



User Manual

V2824

UMN : CLI NOS 1.03

이 설명서는 V2824를 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 V2824를 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 2008 © DASAN Networks, Inc.

경기도 성남시 분당구 수내동 11-4
휴맥스 빌리지 6층
Helpdesk) 1588-7080

Release for Update

Summary :

NOS 1.03 업데이트

Details :

Chapter/Section	Reasons for update
4.1.11	Auto Reset 추가
6.1.13	소프트웨어 Watchdog 설정
6.3.21	부팅 정보 확인 추가
6.3.22	케이블 길이 확인 추가
6.3.23	G-PON 모듈 정보 확인 추가
7.2.2	OAM Link 모니터링 CLI 추가
7.18	Attack Guard 추가
7.19	LLCF (Link Layer Carrier Forward) 추가
7.20	포트 트래픽 모니터링 설정 추가
8.5.4(5)	MAC 등록 추가
8.8.2(2)	패킷 타입별 CPU-Flood-Guard 설정 추가

Version history

Status	Date of release	Reasons for change
1	2008/07	Initial release
2	2008/12	NOS 1.03 업데이트

◆ 목 차 ◆

1.	개요	24
1.1	내용 구성	24
1.2	사용 기호	25
1.3	표기법	25
2.	제품 소개	27
2.1	주요 특징	28
3.	CLI 사용하기	32
3.1	명령어 체계	32
3.1.1	Privilege Exec View 모드	33
3.1.2	Privilege Exec Enable 모드	33
3.1.3	Global 설정 모드	34
3.1.4	Bridge 설정 모드	35
3.1.5	Interface 설정 모드	36
3.1.6	Rule 설정 모드	37
3.1.7	DHCP Pool 설정 모드	38
3.1.8	DHCP Option-82 설정 모드	38
3.1.9	RMON 설정 모드	39
3.2	명령어 기본 사용법	40
3.2.1	사용 가능한 명령어 보기	40
3.2.2	이전 명령어 불러내기	43
3.2.3	축약된 명령어 사용하기	43
3.2.4	실행된 명령어 목록 확인하기	44
3.2.5	Privilege Exec Enable 모드 명령어 사용하기	44
3.2.6	no 명령어 사용하기	45
3.2.7	show 명령어 사용하기	45
3.2.8	다른 모드로 이동하기	45
4.	시스템 접속 및 IP 주소 설정	47
4.1	시스템 접속	47
4.1.1	시스템 로그인	47

4.1.2 시스템 로그인 패스워드 변경.....	49
4.1.3 Privilege Exec Enable 모드 접속 패스워드 설정	50
4.1.4 패스워드 초기화	52
4.1.5 자동 로그 아웃 기능 설정	53
4.1.6 사용자 계정 관리	54
(1) 사용자 계정 추가	54
(2) 사용자 권한 설정	55
(3) 설정 예제.....	58
4.1.7 접속자 수 제한.....	60
4.1.8 원격 접속.....	61
4.1.9 원격 접속자 확인 및 연결 강제 해제	61
4.1.10 시스템 리부팅.....	62
4.1.11 Auto Reset	63
(1) CPU Load에 의한 자동 리부팅 설정	63
(2) Memory 용량에 의한 자동 리부팅	64
(3) 네트워크 접속상태에 의한 자동 리부팅 설정.....	69
4.1.12 시스템 로그 아웃	73
4.2 IP 주소 설정.....	74
4.2.1 인터페이스 활성화	74
4.2.2 인터페이스 활성화 해제.....	75
4.2.3 네트워크 인터페이스에 IP 주소 설정	75
(1) 수동 설정.....	75
(2) 자동 할당 설정	76
4.2.4 Static 경로 및 Default Gateway 지정	76
4.2.5 인터페이스 설명하기	78
4.2.6 설정 예제.....	79
4.3 SSH(Secure Shell).....	80
4.3.1 SSH 서버.....	80
(1) SSH 서버 활성화	80
(2) 클라이언트 확인	80
(3) 클라이언트 접속 해제	81
(4) 클라이언트 접속 History 확인	81
4.3.2 SSH 클라이언트	81
(1) SSH 서버 로그인	81
4.3.3 인증키 설정	82
(1) 인증키 생성	82
(2) 인증키 검증	82

(3) 인증키 목록 확인	83
4.3.4 설정 예제	83
4.4 사용자 인증 포트 설정(802.1x)	86
4.4.1 802.1x 기본 설정	88
(1) 802.1x 활성화	88
(2) 인증 서버 설정	88
(3) 인증 모드 설정	90
(4) 인증 포트 설정	90
(5) 인증 포트 상태 설정	91
(6) Request/Identity 패킷 재전송 시간 설정	91
(7) 인증 시도 요청 횟수 설정	92
(8) 인증 시도 주기 설정	92
4.4.2 802.1x 재인증 설정	93
(1) 802.1x 재인증 활성화	94
(2) 재인증 주기 설정	94
(3) 재인증 시도 주기 설정	94
(4) 포트 재인증 실행	95
4.4.3 802.1x 인증 상태 초기화	95
4.4.4 802.1x 설정 내용 초기화	95
4.4.5 802.1x 설정 내용 확인	96
4.4.6 802.1x 사용자 인증 통계 확인 및 삭제	96
4.4.7 설정 예제	96
4.5 시스템 사용자 인증	99
4.5.1 사용자 인증 방법 설정	100
4.5.2 사용자 인증 인터페이스 지정	101
4.5.3 사용자 인증 방법 우선 순위 설정	101
4.5.4 사용자 인증 방법 설정 내용 확인	102
4.5.5 RADIUS 설정	102
(1) RADIUS 서버 설정	102
(2) RADIUS 서버 우선 순위 설정	103
(3) 재전송 시도 횟수 설정	103
(4) 응답 시간 제한	104
4.5.6 TACACS+ 설정	105
(1) TACACS 서버 설정	105
(2) TACACS 서버 우선 순위 설정	106
(3) 인증 방식 설정	106
(4) 응답 시간 제한	107

(5) 사용자 권한 범위 지정	107
4.5.7 사용자 작업 내용 기록	108
4.5.8 설정 예제.....	109

5.	포트 기본 설정	112
-----------	-----------------------	------------

5.1 논리적 포트 활성화 설정	113
5.2 Auto Nego 설정	114
5.3 전송 속도 설정	115
5.4 Duplex 모드 설정	116
5.5 Flow Control 설정	117
5.6 포트 설명하기.....	118
5.7 포트 통계 확인 및 초기화	119
5.8 포트 상태 확인	121
5.9 포트 미러링 설정	122
5.9.1 Monitor 포트와 Mirrored 포트 지정	123
5.9.2 포트 미러링 활성화.....	124
5.9.3 포트 미러링 설정 내용 확인	124
5.9.4 설정 예제.....	124

6.	시스템 환경.....	126
-----------	--------------------	------------

6.1 환경 설정	126
6.1.1 호스트 네임 설정	127
6.1.2 날짜 및 시간 설정	127
6.1.3 Time-zone 설정	128
6.1.4 NTP 설정	129
6.1.5 NTP 메시지 주소 설정	131
6.1.6 SNTP 설정	132
6.1.7 터미널 스크린 출력 상태 설정	133
6.1.8 DNS 서버 설정	134
6.1.9 로그인 배너 설정	138
6.1.10 Fan 동작 설정	140
6.1.11 대문 강제 종료	141
6.1.12 MAC Learning 모드 설정	141
6.1.13 소프트웨어 Watchdog 설정	142
6.1.14 FTP 서버 활성화.....	145
6.1.15 FTP 클라이언트 주소 설정.....	146
6.2 설정 관리	146

6.2.1	설정 내용 확인	147
6.2.2	설정 내용 저장	147
6.2.3	설정 내용 자동 저장	148
6.2.4	설정 초기화 하기	149
6.2.5	설정 내용 Backup 하기	149
(1)	일반 Backup 하기	149
(2)	SSH를 이용하여 데이터 Backup 하기	151
(3)	Backup 파일 확인	151
(4)	Backup 파일 삭제	152
6.3	시스템 확인	153
6.3.1	네트워크 연결 상태 확인	154
6.3.2	IP ICMP Source Routing	155
6.3.3	패킷 경로 추적	157
6.3.4	원격 접속자 확인	158
6.3.5	MAC table 확인 및 삭제	158
6.3.6	Aging Time 설정	159
6.3.7	장비 사용 시간 확인	160
6.3.8	시스템 구성 정보 확인	160
6.3.9	CPU 사용량 확인	161
6.3.10	CPU 프로세스 확인	161
6.3.11	CPU 처리 패킷 제한	162
6.3.12	CPU 통계 확인	162
6.3.13	메모리 사용 정보 확인	163
6.3.14	시스템 이미지 확인	163
6.3.15	시스템 이미지 버전 확인	163
6.3.16	시스템 이미지 파일 크기 확인	163
6.3.17	Default OS 설정	164
6.3.18	시스템 상태 확인	165
6.3.19	Tech-support 확인	166
6.3.20	프로토콜 통계 확인	166
6.3.21	부팅 정보 확인	167
6.3.22	케이블 길이 확인	168
6.3.23	G-PON 모듈 정보 확인	168
7.	네트워크 관리 기능 설정	169
7.1	SNMP	170
7.1.1	SNMP v1의 Community 설정	171

7.1.2	SNMP 에이전트 관리자에 대한 연락처와 설치 위치 정보 지정.....	172
7.1.3	SNMP v2c의 com2sec 설정	173
7.1.4	SNMP v2c 및 v3의 Group 설정	174
7.1.5	SNMP v2c 및 v3의 OID 공개 범위 제한(View 설정).....	175
7.1.6	SNMP v2c 및 v3 제한 OID에 대한 접속권한부여(Access 설정).....	176
7.1.7	SNMP v3의 User 설정	177
7.1.8	SNMP 트랩 설정	178
(1)	SNMP 트랩 호스트 지정	178
(2)	SNMP 트랩 모드 설정.....	180
(3)	Event 모드에서 SNMP 트랩 설정	180
(4)	Alarm-report 모드에서 SNMP 트랩 설정	183
(5)	ERP Alarm 중요도 설정 및 해제.....	188
(6)	Notify-Activity 활성화.....	189
(7)	SNMP 트랩 설정 확인.....	189
7.1.9	SNMP 에이전트의 IP 지정	192
7.1.10	SNMP 설정 확인	193
7.1.11	SNMP 기능 해제	193
7.1.12	설정 예제	194
7.2	EFM OAM	198
7.2.1	OAM 활성화	199
7.2.2	OAM Link 모니터링	200
7.2.3	EFM OAM 모드 설정	201
7.2.4	OAM Loopback 설정	201
7.2.5	OAM Unidirection 설정	202
7.2.6	Remote OAM 설정	203
7.2.7	OAM 설정 확인	204
7.3	LLDP	206
7.3.1	LLDP 활성화	206
7.3.2	LLDP 동작 방식 설정	207
7.3.3	Basic TLV 설정	208
7.3.4	LLDP 메시지 송신 관련 설정	208
7.3.5	Reinitdelay 설정	209
7.3.6	LLDP 프레임 전송 Delay 시간 설정	209
7.3.7	LLDP 설정 확인	210
7.3.8	LLDP 통계 확인	210
7.3.9	Remote 엔트리 통계 확인	210
7.3.10	설정 예제	211

7.4	RMON 설정	214
7.4.1	RMON History 설정	214
(1)	통계 데이터 발생 포트 지정	216
(2)	RMON History 사용 주체 명시	217
(3)	표본 데이터 수 설정	217
(4)	표본 조사 간격 설정	218
(5)	RMON History 활성화 하기	218
(6)	RMON History 삭제 및 설정 변경	219
7.4.2	RMON Alarm 설정	220
(1)	RMON Alarm 사용 주체 명시	221
(2)	표본 조사에 사용될 object 설정	221
(3)	절대 비교 및 멜타 비교 설정	222
(4)	상한 임계 값 설정	223
(5)	하한 임계 값 설정	224
(6)	최초 Alarm 기준 설정	225
(7)	표본 조사 간격 설정	225
(8)	RMON Alarm 활성화 하기	226
(9)	RMON Alarm 삭제 및 설정 변경	227
7.4.3	RMON Event 설정	227
(1)	Event Community 설정	229
(2)	Event 설명	229
(3)	Event 사용 주체 명시	230
(4)	Event 공지 형태 설정	230
(5)	Event 활성화 하기	231
(6)	RMON Event 삭제 및 설정 변경	231
7.5	Syslog 설정	232
7.5.1	Syslog 메시지 Level 설정	233
7.5.2	System Facility 설정	234
7.5.3	Syslog Message Priority 설정	234
7.5.4	Syslog 해제	237
7.5.5	Syslog 설정 확인	237
7.5.6	Syslog 메시지 IP 주소 지정	239
7.5.7	원격에서 Debug 메시지 확인하기	239
7.5.8	CPU 사용량 임계값 설정	240
7.5.9	CPU 처리 패킷수 임계값 설정	242
7.5.10	포트 트래픽 임계값 설정	243
7.5.11	Fan 임계값 설정	244

7.5.12 온도 임계값 설정	245
7.5.13 메모리량 임계값 설정	246
7.6 QoS(Quality of Service)	247
7.6.1 QoS 동작 원리	248
7.6.2 패킷 분류(Classify) 설정	249
7.6.3 패킷 정책(Policing) 설정	254
7.6.4 Rule 동작 설정	263
(4) CoS값 및 ToS값 설정	266
7.6.5 Rule 설정 내용 확인	269
7.6.6 스케줄링(Scheduling) 설정	269
(2) Weight 설정	271
(3) Min-bandwidth 설정	272
(4) Max-bandwidth 제한	273
(5) 특정 포트의 트래픽 제한 설정	274
(6) CPU 패킷에 대한 사용자 정의	275
(7) QoS 내용 확인	275
(8) 포트별 Queue 트래픽 확인	276
7.6.7 Admin Rule 설정	276
7.6.8 Admin Rule 패킷 분류(Classify) 설정	276
7.6.9 Admin Rule 동작 설정	280
7.6.10 Admin Rule 설정 내용 확인	283
7.7 NetBIOS 필터링	284
7.8 MAC 필터링	285
7.8.1 MAC 필터 기본 정책 설정	285
7.8.2 MAC 필터 정책 추가	286
7.8.3 MAC 필터 정책 삭제	287
7.8.4 MAC 필터 정책 확인	287
7.8.5 MAC 필터링 정책 목록 불러오기	287
7.8.6 설정 예제	289
7.9 Martian Filter 통계 확인	291
7.10 접속가능 사용자수 제한	291
7.11 MAC 테이블 관리	294
7.12 ARP	295
7.12.1 ARP 테이블 설정	296
7.12.2 ARP Inspection	296
7.12.3 ARP-Alias 설정	303
7.12.4 Proxy-ARP 설정	304

7.12.5	Gratuitous ARP	306
7.13	ICMP 메시지 Control	307
7.13.1	Echo Reply 메시지 제한	308
7.13.2	ICMP 메시지 전송 시간 제한.....	309
(1)	전송 제한 메시지 지정	309
(2)	전송 제한 시간 설정	311
(3)	전송 제한 설정 확인	311
(4)	전송 제한 설정 초기화	311
7.13.3	인터페이스 별 ICMP 메시지 전송 제한.....	312
7.14	TCP Flag Control	312
7.14.1	RST 설정	312
7.14.2	SYN Attack 방지 기능 설정	313
7.14.3	SYN Guard 대역폭 설정	315
7.15	덤프 패킷 (Dump Packet).....	315
7.15.1	덤프 패킷 확인	315
(1)	프로토콜별 덤프 패킷 확인	316
(2)	호스트 덤프 패킷 확인	316
(3)	멀티캐스트 덤프 패킷 확인	317
(4)	사용자 지정 덤프 패킷 확인	317
(5)	설정 내용 확인	319
7.15.2	덤프 패킷 디버그	319
7.16	Port Security	320
7.16.1	Port Security 활성화	320
7.16.2	MAC 주소 갯수 지정	320
7.16.3	Port Security Age Time 지정	321
7.16.4	Port Security Age Type 지정	321
7.16.5	Port Security Age Static 지정	322
7.16.6	Violation Action 지정	322
7.16.7	Secure MAC 주소 등록	323
7.16.8	Port Security 설정 확인	323
7.17	PPS-Control	323
7.18	Attack Guard	325
7.18.1	Attack Guard 설정	325
7.18.2	포트 수동 활성화	326
7.18.3	설정 내용 확인	327
7.19	LLCF (Link Layer Carrier Forward)	327
7.20	포트 트래픽 모니터링 설정	329

7.21 ECMP(Equal Cost Multi-Path) 설정	330
---	-----

8. 시스템 주요 기능 설정	332
------------------------------	------------

8.1 Access List 설정	332
8.1.1 Standard Access List 설정	336
8.1.2 Extended Access List 설정	337
8.1.3 Named Access List 설정	340
8.1.4 Access List 설정 내용 확인	342
8.2 VLAN(Virtual Local Area Network)	342
8.2.1 Default VLAN	345
8.2.2 포트 기반 VLAN 설정	346
(1) VLAN 만들기	346
(2) PVID 지정	347
(3) 포트 할당 및 삭제	347
(4) VLAN 기능 해제	348
8.2.3 프로토콜 기반 VLAN 설정	348
8.2.4 MAC 주소 기반 VLAN 설정	349
8.2.5 Subnet 기반 VLAN 설정	349
8.2.6 VLAN 우선 순위 지정	350
8.2.7 QinQ 설정	350
(1) QinQ 설정 방법	352
(2) TPID 종류 설정	352
(3) QinQ 해제	353
8.2.8 Shared-VLAN 설정	353
8.2.9 Protected 포트의 설정	357
8.2.10 VLAN 설명하기	357
8.2.11 VLAN Translation 설정	358
8.2.12 VLAN 관련 설정 내용 확인	359
8.2.13 설정 예제	359
8.3 Link Aggregation	364
8.3.1 포트 트렁크	366
(1) 트렁크 그룹 및 멤버 포트 설정	366
(2) 트렁크 그룹 패킷 분배 모드 지정	367
(3) 트렁크 그룹 설정 내용 확인	368
8.3.2 LACP	368
(1) LACP 활성화	369
(2) 패킷 경로 규정 설정	369

(3) 멤버 포트 설정	370
(4) 멤버 포트의 동작 모드 설정	371
(5) 멤버 포트 우선 순위 지정	372
(6) 멤버 포트의 LACP 참가 여부 설정	372
(7) 멤버 포트의 BPDU 전송 주기 설정	373
(8) 멤버 포트의 Key 값 설정	373
(9) LACP 장비 우선 순위 지정	375
(10) LACP 설정 내용 확인	376
(11) LACP 통계 확인	377
(12) LACP 통계 삭제	377
(13) 설정 예제	377
8.4 STP	383
8.4.1 STP 동작 원리	385
8.4.2 RSTP의 동작 원리	388
(1) 포트 상태의 변화	389
(2) BPDU 정책 변화	390
(3) 네트워크 convergence 시간 단축	391
(4) 802.1d와의 호환성	393
8.4.3 PVSTP 와 MSTP	394
8.4.4 STP 모드 설정	399
8.4.5 STP/RSTP/MSTP 설정	399
(1) STP/RSTP/MSTP 활성화	399
(2) Root 설정	400
(3) Path-cost 설정	401
(4) Port-priority 설정	402
(5) MST Region 설정	403
(6) 설정 내용 확인	404
8.4.6 PVSTP/PVRSTP 설정	405
(1) PVSTP/PVRSTP 활성화	406
(2) Root 설정	406
(3) Path-cost 설정	407
(4) Port-priority 설정	408
(5) 설정 내용 확인	408
8.4.7 BPDU 전송 설정	409
(1) Hello Time 설정	410
(2) Forward Delay 설정	410
(3) Max Age 설정	411

(4) BPDU Hop 설정	412
(5) BPDU 설정 내용 확인	412
8.4.8 BPDU Filtering 설정	412
8.4.9 Point-to-Point MAC 설정	413
8.4.10 STP 모드 변경 감지	414
8.4.11 STP Guard 설정	414
(1) Edge Port 설정	414
(2) Root Guard 설정	414
(3) BPDU Guard 설정	415
(4) 설정 내용 확인	417
8.4.12 설정 예제	417
8.5 ERP 설정	419
8.5.1 ERP 동작 원리	420
8.5.2 LOTP (Loss of Test Packet)	423
8.5.3 Shared Link 환경	423
8.5.4 ERP 도메인 설정	424
(1) ERP ID 설정	424
(2) ERP 도메인 설명	425
(3) Node 설정	425
(4) Primary/Secondary 포트 설정	425
(5) MAC 등록	426
8.5.5 Protected Activation 설정	426
8.5.6 Manual Switch to Secondary 설정	427
8.5.7 Wait-to-Restore Time 설정	427
8.5.8 Learning Disable Time 설정	428
8.5.9 Test Packet Interval 설정	428
8.5.10 ERP Ring 우선순위 정하기	429
8.5.11 LOTP Hold Off Time 설정	429
8.5.12 ERP 트랩 메시지	430
8.5.13 ERP 설정 확인	431
8.6 Loop 감지 기능 설정	431
8.6.1 Loop 감지 기능 설정	431
(1) Loop 감지 기능 활성화	432
(2) 포트 정책 설정	432
(3) Loop 감지 패킷 전송 시간 설정	433
(4) Loop 감지 리스트 해제 timer 설정	433
(5) Loop 감지 패킷 전송 소스 MAC 주소 설정	434

(6) Loop 감지 설정 확인	435
8.7 스택킹 설정	435
8.7.1 장비 그룹 설정	436
8.7.2 Master 장비 지정	437
8.7.3 Slave 장비 설정	437
8.7.4 스택킹 설정 해제	438
8.7.5 스택킹 설정 내용 확인	438
8.7.6 Master에서 Slave로 접속	438
8.7.7 설정 예제	439
8.8 Rate Limit와 Flood Guard	440
8.8.1 Rate Limit 설정	441
8.8.2 Flood Guard 설정	442
(1) MAC-Flood-Guard 설정	442
(2) CPU-Flood-Guard 설정	443
(3) System-Flood-Guard 설정	445
8.8.3 설정 예제	448
8.9 DHCP(Dynamic Host Configuration Protocol)	449
8.9.1 DHCP 서버 설정	451
(1) IP Pool 만들기	451
(2) 서브넷 설정	452
(3) 서브넷 디플트 게이트웨이 설정	452
(4) IP 주소 범위 설정	453
(5) IP 사용 가능 시간 설정	453
(6) DNS 등록	454
(7) IP 주소 수동 할당	454
(8) 도메인 이름 설정	455
(9) Option Code 설정	455
(10) Static Lease database 파일 확인	456
(11) IP Pool 설정 내용 확인	456
(12) IP 주소 할당 제한	457
(13) 할당 IP 주소의 사용 여부 확인	458
(14) BOOTP Request 차단	459
(15) IP 주소 할당 기준 설정	459
(16) IP 주소 1:N 할당 방지	459
(17) Authorized ARP	460
(18) Lease 데이터베이스 Backup	462
(19) Lease 데이터베이스 확인	462

(20) Lease 데이터베이스 초기화	463
(21) IP Pool 사이즈 설정	463
(22) DHCP 패킷 통계 확인	464
8.9.2 DHCP 릴레이 에이전트 설정	464
(1) DHCP Relay 에이전트 활성화	465
(2) Vendor별 DHCP 서버 지정	465
(3) Smart Relay 설정	466
(4) DHCP 서버 ID 설정	467
(5) DHCP 릴레이 에이전트 패킷 통계 확인	467
8.9.3 DHCP Option 설정	468
(1) DHCP Option 활성화	468
(2) DHCP Option 설정하기	469
(3) DHCP Option 삭제	470
(4) DHCP Option 확인	470
8.9.4 DHCP Option-82 설정	470
(1) DHCP Option-82 활성화	471
(2) Option-82 패킷 정책 설정	471
(3) 시스템 Remote-ID, Circuit-ID 설정	472
(4) DHCP Option82 Trust 패킷 설정	473
8.9.5 Class 설정	474
(1) Class 만들기	475
(2) Option 82 패킷 설정	475
(3) IP 주소 범위 설정	477
(4) Class 기능 활성화	477
8.9.6 DHCP 클라이언트	478
(1) DHCP 클라이언트 활성화	478
(2) Client-id 설정	478
(3) Class-id 설정	479
(4) 호스트 이름	479
(5) IP 주소 사용 시간 제한	480
(6) DHCP 서버로부터 정보 요청	481
(7) IP 주소 사용 중단	481
(8) IP 주소 재요청	482
(9) DHCP 클라이언트 설정 확인	482
8.9.7 DHCP Snooping 설정	482
(1) DHCP Snooping 활성화	482
(2) VLAN별 DHCP Snooping 설정	483

(3) Trust 포트 지정	483
(4) Trust 포트 DHCP 패킷 필터링	483
(5) DHCP 패킷 수 제한	484
(6) 바인딩 테이블에 등록되는 IP 주소 개수 제한	484
(7) 바인딩 테이블 Backup	485
(8) 바인딩 테이블 Static 등록	485
(9) MAC 주소를 통한 관리	485
(10) 고정 IP 사용자 차단	486
(11) DHCP Option-82 추가 설정	486
(12) DHCP Snooping Option 설정	487
(13) DHCP Snooping 설정 내용 확인	488
8.9.8 IP Source Guard	489
(1) IP Source Guard 활성화	489
(2) Static IP Source Guard	490
(3) IP Source Guard 설정 내용 확인	490
8.9.9 DHCP 디버깅	490
8.10 Storm Control	491
8.11 Jumbo-frame 수용하기	492
8.12 최대 전송 단위 (MTU) 설정	493
8.13 대역폭 설정	494

9. 멀티캐스트(Multicast) 설정 495

9.1 IGMP (Internet Group Management Protocol)	496
9.1.1 IGMP 기본 설정	498
(1) IGMP 버전 설정	499
(2) QRV 설정	499
(3) IGMP 엔트리 초기화	500
9.1.2 IGMP 버전 2 설정	501
(1) IGMP Static Join 설정	503
(2) 접속 가능한 IGMP 그룹 리스트 설정	505
(3) IGMP Querier 설정	505
(4) Immediate Leave 설정	511
9.1.3 IGMP 버전 3 설정	512
9.1.4 IGMP 설정 확인	514
9.2 멀티캐스트 부가 기능 설정	515
9.2.1 멀티캐스트 포워딩 데이터베이스 설정	515
(1) Unknown 멀티캐스트 트래픽 처리	515

(2) 포워딩 엔트리 설정	516
(3) 멀티캐스트 포워딩 데이터베이스 확인 및 초기화	517
9.2.2 IGMP Snooping 기본 설정	517
(1) IGMP Snooping 활성화	518
(2) IGMP Snooping 버전 설정	519
(3) Robustness Variable 설정	520
9.2.3 IGMP 버전 2 Snooping 설정	521
(1) IGMP Snooping Querier 설정	521
(2) IGMP Snooping Last Member Query의 전송 주기 설정	524
(3) IGMP Snooping Immediate-Leave 설정	525
(4) IGMP Snooping Report Suppression 설정	526
(5) IGMP Snooping S-Query Report Agency 설정	527
(6) 호스트 트래킹 기능 설정	527
(7) 멀티캐스트 라우터 포트 설정	530
(8) 멀티캐스트 TCN Flooding 설정	532
9.2.4 IGMP 버전 3 Snooping 설정	536
9.2.5 IGMP Snooping 정보 확인	537
9.2.6 MVR (Multicast VLAN Registration)	539
(1) MVR 활성화	540
(2) MVR 그룹 설정	541
(3) Source/Receiver 포트 설정	541
(4) MVR Helper 주소 설정	542
(5) MVR 설정 확인	543
9.2.7 IGMP 필터링 기능 설정	543
(1) IGMP 필터링 설정	543
(2) IGMP 그룹의 최대값 설정	546
(3) 패킷 종류에 따른 IGMP 필터링 설정	546
(4) IGMP 필터링 확인	547
9.2.8 Static SSM 맵핑 설정	547
9.2.9 IGMP State 제한 설정	549
9.2.10 멀티캐스트 Source Trust 포트 설정	550
9.2.11 MRIB Debug	551

부록 A. 시스템 이미지 설치하기	552
---------------------------------	------------

A.1 Enable 설정 모드에서 시스템 이미지 설치	552
A.1.1 FTP/TFTP 서버로 시스템 이미지 내려 받기	553
A.1.2 시스템 이미지 설치 준비	555

A.1.3	시스템 이미지 설치.....	556
A.2	Boot 모드에서 시스템 이미지 설치	558
A.2.1	시스템 이미지 설치 준비.....	558
A.2.2	시스템 이미지 설치.....	560
A.3	원격으로 시스템 이미지 설치.....	560

◆ 그 림 ◆

【 그림 2-1 】 V2824를 이용한 네트워크 구성의 예	27
【 그림 3-1 】 콘솔 터미널을 통한 시스템 설정 및 관리	32
【 그림 4-1 】 Auto-reset을 위한 Memory Check 동작.....	65
【 그림 4-2 】 Auto-reset을 위한 Ping 동작	70
【 그림 4-3 】 802.1x 사용자 인증 과정	87
【 그림 4-4 】 Multi Authentication Server.....	88
【 그림 4-5 】 시스템 사용자 인증 과정	99
【 그림 5-1 】 포트 미러링의 예.....	122
【 그림 6-1 】 도메인 네임 서버.....	136
【 그림 6-2 】 네트워크 연결 확인을 위한 Ping 테스트	155
【 그림 6-3 】 IP ICMP Source Routing.....	156
【 그림 7-1 】 SNMP 구성의 예	170
【 그림 7-2 】 SNMP 에이전트의 IP 주소	192
【 그림 7-3 】 EFM OAM 시나리오.....	198
【 그림 7-4 】 QoS의 동작 구조	248
【 그림 7-5 】 Rule의 구조	249
【 그림 7-6 】 Token Bucket 방식	255
【 그림 7-7 】 Single Rate Three Color Marker의 Color Marking	256
【 그림 7-8 】 Two Rate Three Color Marker의 Color Marking.....	258
【 그림 7-9 】 Strict Priority Queuing에서의 패킷 처리	270
【 그림 7-10 】 WRR에서의 패킷 처리	270
【 그림 7-11 】 DRR에서의 Min-bandwidth와 Max-bandwidth.....	273
【 그림 7-12 】 NetBIOS 필터링의 필요성	284
【 그림 7-13 】 Proxy-ARP	305
【 그림 7-14 】 ICMP 메시지	307
【 그림 7-15 】 3 Way Hand Shaking	313
【 그림 7-16 】 LLCF 절차.....	327
【 그림 8-1 】 ACL의 적용 순서	334
【 그림 8-2 】 Layer 2 환경 포트 기준 VLAN 구성도	343
【 그림 8-3 】 VLAN 기준 패킷 경로 결정 절차	344
【 그림 8-4 】 QinQ 설정 네트워크 구성의 예	351
【 그림 8-5 】 Layer 2 환경에서 외부로 패킷이 나가는 경우	354
【 그림 8-6 】 Layer 2 환경에서 외부 패킷이 들어오는 경우 ①.....	355

【 그림 8-7 】 Layer 2 환경에서 외부 패킷이 들어오는 경우 ②.....	356
【 그림 8-8 】 Link Aggregation.....	364
【 그림 8-9 】 Link Aggregation 구성 예 ①.....	365
【 그림 8-10 】 LACP의 구성 예 ①.....	374
【 그림 8-11 】 LACP의 구성 예 ②.....	375
【 그림 8-12 】 루프 현상의 예	383
【 그림 8-13 】 STP의 원리	384
【 그림 8-14 】 Root 스위치	385
【 그림 8-15 】 Designated 스위치 결정	386
【 그림 8-16 】 Designated 스위치와 Designated 포트	387
【 그림 8-17 】 Port priority를 사용한 결정	388
【 그림 8-18 】 Alternate 포트와 Backup 포트	389
【 그림 8-19 】 낮은 BPDU를 받아들이는 경우	390
【 그림 8-20 】 802.1d의 네트워크 convergence.....	391
【 그림 8-21 】 802.1w의 네트워크 convergence ①.....	392
【 그림 8-22 】 802.1w의 네트워크 convergence ②.....	392
【 그림 8-23 】 802.1w의 네트워크 convergence ③.....	393
【 그림 8-24 】 STP와의 호환 ①	394
【 그림 8-25 】 STP와의 호환 ②	394
【 그림 8-26 】 STP	395
【 그림 8-27 】 PVSTP.....	395
【 그림 8-28 】 MSTP	396
【 그림 8-29 】 MSTP의 CST와 IST①	397
【 그림 8-30 】 MSTP의 CST와 IST②	398
【 그림 8-31 】 Link failure 발생	421
【 그림 8-32 】 Ring Protection.....	422
【 그림 8-33 】 Link Failure 복구	422
【 그림 8-34 】 Ring Recovery.....	423
【 그림 8-35 】 Shared Link 환경	424
【 그림 8-36 】 스택킹 설정의 예	436
【 그림 8-37 】 Rate Limit와 Flood Guard.....	441
【 그림 8-38 】 DHCP 서비스 구성의 예	450
【 그림 8-39 】 DHCP 서버와 Relay 에이전트 구성도의 예	464
【 그림 8-40 】 DHCP Option-82를 사용하는 경우의 패킷 흐름.....	471
【 그림 9-1 】 IGMP 버전 1 메시지 형식	496
【 그림 9-2 】 IGMP 버전 2 메시지 형식	497
【 그림 9-3 】 IGMP 버전 3 Query 메시지 형식	513

【 그림 9-4 】 IGMP 버전 3 Report 메시지 형식	513
【 그림 9-5 】 IGMP Snooping을 설정했을 경우	518
【 그림 9-6 】 MVR 동작	539

◆ 표 ◆

【 표 1-1 】 콘솔 터미널 명령어 표기법	25
【 표 1-2 】 안내서 명령어 표기법	26
【 표 3-1 】 Privilege Exec View 모드 주요 명령어	33
【 표 3-2 】 Privilege Exec Enable 모드 주요 명령어	34
【 표 3-3 】 Global 설정 모드 주요 명령어	35
【 표 3-4 】 Bridge 설정 모드 주요 명령어	36
【 표 3-5 】 Interface 설정 모드 주요 명령어	36
【 표 3-6 】 Rule 설정 모드 주요 명령어	37
【 표 3-7 】 DHCP Pool 설정 모드 주요 명령어	38
【 표 3-8 】 DHCP Option-82 설정 모드 주요 명령어	39
【 표 3-9 】 RMON 설정 모드 공통 명령어	39
【 표 5-1 】 이더넷 포트의 기본 설정	112
【 표 6-1 】 GMT 시각	128
【 표 6-2 】 CML 모드와 SML 모드의 성능 비교	141
【 표 6-3 】 Ping 테스트 실행을 위한 기본 설정	154
【 표 6-4 】 Traceroute 실행을 위한 기본 설정	157
【 표 7-1 】 V2824의 기본 SNMP 트랩	181
【 표 7-1 】 ICMP Message Type	307
【 표 7-2 】 ICMP 메시지의 값	309
【 표 7-3 】 Default Mask 계산 결과표	310
【 표 7-4 】 TCP 덤프 옵션	317
【 표 8-1 】 Wildcard mask의 설정 예	335
【 표 8-2 】 STP path-cost	401
【 표 8-3 】 RSTP의 path-cost	401

1. 개요

이 설명서는 주다산네트웍스의 V2824를 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 V2824를 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.

이 장은 다음과 같은 내용으로 구성되어 있습니다.

- 내용 구성
- 사용 기호
- 표기법

1.1 내용 구성

- 제품 소개 :** V2824가 가지고 있는 기능을 소개합니다.
- CLI 사용하기 :** 주다산네트워크에서 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 :** V2824의 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 :** V2824가 가지고 있는 VLAN, STP(Spanning Tree Protocol), IP 멀티캐스팅 등의 주요 기능을 설정하는 방법에 대해 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

V2824의 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	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.

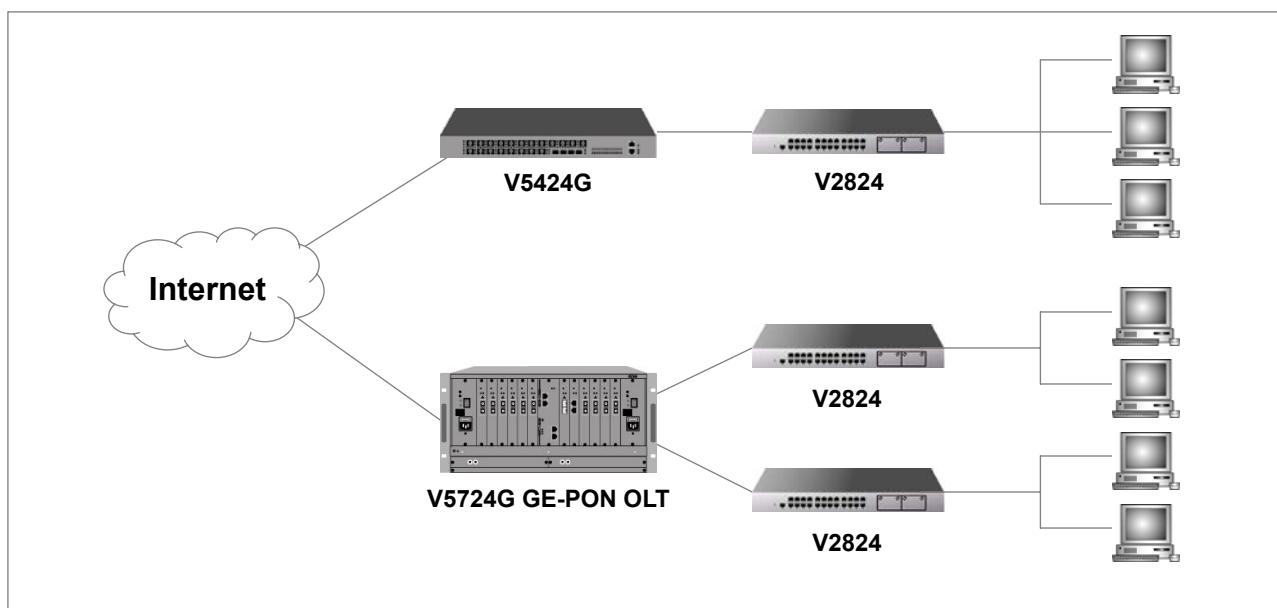
2. 제품 소개

기하급수적으로 증가하는 인터넷 사용자수에 대응하고 그래픽이나 음성 파일과 같은 대용량 데이터를 원활하게 주고 받을 수 있는 네트워크 환경을 구축하기 위해 기존 패스트 이더넷(Fast Ethernet), 기가비트 이더넷(Gigabit Ethernet)과 더불어 광케이블을 이용한 GE-PON의 이용이 널리 확산되고 있습니다.

이러한 백본용 LAN은 사무실이나 데이터 센터 또는 통신 사업자의 국사에 설치되어 있는 워크 그룹용 스위치와 연결되어 클라이언트들이 네트워크 통신을 이용할 수 있도록 합니다. (주)다산네트웍스의 V2848는 네트워크 상에 있는 개인 PC나 웹 서버의 트래픽을 백본용 장비에 전송하는 전형적인 워크 그룹용 Layer2 스위치입니다.

V2824는 Wire speed를 지원하는 10/100BASE-T 서비스 포트 이외에 옵션 모듈 형태의 업링크 포트 2개를 제공하며, 업링크 포트는 사용자의 환경에 따라 1000BASE-X SFP, 1000BASE-X GBIC, GE-PON 포트를 선택하여 설치할 수 있기 때문에 보다 다양한 네트워크 구축이 가능합니다.

다음은 V2824를 이용한 네트워크 구성의 예입니다.



【 그림 2-1 】 V2824를 이용한 네트워크 구성의 예

2.1 주요 특징

Layer 2 스위치인 V2824는 QoS, IP 멀티캐스팅, STP, VLAN 등의 다양한 기능을 제공합니다. 장비의 재부팅 없이 사용자가 설정한 내용이 적용되는 것은 물론, syslog와 SNMP 등으로 장비의 상태를 관리 및 모니터링 할 수 있으며 중복 IP 주소와 MAC 주소에 대한 자동 감지 및 경고 기능도 가지고 있습니다.

다음은 V2824가 가지고 있는 주요 특징입니다.

- **CLI 기반 DSH**

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

- **QoS (Quality of Service)**

일반적인 네트워크 환경에서는 트래픽이 폭주할 경우 사용자의 데이터는 자동적으로 유실(drop)됩니다. 그러나 QoS를 지원하는 V2824는 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**

V2824는 IGMP Snooping 기능과 IGMP Querier 기능을 제공하기 때문에 멀티캐스트 통신이 가능한 장비입니다. 멀티캐스트 통신은 필요로 하는 호스트들에게만 패킷을 전송하기 때문에 불필요한 패킷으로 인해 일어나는 과부하 현상을 막을 수 있습니다.

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

SNMP 기능이 탑재된 스위치는 원격에서 스위치 상태를 확인하고 관리할 수 있습니다. V2824는 SNMP 버전 1과 2와 4가지 그룹의 RMON을 지원, 관리자가 원하는 때에 원하는 통계 자료를 볼 수 있습니다.

- **DHCP Server 및 Relay 기능**

V2824는 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.

- **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. V2824는 하나의 시스템 당 최대 256개의 VLAN을 구성할 수 있습니다.

- **스택킹 (Stacking)**

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

- **Link aggregation**

V2824는 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. V2824는 트래픽을 줄이고 장애 복구 기능을 향상 시키기 위해 IEEE 802.3ad 표준안에 따라 최대 8개의 포트를 포괄하는 통합 포트를 6개까지 설정할 수 있습니다.

- **대역폭 설정(Rate-limit)**

V2824는 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. V2824는 이러한 STP 기능을 가지고 있습니다.

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

V2824는 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)**

V2824는 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 스위치 네트워크에서 STP Reconvergencys 시간을 혁신적으로 감소시키기 위한 목적으로 개발된 것으로, Redundant link를 갖는 Layer 2 스위치에서 Fail over 시간을 획기적으로 단축시킵니다.

- **802.1x 기반 사용자 인증**

V2824는 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.

- **SSH 서버**

V2824는 SSH(Secure Shell) 서버를 활성화 함으로써 TELNET, FTP 서비스에 보안성을 높일 수 있습니다.

- **RADIUS 및 TACACS+**

V2824는 사용자 인증 프로토콜로 RADIUS(Remote Authentication Dial-In User Service)와 Tacacs+(Terminal Access Controller Access Control System+)를 지원합니다. 스위치에 등록되어 있는 사용자 ID와 Password 이외에도 RADIUS 서버와 TACACS+ 서버를 통하여 인증을 받아야 하기 때문에 시스템 관리 및 네트워크 관리의 보안성을 높였습니다.

- **Storm Control**

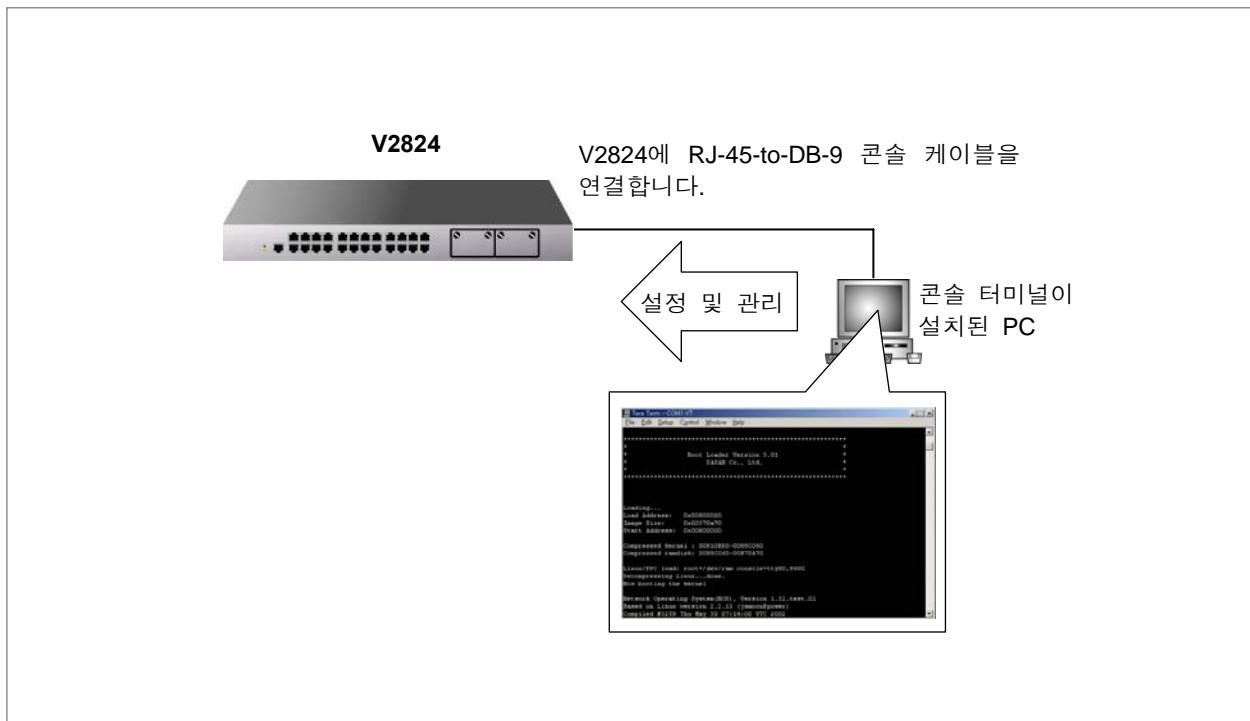
Storm이란, 다량의 특정 패킷이 네트워크상에 전송되면서 전송 용량의 대부분을 점유함에 따라 네트워크 타임 아웃이 발생하는 현상을 말합니다. V2824는 사용자가 설정한 시간동안 한계 값을 넘는 브로드캐스트 패킷, 멀티캐스트 패킷, 그리고 DLF 패킷을 Drop 하는 Storm Control을 지원합니다.

3. CLI 사용하기

- 명령어 체계
- 명령어 기본 사용법

3.1 명령어 체계

V2824는 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.



【 그림 3-1 】 콘솔 터미널을 통한 시스템 설정 및 관리

다음은 V2824에서 사용하는 DSH 명령어를 구성하는 모드입니다.

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

3.1.1 Privilege Exec View 모드

사용자가 스위치에 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 V2824의 Privilege Exec View 모드에서 사용하는 주요 명령어입니다.

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

명령어	기능
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 가지려면 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 바くなります.

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 스위치에 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 】는 V2824의 Privilege Exec Enable 모드에서 사용하는 주요 명령어입니다.

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

명령어	기 능
clock	시스템에 시간 및 날짜를 입력합니다.
configure terminal	Global 설정 모드로 들어갑니다.
reload	시스템을 다시 부팅합니다.
telnet	telnet으로 다른 장비에 접속합니다.
terminal length	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 다음 명령어를 입력하면 들어갈 수 있습니다. Global 설정 모드로 들어가면 시스템 프롬프트가 SWITCH#에서 SWITCH(config)#로 바くなります.

명령어	모 드	기 능
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, Bridge 설정 모드로 들어갈 수 있습니다. 【 표 3-3 】은 V2824의 Global 설정 모드의 주요 명령어입니다.

【 표 3-3 】 Global 설정 모드 주요 명령어

명령어	기 능
arp	IP 주소와 MAC 주소를 ARP 테이블에 등록합니다.
bridge	Bridge 설정 모드로 들어갑니다.
copy	설정한 내용을 Backup하거나 Backup한 설정을 불러 옵니다.
disconnect	원격 접속자의 연결을 해제합니다.
exec-timeout	자동 로그 아웃 기능을 설정합니다.
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.
snmp	Snmp를 설정합니다.
syslog	Syslog를 설정합니다.
time-zone	Time-zone을 설정합니다.

3.1.4 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, 스택킹, 미러링 등 Layer 2 스위치로서의 기능을 설정합니다.

【 표 3-4 】 은 V2824의 Bridge 설정 모드에서 사용하는 주요 명령어입니다.

【 표 3-4 】 Bridge 설정 모드 주요 명령어

명령어	기 능
exit	현재 모드를 마치고 이전 모드로 전환합니다.
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.

3.1.5 Interface 설정 모드

V2824의 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 3-5 】 는 V2824의 Interface 설정 모드에서 사용하는 주요 명령입니다.

【 표 3-5 】 Interface 설정 모드 주요 명령어

명령어	기 능
descripton	인터페이스에 대한 설명을 기록합니다.
end	현재 모드를 마치고 Privilege Exec Enable 모드로 전환합니다
exit	현재 모드를 마치고 이전 모드로 전환합니다.
interface interface-name	다른 인터페이스 설정 모드로 이동합니다.
ip	IP 주소를 설정합니다.
shutdown	인터페이스를 비활성화 시킵니다.

3.1.6 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 설정 모드에서 Flow 설정 모드로 들어갑니다.
policer policer-name create	Global	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. 【표 3-5】는 V2824의 Rule 설정 모드의 주요 명령어입니다.

【표 3-6】 Rule 설정 모드 주요 명령어

명령어	기 능
apply	설정한 Rule 내용을 저장하고 장비에 적용시킵니다.
color	패킷 Coloring 분류를 설정합니다.
counter	패킷 Counter를 설정합니다.
cos	해당 Rule에 CoS를 설정합니다.
dscp	패킷의 ToS 영역에 있는 DSCP값으로 정책을 설정합니다.
ethtype	Ethernet type으로 패킷 조건을 설정합니다.
include-	특정 Class, Flow 혹은 Policer를 바인딩합니다.
interface-binding	포트 및 VLAN에 바인딩을 설정합니다.
ip	IP 주소로 패킷 조건을 설정합니다.
ip-precedence	IP TOS precedence로 정책을 설정합니다.
length	패킷 길이로 패킷 조건을 설정합니다.

3.1.7 DHCP Pool 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	모 드	기 능
ip dhcp pool pool-name	Global	DHCP 설정을 위한 DHCP 설정 모드로 들어갑니다.

DHCP Pool 설정 모드에서는 DHCP 서버에서 사용하는 IP 주소 범위를 설정하고, 서브넷에 그룹을 지정하고, 서브넷의 디폴트 게이트웨이를 설정합니다. 【 표 3-7 】는 V2824의 DHCP Pool 설정 모드의 주요 명령어입니다.

【 표 3-7 】 DHCP Pool 설정 모드 주요 명령어

명령어	기 능
default-gateway	서브넷의 디폴트 게이트웨이를 설정합니다.
dns-server	DNS 서버를 설정합니다.
fixed-address	IP 주소를 특정 MAC 주소를 가진 호스트에게 지정합니다.
lease-time	IP 사용 가능 시간으로 설정합니다.
range	DHCP 서버에서 사용하는 IP 주소의 범위를 설정합니다.

3.1.8 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 】은 V2824의 DHCP Option82 설정 모드의 주요 명령어입니다.

【 표 3-8 】 DHCP Option-82 설정 모드 주요 명령어

명령어	기능
end	현재 모드를 마치고 Privilege Exec Enable 모드로 전환합니다
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.

3.1.9 RMON 설정 모드

Global 설정 모드에서 “rmon-alarm <1-65,535>”, “rmon-event <1-65,535>”, “rmon-history <1-65,535>” 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 】은 V2824의 RMON 설정 모드에서 공통적으로 사용하는 명령어입니다.

【 표 3-9 】 RMON 설정 모드 공통 명령어

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

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
- 실행된 명령어 목록 확인하기
- Privilege Exec Enable 모드 명령어 사용하기
- no 명령어 사용하기
- show 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 V2824의 Priveilege 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 (see also 'undebbug')
  enable     Turn on privileged mode command
  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
```

(중략)

```
SWITCH#
```

 주 의

물음표(?)는 입력해도 화면에는 출력되지 않으며 Enter 키를 누르지 않아도 곧장 명령어 리스트를 출력해줍니다. 이 매뉴얼은 1.03 버전의 NOS를 기준으로 작성된 것입니다. 제품에 설치된 NOS에 따라 출력된 내용이 다를 수 있으니 주의하시기 바랍니다.

DSH이 탑재되어 있는 V2824의 사용자는 특정 알파벳으로 시작하는 명령어를 알아볼 수 있습니다. 알고 싶은 첫 단어를 입력한 뒤 빈 칸없이 물음표를 입력하십시오.

다음은 V2824의 Privilege Exec Enable 모드에서 **s**으로 시작하는 명령어를 알아보는 방법입니다.

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

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

```
SWITCH# traceroute?  
WORD Trace route to destination address or hostname  
ip     IP Trace  
<cr>  
  
SWITCH# traceroute
```

각 명령어 모드에서 사용할 수 있는 명령어와 입력해야 하는 변수의 목록을 더욱 자세히 알기를 원한다면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show list	All	현재 모드에서 사용 가능한 명령어 목록을 확인합니다.
show cli		현재 모드에서 사용 가능한 명령어 목록을 트리 구조로 확인합니다.

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 log
    clear ip arp inspection statistics (vlan VLAN_NAME| )
    clear ip dhcp authorized-arp invalid
    clear ip dhcp leasedb A.B.C.D/M
    clear ip dhcp leasedb all
    clear ip dhcp leasedb pool POOL
    clear ip dhcp relay statistics
    clear ip dhcp statistics
    clear ip igmp
    clear ip igmp group *
    clear ip igmp group A.B.C.D
    clear ip igmp group A.B.C.D IFNAME
    clear ip igmp interface IFNAME
    clear ip igmp snooping stats port (PORTS|cpu| )
    clear ip mcfdb (*|vlan VLAN)
    clear ip mcfdb vlan VLAN group A.B.C.D source A.B.C.D
    clear ip mroute *
    clear ip mroute A.B.C.D
    clear ip mroute A.B.C.D A.B.C.D
    clear ip mroute statistics *
    clear ip mroute statistics A.B.C.D
    clear ip mroute statistics A.B.C.D A.B.C.D
--More--
```

참 고

More가 출력된 상태에서 다음 리스트를 확인하려면, 엔터키를 제외한 키를 입력하십시오. 엔터키를 누르면 다음 한 개의 명령어만 보여집니다.

참 고

More가 출력된 상태에서 명령어 리스트 확인을 종단하려면, **q**키 또는 **Ctrl+C**를 입력하십시오.

주 의

이 매뉴얼은 NOS 1.03 버전을 기준으로 작성된 것입니다. 제품에 설치된 NOS에 따라 출력된 내용이 다를 수 있으니 주의하시기 바랍니다.

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
Fri, 30 Sep 2005 07:10:07 +0000
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.

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 실행된 명령어 목록 확인하기

V2824에서는 실행된 명령어들을 오름차순으로 최대 20개까지 확인할 수 있습니다. DSH에서 실행된 명령어들은 FIFO(First In First Out) 구조의 명령어 버퍼에 기록됩니다. 20개 이상의 명령어가 실행된 경우에는 시간상 먼저 실행된 명령어들이 차례로 지워지면서, 각 명령어들의 순번이 낮아지고 나중에 실행된 명령어가 높은 순번으로 명령어 목록에 추가됩니다.

이전에 실행되었던 명령어 목록을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show history	View / Enable / Global / Bridge	실행된 명령어 목록을 확인합니다.

3.2.5 Privilege Exec Enable 모드 명령어 사용하기

V2824에서는 다음 명령어로 Privilege Exec Enable 모드의 명령어를 다른 모드에서 사용할 수 있습니다.

명령어	모 드	기 능
do command	Global/RMON/DHCP/Option-82/Bridge Interface/Rule	다른 모드에서 Privilege Exec Enable 모드의 명령어를 사용할 수 있습니다.

다음은 Bridge 설정 모드에서 Ping 테스트를 실시하는 경우의 예입니다.

```
SWITCH(bridge)# do ping 203.236.124.209
PING 203.236.124.209 (203.236.124.209) from 173.03.209.87 : 56(84) bytes of data
.
64 bytes from 203.236.124.209: icmp_seq=0 ttl=127 time=0.0 ms
64 bytes from 203.236.124.209: icmp_seq=1 ttl=127 time=1.0 ms
64 bytes from 203.236.124.209: icmp_seq=2 ttl=127 time=1.0 ms
64 bytes from 203.236.124.209: icmp_seq=3 ttl=127 time=1.0 ms
64 bytes from 203.236.124.209: icmp_seq=4 ttl=127 time=1.1 ms
64 bytes from 203.236.124.209: icmp_seq=5 ttl=127 time=1.0 ms
64 bytes from 203.236.124.209: icmp_seq=6 ttl=127 time=1.0 ms
64 bytes from 203.236.124.209: icmp_seq=7 ttl=127 time=1.0 ms

--- 203.236.124.209 ping statistics ---
9 packets transmitted, 9 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.9/1.1 ms
% Unknown command.
SWITCH(bridge)#

```

3.2.6 no 명령어 사용하기

V2824의 **no** 명령어는 설정된 기능을 해제하거나, 사용자 설정값을 시스템에서 기본으로 지정한 값으로 되돌립니다.

3.2.7 show 명령어 사용하기

V2824 기능 설정 여부 또는 설정 내용은 **show** 명령어로 확인 가능합니다.

V2824에서 제공되는 모든 **show** 명령어는 마지막에 다음과 같은 옵션으로 키워드에 해당하는 정보만 확인 가능합니다.

- **| begin** : 지정된 키워드로 시작되는 설정을 확인합니다.
- **| include** : 지정된 키워드가 포함된 설정을 확인합니다.
- **| exclude** : 지정된 키워드를 제외한 설정을 확인합니다.

명령어	모 드	기 능
show {command command} [begin]		
show {command command} [include]	All	장비 설정을 확인합니다.
show {command command} [exclude]		

3.2.8 다른 모드로 이동하기

V2824는 CLI를 사용하여 설정하면서 전 단계 모드로 돌아가거나 **Enable** 모드로 돌아갈 수 있습니다. 한편, **Enable** 모드에서는 전 단계 모드로 돌아갈 수 있는 명령어는 없고, 대신 시스템에서 로그 아웃하는 명령어가 존재합니다.

전 단계 모드로 돌아가거나 Enable 모드로 돌아가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
exit	Global / RMON / DHCP / Option-82 / Bridge Interface / Rule	전 단계 모드로 돌아갑니다.
end	Global / RMON / DHCP / Option-82 / Bridge Interface / Rule	Enable 모드로 돌아갑니다.

다음은 시스템에서 로그아웃할 때 사용하는 명령어입니다.

명령어	모 드	기 능
exit	View / Enable	시스템에서 로그아웃합니다.

4. 시스템 접속 및 IP 주소 설정

- 시스템 접속
- IP 주소 설정

4.1 시스템 접속

설치가 끝난 V2824는 각 포트가 네트워크와 관리용 PC에 올바르게 연결되어 있는지 최종 점검을 거치게 됩니다. 모든 점검이 끝나면, 사용자는 V2824를 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
- 패스워드 초기화
- 자동 로그 아웃 기능 설정
- 사용자 계정 관리
- 접속자 수 제한
- 원격 접속
- 원격 접속자 확인 및 연결 강제 해제
- 시스템 리부팅
- 시스템 로그 아웃

4.1.1 시스템 로그인

V2824의 설치가 끝나면 각 포트가 네트워크와 관리용 PC에 올바르게 연결되어 있는지 최종 점검 하십시오. 모든 점검이 끝나면, 전원 스위치를 켜고 다음과 같이 부팅 시킵니다.

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

```
*****
*
*          Boot Loader Version 4.84
*
*          DASAN Networks Inc.
*
*****
Press 's' key to go to Boot Mode: 0

Load Address: 0x83000000
Image Size: 0x00b31b80
Start Address: 0x83000000

NOS version 3.13 #4450
CPU : BCM5836 at 264 MHz
Total Memory Size : 128 MB
Calibrating delay loop... 262.96 BogoMIPS
Switch init...
INIT: version 2.85 booting
Extracting configuration
Sat, 01 Jan 2000 00:00:06 +0000
INIT: Start UP

SWITCH login:
```

참 고

사용자 장비의 버전에 따라 위의 출력 내용은 달라질 수 있습니다.

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

스위치를 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 삼가 해 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 사용자의 패스워드를 **networks**로 변경하는 경우의 예입니다.

```
SWITCH(config)# passwd
Changing password for admin
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	패스워드 보안 설정을 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.



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.



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
(종략)
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 bJ6fc1PZlAIRk
!
service password-encryption
exec-timeout 0 0
!
(중략)
SWITCH(config)#

```

[설정 예제 2]

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



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 bJ6fc1PZlAIRk
SWITCH(config)# exit
SWITCH# exit

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

```

4.1.4 패스워드 초기화

사용자는 다음 단계에 따라, 현재 설정 내용을 유지하면서 시스템 로그인 패스워드와 Enable 접속 모드 패스워드를 초기화할 수 있습니다.

V2824에 기본으로 설정되어 있는 패스워드는 없습니다. 그러므로 초기화 후, 패스워드 대신에 엔터를 입력하여 시스템 로그인 및 Enable 모드 진입이 가능합니다.

1 단계 시스템 로그인 과정에서 **Start Address: 0x00800000** 메시지가 보이면 스페이스바를 반복하여 누르십시오.

2 단계 **console=ttyS0,9600 root=/dev/ram rw** 메시지가 보이면 스페이스바 누르기를 멈추고, **password**를 입력하십시오.

3 단계 부팅 메시지에 **Initialize Password**라는 문구가 보이면 패스워드가 시스템 로그인 및 Enable 패스워드가 초기화가 이루어진 것입니다.

4 단계 시스템에 로그인하거나 Enable 모드로 들어갈 때 패스워드 대신 엔터를 입력하십시오.



시스템 로그인 및 Enable 모드 접속 패스워드를 재설정 하시려면, 각각 **시스템 로그인 패스워드 변경**과 **Enable 모드 접속 패스워드 설정**을 참고하십시오.

4.1.5 자동 로그 아웃 기능 설정

V2824의 관리자가 콘솔 터미널 스크린을 켜 둔 채 자리를 비우게 되는 경우, 계속 로그인 상태로 방치된다면 다른 사람이 관리자의 설정을 변경할 수도 있습니다. 따라서 V2824에는 관리자가 정해놓은 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 exec-minute [exec-seconds]	Global	자동 로그 아웃 기능을 설정합니다.
exec-timeout 0		자동 로그 아웃 기능을 해제합니다.



참 고

자동 로그 아웃 기능은 분단위(*exec-minute*)와, 초단위(*exec-seconds*)로 나누어 설정 가능합니다.

분단위(*exec-minute*)는 <1 – 35, 791> 사이에서, 초단위(*exec-seconds*)는 <0 – 59> 사이에서 설정 가능합니다. 기본으로 설정되어 있는 시간은 10분입니다.

사용자의 장비에 설정된 자동 로그 아웃 시간을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show exec-timeout	Enable / Global	자동 로그 아웃 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 seconds
SWITCH(config)#{
```

4.1.6 사용자 계정 관리

V2824는 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.

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

- 사용자 계정 추가
- 사용자 권한 설정
- 설정 예제

(1) 사용자 계정 추가

V2824는 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	Enable / Global	추가된 사용자 계정을 확인합니다.

(2) 사용자 권한 설정

V2824는 장비에 접속하는 사용자 권한 Level을 0부터 15까지 16단계로 구분하여 설정할 수 있습니다. 가장 높은 Level 15는 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 모드에서 **exit**와 **help** 명령어만 사용할 수 있고, Privilege Exec Enable 모드에 접속할 수 없게 되어 있습니다.

다음은 사용자 Level에 따른 명령어 사용 권한을 설정하는 명령어입니다.

명령어	모 드	기 능
privilege bridge level <0-15> {command all}	Global	Bridge 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 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege dhcp-pool-class level <0-15> {command all}		DHCP Pool Class 설정 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 interface level <0-15> {command all}		Interface 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege route-map level <0-15> {command all}		Route-map 설정 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 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 rmon-alarm level <0-15> {command all}		RMON 설정 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.
privilege rmon-event level <0-15> {command all}		
privilege rmon-history level <0-15> {command all}		
privilege view level <0-15> {command all}		Privilege Exec View 모드의 어떤 명령어를 해당 Level에서 사용할 수 있게 합니다.



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.



참 고

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 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 interface 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 flow level <0-15> {command all}		
no privilege policer level <0-15> {command all}		
no privilege policy level <0-15> {command all}		
no privilege view level <0-15> {command all}		
	Global	각 모드의 명령어에 대해 사용자 권한으로 설정한 내용을 삭제합니다.

관리자가 설정한 Level에 따른 권한을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show privilege	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)#

```

[설정 예제 3]

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.

4.1.7 접속자 수 제한

V2824 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.



참 고

V2824는 기본적으로 접속자 수를 8명으로 제한하고 있습니다.

장비에 접속할 수 있는 사용자 수를 제한했던 설정을 해제합니다.

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

4.1.8 원격 접속

V2824는 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.



주 의

write memory을 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#
```

4.1.9 원격 접속자 확인 및 연결 강제 해제

V2824의 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	Enable	원격 접속자의 연결을 해제합니다.

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

```
SWITCH(config)# where
접속자의 ID          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)#

```

4.1.10 시스템 리부팅

TFTP/FTP 서버에서 새로운 시스템 이미지를 내려 받은 이후에는 반드시 시스템을 리부팅해야 하고, 이 밖에도 터미널 프로그램을 통해 스위치를 설정 및 관리하는 도중에 다시 시스템을 부팅시켜야 하는 경우가 발생할 수 있습니다.

시스템을 리부팅하려면 Privilege Exec Enable 모드에서 다음의 명령어를 사용하십시오.

명령어	모 드	기 능
reload [os1 os2]	Enable	시스템을 다시 부팅시킵니다.



주의

시스템을 리부팅하면 저장하지 않은 설정 내용은 지워지게 됩니다. 따라서 시스템을 리부팅하기 전에는 설정 내용을 반드시 저장하십시오.

V2824는 사용자가 설정한 내용을 저장하지 않고 리부팅하는 것을 방지하기 위해서 설정한 내용이 있는데 **write memory** 명령어로 저장하지 않았을 경우, 다시 한번 저장 의사를 확인합니다. 새로운 설정 내용을 저장하기를 원한다면 **y**를 입력하시고, 설정 내용을 그대로 삭제하려면 **n**을 입력한 후 시스템을 리부팅 하시기 바랍니다.

다음은 시스템을 설정한 후 내용을 저장하고 리부팅했을 경우 보여지는 메시지입니다.

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

4.1.11 Auto Reset

V2824는 사용자가 설정한 조건에 따라 자동적으로 시스템을 리부팅하는 기능이 있습니다. 시스템을 리부팅하는 기준이 되는 것은 CPU 로드와 Memory 용량, 그리고 네트워크 접속상태입니다.

