 인터페이스에 IGMP 호스트 하니만 연결되어 있는 네트워크 환경에서 사용하시기 바랍니다. 만약 같은 인터페이스안에 두대 이상의 호스트가 존재할 경우 Immediate-leave 기능이 활성화된 라우터는 하나의 호스트로부터 Leave 메시지 수신하면 다른 확인없이 해당 그룹의 모든 호스트들을 탈퇴시킵니다.

9.1.3. IGMP 버전 3 설정

IGMP 버전 3은 앞에서도 설명한 바와 같이 Source 필터링 기능을 제공합니다. 이 기능은 특정한 Source 주소를 가진 그룹으로부터만 멀티캐스트 패킷을 수신하거나, 그 그룹만을 제외할 수 있습니다.

Source 필터링 기능은 IGMP 버전 3 멤버쉽 Report 메시지를 통해 구현됩니다. IGMP 버전 3 멤버쉽 Report 메시지에는 여러가지 정보가 포함되는데, 하나는 해당 호스트가 가입된 멀티캐스트 그룹의 현재 상태에 대한 기록이고, 다른 하나는 멤버쉽 변경 사항에 대한 기록입니다. 이 두가지 기록은 필터 모드와 Source 리스트에 대한 정보를 기반으로 만들어집니다. 또한 하나의 Report 메시지에 복수의 멀티캐스트 그룹에 대한 Record를 포함할 수 있어서 적은 양의 패킷을 이용하여 최근 업데이트된 상태를 효율적으로 인지 할 수 있습니다.

V5812G는 기본적으로 IGMP 버전 3으로 동작하며 IGMP 버전 3 snooping 기능을 지원합니다.

IGMP 버전 3 메시지

호스트와 멀티캐스트 라우터 간에 송수신되는 IGMP 버전 3 메시지는 아래와 같이 2가지 종류가 있습니다.

- 멤버쉽 Query 메시지

IGMP 버전 3의 Query 메시지 형식은 다음 그림과 같습니다.

0	8	16	32
IGMP Type = 0x11	Max Response Time	Checksum	
Group Address (그룹 주소)			
Resv	S	QRV	Querier's Query Interval
Number of sources			
Source address(1)			
Source address(...)			
Source address(n)			

【 그림 9-5 】 IGMP 버전 3 Query 메시지 형식

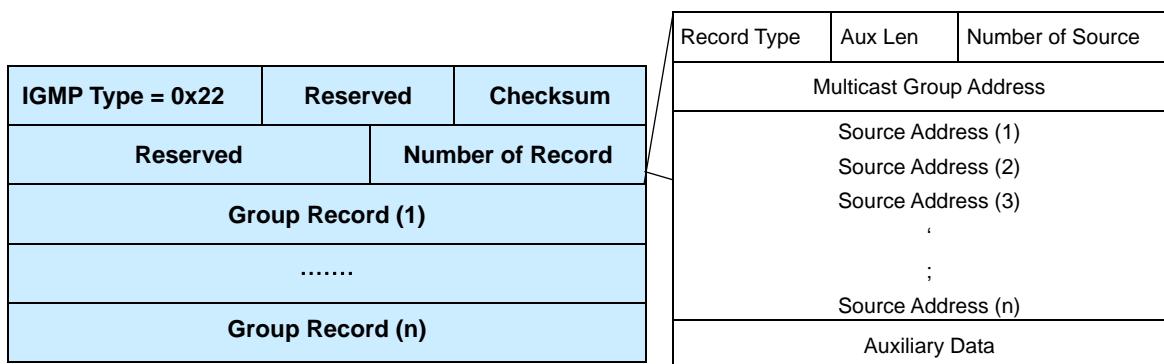
멀티캐스트 라우터는 호스트가 그룹에 가입 유무를 멤버쉽 Query 메시지를 전송하여 확인합니다.

- General Query : Querier가 호스트 그룹 전체에 주기적으로 보내 그룹 가입 여부를 확인합니다.
(IGMP 버전 2 메시지와 동일)
- Group-specific Query : Querier가 Leave 메시지를 수신한 후 해당 그룹으로 메시지를 보내 그룹에 멀티캐스트 트래픽 전송을 원하는 다른 호스트는 없는지 재확인합니다. (IGMP 버전 2 메시지와 동일)

- Group-source-specific Query : Querier가 특정 source 주소를 가진 멀티캐스트 그룹의 호스트로부터 Report 메시지를 수신하면 해당 source 주소로 메시지를 보내 호스트의 가입 유무를 재확인합니다.

- IGMP 버전 3 멤버쉽 Report 메시지

다음은 IGMP 버전 3 Report 메시지 형식입니다.



【 그림 9-6 】 IGMP 버전 3 Report 메시지 형식

IGMP 버전 3 Report 메시지는 해당 호스트가 가입된 멀티캐스트 그룹의 멤버쉽 상태, 변경 사항, 해당 인터페이스에 대한 정보를 포함합니다. 또한 IGMP 버전 3 Report 메시지에는 여러 그룹에 대한 Source 주소, 멀티캐스트 그룹 주소등의 정보가 기록되는데 이것을 Group Record 라고 합니다. 라우터는 이 기록을 기반으로 호스트가 어느 멀티캐스트 그룹에 가입하고자 하는지 또는 탈퇴하고자 하는지를 판단하게 됩니다. 하나의 Report 메시지는 복수의 Group Record를 가질 수 있으며 각각의 Group Record는 다음과 같은 정보들을 포함합니다.

- Current-state: 호스트가 특정 멀티캐스트 주소에서 전송된 패킷만을 받거나 제외했던 기록으로 변경된 정보를 담고 있으며 호스트의 Join/Leave 상태를 확인합니다.
- Filter-mode-change: 최근 include/exclude 필터 모드 상태에서 변경된 사항을 확인합니다.
- Source-list-change: 새롭게 추가되거나 삭제된 Source 멀티캐스트 주소 변경 리스트입니다.

IGMP 버전 3 동작 방식

IGMP 버전 3 동작 방식은 기본적으로 IGMP 버전 2와 유사한 방법으로 멀티캐스트 그룹 멤버의 Join과 Leave가 이루어집니다.

하지만 IGMP 버전 3의 Report 메시지는 기존의 Leave 메시지를 송신하는 절차 없이 메시지에 담긴 정보만을 가지고 특정 source 주소의 패킷만을 허용 또는 차단할 수 있습니다. 다시 말해서, Report 메시지에는 Query 메시지에 대한 응답으로 특정한 호스트가 멀티캐스트 그룹에 Join/Leave에 관한 변경된 정보와 최신 업데이트된 상황까지 기록됩니다. 따라서 멀티캐스트 라우터가 각각의 호스트의 멤버쉽 상태에 대한 정보를 자세하게 인지할 수 있기 때문에 IGMP 버전 2에서 지원했던 Report Suppression은 없어지게 됩니다.

9.1.4. IGMP 설정 확인

사용자가 설정한 V5812G 스위치의 IGMP 그룹과 관련 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip igmp groups [detail]		
show ip igmp groups group-address [detail]		
show ip igmp groups interface-name [detail]	Enable/ Global/ Bridge	멀티캐스트 그룹들과 라우터와 직접적으로 연결되어 있는 스위치들의 IGMP 설정 내용을 확인합니다.
show ip igmp groups interface-name group-address [detail]		
show ip igmp groups interface-name summary		
show ip igmp interface		해당 혹은 모든 인터페이스에 있는 멀티캐스트 관련 설정 내용을 확인합니다.
show ip igmp interface interface-name		

9.2 멀티캐스트 부가 기능 설정

V5812G 는 매우 효율적이고 유연한 멀티캐스트 통신을 구현하기 위해 IGMP Snooping, PIM Snooping, MVR 등의 기능을 지원합니다.

이 장은 다음과 같은 내용으로 이루어집니다.

- 멀티캐스트 포워딩 데이터베이스 설정
- IGMP Snooping 기본 설정
- IGMP 버전 2 Snooping 설정
- IGMP 버전 3 Snooping 설정
- IGMP Snooping 정보 확인
- MVR (Multicast VLAN Registration)
- IGMP 필터링 기능 설정

9.2.1. 멀티캐스트 포워딩 데이터베이스 설정

V5812G 스위치는 내부적으로 멀티캐스트 포워딩 데이터베이스(McFDB) 정보를 이용하여 멀티캐스트 트래픽을 Forwarding 하고, PIM과 IGMP 등 여러가지 멀티캐스트 프로토콜에 의해 수집된 멀티캐스트 포워딩 엔트리 정보를 유지 및 관리합니다.

그리고 멀티캐스트 포워딩 데이터베이스는 L2 FDB(Forwarding Database)의 동작원리와 동일합니다. 특정 멀티캐스트 트래픽이 포트로 유입될 경우, 스위치는 자신의 멀티캐스트 포워딩 데이터베이스와 수신된 트래픽의 엔트리 정보를 비교하여 확인합니다. 만약 기존 데이터베이스에 존재하는 정보라면 특정 포트에 Forwarding 하며, 기존 데이터베이스에 정보가 없다면 Learning 하고 모든 포트에 Flooding 합니다. 일정 시간동안 저장된 멀티캐스트 엔트리 정보를 사용하지 않을 경우, 해당 엔트리 정보를 삭제하여 다른 트래픽이 Forwarding 되도록 허용합니다.

(1) Unknown 멀티캐스트 트래픽 처리

Unknown 멀티캐스트 트래픽이란 한번도 Learning 되지 않아 McFDB에 해당 정보가 없는 트래픽으로 기본적으로 모든 포트에 Flooding 됩니다. 사용자는 Unknown 멀티캐스트 트래픽이 모든 포트에 Flooding 되지 않고 차단하도록 설정 할 수 있습니다. Unknown 멀티캐스트 트래픽을 차단하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip unknown-mcast [port port-number] block	Global	Unknown 멀티캐스트 트래픽을 차단합니다.

Unknown 멀티캐스트 트래픽을 차단하는 설정을 해제하고 다시 Flooding 되도록 하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip unknown-mcast [port port-number] block	Global	Unknown 멀티캐스트 트래픽이 Flooding 되도록 설정합니다.



주의

특정 포트가 멀티캐스트 라우터 포트로 지정되어 있을 경우에는 Unknown 멀티캐스트 트래픽 Flooding을 차단하는 설정을 하지 않도록 주의하십시오.

(2) 포워딩 엔트리 설정

멀티캐스트 포워딩 데이터베이스에 기록된 멀티캐스트 엔트리 정보를 일정한 기간 동안 사용하지 않을 경우, 해당 엔트리 정보를 삭제하여 다른 트래픽이 Forwarding 될 수 있도록 합니다. 즉, 스위치 저장 용량의 한계가 있으므로 시간이 지나면 삭제하여 새로운 주소를 기록할 공간을 만듭니다.

V5812G의 멀티캐스트 포워딩 데이터베이스의 Aging time이나 엔트리 개수를 제한하는 Aging-limit 을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip mcfdb aging-limit aging-limit-value	Global	McFDB의 포워딩 엔트리 최대 개수를 지정합니다.
ip mcfdb aging-time aging-time-value		McFDB의 포워딩 엔트리 정보가 저장되는 aging-time 을 설정합니다.



참 고

“aging-limit-value”는 256개부터 65535개의 범위에서 설정 가능하며 기본값은 5000개입니다.

“aging-time-value” 단위는 초이며 범위는 10초부터 10,000,000초입니다. 기본값은 300초입니다.

설정된 Aging-time 이나 Aging-limit 을 삭제하고 기본값으로 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip mcfdb aging-limit	Global	설정한 aging-limit을 삭제합니다.
no ip mcfdb aging-time		설정한 aging-time을 삭제합니다.

(3) 멀티캐스트 포워딩 데이터베이스 확인 및 초기화

V5812G에 설정되거나 기록된 멀티캐스트 포워딩 엔트리 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip mcfdb	Enable/	시스템에 등록된 멀티캐스트 엔트리의 aging-time과 aging-limit의 설정값을 확인합니다.
show ip mcfdb aging-entry {vlan vlan-id group group-address} [mac-based detail]	Global/ Bridge	각 옵션에 따라 L2 멀티캐스트 포워딩 엔트리 정보를 확인합니다.
show ip mcfdb aging-entry [mac-based detail]		

멀티캐스트 포워딩 엔트리 정보를 초기화 하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip mcfdb [* vlan vlan-id]	Enable/	모든 혹은 특정 VLAN의 멀티캐스트 포워딩 엔트리 정보를 초기화합니다.
clear ip mcfdb vlan vlan-id group group-ip-address source ip-address	Global	특정한 멀티캐스트 그룹 주소와 VLAN으로부터 사용되는 멀티캐스트 포워딩 엔트리 정보를 초기화합니다.

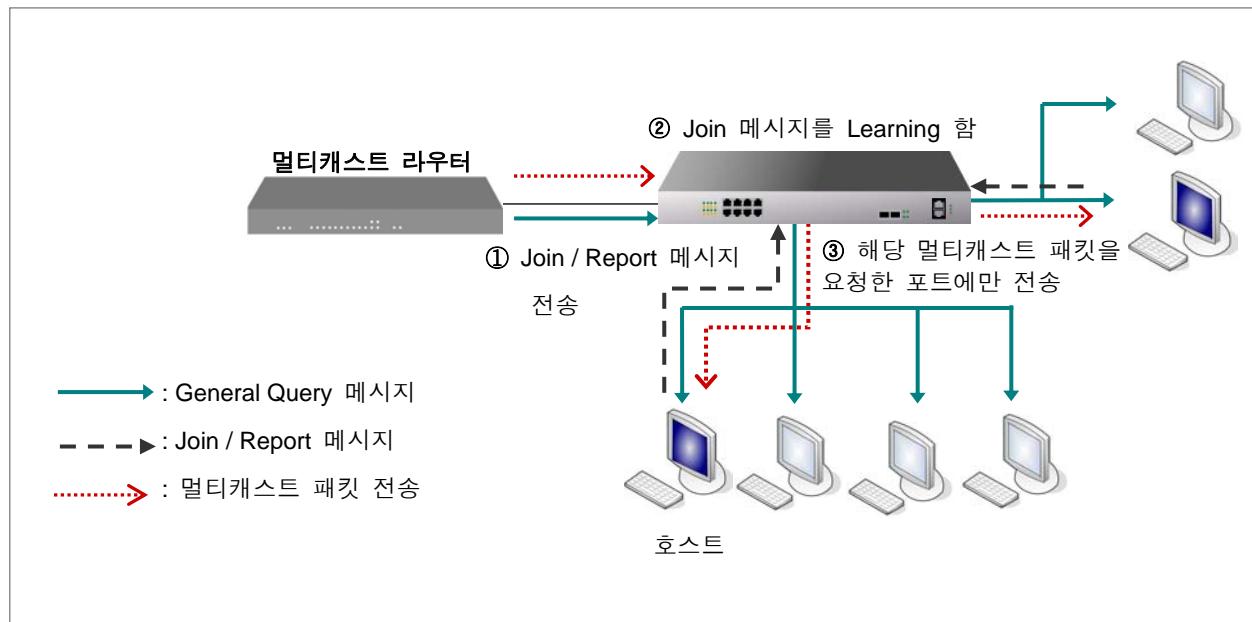
9.2.2. IGMP Snooping 기본 설정

일반적으로 L2 스위치는 멀티캐스트 트래픽을 받으면 브로드캐스트 도메인내의 모든 포트로 Flooding 합니다. 그 이유는 멀티캐스트 주소는 Source 주소로 쓰이지 않기 때문에 스위치가 멀티캐스트 주소를 정상적으로 Learning 하지 못하므로 L2 포워딩 테이블인 MAC 테이블에서는 해당 트래픽의 엔트리 정보를 확인할 수 없습니다. 이러한 멀티캐스트 트래픽의 Flooding은 대역폭을 낭비하게 됩니다.

IGMP Snooping 기능은 L2 네트워크 환경에서 멀티캐스트 트래픽의 Flooding을 막는 역할을 합니다. IGMP Snooping 이 활성화된 스위치는 호스트와 라우터 사이의 송수신되는 패킷 전송 이동경로를 훔쳐보며(Snooping) 관련 정보를 테이블에 저장합니다. 또한 스위치가 특정 멀티캐스트 그룹의 호스트로부터 Join 요청 메시지를 받을 경우, 스위치는 그 호스트와 해당 멀티캐스트 그룹이 연결되어 있는 포트 관련 정보를 포워딩 테이블 엔트리에 저장합니다. 그리고 해당 호스트로부터 Leave 메시지를 수신하면 테이블에서 해당 엔트리를 삭제합니다.

V5812G는 멀티캐스트 포워딩 테이블 관리를 통해 멀티캐스트 트래픽을 필요로 하는 호스트들에게만 패킷을 효과적으로 전송할 수 있습니다.

다음은 IGMP Snooping이 활성화 된 스위치가 호스트와 멀티캐스트 라우터 사이에서 멀티캐스트 통신을 하는 모습입니다.



【 그림 9-7 】 IGMP Snooping을 설정했을 경우

(1) IGMP Snooping 활성화

IGMP Snooping 기능은 각 VLAN 별로 또는 시스템 전체에 활성화 할 수 있습니다. IGMP Snooping 기능을 활성화하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping	Global	시스템 전체에 IGMP snooping 기능을 활성화 합니다.
ip igmp snooping vlan <i>vlan-id</i>		특정 VLAN에 IGMP snooping 기능을 활성화합니다.



참 고

V5812G의 IGMP Snooping 기능은 기본적으로 해제되어 있습니다.

한편, IGMP Snooping 기능을 해제하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping	Global	IGMP Snooping 기능을 해제 합니다.
no ip igmp snooping vlan <i>vlan-id</i>		특정 VLAN에 설정한 IGMP Snooping 기능을 해제 합니다.

IGMP Snooping에 대한 설정을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip igmp snooping [vlan <i>vlan-id</i>]	Enable / Global / Bridge	IGMP Snooping 기능에 대한 설정을 확인합니다.

(2) IGMP Snooping 버전 설정

멀티캐스트 라우터가 수신하는 Report 메시지들은 각 인터페이스의 IGMP 버전에 기초하여 전송됩니다. 사용자는 수동으로 각 인터페이스의 IGMP Snooping 버전을 지정 할 수 있으며, Report 메시지는 해당 버전으로만 송신됩니다. V5812G는 기본적으로 IGMP Snooping 버전 3으로 동작합니다.

IGMP Snooping 버전 3으로 동작하는 스위치가 IGMP 버전 1 Query 메시지를 수신할 경우, 능동적으로 IGMP 버전 1으로 동작하게 되어 해당 라우터에게 버전1 Report 메시지를 보내게 됩니다. 만약 스위치가 지속적으로 IGMP 버전 1 Query 메시지를 받지 않는다면, 일정 시간이 지나고 해당 인터페이스는 IGMP Snooping 버전 3으로 다시 동작하게 됩니다.

특정 VLAN 인터페이스나 시스템 전체의 IGMP Snooping의 버전을 수동으로 지정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping version <1-3>		시스템에 IGMP Snooping 버전을 설정합니다.
ip igmp snooping vlan <i>vlan-id</i> version <1-3>	Global	특정 VLAN에 IGMP Snooping 버전을 설정합니다.



참 고

V5812G의 IGMP Snooping 버전은 Static으로 설정할 때만 변경합니다.

설정한 IGMP Snooping 버전을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping [vlan <i>vlan-id</i>] version	Global	설정했던 IGMP Snooping 버전을 해제하고 기본 설정인 버전 3으로 변경합니다.

(3) Robustness Variable 설정

Robustness Variable 설정은 Link failure나 갑작스러운 Bursty error 등의 이유로 네트워크 상태가 불안정하여 패킷 손실이 예상되는 환경에서 Query에 대한 응답이 전달되지 않는 상황을 방지하기 위해 사용합니다. 이 값은 Query 메시지에 설정되는 것으로 호스트는 Robustness variable 값의 횟수 만큼 Report 메시지를 보냅니다. 네트워크의 패킷 손실이 많을 경우에는 Robustness variable 값을 크게 설정하여 Report 메시지를 여러 번 보내도록 하여 패킷 수신 확률을 높여야 합니다.



참 고

네트워크 상태가 좋지 않을수록 Robustness variable 값은 크게 설정하십시오. 단, Robustness variable 값으로 인해 Query 메시지에 대한 응답 횟수가 늘어나면 Leave Latency도 증가합니다.

Robustness variable 값을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping robustness-variable <1-7>	Global	Robustness variable 값을 설정합니다.
ip igmp snooping vlan <i>vlan-id</i> robustness-variable <1-7>		특정 VLAN에 Robustness variable 값을 설정합니다.



참 고

V5812G 스위치에 IGMP Snooping 기능이 활성화되면, Robustness variable 값은 기본적으로 2회로 설정되어 있습니다. Robustness variable은 2회부터 7회까지 설정 가능합니다.

설정했던 Robustness variable 값을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping robustness-variable	Global	Robustness variable 설정값을 삭제하고 기본 설정값으로 변경됩니다.
no ip igmp snooping vlan <i>vlan-id</i> robustness-variable		

9.2.3. IGMP 버전 2 Snooping 설정

(1) IGMP Snooping Querier 설정

네트워크 상에서 IGMP Querier가 없을 때, IGMP Snooping Querier가 그 역할을 대신합니다. 또한 IGMP Snooping Querier는 PIM 과 IGMP 기능이 설정되지 않은 특정 VLAN에서 IGMP Snooping 기능을 지원하도록 도와줍니다.

V5812G에 IGMP Snooping Querier가 활성화되면, IGMP Querier처럼 주기적으로 General Query 메시지를 보내서 어떤 호스트가 멀티캐스트 트래픽을 받고자 하는지 확인합니다.

IGMP Snooping Querier 활성화

IGMP Snooping Querier를 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping querier [address source-address]	Global	IGMP Snooping Querier를 활성화합니다.
ip igmp snooping vlan <i>vlan-id</i> querier [address source-address]		특정 VLAN에 IGMP Snooping Querier를 활성화합니다.

IGMP Snooping Querier를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping [vian <i>vlan-id</i>] querier [address source-address]	Global	IGMP Snooping Querier 설정을 해제합니다.



만약 IGMP Snooping Querier 지정을 위한 Source 주소가 설정되어 있지 않을 경우에는 우선 해당 VLAN의 Interface의 IP를 사용하고, 그렇지 않을 경우 0.0.0.0으로 설정합니다.

IGMP Snooping Query 전송 주기 설정

IGMP Snooping Querier가 보내는 General Query 메시지의 전송 주기를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping querier query-interval <1-1800>	Global	IGMP Snooping Query 메시지 전송 주기를 설정합니다.
ip igmp snooping vlan <i>vlan-id</i> querier query-interval <1-1800>		특정 VLAN의 IGMP Snooping Query 메시지 전송주기를 설정합니다.



참 고

IGMP Snooping Querier가 보내는 Query 메시지 전송 간격의 단위는 초이며, 기본적으로 125초에 한번씩 주기적으로 General Query 메시지를 전송합니다.

설정된 General Query 메시지 전송 간격을 삭제하려면, Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping [vian <i>vlan-id</i>] querier query-interval	Global	사용자가 설정한 IGMP Snooping Query 메시지 전송 간격을 삭제하고 기본 설정값으로 변경합니다.

IGMP Snooping Query 응답 제한 시간 설정

IGMP 버전 2와 버전 3 멤버쉽 Query 메시지에 추가된 응답 제한 시간(Maximum Response Time:MRT)은 IGMP Snooping Querier가 주기적으로 보내는 Query 메시지를 전송한 후 호스트의 Report 메시지를 최대로 기다려주는 시간입니다. 호스트는 정해진 응답 제한 시간 이내에 Report 메시지를 전송해야 합니다.

General Query 메시지에 대한 호스트의 응답 제한 시간을 지정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping querier max-response-time <1-25>	Global	IGMP Snooping Query 메시지의 응답 제한 시간을 지정합니다.
ip igmp snooping vlan <i>vlan-id</i> querier max-response-time <1-25>		특정 VLAN의 IGMP Snooping Query 메시지의 응답 제한 시간을 지정합니다.



참 고

IGMP Snooping Query에 대한 응답 제한 시간의 단위는 초이며, 1초부터 25초 범위 안에서 지정할 수 있습니다. 기본값은 10초입니다..

설정된 응답 제한 시간을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping querier max-response-time	Global	특정 VLAN 또는 시스템 전체에 설정된 IGMP Snooping Query 메시지의 응답 제한 시간을 삭제하고 기본값으로 변경합니다..
no ip igmp snooping vlan <i>vlan-id</i> querier max-response-time		

IGMP Snooping Querier 정보 확인

한편, IGMP Snooping Querier 정보와 관련 설정값을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip igmp snooping [vlan <i>vlan-id</i>] querier [detail]	Enable/ Global/ Bridge	IGMP Snooping Querier 정보와 관련 설정값을 확인합니다.

(2) IGMP Snooping Last Member Query의 전송 주기 설정

IGMP Snooping이 활성화 된 스위치가 Leave 메시지를 수신하면 해당 호스트가 있는 멀티캐스트 그룹으로 Group-specific Query(IGMP 버전 2) 또는 Group-source-specific Query(IGMP 버전 3) 메시지를 전송하여 해당 호스트의 탈퇴 여부와 다른 호스트의 가입 유무를 재확인 합니다. 만약 호스트의 응답이 없으면 스위치는 해당 그룹으로 멀티캐스트 트래픽을 더 이상 보내지 않습니다.

그러나 네트워크 망이 불안하거나 패킷 손실이 유발되는 상황에는 해당 IGMP 메시지를 유실할 수 있는데 이러한 문제를 방지하기 위해 Query 메시지 전송 주기를 임의로 설정할 수 있습니다.

Group-specific 또는 Group-source-specific Query 메시지를 전송하는 주기를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping last-member-query-interval <100-10000>	Global	마지막 호스트의 탈퇴 여부를 확인하는 Query 메시지 전송 주기를 설정합니다.
ip igmp snooping vlan <i>vlan-id</i> last-member-query-interval <100-10000>		특정 VLAN에 남은 호스트의 탈퇴 여부를 확인하는 Query 메시지 전송 주기를 설정합니다.



참 고

Group-specific 또는 Group-source-specific Query 메시지를 전송하는 주기의 시간 단위는 100 millisecond에서 10000 millisecond까지 설정할 수 있습니다. 기본값은 1000ms 입니다.

설정되어 있는 Group-specific 또는 Group-source-specific Query 메시지 전송 주기를 삭제하고 기본값으로 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping last-member-query-interval	Global	설정된 Group-specific 또는 Group-source-specific Query 메시지 전송 주기를 삭제합니다.
no ip igmp snooping vlan <i>vlan-id</i> last-member-query-interval		특정 VLAN에 설정된 Group-specific 또는 Group-source-specific Query 메시지 전송 주기를 삭제합니다.

(3) IGMP Snooping Immediate-Leave 설정

V5812G의 IGMP Snooping Immediate-leave 기능이 활성화되면 호스트가 Leave 메시지를 보낼 경우 Group-specific 또는 Group-source-specific Query 메시지를 보내는 과정을 생략합니다. 그리고 해당 호스트의 멀티캐스트 그룹 엔트리를 곧바로 IGMP Snooping 맴버쉽 테이블에서 삭제하고 관련 정보를 멀티캐스트 라우터에게 알려줍니다.

IGMP Snooping Immediate-leave 기능을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping immediate-leave	Global	시스템 전체에 Immediate-leave 기능을 활성화 합니다.
ip igmp snooping port port-number immediate-leave		특정 포트에 Immediate-leave 기능을 활성화 합니다.
ip igmp snooping vlan vlan-id immediate-leave		특정 VLAN에 Immediate-leave 기능을 활성화 합니다.



주의

Immediate-leave 기능은 반드시 호스트 트래킹 기능과 같이 사용하십시오. (1.1.1(6) 호스트 트래킹 기능 설정 참고) 만약 호스트 트래킹 기능이 해제된 상태에서 Immediate-leave 기능이 활성화되면 동일한 멀티캐스트 그룹내에 복수의 호스트가 존재할 경우 하나의 호스트가 Leave 메시지를 보내더라도 IGMP Snooping Querier는 바로 해당 그룹의 모든 호스트들을 확인없이 탈퇴시킵니다. 이 때문에 통신을 원하는 다른 호스트들마저 더 이상 트래픽을 받을 수 없게 됩니다.

IGMP Snooping Immediate-leave 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping immediate-leave	Global	
no ip igmp snooping port port-number immediate-leave		IGMP Snooping Immediate-leave 기능을 해제합니다.
no ip igmp snooping vlan vlan-id immediate-leave		

(4) IGMP Snooping Report Suppression 설정

멀티캐스트 라우터는 멀티캐스트 그룹내에 한 호스트에게서만 Report 메시지를 받아도 해당 그룹에 멀티캐스트 트래픽을 보내기 때문에 그룹의 모든 호스트마다 Report 메시지를 받으면 불필요한 트래픽으로 인해 대역폭을 낭비하게 됩니다. 이에 대한 해결책으로 IGMP 버전 2에서는 해당 멀티캐스트 그룹내에서 처음 송신하는 Report 메시지 정보를 공유하여 다른 호스트들은 중복해서 Report 메시지를 보내지 않는 Report Suppression 기능이 제공됩니다.

하지만 호스트와 라우터 사이에 L2 스위치가 존재할 경우, IGMP Snooping이 활성화 된다면 반드시 IGMP Report Suppression 기능을 지원하여 각각의 호스트가 보내는 모든 Report 메시지가 멀티캐스트 라우터에게 전송되는 것을 막아야 합니다.

L2 스위치가 Report Suppression이 활성화되면 각 멀티캐스트 그룹내 호스트들 중 최초로 보내는 Report 메시지 또는 마지막으로 탈퇴하는 호스트가 보내는 Leave 메시지만을 멀티캐스트 라우터에게 전달합니다.

IGMP Snooping Report Suppression 기능을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping report-suppression	Global	시스템 전체에 IGMP Snooping Report Suppression을 활성화합니다.
ip igmp snooping vlan <i>vlan-id</i> report-suppression		특정 VLAN에 IGMP Snooping Report Suppression을 활성화합니다.



주의

IGMP Snooping Report Suppression은 IGMP 버전 1과 버전 2에서만 설정 가능합니다.

IGMP Snooping Report Suppression 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping [vlan <i>vlan-id</i>] report-suppression	Global	IGMP Snooping Report Suppression 기능을 해제합니다.

(5) IGMP Snooping S-Query Report Agency 설정

IGMP snooping이 활성화된 장비는 기본적으로 멀티캐스트 라우터로부터 IGMP Group Specific Query 메시지를 수신하면 모든 포트에 Flooding 합니다. Group Specific Query 메시지를 받는 호스들은 자신의 멤버쉽 정보에 따라 Report 메시지로 응답하기 때문에 연결된 네트워크 장비 및 호스트들의 부하가 커질 수 있습니다. IGMP Snooping Specific-Query Report Agency가 활성화되면 해당 멀티캐스트 그룹 호스트들에게 IGMP Group Specific Query 메시지를 Flooding 하지 않으며, 호스트를 대신하여 IGMP Report 메시지로 응답하게 됩니다.

라우터로부터 IGMP Group Specific Query 메시지를 수신할 경우, 호스트 대신 IGMP Report 메시지로 응답하게 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping s-query-report agency	Global	IGMP Snooping S-Query Report Agency를 활성화 합니다.

라우터로부터 IGMP Group Specific Query 메시지를 수신할 경우, 해당 그룹으로 Flooding 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping s-query-report agency	Global	IGMP Snooping S-Query Report Agency를 해제 합니다.

(6) 호스트 트래킹 기능 설정

호스트 트래킹 기능이란 호스트가 보내는 Report 메시지를 통해 해당 호스트의 멤버쉽 정보를 수집하여 호스트 트래킹 데이터베이스에 저장하는 것으로 Join 된 호스트를 보다 효율적으로 관리 할 수 있습니다. 모든 IGMP 버전에 지원되며 IGMP 버전 3의 Immediate-blocking 또는 IGMP 버전 2의 Immediate-leave 기능을 통해 해당 멀티캐스트 그룹에서 하나의 호스트만 Leave 메시지를 보내더라도 모든 호스트가 멀티캐스트 트래픽을 받지 못하는 문제를 방지합니다.

이 기능은 인터페이스에 IGMP 호스트 하나만 연결되어 있는 네트워크 환경에서 사용해야 하는 Immediate-leave 기능의 제약 사항을 해결하며 호스트가 탈퇴할 때 필요한 지연 시간을 최소화합니다. Join 하는 호스트들을 관리하는 호스트 트래킹 기능을 활성화 하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping explicit-tracking	Global	시스템 전체에 IGMP 호스트 트래킹 기능을 설정 합니다.
ip igmp snooping vlan <i>vlan-id</i> explicit-tracking		특정 VLAN에 IGMP 호스트 트래킹 기능을 설정 합니다.

설정한 호스트 트래킹 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping explicit-tracking		시스템에 IGMP 호스트 트래킹 기능을 해제합니다.
no ip igmp snooping vlan <i>vlan-id</i> explicit-tracking	Global	특정 VLAN의 IGMP 호스트 트래킹 기능을 해제합니다.

사용자는 특정 포트에 대해 Join 하는 호스트의 개수를 제한할 수 있습니다. 만약 설정된 호스트의 개수를 초과하여 Join을 시도할 경우에는 해당 그룹에 Join은 되지만 호스트의 정보는 호스트 트래킹 데이터베이스에 저장되지 않고 이에 대한 메시지를 출력합니다.

특정 포트를 통해 Join 하는 호스트의 최대 개수를 지정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping explicit-tracking max-hosts port <i>port-number</i> count <1-65535>	Global	특정 포트에 Join 하는 호스트의 최대 개수를 설정합니다.
no ip igmp snooping explicit-tracking max-hosts port <i>port-number</i>		설정했던 호스트 최대 개수를 삭제하고 기본값으로 변경합니다.



참 고

특정 포트에 Join 하는 호스트의 최대 개수는 1에서 65535까지 범위 안에서 설정할 수 있습니다. 기본 설정값은 1024입니다.

호스트 트래킹 기능을 통해 호스트가 그룹에 Join 되어 있는지 확인할 수 있으나, 만약 비정상적으로 Leave 메시지를 보내지 않고 종료되는 호스트가 있을 경우에는 호스트 트래킹 데이터 베이스가 항상 정확한 것은 아닙니다. 그러므로 장비는 기본적으로 호스트에게 Leave 메시지를 받으면 Group specific Query 메시지를 보내서 재확인을 합니다. 하지만 이로 인해 장비와 호스트들의 로드 가 커질 수 있으므로, 이에 대한 설정을 해제시킬 수 있습니다.

호스트로부터 Leave 메시지를 받을 경우, Group Specific Query 메시지 전송을 해제 하거나, 활성화 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping explicit-tracking s-query-suppression	Global	호스트로부터 Leave 메시지를 받을 때, Group Specific Query 메시지를 전송하지 않습니다.
no ip igmp snooping explicit-tracking s-query-suppression		호스트로부터 Leave 메시지를 받을 때, Group Specific Query 메시지를 전송합니다.



V5812G는 기본적으로 Leave 메시지를 수신 후 Group Specific Query 메시지를 전송하며, 해당 설정은 모든 VLAN에 적용됩니다.

IGMP Snooping 호스트 트래킹의 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip igmp snooping explicit-tracking		시스템 전체의 호스트 트래킹 정보를 확인합니다.
show ip igmp snooping explicit-tracking vlan <i>vlan-id</i>	Enable/ Global/	특정 VLAN의 호스트 트래킹 정보를 확인합니다.
show ip igmp snooping explicit-tracking port <i>port-number</i>	Bridge	특정 포트의 호스트 트래킹 정보를 확인합니다.
show ip igmp snooping explicit-tracking group <i>group-address</i>		특정 멀티캐스트 그룹 주소의 호스트 트래킹 정보를 확인합니다.

(7) 멀티캐스트 라우터 포트 설정

멀티캐스트 라우터 포트란 멀티캐스트 라우터와 직접적으로 연결되어 있는 포트를 뜻합니다. 사용자는 멀티캐스트 라우터가 연결되어 있는 포트를 직접적으로 설정할 수도 있고, PIM hello 패킷과 IGMP Query 메시지가 수신되는 포트를 통해 지정 할 수 있습니다.

Static 멀티캐스트 라우터 포트 설정

사용자는 L2 포트를 멀티캐스트 라우터와 연결되어 있는 포트로 지정해 줄 수 있습니다. 멀티캐스트 라우터 포트를 지정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping mrouter port {port-number cpu}	Global	멀티캐스트 라우터 포트를 지정합니다.
ip igmp snooping vlan vlan-id mrouter port {port-number cpu}		특정한 VLAN에 멀티캐스트 라우터 포트를 지정합니다.

멀티캐스트 라우터 포트를 지정한 것을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping mrouter port {port-number cpu}	Global	멀티캐스트 라우터 포트를 지정했던 것을 해제합니다.
no ip igmp snooping vlan vlan-id mrouter port {port-number cpu}		

멀티캐스트 라우터 포트 Learning 설정

멀티캐스트 라우터 포트는 L2의 모든 멀티캐스트 엔트리 관리를 위해 포워딩 테이블에 추가됩니다. V5812G 스위치는 PIM hello 패킷이 들어오는 포트를 멀티캐스트 라우터 포트로 인지하도록 지정할 수 있습니다.

PIM hello 패킷이 들어오는 포트를 멀티캐스트 라우터 포트로 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping mrouter learn pim	Global	시스템 전체의 PIM hello 패킷이 들어오는 포트를 멀티캐스트 라우터 포트로 지정합니다.
ip igmp snooping vlan vlan-id mrouter learn pim		특정 VLAN의 PIM hello 패킷이 들어오는 포트를 멀티캐스트 라우터 포트로 지정합니다.

PIM hello 패킷을 이용하여 멀티캐스트 라우터 포트를 지정하는 설정을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping mrouter learn pim		
no ip igmp snooping vlan <i>vlan-id</i> mrouter learn pim	Global	PIM hello 패킷을 이용하여 멀티캐스트 라우터 포트를 지정하는 설정을 해제합니다.

멀티캐스트 라우터 포트 Forwarding 설정

멀티캐스트 Source 정보를 멀티캐스트 라우터로 보내야 하기 때문에, L2 스위치의 경우 IGMP Snooping 멤버쉽 포트들과 멀티캐스트 라우터 포트들로 멀티캐스트 트래픽이 포워딩되어야 합니다

멀티캐스트 라우터 포트는 Static으로 설정되거나, General Query 메시지를 수신 또는 PIM Hello 패킷을 수신한 포트로 설정 할 수 있습니다.

멀티캐스트 라우터 포트로 멀티캐스트 트래픽 Forwarding을 활성화 또는 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip multicast mrouter-pass-through		멀티캐스트 라우터 포트들로 멀티캐스트 트래픽을 포워딩합니다.
no ip multicast mrouter-pass-through	Global	멀티캐스트 라우터 포트들로 멀티캐스트 트래픽이 포워딩되지 않습니다.

멀티캐스트 라우터 포트 확인

IGMP Snooping 멀티캐스트 라우터 포트를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip igmp snooping mrouter	Enable/ Global/	지정된 멀티캐스트 라우터 포트를 확인합니다.
show ip igmp snooping vlan <i>vlan-id</i> mrouter	Bridge	특정 VLAN에 지정된 멀티캐스트 라우터 포트를 확인합니다.

(8) 멀티캐스트 TCN Flooding 설정

IGMP Snooping TCN 기능은 이더넷 망에서의 신뢰성 있는 멀티캐스트 서비스를 위하여 STP(Spanning Tree Protocol) 또는 ERP(Ethernet Ring Protection)와 같은 프로토콜을 사용했을 때, 토폴로지가 갑자기 변경되었을 경우 신속한 통신 서비스 복구를 위한 기능입니다. 이 기능은 이더넷 링 토폴로지와 같은 망을 이용하여 Redundancy를 제공하는데 중요한 역할을 합니다.

IGMP Snooping TCN은 토폴로지의 변화를 감지할 때 일정 시간동안 멀티캐스트 트래픽을 Flooding 하는 기능과 망의 IGMP Querier에게 IGMP General Query를 요청하는 두가지 기능을 제공합니다.

첫번째, Flooding 기능은 토폴로지 변화가 감지되면 서비스 중인 멀티캐스트 트래픽을 모든 포트로 Flooding 하여 토폴로지의 변화로 인해 서비스가 중단되는 것을 막습니다.

이 Flooding은 Query 메시지가 지정된 전송 주기와 개수만큼 수신된 시간 이후 멈추게 됩니다. 그 이후에는 Join 한 포트로만 서비스 합니다. 예를 들면, IGMP General Query 메시지를 보내는 횟수는 2번이고 메시지 전송 주기는 125초로 기본 설정값일 때 멀티캐스트 트래픽은 250초 동안만 Flooding 됩니다. 멀티캐스트 통신 서비스가 많은 환경에서 IGMP Snooping TCN으로 인한 Flooding 은 특정 포트의 대역폭을 낭비할 수 있기 때문에 이 기능만을 해제할 수 있습니다.

두번째, STP나 ERP의 Root 스위치가 토폴로지의 변화를 감지하면 “General Query Solicitation” 메시지를 전 포트로 전송하여 IGMP General Query 메시지를 요청하는 기능입니다. 이 메시지를 받은 IGMP Querier는 General Query를 전송합니다. 단, IGMP Querier가 General Query Solicitation을 인식 할 수 있어야 합니다.

멀티캐스트 TCN 활성화

IGMP Snooping TCN 기능을 활성화하기 위해서는 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping tcn flood		IGMP Snooping TCN 기능을 활성화합니다.
ip igmp snooping tcn vlan valn-id flood	Global	특정 VLAN에 IGMP Snooping TCN 기능을 활성화합니다.

설정한 IGMP Snooping TCN 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping tcn flood		IGMP Snooping TCN 기능을 해제합니다.
no ip igmp snooping tcn vlan <i>vlan-id</i> flood	Global	특정 VLAN에 설정된 IGMP Snooping TCN 기능을 해제합니다.

TCN Flooding Suppression

IGMP Snooping 기능이 활성화되어 있는 스위치가 TCN을 받으면 기본적으로 125초의 전송 주기를 가진 General Query 메시지를 2번 받을 때까지 모든 포트에 멀티캐스트 트래픽을 Flooding 합니다. 사용자는 멀티캐스트 트래픽을 Flooding 하는 것을 멈추는 시간을 결정하는 IGMP Query 메시지의 수신 횟수 혹은 전송 주기를 임의로 설정할 수 있습니다.

멀티캐스트 트래픽의 Flooding을 멈추는 IGMP Query 메시지 전송 횟수를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping tcn flood query count <1-10>	Global	IGMP General Query 수신 횟수를 설정하여 멀티캐스트 Flooding을 멈춥니다.



참 고

멀티캐스트 트래픽 Flooding을 멈추는 IGMP Query 메시지의 전송 횟수는 1회에서 10회 범위 안에서 지정하며, 기본값은 2회입니다..

멀티캐스트 Flooding 관련하여 설정한 Query 메시지 전송 횟수를 해제하려면, Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping tcn flood query count	Global	IGMP General Query 수신 횟수 설정을 삭제하고 기본값으로 설정합니다.



참 고

V5812G가 TCN을 인지하고 멀티캐스트 트래픽 Flooding을 하는 시간은 설정된 Query 메시지의 전송 횟수와 전송 주기를 곱한 시간입니다. 예를 들면 횟수는 3번, 전송 간격은 100초로 설정되어 있다면 멀티캐스트 트래픽의 Flooding은 300초 동안만 지속됩니다.

멀티캐스트 Flooding을 멈추는 IGMP Query 메시지 전송 주기를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping tcn flood query interval <1-1800>	Global	수신할 IGMP General Query 주기를 설정합니다.



참 고

멀티캐스트 트래픽 Flooding을 멈추는 IGMP Query 메시지를 전송 주기의 단위는 초이며 1초부터 1800초 범위 안에서 설정할 수 있습니다. 기본적으로 125초에 한번씩 주기적으로 IGMP Query 메시지를 전송합니다.

멀티캐스트 Flooding을 멈추는 Query 메시지 전송 주기를 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping tcn flood query interval	Global	수신할 IGMP General Query 주기 설정을 삭제하고 기본값으로 설정합니다.

TCN Flooding Solicitation 메시지 전송

네트워크의 토플로지가 변경되었을 경우, Root 스위치는 “General Query Solicitation” 메시지를 그룹 주소 0.0.0.0을 지정하여 모든 포트로 전송합니다. 멀티캐스트 라우터가 이 Solicitation 메시지를 수신하면 바로 IGMP General Query 메시지를 전송합니다.

TCN 을 수신했을 경우 Query Solicitation 메시지를 전송하도록 하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping tcn query solicit	Global	시스템 상에 TCN을 수신했을 때, Query Solicitation 메시지를 보냅니다.
ip igmp snooping tcn query solicit address source-address		Source 주소를 설정하여 Query Solicitation 메시지를 보냅니다.



만약 Source 주소가 설정되어 있지 않을 경우에는 우선 해당 VLAN의 Interface의 IP를 사용하고, 그렇지 않을 경우 0.0.0.0으로 설정합니다.

Query Solicitation 메시지를 전송하는 설정을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping tcn query solicit	Global	Query Solicitation 메시지를 보내지 않습니다.
no ip igmp snooping tcn query solicit address		해당 Source 주소로 Query Solicitation 메시지를 보내는 설정을 해제합니다.

TCN Flooding 디버깅

IGMP Snooping TCN 기능을 효율적으로 디버깅하거나 그 설정을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
debug igmp snooping tcn	Enable	IGMP Snooping TCN 기능을 디버깅합니다.
no debug igmp snooping tcn		디버깅 설정을 해제합니다.

9.2.4. IGMP 버전 3 Snooping 설정

Immediate Blocking 설정

IGMP 버전 3의 Report 메시지에는 include/exclude 필터 모드와 패킷 전송이 허용 또는 차단된 특정 Source 멀티캐스트 주소 리스트를 담은 정보를 담고 있습니다.

IGMP 버전 3의 Immediate Blocking 기능은 호스트 트래킹 데이터 베이스를 참고하여 호스트가 특정 Source 멀티캐스트 주소들로부터 수신되는 트래픽만을 신속하게 차단하는 역할을 합니다. 예를 들면, 호스트가 특정 Source 주소의 멀티캐스트 트래픽 수신을 원하지 않는 정보를 담은 Report 메시지를 보낼 경우, 스위치는 호스트 트래킹 정보를 가진 Source 리스트와 호스트가 보낸 Report 메시지의 Source 주소를 비교합니다. 비교한 내용이 일치하면 해당 Source 엔트리를 리스트에서 삭제하고 그 호스트에게 전송하던 멀티캐스트 트래픽을 차단합니다. 다시 말해서 Immediate Blocking이 활성화 되어 있다면, Group-source-specific Query 메시지를 보내는 절차를 생략합니다.

IGMP 버전 3 Immediate Blocking 기능을 활성화 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp snooping immediate-block	Global	시스템 전체에 Immediate Blocking 기능을 활성화 합니다.
ip igmp snooping vlan <i>vlan-id</i> immediate-block		특정 VLAN에 Immediate Blocking 기능을 활성화 합니다.



주의

Immediate Blocking 기능은 반드시 호스트 트래킹 기능과 같이 활성화되어야 합니다. (**1.1.1(6) 호스트 트래킹 기능 설정 참고**)

설정한 IGMP 버전 3 Immediate Blocking 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping immediate-block	Global	시스템 전체에 Immediate Blocking 기능을 해제합니다.
no ip igmp snooping vlan <i>vlan-id</i> immediate-block		특정 VLAN에 Immediate Blocking 기능을 해제합니다.

9.2.5. IGMP Snooping 정보 확인

최근 IGMP Snooping에 대한 설정을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip igmp snooping [vlan <i>vlan-id</i>]	Enable/Global/ Bridge	IGMP Snooping 관련 정보와 설정값을 확인합니다.

IGMP Snooping 테이블의 정보를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip igmp snooping groups [ip-address mac-based]	Enable/ Global/ Bridge	시스템 전체의 IGMP Snooping 테이블 정보를 확인합니다.
show ip igmp snooping groups port {port-number cpu} [mac-based]		특정 포트의 IGMP Snooping 테이블 정보를 확인합니다.
show ip igmp snooping groups vlan <i>vlan-id</i> [mac-based]		특정 VLAN의 IGMP Snooping 테이블 정보를 확인합니다.

IGMP Snooping 통계 정보를 확인하려면 다음 명령어를 사용하십시오.

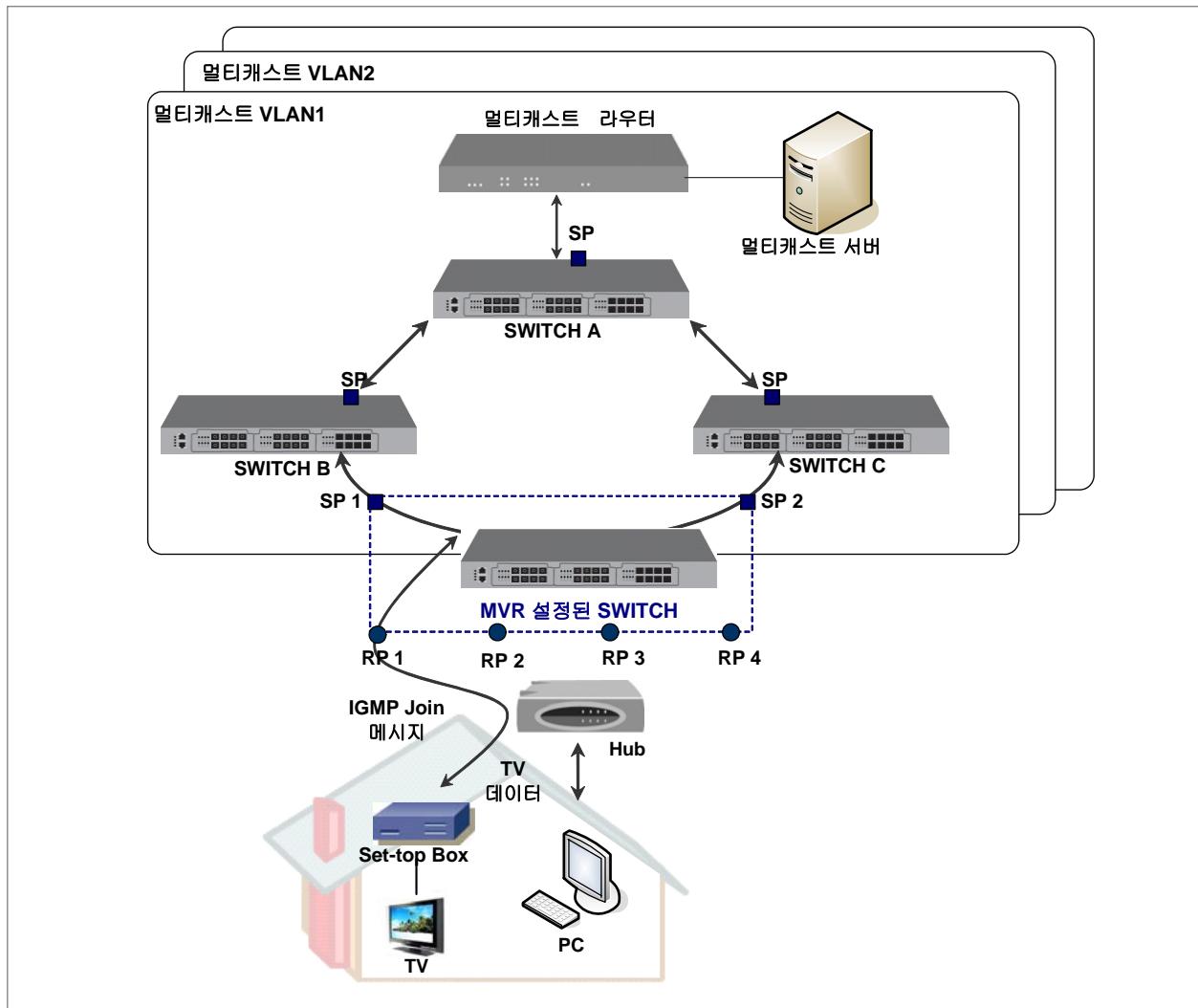
명령어	모 드	기 능
show ip igmp snooping stats port {port-number cpu}	Enable/ Global/ Bridge	IGMP Snooping 통계 정보를 확인합니다.

IGMP Snooping 통계 정보를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip igmp snooping stats port {port-number cpu}	Enable/ Global/ Bridge	IGMP Snooping 통계 정보를 초기화합니다.

