L2 Managed Switch CLI User Manual

for 4MI-G2404FPM, 4MI-G1604FPM

본 매뉴얼의 내용에 대한 저작권은 주식회사 포에망이텍에 있으며, 사전 서면 승인 없이 본 문서의 일부 또는 전체를 무단 복제, 배포, 수정, 전송 또는 저장하는 행위를 금합니다.

본 매뉴얼에 수록된 내용은 제품 성능 향상 및 기능 개선을 위해 사전 예고 없이 변경될 수 있습니다.

문서 내의 정보는 작성 시점을 기준으로 하며, 실제 제품의 사양 및 기능과 차이가 있을 수 있습니다.

본 문서에 기재된 회사명, 제품명 및 로고는 해당 소유자의 상표 또는 등록상표입니다.

© 2026 주식회사 포엠아이텍. All Rights Reserved.

주식회사 포엠아이텍

1. CLI 명령줄 소개 20
1.1. 스위치 CLI 접근 방법 21
1.1.1. Console 포트를 통한 CLI 접근 21
1.1.2. TELNET 을 통한 CLI 접근 22
1.2. CLI 모드 소개 24
1.2.1. CLI 모드의 기능 24
1.2.2. CLI 모드 식별 24
1.2.3. CLI 모드 분류 25
1.3. 명령어 구문 소개 27
1.3.1. 명령어 구성 27
1.3.2. 파라미터 유형 27
1.3.3. 명령어 구문 규칙 28
1.3.4. 명령어 축약 30
1.3.5. 구문 도움말 (Syntax Help) 30
1.3.6. 명령줄 오류 메시지 31
1.4. 명령줄 단축키 31
1.4.1. 라인 편집 단축키 31
1.4.2. Show 명령어 단축키 32
1.5. 히스토리 명령어 32
2. 시스템 관리 설정 33
2.1. 시스템 보안 설정 34
2.1.1. 다중 사용자 관리 제어 34
2.1.2. Enable 비밀번호 제어 35
2.1.3. TELNET 서비스 제어 36
2.1.4. SNMP 서비스 제어 37

2.1.5. HTTP 서비스 제어 38
2.1.6. HTTPS 서비스 제어 38
2.2. 시스템 유지보수 및 점검 39
2.2.1. 시스템 시간 설정 39
2.2.2. 터미널 타임아웃 속성 설정 40
2.2.3. 시스템 재설정 40
2.2.4. 시스템 정보 조회 41
2.2.5. 네트워크 연결 상태 점검 41
2.2.6. Traceroute 디버깅 41
2.2.7. Telnet 클라이언트 42
2.2.8. SSH 클라이언트 42
2.3. 프로파일 관리 42
2.3.1. 설정 정보 조회 43
2.3.2. 설정 저장 44
2.3.3. 프로파일 삭제 44
2.3.4. Configuration file 업로드 및 다운로드 44
2.4. 소프트웨어 버전 업그레이드 47
2.4.1. 소프트웨어 버전 업그레이드 명령어 47
2.4.2. 소프트웨어 업그레이드 절차 49
3. 포트 설정 51
3.1. 포트 기본 설정 52
3.1.1. 포트 활성화 및 비활성화 52
3.1.2. 포트 속도 설정 53
3.1.3. 포트 정보 조회 53
3.2. MIRROR 설정 54

3.2.1. MIRROR 모니터링 포트 및 대상 포트 설정 54
3.2.2. MIRROR 설정 조회 56
3.3. STORM-CONTROL 설정 56
3.3.1. 기본 설정 56
3.3.2. Broadcast 억제 설정 57
3.3.3. Multicast 억제 설정 57
3.3.4. DLF(Unknown Unicast) 억제 설정 57
3.3.5. 억제율(Rate Limit) 설정 58
3.3.6. STORM-CONTROL 설정 조회 58
3.4. STORM-CONSTRAIN 설정 58
3.5. FLOW-CONTROL 설정 61
3.5.1. 기본 설정 61
3.5.2. 포트 Flow Control 설정 61
3.5.3. 포트 Flow Control 해제 62
3.5.4. Flow Control 정보 조회 62
3.6. 포트 대역폭 설정 62
3.6.1. 기본 설정 63
3.6.2. 포트 송신/수신 대역폭 제어 설정 63
3.6.3. 포트 송신/수신 대역폭 제어 해제 63
3.6.4. 포트 대역폭 설정 조회 63
3.7. TRUNK 설정 64
3.7.1. LACP 프로토콜 설정 65
3.7.2. TRUNK 그룹 설정 66
3.7.3. TRUNK 멤버 포트 설정 67
3.7.4. TRUNK 로드밸런싱 정책 설정 68

3.7.5. TRUNK 정보 조회 68
3.8. Jumbo Frame 설정 69
3.8.1. Jumbo Frame 개요 69
3.8.2. Jumbo Frame 설정 69
3.9. 이중화 포트(Redundant Port) 설정 69
3.9.1. 이중화 포트 설정 69
3.9.2. 이중화 포트 정보 조회 71
3.10. UDLD 설정 71
3.11. LLDP 설정 72
3.11.1. LLDP 설정 73
3.11.2. LLDP 정보 조회 74
4. 포트 기반 보안 설정 74
4.1. 개요 75
4.2. MAC 바인딩 설정 76
4.3. MAC 필터링 설정 77
4.4. 포트 MAC 학습 제한 설정 78
4.5. 보호 포트 설정 78
4.5.1. 보호 포트 개요 78
4.5.2. 보호 포트 설정 79
5. 포트 IP 및 MAC 바인딩 설정 81
5.1. 개요 81
5.2. IP 및 MAC 바인딩 설정 83
5.3. 설정 예시 84
5.4. 설정 문제 해결 (Configuration Troubleshooting) 86
6. 포트 루프 감지 (Port Loop Detection) 86

6.1. 개요 86
6.2. 프로토콜 동작 원리 86
6.2.1. 루프 감지 동작 과정 87
6.2.2. 복구 모드 (Recovery Mode) 87
6.2.3. 프로토콜 보안 (Protocol Security) 87
6.3. 설정 개요 (Configuration Introduction) 88
6.3.1. 전역 설정 (Global Configuration) 88
6.3.2. 인터페이스 설정 (Interface Configuration) 88
6.3.3. 설정 조회 (Display Configuration) 89
7. VLAN 설정 90
7.1. VLAN 개요 91
7.1.1. VLAN 의 장점 91
7.1.2. VLAN ID 92
7.1.3. VLAN 포트 멤버십 유형 94
7.1.4. 포트의 기본 VLAN (PVID) 94
7.1.5. 포트의 VLAN 모드 95
7.1.6. VLAN Trunk 95
7.1.7. VLAN 내 트래픽 전달 방식 (Forwarding of Traffic within a VLAN) 96
7.2. VLAN 설정 98
7.2.1. VLAN 생성 및 삭제 98
7.2.2. 포트의 VLAN 모드 설정 98
7.2.3. ACCESS 모드에서 VLAN 설정 99
7.2.4. TRUNK 모드에서 VLAN 설정 99
7.2.5. HYBRID 모드에서 VLAN 설정 100
7.2.6. VLAN 정보 조회 101

7.3. VLAN 설정 예시 101
7.3.1. 포트 기반 VLAN (Port-based VLAN) 102
7.3.2. 802.1Q 기반 VLAN 설정 예시 103
7.4. MAC / IP 서브넷 / 프로토콜 기반 VLAN 106
7.4.1. 개요 106
7.4.2. MAC / IP 서브넷 / 프로토콜 기반 VLAN 설정 107
7.5. Voice VLAN 109
7.5.1. Voice VLAN 개요 109
7.5.2. Voice VLAN 설정 110
7.5.3. Voice VLAN 설정 예시 110
7.6. VLAN 매핑 (VLAN Mapping) 112
7.6.1. 개요 112
7.6.2. VLAN 매핑 설정 113
7.7. QinQ 114
7.7.1. QinQ 개요 114
7.7.2. QinQ 설정 116
7.7.3. QinQ 설정 예시 117
8. QoS 설정 (Quality of Service) 120
8.1. QoS 개요 (QoS Introduction) 120
8.1.1. CoS 기반 QoS (802.1p) 123
8.1.2. DSCP 기반 QoS (Layer 3 QoS) 124
8.1.3. MAC 기반 QoS 125
8.1.4. Policy 기반 QoS 126
8.2. QoS 설정 (Default Configuration) 128
8.2.1. QoS 기본 설정 (Default Configuration) 128

8.2.2. QoS 스케줄링 방식 설정 130
8.2.3. Queue Weight 설정 131
8.2.4. DSCP ↔ QosProfile 매핑 설정 132
8.2.5. 포트 DSCP 기반 QoS 설정 134
8.2.6. 포트 사용자 우선순위 설정 (CoS 값) 135
8.3. QoS 설정 예시 136
8.4. Policy 기반 QoS 설정 예시 137
9. MSTP 설정 (Multiple Spanning Tree Protocol) 139
9.1. MSTP 소개 141
9.1.1. MSTP 개요 (Overview) 142
9.1.2. MST Domain (Multiple Spanning Tree Domain) 143
9.1.3. IST / CIST / CST 개념 정리 (MSTP 핵심 구조) 144
9.1.4. MSTP Domain 내부 동작 (Intra-domain Operation) 145
9.1.5. MSTP Domain 간 동작 (Interdomain Operation) 147
9.1.6. Hop Count 149
9.1.7. Boundary Port 149
9.1.8. MSTP 와 802.1D STP 간 상호 운용성 150
9.1.9. Port Role 150
9.1.10. 802.1D Spanning Tree 소개 152
9.2. MSTP 설정 153
9.2.1. MSTP 기본 설정 154
9.2.2. MSTP 일반 설정 154
9.2.3. Domain Configuration 158
9.2.4. Instance Configuration 158
9.2.5. Port configuration 159

9.2.6. PORTFAST 관련 설정 162
9.2.7. Root Guard 관련 설정 164
9.3. MSTP 설정 예제 165
10. EAPS 설정 166
10.1. EAPS 소개 167
10.2. EAPS 기본 개념 167
10.3. EAPS 프로토콜 소개 168
10.3.1. Link-Down 알림 168
10.3.2. Loop check 169
10.3.3. Ring recovery 169
10.3.4. Extreme 장비와의 EAPS 호환 169
10.3.5. 다중 EAPS 도메인 170
10.4. EAPS 설정 170
10.5. 제약 사항 170
10.6. EAPS 명령어 간략 소개 171
10.6.1. EAPS 설정 명령어 171
10.7. EAPS 구성 예제 (Single Ring) 173
10.8. Cross Ring 데이터 포워딩 설정 예제 177
11. ERPS 설정 181
11.1. ERPS 개요 181
11.2. ERPS 기술 소개 182
11.2.1. ERPS Ring 182
11.2.2. ERPS Node 182
11.2.3. Link 및 Channel 183
11.2.4. ERPS VLAN 184

11.3. ERPS 동작 원리 184
11.3.1. Normal State 184
11.3.2. Link failure 184
11.3.3. Link Recovery 185
11.4. ERPS 기술 특징 186
11.4.1. ERPS Load Balancing 186
11.4.2. 높은 보안성 186
11.4.3. 다중 링 접점/교차 지원 187
11.5. ERPS 프로토콜 명령어 188
11.6. ERPS 대표 적용 예제 189
11.6.1. Single Ring Example 190
11.6.2. Multi-loop 예제 (번역) 193
11.6.3. Multi-Instance Load Balancing Example 198
12. AAA 설정 201
12.1. 802.1X 소개 202
12.1.1. 802.1X 장비 구성 203
12.1.2. 프로토콜 패킷 소개 204
12.1.3. 프로토콜 동작 흐름 205
12.1.4. 802.1X 포트 상태 207
12.2. RADIUS 소개 208
12.2.1. 프로토콜 패킷 소개 208
12.2.2. 프로토콜 동작 흐름 209
12.2.3. 사용자 인증 방식 210
12.3. 802.1X 설정 211
12.3.1. 802.1X 기본 설정 211

12.3.2. 802.1X 활성화 및 비활성화 212
12.3.3. 802.1X 포트 상태 설정 212
12.3.4. 재인증(Recertification) 메커니즘 설정 213
12.3.5. 포트 최대 접속 호스트 수 설정 214
12.3.6. 재전송 간격 및 재전송 횟수 설정 214
12.3.7. 포트를 전송 포트(Transmit Port)로 설정 215
12.3.8. 802.1X 클라이언트 버전 설정 215
12.3.9. 802.1X 클라이언트 버전 검사 설정 216
12.3.10. 인증 방식 설정 216
12.3.11. 클라이언트 타이밍 패킷 검사 설정 216
12.3.12. 802.1X 정보 확인 217
12.4. RADIUS 설정 217
12.4.1. RADIUS 기본 설정 217
12.4.2. 인증 서버 IP 주소 설정 218
12.4.3. Shared Secret 설정 218
12.4.4. 과금(Accounting) 활성화 및 비활성화 218
12.4.5. RADIUS 포트 및 속성(Attribute) 설정 219
12.4.6. RADIUS 로밍 설정 219
12.4.7. RADIUS 정보 확인 220
12.5. 설정 예제 (번역) 220
12.6. TACACS+ 소개 221
13. GMRP 설정 222
13.1. GMRP 소개 222
13.2. GMRP 설정 223
13.2.1. GMRP 활성화 설정 223

13.2.2. GMRP 정보 확인 224
13.3. GMRP 대표 설정 예제 224
14. IGMP SNOOPING 설정 225
14.1. IGMP Snooping 소개 226
14.1.1. IGMP Snooping 동작 과정 226
14.1.2. Layer 2 동적 멀티캐스트 227
14.1.3. 그룹 가입 (Join a Group) 227
14.1.4. 그룹 탈퇴 (Leave a Group) 229
14.1.5. IGMP Querier 230
14.1.6. IGMP Snooping 멀티캐스트 필터링 231
14.2. IGMP Snooping 설정 231
14.2.1. IGMP Snooping 기본 설정 231
14.2.2. IGMP Snooping 활성화 및 비활성화 231
14.2.3. 멀티캐스트 그룹 유지 시간(Lifetime) 설정 232
14.2.4. Fast-Leave 설정 233
14.2.5. MROUTER 설정 (정적 멀티캐스트 라우터 포트) 233
14.2.6. IGMP Snooping Query 포트 설정 (정적 Query/Mrouter 포트) 234
14.2.7. IGMP Snooping Query 기능 설정 234
14.2.8. IGMP Snooping 멀티캐스트 필터링 설정 234
14.2.9. IGMP Snooping 정보 확인 234
14.3. IGMP Snooping 예제 235
14.3.1. 설정 예제 235
15. MVR 설정 237
15.1. MVR 소개 238
15.2. MVR 설정 238

15.3. MVR 설정 예제 239
16. DHCP Snooping 설정 240
16.1. DHCP Snooping 소개 241
16.1.1. DHCP Snooping 처리 과정 241
16.1.2. DHCP Snooping 바인딩 테이블 241
16.1.3. DHCP Snooping 서버 연결 포트 지정 243
16.2. DHCP Snooping 설정 243
16.2.1. 기본 설정 243
16.2.2. DHCP Snooping 글로벌 활성화 및 비활성화 243
16.2.3. 인터페이스 DHCP Snooping 활성화 및 비활성화 244
16.2.4. 인터페이스 DHCP Snooping Option82 설정 244
16.2.5. DHCP Snooping 정보 확인 245
16.3. DHCP Snooping 설정 예제 245
16.4. DHCP Snooping 설정 문제 해결 247
17. DHCP Client 설정 247
17.1. DHCP Client 소개 248
17.2. DHCP Client 설정 248
18. DHCP Relay 설정 248
18.1. DHCP Relay 소개 249
18.2. DHCP Relay 설정 250
18.2.1. 인터페이스 DHCP Relay 기능 활성화 250
18.2.2. DHCP Relay 정보 확인 250
18.3. DHCP Relay 설정 예제 251
19. DHCP Server 설정 252
19.1. DHCP Server 소개 253

19.2. DHCP Server 설정 254
19.2.1. 글로벌 DHCP Server 기능 활성화 254
19.2.2. 인터페이스 DHCP Server 메시지 수신 설정 254
19.2.3. 주소 풀(Address Pool) 설정 255
19.2.4. 주소 풀 범위 설정 255
19.2.5. 주소 풀 서브넷 마스크 설정 256
19.2.6. 주소 풀 Lease(임대 기간) 설정 256
19.2.7. 주소 풀 기본 게이트웨이 설정 256
19.2.8. 주소 풀 DNS 서버 설정 257
19.2.9. 주소 풀 수동 제외 주소 설정 257
19.2.10. Option82 설정 258
19.2.11. 할당된 주소 테이블 엔트리 삭제 258
19.2.12. 충돌 감지 주소 엔트리 삭제 258
19.3. DHCP Server 설정 예제 259
20. ACL 설정 261
20.1. ACL 리소스 라이브러리 소개 262
20.2. ACL 필터링 소개 264
20.3. ACL 리소스 풀 설정 266
20.4. Time-based ACL (시간 기반 ACL) 269
20.5. ACL 필터링 설정 271
20.6. ACL 설정 예제 272
20.7. ACL 설정 문제 해결 274
21. 기본 TCP/IP 설정 274
21.1. VLAN 인터페이스 설정 275
21.2. ARP 설정 276

21.2.1. 정적 ARP 설정 277
21.2.2. ARP 정보 확인 278
21.3. 정적 라우팅 설정 278
21.4. TCP/IP 기본 설정 예제 280
21.4.1. 3 계층 인터페이스 설정 280
21.4.2. 정적 라우트 설정 281
21.4.3. ARP 설정 281
22. SNMP 설정 282
22.1. SNMP 소개 283
22.2. SNMP 설정 284
22.3. SNMP 설정 예제 285
22.3.1. 설정 286
23. RMON 설정 286
23.1. RMON 소개 286
23.2. RMON 설정 287
23.3. RMON 설정 예제 288
24. 클러스터 설정 290
24.1. 클러스터 관리 소개 290
24.1.1. 클러스터 정의 291
24.1.2. Cluster Role 291
24.1.3. NDP 소개 292
24.1.4. NTDP 소개 293
24.1.5. 클러스터 관리 및 유지보수 293
24.1.6. Management VLAN 296
24.2. 클러스터 설정 소개 296