(1) CPU Load에 의한 자동 리부팅 설정

V2824는 CPU Load나 Interrupt Load가 일정한 시간 동안에 지정한 값이 지속될 경우에 시스템을 리부팅하도록 설정할 수 있습니다.

CPU Load를 기준으로 시스템 자동 리부팅 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
auto-reset cpu cpu-load-average interrupt-load-average time	Bridge	<i>time</i> 동안 <i>cpu-load-average</i> 또는 <i>interrupt-load-average</i> 가 지속되면 자동 리부팅되도록 설정합니다.
no auto-reset cpu		CPU Load를 기준으로 설정한 시스템 자동 리부팅 기능을 해제합니다.



*cpu-load-average*는 50부터 100까지 설정이 가능하며, *interrupt-load-average*은 1부터 100까지 설정 할수 있습니다.

CPU Load를 기준으로 설정한 시스템 자동 리부팅 기능에 대한 내용을 확인하려면 다음 명령어 사용하십시오.

명령어	모 드	기 능
show auto-reset cpu	Enable/Global/Bridge	CPU Load를 기준으로 설정한 시스템 자동 리부팅에 대한 설정을 확인합니다.

[설정 예제 1]

다음은 1분간 CPU Load가 70%로 지속되거나 Interrupt Load가 70%로 지속될 경우에 시스템이 자동 리부팅되도록 설정한 예입니다.

```
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)#

```

(2) Memory 용량에 의한 자동 리부팅

V2824는 Memory의 하한임계치에 해당하는 Memory-low가 일정 시간 동안 사용자가 지정한 회수만큼 발생하면 자동적으로 리부팅되도록 설정할 수 있습니다. Memory 용량에 의한 자동 재부팅 기능을 설정하기 위하여 Memory-low의 발생시간과 Memory-low의 발생회수를 설정할 경우에는 다음 명령어를 사용하십시오.

명령어	모 드	기 능
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 리부팅되도록 설정합니다.
no auto-reset memory		Memory로 설정한 자동 리부팅 기능을 해제합니다.

i 참 고

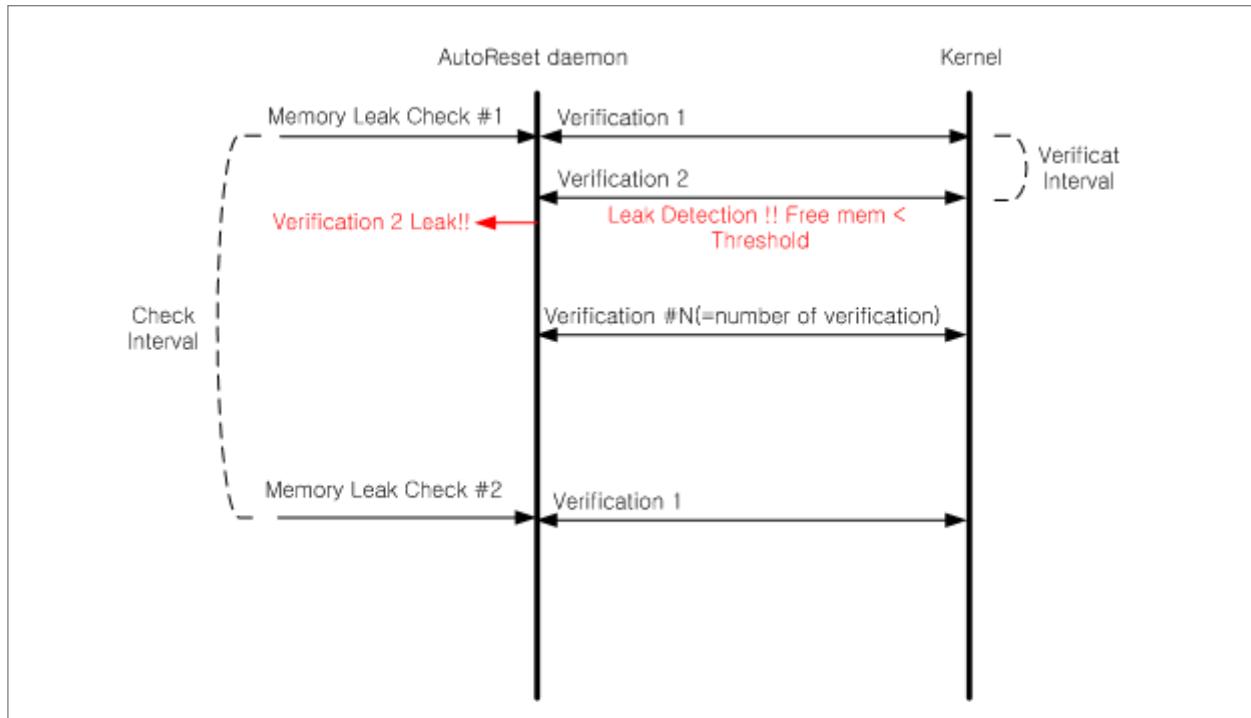
*time-threshold-of-memory-low*는 1부터 120까지 설정할 수 있고, *count-of-memory-low*는 1부터 10까지 설정할 수 있습니다.

i 참 고

auto-reset memory 명령어에서 *time-threshold--memory-low*는 기본적으로 10분으로 설정되어 있으며, *count-memory-low*는 기본적으로 5회로 설정되어 있습니다.

한편, 더욱 개선된 V2824는 Memory-leak를 이용하여 시스템 자동 재부팅 기능을 설정할 수 있습니다. Memory-leak란 Memory 용량이 사용자가 지정한 Memory 임계치 이하로 떨어지는 현상을 말합니다. 이 기능을 설정하면 사용자가 지정한 시간 간격에 따라 주기적으로 Memory 용량을 Check하게 되고, 이 때 사용자가 정해 놓은 기준 이상으로 memory-leak가 발생하면 장비는 자동으로 재부팅을 하게 됩니다. Memory-leak에 따라 자동으로 재부팅하도록 설정하였을 때, 실시하게 되는 Memory Check는 1회 실시할 때마다 지정된 횟수만큼의 Verification을 실행하게 되고, 지정된 횟수 만큼의 Verification에 대해 모두 memory-leak로 확인되었을 때, Memory Check에 대한 memory-leak 가 1회 발생한 것으로 간주됩니다.

다음 그림은 Memory-leak를 확인하기 위하여 Memory를 체크하는 내부동작을 설명하는 것입니다.



【 그림 4-1 】 Auto-reset을 위한 Memory Check 동작

위의 그림을 살펴보면, Memory Check를 1회 실시될 때 사용자가 설정한 횟수만큼 Verification을 실행하고, Memory가 설정한 임계치보다 낮으면 memory-leak로 확인되지만, 여러 번 실시한 Verification에서 1번 memory-leak가 확인된 것은 Memory Check에 대한 memory-leak로 간주되지 않습니다. Memory Check를 실시하는 시간 간격이나 Verification을 실시하는 시간 간격 모두 사용자가 설정할 수 있으며, Memory Check에 대한 memory-leak가 사용자가 설정한 기준 이상의 횟수만큼 발생하였을 때 장비는 자동적으로 재부팅됩니다. 이 때 재부팅되는 시간도 사용자가 설정할 수 있습니다.

메모리 용량에 따라 장비가 자동적으로 재부팅 되도록 설정하는 방법은 다음과 같습니다.

1 단계 메모리 용량을 확인하는 Memory Check를 실행할 때 필요한 옵션을 설정합니다.

Memory Check 실행에 필요한 옵션을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
auto-reset memory-leak <i>memory-threshold-size</i> <i>memory-check-interval</i> <i>verification-number</i> <i>verification-interval</i> <i>reboot-counter</i>	Bridge	메모리 용량을 확인하기 위한 Memory check를 실행할 때 필요한 옵션들을 설정합니다.



참 고

*memory-threshold-size*는 memory-leak를 판단하기 위한 임계값입니다. 설정된 임계값보다 Free 메모리 용량이 적을 때, memory-leak으로 판단됩니다. 1Kbyte부터 524,288Kbytes까지 입력이 가능하며 입력 단위는 킬로바이트(Kbytes)입니다.

*memory-check-interval*은 Memory check를 실행하는 주기 간격으로 초 단위로 10초부터 86,400초까지 설정이 가능합니다.

*verification-number*는 1회의 Memory check에서 실시하게 되는 Verification 회수로, 1회부터 10회 까지 설정할 수 있습니다.

*verification-interval*은 Verification을 실행하는 주기 간격으로 초 단위로 1초부터 10초까지 설정할 수 있습니다.

*reboot-counter*는 자동 재부팅을 실행하는 기준이 되는 값으로, 이 임계치 이상으로 memory-leak가 발생하면, 장비가 자동으로 재부팅합니다. 1부터 100까지 설정 가능합니다.



참 고

*memory-check-interval*은 (*verification-number*×*verification-interval*) 보다 크게 설정해야 합니다.

Memory-leak를 확인하기 위해 Memory Check를 실행하도록 설정한 옵션을 해체할 경우에는 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no auto-reset memory-leak	Bridge	Memory Check 실행에 필요한 옵션을 해제합니다.

2 단계 Memory-leak에 따른 자동 재부팅 기능을 활성화합니다.

명령어	모 드	기 능
auto-reset memory-leak enable	Bridge	Memory-leak에 따른 자동 재부팅 기능을 활성화합니다.



참 고

Memory Check 실행을 위해 필요한 옵션을 설정하지 않으면 메모리 용량 상태에 따른 자동 재부팅 기능을 활성화 할 수 없습니다.

3 단계 Memory-leak에 따른 자동 재부팅을 실행할 시간을 지정합니다.



참 고

Memory-leak에 따른 자동 재부팅은 지정한 시간대에서만 실행됩니다. 지정된 시간대가 아닌 경우 memory-leak가 발생하였더라도 다시 메모리 용량의 상태가 복구되면 지정된 시간대에도 자동 재부팅은 실행되지 않습니다.

Memory-leak에 따른 자동 재부팅 기능을 실행할 시간을 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
auto-reset memory-leak reboot-time <i>start-hour start-minute end-hour end-minute</i>	Bridge	Memory-leak에 따른 자동 재부팅 기능을 실행할 시간대를 설정합니다.
no auto-reset memory-leak reboot-time		Memory-leak에 따른 자동 재부팅 기능을 실행할 시간대를 설정한 것을 해제합니다.



참 고

*start-hour*는 <0-23>, *start-minute*는 <0-59>, *end-hour*는 <0-23>, *end-minute*는 <0-59> 범위에서 입력할 수 있습니다.

한편, V2824는 메모리 용량 상태에 따른 자동 재부팅 기능을 설정하였을 때, 자동 재부팅이 어느 정도 반복되었을 때, 더 이상 자동 재부팅이 이루어지지 않도록 제어할 수 있습니다. 사용자가 자동 재부팅 횟수를 제한해 놓으면, 그 이상으로 재부팅이 이루어졌을 때 더 이상 자동 재부팅을 실행하지 않습니다.

메모리 용량 상태에 따라 자동 재부팅이 이루어지도록 설정했을 때, 사용자가 설정한 횟수 이상으로 재부팅이 이루어졌을 때 더 이상 자동 재부팅을 실행하지 않도록 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
auto-reset memory-leak reboot-threshold <1-100>	Bridge	설정한 횟수 이상으로 재부팅이 이루어지면 더 이상 자동 재부팅이 실행되지 않도록 합니다.
no auto-reset memory-leak reboot-threshold		설정한 횟수 이상으로 리부팅이 실행되면 더 이상 자동 리부팅이 실행되지 않도록 설정한 것을 해제합니다.

메모리 용량 상태에 따른 자동 재부팅 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
auto-reset memory-leak disable	Bridge	메모리 용량 상태에 따른 자동 재부팅 기능을 해제합니다.

메모리 용량 및 Memory-leak에 따른 자동 재부팅 기능에 대한 설정 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show auto-reset memory	Enable/Global/Bridge	메모리 상태에 따른 자동 재부팅 기능에 대한 설정 내용을 확인합니다.
show auto-reset memory-leak		

[설정 예제 2]

다음은 10분 동안 Memory low가 3번 발생하였을 때 자동으로 리부팅하도록 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)#

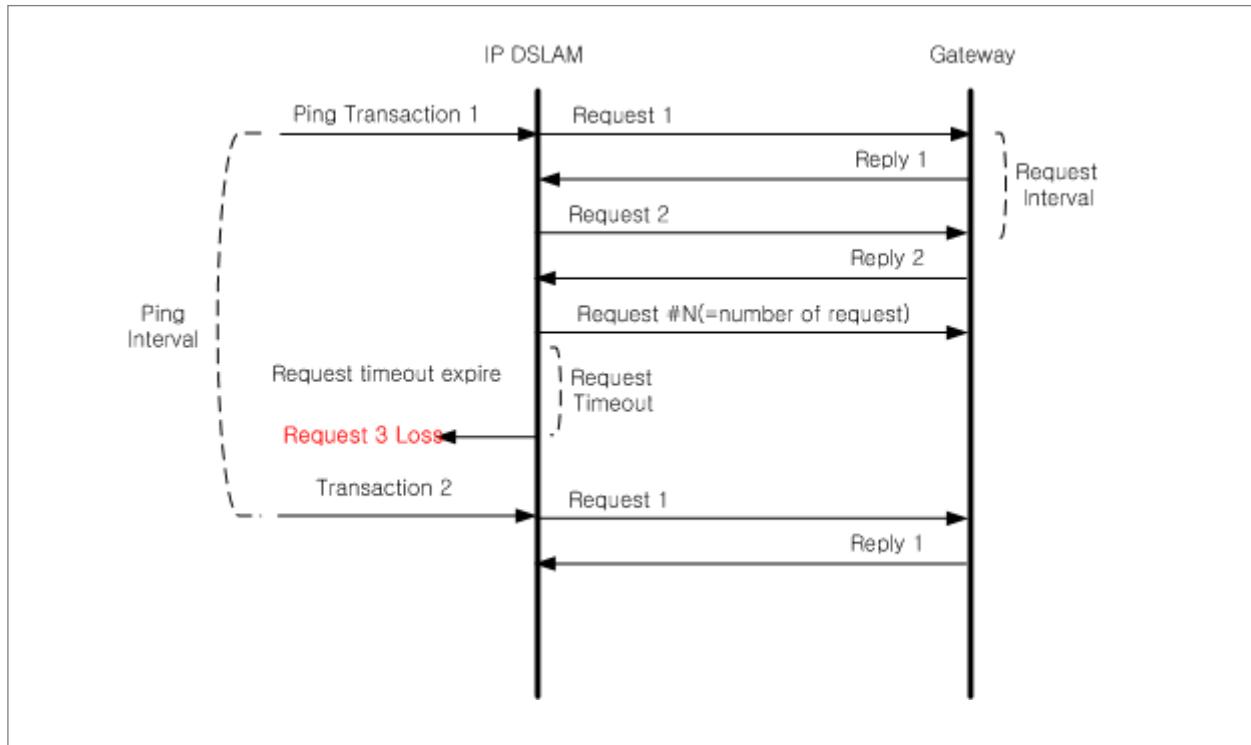
```

(3) 네트워크 접속상태에 의한 자동 리부팅 설정

V2824는 CPU load나 Memory 상태뿐만 아니라 네트워크 연결 상태에 따라 자동으로 장비를 재부팅 할 수 있습니다. 네트워크 연결 상태를 확인하기 위해 “Ping”을 실행할 때, 사용자가 설정해 놓은 기준 이상으로 응답이 없으면 장비는 자동으로 재부팅을 하게 됩니다.

네트워크 연결 상태에 따라 자동으로 재부팅하도록 설정하였을 때 실행하게 되는 “Ping”은 1회 실시할 때마다 지정된 횟수 만큼의 Request를 실행하게 되고, 지정된 횟수 만큼의 Request에 대해 모두 응답이 없을 때, “Ping”에 대한 응답이 없는 것으로 간주됩니다.

다음 그림을 살펴보면, Ping이 1회 실시될 때 사용자가 설정한 회수 만큼 Request를 보내고, 이에 대한 Reply가 없을 때, Request loss가 발생하지만, 여러 번 보내어진 Request에 대해 1번 loss가 발생한 것은 Ping에 대한 loss로는 간주되지 않습니다. Ping을 실시하는 시간 간격이나 Request를 보내는 시간 간격 모두 사용자가 설정할 수 있으며, Reply를 받을 때까지 기다리는 대기 시간 역시 사용자가 설정할 수 있습니다. 대기 시간 내에 Reply가 없으면 Request loss로 처리됩니다. 이렇게 Ping에 대한 loss가 사용자가 설정한 기준 이상으로 발생하였을 때 장비는 자동적으로 재부팅됩니다.



【 그림 4-2 】 Auto-reset을 위한 Ping 동작

네트워크 연결 상태에 따라 장비가 자동적으로 재부팅 되도록 설정하는 방법은 다음과 같습니다.

1 단계 네트워크 연결 상태를 확인하기 위한 Ping을 실행할 때 필요한 옵션들을 설정합니다.

Ping 실행에 필요한 옵션을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
auto-reset ping gateway-ip-address ping-transaction-interval request-number request-interval timeout-of-request ping-loss-threshold		네트워크 연결 상태를 확인하기 위한 Ping을 실행할 때 필요한 옵션들을 설정합니다.
auto-reset ping default-gw ping-transaction-interval request-number request-interval timeout-of-request ping-loss-threshold	Bridge	장비에 설정되어 있는 Default gateway를 기준으로 네트워크 연결 상태를 확인하기 위한 Ping을 실행할 때 필요한 옵션들을 설정합니다.



참 고

*gateway-ip-address*는 Ping을 실행할 Gateway의 IP 주소입니다.

*ping-transaction-interval*은 Ping을 실행하는 주기 간격으로 초 단위로 10초부터 86,400초까지 설정이 가능합니다.

*request-number*는 1회의 Ping에서 실시하게 되는 Request 회수로, 1회부터 10회까지 설정할 수 있습니다.

*request-interval*은 Request를 실행하는 주기 간격으로 초 단위로 1초부터 10초까지 설정할 수 있습니다.

*timeout-of-request*는 Request에 대한 응답을 기다리는 시간으로, 이 시간 내에 응답이 오지 않으면, Request Loss가 발생하였다고 간주됩니다. 1초부터 10초까지 설정할 수 있습니다.

*ping-loss-threshold*는 자동 재부팅을 시행하는 기준이 되는 값으로, 이 임계치 이상으로 Ping loss 가 발생하면, 장비가 자동으로 재부팅됩니다. 1부터 100까지 설정 가능합니다.



참 고

*ping-transaction-interval*은 (*request-number*×*request-interval*) 보다 크게 설정해야 합니다.

Ping 실행에 필요한 옵션을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no auto-reset ping	Bridge	Ping 실행에 필요한 옵션을 삭제합니다.

2 단계 네트워크 연결 상태에 따른 자동 재부팅 기능을 활성화합니다.

명령어	모 드	기 능
auto-reset ping enable	Bridge	네트워크 연결 상태에 따른 자동 재부팅 기능을 활성화합니다.



참 고

Ping 실행을 위해 필요한 옵션을 설정하지 않으면 네트워크 연결 상태에 따른 자동 재부팅 기능을 활성화 할 수 없습니다.

한편, V2824는 네트워크 연결 상태에 따른 자동 재부팅 기능을 설정하였을 때, 자동 재부팅이 어느 정도 반복되었을 때, 더 이상 자동 재부팅이 이루어지지 않도록 제어할 수 있습니다. 사용자가 자동 재부팅 횟수를 제한해 놓으면, 그 이상으로 재부팅이 이루어졌을 때 더 이상 자동 재부팅을 실행하지 않습니다.

네트워크 연결 상태에 따라 자동 재부팅이 이루어지도록 설정했을 때, 사용자가 설정한 횟수 이상으로 재부팅이 이루어졌을 때 더 이상 자동 재부팅을 실행하지 않도록 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
auto-reset ping reboot-threshold <1-100>	Bridge	설정한 횟수 이상으로 재부팅이 이루어지면 더 이상 자동 재부팅이 실행되지 않도록 합니다.
no auto-reset ping reboot-threshold		설정한 횟수 이상으로 재부팅이 이루어지면 더 이상 자동 재부팅이 실행되지 않도록 설정한 것을 해제합니다.

네트워크 연결 상태에 따른 자동 재부팅 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
auto-reset ping disable	Bridge	네트워크 연결 상태에 따른 자동 재부팅 기능을 해제합니다.

네트워크 연결 상태에 따른 자동 재부팅 기능에 대한 설정 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show auto-reset ping	Bridge	네트워크 연결 상태에 따른 자동 재부팅 기능을 확인합니다.

네트워크 연결 상태에 따른 자동 리부팅 기능을 이용하여 V2824가 리부팅되도록 설정한 횟수를 초기화려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear auto-reset ping-reboot-counter	Bridge	자동 리부팅 기능을 이용하여 V2824가 리부팅되도록 설정한 횟수를 초기화합니다.

4.1.12 시스템 로그 아웃

시스템에서 로그아웃 하는 것은 Privilege Exec View 모드나 Privilege Exec Enable 모드에서 가능합니다. 따라서 다른 모드에서 설정하던 종이라면, Privilege Exec Enable 모드로 돌아가야 합니다.

시스템에서 로그아웃 하려면, 다음 명령어를 사용하십시오.

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

4.2 IP 주소 설정

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



V2824는 가상 인터페이스 `default(interface 1)`가 설정되어 있고, 모든 포트가 `default`에 멤버 포트로 설정되어 있습니다.

스위치에 IP 주소를 설정하려면 다음의 절차를 따르십시오.

- 인터페이스 활성화
- 인터페이스 활성화 해제
- 네트워크 인터페이스에 IP 주소 설정
- Static 경로 및 Default Gateway 지정
- 오류! 참조 원본을 찾을 수 없습니다.
- 인터페이스 설명하기
- 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 | interface** 명령어를 사용하십시오.

다음은 인터페이스가 활성화 되어 있는지 확인하는 경우입니다.

```
SWITCH# show running-config
interface noshutdown lo
interface noshutdown default
SWITCH#
```



Interface 1의 VLAN 이름은 「`default`」 입니다.

인터페이스를 활성화하려면 Interface 설정 모드로 들어가야 합니다. Interface 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
interface interface-name	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

Interface 설정 모드에서 인터페이스 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 할당하는 방법은 수동설정과 자동설정이 있습니다.

(1) 수동 설정

인터페이스에 IP 주소를 수동설정으로 할당하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip address address/M	Interface	인터페이스에 IP 주소를 합니다.
ip address address/M secondary		Secondary IP 주소를 설정합니다.

할당한 IP 주소를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip	Interface	인터페이스에 설정된 IP 주소를 확인합니다.

할당한 IP 주소를 삭제하려면, 다음 명령어를 사용하십시오.

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

(2) 자동 할당 설정

V2824는 DHCP 서버를 통해 인터페이스에 자동으로 IP 주소가 할당되도록 할 수 있습니다. DHCP 클라이언트로서 IP 주소를 자동 할당하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
renew interface-name	View/Enable	인터페이스에 자동으로 IP 주소를 할당하도록 요청합니다.

한편, IP 주소를 DHCP 서버에 반납하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
release interface-name	View/Enable	자동으로 할당받은 IP 주소를 반납합니다.

4.2.4 Static 경로 및 Default Gateway 지정

V2824는 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]	Global	Static 라우트를 설정합니다.
ip route ip-address/m {ip-gateway-address null} [<1-255>]		
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 {default-gateway-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]	Enable / Global / Bridge	Static 라우트를 확인합니다.
show ip route [database]		

설정했던 Static 라우트를 삭제하려면, 다음 명령어를 사용하십시오.

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

4.2.5 인터페이스 설명하기

V2824는 특정 인터페이스에 대한 설명을 등록하여 사용자가 관리하기 편리하게 하였습니다. 각 인터페이스에 대한 설명을 등록하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
description LINE	Interface	인터페이스에 대한 설명을 입력합니다.

다음은 인터페이스에 설명을 등록하고, 그 내용을 확인한 경우입니다.

```
SWITCH(config-if)# description sample_description
SWITCH(config-if)# show interface 1
Interface mgmt
Hardware is Ethernet, address is 00d0.cb00.0d83
Description: sample_description
index 43 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
Bandwidth 100m
inet 10.27.41.91/24 broadcast 10.27.41.255
    input packets 3208070, bytes 198412141, dropped 203750, multicast packets 0
    input errors 12, length 0, overrun 0, CRC 0, frame 0, fifo 12, missed 0
    output packets 11444, bytes 4192789, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
SWITCH(config-if)#

```

한편, 포트에 등록한 설명을 삭제하려면 다음 명령어를 사용하십시오.

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

4.2.6 설정 예제

[설정 예제 1]

다음은 인터페이스 1을 활성화하는 방법입니다.

```
SWITCH# configure terminal
SWITCH(config)# interface 1
SWITCH(config-if)# no shutdown
SWITCH(config-if)#
```

[설정 예제 2]

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)#

```

[설정 예제 3]

다음은 Default gateway를 설정하는 예입니다.

```
SWITCH# configure terminal
SWITCH(config)# ip route default 192.168.1.254
SWITCH(config)#
```

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 셸입니다. 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. V2824는 다음과 같이 SSH 서버와 클라이언트 모드를 제공합니다.

- SSH 서버
- SSH 클라이언트
- 인증키 설정
- 설정 예제

4.3.1 SSH 서버

(1) SSH 서버 활성화

사용자의 V2824에 SSH 서버를 활성화하려면 다음 명령어를 사용하십시오.

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

한편, V2824에서 SSH 서버 기능을 해제하려면 다음 명령어를 사용하십시오.

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

(2) 클라이언트 확인

SSH 서버인 사용자의 V2824에 접속해 있는 클라이언트를 확인할 수 있습니다. SSH 클라이언트를 확인하려면 다음 명령어를 사용하십시오.

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

(3) 클라이언트 접속 해제

SSH 서버에 접속한 클라이언트의 접속을 강제로 해제할 수 있습니다. 클라이언트의 접속을 강제로 해제하려면 다음 Global 설정 모드에서 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

V2824가 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	Enable / Global / Bridge	지금까지 SSH 서버에 접속했던 클라이언트들의 History를 확인합니다.



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

4.3.2 SSH 클라이언트

(1) SSH 서버 로그인

V2824가 SSH 클라이언트가 되어 SSH 서버에 로그인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ssh login destination [public-key]	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.

4.3.3 인증키 설정

SSH는 인증키를 생성하고, 생성된 인증키를 서버와 클라이언트가 공유함으로써 보안을 강화할 수 있습니다.

인증키는 클라이언트의 서버 로그인 과정에서 암호를 직접 입력하는 것보다 더욱 안전하며, 하나의 암호로 여러 SSH서버에 접속할 수 있는 등의 장점을 가집니다.

(1) 인증키 생성

V2824에서 인증키를 생성하시려면 다음 명령어를 사용하십시오. 생성된 인증키는 삭제될 때까지 장비에 저장됩니다.

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



참 고

rsa1은 ssh1에서 지원하는 인증 방식이고, **rsa**와 **dsa**는 ssh2에서 지원하는 인증 방식입니다.

(2) 인증키 검증

V2824에서 생성한 인증키를 검증하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ssh key verify public-key-file-name	Global	생성한 인증키 파일명을 입력하여 인증키를 검증합니다.

(3) 인증키 목록 확인

V2824에 저장되어 있는 인증키 목록을 확인하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show key-list	Enable/Global	인증키 목록을 확인합니다.

4.3.4 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.

```
SWTICH# 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  -----
SWTICH# config terminal
SWTICH(config)# ssh disconnect 150
SWTICH(config)# show ssh
connected clients : 000
num      pid      ppid      srv_usr      remote_ip      Start_Time      Stop_Time
SWTICH(config)#

```

[설정 예제 3] 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)#
```

[설정 예제 4] 인증키를 사용하여 서버에 접속

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@V1824
SWITCH_A(config)#

```

- 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#
```

4.4 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.

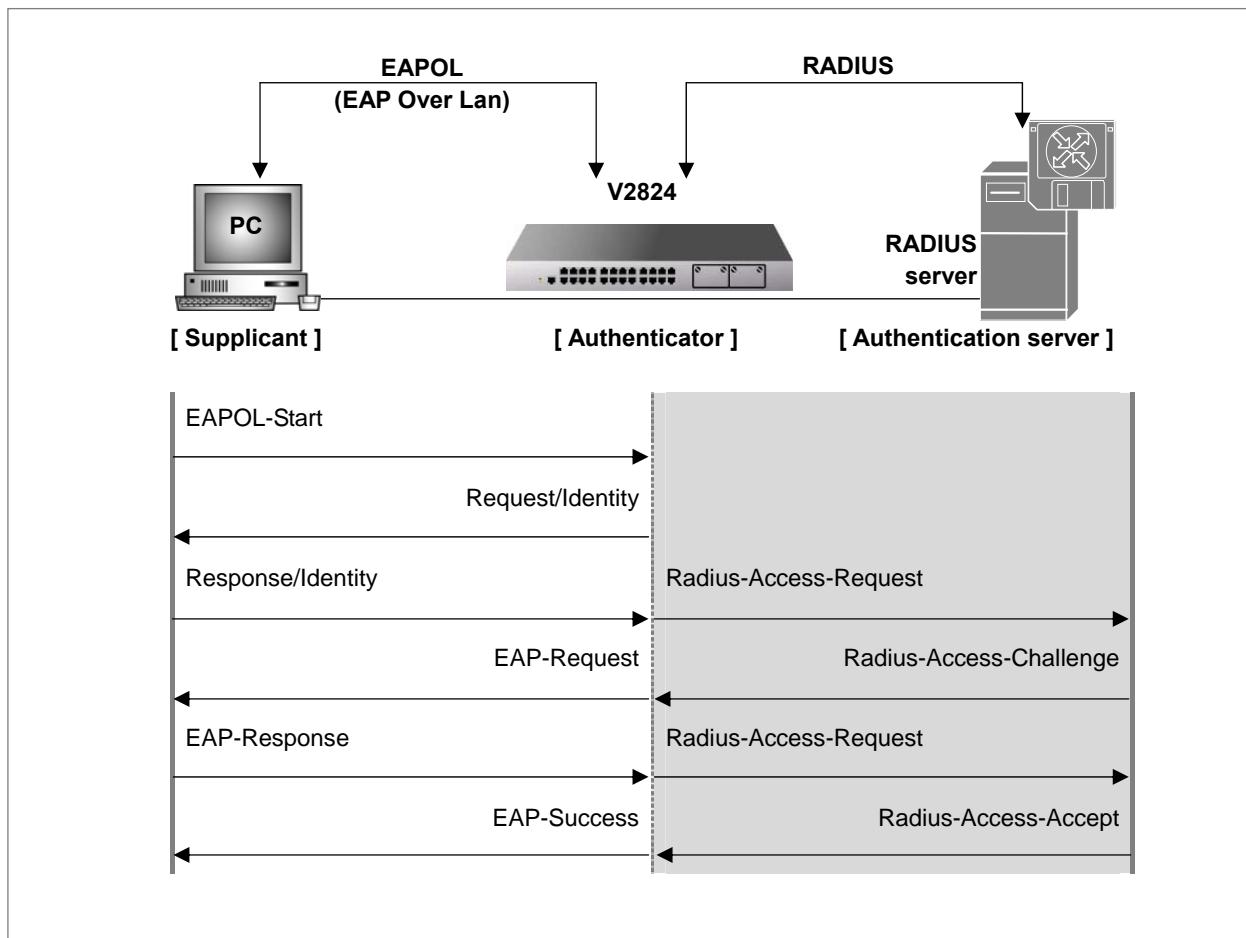
802.1x 인증은 EAP(Extensible Authentication Protocol) 구조를 채택하고 있습니다. EAP 방식에는 EAP-MD5(Message Digest 5), EAP-TLS(Transport Level Security), EAP-SRP(Secure Remote Password), EAP-TTLS(Tunneled TLS) 등이 있으며 V2824는 EAP-MD5와 EAP-TLS 방식을 지원합니다.

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 4-3 】 802.1x 사용자 인증 과정

다음은 V2824의 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
- 설정 예제

4.4.1 802.1x 기본 설정

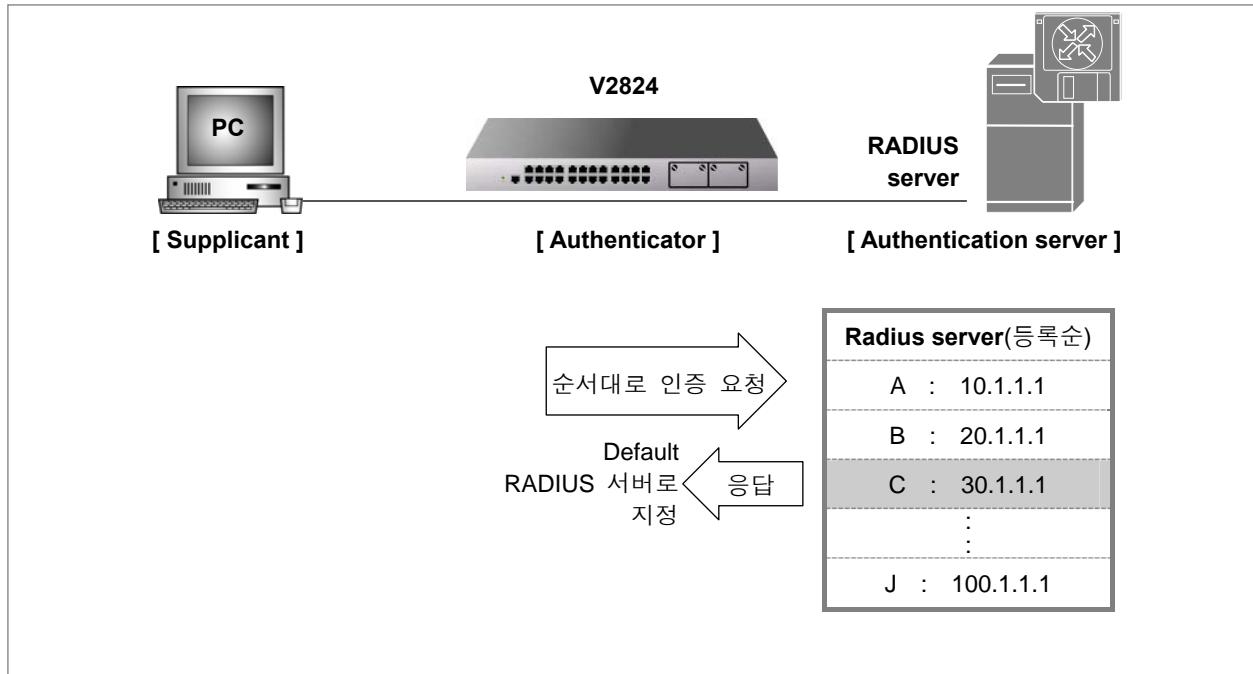
(1) 802.1x 활성화

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 4-4 】 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.

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 넣어야 합니다.

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.



V2824는 인증 서버가 되는 RADIUS 서버를 최대 5개 지정할 수 있습니다.



Key 값인 *value*로는 공백이나 특수 문자를 제외한 모든 문자를 사용할 수 있습니다.



인증에 사용되는 UDP 포트인 *auth-port-num*는 <0 – 65,535> 사이에서 설정 가능합니다.

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.

사용자는 다음 명령어로 등록된 RADIUS 서버들의 우선 순위를 지정할 수 있습니다.

명령어	모 드	기 능
dot1x radius-server move {srv-name srv-ip-address} priority priority	Global	등록된 서버들의 우선 순위를 지정합니다.



*priority*는 <1 - 5> 사이에서 지정 가능합니다.

(3) 인증 모드 설정

V2824의 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.



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

(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

V2824 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. V2824는 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.



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 횟수를 설정하려면, 다음 명령어를 사용하십시오.

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



V2824는 기본적으로 인증 요청을 3번 시도하도록 설정되어 있습니다.

(8) 인증 시도 주기 설정

Authenticator가 되는 장비에서 RADIUS 서버에 접속 인증을 요청한 후 아무런 응답이 없을 경우에는 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.



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



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

V2824의 dot1x에서는 인증 포트에 대해 주기적으로 인증 상태가 갱신될 수 있도록 설정할 수 있습니다. V2824의 스위치의 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 V2824 802.1x의 재인증을 활성화하십시오.

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

(2) 재인증 주기 설정

다음 명령어로 V2824 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

V2824의 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. V2824는 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

V2824 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

V2824에서는 다음 명령어로 포트의 802.1x 설정 내용을 초기화하여, 시스템에서 지정한 디플트 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

V2824의 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.



*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

V2824의 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	Enable/Global/ Bridge	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.

4.4.7 설정 예제

[설정 예제 1] 포트 기반 사용자 인증 설정

다음은 V1824의 4번 포트를 사용자 인증 포트로 설정하고 사용자 인증 포트의 IP 주소와 RADIUS 서버의 정보를 등록한 후 그 내용을 확인한 경우입니다.

```
SWTICH(config)# dot1x system-auth-control
SWTICH(config)# dot1x nas-port 4
SWTICH(config)# dot1x port-control force-authorized 4
SWTICH(config)# dot1x radius host 10.1.1.1 auth-port 4 key test
SWTICH(config)# show dot1x
802.1x authentication is enabled.
RADIUS Server TimeOut: 1(S)
RADIUS Server Retries: 3

RADIUS Server : 10.1.1.1 (Auth key : test)
-----
|       1       2       3       4
802.1x | 1234567890123456789012345678901234567890
-----
PortEnable | ...p.....
PortAuthed | ...u.....
MacEnable | .....
MacAuthed | .....
-----
p = port-based, m = mac-based, a = authenticated, u = unauthenticated
SWTICH(config)#

```

[설정 예제 2]

다음은 재인증 기간을 1800초로 설정하고, 인증 요청 재시도 간격을 1000초로 설정한 이후 활성화 시킨 예입니다.

```
SWTICH(config)# dot1x timeout quiet-period 1000 4
SWTICH(config)# dot1x timeout reauth-period 1800 4
SWTICH(config)# dot1x reauth-enable 4
SWTICH(config)# show dot1x 4
Port 4
    SystemAuthControl : Enabled
    ProtocolVersion   : 0
    PortControl       : Force-Authorized
    PortStatus        : Unauthorized
    ReauthEnabled     : True
    QuietPeriod       : 1000
    ReauthPeriod      : 1800
    TxPeriod          : 30
    PaeState          : INITIALIZE
SWTICH(config)#

```

[설정 예제 3]

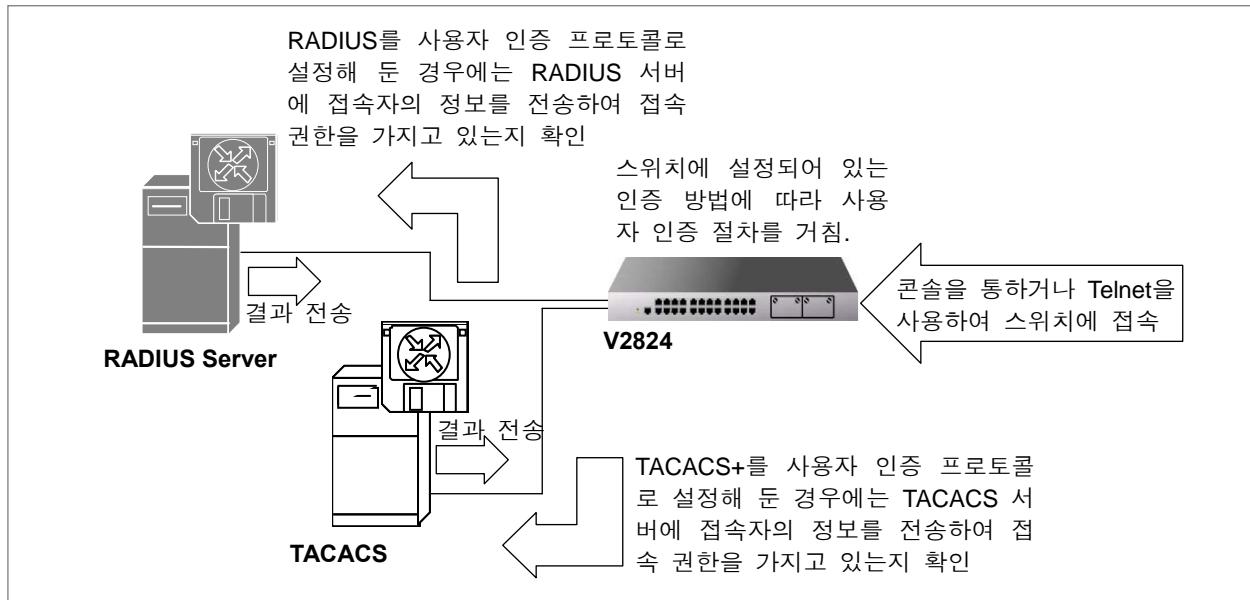
다음은 [설정 예제 1]에서 설정했던 포트 단위 사용자 인증 방식을 MAC 주소를 사용하는 방식으로 설정한 후 그 내용을 확인한 경우입니다.

```
SWTICH(config)# dot1x auth-mode mac-base 4
SWITCH(config)# show dot1x
802.1x authentication is enabled.
RADIUS Server TimeOut: 1(S)
RADIUS Server Retries: 3

RADIUS Server : 10.1.1.1 (Auth key : test)
-----
|           1           2           3           4
802.1x | 1234567890123456789012345678901234567890
-----
PortEnable | .....
PortAuthed | .....
MacEnable | ...m.....
MacAuthed | ...u.....
-----
p = port-based, m = mac-based, a = authenticated, u = unauthenticated
SWITCH(config)#

```

4.5 시스템 사용자 인증



【 그림 4-5 】 시스템 사용자 인증 과정

시스템 사용자 인증에 대한 보안이 한 단계 더 높아진 V2824는 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. V2824에 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 예제



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」 매뉴얼을 참고하십시오.

4.5.1 사용자 인증 방법 설정

V2824는 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} {enable disable}	Global	콘솔을 통해 접속하는 사용자의 인증 방법을 설정합니다.
login remote {radius tacacs host all} {enable disable}		원격 접속 사용자의 인증 방법을 설정합니다.



참 고

「**host**」는 장비에 등록되어 있는 사용자 ID와 패스워드를 이용한 접속 방법입니다. V2824는 기본적으로 이 방법을 사용하도록 설정되어 있습니다.



참 고

disable 옵션은 '**radius**' 나 '**tacacs**' 를 선택하는 경우에 기본값으로 설정되며, **enable** 옵션은 '**host**'를 선택하는 경우 기본값으로 설정됩니다.

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 V2824에서 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 거칠 지 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

V2824의 사용자 인증 방법은 기본적으로 「host → radius → tacacs」 의 순서로 설정되어 있습니다.

4.5.4 사용자 인증 방법 설정 내용 확인

V2824에 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/Bridge	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 add ip-address key	Global	사용자의 장비에서 사용하게 될 RADIUS 서버의 IP 주소와 Key 값을 등록합니다.
login radius server add ip-address key auth_port port-number acct_port port-number		인증 포트와 Accounting 포트도 함께 RADIUS 서버를 등록합니다.



참 고

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



참 고

V2824는 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

V2824는 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
login radius server move ip-address priority	Global	RADIUS 서버의 우선 순위를 설정합니다.



참 고

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
login radius retransmit count	Global	사용자 인증을 위해 정보를 재전송하는 횟수를 설정합니다.



재전송 시도 횟수는 1번부터 10번까지 설정할 수 있습니다.



V2824는 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

V2824는 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.



V2824는 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 add ip-address key	Global	사용자의 장비에서 사용하게 될 TACACS 서버의 IP 주소와 Key 값을 등록합니다.



V2824는 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 연결돼 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.

(2) TACACS 서버 우선 순위 설정

V2824는 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

V2824의 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.



V2824는 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

V2824는 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.



V2824는 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

V2824는 TACACS 서버의 권한 수준 설정에 따라 시스템 사용자의 권한 범위를 지정할 수 있습니다. 이 권한 설정은 V2824에서의 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.

시스템 사용자의 권한 수준을 설정하려면 다음 명령어를 사용하십시오. 권한 수준을 비교해보면 「**max > user > min**」 입니다.

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



V2824는 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

V2824는 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**」은 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 설정 예제

[설정 예제 1] RADIUS 서버 설정

다음은 V2824에 사용자 인증 방법을 설정하는 하나의 예입니다. 콘솔을 통해 접속하는 사용자와 원격으로 접속하는 사용자에 대한 모든 인증 방법으로 기본 방법에 RADIUS를 추가합니다. 그리고, 콘솔을 통해 접속하는 사용자에 대한 인증 방법은 RADIUS에 우선 순위를 두고, 원격으로 접속하는 사용자에 대한 인증 방법은 기본 방법에 두도록 설정합니다. 그리고, RADIUS 서버를 등록, 재전송 시도 횟수와 응답 시간 제한을 설정하는 하나의 예입니다.

```
SWITCH(config)# user add user test1
Changing password for user
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:vertex
Re-enter new password:vertex
Password changed.
SWITCH(config)# login local radius enable
SWITCH(config)# login remote radius enable
SWITCH(config)# login local radius primary
SWITCH(config)# login remote host primary
SWITCH(config)# login radius server add 100.1.1.1 1
SWITCH(config)# login radius retransmit 5
SWITCH(config)# login radius timeout 10
```

```
SWITCH(config)# show login
[AUTHEN]
Local login : radius host
Remote login : host radius ← 우선 순위에 따라 출력.
Accounting mode : both
-----
[HOST]
maximum_login_counts : 8

-----
[RADIUS]
<Radius Servers & Key>
100.1.1.1 1

Radius Retries : 5
Radius Timeout : 10
Radius Interface : default
-----
[TACACS]
<Tacacs Servers & Key>

Tacacs Timeout : 3
Tacacs Socket Port : 49
Tacacs Interface : default
Tacacs PPP Id : 1
Tacacs Authen Type : ASCII
Tacacs Priority Level : MIN
SWITCH(config)#

```

[설정 예제 2] TACACS+ 설정

다음은 사용자의 장비에서 사용하는 시스템 사용자 인증 방법을 TACACS+로 설정하는 경우의 예입니다.

```
SWITCH(config)# user add user test1
Changing password for user
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:vertex
Re-enter new password:vertex
Password changed.

SWITCH(config)# login local tacacs enable
SWITCH(config)# login remote tacacs enable
SWITCH(config)# login local tacacs primary
SWITCH(config)# login remote tacacs primary
SWITCH(config)# login tacacs server add 200.1.1.1 1
SWITCH(config)# login tacacs interface default
SWITCH(config)# login tacacs socket-port 1
SWITCH(config)# login tacacs auth-type pap
SWITCH(config)# login tacacs timeout 10
SWITCH(config)# login tacacs priority-level root
SWITCH(config)# show login
[AUTHEN]
Local login : tacacs host
Remote login : tacacs host
Accounting mode : both
-----
[HOST]
maximum_login_counts : 8

-----
[RADIUS]
<Radius Servers & Key>

Radius Retries : 3
Radius Timeout : 3
Radius Interface : default
-----
[TACACS]
<Tacacs Servers & Key>
200.1.1.1 1

Tacacs Timeout : 10
Tacacs Socket Port : 1
Tacacs Interface : default
Tacacs PPP Id : 1
Tacacs Authen Type : PAP
Tacacs Priority Level : MAX(ROOT)
SWITCH(config)#

```

← 우선 순위에 따라 출력.

5. 포트 기본 설정

사용자는 V2824 포트의 Auto-negotiate, 전송 속도, Flow-control 등의 기본 환경을 설정할 수 있습니다. 포트 설정을 위해서는 Global 설정 모드에서 bridge 명령어를 입력, Bridge 설정 모드로 들어가야 합니다. Bridge 설정 모드로 들어가면 다음과 같이 시스템 프롬프트가 SWITCH(config)#에서 SWITCH(bridge)#로 바뀝니다.

```
SWITCH(config)# bridge
SWITCH(bridge)#{
```

다음은 V2824의 이더넷 포트에 기본적으로 설정되어 있는 내용입니다.

【 표 5-1 】 이더넷 포트의 기본 설정

내 용	기 본 설 정
포트상태	동작 가능
Auto-negotiate	ON(100BASE-FX 제외)
Duplex mode	Full Duplex Mode
플로우 컨트롤	Off
VLAN	Default VLAN
STP	Defualt VLAN에 대해 설정

한편, 사용자 스위치 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.



*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.

포트의 기본 환경을 설정하는 명령어에서 *port-number*에 임의의 문자를 입력하면 **%Wrong expression.** ex) 'show port 1,3' , 'show port 1-3,10'라는 메시지가 출력되고 잘못된 숫자를 입력하면 **%Port number invalid**라는 메시지가 출력됩니다.

```
SWITCH(bridge)# show port port
%Invalid port: port
SWITCH(bridge)# show port 100
%Invalid range: 100 [1-40]
SWITCH(bridge)#{
```

포트 기본 환경 설정과 관련하여 다음과 같은 내용을 설명합니다.

- 논리적 포트 활성화 설정
- Auto Nego 설정
- 전송 속도 설정
- Duplex 모드 설정
- Flow Control 설정
- 오류! 참조 원본을 찾을 수 없습니다.
- 포트 설명하기
- 포트 통계 확인 및 초기화
- 포트 미러링 설정

5.1 논리적 포트 활성화 설정

케이블이 연결되어 물리적으로는 활성화 상태인 포트를 논리적으로 비활성화 상태로 만들 수 있습니다. V2824의 모든 포트는 기본적으로 활성화 되어 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 활성화합니다.
port disable port-number		포트를 비활성화합니다.

주 의

V2824는 운용 도중에 업링크 포트 모듈을 교체할 경우, 반드시 먼저 포트를 비활성화 시켜야만 합니다. 포트가 물리적으로 활성화 되어있을 경우에는 논리적으로 비활성화해야 합니다. 상기 동작 미 시행후 다른 포트 모듈로 교체시 시스템이 오작동 할 가능성이 있음을 주의하시기 바랍니다.

다음은 활성화 상태인 포트 1번을 물리적으로 비활성화 시킨 후 그 내용을 확인한 경우입니다.

```
SWITCH(bridge)# show port 1
-----
NO      TYPE      PVID      STATUS      MODE      FLOWCTRL  INSTALLED
          (ADMIN/OPER)
-----
1: Ethernet    1  Up/Up     Auto/Full/100   Off       Y
SWITCH(bridge)# port disable 1
SWITCH(bridge)# show port 1
-----
NO      TYPE      PVID      STATUS      MODE      FLOWCTRL  INSTALLED
          (ADMIN/OPER)
-----
1: Ethernet    1  Down/Down  Auto/Full/100   Off       Y
SWITCH(bridge)#

```

5.2 Auto Nego 설정

사용자는 V2824의 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.

1000BASE-X 기가비트 포트인 경우에는, 광모듈이 설치되어 있어야 활성화 상태로 설정됩니다.

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

참 고

V2824의 포트는 기본적으로 Auto Nego가 활성화 상태로 설정되어 있습니다.

주 의

V2824는 Auto Nego가 설정된 상태에서도 전송 속도나 Duplex 모드를 변경하여 연결된 장비의 전송 속도나 Duplex 모드를 조절하는 기준을 임의로 정할 수 있습니다.

주 의

100BASE-FX 포트는 Auto Nego에 대한 설정이 불가능합니다.

주 의

Auto Nego 기능이 **on**으로 설정되지 않은 포트는 Auto MDIX를 지원하지 않습니다.

V2824는 Auto Nego가 설정된 상태에서도 전송 속도나 Duplex 모드를 변경하여 연결된 장비의 전송 속도나 Duplex 모드를 조절하는 기준을 임의로 정할 수 있습니다.

예를 들면, Auto Nego가 설정된 상태에서 전송 속도를 10Mbps로 설정하면, 10Mbps/Full Duplex를 기준으로 Auto Nego가 성립됩니다.

5.3 전송 속도 설정

V2824는 각 포트의 전송 속도를 설정할 수 있습니다. V2824 포트의 전송 속도를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port speed port-number {10 100 1000}	Bridge	포트의 전송 속도를 설정합니다.

다음은 1번 포트의 전송 속도를 10Mbps로 설정하고 확인하는 경우입니다.

```
SWITCH(bridge)# show port 1
-----
NO      TYPE      PVID      STATUS      MODE      FLOWCTRL  INSTALLED
                           (ADMIN/OPER)
-----
1: Ethernet      1      Up/Up     Auto/Full/100   Off       Y
SWITCH(bridge)# port speed 1 10
SWITCH(bridge)# show port 1
-----
NO      TYPE      PVID      STATUS      MODE      FLOWCTRL  INSTALLED
                           (ADMIN/OPER)
-----
1: Ethernet      1      Up/Down   Auto/Full/10   Off       Y
SWITCH(bridge)#

```



주의

1000BASE-X의 Gigabit 포트에는 전송 속도를 설정할 수 없습니다.

5.4 Duplex 모드 설정

V2824는 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. 링크가 연결되기 전 V2824의 포트는 기본적으로 **half**로 설정되어 있습니다.

포트의 Duplex 모드를 설정하시려면, 다음 명령어를 사용하십시오.

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

다음은 1번 포트의 Duplex 모드를 half로 설정하고, 확인하는 경우입니다.

```
SWITCH(bridge)# show port 1
-----
NO      TYPE      PVID      STATUS      MODE      FLOWCTRL  INSTALLED
                  (ADMIN/OPER)
-----
1: Ethernet      1      Up/Up     Force/Full/100    Off       Y
SWITCH(bridge)# port duplex 1 half
SWITCH(bridge)# show port 1
-----
NO      TYPE      PVID      STATUS      MODE      FLOWCTRL  INSTALLED
                  (ADMIN/OPER)
-----
1: Ethernet      1      Up/Down   Force/Half/100   Off       Y
SWITCH(bridge)#

```



주의

100BASE-FX 이더넷과 1000BASE-X 이더넷은 Full Duplex만 가능합니다. 사용자는 두 전송 속도가 설정된 포트의 Duplex 모드를 변경할 수 없습니다.

5.5 Flow Control 설정

V2824의 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

V2824의 포트는 기본적으로 Flow Control이 **off**로 설정되어 있습니다.

다음은 4번 포트에 전송 중지 기능을 off로 설정하고 이를 확인하는 경우입니다.

```
SWITCH(bridge)# port flow-control 4 on
SWITCH(bridge)# show port 4
-----
NO      TYPE      PVID      STATUS      MODE      FLOWCTRL  INSTALLED
                  (ADMIN/OPER)
-----
4:  Ethernet    4     Up/Down  Auto/Half/0    On       Y
SWITCH(bridge)#

```

5.6 포트 설명하기

V2824는 각 포트에 대한 설명을 등록하여 사용자가 관리하기 편리하게 하였습니다. 각 포트에 대한 설명을 등록하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port description <i>port-number description</i>	Bridge	포트에 대한 설명을 입력합니다.

포트에 등록한 설명을 삭제하려면 다음 명령어를 사용하십시오.

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

각 포트에 등록된 설명을 보려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show port description [<i>port-number</i>]	Enable / Global / Bridge	포트에 등록된 설명을 확인합니다.

다음은 11번, 12번 포트에 설명을 등록하고, 그 내용을 확인한 경우입니다.

```
SWITCH(bridge)# port description 11 test1
SWITCH(bridge)# port description 12 test2
SWITCH(bridge)# show port description 22-23
-----
NO  TYPE      STATE     LINK      DESCRIPTION
      (ADM/OPR)
-----
11  Ethernet   Up/Down   100FDX   test1
12  Ethernet   Up/Down   100FDX   test2
SWITCH(bridge)#
-----
```

5.7 포트 통계 확인 및 초기화

V2824의 사용자는 각 포트의 평균적인 트래픽이나 SNMP MIB에 정의된 interface MIB, RMON MIB 데이터를 확인할 수 있습니다.

다음은 각 포트의 평균 트래픽, SNMP MIB에 정의된 interface MIB, RMON MIB 데이터를 확인할 때 사용하는 명령어입니다.

명령어	모 드	기 능
show port statistics avg-pkt [port-number]		포트의 평균 트래픽을 확인합니다.
show port statistics avg-pps [port-number]	Enable / Global /	포트의 Unicast/ Multicast/ Broadcast 트래픽의 평균 수치를 확인합니다.
show port statistics interface [port-number]	Bridge	포트의 인터페이스 MIB 데이터를 확인합니다.
show port statistics rmon [port-number]		포트의 RMON MIB 데이터를 확인합니다.

포트에 기록된 통계를 지우고 초기화하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear port statistics {port-number all}	Enable/Global/Bridge	포트 통계를 초기화합니다.

다음은 1번 포트의 평균 트래픽을 확인하는 경우입니다.

```
SWITCH(bridge)# show port statistics avg-pkt 1
=====
Port | Tx | Rx
-----
Time | pkts/s | bytes/s | bits/s | pkts/s | bytes/s | bits/s
-----
port 1 -----
5 sec: 0 0 0 11 1106 8,848
1 min: 0 1 8 1 155 1,240
10 min: 0 0 0 0 15 120
SWITCH(bridge)#

```

다음은 1번 포트의 인터페이스 MIB 정보를 확인하는 경우입니다.

```
SWITCH(bridge)# show port statistics interface 1
Port 1
ifDescr          port1-TX-10/100
iftType          6
ifMtu           1500
ifSpeed          100Mbps
ifPhysAddress   00:d0:cb:0a:a4:6d
ifAdminStatus    UP
ifOperStatus     UP
ifLastChange    1653719
ifInOctets      501879
ifInUcastPkts   296
ifInNUcastPkts  4790
ifInDiscards     0
ifInErrors       0
ifInUnknownProtos 0
ifOutOctets     256
ifOutUcastPkts  2
ifOutNUcastPkts 2
ifOutDiscards   0
ifOutErrors     0
ifOutQLen       100
ifSpecific      0
SWITCH(bridge)#

```

다음은 1번 포트의 RMON MIB 정보를 확인하는 경우입니다.

```
SWITCH(bridge)# show port statistics rmon 1
Port 1    ethernet
etherStatsDropEvents      0
etherStatsOctets          573280
etherStatsPkts            5774
etherStatsBroadcastPkts   4634
etherStatsMulticastPkts   784
etherStatsCRCAlignErrors  0
etherStatsUndersizePkts   0
etherStatsOversizePkts    0
etherStatsFragments       0
etherStatsJabbers         0
etherStatsCollisions      0
etherStatsPkts64Octets    3343
etherStatsPkts65to127Octets 1559
etherStatsPkts128to255Octets 805
etherStatsPkts256to511Octets 57
etherStatsPkts512to1023Octets 10
etherStatsPkts1024to1518Octets 0
SWITCH(bridge)#

```

5.8 포트 상태 확인

포트 상태를 확인하려면, 다음 명령어를 사용하십시오.

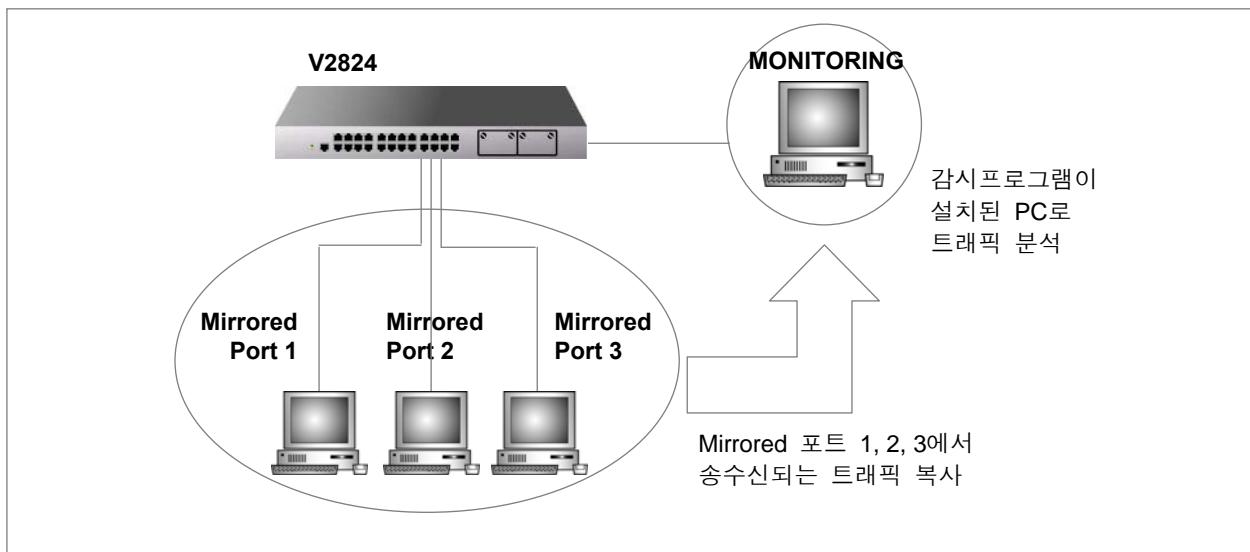
명령어	모 드	기 능
show port status [port-number]	Enable / Global / Bridge	포트 상태를 확인합니다.

5.9 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 포트라고 하고, 모니터링 대상이 되는 포트를 Mirrored 포트라고 합니다.

포트 미러링의 원리는 Mirrored 포트에서 전송이 이루어지는 패킷을 Monitor 포트로 복사, 모니터링 할 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 PC를 연결하여 스위치의 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.

5.9.1 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 Bridge 설정 모드에서 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.

예) SWITCH(bridge)# **mirror add 1,2,3** or SWITCH(bridge)# **mirror add 1-3**



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.

5.9.2 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 삭제(del)하거나, Mirroring 포트를 disable 해주는 것을 권장합니다. Mirroring 기능을 장시간 사용하면 CPU에 부담을 주기 때문에, 장비의 패킷 처리 속도가 늦어질 수 있습니다.

5.9.3 포트 미러링 설정 내용 확인

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

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

5.9.4 설정 예제

[설정 예제 1] 포트를 통한 모니터링 설정

다음은 1번 포트에서 2,3,4,5번 포트를 모니터링하도록 설정하는 경우입니다.

1 단계 사용자의 장비에서 Monitor 포트로 사용할 1번 포트에 감시 프로그램이 설치되어 있는 PC를 연결합니다.

2 단계 다음과 같이 1번 포트를 Monitor 포트로 설정하고, 2,3,4,5번 포트를 Mirroring 포트를 설정합니다.

```
SWITCH(bridge)# mirror monitor 1
SWITCH(bridge)# mirror add 2-5
SWITCH(bridge)#{/pre}
```

3 단계 미러링 기능을 활성화하십시오.

```
SWITCH(bridge)# mirror enable
SWITCH(bridge)#{/pre}
```

4 단계 포트 미러링을 설정한 것을 확인합니다.

```
SWITCH(bridge)# show mirror
Mirroring enabled
Monitor port = 1
Ingress mirrored ports
-- 02 03 04 05 --
Egress mirrored ports
-- 02 03 04 05 --
SWITCH(bridge)#{/pre}
```

[설정 예제 2] CPU를 통한 모니터링 설정

다음은 장비의 CPU에서 2,3,4,5번 포트를 모니터링하도록 설정하는 경우입니다.

```
SWITCH(bridge)# mirror monitor cpu
SWITCH(bridge)# mirror add 2-5
SWITCH(bridge)# mirror enable
SWITCH(bridge)# show mirror
Mirroring enabled
Monitor port = cpu
Ingress mirrored ports
-- 02 03 04 05 --
Egress mirrored ports
-- 02 03 04 05 --
SWITCH(bridge)#{/pre}
```

6. 시스템 환경

시스템 환경에서는 시스템의 호스트 네임, 시간 등을 설정하는 방법과 설정 내용을 관리하는 방법 등에 대해 설명합니다. 이 장은 다음과 같은 내용으로 이루어집니다.

- 환경 설정
- 설정 관리
- 시스템 확인

6.1 환경 설정

V2824의 시스템 환경 설정에 대해 다음과 같은 내용을 설명합니다.

- 호스트 네임 설정
- 날짜 및 시간 설정
- Time-zone 설정
- NTP 설정
- NTP 메시지 주소 설정
- SNTP 설정
- 터미널 스크린 출력 상태 설정
- DNS 서버 설정
- 로그인 배너 설정
- Fan 동작 설정
- 데몬 강제 종료
- 소프트웨어 Watchdog 설정
- MAC Learning 모드 설정
- FTP 서버 활성화
- FTP 클라이언트 주소 설정

6.1.1 호스트 네임 설정

프롬프트 상태에서 출력되는 호스트 네임은 네트워크에 연결된 각 장비를 서로 구분하기 위해 필요합니다. 스위치의 호스트 네임을 설정하거나 변경하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
hostname name	Global	Host Name을 설정합니다.
show running-config include hostname		Host Name을 확인합니다.



참 고

*name*은 사용자가 부여하는 스위치의 새로운 이름입니다. 이 이름은 대, 소문자를 구분합니다.



참 고

공장에서 출하된 V2824에는 호스트 네임이 기본적으로 **SWITCH**로 설정되어 있습니다.

다음은 호스트 이름을 DASAN으로 변경하는 예입니다.

```
SWITCH(config)# hostname DASAN
DASAN(config)#{
```

6.1.2 날짜 및 시간 설정

V2824는 스위치에 현재 시각과 날짜를 설정하거나 변경할 수 있습니다. 스위치의 시각과 날짜를 변경하려면 다음 명령어를 사용하십시오.

날짜 및 시간 입력하는 형식은 자유롭게 입력할 수 있습니다. 예를 들면, 「17:25 Mar 15 2001」, 「15 Mar 2001 5:25pm」 등이 있습니다.

명령어	모 드	기 능
clock datetime	Enable	사용자 스위치에 현재 시간과 날짜를 설정, 변경합니다.
show clock		사용자 스위치에 설정된 현재 시간과 날짜를 확인합니다.

다음은 2007년 3월 23일 오후 1시 50분이라는 시각을 설정하는 예입니다.

```
SWITCH# clock 23 Mar 2007 1:50 pm
SWITCH# show clock
Thu, 23 Mar 2006 13:50:02 +0000
SWITCH#
```

6.1.3 Time-zone 설정

사용자는 스위치에 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	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.

【 표 6-1 】 GMT 시각

Time-zone	국 가	Time-zone	국 가	Time-zone	국 가
GMT-12	에니워톡	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, 달라스	GMT+3	모스크바	GMT+12	웰링턴
GMT-5	뉴욕, 마이애미	GMT+4	테헤란		
GMT-4	조지타운	GMT+5	뉴델리		

V2824에 Time-zone을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
time-zone time-zone	Global	스위치에 Time-zone을 설정합니다.
show clock		스위치의 Time-zone을 확인합니다.



참 고

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



주 의

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

설정한 Time-zone을 삭제하고 기본 설정으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear time-zone	Global	설정한 Time-zone을 삭제하고 기본 설정으로 되돌립니다.

다음은 서울의 Time-zone에서 일시를 2006년 3월 23일 오후 1시 50분으로 설정하고, 그 내용을 확인하는 경우입니다.