9.2.6. MVR (Multicast VLAN Registration)

MVR(Multicast VLAN Registration)은 서로 다른 VLAN에서 동일한 멀티캐스트 패킷을 수신하는 가입자들을 멀티캐스트 VLAN으로 설정함으로써 L3가 아닌 L2로 멀티캐스트 통신이 가능하도록 하는 기능입니다. 따라서 하드웨어 자원을 절약할 수 있는 것은 물론 끊김이 없는 연속적인 멀티캐스트 스트림의 전송이 가능합니다. 한편, 멀티캐스트 VLAN은 하나의 독립된 VLAN으로서 다른 가입자 VLAN과 차단되기 때문에 멀티캐스트 통신의 대역폭과 보안(Security)이 보장됩니다.



【 그림 9-8 】 MVR 동작

위의 그림은 멀티캐스트 서버와 멀티캐스트 라우터, 그리고 SWITCH 등 모든 장비가 같은 한 VLAN에 속하고 MVR 설정이 되어 있는 경우입니다. MVR 설정이 되어 있는 스위치는 가입자 포트에 연결된 PC나 Set-top box로부터 받은 IGMP Join 메시지를 Source 포트(SP: Source Port)를 통해 멀티캐스트 라우터로 전송합니다. 그리고, 멀티캐스트 라우터에서 전송된 멀티캐스트 트래픽은 Receiver 포트(RP: Receiver Port)를 통해 요청했던 가입자에게 전송합니다.



주의

V5812G에 MVR을 설정할 때 Receiver 포트는 반드시 MVR VLAN과 가입자 VLAN에 모두 untagged VLAN으로 설정되어 있어야 합니다.



주의

V5812G에 MVR을 활성화하기 위해서는 IGMP Snooping 기능이 활성화되어 있어야 합니다.

이 장에서는 MVR 설정과 관련하여 다음과 같은 내용을 설명합니다.

- MVR 활성화
- MVR 그룹 설정
- MVR Helper 주소 설정
- Source/Receiver 포트 설정
- MVR 설정 확인

(1) MVR 활성화

MVR를 활성화 하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
mvr	Global	MVR 기능을 활성화 합니다.

한편, MVR 기능을 해제하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no mvr	Global	MVR 기능을 해제합니다.



참 고

V5812G에서 MVR 기능은 기본적으로 해제되어 있습니다.

(2) MVR 그룹 설정

MVR 기능을 설정하기 위해서는 MVR 그룹과 주소를 지정해야 합니다. 사용자가 여러 개의 MVR 그룹을 지정 할 경우, IGMP 패킷은 지정된 MVR 그룹 주소에 따라 RP(Receiver Port)로부터 해당 MVR 그룹에 속한 SP(Source Port)로 전송됩니다.

MVR 그룹과 그룹 주소를 지정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
mvr vlan <i>vlan-id</i> group <i>group-address</i>	Global	MVR 그룹을 지정하고 대응하는 MVR 그룹 주소를 등록합니다.

설정한 MVR 그룹과 그룹 주소를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no mvr vlan <i>vlan-id</i> group <i>group-address</i>	Global	설정된 MVR 그룹과 그룹 주소를 삭제합니다.



참 고

하나의 MVR 그룹 주소는 두개 이상의 MVR 그룹에 포함될 수 없습니다.

(3) Source/Receiver 포트 설정

MVR 포트를 설정하면 설정된 포트가 해당 멤버 그룹에 추가되거나 삭제됩니다. 여기서 “**receiver**” 옵션은 Receiver 포트를 설정할 때 사용합니다. Receiver 포트는 가입자와 직접적으로 연결되어 있는 포트로 멀티캐스트 트래픽을 받을 수만 있습니다. 이 포트는 반드시 가입자 VLAN과 멀티캐스트 VLAN에 동시에 Untagged로 포함되어야 합니다.

“**source**” 옵션은 Source 포트를 설정할 때 사용합니다. Source 포트는 업링크 포트로 멀티캐스트 라우터나 Source와 멀티캐스트 트래픽을 주고 받을 수 있습니다. 가입자는 Source 포트에 직접적으로 연결되지 않으며, 모든 Source 포트는 Tagged 멀티캐스트 VLAN에만 속합니다.

특정 포트를 MVR의 Source 포트 또는 Receiver 포트로 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
mvr port port-number type {receiver source}	Global	특정 포트를 Source 포트 또는 Receiver 포트로 설정합니다.

Source 포트나 Receiver 포트로 지정되어 있는 설정을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no mvr port port-number	Global	Source 및 Receiver 포트 설정을 삭제합니다.

(4) MVR Helper 주소 설정

멀티캐스트 서버가 사용자의 장비와 다른 네트워크에 속해 있을 경우에는 멀티캐스트 라우터는 각 MVR 그룹에 대해 L3 멀티캐스트 라우팅으로 동작하게 됩니다. 이러한 경우, 가입자의 IGMP 패킷이 멀티캐스트 라우터에게 전달될 때 IGMP 패킷의 Source 주소가 MVR 그룹의 네트워크와 일치하지 않을 수 있습니다. 일치하지 않을 경우에 라우터는 해당 IGMP 패킷을 차단합니다. 이러한 문제를 해결하기 위해 사용자는 IGMP 패킷의 Source 주소를 특정한 MVR helper 주소로 대체할 수 있습니다. 이 Helper 주소는 반드시 MVR 그룹 네트워크에 포함되어야 합니다.

IGMP 패킷 Source 주소를 대체할 MVR helper 주소를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
mvr vlan vlan-id helper ip-address	Global	IGMP 패킷 Source 주소를 대체할 helper 주소를 설정합니다.

설정했던 MVR helper 주소를 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no mvr vlan vlan-id helper	Global	설정했던 MVR helper 주소를 삭제합니다.

(5) MVR 설정 확인

MVR 관련 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show mvr	Enable/	
show mvr vlan <i>vlan-id</i>	Global/	MVR 관련 설정 내용을 확인합니다.
show mvr port	Bridge	

9.2.7. IGMP 필터링 기능 설정

IGMP 필터링 기능은 스위치 각 포트의 실제 사용자가 멀티캐스트 통신 서비스를 보다 효율적으로 제공받을 수 있도록 합니다. 사용자는 IGMP Profile을 만들어서 한 개 혹은 여러 개의 IGMP 그룹을 포함시키고 해당 그룹만 접속을 허용하거나 차단할 수 있습니다. 다시 말해서 IGMP 필터링은 비가입자들을 제외시킴으로서 멀티캐스트 인증을 제공합니다. 이 기능은 포트 당 설정이 가능하며 멀티캐스트 그룹의 수를 제한할 수 있습니다. IGMP 필터링 기능은 IGMP 버전 2를 지원합니다.



참 고

IGMP 필터링은 호스트로부터 전송된 Report 메시지만을 관리할 수 있으며 다른 네트워크를 통해 유입되는 멀티캐스트 스트림은 제한할 수 없습니다.

(1) IGMP 필터링 설정

IGMP Profile 생성

IGMP 필터링 기능을 사용하려면, Global 설정 모드에서 다음과 같은 명령어를 사용하여 IGMP Profile을 생성해서 IGMP Profile 모드로 들어가서 세부적인 설정을 해야합니다.

IGMP Profile을 생성하거나 수정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp profile <i>profile-number</i>	Global	IGMP Profile을 생성 또는 수정합니다.
no ip igmp profile <i>profile-number</i>		해당 IGMP Profile을 삭제합니다.



참 고

“profile-number”는 IGMP Profile의 고유한 이름인 동시에 최대 개수로 1에서 2,147,483,647까지 범위 안에서 설정 할 수 있습니다.

Global 설정 모드에서 “**ip igmp profile profile-number**”를 입력하면 시스템 프롬프트가 SWITCH(config)#에서 SWITCH(config-igmp-profile[profile-number])#로 바뀌면서 IGMP Profile이 생성 됩니다.

```
SWITCH(config)# ip igmp profile 1
SWITCH(config-igmp-profile[1])#
```

IGMP 그룹 범위

IGMP 필터링 기능을 적용하고자 하는 IGMP 그룹 범위를 지정하려면 IGMP Profile 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
range low- multicast-address [high-multicast-address]	IGMP Profile	IGMP 그룹 범위를 지정합니다.
no range low- multicast-address [high- multicast-address]		설정된 IGMP 그룹 범위를 해제합니다.



참 고

“low-multicast-address”와 “high-multicast-address” 를 동시에 지정하여 IGMP 그룹 범위를 설정할 수 있습니다. 또한 특정 범위를 정하지 않고 하나의 멀티캐스트 그룹 주소만을 지정할 수 있습니다.

IGMP 필터링 정책 적용

해당 멀티캐스트 주소 범위에 접속하기 위한 IGMP 필터링 정책을 설정할 수 있습니다. IGMP 필터링 정책을 설정하려면 해당 IGMP Profile 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
{permit deny}	IGMP Profile	IGMP Profile에 설정된 IGMP 그룹의 필터링 정책을 설정합니다.

IGMP 필터링 활성화

IGMP 필터링 기능을 포트에 활성화하려면 설정된 IGMP Profile을 특정 포트에 적용시켜줘야 합니다. IGMP Profile을 포트에 적용하여 IGMP 필터링 기능을 활성화 하려면 다음과 같은 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp filter port port-number profile profile-number	Global	IGMP Profile을 특정 포트에 적용합니다.
no ip igmp filter port port-number		해당 포트에 적용된 IGMP Profile을 해제합니다.



주의

복수의 IGMP Profile은 하나의 포트에 적용할 수 없으며, IGMP Snooping 기능이 활성화 되어 있는 상태에서 IGMP 필터링 기능을 활성화 할 수 있습니다.



주의

이미 생성된 IGMP Profile을 삭제하려면, 해당 프로파일이 적용된 모든 포트를 해제한 후 가능합니다.

V5812G는 또한 DHCP Snooping 바인딩 테이블을 참고하여, 특정 IGMP 패킷을 필터링 할 수 있습니다. 다시 말하면, DHCP Snooping 바인딩 테이블에 의해 검증된 호스트의 source IP 주소와 MAC 주소의 IGMP 패킷만을 허용할 수 있습니다.

DHCP Snooping 바인딩 테이블의 엔트리를 통해 허가된 호스트의 IGMP 패킷만을 허용하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp filter port port-number permit dhcp-snoop-binding	Global	DHCP Snooping 바인딩 테이블을 참고하여 해당 엔트리만을 IGMP Snooping 테이블에 추가합니다.
no ip igmp filter port port-number permit dhcp-snoop-binding		DHCP Snooping 바인딩 테이블을 참고하는 설정을 해제합니다.

(2) 패킷 종류에 따른 IGMP 필터링 설정

IGMP 패킷의 유형에 따라 포트 별로 IGMP 필터링 기능을 설정 할 수 있습니다. 특정 멀티캐스트 패킷을 차단하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp filter port port-number packet-type { leave query reportv1 reportv2 reportv3}	Global	해당 포트로 들어오는 특정 IGMP 패킷을 차단합니다.
ip igmp filter port port-number packet-type all		해당 포트로 들어오는 모든 IGMP 패킷을 차단합니다.



참 고

IGMP 필터링은 기본적으로 IGMP 버전 2 만 지원하지만, 패킷 유형별로 IGMP 필터링을 설정할 때는 IGMP 버전 3 Report 메시지까지 차단할 수 있습니다.

IGMP 패킷의 유형에 따라 포트 별로 IGMP 필터링 기능을 설정했던 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp filter port port-number packet-type { all leave query reportv1 reportv2 reportv3}	Global	특정 IGMP 패킷에 대한 필터링 설정을 해제합니다.

(3) IGMP 그룹의 최대값 설정

사용자는 포트에 연결되어 있는 호스트가 Join 할 수 있는 IGMP 그룹의 최대 개수를 설정할 수 있습니다. 모든 포트 또는 특정 포트당 접속할 수 있는 IGMP 그룹의 최대 개수를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp max-groups port sum count <1-2147483647>	Global	모든 포트에 Join할 수 있는 최대 IGMP 그룹의 수를 설정합니다.
ip igmp max-groups port port-number count <1-2147483647>		특정 포트에 Join할 수 있는 최대 IGMP 그룹의 수를 설정합니다.
no ip igmp max-groups port {sum port-number}		설정된 최대 IGMP 그룹의 수를 삭제합니다.

시스템에 접속할 수 있는 IGMP 그룹의 최대 개수를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp max-groups system count <1-2147483647>	Global	시스템에 Join할 수 있는 최대 IGMP 그룹의 수를 설정합니다.
no ip igmp max-groups system		시스템에 설정된 최대 IGMP 그룹의 수를 삭제합니다.

(4) IGMP 필터링 확인

IGMP 필터링 관련 설정 내용을 확인하려면 다음과 같은 명령어를 사용하십시오.

명령어	모 드	기 능
show ip igmp filter [port port-number]	Global	IGMP 필터링 관련 설정 내용을 확인합니다.

IGMP Profile을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip igmp profile [profile-number]	Enable / Global / Bridge	설정된 IGMP Profile을 확인합니다.

9.2.8. IGMP Proxy 설정

IGMP Proxy 기능은 L3 스위치가 하부 망에 연결된 IGMP 호스트들을 대신해서 멀티캐스트 라우터에게 IGMP 메시지를 보내고 받을 수 있게 하는 기능입니다. 즉, L3 스위치가 멀티캐스트 호스트의 역할을 프록시하는 것입니다. V5812G는 IGMPv2를 지원합니다. IGMP Proxy 기능은 실제로 간단한 트리 토플로지 상에서만 사용될 수 있습니다. 즉, 하나의 업스트림 인터페이스와 여러 개의 다운스트림 인터페이스로 이루어진 네트워크 환경에서만 사용 가능하며, 본 기능으로 멀티캐스트 라우팅 프로토콜 없이도 멀티캐스트 서비스가 가능합니다.

IGMP Proxy 스위치는 멀티캐스트 라우팅 프로토콜을 사용하지 않음으로써, 복잡한 작업의 수행을 줄일 수 있으며 쉽게 배치할 수 있습니다. 기본적으로 IGMP 멤버십 정보만을 사용해서 멀티캐스트 패킷을 포워딩하며, IGMPv2를 지원합니다. 본 기능을 사용하려면 스위치 상에서 업스트림 인터페이스와 다운스트림 인터페이스를 수동으로 지정해야 합니다.

IGMP Proxy는 동작에 있어 다음과 같은 제약 사항이 있으므로, 사용자는 IGMP Proxy 명령어나 파라미터를 설정할 때 이를 주의해야 합니다.



주의

- 본 기능은 간단한 트리 토플로지에서만 사용될 수 있습니다.
- IGMP Proxy 기능을 실행시키기 위해서는 사용자가 직접 업스트림 인터페이스와 다운스트림 인터페이스를 설정해야 합니다.
- PIM이 설정된 인터페이스에 IGMP Proxy를 위한 업스트림/다운스트림 인터페이스를 설정할 수 없습니다. 반대로 업스트림/다운스트림 인터페이스에도 PIM을 설정할 수 없습니다.
- IGMPv3를 지원하지 않습니다. 인터페이스의 버전이 IGMPv3일 때, 업스트림 또는 다운스트림 인터페이스로 설정할 수 없습니다. 반대로, 업스트림 또는 다운스트림 인터페이스로 설정되면 IGMPv3를 설정할 수 없습니다.
- IGMPv3를 지원하지 않기 때문에 SSM-map 기능의 사용이 불가능합니다. SSM-map이 설정되어 있을 때, 업스트림 또는 다운스트림 인터페이스로 설정할 수 없습니다. 반대로 업스트림 또는 다운스트림 인터페이스가 설정되어 있을 때 SSM-map 기능을 활성화할 수 없습니다.
- IGMP Proxy는 L3기능이므로 해당되는 L3 인터페이스가 존재해야 합니다. 그리고 설정 전에 해당 인터페이스를 활성화하기 위해서 no shutdown 명령이 먼저 수행되어야 합니다.
- 만약 ip igmp proxy-service sip first-reporter 명령어가 설정된 경우, 업스트림 인터페이스가 report 메시지를 보낼 때 해당 그룹에 처음으로 조인한 호스트의 Source IP로 보내집니다. first-reporter는 그룹에 처음으로 조인한 호스트의 IP로 기록되며, 이 후 그 호스트가 leave되더라도 다른 호스트로 갱신되지 않습니다. 즉, 그룹 멤버십 레코드가 삭제되기 전까지는 처음 조인된 호스트의 IP가 남습니다.

(1) 다운스트림 인터페이스 설정

IGMP Proxy 기능을 실행하기 위해서 다운스트림 인터페이스를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp mroute-proxy interface-name	Interface	mroute proxy 다운스트림 인터페이스를 지정합니다.
no ip igmp mroute-proxy interface-name		mroute proxy 다운스트림 인터페이스를 해제합니다.

(2) 업스트림 인터페이스 설정

IGMP Proxy 기능을 실행하기 위해서 업스트림 인터페이스를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp proxy-service interface-name	Interface	mroute-service 업스트림 인터페이스를 지정합니다.
no ip igmp proxy-service		mroute-service 업스트림 인터페이스를 해제합니다.

(3) 업스트림 인터페이스 모드 설정

V5812G는 하나의 다운스트림 인터페이스를 여러 개의 업스트림 인터페이스와 연결이 가능하며, IGMP proxy 서비스를 담당하던 업스트림 인터페이스에 문제가 발생하더라도 다른 업스트림 인터페이스에 연결되어 서비스의 안정성을 보장합니다.

복수의 업스트림 인터페이스가 하나의 다운스트림 인터페이스가 연결되어 있을 경우, 우선순위 모드와 로드 밸런스 모드로 설정할 수 있습니다. 각각의 업스트림 인터페이스는 Credit과 Priority를 갖습니다. Credit과 Priority는 그 값이 클수록 우선 순위가 높아지는데, 여러 개의 업스트림 인터페이스가 존재할 경우 이 값을 이용하여 우선 순위를 결정하게 됩니다. 즉, 업스트림 인터페이스의 우선 순위 결정방법은 **Credit > Priority > VID(Priority가 동일한 경우)**입니다.

우선순위 모드는 각 업스트림 인터페이스 별로 우선순위를 설정하여 연결된 인터페이스가 다운되면 그 다음으로 높은 우선순위의 업스트림 인터페이스로 Join 됩니다. 장비 시스템에 기본적으로 활성화되어 있습니다. 한편, 로드 밸런스 모드는 연결된 업스트림 인터페이스가 다운될 경우, 다른 나머지 인터페이스들로 분산되어 IGMP Proxy 서비스를 제공합니다.

업스트림 인터페이스에 Priority를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp proxy-service priority <0-255>	Interface	업스트림 인터페이스에 Priority를 설정합니다.
no ip igmp proxy-service priority		해당 인터페이스에 설정한 Priority를 삭제합니다.



참 고

Priority의 기본값은 0이며, Priority값이 동일할 경우에는 낮은 VLAN ID를 가진 인터페이스가 우선순위가 높습니다.

로드 밸런스 모드를 활성화하여 다운된 인터페이스를 제외한 업스트림 인터페이스들로 분산해서 IGMP Proxy 서비스를 제공하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp proxy-service multipath grpip	Global	로드 밸런스 모드를 활성화합니다.
no ip igmp proxy-service multipath grpip		로드 밸런스 모드를 해제하고, 우선순위 모드로 활성화합니다.

(4) IGMP Flap Discredit 설정

IGMP Proxy에서 복수의 업스트림 인터페이스가 존재할 경우 우선 순위에 따라 멀티캐스트 패킷의 전송 경로가 결정됩니다. 이때 업스트림 인터페이스의 우선 순위를 결정하는데 가장 첫번째로 고려되는 것이 Credit입니다. V5812G는 보다 안정적인 멀티캐스트 서비스를 제공하기 위해 네트워크 연결이 불안정한 인터페이스에 대해 벌점을 부과하는 IGMP Flap Discredit 기능을 지원합니다.

인터페이스 Flap이란 어떠한 이유로 네트워크 연결이 불안정하여 해당 인터페이스가 ON/OFF를 반복하는 현상을 말합니다. IGMP Flap Discredit는 Flap이 발생한 인터페이스에 대해 일정한 값의 Credit을 차감하여 해당 인터페이스가 멀티캐스트 경로 설정에서 배제되도록 합니다. 즉, IGMP Proxy의 업스트림 인터페이스 모드가 우선 순위 모드일 경우 Credit이 가장 높은 업링크로 경로가 결정되며, 로드 밸런스 모드일 경우에는 가장 높은 Credit을 갖는 업링크를 기준으로 분산되어 멀티캐스트 패킷이 전송됩니다.

IGMP Flap Discredit 기능을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp if flap discredit	Global	IGMP Flap Discredit 기능을 활성화합니다.
no igmp if flap discredit		IGMP Flap Discredit 기능을 비활성화합니다.



참 고

V5812G는 기본적으로 PIM VIF Flap Discredit 기능이 활성화되어 있습니다.

인터페이스에서 Flap이 발생할 때마다 Credit 값을 감소시키는 Discredit을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp if flap discredit-unit <1-50>	Global	인터페이스에서 Flap이 발생할 때마다 Credit 값을 감소시키는 Discredit을 설정합니다.
no ip igmp if flap discredit-unit		설정한 Discredit을 해제하고 기본값으로 설정합니다.



참 고

Discredit의 기본값은 5입니다.

한편, 모든 IGMP 업스트림 인터페이스에 대해 일정한 시간마다 Credit을 검사하여 기본값(100)보다 낮을 경우 Credit 값을 회복시킵니다. 단, 인터페이스의 Credit 값이 0일 경우에는 그 값이 회복되지 않습니다. 이때 회복되는 Credit 값과 Credit 값의 회복 주기는 사용자가 설정할 수 있습니다.

감소한 Credit 값을 회복시킬 시간 간격을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp if flap recover-interval <0-3600>	Global	감소한 Credit 값을 회복시킬 시간 간격을 설정합니다.
no ip igmp if flap recover-interval		설정한 Credit 회복 주기를 해제하고 기본값으로 설정합니다.



참 고

Credit 회복 시간 간격은 <0-3600> 범위에서 설정할 수 있으며, 기본값은 10초(sec)입니다.



참 고

특정 인터페이스의 Credit이 0인 경우에는 Credit 값이 회복되지 않습니다.

일정 시간이 지난 후 회복될 Credit 값을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp if flap recover-unit <1-50>	Global	일정 시간이 지난 후 회복될 Credit 값을 설정합니다.
no ip igmp if flap recover-unit		설정한 Credit 회복값을 해제하고 기본값으로 설정합니다.



참 고

Credit 회복값의 기본값은 5입니다.

인터페이스의 Credit을 기본값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip igmp if flap discredit [interface-nam]	Enable/Global	인터페이스의 Credit을 기본값 100으로 되돌립니다.



참 고

인터페이스의 Credit 정보는 **show ip igmp interface** 명령어로 확인할 수 있습니다.

(5) IGMP 패킷의 소스 IP 확인 해제

멀티캐스트 라우팅 프로토콜을 사용하는 경우, 대개는 IGMP 패킷과 멀티캐스트 트래픽을 처리할 때에 Reverse Path를 체크합니다. 즉, 패킷이 들어오는 인터페이스의 네트워크에 속하는 소스 IP를 가졌는지를 확인하는 절차를 거치게 됩니다. 하지만 이 명령어를 사용하여 IGMP 패킷의 소스 IP가 들어오는 인터페이스의 네트워크에 해당하는지에 대한 검증 절차를 해제할 수 있습니다.

IGMP Proxy 기능을 사용하는 스위치는 기본적으로 멀티캐스트 트래픽에 대한 Reverse Path를 확인하지 않습니다. 따라서 본 기능과 함께 사용할 경우 Reverse Path와 관계없이 멀티캐스트 서비스를 제공할 수 있습니다.

IGMP 패킷의 소스 IP 확인을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp verify-sip	Global	IGMP 패킷의 소스 IP가 들어온 인터페이스의 네트워크에 해당하는지 확인하지 않습니다.
ip igmp verify-sip		IGMP 패킷의 소스 IP가 들어온 인터페이스의 네트워크에 해당하는지 확인합니다. (기본 설정)

(6) IGMP Report/Leave 메시지의 소스 IP 설정

IGMP Proxy 환경에서 스위치는 호스트들을 대신하여 업스트림 인터페이스를 통해 라우터와 IGMP 통신합니다. IGMP Proxy의 업스트림 인터페이스에서 IGMP Membership Report와 Leave Group 메시지를 보낼 때, 소스 IP는 기본적으로 업스트림 인터페이스의 IP 주소를 사용합니다. 하지만 이때 소스 IP를 사용자가 임의로 설정한 IP 주소, 처음으로 조인한 호스트의 IP 주소로 변경해서 보내도록 사용자가 선택할 수 있습니다.

proxy-service 업스트림 인터페이스에 의해 전송되는 IGMP Membership Report와 Leave Group 메시지의 소스 IP 주소를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp proxy-service sip {ip-address first-reporter}	Interface	proxy-service 인터페이스가 보내는 IGMP 메시지의 소스 IP를 설정합니다. (기본설정: proxy-service 인터페이스의 IP)
no ip igmp proxy-service sip		소스 IP 설정을 삭제합니다.

(7) 실제 소스 IP로 Query 전송

IGMP Proxy 환경에서 스위치는 지정된 다운스트림 인터페이스를 통하여 연결된 호스트들에게 IGMP Query를 보냅니다. 이 때 Query의 소스 IP는 다운스트림 인터페이스의 IP 주소가 사용됩니다. 하지만 본 기능으로 업스트림 인터페이스에서 받은 IGMP Query의 실제 소스 IP로 IGMP Query를 보내도록 할 수 있습니다.

mroute-proxy 다운스트림 인터페이스가 보내는 IGMP Query의 소스 IP를 Query의 실제 소스 IP로 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp mroute-proxy querier address proxy-service	Interface	mroute-proxy 다운스트림 인터페이스가 보내는 IGMP Query의 소스 IP를 업스트림 인터페이스가 받은 Query의 실제 소스 IP로 변경합니다.
no ip igmp mroute-proxy querier address proxy-service		Query의 소스 IP 설정을 삭제합니다.

(8) IGMP Proxy 설정 확인

IGMP proxy-service 설정을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip igmp-proxy groups [detail]		업스트림 IGMP Proxy-service 관련 설정 정보를 확인합니다.
show ip igmp-proxy groups group-address [detail]	Enable/ Global/ Bridge	특정 멀티캐스트 그룹 주소의 IGMP Proxy-service 관련 설정 정보를 확인합니다.
show ip igmp-proxy groups interface-name [detail]		특정 인터페이스에 설정된 IGMP Proxy-service 관련 설정 정보를 확인합니다.
show ip igmp-proxy groups [interface-name] summary		

9.2.9. IGMP State 제한 설정

IGMP State 최대 개수는 설정하는 기능은 IGMP 패킷에 의해 생기는 DoS (denial of service) 공격으로부터 장비를 보호할 수 있습니다. IGMP State란 멀티캐스트 라우터에 Join하는 IGMP. IGMP 버전 3 lite, URD(URL Rendezvous Directory) 맴버쉽 Report 메시지들을 통틀어 지칭하는 단어입니다. 설정 값을 초과하는 맴버쉽 Report들은 IGMP 캐시(Cache)에 들어올 수 없으며 Forwarding되지도 않습니다. 이 기능은 시스템 전체 또는 특정 인터페이스로 설정이 가능하며, 또한 Except 옵션을 통해 특정 access list를 제외시킬 수 있습니다.

라우터에 Join하는 IGMP State의 최대 개수를 시스템 전체에 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp limit <1-2097152> [except {<1 - 99>} <1300 - 1999> access-list-name}]	Global	라우터에 Join할 수 있는 최대 IGMP State의 수를 시스템 전체에 설정합니다.
no ip igmp limit		설정된 최대 IGMP State의 수를 삭제합니다.

라우터에 Join하는 IGMP State의 최대 개수를 특정 인터페이스에 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp limit <1-2097152> [except {<1 - 99>} <1300 - 1999> access-list-name}]	Interface	라우터에 Join할 수 있는 최대 IGMP State의 수를 특정 인터페이스에 설정합니다.
no ip igmp limit		설정된 최대 IGMP State의 수를 삭제합니다.

9.2.10. 멀티캐스트 Source Trust 포트 설정

멀티캐스트 Source Trust 포트를 설정하는 기능을 통해 멀티캐스트 서비스 제공자와 일반 가입자를 구분하여, 특정 포트로만 멀티캐스트 서비스를 제공하여 시스템 자원을 효율적으로 사용할 수 있습니다.

멀티캐스트 Source Trust 포트로 설정되지 않는 포트는 멀티캐스트 트래픽을 Drop 하며, 만약 특정 포트를 Trust 포트로 지정하지 않았을 경우에는 장비의 모든 포트가 멀티캐스트 Source Trust 포트로 설정되어 멀티캐스트 서비스를 제공합니다.

특정 포트를 멀티캐스트 Source Trust 포트로 지정하거나 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip multicast-source trust port port-number	Global	특정 포트를 멀티캐스트 Source Trust 포트로 지정합니다.
no ip multicast-source trust port port-number		지정된 특정 멀티캐스트 Source Trust 포트를 삭제합니다.

9.3 멀티캐스트 라우팅 설정

멀티캐스트 라우터는 호스트가 특정 멀티캐스트 그룹에 Join 하였을 때, 해당 호스트가 속한 그룹에 멀티캐스트 패킷을 전달합니다. 그런데, 동일 네트워크 상에서 멀티캐스트 패킷을 전달할 멀티캐스트 그룹이 여러 개 존재할 경우에는 효율적으로 패킷을 전송하기 위한 라우팅 프로토콜이 필요하게 됩니다.

멀티캐스트 라우터는 멀티캐스트 트래픽 전송 경로를 테이블로 작성합니다. 이때 작성하는 테이블을 Forwarding 테이블이라 하는데, 이 테이블에는 멀티캐스트 Source, 그룹, 인터페이스 및 멀티캐스트 패킷의 전송 방법에 대한 정보가 포함됩니다.

한편, 멀티캐스트 라우터는 이러한 Forwarding 테이블을 바탕으로 Distribution tree를 구성합니다. Distribution tree란 하나의 멀티캐스트 패킷이 목적지로 향하는 동안 라우터를 지날 때마다 복사되어 여러 방향으로 뻗어나가는 형태로 경로가 형성되는 것을 말합니다. 멀티캐스트 Distribution tree는 멀티캐스트 그룹 멤버가 동적으로 그룹에 참가 및 탈퇴하기 때문에 항상 동적으로 형성됩니다.

멀티캐스트 Distribution tree는 Source 분배 트리와 공유 트리로 나뉩니다. Source 분배 트리는 멀티캐스트 Source를 중심으로 목적지까지 최적 경로를 연결하는 토플로지가 형성됩니다. 즉, Source에서 최단 경로를 이용해 멀티캐스트 패킷이 전송되므로 트래픽 전송 지연을 최소화하게 됩니다. 그러나, 라우터는 모든 멀티캐스트 Source에 대한 경로 정보를 보유하고 있어야 하기 때문에, 멀티캐스트 Source와 그룹이 많거나 멀티캐스트 그룹 멤버가 산재되어 있는 경우에는 과부하에 걸릴 수 있습니다. Source 분배 트리는 (S, G) 엔트리를 사용합니다. 여기에서 S 는 특정 멀티캐스트 Source, G 는 특정 멀티캐스트 그룹을 뜻합니다.

공유 트리는 RP(Rendezvous Point)를 중심으로 경로가 형성되며 $(*, G)$ 엔트리를 사용합니다. 여기에서 $*$ 는 모든 멀티캐스트 Source, G 는 특정 멀티캐스트 그룹을 뜻합니다. 한편, RP는 트리 경로의 중심에 위치하는 라우터입니다. 기본적으로 Source에서 전송한 멀티캐스트 패킷은 RP를 거쳐 수신자에게 전달됩니다. 공유 트리에서 RP를 제외한 라우터는 자신이 속해 있는 공유 트리 정보만 알고 있으면 되므로, Source 분배 트리에 비해 상대적으로 부하가 적어집니다. 하지만, RP의 위치에 따라 Source와 수신자를 연결하는 경로가 최단 경로가 아닐 가능성이 있습니다.

다음은 멀티캐스트 라우팅 프로토콜에서 사용되는 RPF에 대한 설명입니다.

◆ Reverse Path Forwarding(RPF)

일반적으로 라우터는 목적지 검색 과정을 거쳐 패킷을 전송합니다. 즉, 패킷을 수신한 라우터는 라우팅 테이블을 참조하여 패킷의 목적지를 찾은 후 목적지와 연결된 인터페이스로 해당 패킷을 전송합니다. 한편, 목적지를 알 수 없는 패킷을 수신한 경우에는 해당 패킷을 Default gateway로 전송합니다.

하지만 멀티캐스트 패킷을 수신한 라우터는 가장 먼저 패킷의 Source 정보를 살펴봅니다. 라우팅 테이블 정보를 참조하여 해당 패킷의 Source와 패킷을 보낸 Source가 직접적으로 연결된, 즉 최단 경로 상에 위치한 인터페이스로부터 수신되었는지 확인합니다.

이처럼 수신한 패킷의 Source address를 보고 적절한 인터페이스를 통해서 전달되었는지 확인하는 방법을 RPF 검사(Reverse Path Forwarding Check)라고 합니다. RPF 검사로 최단 경로를 통해 수신된 것이 확인되면 해당 패킷은 다음 경로로 전송되고, 최단 경로를 통해 수신된 것이 아닌 패킷은 폐기됩니다.

멀티캐스트 라우팅에서 Source에서 멀어지도록 패킷을 전송하는데, 이는 라우팅 루프를 방지하기 위한 것입니다. 한편, RPF 검사 과정에서 생성된 최단 거리 경로를 SPT(Shortest Path Tree)라 합니다.

이 장에서는 멀티캐스트 라우팅 기본 설정과 관련하여 다음과 같은 내용을 설명합니다.

- 멀티캐스트 라우팅
- PIM
- RP 설정
- SSM (Source Specific Multicast) 설정

9.3.1. 멀티캐스트 라우팅

(1) 멀티캐스트 라우팅 활성화

V5812G에 멀티캐스트 라우팅 기능을 설정하여 L3 네트워크 환경에서도 멀티캐스트 트래픽이 전송되도록 하려면, 먼저 멀티캐스트 라우팅 기능을 활성화해야 합니다.

멀티캐스트 라우팅 기능을 활성화하려면, Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip multicast-routing	Global	멀티캐스트 라우팅 기능을 활성화합니다.



주의

V5812G에는 기본적으로 멀티캐스트 라우팅 기능이 비활성화 되어 있습니다. 멀티캐스트 라우팅 기능을 설정하려면, 먼저 멀티캐스트 라우팅 기능을 활성화하십시오.

멀티캐스트 라우팅 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip multicast-routing	Global	멀티캐스트 라우팅 기능을 해제합니다.

(2) 멀티캐스트 TTL 임계값 설정

V5812G는 멀티캐스트 패킷의 TTL 임계값을 설정하여 멀티캐스트 패킷의 전송범위를 제한할 수 있습니다. V5812G가 수신한 멀티캐스트 패킷의 TTL이 사용자 장비의 인터페이스에서 지정한 TTL 임계값보다 크면 패킷을 내보내고, 작으면 패킷을 폐기합니다. 이러한 기능을 이용하여 사용자는 멀티캐스트 패킷을 제어할 수 있습니다.

예를 들어, 사용자가 전체 네트워크에서 특정 부분만 멀티캐스트 전송망으로 사용하고자 할 때, 멀티캐스트 전송망의 경계가 되는 인터페이스의 TTL 임계값을 멀티캐스트 패킷의 TTL값보다 높게 설정하면 멀티캐스트 패킷은 해당 인터페이스에서 폐기되어 외부로 전송되지 않습니다. 따라서, 특정한 범위 내에서만 멀티캐스트 패킷이 전달되도록 제어할 수 있습니다.

멀티캐스트 패킷의 전송범위를 제한하기 위한 TTL 임계값을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip multicast ttl-threshold <0-255>	Interface	멀티캐스트 TTL 임계값을 설정합니다.
no ip multicast ttl-threshold		설정한 멀티캐스트 TTL 임계값을 해제합니다.



참 고

멀티캐스트 TTL 임계값은 <0-255> 범위에서 설정할 수 있으며, 기본값은 1로 설정되어 있습니다.



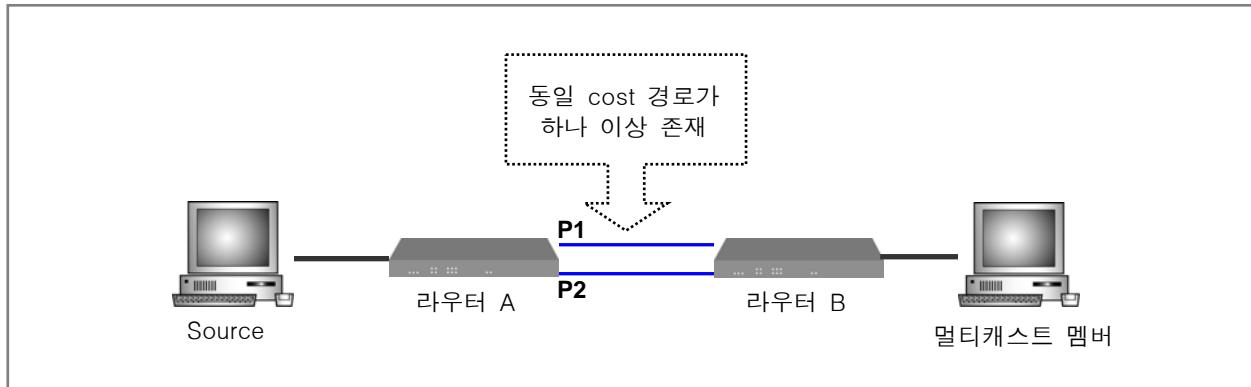
참 고

사용자 장비가 멀티캐스트 네트워크의 경계 라우터로 동작하도록 설정하려면, 멀티캐스트 TTL 임계값을 높은 값으로 지정하십시오.

(3) Multi-Path 설정

특정 목적지로 향하는 멀티캐스트 패킷이 경로값이 동일한 여러 경로를 가질 때에는 어느 경로를 통해 전송할 것인지 결정해야 합니다. 이러한 경우 PIM은 기본적으로 가장 높은 IP를 가지는 인터페이스를 통해 패킷을 전송합니다.

그러나, 멀티캐스트 Multi-path 기능을 사용하면 동일한 경로값을 가지는 여러 경로가 존재할 때, 사용자가 지정한 특정 정보를 기준으로 멀티캐스트 패킷 전송에 사용할 경로를 결정하여 패킷을 분산시킬 수 있습니다. 이와 같은 방법을 Load Splitting이라고 합니다.



【 그림 9-9 】 Equal Cost Multi-path

위의 그림에서 라우터 A와 라우터 B 사이에는 동일한 경로값을 갖는 P1과 P2가 존재합니다. 라우터 A는 P1과 P2 중에서 멀티캐스트 패킷을 전송할 경로를 결정합니다. 만약 Multi-path 기능을 사용하지 않으면, 라우터 A와 라우터 B 사이에서 멀티캐스트 패킷 전송은 처음으로 인식한 경로를 통해서만 이루어집니다. 즉, 멀티캐스트 트래픽 전송에 오직 하나의 링크만 사용하게 되므로 트래픽 폭주로 인한 지연 현상 등이 발생할 수 있습니다.

하지만 사용자가 Multi-path 기능을 장비에 설정하면 멀티캐스트 패킷 전송에 사용할 경로를 라우터가 초기에 결정한 경로와 상관 없이 지정할 수 있습니다. 따라서 Load Splitting을 사용하면 좀더 효과적으로 멀티캐스트 링크를 사용할 수 있게 됩니다.

V5812G에서는 경로값이 같은 경로가 여러 개 존재할 때 패킷의 특정 필드값(Source IP, Destination IP)을 기준으로 사용하여 경로를 결정합니다.

V5812G의 Multi-path 설정은 동작 방식에 따라 다음의 두 가지 모드로 나누어집니다.

- **srcip mode:** Source IP 주소를 이용하여 Next-hop을 결정합니다. 이 모드로 설정하면 동일한 Group IP 주소로 향하는 멀티캐스트 트래픽은 Source IP 주소 별로 다른 경로를 갖게 됩니다.
- **srcgrppip mode:** Source IP와 Group IP 주소를 함께 이용하여 Next-hop을 결정합니다. 이 모드로 설정하면 Source IP 및 Group IP 주소 별로 서로 다른 경로를 갖게 됩니다. 즉, 동일한 Source에서 서로 다른 Group IP 주소로 가는 트래픽에 대한 Splitting이 가능합니다.



참 고

멀티캐스트 Multi-path 기능은 활성화 또는 비활성화되거나 및 모드가 변경되면 멀티캐스트 라우팅 테이블의 엔트리를 삭제한 후 다시 업데이트 합니다.

사용자 장비에 멀티캐스트 Multi-path 기능을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip multicast multipath	Global	멀티캐스트 트래픽에 대하여 Multi-path 기능을 사용하도록 설정합니다.
ip multicast multipath {srcip srcgrppip}		멀티캐스트 트래픽에 대하여 Multi-path를 결정하는 기준이 되는 모드를 선택하여 설정합니다.



참 고

V5812G의 Multi-path 기능은 기본적으로 **srcip** 모드로 설정되어 있습니다.

사용자가 설정한 Multi-path 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip multicast multipath	Global	설정한 Multi-path 기능을 해제합니다.

(4) MRIB 엔트리 제한

사용자는 필요에 따라 MRIB(Multicast Routing Information Base)에서 멀티캐스트 라우팅 테이블의 엔트리 수를 제한할 수 있습니다. 라우팅 엔트리의 개수가 사용자가 제한한 값을 초과하면 시스템에러 메시지가 발생합니다. 한편, 경고 메시지에 대한 임계값을 설정하여 설정된 값 이상으로 라우팅 엔트리가 추가되면 경고 메시지를 발생하도록 설정할 수 있습니다.

멀티캐스트 라우팅 엔트리의 개수를 제한하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip multicast route-limit entry-limit [warning-threshold]	Global	멀티캐스트 라우팅 테이블에 추가 가능한 엔트리의 개수를 제한하도록 설정합니다.



참 고

entry-limit 는 제한되는 멀티캐스트 라우팅 엔트리의 개수로 <1-214,783,647> 범위에서 설정 가능합니다. *warning-threshold* 는 경고 메시지가 발생하는 값으로 <1-214,783,647>의 범위에서 설정할 수 있습니다.



주 의

*warning-threshold*는 추가 가능한 멀티캐스트 라우팅 엔트리의 최대값보다 작아야 합니다.

설정한 멀티캐스트 라우팅 엔트리 개수 제한을 해제하려면, Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip multicast route-limit	Global	설정한 멀티캐스트 라우팅 엔트리 개수 제한을 해제합니다.

(5) MRIB 엔트리 삭제

V5812G는 멀티캐스팅 라우팅 테이블의 멀티캐스트 라우팅 엔트리와 관련된 정보를 모두 삭제하거나 특정 그룹 및 Source 별로 삭제할 수 있습니다.

멀티캐스트 라우팅 테이블의 멀티캐스트 라우팅 엔트리 정보를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip mroute *	Enable/ Global/	멀티캐스트 라우팅 테이블의 모든 멀티캐스트 라우팅 엔트리 정보를 삭제합니다. 변수로 별표(*)를 사용하면 모든 엔트리 그룹 관련 정보를 삭제합니다.
clear ip mroute <i>group-address [source-address]</i>	Bridge	특정 그룹 및 Source를 지정하여 멀티캐스트 라우팅 테이블의 멀티캐스트 라우팅 엔트리 정보를 삭제합니다.

한편, PIM-SM 프로토콜의 MFC(Multicast Forwarding Cache)와 TIB(Tree Information Base)를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip mroute * [pim sparse-mode]	Enable/ Global/	PIM-SM의 모든 MFC 정보와 TIB 정보를 삭제합니다. 변수로 별표(*)를 사용하면 모든 엔트리 관련 통계 정보를 삭제합니다.
clear ip mroute group-address <i>[source-address] [pim sparse-mode]</i>	Bridge	특정 그룹 및 Source에서 MFC 정보와 TIB 정보를 삭제합니다.

(6) MRIB 엔트리 정보 확인

MRIB의 멀티캐스트 라우팅 엔트리 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip mroute [summary]		모든 멀티캐스트 라우팅 엔트리의 정보를 확인합니다.
show ip mroute {dense sparse} [summary]		PIM 모드 별로 멀티캐스트 라우팅 엔트리 정보를 확인합니다.
show ip mroute group-address {dense sparse} [summary]	Enable/ Global/	특정 그룹의 멀티캐스트 라우팅 엔트리 정보를 확인합니다.
show ip mroute group-address source-address {dense sparse} [summary]	Bridge	특정 Source IP 주소를 가진 그룹의 멀티캐스트 라우팅 엔트리 정보를 확인합니다.
show ip mroute A.B.C.D/M {dense sparse} [summary]		특정 범위 그룹의 멀티캐스트 라우팅 엔트리 정보를 확인합니다. 그룹 범위를 직접 입력하거나 Prefix를 이용할 수 있습니다.



summary 옵션을 사용하면 요약 정보를 확인할 수 있습니다.

(7) MRIB Statistics 삭제

IP 멀티캐스트 라우팅 테이블의 통계 정보를 삭제하려면, Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip mroute statistics *	Enable/ Global/	IP 멀티캐스트 라우팅 테이블의 통계 정보를 삭제합니다. 변수로 별표(*)를 사용하면 모든 엔트리 그룹 관련 통계 정보를 삭제합니다.
clear ip mroute statistics group-address [source-address]	Bridge	특정 그룹 및 Source에 대한 멀티캐스트 라우팅 통계정보를 삭제합니다.

(8) MRIB Statistics 정보 확인

MRIB statistics 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip mroute count	Enable/ Global/ Bridge	모든 멀티캐스트 라우팅 통계 정보를 확인합니다.
show ip mroute {dense sparse} count		PIM 모드 별로 멀티캐스트 라우팅 통계 정보를 확인합니다.
show ip mroute group-address {dense sparse} count		특정 그룹의 멀티캐스트 라우팅 통계 정보를 확인합니다.
show ip mroute group-address source-address {dense sparse} count		특정 Source IP 주소를 가진 그룹의 멀티캐스트 라우팅 통계 정보를 확인합니다.
show ip mroute A.B.C.D/M {dense sparse} count		특정 범위 그룹의 멀티캐스트 라우팅 통계 정보를 확인합니다. 그룹 범위를 직접 입력하거나 Prefix를 이용할 수 있습니다.

(9) MRIB Debug

MRIB 관련 정보를 디버깅하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
debug nsm mcast all	Enable	모든 MRIB와 관련된 정보를 디버깅합니다.
debug nsm mcast fib-msg		MFIB(Multicast Forwarding Information Base) 정보를 디버깅합니다.
debug nsm mcast mrt		멀티캐스트 라우터 정보를 디버깅합니다.
debug nsm mcast register		멀티캐스트 PIM Register 메시지를 디버깅합니다.
debug nsm mcast stats		멀티캐스트 관련 통계를 디버깅합니다.
debug nsm mcast vif		멀티캐스트 인터페이스 정보를 디버깅합니다.

설정한 MRIB 디버깅 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no debug nsm mcast all	Enable	모든 MRIB와 관련된 디버깅 기능을 해제합니다.
no debug nsm mcast fib-msg		MFIB(Multicast Forwarding Information Base) 과 관련된 디버깅 기능을 해제합니다.
no debug nsm mcast mrt		멀티캐스트 라우터 정보 디버깅 기능을 해제합니다.
no debug nsm mcast register		멀티캐스트 PIM Register 메시지 디버깅 기능을 해제합니다.
no debug nsm mcast stats		멀티캐스트 관련 통계의 디버깅 기능을 해제합니다.
no debug nsm mcast vif		멀티캐스트 인터페이스 정보의 디버깅 기능을 해제합니다.

(10) MFIB 정보 확인

V5812G는 멀티캐스트 L3 라우팅 엔트리 정보를 확인할 수 있는 기능을 제공합니다. 멀티캐스트 L3 라우팅 엔트리 정보는 패킷이 들어오는 포트를 input 포트, 패킷을 내보내는 포트를 output 포트로 해당 정보를 보여줍니다.

L3로 라우팅 되는 멀티캐스트 정보를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip mfib [vlan vlan-id group group-address] [detail]	Enable/ Global/Bridge	L3의 멀티캐스트 Forwarding 엔트리 정보를 확인합니다.



참 고

show ip mfib 명령어의 **detail** 옵션을 사용하면 각 인터페이스에 Input/Output 포트가 출력되며 각 포트의 그룹도 함께 표시됩니다.

9.3.2. PIM 개요

PIM(Protocol Independent Multicast)은 가장 널리 사용되는 멀티캐스트 라우팅 프로토콜로, 일반적인 라우팅 정보를 이용하지만 특정 라우팅 프로토콜에 의존하지 않습니다. 즉, 라우팅 프로토콜의 종류에 상관 없이 PIM에서 그 정보를 참조할 수 있습니다. PIM에는 PIM-DM(Protocol Independent Multicast-Dense Mode)과 PIM-SM(Protocol Independent Multicast-Sparse Mode)의 두 종류가 있으며, 이들은 서로 다른 환경에서 동작하도록 최적화되어 있습니다.

PIM-SM은 멀티캐스트 그룹이 네트워크 상에서 광범위한 지역에 드물게 존재하고 대역폭의 여유가 없는 환경에서 사용하기에 적합한 프로토콜입니다. PIM-SM은 데이터가 요청되지 않으면 어떤 호스트도 멀티캐스트 데이터를 필요로 하지 않는다고 가정합니다. 따라서, PIM-SM에서 라우터는 하위 멀티캐스트 그룹과 연결된 인접 라우터로부터 PIM Join 메시지를 수신하는 경우에 한하여 멀티캐스트 패킷을 전송합니다. PIM-SM은 효율적인 멀티캐스트 패킷 전달을 위한 공유 트리 및 Source 분배 트리를 지원합니다. 보다 자세한 사항은 뒷장에 설명되는 「**1.1.1(1) PIM-SM 동작 원리**」를 참조하십시오.

PIM-DM은 멀티캐스트 그룹이 네트워크 상에서 밀집되어 있고 대역폭에 여유가 있는 환경에서 사용하기에 적합한 프로토콜입니다. PIM-SM과 달리 PIM-DM은 동일 네트워크 상의 모든 호스트가 멀티캐스트 데이터를 필요로 한다고 가정합니다. 따라서, PIM-DM에서 라우터는 초기에 모든 멀티캐스트 라우터에게 멀티캐스트 패킷을 Flooding하고, 멀티캐스트 그룹과 연결되지 않은 인접 라우터로부터 PIM Prune 메시지를 수신할 경우에 한하여 해당 라우터에 대한 멀티캐스트 패킷 전송을 중단합니다.



참 고

V5812G에서는 PIM-SM만 지원합니다.

(1) PIM-SM 동작 원리

멀티캐스트 통신을 하고자 하는 어떤 호스트가 특정 멀티캐스트 그룹에 가입할 때, DR은 RP에게 (*, G) 엔트리의 PIM Join 메시지를 보냅니다. Join 메시지는 Hop-by-hop으로 RP로 전송됩니다. 이 때 지나게 되는 각각의 PIM 라우터는, Join 메시지를 수신한 인터페이스를 해당 메시지의 그룹 주소와 함께 OIF(Outgoing Interface) 리스트에 추가한 후에 메시지를 전송합니다.

만약 RP가 특정 멀티캐스트 그룹에 가입한 수신자와 연결되어 있다면, RP는 SPT를 통해 Source로부터 멀티캐스트 패킷을 받아 수신자 그룹에 전송해야 합니다. Source측 DR은 멀티캐스트 패킷을 PIM Register 메시지에 캡슐화하여 RP로 유니캐스트 합니다. Register 메시지를 수신하면 RP는 SPT 구성을 위해 멀티캐스트 Source로 (S, G) 엔트리의 Join 메시지를 보냅니다. 이렇게 성립된 SPT로 멀티캐스트 패킷을 받기 시작하면 RP는 이것을 자신과 연결된 멀티캐스트 수신자에게 전달합니다.

멀티캐스트 트래픽은 SPT 전환 메커니즘을 통해 Source에서 수신자에게 직접적으로 전달됩니다. 보다 자세한 사항은 「**9.3.7 SPT 전환**」을 참조하십시오.