24.3. 관리 장비 설정 297
24.3.1. 시스템 및 포트의 NDP 기능 활성화 297
24.3.2. NDP 파라미터 설정 298
24.3.3. 시스템 및 인터페이스의 NTDP 기능 활성화 298
24.3.4. NTDP 파라미터 설정 299
24.3.5. NTDP 정보 수동 수집 설정 299
24.3.6. 클러스터 기능 활성화 299
24.3.7. 클러스터 생성 300
24.3.8. 클러스터 내부 Member 상호작용 설정 302
24.3.9. 클러스터 멤버 관리 설정 302
24.4. Member 장비 설정 303
24.4.1. 시스템 및 포트의 NDP 기능 활성화 303
24.4.2. 시스템 및 포트의 NTDP 기능 활성화 303
24.4.3. NTDP 정보 수동 수집 설정 303
24.4.4. 클러스터 기능 활성화 303
24.5. 클러스터 멤버 접근 설정 303
24.6. 클러스터 관리 조회 및 유지보수 304
24.7. 클러스터 관리 설정 예제 305
25. SNTP 설정 307
25.1. SNTP 소개 307
25.2. SNTP 설정 308
25.2.1. 기본 SNTP 설정 308
25.2.2. SNTP 서버 주소 설정 309
25.2.3. SNTP 동기화 주기 설정 309
25.2.4. 로컬 타임존 설정 310

25.3. SNTP 정보 조회 310
26. System Log 구성 311
26.1. System Log 소개 311
26.1.1. 로그 정보 형식 312
26.1.2. 로그 저장 313
26.1.3. 로그 표시 314
26.1.4. 디버깅 도구 315
26.2. Syslog 구성 315
26.2.1. 터미널 실시간 로그 출력 설정 315
26.2.2. 로그 레벨 설정 316
26.2.3. 로그 정보 확인 316
26.2.4. 디버깅 스위치 설정 316
26.2.5. 디버깅 정보 확인 317
26.3. SYSLOG 구성 318
26.3.1. SYSLOG 소개 318
26.3.2. SYSLOG 구성 319
26.3.3. SYSLOG 구성 예제 319
27. IPv6 기본 구성 320
27.1. IPv6 소개 321
27.1.1. IPv6 프로토콜 특징 321
27.1.2. IPv6 주소 소개 322
27.1.3. IPv6 Neighbor Discovery Protocol 개요 325
27.1.4. IPv6 PMTU Discovery 328
27.1.5. 프로토콜 규격 (Protocol Specification) 328
27.2. IPv6 기본 구성 작업 개요 329

27.3. IPv6 기본 기능 구성 329
27.3.1. IPv6 유니캐스트 주소 구성 329
27.4. IPv6 Neighbor Discovery Protocol 구성 329
27.4.1. RA 메시지 관련 파라미터 구성 330
27.4.2. 중복 주소 검출 시 Neighbor Solicitation 메시지 전송 횟수 설정 332
27.5. IPv6 정적 라우트 설정 333
27.6. IPv6 표시 및 유지보수 333
28. MLD SNOOPING 설정 334
28.1. MLD SNOOPING 개요 335
28.1.1. MLD SNOOPING 동작 과정 335
28.1.2. Layer 2 동적 멀티캐스트 336
28.1.3. 그룹 가입 (Join a group) 337
28.1.4. 그룹 탈퇴 (Leave a group) 338
28.2. MLD SNOOPING 설정 339
28.2.1. MLD SNOOPING 기본 설정 339
28.2.2. MLD SNOOPING 활성화 및 비활성화 340
28.2.3. Lifetime 설정 340
28.2.4. Fast-leave 설정 341
28.2.5. MROUTER 설정 341
28.2.6. VLAN Querier 기능 설정 342
28.2.7. 정보 확인 (Display Information) 342
28.3. MLD SNOOPING 설정 예제 343
29. PoE 설정 345
29.1. PoE 개요 345
29.2. PoE 설정 346

29.2.1. 수동 PoE 설정 346
29.2.2. PoE 정책 설정 347
29.2.3. PD 조회 설정 347
30. GVRP 설정 349
30.1. GVRP 개요 349
30.2. GVRP 설정 349
30.2.1. GVRP 설정 활성화 350
30.2.2. GVRP 정보 확인 350

이 장에서는 CLI(Command Line Interface) 명령줄 인터페이스에 대해 상세히 설명하며, 주요 내용은 다음과 같습니다.

- 스위치 CLI 접근 방법
- CLI 모드 소개
- 명령어 구문 소개
- 명령줄 단축키
- 히스토리 명령어

1.1. 스위치 CLI 접근 방법

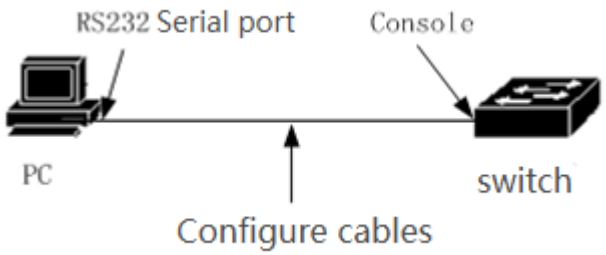
스위치의 CLI(Command Line Interface) 명령줄 인터페이스는 사용자가 스위치를 관리할 수 있도록 인터페이스를 제공합니다.

사용자는 Console 포트 또는 Telnet 터미널을 통해 스위치의 CLI 명령줄 인터페이스에 접근할 수 있으며, 이에 대한 내용은 아래에서 설명합니다.

1.1.1. Console 포트를 통한 CLI 접근

동작 절차는 다음과 같습니다.

Step 1:
PC의 시리얼 포트를 설정 케이블을 이용하여 스위치의 Console 포트에 연결합니다. (아래 그림 참조)



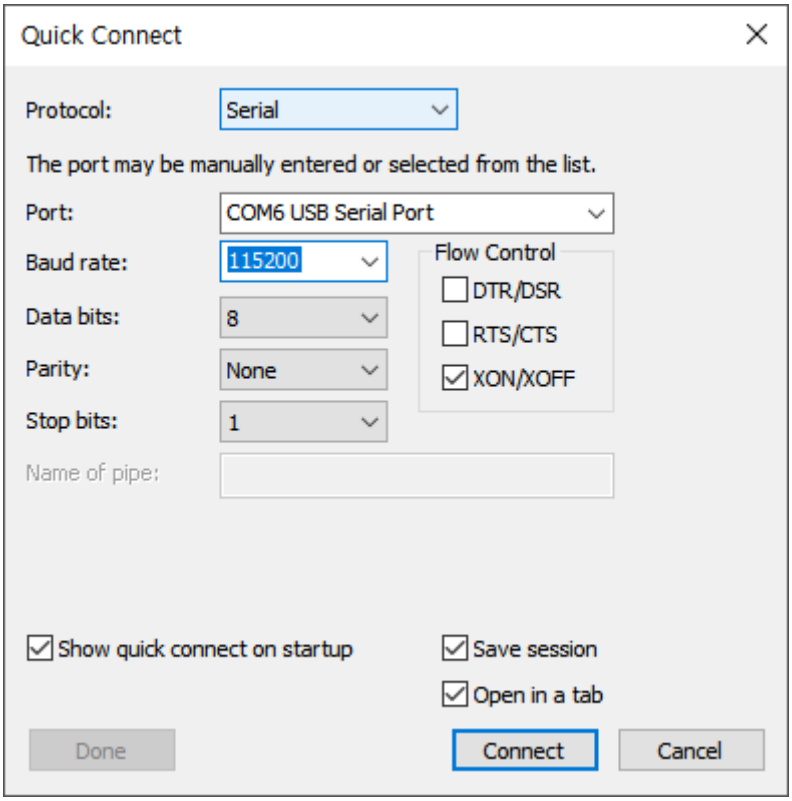
Step 2:
PC에서 터미널 에뮬레이션 프로그램(예: Windows의 HyperTerminal)을 실행한 후, 통신 파라미터를 설정합니다.

터미널의 통신 파라미터는 다음과 같이 설정합니다.

- Baud rate: 115200
- Data bits: 8

- Parity: None
- Stop bit: 1
- Data flow control: none

HyperTerminal의 통신 파라미터 설정 화면은 아래 그림과 같습니다.



스위치를 부팅합니다. 스위치가 정상적으로 기동되면 터미널 화면에 CLI 프롬프트(기본값: Switch >)가 표시됩니다.

사용자는 해당 프롬프트에서 명령어를 입력하여 스위치의 CLI에 접근할 수 있습니다.

1.1.2. TELNET을 통한 CLI 접근

사용자는 스위치의 포트를 통해 CLI에 접근할 수 있습니다.

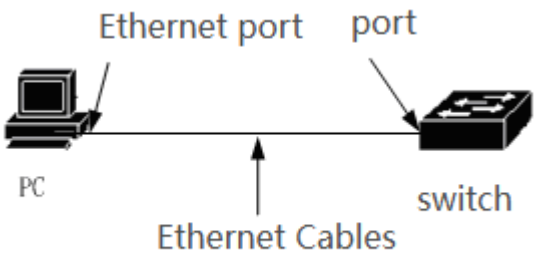
스위치 포트의 기본 IP 주소는 192.168.0.1입니다.

(참고: 실제 장비에 따라 다를 수 있음)

포트를 통해 스위치에 접근하는 절차는 다음과 같습니다.

Step 1:

Ethernet 케이블을 사용하여 PC의 Ethernet 포트를 스위치의 포트에 연결합니다. (아래 그림 참조)



Step 2:

PC의 Ethernet 포트에 IP 주소를 설정합니다.

IP 주소는 192.168.200.0/24 대역이어야 하며, 예를 들어 192.168.200.100과 같이 설정할 수 있습니다.

PC에서 192.168.200.254로 ping을 수행하여 스위치와의 연결 상태를 확인합니다.

Step 3:

PC와 스위치 간 연결이 정상일 경우,

telnet 192.168.200.254 명령을 입력하여 Telnet 터미널에 접속합니다. (아래 그림 참조)



Step 4:

시스템에 비밀번호가 설정되어 있지 않은 경우, Telnet 접속 시 바로 CLI로 진입하며 CLI 프롬프트(기본값: Switch >)가 표시됩니다.

비밀번호가 설정되어 있는 경우, Telnet 화면에서 비밀번호를 입력해야 CLI에 접근할 수 있습니다.

※ 주의사항

- 스위치 포트의 IP 주소는 VLAN의 3계층 인터페이스에 설정됩니다.

따라서 스위치에 접근하기 전에 VLAN 인터페이스에 IP 주소가 설정되어 있어야 합니다.

기본적으로 VLAN1의 IP 주소는 192.168.200.254이며
(참고: 실제 장비에 따라 다를 수 있음)
이를 그대로 사용할 수 있습니다.
VLAN 인터페이스의 IP 주소는 Console 포트를 통해 설정할 수 있습니다.

- 사용자는 스위치 포트를 통해 접근할 때 PC와 포트를 Ethernet 케이블로 직접 연결하거나, 네트워크를 통해 연결할 수 있습니다.
  단, PC와 스위치의 VLAN 간에 통신이 가능해야 합니다.

1.2. CLI 모드 소개

1.2.1. CLI 모드의 기능

CLI 모드는 다음과 같은 두 가지 주요 기능을 제공합니다.

- 사용자를 구분하여 비인가 사용자가 CLI를 불법적으로 사용하는 것을 방지할 수 있습니다.
  사용자는 다음 두 가지 수준으로 구분됩니다.
  a. 일반 사용자(normal user)
     스위치의 일부 동작 상태만 조회할 수 있으며, display 명령만 사용할 수 있습니다.
  b. 관리자 사용자(privileged user)
     스위치의 동작 상태 조회뿐만 아니라, 설정 및 유지보수 작업을 수행할 수 있으며 스위치의 동작을 변경할 수 있습니다.
- 스위치 설정의 효율성 향상
  스위치는 다양한 설정 기능을 가지고 있습니다. 모든 설정을 하나의 모드에 포함할 경우 사용이 매우 불편해집니다.
  이를 해결하기 위해 CLI에서는 여러 개의 모드를 구성하고, 유사한 명령어들을 동일한 모드에 배치합니다. 이를 통해 사용자가 보다 쉽게 이해하고 사용할 수 있도록 합니다.
  예를 들어, VLAN 관련 명령어는 VLAN configuration mode에, 인터페이스 관련 명령어는 interface configuration mode에 배치됩니다.

1.2.2. CLI 모드 식별

CLI 프롬프트는 현재 CLI 모드를 식별하는 기준입니다.

사용자는 CLI를 사용할 때 프롬프트를 확인함으로써 현재 어떤 CLI 모드에 있는지 알 수 있습니다.

CLI 프롬프트는 두 가지 요소로 구성됩니다.

하나는 호스트를 식별하는 부분이며, 다른 하나는 모드를 식별하는 부분입니다.

CLI 프롬프트에서 호스트 부분은 시스템의 호스트 이름을 사용합니다.

호스트 이름은 사용자가 변경할 수 있으며, 기본값은 Switch입니다.

따라서 CLI 프롬프트는 기본적으로 Switch로 시작하며, 이후 설명에서도 기본 호스트 이름을 기준으로 사용합니다.

CLI 프롬프트에서 모드 부분은 사용자가 변경할 수 없습니다.

각 모드는 고유한 모드 문자열을 가지며, 일부는 고정되어 있고 일부는 가변적입니다.

예를 들어, VLAN configuration mode의 모드 문자열은 고정되어 있지만, interface configuration mode의 모드 문자열은 인터페이스에 따라 달라집니다.

예시:

CLI 프롬프트 Switch#

→ privileged mode를 의미하며, Switch는 호스트, #는 모드를 나타냅니다.

CLI 프롬프트 Switch(config-ge1/1)#

→ interface configuration mode를 의미하며, ge1/1 포트가 설정된 상태입니다.

Switch는 호스트, (config-ge1/1)#는 모드를 나타냅니다.

CLI 프롬프트 Switch(config-vlan2)#

→ VLAN configuration mode를 의미하며, vlan2 인터페이스가 설정된 상태입니다.

Switch는 호스트, (config-vlan2)#는 모드를 나타냅니다.

1.2.3. CLI 모드 분류

CLI 모드는 다음과 같이 네 가지로 구분됩니다.

- normal mode
- privileged mode
- global configuration mode
- configuration submode

configuration submode는 여러 개의 CLI 모드로 구성됩니다.

일반 사용자(normal user)는 normal mode에만 접근할 수 있으며, privileged user는 모든 CLI 모드에 접근할 수 있습니다.

Console 및 Telnet 터미널은 처음에 normal mode로 진입합니다.

normal mode에서 enable 명령을 입력하고 비밀번호 인증에 성공하면 privileged mode로 진입합니다.

Telnet 터미널에서는 일반 사용자는 normal mode에만 머무를 수 있으며 privileged mode로 진입할 수 없습니다.

privileged mode에서 configure terminal 명령을 입력하면 global configuration mode로 진입합니다.

각 configuration submode는 global configuration mode에서 해당 명령을 입력하여 진입할 수 있습니다.

아래 표는 스위치에서 사용되는 주요 CLI 모드를 보여줍니다.

모드 / 프롬프트	설명
Normal Mode Switch>	설명: 스위치의 상태 정보를 확인하기 위한 display 명령을 제공합니다. 진입방법: 터미널 접속 시 처음 진입하는 기본 모드입니다. 종료방법: Console 터미널에서는 별도의 종료 명령이 없습니다. Telnet 터미널에서는 exit 또는 quit 명령으로 Telnet 접속을 종료합니다.
Privileged Mode Switch#	설명: 스위치 상태 확인용 display 명령 외에도 debugging, version upgrade, configuration maintenance 관련 명령을 제공합니다. 진입방법: Normal Mode에서 enable 명령을 입력합니다. 종료방법: disable 명령으로 Normal Mode로 돌아갑니다. Console 터미널에서는 exit 또는 quit 명령으로 Normal Mode로 이동하며, Telnet 터미널에서는 exit 또는 quit 명령으로 Telnet 접속을 종료합니다.
Global Configuration Mode Switch(config)#	설명: configuration submode에서 처리할 수 없는 공통 설정 명령을 제공합니다. 예: static route 설정 명령 진입방법: Privileged Mode에서 configure terminal 명령을 입력합니다. 종료방법: exit, quit, 또는 end 명령으로 Privileged Mode로 돌아갑니다.
Interface Configuration Mode Port: Switch(config-ge1/1)# VLAN Interface: Switch(config-vlan1)#	설명: 포트 및 VLAN 인터페이스 설정을 위한 명령을 제공합니다. 진입방법: Global Configuration Mode에서 interface <if-name> 명령을 입력합니다. 종료방법: exit 또는 quit 명령으로 Global Configuration Mode로 돌아갑니다. end 명령을 사용하면 Privileged Mode로 돌아갑니다.
VLAN Configuration Mode Switch(config-vlan)#	설명: VLAN 생성 및 삭제 등 VLAN 관련 설정 명령을 제공합니다. 진입방법: Global Configuration Mode에서 VLAN database 명령을 입력합니다. 종료방법: exit 또는 quit 명령으로 Global Configuration Mode로 돌아갑니다.

	end 명령을 사용하면 Privileged Mode로 돌아갑니다.
MSTP Configuration Mode Switch(config-mst)#	설명: MSTP 설정 명령을 제공합니다. 예: MSTP instance 생성 및 삭제 진입방법: Global Configuration Mode에서 spanning-tree mst configuration 명령을 입력합니다. 종료방법: exit 또는 quit 명령으로 Global Configuration Mode로 돌아갑니다. end 명령을 사용하면 Privileged Mode로 돌아갑니다.
Terminal Configuration Mode Switch(config-line)#	설명: Console 및 Telnet 터미널 설정 명령을 제공합니다. 예: 터미널 timeout 설정 진입방법: Global Configuration Mode에서 line vty 명령을 입력합니다. 종료방법: exit 또는 quit 명령으로 Global Configuration Mode로 돌아갑니다. end 명령을 사용하면 Privileged Mode로 돌아갑니다.

1.3. 명령어 구문 소개

1.3.1. 명령어 구성

CLI 명령어는 keyword와 parameter 두 부분으로 구성됩니다.

첫 번째 단어는 반드시 keyword여야 하며, 그 뒤에 오는 단어는 keyword 또는 parameter가 될 수 있습니다. keyword와 parameter는 번갈아 나타날 수 있습니다. 명령어에는 반드시 keyword가 포함되어야 하지만, parameter는 없어도 됩니다.

예를 들면 다음과 같습니다.

- Write
  → keyword 1개, parameter 없음
- show version
  → keyword 2개, parameter 없음
- VLAN <vlan-id>
  → keyword 1개, parameter 1개
- instance <instance-id> VLAN <vlan-id>
  → keyword 2개, parameter 2개
  → keyword와 parameter가 번갈아 구성됨

1.3.2. 파라미터 유형

CLI 명령어의 파라미터는 필수(required)와 선택(optional) 두 가지 유형으로 구분됩니다.