```
SWITCH(config)# time-zone GMT+9
SWITCH(config)# exit
SWITCH# clock 23 Mar 2006 1:50 pm
SWITCH# show clock
Thu, 23 Mar 2006 13:50:02 GMT+0900
SWITCH#
```

6.1.4 NTP 설정

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

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

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

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



NTP 서버는 최대 3개까지 등록할 수 있습니다.

NTP 기능을 해제하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ntp server 1 [server 2] [server 3]	Global	사용자 스위치에서 NTP 기능을 해제합니다.

NTP에 대한 설정을 확인하려면 다음 명령어를 사용하십시오.

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

[설정 예제 1]

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)# ntp start
SWITCH(config)# show ntp
ntp started
ntp server 203.255.112.96
SWITCH(config)#{
```

[설정 예제 2]

다음은 NTP 기능을 해제하고, 해제 여부를 확인하는 경우입니다.

```
SWITCH(config)# no ntp
SWITCH(config)# show ntp
ntp stoped
SWITCH(config)#{/pre}
```

6.1.5 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 맞춰 지게 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.

6.1.6 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.

V2824에 SNTP를 설정하려면, 다음 명령어를 사용하십시오.

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



V2824는 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.

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

6.1.7 터미널 스크린 출력 상태 설정

V2824는 기본적으로 콘솔 터미널 화면에 80자로 이루어진 행을 24개 출력합니다. 사용자는 출력되는 행 수를 변경할 수 있습니다.

터미널 스크린에 출력할 행 수를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
terminal length <0 - 512>	Enable	터미널 스크린 출력 행 수를 설정합니다.



디폴트 스크린 출력 행 수는 24줄입니다.



참 고

스크린 출력 행 수를 0으로 설정하는 경우에는 사용자가 원하는 모든 정보가 한 번에 보여집니다.

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 <0 - 512>	Enable	터미널 스크린 출력 행 수를 설정을 해제합니다.

6.1.8 DNS 서버 설정

V2824는 telnet, ftp, tftp, ping 명령어를 사용할 때 IP 주소를 입력하는 대신 호스트 네임이나 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 스위치에 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 호스트 네임이나 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	View / Enable / Global	사용자 스위치에 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

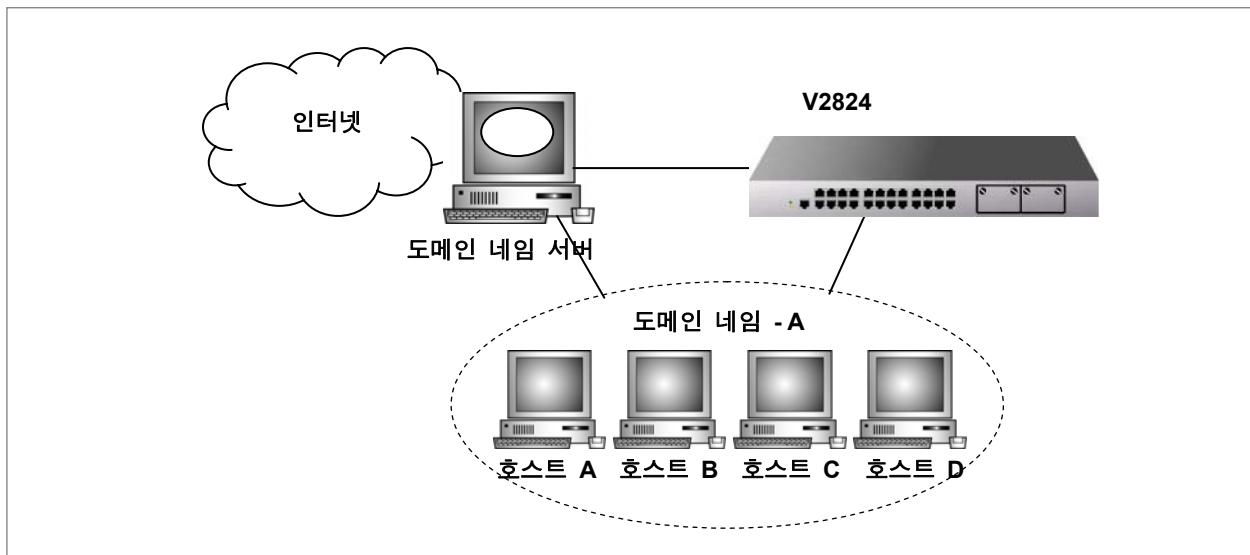
위에서 등록한 DNS 서버는 예시를 보여주기 위해 입력한 것이며 실제로는 사용자가 사용하게 될 DNS 서버를 등록하셔야 합니다.

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, V2824는 특정 도메인 네임을 등록하면 해당하는 도메인 내부에 있는 호스트의 경우에는 IP 주소를 입력하지 않고 호스트 네임을 입력하고도 telnet, ftp, tftp, ping 명령어를 실행할 수 있습니다.



【 그림 6-1 】 도메인 네임 서버

위의 그림으로 예를 들면 V2824에 도메인 네임 “A”를 등록해 두면 A의 내부에 있는 호스트 A, B, C, D를 대상으로 telnet, ftp, tftp, ping 명령어를 실행할 때, IP 주소 대신에 호스트 네임을 입력할 수 있습니다.

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

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



주의

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

다음은 위의 그림의 도메인 “A”를 등록하고 호스트 “B”에 Ping 테스트를 실행할 때 IP 주소 대신 호스트 네임을 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 도메인 네임, B에는 호스트 네임이 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

V2824는 시스템 로그인 화면에 여러 가지 메시지를 등록하여 콘솔 터미널 프로그램을 통하여거나 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		시스템에 로그인 되기 전에 출력되는 메시지를 등록합니다.
banner login	Global	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		시스템에 로그인 되기 전에 출력되는 메시지를 삭제합니다.
no banner login	Global	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 1]

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
V1824 Switch.
Dasan Networks Inc.SWITCH(config)#

```

메시지를 입력하고 Ctrl-D를 누르면 시스템 프롬프트로 돌아갑니다.

위와 같이 입력하면 로그인할 때 다음과 같이 배너가 생깁니다.

```
V1824 Switch.
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 >
V1824 Switch
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 4.82      *
*          DASAN Networks Inc.           *
*                               *
*****
```

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

Load Address: 0x83000000
Image Size: 0x00b31b80
Start Address: 0x83000000

NOS version 3.13 #4450
CPU : BCM5836 at 264 MHz
(종략)

V1824 Switch
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

V2824는 FAN 동작을 설정할 수 있습니다. FAN 동작을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
fan operation {auto on off}	Global	FAN 동작을 설정합니다.



Fan 동작이 'auto' 모드로 설정된 경우에는 스위치 Fan에 설정된 threshold fan 온도의 변화에 따라 동작하게 됩니다.

6.1.11 데몬 강제 종료

V2824는 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.

6.1.12 MAC Learning 모드 설정

V2824는 CML(CPU-based Learning)과 SML(Switching Fabric-based Learning)의 2가지 MAC Learning 모드를 지원합니다. 사용자는 필요에 따라 사용할 MAC Learning 모드를 설정할 수 있습니다.

다음 표는 CML 모드와 SML 모드의 성능을 비교한 것입니다.

【 표 6-2 】 CML 모드와 SML 모드의 성능 비교

기능	CML	SML
MAC Learning 속도	느림	빠름
CPU Load	많음	적음
Chip calling 간격	패킷 수에 따라 변동	주기적
CPU Interconnection	정확	지연
보안 정책	정확	지연

시스템에 MAC Learning 모드를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
mac-learning mode {cml sml}	Bridge	시스템에 MAC Learning 모드를 설정합니다.



MAC Learning 모드는 기본적으로 **sml** 모드로 설정되어 있습니다.

6.1.13 소프트웨어 Watchdog 설정

Watchdog이란 시스템에 문제가 발생하였을 때 자동적으로 장비를 리부팅하는 기능입니다. V2824는 Watchdog 기능을 소프트웨어에 적용시켰습니다. 소프트웨어 Watchdog는 일정한 시간 간격으로 데몬을 감시하고, 제한 횟수만큼 Fail 발생이 나타나면 사용자의 설정대로 시스템이 대응하게 됩니다.

사용자가 설정할 수 있는 시스템 대응 방법에는 3가지가 있습니다.

- **none** : 아무런 동작을 하지 않습니다.
- **daemon-restart** : 데몬을 Restart 합니다.
- **system-reboot** : 시스템을 재부팅합니다. 이 때, 현재 설정을 저장하도록 설정할 수도 있습니다.

IMI 데몬에 소프트웨어 Watchdog를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
sw-watchdog deamon-monitoring <10-86400> <1-10> daemon-restart		IMI 데몬을 감시하는 시간간격과 Fail 발생 제한횟수를 설정하고, 제한횟수 이상으로 Fail이 발생하였을 때 데몬을 Restart 하도록 설정합니다.
sw-watchdog deamon-monitoring <10-86400> <1-10> none	Global	IMI 데몬을 감시하는 시간간격과 Fail 발생 제한횟수를 설정하고, 제한횟수 이상으로 Fail이 발생하였을 때 아무 동작 하지 않도록 설정합니다.
sw-watchdog deamon-monitoring <10-86400> <1-10> system-reboot		IMI 데몬을 감시하는 시간간격과 Fail 발생 제한횟수를 설정하고, 제한횟수 이상으로 Fail이 발생하였을 때 시스템을 재부팅하도록 설정합니다.
sw-watchdog deamon-monitoring <10-86400> <1-10> system-reboot save-config		제한횟수 이상으로 Fail이 발생하였을 때 현재 설정을 저장하면서 시스템을 재부팅하도록 설정합니다.

INET 데몬에 소프트웨어 Watchdog를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
sw-watchdog inet-monitoring <10-86400> <1-10> daemon-restart		INET 데몬을 감시하는 시간간격과 Fail 발생 제한횟수를 설정하고, 제한횟수 이상으로 Fail이 발생하였을 때 데몬을 Restart 하도록 설정합니다.
sw-watchdog inet-monitoring <10-86400> <1-10> none	Global	INET 데몬을 감시하는 시간간격과 Fail 발생 제한횟수를 설정하고, 제한횟수 이상으로 Fail이 발생하였을 때 아무 동작 하지 않도록 설정합니다.
sw-watchdog inet-monitoring <10-86400> <1-10> system-reboot		INET 데몬을 감시하는 시간간격과 Fail 발생 제한횟수를 설정하고, 제한횟수 이상으로 Fail이 발생하였을 때 시스템을 재부팅하도록 설정합니다.
sw-watchdog inet-monitoring <10-86400> <1-10> system-reboot save-config		제한횟수 이상으로 Fail이 발생하였을 때 현재 설정을 저장하면서 시스템을 재부팅하도록 설정합니다.

소프트웨어 Watchdog 설정을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no sw-watchdog		소프트웨어 Watchdog 기능을 비활성화합니다.
no sw-watchdog daemon-monitoring	Global	IMI 데몬에 설정한 소프트웨어 Watchdog 기능을 해제합니다.
no sw-watchdog inet-monitoring		INET 데몬에 설정한 소프트웨어 Watchdog 기능을 해제합니다.

소프트웨어 Watchdog 기능의 설정 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show sw-watchdog	Enable/Global	소프트웨어 Watchdog 기능의 설정 내용을 확인합니다.

[설정 예제 1]

다음은 IMID 데몬을 10초마다 감시하고 연속적으로 5번 이상 Fail 상태가 발생하면 현재의 설정 내용을 저장하면서 시스템을 재부팅하도록 설정하는 경우입니다.

```
SWITCH(config)# sw-watchdog daemon-monitoring 10 5 system-reboot save-config
SWITCH(config)# show sw-watchdog
-----
Type | Interval(sec) | err_cnt/threshold | control action
-----
daemon-monitoring      10          0/5          system-reboot save-config
inet-monitoring        10          0/2          daemon-restart
SWITCH(config)#

```

한편, 현재의 설정 내용을 저장하도록 설정한 경우에는 소프트웨어 Watchdog 기능에 의해 시스템이 재부팅된 후에 다음 예제와 같이 Boot 정보와 저장된 설정 파일을 확인할 수 있습니다.

```
SWITCH# show boot-info
-----
Type           Date           Time
-----
SW_WATCHDOG    2000/01/01    00:49:53
-----  

SWITCH#
SWITCH# show config-list
=====
CONFIG-LIST
=====
sw_watchdog_abnormal
-----  

SWITCH#
```

6.1.14 FTP 서버 활성화

V2824는 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.

V2824에 FTP 서버로서의 기능을 활성화하거나 해제하려면, 다음 명령어를 사용하십시오.

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



V2824는 기본적으로 FTP 서버가 활성화되어 있습니다.

다음은 FTP 서버로서의 기능을 해제하고 설정을 확인한 경우입니다.

```
SWITCH(config)# ftp server disable
SWITCH(config)# show running-config
!
hostname SWITCH
!
dns server 10.7.1.16
!
ftp server disable
!
syslog output info local volatile
syslog output info local non-volatile
!
no ip route compaction
ospf restart helper only-reload
ip ecmp-hash sip
service dhcp
!
bridge

(중략)

SWTICH(config)#

```

6.1.15 FTP 클라이언트 주소 설정

V2824는 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.

6.2 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

V2824는 스위치에 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 arp bridge dns full hostname login qos rmon-alarm rmon-event rmon-history flow policer policy snmp syslog time-out time-zone}	All	특정한 설정에 대한 내용만 보여줍니다.



View 모드에서는 **show running-config** 명령어만 사용 가능합니다.

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 스위치를 설정하거나 설정한 내용을 변경했을 때, 사용자는 반드시 플래시 메모리에 설정, 또는 변경된 내용을 저장해야 합니다. 만일 저장하지 않으면 스위치의 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.

주 의

View 모드에서는 지원되지 않는 명령어입니다.

다음은 설정한 내용을 저장하는 경우의 예입니다.

```
SWITCH# write memory
Building configuration...
[OK]
SWITCH#
```

주 의

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

6.2.3 설정 내용 자동 저장

V2824는 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 interval	Global	설정 내용 자동 저장 간격을 설정합니다.
no write interval		설정 내용 자동 저장 기능을 해제합니다.
show running-config include write	Enable / Global	설정 내용 자동 저장 간격을 확인합니다.

참 고

*Interval*은 분 단위로 <10 – 1, 440> 사이에서 10분 단위로 설정 가능합니다.

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 Global 설정 모드에서 다음의 명령어를 사용하십시오.

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



주의

restore factory-defaults 명령어를 사용하여 설정 내용을 초기화한 후에 반드시 스위치를 재부팅하십시오. 재부팅하지 않으면 초기화 되지 않습니다.

다음은 스위치의 설정 내용을 초기화 한 경우입니다.

```
SWITCH(config)# restore factory-defaults
You have to restart the system to apply the changes
SWITCH(config)#{
```

6.2.5 설정 내용 Backup 하기

V2824는 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, V2824는 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 Global 설정 모드에서 다음의 명령어를 사용하십시오. 변수인 “name”은 Backup하는 내용의 일종의 파일명으로 사용자가 편리한 이름으로 설정할 수 있습니다.

명령어	모 드	기 능
copy running-config {file-name startup-config}	Enable	현재 설정내용을 사용자가 지정한 파일명으로 Backup하거나 Startup의 설정 내용으로 Backup합니다.
copy startup-config file-name		Startup의 설정내용을 Backup합니다.
copy file-name1 file-name2		이미 Backup된 file-name1을 file-name2로 다시 Backup합니다.

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

명령어	모 드	기 능
copy {ftp tftp} config upload {file-name startup-config}	Enable	이미 Backup된 file-name을 원격지의 FTP 또는 TFTP 서버로 업로드하거나 Startup의 설정내용으로 업로드 합니다.
copy {ftp tftp} config download {file-name startup-config}		이미 Backup된 file-name을 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.



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.

사용자가 Backup해 둔 내용을 불러 내어 사용하려면 Global 설정 모드에서 다음의 명령어를 사용하십시오.

명령어	모 드	기 능
copy file-name startup-config	Enable	file-name이라는 이름으로 Backup된 내용을 startup-config에서 사용하기 위해 불러냅니다.



주 의

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

(2) SSH를 이용하여 데이터 Backup 하기

클라이언트가 된 V2824는 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
copy {scp sftp} config {download upload} config-file	Enable	SSH를 이용하여 데이터를 업로드 또는 다운로드 합니다.
copy {scp sftp} key upload key-file		SSH를 이용하여 인증키를 가지고 있는 데이터를 업로드합니다.

(3) Backup 파일 확인

Startup config를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show startup-config	Enable / Global / Bridge	Startup config를 확인합니다.

Backup한 파일을 확인하려면 다음 명령어를 사용하십시오.

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

다음은 V2824에서 현재 설정 내용을 “V2824”라는 파일명으로 Backup한 후 Backup 파일 리스트를 확인한 경우입니다.

```
SWITCH# copy running-config V2824
[OK]
SWITCH# show config-list
=====
CONFIG-LIST
=====
V2824
SWITCH#
```

(4) Backup 파일 삭제

Backup한 파일을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
erase config config-file-name	Enable	Backup된 설정 파일을 삭제합니다.
erase key key-file-name		Backup된 SSH Key 파일을 삭제합니다.

6.3 시스템 확인

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

V2824는 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 확인 및 삭제
- Aging Time 설정
- 장비 사용 시간 확인
- 시스템 구성 정보 확인
- CPU 사용량 확인
- CPU 프로세스 확인
- CPU 처리 패킷 제한
- CPU 통계 확인
- 메모리 사용 정보 확인
- 시스템 이미지 확인
- 시스템 이미지 버전 확인
- 시스템 이미지 파일 크기 확인
- Default OS 설정
- 시스템 상태 확인
- Tech-support 확인
- 프로토콜 통계 확인
- 부팅 정보 확인
- 케이블 길이 확인
- G-PON 모듈 정보 확인

6.3.1 네트워크 연결 상태 확인

사용자의 스위치가 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. 수신자에게 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.

【 표 6-3 】 Ping 테스트 실행을 위한 기본 설정

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.

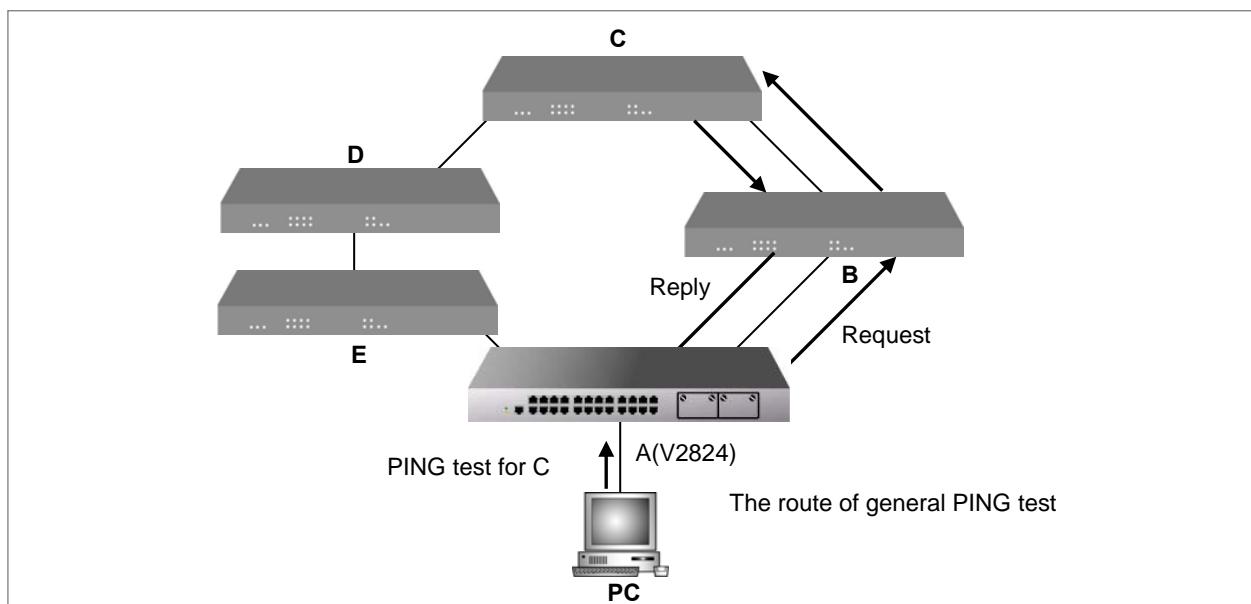
[설정 예제 1]

IP 주소 192.168.1.10과의 네트워크 상태를 확인하기 위해 Ping 테스트 3번 실시한 경우입니다.

```
SWITCH# ping
Protocol [ip]: ip
Target IP address: 172.16.1.254
Repeat count [3]: 3
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
--- 172.16.1.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 8008ms
rtt min/avg/max/mdev = 0.058/0.581/1.632/0.542 ms
SWITCH#
```

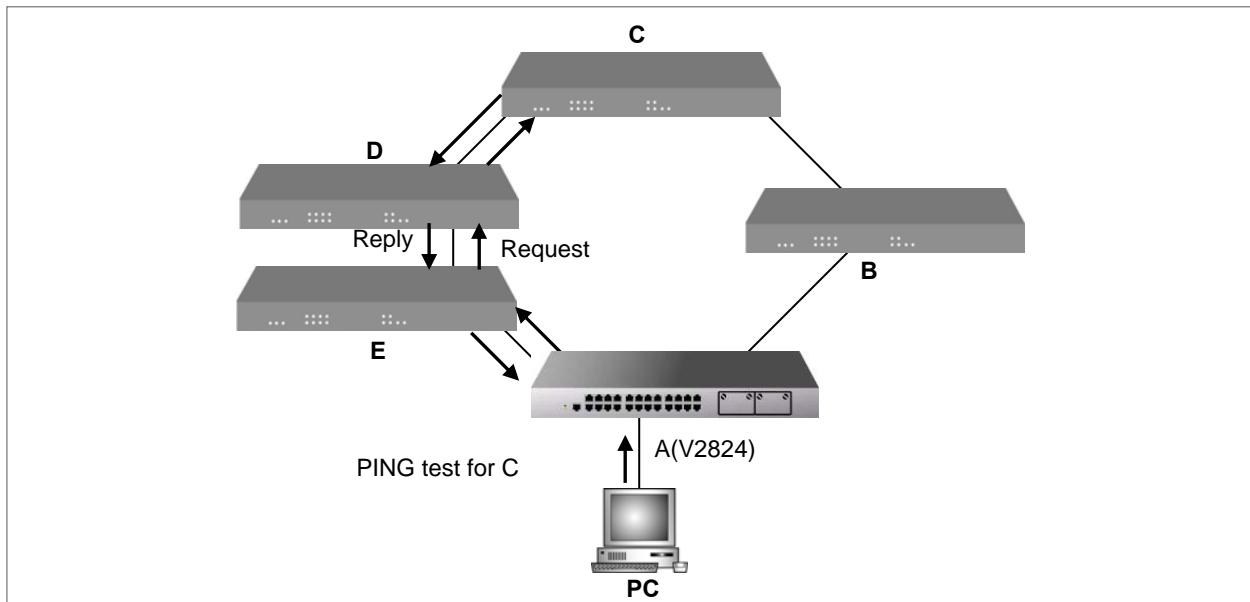
6.3.2 IP ICMP Source Routing

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, V2824는 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.

V2824에 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** 명령어를 사용하여 지정된 경로를 따라 Ping 테스트를 실시하도록 합니다.

6.3.3 패킷 경로 추적

V2824의 사용자는 패킷이 목적지로 가면서 거쳐 가는 경로를 확인할 수 있습니다. 이 경로를 알아내기 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]		

【 표 6-4 】 Traceroute 실행을 위한 기본 설정

내 용	기 본 설 정
Source address or interface:	상대방이 응답해야 하는 주소를 source ip address에 지정해줍니다.
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
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 보여주고 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 확인 및 삭제

특정한 포트에 기록된 MAC 테이블의 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show mac		장비에 등록된 MAC 주소를 출력합니다.
show mac bridge-name	Enable/	특정 인터페이스에 등록된 MAC 주소를 출력합니다.
show mac bridge-name port-number	Global/	특정 포트에 등록된 MAC 주소를 출력합니다.
show usermac [port-number]	Bridge	사용자 MAC 주소 정보를 확인합니다.
show mac count [port-number]		MAC 엔트리 통계 정보를 확인합니다.

다음은 default 인터페이스에 기록된 MAC 테이블을 출력한 경우입니다.

```
SWITCH# show mac default
=====
port      mac addr      permission      in use
=====
eth23     00:0c:f1:da:9c:09    OK          170.66
eth24     00:0c:f1:c0:ea:d8    -           12.53
SWITCH#
```



참 고

위의 출력되는 내용은 장비에 따라 달라질 수 있습니다.



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

6.3.6 Aging Time 설정

MAC 주소를 사용해 패킷을 주고 받는 스위치는 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 time	Bridge	MAC 주소 기록 유지 여부를 가리는 Aging time을 설정합니다.



참 고

*time*은 초 단위로 10초에서 21474830초 사이에서 설정 가능하며, 1800 시리즈 스위치에는 기본적으로 30초로 설정되어 있습니다.

6.3.7 장비 사용 시간 확인

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

명령어	모 드	기 능
show uptime	View / Enable / Global	장비 사용 시간을 확인합니다.

다음은 장비를 사용한 시간을 확인한 예입니다.

```
SWITCH# show uptime
0 days 0 hours 17 minutes 50 seconds
SWITCH#
```

6.3.8 시스템 구성 정보 확인

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

명령어	모 드	기 능
show system	View / Enable / Global	장비의 시스템 구성 정보를 확인합니다.

다음은 장비의 시스템 구성 정보를 확인한 예입니다.

```
SWITCH(config)# show system

SysInfo(System Information)
Model Name      : V1824
Main Memory Size : 128 MB
Flash Memory Size : 16 MB(INTEL 28F128J3)
S/W Compatibility : 4, 1
H/W Revision    : DS-TN-070-B0
NOS Version     : 3.13
B/L Version      : 4.88
H/W Address      : 00:d0:cb:00:0d:8a
RTC Information   : M41T11
Serial Number    : N/A
```

```
SWITCH(config)#

```



참 고

위의 출력되는 내용은 장비에 따라 달라질 수 있습니다.

6.3.9 CPU 사용량 확인

V2824는 CPU의 평균 사용량이나 사용량 통계를 확인할 수 있습니다. CPU 사용량 통계는 5초, 1분, 10분 동안의 CPU 평균 사용량을 기록한 것입니다.

V2824의 CPU 평균 사용량을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show cpupload	View / Enable / Global	장비의 CPU 평균 사용량을 확인합니다.

한편, 5초 간격으로 기록한 최근 CPU 사용량을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show cpu-trueload	View / Enable / Global	최근 10분 동안의 CPU 사용량을 5초 간격으로 확인합니다.

6.3.10 CPU 프로세스 확인

V2824의 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.

V2824의 CPU 프로세스를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show process	Enable / Global	사용자 스위치의 CPU 프로세스를 확인합니다.

6.3.11 CPU 처리 패킷 제한

시스템의 CPU가 처리해야 할 패킷이 많아지면, 장비의 성능이 떨어질 수 있습니다. V2824는 CPU 부하를 막기 위해 CPU에서 처리하는 패킷의 수를 제한할 수 있습니다. CPU에서 처리하는 패킷의 수를 제한하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
cpu packet limit <500-6,000>	Global	CPU에서 처리하는 패킷의 수를 제한합니다.



<500-6,000>의 단위는 초당 패킷의 개수입니다.

CPU에서 처리되는 패킷 수를 제한한 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show cpu packet limit	Enable/Global	CPU에서 처리되는 패킷 수를 제한한 내용을 확인합니다.

6.3.12 CPU 통계 확인

V2824의 사용자는 장비의 CPU 평균 사용량을 확인할 수 있습니다. CPU 평균 사용량을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show cpu statistics avg-pkt [port-number]	Enable/	CPU에 유입되는 유니캐스트, 멀티캐스트, 브로드캐스트 패킷의 평균 트래픽을 확인합니다.
show cpu statistics total {port-number}	Global/	CPU의 모든 통계 정보를 확인합니다.
show cpu counters [port-number]	Bridge	CPU의 포트별 패킷 개수를 확인합니다.
show cpu counters avg [port-number]		CPU의 포트별 평균 패킷 개수를 확인합니다.

특정 포트의 CPU 트래픽 통계 정보를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear cpu statistics [port-number]	Enable / Global / Bridge	해당 포트의 CPU 통계 정보를 초기화합니다.

6.3.13 메모리 사용 정보 확인

사용자 스위치의 메모리에 대한 정보를 확인하려면 Enable 모드나 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show memory	Enable / Global/Bridge	사용자 스위치의 메모리 사용 정보를 확인합니다.
show memory { dhcp imi lib nsm }		특정 기능에 대한 Memory 사용량을 확인합니다.

6.3.14 시스템 이미지 확인

사용자 스위치의 플래시 메모리에 대한 정보를 보면 어떤 이미지가 설치되어 있는지 알 수 있습니다. 플래시 메모리에 대한 정보를 보려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show flash	View / Enable / Global	장비에 설치된 시스템 이미지를 확인합니다.

6.3.15 시스템 이미지 버전 확인

V2824의 사용자는 현재 구동되고 있는 시스템 이미지의 버전을 확인할 수 있습니다. 현재 구동 되고 있는 시스템 이미지 버전을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show version	View / Enable / Global	시스템 이미지 버전을 확인합니다.

6.3.16 시스템 이미지 파일 크기 확인

V2824의 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	시스템 이미지 파일의 크기를 확인한 경우입니다.

6.3.17 Default OS 설정

V2824는 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. V2824 스위치의 사용자는 두 가지의 시스템 이미지를 설치하였을 경우에 자신이 원하는 시스템 이미지를 Default OS로 설정할 수 있습니다.



V2824는 기본적으로 os1에 설치된 시스템 이미지가 Default OS로 지정됩니다.

Default OS를 설정할 때에는 Enable 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
default-os {os1 os2}	Enable	Default OS를 설정합니다.

다음은 os2를 Default OS로 설정하는 경우입니다.

```
SWITCH# default-os os2  
SWITCH#
```

사용자가 설정한대로 Default OS가 지정되어 있는지 확인하려면 **show flash** 명령어로 플래시 메모리에 설치된 시스템 이미지를 확인하십시오.

다음은 os1이 Default OS였던 V2824의 Default OS를 os2로 바꾼 후 그 내용을 확인한 경우입니다.

```
SWITCH# show flash

Flash Information(Bytes)
Area          total        used        free
-----
OS1(default)(running) 16777216  11739168  5038048  V2824.1.03 #1101
OS2              16777216  11739168  5038048  V2824.1.01 #1003
CONFIG          4194304   659456   3534848

Total          37748736  24137792  13610944

SWITCH# default-os os2
SWITCH# show flash

Flash Information(Bytes)

Area          total        used        free
-----
OS1          16777216  11739168  5038048  V2824.1.03 #1101
OS2(default)(running) 16777216  11739168  5038048  V2824.1.01 #1003
CONFIG          4194304   659456   3534848

Total          37748736  24137792  13610944
```

6.3.18 시스템 상태 확인

V2824의 일부 기종은 장비의 온도, 전원 상태, 팬 상태 등을 확인할 수 있습니다.

장비의 온도, 전원 상태, FAN 상태 등을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show status fan		스위치의 팬 상태를 확인합니다.
show status power	Enable /Global / Bridge	스위치의 전원 상태를 확인합니다.
show status temp		스위치의 온도를 확인합니다.
show environment		스위치의 팬 상태 및 온도의 요약 정보를 확인합니다.

6.3.19 Tech-support 확인

V2824는 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	Enable	콘솔에서 Tech-support를 확인합니다.
tech-support {all crash-info} remote ip-address file-name {ftp tftp}		Tech-support를 지정한 IP 주소에 저장합니다.



위의 옵션에서 **all**을 선택하면, 모든 Tech-support 정보를 확인할 수 있고, **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.



콘솔상에서 보여지는 Tech-support 내용은 터미널 스크린 출력 행 수에 관계없이 한번에 모두 보여집니다.

6.3.20 프로토콜 통계 확인

V2824의 사용 프로토콜 통계를 확인하기 위해서는 다음 명령어를 통해 해당 프로토콜의 통계 기능을 활성화 시켜야 합니다. Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
protocol statistics enable {arp icmp ip tcp udp}	Global	ARP, ICMP, IP, TCP, UDP 프로토콜의 통계 기능을 활성화 시킵니다.

사용자의 장비에서 설정했던 프로토콜 통계 확인 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
protocol statistics disable {arp icmp ip tcp udp}	Global	설정한 프로토콜의 통계 기능을 해제합니다.

V2824의 사용 프로토콜의 통계를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show protocol statistics avg-pkt port-number	Enable/ Global/	지정한 포트의 평균 혹은 전체 프로토콜 통계를
show protocol statistics total port-number	Bridge	확인합니다.

V2824의 사용 프로토콜의 통계를 초기화하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear protocol statistics [port-number]	Global/ Bridge	특정 포트의 모든 프로토콜의 통계를 초기화합니다.

6.3.21 부팅 정보 확인

시스템의 리부팅이나 장비 전원 ON/OFF에 의한 부팅 정보를 확인하기 위해서는 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show boot-info	Enable/ Global/ Bridge	장비의 최근 부팅 정보를 확인합니다

6.3.22 케이블 길이 확인

V2824는 서로 연결되어 있는 장비간 케이블 길이를 포트별로 확인할 수 있습니다. 케이블 길이를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show cable-length port-number	Enable /Global / Bridge	장비간 케이블의 길이를 확인합니다.



케이블의 길이를 확인하는 명령어는 RJ-45 커넥터 타입 Category 5 UTP 케이블만 확인이 가능합니다. 광케이블일 경우에는 확인이 불가능하니 참고바랍니다.

6.3.23 G-PON 모듈 정보 확인

V2824는 G-PON 업링크를 선택하여 사용할 경우 G-PON ONU로써 활용할 수 있습니다. G-PON(Gigabit PON)은 상향 최대 약 1.25G, 하향 최대 약 2.5G의 높은 전송 속도를 지원하며 초고 속 인터넷서비스, IPTV, VoIP 등 다양한 멀티미디어 서비스가 가능한 시스템입니다.

G-PON 업링크 모듈 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show port gpon-module-info [port-number]	Global	G-PON 업링크 모듈 정보를 확인합니다.

7. 네트워크 관리 기능 설정

V2824와 장비가 속해 있는 네트워크를 관리할 수 있는 기능에 대한 설정 방법을 설명합니다. 이 장은 다음과 같은 내용으로 이루어져 있습니다.

- SNMP
- EFM OAM
- LLDP
- RMON 설정
- Syslog 설정
- QoS(Quality of Service)
- NetBIOS 필터링
- MAC 필터링
- MAC 테이블 관리
- ICMP 메시지 Control
- ARP
- TCP Flag Control
- 덤프 패킷 (Dump Packet)
- Port Security
- PPS-Control
- Attack Guard
- LLCF (Link Layer Carrier Forward)
- 포트 트래픽 모니터링 설정
- ECMP(Equal Cost Multi-Path) 설정

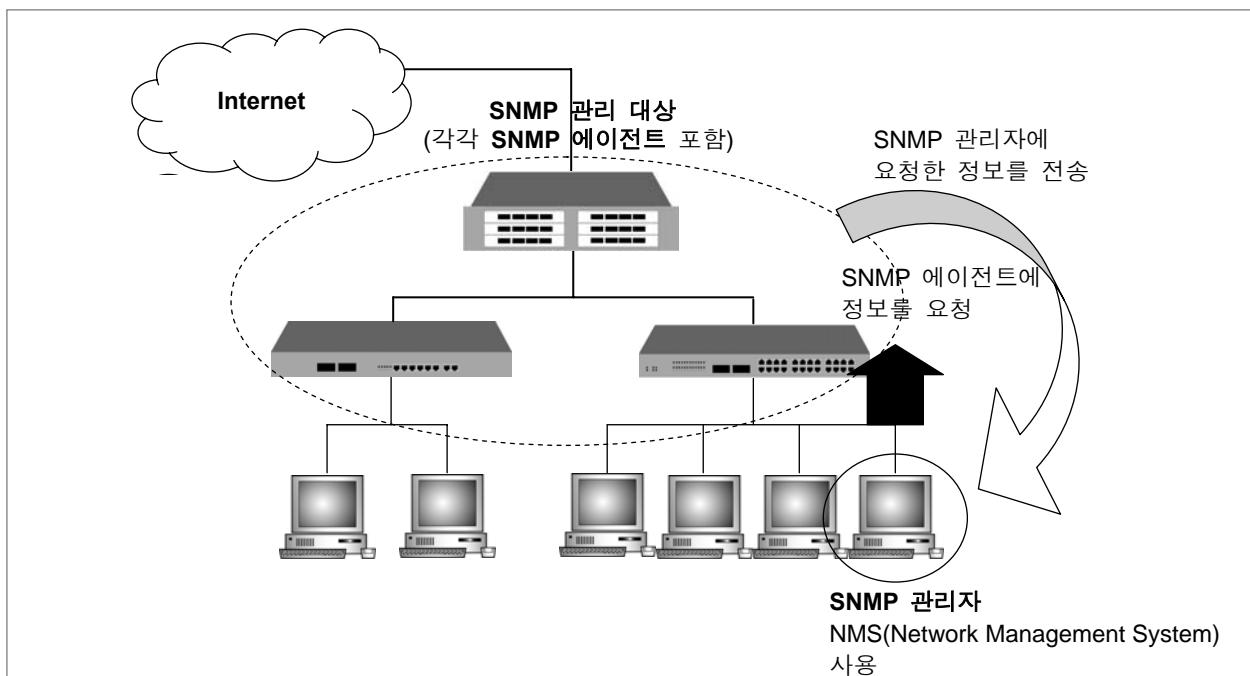
7.1 SNMP

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.

스위치에 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 스위치와 통신 불가능 등과 같은 정보를 알려 줍니다.



【 그림 7-1 】 SNMP 구성의 예

SNMP가 지원되는 (주) 다산네트웍스의 스위치는 v1을 채택하고 있습니다. 한편, V2824는 SNMP v2c 및 v3까지도 지원하여 향상된 기능을 제공합니다. 이렇게 SNMP 기능 향상된 (주)다산네트웍스 스위치는 SNMP 에이전트의 접속 관리를 더욱 강화하였고, 에이전트에게 공개하는 OID의 범위를 제한할 수 있습니다.

다음은 (주)다산네트웍스 스위치에 SNMP를 설정하는 방법에 대한 목록입니다.

- SNMP v1의 Community 설정
- SNMP 에이전트 관리자에 대한 연락처와 설치 위치 정보 지정
- SNMP v2c의 com2sec 설정
- SNMP v2c 및 v3의 Group 설정
- SNMP v2c 및 v3의 OID 공개 범위 제한(View 설정)
- SNMP v2c 및 v3 제한 OID에 대한 접속권한부여(Access 설정)
- SNMP v3의 User 설정
- SNMP 트랩 설정
- SNMP 에이전트의 IP 지정
- SNMP 설정 확인
- SNMP 기능 해제
- 설정 예제



주의

SNMP는 그 발전도에 따라서 v1, v2c, v3가 있습니다. (주)다산네트웍스 스위치는 각 제품별로 지원하는 버전이 다르므로 제품별로 설정의 적용여부가 다를 수 있습니다.

7.1.1 SNMP v1의 Community 설정

스위치에 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 {rw ro} community-name [ip-address] [oid]	Global	접속 권한을 부여하는 Community를 설정합니다.



(주)다산네트웍스의 스위치에는 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. 패스워드에 따라 SNMP 에이전트에 대한 접속 권한을 읽기로 한정하거나 읽기/쓰기의 모든 권한을 부여할 수 있습니다. 명령어 중에 제일 뒤에 오는 ro와 rw는 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 {rw ro} community-name	Global	Community를 삭제합니다.

설정한 Community를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show snmp community	Enable/Global	Community를 확인합니다.

7.1.2 SNMP 에이전트 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 정보와 SNMP 에이전트가 설치된 장비 위치를 입력하는 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 /	등록했던 SNMP 에이전트의 시스템 관리자에 대한 정보를 확인합니다.
show snmp location	Global	등록했던 SNMP 에이전트가 설치된 장비 위치를 확인합니다.

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 <i>security-name {ip-address ip-address/m} community</i>	Global	에이전트에 접근이 허용되는 Manager 와 그Community 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.

7.1.4 SNMP v2c 및 v3의 Group 설정

(주)다산네트웍스 스위치의 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 설정합니다.

{v1 | v2c | v3} 부분에는 설정하는 Group에 부여하고자 하는 보안 모델을 선택하면 됩니다. security-name은 com2sec에서 설정한 security-name을 사용합니다. 다만 SNMP v3 모델은 security-name이 SNMP의 기본 프로토콜의 일부분이므로 v2에서와 같은 com2sec에서의 설정 없이 곧바로 본 명령어에서 지정하여 사용할 수 있습니다.

한편, Group으로 설정했던 것을 해제하려면, 다음 명령어를 사용하십시오.

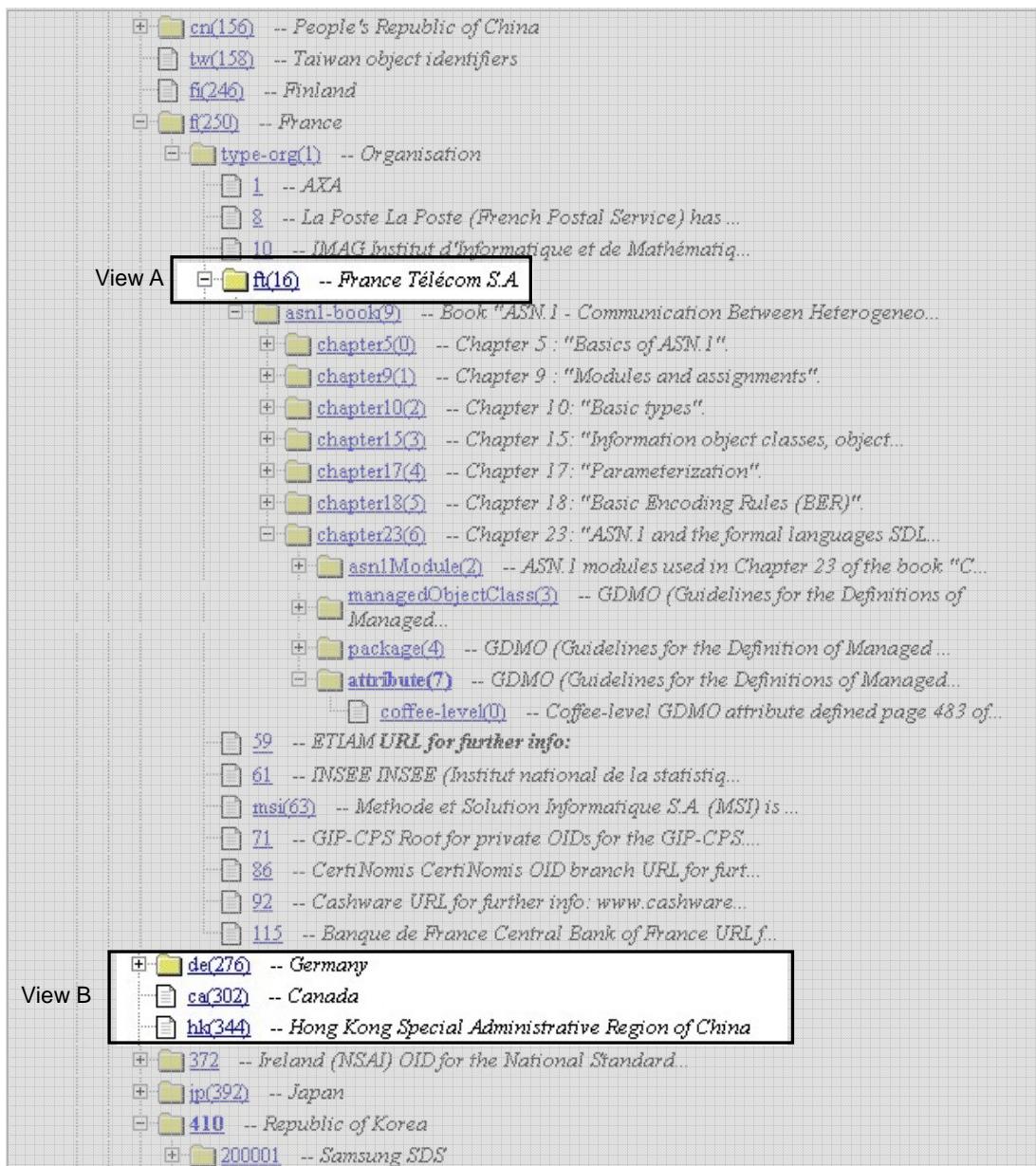
명령어	모 드	기 능
no snmp group group-name [[v1 v2c v3] [security-name]]	Global	Group을 해제합니다.

등록한 group을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show snmp group	Enable / Global	등록한 Group을 확인합니다.

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 스위치에 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 [oid]	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.

7.1.6 SNMP v2c 및 v3 제한 OID에 대한 접속권한부여(Access 설정)

(주)다산네트웍스 스위치 종 SNMP v2c와 v3를 지원하는 스위치의 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
snmp access group-name {v1 v2c} <i>read-name write-name notify-name</i>	Global	SNMP v1과 SNMP v2c에서 해당 그룹에게 허가할 View를 설정합니다.
snmp access group-name v3 {noauth auth priv} <i>read-name write-name notify-name</i>		SNMP v3에서 해당 그룹에게 허가할 View를 설정합니다.

read-name, *write-name*, *notify-name* 에는 View 설정에서 지정한 *view-name*을 사용합니다. 제한 없이 모두 허가할 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 SHA 알고리즘에 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
no snmp access group-name	Global	제한된 OID를 허가했던 Group을 해제합니다.

공개 제한된 OID에 접속 허가를 받은 Group을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show snmp access	Enable / Global	공개 제한된 OID에 접속 허가를 받은 Group을 확인합니다.

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.

참 고

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.

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.

V2824의 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.



참 고

V2824의 SNMP 트랩은 기본적으로 Alarm-report로 설정되어 있습니다.

(1) SNMP 트랩 호스트 지정

SNMP 에이전트가 트랩 메시지를 송신하는 대상을 SNMP 트랩 호스트라고 합니다. V2824는 SNMP 트랩을 전송 받을 트랩 호스트를 지정할 수 있습니다. 이 때, SNMP 관리자에게 트랩이 송신되도록 설정하기를 원한다면 SNMP 관리자의 IP 주소를 사용하여 트랩 호스트로 설정하면 됩니다.

V2824는 SNMP v1의 트랩 호스트와 SNMP v2c의 트랩 호스트, 그리고 SNMP v3의 Inform 트랩 호스트를 각각 설정할 수 있습니다.

SNMP Trap-host를 설정하려면, 다음 명령어를 사용하십시오.

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.

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)#{}
```



V2824의 SNMP Tap-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 V2824 SNMP 트랩은 Event 모드와 Alarm-report 모드의 2종류가 있습니다. 기본적으로는 Event 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 V2824의 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 】 V2824의 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 많아졌을 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.



참 고

V2824는 기본적으로 위에서 설명한 트랩 메시지가 모두 송신되도록 설정되어 있습니다.

V2824의 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 V2824의 관리자는 트랩 호스트에게 전달되는 트랩 메시지의 종류를 선택할 수 있습니다.



참 고

V2824의 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-thrshold		
no snmp trap module		
no snmp trap port-thrshold		
no snmp 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		
no snmp alarm-severity erp-domain-multi-rm	Global	ERP에 대한 Alarm 설정을 해제합니다.
snmp alarm-severity erp-domain-reach-fail		
no snmp alarm-severity erp-domain-ulotp		

(6) Notify-Activity 활성화

V2824는 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.



참 고

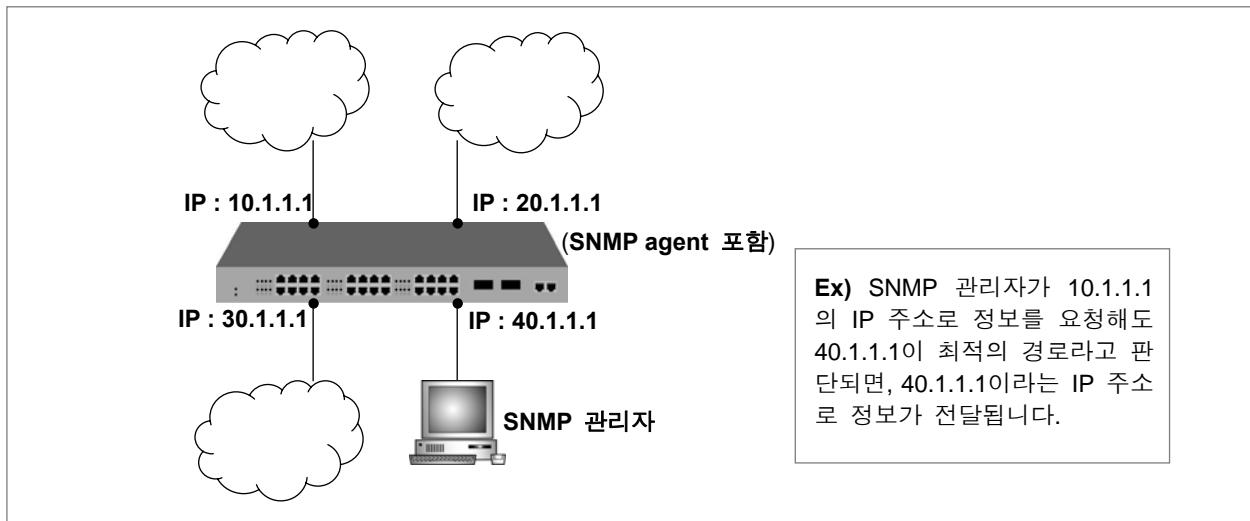
snmp clear alarm-report 명령어는 Trap-mode가 alarm-report 일 때만 사용 가능합니다..

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.



【 그림 7-2 】 SNMP 에이전트의 IP 주소

그러나, V2824는 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.



주 의

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
SWITCH(config)# interface br1
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 종단시키려면, Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no snmp	Global	SNMP 기능을 해제합니다.



주 의

위의 명령어를 사용하면 SNMP와 관련된 모든 설정 내용이 삭제됩니다.

V2824는 fan trap과 door trap의 우선순위를 critical > major > minor > normal의 4레벨로 설정할 수 있습니다.

fan trap과 door trap의 우선순위를 설정 하려면 다음 명령어를 사용하십시오

명령어	모 드	기 능
alarmclass door {nomal minor major critical}	Global	door trap의 우선순위를 설정 합니다.
alarmclass fan1 {nomal minor major critical}		fan trap의 우선순위를 설정 합니다.

7.1.12 설정 예제

[설정 예제 1]

다음은 읽기/쓰기 권한을 주는 community name을 public이라고 설정하고, 읽기 권한만 주는 community name을 private로 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)#

```

[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
SWITCH(config)# snmp location Seoul,Korea
SWITCH(config)#

```

[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
-----
dasan        100.1.1.1    public

SWITCH(config)#[
```

[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)#[
```

[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)#[
```

[설정 예제 6]

다음은 Access를 설정하고 확인하는 경우의 예입니다.

```
SWITCH(config)# snmp access rogroup v1 none none none
SWITCH(config)# show snmp access

Access List
GroupName      SecModel  SecLevel  ReadView      WriteView      NotifyView
-----
rogroup        v1        noauth    none          none          none

SWITCH(config)#

```

[설정 예제 7]

다음은 user를 설정하고 확인하는 경우의 예입니다.

```
SWITCH(config)# snmp user root md5 vertex25 des vertex25
SWITCH(config)# show snmp user

User List
Name      AuthMode  AuthPassphrase  PrivMode  PrivPassphrase
-----
root     md5       vertex25       des       vertex25

SWITCH(config)#

```

[설정 예제 8]

다음은 IP 주소가 10.1.1.3인 관리자에게 트랩을 전송하도록 설정하고, auth-fail 트랩 메시지를 해제하고, 그 내용을 확인한 경우입니다.

```
SWITCH(config)# snmp trap-host 10.1.1.3
SWITCH(config)# no snmp trap auth-fail
SWITCH(config)# show snmp trap

Trap-Host List
      Host          Community
-----
trap-host      10.1.1.3

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
SWITCH(config)#

```

[설정 예제 9]

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)#

```

다음은 장비에 전송된 alarm을 확인하고, 그 기록을 모두 지운 경우입니다.

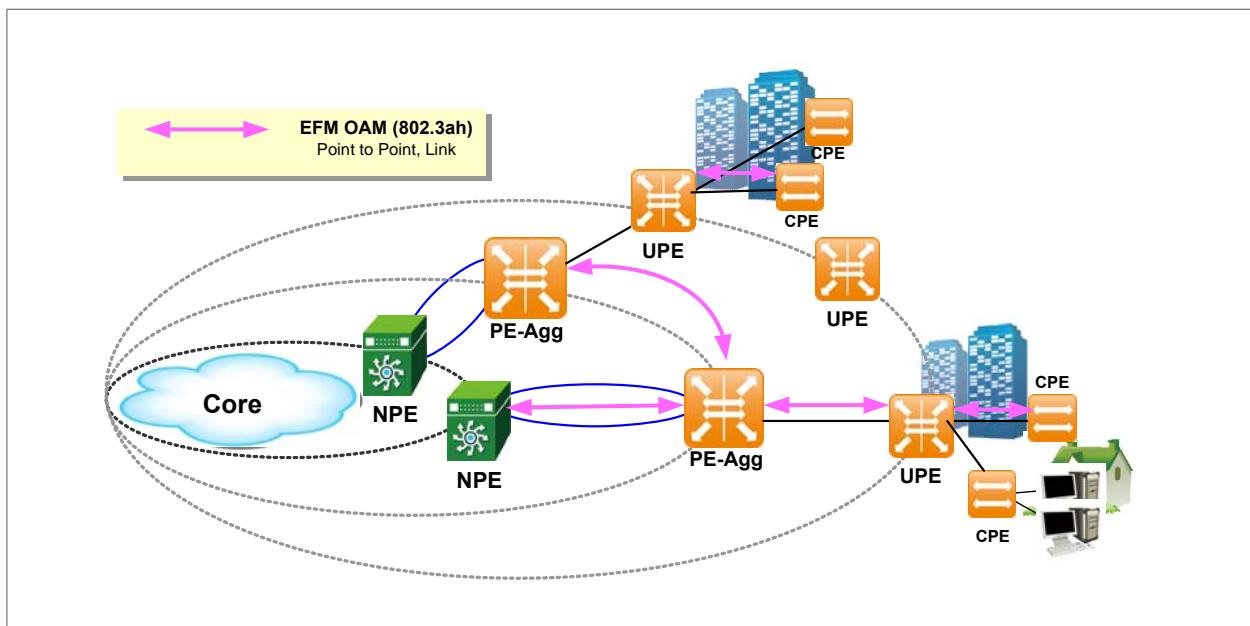
```
SWITCH(config)# show snmp alarm-history
cold-start      minor      Fri Mar 25 15:30:56 2005 System booted.
SWITCH(config)# snmp clear alarm-history
SWITCH(config)# show snmp alarm-history
SWITCH(config)#

```

7.2 EFM OAM

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 7-3 】 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	Bridge	EFM OAM 기능을 활성화 합니다.

EFM OAM 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam efm disable port-number	Bridge	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	Bridge	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 <10-600> threshold <0-65535> port-number	Bridge	특정 시간 동안의 Errorred 프레임의 개수의 임계값을 지정합니다. Window Size는 기본적으로 1초로 설정되어 있으며, 설정 단위는 100msec입니다. 임계값은 기본적으로 1로 설정되어 있습니다.
oam efm link-monitor frame-period window <1000-200000000> threshold <0-65535> port-number	Bridge	특정 프레임의 개수에서 Errorred 프레임의 개수 임계값을 지정합니다. Window Size는 기본적으로 1000000프레임으로 설정되어 있습니다. 임계값은 기본적으로 10로 설정되어 있습니다.
oam efm link-monitor symbol-period window <1-1000000> threshold <0-65535> port-number	Bridge	특정 시간 동안의 Errorred Symbol 개수의 임계값을 지정합니다. Window Size는 기본적으로 625million으로 설정되어 있습니다. 임계값은 기본적으로 1로 설정되어 있습니다.
oam efm link-monitor frame-seconds-summary window <10-900> threshold <0-900> port-number	Bridge	특정 시간 동안의 Errorred Seconds의 임계값을 지정합니다. Window Size는 기본적으로 60초로 설정되어 있습니다. 임계값은 기본적으로 1로 설정되어 있습니다.

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	Bridge	Link 모니터링을 통해 알게 된 정보를 syslog로 출력합니다.
oam efm link-monitor action snmp-trap port-number		Link 모니터링을 통해 알게 된 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	Bridge	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, Loopback를 실행합니다.

Remote DTE의 Loopback 모드를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam efm remote-loopback permit port-number	Bridge	특정 포트에서 Loopback 기능이 동작하도록 Loopback 컨트롤 패킷을 허용합니다.
oam efm remote-loopback deny port-number		특정 포트에서 Loopback 기능이 동작하도록 Loopback 컨트롤 패킷을 차단합니다.

Remote DTE의 Loopback 기능을 활성화하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam efm remote-loopback enable port-number	Bridge	Remote DTE의 Loopback 기능을 활성화합니다.
oam efm remote-loopback disable port-number		Remote DTE의 Loopback 기능을 해제화합니다.

Loopback 기능을 실행하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam efm remote-loopback test <1-100> port-number	Bridge	Loopback 테스트 패킷을 전송하도록 설정합니다.

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	Bridge	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	Bridge	RX가 불가능할 때, TX를 이용해서 자신의 정보를 전송하도록 설정한 것을 해제합니다.

7.2.6 Remote OAM 설정

Remote OAM을 활성화시키려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam remote oam admin <1-2> enable port-number	Bridge	Remote OAM를 활성화합니다.
oam remote oam admin <1-2> disable port-number		Remote OAM를 해제합니다.

Remote OAM의 모드를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam remote oam mode <1-2> {active passive} <i>port-number</i>	Bridge	Remote OAM의 모드를 설정합니다.



참 고

Remote OAM **active**는 Request와 Loopback이 모두 가능한 상태입니다. 반대로 Remote OAM **passive**는 Request와 Loopback을 요청할 수 없는 상태를 나타냅니다.

OAM 기능을 이용하여 상대방 장비의 정보들을 조사하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
oam remote alarm optical <1-3> <0-65535> port-number oam remote alarm temperature <0-255> port-number oam remote alarm voltage {min max} <0-65535> port-number oam remote electrical mode {full half} port-number oam remote general autoneg <1-4> {enable disable} port-number oam remote general forwarding <3-4> {enable disable} port-number oam remote general speed <1-4> <0-4294967295> port-number oam remote general user <1-4> string port-number oam remote system interface {unforced forceA forceB} port-number oam remote system interval <0-255> port-number oam remote system mode {master slave} port-number oam remote system reset port-number	Bridge	OAM 기능을 이용하여 상대방 장비의 정보를 조사합니다.

7.2.7 OAM 설정 확인

OAM 설정 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show oam efm		EFM OAM 활성화 여부를 확인합니다.
show oam efm link-monitor [local remote] port-number	Enable/ Global/ Bridge	포트 별 Link 모니터링 정보를 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.

[설정 예제 1]

다음은 사용자 장비의 1번 포트를 통해 상대편 장비와 OAM Loopback 기능이 가능하도록 설정하고, 1회 실행하는 경우입니다.

```
SWITCH(bridge)# oam efm enable 2
SWITCH(bridge)# oam efm remote-loopback enable 2
SWITCH(bridge)# show oam efm local 2
    LOCAL PORT[1/2]
-----
      item      |      value
-----
      admin      |      ENABLE
      mode       |      ACTIVE
      mux action |      FORWARD
      par action |      DISCARD
      variable   |      SUPPORT
      link event |      SUPPORT
      loopback   |      SUPPORT(disable)
      uni-direction |      SUPPORT(disable)
-----
SWITCH(bridge)#

```

```
SWITCH(bridge)# show oam remote 1/2
REMOTE PORT[1/2]
-----
      item      |      value
-----
mode          |      ACTIVE
MAC address   |      00:d0:cb:27:00:94
variable      |      SUPPORT
link event    |      SUPPORT
loopback      |      SUPPORT(enable)
uni-direction |      UNSUPPORT
-----
SWITCH(bridge)# oam remote loopback test 1/2
PORT[1/2]: The remote DTE loopback is success.
SWITCH(bridge)#

```

7.3 LLDP

LLDP(Link Layer Discovery Protocol)은 IEEE 802.1ab 표준에 따라 LAN에 연결된 장비들 사이에 네트워크 관리에 필요한 자료를 송수신하도록 하는 기능입니다. LLDP를 지원하는 V2824는 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.

LLDP가 동작하기 시작하면, 장비들은 자신의 정보를 근접한 장비들에게 보냅니다. 그리고, Local의 상태가 변화되면, 이를 알리기 위해 또 다시 자신의 바뀐 정보를 근접한 장비들에게 보냅니다.

예들 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.

7.3.1 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 활성화합니다.
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.



참 고

*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.

7.3.2 LLDP 동작 방식 설정

포트에서 LLDP를 활성화시켰다면, LLDP의 동작 방식을 설정해야 합니다. LLDP의 동작 방식을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lldp adminstatus port-number {both tx_only rx_only}	Bridge	포트의 LLDP 동작 방식을 설정합니다.
lldp adminstatus port-number disable		포트의 LLDP 동작 방식을 해제합니다.



참 고

V2824의 LLDP 동작 방식은 기본적으로 프레임에 대한 처리를 진행하지 않도록 설정되어 있습니다.

각 옵션은 다음과 같이 동작합니다.

- **both** : LLDP 프레임을 송수신합니다.
- **tx_only** : LLDP 프레임을 송신만합니다.
- **rx_only** : LLDP 프레임을 수신만합니다.
- **disable** : LLDP 프레임을 처리하지 않습니다.

7.3.3 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. V2824는 관리자가 Basic TLV의 전송을 선택하여 활성화하거나 비활성화 할 수 있습니다.

Basic TLV를 선택하여 활성화하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<pre>lldp port-number {portdescription sysname sysdescription syscap}</pre>	Bridge	해당 포트에서 송신할 Basic TLV를 선택합니다.
<pre>no lldp port-number {portdescription sysname sysdescription syscap}</pre>		해당 포트에서 송신하도록 설정했던 Basic TLV를 송신하지 않도록 합니다.



참 고

*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.

7.3.4 LLDP 메시지 송신 관련 설정

V2824는 LLDP 메시지 송신 간격 및 횟수를 설정할 수 있습니다. LLDP 메시지 송신 간격과 송신 횟수를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lldp msg txinterval interval	Bridge	LLDP 메시지 송신 주기를 설정합니다.
lldp msg txhold times		LLDP 메시지 송신 횟수를 설정합니다.



*Interval*은 초 단위로 <5 – 32, 768> 사이에서 설정 가능합니다. 기본으로 설정되어 있는 *interval*은 30초입니다. V2824는 기본적으로 LLDP 메시지를 30초 마다 4번 송신하도록 되어 있습니다.



*times*는 <2 – 10> 사이에서 설정 가능합니다. 기본으로 설정되어 있는 *time*는 4회입니다.

7.3.5 Reinitdelay 설정

V2824의 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 re-init-delay	Bridge	LLDP 프레임을 처리하지 않도록 설정한 때로부터 다시 이를 활성화하기까지의 시간을 설정합니다.



*re-init-delay*는 초 단위로 <1 – 10> 사이에서 설정 가능합니다. 기본으로 설정되어 있는 *re-init-delay*는 2초입니다.

7.3.6 LLDP 프레임 전송 Delay 시간 설정

V2824 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 tx-delay	Bridge	LLDP 프레임을 주고받는 장비간에서 프레임 전송 Delay 시간을 설정합니다.



참 고

*tx-delay*는 초 단위로 <1 – 8, 192> 사이에서 설정 가능합니다. 기본으로 설정되어 있는 *tx-delay*는 2초입니다.

7.3.7 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.

7.3.8 LLDP 통계 확인

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]	Enable/Global/Bridge	포트에 누적된 통계량을 초기화합니다.

7.3.9 Remote 엔트리 통계 확인

Remote 엔트리의 통계를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show lldp remote [port-number]	Enable / Global / Bridge	Remote 엔트리들의 통계 내용을 확인합니다.