(2) Rendezvous Point Tree(RPT)

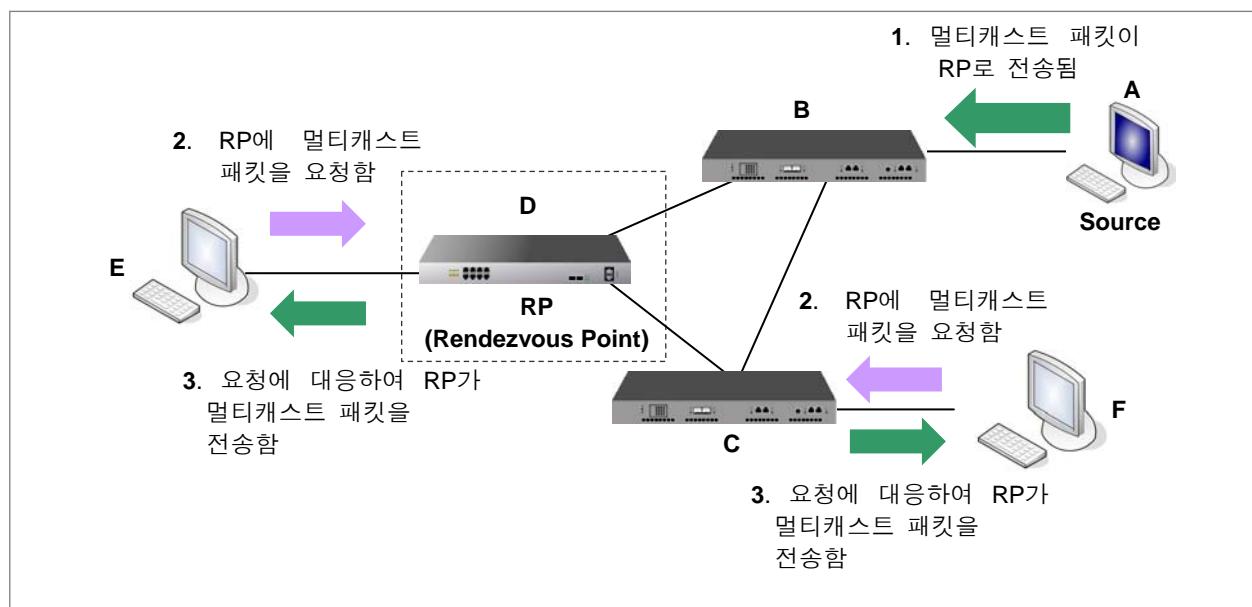
PIM-SM에서는 멀티캐스트 트래픽을 전달할 때 주로 RPT라 불리는 공유 트리를 이용합니다. RPT에서는 RP(Rendezvous Point)라는 코어 라우터를 중심으로 통신이 이루어집니다. RP는 멀티캐스트 그룹 당 하나씩 존재하는데, 이는 모든 멀티캐스트 그룹이 서로 다른 공유 트리를 구성하는 것을 의미합니다.

RP는 모든 멀티캐스트 Source로부터 멀티캐스트 패킷을 전송받아, 그것을 각 멀티캐스트 그룹에게 전달하는 역할을 담당합니다. 이러한 RPT 구조에서 RP를 제외한 각 라우터는 멀티캐스트 Source에 대한 어떠한 정보도 알고 있을 필요가 없으며, 오로지 RP에 대한 정보만 가지고 있으면 됩니다. 왜냐하면, RP가 모든 멀티캐스트 그룹과 관련된 Source 정보를 확실하게 알고 있기 때문입니다. 따라서, 특정 멀티캐스트 그룹에 참가하고자 하는 수신자는 RP로 (*, G) 엔트리의 PIM Join 메시지만 전송하면 됩니다.

RPT에서 각 라우터는 모든 멀티캐스트 Source에 대하여, Source와 Group 정보를 알고 있을 필요가 없습니다. 즉, 각 라우터가 멀티캐스트 Source를 찾지 않아도 되므로 라우터 자원을 절약할 수 있고 네트워크 전체의 효율성을 높이게 됩니다. 또한, 멀티캐스트 전송을 위해 유지해야 할 정보의 양도 줄어들기 때문에 관리도 용이해집니다.

한편, RPT에서 공유 트리는 단일 방향성을 가집니다. 이는 모든 멀티캐스트 트래픽이 RP에서 해당 수신자에게로 전달됨을 의미합니다. 따라서, RPT에서 경로는 멀티캐스트 Source에서부터 수신자까지 최단경로가 되지 않을 수도 있으며, 이로 인한 지연현상이 발생할 가능성이 있습니다.

아래의 그림은 RPT 네트워크의 예를 나타낸 것입니다. 멀티캐스트 패킷은 Source A에서 B를 거쳐 D(RP)로 전달됩니다. 이때 RP는 멀티캐스트 Source로부터 최단 경로를 통해 멀티캐스트 패킷을 전달받습니다. 그리고, D(RP)는 E, 또는 F로부터 Join 메시지를 받은 후에 멀티캐스트 패킷을 전송합니다. 결과적으로, 수신자 E가 멀티캐스트 패킷을 전달받게 되는 경로는 『A → B → D → E』가 되며, 또 다른 수신자 F가 멀티캐스트 패킷을 전달받게 되는 경로는 『A → B → D → C → F』가 됩니다.



【 그림 9-10 】 PIM-SM의 RPT

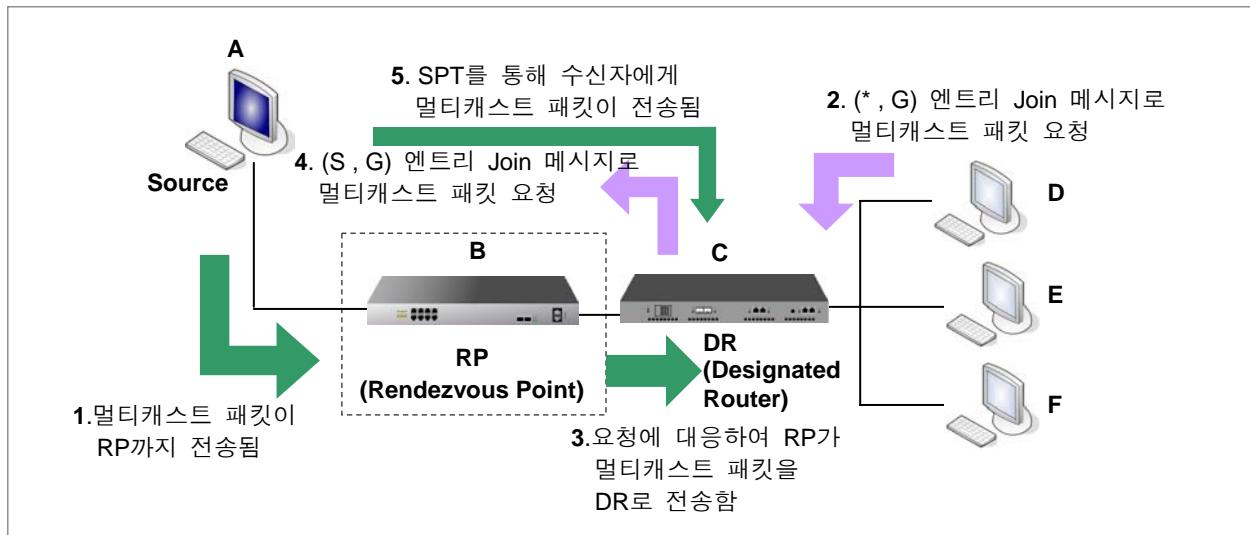
(3) Shortest Path Tree(SPT)

멀티캐스트 그룹 수 증가 등으로 멀티캐스트 수신자가 늘어나게 되면 RPT가 효율적으로 동작하지 않을 수 있습니다. 이러한 경우에 PIM-SM은 멀티캐스트 패킷이 Shortest Path Tree(SPT)를 통하여 전송되도록 경로를 재조정 합니다. 이것을 SPT 전환이라고 하며, SPT로의 전환은 멀티캐스트 트래픽을 전달할 때 최단 경로가 사용됨을 의미합니다.

멀티캐스트 Source와 SPT를 구성하기 위해 DR은 (S, G) 엔트리의 Join 메시지를 Source로 보냅니다. 멀티캐스트 Source와 수신자 사이에 SPT가 구성되면 멀티캐스트 패킷은 SPT를 따라 전송되며, DR은 (*, G) 엔트리의 Prune 메시지를 RP로 보내서 기존의 RPT에서 멀티캐스트 패킷이 전송되지 않도록 합니다.

SPT는 일반 라우팅 테이블 정보를 이용한 RPF 검사를 통해 구성됩니다. SPT에서 RPF 검사는 멀티캐스트 Source IP 주소를 사용하기 때문에, 모든 멀티캐스트 Source마다 다른 Distribution tree를 갖게 됩니다. 따라서, 멀티캐스트 패킷 전송은 효율적으로 이루어질 수 있지만, 각각의 멀티캐스트 라우터는 (S, G) 엔트리 정보를 관리하기 위해 더 많은 자원이 필요합니다.

다음 그림은 SPT 전환을 나타낸 예입니다. Source A에서 전송된 멀티캐스트 패킷은 RPT에 의해 B(RP)와 C(DR)를 거쳐 멀티캐스트 패킷을 요청한 D로 보내집니다. 처음으로 멀티캐스트 패킷을 전달받으면 C(DR)는 Source A와 수신자 D 사이의 SPT를 구성하기 위하여, A에게 (S, G) 엔트리의 Join 메시지를 보냅니다. C로부터 Join 메시지를 받은 A는 불필요한 흡수 제거하고 SPT를 통해서 D로 직접 멀티캐스트 패킷을 전송합니다. 결과적으로 멀티캐스트 패킷이 전송되는 경로는 『A → B → C』가 됩니다.



【 그림 9-11 】 PIM-SM의 SPT

(4) PIM 메시지

PIM-SM과 PIM-DM은 동일한 메시지 포맷을 사용합니다. 다음은 PIM에서 사용되는 메시지의 종류에 대한 설명입니다.

- Hello 메시지

PIM 라우터는 정기적으로 Hello 메시지를 보냅니다. 이를 통해 인접 PIM 라우터를 발견하고 각각의 서브넷에서 DR(Designated Router)로 동작할 라우터를 결정합니다.

- **Register 메시지**

Register 메시지는 DR이 멀티캐스트 Source 정보를 RP에 등록하기 위해 전송하는 것입니다. 여기서 DR은 멀티캐스트 Source의 First-hop 라우터입니다. Register 메시지에는 멀티캐스트 트래픽이 캡슐화되어 포함되어 있습니다. Register 메시지와 Register-stop 메시지는 유니캐스트 형태로 전달됩니다.

- **Register-stop 메시지**

Register-stop 메시지를 수신하면 라우터는 Register 메시지 전송을 중단합니다. RP는 멀티캐스트 패킷을 캡슐화가 풀린 순수 멀티캐스트 패킷 형태로 수신하게 되면, DR에 Register-stop 메시지를 전송합니다. DR은 이 메시지를 받으면 RP는 멀티캐스트 패킷을 Register 메시지에 캡슐화하여 전송하는 것을 멈추게 됩니다. Register-stop 메시지는 RP에서 Register 메시지를 보낸 라우터로 전송됩니다.

- **Join/prune 메시지**

Join/prune 메시지는 라우터에서 Upstream Source 또는 RP로 전송됩니다. Join 메시지는 RPT 및 SPT(Shortest Path Tree)를 통해 멀티캐스트 트래픽을 받고자 할 때 사용됩니다. Prune 메시지는 멀티캐스트 통신을 중지하고자 할 때, 멀티캐스트 분배 트리(Multicast Distribution Tree) 구성을 해제하기 위해 사용됩니다.

- **Bootstrap 메시지**

BSR(Bootstrap Router)는 RP를 선출하기 위하여 Bootstrap 메시지를 보냅니다. Bootstrap 메시지에는 각각의 Candidate RP에 대한 정보(RP-set)가 담겨 있습니다.

- **Assert 메시지**

다중 액세스 네트워크에서 Source나 RP로 가는 동일 cost의 경로가 여러 개 존재할 수 있습니다. 이러한 상황에선 여러 라우터로부터 멀티캐스트 패킷을 중복해서 받는 멀티캐스트 그룹 구성원이 생길 수 있습니다. 따라서, 평행 경로 상에 존재하는 라우터 중에서 한 대를 지정하여 멀티캐스트 패킷이 중복 전달되지 않도록 합니다. 이때 사용되는 메시지가 Assert 메시지입니다.

- **Candidate RP advertisement 메시지**

각각의 RP 지원자들은 Candidate RP advertisement 메시지에 자신의 정보를 담아 BSR에 유니캐스트 합니다. BSR은 전송받은 RP 지원자 정보를 Bootstrap 메시지에 포함시킵니다.

9.3.3. PIM-SM 기본 설정

이 장에서는 PIM 기본 설정과 관련하여 다음과 같은 내용을 설명합니다.

- PIM 모드 설정
- DR Priority 설정
- Neighbor Filtering 설정
- Hello 메시지 설정
- Join/Prune 전송 간격 설정
- VIF Flap Discredit 설정
- PIM 정보 확인

(1) PIM 모드 설정

V5812G에 PIM-SM을 설정하려면 먼저 Interface 모드에서 PIM-SM을 활성화해야 합니다. PIM-SM을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim sparse-mode	Interface	해당 인터페이스에서 PIM-SM을 활성화합니다.
no ip pim sparse-mode		해당 인터페이스에서 PIM-SM을 해제합니다.

한편, V5812G에서는 PIM-SM을 Passive 모드로 활성화할 수 있습니다. Passive 모드로 설정하면 해당 PIM-SM은 로컬 멤버에 대해서만 동작합니다. Passive 모드로 설정된 인터페이스에서는 PIM 패킷의 송수신이 불가능하며, IGMP 동작만 가능합니다. 따라서, PIM-SM Passive 모드는 PIM 라우터가 1개만 존재하는 네트워크에서 사용하는 것이 좋습니다.

PIM-SM을 Passive 모드로 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim sparse-mode passive	Interface	해당 인터페이스에서 PIM-SM을 Passive 모드로 활성화합니다.
no ip pim sparse-mode passive		해당 인터페이스에서 PIM-SM Passive 모드를 해제합니다.

[설정 예제]

다음은 Interface 1에 PIM-SM을 활성화하는 경우입니다.

```
SWITCH(config)# interface 1
SWITCH(config-if)# ip pim sparse-mode
```

(2) DR Priority 설정

일반적으로 PIM-SM에서 DR(Designated Router)은 수신측 호스트의 First-hop 라우터가 됩니다. DR은 해당 그룹 멤버십 등의 정보를 RP에 전달하기 위해 PIM Join/Prune 메시지를 정기적으로 전송합니다.

동일한 서브넷에 여러 개의 라우터가 존재할 경우, 이 중 하나를 선정하여 DR로 동작하도록 해야 합니다. DR을 선택하기 위해서, 먼저 각각의 PIM 라우터는 다른 인접 PIM 라우터로부터 받은 PIM Hello 메시지를 검사하여 DR Priority를 비교합니다. DR Priority를 비교한 결과 그 값이 가장 높은 라우터가 DR로 선정됩니다. DR Priority가 동일한 라우터들 사이에서는 IP 주소가 높은 라우터가 높은 우선 순위를 가집니다.

DR이 결정된 후, 만약 DR로부터 일정 시간 동안 Hello 메시지가 전송되지 않는다면, 위와 같은 방법으로 다른 DR선출 과정이 진행됩니다.

DR Priority를 설정하려면, Interface 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim dr-priority <0-4294967294>	Interface	DR Priority 값을 설정합니다.



참 고

DR Priority는 <0-4294967294> 범위에서 설정할 수 있으며, V5812G에 설정되어 있는 기본값은 1입니다.

설정한 DR Priority 값을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim dr-priority	Interface	설정한 DR Priority를 해제합니다.
no ip pim dr-priority <0-4294967294>		



참 고

일반적으로 IGMP 버전1에서는 DR과 IGMP Querier가 동일한 라우터이지만, IGMP 버전2에서는 다를 수 있습니다. IGMP 버전2에서 DR은 가장 높은 IP 주소를 가진 라우터가 선정되는 반면에 IGMP Querier는 가장 낮은 IP 주소를 가진 라우터가 선정됩니다.

(3) Neighbor Filtering 설정

V5812G는 사용자의 필요에 따라 Access list를 이용하여 Neighbor 라우터를 필터링 할 수 있습니다. 이 기능을 활성화하면 PIM은 Access list에 deny로 설정된 라우터를 제외하고 인접 라우터를 구성합니다.

PIM에서 Neighbor 라우터 필터링 기능을 설정하려면, Interface 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim neighbor-filter { <1-99> access-list-name}	Interface	PIM Neighbor 라우터 필터링 기능을 설정합니다.

Neighbor 라우터 필터링 기능을 해제하려면, Interface 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim neighbor-filter { <1-99> access-list-name}	Interface	PIM Neighbor 라우터 필터링 기능을 해제합니다.

PIM Neighbor 라우터 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip pim neighbor [detail]	Enable/Global/Bridge	PIM Neighbor 라우터 정보를 확인합니다.

(4) Hello 메시지 설정

PIM 라우터는 정기적으로 Hello 메시지를 보냅니다. 이를 통해 인접 PIM 라우터를 발견하고 각각의 서브넷에서 DR(Designated Router)로 동작할 라우터를 결정합니다. PIM Hello 메시지는 224.0.0.13(모든 PIM 라우터 그룹) 주소를 사용하여 멀티캐스트 됩니다.

PIM Hello 메시지의 전송간격을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim query-interval period	Interface	PIM Hello 메시지의 전송 간격을 설정합니다.



참 고

PIM Hello 메시지의 전송간격 *period*은 <1-18724> 범위에서 설정할 수 있으며 단위는 초(sec)입니다.

PIM Hello 메시지의 전송간격을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim query-interval	Interface	설정한 PIM Hello 메시지 전송간격을 해제합니다.

PIM Hello 메시지는 해당 메시지 정보가 유효한 기간을 명시하는 Hold-time을 포함합니다. V5812G에 설정되어 있는 PIM Hello 메시지의 유효기간(*hold-time*)은 기본적으로 위에서 설정한 해당 Hello 메시지 전송간격(*period*)의 3.5배입니다. 예를 들어, 사용자가 PIM Hello 메시지 전송간격을 10초로 설정하였다면, PIM Hello 메시지의 기본 유효기간은 $10 \times 3.5=35(\text{sec})$ 가 됩니다.

PIM Hello 메시지의 유효 기간을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim query-holdtime hold-time	Interface	PIM Hello 메시지의 유효기간을 설정합니다.



참 고

PIM Hello 메시지의 유효기간 *hold-time*은 <1-65535> 범위에서 설정할 수 있으며 단위는 초(sec)입니다.



주의

*hold-time*은 반드시 *period*보다 큰값으로 설정하십시오. 만약, PIM Hello 메시지의 유효기간(*hold-time*)을 해당 메시지의 전송간격(*period*)보다 작은 값으로 설정할 경우, 사용자가 설정한 값은 무시되고 기본값으로 동작합니다.



참고

PIM Hello 메시지의 유효기간은 기본적으로 위에서 설정한 해당 Hello 메시지 전송간격의 3.5배입니다.

PIM Hello 메시지의 유효기간을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim query-holdtime	Interface	설정한 PIM Hello 메시지의 유효기간을 해제합니다.

(5) Join/Prune 전송 간격 설정

PIM 라우터는 정기적으로 PIM Join/Prune 메시지를 멀티캐스트 그룹에 전송합니다. 만약 라우터가 사용자가 설정한 전송간격의 3배 이상의 시간이 지나도록 join 메시지를 보내지 않는다면, 해당 라우터는 멀티캐스트 그룹 멤버에서 자동으로 탈퇴처리 됩니다.

PIM Join/Prune 메시지의 전송 간격을 설정하려면, Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim message-interval <1 - 65535>	Global	PIM Join/Prune 메시지의 전송간격을 설정합니다.



참고

PIM Join/Prune 메시지의 전송간격은 <1-65,535> 범위에서 설정할 수 있으며 단위는 초(sec)입니다.

PIM Join/Prune 메시지의 전송 간격을 해제하려면, Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim message-interval	Global	설정한 PIM Join/Prune 메시지의 전송간격을 해제합니다.

(6) VIF Flap Discredit 설정

PIM VIF는 보다 효율적으로 PIM 컨트롤 패킷을 송수신하기 위해 사용되는 가상 인터페이스입니다. VIF에는 인터페이스의 상태 정보 및 PIM 컨트롤 메시지를 전달하기 위한 정보가 포함되어 있습니다.

PIM 라우터들은 내부적으로 VIF로 연결되어 있으며, 이들 사이에는 경로값이 같은 경로가 여러 개 존재할 수 있습니다. 이러한 경우 PIM 라우터는 멀티캐스트 패킷의 Source IP 주소 또는 Source IP 주소와 Group IP 주소를 참고하여 해당 패킷의 전송 경로를 결정합니다. 보다 자세한 사항은 「(3) Multi-Path 설정」을 참조하십시오.

만일, 이런 상황에서 VIF Flapping이 발생한다면 멀티캐스트 패킷의 전송 경로가 변경되어야 하기 때문에 경로 결정 과정이 반복되고 이로 인해 멀티캐스트 패킷의 전송 효율이 저하될 수 있습니다. 여기서 Flapping이란 특정 VIF가 ON/OFF를 반복하는 현상을 말합니다.

PIM VIF Flap Discredit은 이처럼 VIF Flapping로 인한 경로 결정 과정이 반복되는 것을 최소한으로 억제하여, 안정된 멀티캐스트 서비스를 제공할 수 있도록 하는 기능입니다. 이 기능을 이용하면, V5812G는 VIF Flapping이 발생할 때마다 해당 VIF의 Credit 값을 감소시킵니다. 그리고 VIF Credit이 회복될 때까지 경로 결정 과정에서 해당 VIF를 제외합니다.

PIM VIF Flap Discredit 기능을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim vif flap discredit	Global	PIM VIF Flap Discredit 기능을 활성화합니다.
no ip pim vif flap discredit		PIM VIF Flap Discredit 기능을 비활성화합니다.



참 고

V5812G는 기본적으로 PIM VIF Flap Discredit 기능이 활성화되어 있습니다.

VIF Flapping이 발생할 때마다 Credit 값을 감소시키는 Discredit을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim vif flap discredit unit <10-50>	Global	VIF Flapping이 발생할 때마다 Credit 값을 감소시키는 Discredit을 설정합니다.
no ip pim vif flap discredit unit		설정한 Discredit을 해제하고 기본값으로 설정합니다.



참 고

V5812G에 설정되어 있는 Discredit 기본값은 10입니다.

V5812G는 사용자가 지정한 시간마다 VIF의 Credit을 검사하여 기본값(100)보다 낮은 Credit 값을 회복시킵니다. 이때 회복되는 Credit 값은 기본값에서 해당 VIF의 현재 Credit을 뺀 값의 1/2에 해당합니다. 예를 들어, VIF A에 Flapping이 발생하여 Credit이 30 감소하였고, 사용자가 설정한 Credit 회복 시간이 20초라고 가정합니다. 이 경우 20초 후에 회복되는 Credit 값은 $(100-70)/2=15$ 입니다.

감소한 Credit 값을 회복시킬 시간 간격을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim vif flap discredit half-recover-time <0-3600>	Global	VIF Credit을 회복시킬 시간 간격을 설정합니다.
no ip pim vif flap discredit half-recover-time		설정한 VIF Credit을 회복시킬 시간 간격을 해제하고 기본값으로 설정합니다.



참 고

VIF Credit 회복 시간 간격은 <0-3600> 범위에서 설정할 수 있으며, 기본값은 10초(sec)입니다.

현재 설정되어 있는 VIF Credit을 삭제하고 기본값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip pim vif flap discredit [vif<0-127>]	Global	현재 설정되어 있는 VIF Credit을 삭제하고 기본값 100으로 되돌립니다.

(7) PIM 정보 확인

PIM 정보를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip pim interface [detail]	Enable/ Global/ Bridge	PIM 인터페이스 정보를 확인합니다. detail 옵션을 사용하면 VIF 정보까지 확인할 수 있습니다.
show ip pim local-members [interface-name]		PIM 로컬 멤버십 정보를 확인합니다.
show ip pim mroute group-address [source-address]		특정 그룹 및 Source의 PIM 멀티캐스트 라우터 정보를 확인합니다.
show ip pim mroute [summary]		멀티캐스트 라우터 엔트리의 요약정보를 확인합니다.
show ip pim mroute [A.B.C.D/M]		특정 멀티캐스트 그룹의 범위를 설정하여 PIM 멀티캐스트 라우터 정보를 확인합니다.
show ip pim mroute static		모든 PIM static join 그룹 정보를 확인합니다.
show ip pim nexthop		PIM Next 흡 정보를 확인합니다.
show ip pim nexthop {source-address *} [group-address]		특정 Source 및 그룹의 PIM Next 흡 정보를 확인합니다. 변수 *를 사용하면 모든 Source에 대한 정보를 확인할 수 있습니다.

9.3.4. RP 설정

공유 트리에서 RP(Rendezvous Point)는 수신자가 특정 멀티캐스트 그룹에게 멀티캐스트 패킷을 보내는 Source를 찾아낼 수 있게 하는 수단입니다. RP는 모든 멀티캐스트 패킷을 수신하고 이를 적절한 수신자에게 전달해야 합니다.

(1) Static RP 설정

Candidate RP 중에서 RP를 결정하기 위해 V5812G는 BSR 메커니즘과 Static RP를 지원합니다. BSR 메커니즘은 BSR(Bootstrap Router)이 정기적으로 Candidate RP들의 정보가 담긴 Bootstrap 메시지를 모든 PIM-SM 라우터에게 보내서 RP를 선정하는 방법입니다. 보다 자세한 사항은 「**9.3.5 BSR 설정**」을 참조하십시오.

한편, Static RP는 사용자가 RP를 수동으로 설정하는 기능입니다. V5812G는 Static RP 기능을 이용하여 모든 멀티캐스트 그룹에 대한 RP 또는 Access-list를 이용한 특정 멀티캐스트 그룹에 대한 RP를 수동으로 설정할 수 있습니다.

만약, 하나의 멀티캐스트 그룹에 Static RP가 여러 개 존재할 경우에는 IP 주소가 가장 높은 것이 RP로 동작하게 됩니다. 또한, 한 멀티캐스트 그룹 안에서 Static RP와 BSR 메커니즘을 통해 선정된 RP가 동시에 유효할 경우, 일반적으로 BSR 메커니즘을 통해 선정된 RP가 우선순위를 가지며, 해당 그룹의 RP로 동작하게 됩니다. 하지만 V5812G는 필요에 따라 이러한 상황에서 사용자가 지정한 Static RP를 사용하도록 설정할 수 있습니다.

모든 멀티캐스트 그룹 또는 특정 멀티캐스트 그룹에서 사용할 RP를 수동으로 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim rp-address rp-address [override]		모든 멀티캐스트 그룹에 대한 Static RP를 설정합니다.
ip pim rp-address rp-address [<1-99> <1300-1900>] [override]	Global	특정 멀티캐스트 그룹에 대한 Static RP를 설정합니다.



위 명령어의 **override** 옵션을 사용하면 Static RP가 BSR 메커니즘을 통해 선정된 RP보다 높은 우선순위를 가지게 되며, 해당 멀티캐스트 그룹의 RP로 동작하게 됩니다.



Access-list는 <1-99> 이내에서 입력할 수 있으며, <1300-1900> 이내의 값을 입력하면 확장된 범위의 Access-list를 이용할 수 있습니다.



위 명령어에 사용하는 Access-list는 **Standard access-list**입니다.

설정한 Static RP를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim rp-address rp-address	Global	설정한 Static RP를 삭제합니다.

(2) KAT (Keep Alive Time) 설정

RP를 통한 멀티캐스트 Source Register가 완료되면, Source측 DR은 RP와 (S, G) 엔트리의 Join 상태를 유지하기 위하여 정기적으로 PIM Null-register 메시지를 RP로 전송합니다. Null-register 메시지는 멀티캐스트 패킷이 캡슐화되지 않은 Register 메시지입니다. 멀티캐스트 Source Register에 대한 자세한 내용은 뒤에 나오는 「**9.3.6 Source Registration**」을 참조하십시오.

만약, 일정한 시간 동안 Null-register 메시지가 전송되지 않는다면 (S, G) 엔트리는 삭제되고, Source Register 과정이 반복됩니다. 이때 (S, G) 엔트리가 유효한 시간을 KAT(Keep Alive Time)이라고 하며, 이 시간 이내에 Null-register 메시지가 전송되면 (S, G) 엔트리는 갱신되어 멀티캐스트 통신을 지속하게 됩니다. V5812G는 사용자의 필요에 따라 KAT를 설정할 수 있습니다.

멀티캐스트 라우팅의 (S, G) 엔트리가 유효한 시간인 KAT를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim rp-register-kat <1-65535>	Global	RP에 (S, G) 엔트리 유효시간인 KAT를 설정합니다.



참 고

KAT(Keep Alive Time)은 <1-65535> 범위에서 설정할 수 있으며 단위는 초(sec)입니다.

설정한 KAT를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim rp-register-kat	Global	RP의 KAT를 해제합니다.



참 고

만약, 멀티캐스트 Source측 DR에 Registration Suppression Time이 설정되어 있지 않은 경우, 위 명령어를 이용하여 해당 DR에 KAT(Keep Alive Time)을 설정하면, Registration Suppression Time을 설정한 것과 동일한 동작을 합니다.

(3) Candidate RP 설정

RP를 결정하기 위해서 각각의 Candidate RP는 자신의 정보를 BSR(Bootstrap Router)로 보냅니다. 이 정보에는 해당 라우터의 IP 주소, RP Priority, 그리고 서비스 가능한 멀티캐스트 그룹의 주소 등이 포함되어 있습니다. BSR은 각각의 Candidate RP에게 받은 정보를 Bootstrap 메시지에 담아서 정기적으로 PIM-SM 네트워크 상의 모든 라우터에게 배포합니다. 이때 Bootstrap 메시지에 포함되는 Candidate RP의 정보 집합을 RP-set이라 합니다.

특정 인터페이스를 Candidate RP로 설정하여 BSR로 정보를 보내도록 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim rp-candidate interface-name ([group-list <1 - 99>] [interval <1 - 16383>] [priority <0 - 255>])	Global	특정 인터페이스를 Candidate RP로 설정합니다.



참 고

group-list는 해당 라우터에서 서비스 가능한 멀티캐스트 그룹의 Access-list로 <1-99> 범위에서 입력하십시오. **interval**은 BSR로 Candidate RP 정보를 전송할 간격으로, <1-16,383> 범위에서 입력하며 단위는 초(sec)를 사용합니다. **priority**는 해당 라우터의 RP priority 값을 나타내며, <0-255> 범위에서 입력하십시오.



참 고

위 명령어 사용 시 해당 라우터에서 서비스 가능한 특정 멀티캐스트 그룹의 Access-list를 지정하지 않으면, 모든 멀티캐스트 그룹에 대해 서비스 가능한 것으로 간주됩니다.

설정한 Candidate RP 정보를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim rp-candidate interface-name group-list <1-99>		해당 인터페이스에서 서비스 가능한 멀티캐스트 그룹 리스트를 삭제합니다.
no ip pim rp-candidate interface-name	Global	BSR로 Candidate RP 정보를 보내지 않도록 설정합니다.
no ip pim rp-candidate		Candidate RP 설정을 삭제합니다.



참 고

위의 명령어 사용 시 옵션값으로 `interface-name`만 지정한 경우 `show running-config` 명령어로 해당 인터페이스의 Candidate RP 설정 정보를 확인할 수 있습니다. 그러나, `no ip pim rp-candidate`를 사용하면 Candidate RP 설정 자체가 삭제되기 때문에 `show running-config` 명령어로 해당 정보를 확인할 수 없습니다.

(4) RP Priority 사용 중지

일반적으로 Candidate RP 중에서 RP를 선정할 때 라우터는 BSR에게서 받은 Bootstrap 메시지의 RP-set 정보를 검사하여, RP Priority가 가장 높은 것을 찾아내 RP로 결정합니다. 하지만, V5812G에서는 Candidate-RP에 설정된 RP Priority 값을 무시하고 Hash 메커니즘을 이용하여 RP를 결정하도록 설정할 수 있습니다. 이 기능은 RP Priority를 인식하지 못하는 라우터에 사용하면 좋습니다. RP를 결정할 때 RP Priority를 무시하고 Hash 메커니즘을 이용하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>ip pim ignore-rp-set-priority</code>	Global	RP Priority를 무시하고 Hash 메커니즘을 이용하여 RP를 결정하도록 설정합니다.

다시 Candidate-RP에 설정된 RP Priority 값에 따라 RP를 결정하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>no ip pim ignore-rp-set-priority</code>	Global	RP를 결정할 때 Hash 메커니즘을 이용하도록 한 것을 해제하고 RP Priority 값을 이용하도록 설정합니다.

(5) RP 설정 확인

RP 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>show ip pim rp mapping</code>	Enable/ Global/	RP-set 정보와 각 멀티캐스트 그룹의 RP 정보를 확인합니다.
<code>show ip pim rp-hash group-address</code>	Bridge	특정 멀티캐스트 그룹의 RP 정보를 확인합니다.

9.3.5. BSR 설정

BSR(Bootstrap Router) 메커니즘은 멀티캐스트 라우터가 각 멀티캐스트 그룹에 대한 RP 정보를 알 수 있는 방법 중에 하나입니다. PIM-SM에서 모든 라우터들은 잠재적으로 BSR이 될 수 있으며, 이들은 자신을 Candidate BSR로 생각합니다. 이러한 Candidate BSR 중에서 BSR을 결정하기 위하여, 각각의 Candidate BSR은 자신의 정보를 담은 Bootstrap 메시지를 Flooding 합니다. Bootstrap 메시지를 받으면 Candidate BSR은 그 내용을 검사하여 BSR Priority가 가장 높은 라우터를 BSR로 결정합니다. 한편, BSR Priority 값이 같은 라우터가 하나 이상 존재할 경우에는 IP 주소가 가장 높은 라우터가 BSR이 됩니다.

이러한 과정을 거쳐 결정된 BSR은 정기적으로 RP-set 정보가 포함된 Bootstrap 메시지를 모든 PIM-SM 라우터에게 보내야 하며, 각 라우터들은 이 메시지를 통해 특정 멀티캐스트 그룹을 관리하는 RP 정보를 알 수 있습니다.

(1) Candidate BSR 설정

특정 인터페이스를 Candidate BSR로 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim bsr-candidate interface-name	Global	특정 인터페이스를 Candidate BSR로 설정합니다.
ip pim bsr-candidate interface-name <0-32>		특정 인터페이스를 Candidate BSR로 설정하면서, RP 결정을 위한 Hash mask 길이를 지정합니다..
ip pim bsr-candidate interface-name <0-32> <0-255>		특정 인터페이스를 Candidate BSR로 설정하면서, RP 결정을 위한 Hash mask 길이와 BSR Priority도 지정합니다.



참 고

RP 결정을 위한 Hash mask 길이는 <0-32> 범위에서 지정하며, BSR Priority는 <0-255> 범위에서 입력할 수 있습니다.

설정한 Candidate BSR을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim bsr-candidate	Global	설정한 Candidate BSR을 해제합니다.

(2) RP-set 정보 삭제

BSR은 각각의 Candidate RP에게서 받은 정보를 모아 Bootstrap 메시지에 담아 PIM-SM 네트워크에 존재하는 모든 라우터에게 정기적으로 배포합니다. 이때 Bootstrap 메시지에 포함되는 Candidate RP의 정보 집합을 RP-set이라 합니다. V5812G는 모든 RP-set 정보를 삭제할 수 있습니다. 모든 RP-set을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip pim sparse-mode bsr rp-set *	Enable/Global	모든 RP-set을 삭제합니다.

(3) BSR 설정 확인

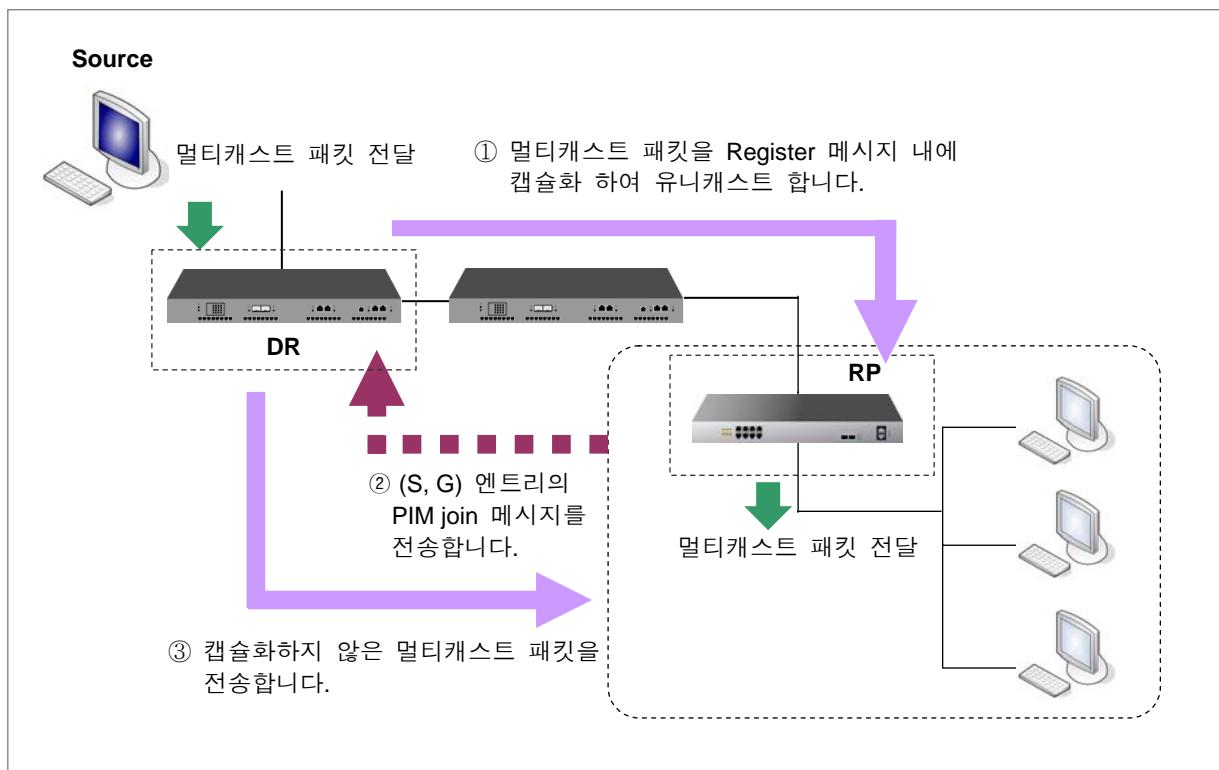
BSR 정보를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip pim bsr-router	Enable/Global/Bridge	BSR 정보를 확인합니다.

9.3.6. Source Registration

멀티캐스트 Source는 멀티캐스트 패킷을 전송할 때 Join 메시지를 보낼 필요가 없습니다. 왜냐하면, 멀티캐스트 Source의 DR이 아무런 정보 없이 Source로부터 멀티캐스트 패킷을 받기 때문입니다. RPT에서도 RP는 최단 경로를 이용하여 Source로부터 멀티캐스트 패킷을 받아, 공유 트리를 이용해 특정 수신자에게 멀티캐스트 패킷을 전달하게 됩니다. 따라서, DR은 RP에게 Source 정보를 제공해야 하며, SPT는 DR과 RP 사이에서 (S, G) 엔트리로 성립되어야 합니다.

다음 그림은 Source Registration이 이루어지는 과정을 나타낸 그림입니다.



【 그림 9-12 】 멀티캐스트 Source Registration

Source Registration은 다음과 같이 이루어집니다. Source로부터 멀티캐스트 패킷을 받으면, DR은 해당 패킷을 캡슐화 한 후에 PIM Register 메시지에 넣어서 지속적으로 RP에 유니캐스트 합니다. 한편, Register 메시지를 받은 RP는 DR과 SPT 구성을 위해서, (S, G) 엔트리의 PIM Join 메시지를 DR로 전송합니다. PIM Join 메시지가 DR에 수신되어 SPT가 구성되면, DR은 캡슐화 과정을 거치지 않은 멀티캐스트 패킷을 RP로 전달합니다. 이렇게 캡슐화 되지 않은 순수한 멀티캐스트 패킷을 받은 후, RP는 Register-stop 메시지를 DR로 보냅니다. 그리고, Register-stop 메시지가 DR에 전송되면 DR은 멀티캐스트 패킷을 캡슐화 하여 Register 메시지에 포함시키는 작업을 중단하게 됩니다.

V5812G를 멀티캐스트 Source측의 DR로 사용할 경우, Source Registration을 위한 세부 설정이 가능합니다. Source Registration을 위한 세부 설정을 하려면 다음 설명을 참조하십시오.

(1) Registration Rate Limit 설정

V5812G는 초당 전송되는 PIM Register 메시지의 최대 개수를 제한할 수 있습니다. 이 기능을 활성화하면, DR과 RP는 최대 개수를 초과하는 PIM Register 메시지를 모두 무시합니다. PIM Register 메시지의 초당 최대 전송 개수를 제한하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim register-rate-limit <1-65535>	Global	PIM Register 메시지의 초당 최대 전송 개수를 제한합니다.



참 고

PIM Register 메시지의 초당 최대 전송 개수는 <1-65,535> 범위에서 설정할 수 있으며, 사용자가 설정한 최대 전송 개수를 초과하여 전송한 PIM Register 메시지는 DR과 RP에서 모두 무시됩니다.

설정한 PIM Register 메시지의 초당 최대 전송 개수를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim register-rate-limit	Global	설정한 PIM Register 메시지의 초당 최대 전송 개수를 해제합니다.

(2) Registration Suppression Time 설정

Source Registration 과정을 통해서 (S, G) 엔트리가 생성됐다면, 해당 엔트리 상태를 유지하기 위해 정적으로 Registration 확인이 이루어져야 합니다. 최초에 Source Registration이 이루어지면 DR은 정기적으로 캡슐화된 멀티캐스트 패킷을 포함하지 않는 PIM Null-register 메시지를 RP로 전송합니다. 그러면 RP는 Register-stop 메시지로 회신합니다. 만약, 일정한 기간 동안 Null-register 메시지에 대한 회신이 없다면, (S, G) 엔트리는 삭제되고, Source Registration 과정이 다시 시작됩니다. PIM Null-register 메시지의 전송 간격을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim register-suppression <1-65535>	Global	Registration Suppression Time을 이용하여 PIM Null-register 메시지의 전송 간격을 설정합니다.



참 고

Registration Suppression Time은 <1-65,535> 범위에서 설정할 수 있으며 단위는 초(sec)입니다.



참 고

만약, RP에 KAT(Keep Alive Time)이 설정되어 있지 않은 경우, 위 명령어를 이용하여 RP에 Registration Suppression Time을 설정하면 해당 RP에 KAT를 설정한 것과 동일한 효과를 얻을 수 있습니다.

설정한 Registration Suppression Time을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim register-suppression	Global	Registration Suppression Time을 해제합니다.

(3) Register 메시지 Filtering

V5812G는 RP에 지정된 Access-list에 해당하는 멀티캐스트 Source를 필터링 할 수 있습니다. 이 기능을 활성화 하면 특정 Source에서 보낸 PIM Register 메시지를 허용하거나 차단할 수 있습니다. 만약, 허용되지 않은 Source에서 RP에 등록을 요청한다면 RP는 해당 Source에서 보낸 PIM Register 메시지를 폐기합니다. 또한, V5812G는 Access-list에 멀티캐스트 Source와 DR의 IP 주소를 지정할 수 있습니다.

멀티캐스트 Source 필터링 기능을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim accept-register list {<100 - 199> <2000 - 2699> access-list-name}	Global	특정 Access-list에 해당하는 멀티캐스트 Source를 필터링 하는 기능을 설정합니다.



참 고

Access-list는 <100-199> 이내에서 입력할 수 있으며, <2,000-2,699> 이내의 값을 입력하면 확장된 범위의 Access-list를 이용할 수 있습니다.



참 고

위 명령어에 사용하는 Access-list는 **Extended access-list**입니다.

한편, 설정한 멀티캐스트 Source 필터링 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim accept-register	Global	설정한 멀티캐스트 Source 필터링 기능을 해제합니다.

(4) RP Reachability Validation 설정

PIM Source Registration 과정을 위한 RP Reachability Validation을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim register-rp-reachability	Global	RP Reachability Validation을 활성화합니다.



참 고

V5812G의 RP Reachability Validation은 기본적으로 비활성화 되어 있습니다.

설정한 RP Reachability Validation을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim register-rp-reachability	Global	설정한 RP Reachability Validation을 해제합니다.

(5) Register 메시지의 Source Address 설정

기본적으로 PIM Register 메시지의 Source IP 주소는 RP로 가는 경로에 위치한 인터페이스의 IP 주소입니다. 이 주소는 DR에 저장되어 있는 일반적인 라우팅 프로토콜 정보를 이용하여 Learning 하게 됩니다. 하지만, V5812G는 DR로 보낼 PIM Register 메시지의 Source IP 주소를 수동으로 설정할 수 있습니다. 설정한 Source IP 주소는 PIM Register-stop 메시지를 회신받는 주소로 사용됩니다.

PIM Register 메시지의 Source IP 주소를 수동으로 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim register-source <i>{source-address interface-name}</i>	Global	PIM Register 메시지의 Source IP 주소를 설정합니다.

설정한 PIM Register 메시지의 Source IP 주소를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim register-source	Global	설정한 PIM Register 메시지의 Source IP 주소를 해제합니다.

9.3.7. SPT 전환

PIM-SM은 멀티캐스트 트래픽이 SPT로 전달되도록 전환하는 기능을 제공합니다. SPT를 통한 멀티캐스트 패킷의 전송은 최단 경로가 사용됨을 의미합니다. 따라서, RPT를 통한 멀티캐스트 패킷의 전달보다 훨씬 효율적이며, 네트워크 대기 시간(Latency)도 현저하게 줄일 수 있습니다.

V5812G에서 제공하는 SPT 전환 기능은 새로운 표준 권고사항에 따라 네트워크 상의 멀티캐스트 트래픽 대역폭에 관계 없이 동작합니다. 즉, SPT 전환 기능이 활성화되면 Source에서 전송된 멀티캐스트 패킷이 최초로 DR에 도착한 후 곧바로 SPT 전환이 일어나게 됩니다. 반면에, SPT 전환 기능이 비활성화일 경우라면 멀티캐스트 트래픽 대역폭 상태에 상관 없이 SPT 전환은 이루어지지 않습니다.

한편, V5812G는 사용자의 필요에 따라 Access-list를 이용한 멀티캐스트 그룹에만 SPT 전환 기능이 동작하도록 설정할 수 있습니다.

SPT 전환 기능을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim spt-threshold		SPT 전환 기능을 활성화합니다.
ip pim spt-threshold group-list [<1 - 99> <1300 - 1999> access-list-name]	Global	특정 멀티캐스트 그룹에 대해 SPT 전환 기능을 활성화합니다.



참 고

Access-list는 <1-99> 이내에서 입력할 수 있으며, <1,300-1,900> 이내의 값을 입력하면 확장된 범위의 Access-list를 이용할 수 있습니다.



참 고

위 명령어에 사용하는 Access-list는 **Standard access-list**입니다.



참 고

V5812G에는 SPT 전환 기능이 기본적으로 비활성화 되어 있습니다.

SPT 전환 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim spt-threshold		
no ip pim spt-threshold group-list [<1 - 99> <1300 - 1999> access-list-name]	Global	SPT 전환 기능을 해제합니다.

9.3.8. Cisco 라우터와의 호환

(1) Register 메시지 Checksum 설정

멀티캐스트 Source Registration 과정에서, DR은 Source로부터 받은 멀티캐스트 패킷을 캡슐화하여 PIM Register 메시지에 포함시켜 이를 RP로 유니캐스트 합니다. RFC에 명시된 PIM 프로토콜의 표준에 따르면 Register 메시지의 체크섬 영역은 캡슐화된 멀티캐스트 패킷의 데이터 부분을 제외한 나머지 부분입니다.

하지만 Cisco 라우터는 Register 메시지의 체크섬 영역을 데이터 부분을 포함한 메시지 전체로 인식하기 때문에, 표준을 따른 라우터 체크섬 영역과 다릅니다. 하지만, V5812G 이러한 Cisco 라우터와 함께 사용할 수 있도록 체크섬 영역을 확장시킬 수 있습니다.

Cisco 라우터와 호환성을 가질 수 있도록 Register 메시지의 체크섬 영역을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim cisco-register-checksum		Cisco 라우터와 호환성을 가질 수 있도록 Register 메시지의 체크섬 영역을 패킷 전체로 설정합니다.
ip pim cisco-register-checksum group-list {<1 - 99>} <1300 - 1999> access-list-name}	Global	특정 멀티캐스트 그룹에 대해 Cisco 라우터와 호환성을 가질 수 있도록 Register 메시지의 체크섬 영역을 패킷 전체로 설정합니다.



참 고

Access-list는 <1-99> 이내에서 입력할 수 있으며, <1,300-1,900> 이내의 값을 입력하면 확장된 범위의 Access-list를 이용할 수 있습니다.



참 고

위 명령어에 사용하는 Access-list는 **Standard access-list**입니다.

Cisco 라우터와의 호환성을 가질 수 있도록 체크섬 영역을 설정했던 것을 해제하고 다시 RFC 표준에 따르도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim cisco-register-checksum	Global	Cisco 라우터와 호환성을 가질 수 있도록 설정한 체크섬 영역을 해제하고 표준에 따르도록 설정합니다.

(2) Candidate RP 메시지 설정

일부 Cisco의 BSR 같은 경우에는 RFC에 명기된 BSR 표준에 적합하지 않게 구현되어 있기 때문에, 그룹 Prefix 0인 Candidate RP를 수락하지 않습니다. V5812G는 이러한 일부 Cisco BSR과 호환되도록 Candidate RP 메시지의 옵션을 조절할 수 있습니다.

Cisco BSR과 호환성을 갖도록 Candidate RP 메시지의 옵션을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim crp-cisco-prefix	Global	Cisco BSR과 호환성을 갖도록 Candidate RP 메시지의 옵션을 설정합니다.

설정한 Candidate RP 옵션을 해제하고 다시 BSR 표준에 따르도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim crp-cisco-prefix	Global	Cisco BSR과 호환성을 갖도록 설정한 Candidate RP 메시지의 옵션을 해제하고 표준 BSR에 따르도록 합니다.

(3) GenID 옵션 설정

PIM Hello 메시지에는 Generation ID(GenID)가 포함되어 있습니다. GenID는 Hello 메시지가 전송되는 인터페이스를 위해 생성되는 랜덤한 값으로, 인접한 라우터의 리부팅을 신속히 감지할 수 있습니다. 또한, GenID는 해당 인터페이스에서 PIM Forwarding이 최초로 시작되는지, 재시작 되는지 여부에 상관없이 다시 생성됩니다.

예를 들어, GenID를 통해 어떤 인접 라우터가 리부팅 된 것을 감지하면 Bootstrap 메시지 및 Join/Prune 메시지를 갱신하고, RP-set 및 멀티캐스트 전송 상태의 최신 정보를 재빨리 반영하게 됩니다. 결과적으로 해당 라우터는 리부팅으로 인한 초기화 상태에서 신속히 네트워크 구성을 복귀할 수 있습니다.

그러나, Cisco의 라우터 중 일부는 PIM Hello 메시지에 포함된 GenID를 인식하지 못합니다. V5812G는 이러한 Cisco 라우터와 호환성을 갖기 위해 GenID를 무시하는 기능을 제공합니다.

PIM Hello 메시지의 GenID를 무시하도록 설정하려면, 다음 명령어를 사용하십시오

명령어	모 드	기 능
ip pim exclude-genid	Interface	Cisco 라우터와의 호환성을 위해 PIM Hello 메시지의 GenID를 무시합니다.

설정한 GenID 무시 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim exclude-genid	Interface	PIM Hello 메시지의 GenID 무시 기능을 해제하고 다시 인식할 수 있도록 합니다.

9.3.9. PIM Debug

PIM-SM 디버깅 기능을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
debug pim all	Enable	PIM-SM에 대한 모든 정보를 디버깅합니다.
debug pim events		Event 관련된 정보를 디버깅합니다.
debug pim nexthop		Next-hop 통신 정보를 디버깅합니다.
debug pim mib		MIB 정보를 디버깅합니다.
debug pim mfc		MFC 추가, 삭제, 업데이트에 관한 정보를 디버깅합니다.
debug pim nsm		NSM 통신 정보를 디버깅합니다.
debug pim packet [in out]		패킷의 송수신 정보를 디버깅합니다.
debug pim state		모든 FSM의 변화 상태를 디버깅합니다.