필수 파라미터는 명령어 입력 시 반드시 입력해야 하며, 선택 파라미터는 입력하지 않아도 됩니다.

예를 들면 다음과 같습니다.

- VLAN <vlan-id>
  → <vlan-id>는 필수 파라미터로, 반드시 입력해야 합니다.
- show interface [if-name]
  → [if-name]는 선택 파라미터로, 입력하지 않아도 명령어를 실행할 수 있습니다.

1.3.3. 명령어 구문 규칙

명령어를 텍스트로 표현할 때는 다음 규칙을 따라야 합니다.

1) Keyword 표현

Keyword는 그대로 단어로 표현합니다.

예:
show version

2) 필수 파라미터 표현

필수 파라미터는 < >로 감쌉니다.

예:
VLAN <vlan-id>

3) 선택 파라미터 표현

선택 파라미터는 [ ]로 감쌉니다.

예:
show VLAN [vlan-id]

이 경우 < >는 생략하고 대문자 형태로 표기할 수 있습니다.

예:
show VLAN VLAN-ID

※ 필수 파라미터에는 [ ]를 사용할 수 없습니다.

4) 여러 항목 중 하나 선택 (필수 선택)

여러 keyword 또는 parameter 중 하나를 반드시 선택해야 하는 경우 { }를 사용하며, 항목은 |로 구분합니다. (| 앞뒤 공백 필요)

예:
spanning-tree mst link-type {point-to-point | shared}
→ 반드시 point-to-point 또는 shared 중 하나 선택

또 다른 예:
no arp {<ip-address> | <ip-prefix>}

5) 여러 항목 중 선택 (선택 입력)

여러 keyword 또는 parameter 중 선택적으로 입력할 수 있는 경우 [ ]를 사용하며, 항목은 |로 구분합니다.

예:
debug ip tcp [recv | send]
→ recv, send 모두 생략 가능

또 다른 예:
show ip route [<ip-address> | <ip-prefix>]
show interface [<if-name> | switchport]

6) **반복 입력 가능 항목**

반복 입력이 가능한 keyword 또는 parameter(또는 그룹) 뒤에는 *를 붙입니다.

예:
ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]*

- -j <count> <ip-address>*
- -k <count> <ip-address>*

→ 여러 개의 IP 주소를 반복 입력 가능

전체 옵션 그룹도 반복 입력할 수 있습니다.

7) 파라미터 표기 규칙

파라미터는 하나 이상의 단어로 구성될 수 있으며, 여러 단어일 경우 -로 구분합니다.
각 단어는 소문자로 작성합니다.

올바른 예:
<vlan-id>, <if-name>, <router-id>, <count>

잘못된 예:

<1-255>, <A.B.C.D>, <WORD>, <IFNAME>

1.3.4. 명령어 축약

사용자가 CLI 인터페이스에서 명령어를 입력할 때, 명령어의 keyword는 축약하여 입력할 수 있습니다.

CLI는 명령어의 prefix matching 기능을 지원합니다.

입력한 단어가 특정 keyword의 접두어와 유일하게 일치하는 경우, CLI는 해당 입력값을 일치하는 keyword로 해석합니다.

이 기능은 사용자가 CLI를 사용할 때 매우 편리하며, 적은 수의 문자만 입력해도 명령어를 실행할 수 있습니다.

예를 들어, show version 명령어는 다음과 같이 축약하여 입력할 수 있습니다.

sh ver

1.3.5. 구문 도움말 (Syntax Help)

CLI 명령줄 인터페이스에는 각 단계별 명령어와 파라미터에 대한 도움 기능이 제공되며, 사용 방법은 다음과 같습니다.

1) CLI 모드에서 ?를 직접 입력하면, 해당 모드에서 사용할 수 있는 모든 명령어의 첫 번째 keyword와 설명이 터미널에 표시됩니다.

   예:
   Switch(config)?

2) 명령어의 일부를 입력한 후 공백을 입력하고 ?를 입력하면, 다음 단계에서 사용할 수 있는 모든 keyword 또는 파라미터와 그 설명이 표시됩니다.

   예:
   Switch# show ?

3) 완성되지 않은 keyword를 입력한 상태에서 ?를 입력하면, 해당 입력값과 일치하는 모든 keyword와 그 설명이 표시됩니다.

   예:
   Switch# show ver?

4) 명령어의 일부를 입력한 후 공백을 입력하고 Tab 키를 누르면, 다음 단계에서 사용할 수 있는 keyword 목록이 표시됩니다.

※ 다음 단계가 파라미터인 경우에는 표시되지 않습니다.

5) 완성되지 않은 keyword를 입력한 상태에서 Tab 키를 누르면 다음과 같이 동작합니다.
   - 일치하는 keyword가 하나인 경우 → 자동 완성됨
   - 일치하는 keyword가 여러 개인 경우 → 가능한 모든 keyword 목록이 표시됨

1.3.6. 명령줄 오류 메시지

사용자가 입력한 명령어가 구문 검사를 통과하지 못할 경우, 터미널에 오류 메시지가 표시됩니다.

일반적으로 발생하는 오류 메시지는 다음 표와 같습니다.

오류 메시지	원인
Invalid input 또는 Unrecognized command	- 일치하는 keyword가 없음 - 파라미터 입력 오류 - keyword 또는 파라미터를 과도하게 입력한 경우
Incomplete command	- 명령어 입력이 완료되지 않음 - 필요한 keyword 또는 파라미터가 누락됨
Ambiguous command	- keyword 입력이 불완전함 - 입력한 prefix에 대해 여러 개의 keyword가 일치함

1.4. 명령줄 단축키

1.4.1. 라인 편집 단축키

CLI 명령줄 인터페이스는 라인 편집 단축키 기능을 지원하며, 이를 통해 CLI 명령어의 입력 및 편집을 보다 편리하게 수행할 수 있습니다.

사용자는 명령어를 입력하거나 수정할 때 라인 편집 단축키를 활용하여 입력 속도를 향상시킬 수 있습니다.

아래 표는 지원되는 라인 편집 단축키와 각 기능을 나타냅니다.

단축키	기능
Ctrl + p 또는 ↑	이전 명령어
Ctrl + n 또는 ↓	다음 명령어

Ctrl + u	현재 라인 전체 삭제
Ctrl + a	커서를 라인의 시작으로 이동
Ctrl + f 또는 →	커서를 오른쪽으로 한 칸 이동
Ctrl + b 또는 ←	커서를 왼쪽으로 한 칸 이동
Ctrl + d	현재 커서 위치의 문자 삭제
Ctrl + h	커서 앞의 문자 삭제
Ctrl + k	커서 위치부터 오른쪽(이후)의 모든 문자 삭제
Ctrl + w	커서 위치 이전의 모든 문자 삭제
Ctrl + e	커서를 라인의 끝으로 이동
Ctrl + c	명령어를 실행하지 않고 중단 → global configuration mode 또는 submode에서는 privileged mode로 이동 → normal/privileged mode에서는 현재 모드는 유지되며 새 줄로 이동
Ctrl + z	Ctrl + C와 동일
Tab	미완성 keyword 입력 후 사용 → 하나만 일치하면 자동 완성 → 여러 개 일치하면 목록 출력 → 일치하는 keyword가 없으면 동작하지 않음

1.4.2. Show 명령어 단축키

show keyword로 시작하는 명령어는 모두 조회(display) 명령입니다.

일부 조회 명령은 출력되는 내용이 많아 한 화면에 모두 표시되지 않을 수 있습니다. 이를 위해 터미널은 화면을 나누어 출력하는(split-screen display) 기능을 제공합니다. 한 화면의 출력이 완료되면, 터미널은 다음 동작을 위해 사용자 입력을 대기합니다.

아래 표는 display 명령어 실행 시 사용할 수 있는 단축키와 그 기능을 나타냅니다.

단축키	기능
Space	다음 화면 표시
Enter	다음 줄 표시
Ctrl + c	명령어 실행을 중단하고 CLI 모드로 복귀
기타 키	Ctrl + C와 동일하게 동작

1.5. 히스토리 명령어

CLI 명령줄 인터페이스는 명령어 히스토리 기능을 지원합니다.

이 기능은 사용자가 최근에 입력한 최대 20개의 명령어를 기억하며, 이전에 입력한 명령어를 다시 사용할 수 있도록 합니다.

show history 명령을 사용하면 지금까지 입력한 명령어 목록을 확인할 수 있습니다.

또한 Ctrl + p, Ctrl + n, 또는 ↑, ↓ 키를 사용하여 이전에 입력한 명령어를 선택할 수 있습니다.

히스토리 기능을 통해 사용자는 명령어 입력을 보다 효율적으로 수행할 수 있습니다.

2. 시스템 관리 설정

스위치의 다양한 기능 설정을 수행하기 전에, 사용자는 먼저 시스템 관리 및 유지보수에 대한 기본 설정을 숙지해야 합니다.

이 장에서는 시스템 관리 및 유지보수에 대한 기본 설정을 설명하며, 주요 내용은 다음과 같습니다.

- 시스템 보안 설정
- 시스템 유지보수 및 점검
- 시스템 모니터링
- 프로파일 관리
- 소프트웨어 버전 업그레이드

2.1. 시스템 보안 설정

불법 사용자의 스위치 접근을 방지하기 위해, 시스템은 시스템 관리를 위한 다양한 보안 기능을 제공합니다.

주요 보안 기능은 다음과 같습니다.

- 다중 사용자 관리 제어
- Enable 비밀번호 제어
- TELNET 서비스 제어
- SNMP 서비스 제어
- HTTP 서비스 제어

2.1.1. 다중 사용자 관리 제어

다중 사용자 관리 기능은 스위치 시스템의 보안을 강화할 뿐만 아니라, 여러 사용자가 동시에 스위치를 관리하고 유지보수할 수 있도록 합니다.

이 기능은 각 사용자에게 사용자 이름, 비밀번호 및 권한을 부여함으로써 시스템 보안을 유지합니다.

사용자는 스위치에 접근할 때 먼저 사용자 이름과 비밀번호를 인증해야 하며, 입력한 정보가 정확하게 일치해야만 인증이 완료됩니다.

인증에 성공한 후 스위치에 접근할 수 있지만, 사용자의 권한에 따라 접근 가능한 범위가 제한됩니다.

다중 사용자 관리는 사용자의 권한을 다음 두 가지 수준으로 구분합니다.

일반 사용자 (ordinary user)

CLI의 normal mode에만 접근할 수 있으며, display 명령을 통해 스위치 정보를 조회만 할 수 있습니다.

관리자 사용자 (privileged user)

CLI의 모든 모드에 접근할 수 있으며, 모든 명령어를 사용하여 스위치 정보를 조회하고 설정 및 유지보수 작업을 수행할 수 있습니다.

다중 사용자 관리 기능은 Telnet 터미널에만 적용되며, Console 터미널에는 적용되지 않습니다.

Console 터미널을 통해 스위치에 접근할 경우 사용자 이름과 비밀번호 인증이 필요 없으며, CLI에 바로 접근할 수 있습니다.

반면, Telnet 터미널을 통해 접근할 경우 사용자 이름과 비밀번호 인증을 반드시 수행해야 하며, 인증이 완료되어야 CLI에 접근할 수 있습니다.

스위치의 기본 사용자 이름과 비밀번호는 admin입니다.

admin 계정은 반드시 관리자(privileged user) 권한을 가지며, 일반 사용자로 변경할 수 없습니다. 또한 admin 계정은 삭제할 수 없습니다.

다중 사용자 관리와 관련된 명령어는 다음 표에 설명되어 있습니다.

명령어	설명	CLI 모드
username <user-name> password <key> {normal | privilege}	사용자 추가 명령어 이미 존재하는 사용자일 경우, 비밀번호 및 권한을 수정합니다. - <user-name>: 사용자 이름 - <key>: 비밀번호 - normal: 일반 사용자 권한 - privilege: 관리자 권한	Global Configuration Mode
no username [user-name]	지정한 사용자 이름의 계정을 삭제합니다.	Global Configuration Mode
show running-config	현재 시스템 설정을 확인하여 다중 사용자 설정 내용을 조회합니다.	Privileged Mode

2.1.2. Enable 비밀번호 제어

Enable 비밀번호는 스위치에서 normal mode에서 privileged mode로 전환을 제어하기 위해 사용됩니다.

Enable 비밀번호가 인증되기 전에는 사용자는 스위치의 정보 조회만 가능하며, 인증이 완료된 후에는 스위치의 설정 및 유지보수 작업을 수행할 수 있습니다.

Enable 비밀번호는 특정 사용자 계정에 종속되지 않습니다.

즉, Console 또는 Telnet 터미널로 로그인한 모든 사용자는 privileged mode로 진입하기 위해 반드시 Enable 비밀번호를 입력해야 합니다.

비밀번호 인증에 실패할 경우, 사용자는 normal mode에만 머무르게 됩니다.

normal mode에서 enable 명령을 입력하면, 터미널은 사용자에게 비밀번호 입력을 요청합니다.

이때 Enable 비밀번호를 입력하여 인증에 성공하면 privileged mode로 전환되며, 인증에 실패하면 normal mode 상태를 유지합니다.

단, 일반 사용자(ordinary user)의 경우 비밀번호 인증 성공 여부와 관계없이 privileged mode로 진입할 수 없습니다.

Enable 비밀번호의 기본값은 설정되어 있지 않은 상태(공백)입니다.

이 경우 normal mode에서 enable 명령을 입력하면 비밀번호 입력 없이 바로 privileged mode로 진입합니다.

Enable 비밀번호와 관련된 명령어는 다음 표에 설명되어 있습니다.

명령어	설명	CLI 모드
enable password <key>	시스템의 Enable 비밀번호를 설정합니다.	Global Configuration Mode
no enable password	시스템의 Enable 비밀번호를 삭제합니다. Enable 비밀번호는 공백 상태가 됩니다.	Global Configuration Mode
show running-config	현재 시스템 설정을 확인하여 Enable 비밀번호 설정 내용을 조회합니다.	Privileged Mode
enable	시스템의 Enable 비밀번호를 인증하기 위한 대화형 명령어입니다. 인증에 성공하면 터미널은 privileged mode로 진입합니다.	Normal Mode

※ 참고:

시스템 보안을 위해 관리자는 반드시 Enable 비밀번호를 설정해야 합니다.

2.1.3. TELNET 서비스 제어

일부 환경에서는 관리자가 스위치를 원격으로 관리할 필요 없이, Console 터미널을 통해 로컬에서만 관리하는 경우가 있습니다.

이 경우 시스템 보안을 강화하고, 비인가 사용자의 Telnet을 통한 원격 접속을 방지하기 위해 관리자는 Telnet 서비스를 비활성화할 수 있습니다.

Telnet 서비스는 기본적으로 활성화되어 있습니다.

명령어	**설명**	**CLI 모드**
security-manage telnet enable	Telnet 서비스를 활성화합니다.	Global Configuration Mode

명령어	설명	CLI 모드
security-manage telnet disable	Telnet 서비스를 비활성화합니다.	Global Configuration Mode
security-manage telnet number <1-100>	Telnet 접속 세션 수를 설정합니다.설정 범위: 1 ~ 100, 기본값: 5	Global Configuration Mode
security-manage telnet access-group <1-99>*(참고: 실제 장비 기준)*	ACL 그룹을 지정하여 접속 가능한 Source IP를 제한합니다.지정한 ACL이 존재하지 않거나 표준 ACL이 아닌 경우, Source IP 제어는 적용되지 않습니다.	Global Configuration Mode
no security-manage telnet access-group	Source IP 주소 기반 접근 제어를 해제합니다.	Global Configuration Mode
show security-manage	서비스 제어 설정 상태를 확인합니다.	Privileged Mode

2.1.4. SNMP 서비스 제어

SNMP 서비스 제어 기능은 SNMP 서비스를 활성화/비활성화할 수 있으며, ACL을 통해 스위치에 접근할 수 있는 IP 주소를 제어할 수 있습니다.

명령어	설명	CLI 모드
security-manage snmp enable	SNMP 서비스를 활성화합니다.	Global Configuration Mode
security-manage snmp disable	SNMP 서비스를 비활성화합니다.	Global Configuration Mode
security-manage snmp access-group <1-99>*(참고: 실제 장비 기준)*	ACL 그룹을 지정하여 Source IP 주소 기반 접근 제어를 활성화합니다. 지정한 ACL이 존재하지 않거나 표준 ACL이 아닌 경우, Source IP 제어는 적용되지 않습니다.	Global Configuration Mode
no security-manage snmp access-group	Source IP 주소 기반 접근 제어를 해제합니다.	Global Configuration Mode

명령어	설명	CLI 모드
show security-manage	서비스 제어 설정 상태를 확인합니다.	Privileged Mode

2.1.5. HTTP 서비스 제어

HTTP 서비스 제어 기능은 HTTP 서비스를 활성화/비활성화할 수 있으며, ACL을 통해 스위치에 접근할 수 있는 IP 주소를 제어할 수 있습니다.

HTTP 서비스 제어와 관련된 명령어는 다음 표와 같습니다.

명령어	설명	CLI 모드
security-manage http enable	HTTP 서비스를 활성화합니다.	Global Configuration Mode
security-manage http disable	HTTP 서비스를 비활성화합니다.	Global Configuration Mode
security-manage http access-group <1-99>*(참고: 실제 장비 기준)*	ACL 그룹을 지정하여 Source IP 주소 기반 접근 제어를 활성화합니다. 지정한 ACL이 존재하지 않거나 표준 ACL이 아닌 경우, Source IP 제어는 적용되지 않습니다.	Global Configuration Mode
no security-manage http access-group	Source IP 주소 기반 접근 제어를 해제합니다.	Global Configuration Mode
show security-manage	서비스 제어 설정 상태를 확인합니다.	Privileged Mode

2.1.6. HTTPS 서비스 제어

HTTPS 서비스 제어 기능은 HTTPS 서비스를 활성화/비활성화할 수 있으며, ACL을 통해 스위치에 접근할 수 있는 IP 주소를 제어할 수 있습니다.

HTTPS 서비스 제어와 관련된 명령어는 다음 표와 같습니다.

명령어	설명	CLI 모드
security-manage https enable	HTTPS 서비스를 활성화합니다.	Global Configuration

명령어	설명	CLI 모드
		Mode
security-manage https disable	HTTPS 서비스를 비활성화합니다.	Global Configuration Mode
security-manage https access-group <1-99>*(참고: 실제 장비 기준)*	ACL 그룹을 지정하여 Source IP 주소 기반 접근 제어를 활성화합니다. 지정한 ACL이 존재하지 않거나 표준 ACL이 아닌 경우, Source IP 제어는 적용되지 않습니다.	Global Configuration Mode
no security-manage https access-group	Source IP 주소 기반 접근 제어를 해제합니다.	Global Configuration Mode
show security-manage	서비스 제어 설정 상태를 확인합니다.	Privileged Mode

2.2. 시스템 유지보수 및 점검

기본적인 시스템 유지보수 및 점검 기능은 다음과 같습니다.