7.3.10 설정 예제

【 설정 예제 1 】

다음은 23,24번 포트에 LLDP를 활성화하고 이를 확인한 경우입니다.

```
SWITCH(bridge)# lldp disable 23-24
SWITCH(bridge)# show lldp config
GLOBL:
-----
MsgTxInterval      = 30
MsgTxHold         = 4    => txTTL = 120
ReInitDelay       = 2
TxDelay           = 2
-----
PORTS active      adminStat|optTLVs
  1: disable      Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
  2: disable      Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
  3: disable      Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
  4: disable      Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
  5: disable      Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
  6: disable      Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
  7: disable      Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
  8: disable      Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
  9: disable      Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 10: disable     Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 11: disable     Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 12: disable     Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 13: disable     Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 14: disable     Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 15: disable     Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 16: disable     Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 17: disable     Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 18: disable     Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 19: disable     Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 20: disable     Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 21: disable     Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 22: disable     Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 23: enable      Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 24: enable      Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 25: disable     Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
 26: disable     Tx<->Rx|0xf= PortDesc, SysName, SysDesc, SysCap
```

[설정 예제 2]

다음은 LLDP Remote 엔트리들의 Statistics 내용을 확인하는 경우입니다.

```
SWITCH(bridge)# show lldp remote
Port 23:
MSAP-Identifier: 00 d0 cb 27 00 88 65 74 68 32 35
ChassisType      : macAddress(4)
ChassisID        : 00 d0 cb 27 00 88
PortType         : interfaceAlias(1)
PortID          : 'eth23'
PortDescription: 'port23-TX-10/100/1000'
SystemName       : 'EL2'
SystemDescript.: 'V1824 NOS 3.13/DS-QA-07D-B0'
SysCapabilities: [0x16] repeater(0x02), bridge(0x04), router(0x10),
SysCapEnabled   : [0x04] bridge(0x04),
Mgmt: ifType      ifId ifAddress      |OID

Port 24:
MSAP-Identifier: 00 d0 cb 27 00 8d 65 74 68 32 36
ChassisType      : macAddress(4)
ChassisID        : 00 d0 cb 27 00 8d
PortType         : interfaceAlias(1)
PortID          : 'eth24'
PortDescription: 'port24-TX-10/100/1000'
SystemName       : 'EL3'
SystemDescript.: 'V1824 NOS 3.13/DS-QA-07D-B0'
SysCapabilities: [0x16] repeater(0x02), bridge(0x04), router(0x10),
SysCapEnabled   : [0x04] bridge(0x04),
Mgmt: ifType      ifId ifAddress      |OID

SWITCH(bridge)#

```

[설정 예제 3]

다음은 통계를 초기화하는 경우입니다.

```
SWITCH(bridge)# clear lldp statistics
SWITCH(bridge)# show lldp statistics
    GLOBL:
RemTabInserts = 0          RemTabAgeouts = 0
RemTabDeletes = 0          RemTabDrops   = 0

      TX | RX
      PORTS   Frames | Frames   Drop  Error  Disc  Unknown  Ageouts  Drop  CurrentRem
           1:     0 |     0     0     0     0     0     0     0     0     0     0
           2:     0 |     0     0     0     0     0     0     0     0     0     0
           3:     0 |     0     0     0     0     0     0     0     0     0     0
           4:     0 |     0     0     0     0     0     0     0     0     0     0
           5:     0 |     0     0     0     0     0     0     0     0     0     0
           6:     0 |     0     0     0     0     0     0     0     0     0     0
           7:     0 |     0     0     0     0     0     0     0     0     0     0
           8:     0 |     0     0     0     0     0     0     0     0     0     0
           9:     0 |     0     0     0     0     0     0     0     0     0     0
          10:    0 |     0     0     0     0     0     0     0     0     0     0
          11:    0 |     0     0     0     0     0     0     0     0     0     0
          12:    0 |     0     0     0     0     0     0     0     0     0     0
          13:    0 |     0     0     0     0     0     0     0     0     0     0
          14:    0 |     0     0     0     0     0     0     0     0     0     0
          15:    0 |     0     0     0     0     0     0     0     0     0     0
          16:    0 |     0     0     0     0     0     0     0     0     0     0
          17:    0 |     0     0     0     0     0     0     0     0     0     0
          18:    0 |     0     0     0     0     0     0     0     0     0     0
          19:    0 |     0     0     0     0     0     0     0     0     0     0
          20:    0 |     0     0     0     0     0     0     0     0     0     0
          21:    0 |     0     0     0     0     0     0     0     0     0     0
          22:    0 |     0     0     0     0     0     0     0     0     0     0
          23:    0 |     0     0     0     0     0     0     0     0     0     0
          24:    0 |     0     0     0     0     0     0     0     0     0     0

SWITCH(bridge)#

```

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, 호스트들간의 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 Enable N, Matrix, Filter, Packet capture, Event의 9 가지의 RMON MIB그룹이 정의되어 있습니다. (주)다산네트웍스의 V2824는 이 가운데 가장 기본적인 Statistics, History, Alarm, Event의 4가지 MIB그룹을 지원합니다.

V2824는 다음과 같은 RMON을 제공합니다.

- RMON History 설정
- RMON Alarm 설정
- RMON Event 설정

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.

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.

명령어	모 드	기 능
rmon-history number	Global	RMON 히스토리를 구별할 수 있도록 번호를 설정합니다. 1부터 65,535까지 쓸 수 있습니다.

다음은 1번 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])# ?
RMON history configuration commands:
  active          Activate the history
  data-source     Set data source name for the ethernet port
  do              To run exec commands in config mode
  exit            End current mode and down to previous mode
  help            Description of the interactive help system
  interval        Define the time interval for the history
  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
  write           Write running configuration to memory or terminal

```

```
SWITCH(config-rmonhistory[1])#
```



주의

실제로 물음표는 출력되지 않고, 물음표를 입력하면 곧장 명령어가 출력됩니다.

한편, History 설정 모드에서 빠져나와 Global 설정 모드로 돌아가거나 Enable 모드로 곧장 돌아가려면 다음의 명령어를 사용하십시오.

명령어	모 드	기 능
exit	RMON	Global 설정 모드로 돌아갑니다.
end		곧장 Enable 모드로 돌아갑니다.

(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.br1
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 dasan으로 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.



표본 조사할 데이터 수는 65535개까지 가능합니다.

다음은 History에서 표본 조사할 데이터 수를 25개로 설정하는 경우의 예입니다.

```
SWITCH(config-rmonhistory[1])# requested-buckets 25
SWITCH(config-rmonhistory[1])#
```

(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.



표본 조사를 하는 시간 간격을 설정할 때, 3600초까지 설정이 가능합니다.

다음은 표본 조사 시간을 60초로 지정한 예입니다.

```
SWITCH(config-rmonhistory[1])# interval 60
SWITCH(config-rmonhistory[1])#
```

(5) RMON History 활성화 하기

모든 설정이 끝난 RMON History를 활성화하려면 반드시 다음 명령어를 사용하여 활성화 설정을 해주어야 합니다. History를 활성화 시키려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
active	RMON	History를 활성화 시킵니다.



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.

다음은 RMON History를 활성화시키고, 위에서 설정한 내용들을 확인한 경우의 예입니다.

```
SWITCH(config-rmonhistory[1])# active
SWITCH(config-rmonhistory[1])# show running-config
Building configuration...
```

(종략)

```
rmon-history 5
owner dasan
data-source ifindex.hdlc1
interval 60
requested-buckets 25
active
```

(종략)

```
SWITCH(config-rmonhistory[1])#
```

(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 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no rmon-history number	Global	해당 번호의 RMON History를 삭제합니다.



RMON History의 *number*는 <1 – 65, 535> 사이에서 설정 가능합니다.

다음은 1번 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. 다음의 명령어를 사용하여 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.

명령어	모 드	기 능
rmon-alarm <1-65535>	Global	RMON Alarm 설정 모드로 들어갑니다.

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])# ?
RMON alarm configuration commands:
  active          Activate the event
  exit            End current mode and down to previous mode
  falling-event   Associate the falling threshold with an existing RMON
                  event
  falling-threshold Define the falling threshold
  help             Description of the interactive help system
  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
SWITCH(config-rmonalarm[1])#

```

**주 의**

실제로 물음표는 출력되지 않고, 물음표를 입력하면 곧장 명령어가 출력됩니다.

한편, Alarm 설정 모드에서 빠져나와 Global 설정 모드로 돌아가거나 Enable 모드로 곧장 돌아가려면 다음의 명령어를 사용하십시오.

명령어	모 드	기 능
exit	RMON	Global 설정 모드로 돌아갑니다.
end		곧장 Enable 모드로 돌아갑니다.

(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 <i>number</i>	RMON	상한 임계값을 설정합니다.



참 고

상한 임계값은 2,147,483,647까지 입력 가능하며 “0”을 입력하면 Alarm은 발생하지 않습니다.

다음은 상한 임계값을 100으로 설정한 경우입니다.

```
SWITCH(config-rmonalarm[1])# rising-threshold 100
SWITCH(config-rmonalarm[1])#
```

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 – 65, 535>	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])#
```



주 의

기준이 되는 상한 임계값을 0으로 입력하면 Event는 발생하지 않습니다.

(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.

```
SWITCH(config-rmonalarm[1])# falling-threshold 90
SWITCH(config-rmonalarm[1])#
```



하한 임계값은 2,147,483,647까지 입력 가능하며 0을 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 <0 – 65, 535>	RMON	하한 임계값 이하가 될때 RMON 알람 이벤트를 발생시킵니다.

다음 에서는 하한 임계값 이하일 때 RMON 이벤트 2가 발생하도록 설정했습니다.

```
SWITCH(config-rmonalarm[1])# falling-event 2
SWITCH(config-rmonalarm[1])#
```



기준이 되는 하한 임계값을 0으로 입력하면 Event는 발생하지 않습니다.

(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 수도 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 60초마다 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...
(종략)
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
(종략)
SWITCH(config-rmonalarm[1])#
```



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
<code>no rmon-alarm number</code>	Global	해당 번호의 RMON Alarm을 삭제합니다.



RMON Alarm의 *number*는 <1 – 65, 535> 사이에서 설정 가능합니다.

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 스위치에서 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.

다음 명령어를 사용하여 Event 설정 모드로 들어가면, 시스템 프롬프트가 `SWITCH(config)#`에서 `SWITCH(config-rmonevent[n])#`로 변경됩니다. 변수 *n*은 서로 다른 Event를 구별하기 위한 번호입니다.

명령어	모 드	기 능
<code>rmon-event <1 ~ 65, 535></code>	Global	RMON Event 설정 모드로 들어갑니다.

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])# ?
RMON event configuration commands:
  active      Activate the event
  community   Define a community to an unactivated event
  description Define description of RMON event
  do          To run exec commands in config mode
  exit        End current mode and down to previous mode
  help        Description of the interactive help system
  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
  write       Write running configuration to memory or terminal

SWITCH(config-rmonevent[1])#
```



주의

실제로 물음표는 출력되지 않고, 물음표를 입력하면 곧장 명령어가 출력됩니다.

한편, Event 설정 모드에서 빠져나와 Global 설정 모드로 돌아가거나 Enable 모드로 곧장 돌아가려면 다음의 명령어를 사용하십시오.

명령어	모 드	기 능
exit	RMON	Global 설정 모드로 돌아갑니다.
end		곧장 Enable 모드로 돌아갑니다.

다음은 각각 Event 설정 모드에서 Global 설정 모드로 돌아가는 경우와 Enable 설정 모드로 돌아가는 경우의 예입니다.

```
SWITCH(config-rmonevent[1])# exit
SWITCH(config)# 
SWITCH(config-rmonevent[1])# end
SWITCH#
```

(1) Event Community 설정

RMON Event가 발생했을 때 호스트로 SNMP 트랩(trap) 메시지를 전송하려면 community를 입력해야 합니다. community란 메시지 전송 권한을 부여하는 패스워드를 의미합니다. 트랩 메시지 전송에 필요한 community를 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 community를 password으로 설정하는 경우입니다.

```
SWITCH(config-rmonevent[1])# community password  
SWITCH(config-rmonevent[1])#
```

(2) Event 설명

V2824는 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.



Event에 대한 설명은 최대 126자까지 입력 가능합니다.

다음은 이벤트에 대해 설명하는 방법입니다.

```
SWITCH(config-rmonevent[1])# description This event ..  
SWITCH(config-rmonevent[1])#
```

(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	RMON	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	RMON	로그와 트랩 타입의 Event 둘 다 지정합니다.
type none		Event를 공지하지 않습니다.

(5) Event 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...
(종략)
!
rmon-event 1
  owner dasan
  community password
  description This event ...
  type log-and-trap
  active
(종략)
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 Event를 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.



참 고

RMON Event의 *number*는 <1 – 65, 535> 사이에서 설정 가능합니다.

다음은 1번 RMON Event를 삭제하는 경우의 예입니다.

```
SWITCH(config)# no rmon-event 1  
SWITCH(config)#
```

7.5 Syslog 설정

Syslog는 사용자의 스위치에서 발생하는 오류 등의 정보를 관리자에게 메시지를 통해 알려주는 역할을 합니다. V2824에는 기본적으로 System Logger(Syslog) 기능이 설정되어 있습니다. 따라서 이 기능을 해제한다고 해도 스위치를 다시 부팅하면 다시 설정된 상태로 되돌아가게 됩니다.

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 지정
- 원격에서 Debug 메시지 확인하기
- CPU 사용량 임계값 설정
- CPU 처리 패킷수 임계값 설정
- 포트 트래픽 임계값 설정
- Fan 임계값 설정
- 온도 임계값 설정
- 메모리량 임계값 설정
- 오류! 참조 원본을 찾을 수 없습니다.**

7.5.1 Syslog 메시지 Level 설정

V2824의 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>		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>		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 V2824 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

V2824는 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 kern syslog user} {emerg alert crit err warning notice info} console</code>		사용자가 선택한 Priority에 해당하는 Syslog 메시지만 콘솔로 전송합니다.
<code>syslog output priority {auth authpriv kern syslog user} {emerg alert crit err warning notice info} local {volatile non-volatile}</code>	Global	사용자가 선택한 Priority에 해당하는 Syslog 메시지만 시스템 내부로 전송합니다.
<code>syslog output priority {{auth authpriv kern syslog user} {emerg alert crit err warning notice info} remote ip-address</code>		사용자가 선택한 Priority에 해당하는 Syslog 메시지만 원격으로 전송합니다.

V2824에서 선택할 수 있는 priority는 auth, authpriv, kern, syslog, user가 있습니다.

한편, V2824는 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 syslog user} {emerg alert crit err warning notice info } console</code>		
<code>syslog output priority {local0 local1 local2 local3 local4 local5 local6 local7 syslog user} {emerg alert crit err warning notice info } 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 syslog user} {emerg alert crit err warning notice info } remote ip-address</code>		

한편, Syslog 메시지의 Priority를 해제하려면 다음 명령어를 이용하십시오.

명령어	모 드	기 능
no syslog output priority {auth authpriv kern local <0 – 7> syslog user} {emerg alert crit err warning notice info} console		
no syslog output priority {auth authpriv kern local <0 – 7> syslog user} {emerg alert crit err warning notice info} local {volatile non-volatile}	Global	사용자 정의 Syslog 메시지와 메시지 전송 장소 등의 내용을 해제합니다.
no syslog output priority {auth authpriv kern local <0 – 7> syslog user} {emerg alert crit err warning notice info} remote ip-address		

[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)#

```

[설정 예제 2]

다음은 원격으로 전송되는 모든 Syslog 메시지의 Priority를 local0으로 변환하기 위한 설정입니다.

```
SWITCH(config)# syslog output err remote 10.1.1.1
SWITCH(config)# syslog local-code 0
SWITCH(config)# show syslog
System logger on running!

info          local volatile
info          local non-volatile
err           remote 10.1.1.1
local_code    0
SWITCH(config)#

```

7.5.4 Syslog 해제

Syslog를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no syslog	Global	Syslog를 해제합니다.

System logger의 기능은 장비를 부팅하면 기본적으로 활성화 상태이기 때문에 다음 명령어는 syslog를 해제하지 않은 상태에서는 의미가 없습니다.

“**no syslog**”로 syslog를 해제한 이후, 다시 이를 복귀하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
syslog start	Global	해제 했던 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 local {volatile non-volatile} reverse		syslog 메시지를 가장 최근 것부터 차례대로 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}	Enable/Global/Bridge	Syslog 파일에 저장된 로그 메시지를 삭제합니다.

한편, Syslog 상태 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show syslog status	Enable/Global/Bridge	Syslog 상태 정보를 확인합니다.

7.5.6 Syslog 메시지 IP 주소 지정

V2824는 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	Global	원격으로 내보내는 Syslog 메시지에 IP 주소를 지정합니다.
no syslog bind-address		원격으로 내보내는 Syslog 메시지에 설정될 IP 주소를 해제합니다.

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 V2824는 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	기 능
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	기 능
no terminal monitor	Enable	원격 접속자가 자신의 Console 창에서 Debug 메시지를 확인할 수 있도록 하는 것을 해제합니다.

7.5.8 CPU 사용량 임계값 설정

V2824는 사용자가 CPU 사용량에 대한 임계값을 설정해 두면, CPU 사용량이 상한 임계값을 넘어섰을 때, 그리고 하한 임계값 아래로 떨어졌을 때 syslog 메시지를 통해 알려주는 기능을 가지고 있습니다. V2824에 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 사용량 임계값의 상한값을 설정합니다.
threshold cpu <21-100> {5 60 600} <20-100> {5 60 600}		사용자 장비의 CPU 사용량 임계값의 상한값과 하한값을 함께 설정합니다.



참 고

임계값의 단위는 "%"입니다. 상한값은 21%부터 100%까지 설정할 수 있고, 하한값은 20%부터 100%까지 설정 가능합니다.

참 고

V2824는 CPU 사용량 임계값이 기본적으로 상한값은 70%, 하한값은 30%로 설정되어 있습니다.

참 고

시간 간격은 5초, 60초, 600초로 설정할 수 있습니다. 기본적으로 60초로 설정되어 있습니다.

사용자가 설정한 CPU 사용량 임계값을 기본값으로 되돌리려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no threshold cpu	Global	사용자가 설정한 CPU 사용량 임계값을 기본값으로 되돌립니다.

사용자가 설정한 CPU 사용량 임계값을 확인하려면 다음 명령어를 사용하십시오.

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

다음은 사용자 장비의 CPU 사용량 임계값의 상한값을 80%로 설정하고, 그 내용을 확인하는 경우입니다.

```
SWITCH(config)# threshold cpu 80 60 40 600
SWITCH(config)# show cpupload
-----
Average CPU load
-----
 5 sec: 3.04( 0.42) %
 1 min: 3.04( 0.41) %
10 min: 4.44( 0.41) %

cpupload threshold (high) : 80
timer interval (high) : 60
cpupload threshold (low) : 40
timer interval (low) : 600
SWITCH(config)#

```

7.5.9 CPU 처리 패킷수 임계값 설정

V2824는 CPU에 의해 처리된 패킷수가 특정한 값을 초과했을 때 Syslog 메시지로 알리도록 설정할 수 있습니다. 이러한 기능은 장비 관리자가 스위치와 네트워크 상태를 더욱 효과적으로 관리할 수 있도록 해줍니다.

CPU에 의해 처리되는 패킷수가 지정된 값을 넘으면 Syslog 메시지를 보내어 알리도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
cpu statistics-limit {unicast multicast broadcast} PORTS <10-100>	Global	CPU에 의해 처리되는 패킷 수가 지정된 값을 넘으면 Syslog 메시지를 보내도록 설정합니다.



사용자가 지정하는 패킷 수의 단위는 1,000입니다. 따라서 10으로 설정하면 실제로 설정되는 값은 10,000이 되는 것입니다.

CPU가 처리하는 패킷 수에 따라 Syslog 메시지를 사용하도록 설정한 것을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no cpu statistics-limit {unicast multicast broadcast all} {PORTS all}	Global	CPU에 의해 처리되는 패킷 수가 지정된 값을 넘으면 Syslog 메시지를 보내도록 설정한 것을 해제합니다.

CPU에 의해 처리된 패킷의 수가 지정된 값을 넘으면 Syslog 메시지를 보내도록 설정한 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show cpu statistics-limit	Enable/Global/Bridge	CPU에 의해 처리된 패킷의 수가 지정된 값을 넘으면 Syslog 메시지를 보내도록 설정한 내용을 확인합니다.

7.5.10 포트 트래픽 임계값 설정

V2824는 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.

V2824의 각 포트에 트래픽 임계값을 설정하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
threshold port port-number range {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.

사용자가 설정한 포트 트래픽 임계값을 기본값으로 되돌리려면 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/Bridge	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)# show port threshold
-----
port | current(Kbps) | threshold(Kbps) | interval(sec) | mode
-----
1      0            500             5           rx
SWITCH(config)#

```

7.5.11 Fan 임계값 설정

V2824는 일정한 온도가 되면 Fan의 동작을 시작하거나 멈추도록 설정할 수 있습니다. 다음 명령어를 사용하여 Fan이 동작을 시작하는 온도와 동작을 멈추는 온도를 설정하십시오.

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



참 고

기본적으로 Fan이 동작을 시작하는 온도는 20°C, 동작을 멈추는 온도는 5°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.

FAN이 동작을 시작하는 온도와 멈추게 하는 온도를 기본값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no threshold fan	Global	FAN이 동작을 시작하는 온도와 멈추게 되는 온도를 기본값으로 되돌립니다.

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

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



출력되는 Fan status는 RUN / STOP / FAIL 상태를 가집니다.

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 1 status : RUN
Fan 2 status : RUN
Fan 3 status : RUN
Fan operation : ON
Fan threshold : Run 25 C / Stop 5 C

SWITCH(config)#{
```

7.5.12 온도 임계값 설정

V2824는 장비 온도에 대한 임계값을 설정해 두면, 장비 온도가 상한 임계값을 넘어섰을 때, 그리고 다시 하한 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.



기본적으로 장비 온도 임계값은 상한값이 80°C, 하한값이 -20°C로 설정되어 있습니다.

장비 온도 임계값을 기본값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no threshold temp	Global	장비 온도 임계값을 기본값으로 되돌립니다.

장비 온도 상태와 장비 온도 임계값을 확인하려면 다음 명령어를 사용하십시오.

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

다음은 장비 온도 상한 임계값을 65°C, 하한 임계값을 -10°C로 설정하고 그 내용을 확인한 경우의 예입니다.

```
SWITCH(config)# threshold temp 65 -10
SWITCH(config)# show status temp

Temperature 1 current : 36 C
Temperature Threshold : High (80 C) Low (-20 C)

SWITCH(config)#{
```

7.5.13 메모리량 임계값 설정

V2824는 사용하지 않는 메모리량 임계값을 설정하여 장비에서 사용되는 않는 메모리량이 임계값보다 작아지면 Syslog 메시지를 통해 알려주고, 다시 사용되지 않는 메모리량이 임계값보다 커져도 Syslog 메시지를 통해 알려주도록 할 수 있습니다. 사용하지 않는 메모리량 임계값을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
threshold memory <20-100>	Global	사용자 장비의 사용하지 않는 메모리량 임계값을 설정합니다.

사용하지 않는 메모리량 임계값을 기본값으로 되돌리려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no threshold memory	Global	사용자 장비의 사용하지 않는 메모리량 임계값을 기본값으로 되돌립니다.

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

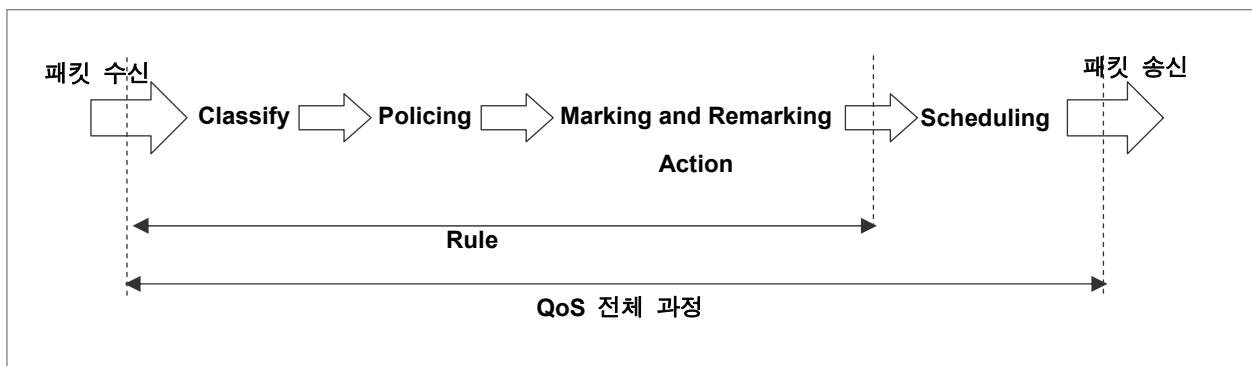
다산이 제공하는 QoS는 중요도가 가장 높은 데이터나 음성 데이터가 우선 처리되도록 대역폭을 보장하고 지연 시간을 최소화 시킵니다. 나머지 일반 데이터는 우선 순위가 높은 데이터를 먼저 처리하고 난 후 시간 순서대로 차례로 처리합니다.

한편, QoS 설정에서 주의해야 할 것은 사용자가 설정한 우선 순위가 높은 패킷으로 인해 다른 패킷들의 전송이 실패하는 일이 없어야 한다는 점입니다.

7.6.1 QoS 동작 원리

V2824의 QoS가 이루어지는 과정을 간단히 설명하면 다음과 같습니다. 사용자가 장비에 전송된 패킷을 분류(Classify)하기 위한 조건과 패킷에 대한 정책(Policing)을 설정하고, 패킷 처리 방법을 적용하면, 특정 패킷이 사용자의 설정에 따라 처리됩니다. 그리고, 이렇게 처리된 패킷은 사용자가 설정한 스케줄링(Scheduling) 방법에 따라 외부에 전송됩니다.

다음은 QoS의 동작 구조를 간단히 나타낸 그림입니다.



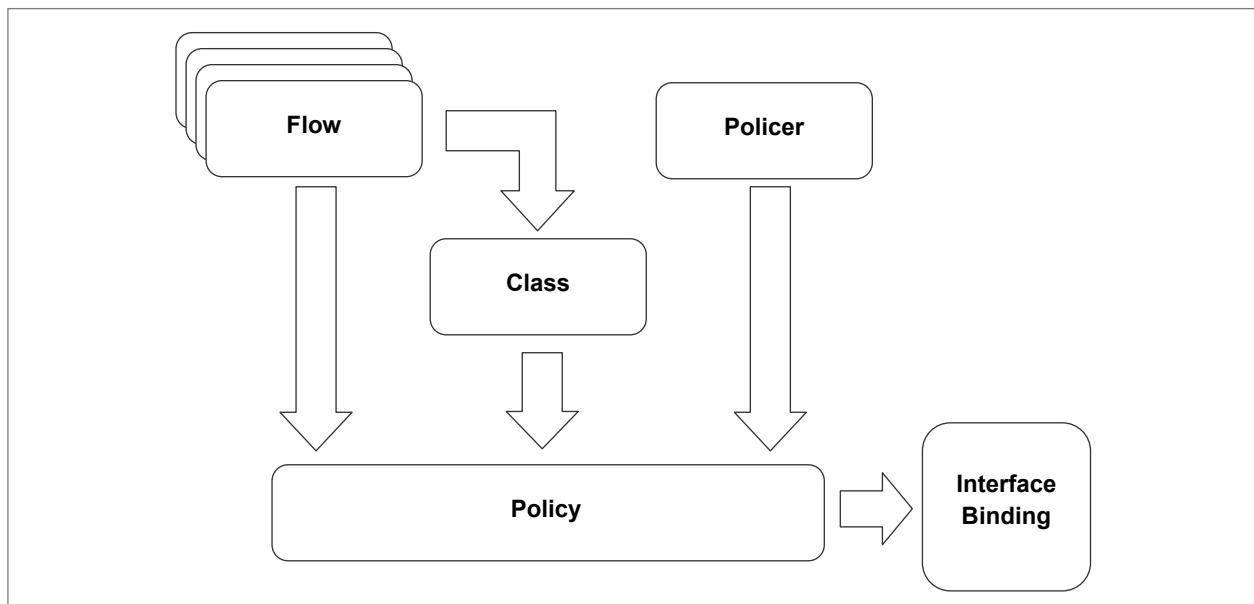
【 그림 7-4 】 QoS의 동작 구조

QoS 과정에서 패킷을 분류하고, 패킷을 처리하는 일부 과정은 Rule이라는 기능을 통해 이루어집니다. Rule은 다양한 설정 내용을 하나의 규칙으로 묶어 한번에 실행할 수 있도록 도와주기 때문에 편리합니다.

Rule의 기본 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, Policer를 필요에 따라 선택하고, 패킷의 Action을 결정하거나 우선 순위를 결정하는 다양한 값을 설정 및 재조정(Marking/Remarking) 할 수 있습니다.

Rule의 기본 구조를 이루는 Flow, Class, Policer, Policy의 관계는 아래 그림과 같습니다.



【 그림 7-5 】 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 Policer는 하나의 Policy에만 포함이 가능합니다.

V2824에서 Policy를 설정하여 실제로 동작하게 되는 Rule은 약 1천 개 정도가 지원됩니다.

7.6.2 패킷 분류(Classify) 설정

V2824은 Rule을 적용할 패킷을 분류하는 조건을 Flow로 만들어 설정하고, 복수의 Flow를 관리할 때에는 Class를 활용하도록 되어 있습니다.

(1) Flow 모드 설정

V2824의 Flow는 default와 extension의 2가지 모드를 지원합니다. Default 모드는 장비에서 지원하는 최대 1,024개의 Flow를 설정할 수 있으나 NetBIOS Filtering 등 일부 기능을 설정할 수 없는 제약이 따릅니다. 한편, Extension 모드는 특별한 기능 상의 제약은 없으나 설정할 수 있는 Flow의 최대 개수가 512개로 줄어듭니다.

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.

(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, Ethertype, CoS, DSCP 등이 있습니다.

MAC 주소를 기준으로 패킷을 분류하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>mac {src-mac-address src-mac-address/mask any} {dst-mac-address dst-mac-address/mask any}</code>	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
<code>ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any}</code>	Flow	설정한 Source IP 주소와 Destination IP 주소에 해당하는 패킷을 분류합니다.
<code>ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} <0-255></code>		설정한 IP 주소와 해당 프로토콜에 해당하는 패킷을 분류합니다.
<code>ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} {icmp tcp udp}</code>		설정한 IP 주소와 ICMP의 Message type, Code 값에 해당하는 패킷을 분류합니다.
<code>ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} icmp <0-255> any {<0-255> any}</code>		설정한 IP 주소와 TCP 포트에 해당하는 패킷을 분류합니다.
<code>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]</code>		설정한 IP 주소와 UDP 포트에 해당하는 패킷을 분류합니다.
<code>ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} udp <1-65535> any {<1-65535> any}</code>		

IP ToS precedence, CoS, ToS, DSCP, Ethertype, 패킷 길이, IP-Header 등을 기준으로 패킷을 분류하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip-precedence {<0-7> any}	Flow	설정한 IP TOS precedence에 해당하는 패킷을 분류합니다.
cos {<0-7> any}		설정한 CoS 값에 해당하는 패킷을 분류합니다.
tos {<0-255> any}		설정한 ToS 값에 해당하는 패킷을 분류합니다.
dscp {<0-63> any}		설정한 DSCP 값에 해당하는 패킷을 분류합니다.
ethertype {ethertype arp any}		설정한 Ethertype에 해당하는 패킷을 분류합니다.
length {<21-65 535> any}		설정한 패킷 길이에 해당하는 패킷을 분류합니다.



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	Flow	Flow에 설정한 패킷 분류 조건을 삭제합니다.
no dscp		
no ethertype		
no ip		
no ip-precedence		
no length		
no mac		
no tos		

(2) 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.

(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 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 해 주는 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	Policer를 생성하고 Policer 설정 모드로 들어갑니다.

Policer에 설정하는 패킷 정책들의 내용은 Metering과 Rate-limit, Counter 등이 있습니다.

한편, 설정했던 Policer를 삭제하려면, 다음 명령어를 사용하십시오.

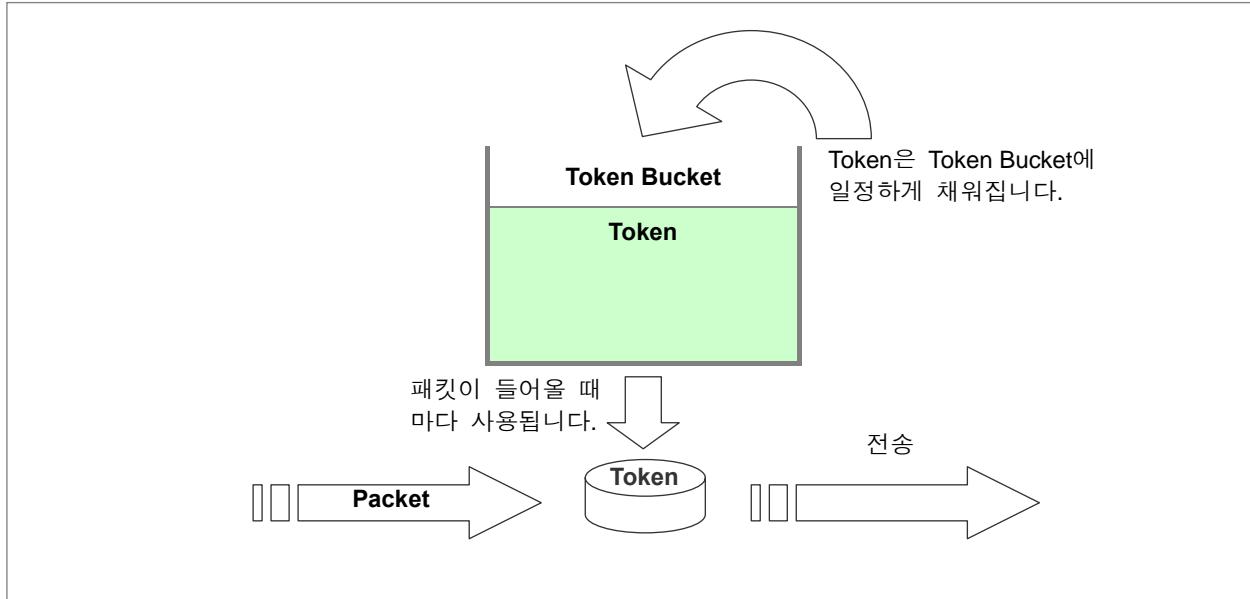
명령어	모 드	기 능
no policer policer-name	Global	생성했던 해당 Policer를 삭제합니다.
no policer all		모든 Policer를 삭제합니다.

(2) Metering

V2824 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

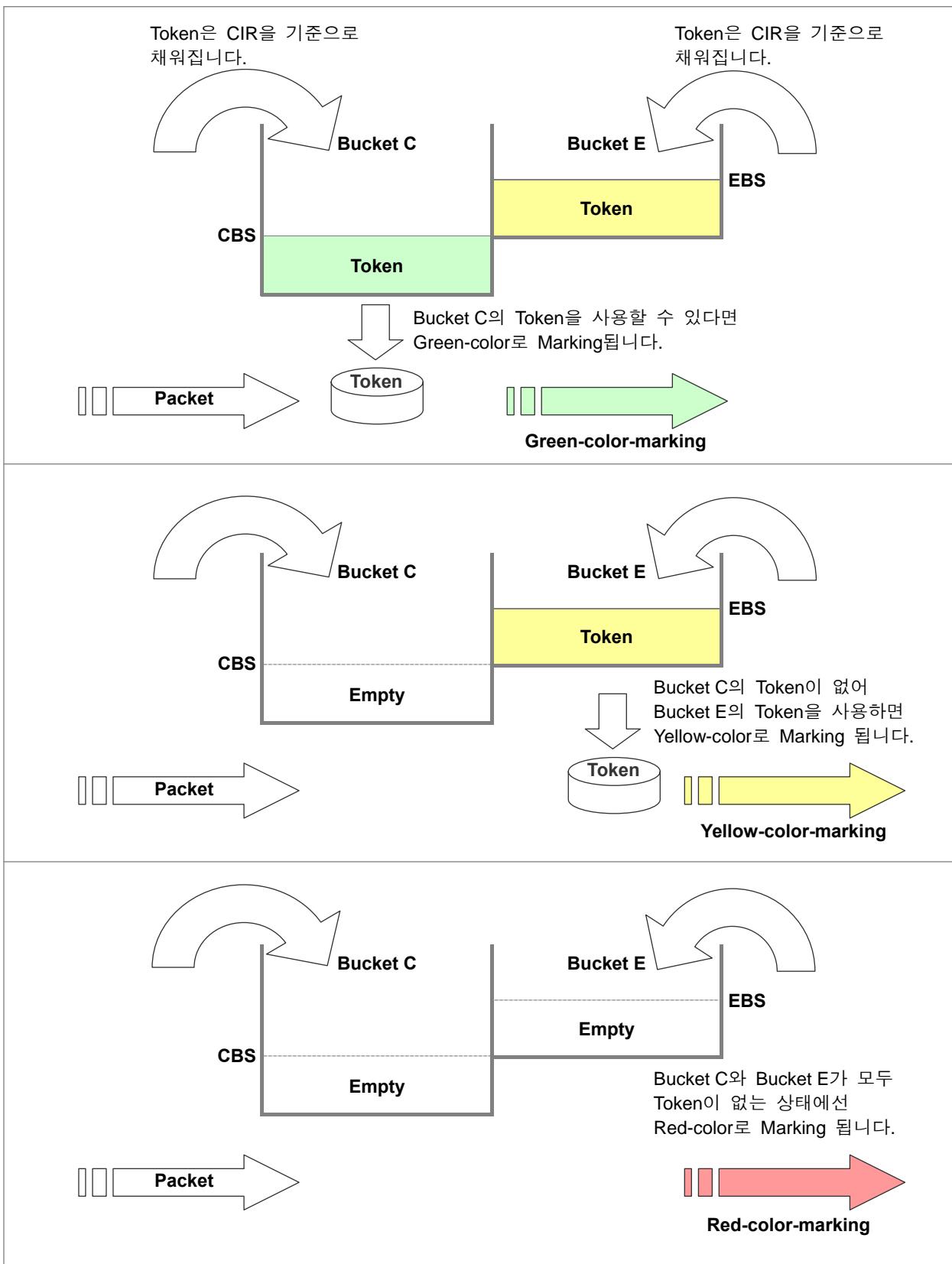
Token Bucket 방식이란, 우리가 일상 생활에서 특정한 목적지에 도착하기 위해 대중 교통을 이용할 때 요금을 내듯이, Token이 있어야만 패킷 전송이 가능하도록 하는 것입니다. Token Bucket에 Token은 일정하게 계속해서 채워지고, 패킷이 들어올 때마다 Token이 사용되기 때문에 패킷이 폭주하여 Token이 바닥나면 다시 Token이 채워질 때까지 패킷을 전송할 수 없게 됩니다.



【 그림 7-6 】 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.



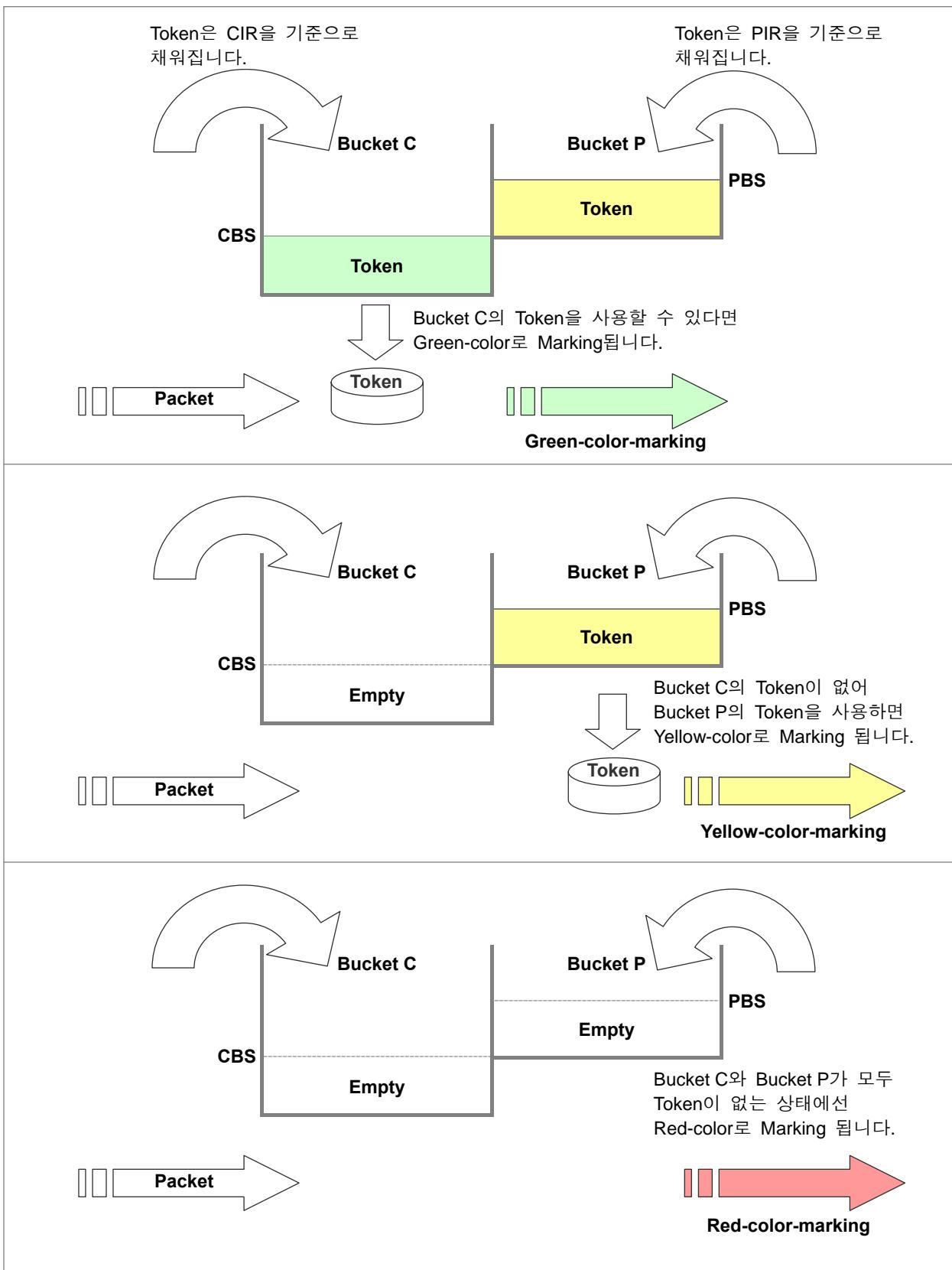
【 그림 7-7 】 Single Rate Three Color Marker의 Color Marking

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 7-8 】 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.



참 고

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}]	Policer	Red 또는 yellow-color가 marking된 패킷을 remarking 하도록 설정합니다.

(3) 패킷 Counter

V2824은 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.



주의

V2824은 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.

V2824 Policy Counter를 초기화 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear policy counter {policer-name all}	Enable/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 policer statistics		Policer의 Count 개수를 확인합니다.
show policy statistics		Policy의 Count 개수를 확인합니다.

(4) 패킷 Rate-limit

V2824은 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-limit의 설정 단위는 Kbps입니다.

(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.



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.



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 policy-name	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.

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	모 드	기 능
action match copy-to-cpu	Policy	분류된 패킷을 CPU로 옮겨보냅니다.
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.



주 의

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		
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		
	Policy	Rule에 해당하는 패킷의 처리 방법을 설정했던 것을 해제합니다.

(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 overwrite		Rule에 해당하는 패킷에 CoS 값을 IP ToS precedence 값으로 지정합니다.
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 값으로 지정합니다.

위에서 설정한 것을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no action match cos [overwrite]	Policy	
no action match cos same-as-tos overwrite		
no action match ip-precedence		Rule에 해당하는 패킷에 CoS 또는 IP ToS precedence 값을 부여했던 것을 해제합니다.
no action match ip-precedence same-as-cos		

(5) Rule 적용 인터페이스 지정

V2824에서 Classify와 Policing, Rule 동작에 대한 설정이 끝났다면, 해당 Rule을 적용할 인페이스를 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 {src-port-number any}	Policy	해당 포트로 들어오는 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 [src-port-number]	Policy	Rule을 적용할 인터페이스를 지정했던 것을 해제합니다.
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]	View/Enable/ Global/Bridge	설정한 Rule의 내용을 확인합니다.
show {flow class policer policy} detail [name]		

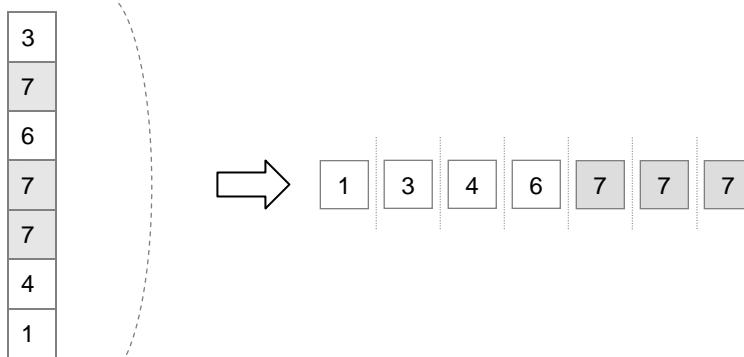
7.6.6 스케줄링(Scheduling) 설정

사용자가 설정한 Rule에 따라 처리된 패킷은 최종적으로 스케줄링(Scheduling) 단계를 거쳐 외부로 전송됩니다. V2824은 Queue를 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 말하면, 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

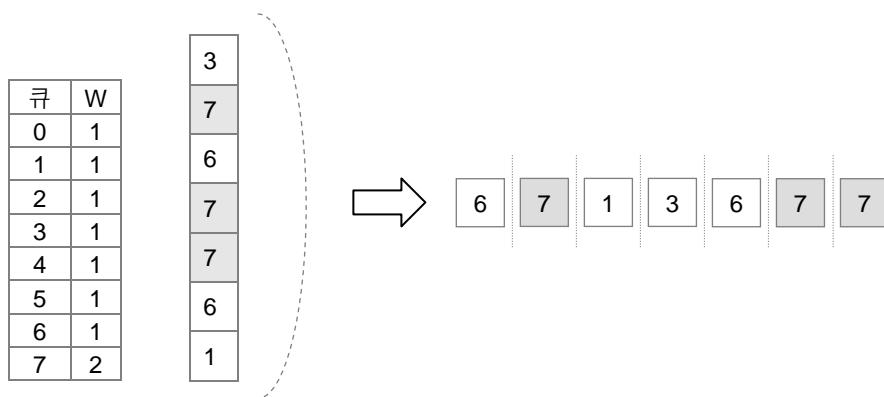


【 그림 7-9 】 Strict Priority Queuing에서의 패킷 처리

- **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 7-10 】 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.

(1) 스케줄링 방식 설정

세 가지 스케줄링 방식 가운데 어떤 방식을 사용할지 선택하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
qos scheduling-mode {sp wrr drr} port-number	Global	스케줄링 방식을 선택합니다.



V2824는 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.



V2824는 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 Queuing 으로 진행합니다.



queue-number 는 <0-3>, *quantum-value*는 <1-127> 범위 내에서 입력합니다.



V2824는 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-bandwidth라고 합니다.



V2824는 기본적으로 모든 큐의 최소 보장 대역폭이 “0”으로 설정되어 있습니다.

보장 대역폭을 설정하려면 다음 명령어를 사용하십시오.

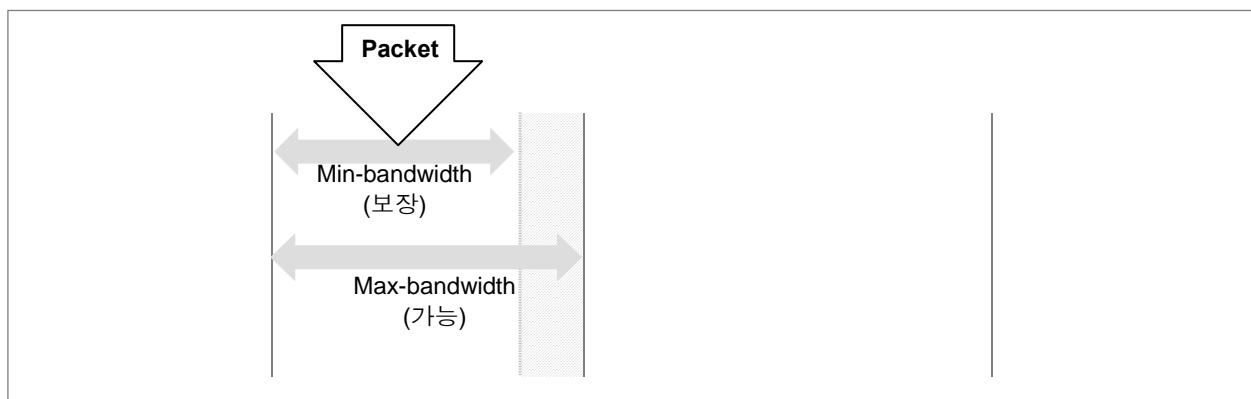
명령어	모 드	기 능
qos min-bandwidth port-number <0-3> <1-100>	Global	보장 대역폭을 설정합니다.
qos min-bandwidth port-number <0-3> unlimited		보장 대역폭을 제한하지 않습니다.



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 7-11 】 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 <0-3> <1-100>	Global	최대 사용 가능한 대역폭을 설정합니다.
qos max-bandwidth port-number unlimited		최대 사용 가능한 대역폭에 제한을 없앱니다.



V2824는 기본적으로 사용 가능한 대역폭에 제한을 두고 있지 않습니다.



SP 방식이나 WRR 방식을 선택한 상태에서는 가능 대역폭을 설정할 수 없습니다.

(5) 특정 포트의 트래픽 제한 설정

V2824에서는 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.



버퍼 크기를 제한하는 단위는 Kbit입니다.



V2824에는 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>	Global	송신 포트로 지정된 특정 포트의 Queue에서 사용하는 버퍼 크기를 제한합니다. 장비의 기본값은 24Kbit로 설정되어 있습니다.

**참 고**

*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	Enable/Global/Brdige	송신 포트 및 수신 포트의 트래픽 제한 정보를 확인합니다.

(6) CPU 패킷에 대한 사용자 정의

V2824는 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/	QoS 스케줄링에 대한 설정 내용을 확인합니다.
show qos port-number	Bridge	포트별로 QoS 스케줄링에 대한 설정 내용을 확인합니다.
show qos cpu		CPU 패킷에 대한 QoS 설정 내용을 확인합니다.

(8) 포트별 Queue 트래픽 확인

V2824는 포트별 Queue의 트래픽 양을 확인할 수 있습니다. 포트별로 각각의 Queue에 해당하는 트래픽이 얼마나 되는지 확인하려면, 다음 명령어를 사용하십시오.

명령어	Mode	기능
show queue status port-number [0-3]	Enable/Global/ Bridge	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 V2824에서는 스위치에 연결된 장비에 패킷이 포워딩 되기 전에 필터링을 수행할 수 있는 기능을 지원합니다. 스위치 자체로 들어오는 Telnet, FTP, ICMP, SNMP 등 의 서비스 접속을 막을 때에는 Admin Rule이라는 기능이 사용됩니다.

7.6.8 Admin Rule 패킷 분류(Classify) 설정

V2824은 Admin Rule을 적용할 패킷을 분류하는 조건을 Flow로 만들어 설정하고, 복수의 Admin Flow를 관리할 때에는 Class를 활용하도록 되어 있습니다.

(1) Admin Flow 설정

V2824는 Admin Rule을 설정하려면 가장 먼저 Admin Flow를 생성하여 Flow 설정 모드로 들어가야 합니다. 그래야 세부적인 패킷 조건을 설정할 수 있게 됩니다. 패킷의 세부적인 조건을 정해 분류하기 위해 먼저 Admin Flow 설정 모드로 들어가려면 다음 명령어를 사용하십시오.

명령어	모드	기능
flow admin name create	Global	새로운 Admin Rule의 Admin Flow를 생성하고 Admin Flow 설정 모드로 들어갑니다.

Admin Flow 설정 모드로 들어가면 명령어의 프롬프트가 SWITCH(config)#에서 SWITCH(config-admin-flow[name])#, SWITCH(config-admin-policy[name])#으로 바뀝니다.



참 고

하나의 Admin Flow나 Policy에 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/Policy 설정 모드로 들어간 후에는 사용자가 원하는 Admin Flow/Policy를 알맞게 설정하십시오. Admin Flow/Policy에는 Admin Flow/Policy에 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
<code>ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any}</code>	Admin Flow	Source IP 주소와 Destination IP 주소 기준으로 정책을 설정합니다.
<code>ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} <0-255></code>		Source IP 주소, Destination IP 주소, 그리고 프로토콜을 기준으로 정책을 설정합니다.
<code>ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} {icmp tcp udp}</code>		ICMP의 Message type과 Code 값도 정책 기준으로 설정합니다.
<code>ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} icmp <0-255> any} <0-255> any}</code>		TCP Source 포트와 Destination 포트까지 정책 기준으로 설정합니다.
<code>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]</code>		UDP Source 포트와 Destination 포트까지 정책 기준으로 설정합니다.
<code>ip {src-ip-address src-ip-address/m any} {dst-ip-address dst-ip-address/m any} udp <1-65535> any} <1-65535> any}</code>		Source IP 주소와 Destination IP 주소 기준으로 정책을 설정합니다.
<code>ip header-length <1-15></code>		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
<code>no ip</code>	Admin Flow	Admin Flow에 설정한 패킷 분류 조건을 삭제합니다.
<code>no ip header-length</code>		

(2) Admin Flow 내용 저장 및 수정

패킷 분류 조건에 대한 설정이 마친 Admin Flow는 반드시 장비에 저장해야 합니다. 설정이 끝난 Admin Flow를 장비에 저장하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
apply	Admin Flow	Admin 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, 해당 Admin Flow의 설정 모드로 들어가야 합니다. Admin 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.



Flow의 내용을 수정한 후에도 반드시 **apply** 명령어를 사용하여 내용을 저장해야 합니다.

(3) Admin Class 설정

여러 가지 조건을 가지고 패킷을 분류하게 될 경우, 2개 이상의 Admin Flow가 필요로 할 경우가 있습니다. 이러한 경우 여러 개의 Admin Flow를 Admin Class로 묶어서 사용하면 관리하기도 쉽고, 설정도 간편해집니다. 2개 이상의 Admin Flow를 하나의 Admin 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 Admin Class를 삭제합니다.
no class admin class-name flow flow-name [flow-name] [flow-name] ...		해당 Admin Class에서 특정 Flow를 삭제합니다.

7.6.9 Admin Rule 동작 설정

패킷을 분류하도록 Admin Flow 및 Admin Class를 설정하였다면, 사용자가 필요로 하는 Admin Flow 또는 Admin Class와 Admin Policer를 선택적으로 구성하여 Admin Policy를 설정하고 Admin Rule의 동작을 실행해야 합니다.

(1) Admin 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 Policy에 포함시킵니다.
include-flow flow-name		해당 Admin Flow를 Policy에 포함시킵니다.



주의

Admin Policy에서는 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) Admin 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 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		

(3) Admin 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	Admin 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 Admin Policy의 내용을 수정하려면, 일단 수정하려는 Policy의 설정 모드로 들어가야 합니다. 이미 생성되어 있는 Admin Policy 중 수정하고자 하는 Admin Policy의 설정 모드로 들어가려면, 다음 명령어를 사용하십시오.

명령어		모 드	기 능
policy	admin <i>policy-name</i>	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.

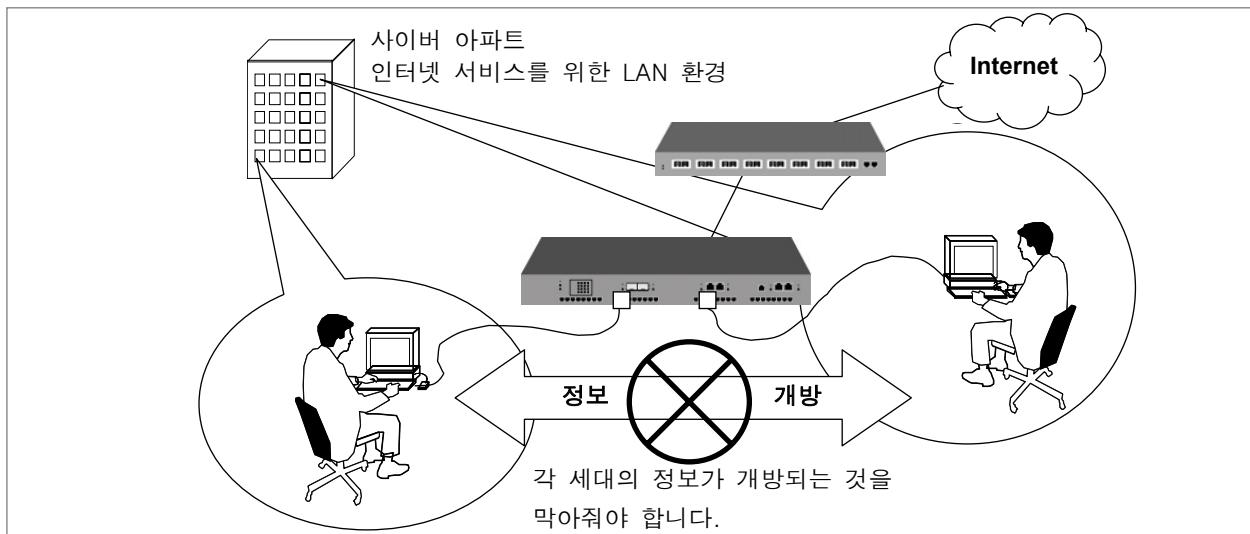
명령어	모 드	기 능
show flow-profile admin	Admin Flow	해당 Flow의 Admin Profile을 확인합니다.
show policy-profile admin	Admin Policy	해당 Policy의 Admin Profile을 확인합니다.

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 필터링

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 7-12 】 NetBIOS 필터링의 필요성

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	NetBIOS 필터링을 설정합니다.
<code>no netbios-filter port-number</code>		NetBIOS 필터링을 해제합니다.
<code>show netbios-filter</code>	Enable / Global / Bridge	NetBIOS 필터링 설정 내용을 확인합니다.



*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.

다음은 1번부터 5번까지의 포트에 NetBIOS 필터링을 설정하고 그 내용을 확인한 경우입니다.

```
SWITCH(bridge)# netbios-filter 1-5
SWITCH(bridge)# show netbios-filter
o:enable .:disable
-----
1          2
12345678901234567890123456
-----
oooooo.....
-----
SWITCH(bridge)#

```

7.8 MAC 필터링

사용자의 장비는 별다른 성능 저하 없이 최대 8,192개의 MAC 주소를 등록하여 프레임 전송 제한에 참고합니다.

7.8.1 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.

MAC 필터링을 설정할 때에는 모든 MAC 주소의 패킷을 차단하도록 설정한 후, 특정 MAC 주소의 패킷을 받아들이도록 설정을 추가해 나가는 것이 편리합니다. 시스템에서 제공하는 기본적인 필터링 정책은 각 포트마다 모든 패킷을 허용하는 것으로 설정되어 있습니다.

명령어	모 드	기 능
mac-filter default-policy {deny permit} port-number	Bridge	해당 포트에 기본 정책을 설정합니다.



*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.



주 의

MAC 필터링 기본 정책은 삭제 또는 해제되지 않습니다.

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.

7.8.2 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] [port-number]	Bridge	해당 MAC 주소의 패킷을 허용 또는 차단합니다.



참 고

변수 *mac-address*는 12개의 16 진수로 이루어졌는데 **show mac** 명령어로 확인할 수 있습니다.

00:d0:cb:06:01:32 는 MAC 주소의 한 예입니다.



참 고

*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.



참 고

MAC 필터 정책은 사용자가 최근에 설정한 것이 1번으로 기록됩니다. 지정한 개수 만큼의 필터 정책을 보여줄 때에는 테이블의 기록된 순서를 기준으로 보여줍니다.

7.8.3 MAC 필터 정책 삭제

특정 MAC 주소에 대해 설정했던 필터링 정책을 삭제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
mac-filter del mac-address [vlan-id]	Bridge	특정 MAC 필터 정책을 삭제합니다.
no mac-filter		모든 MAC 필터 정책을 삭제합니다.



MAC 필터링 기본 정책은 위 명령어로 삭제할 수 없습니다.

7.8.4 MAC 필터 정책 확인

특정 MAC 주소에 대해 설정했던 필터링 정책을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show mac-filter		MAC 필터 정책을 확인합니다.
show mac-filter numbers	Enable/ Global/	MAC 필터 정책을 숫자만큼 제한해서 보여줍니다.
show mac-filter numbers start-mac-address	Bridge	MAC 주소에 따라 MAC 필터 정책을 숫자만큼 제한해서 보여줍니다. .

7.8.5 MAC 필터링 정책 목록 불러오기

MAC 필터링 정책을 많이 만들어야 하는 상황에서는, 각각의 MAC별로 정책을 등록하는 것보다 이미 만들어진 정책 목록을 불러오는 방법이 효율적입니다.

다음 방법에 따라 MAC 필터링 정책 목록을 V2824에 적용시키십시오.



장비에 새로운 MAC 필터링 정책 목록을 적용되기 위해서는, 먼저 **no mac-filter** 명령어로 기존에 설정되어 있는 MAC 필터링 정책이 삭제되어야 합니다.

1 단계 Enable 모드에서 **quote sh -l** 명령어로 DSH에서 KSH로 들어갑니다.

```
SWITCH# quote sh -l
```

2 단계 `vi mfdb.conf` 명령어로 MAC 필터링 정책 목록인 `mfdb.conf` 파일을 편집기로 불러 들입니다. 이 파일은 `/etc` 디렉토리 안에 저장됩니다.

3 단계 `mac-address {deny | permit} {vlan-id | any} port-number` 명령어로 각각의 MAC 정책을 설정하십시오.

```
00:0e:e8:8c:c8:48 permit any 16  
00:0e:e8:8c:c8:44 permit any 16  
00:0e:e8:8c:c8:45 permit any 16  
00:0e:e8:8c:c8:46 permit any 16  
00:0e:e8:8c:c8:42 permit any 16
```



주 의

반드시 *port-number*까지 지정해야 설정 내용이 장비에 적용됩니다.

4 단계 정책 입력이 완료된 후에는 **Esc** 키를 눌러 편집 모드를 변경하고, **:w**를 입력하여 설정 내용을 저장하고 파일 편집을 마치십시오.

5 단계 **vtysh** 명령어로 KSH에서 DSH로 들어갑니다.

```
*SWITCH# vtysh
SWITCH#
```

6 단계 **mac-filter list** 명령어로 설정한 MAC 필터 정책 목록을 장비에 적용시키십시오.

```
SWITCH# configure terminal
SWITCH(config)# brdige
SWITCH(bridge)# mac-filter list
```

7 단계 **show mac-filter** 명령어로 MAC 필터 정책 목록이 바르게 장비에 적용되었는지 확인하십시오.

```
SWITCH(bridge)# show mac-filter
=====
ID |      MAC      | ACTION | VID | PORT
=====
1  00:0e:e8:8c:c8:42  PERMIT  Any   16
2  00:0e:e8:8c:c8:44  PERMIT  Any   16
3  00:0e:e8:8c:c8:45  PERMIT  Any   16
4  00:0e:e8:8c:c8:46  PERMIT  Any   16
5  00:0e:e8:8c:c8:48  PERMIT  Any   16
SWITCH(bridge)#
=====
```

7.8.6 설정 예제

[설정 예제 1] 기본적인 패킷 정책 설정

다음은 1번부터 3번까지의 포트와 7번 포트에 기본적으로 모든 패킷을 차단하도록 설정하고, 그 내용을 확인한 경우의 예입니다.

```

SWTICH(bridge)# set mac-filter default-policy deny 1-3
SWTICH(bridge)# set mac-filter default-policy deny 7,13
SWTICH(bridge)# show mac-filter default-policy
-----
PORT POLICY | PORT POLICY
-----+-----
 1 DENY      |    2 DENY
 3 DENY      |    4 PERMIT
 5 PERMIT    |    6 PERMIT
 7 DENY      |    8 PERMIT
 9 PERMIT    |   10 PERMIT
11 PERMIT    |   12 PERMIT
13 DENY      |   14 PERMIT
15 PERMIT    |   16 PERMIT
17 PERMIT    |   18 PERMIT
19 PERMIT    |   20 PERMIT
21 PERMIT    |   22 PERMIT
23 PERMIT    |   24 PERMIT
25 PERMIT    |   26 PERMIT
SWTICH(bridge)#

```

[설정 예제 2] MAC 필터링 설정

다음은 VLAN 1의 3번 포트에 MAC 주소 00:02:a5:74:9b:17, 00:01:a7:70:01:d2에 대한 통신을 허용하도록 설정하고 필터 정책 테이블을 확인한 경우의 예입니다.

```

SWTICH(bridge)# mac-filter add 00:02:a5:74:9b:17 permit 1 3
SWTICH(bridge)# mac-filter add 00:01:a7:70:01:d2 permit 1 3
SWTICH(bridge)# show mac-filter
=====
ID |      MAC      | ACTION | VID | PORT
=====
 1 00:01:a7:70:01:d2  PERMIT   1  3
 2 00:02:a5:74:9b:17  PERMIT   1  3

```

한편, 다음은 위의 설정에서 필터 정책을 한 개만 확인한 경우의 예입니다.

```

SWTICH(bridge)# show mac-filter 1
=====
ID |      MAC      | ACTION
=====
 1 00:01:a7:70:01:d2  PERMIT
SWTICH(bridge)#

```

[설정 예제 3] MAC 필터링 정책 삭제

다음은 위에서 설정했던 MAC 주소 00:02:a5:74:9b:17에 대한 정책을 삭제하는 경우입니다.

```
SWITCH(bridge)# mac-filter del 00:02:a5:74:9b:17
SWITCH(bridge)#{
```

7.9 Martian Filter 통계 확인

V2824는 같은 네트워크 안에서 다른 Source IP 주소를 가지고 외부로 나가려는 패킷을 막을 수 있는 Martian Filter를 지원합니다. Martian Filter를 사용하면 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.

Martian Filter가 동작한 회수에 대한 통계 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip martian-filter counter [interface-name]		Martian Filter 관련 통계 정보를 확인합니다.
clear ip martian-filter counter {interface-name all }	Golbal	특정 인터페이스 또는 모든 인터페이스의 Martian Filter 관련 통계 정보를 삭제합니다.

7.10 접속가능 사용자수 제한

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 Learning 될 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 설정하시려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
max-new-hosts <i>port-number max-mac-number</i>	Bridge	1초동안 포트에 Learning될 수 있는 MAC 갯수를 설정합니다.
max-new-hosts system <i>max-mac-number</i>		1초동안 시스템에 Learning될 수 있는 MAC 갯수를 설정합니다.



주의

카운트 된 MAC이 1초가 지나기 전에 사라졌다가 다시 Learning될 때에는 카운트 하지 않습니다.



주의

같은 MAC이 포트를 이동한 경우에는, 다시 카운트 하지 않습니다. 다시 말해 1번 포트에서 Learning된 MAC이 2번 포트에서 Learning되는 경우에는, 포트를 이동했다고 간주하여 1번 포트에서는 삭제하고 2번 포트에서 Learning하지만, 카운트는 하지 않습니다.

설정한 Max-new-hosts를 삭제하시려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no max-new-hosts [<i>port-number</i>]	Bridge	1초동안 포트에 Learning될 수 있는 MAC 갯수를 삭제합니다.
no max-new-hosts system		1초동안 시스템에 Learning될 수 있는 MAC 갯수를 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.

[설정 예제 1]

다음은 1초 동안 시스템에 Learning될 수 있는 MAC 갯수를 10개로 제한하고, 1번부터 10번까지의 포트에 각각 1초 동안 Learning될 수 있는 MAC 갯수를 3개로 제한하는 경우입니다.

```
SWITCH(bridge)# max-new-hosts system 10
SWITCH(bridge)# max-new-hosts 1-10 3
SWITCH(bridge)# show max-new-hosts
System : 10

port 1 : 3
port 2 : 3
port 3 : 3
port 4 : 3
port 5 : 3
port 6 : 3
port 7 : 3
port 8 : 3
port 9 : 3
port 10 : 3
port 11 : Unlimited
port 12 : Unlimited
port 13 : Unlimited
port 14 : Unlimited
port 15 : Unlimited
port 16 : Unlimited
port 17 : Unlimited
port 18 : Unlimited
port 19 : Unlimited
port 20 : Unlimited
port 21 : Unlimited
port 22 : Unlimited
port 23 : Unlimited
port 24 : Unlimited
port 25 : Unlimited
(종략)
SWITCH(bridge)#

```

위와 같이 설정하였을 때 발생할 수 있는 경우의 예를 들어 봅시다.