PIM-SM 디버깅 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no debug pim { all events nexthop mib mfc nsm packet [in out] state }	Enable	PIM-SM 디버깅 설정을 해제합니다.

한편, PIM-SM timer 디버깅 기능을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
debug pim timer	Enable	PIM-SM timer 디버깅 기능을 활성화합니다.
debug pim timer assert [at]		Assert timer 관련 정보를 디버깅합니다.
debug pim timer bsr [bst crp]		BSR timer 관련 정보를 디버깅합니다. bst 는 Bootstrap timer, crp 는 Candidate RP timer 옵션입니다.
debug pim timer hello [ht nlt tht]		Hello timer 관련 정보를 디버깅합니다. ht 는 Hello timer, nlt 는 Neighbor liveness timer, tht 는 Triggered hello timer 옵션입니다.
debug pim timer joinprune [jt et ppt kat ot]		Join/Prune timer 관련 정보를 디버깅합니다. jt 는 Join timer, et 는 Exipre timer, ppt 는 Prune pending timer, kat 는 Keep alive timer, ot 는 Override timer 옵션입니다.
debug pim timer register [rst]		Register timer 관련 정보를 디버깅합니다.

PIM-SM timer 디버깅 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no debug pim timer	Enable	
no debug pim timer assert [at]		
no debug pim timer bsr [bst crp]		
no debug pim timer hello [ht nlt tht]		PIM-SM timer 디버깅 설정을 해제합니다.
no debug pim timer joinprune [jt et ppt kat ot]		
no debug pim timer register [rst]		

9.3.10. SSM (Source Specific Multicast) 설정

멀티캐스트는 하나의 Source와 여러 호스트 또는 여러 Source와 여러 호스트로 구성된 네트워크에서 사용할 수 있습니다. 이처럼 Source의 개수에 상관 없이 동작하는 멀티캐스트를 ASM(Any Source Multicast)라고 합니다. ASM에서 호스트는 (*, G) 엔트리로 멀티캐스트 그룹에 Join/Leave 합니다. 여기서 *는 어떤 Source를 나타내며, G는 멀티캐스트 그룹을 나타냅니다.

한편, ASM에서는 Source를 특정하는 어떠한 정보도 알 수 없기 때문에 PIM-SM에서 널리 사용되는 RP 메커니즘처럼 Source를 찾아낼 수 있는 프로세스가 필요합니다. 이러한 Source 발견 과정이 ASM의 핵심 기능이라 할 수 있습니다. IPv4에서 멀티캐스트 그룹은 224.0.0.0 ~ 239.255.255.255 (224/4) 범위의 주소를 갖습니다.

한편, SSM(Source Specific Multicast)은 하나의 Source와 여러 호스트로 구성된 멀티캐스트 네트워크에 특히 적합하도록 고안된 멀티캐스트 프로토콜입니다. SSM에서 멀티캐스트 수신자는 (S, G) 트리로 멀티캐스트 패킷을 요청합니다. 여기서 S는 특정 멀티캐스트 Source를 나타내며, G는 멀티캐스트 그룹을 나타냅니다.

ASM과 달리 SSM에서는 멀티캐스트 패킷의 수신을 원하는 호스트가 Source에 대한 정보를 이미 알고 있다고 가정합니다. 따라서, 별도의 Source 발견 과정이 존재하지 않습니다. 즉, SSM에서 각각의 멀티캐스트 수신자는 자체적인 방법으로 멀티캐스트 Source에 대한 정보를 알아내야 합니다. 기본적으로 SSM에 해당하는 멀티캐스트 그룹은 232.0.0.0 ~ 232.255.255.255 (232/8) 범위의 주소를 갖습니다.

(1) PIM SSM 설정

PIM-SSM(PIM-Source Specific Multicast)는 PIM-SM에 포함되는 하위 프로토콜입니다. PIM-SSM에서는 하나의 Source와 여러 호스트가 연결된 경우만 고려하기 때문에, PIM-SM보다 동작 원리가 훨씬 간단합니다. PIM-SSM에서 멀티캐스트 패킷 전송은 SPT를 통해서만 이루어지기 때문에 RP, BSR, 공유 트리, SPT 전환 등의 복잡한 과정이 필요하지 않습니다. 한편, PIM-SSM은 PIM-SM과 동일한 PIM 메시지 포맷을 사용합니다.

V5812G는 멀티캐스트 네트워크의 모든 라우터에 PIM-SM과 IGMP 버전3이 설정되어 있다면 PIM-SSM을 활성화할 수 있습니다. 또한, 사용자의 필요에 따라 RFC 표준에 지정된 기본 SSM 그룹의 IP 주소 범위(232/8)보다 확장된 범위의 SSM 그룹을 설정할 수 있습니다.

PIM-SSM을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip pim ssm default	Global	표준 IP 범위의 SSM 그룹(232/8)에 사용하도록 PIM-SSM을 활성화합니다.
ip pim ssm range {<1 - 99> access-list-name}		특정한 범위의 그룹에 대하여 PIM-SSM을 활성화합니다.

PIM-SSM을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip pim ssm	Global	PIM-SSM을 해제합니다.

(2) Static SSM 맵핑 설정

Static SSM 맵핑은 쉽게 말해서 SSM 서비스를 IGMP 버전 1 과 버전 2 메시지에 지원하는 것입니다. 다시 말하면, 멀티캐스트 호스트는 특정 그룹으로부터 멀티캐스트 트래픽을 받을 수 있으며, 그 출처인 source 또한 설정할 수 있습니다. 사용자는 특정 Source로부터 트래픽을 받기 위해서 해당 source 주소를 지정해야 합니다.

만약 V5812G가 static SSM 맵핑이 활성화되어 있는 상태에서, 호스트로부터 IGMP 버전 1 또는 버전 2 Report 메시지를 받았다면 해당 메시지를 IGMP 버전 3 Report 메시지로 처리하게 됩니다.



참 고

IGMP Proxy는 IGMP 버전 3를 지원하지 않으므로, 인터페이스에 Upstream 또는 Downstream 인터페이스가 설정되어 있다면 Static SSM 맵핑은 활성화 할 수 없습니다.

Static SSM 맵핑을 설정하려면 먼저 SSM 맵핑이 시스템 전체에 활성화되어야 합니다. SSM 맵핑을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp ssm-map enable	Global	표준 IP 범위의 SSM 그룹(232/8)에 사용하도록 PIM-SSM을 활성화합니다.

SSM 맵핑을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp ssm-map enable	Global	표준 IP 범위의 SSM 그룹(232/8)에 사용하도록 PIM-SSM을 활성화합니다.

특정 access list에 따라 멀티캐스트 서버의 Source IP 주소를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp ssm-map static {<1 - 99> <1300-1999> access-list-name} ip-address	Global	특정 Access list에 따라 멀티캐스트 서버의 Source IP 주소를 지정합니다.
no ip igmp ssm-map static {<1 - 99> <1300-1999> access-list-name} ip-address		지정된 멀티캐스트 서버의 Source IP 주소를 삭제합니다.

SSM 맵핑 관련한 설정 및 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip igmp ssm-map [ip-address]	Enable Global Bridge	SSM 맵핑에 대한 설정 정보를 확인합니다.

10. G-PON 설정

PON(Passive Optical Network)이란 광케이블을 이용하여 중소 기업이나 일반 가정에까지 초고속 광 대역서비스를 제공할 수 있는 광 가입자 망 구축 기술의 하나입니다. PON은 하나의 총 대역폭을 여러 가입자들이 공유할 수 있도록 분기가 가능한 트리 형태의 점 대 다점 토플로지를 지원하므로 광 선로 구축 비용이 다른 방식들에 비교하여 적게 소요되며, Outside Plant에서 스플리터와 같은 수동형 장치를 사용하기 때문에 전력 공급 문제를 걱정할 필요가 없습니다. 수동형 광 스플리터(Passive Optical Splitter)를 이용하여 하나의 OLT(Optical Line Terminal)에 DSLAM이나 스위치 등에서 업링크 인터페이스로 사용되는 ONU(Optical Network Unit) 또는 단독으로 사용되는 단말장치인 ONT(Optical Network Termination)가 여러 개 접속할 수 있도록 하는 방식입니다.

PON은 크게 서비스 제공자 쪽에 설치되는 OLT 장비와 가입자 쪽에 설치되는 ONU 및 ONT 장비, 그리고 이 두 가지 장비들을 서로 연결해주는 광 스플리터로 구성됩니다. OLT와 ONU 사이에 위치하는 광 스플리터는 광신호를 분기하기 때문에, 하나의 OLT에 다수의 ONU가 연결되는 P2MP(Point-to-Multipoint) 형태가 됩니다. OLT는 ONU에서 보낸 광신호를 상위장비 또는 네트워크로 전송하고, PON 구간 및 ONU를 제어, 관리하는 역할을 담당합니다. 한편, ONU는 OLT에서 보낸 광신호를 전기신호로 변환하여 가입자 단말기로 전송하고, 가입자 단말기에서 보낸 전기신호를 광 신호로 변환하여 OLT로 전달합니다.

10.1 G-PON 개요

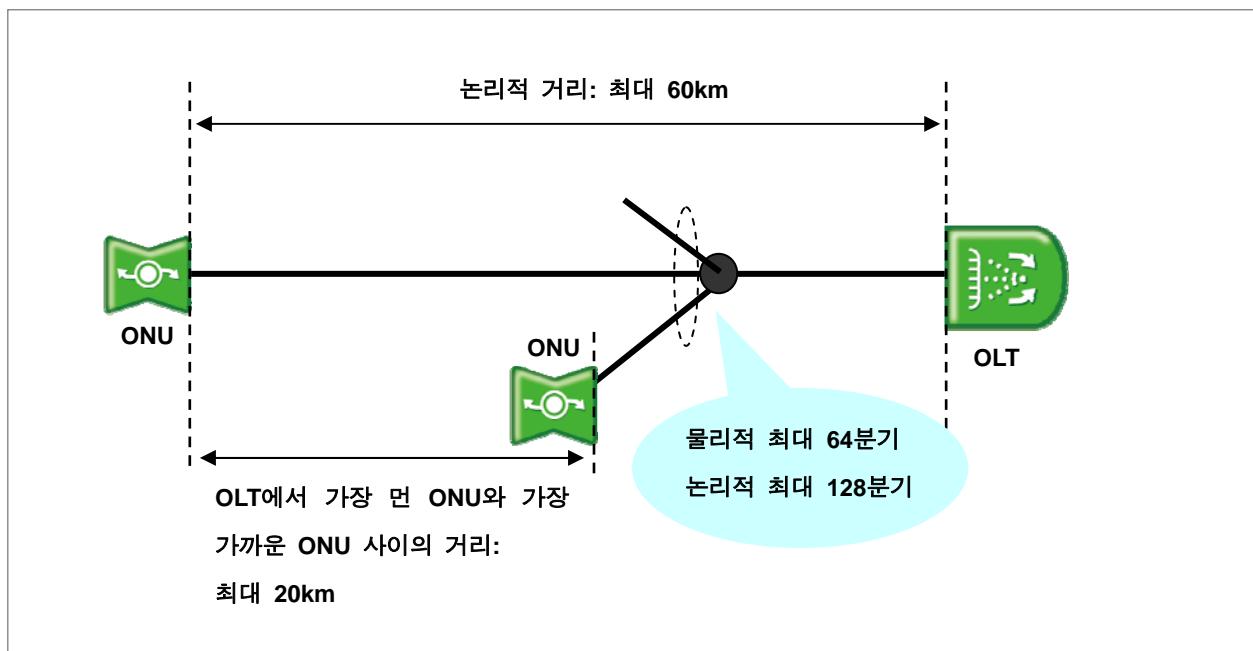
G-PON(Gigabit PON)은 상향 최대 약 1.25G, 하향 최대 약 2.5G의 높은 전송 속도를 지원하며 초고속 인터넷서비스, IPTV, VoIP 등 다양한 멀티미디어 서비스가 가능한 시스템입니다. G-PON은 ITU-T SG15에 의해 표준화가 완료되었으며, 현재 4개의 표준문서로 그 기술이 정의되어 있습니다.

【 표 10-1 】 G-PON 표준 문서의 종류

표준화 기구	표준문서	주요 내용
ITU-T SG15	G 984.1	G-PON 전송 속도, 분기율, 제공 서비스 등 일반적인 규격
	G 984.2	G-PON PMD(Physical Media Dependent) 규격
	G 984.3	G-PON TC(Transmission Convergence) 기능 규격
	G 984.4	G-PON OLT 및 ONT 관리 MIB, 관리 제어 채널 관련 규격

G-PON은 이더넷, TDM 등 멀티 프로토콜을 수용하며 전송대역 하향 1.244Gbps/2.488Gbps와 상향 155Mbps/622Mbps/1.244Gbps/2.488Gbps의 대칭/비대칭 구성 모두 지원합니다. 또한, G-PON은 새롭게 정의된 GEM(G-PON Encapsulation Method) 프레임을 이용해 가변 길이 IP 서비스 및 TDM 서비스를 효율적으로 전송합니다.

G-PON은 하나의 OLT에 다수의 ONU가 연결되는 P2MP(Point-to-Multipoint) 구조를 취하며 ITU-T G984.2 G-PON PMD 규격에 따라 하나의 OLT에 최대 64개의 ONU가 접속할 수 있습니다. 그러나 G-PON TC(Transmission Convergence) 계층에서는 최대 128개의 ONU 접속을 제공합니다. G-PON은 OLT와 ONU 사이에 최대 60Km 논리적 거리와 10Km/20Km의 물리적 거리를 제공하며, ONU간의 거리는 최대 20Km까지 지원합니다.



【 그림 10-1 】 G-PON 시스템 구성도

G-PON은 T-CONT(Traffic Container) 단위로 GEM 서비스를 제공합니다. 하나의 T-CONT는 ONU의 논리적인 큐와 동일한 개념으로 사용되며 5가지 타입으로 제공됩니다. 하나의 ONU는 제공되는 서비스 타입에 따라 다수의 T-CONT로 구성되며, OLT는 ONU내의 T-CONT 단위로 업스트림 전송대역을 할당하고 QoS를 제공합니다.

【 표 10-2 】 T-CONT 타입

타입	서비스	대역제어	설명
1	Fixed BW	Provisioned	예약된 대역폭으로 ONU의 요구에 상관 없이 일정한 주기로 동일한 크기의 대역폭을 할당합니다.
2	Assures BW	Provisioned	보장된 대역폭 범위에서 ONU의 요구에 따라 대역폭을 할당합니다.
3	Assured BW + Non-assured	Dynamic	보장된 대역폭에 대해서는 타입2를 사용하고, 그 이상에서는 타입2에 보장된 대역폭에 비례하여 WRR 방식으로 할당합니다.
4	Best-effort	Dynamic	유효한 대역폭이 존재할 경우 ONU에 요구에 따라 대역폭을 할당합니다.
5	All types	Provisioned + Dynamic	타입 1, 2, 3, 4를 모두 이용해 대역폭을 할당합니다.

10.2 G-PON 설정

V5812G의 G-PON 관련 각종 기능은 Gpon 모드와 Gpon-olt 모드에서 설정할 수 있습니다. Gpon 설정 모드와 Gpon-olt 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어	모드	기능
gpon	Global	G-PON 설정 모드로 들어갑니다.
gpon-olt olt-id	Gpon	G-PON OLT 설정 모드로 들어갑니다.

Global 설정 모드에서 Gpon 설정 모드로 들어가면 시스템 프롬프트가 SWITCH(config)#에서 SWITCH(gpon)#으로 바뀝니다. 또한, Gpon 설정 모드에서 Gpon-olt 설정 모드로 들어가면 시스템 프롬프트가 SWITCH(pon)#에서 SWITCH(config-gpon-olt[olt-id])#로 바뀝니다.

10.2.1. OLT 활성화

OLT를 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모드	기능
gpon-olt olt-id	Gpon	OLT를 활성화합니다.

10.2.2. ONU(ONT) 등록

V5812G에서 개별 ONU(ONT)에 대한 각종 설정은 ONU(ONT) ID를 통해 이루어집니다. 따라서, ONU(ONT)에 설정을 하기 전에 먼저 관리하고자 하는 ONU(ONT)를 등록하고 ID를 부여해야 합니다.

(1) ONU(ONT) 자동 등록

G-PON 네트워크에서 OLT는 ONU(ONT)의 시리얼 넘버 검출을 통해 ONU(ONT)를 발견하고 자동으로 등록할 수 있습니다. 즉, OLT는 주기적으로 네트워크에 연결된 모든 ONU(ONT)에 시리얼 넘버를 요청하고, 새로운 시리얼 넘버가 검출되면 해당 시리얼 넘버를 전송한 ONU(ONT)에 대하여 ONU ID를 부여합니다.

ONU(ONT) 자동 등록 기능을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
discover-serial-number start <1-1200>	Gpon-olt	OLT가 주기적으로 ONU(ONT)의 시리얼 넘버를 확인하여 자동으로 등록하도록 설정합니다.
discover-serial-number stop		설정한 ONU(ONT) 자동 등록 기능을 해제합니다.

ONU(ONT) 자동 등록 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show discover-serial-number interval	Gpon-olt	OLT가 주기적으로 시리얼 넘버를 요청하는 시간 간격을 확인합니다.

(2) ONU(ONT) 수동 등록

수동으로 ONU(ONT)를 등록하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
onu add onu-id serial-number password { enable disable }	Gpon-olt	시리얼 넘버를 이용하여 ONU(ONT)를 수동으로 등록합니다. 동시에 패스워드 auto-learning을 설정합니다.
onu add onu-id mac-address { enable disable }		MAC 주소를 이용하여 ONU(ONT)를 수동으로 등록합니다. 동시에 패스워드 auto-learning을 설정합니다.



참 고

*onu-id*는 <1-127> 범위에서 입력 가능합니다.

수동으로 등록한 ONU(ONT)를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no onu <i>onu-id</i>	Gpon-olt	등록한 ONU(ONT)를 삭제합니다.

(3) ONU(ONT) 등록 상태 변경

자동으로 등록된 ONU(ONT)의 등록 모드 상태를 수동으로 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
onu fix <i>onu-id</i>	Gpon-olt	자동으로 등록된 특정 ONU(ONT)의 등록 모드 상태를 수동으로 변경합니다.
onu fix all		자동으로 등록된 모든 ONU(ONT)의 등록 모드 상태를 수동으로 변경합니다.



참 고

*onu-id*는 <1-127> 범위에서 입력 가능합니다.

10.2.3. ONU(ONT) 펌웨어 관리

(1) 펌웨어 업그레이드

V5812G는 ONU(ONT)의 기능을 향상 시키기 위해서 펌웨어의 업그레이드를 지원합니다. ONU(ONT) 펌웨어를 수동으로 업그레이드 하는 방법은 다음과 같습니다.

1 단계 시스템에 업그레이드할 ONU(ONT)의 펌웨어를 저장합니다.

시스템에 ONU(ONT)의 펌웨어를 저장하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
copy {ftp tftp} onu download	Enable	FTP나 TFTP 서버에서 ONU(ONT)의 펌웨어를 다운받아 저장합니다.

다음과 같이 펌웨어를 다운 받을 서버의 IP 주소, 펌웨어 파일 이름, 사용자 ID, 패스워드를 입력하고 펌웨어를 내려 받습니다.

```
SWITCH# copy ftp onu download
To exit : press Ctrl+D
-----
IP address or name of remote host (FTP): IP 주소
Download File Name : 파일 이름
User Name : 사용자 ID
Password: 패스워드
```

2 단계 시스템에 저장한 펌웨어를 ONU(ONT)에 설치합니다.

ONU(ONT)의 펌웨어 업그레이드를 설정할 경우에는 다음 명령어를 사용하십시오.

명령어	모 드	기 능
onu upgrade <1-64> file-name	Gpon-olt	ONU(ONT)의 펌웨어를 업그레이드 합니다.



참 고

ONU(ONT) 펌웨어의 업그레이드는 장비의 사양에 따라 소요 시간이 달라지지만, 대략 10분 정도의 시간이 요구됩니다.



참 고

ONU 펌웨어 업그레이드가 완료되면 Syslog 메시지로 결과가 출력됩니다.

3 단계 업그레이드한 펌웨어를 활성화시켜 적용합니다.

ONU(ONT) 펌웨어를 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
onu firmware active-change onu-id	Gpon-olt	특정 ONU(ONT)에 업그레이드한 펌웨어를 활성화합니다.
onu firmware active-change all		모든 ONU(ONT)에 업그레이드한 펌웨어를 활성화합니다.



참 고

위의 명령어를 사용하면 ONU(ONT)가 자동으로 재부팅됩니다.

(2) 펌웨어 삭제

ONU(ONT)의 펌웨어를 삭제하는 방법은 다음과 같습니다.

- 1 단계 삭제하려는 펌웨어의 파일명을 확인합니다. 펌웨어의 파일명을 확인하는 명령어는 다음과 같습니다.

명령어	모 드	기 능
show onu firmware-list	Enable/Global/ Gpon/Gpon-olt	시스템에 저장되어 있는 ONU(ONT)의 펌웨어를 확인합니다.

- 2 단계 다음 명령어를 사용하여 펌웨어를 삭제합니다.

명령어	모 드	기 능
remove onu firmware file-name	Gpon	ONU(ONT)의 펌웨어를 삭제합니다.

(3) 펌웨어 정보 확인

시스템에 저장한 ONU(ONT) 펌웨어 리스트를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show onu firmware-list	Enable/Global/ Gpon/Gpon-olt	시스템에 저장한 ONU(ONT) 펌웨어를 확인합니다.

ONU(ONT)의 펌웨어 버전을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show onu firmware version [onu_id]	Gpon-olt	ONU(ONT)의 펌웨어 버전 정보를 확인합니다.

ONU(ONT)의 펌웨어 업그레이드 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show onu upgrade info	Gpon	ONU(ONT)의 펌웨어 업그레이드 정보를 확인합니다.

10.2.4. T-CONT 설정

T-CONT(Traffic Container)는 G-PON 시스템에서 GEM 서비스 제공 단위로 사용되는 것으로, ONU의 논리적인 큐와 동일한 개념으로 사용됩니다. OLT는 ONU(ONT)의 T-CONT 단위로 업스트림 대역폭을 할당합니다. 따라서, ONU(ONT)가 업스트림 대역폭을 할당 받으려면 반드시 T-CONT를 설정해야 합니다. T-CONT는 12비트의 Alloc-ID 정보를 통해 인식됩니다.

T-CONT ID를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
tcont onu-id <256-1023> fixed-bw <512-1031616>	Gpon-olt	ONU에 T-CONT ID를 할당하고 업스트림 대역폭을 고정값으로 설정합니다.
tcont onu-id <256-1023> { sr nsr } fixed-bw assured-bw max-bw		ONU에 T-CONT ID를 할당하고 업스트림 대역폭을 동적으로 할당하도록 설정합니다. SR DBA 모드는 모든 ONU(ONT)가 Queue Occupancy 상태를 OLT에 보고하여 OLT가 동적으로 업스트림 대역폭을 할당합니다. NSR DBA 모드는 옵션은 OLT가 스스로 ONU(ONT)의 트래픽을 모니터링 하여 업스트림 대역폭을 할당합니다.



참 고

fixed-bw는 <128-1031616>, **assured-bw**는 <0-1031616>, **max-bw**는 <128-1031616> 범위에서 입력하십시오.



참 고

max-bw의 설정값은 **fixed-bw**와 **assured-bw**의 값의 합계보다 크거나 같아야 합니다.
 $(max-bw \geq fixed-bw + assured-bw)$



참 고

각 대역폭의 설정 단위는 64kbps입니다.



SR DBA 모드를 사용하려면 먼저 ONU(ONT)가 해당 기능을 지원하는지 확인하십시오. **SR DBA** 모드로 설정하여도 ONU(ONT)가 SR DBA를 지원하지 않으면 내부적으로 **NSR DBA** 모드로 동작합니다.



SR DBA 모드에서 사용하면 OLT는 ONU(ONT)로부터 보고 받은 정보를 참조하여 보다 정확하게 ONU(ONT)의 업스트림 대역폭 사용량을 파악하기 때문에 대역폭을 효율적으로 할당하고 지연(Latency)을 줄일 수 있습니다.

설정한 T-CONT ID를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no tcont onu-id <256-1023>	Gpon-olt	설정한 T-CONT ID를 삭제합니다.

T-CONT 설정 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show tcont-id olt-id [onu-id]	Gpon	T-CONT 설정 내용을 확인합니다.
show tcont [onu-id]	Gpon-olt	

10.2.5. 최대 거리 설정

G-PON 시스템은 OLT와 ONU(ONT) 사이에 최대 60km의 논리적 거리와 10km 또는 20km의 물리적 거리를 제공합니다. V5812G는 OLT와 ONU(ONT) 사이에 최대 거리를 설정할 수 있습니다.

최대 거리를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
olt max-distance { default 30 40 50 60 }	Gpon-olt	OLT와 ONU(ONT) 사이에 최대 거리를 설정합니다.



참 고

각 옵션의 거리 설정값은 다음과 같습니다.

- **default** : 0~20km
- **30** : 10~30km
- **40** : 20~40km
- **50** : 30~50km
- **60** : 40~60km

10.2.6. ONU(ONT) 오류 자동 감지 기능

하나의 OLT와 다수의 ONU(ONT)가 연결된 G-PON 시스템에서 OLT는 DBA(Dynamic Bandwidth Allocation)를 이용해 트래픽량에 따라 각각의 ONU(ONT)에 대한 업스트림 대역폭을 유동적으로 할당합니다. 즉, 실제로 트래픽 교환이 일어나는 ONU(ONT)에 대해 일정한 범위 내에서 보다 많은 대역폭을 할당하여 보다 효율적으로 네트워크 자원을 활용하는 것입니다. 그러나 만약 특정 ONU(ONT)가 광모듈에 문제가 생겨 OLT와의 광신호 통신에 오류가 발생하면 광신호가 계속 켜져 있는 상태가 되고, 이로 인해 다른 ONU(ONT)들이 OLT와 통신을 못하게 되어 원활한 네트워크 서비스가 불가능해지는 문제가 발생할 수 있습니다. 이러한 문제가 발생하는 것을 방지하기 위해 V5812G는 ONU(ONT) 오류 자동 감지 기능을 제공합니다.

ONU(ONT) 오류 자동 감지 기능을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
olt signal-check enable	Gpon-olt	ONU(ONT) 오류 자동 감지 기능을 활성화합니다.
olt signal-check disable		ONU(ONT) 오류 자동 감지 기능을 해제합니다.



참 고

ONU(ONT) 오류 자동 감지 기능을 설정하기 전에 ONU(ONT) 자동 등록 모드를 활성화시키십시오.

한편, ONU(ONT) 오류 자동 감지 기능을 이용하여 오류가 발견될 경우 해당 ONU(ONT)를 자동으로 차단하도록 설정할 수 있습니다.

오류가 발견된 ONU(ONT)를 자동으로 차단하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
olt signal-check auto-onu-block enable		오류가 발견된 ONU(ONT)를 자동으로 차단합니다.
olt signal-check auto-onu-block disable	Gpon-olt	오류가 발견된 ONU(ONT)를 자동으로 차단하도록 설정한 것을 해제합니다.

ONU(ONT) 오류 자동 감지 기능에 대한 설정 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show olt signal-check	Gpon-olt	ONU(ONT) 오류 자동 감지 기능에 대한 설정 내용을 확인합니다.

10.2.7. 재부팅

V5812G의 G-PON 기능 및 다른 소프트웨어의 장애가 발생했을 경우 ONU(ONT)를 재부팅 하여 다시 동작하게 할 수 있습니다. ONU를 재부팅하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
onu reset onu-id	Gpon-olt	ONU(ONT)를 재부팅 합니다.

10.2.8. Security 설정

G-PON은 하향 프레임에 대하여 AES 128Bit 대칭형 암호화 기능을 제공합니다. G-PON G.984.3 표준에서는 PON 링크의 물리적인 특성상 인접 ONU로 전송될 수 없다고 가정하여 상향 프레임에 대한 암호화 기능은 규정하지 않습니다. 암호화 키는 OLT의 요구에 따라 ONU(ONT)가 랜덤으로 생성하여 OLT로 전달하며, 암호화 키의 교환은 PLOAM(Physical Layer OAM)을 이용합니다. PLOAM은 PON 물리계층의 관리 및 프레임부계층의 운용 관리 등의 정보를 전달합니다.

G-PON 암호화 기능을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
onu encryption onu-id enable		ONU(ONT)에 암호화 키를 생성합니다.
onu encryption onu-id disable	Gpon-olt	암호화 기능을 해제합니다.

한편, ONU(ONT)에서 생성된 암호화 키를 교환하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
olt key-exchange start <10-86400>	Gpon-olt	암호화 키를 설정한 시간 간격으로 주기적으로 교환하도록 설정합니다.
olt key-exchange stop		암호화 키 교환 기능을 해제합니다.

암호화 기능 설정 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show onu encryption [onu-id]	Gpon-olt	ONU(ONT) 암호화 키 설정 내용을 확인합니다.
show olt key-exchange		암호화 키 교환 설정 내용을 확인합니다.

10.2.9. FEC 설정

V5812G는 다운스트림 패킷에 대하여 FEC 기능을 설정할 수 있습니다. FEC(Forward Error Correction)은 OLT에서 데이터를 전송할 때 발생한 오류를 검출하고 이를 수정할 수 있도록 Redendancy Bit를 추가하는 기능입니다.

FEC 기능을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
olt fec-mode enable	Gpon-olt	FEC 기능을 활성화합니다.
olt fec-mode disable		FEC 기능을 해제합니다.

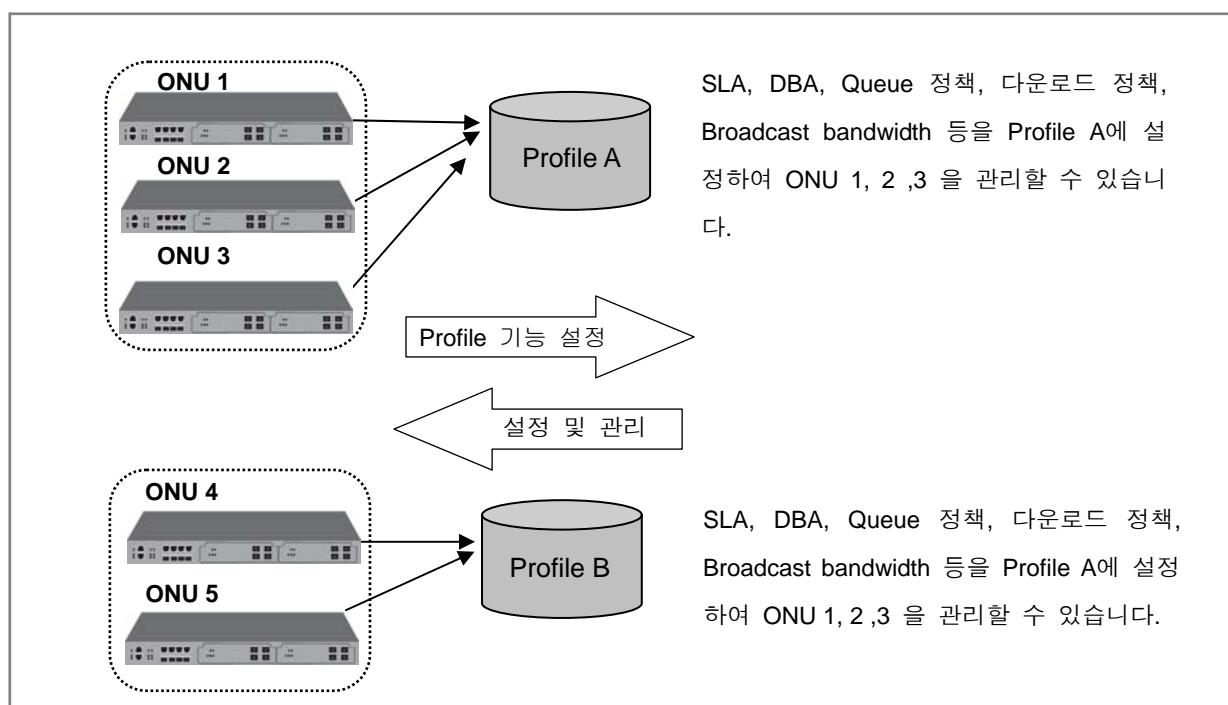
10.2.10. Admin 트래픽 제한 설정

ONU의 Admin 트래픽을 제어하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
onu port-admin onu-id eth uni-port enable	Gpon-olt	ONU의 Admin 트래픽 제어 기능을 활성화합니다.
onu port-admin onu-id eth uni-port disable		ONU의 Admin 트래픽 제어 기능을 해제합니다.

10.3 Profile 설정

Profile이란 ONU(ONT)를 운용하기 위해 필요한 설정 집합으로, 각각의 ONU(ONT)를 하나의 Profile로 설정하여 짧은 시간에 간단히 관리할 수 있는 기능입니다. 따라서 ONU(ONT)마다 개별적으로 설정을 해야 하는 번거로움 없이 해당 ONU(ONT)가 포함되어 있는 Profile을 수정함으로써 ONU(ONT) 각각의 설정값을 변경할 수 있습니다. 다시 말해서, 여러 개의 Profile을 생성하여 특성에 맞는 설정을 한 후, 각각의 ONU(ONT)에서 어떤 Profile을 사용 할 것인지 지정하면 자동으로 설정값이 해당 ONU(ONT)에 반영됩니다. 또한 추후에 각 Profile의 설정값을 변경하게 되면 해당 Profile을 사용하고 있는 ONU(ONT)에 변경된 값이 자동으로 적용됩니다. Profile 기능을 설정하면 사용자의 정책적인 측면 및 서비스 환경에 맞추어 장비를 쉽고 간편하게 관리할 수 있습니다. 다음은 Profile 기능을 알기 쉽게 설명해 놓은 그림입니다.



【 그림 10-2 】 Profile 기능



주의

하나의 Profile을 여러 개의 ONU(ONT)가 공유할 수는 있으나, 하나의 ONU(ONT)는 복수 개의 Profile을 가질 수 없습니다.

10.3.1. Profile의 생성 및 삭제

V5812G는 하나의 Profile 설정을 통해 여러 개의 ONU(ONT)를 관리할 수 있습니다. 다음은 Profile 을 설정하거나 설정 값을 확인하는 방법입니다.



참 고

ONU(ONT)에서 지원하지 않는 기능은 Profile을 설정하여도 적용되지 않습니다. Profile을 설정할 때에는 해당 기능이 적용하고자 하는 ONU(ONT)에서 지원되는 기능인지 확인하시기 바랍니다.

ONU(ONT) Profile을 생성하려면 G-PON 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
onu-profile profile-name create	Gpon	ONU(ONT) Profile을 생성합니다.

위의 명령어를 사용하여 ONU Profile을 생성하면 세부기능을 설정할 수 있는 Onu-profile 설정모드로 들어갑니다. G-PON 설정 모드에서 Onu-profile 설정 모드로 들어가면 시스템 프롬프트가 SWITCH(gpon)#에서 SWITCH(config-onu-profile[profile-name])#으로 바뀝니다.

이미 생성한 ONU(ONT) Profile을 수정할 경우, G-PON 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
onu-profile profile-name modify	Gpon	해당 ONU(ONT) profile을 수정합니다.



참 고

Profile의 설정을 변경하는 경우에는 해당 Profile을 사용하고 있는 ONU(ONT)에 변경된 값이 자동으로 적용됩니다.

생성한 Profile을 삭제할 경우, G-PON 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no onu-profile profile-name	Gpon	생성한 ONU(ONT) Profile을 삭제합니다.

설정된 Profile을 저장할 경우에는 Onu-profile 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
apply	Onu-profile	설정된 Profile을 저장합니다.



주의

apply 명령어를 사용하여 저장하지 않은 내용은 show 명령어를 사용해서 확인할 수 없습니다.

10.3.2. Profile의 설정

(1) 포트 VLAN 설정

G-PON에서 포트 VLAN은 업스트림 트래픽에 대해 적용되며, VLAN 태그는 T-CONT에 매핑됩니다. 포트 VLAN을 생성하고 VLAN 태그 옵션을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
vlan-oper eth uni-port vlan-name <0-7> {keep remove}	Onu-profile	포트 VLAN을 생성하고 VLAN 태그를 유지하거나 제거하도록 설정합니다.
no vlan-oper [eth uni-port]		설정한 포트 VLAN을 삭제합니다.

(2) VLAN 필터링 설정

VLAN 태그 정보에 따른 필터링을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
vlan-filter eth uni-port vlan-name	Onu-profile	VLAN 태그 정보에 따른 필터링을 설정합니다.
no vlan-filter [eth uni-port]		설정한 VLAN 필터링을 삭제합니다.

(3) Rate-limit 설정

V5812G는 ONU(ONT)에 Rate Limit를 설정할 수 있습니다. 이 기능은 특정한 포트가 모든 대역폭을 독점하게 되는 상황을 방지하고 모든 포트가 균등한 대역폭을 사용할 수 있게 할 수 있습니다.

ONU(ONT)에 Rate Limit를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
rate-limit eth uni-port rate	Onu-profile	ONU(ONT)에 Rate Limit를 설정합니다.
no rate-limit [eth uni-port]		설정한 ONU(ONT) Rate Limit를 해제합니다.



rate는 64Kbps 단위로 입력하십시오.

(4) 접속 가능한 사용자수 제한

V5812G는 ONU(ONT) 포트 별로 접속 가능한 MAC 개수를 설정함으로써 사용자 수를 제한할 수 있습니다. 이 때, 사용자는 단순히 네트워크 내에 있는 PC의 개수만 생각하고 접속자 수를 제한하면 안 되며, 네트워크 내에 있는 스위치 등 다른 장비들도 고려하여 설정해야 합니다.

ONU(ONT) 포트 별로 사용자 수를 제한하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
max-host eth uni-port <0-255>	Onu-profile	ONU 포트 별로 접속 가능한 사용자 수를 제한합니다.

포트 별로 사용자 수를 제한한 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no max-host [eth uni-port]	Onu-profile	포트 별로 사용자 수를 제한한 것을 해제합니다.

(5) 패킷 처리 정책 설정

DSCP에 해당하는 패킷을 P bit에 마킹하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
dscp-to-pbit enable	Onu-profile	DSCP에 해당하는 패킷을 P bit에 마킹하도록 설정합니다.
dscp-to-pbit disable		DSCP에 해당하는 패킷을 P bit에 마킹하는 설정을 해제합니다.

10.3.3. Profile 적용

설정한 Profile을 ONU(ONT)에 적용하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
onu-profile onu-id profile-name	Gpon-olt	특정 ONU(ONT)에 적용할 Profile을 지정합니다.

ONU(ONT)에 적용한 Profile을 해제할 경우, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no onu-profile onu-id	Gpon-olt	ONU(ONT)에 적용한 Profile을 해제합니다.

10.3.4. Profile 정보 확인

ONU Profile 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show onu-profile profile-name	Gpon/Onu-profile	ONU Profile 정보를 확인합니다.
show onu-profile onu-list profile-name	Gpon	해당 프로파일이 적용된 ONU(ONT) 리스트를 확인합니다.

10.4 G-PON 정보 확인

10.4.1. OLT MAC 정보 확인

OLT의 MAC 테이블 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show olt mac [olt-id] [onu-id]	Gpon	OLT에 연결된 ONU(ONT)의 MAC 주소를 확인합니다.
show olt mac [onu-id]	Gpon-olt	

OLT MAC 통계 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show olt mac count [olt-id] [onu-id]	Gpon	
show olt mac count [onu-id]	Gpon-olt	MAC 엔트리 통계 정보를 확인합니다.

OLT MAC 정보를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear olt mac [onu-id mac-address vlan-id]	Gpon-olt	OLT MAC 정보를 삭제합니다.

10.4.2. G-PON Slot 상태 확인

V5812G의 G-PON 슬롯 상태를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show gpon slot-status	Gpon	G-PON 슬롯 상태를 확인합니다.

10.4.3. OLT 상태 확인

OLT 상태를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show olt status [olt-id]	Gpon	OLT 상태를 확인합니다.

10.4.4. ONU(ONT) 정보 확인

ONU(ONT) 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show onu info [onu-id]	Gpon-olt	ONU(ONT) 정보를 확인합니다.
show onu active [olt-id]	Gpon	ONU(ONT) 상태 정보를 확인합니다.
show onu active [onu-id]	Gpon-olt	
show onu uni-status [onu-id]		ONU의 UNI 인터페이스 정보를 확인합니다.

10.4.5. 통계 정보 확인

G-PON 통계 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show olt statistics	Gpon-olt	전체 통계 정보를 확인합니다.
show olt statistics alloc-id alloc-id		Alloc-ID 통계 정보를 확인합니다.
show olt statistics onu onu-id		ONU 통계 정보를 확인합니다.

G-PON 통계 정보를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear olt statistics	Gpon-olt	G-PON 통계 정보를 삭제합니다.

10.5 G-PON 디버깅

G-PON 디버깅 기능을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
debug gpon { func device statistics mac profile volatile all }	Gpon	G-PON 기능 및 데이터베이스 정보를 디버깅합니다.
no debug gpon { func device statistics mac profile volatile all }		G-PON 디버깅 기능을 해제합니다.
show debug gpon		G-PON 디버깅 상태를 확인합니다.

11. IP 라우팅 프로토콜 설정

네트워크와 네트워크는 라우터나 Layer 3 스위치와 같은 Layer 3 장비로 연결됩니다. 두 네트워크 간의 통신을 위해서는 Layer 3 장비가 패킷을 목적지까지 올바르게 전달해야 하는데, 이렇게 패킷을 목적지까지 전달하는 것을 라우팅이라고 하고, 패킷을 올바르게 라우팅하기 위해 라우팅 테이블이라는 정보를 사용합니다.

라우팅에는 Static 라우팅과 Dynamic 라우팅의 두 가지 종류가 있습니다. Static 라우팅은 패킷이 지나가는 경로를 하나 하나 고정적으로 지정하여 라우팅 테이블을 만드는 방법인데, 요즘과 같이 네트워크 환경이 거대하고 복잡해진 상황에서는 설정해줘야 하는 라우팅 테이블의 수가 무수히 많기 때문에 시간과 노력을 많이 투자해야 하는 단점이 있습니다. 또한 일부 네트워크의 고장으로 인해 경로를 바꿔야하는 상황에서도 수동으로 바뀐 경로를 다시 설정해야 하는 불편함이 있습니다. 한편, Dynamic 라우팅은 라우팅 프로토콜을 이용하여 자동적으로 라우팅 테이블을 만들고 패킷의 올바르게 라우팅 되도록 하는 방법입니다.

Dynamic 라우팅에 사용되는 라우팅 프로토콜은 라우팅이 이루어지는 범위에 따라 IGP(Interior Gateway Protocol)과 EGP(Exterior Gateway Protocol)로 나뉩니다. IGP는 지역 네트워크 안에서 이루어지는 라우팅을 말하며 EGP는 네트워크와 네트워크 간의 라우팅을 의미합니다. 또한 라우팅의 동작 원리에 따라 RIP(Routing Information Protocol), OSPF(Open Shortest Path First), BGP(Border Gateway Protocol)로 나눌 수 있는데 일반적으로 RIP와 OSPF는 IGP에 사용되고, BGP는 EGP로 사용됩니다.

라우팅 프로토콜과 관련되어 다음의 내용을 설명합니다.

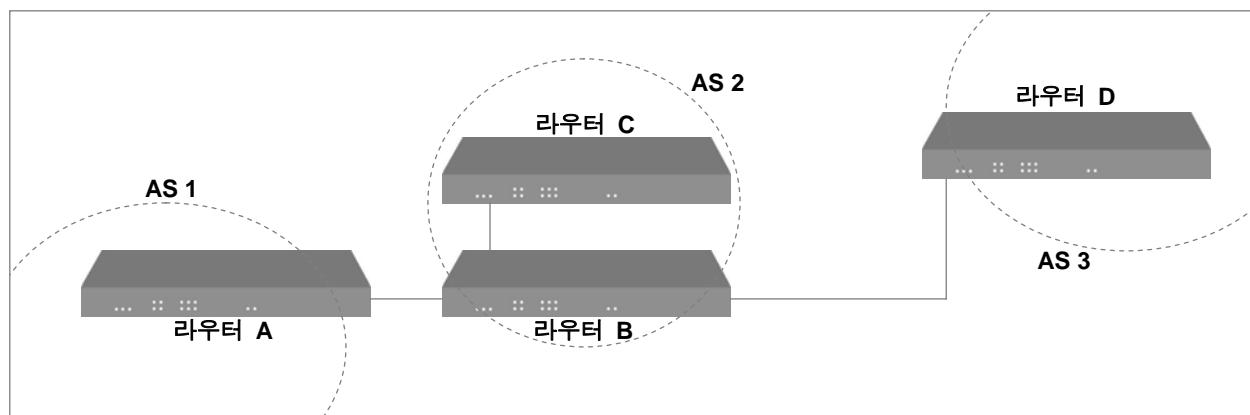
- BGP(Border Gateway Protocol)
- OSPF(Open Shortest Path First)
- RIP(Routing Information Protocol)

11.1 BGP 개요

네트워크 통신의 규모가 점점 더 커지면서 네트워크 장비간의 연결이 복잡해지고, 이에 따라 관리해야 할 라우팅 정보 또한 늘어났습니다. 이에 따라 EGP의 필요성이 대두되었고, 대규모 네트워크에서 적절하게 사용할 수 있는 BGP가 등장하게 되었습니다.

BGP는 AS(Autonomous System)을 단위로 라우팅이 이루어 지는데, AS란, 하나의 네트워크 또는 동일하게 관리가 이루어지는 네트워크 그룹을 의미합니다. BGP는 AS 간의 라우팅에서 사용되는 EBGP(External BGP)와 ISP 사업자 등과 같은 서비스 제공자가 AS 내에서 라우팅 정보를 교환하는데 사용하는 IBGP(Internal BGP)의 두 종류가 있습니다.

아래 【그림 11-1】을 보면서 다시 설명하자면, AS 1과 AS 2와 AS 3간의 통신에 사용되는 BGP는 EBGP이며 AS 2에 있는 라우터 C와 라우터 B간의 통신에 사용되는 BGP는 IBGP가 됩니다.



【그림 11-1】 BGP의 구성원

한편, 라우팅 정보를 주고 받는 인접한 라우터를 Neighbor 라우터라고 합니다. 【그림 11-1】에서 라우터 A의 Neighbor 라우터는 라우터 B가 되고, 라우터 B의 Neighbor 라우터는 라우터 C와 라우터 D가 됩니다.

BGP는 대규모 네트워크 통신을 관리하기 위해 Attribute라고 불리는 수많은 파라미터를 사용하여 라우팅 정책을 정의하고 안정적인 라우팅 환경을 마련합니다. 뿐만 아니라, 네트워크 규모가 큰 만큼 라우팅 테이블의 수도 많아지는데, CIDR(Classless Inter-Domain Routing)를 사용하여 네트워크 정보를 줄임으로써 라우팅 테이블의 규모도 줄일 수 있도록 하였습니다.

BGP의 Neighbor는 Neighbor 간에 최초로 연결이 이루어졌을 때, 모든 라우팅 정보를 주고 받습니다. 그러나, 라우팅 정보가 변경되었을 때에는 변경된 정보만 주고 받게 됩니다. BGP 라우터는 정기적으로 라우팅 테이블을 업데이트하지 않고, 목적지의 네트워크로 가는 최적의 경로에만 라우팅 테이블 업데이트를 알리도록 합니다.

11.1.1. 기본 설정

BGP 라우팅 프로토콜을 설정하여 네트워크 간의 통신을 하도록 하려면, 다음의 설정은 반드시 해야 합니다.

1 단계 BGP 라우팅 프로토콜을 활성화합니다. BGP 라우팅 프로토콜을 활성화할 때에는 반드시 설정하는 AS의 네트워크 주소를 라우팅 테이블에 등록하십시오.

2 단계 BGP 라우팅 프로토콜을 사용하여 통신하게 될 Neighbor 장비를 등록합니다.

(1) BGP 라우팅 프로토콜 활성화

BGP 라우팅 프로토콜을 활성화 하려면, 다음 단계를 따르십시오.

1 단계 BGP를 사용할 장비를 AS로 지정합니다. BGP를 사용할 장비를 AS로 지정하면, 해당 AS의 BGP 설정 모드로 들어갑니다.

다음은 BGP를 사용할 장비를 AS로 지정할 때 사용하는 명령어입니다.

명령어	모 드	기 능
router bgp as-number	Global	지정된 AS의 BGP 라우팅을 활성화 시킵니다.



as-number의 설정 가능 범위는 <1~65,535> 입니다.

2 단계 BGP 라우팅 테이블에 해당 AS의 네트워크를 추가합니다. 다음 명령어를 사용하여 AS의 네트워크를 지정하면, 해당 네트워크가 BGP 라우팅 테이블에 등록됩니다.

명령어	모 드	기 능
network net-address/m	Router	BGP 네트워크를 추가합니다.
network net-address mask netmask		

다음은 BGP를 사용할 장비를 AS로 설정하고 네트워크 주소를 BGP 라우팅 테이블에 등록하는 경우의 예입니다.

```
SWITCH(config)# router bgp 3
SWITCH(config-router)# network 10.1.1.0/24
SWITCH(config-router)# exit
SWITCH(config)# exit
SWITCH# show ip bgp
BGP table version is 0, local router ID is 10.1.1.10
Status codes: s suppressed, d damped, h history, p stale, * valid, > best, i - i
nternal
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop           Metric LocPrf Weight Path
*-> 10.1.1.0/24      0.0.0.0                  32768 i
```

 **추가**

Total number of prefixes 1
SWITCH#

한편, V5812G 스위치의 라우팅을 비활성화 시키려면 다음 단계를 따르십시오.

1 단계 BGP 네트워크를 삭제합니다.

명령어	모 드	기 능
no network net-address/m	Router	BGP 네트워크를 삭제합니다.
no network net-address mask netmask		

2 단계 **exit** 명령어로 Global 설정 모드로 이동합니다.

3 단계 다음 명령어를 사용하여 해당 AS의 BGP 라우팅을 비활성화 시킵니다.

명령어	모 드	기 능
no router bgp as-number	Global	지정된 AS의 BGP 라우팅을 비활성화 시킵니다.

(2) Neighbor 등록

BGP 라우팅 프로토콜을 활성화하였다면 라우팅 정보를 주고 받을 Neighbor를 등록해야 합니다.

BGP 라우팅 프로토콜을 활성화했어도, Neighbor를 등록하지 않으면, 서로 라우팅 정보를 주고 받을 Neighbor 간의 연결 관계를 알지 못하기 때문에 패킷을 라우팅 할 수 없습니다.

BGP Neighbor를 등록하려면, 다음 명령어를 사용하십시오. BGP Neighbor는 IP 주소나 Peer Group 이름으로 설정이 가능합니다.

명령어	모 드	기 능
neighbor {neighbor-ip-address peer-group-name} remote-as remote-as-number	Router	BGP Neighbor를 지정합니다.
no neighbor {neighbor-ip-address peer-group-name} remote-as remote-as-number		BGP Neighbor를 해제합니다.



참 고

Neighbor의 IP 주소는 해당 AS와 연결되는 인터페이스의 IP 주소를 입력합니다.

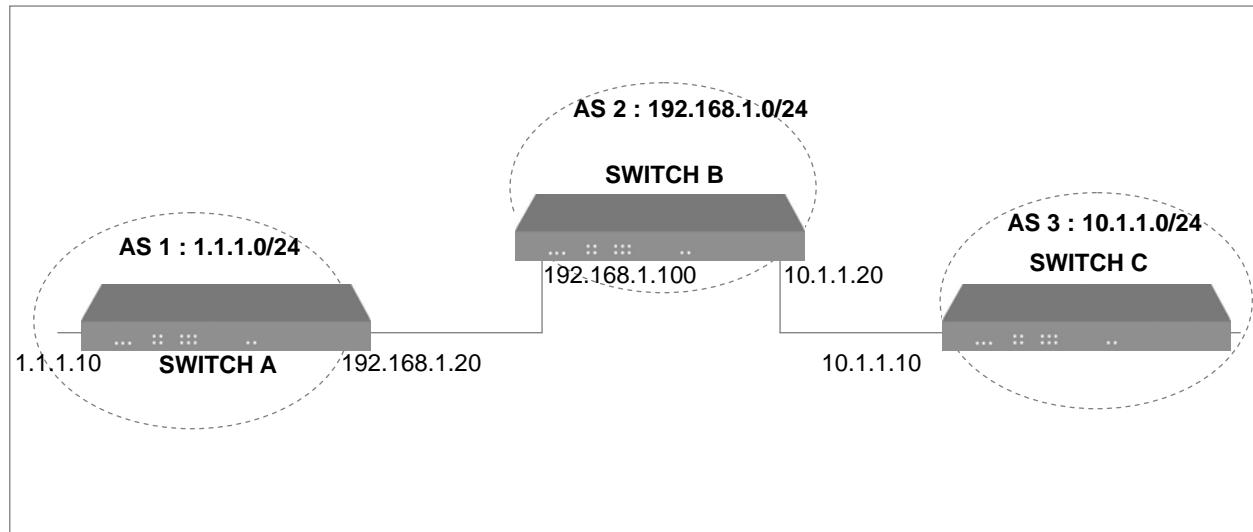


참 고

remote-as-number는 Neighbor가 속해 있는 AS 번호를 입력하십시오.