- 시스템 시간 설정
- 터미널 타임아웃 속성 설정
- 시스템 재부팅
- 시스템 정보 조회
- 네트워크 연결 상태 점검
- Traceroute 디버깅

2.2.1. 시스템 시간 설정

스위치는 실시간 시계(Real-Time Clock, RTC) 기능을 제공합니다.

명령어를 통해 현재 시간을 설정하거나 확인할 수 있습니다.

시스템의 시계는 내부 전원을 통해 유지되므로, 장비 전원이 꺼진 상태에서도 시간이 지속적으로 유지됩니다. 따라서 시스템을 재부팅하더라도 시간을 다시 설정할 필요가 없습니다.

스위치는 출고 시 기본 시간이 설정되어 있으므로, 일반적으로 사용자가 별도로 설정할 필요는 없습니다.

다만, 시간이 정확하지 않은 경우 사용자가 직접 시간을 재설정할 수 있습니다.

시스템 시간과 관련된 명령어는 다음 표와 같습니다.

명령어	설명	CLI 모드
set date-time <year> <month> <day> <hour> <minute> <second>	시스템의 현재 시간을 설정합니다. 연도, 월, 일, 시, 분, 초 값을 입력해야 합니다.	Privileged Mode
show date-time	시스템의 현재 시간을 표시합니다.	Normal Mode, Privileged Mode

2.2.2. 터미널 타임아웃 속성 설정

터미널 보안을 위해 일정 시간 동안 키 입력이 없을 경우, 터미널은 자동으로 종료됩니다.

Console 터미널과 Telnet 터미널의 타임아웃 동작은 서로 다릅니다.

Console 터미널

타임아웃 발생 시 CLI 모드가 종료되고 normal mode로 돌아갑니다.

Telnet 터미널

타임아웃 발생 시 Telnet 연결이 종료되며, 세션이 완전히 종료됩니다.

터미널의 기본 타임아웃 시간은 10분이며, 사용자는 타임아웃이 발생하지 않도록 설정할 수도 있습니다.

명령어	설명	CLI 모드
exec-timeout <minutes> [seconds]	터미널의 타임아웃 시간을 설정합니다. 모든 파라미터를 0으로 설정하면 타임아웃이 발생하지 않습니다.	Terminal Configuration Mode
no exec-timeout	터미널 타임아웃을 기본값(10분)으로 복원합니다.	Terminal Configuration Mode
show running-config	현재 시스템 설정을 확인하여 터미널 타임아웃 설정을 조회합니다.	Privileged Mode

2.2.3. 시스템 재설정

시스템은 다음과 같은 재설정 기능을 제공합니다.

- 스위치 재부팅

시스템 재설정과 관련된 명령어는 다음 표와 같습니다.

명령어	설명	CLI 모드
reset	스위치를 재부팅합니다.	Privileged Mode

2.2.4. 시스템 정보 조회

시스템은 다양한 display 명령어를 통해 시스템의 동작 상태 및 정보를 확인할 수 있도록 제공합니다.

여기에서는 시스템 유지보수에 자주 사용되는 일부 주요 display 명령어만을 소개합니다.

명령어	설명	CLI 모드
show version	시스템의 버전 정보와 파일이 컴파일 및 링크된 시간을 표시합니다.	Normal Mode, Privileged Mode
show snmp system information	시스템의 기본 정보를 표시하며, 시스템 기동 이후의 동작 시간(uptime) 등을 포함합니다.	Normal Mode, Privileged Mode
show history	CLI에서 최근에 입력한 명령어 목록을 표시합니다.	Normal Mode, Privileged Mode

2.2.5. 네트워크 연결 상태 점검

스위치와 네트워크 내 다른 장비 간의 연결 상태를 점검하기 위해, 스위치에서 ping 명령을 사용하여 상대 장비의 IP 주소로 테스트를 수행할 수 있습니다.

스위치가 상대 장비로부터 ping 응답을 수신하면 두 장비 간 통신이 정상적으로 이루어지고 있음을 의미하며, 응답이 없을 경우 두 장비 간 통신이 불가능한 상태임을 의미합니다.

스위치는 기본적인 ping 기능뿐만 아니라, 보다 정밀하고 다양한 점검을 위해 여러 옵션을 지원합니다.

ping 명령어는 다음 표와 같습니다.

명령어	설명	CLI 모드
ping <ip-address> [-n <count> | -l <size> | -w <timeout>]*	옵션 없이 기본 ping을 수행하거나, 하나 이상의 옵션을 함께 사용할 수 있습니다. 옵션 없이 사용할 경우 가장 기본적인 ping 테스트가 수행됩니다. 명령 실행 중 Ctrl + C를 입력하면 실행을 중단할 수 있습니다.	Privileged Mode

2.2.6. Traceroute 디버깅

스위치에서 다른 네트워크 장비와 통신할 때, 중간에 어떤 경로를 거치는지 확인하기 위해 trace-route 명령을 사용할 수 있습니다.

스위치에서 trace-route 명령을 실행할 때 상대 장비의 IP 주소를 지정하면, 명령 실행 과정에서 경유하는 모든 중간 경로가 표시됩니다.

이를 통해 통신 경로 상의 문제를 보다 정확하게 분석할 수 있습니다.

스위치는 기본적인 trace-route 기능뿐만 아니라, 보다 정밀한 분석을 위해 다양한 옵션을 지원합니다.

trace-route 명령어는 다음 표와 같습니다.

명령어	설명	CLI 모드
trace-route <ip-address> [-h <maximum-hops> | -j <count> <ip-address>* | -w <timeout>]*	옵션 없이 기본 trace-route를 수행하거나, 하나 이상의 옵션을 함께 사용할 수 있습니다. 옵션 없이 사용할 경우 가장 기본적인 경로 추적이 수행됩니다. 명령 실행 중 Ctrl + C를 입력하면 실행을 중단할 수 있습니다.	Privileged Mode

2.2.7. Telnet 클라이언트

스위치는 Telnet 클라이언트 기능을 제공하며, 사용자는 이 기능을 통해 다른 장비에 원격으로 접속할 수 있습니다.

명령어	설명	CLI 모드
telnet <ip-address>	파라미터는 대상 장비의 IP 주소입니다.	Privileged Mode

2.2.8. SSH 클라이언트

스위치는 SSH 클라이언트 기능을 제공하며, 사용자는 이를 통해 다른 장비에 원격으로 접속할 수 있습니다.

명령어	설명	CLI 모드
ssh <ip-address> [user-name]	SSH 클라이언트를 통해 다른 장비에 원격 접속할 수 있습니다. [user-name]은 선택 파라미터입니다.	Privileged Mode

2.3. 프로파일 관리

설정은 current configuration과 initial configuration으로 구분됩니다.

current configuration은 시스템이 동작 중일 때 적용되는 설정을 의미하며, 시스템의 메모리에 저장됩니다.

반면 initial configuration은 시스템이 시작될 때 사용되는 설정을 의미하며, 시스템의 FLASH에 저장됩니다. 즉, configuration file을 의미합니다.

사용자가 관련 명령어를 실행하면 시스템의 current configuration이 변경됩니다.

그러나 save 명령을 실행해야만 current configuration이 initial configuration에 저장되어, 다음 시스템 부팅 시에도 해당 설정이 적용됩니다.

시스템이 부팅된 후 사용자가 별도의 설정을 변경하지 않았다면, 시스템의 current configuration 정보는 initial configuration 정보와 동일합니다.

current configuration과 initial configuration은 동일한 형식을 사용합니다.

해당 형식은 명령줄 텍스트(command line text) 형식이며, 사용자가 직관적으로 읽고 이해하기 쉽습니다.

configuration file 형식의 주요 특징은 다음과 같습니다.

- configuration file은 텍스트 파일입니다.
- 저장되는 내용은 모두 명령어입니다.
- 기본 설정값은 저장하지 않고, 기본값이 아닌 설정만 저장합니다.
- 명령어는 CLI 모드에 따라 구성됩니다. 같은 CLI 모드의 명령어는 하나의 구간으로 묶이며, 각 구간은 !로 구분됩니다.
- global configuration mode의 명령어는 동일하거나 유사한 기능을 가진 명령어끼리 하나의 구간으로 구성되며, !로 구분됩니다.
- configuration submode의 명령어 앞에는 공백이 추가됩니다. 반면 global configuration mode의 명령어 앞에는 공백이 필요하지 않습니다.
- 설정 파일은 end로 종료됩니다.

configuration file 관리는 주로 다음 내용을 포함합니다.

- 설정 정보 조회
- 설정 저장
- 프로파일 삭제
- configuration file 업로드 및 다운로드

2.3.1. 설정 정보 조회

설정 정보 조회는 시스템의 current configuration과 initial configuration을 확인하는 기능을 포함합니다.

initial configuration은 실제로 시스템의 FLASH에 저장된 configuration file을 의미합니다.

FLASH에 configuration file이 존재하지 않는 경우, 시스템은 부팅 시 기본 설정(default configuration)을 사용합니다.

이 상태에서 initial configuration을 조회하면, configuration file이 존재하지 않는다는 메시지가 표시됩니다.

명령어	설명	CLI 모드
show running-config	시스템의 current configuration을 확인합니다.	Privileged Mode
show startup-config	시스템의 initial configuration을 확인합니다.	Privileged Mode

2.3.2. 설정 저장

사용자가 시스템의 current configuration을 변경한 경우, 해당 설정을 configuration file에 저장해야 합니다.

이렇게 저장된 설정은 다음 부팅 이후에도 유지되며, 저장하지 않을 경우 시스템 재부팅 시 모든 변경 내용이 사라집니다.

설정을 저장한다는 것은 current configuration을 initial configuration으로 반영하는 것을 의미합니다.

명령어	설명	CLI 모드
write	current configuration을 저장합니다.	Privileged Mode

2.3.3. 프로파일 삭제

사용자가 시스템의 initial configuration을 기본 설정(default configuration)으로 되돌리고자 할 경우, configuration file을 삭제할 수 있습니다.

configuration file을 삭제해도 현재 동작 중인 current configuration에는 영향을 주지 않습니다.

current configuration까지 기본 설정으로 되돌리려면 스위치를 재부팅해야 합니다.

configuration file 삭제 시 설정 정보가 손실될 수 있으므로, 사용자는 해당 작업을 신중하게 수행해야 합니다.

명령어	설명	CLI 모드
delete startup-config	시스템의 startup configuration file을 삭제합니다.	Privileged Mode

2.3.4. Configuration file 업로드 및 다운로드

configuration file의 보안을 위해, 사용자는 명령어를 사용하여 configuration file을 PC로 업로드하고 백업할 수 있습니다.

시스템 설정이 비정상적으로 손실되었거나 변경되어 기존 설정으로 복구해야 하는 경우, 사용자는 PC에 저장된 기존 configuration file을 스위치로 다운로드할 수 있습니다.

다운로드한 configuration file은 현재 동작 중인 current configuration에는 영향을 주지 않습니다.

해당 설정은 스위치를 재부팅한 후 적용됩니다.

configuration file은 WEB을 통해서도 업로드 및 다운로드할 수 있습니다.

자세한 작업 방법은 WEB Operation Manual을 참조하십시오.

명령어	**설명**	**CLI 모드**
upload configure <ip-address> <file-name>	configuration file을 PC로 업로드합니다. 첫 번째 파라미터는 PC의 IP 주소이며, 두 번째 파라미터는 PC에 저장할 configuration file 이름입니다.	Privileged Mode
download configure <ip-address> <file-name>	PC에 저장된 configuration file을 스위치로 다운로드합니다. 첫 번째 파라미터는 PC의 IP 주소이며, 두 번째 파라미터는 PC에 저장된 configuration file 이름입니다.	Privileged Mode

configuration file 업로드 및 다운로드는 TFTP 프로토콜을 사용합니다.

스위치에서는 TFTP client software가 동작하며, PC에서는 TFTP server software가 동작해야 합니다.

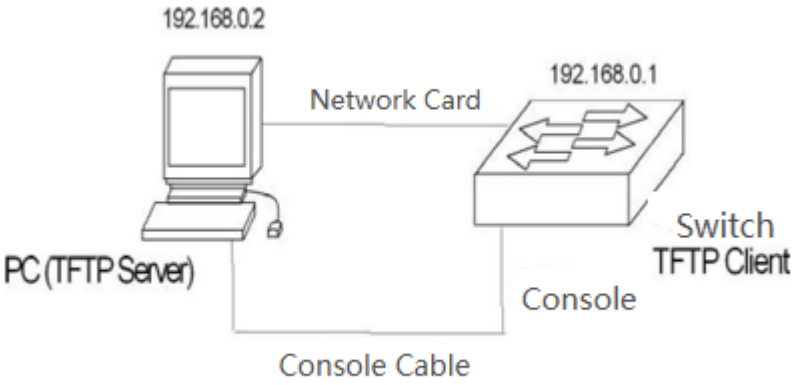
configuration file을 업로드하거나 다운로드하는 절차는 다음과 같습니다.

- Step 1:
  네트워크 환경을 구성합니다.
- Step 2:
  PC에서 TFTP server software를 실행하고, configuration file이 저장될 디렉터리를 설정합니다.
- Step 3:
  스위치에서 설정을 저장합니다.
- Step 4:
  스위치에서 configuration file upload 명령을 실행하여 configuration file을 PC에 백업합니다.
- Step 5:
  스위치에서 PC에 저장된 configuration file이 필요한 경우, configuration file download 명령을 실행하여 PC의 configuration file을 스위치로 다운로드합니다.
- Step 6:
  다운로드한 configuration file을 적용하려면 스위치를 재부팅해야 합니다.

예시

VLAN 및 interface address가 설정된 스위치에서 configuration file을 업로드 및 다운로드해야 하는 경우의 예시는 다음과 같습니다.

- Step 1:
  아래 그림과 같이 네트워크 환경을 구성합니다.



아래처럼 번역하시면 매뉴얼 흐름 + 실제 작업 절차 자연스럽게 이어집니다.

- Step 1:
  스위치의 설정 포트를 케이블을 통해 설정용 터미널에 연결하고, 네트워크 케이블을 통해 PC 와 연결합니다.

PC에는 TFTP Server를 설치하고, PC의 Ethernet 포트에 IP 주소를 설정합니다.

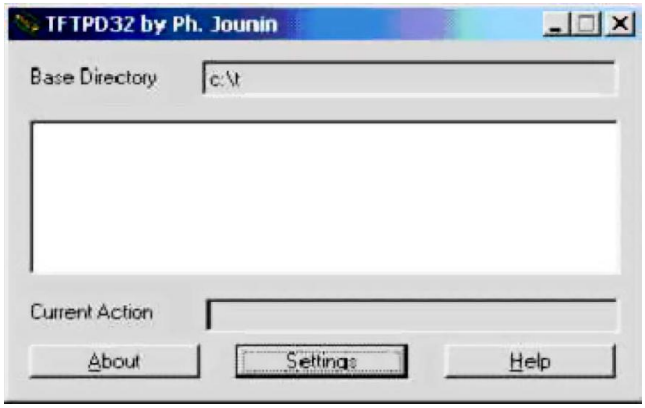
여기서는 PC의 IP 주소를 192.168.0.2로 가정합니다.

이후 스위치의 IP 주소를 설정하며, 스위치의 IP 주소는 192.168.0.1로 가정합니다.

PC와 스위치 간의 통신이 정상적으로 이루어지는지 확인합니다.

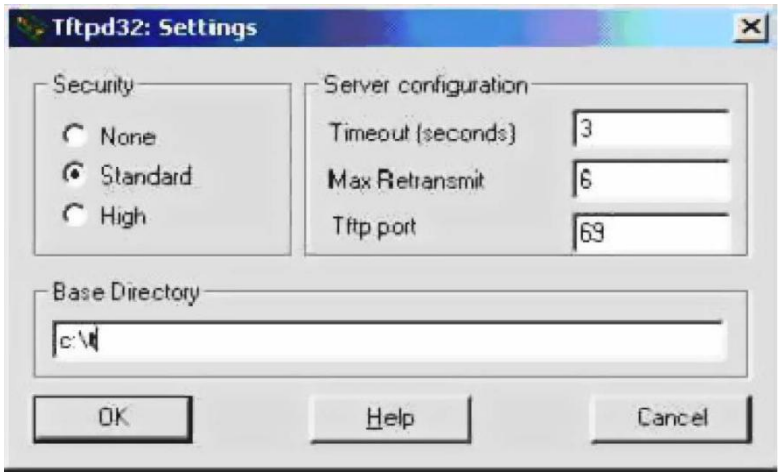
- Step 2:
  TFTP Server를 실행하고 관련 파라미터를 설정합니다.

TFTP Server를 실행하면, 아래와 같은 화면이 표시됩니다.



이후 configuration file이 백업될 디렉터리를 설정합니다.

구체적인 작업 방법은 [Settings] 버튼을 클릭하여 설정 화면으로 진입하는 것이며, 아래 그림과 같습니다.



Base Directory에 파일 경로를 입력한 후, [OK] 버튼을 클릭하여 설정을 완료합니다.

- Step 3:
  스위치에서 write 명령을 실행하여 current configuration을 configuration file에 저장합니다.
- Step 4:
  configuration file을 PC로 백업하기 위해 다음 명령을 실행합니다.
  Switch# upload configuration 192.168.0.2 beifen.cfg
- Step 5:
  필요한 경우, PC에 백업된 configuration file을 스위치로 다운로드하기 위해 다음 명령을 실행합니다.
  Switch# download configuration 192.168.0.2 beifen.cfg
- Step 6:
  다운로드한 configuration file을 적용하려면 스위치를 재부팅해야 하며, 다음 명령을 실행합니다.
  Switch# reset

2.4. 소프트웨어 버전 업그레이드

스위치는 소프트웨어 버전의 온라인 업그레이드를 지원합니다.

업그레이드는 TFTP 도구를 통해 수행됩니다.