1번부터 10번까지의 포트에 각각 1개씩 MAC이 Learning된 후 11번째 MAC이 Learning되려고 하면, 이미 전체 시스템에 1초 동안 Learning될 수 있는 MAC의 갯수를 초과했기 때문에 제한됩니다. 물론, 1초 동안 1번 포트에만 4개의 MAC이 Learning되면, 4번째 MAC은 제한됩니다.

7.11 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 설정한 주소로 장비가 재 부팅해도 테이블에 그대로 남아 있는 주소입니다. MAC 테이블에 static 주소를 입력하려면, Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
mac bridge-name port-number mac-address	Bridge	MAC 주소, Bridge 이름, 그리고 포트 번호를 입력합니다.
show mac bridge-name port-number	Enable /Global/Bridge	사용자가 등록한 MAC 주소를 확인합니다.

다음 명령어는 MAC 주소를 테이블에 등록하는 경우의 예입니다.

```
SWITCH(bridge)# mac default 00:01:02:9a:61:1a
SWITCH(bridge)#{
```

다음은 목적지 MAC 주소, 해당 포트 번호, VLAN ID, 그리고 테이블에 등록되어 있는 시간값 등을 보여주는 예입니다.

```
SWITCH(bridge)# show mac 1 24
port (id)      mac addr          permission    in use
eth24(24)      00:01:02:9a:61:1a  static        0.00
eth24(24)      00:10:5a:84:46:76  OK            0.01
eth24(24)      00:e0:4c:1a:37:17  OK            0.07
eth24(24)      00:d0:cb:0a:a0:b7  OK            0.15
eth24(24)      00:c0:ca:33:5b:90  OK            0.18
(종략)
```

```
SWITCH(bridge)#{
```

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	Enable/ Global/Bridge	MAC 테이블을 초기화합니다.

7.12 ARP

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. 이때 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.

V2824의 사용자는 ARP와 관련하여 다음과 같은 설정이 가능합니다.

- ARP 테이블 설정
- ARP Inspection
- ARP-Alias 설정
- Proxy-ARP 설정
- Gratuitous ARP

7.12.1 ARP 테이블 설정

ARP 테이블의 내용은 ARP를 통해 IP 주소와 일치하는 MAC 주소를 찾았을 때 자동적으로 기록됩니다. 네트워크 관리자는 특정 IP 주소의 MAC 주소를 직접 ARP 테이블에 등록하여 네트워크 상에서 사용할 수도 있습니다.

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	Global	모든 IP 주소와 MAC 주소를 삭제합니다.
no arp ip-address [interface-name]		해당 IP 주소나 Interface 이름을 삭제합니다.
clear arp [interface-name]		ARP 테이블의 내용을 모두 삭제합니다.

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.

7.12.2 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.

ARP Inspection은 ARP 패킷에 대한 보안성을 높이기 위한 기능으로 네트워크 통신을 방해하기 위한 목적으로 전송된 ARP 패킷을 차단할 수 있습니다. ARP Inspection 기능을 이용하여 ARP 패킷을 차단하려면, 먼저 이 기능을 활성화하고 ARP 패킷에 대한 정책을 설정해야 합니다.

(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.



주의

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.



참 고

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.



참 고

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 end-ip-address mac any		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 end-ip-address mac any		
no permit ip any mac { any host mac-address }		
no permit ip host ip-address mac { any host mac-address }		
no permit ip A.B.C.D/M mac { any host mac-address }		특정 범위의 IP 주소에 대하여 ARP 패킷을 허용하도록 설정한 것을 삭제합니다.
no permit ip range start-ip-address end-ip-address mac any		



주 의

필터링을 적용한 ARP ACL을 삭제하면 해당 필터링까지 동시에 삭제됩니다.

한편, V2824는 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		DHCP 사용자에 대해 ARP 패킷을 허용하도록 설정합니다.
no permit dhcp-snoop-inspection	Arp-acl	DHCP 사용자에 대해 ARP 패킷을 허용하도록 설정한 것을 해제합니다.



참 고

ARP ACL의 설정 후 반드시 필터링을 설정하여야 ARP ACL의 설정 내용이 적용됩니다.

(3) ARP Inspection 필터링 설정

V2824는 ARP Inspection 기능을 활성화하면 기본적으로 모든 MAC 주소를 허용하도록 되어 있습니다. 따라서 허용 또는 차단할 IP 주소 범위를 ARP ACL로 지정한 후에 이를 적용하도록 설정하여야만 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 arp-acl-name vlan vlan-name		ARP 패킷 차단 기능이 동작하도록 설정합니다.
no ip arp inspection filter arp-acl-name vlan vlan-name	Global	ARP 패킷 차단 기능이 동작하도록 설정한 것을 해제합니다.



참 고

V2824는 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 port-number		해당 포트를 Trust 포트로 설정합니다.
no ip arp inspection trust port port-number	Global	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 port-number	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) 설정 내용 및 통계 확인

ARP Inspection의 설정 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip arp inspection		ARP Inspection의 설정 내용을 확인합니다.
show ip arp inspection vlan vlan-name	Global/	
show ip arp inspection statistics	Bridge	ARP Inspection의 통계 내용을 확인합니다.
show ip arp inspection statistics vlan vlan-name		

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 vlan-name	Global/Bridge	

7.12.3 ARP-Alias 설정

V2824는 장비에 등록된 IP 주소가 아니더라도 ARP 응답을 할 수 있습니다. 가입자들의 보안 유지를 위해 가입자 간의 통신이 불가능하도록 설정된 상태의 가입자망에서 집선 장비에 ARP-Alias를 등록하게 되면, 가입자 간의 ARP 통신을 집선 장비에서 대신하게 되어 마치 가입자들끼리 통신이 가능한 것처럼 보입니다.

(1) ARP-Alias 등록

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 vian vlan-ID gateway gateway-ip-address		사용자의 장비가 ARP 응답을 하도록 게이트웨이 주소와 vlan Id를 입력합니다.



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.

등록되어 있는 ARP-Alias를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show arp alias	View/ Enable/ Global	등록한 모든 ARP-Alias를 확인합니다.

(2) Aging Time 설정

ARP-Alias를 사용해 패킷을 주고 받는 스위치는 패킷이 전송될 때마다 브로드캐스팅하는 것을 막기 위해 기록합니다. 이 때 불필요한 ARP-Alias를 기록에서 삭제하는데, 일정한 시간 내에 응답이 없는 ARP-Alias를 삭제하도록 설정하는 시간을 Aging Time이라고 합니다.

이러한 Aging Time을 설정하는 명령어는 다음과 같습니다.

명령어	모 드	기 능
arp alias aging-time time	Global	ARP-Alias 기록 유지 여부를 가리는 Aging time을 설정합니다.



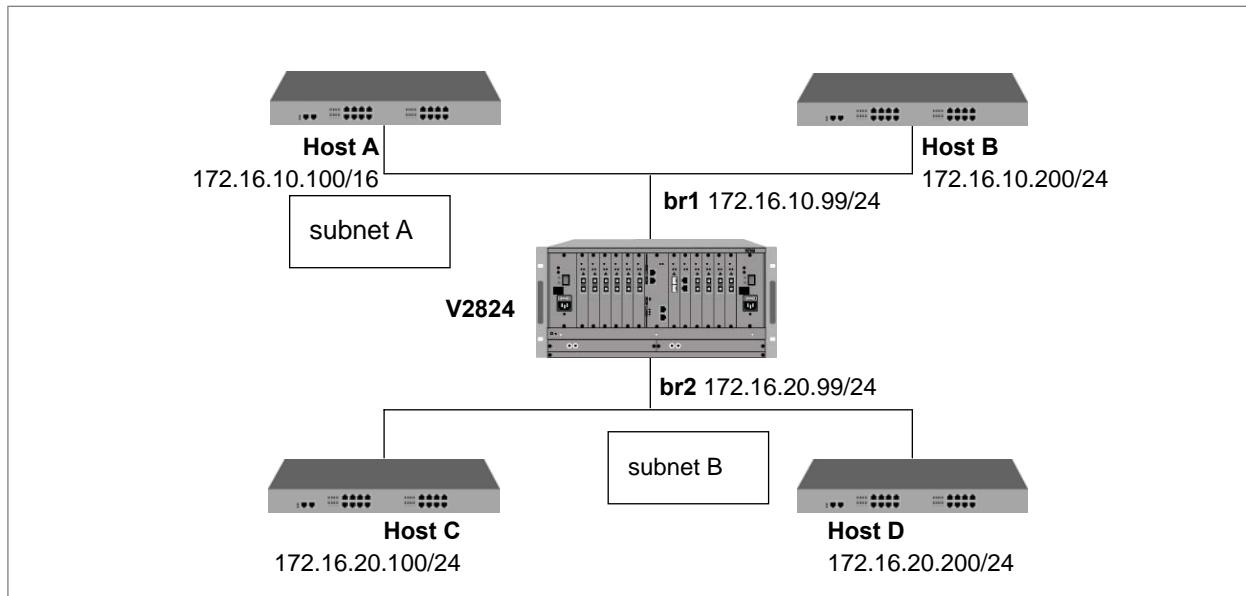
*time*은 초 단위로 <5 – 2,147,483,647> 사이에서 설정 가능합니다.

7.12.4 Proxy-ARP 설정

V2824는 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 V2824의 br1에 해당하는 인터페이스와 subnet A에 속해 있는 노드들에게만 전달되고, Host D에게는 전달되지 않습니다.

하지만, V2824는 Host D가 다른 subnet에 속해 있음을 알고 있으며 Host D에 패킷을 전송할 수도 있습니다. 따라서, Host A로부터 ARP 요청에 대해 자신의 MAC 주소를 응답을 해줍니다.



【 그림 7-13 】 Proxy-ARP

이러한 방법으로 subnet A로부터 들어오는 subnet B에 대한 ARP 요청은 모두 V2824의 MAC 주소로 응답하게 되고, Host A로부터 Host D로 전송되어야 하는 패킷은 V2824를 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.

[설정 예제 1]

다음은 br1에 Proxy-ARP를 설정하는 경우의 예입니다.

```
SWITCH# configure terminal
SWITCH(config)# interface default
SWITCH(config-if)# ip proxy-arp
SWITCH(config-if)# show running-config
(종략)
interface default
no shutdown
ip proxy-arp
ip address 172.16.209.50/16
!
ip route 0.0.0.0/0 172.16.1.254
!
no snmp
!
SWITCH(config-if)#

```

7.12.5 Gratuitous ARP

V2824는 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.

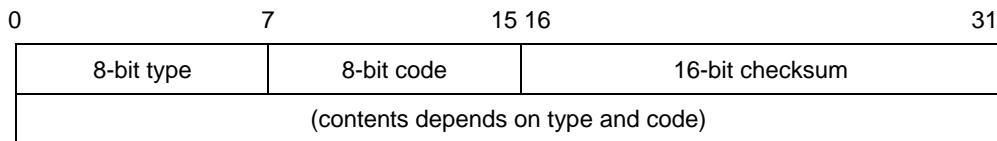
명령어	모 드	기 능
arp patrol <i>interval count {delivery-start}</i>		Gratuitous ARP를 설정합니다.
no arp patrol	Global	Gratuitous ARP를 해제합니다.
show running-config		Gratuitous ARP 설정 내용을 확인합니다.

7.13 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 7-14 】 ICMP 메시지

다음은 ICMP 메시지의 Type 값을 설명한 표입니다.

【 표 7-2 】 ICMP Message 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		

V2824는 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 V2824에서 가능한 ICMP 메시지 조절 기능입니다.

- Echo Reply 메시지 제한
- ICMP 메시지 전송 시간 제한
- 인터페이스 별 ICMP 메시지 전송 제한

7.13.1 Echo Reply 메시지 제한

V2824는 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.

Echo Reply 메시지 제한 설정 내용을 확인하시려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show running-config	All	Echo Reply 메시지 제한 설정 내용을 확인합니다.

7.13.2 ICMP 메시지 전송 시간 제한

V2824는 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.

V2824에서 ICMP 메시지의 전송 시간을 제한하기 위해서는 전송 제한 메시지와 해당 메시지의 전송 제한 시간을 설정해야 합니다.

(1) 전송 제한 메시지 지정

ICMP 메시지 가운데 전송 시간을 제한할 메시지를 선택하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>ip icmp interval rate-mask mask</code>	Global	ICMP 메시지 중에서 전송 시간을 제한할 메시지를 설정합니다.



참 고

*mask*는 16진수로 0xFFFFFFFF까지 입력 가능합니다. 기본 설정은 0x1818입니다.

각 ICMP 메시지는 아래표와 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.

주 의

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. 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 10_{ms}(1/100s)로, 기본 설정은 1초(100_{ms})입니다. *interval*에 0을 입력하면 시간 제한을 두지 않고 항상 메시지를 내보내는 것입니다. 0~2000000000 까지 설정할 수 있습니다.

(3) 전송 제한 설정 확인

ICMP 메시지 전송 제한 설정 내용을 확인하시려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip icmp interval	Enable/Global	ICMP 메시지 전송 설정 내용을 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.



기본으로 설정된 전송 제한 메시지는 0x1818, 전송 제한 시간은 1초(100_{ms})입니다.

7.13.3 인터페이스 별 ICMP 메시지 전송 제한

만약 목적지인 호스트나 네트워크로 패킷들을 보낼 수 없을 때 장비는 source IP 주소의 정보를 이용하여 이러한 메시지들을 되돌려 보내도록 되어 있습니다. 하지만 특정한 목적지에 도착할 수 없는 패킷들이 과도하게 들어올 경우, 되돌려 보내는 작업 또한 시스템에 영향을 줄 수 있습니다. 따라서 이를 인터페이스 단위로 선택적으로 기능을 해제 시킬 수 있도록 기능이 추가되었습니다.

특정한 인터페이스의 목적지 호스트나 네트워크에 도달하지 못하는 패킷들을 발신지 주소로 되돌려 보내는 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip unreachable	Interface	특정한 인터페이스의 도달하지 못하는 패킷들을 되돌려 보내는 기능을 해제합니다.

해당 패킷들을 다시 발신지 주소로 되돌리고자 한다면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip unreachable	Interface	특정한 인터페이스의 도달하지 못하는 패킷들을 되돌려 보내는 기능을 설정합니다.

7.14 TCP Flag Control

TCP(Transmission Control Protocol) 패킷의 Header에는 URG, ACK, PSH, RST, SYN, FIN 등 6가지 플래그가 포함되어 있습니다. V2824는 이 가운데 RST와 SYN에 대해 다음과 같은 설정을 할 수 있습니다.

- RST 설정
- SYN Attack 방지 기능 설정

7.14.1 RST 설정

RST는 TCP 연결을 시도하는 상대에게 접속이 불가능함을 응답해 주는 기능을 가지고 있습니다.

그러나, V2824의 사용자는 RST가 TCP 연결을 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 연결을 시도하는 상대에게 접속이 불가능함을 응답하지 않습니다.

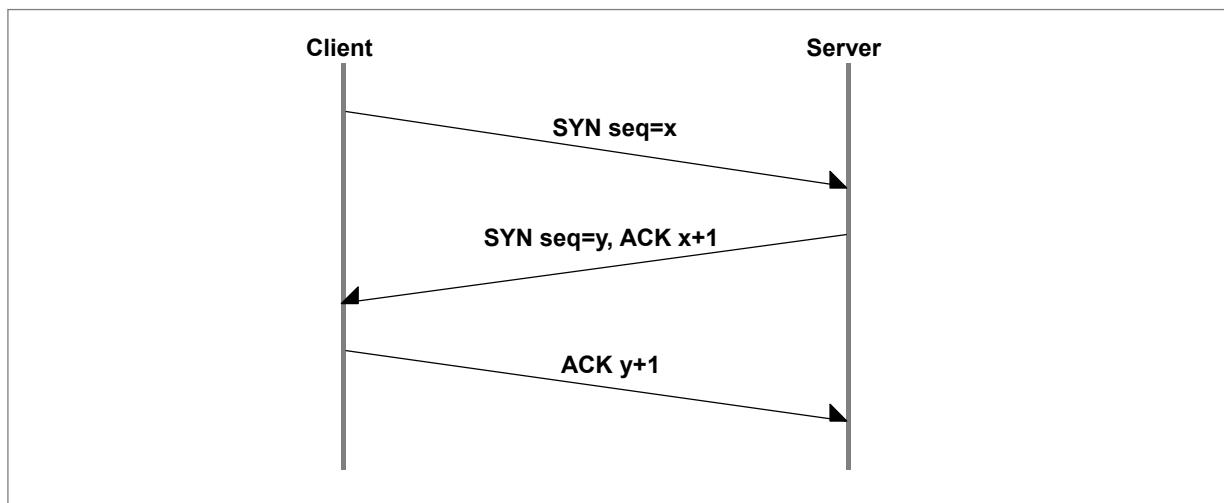
명령어	모 드	기 능
ip tcp ignore rst-unknown	Global	TCP 연결을 시도하는 상대에게 접속이 불가능함을 응답하지 않도록 설정합니다.
no ip tcp ignore rst-unknown		TCP 연결을 시도하는 상대에게 접속이 불가능함을 응답하도록 설정합니다.
show running-config include rst-unknown	Enable / Global	TCP RST 설정 내용을 확인합니다.



V2824는 기본적으로 TCP connection을 시도하는 상대에게 접속이 불가능함을 응답하도록 설정되어 있습니다.

7.14.2 SYN Attack 방지 기능 설정

클라이언트와 서버의 TCP 통신은 다음과 같이 세 방향(3 Way Hand Shaking)으로 이루어집니다.



【 그림 7-15 】 3 Way Hand Shaking

클라이언트는 연결을 시도하기 위해 1Bit의 SYN Bit를 설정하고, sequence number=x와 함께 보냅니다. 이에 대해 서버는 Hand Shaking이 계속 이루어지고 있다는 것 뿐만 아니라 SYN에 대한 응답을 SYN와 ACK Bit 집합으로 보냅니다.

이 때 ACK 비트에는 클라이언트가 보낸 sequence number에 1을 더해 “x+1”의 sequence number가 포함되고, SYN에는 새로운 sequence number=y가 포함됩니다. 마지막으로 클라이언트는 서버에게 보내는 응답으로 ACK 비트와 “y+1”의 sequence number를 보내면서 서로 연결이 이루어졌음을 알립니다.

3 Way Hand Shaking에서 연결을 맺기 위해 전송된 SYN는 서버의 Incomplete Connection Queue에 Entry로 추가되고, TCP 연결이 완료되면 이 연결은 Completed Connection Queue에 추가됩니다. 그리고, 이러한 Queue들의 합은 일정한 값을 넘을 수 없습니다.

이 때, 어떤 Client가 무작위로 선출된 Source IP를 가진 SYN를 전송하면 서버는 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 한계값에 이르게 됩니다. 이러한 상태가 되면 정상적으로 패킷을 처리할 수 없고, 통신이 불가능하게 됩니다.

V2824는 이러한 SYN Flooding을 막기 위해 Sequence Number 대신에 쿠키(Cookies)를 SYN과 함께 전송하고, 전송했던 쿠키에 대한 응답이 되돌아오는 경우에만 연결을 승인하도록 하는 기능을 가지고 있습니다.

SYN에 쿠키를 함께 전송하여 쿠키가 되돌아왔을 때만 접속을 승인하도록 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip tcp syncookies	Global	SYN에 쿠키를 함께 전송하여 쿠키가 되돌아왔을 때만 접속을 승인하도록 설정합니다.
no ip tcp syncookies		SYN에 쿠키를 함께 전송하여 쿠키가 되돌아왔을 때만 접속을 승인하지 않도록 설정합니다.
show running-config include syncookies	Enable / Global	TCP SYN 설정 내용을 확인합니다.

7.14.3 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.

7.15 덤프 패킷 (Dump Packet)

이 장에서는 다음과 같은 내용을 설명합니다.

- 덤프 패킷 확인
- 덤프 패킷 디버그

7.15.1 덤프 패킷 확인

V2824에서는 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		
debug packet {interface interface-name port port-number} host src-ip src-ip-address dest-ip dest-ip-address src-port src-port-number	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 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

V2824에서는 사용자가 다음 명령어로 덤프 패킷 출력 형식을 *option*으로 지정하여 결과를 확인할 수 있습니다. *option*은 TCP 덤프에서 사용하는 것을 모두 사용할 수 있습니다.

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, 종료 합니다.
-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.

Option	내 용
-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 sequence번호를 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 핵사코드로 출력합니다.
-c number	제시된 수의 패킷을 받은 후 종료합니다.
-F file	filter 표현의 입력으로 파일을 받아들입니다. 커맨드라인에 주어진 추가의 표현들은 모두 무시됩니다.
-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 표시합니다. type에는 다음과 같은 것들이 올 수 있습니다. 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.

(5) 설정 내용 확인

덤프 패킷 관련 설정 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show dump packets	Enable/Global	덤프 패킷 관련 설정 내용을 확인합니다.

7.15.2 덤프 패킷 디버그

V2824에서는 다량의 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 명령을 사용하십시오.

명령어	모 드	기 능
debug packets log packet-counting <i>cpu-threshold time [file-number]</i>	Enable	조건에 해당되는 덤프 패킷들을 디버깅합니다.
no debug packet log		디버깅 설정을 해제합니다.



*file-number*의 기본 설정은 1로, <1 – 10> 사이에서 설정 가능합니다.



*file-number*에 설정된 수보다 더 많은 덤프 파일이 생성되는 경우에는, 낮은 번호의 파일에서부터 덮어 쓰기 됩니다.



write memory 명령어로 현재 설정 내용을 저장하는 경우에도, 덤프 파일은 저장되지 않습니다.

7.16 Port Security

V2824는 MAC 주소를 변조하거나 패킷 Flooding을 막기 위해 Port Security 기능을 구현하고 있습니다. 특정 포트에 Learning 될 수 있는 MAC 주소의 갯수를 지정하고, 지정된 갯수가 넘었을 때에는 사용자가 설정한 대로 포트가 관리되게 됩니다.

7.16.1 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.

7.16.2 MAC 주소 갯수 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 <1-1440>	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.



참 고

Learning 될 수 있는 MAC 주소는 기본적으로 1개로 설정되어 있습니다.



최대 MAC 주소의 개수를 변경하면 해당 포트의 MAC 주소들을 모두 삭제되고 등록된 MAC 주소들도 전부 삭제됩니다.

7.16.3 Port Security Age 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.

7.16.4 Port Security Age Type 지정

Aging type을 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.



참 고

Aging-out 형식은 기본적으로 absolute로 설정되어 있습니다.



참 고

Absolute는 설정된 aging time이 만료되면 secure MAC을 삭제합니다. Inactivity는 해당 secure MAC을 가진 패킷이 들어오지 않은때부터 aging time이 경과하면 해당 MAC을 삭제합니다.

7.16.5 Port Security Age 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 MAC 들의 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.

7.16.6 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.

7.16.7 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 <i>mac-address vlan vlan-id</i>	Bridge	해당 포트에 secure MAC 주소를 static으로 등록합니다.
no security port-number mac-address <i>mac-address [vlan vlan-id]</i>		해당 포트에 static 으로 등록된 secure MAC 주소를 삭제합니다.
clear port security port-number mac-address <i>[mac-address]</i>		해당 포트에 dynamic 으로 등록된 secure MAC 주소를 삭제합니다.
clear port security port-number mac-address <i>mac-address [vlan vlan-id]</i>		



Mac 주소를 지정하지 않는 경우는 전체 MAC을 삭제하고, vlan 지정을 하지 않는 경우에는 전체 vlan에 대해서 적용합니다.

7.16.8 Port Security 설정 확인

명령어	모 드	기 능
show port security [port-number]	Enable /Global /Bridge	포트 별 security 설정 상태를 보여줍니다.

7.17 PPS-Control

V2824는 포트에 트래픽이 폭주하는 것을 막기 위해 PPS-Control 기능을 지원합니다. 이 기능은 일정한 시간 간격으로 포트에 전송되는 트래픽량을 검사합니다. 사용자는 각 포트 별로 PPS-Control 관련 임계값을 설정하여, 이 임계값 이상으로 패킷을 수신하면 syslog 및 trap 메시지가 발생하도록 할 수 있습니다.

PPS-Control 기능에서 트래픽량을 검사하는 시간 간격과 포트 트래픽의 임계값을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
pps-control port port-number thres <5 60 600>	Global	PPS-Control 기능에서 트래픽량을 검사하는 시간 간격과 포트 트래픽의 임계값을 설정합니다.



포트 트래픽 임계값의 단위는 pps 입니다.



PPS-Control **port block**이 설정되어 있지 않은 경우에 한하여, 트래픽이 사용자가 지정한 임계값을 초과했을 때 syslog 및 trap 메시지가 발생합니다.

포트에 설정한 트래픽량 검사 시간 간격과 포트 트래픽 임계값을 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no pps-control port port-number	Global	포트에 설정한 트래픽량 검사 시간 간격과 포트 트래픽 임계값을 삭제합니다.

포트 트래픽이 임계값을 초과했을 때, 일정 시간 동안 포트를 Block 상태로 변경하게 되는데 이 때 포트를 Block 상태로 유지하는 시간을 설정할 수 있습니다. 트래픽이 임계값을 초과한 포트를 Block 상태로 유지하는 시간을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
pps-control port port-number block timer <10-3600>	Global	트래픽이 임계값을 초과한 포트를 Block 상태로 유지하는 시간을 설정합니다.



위의 명령어를 통해서만 PPS-Control **port block** 기능이 실행됩니다. 만약, port block이 설정되어 있지 않다면, 트래픽이 임계값을 초과해도 syslog와 trap 메시지만 발생됩니다.

트래픽이 임계값을 초과한 포트를 Block 상태로 유지하는 시간 설정값을 삭제하면서, 포트의 Block 상태를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no pps-control port <i>port-number</i> block	Global	포트를 Block 상태로 유지하는 시간 설정값을 삭제하면서, 포트의 Block 상태를 해제합니다.

PPS-Control 기능에 대한 설정 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show pps-control port [<i>port-number</i>]	Global	PPS-Control 기능에 대한 설정 내용을 확인합니다.

7.18 Attack Guard

V2824는 바이러스나 해킹, 혹은 그 외 다른 요인에 의해 발생된 다량의 패킷이 한꺼번에 스위치로 유입되는 것을 제한할 수 있습니다. 이러한 패킷들은 하나의 스위치에만 영향을 미치는 것이 아니라 해당 스위치가 속해 있는 전체 네트워크에 영향을 미칠 수 있으므로 네트워크 관리자에 의해 철저히 관리되어야 합니다.

Attack Guard는 포트로 들어오는 패킷의 양을 1초 간격으로 검사하여 패킷의 유입량이 특정한 값 이상이면 포트를 차단하거나 차단된 포트를 해제하는 기능입니다. 한편, 특정 포트에 유입된 패킷의 양이 한계값을 초과하여 포트가 차단된 경우, 바이러스로 의심이 되어 사용자가 해당 포트의 사용을 원치 않게 될 수 있습니다. V2824는 이러한 상황에서 해당 포트를 완전히 차단하는 기능을 제공합니다.

7.18.1 Attack Guard 설정

패킷 유입량이 *high-water-mark* 이상이 되면 해당 포트를 차단하여 패킷을 Drop 시키고, 패킷 유입량이 *low-water-mark* 이하로 떨어지면 차단을 해제합니다. **static**을 선택하는 경우에는 *low-water-mark*가 0으로 설정되며, Attack Guard에 의해 차단된 포트를 사용자가 직접 해제해야 합니다.

Attack Guard를 설정 하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
attack-guard {unicast multicast broadcast} port-number high-water-mark {low-water-mark static}	Bridge	Attack Guard를 설정합니다.
no attack-guard {unicast multicast broadcast} port-number		Attack Guard를 해제합니다.



참 고

*high-water-mark*과 *low-water-mark*은 pps(packet per seconds) 단위로, <10 – 148, 810> 사이에서 설정 가능합니다.



참 고

*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.

7.18.2 포트 수동 활성화

*low-water-mark*가 0(static)으로 설정된 포트는, Attack Guard에 의한 차단 상태를 다음 명령어로 사용자가 직접 해제해야 합니다. Attack Guard에 의해 차단된 포트는 다음의 명령어를 이용하여 쉽게 해제할 수 있습니다.

Attack Guard에 의해 차단된 포트를 수동으로 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
attack-guard-recovery port-number	Bridge	Attack Guard에 의해 차단된 포트를 수동으로 해제합니다.



참 고

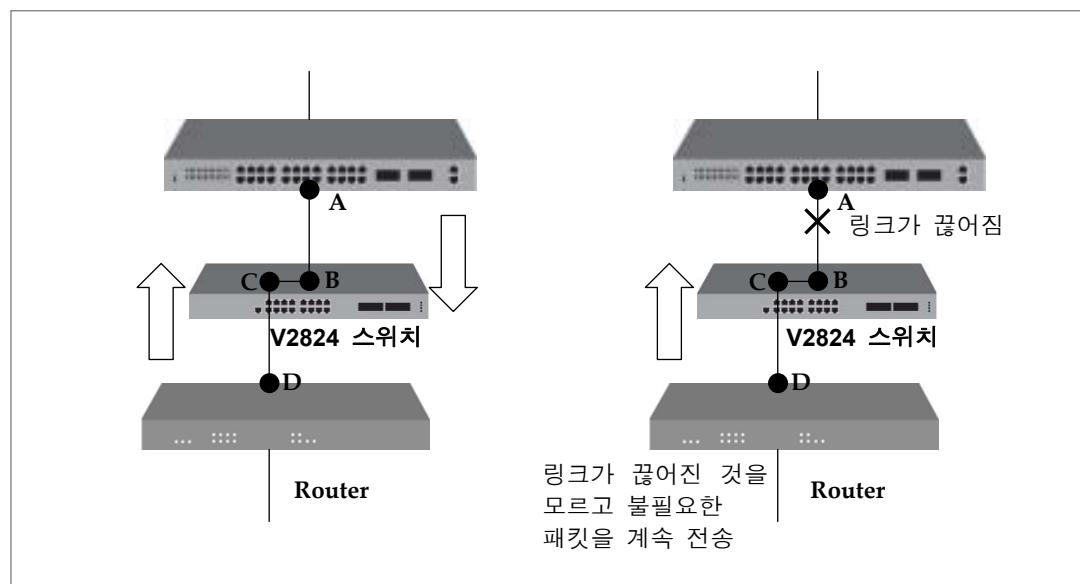
*port-number*는 한번에 여러 개를 입력할 수 있습니다. 각 입력값 사이를 빈칸 없이 쉼표(,)로 구분하거나, 입력 범위의 처음과 마지막 값을 빈칸 없이 이음표(-)로 연결하여 복수의 *port-number*를 입력하십시오.

7.18.3 설정 내용 확인

Attack Guard 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모드	기능
<code>show attack-guard { port-number all}</code>	Enable/Global/Bridge	Attack Guard 설정을 확인합니다.

7.19 LLCF (Link Layer Carrier Forward)



【 그림 7-16 】 LLCF 절차

위의 그림과 같이 V2824 스위치가 라우터와 또 다른 장비를 연결해 주는 경우, A와 B의 링크가 끊어지면 C와 D의 링크도 쓸모가 없어집니다. 그러나, D는 C를 보고 링크가 A와 B의 링크가 끊어졌음을 알 수가 없고, 따라서, D는 계속적으로 C에게 불필요한 패킷들을 보내게 됩니다.

이러한 현상을 막기 위해서 V2824 스위치는 같은 장비의 포트 2개로 서로 다른 장비가 연결되어 있는 상황에서 한 쪽 포트의 링크가 끊어지면 다른 한 편의 링크도 끊어지고, 다시 연결되면 다른 한 편의 링크도 연결되도록 설정할 수 있습니다. 이러한 기능을 LLCF (Link Layer Carrier Forward)라고 합니다.

LLCF 기능을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port llcf port-number port-number	Bridge	두 포트 사이에 LLCF 기능을 설치합니다.

LLCF 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear port llcf	Bridge	LLCF 기능을 해제합니다.

한편, 링크가 끊어졌다가 다시 연결되었을 때, 링크가 살아나기까지는 약간의 시간이 걸릴 수도 있습니다. 링크가 되살아나기까지 걸리는 시간 동안 링크가 끊어져있는 상태로 인식한다면, 그대로 링크를 되살리지 못할 것입니다. 이러한 문제점을 해결하기 위해 V2824 스위치는 장비에 설정되어 있는 일정한 시간이 지난 후에 상대 포트의 링크 상태를 검토하도록 되어 있습니다.

상대 포트의 링크 상태를 검사할 때의 시간 간격을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port llcf timer <1000-10000>	Global	상대 포트의 링크 상태를 검사할 때의 시간 간격을 설정합니다.



참 고

설정할 시간 간격의 단위는 ms이며, V2824 스위치에는 기본적으로 2500ms(2.5초)로 설정되어 있습니다.

상대 포트의 링크 상태를 검사하는 시간 간격을 해제하려면 다음 명령어를 사용하십시오.

명령어	Mode	기 능
clear port llcf timer	Global	상대 포트의 링크 상태를 검사할 때의 시간 간격을 해제합니다.

LLCF 기능에 대한 설정을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show port llcf	Enable/Global/Bridge	Link Layer Carrier Forward 기능에 대한 설정을 확인합니다.

7.20 포트 트래픽 모니터링 설정

V2824는 포트에서 특정 트래픽이 일정 시간 이상으로 지속되었을 때 Syslog 및 Trap 메시지를 발생시킬 수 있습니다. 사용자는 트래픽을 검사할 포트를 특정 포트 또는 특정 방향(Ingress 또는 Egress)의 포트를 지정할 수 있습니다. 사용자가 지정한 포트에서 트래픽이 기준 이상으로 발생하면, 그 이후부터 설정한 모니터링 시간 동안에 평균 트래픽량이 기준 트래픽량을 초과할 때마다 Trap 메시지가 발생합니다.

또한, 사용자는 Trap 메시지 발생 간격을 설정할 수 있습니다. 포트의 평균 트래픽량이 기준 트래픽량을 초과하여 한번 Trap 메시지가 발생하면, V2824는 사용자가 지정한 일정 시간이 지난 후에 평균 트래픽량을 다시 계산합니다. 만약, 이 기간 동안에도 평균 트래픽량이 기준 트래픽량을 초과한다면 다시 Trap 메시지가 발생됩니다. 이후에도 계속해서 평균 트래픽량이 기준 트래픽량을 초과한다면, V2824는 앞의 과정을 반복하여 포트의 트래픽량을 모니터링하고 그 결과를 trap 메시지로 알리게 됩니다.

특정 포트의 트래픽량을 모니터링 하여 기준치를 초과할 경우 Trap 메시지가 발생하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
port traffic-monitor port-number traffic-threshold expire-time trap-interval {ingress egress all}	Bridge	특정 포트의 트래픽량을 모니터링 하여 기준치를 초과할 경우 Trap 메시지가 발생하도록 설정합니다.
clear port traffic-monitor port-number {ingress egress all}		설정한 포트 트래픽 모니터링 기능을 해제합니다.



참 고

*traffic-threshold*는 Trap 메시지가 발생하게 되는 기준 트래픽량을 설정합니다. <1-1,000> 범위에서 설정할 수 있으며 단위는 Mbps입니다.



참 고

*expiere-time*은 특정 포트의 평균 트래픽량을 산출하기 위해 모니터링 하는 시간입니다. <1-144> 범위에서 설정할 수 있으며 단위는 10분입니다. 예를 들어, 사용자가 10을 설정하면 실제로 장비에 적용되는 시간은 $10 \times 10 = 100$ 분이 되는 것입니다.



참 고

*trap-interval*은 trap 메시지가 발생하는 시간 간격으로, 한번 Trap 메시지가 발생하면 이 시간이 지난 후에 다시 한번 평균 트래픽량을 모니터링 합니다.. <1-144> 범위에서 설정할 수 있으며 단위는 10분입니다. 예를 들어, 사용자가 10을 설정하면 실제로 장비에 적용되는 시간은 $10 \times 10 = 100$ 분이 되는 것입니다.

설정한 특정 포트의 트래픽 모니터링 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>show port traffic-monitor port-number</code>	Enable/Global/Bridge	포트 트래픽 모니터링 정보를 확인합니다.

7.21 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 과부화 현상을 막는 용도로 사용됩니다.

V2824는 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.



참 고

ECMP에서 사용할 수 있는 최대 링크 개수는 기본적으로 4개로 설정되어 있습니다.

8. 시스템 주요 기능 설정

시스템 주요 기능 설정에서는 VLAN, 포트 트렁킹, STP 등 V2824가 가지고 있는 주요 기능에 대해 설명합니다.

이 장은 다음과 같은 내용으로 이루어집니다.

- Access List 설정
- VLAN(Virtual Local Area Network)
- Link Aggregation
- STP
- Loop 감지 기능 설정
- 스택킹 설정
- Rate Limit와 Flood Guard
- DHCP(Dynamic Host Configuration Protocol)
- Storm Control
- Jumbo-frame 수용하기
- 최대 전송 단위 (MTU) 설정
- 대역폭 설정

8.1 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.

ACL(Access Control List)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.

V2824는 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.



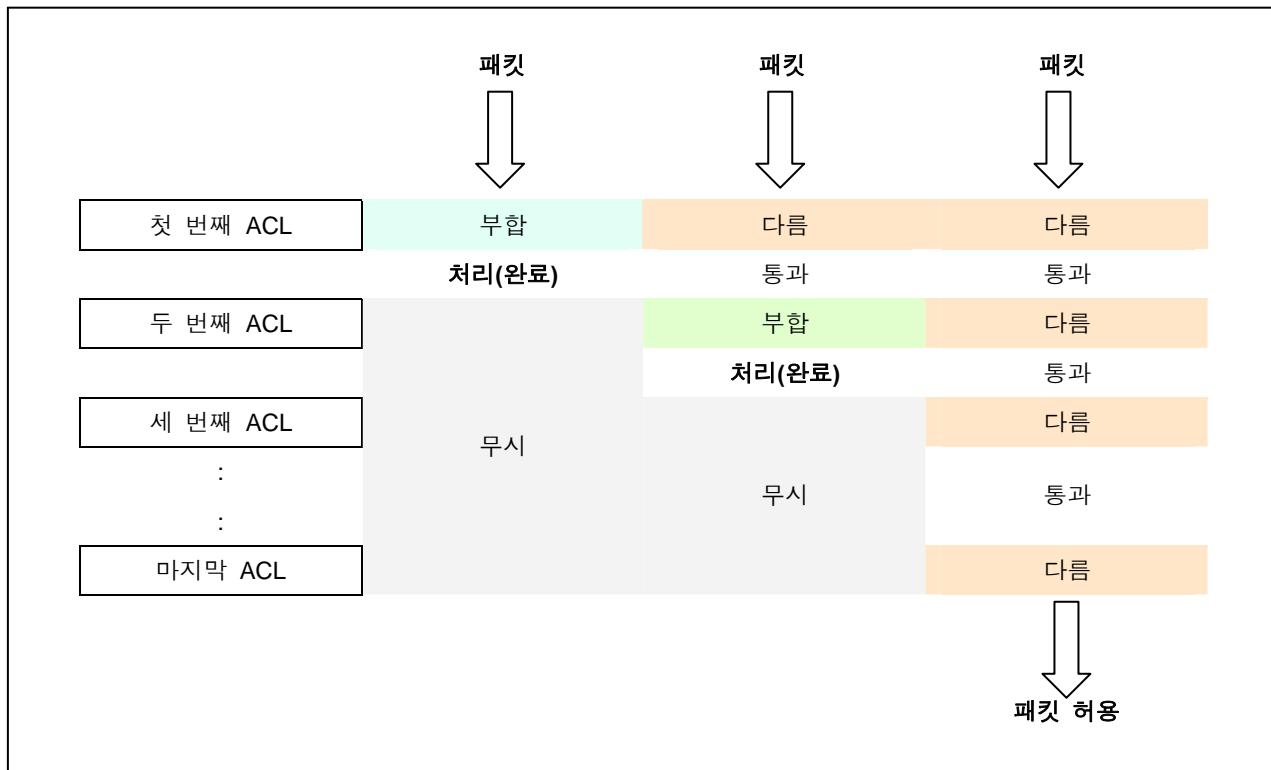
참 고

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.

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 8-1 】 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.

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 8-1 】 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.

8.1.1 Standard Access List 설정

Standard access-list는 지정한 IP 주소를 참조하여 IP 패킷을 허용 또는 거부하도록 설정합니다.

V2824는 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]		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		특정 호스트 IP 주소를 가진 패킷을 허용 또는 거부하도록 설정합니다.



참 고

<1-99>는 Standard access-list의 식별번호로 설정할 수 있는 범위입니다. <1,300-1,900> 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]		
no access-list {<1-99> <1300-1999>} {deny permit} any	Global	설정한 Standard access-list를 삭제합니다.
no access-list {<1-99> <1300-1999>} {deny permit} host ip-address		

한편, V2824는 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>} remark description	Global	특정 ACL 엔트리에 부가설명을 저장합니다.
no access-list {<1-99> <1300-1999>} remark description		설정한 ACL 엔트리의 부가설명을 삭제합니다.



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)#{
```

8.1.2 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.

V2824는 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 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 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, V2824는 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 description	Global	특정 ACL 엔트리에 부가설명을 저장합니다.
no access-list {<100-199> <2000-2699>} remark description		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)#{/pre}
```

8.1.3 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 access-list-name {deny permit} A.B.C.D/M [exact-match]	Global	특정 Prefix에 해당하는 패킷을 허용 또는 거부하도록 Named access-list를 설정합니다.
access-list access-list-name {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, V2824는 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)#{
```

8.1.4 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)#

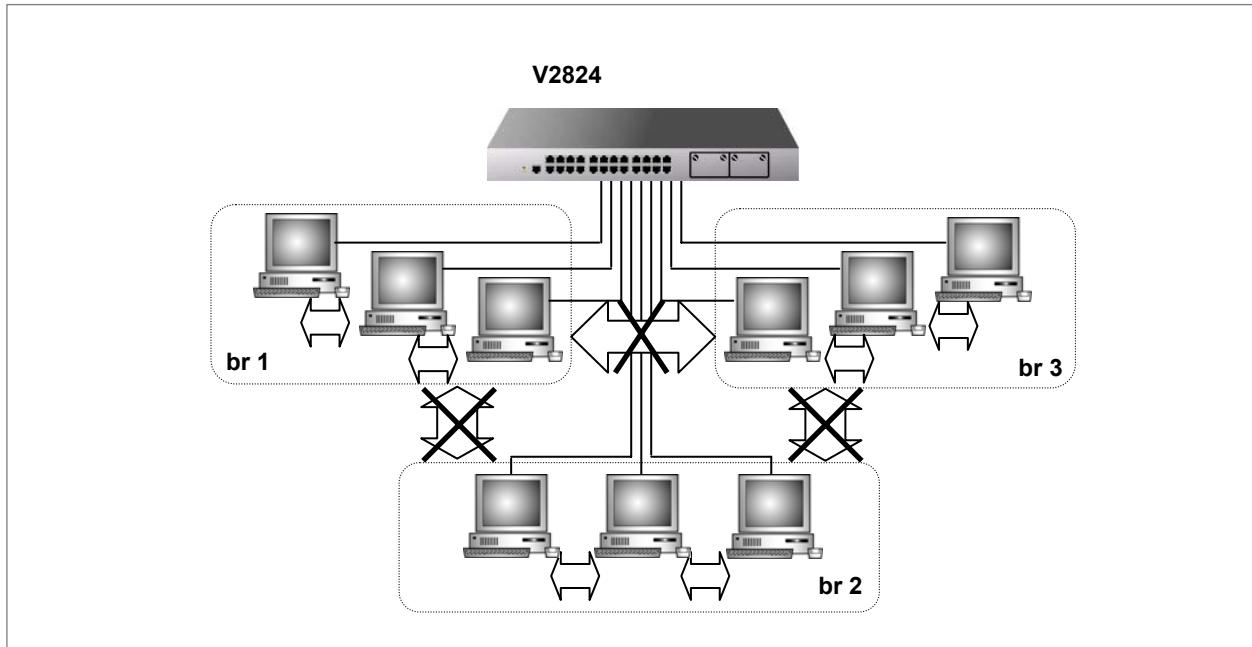
```

8.2 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.

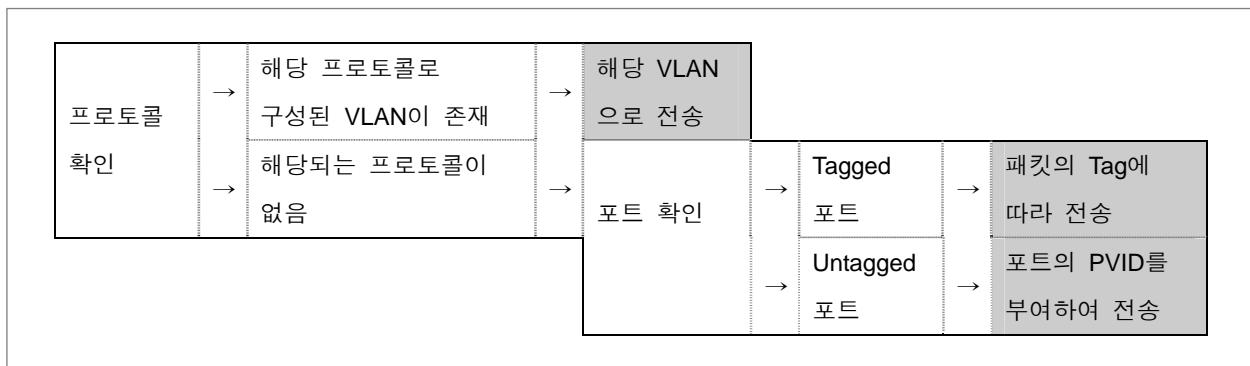


【 그림 8-2 】 Layer 2 환경 포트 기준 VLAN 구성도

위의 그림에서 VLAN으로 설정된 br1, br2, br3는 논리적으로 설정된 가상 네트워크입니다. Layer 2 스위치로 동작할 경우, 가상 네트워크 내에서는 통신이 가능하지만, 서로 다른 가상 네트워크간에는 통신이 불가능합니다.

V2824는 포트 기반 VLAN과 프로토콜 기반 VLAN을 지원합니다. V2824에서 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. V2824의 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 V2824는 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, V2824의 A번 포트를 Untagged 포트로 설정해 놓았다면, 패킷이 전송되었을 때에는 A번이 가지고 있는 PVID를 패킷에 부여하게 되는 것입니다. 따라서, VLAN 네트워크를 구성하고 있는 스위치 포트들은 PVID를 통해 해당 번호와 일치하는 VLAN으로 패킷을 전송할 수 있습니다. 다음은 V2824에 설정되어 있는 VLAN을 기준으로 패킷 경로를 결정하는 방법입니다.



【그림 8-3】 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 스위치를 설치하는 등 여러 대의 다른 장비를 이용하지 않고 하나의 스위치로 VLAN을 이용하면 저렴한 가격으로 네트워크를 구성할 수 있습니다.

◆ 보안 강화

일반 스위치에서는 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
- Shared-VLAN 설정
- Protected 포트의 설정
- VLAN 설명하기
- VLAN Translation 설정
- VLAN 관련 설정 내용 확인
- 설정 예제

8.2.1 Default VLAN

V2824는 기본적으로 모든 포트가 Default VLAN으로 설정되어 있습니다. Default VLAN은 PVID를 1로 가지고 있으며, 절대 삭제할 수 없습니다. 사용자가 새롭게 만든 VLAN에 중복 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.

다음은 3번 포트를 2에서 삭제하였을 때, 다시 Default로 돌아가는 것을 보여주는 예입니다.

```

SWITCH(bridge)# vlan create 2
SWITCH(bridge)# vlan del 1 3,4
SWITCH(bridge)# vlan add 2 3,4 untagged
SWITCH(bridge)# show vlan
      u: untagged port, t: tagged port
-----
|           1           2           3           4
Name( VID| FID) |1234567890123456789012345678901234567890
-----
default( 1| 1) |uu..uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
      br2( 2| 2) |...uu.....
SWITCH(bridge)# vlan del 2 3
SWITCH(bridge)# show vlan
      u: untagged port, t: tagged port
-----
|           1           2           3           4
Name( VID| FID) |1234567890123456789012345678901234567890
-----
default( 1| 1) |uuu.uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
      br2( 2| 2) |...u.....
SWITCH(bridge)#

```

8.2.2 포트 기반 VLAN 설정

V2824에 포트 기반 VLAN을 설정하려면, 일단 VLAN을 새롭게 만들고, 구성원을 지정하고, PVID를 할당하면 됩니다. VLAN 설정과 관련하여 다음과 같은 내용으로 설명합니다.

- VLAN 만들기
- PVID 지정
- 포트 할당 및 삭제
- VLAN 기능 해제

(1) VLAN 만들기

V2824는 VLAN을 만들 때 VLAN명이 “**brN(N=정수)**”으로 만들어지고(“**N**”으로도 입력 가능), 이때 각 VLAN이 가지는 VID는 자동적으로 “**N**”으로 정해집니다. 다시 말하자면, br2의 VID는 2이고, br100의 VID는 100입니다. VID가 1인 VLAN은 Default VLAN으로 정해져 있습니다. 따라서 사용자는 br1이라는 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-id	Bridge	VLAN 이름을 지정하여 새로운 VLAN을 만듭니다.



*vlan-id*은 “**brN**” (**N=정수**) 의 형태나 **N**의 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-id*은 정수 “**N**”을 사용할 때, “-” 기호를 이용하여 넓은 범위를 입력하거나 “,” 기호를 사용하여 나열할 수 있습니다. “**brN**”의 형태로는 하나씩 설정해야 합니다.

(2) PVID 지정

V2824는 *vlan-id*에 입력되는 정수, **N**을 VID로 자동적으로 부여됩니다. 예를 들어 *vlan-id*을 “**br2**”, 또는 “**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. V2824는 기본적으로 모든 포트가 “**default**”라는 인터페이스에 통합되어 있기 때문에 중복 없이 다른 VLAN에 포트를 할당하려면 “**default**”로 부터 포트를 삭제해야 합니다.



V2824의 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-id port-number {tagged untagged}	Bridge	VLAN에 속하는 포트를 지정하고 해당 포트의 속성을 tagged나 untagged로 설정합니다.
vlan del vlan-id port-number		VLAN에 속해 있는 포트를 삭제합니다.



*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.

(4) VLAN 기능 해제

V2824에 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 설정 모드에서 다음 명령어를 사용하여 VLAN에 속하는 모든 포트를 삭제 하십시오.

명령어	모 드	기 능
vlan del vlan-id port-number	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 vlan-id	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 vlan-id	Bridge	VLAN을 삭제합니다.



주의

VLAN을 삭제하면 해당 VLAN에 속해있던 모든 포트가 비활성화 상태로 됩니다. 이 포트들은 새로운 VLAN에 할당할 때까지 비활성화 상태를 유지합니다.

8.2.3 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 port-number ethertype ethertype <1-4094>	Bridge	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.

8.2.4 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 <1-4094>	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.

8.2.5 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 <1-4094>	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.

8.2.6 VLAN 우선 순위 지정

V2824에 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.

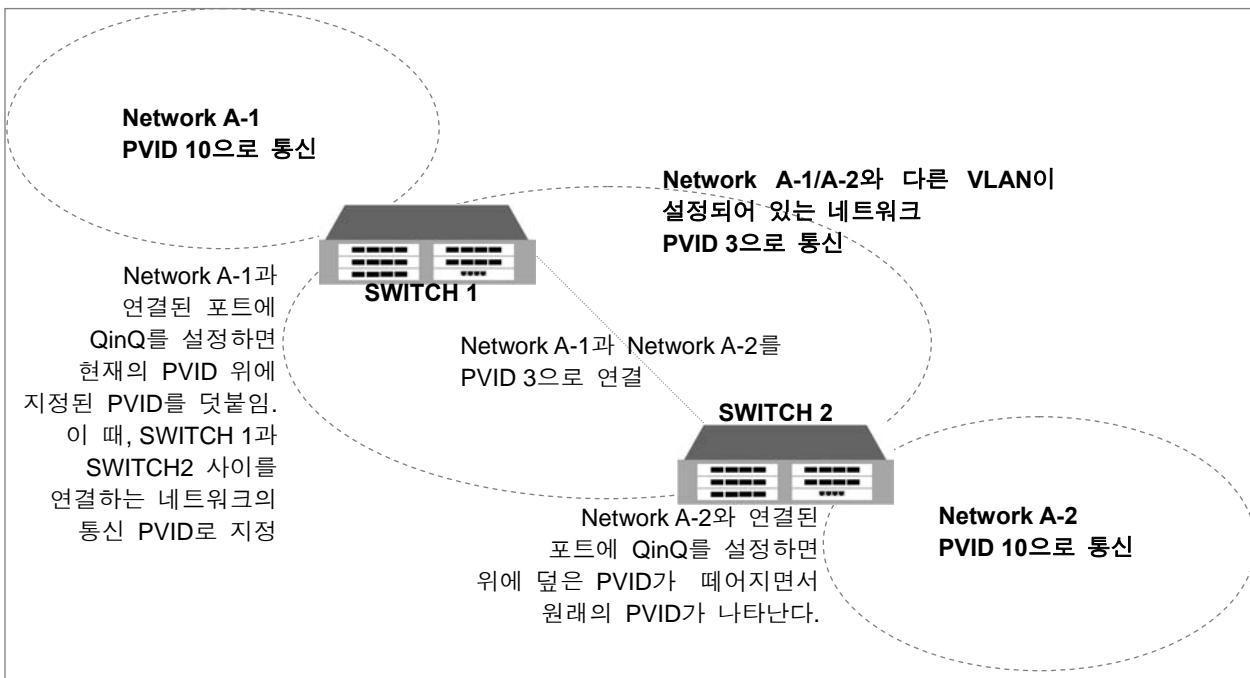


기본으로 설정되어 있는 우선 순위는 **MAC 주소 기반 VLAN > Subnet 주소 기반 VLAN** 입니다.

8.2.7 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, V2824가 가지고 있는 QinQ 기능을 이용하면 번거롭게 모든 장비에 여러 개의 VLAN을 설정할 필요가 없습니다.



【 그림 8-4 】 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 붙였던 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 8-4】 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.



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 tpid	Bridge	QinQ 포트의 TPID를 설정합니다.

(3) QinQ 해제

QinQ 포트로 설정했던 것을 해제하려면, 다음 명령어를 사용하십시오.

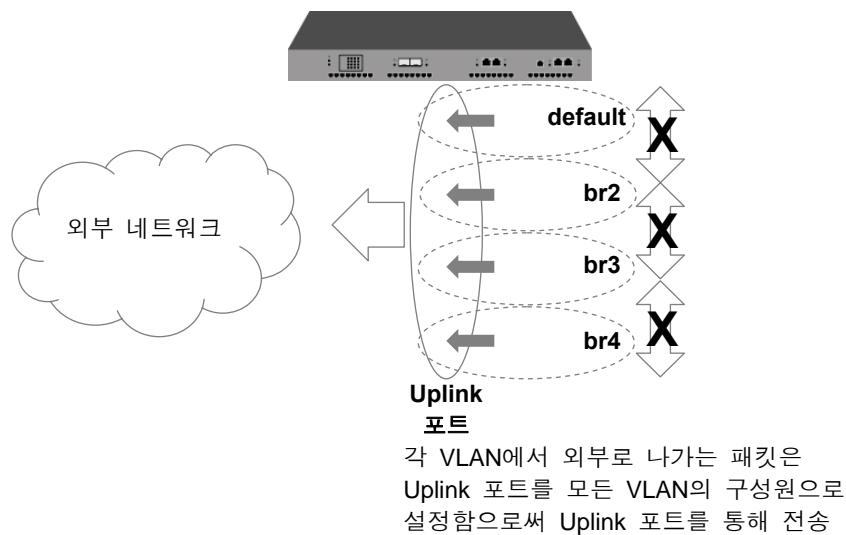
명령어	모 드	기 능
vlan dot1q-tunnel disable port-number	Bridge	QinQ 포트로 설정한 것을 해제합니다.

8.2.8 Shared-VLAN 설정

V2824는 라우팅의 기능이 없는 Layer 2 스위치이기 때문에 VLAN 간의 통신이 불가능합니다. 특히, Uplink 포트로 지정한 포트는 모든 VLAN으로부터 패킷을 받아야 하는데, 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.

```
SWITCH(bridge)# show vlan
      u: untagged port, t: tagged port
-----
|       1       2       3       4
Name( VID| FID) | 1234567890123456789012345678901234567890
-----
default( 1| 1) |u...uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
      br2( 2| 2) |.u.....u.....u.....u.....u.....u.....u.....
      br3( 3| 3) | ..u.....u.....u.....u.....u.....u.....
      br4( 4| 4) | ....u.....u.....u.....u.....
SWITCH(bridge)#

```



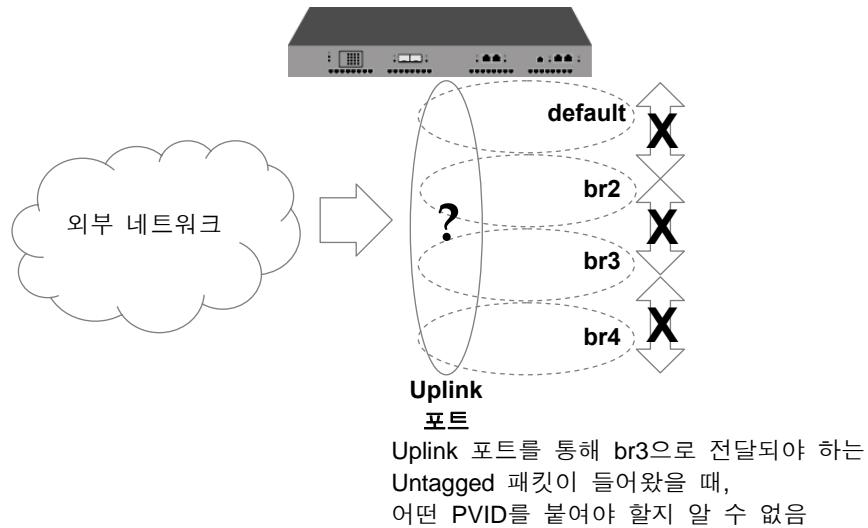
【 그림 8-5 】 Layer 2 환경에서 외부로 패킷이 나가는 경우

한편, 위와 같이 설정한 경우에서 Untagged 패킷이 통신을 할 때, Untagged 패킷이 1번 포트로 들어오면, PVID가 1이므로 tag 1을 달게 되고, Uplink 포트인 24번 역시 VLAN 1에 속하기 때문에 24번 포트로 전송이 가능합니다.

그러나 문제는 Uplink 포트로 들어오는 Untagged 패킷입니다. Uplink 포트로 내려오는 Untagged 패킷은 어떤 PVID를 가지고 어떤 포트로 전송되어야 할지를 알 수 없습니다.

```
SWITCH(bridge)# show vlan
              u: untagged port, t: tagged port
-----
|           1   2   3   4
Name( VID| FID) | 1234567890123456789012345678901234567890
-----
default( 1| 1) |u...uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
      br2( 2| 2) | .u.....u.....u.....u.....u.....u.....u
      br3( 3| 3) | ..u.....u.....u.....u.....u.....u.....u
      br4( 4| 4) | ...u.....u.....u.....u.....u.....u.....u
SWITCH(bridge)#

```

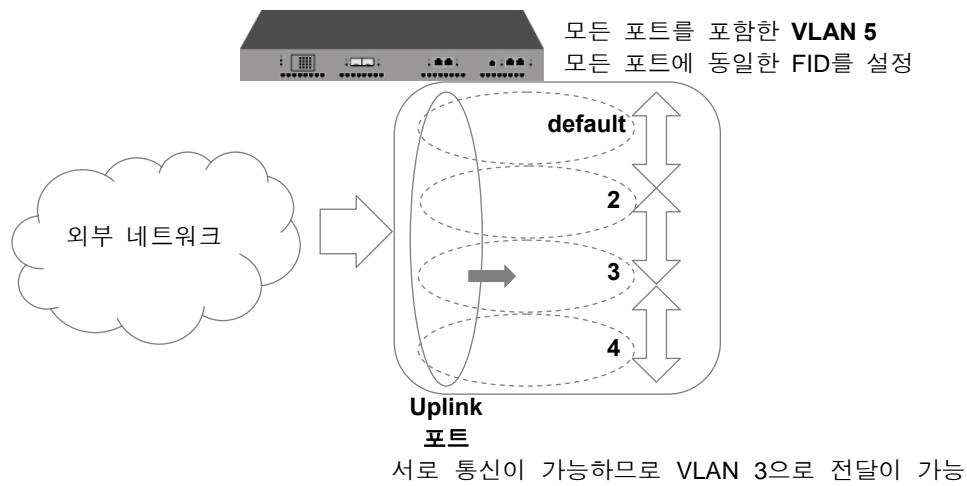


【 그림 8-6 】 Layer 2 환경에서 외부 패킷이 들어오는 경우 ①

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.

```
SWITCH(bridge)# show vlan
          u: untagged port, t: tagged port
-----
Name( VID | FID) | 1234567890123456789012345678901234567890
-----  
default( 1 | 5 ) | u....uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu  
      br2( 2 | 5 ) | .u.....u.....u.....u.....  
      br3( 3 | 5 ) | ..u.....u.....u.....u.....  
      br4( 4 | 5 ) | ...u.....u.....u.....u.....  
      br5( 5 | 5 ) | uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu  
SWITCH(bridge)#

```



【 그림 8-7 】 Layer 2 환경에서 외부 패킷이 들어오는 경우 ②

따라서 Layer 2 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-id FID value	Bridge	VLAN의 FID를 설정합니다.

8.2.9 Protected 포트의 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. V2824가 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 해 주는 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.

8.2.10 VLAN 설명하기

V2824는 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-id 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.

8.2.11 VLAN Translation 설정

VLAN Translation은 패킷의 VID를 사용자가 지정한 VID로 바꾸어 트래픽 흐름을 조정합니다.

VLAN Translation을 설정하시려면 다음 단계를 따르십시오. V2824의 VLAN Translation은 Rule 설정을 통해 VID가 변경됩니다.

1 단계 **rule name create** Rule 설정 모드로 들어가십시오.

(※ Rule과 QoS의 Rule 만들기 참고)

2 단계 Rule을 설정하여 VLAN Translation이 적용될 패킷을 분류하십시오.

(※ Rule과 QoS의 패킷 조건 규정 참고)

3 단계 **match vlan vlan-id** 명령어로 1단계 패킷의 변경될 VID를 지정하십시오.

(※ Rule과 QoS의 Rule 동작 설정 참고)

4 단계 **bridge vlan-id** 명령어로 Bridge 설정 모드로 들어가십시오.

5 단계 각 VLAN 설정 방법을 참고하여 분류된 패킷을 변경될 VID의 VLAN 멤버로 추가하십시오.



주의

Untagged 포트의 VLAN Translation을 설정하는 경우에는, **vlan fid vlan-id port-number** 명령어로 포트의 VLAN FID와 변경될 VID의 VLAN FID를 동일하게 설정하십시오. 패킷이 Flooding되어 VLAN 사이의 통신이 가능해집니다.

8.2.12 VLAN 관련 설정 내용 확인

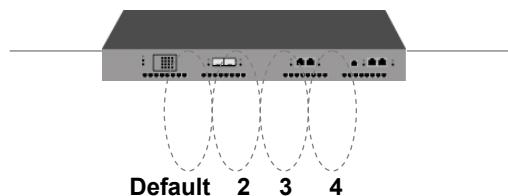
V2824는 사용자가 설정해 놓은 포트 기반 VLAN, 프로토콜 기반 VLAN, MAC 주소기반 VLAN, Subnet 주소 기반 VLAN, QinQ 등의 설정을 각각 확인할 수 있습니다. 각각의 설정 내용을 확인하는 방법은 다음과 같습니다.

명령어	모 드	기 능
show vlan	Enable / Global / Bridge	모든 VLAN 설정을 확인합니다.
show vlan vlan-id		특정 VLAN 설정을 확인합니다.
show vlan description		모든 VLAN 설명을 확인합니다.
show vlan dot1q-tunnel		QinQ 설정을 확인합니다.
show vlan protocol		프로토콜 기반 VLAN을 확인합니다.
show port protected		Protected Port 설정을 확인합니다.

8.2.13 설정 예제

[설정 예제 1] 포트 기반 VLAN 설정

다음은 VLAN 2, 3, 4를 새롭게 만들어서 각각에 2번 포트, 3번 포트, 4번 포트를 할당하는 경우입니다.



```
SWITCH(bridge)# vlan create 2
SWITCH(bridge)# vlan create 3
SWITCH(bridge)# vlan create 4
SWITCH(bridge)# vlan del 1 2,3,4
SWITCH(bridge)# vlan add 2 2 untagged
SWITCH(bridge)# vlan add 3 3 untagged
SWITCH(bridge)# vlan add 4 4 untagged
SWITCH(bridge)# vlan pvid 2 2
SWITCH(bridge)# vlan pvid 3 3
SWITCH(bridge)# vlan pvid 4 4
```

```
SWITCH(bridge)# show vlan
              u: untagged port, t: tagged port
-----
|       1       2       3       4
Name( VID| FID) |1234567890123456789012345678901234567890
-----
default( 1| 1) |u...uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
br2( 2| 2) |.u.....
br3( 3| 3) |..u.....
br4( 4| 4) |...u.....
SWITCH(bridge)#

```

[설정 예제 2] 포트 기반 VLAN 삭제

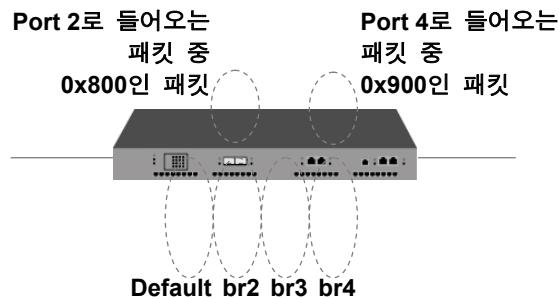
위에서 설정한 VLAN 가운데 VLAN 3을 삭제하는 경우입니다.

```
SWITCH(bridge)# vlan del 3 3
SWITCH(bridge)# exit
SWITCH(config)# interface 3
SWITCH(config-if)# shutdown
SWITCH(config-if)# exit
SWITCH(config)# bridge
SWITCH(bridge)# no vlan 3
SWITCH(bridge)# show vlan
              u: untagged port, t: tagged port
-----
|       1       2       3       4
Name( VID| FID) |1234567890123456789012345678901234567890
-----
default( 1| 1) |u.u.uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
br2( 2| 2) |.u.....
br4( 4| 4) |...u.....
SWITCH(bridge)#

```

[설정 예제 3] 프로토콜 기반 VLAN 설정

다음은 [설정 예제 1]과 서 설정한 상태에서 2번 포트와 4번 포트에 프로토콜 기반 VLAN을 설정하는 경우입니다.



```
SWITCH(bridge)# vlan pvid 2 ethertype 0x800 5
SWITCH(bridge)# vlan pvid 4 ethertype 0x900 6
SWITCH(bridge)# show vlan
      u: untagged port, t: tagged port
-----
|           1           2           3
Name( VID| FID) |1234567890123456789012345678901234567890
-----
default( 1| 1) |u...uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
      br2( 2| 2) |.u.....
      br3( 3| 3) |..u.....
      br4( 4| 4) |...u.....
SWITCH(bridge)# show vlan protocol
-----
|           1           2           3
Ethertype | VID |1234567890123456789012345678901234567890
-----
      0x0800    5  .p.....
      0x0900    6  ...p.....
SWITCH(bridge)#

```

위와 같이 설정하면, 2번과 4번 포트로 들어오는 패킷은 일단 프로토콜 종류에 따라 경로가 결정되고 일치하는 프로토콜이 아닐 경우에는 포트 기반 VLAN을 기준으로 경로가 결정됩니다.