[설정 예제 1]

다음은 Layer 3 스위치인 V5812G를 사용하여 구성한 네트워크에서 AS1, AS2, AS 3이 BGP 라우팅 프로토콜을 이용하여 라우팅 되도록 설정하는 경우의 기본 설정 예입니다.



< SWITCH A >

SWITCH A는 AS 1로 BGP 라우팅 프로토콜을 활성화하고, 1.1.1.0/24 네트워크 임을 등록해야 합니다. 그리고, SWITCH A의 Neighbor는 192.168.1.0/24 네트워크로 연결되는 SWITCH B이고, AS 1과 연결되는 SWITCH B의 인터페이스는 192.168.1.100/24이므로 해당 IP 주소로 등록합니다. 또한, SWITCH B는 AS 2이므로 Neighbor를 등록할 때 **remote-as**는 2번으로 등록해야 합니다.

```

SWITCH_A# configure terminal
SWITCH_A(config)# router bgp 1
SWITCH_A(config-router)# network 1.1.1.0/24
SWITCH_A(config-router)# neighbor 192.168.1.100 remote-as 2
SWITCH_A(config-router)# exit
SWITCH_A(config)# exit
SWITCH_A# show running-config
(중략)
interface br1
  ip address 1.1.1.10/24
!
interface br2
  ip address 192.168.1.20/24
!
router bgp 1
  network 1.1.1.0/24
  neighbor 192.168.1.100 remote-as 2
!
SWITCH_A#

```

< SWITCH B>

SWITCH B는 AS 2로 BGP 라우팅 프로토콜을 활성화하고, 192.168.1.0/24 네트워크 임을 등록해야 합니다. 그리고, SWITCH B의 Neighbor는 1.1.1.0/24 네트워크로 연결되는 SWITCH A와 10.1.1.0/24 네트워크로 연결되는 SWITCH C인데, SWITCH B와 연결되는 SWITCH A 및 SWITCH C의 인터페이스는 각각 그 주소가 192.168.1.20, 10.1.1.10이므로 해당 IP 주소로 등록합니다. 또한, SWITCH A는 AS 1, SWITCH C는 AS 3이므로 Neighbor를 등록할 때 **remote-as**는 각각 1번, 3번으로 등록합니다.

```
SWITCH_B# configure terminal
SWITCH_B(config)# router bgp 2
SWITCH_B(config-router)# network 192.168.1.0/24
SWITCH_B(config-router)# neighbor 10.1.1.10 remote-as 3
SWITCH_B(config-router)# neighbor 192.168.1.20 remote-as 1
SWITCH_B(config-router)# exit
SWITCH_B(config)# exit
SWITCH_B# show running-config
(종략)
bridge
vlan create 2
!
vlan add default 1-25,27-42 untagged
vlan add br2 26 untagged
!
vlan pvid 1-25,27-42 1
vlan pvid 26 2
!
!
interface noshutdown lo
interface noshutdown default
interface noshutdown br2
!
interface default
ip address 192.168.1.100/24
!
interface br2
ip address 10.1.1.20/24
!
router bgp 2
bgp log-neighbor-changes
bgp network import-check
network 192.168.1.0/24
neighbor 10.1.1.10 remote-as 3
neighbor 192.168.1.20 remote-as 1
!
SWITCH_B#
```

< SWITCH C>

SWITCH C는 AS 3으로 BGP 라우팅 프로토콜을 활성화하고, 10.1.1.0/24 네트워크 임을 등록해야 합니다. 그리고, SWITCH C의 Neighbor는 192.168.1.0/24 네트워크로 연결되는 SWITCH B이고, SWITCH C와 연결되는 SWITCH B의 인터페이스 주소는 10.1.1.20이므로 해당 주소를 등록합니다. 또한, SWITCH B는 AS 20이므로 Neighbor를 등록할 때 **remote-as**는 2번으로 등록합니다.

```
SWITCH_C# configure terminal
SWITCH_C(config)# router bgp 3
SWITCH_C(config-router)# network 10.1.1.0/24
SWITCH_C(config-router)# neighbor 10.1.1.20 remote-as 2
SWITCH_C(config-router)# exit
SWITCH_C(config)# exit
SWITCH_C# show running-config
(종략)
bridge
set hash-algorithm mac-ip-port
!
set vlan pvid 1-16 1
!
set vlan create br1
set vlan add br1 1-16 untagged
!
!
!
!
!
!
!
!
!
!
!
interface noshutdown lo
!
interface noshutdown mgmt
!
interface noshutdown br1
!
interface br1
ip address 10.1.1.10/24
!
!
router bgp 3
network 10.1.1.0/24
neighbor 10.1.1.20 remote-as 2
!
!
!
SWITCH_C#
```

다음은 위와 같이 3개의 AS를 설정하고, 네트워크가 올바르게 연결되었는지 확인한 결과입니다.

SWITCH A와 SWITCH B의 연결 상태 입니다.

```
SWITCH_A# ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) from 192.168.1.20 : 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=0 ttl=64 time=0.4 ms
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=1.0 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.9 ms

--- 192.168.1.100 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.7/1.0 ms
SWITCH_A#
```

SWITCH A와 SWITCH C의 연결 상태 입니다.

```
SWITCH_A# ping 10.1.1.10
PING 10.1.1.10 (10.1.1.10) from 192.168.1.20 : 56(84) bytes of data.
64 bytes from 10.1.1.10: icmp_seq=0 ttl=253 time=0.6 ms
64 bytes from 10.1.1.10: icmp_seq=1 ttl=253 time=1.3 ms
64 bytes from 10.1.1.10: icmp_seq=2 ttl=253 time=1.1 ms

--- 10.1.1.10 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.6/1.0/1.3 ms
SWITCH_A#
```

SWITCH A의 BGP 라우팅 테이블입니다.

```
SWITCH_A# show ip bgp
BGP table version is 0, local router ID is 192.168.1.20
Status codes: s suppressed, d damped, h history, p stale, * valid, > best, i - i
nternal
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop           Metric LocPrf Weight Path
* > 10.1.1.0/24      192.168.1.100            0 2 3 i
* > 192.168.1.0      192.168.1.100            0 2 i

Total number of prefixes 3
SWITCH_A#
```

SWITCH B의 BGP 라우팅 테이블입니다.

```
SWITCH_B# show ip bgp
BGP table version is 109, local router ID is 192.168.1.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop            Metric LocPrf Weight Path
* > 10.1.1.0/24      10.1.1.10          0        0 3 i
* > 192.168.1.0     0.0.0.0           100    32768 i

Total number of prefixes 3
SWITCH_B#
```

SWITCH C의 BGP 라우팅 테이블입니다.

```
SWITCH_C# show ip bgp
BGP table version is 0, local router ID is 10.1.1.10
Status codes: s suppressed, d damped, h history, p stale, * valid, > best, i - i
nternal
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop            Metric LocPrf Weight Path
* > 10.1.1.0/24      0.0.0.0           32768 i
* > 192.168.1.0     10.1.1.20          0 2 i

Total number of prefixes 3
SWITCH_C#
```

11.1.2. IGP와 BGP의 Synchronization

IGP와 BGP가 혼재하는 네트워크 구성에서 IGP 라우터가 IGP 프로토콜을 통해 라우팅 정보를 받기 전에 BGP로부터 라우팅 정보가 전송된다면, 어떤 라우터는 아직 라우팅을 할 수 없는 트래픽을 받게 될 수도 있습니다. 이러한 현상을 막기 위해 BGP는 네트워크에 존재하는 IGP에서 라우팅 정보를 전파할 때까지 기다려야 할 필요가 있습니다. 이와 같이 IGP의 라우팅 정보가 전달되기 전까지 BGP에서 라우팅 정보를 보내지 않고 기다리는 상태를 **Synchronization**이라고 합니다.

어떤 경우에는 Synchronization이 필요 없습니다. 특정 AS에서 다른 AS로 트래픽을 전송할 때 경유하는 AS가 존재하지 않는 경우나 AS에 있는 모든 라우터가 BGP로 동작하는 경우에는 IGP와 BGP간의 Synchronization이 불필요합니다. 불필요한 Synchronization을 해제하면, IGP에서 라우팅 정보가 전달되기까지 기다리지 않기 때문에 BGP로 경로를 수렴하는 것이 더욱 빨라집니다.

BGP와 IGP간의 Synchronization을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
synchronization	Router	BGP와 IGP간의 Synchronization을 활성화합니다.

BGP와 IGP간의 Synchronization을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no synchronization	Router	BGP와 IGP간의 Synchronization을 해제합니다.

11.1.3. 네트워크 Aggregate

네트워크 규모가 거대해지면서 라우팅 경로를 결정하기 위해 주고받는 라우팅 정보 또한 많아지면, 장비가 관리해야 하는 라우팅 테이블의 양이 늘어나기 때문에 부담이 될 수 있습니다. 이러한 문제점을 보완하기 위해 CIDR(Classless Inter-domain Routing)을 사용하여 관리해야 할 라우팅 테이블을 줄일 수 있습니다.

예를 들어, 전형적인 C 클래스의 195.10.x.x를 관리하고 있다면, 195.10.0.x부터 195.10.255.x의 256 개 대역으로 구성될 수 있습니다. 이러한 경우에 CIDR을 사용하지 않는다면 BGP로 연결된 모든 장비가 256개의 대역에 대한 라우팅 정보를 모두 관리하게 됩니다. 그러나, 이 때 CIDR을 사용하면, B 클래스와 동일한 크기인 195.10.x.x 하나의 대역에 대한 경로 정보만 관리할 수 있습니다. 이와 같은 방식을 사용하면 BGP에서 사용되는 라우팅 테이블의 규모가 대대적으로 감소되는 것입니다.

V5812G는 CIDR을 사용하는 방법으로 네트워크 Aggregate 기능을 사용합니다. 이는 위에서 설명한 것과 같이 여러 개의 네트워크 대역을 사용자가 지정한 하나의 네트워크 대역으로 통합하여 라우팅 정보를 관리하게 되는 것입니다.

네트워크 Aggregate를 사용하여 경로 정보를 관리하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
aggregate-address net-address/m	Router	지정한 네트워크 대역에 속할 수 있는 모든 네트워크의 경로 정보를 하나의 통합 네트워크 경로 정보로 관리합니다.

예를 들어, 다음과 같이 설정하면, 10.1.x.x에 속할 수 있는 모든 네트워크 대역의 경로 정보가 10.1.x.x 하나의 네트워크에 대한 경로 정보로 통합되어 사용되는 것입니다.

```
SWITCH_C(config)# router bgp 3
SWITCH_C(config-router)# aggregate-address 10.1.0.0/16
SWITCH_C(config-router)#

```

네트워크 Aggregate 기능을 사용할 때 사용자의 필요에 따라 몇 가지 옵션 기능을 선택할 수 있습니다. 사용자가 선택할 수 있는 옵션 기능은 다음과 같습니다.

1) **as-set** : 네트워크 Aggregate 기능을 적용하여 하나로 통합된 네트워크의 라우팅 정보만 관리하는 것은 동일하지만, 통합된 네트워크에 속하는 모든 AS에 대한 정보를 유지하게 됩니다.

2) **summary-only** : 네트워크 Aggregate 기능을 적용하여 통합된 네트워크에 대한 라우팅 정보만 다른 라우터에 전달하도록 합니다.

명령어	모 드	기 능
aggregate-address net-address/m as-set [summary-only]	Router	네트워크 Aggregate 기능에 선택한 옵션 기능을 추가합니다.
aggregate-address net-address/m summary-only [as-set]		

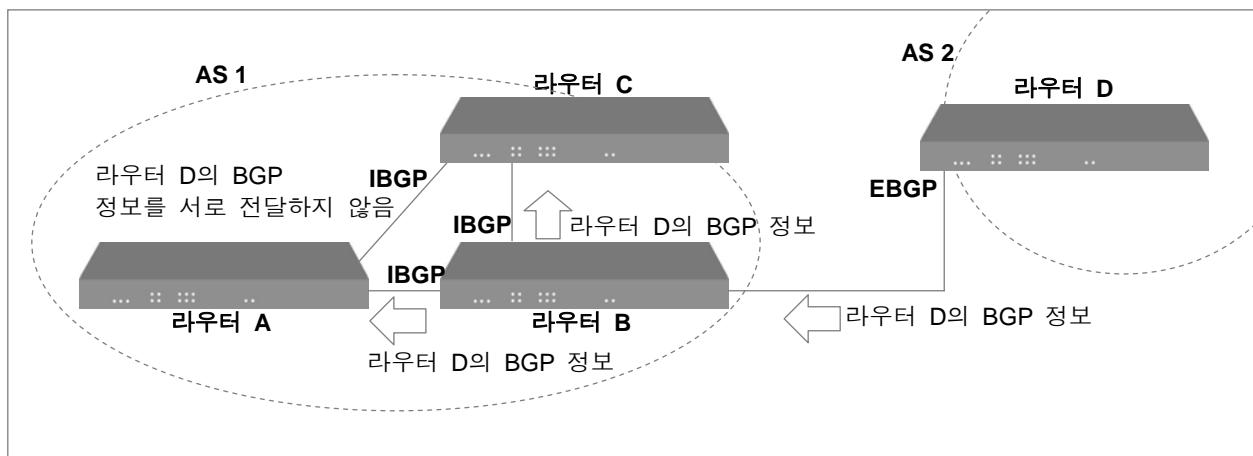
네트워크 Aggregate를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no aggregate-address net-address/m		
no aggregate-address net-address/m as-set [summary-only]	Router	경로 정보 요약 설정을 해제합니다.
no aggregate-address net-address/m summary-only [as-set]		

11.1.4. Route-Reflector

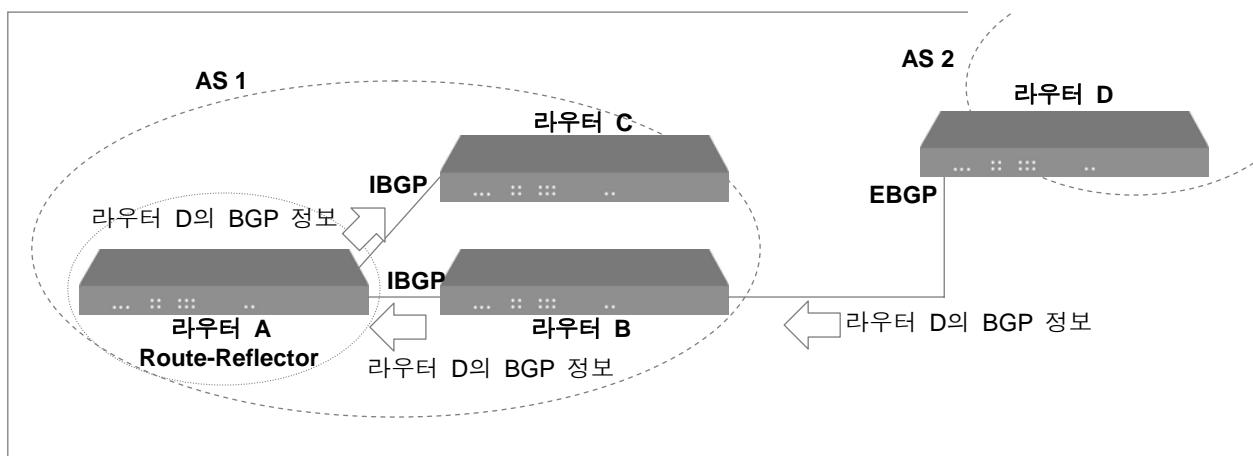
BGP는 주로 규모가 큰 네트워크에서 사용하기 때문에 네트워크에 존재하는 라우터들이 모두 그물처럼 얹혀 있는 Full Mesh 형태로 구성된다면 설정이 매우 복잡해집니다. 이러한 문제점을 보완할 수 있는 방법으로 Router-Reflector를 사용하여 IBGP를 구성하는 것이 있습니다.

BGP 프로토콜은 BGP 라우팅 정보의 루프를 방지하기 위해, EBGP로부터 받은 BGP 정보는 IBGP로 보내지만, IBGP로부터 받은 BGP는 정보는 다른 IBGP로 보내지 않습니다. 예를 들어 아래 그림에서 라우터 D로부터 라우터 B로 전달된 BGP 정보는 라우터 B로부터 라우터 A와 라우터 C에게 전달되지만, 이 정보를 라우터 A와 라우터 C는 서로 전달하지 않습니다.



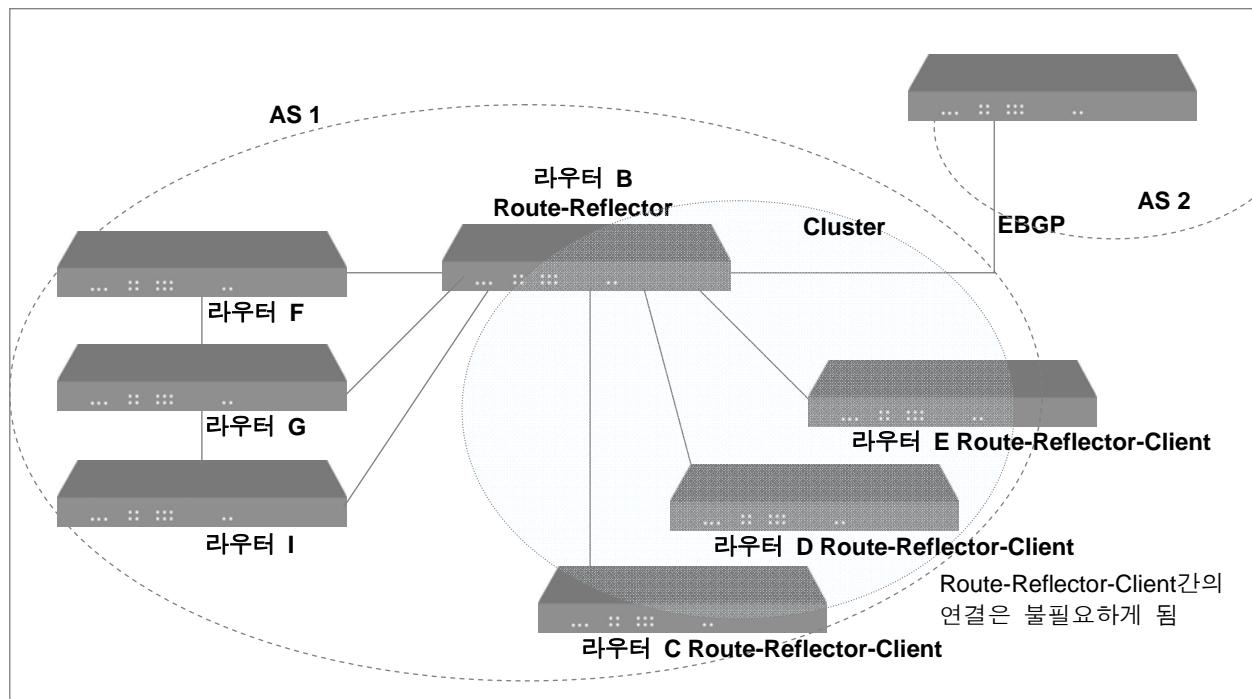
【 그림 11-2 】 Full Mesh IBGP내의 라우팅 정보 전송

Route-Reflector는 Full-Mesh 구조가 아닌 환경에서 IBGP 라우터가 Neighbor에게 BGP 정보를 전달하는 역할을 합니다. 아래 그림을 예로 Route-Reflector의 동작을 간단히 설명하자면, Route-Reflector인 라우터 A는 라우터 B로부터 받은 EBGP 라우터 D의 정보를 라우터 C에게 전달하게 됩니다. 따라서 라우터 B와 라우터 C간의 연결은 필요 없게 되는 것입니다. 이와 같이 Route-Reflector를 사용하면 IBGP간의 불필요한 연결을 줄여 복잡한 구조를 피할 수 있게 됩니다.



【 그림 11-3 】 Route-Reflector를 이용한 BGP 구성예①

Route-Reflector를 중심으로 Full Mesh로 구성될 필요한 없는 IBGP 라우터들은 Route-Reflector-Client로 설정됩니다. 동일한 AS에 속한 IBGP 라우터들 중 Route-Reflector-Client가 아닌 나머지 IBGP 라우터는 Full Mesh 형태로 연결되어야 합니다. Route-Reflector와 Route-Reflector-Client는 Cluster를 형성하게 되고, Route-Reflector-Client는 Cluster 외부의 IBGP 라우터들과 라우팅 정보를 교환하지 않습니다.



【 그림 11-4 】 Route-Reflector를 이용한 BGP 구성예②

Route-Reflector, Route-Reflector-Client가 존재하는 IBGP 네트워크 구성에서 라우팅 정보의 전송은 다음과 같은 규칙을 갖습니다.

- Route-Reflector가 EBGP로부터 받은 라우팅 정보는 Route-Reflector-Client와 Cluster 외부의 IBGP 라우터들에게 전송합니다.
- Route-Reflector가 Cluster 외부의 IBGP 라우터로부터 받은 라우팅 정보는 Route-Reflector-Client에게 전송합니다.
- Route-Reflector가 Route-Reflector-Client로부터 받은 라우팅 정보는 다른 Route-Reflector-Client 와 Cluster 외부의 IBGP 라우터들에게 전송합니다.

Route-Reflector와 Route-Reflector-Client를 설정하려면, 다음 명령어를 사용하십시오. 다음 명령어를 설정하면, Route-Reflector로 설정되면서 지정한 Neighbor가 Route-Reflector-Client로 설정됩니다.

명령어	모 드	기 능
neighbor {neighbor-ip-address peer-group-name} route-reflector-client	Router	Route-Reflector로 설정하면서 특정 Neighbor를 Route-Reflector-Client로 설정합니다.

특정 Neighbor를 Route-Reflector-Client에서 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no neighbor {neighbor-ip-address peer-group-name} route-reflector-client	Router	특정 Neighbor를 Route-Reflector-Client에서 삭제합니다.



참 고

설정된 모든 Route-Reflector-Client를 삭제하면, Route-Reflector의 역할도 없어집니다.

하나의 AS 내에는 여러 개의 Route-Reflector가 설정될 수 있는데, Route-Reflector-Client가 또 다른 Route-Reflector가 될 수도 있습니다. 이러한 다양한 구성이 가능하기 때문에 Backbone 망에는 여러 개의 Cluster가 존재할 수도 있습니다. Route-Reflector와 Route-Reflector는 서로를 단순히 IBGP 라우터로 간주하기 때문에 Full Mesh 형태로 구성되어야 합니다.

한편, 일반적으로 하나의 Cluster에 하나의 Route-Reflector가 존재할 때, Route-Reflector의 Router-ID로 Cluster를 구별하게 됩니다. 그러나, 하나뿐인 Route-Reflector에 문제가 생겨 Cluster 외부와의 라우팅에 문제가 발생하는 것을 막기 위해 2개 이상의 Route-Reflector를 설정한 경우에는 모든 Route-Reflector에 Cluster-ID를 설정하여 동일한 Cluster에 속한 Route-Reflector임을 구분해야 합니다.

Cluster에 여러 개의 Route-Reflector가 존재한다면, 다음 명령어를 사용하여 Cluster-ID를 설정하십시오.

명령어	모 드	기 능
bgp cluster-id <1-4,294,967,295>	Router	Cluster에 여러 개의 Route-Reflector가 존재할 때, Cluster-ID를 설정합니다.

설정한 Cluster-ID를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no bgp cluster-id	Router	Cluster-ID를 삭제합니다.

기본적으로 동일한 Cluster 내에 있는 Route-Reflector-Client들은 Route-Reflector-Client간의 라우팅 정보를 Route-Reflector를 통해 받을 수 있다고 설명하였습니다. 따라서 Route-Reflector-Client들 간에는 Full Mesh 형태로 구성될 필요가 없습니다.

그러나, 만일 Full Mesh로 구성된 Route-Reflector-Client가 존재한다면, 이들은 서로의 라우팅 정보를 Route-Reflector를 통해 전달받을 필요가 없기 때문에 Route-Reflector가 Route-Reflector-Client로부터 받은 라우팅 정보를 다른 Route-Reflector-Client에 전송하는 동작을 해제할 수 있습니다.

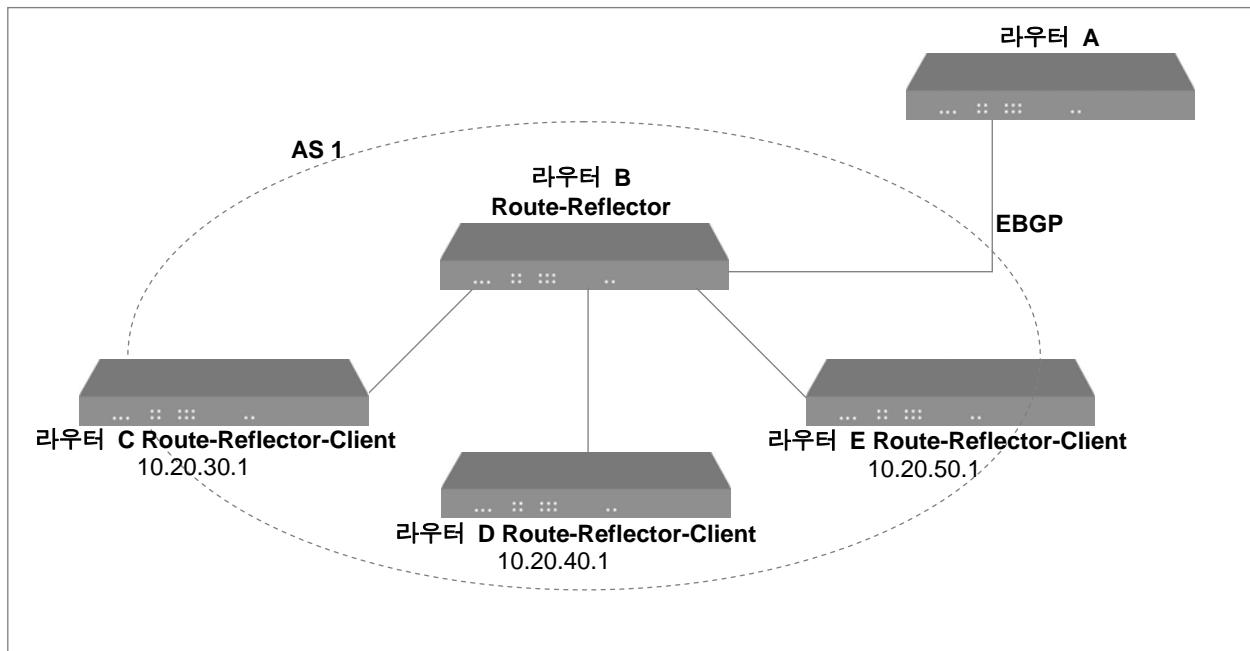
Route-Reflector가 Route-Reflector-Client로부터 받은 라우팅 정보를 다른 Route-Reflector-Client에 전송하는 동작을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no bgp client-to-client reflection	Router	Route-Reflector-Client로부터 받은 라우팅 정보를 다른 Route-Reflector-Client에 전송하는 동작을 해제합니다.

Route-Reflector가 Route-Reflector-Client로부터 받은 라우팅 정보를 다른 Route-Reflector-Client에 전송하는 기본 동작을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp client-to-client reflection	Router	Route-Reflector-Client로부터 받은 라우팅 정보를 다른 Route-Reflector-Client에 전송하는 동작을 활성화합니다.

[설정 예제 1]



위의 그림과 같이 라우터 B를 Route-Reflector로 설정하고 라우터 C, D, E를 Route-Reflector-Client로 설정하려면, 라우터 B에서 다음과 같이 설정하십시오.

```
SWITCH# config terminal
SWITCH(config)# router bgp 1
SWITCH(config-router)# neighbor 10.20.30.1 route-reflector-client
SWITCH(config-router)# neighbor 10.20.40.1 route-reflector-client
SWITCH(config-router)# neighbor 10.20.50.1 route-reflector-client
SWITCH(config-router)#

```

[설정 예제 2]

다음은 Route-Reflector-Client인 3개의 Neighbor가 Full Mesh 형태일 때 Route-Reflector-Client로부터 받은 라우팅 정보를 다른 Route-Reflector-Client에 전송하는 동작을 해제한 경우의 예입니다.

```
SWITCH# config terminal
SWITCH(config)# router bgp 1
SWITCH(config-router)# neighbor 10.24.95.22 route-reflector-client
SWITCH(config-router)# neighbor 10.24.95.23 route-reflector-client
SWITCH(config-router)# neighbor 10.24.95.24 route-reflector-client
SWITCH(config-router)# no bgp client-to-client reflection
SWITCH(config-router)#

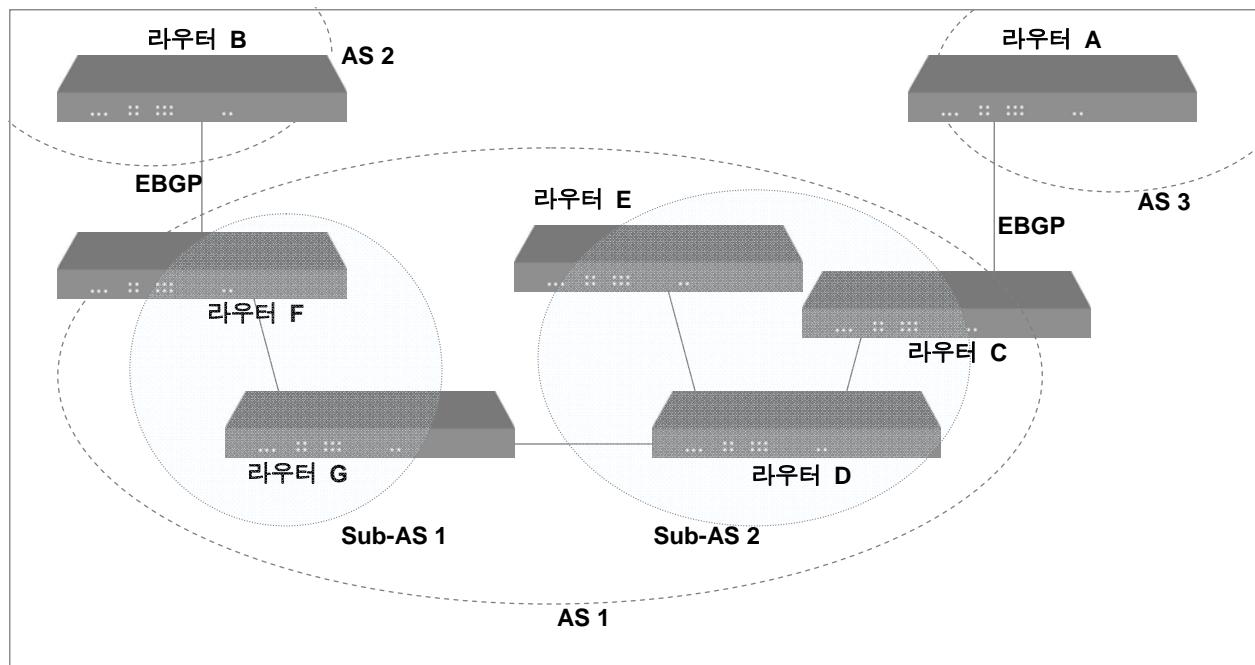
```

Route-Reflector 및 Route-Reflector-Client 설정을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip bgp	Enable/Global	Route-Reflector 및 Route-Reflector-Client 설정을 확인합니다.

11.1.5. Confederation

복잡한 BGP의 네트워크 구성을 줄일 수 있는 또 다른 방법으로 Confederation이 있습니다. Confederation은 동일한 AS내에 있는 IBGP 라우터들을 Sub-AS의 그룹으로 설정하기 때문에 모든 IBGP 라우터들을 각각 연결하는 것보다 복잡하지 않게 구성할 수 있습니다.



【 그림 11-5 】 Confederation을 이용한 BGP 구성

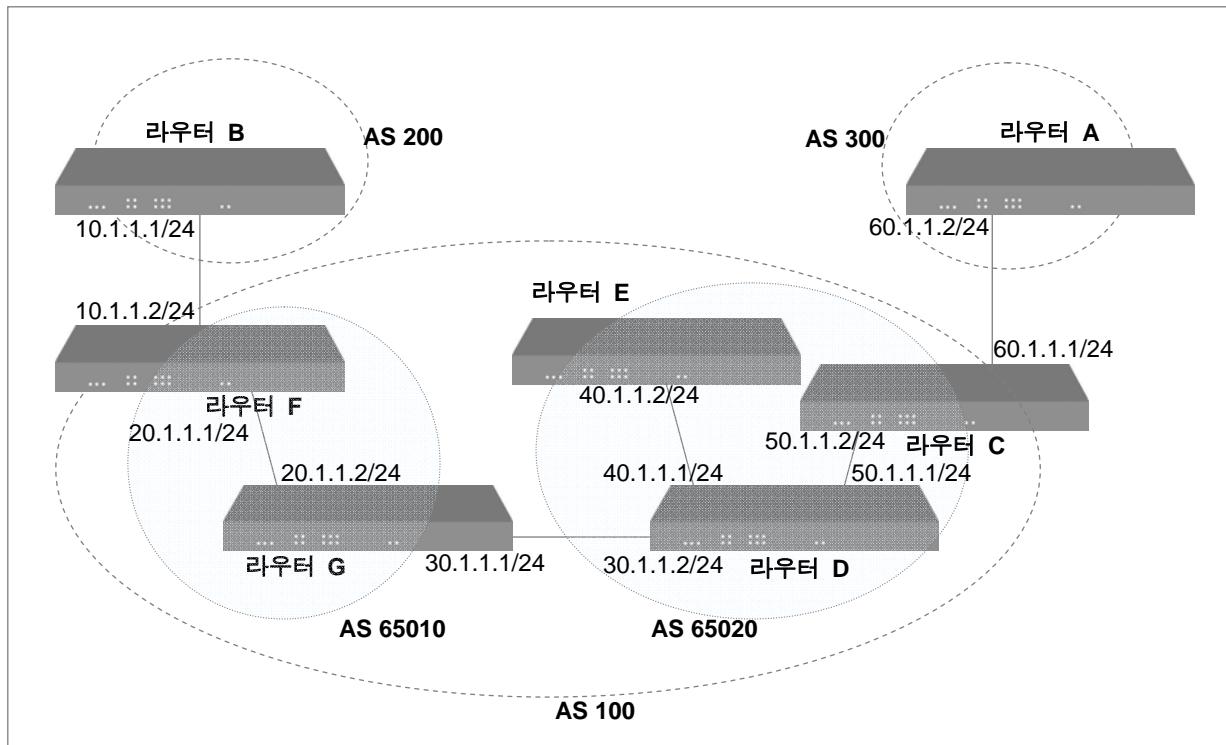
위의 그림을 살펴보면, AS 1의 IBGP 라우터들을 2개의 Sub-AS로 나누어 구성하였습니다. 그렇게 함으로써 AS 1 내부에 있는 IBGP 라우터들의 연결을 간단하게 할 수 있습니다. Sub-AS는 AS 1 내부에서만 의미가 있는 사설 AS입니다. 따라서 AS2나 AS3와 같은 외부 라우터들과 라우팅을 할 때에는 Sub-AS에 속한 라우터가 아닌 AS 1에 속한 라우터가 됩니다. Confederation에서 설정하는 Sub AS, 즉 사설 AS의 AS 번호는 64512번부터 65530번까지 사용합니다. 하지만, 사설 AS는 EBGP 라우터와의 통신에서 자신이 속한 공인 AS로서 구분되어야 합니다. 따라서, 사설 AS를 설정한 후에는 외부에서 구분되는 공인 AS 번호를 설정을 통해 알려주어야 합니다.

사설 AS가 속한 공인 AS를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp confederation identifier <1-65,535>	Router	사설 AS가 속한 공인 AS를 설정합니다.

공인 AS 내에 여러 개의 사설 AS가 존재할 때에는 사설 AS 간의 연결을 알려주어야 합니다. 사설 AS과 연결된 다른 사설 AS를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp confederation peers <1-65,535> [1-65,535]	Router	사설 AS와 연결된 다른 사설 AS를 지정합니다.



다음은 위와 같은 Confederation 구성에서 각 라우터의 설정 중 Confederation 관련 설정입니다.

<Router C>

```
SWITCH# config terminal
SWITCH(config)# router bgp 65020
SWITCH(config-router)# bgp confederation identifier 100
SWITCH(config-router)#

```

<Router D>

```
SWITCH# config terminal
SWITCH(config)# router bgp 65020
SWITCH(config-router)# bgp confederation identifier 100
SWITCH(config-router)# bgp confederation peer 65010
SWITCH(config-router)#+
```

<Router E>

```
SWITCH# config terminal
SWITCH(config)# router bgp 65020
SWITCH(config-router)# bgp confederation identifier 100
SWITCH(config-router)# bgp confederation peer 65010
SWITCH(config-router)#+
```

<Router F>

```
SWITCH# config terminal
SWITCH(config)# router bgp 65010
SWITCH(config-router)# bgp confederation identifier 100
SWITCH(config-router)#+
```

<Router G>

```
SWITCH# config terminal
SWITCH(config)# router bgp 65010
SWITCH(config-router)# bgp confederation identifier 100
SWITCH(config-router)# bgp confederation peer 65020
SWITCH(config-router)#+
```

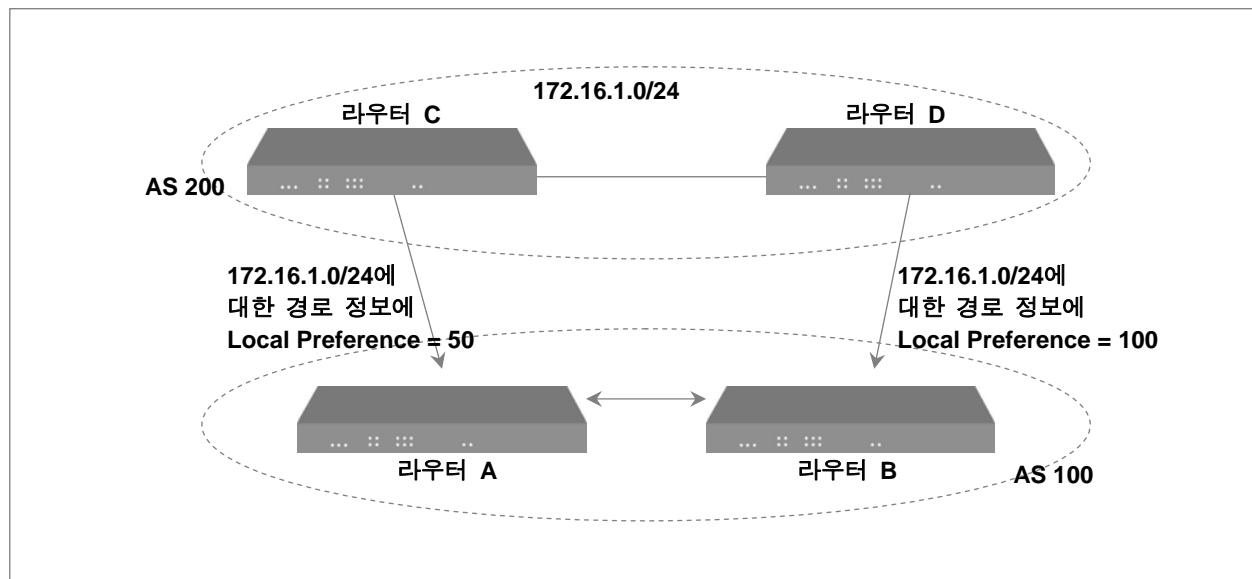
11.1.6. 최적 경로 선택

앞서 설명한 바와 같이 BGP는 효율적으로 경로를 선택하는 기준으로 Attribute라고 하는 경로 파라미터를 사용하게 됩니다. RFC 1771에 정의되어 있는 Attribute에는 다음과 같은 종류가 있습니다.

◆ Local Preference

Local Preference는 Local AS에서 외부 AS로 가는 출구 역할을 하는 경로로 어떤 경로를 사용하면 좋을지를 결정해줍니다. Local Preference는 높은 값을 가질수록 우선 순위가 높습니다.

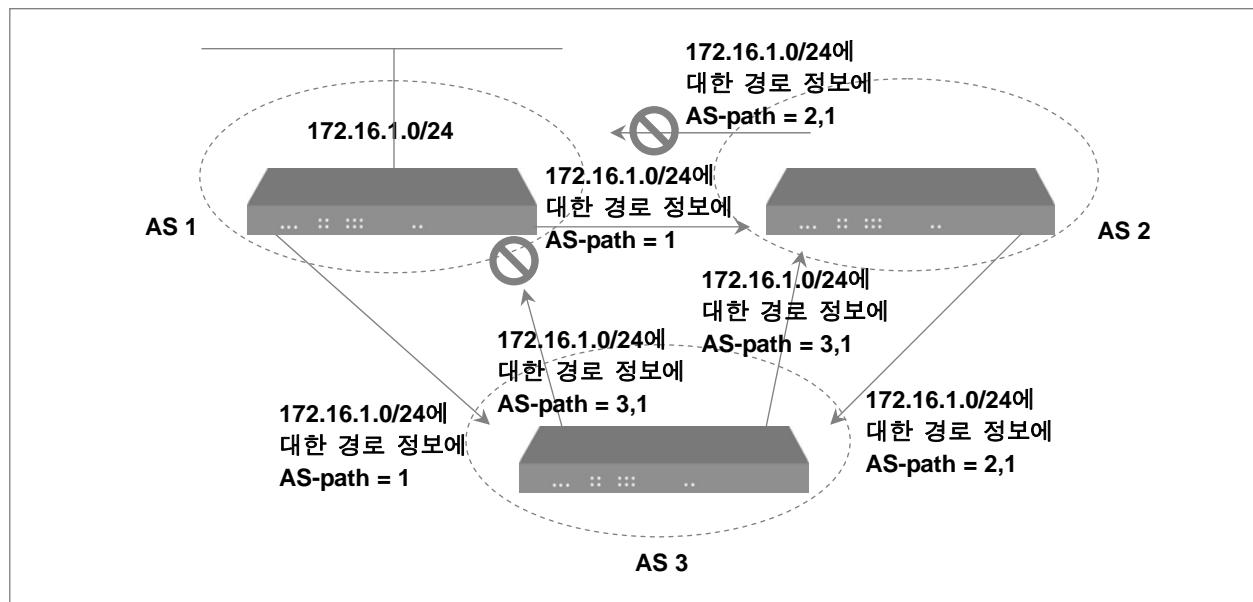
아래 그림에서 AS 100은 AS 200으로부터 172.16.1.0 네트워크에 대해 2개의 정보를 받게 됩니다. 라우터 A가 172.16.1.0에 대한 정보를 받을 때 Local Preference가 50이고, 라우터 B가 172.16.1.0에 대한 정보를 받을 때 Local Preference가 100라고 가정합니다. 그러면, 라우터 A와 B 사이에서 Local Preference가 비교되고, Local Preference가 더 높은 라우터 B가 AS 200의 172.16.1.0 네트워크에 도달하는 출구 역할을 하도록 결정됩니다.



【 그림 11-6 】 Local Preference

◆ AS-path

AS-path는 경로 정보를 전달할 때 거치게 된 AS 번호를 추가한 리스트입니다. 아래 그림은 경로가 3개의 AS를 지나가고 있는 경우의 예입니다.



【 그림 11-7 】 AS-path

AS 1은 172.16.1.0으로 가는 경로의 근원이 되고, 이 경로를 AS-path (1)로 AS 2와 AS 3에 알립니다. AS 3은 AS 1에 AS-path (3.1)로 다시 알리고, AS2는 AS1에 AS-path (2.1)로 다시 알립니다. 이 때, AS 1은 라우팅 루프를 방지하기 위해 자신의 AS 번호가 포함된 경로 정보는 받지 않습니다. AS 2와 AS 3은 AS-path (1)에 자신의 AS 번호를 추가한 정보를 서로 전달하고, AS-path (1)을 보낸 AS 1을 통하는 것이 172.16.1.0으로 가는 짧은 경로로 결정됩니다. 이 때 172.16.1.0으로 가는 경로가 결정되었기 때문에 AS 2와 AS 3이 서로 주고 받은 경로는 라우팅 테이블에 등록하지 않습니다.

◆ Origin

Origin은 BGP 경로 정보를 어디로부터 습득하였는지를 알려줍니다. Origin에는 3가지 종류가 있습니다.

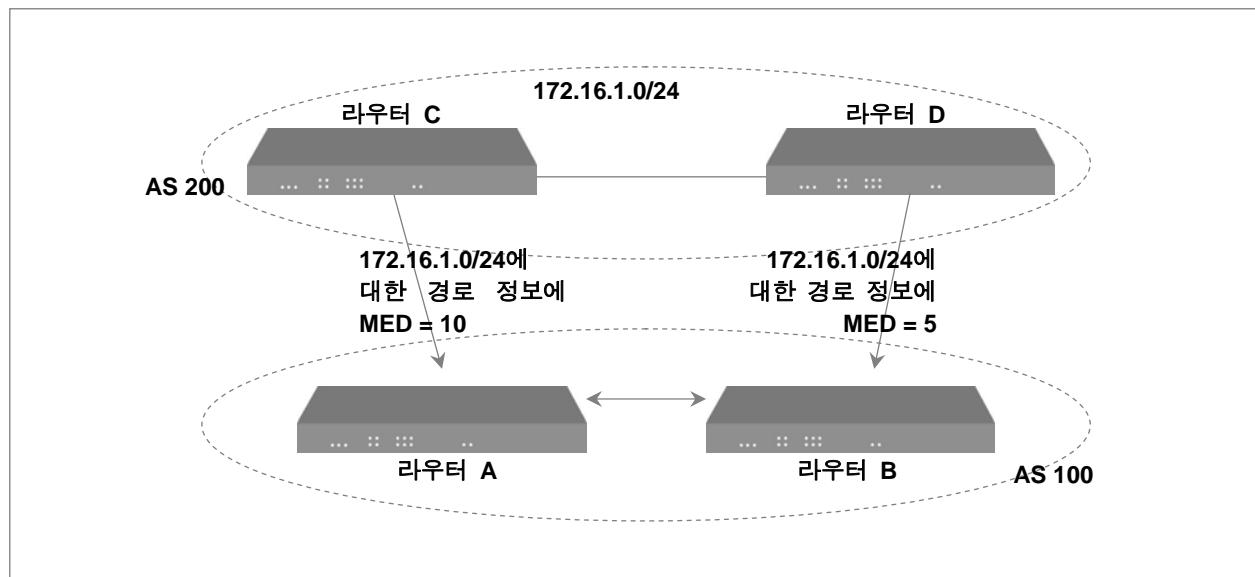
- **IGP** – 경로 정보를 AS 내부로부터 받은 경우입니다.
- **EGP** – 경로 정보를 EBGP로부터 받은 경우입니다.
- **Incomplete** – 경로 정보를 위의 2가지 경우 이외의 방법으로 받은 경우입니다.

Origin은 낮은 값이 우선 순위가 높습니다. Origin은 IGP<EGP<Incomplete입니다. 따라서 Origin의 우선 순위는 IGP>EGP>Incomplete 입니다.

◆ Multi-Exit Discriminator(MED)

Multi-exit discriminator(MED)는 특정 목적지로 가는 경로가 여러 개가 존재할 때, MED가 작은 경로의 우선 순위를 높게 평가하게 됩니다.

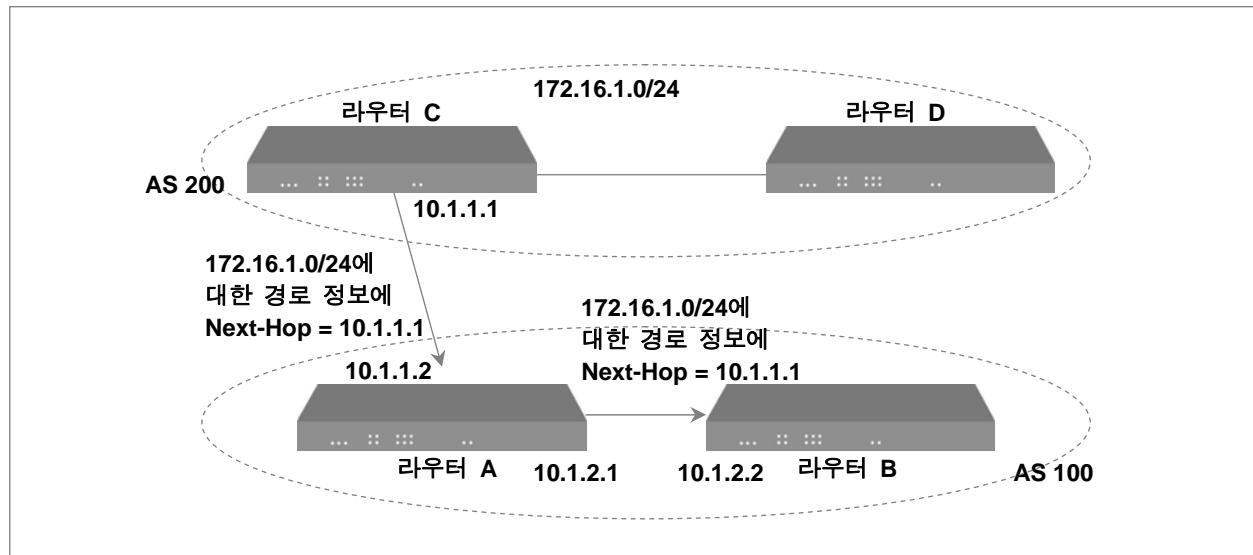
아래 그림에서 라우터 C는 Metric 10과 함께 172.16.1.0 경로 정보를 전송하고, 라우터 D는 Metric 5와 함께 172.16.1.0의 경로 정보를 전달했다고 가정합니다. MED는 낮을수록 우선 순위가 높기 때문에 AS 100은 172.16.1.0으로 가는 경로로 Router D를 선택하게 됩니다.



【 그림 11-8 】 MED

◆ Next-Hop

Next-Hop은 경로 정보를 전달하는 네트워크에 도달할 수 있는 IP 주소입니다.



【 그림 11-9 】 Next-Hop

위의 그림에서 라우터 C가 라우터 A에게 전달한 172.16.1.0/24의 경로 정보에 Next-Hop은 10.1.1.1이 됩니다. 그리고, 라우터 A가 라우터 B에 172.16.1.0/24에 대한 경로 정보를 전달할 때 Next-Hop은 10.1.1.1으로 유지됩니다. 이 때, 라우터 B가 10.1.1.1에 대한 경로 정보를 가지고 있지 않아서 도달하라 수 없는 네트워크라면, 이 경로는 무시됩니다.

◆ Community

Community는 특정 네트워크를 Community라고 하는 그룹으로 지정하여 Community로 가는 경로에 대한 정보를 알려줍니다. Community에 속한 네트워크는 Community에서 지정한 정보를 공유하게 됩니다. 또한, Community에는 No-export, No-advertise, Internet이라는 3가지 특성을 가질 수 있습니다. 각 특성은 다음과 같습니다.

- **No-export** : 이 경로는 EBGP Peer들에게 알리지 않습니다. AS 1가 AS 2에게 전달한 경로 정보에 No-export라는 Community가 포함되어 있으면 해당 경로를 AS 2 내부에서만 전달하고 외부 AS에는 전달하지 않습니다.