2.4.1. 소프트웨어 버전 업그레이드 명령어

1) 스위치 파일을 업그레이드하려면 global configuration mode에서 다음 명령을 실행합니다.

download switch <ip-address> <file-name>

- <ip-address>: TFTP 서버가 실행 중인 PC의 IP 주소
- <file-name>: TFTP 서버에 저장된 스위치 파일 이름

2) 커널 파일을 업그레이드하려면 global configuration mode에서 다음 명령을 실행합니다.

download kernel <ip-address> <file-name>

- <ip-address>: TFTP 서버가 실행 중인 PC의 IP 주소
- <file-name>: TFTP 서버에 저장된 커널 파일 이름

3) 패치 파일을 업그레이드하려면 global configuration mode에서 다음 명령을 실행합니다.

download patch <ip-address> <file-name>

- <ip-address>: TFTP 서버가 실행 중인 PC의 IP 주소
- <file-name>: TFTP 서버에 저장된 패치 파일 이름

4) uboot 파일을 업그레이드하려면 global configuration mode에서 다음 명령을 실행합니다.

download uboot <ip-address> <file-name>

- <ip-address>: TFTP 서버가 실행 중인 PC의 IP 주소
- <file-name>: TFTP 서버에 저장된 uboot 파일 이름

※ 주의사항

업그레이드 진행 중에는 절대로 스위치의 전원을 차단하면 안 됩니다.

전원이 차단될 경우 파일이 손상되어 스위치가 정상적으로 부팅되지 않을 수 있습니다.

파일 다운로드가 완료된 후에는 스위치를 재부팅해야 새로운 파일이 적용됩니다.

전체 업그레이드 과정은 수 분 정도 소요되므로, 완료될 때까지 기다려야 합니다.

소프트웨어 버전 업그레이드는 WEB을 통해서도 수행할 수 있습니다.

자세한 내용은 WEB Operation Manual을 참조하십시오.

주식회사 포엠아이텍

2.4.2. 소프트웨어 업그레이드 절차

스위치 및 기타 파일의 업그레이드 절차는 다음과 같습니다.

- Step 1:
  업그레이드 환경을 구성합니다. (아래 그림 참조)

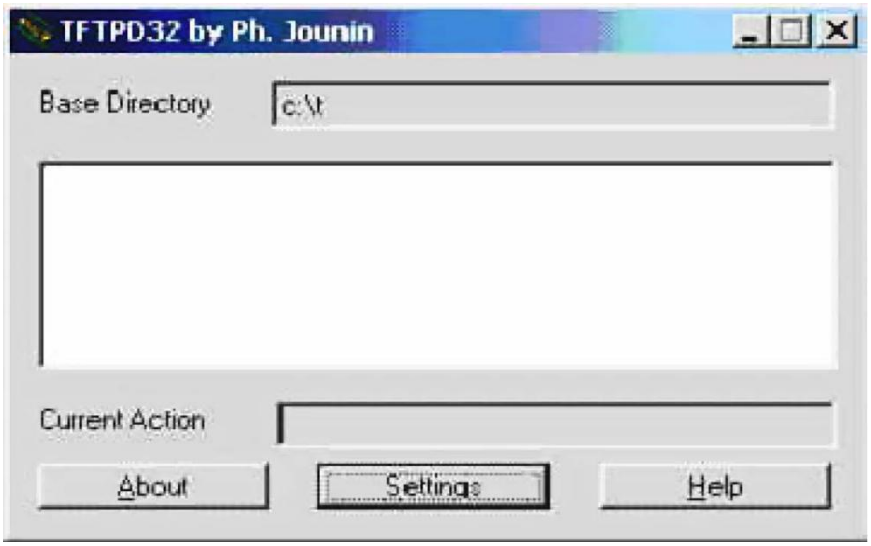
구성 절차는 다음과 같습니다.

- 케이블을 이용하여 스위치의 Console 포트를 설정용 터미널(PC)에 연결합니다.
- PC에 TFTP Server를 설치합니다.
- 새로운 스위치 파일 및 기타 파일을 PC의 특정 경로에 복사합니다.
  (예: C:₩t)
- PC의 Ethernet 포트에 IP 주소를 설정합니다.
  (예: 192.168.0.2)
- 스위치의 IP 주소를 설정합니다.
  (예: 192.168.0.1)

- Step 2:
  TFTP Server를 실행하고 설정을 구성합니다.

먼저 TFTP Server를 실행합니다.

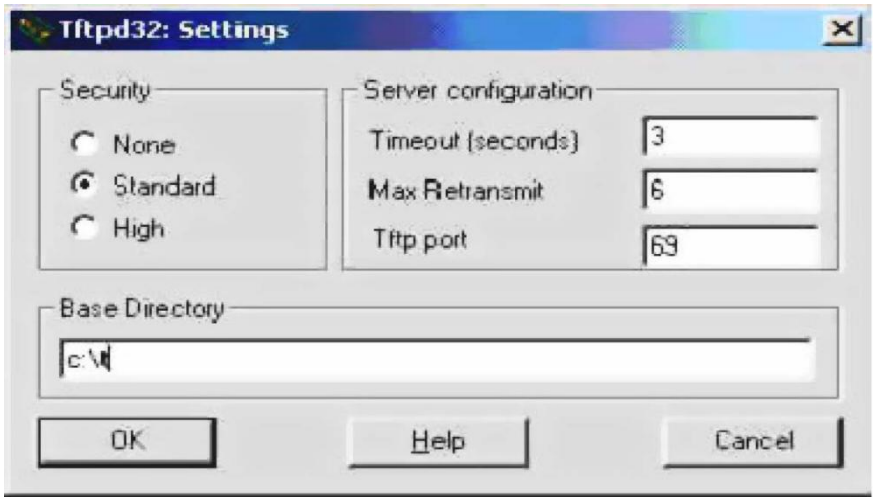
TFTPD32 실행 화면은 아래 그림과 같습니다.



이후 TFTP Server의 파일 디렉터리를 설정합니다.

TFTP Server를 실행한 후, 파일이 저장될 디렉터리를 설정하고 업로드할 스위치 파일 및 기타 파일을 해당 디렉터리에 복사합니다.

설정 방법은 [Settings] 버튼을 클릭하여 TFTPD32 설정 화면으로 진입하는 것이며, 아래 그림과 같습니다.



Base Directory에 파일 경로를 입력한 후, [OK] 버튼을 클릭하여 설정을 완료합니다.

- Step 3: 파일 업그레이드
  먼저, 스위치의 포트를 Ethernet 케이블로 TFTP Server가 실행 중인 PC와 연결합니다.
  이후 ping 명령을 사용하여 PC와 스위치 간의 연결 상태를 확인합니다.
  그 다음, HyperTerminal에서 다음 명령을 입력합니다.

  Switch# download switch 192.168.0.2 switch.img

  Enter 키를 누른 후 파일 업그레이드가 완료될 때까지 기다립니다.

  Software is updating. Please wait and don't power down!
  ……
  Updating is completed. Do you wish to reset? [Y/N]

  파일 전송이 완료되면, 시스템은 스위치 재부팅 여부를 묻습니다.
  일반적으로 업그레이드 적용을 위해 Y를 선택하여 스위치를 재부팅하는 것을 권장합니다.
  단, 설정이 저장되지 않은 경우에는 먼저 N을 선택한 후, 설정 저장 등의 작업을 완료한 뒤 재부팅할 수 있습니다.

  Switch#

  ※ 주의사항

업그레이드 진행 중에는 스위치의 전원을 차단해서는 안 됩니다.

- Step 4: 스위치 재부팅

  Switch# reset

3. 포트 설정

이 장에서는 포트와 관련된 설정을 소개하며, 주요 내용은 다음과 같습니다.

- 포트 기본 설정
- MIRROR 설정
- STORM-CONTROL 설정
- flow-control 설정
- 포트 대역폭 설정
- TRUNK 설정

3.1. 포트 기본 설정

관리자는 스위치의 포트를 설정하여 해당 포트에 연결된 사용자의 네트워크 접근을 제어할 수 있습니다.

포트에 연결된 사용자의 네트워크 접근을 허용하지 않으려는 경우, 관리자는 해당 포트를 비활성화(차단)할 수 있습니다.

이 절에서는 포트의 기본 설정에 대해 설명하며, 주요 내용은 다음과 같습니다.

- 포트 활성화 및 비활성화
- 포트 속도 설정
- 포트 정보 조회

3.1.1. 포트 활성화 및 비활성화

스위치의 포트는 기본적으로 활성화되어 있습니다.

관리자가 해당 포트에 연결된 사용자의 네트워크 접근을 차단하려는 경우, 포트를 비활성화할 수 있습니다.

다음 명령어는 interface configuration mode에서 포트를 활성화합니다.

no shutdown

예: 포트 ge1/1을 활성화하는 경우

Switch(config-ge1/1)# no shutdown

다음 명령어는 interface configuration mode에서 포트를 비활성화합니다.

shutdown

예: 포트 ge1/1을 비활성화하는 경우

Switch(config-ge1/1)# shut

3.1.2. 포트 속도 설정

모든 포트의 기본 속도 설정은 autonegotiate(자동 협상)입니다.

다음 명령어를 사용하여 interface configuration mode에서 포트의 속도를 설정할 수 있습니다.

speed {autonegotiate | full-1000 | full-100 | full-10 | half-100 | half-10}

각 옵션의 의미는 다음과 같습니다.

- autonegotiate → 자동 협상
- full-1000 → 1Gbps Full-Duplex
- full-100 → 100Mbps Full-Duplex
- full-10 → 10Mbps Full-Duplex
- half-100 → 100Mbps Half-Duplex
- half-10 → 10Mbps Half-Duplex

예시:

포트 ge1/1을 100Mbps Full-Duplex로 설정하는 경우

Switch(config-ge1/1)# speed full-100

3.1.3. 포트 정보 조회

다음 명령어를 사용하여 normal mode 또는 privileged mode에서 하나 이상의 포트 정보를 확인할 수 있습니다.

show interface [if-name]

예시:

포트 ge1/1의 정보를 조회하는 경우

Switch# show interface ge1/1

모든 포트의 정보를 조회하는 경우

Switch# show interface

3.2. MIRROR 설정

포트 미러링(Port Mirroring)은 하나 이상의 포트에서 송수신되는 트래픽을 모니터링하기 위한 매우 유용한 기능입니다.

미러링 포트를 통해 특정 포트(또는 여러 포트)의 수신 및 송신 패킷을 복사하여 분석할 수 있습니다.

스위치는 포트 미러링 기능을 지원하며, 미러링 포트는 다른 포트의 인바운드 및 아웃바운드 트래픽을 모두 수집할 수 있습니다.

또한 하나의 미러링 포트는 여러 개의 포트를 동시에 모니터링할 수 있습니다.

이 절에서는 MIRROR 설정에 대해 설명하며, 주요 내용은 다음과 같습니다.

- MIRROR의 모니터링 포트(Listener) 및 대상 포트(Source) 설정
- MIRROR 설정 정보 조회

3.2.1. MIRROR 모니터링 포트 및 대상 포트 설정

MIRROR 설정 시, 관리자는 interface configuration mode에서 모니터링 포트를 설정해야 합니다.

예를 들어, 포트 ge1/1에서 포트 ge1/2의 트래픽을 모니터링하려면 다음과 같이 설정합니다.

Switch(config-ge1/1)# mirror interface ge1/2 direction both

이 경우

ge1/1 → 모니터링 포트(Listener, Mirror Port)

ge1/2 → 대상 포트(Source Port) 로 설정됩니다.

모니터링 포트 설정 명령어

Switch(config-ge1/1)# mirror interface <if-name> direction {both | receive | transmit}

<if-name> → 모니터링 대상 포트

direction → 모니터링 방향 설정

각 옵션의 의미는 다음과 같습니다.

receive → 수신(Ingress) 패킷 모니터링

transmit → 송신(Egress) 패킷 모니터링

both → 수신 + 송신 패킷 모두 모니터링

예시:

Switch(config-ge1/1)# mirror interface ge1/2 direction both

→ ge1/1 포트에서 ge1/2의 송수신 트래픽을 모두 모니터링함

여러 개의 포트를 모니터링하려면, 해당 명령어를 반복 실행하면 됩니다.

모니터링 대상 포트 해제

interface configuration mode에서 다음 명령어로 모니터링을 해제할 수 있습니다.

Switch(config-ge1/1)# no mirror interface <if-name>

<if-name> → 모니터링 해제할 대상 포트

예시:

Switch(config-ge1/1)# no mirror interface ge1/2

→ ge1/1 포트가 더 이상 ge1/2의 트래픽을 모니터링하지 않음

모든 대상 포트를 해제하면, 해당 모니터링 포트 설정도 함께 제거됩니다.

3.2.2. MIRROR 설정 조회

관리자는 normal mode 또는 privileged mode에서 다음 명령어를 사용하여 설정된 MIRROR 구성을 확인할 수 있습니다.

Switch# show mirror

※ 주의사항

하나의 포트는 동시에 모니터링 포트(Listener)와 대상 포트(Source)로 설정할 수 없습니다.

- 모니터링 포트(Listener)는 1개만 설정 가능하며,
- 대상 포트(Source)는 여러 개 설정할 수 있습니다.

3.3. STORM-CONTROL 설정

실제 네트워크 환경에서 NIC(Network Interface Card)가 과도한 속도로 유니캐스트, 멀티캐스트, 브로드캐스트 패킷을 전송할 경우, 네트워크 장애가 발생할 수 있습니다.

이러한 상황에서 스위치의 Storm Control 기능은 매우 중요하며, 과도한 트래픽이 네트워크로 유입되는 것을 제한하여 네트워크 혼잡을 방지할 수 있습니다.

스위치의 모든 포트는 브로드캐스트, 멀티캐스트, DLF(Unknown Unicast) 패킷에 대한 트래픽 억제 기능을 지원합니다.

이 절에서는 STORM-CONTROL 설정에 대해 설명하며, 주요 내용은 다음과 같습니다.

- 기본 설정
- Broadcast 억제 설정
- Multicast 억제 설정
- DLF(Unknown Unicast) 억제 설정
- STORM-CONTROL 설정 정보 조회

3.3.1. 기본 설정

스위치는 각 포트별로 Broadcast, Multicast, DLF 트래픽 억제 기능을 설정할 수 있으며, 세 가지 설정은 동일한 rate limit 값을 공유합니다.

기본적으로 포트의 Broadcast 패킷 억제 기능은 활성화되어 있으며, rate limit 값은 64K로 설정되어 있습니다. 이는 네트워크에서 Broadcast Storm이 발생하는 것을 방지하기 위한 설정입니다.

DLF 패킷과 Multicast 패킷은 기본적으로 억제되지 않습니다.

3.3.2. Broadcast 억제 설정

다음 명령어를 사용하여 interface configuration mode에서 해당 포트의 Broadcast 트래픽 억제를 설정할 수 있습니다.

storm-control broadcast

다음 명령어를 사용하여 해당 포트의 Broadcast 트래픽 억제 설정을 해제할 수 있습니다.

no storm-control broadcast

3.3.3. Multicast 억제 설정

다음 명령어를 사용하여 interface configuration mode에서 해당 포트의 Multicast 트래픽 억제를 설정할 수 있습니다.

storm-control multicast

다음 명령어를 사용하여 해당 포트의 Multicast 트래픽 억제 설정을 해제할 수 있습니다.

no storm-control multicast

3.3.4. DLF(Unknown Unicast) 억제 설정

다음 명령어를 사용하여 interface configuration mode에서 해당 포트의 DLF(Unknown Unicast) 트래픽 억제를 설정할 수 있습니다.

storm-control dlf

다음 명령어를 사용하여 해당 포트의 DLF 트래픽 억제 설정을 해제할 수 있습니다.

no storm-control dlf

3.3.5. 억제율(Rate Limit) 설정

다음 명령어를 사용하여 interface configuration mode에서 해당 포트의 트래픽 억제율(rate limit)을 설정할 수 있습니다.

storm-control ratelimit <1-1024000>

3.3.6. STORM-CONTROL 설정 조회

다음 명령어를 사용하여 normal mode 또는 privileged mode에서 STORM-CONTROL 설정을 확인할 수 있습니다.

show storm-control

3.4. STORM-CONSTRAIN 설정

포트 트래픽 임계값 제어(STORM-CONSTRAIN) 기능은 이더넷에서 발생할 수 있는 패킷 폭주(Storm)를 제어하기 위해 사용됩니다.

이 기능이 활성화된 포트는 유니캐스트, 멀티캐스트, 브로드캐스트 트래픽을 주기적으로 검사하며, 특정 유형의 트래픽이 설정된 임계값을 초과할 경우 관리자가 설정한 방식으로 제어를 수행합니다. 또한 필요 시 로그 기록 여부도 설정할 수 있습니다.

특정 트래픽이 설정된 최대 임계값을 초과하면, 시스템은 다음 두 가지 방식 중 하나로 처리합니다.

1) Block 모드
   - 트래픽이 임계값을 초과하면 해당 트래픽의 전달을 차단합니다.
   - 포트는 Block 상태가 되지만 트래픽 카운팅은 계속 수행합니다.
   - 트래픽이 설정된 최소 임계값 이하로 감소하면 정상적으로 전달을 재개합니다.
2) Shutdown 모드
   - 트래픽이 임계값을 초과하면 포트를 비활성화(shutdown)합니다.
   - 모든 트래픽 전달이 중단됩니다.

- no shutdown 명령 또는 설정 해제를 통해 포트를 다시 활성화할 수 있습니다.

※ 주의사항

특정 트래픽 유형에 대해 STORM-CONSTRAIN 기능과 STORM-CONTROL 기능을 동시에 설정할 수 없습니다. 두 기능을 동시에 설정할 경우 트래픽 제어 동작이 불확실해질 수 있습니다.

예를 들어, Unicast 트래픽에 대해

- STORM-CONSTRAIN
- STORM-CONTROL

을 동시에 적용할 수 없습니다.