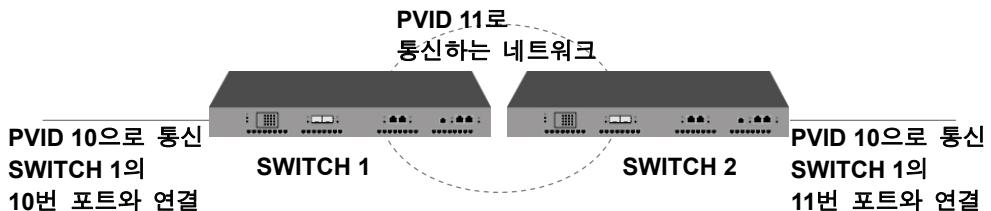
[설정 예제 4] QinQ 설정

SWITCH 1의 10번 포트와 SWITCH 2의 11번 포트는 아래 그림과 같이 다른 VLAN이 설정되어 있는 네트워크와 연결되어 있습니다. PVID 10으로 통신하는 SWITCH 1과 SWITCH 2의 VLAN 설정을 변경하지 않고 QinQ를 사용하여 통신하도록 하려면 다음과 같이 설정합니다.



주의

SWITCH 1과 SWITCH 2의 포트들 중 PVID 11로 통신하는 네트워크에 연결된 포트들은 Tagged VLAN포트로 설정되어야 합니다.



< SWITCH 1 >

```
SWITCH(bridge)# vlan dot1q-tunnel enable 10
SWITCH(bridge)# vlan pvid 10 11
SWITCH(bridge)# show vlan dot1q-tunnel
    Tag Protocol Id : 0x8100 (d: double-tagging port)
    -----
    |      1      2      3
Port | 1234567890123456789012345678901234567890
    -----
    dtag .....d.....
SWITCH(bridge)#

```

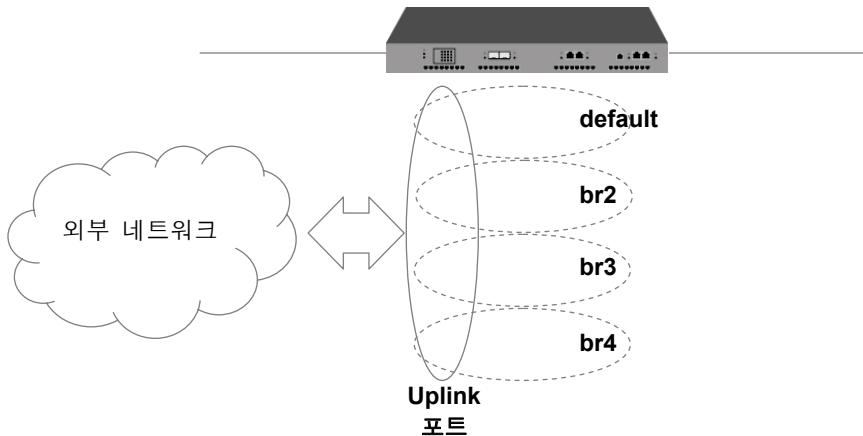
< SWITCH 2 >

```
SWITCH(bridge)# vlan dot1q-tunnel enable 11
SWITCH(bridge)# vlan pvid 11 11
SWITCH(bridge)# show vlan dot1q-tunnel
    Tag Protocol Id : 0x8100 (d: double-tagging port)
    -----
    |      1      2      3
Port | 1234567890123456789012345678901234567890
    -----
    dtag .....d.....
SWITCH(bridge)#

```

[설정 예제 5] FID를 이용한 Shared-VLAN 설정

V2824에 VLAN 2, 3, 4를 설정하고, Uplink 포트인 20번 포트는 모든 VLAN에 속하도록 설정하였습니다. 외부에서 Uplink 포트를 통해 들어오는 Untagged 패킷을 올바르게 전달하기 위해서는 다음과 같이 설정합니다.

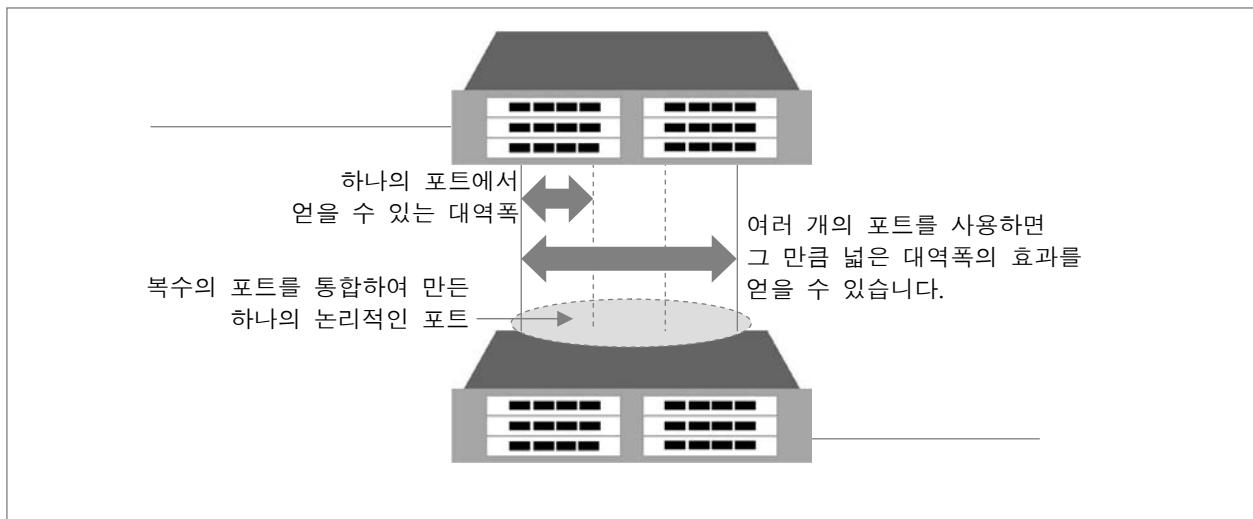


```
SWITCH(bridge)# vlan create 2
SWITCH(bridge)# vlan create 3
SWITCH(bridge)# vlan create 4
SWITCH(bridge)# vlan del 1 3-8
SWITCH(bridge)# vlan add 2 3,4 untagged
SWITCH(bridge)# vlan add 3 5,6 untagged
SWITCH(bridge)# vlan add 4 7,8 untagged
SWITCH(bridge)# vlan add 2 20 untagged
SWITCH(bridge)# vlan add 3 20 untagged
SWITCH(bridge)# vlan add 4 20 untagged
SWITCH(bridge)# vlan create 5
SWITCH(bridge)# vlan add 5 1-34 untagged
SWITCH(bridge)# vlan fid 1-5 5
SWITCH(bridge)# show vlan
              u: untagged port, t: tagged port
-----
|           1           2           3
Name( VID| FID) |1234567890123456789012345678901234567890
-----
default( 1| 5) |uu.....uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
      br2( 2| 5) |..uu.....u.....u.....u.....u.....u.....u.....u
      br3( 3| 5) |.....uu.....u.....u.....u.....u.....u.....u
      br4( 4| 5) |.....uu.....u.....u.....u.....u.....u.....u
      br5( 5| 5) |uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
SWITCH(bridge)#

```

8.3 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 8-8 】 Link Aggregation

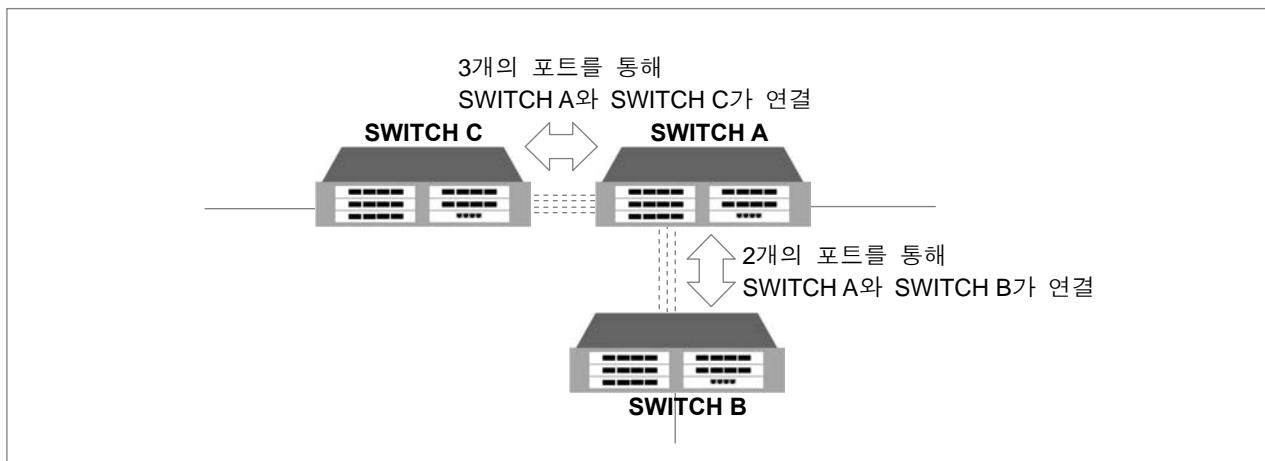


V2824는 Link Aggregation으로 설정한 논리적인 포트를 최대 14개까지 만들 수 있고, 하나의 논리적인 포트에는 물리적인 포트를 8개까지 포함시킬 수 있습니다.

V2824는 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 8-9 】 Link Aggregation 구성 예 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.

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.

이 장에서는 다음과 같이 Link Aggregation을 설명합니다.

- 포트 트렁크
- LACP

8.3.1 포트 트렁크

포트 트렁킹은 두 개 이상의 포트를 하나의 논리적인 포트로 통합함으로써 보다 넓은 대역폭을 사용할 수 있도록 하는 기능입니다. V2824에서는 총 14개의 트렁크 그룹이 제공되며, 이 그룹들은 <0 – 13> 사이의 ID를 가질 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.



참고

*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.



*group-id*는 <0 – 4> 사이에서 입력 가능합니다.



포트 트렁크의 그룹 ID와 LACP의 통합 포트에는 같은 ID가 할당 될 수 없습니다. ID를 설정하실 때 주의하십시오.

(2) 트렁크 그룹 패킷 분배 모드 지정

V2824의 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 지정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
trunk distmode <0-4> {srcdstmac srcdstip srcdstl4 }	Bridge	패킷 분배 모드를 지정합니다.
no trunk distmode <0-4>		설정한 패킷 분배 모드를 해제합니다.



패킷 분배 모드의 기본값은 **srcdstmac**으로 설정되어 있습니다.

패킷 분배의 기준이 되는 각 모드의 의미는 다음과 같습니다.

- **srcdstmac** : Source MAC 주소와 Destination MAC 주소를 동시에 참조합니다.
- **srcdstip** : Source IP 주소와 Destination IP 주소를 동시에 참조합니다.
- **srcdstl4** : Source TCP/UDP와 Destination TCP/UDP를 동시에 참조합니다.

(3) 트렁크 그룹 설정 내용 확인

포트 트렁크 설정을 확인하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show trunk	Global / Enable / Bridge	포트 트렁크 설정 내용을 확인합니다.

8.3.2 LACP

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.

V2824에서는 총 14개의 통합 포트가 제공되며, 이 포트은 <0 – 13> 사이의 ID를 가질 수 있습니다.



주의

포트 트렁크의 그룹 ID와 LACP의 통합 포트에는 같은 ID가 할당 될 수 없습니다. 각 ID를 설정하실 때 주의하십시오.

사용자가 LACP를 설정할 수 있도록 다음의 내용으로 설정 방법을 설명합니다.

- LACP 활성화
- 패킷 경로 규정 설정
- 멤버 포트 설정
- 멤버 포트의 동작 모드 설정
- 멤버 포트 우선 순위 지정
- 멤버 포트의 LACP 참가 여부 설정

- 멤버 포트의 BPDU 전송 주기 설정
- 멤버 포트의 Key 값 설정
- LACP 장비 우선 순위 지정
- LACP 설정 내용 확인
- LACP 통계 확인
- LACP 통계 삭제
- 설정 예제

(1) LACP 활성화

V2824 LACP의 통합 포트를 설정하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lacp aggregator <i>aggregator-id</i>	Bridge	통합 포트를 설정합니다.
no lacp aggregator <i>aggregator-id</i>		통합 포트를 해제합니다.



*aggregator-id*는 <0 – 13> 사이에서 입력 가능합니다.



*aggregation-id*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 *aggregation-id*를 입력하십시오.



주의

포트 트렁크의 그룹 ID와 LACP의 통합 포트에는 같은 ID가 할당 될 수 없습니다. ID를 설정하실 때 주의하십시오.

(2) 패킷 경로 규정 설정

V2824의 통합 포트로 들어오는 패킷들은 지정된 기준에 따라 각 멤버 포트에 분산되어 처리됩니다. 이 방법은 특정 멤버 포트로의 트래픽 집중을 방지하여 보다 안정적이고 효율적인 통합 포트 운영이 가능하도록 합니다.

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.

LACP 통합 포트의 패킷 분배 모드를 지정하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lacp aggregator distmode aggregatr-id {srcmac dstmac srcdstmac srcip dstip srcdstip}	Bridge	패킷 분배 모드를 지정합니다.



참 고

*aggregation-id*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 *aggregation-id*를 입력하십시오.

(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	멤버 포트를 설정합니다.
no lacp port port-number		멤버 포트를 해제합니다.



참 고

*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.

(4) 멤버 포트의 동작 모드 설정

멤버 포트를 설정한 후에는 멤버 포트의 동작 모드를 설정하십시오. 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 링크가 이루어지지 않습니다.

멤버 포트의 모드를 설정하려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오. 멤버 포트의 기본 동작 모드는 Active입니다.

명령어	모 드	기 능
lacp port activity port-number {active passive}	Bridge	멤버 포트의 동작 모드를 설정합니다.
no lacp port activity port-number		멤버 포트의 동작 모드를 해제합니다.



참 고

*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.

(5) 멤버 포트 우선 순위 지정

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 순위를 지정할 수 있습니다.

LACP의 멤버 포트에 우선 순위를 지정하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lacp port priority port-number priority	Bridge	멤버 포트의 우선 순위를 지정합니다.
no lacp port priority port-number		멤버 포트의 우선 순위를 해제합니다.



*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.



*priority*는 <1 – 65, 535> 사이에서 설정 가능합니다. 기본적으로 *priority*는 32768(=0x8000)로 설정되어 있습니다.

(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.
no lacp port aggregation port-number		LACP 참가 여부를 해제합니다.



참 고

V2824는 기본적으로 멤버 포트가 LACP에 참가하도록 설정되어 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.

(7) 멤버 포트의 BPDU 전송 주기 설정

멤버 포트는 일정한 주기로 자신의 정보를 담은 BPDU를 전송합니다. V2824는 BPDU 전송 주기를 설정할 수 있는데, BPDU 전송 주기를 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lacp port timeout port-number {short long}	Bridge	멤버 포트의 BPDU 전송 주기를 설정합니다.
no lacp port timeout port-number		멤버 포트의 BPDU 전송 주기를 해제합니다.



참 고

short의 전송 주기는 1초, **long**의 전송 주기는 30초입니다. V2824는 기본적으로 멤버 포트의 BPDU 전송 주기가 **long**입니다.



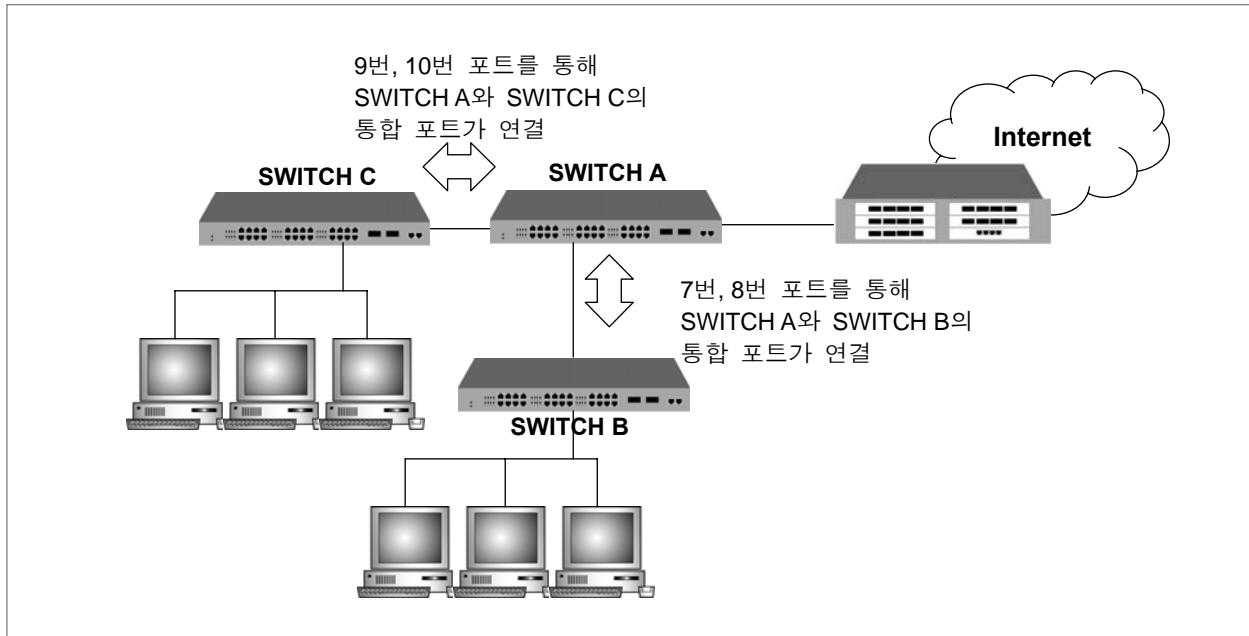
참 고

*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) 멤버 포트의 Key 값 설정

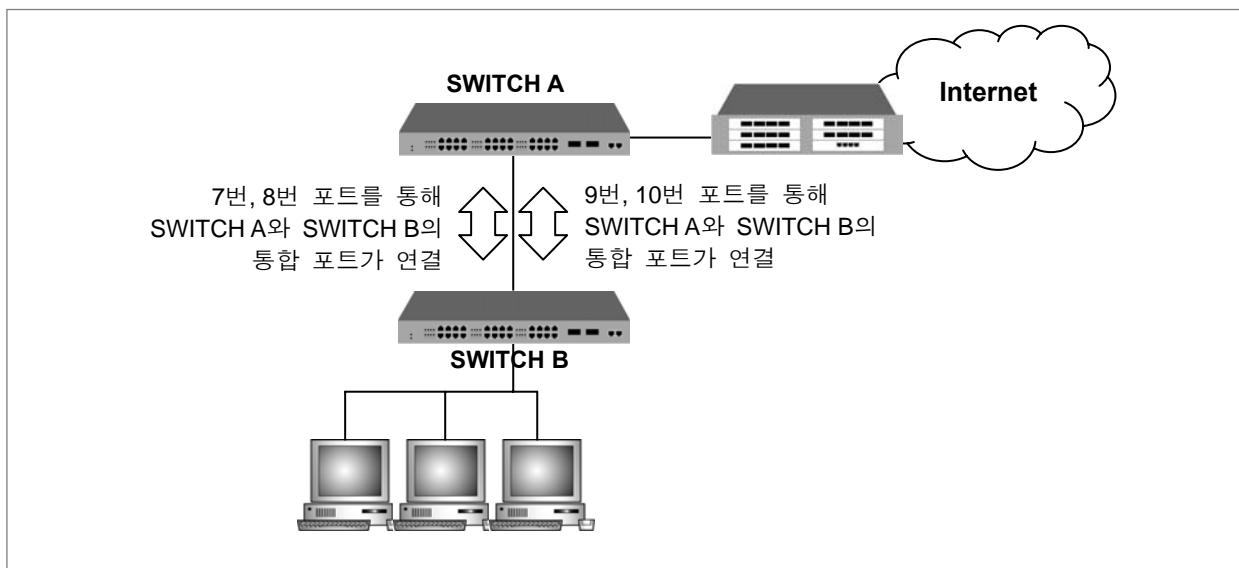
LACP의 멤버 포트는 Key 값을 가지고 있습니다. 동일한 통합 포트에 속해 있는 멤버 포트들은 모두 동일한 Key 값을 가지고 있습니다. 따라서 특정한 멤버 포트로만 이루어진 하나의 통합 포트를 만들려면 다른 통합 포트에 속한 멤버 포트와 구별되는 Key 값을 설정해주면 됩니다.

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 8-10 】 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 8-11 】 LACP의 구성예 ②

멤버 포트의 Key 값을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lacp port admin-key port-number key	Bridge	멤버 포트의 Key 값을 설정합니다.
no lacp port admin-key port-number		멤버 포트의 Key 값을 해제합니다.



*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.



Key는 <1 – 15> 사이에서 설정 가능합니다. Key 값은 기본으로 1로 설정되어 있습니다.

(9) LACP 장비 우선 순위 지정

서로 연결된 두 장비의 멤버 포트가 모두 active 모드로 설정되어 있는 경우에는 어떤 장비를 기준으로 정할 것인지에 대한 우선 순위를 정해야 할 필요가 있습니다. V2824에서는 이러한 경우를 대비해서 장비 우선 순위 지정이 가능합니다.

서로 연결된 두 장비의 멤버 포트가 각각 **active** 모드와 **passive** 모드로 설정되면 **active** 모드로 설정된 장비가 기준이 되고, 모두 **active** 모드로 설정되어 있으면 우선 순위 값이 높은 장비가 기준이 됩니다.

LACP 장비 우선 순위를 지정하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
lacp system priority <i>priority</i>	Bridge	LACP의 장비 우선 순위를 지정합니다.
no lacp system priority		LACP의 장비 우선 순위를 해제합니다.



참 고

*priority*는 <1 – 65, 535> 사이에서 설정 가능합니다. 기본적으로 *priority*는 32768(=0x8000)로 설정되어 있습니다.

(10) LACP 설정 내용 확인

LACP 설정 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show lacp aggregator [<i>aggregator-id</i>]	Enable / Global / Bridge	통합 포트의 설정 내용을 확인합니다.
show lacp port [<i>port-number</i>]		멤버 포트의 설정 내용을 확인합니다.



*aggregation-id*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 *aggregation-id*를 입력하십시오.



*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.

(11) LACP 통계 확인

LACP 관련 통계를 확인하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show lacp statistic	Enable / Global / Bridge	LACP 관련 통계를 확인합니다.

(12) LACP 통계 삭제

LACP 관련 통계를 삭제하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear lacp statistic	Enable/Global/Bridge	LACP 관련 통계를 삭제합니다.

(13) 설정 예제

[설정 예제 1] 포트 트렁크 설정①

다음은 17번, 18번의 포트를 0번 트렁크로 설정하고, 설정한 내용을 확인한 경우의 예입니다.

```
SWITCH(bridge)# trunk add 0 17,18 srcmac
SWITCH(bridge)# show trunk
Trunk Group 0 : SRC_MAC : 17(o) 18(x)
Trunk Group 1 : Inactive
Trunk Group 2 : Inactive
Trunk Group 3 : Inactive
Trunk Group 4 : Inactive
Trunk Group 5 : Inactive
Trunk Group 6 : Inactive
Trunk Group 7 : Inactive
Trunk Group 8 : Inactive
Trunk Group 9 : Inactive
Trunk Group 10 : Inactive
Trunk Group 11 : Inactive
Trunk Group 12 : Inactive
Trunk Group 13 : Inactive
```

```
SWITCH(bridge)# show vlan
      u: untagged port, t: tagged port
-----
|           1           2           3
Name( VID| FID) |1234567890123456789012345678901234567890
-----
default( 1| 1) |uuuu.uuuuuuuuuuuuu..uuuuuuuuuuuuuuuuuuuuuuuuuuuu
br2( 2| 2) |....u.....
SWITCH(bridge)#

```

[설정 예제 2] 포트 트렁크 설정②

다음은 br2에 속해 있는 17번, 18번 포트를 default VLAN에 속해 있는 0번 트렁크로 통합했을 때의 설정 방법입니다. 17번, 18번 포트를 트렁크 설정 전과 동일한 상태로 만들려면 통합 포트를 br2에 속하도록 설정해주어야 합니다.

```
SWITCH(bridge)# show vlan
      u: untagged port, t: tagged port
-----
|           1           2           3           4
Name( VID| FID) |1234567890123456789012345678901234567890
-----
default( 1| 1) |uuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu
br2( 2| 2) |.....
SWITCH(bridge)# vlan add 2 17,18 untagged
SWITCH(bridge)# show vlan
      u: untagged port, t: tagged port
-----
|           1           2           3           4
Name( VID| FID) |1234567890123456789012345678901234567890
-----
default( 1| 1) |uuuuuuuuuuuuuuuu..uuuuuuuuuuuuuuuuuuuuuuuuuu
br2( 2| 2) |....uu.....
SWITCH(bridge)# trunk add 0 17,18 srcdstmac
SWITCH(bridge)# show vlan
      u: untagged port, t: tagged port
-----
|           1           2           3           4
Name( VID| FID) |1234567890123456789012345678901234567890
-----
default( 1| 1) |uuuuuuuuuuuuuuuu..uuuuuuuuuuuuuuuuuuuuuuuuuu
br2( 2| 2) |.....
SWITCH(bridge)# vlan del default 27
SWITCH(bridge)# vlan add 2 27 untagged

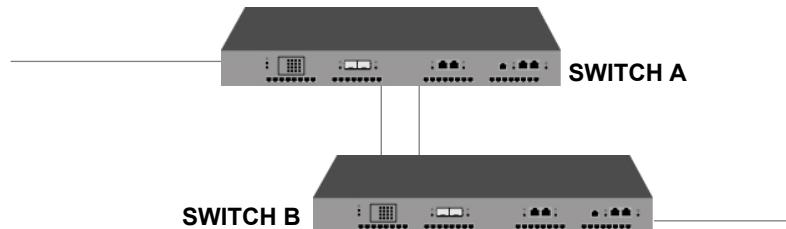
```

```
SWITCH(bridge)# show vlan
      u: untagged port, t: tagged port
-----
|       1       2       3       4
Name( VID| FID) |1234567890123456789012345678901234567890
-----
default( 1| 1) |uuuuuuuuuuuuuuuu..uuuuuuuu.uuuuuuuuuuuuuu
      br2( 2| 2) |.....u.....
SWITCH(bridge)#

```

[설정 예제 3] LACP 설정

다음은 SWITCH A와 SWITCH B에 Aggregator 0를 설정하고, 2번, 3번 포트를 멤버 포트로 설정한 후 그 내용을 확인한 경우입니다. 이 때, 무조건 SWITCH A를 기준이 되도록 하려면, SWITCH B의 멤버 포트 동작 모드를 “**Passive 모드**”로 설정하시면 됩니다. 멤버 포트의 동작 모드를 설정하지 않으면 두 장비 사이에서 자동적으로 기준이 되는 장비가 선출 됩니다.



<SWITCH A에서의 설정>

```
SWITCH_A(bridge)# lacp aggregator 0
SWITCH_A(bridge)# lacp aggregator distmode 0 srcdstmac
SWITCH_A(bridge)# lacp port 1-3
SWITCH_A(bridge)# show lacp aggregator
AGGR ACTOR SYSTEM          PARTNER SYSTEM          MEMBER
----- ----- ----- ----- -----
0  8000.00d0cb-00017b  8000.00d0cb-08002f  2(o)-3(o)  멤버 포트간에 Link가
                                                               형성됐을 때 보여집니다.

SWITCH_A(bridge)# show lacp port
PORT AGGR (A) KEY (P) PORT          (P) KEY (A)-(P) ACTIVITY
----- ----- ----- ----- -----
01     -    1000  00d0cd-08002f(P 1) 100a    ACTIVE - ACTIVE
02     -    1000  00d0cd-08002f(P 2) 100a    ACTIVE - ACTIVE

SWITCH_A(bridge)#

```

<SWITCH B에서의 설정>

```
SWITCH_B(bridge)# lacp aggregator 0
SWITCH_B(bridge)# lacp aggregator distmode 0 srcdstmac
SWITCH_B(bridge)# lacp port 1-3
SWITCH_B(bridge)# lacp port activity 1-3 passive
SWITCH_A(bridge)# show lacp aggregator
AGGR ACTOR SYSTEM          PARTNER SYSTEM        MEMBER
----- ----- ----- ----- -----
0  8000.00d0cb-08002f 8000.00d0cb-00017b 2(o)-3(o) 멤버 포트간에 Link가
                                                               형성됐을 때 보여집니다.

SWITCH_A(bridge)# show lacp port
SWITCH_A(bridge)# show lacp port
PORT AGGR (A) KEY (P) PORT          (P) KEY (A)-(P) ACTIVITY
----- ----- ----- ----- -----
01     -    1000  00d0cd-08002f(P 1) 100a   ACTIVE - ACTIVE
02     -    1000  00d0cd-08002f(P 2) 100a   ACTIVE - ACTIVE

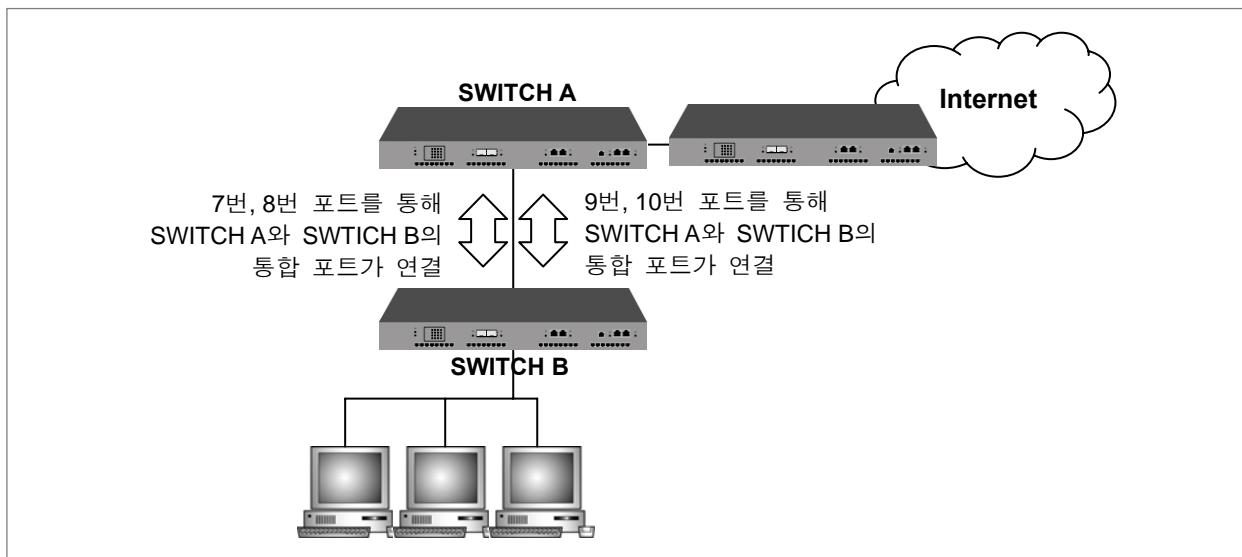
SWITCH_A(bridge)#

```



"show lacp port" 명령어를 사용하였을 때 보여지는 정보 가운데 "AGGR"이 나타내는 것은 Aggregator의 ID입니다. 사용자가 Aggregator를 설정할 때 입력하는 Aggregator-number와는 다릅니다.

[설정 예제 4] Admin-key 설정



다음은 위의 그림과 같이 SWITCH A와 SWITCH B의 7번, 8번 포트와 9번, 10번 포트를 각각 다른 포트로 통합하도록 설정하는 경우의 예입니다. 일단 Key 값을 변경하지 않은 상태에서 SWITCH A와 SWITCH B에 두 개의 통합 포트와 7번부터 10번까지의 포트를 멤버 포트로 각각에 설정한 경우입니다.

<SWITCH A>

```
SWITCH_A(bridge)# lacp aggregator 0
SWITCH_A(bridge)# lacp aggregator 1
SWITCH_A(bridge)# lacp aggregator distmode 0 srcdstmac
SWITCH_A(bridge)# lacp port 7-10
SWITCH_A(bridge)# show lacp aggregator

AGGR  PRIORITY          PARTNER          MEMBER
----  -----  -----
0      0x8000.00D0CB0A01B3 00D0CB0AA790  eth07(o)-eth08(o)-eth09(o)-eth10(o)
1      0x8000.000000000000
SWITCH_A(bridge)#

```

<SWITCH B>

```
SWITCH_B(bridge)# lacp aggregator 0
SWITCH_B(bridge)# lacp aggregator 1
SWITCH_B(bridge)# lacp aggregator distmode 0 srcdstmac
SWITCH_B(bridge)# lacp port 7-10

SWITCH_B(bridge)# lacp port activity 7-10 passive
SWITCH_A(bridge)# show lacp aggregator
SWITCH_B(bridge)# show lacp aggregator

AGGR  PRIORITY          PARTNER          MEMBER
----  -----  -----
0      0x8000.00D0CB0A01B3 00D0CB0AA790  eth07(o)-eth08(o)-eth09(o)-eth10(o)
1      0x8000.000000000000
SWITCH_B(bridge)#

```

위에서 설정 내용을 확인한 결과, 하나의 통합 포트에 4개의 포트가 통합되었음을 알 수 있습니다. 그러나, SWITCH A와 SWITCH B에 7번, 8번 포트와 9번, 10번 포트의 Key 값이 다르도록 다음과 같이 설정해 주면 두 개의 통합 포트가 생성되는 것을 볼 수 있습니다.

<SWITCH A>

```
SWITCH_A(bridge)# lacp port admin-key 9-10 2
SWITCH_A(bridge)# show lacp aggregator

AGGR  PRIORITY          PARTNER          MEMBER
-----  -----
0      0x8000.00D0CB0A01B3 00D0CB0AA790 eth07(o)-eth08(o)
1      0x8000.000000000000 00D0CB0AA790 eth09(o)-eth10(o)

SWITCH_A(bridge)#+
```

<SWITCH B>

```
SWITCH_B(bridge)# lacp port admin-key 9-10 2
SWITCH_B(bridge)# show lacp aggregator

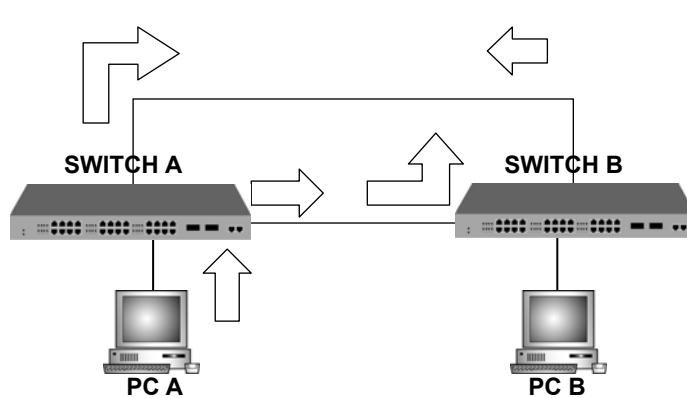
AGGR  PRIORITY          PARTNER          MEMBER
-----  -----
0      0x8000.00D0CB0A01B3 00D0CB0AA46C eth07(o)-eth08(o)
1      0x8000.000000000000 00D0CB0AA46C eth09(o)-eth10(o)

SWITCH_B(bridge)#+
```

8.4 STP

토큰 링 방식과 같이 이중 경로로 구성된 LAN은 하나의 경로가 끊어지더라도 또 다른 경로를 통하여 통신이 가능하다는 장점을 가집니다. 그러나, 항상 두 가지 경로를 사용하다 보면 루프 현상이라고 하는 또 다른 문제가 발생하게 됩니다.

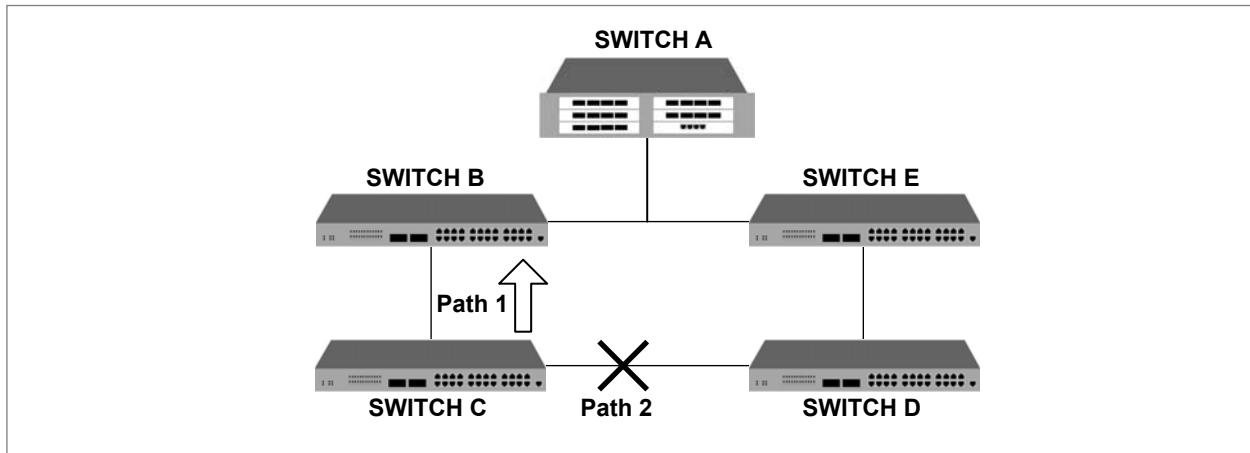
루프(Loop) 현상이란, 아래의 그림과 같이 SWITCH A와 SWITCH B 사이에 두 개 이상의 경로가 존재할 때 PC A에서 브로드캐스트나 멀티캐스트로 패킷이 전송되면 패킷이 계속 회전하게 되는 것을 말하며 이러한 현상이 발생하면 불필요한 데이터가 계속해서 전송되기 때문에 네트워크가 불안정해집니다.



【 그림 8-12 】 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 표준 안에 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 8-13 】 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
- RSTP의 동작 원리
- PVSTP 와 MSTP
- STP 모드 설정
- STP/RSTP/MSTP 설정
- PVSTP/PVRSTP 설정
- BPDU 전송 설정
- BPDU Filtering 설정
- Point-to-Point MAC 설정
- STP 모드 변경 감지
- STP Guard 설정
- 설정 예제

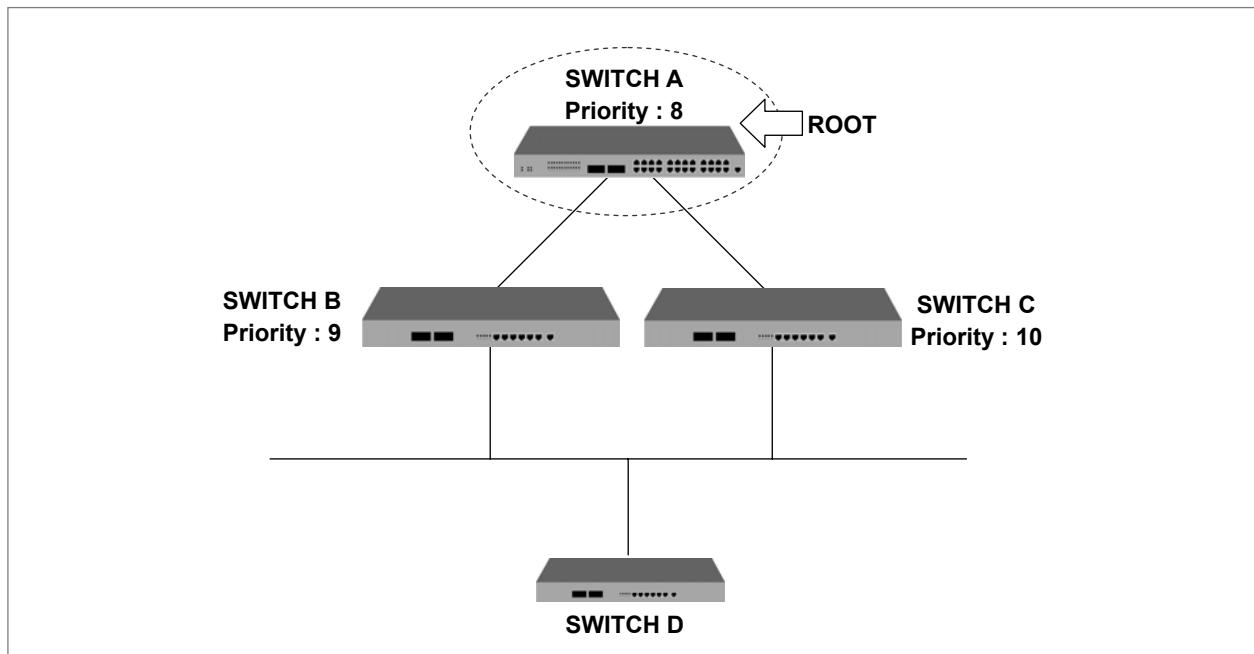
8.4.1 STP 동작 원리

802.1d의 STP에서는 포트 상태를 Blocking, Listening, Learning, Forwarding의 네 가지로 정의합니다. 이중 경로를 가지고 있는 LAN에 STP를 설정하면 스위치들은 Bridge ID를 포함한 자신의 정보를 교환하게 되는데 이를 BPDU(Bridge Protocol Data Unit)라고 합니다.

스위치들은 서로 주고 받은 BPDU를 바탕으로 포트의 상태를 결정하고, Spanning-Tree의 기준이 되는 Root 스위치와 Root 스위치와 통신할 때의 최적 경로를 자동적으로 결정합니다.

◆ Root 스위치

Root 스위치를 결정하는 중요한 정보는 바로 Bridge ID입니다. Bridge ID는 2Bytes로 된 Priority와 6Bytes로 된 MAC 주소로 구성되는데, Bridge ID가 가장 작은 것을 Root 스위치로 결정합니다.

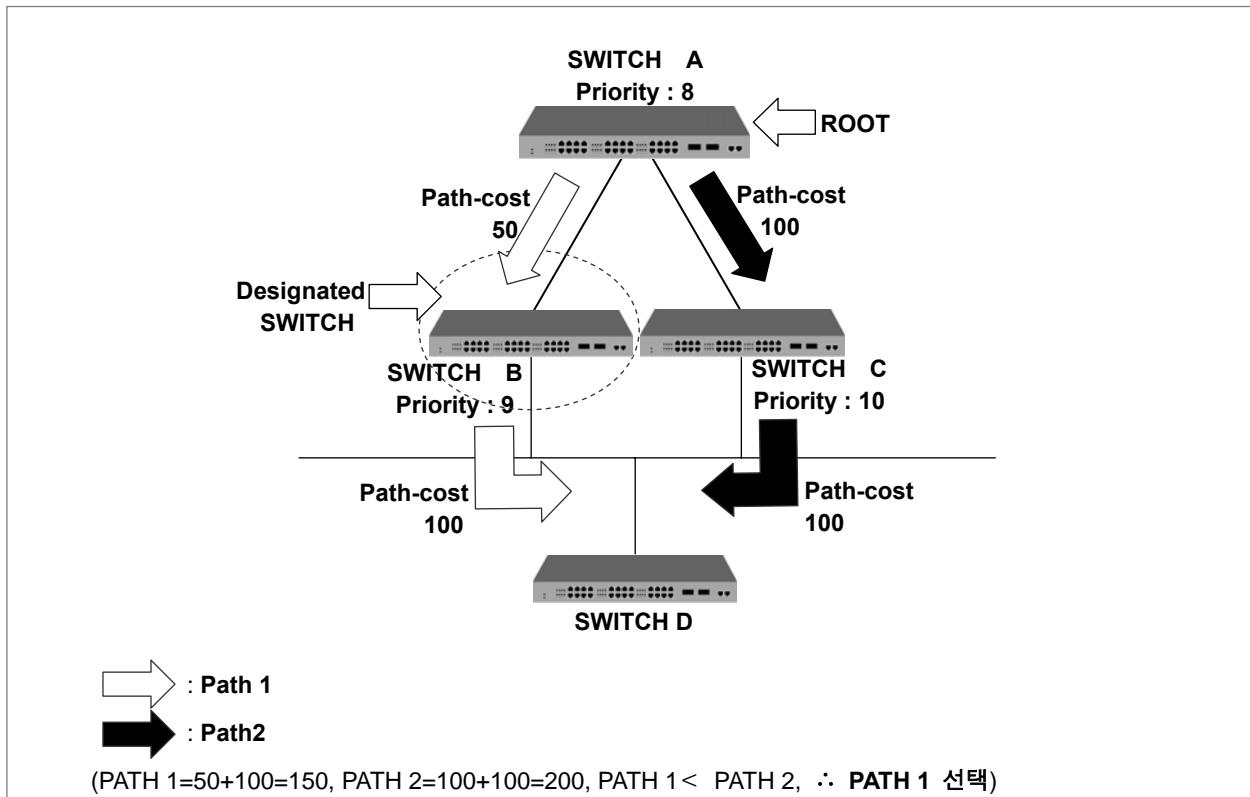


【 그림 8-14 】 Root 스위치

예를 들어 위의 그림과 같이 스위치 3개가 연결되어 있다고 가정합니다. STP 기능을 설정하면 스위치들은 서로 자신의 정보를 교환합니다. 이 때 SWITCH A의 Priority가 8, SWITCH B의 Priority가 9, SWITCH C의 Priority가 10이라고 하면, 자동적으로 SWITCH A가 Root 스위치로 설정됩니다.

◆ Designated 스위치

Root 스위치가 결정된 후 SWITCH A에서 패킷을 전송해야 하는 상황이 되었을 때, SWITCH A는 서로 주고 받은 BPDU를 비교하여 Designated 스위치를 선택, 어떤 경로를 사용할지를 결정합니다. Designated 스위치는 하나의 세그먼트 안에서 통신이 이루어질 수 있도록 선택된 스위치입니다. Designated 스위치를 선택할 때 기준이 되는 것은 Root 스위치까지의 path-cost를 합산한 Root path-cost입니다. Path-cost는 스위치의 LAN 인터페이스 전송 속도에 따라 정해지며 path-cost 값이 작은 경로에 있는 스위치가 Designated 스위치가 됩니다.



【 그림 8-15 】 Designated 스위치 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 스위치가 Designated 스위치로 선택됩니다.

i 참고

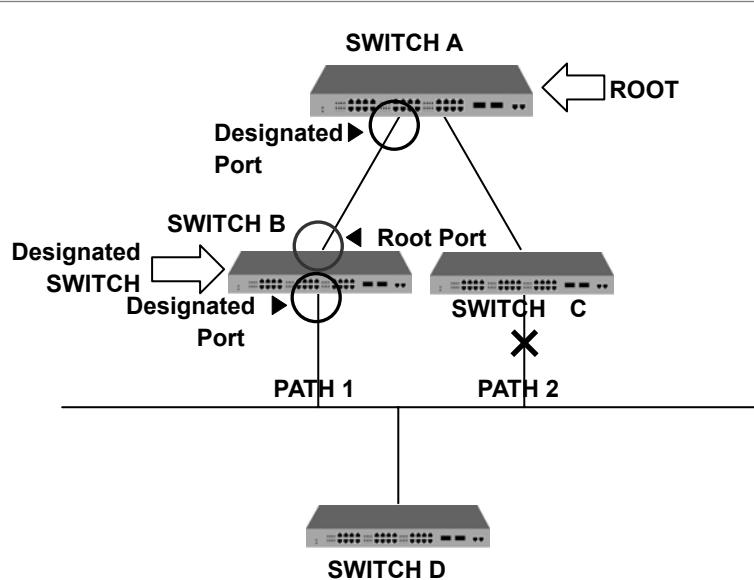
Designated 스위치를 선택할 때에는 Root 까지의 path-cost를 합산한 Root path-cost를 비교합니다. Root path-cost가 작은 쪽이 Designated 스위치로 결정됩니다. Root path-cost가 동일할 경우에는 Bridge ID를 비교합니다.

◆ Designated 포트와 Root 포트

아래의 그림에서 Root 스위치에서 SWITCH D로 패킷이 전송된다고 가정을 합니다. 일단 SWITCH B와 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 스위치는 SWITCH B가 됩니다.

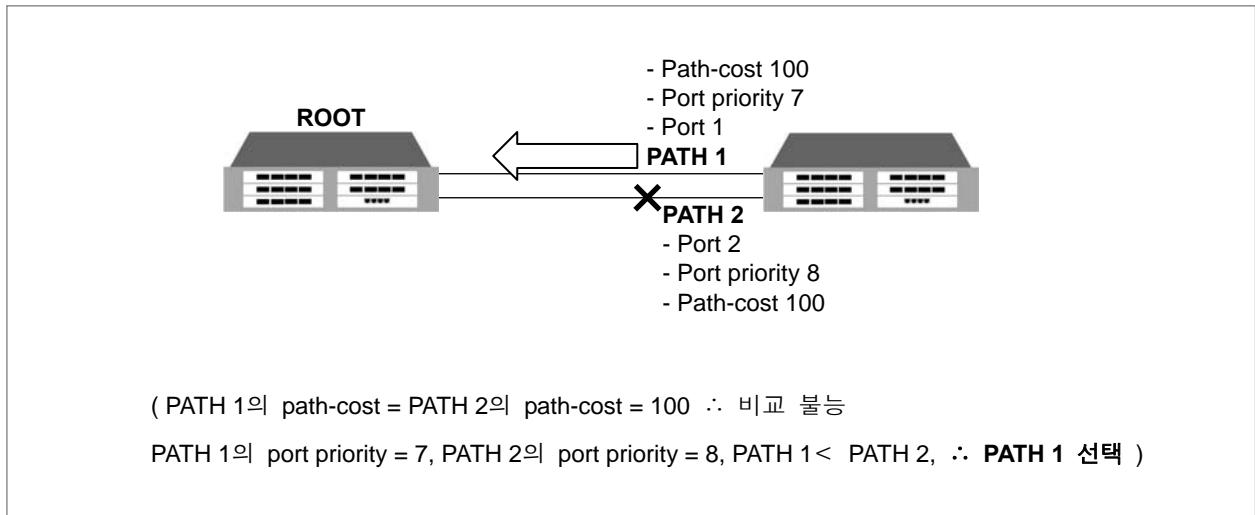
이 때 Root 스위치에 연결되는 포트를 Root 포트라고 합니다. 아래의 그림과 같은 경우에는 Root 스위치인 SWITCH A와 연결되는 SWITCH B의 포트가 Root 포트가 됩니다. 하나의 장비에 Root 포트는 한 개만 존재할 수 있습니다. 각 장비에서 Root 포트를 제외하고, 통신이 이루어지도록 선택된 포트는 Designated 포트입니다. 또한, Root 포트와 Designated 포트를 제외한 통신이 이루어지지 않는 포트는 Blocked 포트라고 합니다.



【 그림 8-16 】 Designated 스위치와 Designated 포트

◆ Port-priority

한편, 두 경로의 path-cost가 동일한 경우에는 port-priority가 경로를 결정하는 기준이 됩니다. 다음과 같이 2개의 스위치가 연결되어 있다고 가정합니다. 두 경로의 path-cost가 100으로 똑같을 때에는 port-priority를 비교, 값이 작은 포트가 root 포트로 선택되어 패킷을 전송합니다.



【 그림 8-17 】 Port priority를 사용한 결정

이 모든 동작 원리는 이미 각 스위치가 가지고 있는 정보인 BPDU를 통해 자동적으로 결정되지만, V2824의 사용자는 Root 스위치나 경로를 인위적으로 변경하기 위해 BPDU의 값을 설정해 줄 수 있습니다. 설정 방법은 **BPDU (Bridge Protocol Data Unit) 전송 설정**에 나와 있습니다.

8.4.2 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.

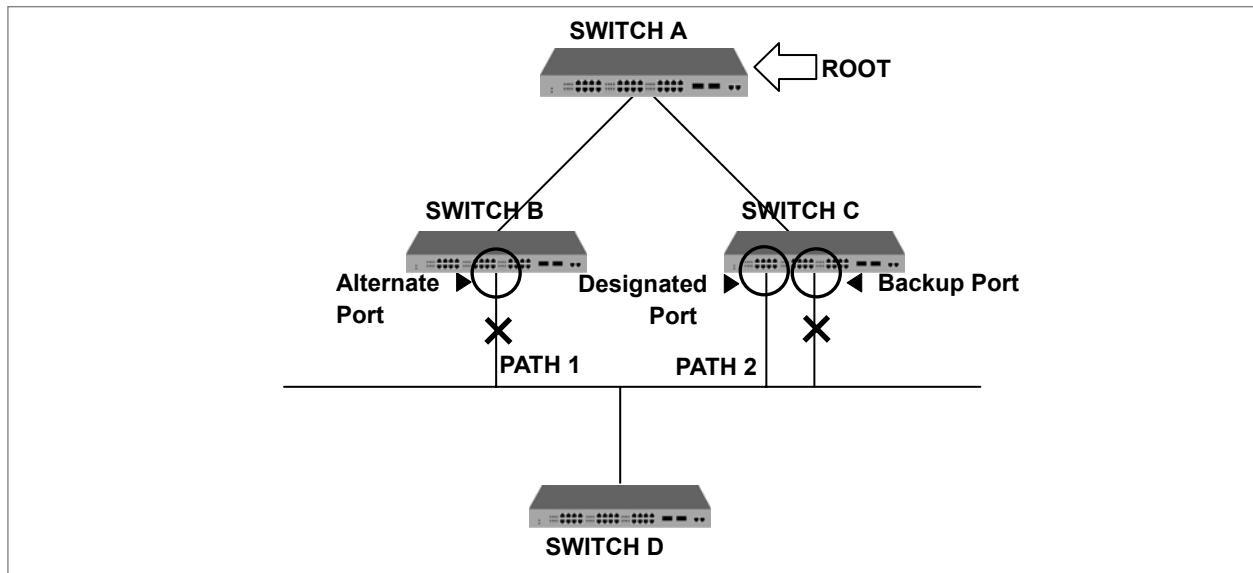
- 포트 상태의 변화
- BPDU 정책 변화
- 네트워크 convergence 시간 단축
- 802.1d와의 호환성

(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 8-18 】 Alternate 포트와 Backup 포트

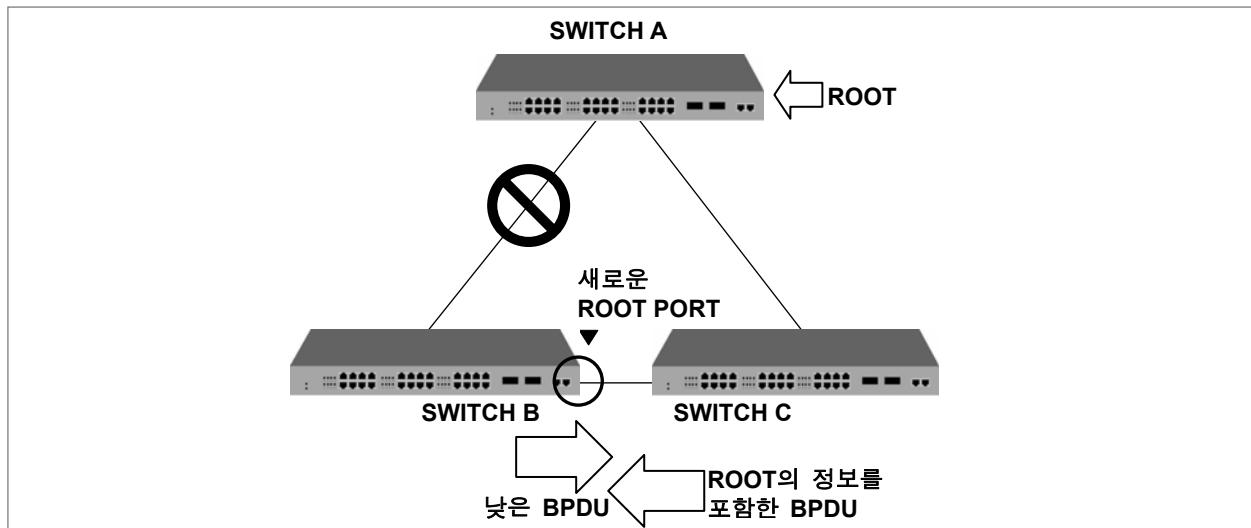
Alternate 포트와 Backup 포트의 차이점은 위의 그림에서 Root 스위치와 SWITCH C 사이에 문제가 발생하였을 때 패킷의 경로를 대체해줄 수 있지만, Backup 포트는 Root 스위치와 SWITCH C 사이에 문제가 발생하여도 끊임없는 접속을 보장할 수는 없다는 것입니다.

(2) BPDU 정책 변화

802.1d는 Root 스위치만 설정된 Hello-time에 따라 BPDU를 전송하고, Root 스위치를 제외한 다른 스위치는 Root 스위치로부터 BPDU를 받았을 때에만 자신의 BPDU를 전송하였습니다.

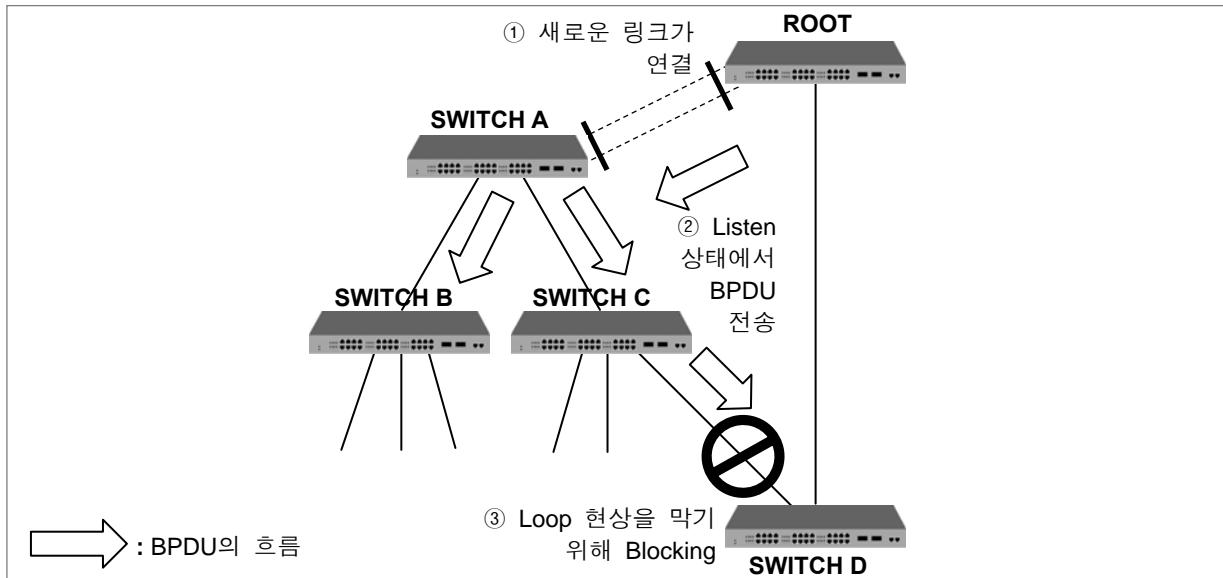
그러나 802.1w는 Root 스위치가 아닌 모든 스위치도 Hello-time에 따라 BPDU를 전송합니다. BPDU는 실제로 Root 스위치에 의해 주고받는 시간 간격보다 더 자주 변화하는데 802.1w에서는 변화하는 네트워크 환경에 더욱 빨리 대응할 수 있게 되었습니다.

한편, Root 스위치나 Designated 스위치로부터 낮은 BPDU를 받았을 경우에는 이를 즉시 받아들입니다. 예를 들어, 아래의 그림과 같이 Root 스위치와 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.



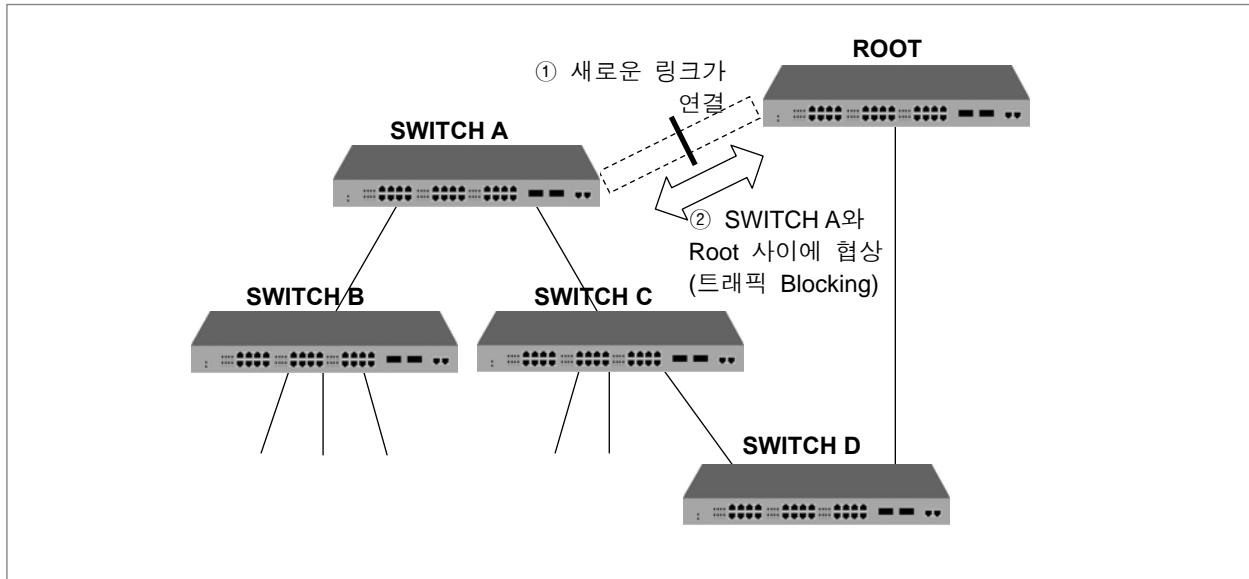
【 그림 8-19 】 낮은 BPDU를 받아들이는 경우

(3) 네트워크 convergence 시간 단축



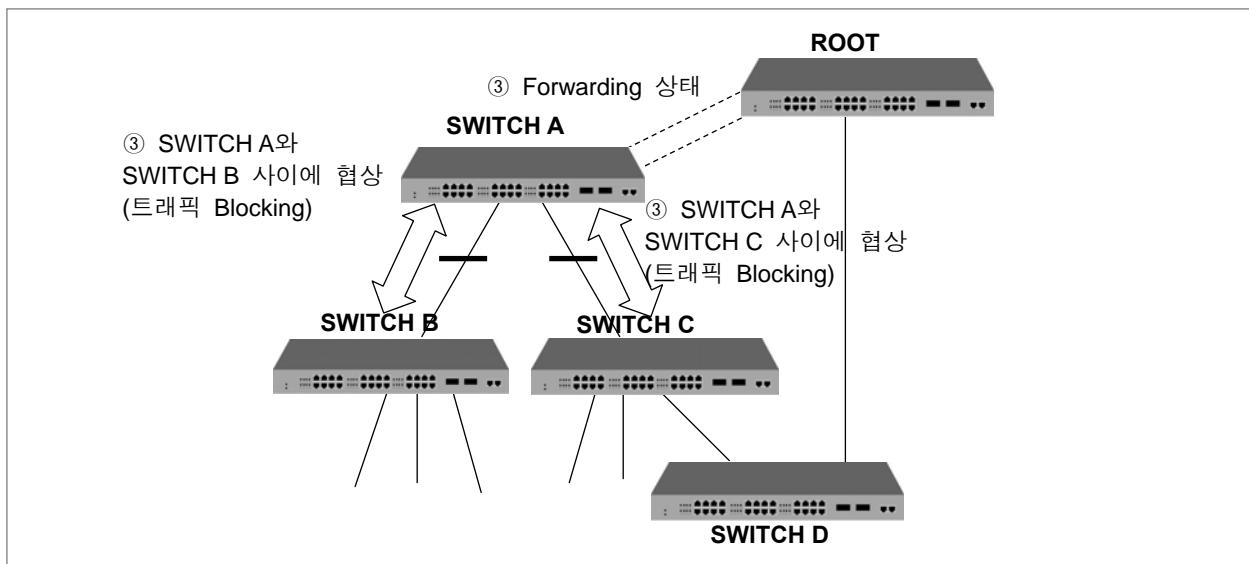
【 그림 8-20 】 802.1d의 네트워크 convergence

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 스위치는 일단 두 스위치는 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.