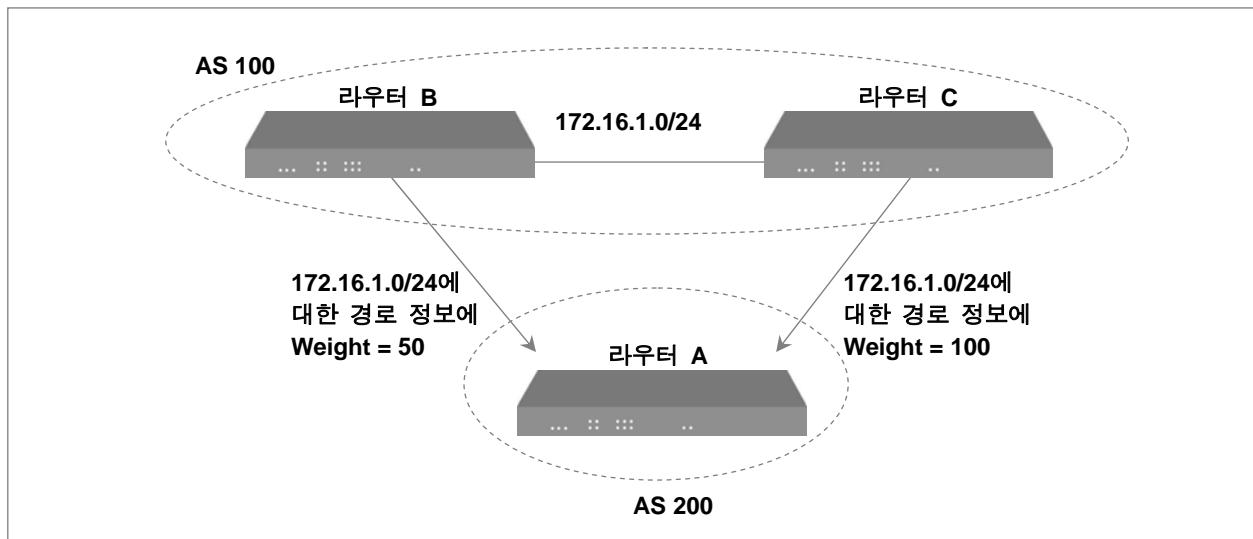
- **No-advertise** : 이 경로는 어떤 Peer에도 알리지 않습니다. AS 1가 AS 2에게 전달한 경로 정보에 No-advertise라는 Community가 포함되어 있으면 해당 경로를 외부 AS는 물론 AS 2 내부의 다른 라우터에게도 전달하지 않습니다.
- **Internet** : 이 경로는 제한 없이 네트워크 안에 존재하는 모든 라우터에게 알립니다. AS 1가 AS 2에게 전달한 경로 정보에 Internet이라는 Community가 포함되어 있으면 해당 경로를 모든 라우터에게 전달합니다.

한편, V5812G의 BGP는 Cisco에서 정의한 고유 Attribute인 Weight를 사용합니다. Weight는 Cisco 고유의 Attribute인 만큼 일반적인 BGP에 모두 적용되는 것이 아니니 주의바랍니다.

◆ Weight

Weight는 Cisco에서 정의한 것으로 동일한 목적지에 대한 경로 정보가 여러 개 있을 때 Weight가 높은 경로가 최적의 경로로 선택됩니다. Weight는 Neighbor에게 전달하는 것이 아니라 Weight 값이 설정된 라우터에서만 적용됩니다.

아래 그림에서 라우터 A는 172.16.1.0라는 네트워크에 대해 라우터 B와 라우터 C로부터 경로 정보를 전달받습니다. 라우터 A가 라우터 B로부터 경로 정보를 받을 때, 서로의 Weight는 50으로 설정되고, 라우터 C로부터 경로 정보를 받을 때 Wight가 100으로 설정되었다면, Wight가 높은 경로가 IP 라우팅 테이블에 생성 되는 것입니다. 라우터 A는 Weight에 대한 정보를 내부에 있는 어떤 라우터에게도 전달하지 않습니다.



【 그림 11-10 】 Weight

BGP는 위에서 설명한 Attribute 등을 사용하여 최적의 경로를 선택합니다. BGP에서 최적의 경로가 선택될 때에는 다음의 원리가 적용됩니다.

1. 접근이 가능한 Next-Hop은 최적의 경로가 선택됩니다. 만일 Next-Hop이 도달할 수 없는 경로라면 해당 경로 정보는 무시됩니다.
2. Next-Hop이 도달할 수 없는 경로라면, 그 다음으로 Weight가 높은 경로를 선택합니다.



Weight는 Cisco 고유의 Attribute입니다.

3. Weight가 같다면, Local preference가 높은 경로를 선택합니다.
4. Local preference가 같다면, 경로의 근원지로부터 전달된 경로를 경로를 우선으로 합니다.
5. 경로의 근원지로부터 전달된 경로가 없다면, AS-path가 짧은 경로를 우선으로 합니다.
6. AS-path가 같다면, Origin이 낮은 경로를 우선으로 합니다.(IGP<EGP<incomplete)
7. Origin이 같다면, MED가 낮은 경로를 우선으로 합니다.
8. MED가 같다면, IBGP 경로보다 EBGP 경로를 우선으로 합니다.
9. 8번에 대한 결과가 동일할 때, 가까운 IGP의 Neighbor에서 제공된 경로를 우선으로 합니다.
한편, 경로 정보가 모두 EBGP 경로일 경우에는 먼저 받은 경로를 우선시합니다.
10. BGP Router-ID로 지정되는 IP 주소가 가장 낮은 경로를 우선으로 합니다.

BGP는 위에서 설명한 원리를 사용하여 최적의 경로를 선택합니다. 이 원리를 바탕으로 네트워크 환경에 따라 발생할 수 있는 여러 가지 경우에 따라 사용자가 적절하게 설정해줘야 할 부분들이 있습니다. 최적 경로 선택과 관련된 설정에는 다음과 같은 내용이 있습니다.

(1) Next-Hop Address Tracking

BGP는 RIB(Routing Information Base)에 등록된 경로들의 상태를 모니터링하고 Next-Hop의 변화를 알려주기 위한 Next-Hop Address Tracking 기능을 지원합니다. 이 기능은 Next-Hop의 변화에 재빠르게 대응함으로써 BGP 네트워크 전체의 경로 선택에 걸리는 시간을 줄일 수 있도록 도와줍니다.

Next-Hop Address Tracking은 기본적으로 활성화되어 있어 BGP Session이 연결되면 자동으로 동작합니다. 그런데, 이러한 모니터링이 동작하는 동안 IGP가 불안정하거나 네트워크 연결이 끊어진다면 일시적인 형태의 라우팅 루프나 네트워크 불안정의 원인이 될 수 있습니다. 따라서 네트워크가 불안정한 상태에서는 Next-Hop Address Tracking을 해제하는 것이 좋습니다.

Next-Hop Address Tracking을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp nexthop trigger disable	Router	Next-Hop Address Tracking을 해제합니다.

Next-Hop Address Tracking을 다시 재개하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp nexthop trigger enable	Router	Next-Hop Address Tracking을 활성화합니다.

한편, Next-Hop Address Tracking에서 전달한 정보를 받고 IGP에서 파라미터들을 조율한 후 전체 라우팅 테이블이 동작을 시작하기까지의 시간을 설정할 수 있습니다. IGP에서 파라미터의 조율이 빨리 가능한 경우에는 이 시간 간격이 짧아도 상관없지만, IGP 파라미터 조율이 끝나지 않은 채 전체 라우팅 테이블이 동작을 시작하여 IGP Session이 불안정해지면 전체 네트워크에 영향을 미칠 수 있습니다. 따라서, IGP 파라미터 조율 시간에 맞춰 이 시간 간격을 조절하는 것이 바람직합니다. 이 시간 간격을 Next-Hop Address Tracking delay interval이라고 합니다.

Next-Hop Address Tracking delay interval을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp nexthop trigger delay <2-30>	Router	Next-Hop Address Tracking delay interval을 설정합니다.



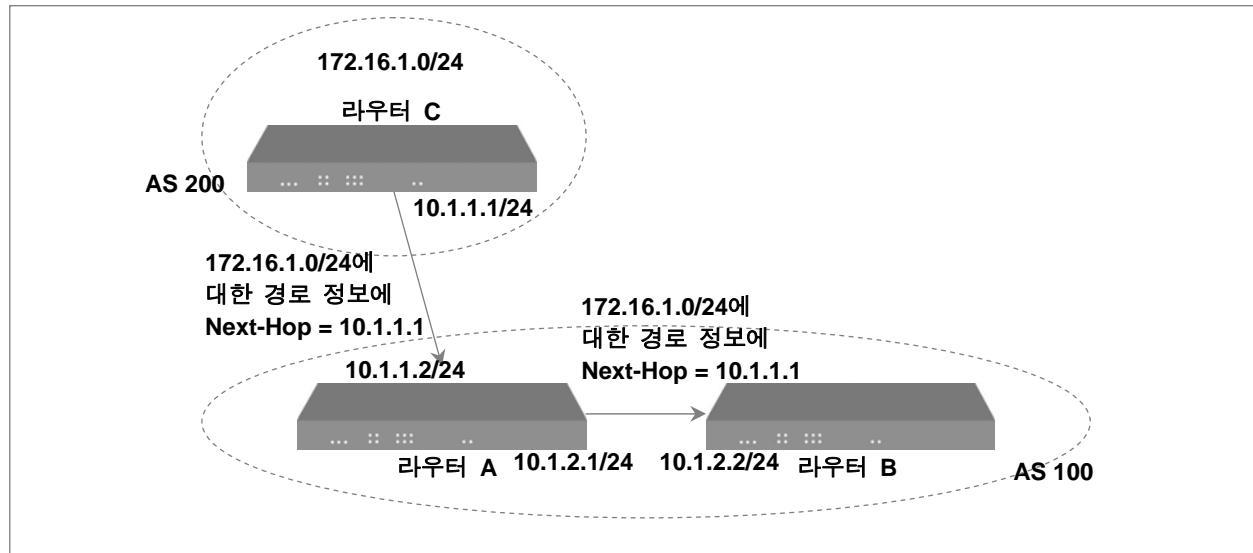
기본적으로 Next-Hop Address Tracking delay Interval은 5초로 설정되어 있습니다.

설정한 Next-Hop Address Tracking delay interval을 삭제하고 기본값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no bgp nexthop trigger delay	Router	설정한 Next-Hop Address Tracking delay interval을 삭제합니다.

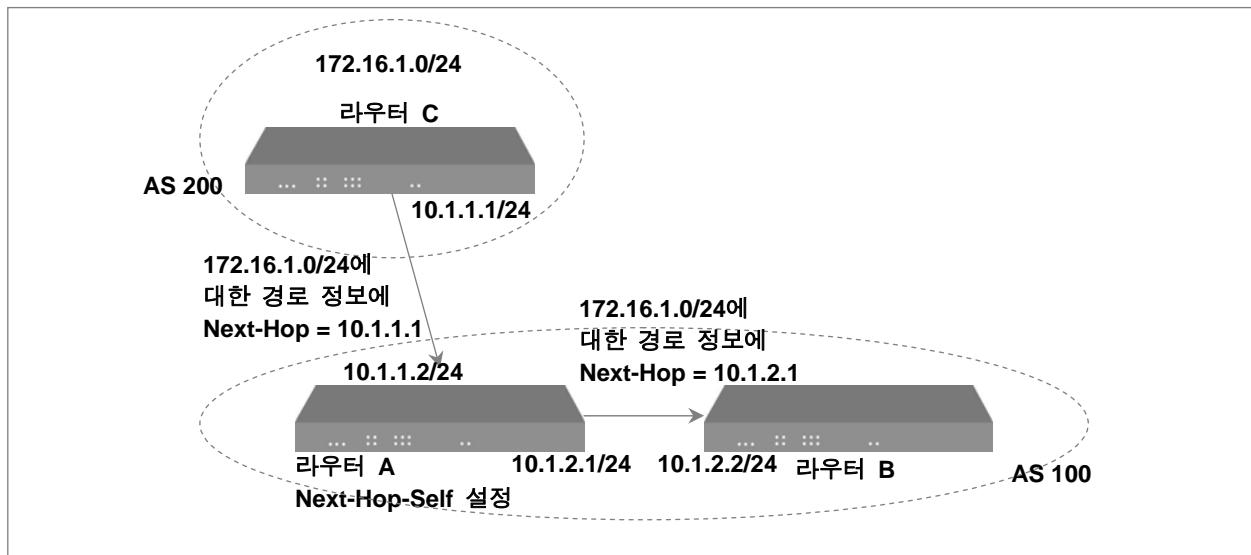
(2) Next-Hop-Self

Next-Hop은 경로 정보를 전달하는 네트워크에 도달할 수 있는 IP 주소를 나타내는 것인데 EBGP에서는 문제가 되지 않지만, IBGP내에서 전달 받은 경로 정보에 도달할 수 없는 주소의 Next-Hop을 포함하고 있는 경우, 해당 경로는 무시하게 되므로 문제가 될 수 있습니다.



【 그림 11-11 】 Next-Hop

위의 그림에서 라우터 B는 라우터 A로부터 172.16.1.0/24 네트워크로 가는 경로 정보를 받을 때 Next-Hop은 10.1.1.1이 됩니다. 그러나, 10.1.1.1은 라우터 B가 직접 도달할 수 없는 네트워크이기 때문에 이 경로를 무시하게 됩니다. 따라서, 이 때 라우터 A는 172.16.1.0/24 네트워크로 가는 경로 정보에 자신의 IP 주소인 10.1.2.1을 Next-Hop으로 포함시켜 라우터 B가 라우터 A를 거쳐 172.16.1.0/24 네트워크에 도달할 수 있도록 해야 합니다. 이러한 기능을 도와 주는 것이 Next-Hop-Self이며, 위의 경우 라우터 A에 Next-Hop-Self를 설정하면, 라우터 B에 라우터 C에서 받은 경로 정보를 전달할 때 자신의 IP 주소를 Next-Hop으로 보내게 됩니다.



【 그림 11-12 】 Next-Hop-Self

Next-Hop-Self를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
neighbor ip-address next-hop-self	Router	특정 라우터에 Next-Hop-Self를 설정합니다.
neighbor peer-group-name next-hop-self	Router	특정 Peer 그룹에 속한 모든 라우터에 Next-Hop-Self를 설정합니다.

Next-Hop-Self를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no neighbor {ip-address peer-group-name} next-hop-self	Router	Next-Hop-Self를 해제합니다.

(3) Local Preference 설정

BGP에서 최적의 경로를 선택할 때 사용하는 Attribute 중 하나인 Local Preference는 특정하게 지정한 값이 없을 경우, 기본적으로 100으로 설정됩니다. 현재 장비에 설정되어 있는 Local Preference를 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp default local-preference <0-4,292,967,295>	Router	장비에 설정되어 있는 Local Preference를 변경합니다.



참 고

기본적으로 Local Preference는 100으로 설정되어 있습니다.

설정한 Local Preference를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no bgp default local-preference [0-4,292,967,295]	Router	장비에 설정한 Local Preference를 삭제합니다.

(4) As-path 비교 생략

BGP에서 최적 경로를 선택하는 과정에서 As-path 비교를 생략하도록 할 수 있습니다. As-path를 비교하는 과정을 생략하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp bestpath as-path ignore	Router	As-path를 비교하는 과정을 생략합니다.

As-path를 비교하는 과정을 생략하도록 설정했던 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no bgp bestpath as-path ignore	Router	As-path 비교 과정을 다시 활성화합니다.

(5) Confederation AS-path 비교

최적 경로를 선택하는 기준으로 Confederation의 AS-path를 비교하도록 설정할 수 있습니다. 그러나, Confederation의 AS-path를 비교하도록 하려면, 먼저 위에서 설명한 명령어를 사용하여 As-path를 고려하지 않고 최적 경로를 계산하도록 설정해야 합니다.



참 고

최적 경로를 선택할 때 Confederation의 AS-path를 비교하도록 설정하려면, **bgp bestpath as-path ignore**를 설정하여 최적 경로 선택 과정에서 AS-path 비교를 생략하도록 해야 합니다.

최적 경로를 선택할 때 Confederation의 AS-path 경로 길이를 고려하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp bestpath compare-confed-aspath	Router	최적 경로 계산 시 Confederation의 AS-path를 고려하도록 설정합니다.
no bgp bestpath compare-confed-aspath		최적 경로 계산에서 Confederation의 AS-path를 고려하지 않습니다.

(6) 외부 AS 경로의 MED 비교 설정

BGP에서 최적의 경로를 선택할 때, 일반적으로 MED의 비교는 동일한 AS내에서 동일한 목적지에 대한 경로 정보의 MED를 비교하여 MED가 낮은 경로를 선택하도록 되어 있습니다. 그러나, 동일한 목적지에 대한 경로 정보라면 다른 AS에 속한 Neighbor가 가진 경로 정보까지 포함하여 모든 경로의 MED를 비교한 후 최적의 경로를 선택하도록 할 수 있습니다.

다른 AS에 속한 Neighbor의 MED도 모두 비교하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp always-compare-med	Router	다른 AS에 속한 Neighbor의 MED도 모두 비교하여 최적의 경로를 선택하도록 설정합니다.
no bgp always-compare-med		다른 AS에 속한 Neighbor의 MED도 모두 비교하여 최적의 경로를 선택하도록 설정한 것을 해제합니다.

(7) AS 그룹별 MED 비교 설정

한편, 다양한 경로 정보를 받았을 때, 동일한 AS의 경로 정보 가운데서 MED를 비교하여 후보 경로를 선출한 후 후보 경로들 가운데서 최적의 경로를 선택하도록 할 수 있습니다. 이러한 방법은 경로 정보를 2개 이상의 AS 그룹으로 분류할 수 있어야 하며 모든 경로 정보가 각각 다른 AS에 속하거나 모든 경로 정보가 하나의 AS에 속한다면 의미가 없습니다. 모든 경로 정보가 각각 다른 AS에 속한다면, **bgp always-compare-med** 명령어를 설정하지 않는 한 MED를 비교하지 않게 되고, 모든 경로 정보가 하나의 AS에 속한다면, 기본적인 MED 비교 방법으로 진행될 것이기 때문입니다.

동일한 AS에 속한 경로 정보들 중에서 MED를 비교하여 후보 경로를 선출한 후 최적의 경로를 선택하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp deterministic-med	Router	동일한 AS에 속한 경로 정보들 중에서 MED를 비교하여 후보 경로를 선출한 후 최적의 경로를 선택하도록 설정합니다.
no bgp deterministic-med		동일한 AS에 속한 경로 정보들 중에서 MED를 비교하여 후보 경로를 선출한 후 최적의 경로를 선택하도록 설정한 것을 해제합니다.



참 고

최적 경로를 선택할 때, AS 경로에 관계없이 MED 값을 비교할 경우는 **bgp always-compare-med** 명령어를, 동일한 AS 정보를 가지는 경로들 가운데 MED 값을 비교할 경우는 **bgp deterministic-med** 명령어를 사용합니다.

(8) Missing-as-Worst

기본적으로 BGP에서 MED를 가지지 않은 경로 정보의 MED는 「0」으로 간주됩니다. 따라서, MED를 비교하는 단계에서 MED를 가지지 않는 경로가 존재한다면, 그 경로가 최적의 경로로 선택되게 됩니다. 이러한 상황을 막기 위해 MED를 가지지 않는 경로를 가장 나쁜 경로로 선택하도록 설정해 줄 수 있습니다.

MED가 없는 경로를 가장 나쁜 경로로 선택하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp bestpath med missing-as-worst	Router	MED가 없는 경로를 가장 나쁜 경로로 선택하도록 설정합니다.
no bgp bestpath med missing-as-worst		MED가 없는 경로를 가장 나쁜 경로로 선택하도록 설정한 것을 해제합니다.

(9) Confederation MED 비교

BGP에 Confederation이 설정되어 있을 때, Confederation에 속한 Peer로부터 받은 경로 정보의 MED를 비교하도록 설정할 수 있습니다. 이러한 경우에는 Confederation에 속하지 않는 AS의 MED는 비교하지 않습니다.

Confederation에 속한 Peer의 MED를 비교하여 최적의 경로를 선택하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp bestpath med confed	Router	Confederation Peer 사이에 교환되는 경로 정보에 대해서 MED 값을 비교하여 최적 경로를 선택하도록 설정합니다.
no bgp bestpath med confed		Confederation Peer 사이에 교환되는 경로 정보에 대해서 MED 값을 비교하여 최적 경로를 선택하도록 설정한 것을 해제합니다.

Confederation Peer 사이에서 교환되는 경로 정보에 대해 MED를 비교할 때, MED가 없는 경로를 가장 나쁜 경로로 판단하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp bestpath med confed		
missing-as-worst		Confederation Peer 사이에서 교환되는 경로 정보에 대해 MED를 비교할 때, MED가 없는 경로를 가장 나쁜 경로로 판단하도록 설정합니다.
bgp bestpath med		
missing-as-worst confed		
no bgp bestpath med		
confed missing-as-worst		Confederation Peer 사이에서 교환되는 경로 정보에 대해 MED를 비교할 때, MED가 없는 경로를 가장 나쁜 경로로 판단하도록 설정한 것을 해제합니다.
no bgp bestpath med		
missing-as-worst confed		

(10) Router-ID 비교 설정

BGP에서 최적의 경로를 선택하는 원리에서 모든 Attribute가 동일한 EBGP의 경로 정보들 가장 먼저 받은 경로 정보를 최적의 경로로 선택하도록 되어 있습니다. 그리고, 만일 이 단계에서도 최적의 경로를 판단하지 못할 때에는 Router-ID를 이용하여 최적의 경로를 선택하도록 되어 있습니다. 그러나, 모든 Attribute가 동일한 EBGP의 경로 정보들 중에서 최적의 경로를 선택할 때 경로 정보를 받은 시점에 대한 비교는 생략하고 Router-ID를 비교하여 최적의 경로를 선택할 수 있습니다.

모든 Attribute가 동일한 EBGP의 경로 정보들 중에서 Router-ID를 비교하여 최적의 경로를 선택하도록 설정하려면, 다음 명령어를 사용하십시오. 단, 이 명령어는 EBGP간의 경로 정보에 대해서만 동작이 가능합니다.

명령어	모 드	기 능
bgp bestpath compare-routerid	Router	라우터 ID를 사용하여 최적의 경로를 계산합니다.
no bgp bestpath compare-routerid		라우터 ID를 사용하여 최적의 경로를 계산하도록 설정한 것을 해제합니다.

11.1.7. Address-Family 설정 모드

BGP 프로토콜은 여러 가지 유형의 IP 주소에 대한 설정을 위한 Address-Family 모드가 있습니다. 현재 V5812G는 IPv4의 유니캐스트와 멀티캐스트 주소 형식, VPNv4의 유니캐스트와 멀티캐스트 주소 형식을 지원합니다. 각 주소 형식을 선택하면 해당하는 Address-Family(AF) 설정 모드로 들어가게 됩니다.

라우팅 세션에서 사용하는 주소 형식을 선택하면서 AF 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
address-family ipv4 [multicast unicast]	Router	IPv4 주소 형식에 대한 AF 설정모드로 진입합니다.
address-family vpnv4 [multicast unicast]		VPNV4 주소 형식에 대한 AF 설정모드로 진입합니다.

AF 설정 모드를 끝내려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
exit-address-family	AF	AF 설정 모드에서 빠져 나옵니다.

11.1.8. Route Dampening

BGP는 네트워크가 불안한 경로의 Advertise를 일정 시간 동안 차단하는 Route Dampening 기능을 지원합니다. 인터페이스의 Link가 down, up을 반복하는 현상을 Flap이라고 하는데 일반적으로 Route Dampening 기능이 활성화되지 않은 상태에서 Flap 현상이 계속되면, Link down이 발생하였을 때에는 경로 삭제 메시지가 전송되고, Link up 상태로 되돌아왔을 때 해당 경로의 Advertise가 재개됩니다. 만일 수 많은 경로가 존재하는 백본 망에서 이러한 현상이 발생한다면, Flap 상태로 인해 서로 주고 받는 수 많은 경로 삭제 메시지와 Advertise가 네트워크 상에 문제를 일으킬 수 있습니다.

이러한 문제를 해결하는 것이 Route Dampening 기능입니다. Route Dampening은 Flap이 발생한 경로에 패널티를 주고 패널티가 누적되어 일정 기준 이상으로 쌓이면, 해당 경로에 대한 Advertise를 차단합니다. 따라서 Flap 상태로 인해 주고 받는 메시지와 Advertise를 줄여 네트워크의 안정화를 유지하도록 합니다.

참 고

Route dampening이 활성화되었을 때 BGP Session Reset에는 패널티가 주어지지 않습니다.

Route Dampening 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp dampening	Router/AF	Dampening을 활성화합니다.

경로에 Flap 상태가 한 번이라도 발생하면 패널티가 주어지면서 BGP 라우팅 테이블에 h(History-state)로 표시됩니다. 그리고, 패널티가 누적되어 장비에 설정되어 있는 기준치를 넘어서면 해당 경로를 Advertise하지 않게 되는 Damp state가 됩니다. 이 때 Damp state로 바뀌게 되는 기준치를 Suppress limit이라고 합니다. Damp state는 Max-suppress-limit로 설정되어 있는 시간 동안만 유지됩니다.

한편, Flap 상태가 해결되면 더 이상 해당 경로의 Advertise를 차단할 필요가 없게 됩니다. Flap이 발생하지 않아서 일정 기간 동안 패널티가 누적되지 않으면, 패널티를 반으로 줄입니다. 이런 식으로 패널티가 줄어드는 것을 보면 Flap의 발생이 없어졌음을 감지할 수 있습니다. 일반적으로 패널티가 추가적으로 누적되었는지를 5초에 한 번씩 확인하고, 장비에 설정되어 있는 Half-life 시간 동안 패널티 누적이 없다면 패널티를 반으로 줄입니다. 이런 식으로 패널티를 줄여 특정 기준 이하로 떨어지면 다시 Advertise를 재개하게 됩니다. Advertise를 재개하는 기준이 되는 값을 Reuse limit라고 합니다. 패널티가 Reuse limit 이하로 떨어졌는지 확인하는 것은 보통 10초마다 한 번씩 실행됩니다.

Route Dampening에서 Suppress-limit, Half-life, Reuse-limit, Max-suppress-limit는 설정이 가능합니다. Route Dampening과 관련된 기준값을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp dampening half-time	Router	Route Dampening에서 Half-life를 설정합니다.
bgp dampening half-time reuse-limit suppress-limit max-suppress-time	/AF	Route Dampening에서 Half-life, Reuse-limit, Suppress-limit, Max-suppress-limit를 설정합니다.



참 고

Half-life는 분(minutes) 단위로 설정하며, 1분부터 45분까지 설정 가능합니다. 기본 설정값은 15분입니다.



Reuse-limit는 1부터 2000까지 설정 가능합니다. 기본 설정값은 750입니다.



SUPPRESS LIMIT는 1부터 2000까지 설정 가능합니다. 기본 설정값은 2000입니다.



MAXIMUM-SUPPRESS-LIMIT는 분(minutes) 단위이며 1분부터 45분까지 설정 가능합니다. 기본 설정값은 Half-life의 4배(15분일 경우 60분)입니다.

Route Dampening과 관련된 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip bgp dampening flap-statistics		경로의 Flap 상태를 확인합니다.
show ip bgp dampening dampened-paths	Enable/Global	Damp 상태의 경로를 확인합니다.
show ip bgp dampening parameters		Route Dampening 관련 설정값을 확인합니다.

BGP 경로 dampening 정보를 초기화하고, Advertise를 중지했던 경로를 다시 전달하도록 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip bgp dampening		BGP 경로 dampening 정보를 초기화합니다.
clear ip bgp dampening [ip-address ip-address/m]	Enable/Global	지정된 네트워크의 BGP 경로 dampening 정보를 초기화합니다.

BGP flap 통계를 초기화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip bgp flap-statistics		BGP flap 통계를 초기화합니다.
clear ip bgp flap-statistics [ip-address ip-address/m]	Enable/Global	지정된 네트워크의 BGP flap 통계를 초기화합니다.

11.1.9. BGP Session Reset

네트워크를 구성하는 BGP 라우터의 라우팅 정책에 변화가 생기면 연결되어 있는 라우터도 새로운 정책이 적용되어야 합니다. 변경된 내용을 적용하기 위해서는 장비간의 연결을 Reset해야 하는데, 장비의 전원을 깼다 켜는 방법은 설정이 변경될 때마다 실현하기도 불가능하고 다른 정보를 잃어버릴 위험이 있기 때문에 좋은 방법이라 할 수 없습니다. 따라서 내부적으로 Session을 Reset하여 경로 정보를 초기화한 후 라우팅 테이블을 새롭게 업데이트 하는 방법을 사용할 수 있습니다.

BGP 라우팅 테이블을 Reset 하기 위해 Session을 Reset하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip bgp *		모든 Peer와의 Session을 Reset 합니다.
clear ip bgp ip-address	Enable	특정 경로에 대한 Session을 Reset 합니다.
clear ip bgp <1-65,535>	/Global	특정 AS에 속한 Neighbor 라우터와의 Session을 Reset 합니다.
clear ip bgp external		외부 Peer에 대한 Session을 Reset 합니다.
clear ip bgp peer-group name		특정 Peer 그룹에 속한 모든 Peer에 대한 Session을 Reset 합니다.



위의 명령어에서 「*」는 라우터와 연결된 모든 BGP Peer를 의미합니다. 따라서, 모든 Peer와의 Session을 Reset합니다.

라우팅 테이블에는 Neighbor로부터 전달되는 Inbound 라우팅 테이블과 Neighbor에게 전달하는 Outbound 라우팅 테이블이 있습니다. 일반적으로 Inbound, Outbound를 구별하지 않으면 라우팅 테이블 전체를 Reset하게 됩니다.

Inbound 또는 Outbound를 구별하여 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip bgp * {in out}	Enable /Global	Inbound 또는 Outbound를 구별하여 모든 Peer와의 Session을 Reset 합니다.
clear ip bgp ip-address {in out}		Inbound 또는 Outbound를 구별하여 특정 경로에 대한 Session을 Reset 합니다.
clear ip bgp <1-65,535> {in out}		Inbound 또는 Outbound를 구별하여 특정 AS에 속한 Neighbor 라우터와의 Session을 Reset 합니다.
clear ip bgp external {in out}		Inbound 또는 Outbound를 구별하여 외부 Peer에 대한 Session을 Reset 합니다.
clear ip bgp peer-group name {in out}		Inbound 또는 Outbound를 구별하여 특정 Peer 그룹에 속한 모든 Peer에 대한 Session을 Reset 합니다.

한편, Session을 Reset 하지 않고 변경된 라우팅 정보를 적용하기 위해서는 자동적으로 업데이트 하는 방법이 있습니다. 이러한 방법을 Soft Reset이라고 하는데, 이 방법을 사용하려면, 라우팅 테이블을 업데이트하는 모든 라우터들이 route refresh 기능을 지원해야 합니다.



Soft Reset을 사용하려면, route refresh 기능을 지원해야 합니다.

Soft Reset을 사용하여 변경된 라우팅 정보를 업데이트 하도록 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip bgp * soft	Enable /Global	모든 Peer를 대상으로 Soft Reset 합니다.
clear ip bgp * soft {in out}		Inbound 또는 Outbound를 구별하여 모든 Peer를 대상으로 Soft Reset 합니다.
clear ip bgp ip-address soft		특정 경로에 대해 Soft Reset 합니다.
clear ip bgp ip-address soft {in out}		Inbound 또는 Outbound를 구별하여 특정 경로에 대해 Soft Reset 합니다.
clear ip bgp <1-65,535> soft		특정 AS에 속한 Neighbor 라우터를 대상으로 Soft Reset 합니다.
clear ip bgp <1-65,535> soft {in out}		Inbound 또는 Outbound를 구별하여 특정 AS에 속한 Neighbor 라우터를 대상으로 Soft Reset 합니다.
clear ip bgp external soft		외부 Peer를 대상으로 Soft Reset 합니다.
clear ip bgp external soft {in out}		Inbound 또는 Outbound를 구별하여 외부 Peer를 대상으로 Soft Reset 합니다.
clear ip bgp peer-group name soft		특정 Peer 그룹에 속한 모든 Peer를 대상으로 Soft Reset 합니다.
clear ip bgp peer-group name soft {in out}		Inbound 또는 Outbound를 구별하여 특정 Peer 그룹에 속한 모든 Peer를 대상으로 Soft Reset 합니다.

Outbound soft reset은 Local 라우터의 Outbound 라우팅 테이블을 업데이트하는 것과 함께 BGP 세션으로 연결된 맞은 편 장비의 Inbound 라우팅 테이블에 대한 정보를 얻을 수 있습니다. Route refresh 기능을 지원하지 않는 경우에는, 저장된 라우팅 정보를 통해 새롭게 라우팅 테이블을 업데이트합니다. 이 방법을 사용하려면, 먼저 Local 라우터가 받은 모든 경로 정보를 저장하도록 설정한 후, Soft reset을 실행합니다.

1 단계 Local 라우터에 모든 경로 정보를 저장합니다. 경로 정보를 저장하도록 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
neighbor soft-reconfiguration inbound	Router	Local 라우터에 모든 경로 정보를 저장합니다.

2 단계 Soft Reset을 사용하여 변경된 라우팅 정보를 업데이트 하도록 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip bgp {* ip-address peer-group name} soft in	Enable/Global	Soft Reset 합니다.

11.1.10. Graceful Restart

사용자는 네트워크에 문제가 발생하였거나 특별한 경우에 BGP 프로토콜의 프로세서를 재부팅 해야 할 때가 있습니다. 이러한 경우에는 일반적으로 BGP가 멈추었다가 시작하기까지는 시간이 많이 소요되는데 이 기간 동안은 패킷이 전달되지 못하게 됩니다. 또한 주변 라우터들은 OSPF를 재부팅 하는 라우터에 대한 경로 정보를 삭제하였다가, 재부팅이 된 이후에 다시 이를 등록하는 과정을 거쳐야 하는 불편함이 있습니다.

이러한 문제점을 개선한 것이 Graceful Restart인데, 이 기능을 사용하면 BGP를 재부팅하는 중에도 기존에 사용되고 있던 경로 정보를 통해 패킷을 계속해서 전달할 수 있습니다. 따라서 Neighbor 라우터와 정상적으로 경로 정보를 교환할 수 있습니다.

Graceful Restart를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp graceful-restart	Router	BGP 프로토콜에서 Graceful Restart를 사용할 수 있도록 설정합니다

한편, Graceful Restart와 관련하여 다음의 두 가지 시간 간격을 설정할 수 있습니다.

- **Restart-time** : Neighbor 라우터의 BGP 프로세스가 재부팅 되는 것을 기다려주는 시간을 말하며 이 시간 동안 BGP가 재부팅 되어 내부적인 연결(이하 Session이라고 함)이 이루어지지 않으면 라우터가 동작을 중단한 것으로 판단하여 그에 따른 처리를 하게 됩니다.
- **Stalepath-time** : Neighbor 라우터의 BGP 프로세스가 재부팅되고 해당 경로 정보를 다시 업데이트해 줄 때까지 대기하는 시간으로, 이 시간 동안 경로 정보가 업데이트 되지 않으면 해당 경로 정보를 삭제합니다.

Graceful Restart 기능의 restart-time과 stalepath-time을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bgp graceful-restart restart-time <1-3,600>	Router	Graceful Restart 기능의 restart-time을 설정합니다.
bgp graceful-restart stalepath-time <1-3,600>		Graceful Restart 기능의 stalepath-time 을 설정합니다



restart-time과 stalepath-time의 단위는 초입니다.



기본적으로 restart-time은 120초, stalepath-time은 360초로 설정되어 있습니다.

Graceful Restart 기능을 사용하지 않거나, **restart-time**, **stalepath-time** 등을 시스템 기본값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no bgp graceful-restart		BGP 프로토콜에서 Graceful Restart 기능을 사용하지 않습니다.
no bgp graceful-restart restart-time [restart-time]	Router	Graceful Restart 기능의 restart-time을 시스템 기본 값을 복구합니다.
no bgp graceful-restart stalepath-time [stalepath-time]		Graceful Restart 기능의 stalepath-time을 시스템 기본 값을 복구합니다.

11.1.11. BGP Neighbor 설정

(1) 기본 경로 설정

V5812G는 특정한 Neighbor 라우터들이나 Peer Group에 대해 기본 경로인 0.0.0.0을 설정할 수 있습니다. 이 때 Neighbor 라우터나 Peer Group의 라우터들은 이 설정에서 지정된 라우터로부터 기본 경로 정보를 받게 됩니다.

이 명령어는 특정한 이웃 BGP 라우터들이나 Peer Group에 대해 기본 경로인 0.0.0.0 을 전달하게 합니다. 이 경우 이웃 BGP 라우터나 Peer Group의 라우터들은 이 설정이 지정된 라우터로부터 기본 경로 정보를 받게 됩니다.

기본 경로를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
neighbor {neighbor-ip-address peer-group-name} default originate [route-map route-map-name]	Router	특정 Neighbor 라우터 혹은 Peer Group에 대해 기본 경로를 설정합니다.
no neighbor {neighbor-ip-address peer-group-name} default originate [route-map route-map-name]		Neighbor 라우터에 설정된 기본 경로를 해제합니다.

(2) Peer Group 설정

BGP는 네트워크 구성에 따라 많은 Neighbor 라우터들과 연결을 맺어야 할 때도 있습니다. 원칙적으로 하나의 AS 내에 속해 있는 모든 BGP 라우터들은 다른 Neighbor 라우터들과 연결되어 있어야 합니다. 이 경우, 수십 개 이상의 BGP 라우터들이 연결되어 각 Neighbor 라우터들과 경로 정보를 교환할 때에는 특정 라우터들을 그룹으로 관리하는 것이 더 효율적입니다. 동일한 그룹에 속해 있는 라우터들은 동일한 설정이 적용되고 이렇게 동일한 설정을 적용한 라우터 그룹을 Peer Group이라고 합니다.

Peer Group을 생성하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
neighbor peer-group-name peer-group	Router	BGP Peer Group을 생성합니다.
no neighbor peer-group-name peer-group		생성된 BGP Peer Group을 삭제합니다.

생성된 Peer Group에 특정 Neighbor 라우터를 추가하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
neighbor neighbor-ip-address peer-group <i>peer-group-name</i>	Router	해당 IP주소의 BGP Neighbor를 특정 Peer Group에 포함시킵니다.
no neighbor neighbor-ip-address peer-group <i>peer-group-name</i>		특정 Peer Group에 소속된 BGP Neighbor를 Peer Group으로부터 제외시킵니다.

(3) 강제 종료 기능

V5812G가 BGP Neighbor 라우터나 Peer Group과 Session을 맺고 경로를 교환하고 있는 경우, 특정한 라우터 또는 Peer Group과의 정보 교환을 차단할 수 있습니다. 이러한 경우에는 맺어진 Session을 종료하고 해당 Neighbor 라우터나 Peer Group으로부터 수신된 모든 경로 정보를 삭제하도록 합니다.

특정 라우터나 Peer Group과의 정보 교환을 차단하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
neighbor {neighbor-ip-address peer-group-name} shutdown	Router	특정 라우터 혹은 Peer Group과의 Session을 중단합니다.
no neighbor {neighbor-ip-address peer-group-name} shutdown		특정 라우터 혹은 Peer Group과의 중단된 Session을 다시 복귀시킵니다.

11.1.12. BGP 설정 내용 확인

V5812G의 사용자는 BGP 라우팅 프로토콜과 관련된 여러 가지 설정 내용 및 경로 정보 등을 확인 할 수 있습니다. 이러한 정보들은 시스템의 효율성을 높이고 장애 발생시 문제를 해결하는데 유용하게 사용됩니다.

BGP 라우팅 프로토콜에 대한 설정 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip bgp summary show ip bgp [ipv4 {unicast multicast}] summary	Enable/Global	BGP 이웃 라우터들의 상황을 요약해 보여줍니다.

Session을 맺고 있는 BGP Neighbor 라우터들의 세부 정보들도 모니터링 할 수 있습니다. Neighbor 라우터들의 세부 정보를 모니터링하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip bgp neighbors		현재 Session을 맺고 있는 모든 Neighbor 라우터들의 기본 정보사항을 보여줍니다.
show ip bgp ipv4 {unicast multicast} neighbors		Neighbor 라우터의 IP 주소를 통해 해당 Neighbor 라우터의 정보만 확인합니다.
show ip bgp neighbors neighbor-ip-address		
show ip bgp ipv4 {unicast multicast}		
neighbors neighbor-ip-address		
show ip bgp neighbors neighbor-ip-address advertised-routes		해당 Neighbor 라우터에 전달해 준 경로 정보들을 보여줍니다.
show ip bgp ipv4 {unicast multicast}		
neighbors neighbor-ip-address advertised-routes		
show ip bgp neighbors neighbor-ip-address received-prefix-filter	Enable / Global	해당 Neighbor 라우터로부터 수신받은 경로 정보 전부를 보여줍니다. 이 정보내에는 수신을 거부한 경로 정보도 포함합니다.
show ip bgp ipv4 {unicast multicast}		
neighbors neighbor-ip-address received-prefix-filter		
show ip bgp neighbors neighbor-ip-address received-routes		해당 Neighbor 라우터로부터 수신받은 경로들을 보여줍니다. 이 기능을 사용하기 위해선 BGP Soft Reconfiguration 기능을 설정해야 합니다.
show ip bgp ipv4 {unicast multicast}		
neighbors neighbor-ip-address received-routes		
show ip bgp neighbors neighbor-ip-address routes		해당 Neighbor 라우터로부터 수신한 모든 경로들중 허용된 경로들만 보여줍니다.
show ip bgp ipv4 {unicast multicast} neighbors		
neighbors neighbor-ip-address routes		

11.2 OSPF(Open Shortest Path First)

OSPF(Open Shortest Path First)는 IETF(Internet Engineering Task Force)의 OSPF 분과가 개발한 프로토콜입니다. IP 네트워크를 위해 고안된 OSPF는 IP subnetting을 지원하고 외부 네트워크에서 들어온 라우팅 정보는 구분하여 관리할 수 있습니다. 또한 OSPF는 패킷 인증을 지원하고 IP 멀티캐스트로 라우팅 정보를 주고 받습니다.

OSPF는 계층화된 네트워크 환경에서 가장 적합한 라우팅 프로토콜입니다. OSPF 네트워크에서 가장 먼저 해야 하는 일은 라우터들로 구성된 네트워크를 설계하고, 그에 따라 여러 영역과 접하는 라우터인 **Border** 라우터와 AS 경계 라우터를 설정하는 것입니다.

그 이후 OSPF 라우터가 구동하는데 필요한 최소한의 기본 설정을 하고 Area에 인터페이스를 지정합니다. 사용자의 환경에 맞게 OSPF 라우터를 설정할 때는 각 라우터에 설정한 내용들이 서로 일치하는지 확인해야 합니다.

다음은 OSPF 라우팅 프로토콜을 설정하는 방법입니다.

- OSPF 활성화
- ABR 유형 설정
- RFC1583 호환성 지원
- OSPF 인터페이스 설정
- Non-broadcast 네트워크 설정
- Area 설정
- 기본 경로값 변경
- Graceful Restart 지원
- Opaque-LSA 지원
- 기본 경로 설정
- ECMP(Equal Cost Multi-Path) 설정
- 경로 계산 주기 설정
- 외부 경로 전달
- OSPF 거리값 변경
- 호스트 경로 설정
- 수동 인터페이스 설정
- 경로 정보 차단
- 요약 경로 정보 전달
- OSPF 모니터 및 관리

11.2.1. OSPF 활성화

다른 라우팅 프로토콜과 마찬가지로 OSPF 라우팅 프로토콜을 사용하려면, 해당 프로토콜을 활성화한 후, OSPF로 운영할 네트워크 주소와 네트워크 번호(ID)를 설정합니다.

다음은 OSPF를 활성화하는 방법입니다.

1 단계 Global 설정 모드에서 Router 설정모드로 들어갑니다.

명령어	모 드	기 능
router ospf [<1-65,535>]	Global	OSPF 프로토콜이 활성화되면서 Router 모드로 들어갑니다.
no router ospf [<1-65,535>]		OSPF 라우팅 프로토콜을 해제합니다.



참 고

OSPF 라우팅 프로토콜을 해제하면, 관련된 설정들이 모두 초기화 됩니다.



참 고

만약 두개 이상의 OSPF 프로세스를 운영할 경우에는 프로세스 번호를 명기해 주시기 바랍니다.
일반적으로 하나의 라우터에서는 하나의 OSPF 프로세스만 운영합니다.

2 단계 OSPF의 네트워크 ID를 지정합니다. 네트워크 ID는 네트워크의 IPv4 주소를 사용하여 설정합니다.

명령어	모 드	기 능
router-id ip-address	Router	활성화된 OSPF 프로세스의 라우터 ID를 지정합니다.
no router-id ip-address		설정한 라우터 ID를 삭제합니다.

router-id ip-address 명령어를 사용하여 새로운 라우터 ID를 OSPF 프로세스에 적용한 경우, OSPF 프로세스를 다시 시작해 주어야 새롭게 추가된 내용이 적용됩니다. 이를 위해서는 Global 모드에서 '**clear ip ospf process**' 명령어를 이용해 OSPF 프로세스를 재시작 해 주십시오.

한편 이미 OSPF 프로세스가 동작하고 있는 중에 router-id를 변경하게 되면 기존의 설정을 처음부터 다시 진행해야 하는 불편함이 있습니다. 이러한 경우, V5812G는 Router-id와 관련된 설정을 그대로 두고 Router-id만 변경할 수 있습니다.

Router-id와 관련된 설정을 그대로 두고 Router-id만 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ospf router-id ip-address	Router	Router-id와 관련된 설정을 그대로 두고 Router-id만 변경하도록 지정합니다.
no ospf router-id ip-address		Router-id와 관련된 설정을 그대로 두고 Router-id만 변경하도록 지정한 것을 해제합니다.

위에서 설정한 내용을 주변 라우터들에게 전송하려면, Global 모드에서 '**clear ip ospf process**'로 OSPF 프로세스를 재시작해야 합니다.

3 단계 **network** 명령어를 통해 OSPF로 동작하는 네트워크 정보를 설정합니다.

네트워크 정보 설정은 두가지 방법을 사용할 수 있습니다. 첫번째는 설정할 네트워크 정보를 네트워크 주소와 비트 마스크 정보를 함께 나타내는 방식으로, 예를 들면 '10.0.0.0/8' 와 같이 표현됩니다. 두 번째는 네트워크 주소와 와일드카드 비트 정보를 이용하여 나타내는 방식으로 예를 들면, '10.0.0.0 0.0.0.255'로 표현됩니다.

한편, **area** 뒤에 옵션 변수는 IP 주소 형태 혹은 정수값으로 된 OSPF Area ID를 넣어 설정합니다.

다음은 OSPF로 동작하는 네트워크 정보를 설정할 때 사용하는 명령어입니다.

명령어	모 드	기 능
network ip-address/m		
area {<0 – 4,294,967,295> ip-address }	Router	OSPF area ID를 지정합니다.
network ip-address mask-address		
area {<0 – 4,294,967,295> ip-address }		



참 고

OSPF area-ID는 <0-4,294,967,295> 사이의 십진수나 IP 주소 중 한 가지를 선택하여 입력하십시오.

이와 같은 명령으로 기본적인 OSPF 프로토콜을 활성화 시킬 수 있으며 그 이후엔 사용자가 다음과 같은 항목들을 선택하여 설정할 수 있습니다.

11.2.2. ABR 유형 설정

V5812G는 4가지 유형의 OSPF ABR 유형을 지원합니다. Cisco 형태의 ABR(RFC 3509)와 Ibm 방식의 ABR(RFC 3509), IETF Draft에서 지정한 방식, 그리고 RFC 2328에서 지정한 방식입니다.

OSPF의 ABR 유형을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ospf abr-type {cisco ibm shortcut standard}		ABR 유형을 지정합니다.
no ospf abr-type {cisco ibm shortcut standard}	Router	설정된 ABR 유형을 시스템 기본값으로 변경합니다.



cisco는 Cisco 형태의 ABR (RFC 3509), **ibm**은 RFC 3509의 IBM 방식, **shortcut**은 IETF Draft에서 지정한 방식, **standard**는 RFC2328에서 지정한 방식을 나타냅니다.



V5812G는 기본적으로 OSPF의 ABR이 **cisco**로 지정되어 있습니다.

11.2.3. RFC 1583 호환성 지원

V5812G의 OSPF 프로토콜은 경로를 요약하여 계산하는 방법에 RFC 2328의 방식을 사용합니다. 그러나, 네트워크를 운영하는데 있어서 이전의 표준이 되는 RFC 1583의 요약 경로 계산 방법과 호환성을 가져야 할 경우가 있습니다. 이러한 경우 V5812G는 이전 표준과의 호환성을 지원이 가능하도록 개발되었습니다.

요약 경로 계산에 있어서 RFC 1583과 호환성을 가지도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
compatible rfc1583		요약 경로 계산에 있어서 RFC 1583와 호환성을 가집니다.
no compatible rfc1583	Router	요약 경로 계산 방식을 기본값으로 되돌립니다.

11.2.4. OSPF 인터페이스 설정

사용자는 필요에 따라 OSPF의 인터페이스 설정을 변경할 수 있습니다. OSPF 인터페이스 설정과 관련된 항목을 전부 변경할 필요는 없지만 그 중 몇 가지는 동일한 네트워크에 존재하는 다른 라우터들의 설정과 일치해야 합니다.

(1) 인증 관련 설정

OSPF 라우터들 사이에서 경로 계산을 위해 주고 받는 정보에 보안을 위해 인증 기능을 사용할 수 있습니다. 인증 기능을 사용하게 되면 라우터들 사이에서 주고 받는 정보들이 암호화되어 타인이 쉽게 확인할 수 없게 됩니다. OSPF 라우터에 보안을 위해 인증을 설정하려면, 다음 명령어를 사용 하십시오.

명령어	모 드	기 능
ip ospf authentication [message-digest null]	Interface	OSPF 인터페이스에 인증 기능을 활성화합니다.
Ip ospf ip-address authentication [message-digest null]		



위의 명령어에서 인증 방식을 선택하지 않으면 암호값을 단순히 텍스트 기반으로 나타내여 교환하게 됩니다.



message-digest는 인증을 위한 암호화 방식을 MD5 형식으로 사용하는 것이고, **null**은 인증 없이 동작하게 됩니다



*ip-address*는 인터페이스의 특정 IP 주소를 지정하는 옵션입니다.

인증 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip ospf authentication [message-digest null]	Interface	해당 인터페이스에서 인증 기능을 해제합니다.
no ip ospf ip-address authentication [message-digest null]		

(2) 인증 키 설정

OSPF 라우터의 인터페이스에 인증 기능을 사용하게 되면, 인증에 사용될 암호가 필요합니다. 인증 키는 이러한 인증 기능에서 사용하는 암호의 역할을 하게 됩니다. 인증 키는 동일한 네트워크에 존재하는 모든 라우터들이 동일하게 설정되어야 합니다.



인증키는 동일한 네트워크에 존재하는 다른 라우터들과 동일하게 설정되어야 합니다.

인증은 사용자의 선택에 따라 암호값을 단순히 텍스트 기반으로 표현하여 정보를 교환하는 방식과 md5 방식으로 설정됩니다. 텍스트 기반으로 암호값을 사용하여 정보를 교환하는 방식에서 사용할 인증 키를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip ospf authentication-key key	Interface	텍스트 기반의 인증 키를 설정합니다.
ip ospf authentication-key key {first second} [active]		
ip ospf ip-address authentication-key key		
ip ospf ip-address authentication-key key {first second} [active]		

다음은 md5 방식의 인증 기능에서 사용할 인증 키를 설정할 때 사용하는 명령어입니다.

명령어	모 드	기 능
ip ospf message-digest-key <1-255> md5 key [active]	Interface	Md5 방식의 인증에서 사용할 인증 키를 설정합니다.
ip ospf message-digest-key <1-255> md5 [active]		
ip ospf ip-address message-digest-key <1-255> md5 key [active]		
ip ospf ip-address message-digest-key <1-255> md5 [active]		



key는 최대 16자까지 입력할 수 있습니다.

한편, 설정한 인증 키를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip ospf authentication-key key	Interface	인증 키를 삭제합니다.
no ip ospf authentication-key key {first second}		
no ip ospf ip-address authentication-key key		
no ip ospf ip-address authentication-key key {first second}		
no ip ospf message-digest-key <1-255>		
no ip ospf ip-address message-digest-key <1-255>		

(3) 인터페이스 Cost 설정

OSPF 프로토콜은 라우팅 경로를 계산하기 위해 각 인터페이스에 대역폭에 따라 적절한 Cost를 부여합니다. Cost는 각 인터페이스에서 패킷을 라우팅하기 위한 경로를 계산하는데 활용되고, 라우터 사이에서는 Cost가 교환됩니다. 해당 인터페이스의 Cost를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip ospf cost <1-65,535>	Interface	OSPF 인터페이스의 Cost를 설정합니다
ip ospf ip-address cost <1-65,535>		

설정한 Cost를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip ospf cost	Interface	설정한 Cost를 삭제합니다
no ip ospf ip-address cost		

(4) 경로 정보 Database 송신 차단

OSPF 프로토콜으로 라우팅을 하는 라우터들은 LSA를 통해 서로가 가지고 있는 경로들의 정보를 교환합니다. 각 경로에 대한 정보는 라우터 내부에 Database로 저장되어 있고, 다른 라우터와 서로의 정보를 송수신하며 교환하게 됩니다. 그러나, 사용자의 필요에 따라 특정 인터페이스의 경로 정보 Database를 외부에 송신하지 못하도록 할 수 있습니다.