명령어	**설명**	**CLI 모드**
storm-constrain (broadcast|multicast|unicast) min-rate <1-1488100> max-rate <1-1488100>	Broadcast, Multicast, Unicast 트래픽에 대해 임계값 기반 제어를 설정합니다.	Interface Configuration Mode
no storm-constrain (broadcast|multicast|unicast|all)	설정된 트래픽 제어를 해제합니다.	Interface Configuration Mode
storm-constrain action (block|shutdown)	트래픽 초과 시 동작 방식을 설정합니다. (block 또는 shutdown)	Interface Configuration Mode
no storm-constrain action	설정된 동작 방식을 해제합니다.	Interface Configuration Mode
storm-constrain enable (trap)	트래픽 제어 발생 시 로그(Trap)를 활성화합니다.	Interface Configuration Mode
no storm-constrain enable (log)	트래픽 제어 로그 기능을 비활성화합니다.	Interface Configuration Mode
storm-constrain interval <6-180>	트래픽 검사 주기를 설정합니다. (기본값: 5초)	Interface Configuration Mode
no storm-constrain interval	트래픽 검사 주기를 기본값으로 복원합니다.	Interface

명령어	설명	CLI 모드
		Configuration Mode
no storm-constrain	인터페이스에서 STORM-CONSTRAIN 기능을 완전히 제거합니다.	Interface Configuration Mode
show storm-constrain	모든 인터페이스의 STORM-CONSTRAIN 설정을 조회합니다.	Privileged Mode
show storm-constrain interface IFNAME	특정 인터페이스의 STORM-CONSTRAIN 설정을 조회합니다.	Privileged Mode

1) 인터페이스의 STORM-CONSTRAIN 정보 항목 설명

항목	설명
interface	인터페이스 이름
type	트래픽 유형(1) broadcast: 브로드캐스트 패킷(2) multicast: 멀티캐스트 패킷(3) unicast: 유니캐스트 패킷
rate	트래픽 임계값Min: 하한 임계값Max: 상한 임계값
action	STORM 제어 동작 방식(1) block: 트래픽 차단(2) shutdown: 인터페이스 비활성화
punish-status	현재 인터페이스 상태(1) block: 트래픽이 max-rate를 초과하고 동작이 block인 경우(2) normal: 정상 전달 상태(3) shutdown: 트래픽이 max-rate를 초과하고 동작이 shutdown인 경우
log	로그 기능 활성화 여부 (on/off)
interval	트래픽 검사 주기 (초 단위, 기본값: 5초)
last-punish-time	마지막으로 STORM 제어가 수행된 시간

2) storm-constrain action 명령으로 STORM 제어 동작 방식을 설정하고, storm-constrain 명령으로 STORM 제어의 상한/하한 임계값을 설정하면, Storm 트래픽을 제어하여 네트워크 플러딩을 방지할 수 있습니다.

STORM 제어 검사 주기 동안, 인터페이스에서 수신되는 Broadcast, Multicast 또는 Unicast 패킷의 평균 속도가 지정된 상한 임계값보다 높을 경우, 설정된 동작 방식에 따라 해당 트래픽을 차단하거나 인터페이스를 shutdown합니다.
STORM 제어 동작이 block인 경우, 트래픽이 최소 임계값보다 낮아지면 인터페이스는 정상 forwarding 상태로 복구됩니다.
STORM 제어 동작이 shutdown인 경우, 인터페이스는 자동으로 복구되지 않으며 no shutdown 명령을 수동으로 실행해야 복구됩니다. 또는 포트의 STORM 제어 shutdown 동작 설정을 해제하여 복구할 수 있습니다.

3) 포트 트래픽이 상한 임계값을 초과하거나, 상한 임계값을 초과한 상태에서 다시 하한 임계값 이하로 감소할 경우, log/trap 정보가 출력됩니다.

3.5. FLOW-CONTROL 설정

FLOW-CONTROL은 포트 혼잡으로 인해 패킷 손실이 발생하는 것을 방지하기 위해 사용됩니다.

Half-duplex 모드에서는 Backpressure 기술을 사용하여 송신 측의 전송 속도를 낮추는 방식으로 흐름 제어가 이루어집니다.

Full-duplex 모드에서는 IEEE 802.3x 표준을 따르며, 혼잡 상태의 포트가 송신 측에 Pause 프레임을 전송하여 데이터 전송을 일시 중지하도록 합니다.

이 절에서는 FLOW-CONTROL 설정에 대해 설명하며, 주요 내용은 다음과 같습니다.

- 기본 설정
- 포트 Flow Control 설정
- 포트 Flow Control 해제
- Flow Control 정보 조회

3.5.1. 기본 설정

스위치는 각 포트별로 송신 및 수신에 대한 Flow Control을 설정할 수 있습니다.

기본적으로 모든 포트의 Flow Control 기능은 비활성화되어 있습니다.

3.5.2. 포트 Flow Control 설정

다음 명령어를 사용하여 interface configuration mode에서 포트의 Flow Control 기능을 활성화할 수 있습니다.

flowcontrol

3.5.3. 포트 Flow Control 해제

다음 명령어를 사용하여 interface configuration mode에서 포트의 송신 및 수신 Flow Control 기능을 비활성화할 수 있습니다.

no flowcontrol

3.5.4. Flow Control 정보 조회

다음 명령어를 사용하여 normal mode 또는 privileged mode에서 모든 포트의 Flow Control 정보를 확인할 수 있습니다.

show flowcontrol

다음 명령어를 사용하여 특정 포트의 Flow Control 정보를 확인할 수 있습니다.

show flowcontrol interface <if-name>

- <if-name>: Flow Control 정보를 조회할 포트 이름

3.6. 포트 대역폭 설정

포트 대역폭 제어는 포트의 송신 및 수신 속도를 제한하기 위해 사용됩니다.

이를 통해 특정 포트에서 과도한 트래픽이 발생하는 것을 방지하고, 네트워크 자원을 효율적으로 분배할 수 있습니다.

이 절에서는 포트 대역폭 설정에 대해 설명하며, 주요 내용은 다음과 같습니다.

- 기본 설정
- 포트 송신/수신 대역폭 제어 설정
- 포트 송신/수신 대역폭 제어 해제
- 포트 대역폭 설정 정보 조회

3.6.1. 기본 설정

스위치는 각 포트별로 송신 및 수신 대역폭을 개별적으로 설정할 수 있습니다.

기본적으로 모든 포트에는 대역폭 제어가 적용되어 있지 않습니다.

3.6.2. 포트 송신/수신 대역폭 제어 설정

다음 명령어를 사용하여 interface configuration mode에서 포트의 송신 또는 수신 대역폭 제어를 설정할 수 있습니다.

portrate {egress | ingress} <rate>

각 옵션의 의미는 다음과 같습니다.

- egress → 송신(출력) 트래픽 대역폭 제어
- ingress → 수신(입력) 트래픽 대역폭 제어
- <rate> → 설정할 대역폭 값 (범위: 1 ~ 1024000, 단위: Kbps)

3.6.3. 포트 송신/수신 대역폭 제어 해제

다음 명령어를 사용하여 interface configuration mode에서 포트의 대역폭 제어를 해제할 수 있습니다.

no portrate {egress | ingress}

각 옵션의 의미는 다음과 같습니다.

- egress → 송신(출력) 트래픽 대역폭 제어 해제
- ingress → 수신(입력) 트래픽 대역폭 제어 해제

3.6.4. 포트 대역폭 설정 조회

다음 명령어를 사용하여 normal mode 또는 privileged mode에서 포트의 대역폭 제어 설정을 확인할 수 있습니다.

show portrate interface <if-name>

- <if-name>: 대역폭 제어 정보를 조회할 포트 이름

3.7. TRUNK 설정

TRUNK는 여러 개의 물리 포트를 하나의 논리 포트로 묶는 기능으로, 대역폭 증가, 이중화(백업), 로드밸런싱을 제공하기 위해 사용됩니다.

TRUNK 그룹이 출력 논리 포트로 동작할 때, 스위치는 설정된 집계 정책에 따라 포트 그룹 내 특정 포트를 선택하여 패킷을 전송합니다.

TRUNK 그룹의 포트 구성 및 집계 정책은 소프트웨어에서 설정되며, 실제 데이터 전달은 하드웨어에서 처리됩니다.

TRUNK 그룹에 포함된 모든 포트는 동일한 속도와 Full-Duplex 모드로 설정되어야 합니다.

스위치는 최대 32개의 TRUNK 그룹을 지원하며, 각 그룹에는 최대 8개의 포트를 구성할 수 있습니다.

또한 하나의 포트는 하나의 TRUNK 그룹에만 속할 수 있습니다.

LACP 프로토콜

LACP(Link Aggregation Control Protocol)는 IEEE 802.3ad 표준 기반의 프로토콜입니다.

LACP는 LACPDU(Link Aggregation Control Protocol Data Unit)를 통해 상대 장비와 정보를 교환합니다.

포트가 LACP를 활성화하면, 다음 정보를 포함한 LACPDU를 상대 장비로 전송합니다.

- 시스템 LACP 우선순위
- 시스템 MAC 주소
- 포트 LACP 우선순위
- 포트 번호
- Operation Key

상대 장비는 수신한 LACPDU 정보를 다른 포트 정보와 비교하여, Selected 상태로 동작할 포트를 선택하게 되며, 이를 통해 양쪽 장비 간 링크 집계 구성이 일치하게 됩니다.

Action Key 설명

Action Key는 링크 집계 시 자동으로 생성되는 설정 값의 조합으로, 다음 요소들을 포함합니다.

- 포트 속도
- Duplex 모드
- 포트 상태 (Up/Down)
- 허용 VLAN
- 기본 VLAN ID
- 포트 링크 타입 (Trunk / Hybrid / Access)

같은 TRUNK 그룹 내에서 Selected 상태의 포트들은 동일한 Action Key를 가져야 합니다.

이 절에서는 TRUNK 설정에 대해 설명하며, 주요 내용은 다음과 같습니다.

- LACP 프로토콜 설정
- TRUNK 그룹 설정
- TRUNK 멤버 포트 설정
- TRUNK 로드밸런싱 정책 설정
- TRUNK 정보 조회

3.7.1. LACP 프로토콜 설정

명령어	**설명**	**CLI 모드**
lacp system-priority <1-65535>	LACP 시스템 우선순위를 설정합니다.	Global Configuration Mode
no lacp system-priority	LACP 시스템 우선순위를 기본값(32768)으로 복원합니다.	Global Configuration Mode
lacp max-active-link-number <1-8>	활성화 가능한 LACP 집계 포트 수의 최대값을 설정합니다.	Global Configuration Mode
no lacp max-active-link-number	LACP 집계 포트 최대 활성 수를 기본값(8)으로 복원합니다.	Global Configuration Mode
lacp port-priority <1-65535>	포트의 LACP 우선순위를 설정합니다.	Interface Configuration Mode
no lacp port-priority	포트 LACP 우선순위를 기본값(32768)으로 복원합니다.	Interface Configuration Mode
lacp timeout (short | long)	LACP 포트 타임아웃을 설정합니다. (기본값: long)	Interface Configuration Mode

명령어	설명	CLI 모드
show lacp summary	전체 LACP 집계 상태를 요약하여 표시합니다.	Privileged Mode
show lacp detail	전체 LACP 집계의 상세 정보를 표시합니다.	Privileged Mode
show lacp <1-8>	특정 LACP 집계 포트의 상세 정보를 표시합니다.	Privileged Mode
show lacp port IFNAME	특정 포트의 LACP 상태 정보를 표시합니다.	Privileged Mode
show lacp system-id	LACP 시스템 정보를 표시합니다.	Privileged Mode
show lacp counter <1-8>	특정 LACP 집계 포트의 통계 정보를 표시합니다.	Privileged Mode
show lacp counter	모든 LACP 집계 포트의 통계 정보를 표시합니다.	Privileged Mode
clear lacp <1-8> counters	특정 LACP 집계 포트의 통계 정보를 초기화합니다.	Privileged Mode
clear lacp counters	모든 LACP 집계 포트의 통계 정보를 초기화합니다.	Privileged Mode

3.7.2. TRUNK 그룹 설정

다음 명령어를 사용하여 global configuration mode에서 수동(TRUNK) 그룹을 생성할 수 있습니다.

trunk <trunk-id>

- <trunk-id>: TRUNK 그룹 ID (범위: 1~32)
- 생성 후 인터페이스 이름은 trunk + ID 형태로 구성됩니다.
  (예: trunk1)

TRUNK 그룹 생성 후, 다음 명령어를 사용하여 해당 TRUNK 인터페이스 설정 모드로 진입할 수 있습니다.

interface trunk<ID>

예:

interface trunk1

다음 명령어를 사용하여 LACP 기반 동적 TRUNK 그룹을 생성할 수 있습니다.

trunk <1-32> dynamic

다음 명령어를 사용하여 TRUNK 그룹을 삭제할 수 있습니다.

no trunk <trunk-id>

※ TRUNK 그룹 삭제 시, 해당 그룹에 포함된 멤버 포트가 없어야 합니다.

3.7.3. TRUNK 멤버 포트 설정

다음 명령어를 사용하여 interface configuration mode에서 TRUNK 그룹에 멤버 포트를 추가할 수 있습니다.

trunk interface IFNAME (passive|)

- IFNAME: TRUNK 그룹에 추가할 포트 이름
- 추가할 포트는 반드시 Layer 2 interface여야 합니다.
- 각 TRUNK 그룹에는 최대 8개의 Layer 2 interface를 추가할 수 있습니다.
- TRUNK 그룹이 static LACP trunk group인 경우, 추가된 인터페이스는 기본적으로 active 상태가 되며, 필요 시 passive 상태로 설정할 수 있습니다.

다음 명령어를 사용하여 TRUNK 그룹의 모든 멤버 포트를 제거할 수 있습니다.

no trunk interface

다음 명령어를 사용하여 TRUNK 그룹에서 지정한 멤버 포트를 제거할 수 있습니다.

no trunk interface <if-name>

이 명령어를 여러 번 실행하여 TRUNK 그룹에 포함된 여러 멤버 포트를 삭제할 수 있습니다.

3.7.4. TRUNK 로드밸런싱 정책 설정

다음 명령어를 사용하여 interface configuration mode에서 TRUNK의 로드밸런싱 정책을 설정할 수 있습니다.

trunk load-balance {dst-mac | dst-ip | src-dst-mac | src-dst-ip | src-mac | src-ip}

각 옵션의 의미는 다음과 같습니다.

- dst-mac → 목적지 MAC 기반 로드밸런싱
- dst-ip → 목적지 IP 기반 로드밸런싱
- src-dst-mac → 출발지 MAC + 목적지 MAC 기반 로드밸런싱
- src-dst-ip → 출발지 IP + 목적지 IP 기반 로드밸런싱
- src-mac → 출발지 MAC 기반 로드밸런싱
- src-ip → 출발지 IP 기반 로드밸런싱

다음 명령어를 사용하여 TRUNK 로드밸런싱 정책을 기본값으로 복원할 수 있습니다.

no trunk load-balance

기본 로드밸런싱 정책은 src-dst-mac (출발지 MAC + 목적지 MAC 기반)입니다.

3.7.5. TRUNK 정보 조회

다음 명령어를 사용하여 normal mode 또는 privileged mode에서 모든 TRUNK 정보를 확인할 수 있습니다.

show trunk

다음 명령어를 사용하여 특정 TRUNK 그룹의 설정 정보를 확인할 수 있습니다.

show trunk <trunk-id>

- <trunk-id>: 조회할 TRUNK 그룹의 ID 번호

3.8. Jumbo Frame 설정

3.8.1. Jumbo Frame 개요

포트가 Jumbo Frame을 수신할 수 있도록 하기 위해, 해당 포트에 특정 Jumbo Frame 길이를 지원하도록 설정할 수 있습니다.

3.8.2. Jumbo Frame 설정

포트가 더 큰 프레임(Jumbo Frame)을 처리할 수 있도록 프레임 크기를 설정할 수 있습니다.

config mode에서 포트 설정 모드로 진입한 후(예: interface ge1/1), 다음 명령어를 실행합니다.

Switch(config-ge1/1)# jumbo frame 2000

→ 해당 포트의 Jumbo Frame 크기를 2000 bytes로 설정

3.9. 이중화 포트(Redundant Port) 설정

특정 환경(예: 서버 안정성이 중요한 경우)에서는 스위치의 이중화 포트 기능을 사용하여 하나의 서버에 두 개의 포트를 연결할 수 있습니다.

이 기능은 동시에 하나의 포트만 LINK UP 상태로 유지되도록 하며, 현재 활성 포트에 장애(LINK DOWN)가 발생하면 다른 포트를 자동으로 활성화합니다.

이중화 포트 그룹에서의 상태 정의는 다음과 같습니다.

- Active 상태 → LINK UP 상태의 포트 (현재 사용 중인 포트)
- Disable 상태 → LINK DOWN 상태의 포트 (대기 상태 포트)

이 절에서는 이중화 포트 설정에 대해 설명하며, 주요 내용은 다음과 같습니다.

- 이중화 포트 설정
- 이중화 포트 정보 조회

3.9.1. 이중화 포트 설정

스위치는 최대 8개의 이중화 포트 그룹을 구성할 수 있으며, 각 그룹에는 2개의 포트만 포함될 수 있습니다.

또한 하나의 포트는 하나의 이중화 포트 그룹에만 속할 수 있습니다.

각 이중화 포트 그룹은 다음과 같이 구성됩니다.

- Primary Port (주 포트)
- Secondary Port (보조 포트)

동작 방식

이중화 포트 그룹이 활성화되면 다음과 같이 동작합니다.

1) 두 포트 모두 LINK UP 상태인 경우
   → Primary Port: Active 상태
   → Secondary Port: Disable 상태
2) 하나의 포트만 LINK UP 상태인 경우
   → LINK UP 상태의 포트: Active 상태
   → 나머지 포트: Disable 상태
3) 두 포트 모두 LINK DOWN 상태인 경우
   → 두 포트 모두 Disable 상태

Active 상태의 포트에서 LINK DOWN이 발생하면, 다른 포트가 자동으로 Active 상태로 전환됩니다.

Force-Switch 기능

Force-Switch는 다음 상황에서 동작합니다.

- Secondary Port가 Active 상태
- Primary Port가 Disable 상태

이때 Primary Port가 LINK UP 상태로 변경되면, Primary Port를 다시 Active 상태로 전환할지 여부를 결정합니다.

- force-switch 활성화 → Primary Port로 강제 전환
- force-switch 비활성화 → 현재 상태 유지

이중화 포트 관련 명령어

명령어	설명	CLI 모드
redundant-port <1-8> primary-port IFNAME secondary-port IFNAME [force-switch]	이중화 포트 그룹을 설정합니다. <1-8>: 그룹 번호 primary-port: 주 포트secondary-port: 보조 포트 [force-switch]: 강제 전환 옵션	Global Configuration Mode

명령어	설명	CLI 모드
redundant-port <1-8> force-switch	해당 이중화 포트 그룹의 force-switch 기능을 활성화합니다.	Global Configuration Mode
no redundant-port <1-8>	이중화 포트 그룹을 삭제합니다.	Global Configuration Mode
no redundant-port <1-8> force-switch	force-switch 기능을 비활성화합니다.	Global Configuration Mode

3.9.2. 이중화 포트 정보 조회

다음 명령어를 사용하여 시스템의 모든 이중화 포트 그룹 설정을 확인할 수 있습니다.

명령어	설명	CLI 모드
show redundant-port	시스템에 구성된 모든 이중화 포트 그룹의 설정 정보를 표시합니다.	Privileged Mode

3.10. UDLD 설정

UDLD(UDLD, Device Link Detection Protocol)는 광 케이블 또는 트위스트 페어로 연결된 이더넷 링크의 물리 상태를 모니터링하기 위한 Layer 2 프로토콜입니다.