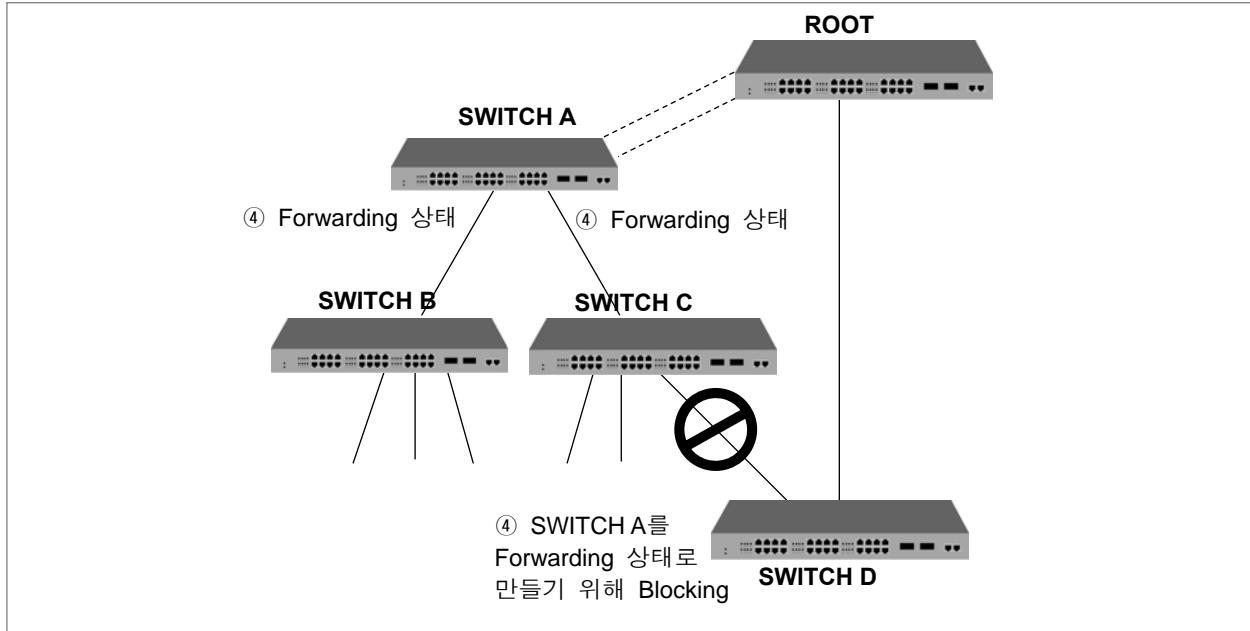
【 그림 8-21 】 802.1w의 네트워크 convergence ①

BPDUs를 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 8-22 】 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.

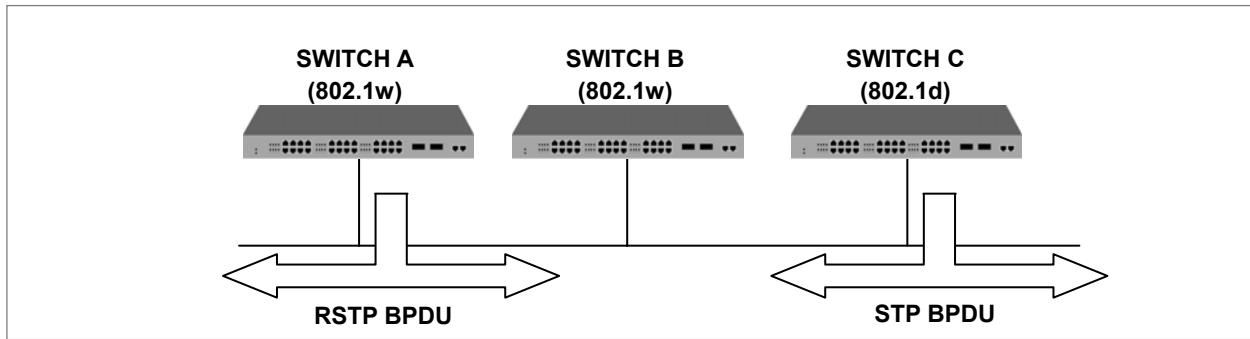


【 그림 8-23 】 802.1w의 네트워크 convergence ③

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.

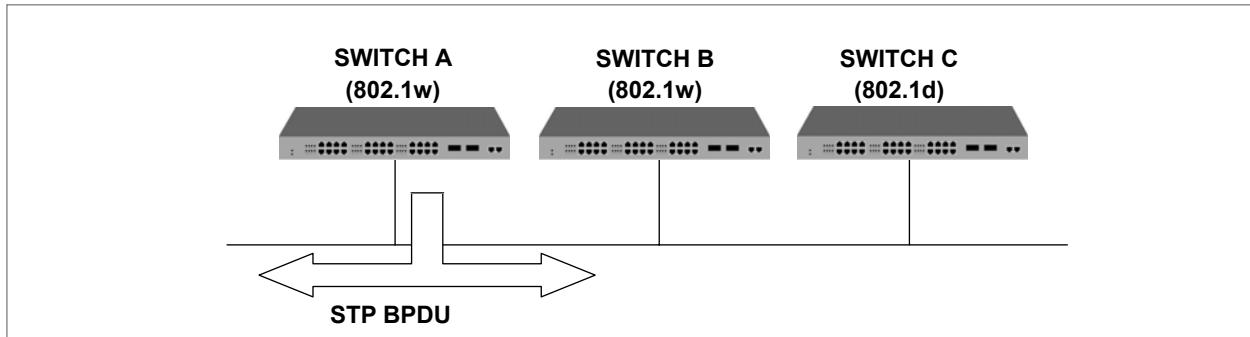
(4) 802.1d와의 호환성

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 스위치로 SWITCH C와 연결이 이루어졌다고 가정합시다. 802.1d인 SWITCH C는 RSTP BPDU를 무시하고 버리기 때문에 SWITCH C는 어떤 스위치나 세그먼트와도 연결되어 있지 않다고 판단합니다.



【 그림 8-24 】 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 스위치로 받아들입니다.



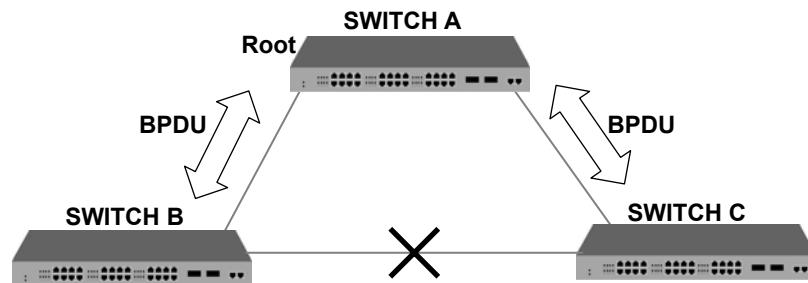
【 그림 8-25 】 STP와의 호환 ②

8.4.3 PVSTP 와 MSTP

좀 더 효율적으로 망을 운영하기 위하여 V2824는 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.

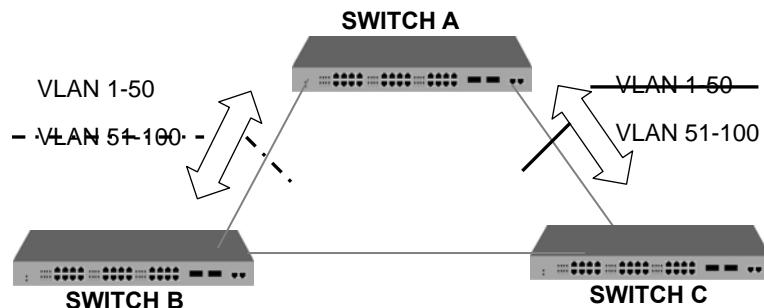
MSTP를 사용하면, 별도의 RSTP를 구현하지 않고도 토플로지 변경 시 트리 재구성 시간을 최소화 할 수 있습니다.

다음은 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.



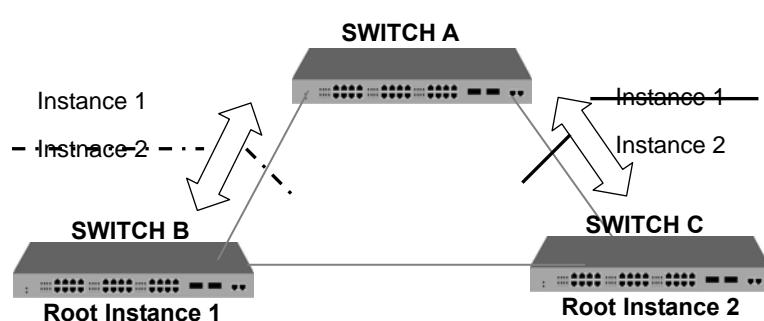
【 그림 8-26 】 STP

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 스위치의 부하가 걸리는 단점이 있습니다.



【 그림 8-27 】 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.

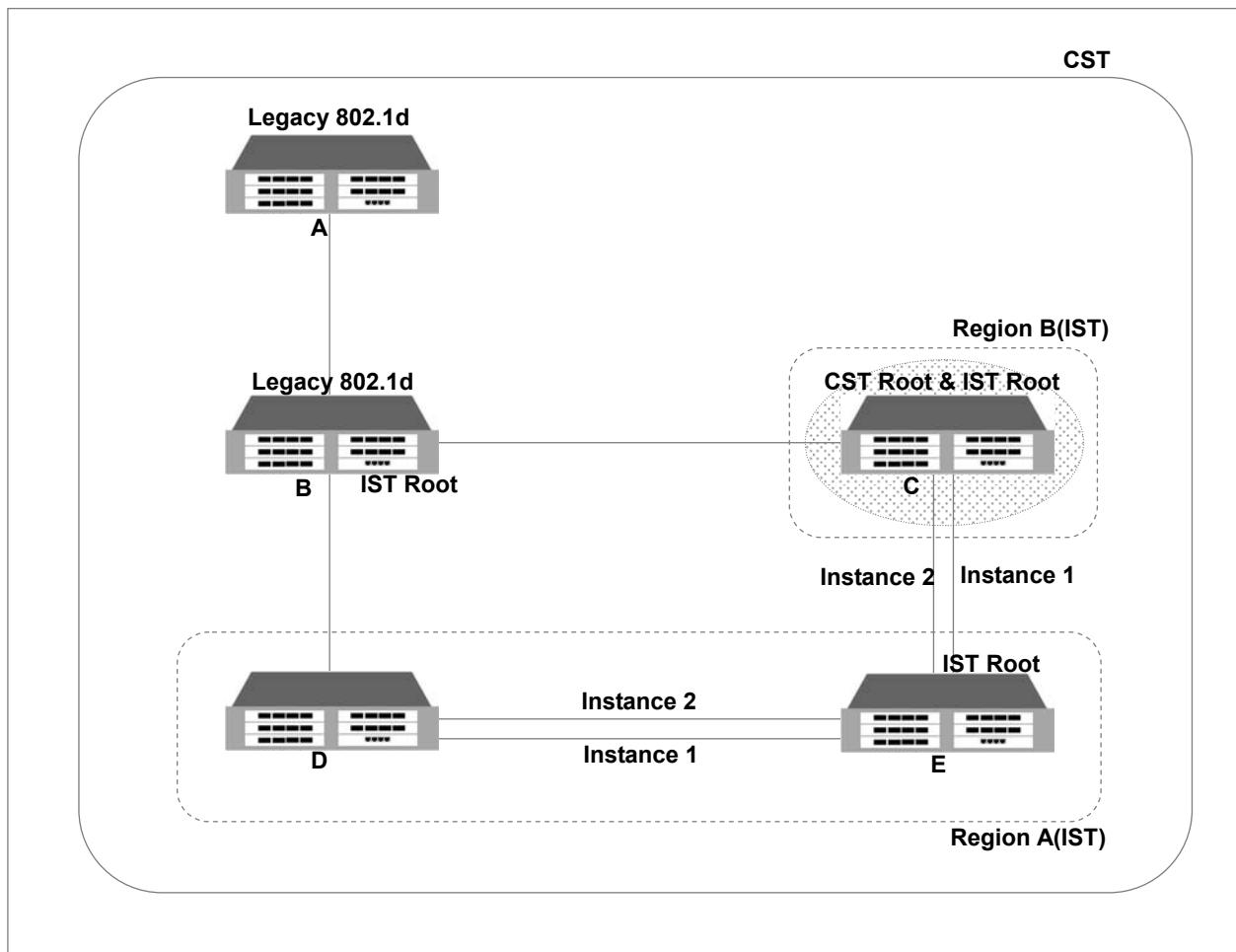


【 그림 8-28 】 MSTP

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.

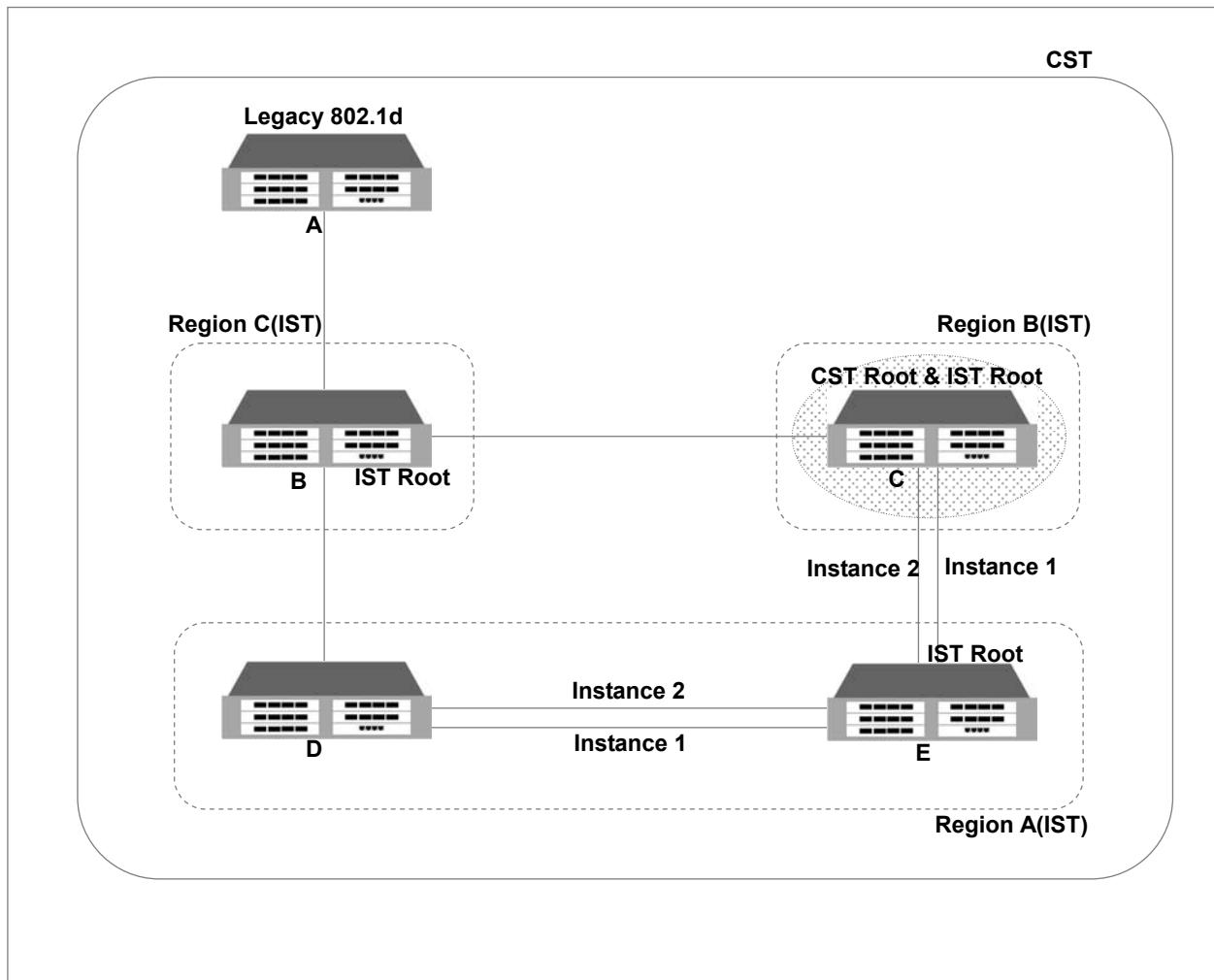
각 Region에는 오직 하나의 STP가 구동 되기 때문에 PVSTP에 비해 STP수를 줄일 수 있고, 이에 따라 BPDU 트래픽을 줄일 수 있습니다. 하나의 네트워크 환경에서 설정할 수 있는 Region 수는 제한이 없지만, Instance는 최대 64개까지만 생성 할 수 있습니다. 따라서 Instance는 1부터 64까지 설정할 수 있습니다. 각 Region에서 동작하는 Spanning-Tree를 IST(Internal Spanning-Tree)라고 합니다. 그리고, Region의 Spanning-Tree를 각각 연계했을 때 적용되는 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 스위치가 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 스위치를 정하기 위한 동작을 CIST(Common & Internal Spanning-Tree)라고 합니다.



【 그림 8-29 】 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 8-30 】 MSTP의 CST와 IST②

위와 같은 상황에서 B가 MSTP로 동작하기 시작한다면, B는 자신이 CST Root가 될 것을 요청하기 위해 자신 BPDU를 CST Root 와 IST Root로 보냅니다. 그러나, 만약 B보다 우선 순위가 높은 BPDU가 전달된다면, B는 CST Root이 될 수 없습니다.

V2824는 MSTP를 설정하는 명령어를 STP와 RSTP를 설정할 때도 공통적으로 사용하고 있고, PVSPT를 설정하는 명령어는 PVRSTP를 설정할 때에도 사용하고 있습니다.

8.4.4 STP 모드 설정

V2824에 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 스위치에서 STP 설정을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no stp force-version	Bridge	STP 설정을 해제합니다.

8.4.5 STP/RSTP/MSTP 설정

STP/RSPT/MSTP 설정 방법에 대해 다음의 내용으로 설명합니다.

- STP/RSTP/MSTP 활성화
- Root 설정
- Path-cost 설정
- Port-priority 설정
- MST Region 설정
- 설정 내용 확인

(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.



참 고

사용자가 Force-version에서 STP를 선택한 후에 위의 명령어를 사용하면 STP가 활성화되고, RSTP를 선택한 후에 위의 명령어를 사용하면 RSTP가 활성화 됩니다. 마찬가지로 MSTP를 설정하면 MSTP가 활성화 되는 것입니다.

이중 경로가 존재하지 않는 LAN에 속해 있는 스위치에는 굳이 STP 기능을 설정하지 않아도 루프 현상은 발생하지 않습니다.

사용자의 스위치에서 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 스위치가 정해져야 합니다. STP나 RSTP에서는 Root 스위치가 되는 것이고, MSTP에서는 IST Root 스위치가 되는 것입니다. 각 스위치는 자신의 Bridge ID를 가지고 있으며 동일한 LAN에 존재하는 스위치의 Bridge ID를 비교하여 Root 스위치를 결정합니다. 그러나, V2824는 사용자의 요구에 따라 Priority를 설정하면 인위적으로 Root 스위치를 변경할 수도 있습니다. Priority가 변경되면 가장 작은 Priority가 Root 스위치로 결정되도록 재설정됩니다.

스위치에 Priority를 설정하여 인위적으로 Root 스위치를 변경하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp mst priority mstid_range <0 – 61, 440>	Bridge	스위치의 Priority를 설정합니다.
no stp mst priority mstid_range		스위치의 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

V2824는 기본적으로 Priority가 32768로 설정되어 있습니다.

(3) Path-cost 설정

Root 스위치가 결정된 후에는 어떤 경로로 패킷을 전송할지를 정해야 합니다. 이 때 path-cost를 기준으로 경로가 결정되는데 기본적으로 path-cost는 스위치의 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 8-2 】 STP path-cost

전송 속도	Path-cost
4M	250
10M	100
100M	19
1G	4
10G	2

【 표 8-3 】 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 V2824는 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	Path-Cost를 설정합니다.
no stp mst path-cost mstid_range port-number		Path-Cost를 해제합니다.



*mstid_range*는 Instance의 번호를 입력합니다. 따라서 0부터 64까지 입력 가능합니다.



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 mstid_range port-number <0-240>	Bridge	포트의 우선 순위 값을 설정합니다.
no stp mst port-priority mstid_range port-number		포트의 우선 순위 값을 해제합니다.



*mstid_range*는 Instance의 번호를 입력합니다. 따라서 0부터 64까지 입력 가능합니다.



STP와 RSTP의 Priority를 설정할 경우에는 *mstid_range*가 「0」이 됩니다.



주 의

Priority는 16의 배수로 입력해야 합니다.



참 고

V2824는 기본적으로 Priority가 128로 설정되어 있습니다.

(5) MST Region 설정

V2824에 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> <i>vlan-range</i>		하나의 Region으로 그룹화할 VLAN의 범위를 설정합니다.
stp mst config-id revision <0-65535>		같은 MST boundary 안의 스위치들은 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.

V2824는 Configuration ID를 설정한 후에 스위치에 설정한 내용을 적용시켜야 합니다. 설정한 내용을 변경하거나 설정한 내용을 삭제한 후에도 그 내용을 적용하지 않으면 변경된 내용이 스위치에 반영되지 않습니다.

Configuration ID를 설정한 후 그 내용을 스위치에 적용하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp mst config-id commit	Bridge	해당 Region의 설정내용을 실행합니다.



주의

설정한 Configuration ID를 삭제한 후에도 위의 명령어를 사용하여 스위치에 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	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

V2824가 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 currnet	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 currnet**과 **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 currnet**에서는 이전에 설정하여 적용한 설정 내용이 확인됩니다.

8.4.6 PVSTP/PVRSTP 설정

PVSTP/PVRSTP 설정과 관련하여 다음의 내용으로 설명합니다.

- PVSTP/PVRSTP 활성화
- Root 설정
- Path-cost 설정
- Port-priority 설정
- 설정 내용 확인

(1) PVSTP/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*은 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 스위치에는 굳이 STP 기능을 설정하지 않아도 루프 현상은 발생하지 않습니다. 사용자의 스위치에서 설정했던 PVSTP 또는 PVRSTP를 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp pvst disable <i>vlan-range</i>	Bridge	VLAN에서 STP, RSTP, 또는 MSTP를 비활성화 시킵니다.

(2) Root 설정

PVSTP 또는 PVRSTP 기능을 실행시키기 위해서는 우선, Root 스위치가 정해져야 합니다. 각 스위치는 자신의 Bridge ID를 가지고 있으며 동일한 LAN에 존재하는 스위치의 Bridge ID를 비교하여 Root 스위치를 결정합니다.

그러나, V2824는 사용자의 요구에 따라 Priority를 설정하면 인위적으로 Root 스위치를 변경할 수도 있습니다. Priority가 변경되면 가장 작은 Priority가 Root 스위치로 결정되도록 재설정됩니다. 스위치에 Priority를 설정하여 인위적으로 Root 스위치를 변경하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
stp pvst priority <i>vlan_range <0-61440></i>	Bridge	스위치의 Priority를 설정합니다.
no stp pvst priority <i>vlan_range</i>		스위치의 Priority를 삭제합니다.



*mstid_range*는 Instance의 번호를 입력합니다. 따라서 0부터 64까지 입력 가능합니다.



Priority는 4096의 배수로 입력해야 합니다.



V2824는 기본적으로 Priority가 32768로 설정되어 있습니다.

(3) Path-cost 설정

Root 스위치가 결정된 후에는 어떤 경로로 패킷을 전송할지를 정해야 합니다. 이 때 Path-cost를 기준으로 경로가 결정되는데 기본적으로 Path-cost는 스위치의 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 V2824는 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.
no stp pvst path-cost <i>vlan_range port-number</i>		설정한 Path-cost를 삭제합니다.



*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.
no stp pvst port-priority <i>vlan_range port-number</i>		포트의 우선 순위 값을 해제합니다.



*mstid_range*는 Instance의 번호를 입력합니다. 따라서 0부터 64까지 입력 가능합니다.



Priority는 16의 배수로 입력해야 합니다.



V2824는 기본적으로 Priority가 128로 설정되어 있습니다.

(5) 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.

8.4.7 BPDU 전송 설정

BPDU란 STP/RSTP/MSTP를 설정, 유지하기 위해서 LAN에 이용되는 전송 메시지입니다. STP 기능이 설정된 스위치들은 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 스위치가 BPDU를 전송하는 간격을 나타내는 시간으로 1초부터 10초까지 설정할 수 있습니다. 기본적으로 설정되어 있는 Hello Time은 2초 입니다.

◆ 유효 시간 (Max Age)

Root 스위치는 다른 스위치들이 보내주는 정보를 토대로 매번 새로운 정보를 송신합니다. 그러나 네트워크에 많은 스위치들이 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.

BPDU 설정에 대해 다음의 내용을 설명합니다.

- Hello Time 설정
- Forward Delay 설정
- Max Age 설정
- BPDU Hop 설정
- BPDU 설정 내용 확인



참 고

BPDU 설정은 Force-version에서 선택한 기능에 대한 것으로 적용됩니다. STP, RSTP 그리고 MSTP가 동일한 명령어를 사용하고, PVSTP와 PVRSTP가 동일한 명령어를 사용합니다.

(1) Hello Time 설정

Hello 타임은 스위치가 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 스위치가 경로 메시지를 전송하는 시간을 설정합니다.
stp pvst hello-time vlan-range <1 – 10>		PVST 또는 PVRSTP에서 스위치가 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	스위치가 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		
no stp pvst forward-delay vlan-range	Bridge	설정된 Forward-delay 해제합니다.

(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 vlan-range <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		
no stp pvst max-age vlan-range	Bridge	설정한 경로 메시지의 Max age를 해제합니다.

(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 mstid_range	Enable / Global /	STP/RSTP/MSTP의 BPDU 설정내용을 확인할 수 있습니다.
show stp pvst vlan-range	Bridge	PVSTP/PVRSTP의 BPDU 설정내용을 확인할 수 있습니다.

8.4.8 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.

8.4.9 Point-to-Point MAC 설정

STP 운영상 1:1 연결이 아닌 shared edge 포트로 연결이 되어 있는 경우 한 장비에서 보낸 BPDU 가 두 장비에서 받게 될 수 있으며 그로 인해 STP 운영의 Rapid transition이 가능한지에 대한 확신 을 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. “force-true”는 한 인터페이스가 다른 하나의 bridge 즉 일대일로 연결되어 있을 때 사용하며 항상 point-to-point 링크로 연결되어 있다고 간주합니다.

8.4.10 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
<code>stp clear-detected-protocol port-number</code>	Bridge	STP 모드 변경 여부를 확인합니다.

8.4.11 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
<code>stp edge-port { port-number default }</code>	Bridge	해당 포트를 Edge Port로 설정합니다. default 옵션을 사용하면 STP가 설정된 기본 포트가 Edge Port로 설정됩니다.
<code>no stp edge-port { port-number default }</code>		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.

V2824에서는 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	Bridge	MST Root Guard를 활성화합니다.
no stp mst root-guard mstid_range port-number		MST Root Guard를 비활성화합니다.
stp pvst root-guard vlan-range port-number		PVST Root Guard를 활성화합니다.
no stp pvst root-guard vlan-range port-number		PVST Root Guard를 비활성화합니다.

(3) BPDU Guard 설정

네트워크와의 연결이 필요하지만, STP 토플로지(Topology)를 바꿀 가능성이 있는 장비 또는 시스템이 연결되어 있는 포트에 BPDU Guard를 설정하십시오. V2824는 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.

V2824에 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.

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.

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.

(4) 설정 내용 확인

STP Guard 설정 내용을 확인하시려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show stp	Global / Enable / Bridge	STP Guard 설정 내용을 확인합니다.

8.4.12 설정 예제

[설정 예제 1] MSTP 설정

다음은 장비에 MSTP를 설정하는 예입니다.

```
SWITCH(bridge)# stp force-version mstp
SWITCH(bridge)# stp mst enable
SWITCH(bridge)# stp mst config-id map 2 1-50
SWITCH(bridge)# stp mst config-id name 1
SWITCH(bridge)# stp mst config-id revision 1
SWITCH(bridge)# stp mst config-id commit
SWITCH(bridge)# show stp mst
      Status          enabled
      bridge id       8000.00d0cb000183
      designated root 8000.00d0cb000183
      root port        0          path cost        0
      max age          20.00     bridge max age   20.00
      hello time       2.00      bridge hello time 2.00
      forward delay    15.00     bridge forward delay 15.00
      CIST regional root 8000.00d0cb000183  CIST path cost 0
      max hops         20
      name             TEST
      revision         1
      instance vlans
-----
      CIST 51-4094
      2 1-50
-----
SWITCH(bridge)#

```

[설정 예제 2] PVSTP 설정

다음은 장비에 VLAN이 Default와 br2, br3이 설정되어 있을 때, PVSTP를 설정하는 경우입니다.

```
SWITCH(bridge)# stp force-version pvst
SWITCH(bridge)# stp pvst enable 1-3
SWITCH(bridge)# show stp
Spanning tree operation mode is PVSTP
self-loop-detect is disabled
-----
bridge id (VID)          status
-----
8001.00d0cb000183 ( 1)   enabled
8002.00d0cb000183 ( 2)   enabled
8003.00d0cb000183 ( 3)   enabled
SWITCH(bridge)#
-----
```

[설정 예제 3] Path-cost 변경

다음은 PVSTP에서 1번 포트의 Path-cost를 100으로 변경하고 그 내용을 확인한 경우의 예입니다.

```
SWITCH(bridge)# show stp pvst 1 1 detail
(종략)
port01
  port id          8001
  state            forwarding
  designated root  8000.00d0cb036023
  designated bridge 8001.00d0cb000183
  designated port   8001
  designated cost   38
  flags             STP P2P Boundary

-----
```

role	designated
path cost	19
message age timer	0.00
forward delay timer	0.00

```
SWITCH(bridge)# stp pvst path-cost 1 1 100
SWITCH(bridge)# show stp pvst 1 1 detail
(종략)
port01
  port id          8001
  state            forwarding
  designated root  8000.00d0cb036023
  designated bridge 8001.00d0cb000183
  designated port   8001
  designated cost   38
  flags             STP P2P Boundary

-----
```

role	designated
path cost	100
message age timer	0.00
forward delay timer	0.00

```
SWITCH(bridge)#
-----
```

[설정 예제 4] BPDU 설정 변경

다음은 MSTP에서 mstp Hello time을 3초, Forward-delay를 15초, Max-age를 20초로 설정하는 예입니다.

```
SWITCH(bridge)# stp mst hello-time 3
SWITCH(bridge)# stp mst forward-delay 15
SWITCH(bridge)# stp mst max-age 20
SWITCH(bridge)# show stp mst
  Status          disabled
  bridge id      8000.00d0cb000183
  designated root 0000.000000000000
  root port       0           path cost      0
  max age        0.00         bridge max age 30.00
  hello time     0.00         bridge hello time 3.00
  forward delay   0.00         bridge forward delay 15.00
  CIST regional root 0000.000000000000    CIST path cost 0
  max hops       20

  name          TEST
  revision      1
  instance vlans
-----
  CIST 51-4094
  2 1-50
-----
SWITCH(bridge)#

```

8.5 ERP 설정

ERP(Ethernet Ring Protection)는 메트로 이더넷망에서 발생하는 Loop를 방지하고 빠른 시간 내에 망의 복구를 위해 개발된 프로토콜입니다. V2824는 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

V2824에서 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.

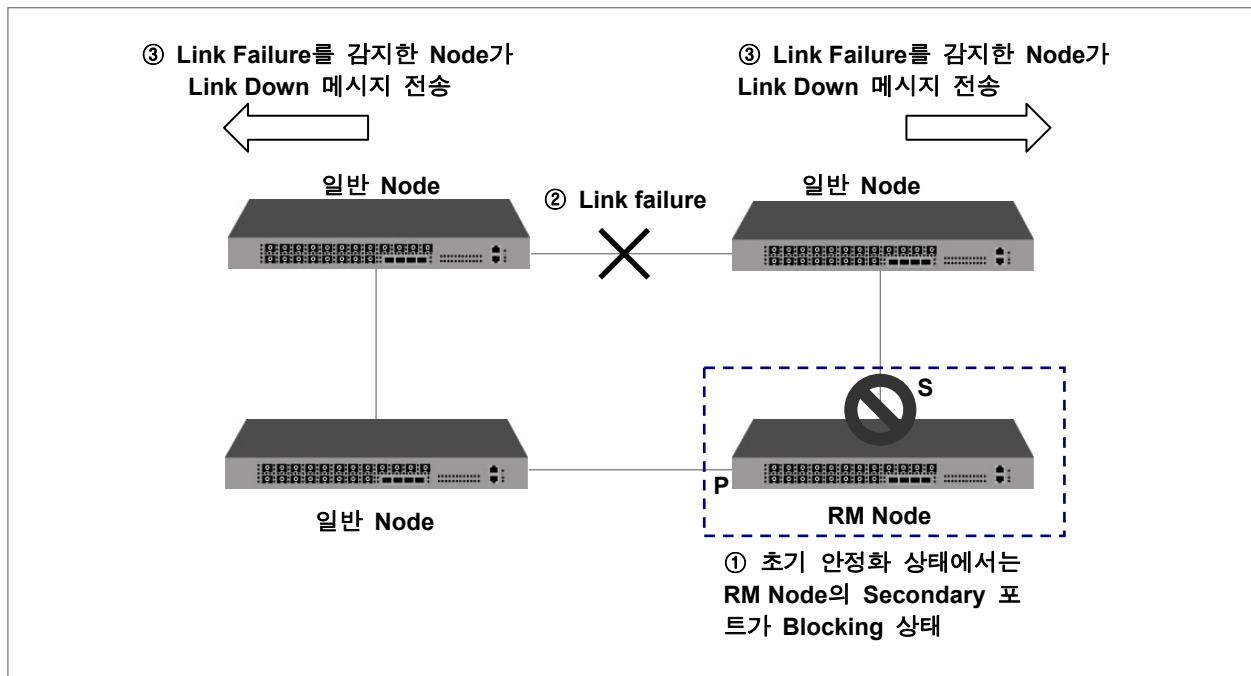


주의

ERP는 이더넷 Ring 토플로지에서만 구현할 수 있습니다..

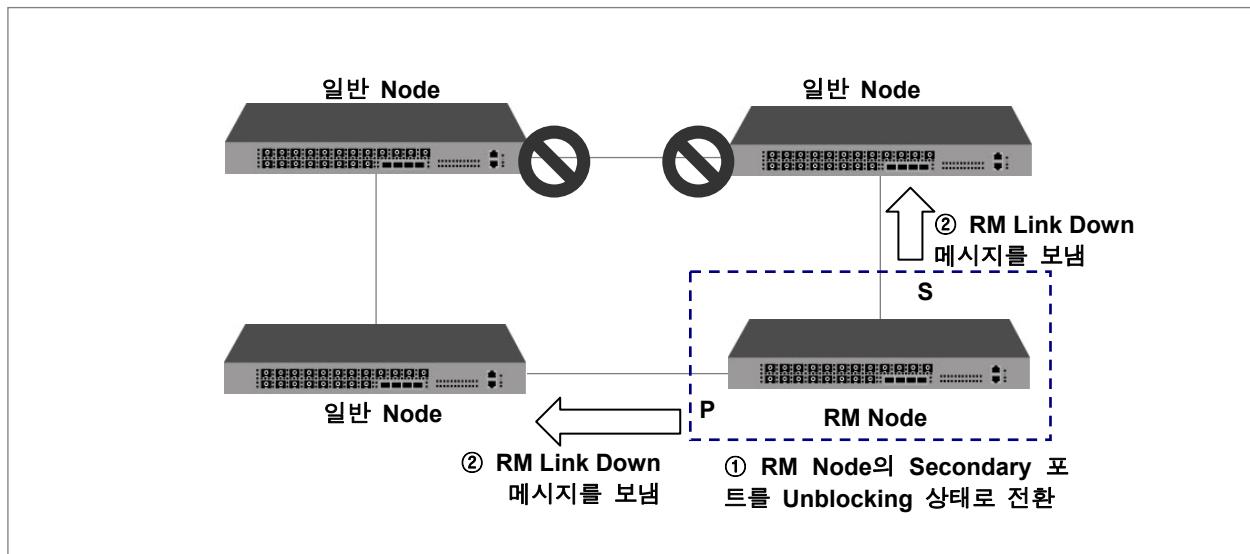
일반적으로 ERP가 동작하고 있는 Ethernet Ring이 안정화된 상태에서는 RM Node의 Secondary 포트가 Blocking 상태를 유지합니다. 이 때, 임의의 곳에서 Link Failure가 발생하게 되면, Link Failure를 감지한 일반 Node들은 Link Down 메시지를 RM Node로 발송하고, Link Failure 상태가 된 포트는 Blocking 상태가 됩니다.

다음 그림은 Link Failure가 발생했을 때의 ERP의 동작 원리를 나타낸 것입니다.



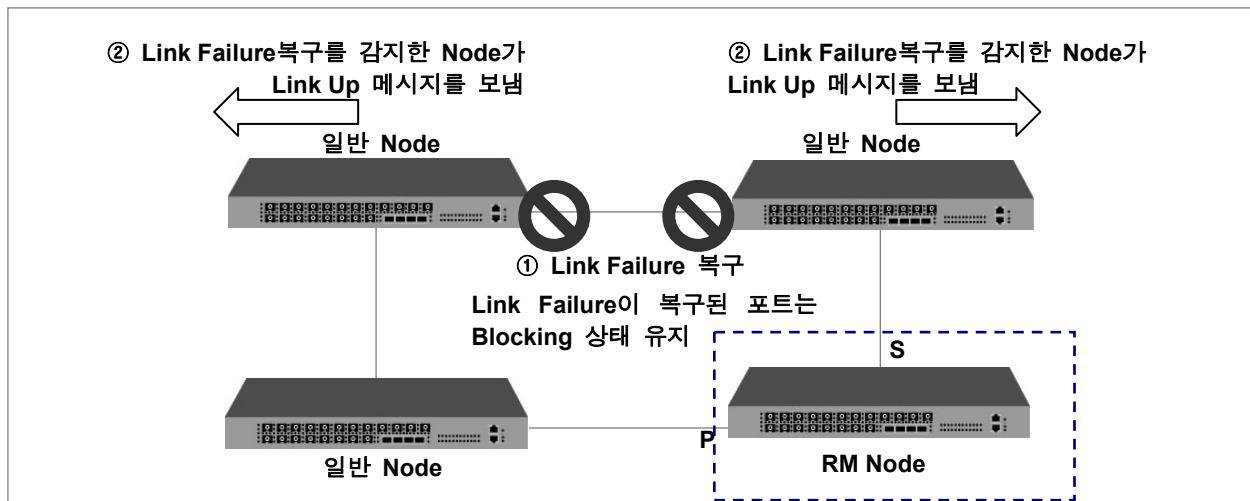
【 그림 8-31 】 Link failure 발생

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.



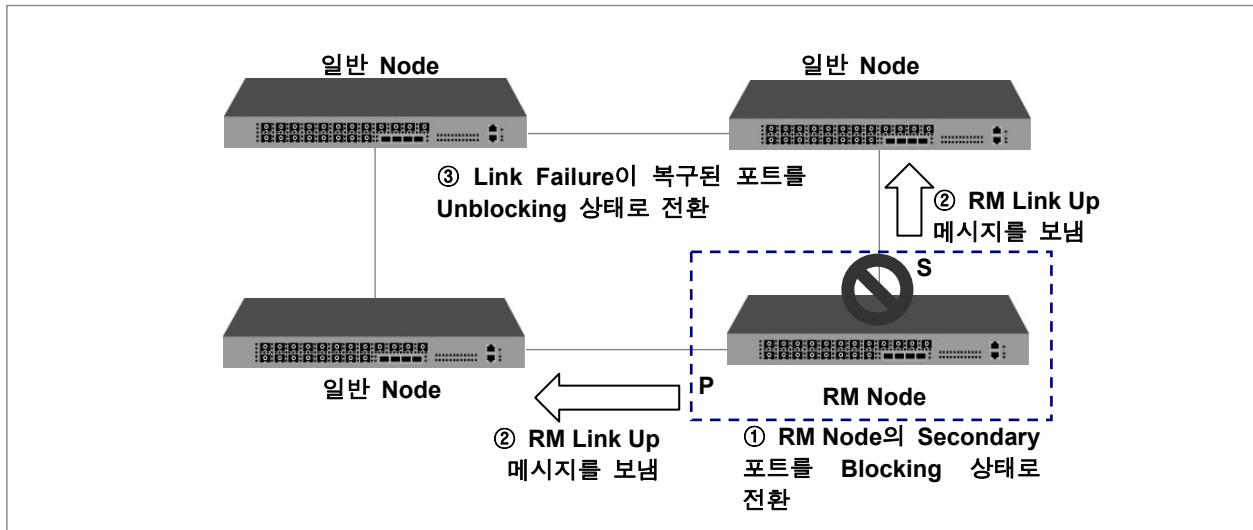
【 그림 8-32 】 Ring Protection

한편, RM Node의 Secondary 포트가 Unblocking 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 8-33 】 Link Failure 복구

Link Up 메시지가 RM Node에 수신되면, RM Node는 자신의 Secondary 포트를 다시 Blocking시키고 RM Link Up 메시지를 응답으로 발송합니다. Link Up메시지를 발송하였던 Node에서 RM Link Up 메시지를 받으면, Link Failure이 복구된 포트를 Unblocking 상태로 전환하여 통신을 재개합니다. 이러한 방법으로 Ethernet Ring은 다시 안정화 상태로 돌아가게 되는 것입니다.



【 그림 8-34 】 Ring Recovery

8.5.2 LOTP (Loss of Test Packet)

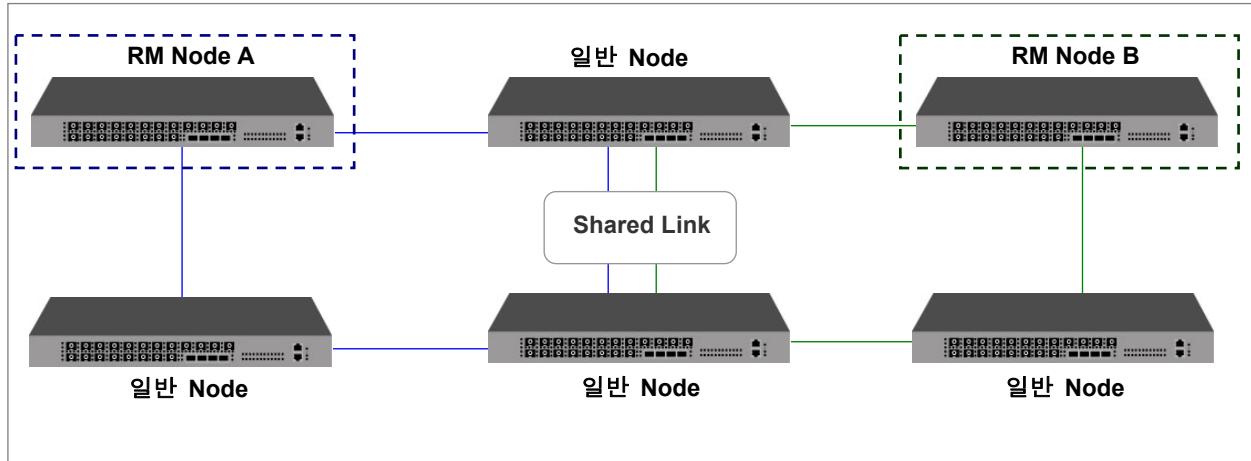
RM Node는 일반 Node의 Link Up/Down 메시지의 정보만으로는 전체 토플로지 상태를 알 수 없기 때문에 주기적으로 TP (Test Packet)을 전송하여 ERP Ring의 Loop 상태를 검출 합니다. RM Node의 두 ERP 포트에서 3번 이상 연속으로 TP가 손실되어 자기 자신으로 되돌아 오지 않은 경우에는 Loop 가 형성되지 않은 것으로 판단하고 이러한 경우는 LOTP(Loss of Test Packet) 상태라고 합니다. 따라서 이러한 경우에는 RM Node가 자신의 Secondary 포트를 Blocking 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 8-35 】 Shared Link 환경

8.5.4 ERP 도메인 설정

(1) ERP ID 설정

ERP를 구현하려면, ERP를 구현할 도메인 아이디를 설정해야 합니다. ERP를 구현할 도메인 ID를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	Function
<code>erp domain domain-id</code>	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
<code>no erp domain {all domain-id}</code>	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.



주의

Primary 포트와 Secondary 포트는 장비의 같은 포트 번호로 사용할 수 없습니다.

(5) MAC 등록

ERP에서 사용할 포트의 MAC 주소를 등록하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
erp register-mac <i>vlan-id port-number</i>	Bridge	ERP에서 사용할 포트의 MAC 주소를 등록합니다.

등록한 ERP MAC 주소를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no erp register-mac <i>vlan-id [port-number]</i>	Bridge	등록한 ERP MAC 주소를 삭제합니다.

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 <i>domain-id</i>	Bridge	특정 ERP 도메인 설정을 활성화합니다.

특정한 ERP 도메인의 Protected Activation 설정을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no erp activation <i>domain-id</i>	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 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

8.5.13 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 Loop 감지 기능 설정

8.6.1 Loop 감지 기능 설정

사용자의 장비에 이중 경로가 존재하지 않는다고 해도 네트워크 환경이나 장비에 연결되어 있는 케이블 상태 등에 따라 Loop 현상이 발생할 수 있습니다. V2824는 네트워크에 Loop가 발생하였는지 확인하기 위해 주기적으로 Loop 감지 패킷을 전송하도록 설정할 수 있습니다. Loop 상태가 발견된 경우에는 사용자가 설정한 정책에 따라 해당 포트를 Block 하는 등 Loop 현상으로 인해 발생되는 네트워크 문제들을 방지 할 수 있습니다. Loop가 발견되어 감지 패킷이 수신된 포트는 Loop 감지 리스트에 기록되어 관리됩니다.

한편, 해당 포트가 속한 VLAN의 STP 설정이 활성화되어 있다면, 포트 상태는 변경하지 않고 로그만 남깁니다.

(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 해제합니다.



Loop-detect 기능을 활성화하려면, 먼저 STP를 해제해야 합니다.

한편, 특정 포트에만 Loop 감지 기능을 활성화할 수 있습니다. 특정 포트에 이 기능을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
loop-detect port-number	Bridge	특정 포트에 Loop 감지 기능을 활성화합니다.
no loop-detect port-number		특정 포트에 Loop 감지 기능을 해제합니다.

(2) 포트 정책 설정

Loop가 발생한 포트를 Block 상태로 변경하도록 하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
loop-detect port-number block	Bridge	Loop가 발생했을 때 해당 포트를 차단합니다.
no loop-detect port-number block		해당 포트를 차단하는 설정을 해제합니다.



V2824는 기본적으로 Loop가 발생했을 때, 해당 포트를 차단하지 않고 Loop 상태에 대한 로그를 남기도록 설정되어 있습니다.

(3) Loop 감지 패킷 전송 시간 설정

Loop를 감지하는 패킷은 일정한 간격으로 전송됩니다. 이 때, 사용자는 Loop 감지 패킷의 전송 간격을 직접 설정할 수 있습니다.

Loop 감지 패킷의 전송 시간 간격을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
loop-detect port-number period <1-60>	Bridge	Loop 감지 패킷의 전송 간격을 설정합니다.



V2824의 Loop 감지 패킷을 전송하는 시간 간격은 기본적으로 30초로 설정되어 있습니다. 설정 단위는 초입니다.

(4) Loop 감지 리스트 해제 timer 설정

Loop가 발생한 포트는 Loop 감지 리스트에 등록되어 관리됩니다. Loop 감지 리스트에 등록된 포트는 사용자가 설정한 정책에 따라 Block 상태가 되기도 하는데, 일정한 시간 이후에는 다시 정상 상태로 돌아가서 Loop 감지 대상이 됩니다.

해당 포트가 Loop 감지 리스트에 등록되면 timer가 동작하여 설정된 시간이 지난 후, Loop 상태가 아니라고 가정하여 정상 상태로 돌아가게 됩니다. 다시 Loop 감지 대상이 되는 timer를 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
loop-detect port-number timer <1-86400>	Bridge	특정 포트가 Loop 감지 리스트에서 제외되어, 다시 Loop 감지 대상이 되는 timer를 설정합니다.
loop-detect port-number timer 0		해당 포트에 설정된 timer를 해제합니다.



장비는 timer가 기본적으로 600초(10분)으로 설정되어 있습니다.

한편, 사용자는 Loop 현상이 발생하여 설정에 따라 해당 포트를 Block 할 경우, Loop 현상이 사라지면서 언제든지 포트의 통신을 재개해도 될 경우가 발생 할 수도 있습니다. V2824는 이런 경우에 설정된 시간동안 기다릴 필요없이 사용자가 강제로 Block 상태의 포트를 해제할 수 있습니다.

Loop 가 감지되어 Block 상태인 포트의 통신을 재개하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
loop-detect port-number unblock	Bridge	사용자가 수동으로 해당 포트를 Loop 감지 리스트에서 삭제하므로써 통신을 재개합니다.

(5) Loop 감지 패킷 전송 소스 MAC 주소 설정

V2824는 Loop 감지 기능에서 주기적으로 전송하는 Loop 감지 패킷의 Source MAC 주소를 시스템 MAC 주소로 설정하거나 LAA(Locally Administered Address)로 설정할 수 있습니다.

LAA란, 장비의 MAC 주소에서 첫 번째 Byte의 두 번째 Bit를 1로 설정하여 MAC 주소가 무조건 02로 시작하도록 설정하는 것입니다. 예를 들어 장비의 MAC 주소가 00:D0:cb:00:00:01인 경우, LAA는 02:D0:cb:00:00:01가 됩니다.

Loop 감지 패킷의 MAC 주소를 지정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
loop-detect srcmac laa	Bridge	LAA MAC 주소를 source MAC 주소로 사용합니다.
loop-detect srcmac system		System MAC 주소를 source MAC 주소로 사용합니다.



V2824는 기본적으로 System MAC 주소를 Loop 감지 패킷의 source MAC 주소로 사용하도록 설정되어 있습니다.



감지 패킷의 source MAC 주소를 변경하기 위해서는 먼저 **loop-detect disable** 명령어를 사용하여, Loop 감지 기능을 해제해 주십시오.

(6) Loop 감지 설정 확인

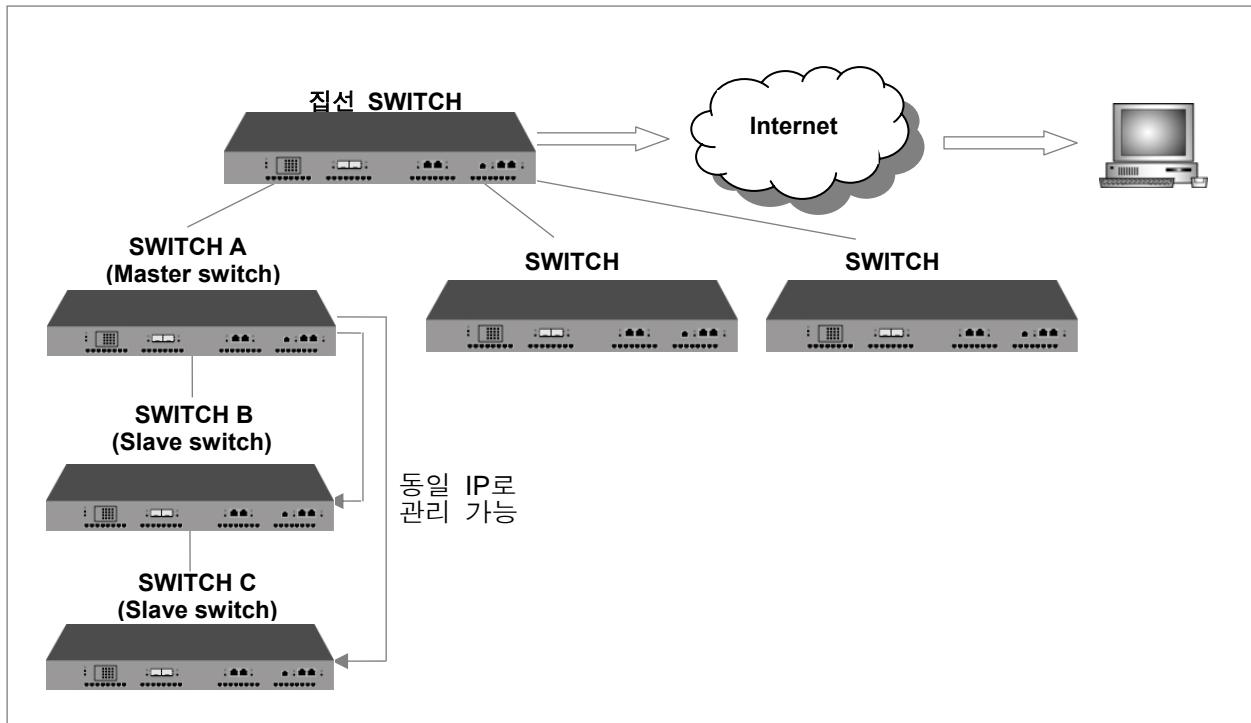
Loop 감지 설정을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show loop-detect	Enable/ Global/	Loop 감지에 대한 활성화/ 해제 설정 내용을 확인합니다.
show loop-detect {port-number all}	Bridge	해당 포트 또는 모든 포트의 Loop 감지 설정 내용을 확인합니다.

8.7 스택킹 설정

스택킹이란 하나의 IP 주소로 여러 대의 장비를 관리 할 수 있는 기능입니다. 사용 가능한 IP는 한정 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) 다산네트웍스의 장비는 이러한 스택킹 기능을 지원합니다.

다음은 스택킹을 설정한 네트워크의 예를 나타낸 것입니다. 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.



【 그림 8-36 】 스택킹 설정의 예

여기에서는 스택킹 설정 방법을 다음 순서로 설명합니다.

- 장비 그룹 설정
- Master 장비 지정
- Slave 장비 설정
- 스택킹 설정 해제
- 스택킹 설정 내용 확인
- Master에서 Slave로 접속
- 설정 예제

8.7.1 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.

8.7.2 Master 장비 지정

Master가 되는 장비는 다음 명령어를 사용하여 Master 장비로 설정하십시오.

명령어	모 드	기 능
stack master	Global	Master 장비를 설정합니다.

8.7.3 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.

8.7.4 스택킹 설정 해제

스택킹 기능을 해제하려면 다음과 같은 명령어를 사용하십시오.

명령어	모 드	기 능
no stack	Global	Stack 기능 설정이 해제됩니다.

8.7.5 스택킹 설정 내용 확인

스택킹에 대한 설정 내용을 확인하려면 다음 명령어를 사용하십시오. Master 장비는 등록되어 있는 Slave 장비의 정보를 알 수 있고, Slave 장비는 자신의 Node ID를 알 수 있습니다.

명령어	모 드	기 능
show stack	Enable/Global/Bridge	스택킹에 대한 설정 내용을 확인합니다.

8.7.6 Master에서 Slave로 접속

모든 스택킹 설정을 마치고 나면 Master에서 Slave로 접속하여 설정 및 관리를 할 수 있습니다. Master 스위치에서 Slave 스위치로 접속하려면 Global 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
rcommand node-number	Global	Slave 스위치로 접속합니다.

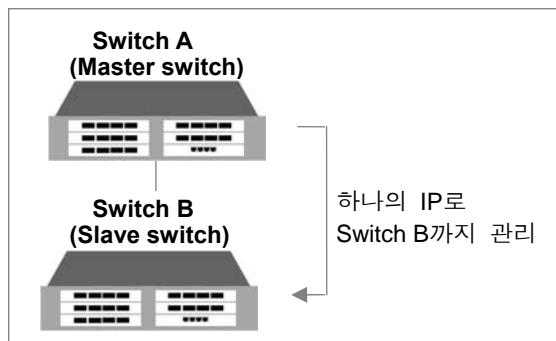
위의 명령어에서 입력하는 *node-number*는 Slave 장비에서 스택킹 설정 내용을 확인하면 얻어지는 정보 중 “**node ID**”에 해당합니다.

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.

8.7.7 설정 예제

[설정 예제 1] 스택킹 설정

다음은 위의 방법에 따라 SWITCH A를 master로 지정하고 SWITCH B를 slave로 지정하여 Stacking을 설정한 경우의 예입니다.



1 단계 Switch A를 Master 스위치로 설정합니다. 동일한 스위치 그룹에 속하도록 VLAN을 설정하고, Slave 스위치를 등록한 후 Master 스위치로 설정합니다.

<Switch A – Master Switch>

```
SWITCH_A(config)# stack device br1
SWITCH_A(config)# stack add 00:d0:cb:22:00:11
SWITCH_A(config)# stack master
```

2 단계 Slave 스위치로 Master 스위치에 등록된 Switch B에서 동일한 스위치 그룹에 속하도록 VLAN을 설정하고, Slave 스위치로 설정합니다.

<Switch B – Slave Switch>

```
SWITCH_B(bridge)# set stack slave
SWITCH_B(bridge)# set stack device br1
```

3 단계 설정한 내용을 확인하십시오. Master 스위치와 Slave 스위치에서 확인할 수 있는 정보는 다음과 같이 달라집니다.

<Switch A – Master Switch>

```
SWITCH_A(bridge)# show stack
device : br1
node ID : 1
node   MAC address          status   type           name      port
      1  00:d0:cb:0a:00:aa    active   V1824        SWITCH_A    24
      2  00:d0:cb:22:00:11    active   V1824        SWITCH_B    24
SWITCH_A(bridge)#

```

<Switch B – Slave Switch>

```
SWITCH_B(bridge)# show stack
device : br1
node ID : 2
SWITCH_B(bridge)#

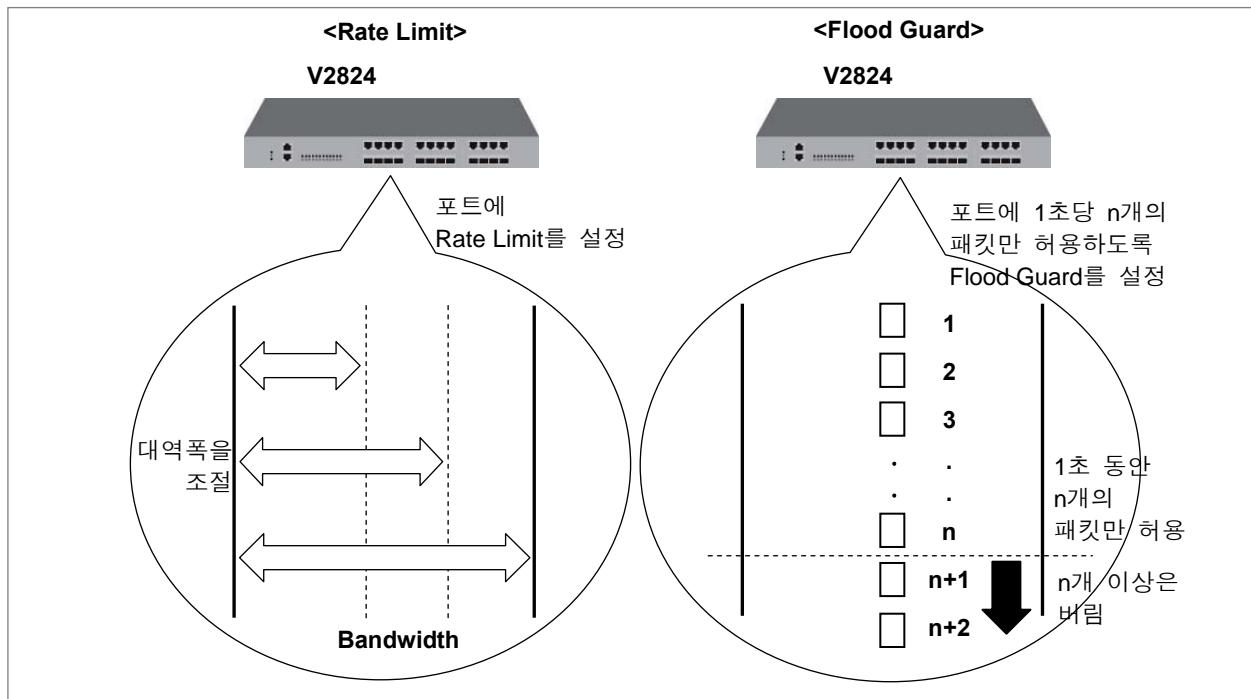
```

8.8 Rate Limit와 Flood Guard

Rate Limit는 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 도 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.

이러한 기능은 대역폭은 일정하게 유지한 채 한꺼번에 많이 전달되는 이상 패킷이 수신되는 것을 막을 수 있습니다.



【 그림 8-37 】 Rate Limit와 Flood Guard

8.8.1 Rate Limit 설정

포트의 대역폭을 설정하려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오. Ingress의 대역폭에 Rate-limit를 설정할 때에는 802.3x 표준에 명기된 대로 Flow-control 기능과 함께 Rate-limit를 설정할 수 있습니다. Ingress는 스위치의 입장에서 수신되는 것이기 때문에 포트에 물려있는 PC 사용자의 입장에선 업로드에 해당됩니다.

명령어	모 드	기 능
rate-limit port port-number rate rate egress		송신 포트에 Rate Limit를 설정합니다.
rate-limit port port-number rate rate	Bridge	
ingress dot3x		수신 포트에 Rate Limit를 설정합니다.



rate는 64Kbps의 배수로 입력하십시오.

사용자가 지정한 대역폭을 취소하려면 Bridge 설정 모드에서 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no rate-limit port port-number egress	Bridge	송신 포트의 Rate Limit를 해제합니다.
no rate-limit port port-number ingress dot3x		수신 포트의 Rate Limit를 해제합니다.

한편, 포트에 설정한 대역폭을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show rate-limit	Enable / Global / Bridge	Rate Limit 설정 내용을 확인합니다.

8.8.2 Flood Guard 설정

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. 이러한 기능은 대역폭은 일정하게 유지한 채 한꺼번에 많이 전달되는 이상 패킷이 수신되는 것을 막을 수 있습니다.

(1) MAC-Flood-Guard 설정

V2824는 동일한 MAC 주소를 가진 패킷에 대해 1초당 수신될 수 있는 개수를 제한할 수 있습니다. 이 기능을 이용하면 등록되지 않은 사용자의 악의의 공격에서 네트워크를 보호할 수 있습니다. 1초당 수신될 수 있는 패킷의 개수를 제한하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
mac-flood-guard port-number packet-num	Bridge	Flood Guard를 설정합니다.



packet-num은 <1 -6,000> 사이에서 설정 가능합니다.

설정한 Flood Guard를 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no mac-flood-guard port-number	Bridge	Flood Guard를 해제합니다.

설정한 Flood Guard의 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show mac-flood-guard	Enable / Global / Bridge	Flood Guard 설정 내용을 확인합니다.
show mac-flood-guard macs		차단된 MAC 주소 정보를 확인합니다.

(2) CPU-Flood-Guard 설정

V2824는 CPU로 올라오는 브로드캐스트와 멀티캐스트 트래픽이 1초당 설정값(threshold) 보다 초과할 경우 해당 포트로 유입되는 패킷을 일정기간동안 차단하는 기능을 지원합니다. 또한 포트를 unblock으로 설정하였을 경우에는 설정된 패킷 개수보다 초과했을 경우에는 1초 단위로 확인하여 설정값보다 이하로 떨어진 경우 trap 메시지로 알려줍니다. 이러한 기능은 포트를 통해서 들어오는 특정 트래픽을 사용자가 원하는 대로 차단 또는 허용하여 통신을 더욱 원활하게 할 수 있습니다.



주의

System-flood-guard 와 **cpu-flood-guard** 기능은 동시에 설정할 수 없습니다.

CPU에 올라오는 트래픽에 대해 **cpu-flood-guard** 기능을 활성화 또는 해제하려면 다음 명령어를 사용하십시오. 이 기능을 활성화하면 Blocked List를 위한 timer가 동작하게 됩니다.

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 패킷의 종류에 따라 트래픽의 1초당 패킷 수를 제한하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
cpu-flood-guard port-number <1-6000>	Bridge	해당 포트를 통해 1초 동안 CPU에 flooding 되는 패킷 개수를 제한합니다.
no cpu-flood-guard [port-number]		해당 포트의 CPU-flood-guard 관련 설정 내용을 삭제합니다.



참 고

Trunk 멤버로 설정되어 있는 포트는 **cpu-flood-guard** 기능을 설정할 수 없습니다.



주 의

일반적으로 CPU가 처리 가능한 패킷의 개수는 6000개입니다. 만약 모든 포트에 대해 **cpu-flood-guard** 임계값을 1000으로 설정하고 Broadcast storm 과 같은 갑자기 많은 양의 트래픽이 유입될 경우 개별 포트별로 초당 패킷 수는 1000에 도달하지 않을 수 있습니다.

해당 포트를 통해 CPU로 수신되는 패킷의 수를 무제한으로 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no cpu-flood-guard [port-number]	Bridge	특정 포트 또는 모든 포트를 통해 CPU에 수신되는 패킷 개수를 무제한(unlimited)으로 설정합니다.

CPU-flood-guard 설정으로 인해 해당 포트를 통해 CPU로 수신되는 초당 패킷수를 초과하여 차단된(block) 포트에 대해 해제되는 시간을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
cpu-flood-guard port-number timer <10-3600>	Bridge	트래픽이 차단된 포트가 해제되는 시간을 설정합니다.



참 고

Timer는 기본적으로 장비에 60초로 설정되어 있습니다. 단위는 초입니다.

CPU에 수신되는 트래픽이 차단된(block) 특정 포트를 강제로 해제하여 패킷 유입을 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.

특정 포트를 통해 수신되는 패킷의 종류에 따라 유니캐스트, 브로드캐스트 또는 멀티캐스트 트래픽의 1초당 패킷 수를 제한하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
cpu-flood-guard port-number { multicast broadcast unicast all } <1-6000> block	Bridge	해당 포트에 패킷 종류에 따라 1초 동안 수신되는 패킷 개수 설정하여 트래픽 유입을 차단합니다.
cpu-flood-guard port-number { multicast broadcast unicast all } <1-6000> unblock	Bridge	해당 포트에 패킷 종류에 따라 1초 동안 수신되는 패킷 개수 설정값을 확인하여 이하로 내려갈 경우 trap 메시지로 알려줍니다. .

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) System-Flood-Guard 설정

V2824는 포트를 통해 유입되는 브로드캐스트와 멀티캐스트 패킷의 개수를 제한하고 일정값을 초과할 경우 해당 포트를 차단하거나 trap 메시지로 알려주는 기능을 지원합니다. 이러한 기능은 특정한 포트를 통해서 들어오는 패킷을 사용자가 임의로 차단하거나 인지하여 통신을 더욱 원활하게 할 수 있습니다.

V2824는 포트 별로 초당 유입되는 패킷의 수를 제한하는 설정과 해당 패킷이 일치하는지 주기적으로 검사를 합니다. 이때 설정값(threshold)을 초과하는 패킷이 유입될 경우 일정기간 동안 해당 포트를 차단(Block)하거나 trap만을 발생시킵니다.

설정에 의해 트래픽이 차단된(Block) 포트의 경우에는 해제하기 위해서 Blocked List를 생성하고 timer에 의해 주기적으로 시간이 만료되었는지 검사한 후 자동으로 해제되는 기능을 지원합니다. 그리고 해당 포트가 unblock으로 설정된 경우에는 1초마다 확인하여 임계값(threshold) 이하로 내려갈 경우에는 trap 메시지로 알려줍니다.



주의

System-flood-guard 와 **cpu-flood-guard** 기능은 동시에 설정할 수 없습니다.