특정 인터페이스에 경로 정보 Database의 외부 송신을 차단하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip ospf database-filter all out	Interface	해당 인터페이스에서 경로 정보 Database를 외부에 송신하지 못하도록 설정합니다.
ip ospf ip-address database-filter all out		

한편, 특정 인터페이스에 경로 정보 Database를 송신하지 못하도록 설정한 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip ospf database-filter	Interface	특정 인터페이스에 경로 정보 Database를 송신하지 못하도록 설정한 것을 해제합니다.
no ip ospf ip-address database-filter		

(5) 라우팅 프로토콜 동작 주기 설정

OSPF 네트워크에 존재하는 라우터들은 서로 정보를 공유하기 위해 다양한 패킷을 교환하는데, 패킷을 송수신하는 것에 관련하여 여러 가지 시간 간격을 설정할 수 있습니다. 다음은 패킷 송수신에 관련하여 사용자가 설정할 수 있는 시간 간격의 종류입니다.

- **Hello-interval** : OSPF 라우터는 자신의 존재를 알리기 위해 일정한 시간 간격을 두고 Hello 패킷을 보내게 됩니다. 이 때, Hello 패킷을 송신하는 간격을 Hello-interval이라고 합니다.
- **Retransmit-interval** : 라우터가 LSA 정보를 송신하면, 이 LSA 정보를 수신한 라우터로부터 정보를 수신했다는 승인 정보를 받게 됩니다. 이 때 LSA를 송신하고 일정 시간 동안 승인 정보를 받지 못하면, 상대방 라우터가 LSA 정보를 수신하지 못한 것으로 인식하고 LSA 정보를 다시 보냅니다. 이와 같이 LSA 정보에 대한 승인 정보를 받지 못하여 LSA 정보를 재송신하기까지의 시간 간격을 Retransmit-interval이라고 합니다.
- **Dead-interval** : OSPF 네트워크에 존재하는 라우터들은 정기적으로 Hello 패킷을 보내도록 되어 있습니다. 그런데, 특정 라우터로부터 일정 시간동안 Hello 패킷이 전송되지 않는다면, 그 라우터는 동작을 멈추었다고 판단하게 됩니다. 이와 같이 특정 라우터가 동작을 멈추었다고 판단하기까지 기다리는 시간을 Dead-interval이라고 합니다.

- **Transmit-delay** : 라우터가 다른 라우터에게 LSA를 송신할 때, 통신 상태에 따라 LSA의 전송이 지연될 수 있습니다. 이를 고려하여 LSA를 전송하는데 걸리는 시간을 설정해 두는데, 이를 Transmit-delay라고 합니다.



참 고

위에서 설명한 시간 간격들은 동일한 네트워크에 존재하는 라우터들 사이에서는 동일한 값을 가져야 합니다.

다음은 Hello-interval을 설정할 때 사용하는 명령어입니다.

명령어	모 드	기 능
ip ospf hello-interval <1-65,535>	Interface	Hello 패킷 송신의 시간간격을 설정합니다.
ip ospf ip-address hello-interval <1-65,535>		



참 고

Hello-interval의 설정 단위는 초이며, 기본적으로 10초로 설정되어 있습니다.

Retransmit-interval을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip ospf retransmit-interval <1-65,535>	Interface	LSA 정보를 재송신하기까지 승인 정보를
ip ospf ip-address retransmit-interval <1-65,535>		기다리는 시간을 설정합니다.



참 고

Retransmit-interval의 설정 단위는 초이며, 기본적으로 5초로 설정되어 있습니다.

Dead-interval을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip ospf dead-interval <1-65,535>	Interface	Dead-interval을 설정합니다.
ip ospf ip-address dead-interval <1-65,535>		



참 고

Dead-interval의 설정 단위는 초이며, 기본적으로 40초로 설정되어 있습니다.

Transmit-delay를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip ospf transmit-delay <1-65,535>	Interface	Transmit-delay를 설정합니다.
ip ospf ip-address transmit-delay <1-65,535>		



참 고

Transmit-delay의 설정 단위는 초이며, 기본적으로 1초로 설정되어 있습니다.

위에서 설정한 내용을 초기화 상태로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip ospf hello-interval	Interface	Hello-interval을 초기값으로 되돌립니다.
no ip ospf ip-address hello-interval		
no ip ospf retransmit-interval		Retransmit-interval을 초기값으로 되돌립니다.
no ip ospf ip-address retransmit-interval		
no ip ospf dead-interval		Dead-interval을 초기값으로 되돌립니다.
no ip ospf ip-address dead-interval		
no ip ospf transmit-delay		Transmit-interval을 초기값으로 되돌립니다.
no ip ospf ip-address transmit-delay		

(6) MTU 관련 설정

OSPF 네트워크에서 인접한 라우터들 사이에 정보를 교환하는 과정인 DD(Database Description) 교환 과정 중에 라우터간의 링크에 대한 MTU를 확인하도록 되어 있습니다. 기본적으로는 MTU 크기가 다른 라우터 사이에서는 OSPF 네트워크를 구성할 수 없습니다. 따라서, 이러한 경우에는 서로 다른 OSPF 인터페이스의 MTU를 동일한 값으로 일치시켜 주어야 합니다. 일반적으로 이더넷 인터페이스의 MTU는 1500Bytes로 설정합니다.

OSPF 인터페이스에서 사용할 MTU를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip ospf mtu <576-65,535>	Interface	OSPF 인터페이스에서 사용할 MTU 값을 설정합니다.
no ip ospf mtu		OSPF 인터페이스에 설정한 MTU 값을 해제합니다.



참 고

위에서 설정하는 MTU는 동일한 OSPF 네트워크에 존재하는 라우터들의 MTU를 일치시키기 위한 것으로, 실제 인터페이스 자체의 MTU는 변하지 않습니다.

한편, OSPF 네트워크에 존재하는 두 라우터의 인터페이스 MTU 값이 다르더라도, OSPF 네트워크에 참가할 수 있도록 DD 교환 과정 중에서 MTU를 확인하는 과정을 생략하도록 설정할 수 있습니다. 이 과정을 생략하면, MTU 값이 다르더라도 OSPF 네트워크에 참가가 가능합니다.

DD 교환 과정 중에서 MTU를 확인하는 과정을 생략하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip ospf mtu-ignore	Interface	DD 과정 중 MTU 확인을 생략하도록 설정합니다.
ip ospf ip-address mtu-ignore		

한편, DD 과정 중에서 MTU를 확인하는 과정을 생략하도록 설정했던 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip ospf mtu-ignore	Interface	DD 과정 중에서 MTU를 확인하는 과정을 생략하도록 설정했던 것을 해제합니다.
no ip ospf ip-address mtu-ignore		

(7) 우선 순위 결정

OSPF 네트워크 내에서는 여러 대의 라우터가 서로 정보를 교환하게 됩니다. 이러한 라우터들간에서는 각각의 역할이 나누어지는데, 그 중 DR(Designated Router)는 하나의 영역 안에서 경로와 관련된 정보를 모으고 전달하는 핵심적인 역할을 하게 됩니다.

여러 대의 라우터들 사이에 우선 순위(Priority)가 가장 높은 값을 가지는 라우터가 DR로 정해지고, 만약 우선 순위가 동일한 경우에는 Router-ID가 높은 라우터가 DR이 됩니다.

일반적으로 라우터들의 우선 순위는 1로 정해져 있지만, 특정 라우터를 DR로 지정하려고 할 경우에는 Priority를 높여서 해당 라우터를 DR로 만들 수 있습니다.

라우터의 우선 순위를 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip ospf priority <0-255>	Interface	OSPF 라우터의 우선 순위를 설정합니다.
ip ospf ip-address priority <0-255>		

라우터의 우선 순위를 초기값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip ospf priority	Interface	OSPF 라우터의 우선 순위를 설정합니다.
no ip ospf ip-address priority		

(8) OSPF 네트워크 유형 설정

OSPF 네트워크는 그 유형을 네가지 타입으로 분류할 수 있습니다. OSPF의 네가지 타입의 네트워크는 Broadcast 네트워크, NBMA(Non-broadcast-multiple-access) 네트워크, Point-to-multipoint 네트워크, Point-to-point 네트워크입니다.

사용자는 OSPF 네트워크를 Broadcast 타입이나 Non-broadcast 타입으로 설정할 수 있습니다. 예를 들어 사용자의 네트워크가 Multicasting을 지원하지 않는다면 Broadcast 네트워크를 Non-broadcast 타입으로 설정할 수도 있고, Frame relay 같은 NBMA 네트워크를 Broadcast 타입으로 설정할 수도 있습니다.

NBMA 타입으로 네트워크를 운영하려면 라우터와 라우터를 모두 가상 회로(virtual circuit)로 연결해야 합니다. 그러나 OSPF는 네트워크 관리 비용을 절감하기 위해 네트워크의 일부분만 가상 회로로 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 가상 회로를 사용하여 연결하면 이러한 중간 라우터인 Neighbor 라우터를 설정해야 하는 번거로움이 사라집니다.

이와 같이 OSPF의 Point-to-multipoint 네트워크는 Neighbor 라우터를 지정할 필요가 없기 때문에 IP 자원이 절약되고 목적지 라우터를 설정하기 위한 별도의 절차가 필요없게 됩니다. 또한, 네트워크에 위치한 모든 라우터와 거미줄처럼 연결되어 할 필요가 없기 때문에 관리 비용이 절감됩니다. 가상 회로는 단절되더라도 통신이 가능하기 때문에 더욱 안정된 네트워크 서비스를 제공할 수 있다는 장점도 가지고 있습니다. 일반적으로 이더넷 인터페이스를 사용하는 라우터와 L3 스위치들은 기본적으로 Broadcast 유형의 네트워크를 사용하게 됩니다.

OSPF 네트워크 타입을 설정하려면, Interface 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip ospf network {broadcast non-broadcast point-to-multipoint point-to-point }	Interface	OSPF 인터페이스에 네트워크 타입을 설정합니다.

11.2.5. Non-broadcast 네트워크 설정

NBMA 형태의 네트워크에 대해 OSPF를 운영하기 위해서는 각 인터페이스와 연결된 네트워크 유형을 NBMA로 설정해야 하며 또한 Neighbor 라우터에 대한 설정이 필요합니다.

Neighbor 라우터를 설정할 때 라우터의 IP 주소와 우선 순위, 그리고 Poll-interval을 설정할 수 있습니다. 우선 순위는 지정 라우터(DR)를 선택할 때 필요한 정보이며 NBMA 네트워크는 기본적으로 「0」으로 설정되어 있습니다. 한편, Poll-interval은 응답이 없는 Neighbor 라우터에 Hello 패킷을 다시 보내기까지 기다리는 시간을 말하며 기본적으로는 120초로 설정되어 있습니다.

Non-broadcast 타입으로 통신하는 라우터를 설정하려면, Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
neighbor ip-address cost <1-65,535>	Router	NBMA 타입으로 통신하는 Neighbor 라우터를 설정합니다. cost, priority, poll-interval 등은 선택적으로 적용할 수 있습니다.
neighbor ip-address priority <0-255>		
neighbor ip-address priority <0-255> poll-interval <1-65,535>		
neighbor ip-address poll-interval <1-65,535>		
neighbor ip-address poll-interval <1-65,535> priority <0-255>		

다음은 위에서 설정한 내용을 기본값으로 되돌릴 때 사용하는 명령어입니다.

명령어	모 드	기 능
no neighbor ip-address cost [1-65,535]	Router	설정했던 Neighbor 라우터에 대한 내용을 삭제하고, 기본값을 되돌립니다.
no neighbor ip-address priority [0-255]		
no neighbor ip-address priority poll-interval [1-65,535]		
no neighbor ip-address poll-interval [1-65,535]		
no neighbor ip-address poll-interval priority [0-255]		

11.2.6. Area 설정

OSPF 네트워크에 포함되는 라우터를 설정할 때, 각 인터페이스, 네트워크 등이 포함되는 Area에 대한 설정을 하게 됩니다. Area는 OSPF 설정에 매우 중요한 부분이며 여러가지 다양한 특징을 가지고 있습니다. Area에 대한 여러 가지 특성을 적절하게 설정해야만 전체 OSPF 네트워크에 참여하는 Area를 효과적으로 관리할 수 있게 됩니다.

OSPF 네트워크에서는 Area를 관리하기 위해 몇 가지 특정한 라우터 유형을 정의하고 있습니다. 그 중 중요한 유형으로 ABR (Area Border Router)이 있는데, 이는 서로 다른 OSPF의 두 영역 사이에서 Area간의 경로 정보를 전달하는 역할을 합니다.

한편 ASBR(Autonomous System Border Router)은 한쪽 Area에서는 OSPF를 사용하고, 다른 한 쪽 인터페이스 혹은 Area에서는 OSPF를 제외한 다른 라우팅 프로토콜을 사용하는 라우터입니다. ASBR은 다른 라우팅 프로토콜간의 Area 정보를 교환하는 역할을 하게 됩니다.

Area의 종류도 여러 가지가 있는데 그 중 중요하게 다루어지는 것은 Stub Area와 NSSA(Not So Stubby Area)입니다. 각 종류별 Area는 해당 설정 항목에서 설명하고 있습니다.

(1) Area 인증 설정

특정 Area에 속한 OSPF 라우터들이 교환하는 경로 정보에 대한 보안을 위해 인증을 통해 정보를 교환하도록 설정할 수 있습니다. 이 때, 암호화하는 방법에는 일반 텍스트를 기반으로 비밀번호를 사용하는 방법과, MD5로 암호화한 비밀번호를 사용하는 방법이 있습니다.

인증을 사용하도록 설정하였을 경우에는 해당 Area에 속한 인터페이스에 비밀번호를 설정해야 합니다. 인터페이스에 비밀번호를 설정할 때에는 Interface 모드에서 **ip ospf authentication-key**, **ip ospf message-digest-key** 등의 명령어를 사용하십시오. 이 설정에 대한 명령은 ‘**9.2.4 OSPF 인터페이스 설정**’에서 ‘**(4) 인증 관련 설정**’을 참고하시기 바랍니다.

Area에서 경로 정보를 교환하는데 인증을 사용하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
area area-ID authentication	Router	Area에서 일반 텍스트 기반의 비밀번호를 이용한 인증을 설정합니다.
area area-ID authentication message-digest		Area에서 MD5로 암호화한 비밀번호를 이용한 인증을 설정합니다.



OSPF area-ID는 <0-4,294,967,295> 사이의 십진수나 IP 주소 중 한 가지를 선택하여 입력합니다.

보다 자세한 설정 방법은 **9.2.2 ABR 유형 설정**을 참조하십시오.

인증 설정을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no area area-ID authentication	Router	인증이 설정된 Area의 인증을 해제합니다.

(2) Area의 기본 Cost값 설정

Area의 기본 Cost는 ABR에서만 설정할 수 있습니다. 이는 ABR이 요약 기본 경로 (summary default route)를 Stub Area나 NSSA로 전달할 때만 사용할 수 있는 기능으로, 그러한 경우에서 전달되는 기본 경로의 cost 값을 설정하게 되는 것입니다. 따라서, ABR이지만 Stub Area나 NSSA를 가지고 있지 않은 라우터에서는 아래 명령어를 사용할 수 없습니다.

Area의 기본 Cost 값을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
area area-ID default-cost <1-16,777,215>	Router	Area의 기본 Cost 값을 설정합니다.



참 고

위의 명령어는 ABR 가운데 요약 기본 경로 (summary default route)를 Stub Area나 NSSA로 전달하는 ABR에서만 설정할 수 있습니다.

설정한 Area의 기본 Cost 값을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no area area-ID default-cost	Router	사용자가 설정한 Area의 기본 Cost 값을 삭제합니다.

(3) Area간 경로 정보 전달 제한 설정

ABR은 둘 이상의 여러 Area 사이에서 각 Area가 가지고 있는 경로 정보를 다른 Area에 전달하는 역할을 합니다. 그러나 특정 경로 정보를 다른 Area로 전달하지 않아야 하는 경우가 발생할 수 있습니다. V5812G는 이러한 경우에 특정 경로 정보를 전달하지 않도록 설정할 수 있습니다. 특정 경로 정보를 전달하지 않도록 차단하려면, 먼저 **access_list** 또는 **prefix_list** 명령어를 이용해 특정 경로 정보에 대한 list_name을 할당합니다. 그리고 아래 명령어를 사용하여 할당된 list_name에 해당하는 경로 정보를 차단하도록 설정합니다. 이러한 설정 역시 OSPF 라우터가 ABR인 경우에만 설정할 수 있습니다.

할당된 list_name에 해당하는 경로 정보를 차단하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
area area-ID filter-list access access_list_name {in out}	Router	할당된 list_name에 해당하는
area area-ID filter-list prefix prefix_list_name {in out}		경로 정보를 차단합니다.



참 고

위의 명령어는 ABR에서만 설정할 수 있습니다.

할당된 list_name에 대해 차단하는 설정을 삭제합니다.

명령어	모 드	기 능
no area area-ID filter-list access access_list_name {in out}	Router	할당된 list_name에 대해 차
no area area-ID filter-list prefix prefix_list_name {in out}		단하는 설정을 삭제합니다.

(4) NSSA 설정

NSSA(Not So Stubby Area)는 Stub Area이지만 다른 라우팅 프로토콜에서 얻은 경로 정보를 ASBR이 해당 Area에 전달할 수 있는 Area입니다. 이에 반해 Stub Area는 다른 라우팅 프로토콜의 경로 정보를 전달할 수 없습니다. 다음은 NSSA를 설정하는 경우의 명령어입니다.

명령어	모 드	기 능
area area-ID nssa	Router	NSSA로 설정합니다.

NSSA와 관련하여 다음과 같은 여러 가지 특성에 대한 내용을 설정할 수 있습니다.

- **Default-information-originate** : NSSA 내에 Type-7의 기본 경로를 허용하도록 하는 설정입니다.

다시 말해 NSSA에 존재하는 라우터들이 가지고 있는 경로 정보 이외에 모든 경로에 대한 기본 경로는 Type-7의 기본 경로를 허용한 인터페이스를 통해 전달되도록 지정되는 것입니다. 이 때, **metric**은 기본 경로의 메트릭 값을 설정하는 것이고, **metric-type**은 경로 계산 방식을 선정하는 것입니다. **metric-type 1**은 내부 경로 cost와 외부 경로 cost를 더한 값을 경로 cost로 사용하게 되고, **metric-type 2**는 언제나 외부 경로의 cost 값만 사용하게 됩니다.

- **No-redistribution** : NSSA에서 외부로부터 받은 경로 정보를 재전송하지 못하도록 설정합니다.

- **No-summary** : OSPF Area 간의 경로 정보를 NSSA내에서 전달하지 못하도록 설정합니다.

- **Translator-role** : NSSA-LSA(Link State Advertisement) 정보를 처리하는 방식에 따라 세 가지 유형으로 설정할 수 있습니다. **always**는 모든 NSSA-LSA를 Type-5 LSA로 변경해 처리하게 하는 것이고, **candidate**는 translator로 선정되었을 때만 NSSA-LSA를 Type-5 LSA로 변환합니다. **never**는 NSSA-LSA를 다른 형식으로 변환하지 않습니다.

주로 NSSA는 Stub Area나 다른 라우팅 프로토콜의 Area 정보를 OSPF 내에 전달할 때 ASBR에 사용하게 됩니다. 이 경우 다른 라우팅 프로토콜에 기본 경로가 있으면 **default-information-originate**를 사용해 OSPF 의 모든 기본 경로가 해당 ASBR를 통해 이동이 이루어지게 설정합니다.

여러 가지 특성에 대한 설정과 함께 NSSA를 설정하려면, 옵션값과 함께 명령어를 사용해야 합니다. 한편, **area <0-4,294,967,295> nssa** 하위에 설정할 수 있는 옵션은 위에서 설명한 바와 같이 크게 **default-information originate**, **no-redistribution**, **no-summary**, **translator-role**의 4가지로 구분되고, 이 4가지에 대한 설정은 순서에 상관없이 복수 설정이 가능합니다. 이 때, **default-information originate**는 **metric <0-16,777,214>**과 **metric-type <1-2>**이라는 선택적인 옵션값을 가지고, **translator-role**은 **candidate**, **never**, **always**이라는 옵션값 중에서 하나를 무조건 설정해야 합니다.

옵션에 대한 명령어를 이해하기 쉽게 풀어보면 다음과 같습니다.

① **default-information originate**

default-information originate metric <0-16,777,214>

default-information originate metric-type <1-2> 중 한 가지 형식으로 입력

② **no-redistribution**

③ **no-summary**

④ **translator-role {candidate | never | always}**

다음은 옵션 중 한 가지만 선택하여 설정한 경우의 명령어입니다.

명령어	모 드	기 능
area area-ID nssa default-information originate		
area area-ID nssa default-information originate metric <0-16,777,214>		옵션 설정과
area area-ID nssa default-information originate metric-type <1-2>		함께 NSSA
area area-ID nssa no-redistribution	Router	로 설정합니
area area-ID nssa no-summary		다.
area area-ID nssa translator-role {candidate never always}		



참 고

두 가지 이상의 옵션값을 설정할 때에는 위에서 설명한 옵션 값을 순서에 상관없이 복수로 입력하시면 됩니다.

예) **area <0-4,294,967,295> nssa no-summary no-redistribution**

area <0-4,294,967,295> nssa translator-role {candidate | never | always} default-information originate metric-type <1-2> no-redistribution

위에서 설정한 내용을 해제하려면, 위의 명령어 앞에 **no** 명령어를 사용하시면 됩니다.

명령어	모 드	기 능
no area area-ID nssa	Router	NSSA로 설정한 것을 해제합니다.
no area area-ID nssa default-information originate		
no area area-ID nssa default-information originate metric <0-16,777,214>		
no area area-ID nssa default-information originate metric-type <1-2>		
no area area-ID nssa no-redistribution		
no area area-ID nssa no-summary		
no area area-ID nssa translator-role {candidate never always}		

(5) Area 경로 정보 요약 설정

OSPF가 여러 Area에 속해 있을 경우, 한 Area의 경로 정보가 실제로는 여러 경로로 나뉘어져 있으나, 그 경로에 대한 정보를 정리하면 하나의 경로로 나타낼 수 있습니다. 이와 같이 Area에 대한 여러 개의 경로 정보를 하나로 정리하여 요약된 정보를 외부로 전달할 수 있습니다.

요약된 경로 정보를 사용하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
area area-ID range ip-address/m	Router	해당 경로에 대해 요약된 정보를 사용하도록 설정합니다.
area area-ID range ip-address/m {advertise not-advertise}		

요약 경로 정보를 사용하면서 외부에도 요약된 경로 정보를 전달하도록 설정하려면 **advertise** 옵션을 사용하고, 외부에는 요약된 경로 정보를 알리지 않도록 하려면 **no-advertise** 옵션을 사용하십시오.

요약 경로 정보에 대한 설정한 내용을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no area area-ID range ip-address/m	Router	해당 경로에 대해 요약된 정보를 사용하도록 설정합니다.
no area area-ID range ip-address/m {advertise not-advertise}		

(6) Shortcut Area 설정

모든 OSPF의 Area 중 기본이 되는 Area를 Backbone Area라고 합니다. 여러 OSPF의 Area들이 서로 연결되어 있을 때에도 다른 Area로 트래픽이 전송될 때에는 반드시 Backbone Area를 통과하도록 OSPF 네트워크는 설계되어야 합니다.

그러나, 때로는 Backbone Area를 통과하지 않는 경로가 더욱 효율적일 때도 있습니다. 이러한 경우에 가장 효율적인 경로를 이용하게 되는 것은 Shortcut 특성을 사용한 것입니다. 이 때, 경로에서 트래픽을 전달하는 ABR은 모두 Shortcut 특성을 사용하도록 설정되어 있어야 하며 이에 대한 명령어는 **ospf abr-type** 명령어를 참조바랍니다.

Area에 Shortcut 특성을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
area area-ID shortcut { default disable enable }	Router	Area에 Shortcut 특성을 설정합니다.

Area에 설정한 Shortcut 특성을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no area area-ID shortcut { disable enable }	Router	설정된 Shortcut 특성을 해제합니다.

(7) Stub Area 설정

Stub Area는 ABR이 Backbone Area에 연결되어 있는 Area를 말합니다. Stub Area로 지정되면 별도로 기본 경로 설정을 하지 않아도 ABR이 기본 경로를 Stub Area에 알려주고, Stub Area에는 다른 라우팅 프로토콜의 경로 정보가 전달되지 않는 특성을 가집니다. Stub Area로 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
area area-ID stub [no-summary]	Router	Stub Area로 설정합니다.

Stub Area에 **no summary** 특성이 부가될 경우는 타 영역의 OSPF 경로 정보도 stub 영역내에 전파되지 않고, 오직 ABR 라우터로부터의 기본 경로 (default route) 만 전달됩니다. 이렇게 **no summary** 특성을 사용한 영역은 Totally Stubby 영역 (Area)로 알려져 있습니다.

Stub Area로 설정한 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no area area-ID stub [no-summary]	Router	Stub Area로 설정한 것을 해제합니다.

(8) Area 최대 개수 설정

사용자가 설정할 수 있는 Area의 최대 개수를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
maximum-area <1-4294967294>	Router	설정할 수 있는 Area의 최대 개수를 제한합니다.



V5812G의 설정 가능한 Area의 최대 개수는 기본적으로 4,294,967,294로 설정되어 있습니다.

설정 가능한 Area 최대 개수의 제한을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no maximum-area	Router	설정 가능한 Area의 최대 개수를 제한한 것을 해제합니다.

(9) 가상 경로 설정

OSPF 네트워크에서 모든 Area는 Backbone Area와 연결되어 있어야 합니다. 그러나 네트워크 설정 과정에서 Backbone Area와 연결되지 못한 Area도 발생하게 되는데, 이러한 경우에 다른 Area를 통해 Backbone Area와 연결하도록 하려면 가상 경로(Virtual Link)를 이용하게 됩니다. 가상 경로를 통해 연결된 라우터들은 OSPF 네트워크에서 Point-to-point를 이용해 연결된 라우터들처럼 처리합니다. 따라서 가상 경로를 통해 연결되어 있는 라우터들은 Hello-interval, Retransmit-interval, Transmit-delay 등 OSPF 인터페이스에 설정되는 값들을 모두 동일하게 가지고 있어야 합니다.

가상 경로에 대해 사용자가 설정할 수 있는 내용은, 경로 정보의 보안을 위한 인증, 인증을 사용할 때 사용하는 암호가 되는 인증키, 그리고, 가상 경로가 동작할 때 필요한 Hello-interval, Retransmit-interval, Transmit-delay, Dead-interval과 같은 시간 주기들입니다.

가상 경로에 대해 사용자가 설정할 수 있는 내용은 크게 7가지로 나눌 수 있습니다.

- **Authentication** : 경로 정보의 보안을 위해 인증을 사용합니다. **message-digest**는 인증을 위한 암호화 방식을 MD5 형식으로 사용하는 것이고, **null**은 인증 없이 동작하게 됩니다.
- **Authentication-key** : 인증을 사용할 때 암호가 되는 인증키 방식을 일반 텍스트 기반으로 사용합니다.
- **Message-digest-key** : 인증을 사용할 때 암호가 되는 인증키 방식을 md5로 사용합니다.
- **Hello-interval** : OSPF 라우터는 자신의 존재를 알리기 위해 일정한 시간 간격을 두고 보내는 Hello 패킷의 송신하는 간격을 설정합니다.
- **Retransmit-interval** : LSA 정보에 대한 승인 정보를 받지 못하여 LSA 정보를 재송신하기까지의 시간 간격을 설정합니다.
- **Dead-interval** : OSPF 네트워크에 존재하는 라우터들은 정기적으로 Hello 패킷을 보내도록 되어 있습니다. 그런데, 특정 라우터로부터 일정 시간동안 Hello 패킷이 전송되지 않는다면, 그 라우터는 동작을 멈추었다고 판단하게 됩니다. 이와 같이 특정 라우터가 동작을 멈추었다고 판단하기까지 기다리는 시간인 Dead-interval을 설정합니다.
- **Transmit-delay** : 라우터가 다른 라우터에게 LSA를 송신할 때, 통신 상태에 따라 LSA의 전송이 지연될 수 있습니다. 이를 고려하여 LSA를 전송하는데 걸리는 시간을 설정합니다.

위에서 설명한 가상 경로에 대해 설정하는 옵션은 순서에 상관없이 복수로 설정이 가능합니다. 옵션에 대한 명령어를 이해하기 쉽게 풀어보면 다음과 같습니다.

- ① **authentication [message-digest | null]**
- ② **authentication-key key**
- ③ **message-digest-key key md5 key**
- ④ **hello-interval <1-65,535>**
- ⑤ **retransmit-interval <1-65,535>**
- ⑥ **dead-interval <1-65,535>**
- ⑦ **transmit-delay <1-65,535>**

다음은 옵션 중 한 가지만 선택하여 설정한 경우의 명령어입니다.

명령어	모드	기능
<code>area <0-4,294,967,295> virtual-link ip-address authentication [message-digest null]</code>	Router	가상 경로에 대해 설정합니다.
<code>area <0-4,294,967,295> virtual-link ip-address authentication-key key</code>		
<code>area <0-4,294,967,295> virtual-link ip-address message-digest-key key md5 key</code>		
<code>area <0-4,294,967,295> virtual-link ip-address hello-interval <1-65,535></code>		
<code>area <0-4,294,967,295> virtual-link ip-address retransmit-interval <1-65,535></code>		
<code>area <0-4,294,967,295> virtual-link ip-address dead-interval <1-65,535></code>		
<code>area <0-4,294,967,295> virtual-link ip-address transmit-delay <1-65,535></code>		



두 가지 이상의 옵션값을 설정할 때에는 위에서 설명한 옵션 값을 순서에 상관없이 복수로 입력하시면 됩니다.

예) `area <0-4,294,967,295> virtual-link ip-address authentication-key key authentication [message-digest | null]`

`area <0-4,294,967,295> virtual-link ip-address hello-interval <1-65,535> dead-interval <1-65,535>`

가상 경로에 대한 설정을 해제하려면, 위에서 설명한 명령어에 no 명령어를 사용하시면 됩니다.

명령어	모드	기능
<code>no area <0-4,294,967,295> virtual-link ip-address authentication [message-digest null]</code>	Router	가상 경로에 대한 설정을 해제합니다.
<code>no area <0-4,294,967,295> virtual-link ip-address authentication-key key</code>		
<code>no area <0-4,294,967,295> virtual-link ip-address message-digest-key key md5 key</code>		
<code>no area <0-4,294,967,295> virtual-link ip-address hello-interval <1-65,535></code>		
<code>no area <0-4,294,967,295> virtual-link ip-address retransmit-interval <1-65,535></code>		
<code>no area <0-4,294,967,295> virtual-link ip-address dead-interval <1-65,535></code>		
<code>no area <0-4,294,967,295> virtual-link ip-address transmit-delay <1-65,535></code>		

11.2.7. 기본 경로값 변경

OSPF는 인터페이스의 대역폭을 기준으로 기본 경로값을 정합니다. 예를 들어, T1 라인의 기본 경로값은 64이지만 64K 라인의 기본 경로값은 1562입니다. 만약 대역폭이 다른 여러 개의 경로가 있다면, 각 경로에 기본 경로값을 할당하여 각 경로를 사용하는데 소요되는 cost를 확인할 수 있습니다.

경로 기본값을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
auto-cost reference-bandwidth <1-4,294,967>	Router	경로 기본값을 설정합니다.



경로 기본값의 설정 단위는 Mbits/second 입니다.



현재 표준 대역폭은 100Mbps로 시스템 설정되어 있습니다.

위에서 설정한 기본 경로값을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no auto-cost reference-bandwidth	Router	설정한 경로 기본값을 삭제합니다.

11.2.8. Graceful Restart 지원

사용자는 네트워크에 문제가 발생하였거나 특별한 경우에 OSPF 프로토콜의 프로세서를 재부팅해야 할 때가 있습니다. 이러한 경우에는 일반적으로 OSPF가 멈추었다가 시작하기까지는 시간이 많이 소요되는데 이 기간 동안은 패킷이 전달되지 못하게 됩니다. 또한 주변 라우터들은 OSPF를 재부팅하는 라우터에 대한 경로 정보를 삭제하였다가, 재부팅이 된 이후에 다시 이를 등록하는 과정을 거쳐야 하는 불편함이 있습니다.

이러한 문제점을 개선한 것이 Graceful Restart인데, 이 기능을 사용하면 OSPF를 재부팅하는 중에도 기존에 사용되고 있던 경로 정보를 통해 패킷을 계속해서 전달할 수 있습니다.

사용자의 장비에 Grace Restart를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
capability restart {graceful reliable-graceful signaling}	Router	Graceful Restart 기능을 설정합니다.

기존의 **graceful**은 helper한테 재가동 메시지를 보낸 후 곧장 재가동하는 것입니다. 한편, NOS 3.27 버전에서 새롭게 추가된 **reliable-graceful**은 장비가 restart 하기 위해 helper에게 메시지를 보내고 응답이 돌아올 때까지 대기했다가, 응답을 받은 후에 재가동하는 기능입니다.

설정한 Graceful Restart 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no capability restart	Router	Graceful Restart 기능을 설정한 것을 해제합니다.

위의 설정을 통해 실제로 Graceful Restart 기능을 사용할 때, 몇 가지 부가적인 설정을 할 수 있습니다.

- **Grace-period** : OSPF 프로세스가 재기동할 경우, **grace-period**로 설정된 시간동안 프로세스의 상태를 **graceful**로 유지합니다. 이 시간이 지나야 정상적인 OSPF 상태로 동작하게 됩니다.

- **Helper** : Graceful Restart 기능이 사용되고 있는 경우, 재부팅하고 있는 라우터 주변의 다른 OSPF 라우터들을 도와주는 기능입니다. 재부팅하고 있는 동안 라우터가 마치 정상적으로 동작하는 것처럼 다른 라우터에 정보를 전달하는 역할 등을 하게 됩니다. **only-reload**는 주변의 OSPF 라우터가 재부팅 할 경우만 helper로 동작하게 되고, **only-upgrade**는 OSPF 소프트웨어가 업그레이드 될 때만 helper로서 동작하게 됩니다. 또한 **max-grace-period**는 주변의 라우터로부터 받은 **grace-period** 정보가 이 값보다 작을 경우만 동작하게 됩니다. Helper에 대한 옵션 설정은 순서에 상관없이 복수로 설정이 가능합니다.

Graceful Restart 기능에 위에서 설명한 부가적인 설정을 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ospf restart grace-period <1-1,800>	Global	Graceful restart에 대해 부가적인 기능을 설정합니다.
ospf restart helper max-grace-period <1-1,800>		
ospf restart helper max-grace-period <1-1,800> only-reload [only-upgrade]		
ospf restart helper max-grace-period <1-1,800> only-upgrade [only-reload]		
ospf restart helper only-reload [only-upgrade]		
ospf restart helper only-reload only-upgrade max-grace-period <1-1,800>		
ospf restart helper only-reload max-grace-period <1-1,800> [only-upgrade]		
ospf restart helper only-upgrade [only-reload]		
ospf restart helper only-upgrade only-reload max-grace-period <1-1,800>		
ospf restart helper only-upgrade max-grace-period <1-1,800> [only-reload]		

Graceful Restart 기능에 설정한 설명한 부가적 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ospf restart grace-period <1-1,800>	Global	Graceful restart에 대한 해당 부가 기능을 해제합니다.
ospf restart helper never		
no ospf restart helper max-grace-period <1-1,800>		

11.2.9. Opaque-LSA 지원

Opaque-LSA는 LSA Type-9, Type-10, Type-11을 말합니다. V5812G의 시스템은 기본적으로 Opaque-LSA를 처리가 가능하도록 설정되어 있지만, 사용자는 이 기능을 해제할 수 있습니다. Opaque-LSA를 처리할 수 있도록 되어 있는 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no capability opaque	Router	Opaque-LSA를 처리하도록 설정되어 있는 것을 해제합니다.

다시 Opaque-LSA를 처리할 수 있도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
capability opaque	Router	Opaque-LSA가 사용가능하도록 설정합니다.

11.2.10. 기본 경로 설정

사용자는 관리 ASBR이 OSPF 네트워크에 기본경로를 전달하도록 설정할 수 있습니다. ASBR은 OSPF 네트워크에 외부에서 생성한 경로를 전달하는 라우터입니다. 그러나 ASBR는 시스템 기본 경로를 생성하지 않습니다.

V5812G는 이러한 경우에 기본 경로를 설정할 수 있습니다. ASBR에 기본 경로를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
default-information originate	Router	기본 경로를 설정합니다.

한편, 기본 경로를 설정할 때에는 다음과 같은 세부 사항도 함께 설정할 수 있습니다.

- **Metric** : 기본 경로의 메트릭 값을 설정합니다.
- **Metric-type** : 경로 계산 방식을 선정하는 것인데 **metric-type 1**은 내부 경로 cost와 외부 경로 cost를 더한 값을 경로 cost로 사용하게 되고, **metric-type 2**는 언제나 외부 경로의 cost 값만 사용하게 됩니다.
- **Always** : 기본 경로를 외부로 전달할 수 있도록 설정합니다.
- **No-summary** : OSPF Area 간의 경로 정보를 NSSA내에서 전달하지 못하도록 설정합니다.
- **Route-map** : 특정 경로 정보를 지정한 map_name을 가진 경로에 적용하여 전달합니다.

위에서 설명한 바와 같이 기본 경로에 설정할 수 있는 세부 항목은 크게 4가지로 구분되고, 이 4가지에 대한 설정은 순서에 상관없이 복수 설정이 가능합니다.

옵션에 대한 명령어를 이해하기 쉽게 풀어보면 다음과 같습니다.

- ① **metric <0-16,777,214>**
- ② **metric-type <1-2>**
- ③ **always**
- ④ **route-map map_name**

다음은 옵션 중 한 가지만 선택하여 설정한 경우의 명령어입니다.

명령어	모 드	기 능
default-information originate metric <0-16,777,214>		
default-information originate metric-type <1-2>	Router	옵션 설정과 함께 기본 경로를 설정합니다.
default-information originate always		
default-information originate route-map map_name		



참 고

두 가지 이상의 옵션값을 설정할 때에는 위에서 설명한 옵션 값을 순서에 상관없이 복수로 입력하시면 됩니다.

예) **default-information originate metric-type <1-2> always**

default-information originate route-map map_name metric <0-16,777,214>

기본 경로 설정에 대한 내용을 삭제하려면, 다음 명령어를 사용하십시오.

기본 경로 설정 명령어는 아래와 같습니다.

명령어	모 드	기 능
no default-information originate		
no default-information originate metric <0-16,777,214>	Router	기본 경로에 대한 설정을 삭제합니다.
no default-information originate metric-type <1-2>		
no default-information originate always		
no default-information originate route-map map_name		

11.2.11. 경로 계산 주기 설정

OSPF 라우터는 일반적으로 OSPF 네트워크의 구성이 변경 되었음을 통지 받으면, 최단 경로를 계산하기 시작합니다. 그러나, 사용자는 경로를 계산하는 주기를 직접 설정할 수 있습니다.

경로를 계산하는 주기를 설정 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
timers spf spf-delay spf-hold	Router	경로 계산 주기를 설정합니다.



참 고

기본적으로 spf-delay는 5초, spf-hold는 10초로 지정되어 있습니다.



참 고

spf-delay와 spf-hold는 각각 <0 – 2,147,483,647> 범위에서 입력할 수 있습니다.

경로 계산 주기를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no timers spf	Router	설정된 경로 계산 주기를 해제하고 시스템 설정값으로 복구시킵니다.

11.2.12. ECMP(Equal Cost Multi-Path) 설정

ECMP는 동일한 경로에 대한 정보가 두 개 이상의 인터페이스에 등록되어 있을 때, 패킷이 가장 적절한 인터페이스를 통한 경로를 이용하여 전달될 수 있도록 하는 기능입니다. 일반적으로 하나의 인터페이스에 트래픽 양이 많을 때, 다른 인터페이스로 패킷을 분산하여 인터페이스의 과부하 현상을 막는 용도로 사용됩니다. V6524G는 ECMP 기능을 기본적으로 제공하며, 패킷을 분산시키기 위한 방법으로는 Source 주소를 이용하는 방법과 Source 주소와 Destination 주소를 모두 이용하는 방법의 2가지 방식을 사용합니다.

ECMP를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip ecmp-hash { sip sip-dip }	Global	ECMP를 설정합니다.

sip는 패킷을 분산시키기 위한 방법 중에 Source 주소를 이용하는 방법을 사용하는 것이고, **sip-dip**는 Source 주소와 Destination 주소를 모두 이용하는 방법입니다.

한편, ECMP 기능을 사용할 때 최대 링크 수를 지정할 수 있습니다. 기본적으로는 2개의 링크를 사용할 수 있도록 설정되어 있으나 최대 8개 링크까지 사용할 수 있도록 설정 가능합니다.

ECMP에서 사용할 수 있는 최대 링크 수를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip maximum-paths <1-8>	Global	ECMP에서 사용할 수 있는 최대 링크 수를 지정합니다.

11.2.13. 외부 경로 전달

OSPF 네트워크에 다른 라우팅 프로토콜이 작성한 경로가 전달되면 이러한 경로는 OSPF 외부 경로가 됩니다. OSPF 네트워크로 전달될 수 있는 프로토콜의 종류로는 RIP, BGP가 있고, 그 밖에도 시스템상에서 수동으로 설정하는 static 경로와 인터페이스에 연결된 connected 경로, 그리고 커널이 가지고 있는 kernel 경로 정보들도 OSPF 네트워크로 전달될 수 있습니다.

이러한 외부 경로의 전달에 대해서 설정할 때에는 4가지 부가적 설정이 가능합니다. **metric**은 기본 경로의 메트릭 값을 설정하는 것이고, **metric-type**은 경로 계산에 쓰는 방식을 선정하는 것입니다. **metric-type 1**은 내부 경로 cost 와 외부 경로 cost 를 더한 값을 경로 cost로 사용하는 반면, **metric-type 2**는 언제나 외부 경로의 cost 값만 사용하게 됩니다. **route-map**은 특정 경로를 처리할 때 지정된 map-name을 사용하는 것이고, **tag**는 특정 map_name에 지정한 tag 번호를 이용할 때 사용합니다.

위에서 설명한 4가지 부가 기능은 순서에 상관없이 복수로 설정할 수 있습니다. 또한, 각 종류의 외부 경로에 모두 동일하게 적용됩니다. 4가지 부가 기능을 설정하는 옵션값을 명령어로 나타내면 다음과 같습니다.

- ① **metric <0-16,777,214>**
- ② **metric-type <1-2>**
- ③ **route-map map_name**
- ④ **tag <0-4,294,967,295>**

다음은 위에서 설명한 옵션을 한가지만 설정하여 외부 경로 전달에 대한 설정을 할 때 사용한 명령어입니다.

명령어	모 드	기 능
redistribute { bgp connected kernel rip static} metric <0-16,777,214>	Router	옵션 설정과 외부 경로 전달에 대한 설정을 합니다.
redistribute { bgp connected kernel rip static} metric-type <1-2>		
redistribute { bgp connected kernel rip static} route-map map_name		
redistribute { bgp connected kernel rip static} tag <0-4,294,967,295>		



참 고

두 가지 이상의 옵션값을 설정할 때에는 위에서 설명한 옵션 값을 순서에 상관없이 복수로 입력하시면 됩니다.

예) **redistribute { bgp | connected | kernel | rip | static} metric <0-16,777,214> tag <0-4,294,967,295>**

redistribute { bgp | connected | kernel | rip | static} tag <0-4,294,967,295> metric-type <1-2>

위에서 설정한 방법에 따라 재전송된 경로에 대해서는 Default-metric을 통해 Metric을 지정할 수 있습니다. 위의 명령어만을 사용하여 OSPF 네트워크에 경로 정보를 재전송할 경우 경로와 Metric이 일치하지 않을 수 있습니다. 이러한 경우에 Default-metric을 설정함으로써 재전송하는 경로에 대한 Metric을 일괄적으로 설정하면, 효율적으로 경로 정보를 전달할 수 있습니다.

외부 경로에 대한 Metric을 일괄적으로 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
default-metric <0-16,777,214>	Router	OSPF로 전달된 모든 외부 경로에 대해 Metric을 일괄적으로 설정합니다.

외부 경로에 대해 일괄적으로 설정한 Metric을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no default-metric [0-16,777,214]	Router	Default-metric을 삭제합니다.

11.2.14. OSPF 거리값 변경

거리값은 라우터가 생성하는 라우팅 정보에 대한 신뢰도를 나타냅니다. 거리값을 나타내기 위해 0부터 255 까지의 숫자를 사용할 수 있는데 거리값이 높을수록 신뢰도는 낮습니다. 따라서 거리값이 255인 라우팅 정보는 거의 신뢰할 수 없는 정보를 의미합니다.

OSPF는 intra-area, inter-area, external의 세 가지 거리값을 사용합니다. 다른 네트워크를 통해 전달 받은 외부 경로는 external 경로, OSPF 도메인 안에 있는 다른 Area 사이에 전달한 경로는 inter-area 경로, 한 Area 내에서 주고 받는 경로는 intra-area 경로라고 합니다. 이 세 가지 경로의 거리값은 순서에 상관없이 복수로 설정할 수 있습니다.



세 가지 경로에 대해 기본적으로 설정되어 있는 기본 거리값은 110입니다.

세 가지 종류의 경로에 대한 거리 값을 설정하는 옵션 명령어는 다음과 같습니다.

- ① **external <1-255>**
- ② **inter-area <1-255>**
- ③ **intra-area <1-255>**

다음은 한 가지 종류의 경로에 대한 거리 값을 설정할 때 사용하는 명령어입니다.

명령어	모 드	기 능
distance ospf external <1-255>		
distance ospf inter-area <1-255>	Router	OSPF의 경로 유형에 따른 거리 값을 설정합니다.
distance ospf intra-area <1-255>		



두 가지 이상의 옵션값을 설정할 때에는 위에서 설명한 옵션 값을 순서에 상관없이 복수로 입력하시면 됩니다.

예) **distance ospf external <1-255> inter-area <1-255>**
distance ospf inter-area <1-255> intra-area <1-255>

경로에 대한 거리값을 기본값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no distance ospf	Router	경로에 대한 거리값을 기본값으로 되돌립니다.

11.2.15. 호스트 경로 설정

OSPF에서는 특정한 호스트에 대한 경로 정보를 stub 링크 정보로 처리할 수 있습니다. 다시 말해, 하나의 라우터에 연결된 개별 호스트들에 대해 필요에 따라 경로 정보를 지정할 수 있습니다.

개별 호스트의 경로 정보를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
host ip-address area ip-address		
host ip-address area ip-address cost <0-65,535>	Router	특정 호스트의 경로 정보를 특정 영역에 할당합니다. 필요시 cost 정보도 설정할 수 있습니다.
host ip-address area <1-4,294,967,295>		
host ip-address area <1-4,294,967,295> cost <0-65,535>		

11.2.16. 수동 인터페이스 설정

OSPF 네트워크에서 passive로 설정한 인터페이스는 stub Area처럼 동작합니다. 따라서 passive 인터페이스에서는 OSPF 라우팅 정보를 주고 받을 수 없습니다. 인터페이스가 라우팅 정보를 전달하지 않도록 하려면, Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
passive-interface interface-name [ip-address]	Router	지정한 인터페이스는 라우팅 정보를 전달하지 않습니다.

지정된 인터페이스에 대한 라우팅 정보를 전달하지 않도록 설정한 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no passive-interface interface-name [ip-address]	Router	지정된 인터페이스에 대한 라우팅 정보를 전달하지 않도록 설정한 것을 해제합니다.

11.2.17. 갱신된 정보 전달 제어

V5812G는 다른 라우팅 프로토콜이나 라우터에 직접 연결된 인터페이스 등에서 생긴 라우팅 정보를 OSPF를 통해 선별적으로 전달하도록 설정할 수 있습니다. 이 기능을 설정하기 위해서는 먼저 외부 라우팅 정보들 중에서 특정한 경로 정보들을 access-list 명령어로 선정하고, access-list로 선정한 경로 정보를 차단합니다. Access-list에 등록한 특정 경로 정보의 외부 전달을 차단하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
distribute-list access_list_name out { bgp connected kernel rip static}	Router	Access-list에 등록한 경로 정보의 외부 전달을 차단합니다.

해당 정보의 외부 전달을 차단하도록 설정한 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no distribute-list access_list_name out { bgp connected kernel rip static}	Router	Access-list에 등록한 경로 정보의 외부 전달을 차단합니다.

11.2.18. 요약 경로 정보 전달

OSPF 네트워크에 외부 라우팅 프로토콜의 경로 정보를 전달할 경우, 두 가지 이상의 경로를 하나의 경로로 요약하여 전달할 수 있습니다. 예를 들어, 192.168.1.0/24와 192.168.2.0/24의 두 외부 경로는 192.168.0.0/16이라는 하나의 경로 정보로 OSPF 네트워크에 전달할 수 있습니다.

이러한 방식으로 외부 경로 정보를 요약하여 전달하면, 경로 정보의 개수를 줄임으로서 OSPF 프로토콜의 안정성을 높일 수 있습니다.

한편, **not-advertise** 옵션을 이용하면 해당하는 외부 경로 정보를 전달하지 못하게 설정할 수도 있고, 특정한 **tag** 번호를 지정하여 설정할 수도 있습니다.

요약 경로 정보를 전달하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
summary-address ip-address/m	Router	특정 경로에 해당하는 외부 경로 정보를 요약하여 OSPF 네트워크 내에 전달합니다.
summary-address ip-address/m not-advertise		요약 경로 정보를 외부로 전달하지 않도록 설정합니다.
no summary-address ip-address/m tag <0-4,294,967,295>		요약 경로 정보를 특정한 tag 번호를 지정하여 설정합니다.

11.2.19. OSPF 모니터링과 관리

V5812G는 OSPF 프로토콜에 대한 설정과 관련된 통계나 데이터베이스를 확인할 수 있습니다. 이러한 정보는 시스템의 효율성을 높이고, 네트워크에 문제가 발생하였을 때 문제를 해결하는데 유용하게 사용됩니다. 또한, 네트워크 연결 상태나 데이터 전송시 데이터가 거쳐간 경로도 확인할 수 있습니다.

(1) OSPF 프로토콜 정보 출력

사용자는 OSPF 프로토콜과 관련된 여러 가지 정보를 확인할 수 있습니다. 다음은 각 정보를 확인하는데 사용하는 명령어에 대한 설명입니다.

OSPF 프로토콜과 관련된 전반적인 내용의 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip ospf	Enable/ Global	OSPF 프로토콜과 관련된 전반적인 정보를 확인합니다.
show ip ospf <0-65,535>		OSPF 프로토콜에 대한 정보 중 특정 Process ID에 대한 내용을 확인합니다.

ABR과 ASBR에게 OSPF 라우팅 테이블 정보를 보여주려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip ospf border-routers	Enable/Global	ABR과 ASBR에게 OSPF 라우팅 테이블 정보를 보여줍니다.

OSPF 데이터베이스와 관련된 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip ospf database {self-originated max-age}		
show ip ospf database adv-router ip-address		
show ip ospf database {asbr-summary external network router summary nssa-external opaque-link opaque-area opaque-as}		
show ip ospf database {asbr-summary external network router summary nssa-external opaque-link opaque-area opaque-as} self-originated		OSPF
show ip ospf database {asbr-summary external network router summary nssa-external opaque-link opaque-area opaque-as} adv-router ip-address	Enable/ Global	프로토콜과 관련된 데이터베이 스를
show ip ospf database {asbr-summary external network router summary nssa-external opaque-link opaque-area opaque-as} ip-address		확인합니다.
show ip ospf database {asbr-summary external network router summary nssa-external opaque-link opaque-area opaque-as} ip-address self-originated		
show ip ospf database {asbr-summary external network router summary nssa-external opaque-link opaque-area opaque-as} ip-address adv-router ip-address		

OSPF 인터페이스의 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip ospf interface [interface_name]	Enable/Global	OSPF 인터페이스 정보를 확인합니다.