링크가 단방향(Unidirectional) 상태가 될 경우(예: 한쪽은 송신 가능하지만 반대쪽은 수신 불가), UDLD는 이를 감지하여 해당 인터페이스를 비활성화하고 경고 메시지를 발생시킵니다.

이러한 단방향 링크는 특히 STP 환경에서 루프를 유발할 수 있어 매우 위험합니다.

※ UDLD는 정상 동작을 위해 링크 양쪽 장비 모두에서 지원 및 설정되어야 합니다.

UDLD 동작 모드

UDLD는 두 가지 동작 모드를 지원합니다.

1) Normal Mode (기본값)
   - 단방향 링크를 감지할 수 있음
   - 포트를 undetermined 상태로 표시하고 로그를 생성
   - 일정 시간 동안 링크 이상이 명확히 확인될 경우에만 포트를 shutdown

2) Aggressive Mode
   - 단방향 링크를 감지하면 링크 복구를 시도
   - 약 8초 동안 UDLD 메시지를 전송하며 응답을 대기
   - 응답이 없을 경우 포트를 errdisable 상태로 전환

UDLD 관련 명령어

명령어	설명	CLI 모드
udld enable	UDLD 기능을 전역(Global)으로 활성화합니다.	Global Configuration Mode
udld message time <time>	UDLD 메시지 전송 주기를 설정합니다.	Global Configuration Mode
udld port	해당 포트에서 UDLD 기능을 활성화합니다.	Interface Configuration Mode
udld aggressive	포트를 Aggressive 모드로 설정합니다. (기본: Normal Mode)	Interface Configuration Mode
show udld <if-name>	특정 포트의 UDLD 상태 정보를 조회합니다.	Privileged Mode

3.11. LLDP 설정

현재 네트워크 장비의 종류가 다양해지고 구성도 복잡해짐에 따라, 서로 다른 제조사의 장비 간에 상호 인식 및 시스템/구성 정보를 교환할 수 있는 표준 방식이 필요합니다.

LLDP(Link Layer Discovery Protocol)는 이러한 요구에 따라 정의된 프로토콜로, Layer 2 수준에서 인접 장비를 탐색하고 정보를 교환할 수 있는 표준 메커니즘을 제공합니다.

LLDP는 로컬 장비의 다음과 같은 정보를 TLV(Type/Length/Value) 형태로 구성합니다.

- 장비의 주요 기능(Capability)
- 관리 IP 주소
- 장비 식별자(Device ID)
- 인터페이스 식별자(Interface ID)

이 정보들은 LLDPDU(Link Layer Discovery Protocol Data Unit)로 캡슐화되어, 직접 연결된 인접 장비로 전송됩니다.

인접 장비는 수신한 정보를 표준 MIB(Management Information Base) 형태로 저장하며, 이를 통해 NMS(Network Management System)가 링크 상태 및 연결 정보를 조회하고 판단할 수 있습니다.

이 절에서는 LLDP 설정에 대해 설명하며, 주요 내용은 다음과 같습니다.

- LLDP 설정
- LLDP 정보 조회

3.11.1. LLDP 설정

LLDP 포트는 다음과 같은 4가지 동작 모드를 지원합니다.

- TxRx → LLDP 메시지 송신 및 수신
- Tx → LLDP 메시지 송신만 수행
- Rx → LLDP 메시지 수신만 수행
- Disable → LLDP 메시지 송수신 모두 비활성화

포트의 LLDP 동작 모드가 변경되면, 해당 포트는 프로토콜 상태 머신을 재초기화합니다.

동작 모드 변경이 빈번할 경우 지속적인 초기화가 발생할 수 있으므로, 이를 방지하기 위해 포트 초기화 지연 시간을 설정할 수 있으며, 모드 변경 후 일정 시간이 지난 뒤 초기화가 수행되도록 할 수 있습니다.

명령어	**설명**	**CLI 모드**
lldp global enable	LLDP 기능을 전역(Global)으로 활성화합니다.	Global Configuration Mode
lldp hold-multiplier <num>	LLDP TTL(Time To Live) 배수를 설정합니다.	Global Configuration Mode
lldp timer [<reinit-delay> <time>] [<tx-delay> <time>] [<tx-interval> <time>]	LLDP 관련 타이머 값을 설정합니다.	Global Configuration Mode
lldp enable	인터페이스에서 LLDP 기능을 활성화합니다.	Interface Configuration Mode
lldp admin-status {disable | rx | tx | rxtx}	포트의 LLDP 동작 모드를 설정합니다.	Interface Configuration Mode
lldp check-change-interval <time>	인터페이스 정보 갱신 주기를 설정합니다.	Interface Configuration Mode
lldp management-address <A.B.C.D>	LLDP에서 사용할 관리 IP 주소를 설정합니다.	Interface Configuration Mode
lldp tlv-enable {dot1-tlv | dot3-tlv | med-tlv}	LLDP 확장 TLV 기능(IEEE 802.1, 802.3, LLDP-MED)을 활성화합니다.	Interface Configuration Mode

3.11.2. LLDP 정보 조회

다음 명령어를 사용하여 LLDP 관련 설정 및 상태 정보를 확인할 수 있습니다.

명령어	설명	CLI 모드
show lldp configuration [ifname]	LLDP 설정 정보를 표시합니다.	Privileged Mode
show lldp local-information [ifname]	로컬 장비의 LLDP 정보를 표시합니다.	Privileged Mode
show lldp neighbor-information [ifname]	인접 장비(Neighbor)의 LLDP 정보를 표시합니다.	Privileged Mode
show lldp statistics [ifname]	LLDP 메시지 통계 정보를 표시합니다.	Privileged Mode
show lldp status [ifname]	LLDP 동작 상태 정보를 표시합니다.	Privileged Mode

4. 포트 기반 보안 설정

이 장에서는 포트 기반 MAC 보안 설정에 대해 설명하며, 주요 내용은 다음과 같습니다.

- 개요
- MAC 바인딩 설정
- MAC 필터링 설정
- 포트 MAC 학습 제한 설정
- 보호 포트 설정

4.1. 개요

포트 기반 MAC 보안은 Layer 2 forwarding의 보안 성능을 향상시키기 위해 다음 네 가지 기능을 제공합니다.

- MAC 바인딩
- MAC 필터링
- 포트 MAC 학습 제어
- 포트 보호

MAC 바인딩은 MAC 주소와 포트를 서로 연결하여, 특정 MAC 주소가 지정된 포트에서만 네트워크에 접근할 수 있도록 제한하는 기능입니다.

동시에 해당 포트는 바인딩된 MAC 주소만 네트워크 접근을 허용합니다. 하나의 포트에는 여러 개의 MAC 주소를 동시에 바인딩할 수 있습니다. MAC 바인딩은 802.1X와 함께 동일한 포트에 적용할 수 있습니다.

이 기능은 802.1X 기능을 지원하지 않거나 802.1X 사용이 적합하지 않은 장비에 유용합니다.

예: 프린터, 파일 서버 등

MAC 필터링은 특정 MAC 주소의 네트워크 접근을 차단하는 기능입니다.

주요 목적은 비인가 장비의 네트워크 접근을 방지하는 것입니다.

MAC 필터링으로 설정된 MAC 주소는 스위치의 어떤 포트에서도 네트워크에 접근할 수 없으며, 해당 MAC 주소를 목적지로 하는 패킷도 수신할 수 없습니다.

MAC 바인딩과 마찬가지로, 하나의 포트에는 여러 개의 MAC 주소 필터링 설정을 동시에 적용할 수 있습니다. 실제 환경에서 일부 악성 소프트웨어가 위조된 MAC 주소를 사용하여 네트워크를 공격하는 경우, ACL 외에도 MAC 필터링을 사용하여 위조 패킷의 접근 및 공격을 제어할 수 있습니다.

포트 MAC 학습 제어는 포트가 동적으로 학습할 수 있는 MAC 주소의 개수를 제한하는 기능입니다.

포트에 동적으로 학습 가능한 MAC 주소 개수를 지정하면, 해당 포트가 학습한 MAC 주소 수가 설정된 값에 도달했을 때 새로운 MAC 주소는 더 이상 학습되지 않습니다.

이후 새 MAC 주소와 관련된 패킷은 폐기됩니다.

※ 참고

여기서 말하는 MAC 주소는 실제로 MAC + VID를 의미합니다.

이후 본 장에서는 이를 반복해서 설명하지 않습니다. 또한 다음과 같은 설정 관계에 주의해야 합니다.

- MAC 바인딩 기능과 802.1X는 동일 포트에 동시에 설정할 수 있습니다.

- MAC 필터링과 포트 MAC 학습 제한은 동일 포트에 동시에 설정할 수 있습니다.
- MAC 바인딩, 802.1X, MAC 필터링, 포트 MAC 학습 제한을 모두 동일 포트에 동시에 설정할 수는 없습니다.

4.2. MAC 바인딩 설정

MAC 바인딩 설정은 수동(MANUAL)과 자동(AUTO) 두 가지 방식을 지원합니다.

- 수동 바인딩
  사용자가 MAC 주소와 포트를 직접 입력하여 바인딩
- 자동 바인딩
  포트의 Layer 2 하드웨어 포워딩 테이블(FDB)에 존재하는 MAC 정보를 읽어 자동으로 바인딩

※ Layer 2 테이블 조회 명령:

show bridge fdb

MAC 바인딩 관련 명령어

명령어	설명	CLI 모드
switchport-security mac-bind HHHH.HHHH.HHHH vlan <1-4094> qosprofile {qp0|qp1|qp2|qp3|qp4|qp5|qp6|qp7}	특정 MAC 주소를 인터페이스에 수동으로 바인딩하고, 해당 엔트리의 QoS 우선순위 큐를 설정합니다.	Interface Configuration Mode
switchport-security mac-bind auto-conversion number <1-8191> qosprofile {qp0|qp1|qp2|qp3|qp4|qp5|qp6|qp7}	인터페이스에서 학습된 MAC 주소 중 지정된 개수만큼을 자동으로 바인딩으로 변환하고, QoS 큐를 설정합니다.	Interface Configuration Mode
switchport-security mac-bind auto-conversion vlan <1-4094> qosprofile {qp0|qp1|qp2|qp3|qp4|qp5|qp6|qp7}	특정 VLAN의 MAC 주소를 자동으로 바인딩으로 변환하고, QoS 큐를 설정합니다.	Interface Configuration Mode
show port-security mac-bind [IFNAME]	MAC 바인딩 설정 정보를 조회합니다.	Privileged Mode

※ 주의사항

다음과 같은 경우 MAC 바인딩이 실패하거나 적용되지 않을 수 있습니다.

- 해당 포트에 802.1X가 이미 설정된 경우
- 해당 포트에 MAC 필터링 또는 포트 MAC 학습 제한이 설정된 경우
- 해당 MAC 주소가 다른 포트에 이미 바인딩되어 있거나 MAC 필터링으로 등록된 경우
- 스위치의 Layer 2 테이블(FDB)이 가득 찬 경우

4.3. MAC 필터링 설정

MAC 필터링 설정은 수동 설정과 자동 설정을 지원합니다.

- 수동 설정
  사용자가 차단할 MAC 주소와 적용할 포트를 직접 입력하여 설정
- 자동 설정
  포트의 Layer 2 하드웨어 포워딩 테이블(FDB)에 존재하는 MAC 정보를 읽어 자동으로 필터링 설정

※ Layer 2 테이블 조회 명령:

show bridge fdb

MAC 필터링 관련 명령어

명령어	설명	CLI 모드
switchport-security mac-filter HHHH.HHHH.HHHH vlan <1-4094>	특정 MAC 주소를 수동으로 필터링(차단) 설정합니다.	Interface Configuration Mode
switchport-security mac-filter auto-conversion number <1-8191>	인터페이스에서 학습된 MAC 주소 중 지정된 개수만큼을 자동으로 MAC 필터링으로 변환합니다.	Interface Configuration Mode
switchport-security mac-filter auto-conversion vlan <1-4094>	특정 VLAN의 MAC 주소를 자동으로 MAC 필터링으로 변환합니다.	Interface Configuration Mode
show port-security mac-filter [IFNAME]	MAC 필터링 설정 정보를 조회합니다.	Privileged Mode

※ 주의사항

다음과 같은 경우 MAC 필터링 설정이 적용되지 않거나 실패할 수 있습니다.

- 해당 포트에 MAC 바인딩 또는 802.1X 기능이 이미 설정된 경우
- 해당 MAC 주소가 다른 포트에 이미 바인딩되어 있거나 MAC 바인딩으로 등록된 경우
- 스위치의 Layer 2 테이블(FDB)이 가득 찬 경우

4.4. 포트 MAC 학습 제한 설정

스위치는 포트별로 동적으로 학습할 수 있는 MAC 주소의 최대 개수를 설정할 수 있습니다.

포트에 학습 제한을 설정하면, 지정된 개수만큼만 MAC 주소를 학습하며, 해당 개수를 초과할 경우 새로운 MAC 주소는 학습되지 않고 해당 트래픽은 전달되지 않습니다.

학습 제한을 설정하지 않은 경우, 하나의 포트는 최대 8191개의 MAC 주소를 학습할 수 있습니다.

명령어	**설명**	**CLI 모드**
switchport port-security learn-limit <0-8191>	인터페이스가 학습할 수 있는 MAC 주소 개수를 설정합니다.	Interface Configuration Mode
no switchport port-security learn-limit	MAC 주소 학습 제한 설정을 해제합니다.	Interface Configuration Mode
show port-security learn-limit [IFNAME]	포트 MAC 학습 제한 설정 정보를 조회합니다.	Privileged Mode

설정 예시

포트 ge1/5에서 최대 7개의 MAC 주소만 학습하도록 설정하는 경우:

Switch# configure terminal

Switch(config)# interface ge1/5

Switch(config-ge1/5)# switchport port-security learn-limit 7

※ 주의사항

다음과 같은 경우 설정이 적용되지 않거나 실패할 수 있습니다.

- 해당 포트에 MAC 바인딩 또는 802.1X 기능이 이미 설정된 경우

4.5. 보호 포트 설정

4.5.1. 보호 포트 개요

Layer 2에서 포트 간 트래픽을 격리하려면 일반적으로 VLAN을 분리해야 하지만, 이 경우 VLAN 자원이 불필

요하게 많이 사용될 수 있습니다.

보호 포트(Protected Port)를 사용하면 동일 VLAN 내에서도 포트 간 통신을 차단할 수 있어, 보다 효율적이고 유연한 네트워크 구성이 가능합니다.

각 포트는 보호 포트로 설정할 수 있으며, 보호 포트 간에는 서로 통신할 수 없습니다.

다만 보호 포트는 비보호 포트(Unprotected Port)와는 통신이 가능합니다.

주요 동작 방식

- 보호 포트 ↔ 보호 포트 → 통신 불가
- 보호 포트 ↔ 비보호 포트 → 통신 가능

적용 예시

1) 단일 허브 포트 구성
   하나의 포트만 비보호 포트로 설정하고, 나머지 모든 포트를 보호 포트로 설정
   → 모든 포트 간 통신 차단 + 중앙 포트만 통신 허용
2) 보안 강화 구성 (스니핑 방지)
   서버와 연결되지 않은 사용자 포트를 보호 포트로 설정
   → 사용자 간 트래픽 차단 → 패킷 스니핑 방지

4.5.2. 보호 포트 설정

포트를 보호 포트로 설정하면 동일 VLAN 내에서도 포트 간 통신을 차단할 수 있습니다.

config mode에서 인터페이스 설정 모드로 진입한 후(예: interface ge1/1), 다음 명령어를 실행합니다.

```
Switch(config-ge1/1)# switchport port-security protect
```

보호 포트 설정 조회

다음 명령어를 사용하여 보호 포트 설정 상태를 확인할 수 있습니다.

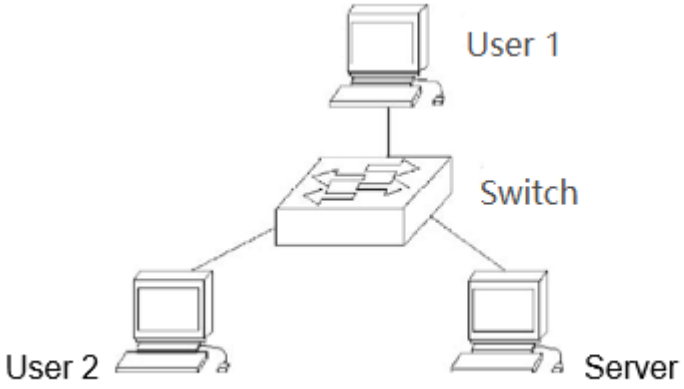
```
Switch# show port-security protect
```

출력 예시:

Port Port protected

----- --------------

ge1/1 ON



설정 절차

Switch> enable

Switch# configure terminal

Switch(config)# interface ge1/1

Switch(config-ge1/1)# switchport port-security protect

Switch(config-ge1/1)# interface ge1/2

Switch(config-ge1/2)# switchport port-security protect

Switch(config-ge1/2)# exit

Switch(config)# exit

설정 결과 확인

Switch# show port-security protect

Port Port protected

----- --------------

ge1/1 ON

ge1/2 ON

5. 포트 IP 및 MAC 바인딩 설정

이 장에서는 포트 기반 IP + MAC 바인딩 설정에 대해 설명하며, 주요 내용은 다음과 같습니다.

- 개요
- IP 및 MAC 바인딩 설정
- 설정 예시
- 설정 문제 해결

5.1. 개요

Layer 2 스위치 포트에 IP 및 MAC 바인딩을 설정하는 것은 ARP 공격을 방어하기 위한 정적 보안 방식입니다.

ARP 공격자는 위조된 MAC 주소가 포함된 ARP 패킷을 전송하여 사용자를 공격합니다.

이로 인해 사용자의 로컬 ARP cache table이 공격자의 MAC 주소로 갱신될 수 있으며, 정상적인 데이터 트래픽이 공격자에게 전달될 수 있습니다.

스위치 포트 설정에서 사용자 IP 주소와 MAC 주소를 정적으로 바인딩하면, 이러한 ARP 공격 패킷을 효과적으로 필터링할 수 있습니다.

IP MAC 바인딩 기능은 ARP Spoofing 방지 기능 외에도, IP와 MAC 간의 1:1 매핑 관계를 보장합니다.

즉,

- 하나의 IP는 하나의 MAC 주소에만 대응 가능
- 하나의 MAC 주소는 하나의 IP에만 대응 가능

합니다.