System-flood-guard 기능을 활성화 또는 해제하려면 다음 명령어를 사용하십시오. 이 기능을 활성화하면 Blocked List를 위한 timer가 동작하게 됩니다.

명령어	모 드	기 능
system-flood-guard enable	Bridge	System-flood-guard 기능을 활성화합니다.
system-flood-guard disable		System-flood-guard 기능을 비활성화합니다.

특정한 포트를 통해 수신되는 패킷의 종류에 따라 브로드캐스트 또는 멀티캐스트 트래픽의 1초당 패킷 수를 제한하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
system-flood-guard port-number { multicast broadcast both } <1-2147483647> block	Bridge	해당 포트에 패킷 종류에 따라 1초 동안 수신되는 패킷 개수 설정하여 트래픽 유입을 차단합니다.
system-flood-guard port-number { multicast broadcast both } <1-2147483647> unblock		해당 포트에 패킷 종류에 따라 1초 동안 수신되는 패킷 개수 설정값을 확인하여 이하로 내려갈 경우 trap 메시지로 알려줍니다. .



참 고

Trunk 멤버로 설정되어 있는 포트는 초당 패킷 수를 제한할 수 없습니다.

해당 포트로 수신되는 패킷의 수를 무제한으로 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no system-flood-guard [port-number]	Bridge	특정 포트 또는 모든 포트에 수신되는 패킷 개수를 무제한(unlimited)으로 설정합니다.

트래픽이 차단된(block) 특정 포트를 강제로 해제하여 패킷 유입을 허용하고자 하면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
system-flood-guard port-number unblock	Bridge	해당 포트를 통해 수신되는 트래픽의 flooding 을 허용합니다.

System-flood-guard 설정으로 인해 해당 포트로 수신되는 초당 패킷수를 초과하여 차단된(block) 포트에 대해 해제되는 시간을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
system-flood-guard port-number timer <10-3600>	Bridge	특정 포트를 차단해 놓는 시간을 설정합니다.

System-flood-guard 설정상태를 확인하고자 하면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show system-flood-guard	Enable / Global/ Bridge	System-flood-guard 설정을 확인합니다.



참 고

포트가 system-flood-guard 설정으로 Block 되었다고 하더라도 BPDU는 수신됩니다.



주 의

CPU-flood-guard와 system-flood-guard는 동시에 설정할 수 없습니다.

8.8.3 설정 예제

[설정 예제 1] Rate Limit 설정

다음은 V2824에서 1번 포트의 대역폭을 64Mbps, 2번 포트의 대역폭을 128Mbps로 설정하고 그 내용을 확인하는 경우입니다.

```
SWTICH(bridge)# rate-limit port 1 rate 64 egress
SWTICH(bridge)# rate-limit port 2 rate 128 ingress dot3x
SWTICH(bridge)# show rate-limit
unit : kbps E : Enhanced
-----
Port | Ingress | Egress | Port | Ingress | Egress
-----+-----+-----+-----+-----+-----+
 1  | N/A     | 64    | 2   | 128   | N/A
 3  | N/A     | N/A   | 4   | N/A   | N/A
(중략)
SWTICH(bridge)#

```

[설정 예제 2] MAC Flood Guard 설정

다음은 포트 1번에 수신될 수 있는 패킷의 개수를 600개로 제한하고 그 내용을 확인하는 경우의 예입니다.

```
SWTICH(bridge)# mac-flood-guard 1 600
SWTICH(bridge)# show mac-flood-guard
-----
Port Rate(fps) | Port Rate(fps)
-----+-----+
 1  600      | 2 Unlimited
 3  Unlimited | 4 Unlimited
 5  Unlimited | 6 Unlimited
 7  Unlimited | 8 Unlimited
 9  Unlimited | 10 Unlimited
11  Unlimited | 12 Unlimited
13  Unlimited | 14 Unlimited
(중략)
SWTICH(bridge)#

```

[설정 예제 3] CPU Flood-Guard 설정

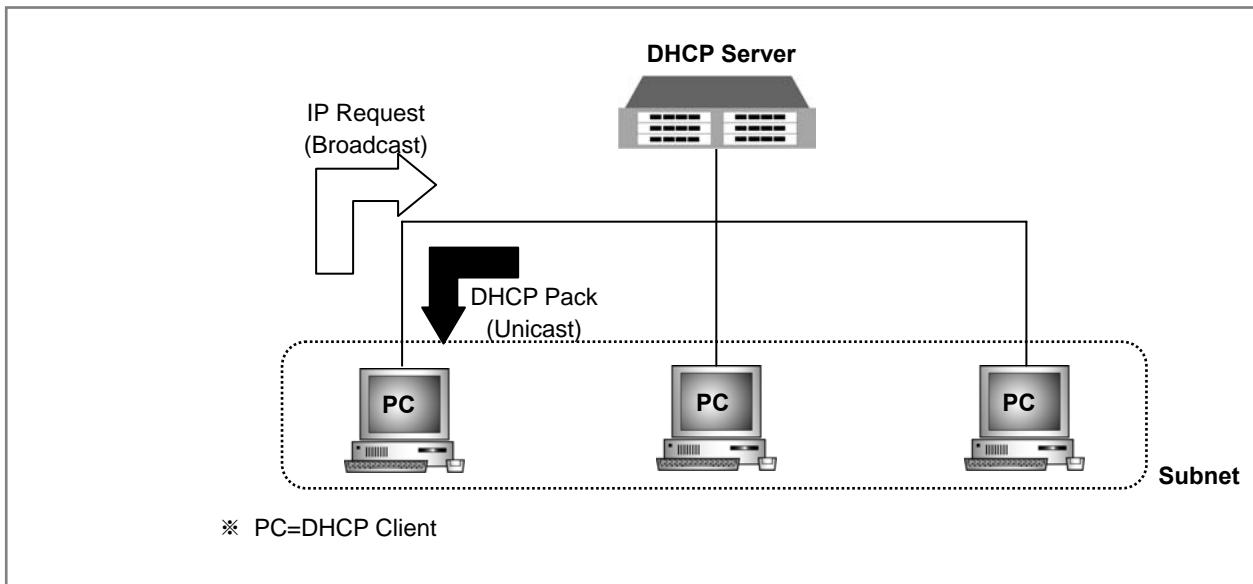
다음은 포트 1번을 통해 CPU에 수신되는 패킷의 개수를 100개로 제한하고 해제되는 시간을 100초로 설정한 내용을 확인하는 경우의 예입니다.

```
SWITCH(bridge)# cpu-flood-guard enable
SWITCH(bridge)# cpu-flood-guard 1 timer 100
SWITCH(bridge)# show cpu-flood-guard
-----
Port Rate(fps)    timer blocked | Port Rate(fps)    timer blocked
-----
  1 Unlimited      100    no     |   2 Unlimited      60    no
  3 Unlimited      60    no     |   4 Unlimited      60    no
  5 Unlimited      60    no     |   6 Unlimited      60    no
  7 Unlimited      60    no     |   8 Unlimited      60    no
  9 Unlimited      60    no     |  10 Unlimited      60    no
 11 Unlimited      60    no     |  12 Unlimited      60    no
 13 Unlimited      60    no     |  14 Unlimited      60    no
 15 Unlimited      60    no     |  16 Unlimited      60    no
 17 Unlimited      60    no     |  18 Unlimited      60    no
 19 Unlimited      60    no     |  20 Unlimited      60    no
 21 Unlimited      60    no     |  22 Unlimited      60    no
(중략)
SWITCH(bridge)#
-----
```

8.9 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.



【 그림 8-38 】 DHCP 서비스 구성의 예

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.

V2824는 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 설정
- IP Source Guard
- DHCP 디버깅

8.9.1 DHCP 서버 설정

V2824를 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 DHCP 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 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.



V2824는 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 gateway-address [gateway-address]	IP Pool	서브넷의 디폴트 게이트웨이를 설정합니다.
no default-router gateway-address [gateway-address]		서브넷의 디폴트 게이트웨이를 해제합니다.
no default-router all		서브넷의 디폴트 게이트웨이를 모두 해제합니다.



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. V2824는 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 192.168.1.40까지의 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.



참 고

IP 사용 시간은 초단위로 <120 - 2,147,483,637> 사이에서 설정 가능합니다.



V2824는 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

V2824의 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 <i>ip-address mac-address</i>	IP Pool	DHCP 클라이언트에게 고정 IP 주소를 할당합니다.
no fixed-address <i>ip-address</i>		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 <i>domain-name</i>	IP Pool	IP Pool에 대한 도메인 이름을 설정합니다.
no domain-name		IP Pool에 대한 도메인 이름을 해제합니다.

(9) Option Code 설정

V2824는 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 <i>format-name</i>	IP-Pool	DHCP 패킷에 설정될 Option을 지정합니다.

설정한 Option 를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no option code <1-254> format	IP-Pool	설정된 Option을 삭제합니다.

DHCP Pool 에 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

V2824는 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) 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/Bridge	IP Pool 설정 내용을 확인합니다.
show ip dhcp pool summary [pool-name]		

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])#
```

(12) IP 주소 할당 제한

DHCP 서버 모드의 V2824는, 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		

(13) 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.

V2824는 DHCP 서버가 할당하려는 IP 주소의 사용여부를 확인하는데 Ping 테스트와 ARP 테스트를 모두 사용할 수 있고, 이 중 한가지 방법을 선택하시면 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, V2824는 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.

(14) 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.

(15) IP 주소 할당 기준 설정

V2824는 IP 주소를 할당하는 기준이 기본적으로 Client-id로 설정되어 있습니다. 그러나 Client-id가 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.

(16) IP 주소 1:N 할당 방지

V2824는 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	Mode	기능
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	Mode	기능
no ip dhcp check client-hardware-address	Global	1:1 IP 할당 기능을 해제합니다.

(17) Authorized ARP

Authorized ARP는 인증받은 사용자에게만 IP 주소를 할당하도록 하는 기능입니다. 이 기능을 사용하면 DHCP 서버는 Lease 테이블을 참조하여 유효한 IP 주소에 ARP 엔트리를 추가하여, 불법으로 고정 IP 주소를 사용하는 등의 유효하지 않은 사용자의 ARP 응답을 무시합니다.

한편, Authorized ARP가 활성화되면 Dynamic ARP Learning 기능은 비활성화 되며, DHCP 서버만이 ARP 엔트리를 추가할 수 있게 됩니다.



Authorized ARP는 DHCP 서버에서만 설정할 수 있습니다.

Authorized ARP 기능을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모드	기능
ip dhcp authorized-arp <120-2,147,483,637>	Global	유효하지 않은 사용자의 ARP 응답을 무시하여 인증받은 사용자에게만 IP 주소를 할당하도록 설정합니다.



Authorized ARP의 완료시간은 <120-2,147,483,637> 범위에서 설정할 수 있으며 단위는 초(sec)입니다.

한편, Authorized ARP 기능이 동작을 시작하는 시간을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp authorized-arp start <120-2147483637> timeout <120-2147483637>	Global	유효하지 않은 사용자의 ARP 응답을 무시하여 인증받은 사용자에게만 IP 주소를 할당하도록 설정합니다.



시작시간은 기본적으로 3600초로 설정되어 있습니다.

Authorized ARP 기능을 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip dhcp authorized-arp	Global	인증받은 사용자에게만 IP 주소를 할당하도록 제한한 것을 해제합니다.

V2824는 Authorized ARP에 의해 정상적으로 IP 주소를 할당한 사용자와 차단된 사용자 정보를 확인할 수 있습니다. 유효 사용자 목록에는 현재 IP 주소가 할당된 사용자 정보가 포함되며, 차단된 사용자 목록에는 ARP 요청 메시지를 보냈지만 IP 주소를 할당받지 못한 사용자 정보가 포함됩니다.

Authorized ARP에 의한 유효 사용자 정보와 차단된 사용자 정보를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip dhcp authorized-arp valid	Enable/ Global/ Bridge	Authorized ARP에 의해 정상적으로 IP 주소를 할당받은 사용자 정보를 확인합니다.
show ip dhcp authorized-arp invalid		Authorized ARP에 의해 IP 주소 할당이 차단된 사용자 정보를 확인합니다.

Authorized ARP에 의해 IP 주소 할당이 차단된 사용자 정보를 삭제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
clear ip dhcp authorized-arp invalid	Enable/ Global/Bridge	Authorized ARP에 의해 IP 주소 할당이 차단된 사용자 정보를 삭제합니다.

(18) Lease 데이터베이스 Backup

V2824는 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.



참 고

*interval*은 초 단위로, <120 - 2, 147, 483,637> 사이에서 설정 가능합니다.

(19) 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	

위의 명령어를 사용하여 확인할 수 있는 각 옵션의 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.

(20) Lease 데이터베이스 초기화

V2824는 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		
clear ip dhcp leasedb pool pool-name	Enable /Global	Lease 데이터베이스를 초기화합니다.
clear ip dhcp leasedb all		

(21) 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.

(22) DHCP 패킷 통계 확인

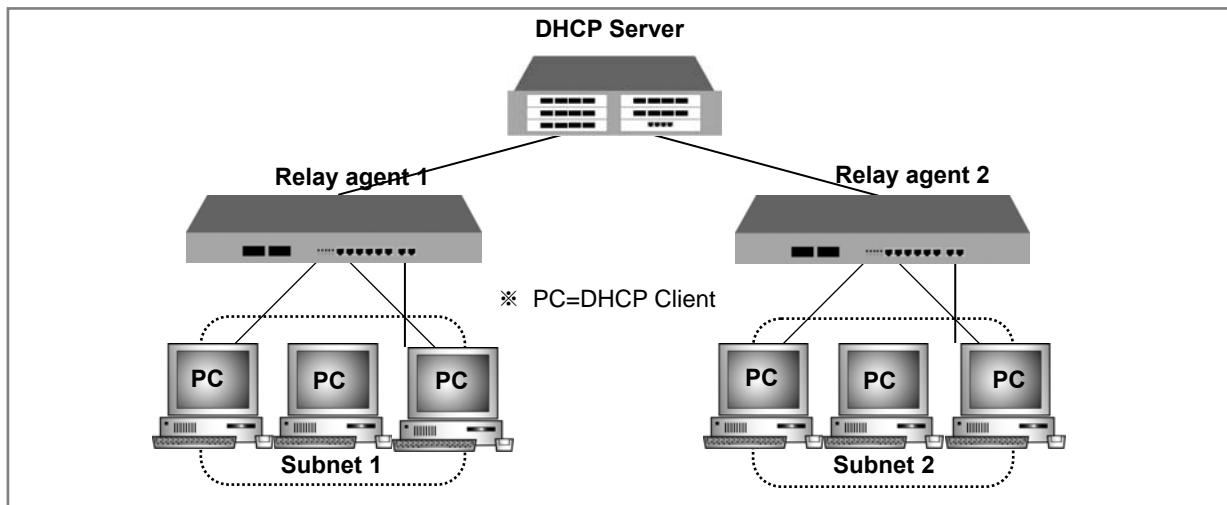
V2824에서는 다음 명령어로 다른 네트워크 장비와 주고 받은 DHCP 패킷 통계를 확인하거나 삭제할 수 있습니다.

명령어	모 드	기 능
show ip dhcp server statistics	Enable/	DHCP 패킷 통계를 확인합니다.
clear ip dhcp statistics	Global/Bridge	DHCP 패킷 통계를 삭제합니다.

8.9.2 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 8-39 】 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

V2824를 DHCP Relay 에이전트로 설정하시려면, 먼저 DHCP 서버로서 활성화 한 다음 DHCP Relay 에이전트로 설정하시면 됩니다.

1 단계 DHCP 서버로서 V2824를 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) Vendor별 DHCP 서버 지정

V2824는 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-id*는 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.

(3) Smart Relay 설정

V2824는 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 설정하려면, 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.

(4) DHCP 서버 ID 설정

두개 이상의 DHCP 서버가 하나의 DHCP 릴레이 에이전트와 연결되어 있을 때, 어떤 클라이언트가 IP를 요청할 경우 그것을 할당해 주기위해 DHCP 릴레이 에이전트와 연결된 모든 DHCP 서버에 관련된 정보를 보내게 됩니다. DHCP 서버 ID를 설정할 경우, 해당 클라이언트에게 IP를 할당할 하나의 서버를 기억해 두었다가 해당 서버에게만 관련 정보를 보내게 됩니다.

DHCP 릴레이 에이전트가 DHCP 서버 ID를 인식하여, 해당 서버로만 DHCP_REQUEST 메시지를 보내게 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp relay aware-server-id	Global	DHCP 서버 ID를 통해 DHCP 서버로 정보를 보내도록 설정합니다.
no ip dhcp relay aware-server-id		DHCP 서버 ID를 인식하는 설정을 해제합니다.

(5) DHCP 릴레이 에이전트 패킷 통계 확인

V2824에서는 DHCP 릴레이 에이전트의 다른 네트워크 장비가 주고 받은 DHCP 패킷 통계를 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip dhcp relay statistics all	Enable/	DHCP 릴레이 에이전트의 패킷 통계를 보여줍니다.
show ip dhcp relay statistics vlan <i>vlan-id</i>	Global/ Bridge	특정한 VLAN 안에서 DHCP 릴레이 에이전트의 패킷 통계를 보여줍니다.

V2824에서는 DHCP 릴레이 에이전트의 다른 네트워크 장비와 주고 받은 DHCP 패킷 통계를 삭제하려면, 다음 명령어를 사용하십시오.

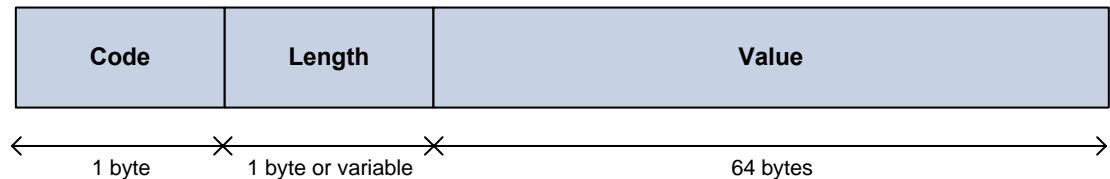
명령어	모 드	기 능
clear ip dhcp relay statistics	Enable/ Global/Bridge	DHCP 릴레이 에이전트의 패킷 통계를 초기화합니다.

8.9.3 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 실제값인 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 실제값으로 **hex**, **index**, **ip**, **string** 형태로 설정 가능합니다.

해당 DHCP Option Format을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<pre>attr <1-32> type <0-255> length { <1-64> variable } value { hex index ip string } value</pre>		DHCP Option을 정의하는 Attribute 값의 Type, Length, Value를 설정합니다.
<pre>attr <1-32> type <0-255> length-hidden { <1-64> variable } value { hex index ip string } value</pre>	DHCP Option	DHCP Option을 정의하는 Attribute 값의 Length와 Value를 설정합니다.
<pre>attr <1-32> length variable value { hex index ip string } value</pre>		DHCP Option을 정의하는 Attribute 값의 Value를 설정합니다.



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
show ip dhcp option format format-name	Enable/ Global/ DHCP Option	DHCP Option 설정을 확인합니다. .
show ip dhcp option format format-name port port-number vlan vid		포트와 VLAN에 따른 DHCP Option 설정을 확인합니다.

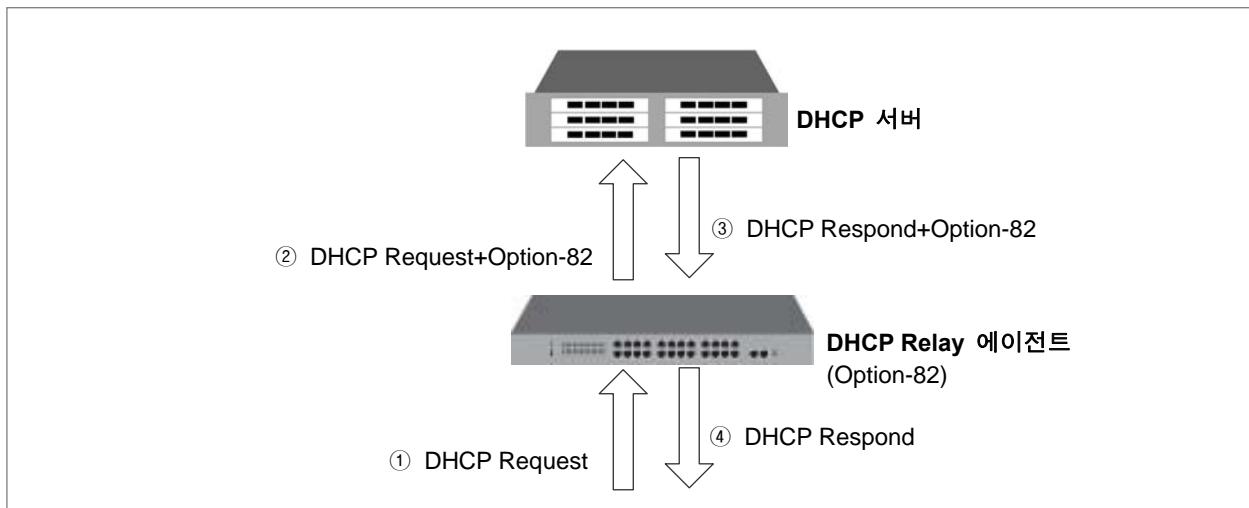
8.9.4 DHCP Option-82 설정

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.

V2824는 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 8-40 】 DHCP Option-82를 사용하는 경우의 패킷 흐름

(1) DHCP Option-82 활성화

V2824에 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

V2824의 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. V2824 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		
system-remote-id text remote-id	Option-82	Remote-ID의 형식을 변경합니다.
system-remote-id option format format-name		
system-remote-id index index		

Circuit-ID의 형식을 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
system-circuit-id port-number hex hexstring	Option-82	Circuit-ID의 형식을 변경합니다.
system-circuit-id port-number index <0-65535>		
system-circuit-id port-number text remote-id		
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	Option-82	Remote-ID와 Circuit-ID의 형식을 변경한 것을 해제합니다.
no system-remote-id option format		
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 정 보 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 <i>hexstring</i>	Option-82	
trust remote-id ip <i>ip-address</i>		Remote-ID의 형식을 변경합니다.
trust remote-id text <i>remote-id</i>		
trust remote-id index <i>index</i>		
no trust remote-id hex <i>hexstring</i>		
no trust remote-id ip <i>ip-address</i>		Remote-ID의 형식을 해제합니다.
no trust remote-id text <i>remote-id</i>		
no trust remote-id index <i>index</i>		

포트에 대한 Option82 패킷의 정책을 변경하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
trust port <i>port-number</i> {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 <i>port-number</i> {normal option82 all}	Option-82	포트에 대한 패킷의 정책을 해제합니다.

8.9.5 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.

V2824는 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.



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 정 보가 되는 Remote-ID 와 Circuit-ID를 설정 합니다.
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 정 보가 되는 Remote-ID 와 Circuit-ID의 설정 을 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.
no address range start-ip-address end-ip-address		설정했던 IP 주소 범위를 삭제합니다.

(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.

8.9.6 DHCP 클라이언트

V2824는 DHCP 클라이언트로 설정하여 DHCP 서버로부터 자동으로 IP 주소를 할당 받도록 할 수 있습니다. V2824가 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 V2824에 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. V2824에 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 V2824가 사용할 호스트 이름을 설정할 수 있습니다. 클라이언트가 된 V2824가 사용할 호스트 이름을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp client host-name <i>hostname</i>	Interface	클라이언트에 호스트 이름을 설정합니다.
no ip dhcp client host-name		설정했던 호스트 이름을 삭제합니다.



DHCP 클라이언트의 호스트 이름은 기본적으로 “switch”로 설정되어 있습니다.

(5) IP 주소 사용 시간 제한

V2824는 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.



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. V2824는 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.



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 V2824의 DHCP 클라이언트 관련 설정 내용을 확인할 수 있습니다.

명령어	모 드	기 능
show ip dhcp client interface-name	Enable/Globla/Interface	클라이언트 설정을 확인합니다.

8.9.7 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. V2824는 DHCP Snooping을 시스템 전체에 설정할 수도 있고, VLAN 별로 설정할 수도 있습니다.

(1) DHCP Snooping 활성화

V2824는 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.



참 고

DHCP Snooping은 기본적으로 비활성화 되어 있습니다.

(2) VLAN별 DHCP Snooping 설정

V2824는 VLAN 별로 DHCP Snooping 기능을 설정할 수도 있습니다. VLAN별로 DHCP Snooping을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping vlan vlan-id	Global	VLAN별로 DHCP Snooping을 설정합니다.
no ip dhcp snooping vlan vlan-id		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 port-number	Global	Trust 포트를 지정합니다.
no ip dhcp snooping trust port-number		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 port-number filter egress bcast-req	Global	지정된 Trust 포트의 Egress 브로드캐스트 요청 패킷을 필터링합니다.
no ip dhcp snooping trust port-number filter egress bcast-req		설정된 Egress 브로드캐스트 요청 패킷 필터링 기능을 해제합니다.

(5) DHCP 패킷 수 제한

V2824는 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 port-number <1-255>	Global	포트에 전송되는 초당 DHCP 패킷 수를 설정합니다.
no ip dhcp snooping limit-rate port-number		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.

(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

V2824는 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

V2824는 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) 고정 IP 사용자 차단

ARP-inspection 기능으로 static ARP 테이블과 더불어 DHCP snooping 바인딩 테이블을 참조하게 하여 고정 IP 사용자를 차단할 수 있습니다. ARP-inspection 기능을 통해 할당된 IP 주소 및 관련 정보를 담은 DHCP Snooping 바인딩 테이블을 참조하게 하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping arp-inspection start <1-2147483637>	Global	DHCP snooping 바인딩 테이블을 참조하는 지역 시간을 설정합니다.
no ip dhcp snooping arp-inspection start		DHCP snooping 바인딩 테이블을 참조하는 지역 시간을 해제합니다.



바인딩 테이블 참조 시간의 단위는 초(second)입니다. 기본값은 1800초로 설정되어 있습니다.

(11) DHCP Option-82 추가 설정

L2 환경에서 DHCP 메시지가 서버로 전송될 때 스위치는 DHCP Option-82 정보를 추가하거나 제거 할 수 있습니다. 사용자 장비가 DHCP Snooping과 DHCP Option-82 기능이 활성화 되어 있는 상태라면 DHCP 패킷은 Option-82 정보가 추가되어 전송됩니다.

DHCP Snooping이 활성화 된 상태에서 Option-82 정보를 추가하거나 제거하도록 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip dhcp snooping information option	Global	DHCP 패킷에 Option-82 정보를 추가하여 서버로 전송하도록 설정합니다.
no ip dhcp snooping information option		DHCP 패킷에 Option-82 정보를 추가하여 서버로 전송하도록 설정한 것을 해제합니다.



참 고

V2824는 DHCP Snooping 기능이 활성화 되어 있다면 기본적으로 DHCP 패킷에 Option-82 정보가 포함되어 있습니다.

(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 제공해야 할 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	Enable/	DHCP Snooping 설정 내용을 확인합니다.
show ip dhcp snooping binding	Global	DHCP Snooping 바인딩 테이블을 확인합니다.



참 고

*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.

8.9.8 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.



주 의

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
<code>ip dhcp verify source port-number</code>		IP 주소를 이용하여 IP Source Guard를 동작시킵니다.
<code>ip dhcp verify source port-security port-number</code>	Global	IP 주소와 MAC 주소를 이용하여 IP Source Guard를 동작시킵니다.



주 의

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 사용하십시오.

명령어	모 드	기 능
show ip dhcp verify source binding	Enable / Global	고정된 IP 소스 바인딩을 확인합니다.

8.9.9 DHCP 디버깅

DHCP 기능을 효율적으로 디버깅하거나 그 설정을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
debug dhcp {filter lease packet service all}	Enable	DHCP 기능을 디버깅 합니다.
no debug dhcp {filter lease packet service all}		디버깅 설정을 해제합니다.

8.10 Storm Control

V2824는 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 Apple talk 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.

V2824에서 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. V2824는 브로드캐스트 Storm 뿐만 아니라 멀티캐스트나 DLF(Destination Lookup Fail) Storm에 대한 조절도 가능하게 되었습니다.



참 고

V2824는 기본적으로 Storm Control이 동작하지 않도록 설정되어 있습니다.

브로드 캐스트, 멀티캐스트, DLF 패킷 종류에 따라 Storm Control을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
storm-control {broadcast multicast dlf} <i>rate [port-number]</i>	Bridge	Storm Control을 설정합니다.
no storm-control {broadcast multicast dlf} <i>rate [port-number]</i>	Bridge	Storm Control을 해제합니다.
show storm-control	Enable / Global / Bridge	Storm Control 설정을 확인합니다.



참 고

*rate*는 FE 포트는 <1 - 262,142>, GE 포트는 <1 - 2,097,150> 사이에서 지정 가능합니다.



참 고

*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.

8.11 Jumbo-frame 수용하기

이더넷 환경에서 수용이 가능한 패킷의 범위는 64Byte부터 1,518Byte까지입니다. 따라서 장비들은 이 범위의 이하가 되거나 이상이 되는 패킷은 취급하지 않습니다. 그러나, V2824는 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

V2824는 최대 9,216Byte까지의 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.

[설정 예제 1]

다음은 17번부터 20번 포트에 2500Byte까지의 Jumbo-frame을 받을 수 있도록 설정한 후 그 내용을 확인한 경우입니다.

```
SWITCH# configure terminal
SWITCH(config)# bridge
SWITCH(bridge)# jumbo-frame 1-10 2500
SWITCH(bridge)# show jumbo-frame
port 17 : 2500 / 1518 (current/default)
port 18 : 2500 / 1518 (current/default)
port 19 : 2500 / 1518 (current/default)
port 20 : 2500 / 1518 (current/default)
(Omitted)
SWITCH(bridge)#

```

8.12 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
mtu <68-1500>	Interface	인터페이스의 최대 전송 단위 MTU 를 설정합니다.
no mtu		최대 전송 단위 MTU 설정을 해제합니다.

8.13 대역폭 설정

라우팅 프로토콜은 라우팅 거리를 보다 효율적으로 측정하기 위해 대역폭 정보를 이용합니다. 인터페이스의 대역폭을 설정하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
bandwidth bandwidth-value	Interface	인터페이스의 대역폭을 설정합니다.
no bandwidth		대역폭 설정을 해제합니다.



참 고

V2824는 최대 1에서 10,000,000 Kbits까지의 대역폭을 인터페이스에서 설정할 수 있습니다. 기본적으로는 100m 으로 설정되어 있습니다.

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 내보내 지는 것이 아니라 단 한번의 데이터 전송으로 여러 수신자에게 전달된다는 점이 유니캐스트와 다른 점입니다.

이러한 특징 때문에 멀티캐스트는 데이터의 중복 전송으로 인한 네트워크 자원 낭비를 최소화 하고, 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.

V2824는 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.

이 장은 다음과 같은 내용으로 이루어집니다.

- IGMP (Internet Group Management Protocol)
- 멀티캐스트 부가 기능 설정

9.1 IGMP (Internet Group Management Protocol)

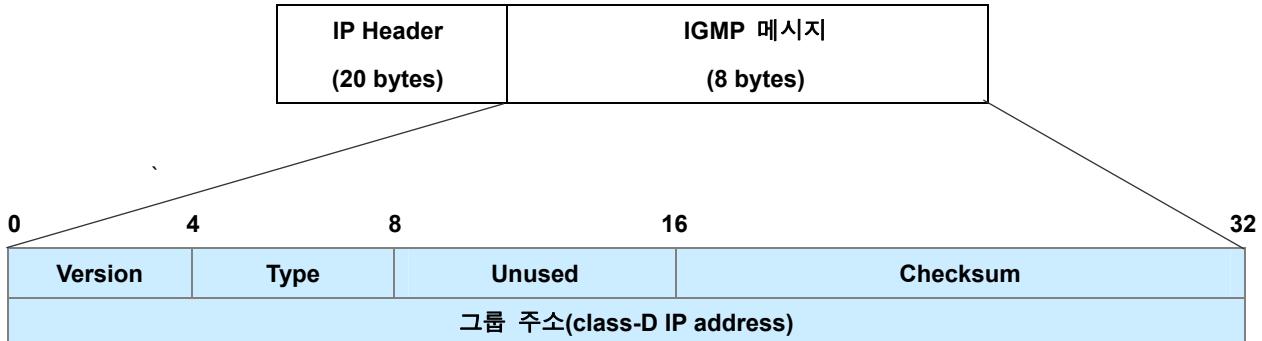
멀티캐스트 전송 방식의 핵심은 멀티캐스트 그룹 관리에 있습니다. 이러한 그룹 멤버쉽을 통하여 라우터는 어떠한 호스트가 멀티캐스트 패킷을 요청하는지 판단하여 해당 그룹에만 트래픽을 보내줍니다.

IGMP(Internet Group Management Protocol)란 멀티캐스트 패킷을 수신하고자 하는 호스트와 멀티캐스트 패킷을 전송하는 라우터 간의 통신을 위한 프로토콜로, 호스트가 멀티캐스트 그룹으로 Join하면 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 9-1 】 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 Join하는 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 대역 폭 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 9-2 】 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.

V2824는 IGMP 버전 1, 버전 2, 버전 3을 지원합니다.

(1) IGMP 버전 설정

V2824는 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.

V2824의 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

V2824에 설정된 QRV 설정값은 기본적으로 2회입니다. 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

V2824는 IGMP 데이터베이스를 초기화할 수 있는 명령어를 제공합니다. IGMP 인터페이스별로 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.

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 V2824는 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]	Global	
no ip igmp static-group list {<1-99> <1300-1999> access-list-name } vlan vlan-id port port-number		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 특정 Static 그룹에게만 호스트들이 접근할 수 있도록 제한 할 수 있습니다. 각 인터페이스당 멀티캐스트 그룹의 접속 리스트를 관리하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip igmp static-group <i>group-address</i>	Interface	해당 인터페이스에 멀티캐스트 그룹 접속 리스트를 설정합니다.
ip igmp static-group range <i>start-ip-address end-ip-address</i>		

설정한 멀티캐스트 그룹들의 접속 리스트를 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp static-group <i>group-address</i>	Interface	해당 인터페이스에 멀티캐스트 그룹 접속 리스트를 해제합니다.
no ip igmp static-group range <i>start-ip-address end-ip-address</i>		

(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 V2824가 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. V2824는 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.

설정한 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 재선출 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 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 인터페이스에 IGMP Proxy 가 설정되어 있는 상태에서 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.

V2824는 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 하나만 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 그룹으로 부터만 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.

V2824는 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
Source address(1)			
Source address(...)			
Source address(n)			

【 그림 9-3 】 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.

IGMP Type = 0x22	Reserved	Checksum	Record Type	Aux Len	Number of Source
Multicast Group Address					
Reserved	Number of Record	Source Address (1)			
Group Record (1)					
.....		Source Address (2)			
Group Record (n)					
		Source Address (3)			
		'			
		;			
		Source Address (n)			
			Auxiliary Data		

【 그

림 9-4 】 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 V2824의 IGMP 그룹과 관련 내용을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip igmp interface	Enable/ Global/ Bridge	해당 혹은 모든 인터페이스에 있는 멀티캐스트 관련 설정 내용을 확인합니다.
show ip igmp interface interface-name		

9.2 멀티캐스트 부가 기능 설정

V2824 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

V2824는 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-multicast [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-multicast [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.

V2824의 멀티캐스트 포워딩 데이터베이스의 Aging time이나 엔트리 개수를 제한하는 Aging-limit을 설정하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip mcfdb aging-limit aging-limit-value		McFDB의 포워딩 엔트리 최대 개수를 지정합니다.
ip mcfdb aging-time aging-time-value	Global	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

V2824에 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 설정 값을 확인합니다.
show ip mcfdb aging-entry {vian 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.

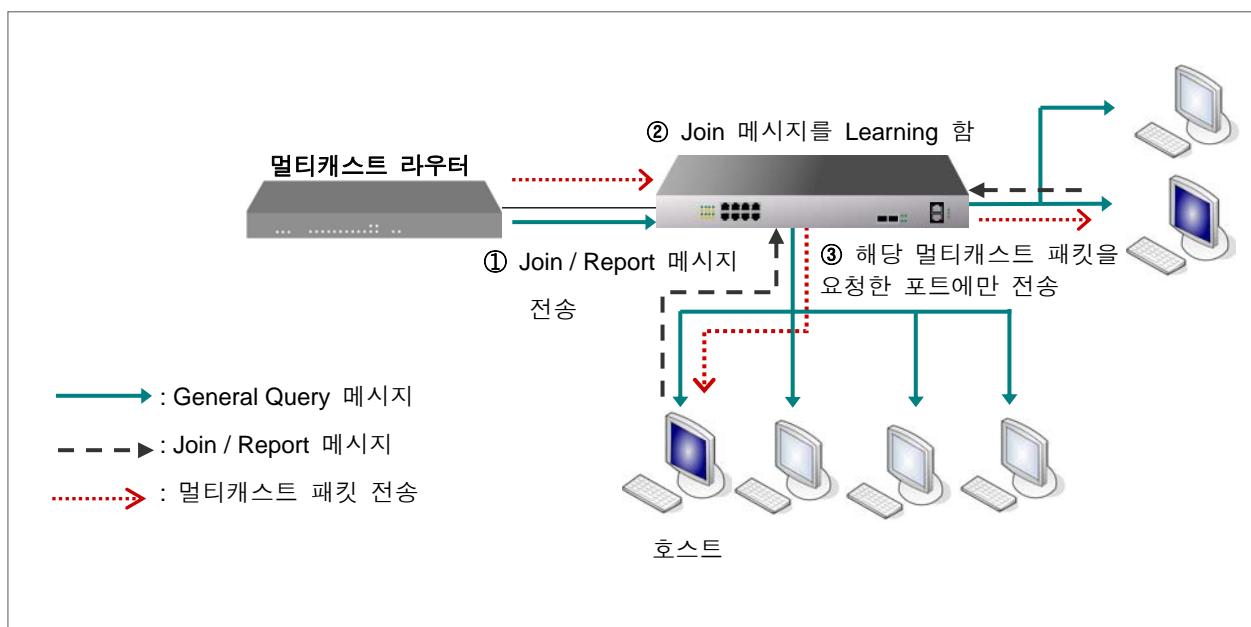
명령어	모 드	기 능
clear ip mcfdb [* vian vlan-id]	Enable/	모든 혹은 특정 VLAN의 멀티캐스트 포워딩 엔트리 정보를 초기화합니다.
clear ip mcfdb vian vlan-id group group-ip-address source ip-address	Global	특정한 멀티캐스트 그룹 주소와 VLAN으로부터 사용되는 멀티캐스트 포워딩 엔트리 정보를 초기화합니다.

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 Snooping이 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.

V2824는 멀티캐스트 포워딩 테이블 관리를 통해 멀티캐스트 트래픽을 필요로 하는 호스트들에게만 패킷을 효과적으로 전송할 수 있습니다. 다음은 IGMP Snooping이 활성화된 스위치가 호스트와 멀티캐스트 라우터 사이에서 멀티캐스트 통신을 하는 모습입니다.



【 그림 9-5 】 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 vlan-id		특정 VLAN에 IGMP snooping 기능을 활성화합니다.



참 고

V2824의 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		IGMP Snooping 기능을 해제 합니다.
no ip igmp snooping vlan <i>vlan-id</i>	Global	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. V2824는 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>	Global	시스템에 IGMP Snooping 버전을 설정합니다.
ip igmp snooping vlan <i>vlan-id</i> version <1 – 3>		특정 VLAN에 IGMP Snooping 버전을 설정합니다.



참 고

V2824의 IGMP Snooping 버전은 Static으로 설정할 때만 변경할 수 있으며, 기본적으로 버전 3으로 설정되어 있습니다.

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 보내도록하여 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

V2824에 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		
no ip igmp snooping vlan <i>vlan-id</i> robustness-variable	Global	Robustness variable 설정값을 삭제하고 기본 설정값으로 변경됩니다.

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 PIM과 IGMP 기능이 설정되지 않은 특정 VLAN에서 IGMP Snooping 기능을 지원하도록 도와줍니다.

V2824에 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]		IGMP Snooping Querier를 활성화합니다.
ip igmp snooping vlan <i>vlan-id</i> querier [address source-address]	Global	특정 VLAN에 IGMP Snooping Querier를 활성화합니다.

IGMP Snooping Querier를 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping [vlan <i>vlan-id</i>] querier [address <i>source-address</i>]	Global	IGMP Snooping Querier 설정을 해제합니다.



참 고

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 [vlan <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>	Global	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 기본 값으로 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	Global	특정 VLAN에 설정된 Group-specific 또는 Group-source-specific Query 메시지 전송 주기를 삭제합니다.

(3) IGMP Snooping Immediate-Leave 설정

V2824의 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. (9.2.3(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 해제 합니다.
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 호스트들은 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 사용해야하는 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 설정합니다.
ip igmp snooping vlan <i>vlan-id</i> explicit-tracking		특정 VLAN에 IGMP 호스트 트래킹 기능을 설정합니다.

설정한 호스트 트래킹 기능을 해제하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
no ip igmp snooping explicit-tracking	Global	시스템에 IGMP 호스트 트래킹 기능을 해제합니다.
no ip igmp snooping vlan <i>vlan-id</i> explicit-tracking		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 1024 입니다.

호스트 트랙킹 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 로드가 커질 수 있으므로, 이에 대한 설정을 해제시킬 수 있습니다.

호스트로부터 Leave 메시지를 받을 경우, Group Specific Query 메시지 전송을 해제하거나, 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.



참 고

V2824는 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>		특정 VLAN의 호스트 트래킹 정보를 확인합니다.
show ip igmp snooping explicit-tracking port <i>port-number</i>	Enable/ Global/ 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.
show ip igmp snooping explicit-tracking summary vlan <i>vlan-id</i>		특정 VLAN의 호스트 트래킹 요약 정보를 확인합니다.
show ip igmp snooping explicit-tracking summary port <i>port-number</i>		특정 포트의 호스트 트래킹 요약 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. V2824는 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 <i>vlan-id</i> 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	Global	PIM hello 패킷을 이용하여 멀티캐스트 라우터 포트를 지정하는 설정을 해제합니다.
no ip igmp snooping vlan <i>vlan-id</i> mrouter learn pim		

멀티캐스트 라우터 포트 Forwarding 설정

멀티캐스트 Source 정보를 멀티캐스트 라우터로 보내야 하기 때문에, L2 스위치의 경우 IGMP Snooping 맴버쉽 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 라터 포트로 멀티캐스트 트래픽 Forwarding을 활성화 또는 해제하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
ip multicast mrouter-pass-through	Global	멀티캐스트 라우터 포트들로 멀티캐스트 트래픽을 포워딩합니다.
no ip multicast mrouter-pass-through		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, 토플로지가 갑자기 변경되었을 경우 신속한 통신 서비스 복구를 위한 기능입니다. 이 기능은 이더넷 링 토플로지와 같은 망을 이용하여 Redundancy를 제공하는데 중요한 역할을 합니다.

IGMP Snooping TCN은 토플로지의 변화를 감지할 때 일정 시간동안 멀티캐스트 트래픽을 Flooding 하는 기능과 망의 IGMP Querier에게 IGMP General Query를 요청하는 두가지 기능을 제공합니다.

첫번째, Flooding 기능은 토플로지 변화가 감지되면 서비스 중인 멀티캐스트 트래픽을 모든 포트로 Flooding 하여 토플로지의 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 토플로지의 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 <i>vlan-id</i> 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.



V2824가 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.



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.



참 고

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. (**9.2.3(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 info [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 table group [ip-address]	Enable/ Global/ Bridge	시스템 전체의 IGMP Snooping 테이블 정보를 확인합니다.
show ip igmp snooping table port [port-number]		특정 포트의 IGMP Snooping 테이블 정보를 확인합니다.
show ip igmp snooping table vlan [vlan-id]		특정 VLAN의 IGMP Snooping 테이블 정보를 확인합니다.
show ip igmp snooping table reporter [ip-address]		특정 Report의 IGMP Snooping 테이블 정보를 확인합니다.

IGMP Snooping 그룹의 요약 정보를 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show ip igmp snooping groups summary [vlan <i>vlan-id</i>]	Enable/ Global/ Bridge	특정 VLAN의 IGMP Snooping 그룹 요약정보를 확인합니다.
show ip igmp snooping groups summary [port <i>port-number</i>]		특정 포트의 IGMP Snooping 그룹 요약정보를 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.

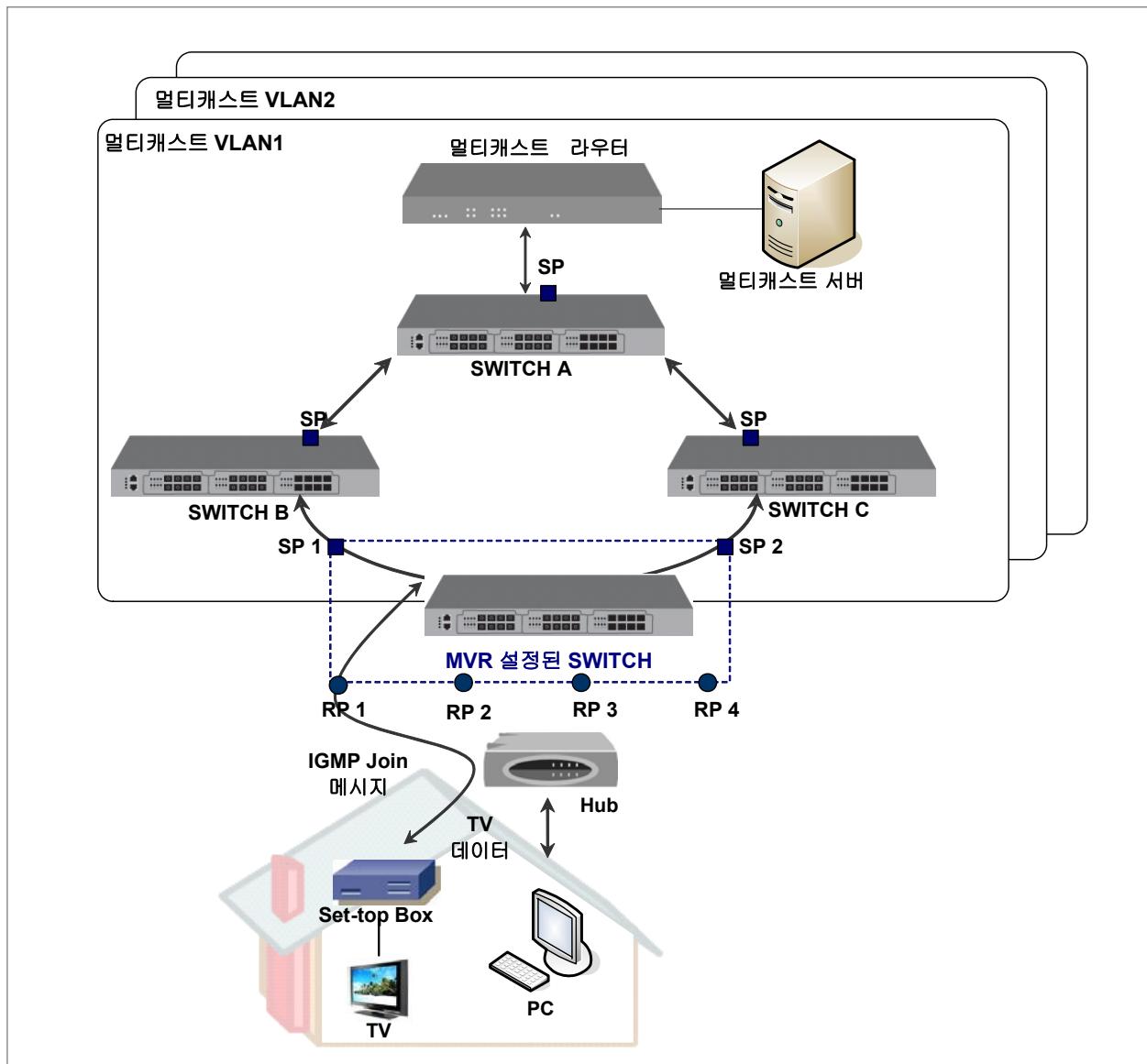
IGMP Snooping 통계 정보를 초기화하려면 다음 명령어를 사용하십시오.

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 9-6 】 MVR 동작

위의 그림은 멀티캐스트 서버와 멀티캐스트 라우터, 그리고 SWITCH 등 모든 장비가 같은 한 VLAN에 속하고 MVR 설정이 되어 있는 스위치가 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 이를 요청했던 가입자에게 전송합니다.



주의

V2824에 MVR을 설정할 때 Receiver 포트는 반드시 MVR VLAN과 가입자 VLAN에 모두 untagged VLAN으로 설정되어 있어야 합니다.



주의

V2824에 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

V2824에서 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.



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.



“profile-number”는 IGMP Profile의 고유한 이름인 동시에 최대 개수로 1에서 2,147,483,648까지 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.



“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.

V2824는 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) 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 all count <1-2147483647>	Global	모든 포트에 Join할 수 있는 최대 IGMP 그룹의 수를 설정합니다.
ip igmp max-groups port port-number count <1-2147483647>	Global	특정 포트에 Join할 수 있는 최대 IGMP 그룹의 수를 설정합니다.
no ip igmp max-groups port {all 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.

(3) 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
<code>no ip igmp filter port port-number packet-type { all leave query reportv1 reportv2 reportv3}</code>	Global	특정 IGMP 패킷에 대한 필터링 설정을 해제합니다.

(4) IGMP 필터링 확인

IGMP 필터링 관련 설정 내용을 확인하려면 다음과 같은 명령어를 사용하십시오.

명령어	모 드	기 능
<code>show ip igmp filter [port port-number]</code>	Global	IGMP 필터링 관련 설정 내용을 확인합니다.

IGMP Profile을 확인하려면 다음 명령어를 사용하십시오.

명령어	모 드	기 능
<code>show ip igmp profile [profile-number]</code>	Enable / Global / Bridge	설정된 IGMP Profile을 확인합니다.

9.2.8 Static SSM 맵핑 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) 엔트리로 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.

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 V5548G가 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.

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) 멤버쉽 Report 메시지들을 통틀어 지칭하는 단어입니다. 설정 값을 초과하는 멤버쉽 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.

9.2.11 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 라우트 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 라우트 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.

MRIB 디버깅의 설정 내용을 확인하려면, 다음 명령어를 사용하십시오.

명령어	모 드	기 능
show debugging nsm mcast	Enable	MRIB 디버깅의 설정 내용을 확인합니다.

부록 A. 시스템 이미지 설치하기

V2824는 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.

- Enable 모드에서 시스템 이미지 설치
- Boot 모드에서 시스템 이미지 설치
- 원격에서 시스템 이미지 설치하기

A.1 Enable 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.

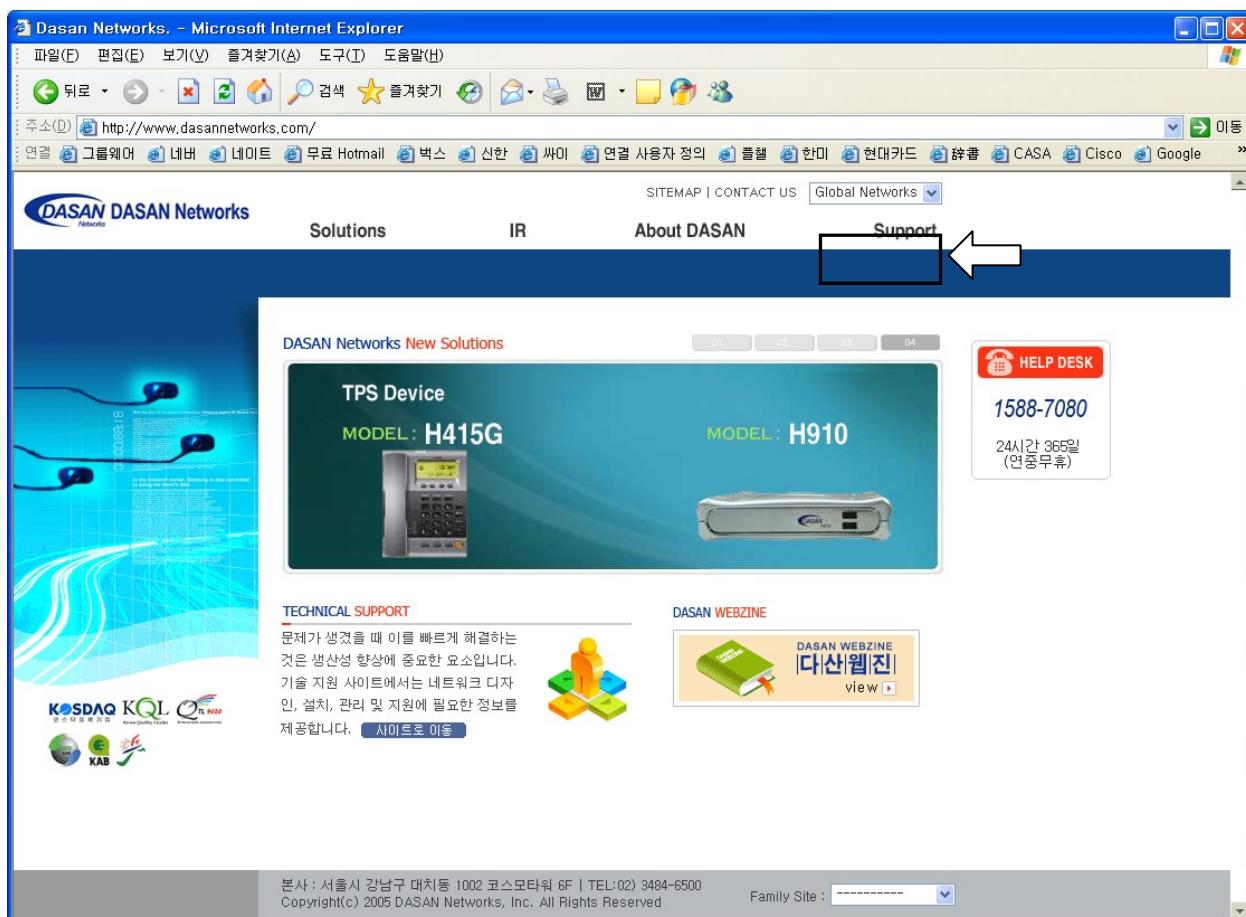
1 단계 FTP/TFTP 서버로 시스템 이미지 내려 받기**2 단계** 시스템 이미지 설치 준비**3 단계** 시스템 이미지 설치**A.1.1 FTP/TFTP 서버로 시스템 이미지 내려 받기**

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.

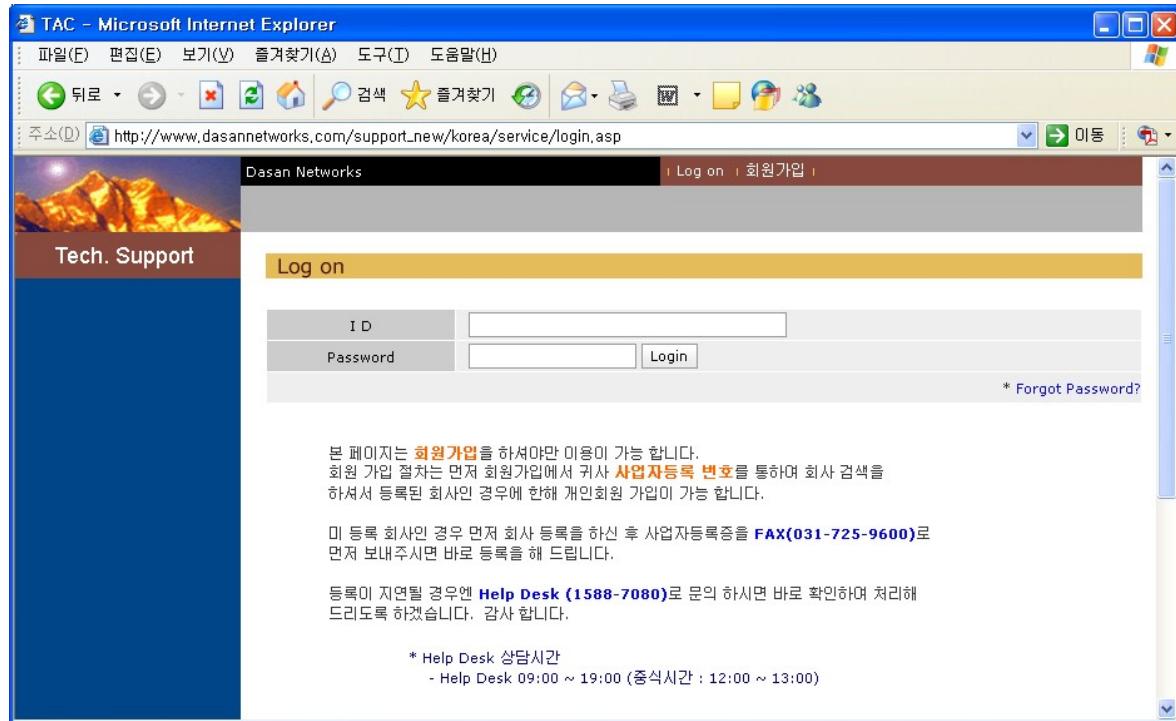
다음은 웹에서 사용자 PC의 FTP/TFTP 서버에 장비의 이미지 파일을 내려 받는 순서입니다.

1 단계 (주)다산네트웍스의 홈페이지에 접속합니다.

홈페이지의 주소는 <http://www.dasannetworks.com/> 입니다.

2 단계 Main의 우측 상단에 있는 “**Support**”를 클릭하여 들어가십시오.

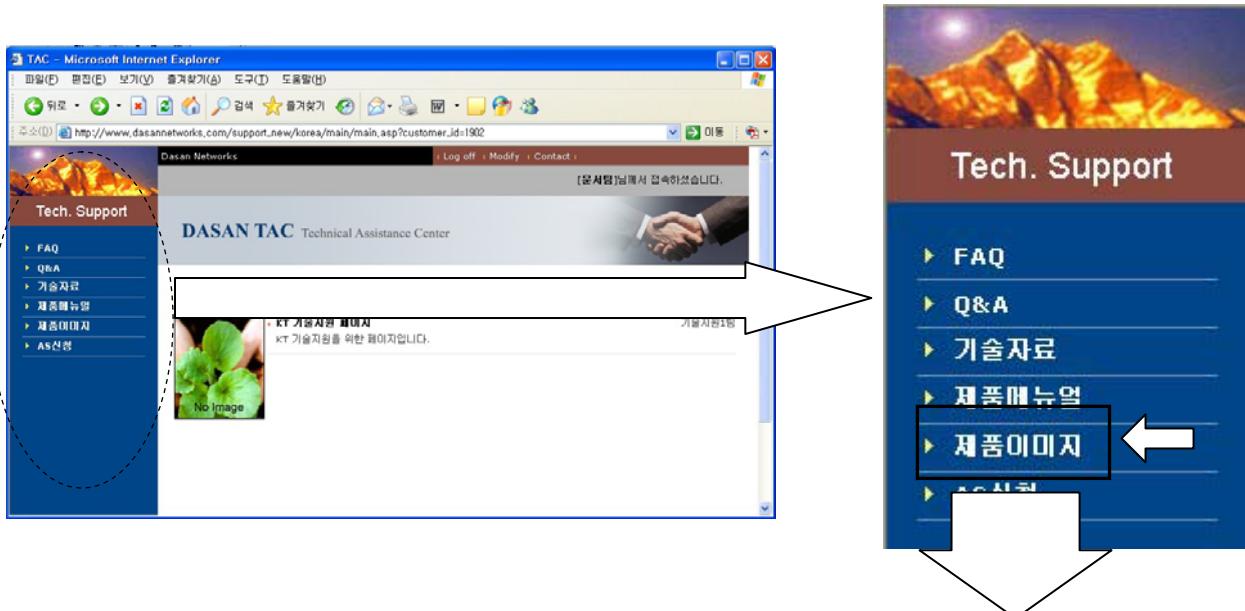
3단계 사용자가 가지고 있는 계정으로 로그인 하십시오.

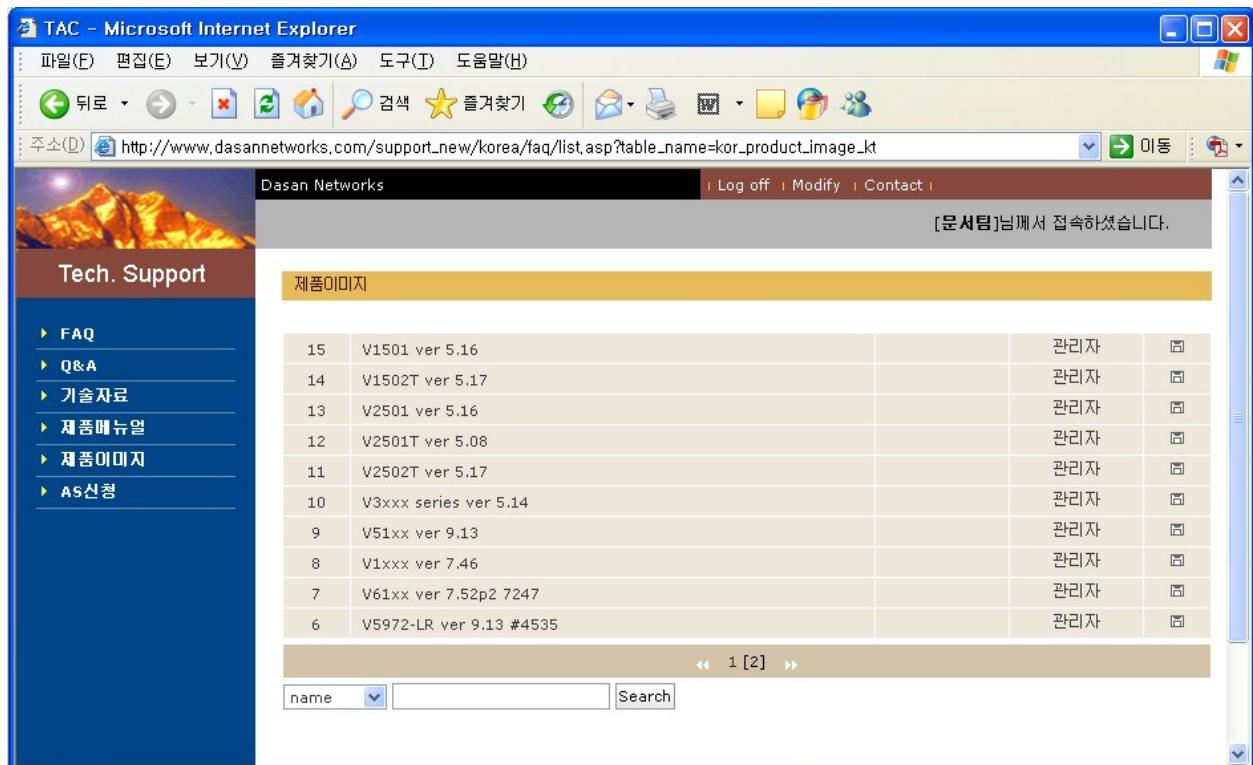


i 참고

Support의 서비스는 회원가입을 하셔야 이용할 수 있습니다. 계정이 없는 사용자는 홈페이지에서 설명한 방법에 따라 먼저 회원가입을 하시기 바랍니다.

5 단계 로그인에 성공하여 페이지가 이동하면, 좌측 메뉴바에서 “제품이미지”를 클릭하십시오.





6 단계 사용자가 원하는 제품의 시스템 이미지에서 왼쪽 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 2번 사용하여 Enable 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.1.3 시스템 이미지 설치

FTP/TFTP를 사용하여 시스템 파일을 설치하려면 사용자 PC에 FTP/TFTP 서버 프로그램이 설치되어 있어야 합니다. 그리고 다음 순서에 따라 사용자의 장비에서 FTP/TFTP 서버로부터 시스템 이미지 파일을 내려 받으십시오.

1 단계 Enable 설정 모드에서 다음 명령어를 사용하여 FTP/TFTP 서버로부터 사용자가 원하는 시스템 이미지 파일을 설치합니다.

명령어	모 드	기 능
copy {ftp tftp} os download os1	Enable	시스템 이미지 파일을 설치합니다.



os1는 시스템 이미지 파일이 저장되는 플래시 메모리 위치를 나타냅니다. 장비에 저장할 때에는 반드시 이 위치를 지정해야 합니다.

FTP/TFTP 서버에 로그인 하기 위해서는 서버에 접근 가능한 사용자 계정과 패스워드를 입력하여야 하며 파일을 내려 받는 동안 마침표(.)가 출력됩니다.

```
SWITCH(config)# copy ftp os download os1
To exit : press Ctrl+D
-----
IP address or name of remote host (FTP): 50.0.158.1
Download File Name : V18XX.3.13.x
User Name : admin      ← FTP user account
Password:            ← FTP user password
Hash mark printing on (1024 bytes/hash mark).
Erasing OS area ..
Downloading NOS ....
#####
#####
9814048 bytes download OK.
SWITCH(config)#+
```

2 단계 멀티 OS를 사용하고자 하는 경우에는 위의 명령어를 사용하여 **1 단계**와는 다른 위치에 이미지 파일을 설치하십시오.

3 단계 Privilege Exec Enable 모드에서 **reload** 명령으로 시스템을 재부팅 시켜 명령으로 시스템 이미지 파일이 성공적으로 설치되었는지 버전을 확인하십시오.

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 4.19   *
*          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 IP 를 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 4.19   *  
*          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 server-ip-address file-name</code>	Boot	시스템 이미지 파일을 설치합니다.



참 고

os1는 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 V18XX.3.13.x
Loading V18XX.3.13.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

V2824와 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>



주 의

위의 내용은 사용자 PC 디렉토리 내용에 따라 달라질 수 있습니다.

5 단계 사용자 PC에서 FTP로 장비에 접속하십시오. 예제에서의 사용자 ID는 admin, 패스워드는 없습니다.

```
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 admin.
Password:
230 User admin 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	FTP	시스템 이미지 파일을 설치합니다.



참 고

os1는 시스템 이미지 파일이 저장되는 플래시 메모리 위치를 나타냅니다. 장비에 저장할 때에는 반드시 이 위치를 지정해야 합니다.



주의

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 지연되는데 도중에 장비의 전원을 끄거나 멈추면 장비가 부팅이 되지 않는 등의 치명적인 영향을 미칠 수 있으므로 주의하시기 바랍니다.

```
ftp> put V18XX.3.13.x os1
200 PORT command successful.
150 Opening BINARY mode data connection for os.
#####
#####
```

(종략)

```
226 Transfer complete.
ftp: 6328412 bytes sent in 72.89Seconds 86.83Kbytes/sec.
ftp>
```

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.



(주)다산네트웍스
경기도 성남시 분당구 수내동 11-4
휴맥스 빌리지 6층
Helpdesk) 1588-7080