OSPF 라우터와 통신하는 Neighbor 라우터의 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip ospf neighbor		
show ip ospf neighbor ip-address [detail]		
show ip ospf neighbor interface ip-address	Enable/Global	OSPF 라우터와 통신하는 Neighbor 라우터의 정보를 확인합니다.
show ip ospf neighbor detail [all]		
show ip ospf neighbor all		

OSPF 라우팅 테이블에 등록된 경로 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip ospf route	Enable/Global	OSPF 라우팅 테이블에 등록된 경로 정보를 확인합니다.

OSPF에 설정된 가상 링크에 대한 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip ospf virtual-links	Enable/Global	OSPF에 설정된 가상 링크에 대한 정보를 확인합니다.

(2) Debugging 정보 출력

V5812G는 네트워크에 문제가 발생하였을 때 debug 명령어를 사용하여 문제의 원인을 재빨리 파악할 수 있습니다. 네트워크에 문제가 발생하였을 때 원인을 파악하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
debug ospf all	Enable	OSPF와 관련된 모든 디버깅 정보를 확인합니다.
debug ospf events [abr asbr lsa nssa os router vlink]		OSPF Neighbor 라우터, 전달한 정보, 목적지 라우터 선출, 최단 경로 계산 등의 정보를 확인합니다.
debug ospf ifsm [events status timers]		OSPF 인터페이스와 관련된 디버깅 정보를 확인합니다.
debug ospf lsa [flooding generate refresh]		OSPF에서 전달한 정보와 최단 경로 계산 등을 확인합니다.
debug ospf fsm [events status timers]		OSPF Neighbor 라우터에 대한 정보를 확인합니다.
debug ospf nsm [events status timers]		OSPF 프로세스와 NSM(Network Services Module) 사이의 디버깅 정보를 확인합니다.
debug ospf packet {hello dd ls-ack ls-request ls-update all} [send recv [detail]]		각 패킷에 대한 정보를 출력한다.
debug ospf route [ase ia install spf]		OSPF의 각종 경로에 대한 세부 디버깅 정보를 확인합니다.
show debugging ospf	Global	OSPF와 관련된 디버깅 메시지를 출력한다.

(3) 데이터베이스 처리 개수 제한

V5812G는 OSPF 프로토콜에서 한 번에 처리할 수 있는 이터베이스의 개수를 제한하여 설정할 수 있습니다. 만약 하나의 라우터에 연결된 라우터의 개수가 너무 많아서 동시에 처리해야 하는 데이터베이스 수가 많아지면 이러한 처리 작업 자체가 라우터에 많은 부하를 줄 수 있습니다. 따라서, 한 번에 처리할 수 있는 데이터베이스의 수를 설정해주면, 처리 작업에 걸리는 시간은 좀 더 길어지지만, 시스템의 부하는 줄일 수 있는 효과가 있습니다.

한 번에 처리하는 데이터베이스의 개수를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
max-concurrent-dd <1-65,535>	Router	한 번에 처리하는 데이터베이스의 개수를 설정합니다.

한 번에 처리하는 데이터베이스 개수를 설정했던 것을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no max-concurrent-dd <1-65,535>	Router	한 번에 처리하는 데이터베이스 개수를 설정했던 것을 삭제합니다.

(4) 최대 처리가능 LSA값 설정

V5812G는 OSPF 프로세스에서 처리할 수 있는 LSA의 최대 개수를 지정할 수 있습니다. LSA는 OSPF 내부 경로에 대한 LSA와 외부경로에 대한 LSA로 나누어지는데, 처리 가능한 LSA의 최대 개수는 각 종류별로 지정이 가능합니다. 한편, OSPF 내부 경로에 대한 LSA의 처리 개수가 지정한 값을 넘었을 때에는 프로세스 자체를 멈추거나 경고 메시지를 전달하도록 설정할 수도 있습니다. 그리고, 외부 경로에 대한 LSA의 처리 개수가 지정한 값을 넘었을 때에는 일정 시간을 기다린 후에 OSPF 프로세스를 재부팅하도록 설정할 수 있습니다. 만약 이때 대기 시간을 0으로 지정한다면, 관리자가 재부팅을 하기 전까지 해당 OSPF 프로세스를 유지하게 됩니다.

OSPF 프로세스에서 처리할 수 있는 LSA의 최대 개수를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
overflow database <1-42,94,967,294> [hard soft]	Router	OSPF 내부 경로에 대한 LSA의 처리 개수를 지정합니다.
overflow database external <0-2,147,483,647> <0-65,535>		OSPF 외부 경로에 대한 LSA의 처리 개수를 지정합니다.

OSPF 내부 경로에 대한 LSA의 처리 개수를 지정할 때, **hard**를 선택하면, 지정한 처리 개수 이상이 되었을 때 프로세스를 멈추도록 하는 것이고, **soft**를 선택하면 경고 메시지를 전달하도록 설정하는 것입니다. OSPF 프로세스에서 처리할 수 있는 LSA의 최대 개수를 지정한 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no overflow database	Router	OSPF 내부 경로에 대한 LSA의 처리 개수를 지정한 것을 해제합니다.
no overflow database external [0-2,147,483,647] [0-65,535]		OSPF 외부 경로에 대한 LSA의 처리 개수를 지정한 것을 해제합니다.

11.3 RIP(Routing Information Protocol)

RIP(Routing Information Protocol)는 다른 라우팅 프로토콜에 비해 상대적으로 오래된 프로토콜이지만 규모가 작고 단일한 프로토콜로 운영되는 네트워크에서는 여전히 많이 쓰이고 있습니다. RFC 1058 (Routing Information Protocol (RIP)) 과 RFC 2453 (Routing Information Protocol (RIP) and Routing Information Protocol version 2 (RIPv2)) 에 정의된 RIP는 경로 수(hop count)로 패킷 경로를 결정하는 라우팅 프로토콜입니다.

RIP는 라우팅 정보를 교환하기 위해 UDP(User Datagram Protocol) 패킷을 사용합니다. V5812G는 30초마다 라우팅 정보를 전달하고, 180초가 지났는데도 다른 라우터로 부터 새로운 정보를 받지 못하면 라우팅 테이블에 등록된 정보를 사용할 수 없는 정보로 표시합니다. 그리고 나서 120초가 지나면 그 정보는 라우팅 테이블에서 삭제 됩니다.

RIP는 서로 다른 경로들을 비교하기 위한 단위로 경로수(hop count)를 사용합니다. 경로수란, 목적지에 도달하기까지 네트워크 내에서 지나가야 하는 라우터 수를 말합니다. 목적지가 직접 연결되어 있는 경우에 경로수는 「0」이고 도달할 수 없는 네트워크는 경로수가 「16」입니다. 경로수 범위가 좁기 때문에 RIP는 규모가 작은 네트워크에 적합합니다.

RIP 라우터는 다른 RIP 라우터에게서 Default network 정보를 전달 받거나 스스로 Default network 정보를 생성합니다. Default network 정보를 생성한 RIP 라우터는 이를 다른 RIP 라우터로 전달합니다. RIP는 구체적으로 명시된 네트워크의 인터페이스로만 라우팅 정보를 전달합니다. 라우팅 정보를 전달할 인터페이스의 네트워크가 명시되어 있지 않은 경우에는 RIP 정보를 Neighbor 라우터에게 전달하지 않습니다.

V5812G는 RIP 1과 RIP 2를 지원합니다. RIP 설정과 관련하여 다음과 같은 내용을 설명합니다.

- RIP 활성화
- RIP Neighbor 라우터 지정
- RIP 버전 지정
- RIP에서만 유효한 static 경로 생성
- 라우팅 정보 전달
- 전달되는 경로의 경로값 설정
- 거리값(Administrative distance) 설정
- 기본 경로(default route) 생성
- 라우팅 정보 필터링

- 최대 RIP 경로 개수 설정
- 시간 설정
- 경로 차단(split-horizon) 활성화/비활성화
- 인증 키 관리
- RIP 재기동
- RIP 수신 버퍼 크기 조절
- RIP 확인 및 관리

11.3.1. RIP 활성화

RIP 프로토콜을 사용하려면 반드시 RIP를 활성화 시켜야 합니다. RIP를 활성화 시키려면, 다음과 같이 설정하십시오.

1 단계 RIP를 활성화 시키려면, Global 설정 모드에서 다음 명령어를 사용하여 Router 설정 모드로 들어가십시오.

명령어	모 드	기 능
router rip	Global	RIP를 활성화하고 Router 설정 모드로 들어갑니다.
no router rip		RIP를 해제합니다.



참 고

위의 명령어를 사용하여 RIP를 해제할 경우, RIP와 관련된 모든 설정 내용은 초기화 됩니다.

2 단계 RIP로 운영할 네트워크를 지정합니다.

명령어	모 드	기 능
network {ip-address interface-name}	Router	RIP로 운영할 네트워크를 지정합니다.
no network {ip-address interface-name}		현재 RIP로 운영중인 네트워크에서 RIP를 해제합니다.

network ip-address 명령어를 이용하여 RIP가 동작하는 특정 네트워크 대역을 지정 할 수 있습니다. 예를 들어, 10.0.0.0/24 네트워크에 RIP가 설정되어 있다면 이 네트워크 대역은 RIP 프로토콜을 통해 관리되게 됩니다. 즉 이 네트워크 대역의 정보는 RIP 라우터들 사이에서 교환하게 되는 것입니다. 한편, RIP 네트워크에 속해 있는 인터페이스라고 해도 위의 **network** 명령어를 통해 RIP 네트워크로 지정하지 않으면 해당 인터페이스는 RIP 라우팅 정보를 주고 받을 수 없습니다. RIP 라우팅 정보를 가진 패킷은 **network interface-name** 명령어에서 지정한 인터페이스로 주고 받게 됩니다.

11.3.2. RIP Neighbor 라우터 지정

RIP는 브로드캐스트 프로토콜이기 때문에, RIP의 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	모 드	기 능
neighbor ip-address	Router	라우팅 정보를 교환할 Neighbor 라우터를 지정합니다.
no neighbor ip-address		지정된 Neighbor 라우터를 삭제합니다.

사용자는 **passive-interface** 명령어를 사용하여 특정 인터페이스에 라우팅 정보가 전달 되지 않도록 설정할 수 있습니다.

11.3.3. RIP 버전 지정

기본적으로 V5812G는 RIP 1과 RIP 2를 지원합니다. 그러나 RIP 1 타입 패킷만 주고 받거나 RIP 2 타입 패킷만 주고 받을 수 있도록 버전을 지정할 수 있습니다. 버전을 지정하려면, Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
version {1 2}	Router	RIP 1 타입 패킷이나 RIP 2 타입 패킷만 전송하기 위해 버전을 지정합니다.
no version {1 2}		특정 버전의 지정을 해제하고 기본 설정 상태로 돌아갑니다.

사용자는 시스템이 지원하는 RIP 버전을 지정할 수 있지만, 특정 인터페이스에서 전달되는 패킷의 RIP 버전을 설정할 수도 있습니다. 특정 인터페이스에서 보내는 RIP 패킷의 버전을 지정하려면, **interface** 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip rip send version 1		해당 인터페이스에서 RIP 1 타입 패킷 만을 보냅니다.
ip rip send version 2	Interface	해당 인터페이스에서 RIP 2 타입 패킷 만을 보냅니다.
ip rip send version 1 2		해당 인터페이스에서 RIP 1와 RIP 2 타입 패킷을 보냅니다.

한편 특정 인터페이스에서 보내는 RIP 패킷의 버전 설정을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip rip send version 1	Interface	해당 인터페이스에서 RIP 1 타입 패킷 만 보내는 설정을 해제합니다.
no ip rip send version 2		해당 인터페이스에서 RIP 2 타입 패킷 만 보내는 설정을 해제합니다.
no ip rip send version 1 2		해당 인터페이스에서 RIP 1, RIP 2 타입 패킷을 보내는 설정을 해제합니다.

마찬가지로 특정 인터페이스가 특정 버전의 RIP 패킷만을 수신하도록 하려면 interface 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip rip receive version 1	Interface	해당 인터페이스에서 RIP 1 타입 패킷 만을 받습니다.
ip rip receive version 2		해당 인터페이스에서 RIP 2 타입 패킷 만을 받습니다.
ip rip receive version 1 2		해당 인터페이스에서 RIP 1, RIP 2 타입 패킷을 받습니다.

역시 특정 버전의 RIP 패킷 수신 설정을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip rip receive version 1	Interface	해당 인터페이스에서 RIP 1 타입 패킷 만을 받는 설정을 해제합니다.
no ip rip receive version 2		해당 인터페이스에서 RIP 2 타입 패킷 만을 받는 설정을 해제합니다.
no ip rip receive version 1 2		해당 인터페이스에서 RIP 1, RIP 2 타입 패킷을 받는 설정을 해제합니다.

11.3.4. RIP에서만 유효한 Static 경로 생성

route 명령어는 RIP 내에서만 유효한 static 경로를 생성합니다. 다음은 RIP 내에서만 유효한 static 경로를 만들 때 사용하는 명령어입니다.

명령어	모 드	기 능
route ip-address/m	Router	RIP 내에서만 사용되는 static 경로를 만듭니다.
no route ip-address/m		route 명령어로 만든 static 경로를 해제합니다.



참 고

만일 RIP 프로토콜을 많이 다루어 본 고급 사용자가 아니라면, 이 명령어 대신에 **redistribute static** 명령어를 사용하여 static 경로를 배포하십시오.

11.3.5. 라우팅 정보 전달

V5812G 스위치는 전달 받은 라우팅 정보를 다른 RIP 라우터로 전달할 수 있습니다. 라우터와 직접 연결된 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.

RIP에서 생성되지 않은 라우팅 정보를 받아 다른 장비 RIP 테이블에 등록하려면, Router 설정모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
redistribute {connected kernel static ospf bgp}	Router	전달 받은 라우팅 정보를 다른 라우터의 RIP 테이블에 등록합니다.
redistribute {connected kernel static ospf bgp} metric <0-16>		
redistribute {connected kernel static ospf bgp} route-map text		
no redistribute {connected kernel static ospf bgp}		다른 라우팅 정보를 전달 받는 설정을 해제합니다.
no redistribute {connected kernel static ospf bgp} metric <0-16>		
no redistribute {connected kernel static ospf bgp} route-map text		

11.3.6. 특정 라우팅 정보 전달

사용자는 필요에 따라 두 네트워크가 특정 정보만을 주고 받을 수 있도록 라우팅 정보를 제한할 수 있습니다. V5812G는 Route map을 이용하여 특정 라우팅 정보를 전달하도록 설정합니다.

전달하는 라우팅 정보를 제한하려면, 다음과 같은 방법으로 설정하십시오.

1 단계 Route map을 이용하여 특정 정보만을 전달하려면, Global 모드에서 다음 명령어를 사용해 Route-map 설정 모드로 들어가십시오.

명령어	모 드	기 능
route-map tag {deny permit} sequence-number	Global	라우트 맵을 생성합니다.

2 단계 라우트 맵을 생성하기 위해 Route-map 설정 모드로 들어간 후에는 **match**와 **set** 명령어를 사용하여 다른 라우터로 전달할 라우팅 정보를 제한하는 설정을 해야 합니다.

다른 라우터로 전달할 라우팅 정보를 제한하려면, Route-map 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
match interface <i>interface-name</i>	Route-map	지정한 인터페이스로만 정보를 전달합니다.
match ip address <i>{<1-199> <1300-2699> access-list-name}</i>		지정한 Access-list에 부합된 정보만 전달합니다.
match ip address prefix-list <i>ip-prefix-list-name</i>		지정한 Prefix-list에 부합된 정보만 전달합니다.
match ip next-hop <i>{<1-199> <1300-2699> access-list-name}</i>		Access-list에 있는 Neighbor 라우터에만 정보를 전달합니다.
match ip next-hop prefix-list <i>ip-prefix-list-name</i>		Access-list에 있는 Neighbor 라우터에만 정보를 전달합니다.
match metric <0-4,294,967,295>		지정한 거리값과 일치하는 정보만 전달합니다.
set ip next-hop <i>ip-address</i>		Neighbor 라우터 주소를 설정합니다.
set metric <0-4,294,967,295>		거리값을 설정합니다.

11.3.7. 전달되는 경로의 경로값 설정

하나의 라우팅 프로토콜이 각 경로를 비교하기 위해 사용하는 경로값은 다른 라우팅 프로토콜에서 사용하는 경로값을 계산하는 방법이 서로 다릅니다. 예를 들면, RIP는 경로 수를 기준값으로 사용하지만 OSPF는 다섯 가지 수치를 조합해서 경로 값을 산출합니다. 라우팅 프로토콜은 전달 받은 경로의 경로값을 자신이 사용하는 경로값으로 바꾸기 때문에 서로 다른 라우팅 프로토콜들이 아무런 규약없이 라우팅 정보를 주고 받게 되면 라우팅 정보가 공전하면서 네트워크 성능이 현격히 떨어질 수 있습니다. 이런 경우를 방지하기 위해 사용자는 다른 라우터로 배포되는 경로의 경로값을 인위적으로 지정합니다. 배포되는 경로의 경로값을 설정하려면, Router 설정 모드에서 다음 명령어를 수행 하십시오.

명령어	모 드	기 능
default-metric <1-16>	Router	라우팅 프로토콜이 전달하는 모든 경로에 동일한 경로값을 지정합니다.
no default-metric [1-16]		라우팅 프로토콜이 전달하는 모든 경로에 동일한 경로값을 지정하도록 설정한 것을 해제 합니다.



참 고

모든 프로토콜에서 사용 가능한 경로값 범위는 0-4294967295 입니다. RIP 에서 유효한 값은 1에서 16입니다.

11.3.8. 9.3.8 거리값(Administrative Distance) 설정

거리값은 라우터가 생성하는 라우팅 정보에 대한 신뢰도를 나타냅니다. 다양한 라우팅 프로토콜과 라우팅 정보를 가지는 큰 규모의 네트워크에서는 그 중에서도 신뢰성이 큰 것이 가려질 것이고, 그러한 경우에 여러 개의 라우팅 프로토콜 중에서 신뢰성이 가장 높은 경로만을 사용할 수 있습니다. 사용자가 거리값을 설정함으로써 라우터는 어디에서 라우팅 정보가 생성 되었는지 명백히 알 수 있습니다. 라우터는 항상 거리값이 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 거리값을 지정해야 합니다.

Router 설정 모드에서 다음 명령어를 사용하여 거리값을 설정하십시오.

명령어	모 드	기 능
distance <1-255> [ip-address/m]	Router	거리값을 지정합니다.
distance value ip-address/m [access-list-name]		
no distance <1-255> [ip-address/m]	Router	거리값 지정을 해제합니다.
no distance value ip-address/m [access-list-name]		

11.3.9. 기본 경로(Default Route) 생성

사용자는 RIP 경계 라우터가 RIP 네트워크에 기본 경로를 전달하도록 설정할 수 있습니다. 사용자가 RIP 네트워크에 라우팅 정보를 전달하도록 설정하면, 해당 라우터는 AS 경계 라우터가 됩니다. 그러나, AS 경계 라우터는 자동으로 기본 경로를 생성해서 RIP 네트워크에 전달하지는 않습니다. AS 경계 라우터가 기본경로를 전달하도록 하려면, Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
default-information originate	Router	AS 경계 라우터가 RIP 네트워크에 기본 경로를 전달하도록 합니다.
no default-information originate		AS 경계 라우터의 기본 경로 전달 설정을 해제합니다.

11.3.10. 라우팅 정보 필터링

V5812G는 다음과 같은 방법으로 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 경로값이 자동으로 증가 되도록 합니다.

(1) 특정 경로 정보에 대한 Access-list 및 Prefix-list 차단

V5812G는 특정한 조건에 맞은 경로 정보를 차단하기 위해 access-list 혹은 prefix-list를 사용합니다. 사용자는 access-list나 prefix-list에 특정한 조건에 맞는 경로 정보를 작성하고, 각 인터페이스에 이에 해당하는 정보가 수신되는 경우, 또는 인터페이스에 외부로 이에 해당하는 정보가 송신되는 경우에 distribute-list 명령어를 사용해 이를 차단할 수 있습니다. 또한, 이러한 설정은 특정 인터페이스 뿐만 아니라 장비의 전체 경로 정보에도 적용할 수 있습니다.

특정 인터페이스나 장비의 전체 경로 정보에 대해 해당 access-list나 prefix-list에 부합되는 경로 정보를 차단하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
distribute-list access_list_name {in out} [interface-name]		특정 인터페이스나 전체 경로 정보에 대해 access-list나 prefix-list를 이용해 경로 정보를 차단합니다.
distribute-list prefix prefix_list_name {in out} [interface-name]	Router	
no distribute-list access_list_name {in out} [interface-name]		특정 인터페이스나 전체 경로 정보에 대해 경로 정보를 차단하도록 설정한 것을 해제합니다.
no distribute-list prefix prefix_list_name {in out} [interface-name]		

(2) 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 BGP를 제외한 모든 IP 기반 라우팅 프로토콜에 적용됩니다.

라우터의 인터페이스에서 라우팅 정보가 나가지 못하도록 차단하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
passive-interface <i>interface-name</i>	Router	라우터의 인터페이스가 라우팅 정보를 전달하지 못하도록 합니다.
no passive-interface <i>interface-name</i>	Router	라우터의 인터페이스가 라우팅 정보를 전달하지 못하도록 설정한 것을 해제합니다.

(3) 경로값 증가 기능 설정

한편, 위에서 설명한 바와 같이 라우팅 정보를 필터링하는 방법 중에는 라우팅 정보의 경로값을 자동으로 증가시키는 것이 있습니다.

Offset-list는 RIP를 이용해서 주고 받는 라우팅 정보의 경로값을 증가시키는 기능입니다. 사용자는 access-list에 offset-list를 설정할 수 있습니다.

전달되는 경로의 경로값을 증가시키려면, Router 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
offset-list access-list-name {in out} <1-16> [interface]	Router	전달되는 경로의 경로값을 증가시킵니다.
no offset-list access-list-name {in out} <1-16> [interface]		경로값 전달 증가 설정을 해제합니다.

11.3.11. 최대 RIP 경로 개수 설정

RIP 프로토콜에서 사용할 수 있는 최대 경로 개수를 지정할 수 있습니다. RIP 프로토콜에서 사용할 수 있는 최대 경로 개수를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
maximum prefix <1-65535> [1-100]	Router	RIP 라우팅 프로토콜의 최대 경로 숫자를 지정합니다.
no maximum prefix <1-65535> [1-100]		RIP 라우팅 프로토콜의 최대 경로 숫자를 해제합니다.

11.3.12. 라우팅 프로토콜 동작 주기 설정

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 동작 주기를 설정할 수 있습니다.

시스템에서 제공하는 동작 주기의 기본 단위는 다음과 같습니다.

- **upadate** : 라우팅 정보는 30초 단위로 전달됩니다. RIP는 자신의 라우팅 테이블을 자신과 연결되어 있는 다른 RIP 라우터에게 30초마다 전달 합니다. 전달 주기는 다음에서 설명할 명령어에서 *update* 값을 지정함으로써 변경할 수 있습니다.

- **timeout** : 라우팅 정보의 유효 시간은 180초입니다. 180초가 지나면, 그 정보는 더 이상 유효하지 않지만 Neighbor 라우터들이 그 경로가 삭제되었다는 것을 통보받을 때까지는 라우팅 테이블에 남아 있습니다. RIP 라우터의 최대 유효시간은 다음에서 설명할 명령어에서 *timeout* 값을 지정하여 변경할 수 있습니다.

- **garbage** : 유효하지 않은 정보를 라우팅 테이블에서 삭제하는 작업은 120초마다 한 번씩 이루어집니다. 유효하지 않은 정보로 분류된 정보들은 120초가 지나면 라우팅 테이블에서 완전히 삭제됩니다. 삭제하는 주기는 다음에서 설명할 명령어에서 *garbage* 값을 지정해 변경할 수 있습니다.

하나의 RIP 네트워크에 속한 모든 라우터들 위에서 설명한 세가지 값을 동일하게 가져야만 합니다. 그렇지 않을 경우에 경로들은 총들을 일으킬 수도 있습니다.



*update, timeout, garbage*의 시간은 기본적으로 각각 30초, 180초, 120초로 설정되어 있습니다.

위에서 설명한 RIP 라우팅 프로토콜 동작 주기를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
timers basic update timeout garbage	Router	RIP 라우팅 프로토콜의 동작 주기를 조절합니다.
no timers basic update timeout garbage		RIP 라우팅 프로토콜 동작 설정을 기본값으로 복귀시킵니다.



참 고

RIP 라우팅 프로토콜의 동작 주기를 설정할 때 설정 가능한 시간 범위는 <5-2,147,483,647> 입니다.

11.3.13. 경로 차단(Split-horizon) 활성화/비활성화

브로드캐스트 타입의 IP 네트워크에 연결되어 각각 다른 거리값을 지닌 라우팅 프로토콜을 사용하는 라우터들은 일반적으로 라우팅 정보가 무한 루프에 빠지지 않도록 Split horizon 기능을 사용합니다. Split horizon이란, 라우팅 정보가 다른 라우터에 전송될 때, 해당 정보를 생성한 라우터에게는 자신의 라우팅 정보가 다시 전송되지 않도록 하는 기능인데 특히, 여러 대의 라우터가 서로 연결되어 있을 때 정상적인 통신이 이루어질 수 있도록 도와줍니다.

한편, Split horizon은 Frame relay처럼 브로드캐스트를 하지 않는 네트워크에서는 사용을 할 수 없기 때문에 이러한 경우에는 Split horizon을 해제해야 합니다.

Split horizon를 활성화하거나 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip rip split-horizon [poisoned]	Interface	Split horizon을 활성화 시킵니다.
no ip rip split-horizon [poisoned]		Split horizon을 해제합니다.

11.3.14. 인증 키 관리

RIP 1은 인증을 지원하지 않습니다. 그러나, 만약 RIP 2 타입의 패킷을 교환하고 있는 경우라면, 인터페이스에서 RIP 인증을 활성화할 수 있습니다. 키 체인은 인터페이스에서 사용할 수 있는 키를 결정합니다. 키 체인을 설정하지 않으면, 인증에서 일반 문자열을 이용하게 됩니다. V5812G는 RIP 인증 중 일반 문자열 인증과 MD5 인증을 지원합니다. RIP 2 타입의 패킷에서 제공하는 기본 인증은 일반 문자열 인증입니다.



참 고

암호화 되지 않은 인증 키는 RIP 2 타입의 패킷 안에 넣어 전달되기 때문에 보안이 필요한 경우에는 일반 문자열 인증을 권장하지 않고 있습니다. 문자열을 이용한 인증은 보안이 필요 없는 경우에 한해서 사용하십시오.

RIP 인증을 설정하려면 인터페이스 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
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		키 체인을 사용하지 않고 일반 문자열 인증에 사용할 문자열을 설정합니다. 이 때 사용하는 문자열은 16 자를 넘지 않아야 합니다.

RIP 인증설정을 해제 하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip rip authentication key-chain [name]	Interface	RIP 인증을 해제합니다.
no ip rip authentication mode [text md5]		설정한 RIP 인증 모드를 해제합니다.
no ip rip authentication string string		RIP 인증에 사용할 문자열 지정을 해제합니다.

11.3.15. RIP 재부팅

RIP를 설정 및 관리하다 보면 사용자의 필요에 따라 장비를 사용하고 있는 도중에 RIP 시스템만 재부팅해야 하는 경우가 있을 수 있습니다. 이 때, 주변의 다른 RIP 라우터들에겐 RIP 시스템이 재부팅 중이며, 재부팅 타이머가 끝날 때 까지 기존에 가지고 있던 경로 정보를 그대로 보유하도록 알려줍니다.

RIP 프로그램을 재부팅하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
rip restart grace-period <1-65,535>	Global	RIP 프로그램을 재부팅시킵니다.

11.3.16. RIP 수신 버퍼 크기 조절

RIP 프로토콜은 UDP 패킷을 이용해 라우터들 사이에서 정보를 교환합니다. V5812G는 이 교환 과정에서 사용되는 네트워크 장비의 UDP 버퍼 크기를 설정할 수 있습니다.

명령어	모 드	기 능
recv-buffer-size < <8,196-2,147,483,647>	Router	RIP에 사용할 UDP 버퍼 크기를 설정합니다.
no recv-buffer-size < <8,196-2,147,483,647>		RIP에 사용할 UDP 버퍼 크기를 기본값으로 되돌립니다.

11.3.17. RIP 설정 확인

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, Enable 모드 또는 Global 설정 모드에서 다음 명령어를 수행하십시오.

명령어	모 드	기 능
show ip rip	Enable/Global	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 **debug** 명령어를 이용하여 문제의 원인을 보다 빨리 파악할 수 있습니다.

RIP 라우터가 주고 받은 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
debug rip events	Enable	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.
debug rip packet detail		
show debugging rip		RIP 디버깅 용으로 설정된 모든 정보를 출력합니다.

부록 A. 시스템 이미지 설치하기

V5812G 스위치는 장비 기종에 따라 두 가지의 시스템 이미지를 저장하여 사용할 수 있습니다. 두 가지 시스템 이미지를 저장하여 사용하면 사용자 환경에 따라 알맞은 이미지 파일을 재빠르게 대응할 수 있습니다.

사용자는 (주)다산네트웍스가 네트워크 서버에서 제공하는 다양한 버전의 시스템 이미지 가운데 사용자 환경에 알맞은 이미지 파일을 선택할 수 있습니다.

시스템 이미지 파일을 내려 받기 위한 절차에 따라 다음과 같은 내용으로 이루어져 있습니다.

- Global 모드에서 시스템 이미지 설치
- Boot 모드에서 시스템 이미지 설치
- 원격에서 시스템 이미지 설치하기

A.1 Global 설정 모드에서 시스템 이미지 설치

사용자는 시스템의 Global 모드에서 FTP/TFTP를 이용하여 장비에 시스템 이미지를 설치할 수 있습니다. 다음은 FTP/TFTP 서버를 설치한 사용자의 PC에 새로운 시스템 이미지를 내려 받은 후 다시 사용자의 장비에서 FTP/TFTP 서버로 접속하여 시스템 이미지를 설치하는 절차입니다.

- 1 단계 사용자 PC에 FTP/TFTP 서버 프로그램을 설치하십시오.
- 2 단계 사용자 PC의 FTP/TFTP 서버의 Root 폴더에 새로운 이미지 파일을 내려 받으십시오.
- 3 단계 사용자 PC와 장비를 콘솔 케이블로 연결합니다.
- 4 단계 FTP/TFTP 서버에 접속하기 위해 장비의 Interface 설정 모드에서 IP 주소를 설정하십시오.
- 5 단계 FTP/TFTP 서버에 접속하여 장비의 플래시 메모리로 새로운 이미지 파일을 설치하십시오.

다음은 FTP 서버가 설치된 사용자의 PC에 새로운 시스템 이미지를 내려 받은 다음 사용자의 장비에 시스템 이미지를 설치하는 순서입니다.

- FTP/TFTP 서버로 시스템 이미지 내려 받기
- 시스템 이미지 설치 준비
- 시스템 이미지 설치

A.1.1 FTP/TFTP 서버로 시스템 이미지 내려 받기

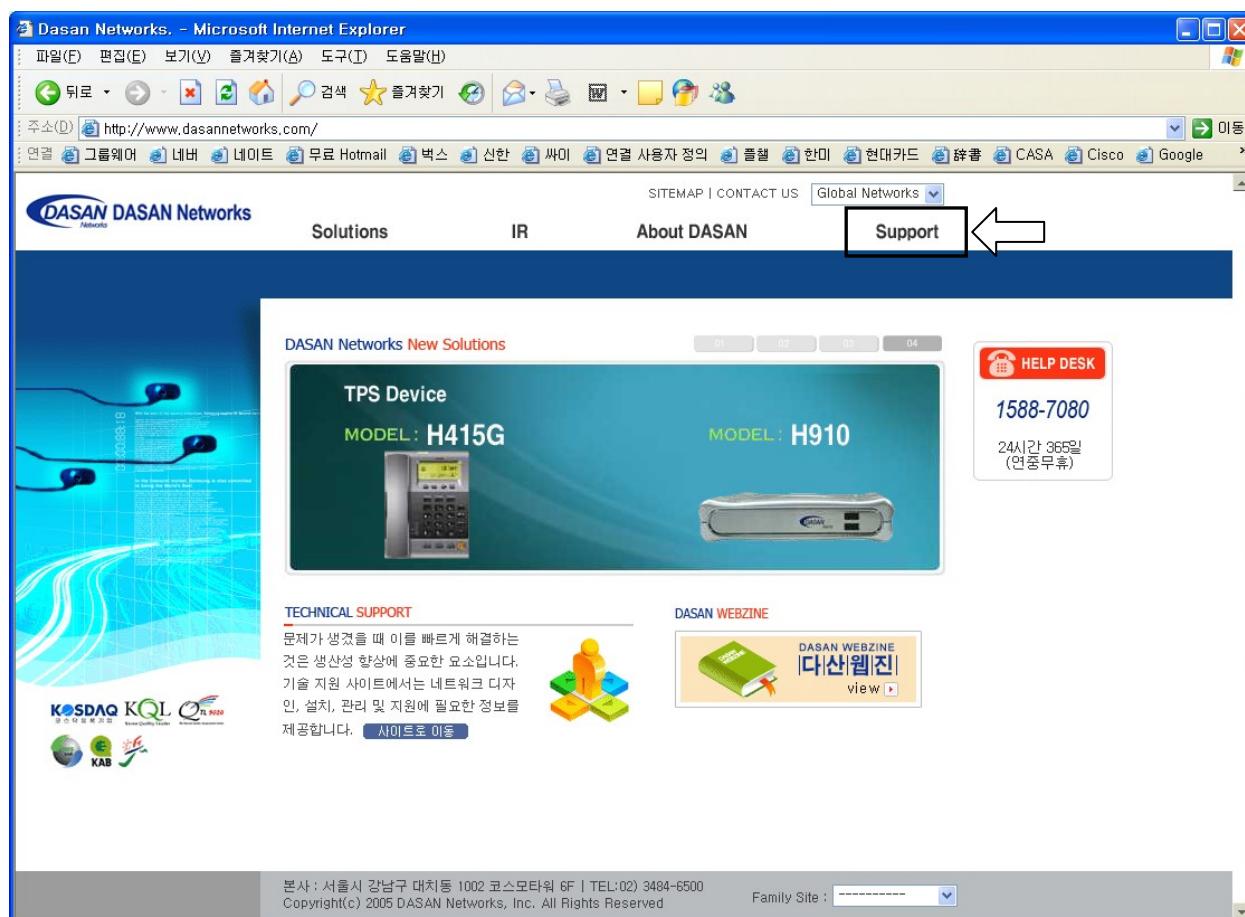
사용자 PC를 FTP/TFTP 서버로 이용하려면 PC에 FTP/TFTP 서버 프로그램이 설치되어 있어야 합니다. 사용자의 PC에 FTP/TFTP 서버 프로그램을 설치하였다면 설치하신 FTP/TFTP 서버의 Root 폴더에 장비의 이미지 파일을 내려 받으십시오.

다음은 웹에서 사용자 PC의 FTP/TFTP 서버에 장비의 이미지 파일을 내려 받는 순서입니다.

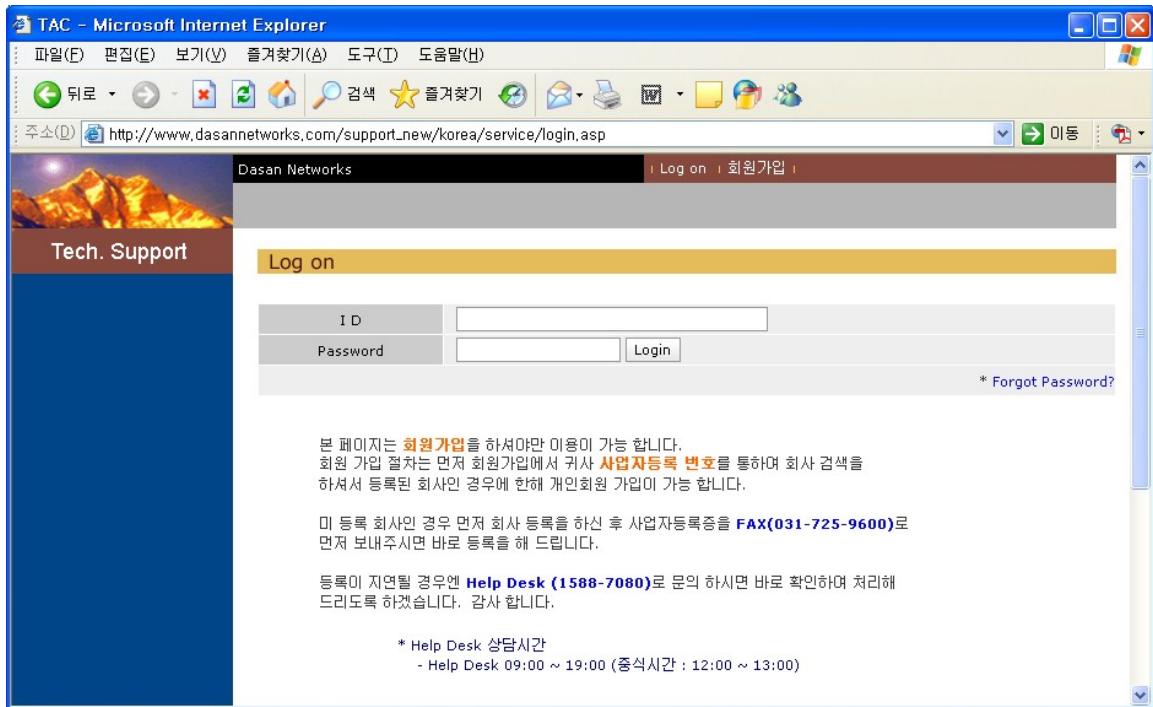
1 단계 (주)다산네트웍스의 홈페이지에 접속합니다.

홈페이지의 주소는 <http://www.dasannetworks.com/> 입니다.

2 단계 Main의 우측 상단에 있는 “**Support**”를 클릭하여 들어가십시오.



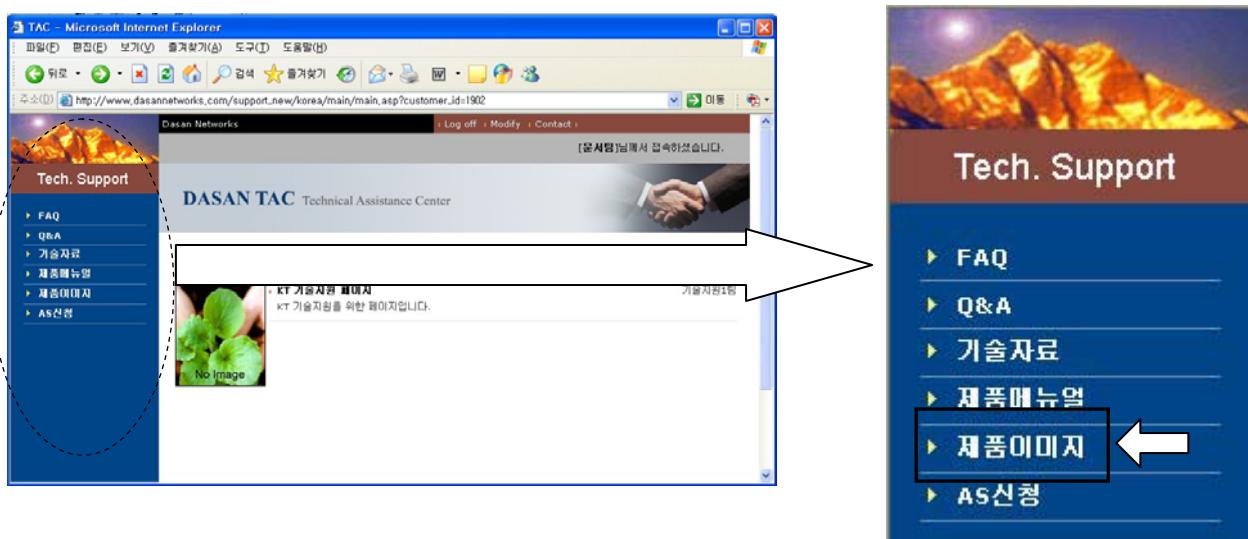
3 단계 사용자가 가지고 있는 계정으로 로그인 하십시오.



i 참고

Support의 서비스는 회원가입을 하셔야 이용할 수 있습니다. 계정이 없는 사용자는 홈페이지에서 설명한 방법에 따라 먼저 회원가입을 하시기 바랍니다.

4 단계 로그인에 성공하여 페이지가 이동하면, 좌측 메뉴바에서 “제품이미지”를 클릭하십시오.



5 단계 아래와 같이 제품 이미지 목록이 나옵니다.

The screenshot shows a Microsoft Internet Explorer window titled "TAC - Microsoft Internet Explorer". The address bar displays the URL: "http://www.dasannetworks.com/support_new/korea/faq/list.asp?table_name=kor_product_image_kt". The page content is a table titled "제품이미지" (Product Images) with the following data:

번호	이미지 파일명	설명	작성자	작성일
15	V1501 ver 5.16		관리자	2010-01-01
14	V1502T ver 5.17		관리자	2010-01-01
13	V2501 ver 5.16		관리자	2010-01-01
12	V2501T ver 5.08		관리자	2010-01-01
11	V2502T ver 5.17		관리자	2010-01-01
10	V3xxx series ver 5.14		관리자	2010-01-01
9	V51xx ver 9.13		관리자	2010-01-01
8	V1xxx ver 7.46		관리자	2010-01-01
7	V61xx ver 7.52p2 7247		관리자	2010-01-01
6	V5972-LR ver 9.13 #4535		관리자	2010-01-01

Below the table, there is a search bar with the placeholder "name" and a "Search" button. The status bar at the bottom of the browser window shows "1 [2]".

6 단계 사용자가 원하는 제품의 시스템 이미지에서 원쪽 클릭하십시오. 파일 저장의 의사를 물으면 “저장”을 선택하시고, PC에 저장하십시오. 이 때, 저장하는 장소는 사용자 PC의 TFTP 서버로 지정하셔야 합니다.

A.1.2 시스템 이미지 설치 준비

사용자 PC에 FTP/TFTP 서버에 시스템 이미지 파일을 내려 받은 후에는 아래의 단계에 따라 FTP/TFTP 서버로 설정된 사용자 PC와 장비를 준비하고 장비가 FTP/TFTP 서버에 접속할 수 있도록 네트워크에 연결되어 있는지 확인하십시오.

1 단계 사용자 PC에 설치된 콘솔 터미널을 9600 baud rates, 8 data bits, one stop bit, no parity로 설정하십시오.

2 단계 사용자 PC와 장비를 콘솔 케이블로 연결하십시오. 이 때 사용자 PC와 장비는 각각 같은 네트워크에 연결되어 있어야 합니다.

3 단계 시스템을 부팅시키십시오.

4 단계 로그인 프롬프트에 로그인명을 입력하면 패스워드 프롬프트가 출력되고, 패스워드를 입력하면 Privilege Exec View 모드로 이동합니다. 제품이 공장에서 출하될 당시 기본적으로 설정된 로그인명은 “**admin**”이고, 패스워드는 없으므로 Enter 키를 입력하십시오.

```
SWITCH login: admin  
Password:  
SWITCH>
```

5 단계 Privilege Exec View 모드에서는 장비의 설정 내용을 확인하는 권한만 가지게 됩니다. 장비를 설정하고 관리하는 권한을 가지려면, Privilege Exec Enable 모드로 들어가야 합니다. 다음은 Privilege Exec Enable 모드로 들어가는 경우입니다.

```
SWITCH> enable  
SWITCH#
```

6 단계 Interface 설정 모드로 들어간 후 **ip address ip-address** 명령으로 인터페이스에 IP 주소를 설정하고 **show ip** 명령으로 IP 주소가 바르게 설정되었는지 확인하십시오. 확인 후에는 **exit** 명령을 사용하여 Global 모드로 가십시오.

```
SWITCH# configure terminal  
SWITCH(config)# interface 1  
SWITCH(config-if)# ip address 192.168.1.10/24  
SWITCH(config-if)# no shutdown  
SWITCH(config-if)# show ip  
IP-Address      Scope    Status  
-----  
192.168.1.10/16      global  
  
SWITCH(config-if)# exit  
SWITCH(config)#
```

A.2 Boot 모드에서 시스템 이미지 설치

Boot 모드에서는 TFTP만을 이용하여 시스템 이미지를 설치할 수 있습니다. 다음은 TFTP 서버를 설치한 사용자의 PC에 새로운 시스템 이미지를 내려 받은 후 다시 사용자의 장비에서 TFTP 서버로 접속하여 시스템 이미지를 설치하는 절차입니다.

- 1 단계 사용자 PC에 TFTP 서버 프로그램을 설치하십시오.
 - 2 단계 사용자 PC의 TFTP 서버의 Root 폴더에 새로운 이미지 파일을 내려 받으십시오.
 - 3 단계 사용자 PC와 장비를 콘솔 케이블로 연결합니다.
-
- 4 단계 TFTP 서버에 접속하기 위해 Boot 모드나 Interface 설정 모드에서 장비에 IP 주소를 설정하십시오.
 - 5 단계 TFTP 서버에 접속하여 장비의 플래시 메모리로 새로운 이미지 파일을 저장, 설치하십시오.



참 고

1 단계부터 4 단계까지는 **FTP/TFTP** 서버로 시스템 이미지 내려 받기와 시스템 이미지 설치 준비를 참고하십시오.

다음은 TFTP 서버가 설치된 사용자의 PC에 새로운 시스템 이미지를 내려 받은 다음 사용자의 장비에 시스템 이미지를 설치하는 순서입니다.

- 시스템 이미지 설치 준비
- 시스템 이미지 설치

A.2.1 시스템 이미지 설치 준비

- 1 단계 콘솔 터미널이 설치된 사용자 PC와 장비 연결이 끝난 후 장비의 전원을 켜면 시스템이 부팅됩니다. 화면에 **If you want to go to boot mode, press s key..**라는 메시지가 보일 때 S키를 눌러 Boot 모드로 들어가십시오.

```
*****
*
*          Boot Loader Version 4.74
*
*          DASAN Networks Inc.
*
*****
Press 's' key to go to Boot Mode: 0
Boot>
```

- 2 단계 TFTP 서버에 접속할 수 있도록 Boot 모드에 IP 주소를 설정합니다. Boot 모드에서 IP를 설정하는 명령어는 **ip ip-address**입니다.

다음은 192.168.1.10으로 IP 주소를 설정, 저장하는 예입니다. 단, 이 IP 주소는 Boot 모드에서만 유용합니다.

```
Boot> ip 192.168.1.10  
Boot>
```

3 단계 IP 주소를 설정한 후에는 **save** 명령어를 사용하여 설정 내용을 저장한 후 **reboot** 명령어를 사용하여 시스템을 다시 부팅시키십시오. 이때 1 단계와 같은 방법으로 Boot 모드로 들어가십시오.

```
Boot> save  
Boot> reboot  
  
*****  
* *  
* Boot Loader Version 4.74 *  
* DASAN Networks Inc. *  
* *  
*****  
Press 's' key to go to Boot Mode: 0  
Boot>
```

4 단계 IP 주소가 제대로 설정되었는지 확인하십시오. **show**를 입력하면 다음과 같이 설정된 IP 주소를 알려줍니다.

```
Boot> show  
IP = 192.168.1.10  
EtherAddr 0 = 00:d0:cb:0a:30:23  
Boot>
```



주의

TFTP 서버에 접속하기 전에 반드시 사용자의 장비와 TFTP 서버가 되는 PC 또는 장비가 동일한 LAN상에 있는지 확인하시기 바랍니다.

A.2.2 시스템 이미지 설치

1 단계 다음 명령어를 사용하여 시스템 이미지 파일을 내려 받으십시오.

명령어	모 드	기 능
<code>load {os1 os2} server-ip-address file-name</code>	Global	시스템 이미지 파일을 설치합니다.



참 고

os1 또는 **os2**는 시스템 이미지 파일이 저장되는 플래시 메모리 위치를 나타냅니다. 장비에 저장할 때에는 반드시 이 위치를 지정해야 합니다.

Update flash: Are you sure (Y/n)?라는 메시지 보일 때 **y**를 입력하십시오. 시스템 이미지 업그레이드가 진행됩니다.

```
Boot> load prog 192.168.1.218 V5812G.3.11.x
Loading V5812G.3.11.x from 192.168.1.218...
Download completed: 5791488 (0x564e88) Bytes.
Update flash: Are you sure (Y/n)? y
```

2 단계 멀티 OS를 사용하고자 하는 경우에는 위의 명령을 사용하여 1 단계와는 다른 위치에 이미지 파일을 설치하십시오.

3 단계 **reboot** 명령어를 사용하여 재부팅하십시오. 재부팅이 이루어지는 과정에서 출력되는 내용을 보면 사용자가 원하는 시스템 이미지 파일이 성공적으로 설치되었는지 여부를 알 수 있습니다.

A.3 원격으로 시스템 이미지 설치

V5812G 스위치와 직접 연결되지 않은 원격의 PC에서 장비에 시스템 이미지 파일을 설치하시려면 다음 방법을 따르십시오.

1 단계 사용자 PC에 새로운 시스템 이미지 파일을 내려 받으십시오. (※ **FTP/TFTP** 서버로 시스템 이미지 내려 받기) 참조)

2 단계 시작 → 실행 → cmd를 실행시키십시오.

3 단계 시스템 이미지 파일을 올릴 장비와 파일을 저장한 사용자 PC가 통신이 되는지 확인하기 위해 사용자 PC에서 ping 테스트를 실시하십시오. 아래 예제에서의 장비의 IP 주소는 192.168.1.218입니다.

```
C:\>ping 192.168.1.218
Pinging 192.168.1.218 with 32 bytes of data:

Reply from 192.168.1.218: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.1.218:
    Packets: Sent = 7, Received = 7, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

4 단계 이미지 파일을 내려 받은 디렉토리로 이동한 후, **dir** 명령으로 내려 받은 파일이 있는지를 확인하십시오.

```
C:\OS>dir
C 드라이브의 볼륨: 로컬 디스크
볼륨 일련 번호: F0F7-18C0

C:\OS 디렉터리

2004-04-22 오전 09:57    <DIR>      .
2004-04-22 오전 09:57    <DIR>      ..
1999-03-28 오후 08:43           251 file_id.diz
1999-03-28 오후 08:29       57,344 tftpd32.exe
1999-03-28 오후 08:41      32,891 TFTPD32.HLP

(이하 생략)

C:\OS>
```



주의

위의 내용은 사용자 PC 디렉토리 내용에 따라 달라질 수 있습니다.

5 단계 사용자 PC에서 FTP로 장비에 접속하십시오. 예제에서의 사용자 ID는 admin, 패스워드는 없는 경우입니다.

```
C:\>ftp 192.168.1.218
Connected to 192.168.1.218.
220 FTP Server 1.2.4 (FTPD)
User (192.168.1.218:(none)): admin
331 Password required for root.
Password:
230 User root logged in.
ftp>
```

6 단계 시스템 이미지 파일을 바이너리 형태로 올리기 위해 **bin** 명령어를 입력하십시오.

```
ftp> bin
200 Type set to I.
ftp>
```

7 단계 파일을 설치하는 동안 진행 상태를 볼 수 있도록 **hash** 명령어를 입력하십시오.

```
ftp> hash
Hash mark printing On ftp: (2048 bytes/hash mark) .
ftp>
```

8 단계 다음 명령어를 사용하여 장비에 시스템 이미지 파일을 설치하십시오.

명령어	모 드	기 능
put file-name {os1 os2}	FTP	시스템 이미지 파일을 설치합니다.



os1 또는 **os2**는 시스템 이미지 파일이 저장되는 플래시 메모리 위치를 나타냅니다. 장비에 저장할 때에는 반드시 이 위치를 지정해야 합니다.



원격으로 시스템 이미지를 설치할 경우, **put** 명령어를 수행하게 되면 새로운 시스템 이미지를 장비의 플래시 메모리에 저장하기 전에 먼저 기존에 있던 시스템 이미지를 삭제하는 작업을 합니다. 이 때 약 30초 간의 딜레이가 생기는데 도중에 장비의 전원을 끄거나 멈추면 장비가 부팅이 되지 않는 등의 치명적인 영향을 미칠 수 있으므로 주의하시기 바랍니다.

9 단계 멀티 OS를 사용하고자 하는 경우에는 위의 명령어를 사용하여 **8 단계**와는 다른 위치에 이미지 파일을 설치하십시오.

10 단계 `reload` 명령어로 장비를 리부팅합니다.

SWITCH# reload

11 단계 `show flash` 명령으로 시스템 이미지 파일이 성공적으로 설치되었는지 확인하십시오.