접속 장비가 이 매핑 관계를 변경할 경우, 해당 장비는 네트워크에서 정상적으로 통신할 수 없습니다.

802.1X anti-ARP spoofing 기능과 DHCP Snooping 프로토콜은 이 기능을 동적으로 구현하는 방식입니다.

IP MAC Binding, ACL, 802.1X anti-ARP spoofing, DHCP Snooping 기능은 모두 동일한 시스템 하드웨어 리소스인 CFP를 사용합니다.

따라서 설정 시 CFP 리소스가 고갈되지 않았는지 주의해야 합니다.

설계상 각 기능 간 호환 관계는 다음과 같습니다.

기능	**IP MAC Binding**	**ACL**	**802.1X**	**DHCP Snooping**
IP MAC Binding	Compatible	Incompatible	Compatible	Compatible
ACL	Incompatible	Compatible	Incompatible	Incompatible
802.1X	Compatible	Incompatible	Compatible	Incompatible
DHCP Snooping	Compatible	Incompatible	Incompatible	Compatible

CFP는 제한된 하드웨어 리소스이며, 각 포트에는 평균적으로 최대 16개의 IP MAC 바인딩 엔트리만 설정할 수 있습니다.

따라서 다수의 접속 호스트가 있는 네트워크에서 일부 포트 또는 일부 IP/MAC 주소만 제어해야 하는 경우에는 정적 IP MAC 바인딩 기능을 사용하는 것이 적합합니다.

이를 통해 CFP 리소스 고갈로 인해 데이터 forwarding이 실패하는 상황을 방지할 수 있습니다.

또한 802.1X 또는 DHCP Snooping 프로토콜 사용 여부는 현재 네트워크 환경에 따라 결정해야 합니다.

- 정적 IP 주소를 사용하고 802.1X 인증을 통해 네트워크에 접속하는 경우
  → 802.1X anti-ARP spoofing 기능을 사용해야 효과적입니다.

- 동적 IP 주소 할당을 사용하는 경우
  → DHCP Snooping 프로토콜을 사용하는 것이 적합합니다.

5.2. IP 및 MAC 바인딩 설정

IP와 MAC 바인딩은 interface configuration mode에서 설정합니다.

IP/MAC 바인딩 설정

포트에 IP와 MAC 주소를 바인딩하는 명령어는 다음과 같습니다.

Switch# configure terminal

Switch(config)# interface ge1/1

Switch(config-ge1/1)# ip mac-bind A.B.C.D MAC

- A.B.C.D → 바인딩할 IP 주소
- MAC → 바인딩할 MAC 주소

IP/MAC 바인딩 해제

포트에 설정된 IP/MAC 바인딩을 삭제하려면 다음 명령어를 사용합니다.

Switch# configure terminal

Switch(config)# interface ge1/1

Switch(config-ge1/1)# no ip mac-bind A.B.C.D MAC

설정 정보 조회

모든 포트의 바인딩 정보 조회

show ip mac-bind

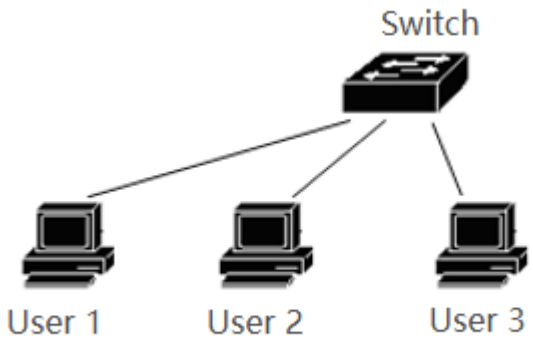
특정 포트의 바인딩 정보 조회

show ip mac-bind IFNAME

IFNAME → 조회할 인터페이스 이름 (예: ge1/1)

5.3. 설정 예시

네트워크에 User 1, User 2, User 3이 있으며, ARP 공격을 방어하기 위해 각 사용자의 IP 주소와 MAC 주소를 해당 포트에 바인딩하는 예시입니다.



Switch# configure terminal

Switch(config)# interface ge1/1

Switch(config-ge1/1)# ip mac-bind 192.168.1.100 5491.afxx.xxx1

Switch(config-ge1/1)# interface ge1/2

Switch(config-ge1/2)# ip mac-bind 192.168.1.101 0011.6452.135d

Switch(config-ge1/2)# interface ge1/3

Switch(config-ge1/3)# ip mac-bind 192.168.1.102 0011.804d.a246

Switch(config-ge1/3)# end

설정 확인

Switch# show ip mac-bind

[ge1/1] sum: 1

MAC IP

5491.afxx.xxx1 192.168.1.100

[ge1/2] sum: 1

MAC IP

5491.afxx.xxx2 192.168.1.101

[ge1/3] sum: 1

MAC IP

5491.afxx.xxx3 192.168.1.102

특정 포트 확인

Switch# show ip mac-bind ge1/1

[ge1/1] sum: 1

MAC IP

5491.afxx.xxx1 192.168.1.100

Running Configuration 확인

Switch# show running-config

!

spanning-tree mst configuration

!

interface vlan1

ip address 10.10.10.1/24

!

interface ge1/1

ip mac-bind 192.168.1.100 5491.afxx.xxx1

!

interface ge1/2

ip mac-bind 192.168.1.101 5491.afxx.xxx2

!

interface ge1/3

ip mac-bind 192.168.1.102 5491.afxx.xxx3

!

line vty

!

end

이 예시에서는 각 사용자의 IP/MAC 정보를 해당 포트에 고정하여, 다른 MAC 또는 IP 조합으로는 정상 통신이 되지 않도록 구성합니다.

5.4. 설정 문제 해결 (Configuration Troubleshooting)

IP/MAC 바인딩 설정이 실패하는 경우, 다음과 같은 원인을 점검해야 합니다.

1) CFP 리소스 부족
   IP/MAC 바인딩은 하드웨어 리소스인 CFP를 사용합니다.
   CFP 자원이 모두 사용된 경우, 추가 바인딩 설정이 적용되지 않습니다.
2) 인터페이스에 ACL이 이미 적용된 경우
   해당 포트에 ACL 필터링이 설정되어 있으면, IP/MAC 바인딩과 충돌하여 설정이 실패할 수 있습니다.
3) Layer 3 인터페이스 또는 TRUNK 포트인 경우
   IP/MAC 바인딩은 Layer 2 Access 포트에서만 적용 가능합니다.
   따라서 다음과 같은 인터페이스에서는 설정이 불가능합니다.
   - Layer 3 인터페이스 (SVI 또는 routed port)
   - TRUNK 포트

6. 포트 루프 감지 (Port Loop Detection)

이 장에서는 포트 루프 감지 기능에 대해 설명하며, 주요 내용은 다음과 같습니다.

- 개요
- 프로토콜 동작 원리
- 설정 방법

6.1. 개요

스위치의 특정 포트 하위에서 루프가 발생하면, 해당 포트에서 Broadcast Storm이 발생할 수 있습니다.

이 경우 모든 Broadcast 패킷의 Source MAC 주소가 루프가 발생한 포트로 학습되어, 장비의 정상적인 forwarding 동작에 문제가 발생할 수 있습니다.

6.2. 프로토콜 동작 원리

ELD(Ethernet Loopback Detection) 프로토콜은 데이터 패킷 교환을 통해 루프 발생 여부를 감지하고, 루프가 발생한 포트를 차단할 수 있습니다.

ELD 프로토콜은 포트 기반 프로토콜이므로, 해당 포트에서 발생한 루프만 감지할 수 있습니다.

6.2.1. 루프 감지 동작 과정

포트에서 ELD(Ethernet Loopback Detection) 기능을 활성화하면, 해당 포트에서 타이머가 동작하며 주기적으로 루프 감지 패킷을 전송합니다.

이때, 자신이 전송한 루프 감지 패킷을 일정 시간 내에 다시 수신하게 되면, 해당 포트에 루프가 존재한다고 판단합니다.

루프가 감지되면 다음과 같은 동작이 수행됩니다.

- 해당 포트를 차단(Block)
- 포트의 FDB(Forwarding Database) 테이블 초기화

포트가 여러 VLAN에 속한 경우, 해당 포트는 모든 VLAN에 대해 루프 감지 패킷을 전송합니다.

즉, 하나의 포트에서 속한 모든 VLAN에 대해 루프 여부를 자동으로 검사합니다.

6.2.2. 복구 모드 (Recovery Mode)

앞서 설명한 것처럼 포트에서 루프가 발생하면 해당 포트는 차단(Block)됩니다.

ELD 프로토콜은 차단된 포트를 복구하기 위해 두 가지 복구 방식을 제공합니다.

1) 자동 복구 (Automatic Recovery)
   포트가 차단되면 ELD는 복구 타이머를 동작시킵니다.
   타이머가 만료되면 다음 동작이 수행됩니다.
   - 포트 차단 상태 해제 (Unblock)
   - 해당 포트에서 다시 루프 감지 기능 활성화

   즉, 일정 시간이 지나면 자동으로 포트를 복구하고 다시 정상 동작을 시도합니다.
2) 수동 복구 (Manual Recovery)
   포트가 차단된 이후에는 자동 복구 타이머가 동작하지 않습니다.
   따라서 관리자가 직접 명령어를 입력하여 포트 차단을 해제해야 합니다.

6.2.3. 프로토콜 보안 (Protocol Security)

ELD 프로토콜은 네트워크 환경에서 공격에 취약할 수 있습니다.

공격자가 ELD 패킷 형식을 모방하여 포트로 전송할 경우, 실제 루프가 없더라도 포트가 차단되는 오동작이 발생할 수 있습니다.

이러한 문제를 방지하기 위해 ELD는 두 가지 보안 전략을 제공합니다.

1) 키 기반 패킷 보호
ELD는 비대화형(Non-interactive) 프로토콜로, 다른 장비에 의존하지 않고 동작합니다.
이를 기반으로 ELD 패킷에 인증 키(Key)를 포함하여 전송함으로써,
해당 키를 모르는 사용자는 ELD 패킷을 위조할 수 없도록 합니다.

2) 패킷 재전송(Replay) 공격 방지
공격자가 패킷 캡처 후 재전송하는 공격을 방지하기 위해,
일정 시간 동안 수신되는 패킷의 형식 및 조건을 검사하도록 설정할 수 있습니다.
이 기능은 사용자가 별도로 설정해야 하며, 이를 통해 잘못된 루프 감지로 인한 오동작을 최소화할 수 있습니다.

6.3. 설정 개요 (Configuration Introduction)

6.3.1. 전역 설정 (Global Configuration)

명령어	설명	CLI 모드
loop-detection detection-time <1-65535>	루프 감지 주기를 설정합니다.복구 시간의 절반 이하로 설정해야 합니다.(기본값: 5초)	Global Configuration Mode
loop-detection resume-time <10-65535>	자동 복구 시간 주기를 설정합니다.감지 주기의 2배 이상이어야 합니다.(기본값: 600초)	Global Configuration Mode
loop-detection protocol-safety	프로토콜 보안 기능을 활성화합니다.(기본값: 비활성화)	Global Configuration Mode
loop-detection respond-packets	일정 시간 동안 수신해야 하는 패킷 수를 설정합니다.프로토콜 보안 활성화 시 적용됩니다.(기본값: 10)	Global Configuration Mode

6.3.2. 인터페이스 설정 (Interface Configuration)

인터페이스 설정은 각 포트별로 ELD 기능을 적용하는 설정입니다.

명령어	설명	CLI 모드
loop-detection enable	해당 포트에서 ELD 기능을 활성화합니다.	Interface Configuration Mode

명령어	설명	CLI 모드
loop-detection resume	수동으로 포트를 복구하고 루프 감지를 다시 시작합니다.	Interface Configuration Mode
loop-detection resume-mode {automation | manual}	복구 모드를 설정합니다.자동(automatic) 또는 수동(manual) 선택(기본값: automatic)	Interface Configuration Mode
loopback-detection shutdown-mode {no-shutdown | shutdown}	루프 발생 시 포트를 shutdown할지 여부를 설정합니다.	Interface Configuration Mode

6.3.3. 설정 조회 (Display Configuration)

다음 명령어를 사용하여 ELD(Loop Detection) 설정 정보를 확인할 수 있습니다.

show loop-detection [ifname]

동작 설명

- 전체 설정 조회
  인터페이스를 지정하지 않으면, 시스템 전체 ELD 설정 정보를 표시합니다.
- 특정 포트 조회
  [ifname]을 지정하면, 해당 인터페이스의 ELD 설정 정보만 표시합니다.
  (예: ge1/1)

7. VLAN 설정

VLAN은 스위치에서 매우 중요한 개념으로, 실제 네트워크 환경에서 광범위하게 사용됩니다.

여러 네트워크를 내부적으로 논리적으로 분리하는 기본 기술입니다.

VLAN(Virtual Local Area Network)은 물리적 위치와 관계없이 여러 장비를 하나의 논리적 네트워크로 구성하는 방식입니다.

각 VLAN은 하나의 독립된 논리 네트워크로, 기존의 물리적 네트워크와 동일한 특성과 동작을 가집니다.

VLAN의 주요 특징

- 각 VLAN은 하나의 Broadcast Domain입니다.
- Broadcast 패킷은 동일 VLAN 내에서만 전달되며, VLAN 간에는 전달되지 않습니다.
- VLAN 간 통신은 반드시 Layer 3 장비(라우터 또는 L3 스위치)를 통해 이루어집니다.

이 장에서는 VLAN 설정에 대해 설명하며, 주요 내용은 다음과 같습니다.

- VLAN 개요
- VLAN 설정
- VLAN 설정 예시

7.1. VLAN 개요

이 절에서는 VLAN에 대해 자세히 설명하며, 주요 내용은 다음과 같습니다.

- VLAN의 장점
- VLAN ID
- VLAN 포트 멤버십 유형
- 포트의 기본 VLAN (Default VLAN)
- 포트의 VLAN 모드
- VLAN Trunk
- VLAN 내부 트래픽 전달 방식
- VLAN 서브넷 구성

7.1.1. VLAN의 장점

VLAN은 물리 네트워크의 확장성을 크게 향상시킵니다.

기존의 물리 네트워크는 규모가 제한적이며, 수용 가능한 장비 수가 많아야 수천 대 수준입니다.

반면 VLAN으로 분리된 물리 네트워크는 수만 대 또는 수십만 대의 장비까지 수용할 수 있습니다.

VLAN은 기존 물리 네트워크와 동일한 기능과 특성을 가지면서도, 논리적으로 네트워크를 분리할 수 있습니다.

VLAN을 사용하면 다음과 같은 장점이 있습니다.

1) 네트워크 트래픽을 효과적으로 제어할 수 있음
   기존 네트워크에서는 Broadcast 패킷이 필요 여부와 관계없이 모든 장비로 전달됩니다.
   이로 인해 네트워크와 장비의 부하가 증가할 수 있습니다.

   VLAN은 장비를 필요에 따라 논리적인 네트워크 단위로 구성할 수 있습니다.
   하나의 VLAN은 하나의 Broadcast Domain이며, Broadcast 패킷은 해당 VLAN 내부에서만 전달되고 다른 VLAN으로는 전달되지 않습니다.

   따라서 VLAN을 분리하면 네트워크 트래픽을 효과적으로 제어할 수 있습니다.

2) 네트워크 보안을 향상시킬 수 있음
VLAN에 속한 장비는 동일 VLAN 내 장비와만 Layer 2 통신을 수행할 수 있습니다.

다른 VLAN과 통신하려면 반드시 Layer 3 forwarding이 필요합니다.
VLAN 간 Layer 3 forwarding이 구성되어 있지 않으면 VLAN 간 통신은 불가능합니다.

이러한 특성을 통해 VLAN은 네트워크를 격리하고, 각 VLAN의 데이터 보안을 강화할 수 있습니다.

예를 들어, 회사의 R&D 부서와 마케팅 부서가 데이터를 서로 공유하지 않아야 하는 경우,
R&D 부서용 VLAN과 마케팅 부서용 VLAN을 각각 구성하고 두 VLAN 간 Layer 3 통신 경로를 만들지 않으면 됩니다.

3) 장비 이동성을 높일 수 있음
기존 네트워크에서는 장비가 한 위치에서 다른 위치로 이동하면서 다른 네트워크에 속하게 되는 경우,
해당 장비의 네트워크 설정을 변경해야 하므로 사용자에게 불편이 발생합니다.

VLAN은 논리 네트워크이기 때문에 물리적으로 서로 다른 위치에 있는 장비도 동일한 VLAN에 포함시킬 수 있습니다.

따라서 장비가 이동하더라도 동일 VLAN에 속하도록 설정하면,
장비의 네트워크 설정을 변경하지 않고도 기존과 동일하게 사용할 수 있습니다.

7.1.2. VLAN ID

각 VLAN에는 이를 식별하기 위한 VLAN ID가 존재합니다.

VLAN ID의 범위는 0 ~ 4095이며, 이 중 실제 사용 가능한 값은 1 ~ 4094입니다.

(0과 4095는 예약되어 사용되지 않음)

VLAN ID는 각 VLAN을 유일하게 식별하는 역할을 합니다.

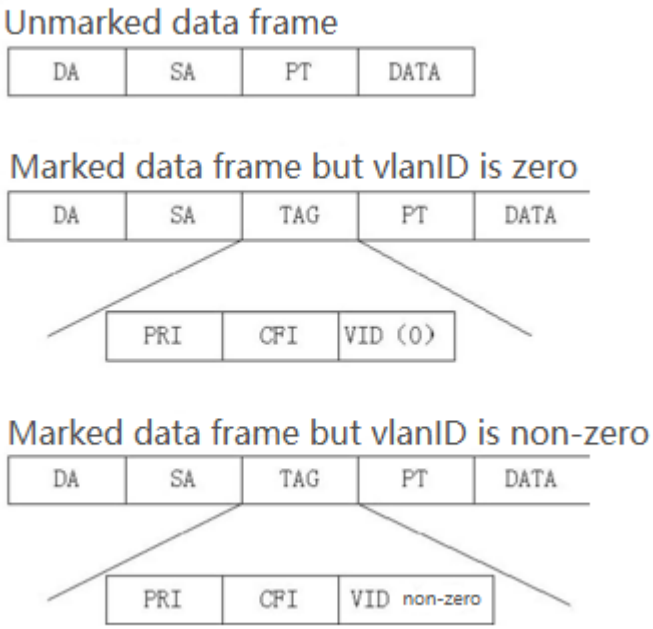
VLAN 생성 및 기본 VLAN

- 스위치는 최대 4094개의 VLAN을 지원합니다.
- VLAN 생성 시 사용할 수 있는 ID 범위는 2 ~ 4094입니다.
- VLAN 1은 기본(Default VLAN)으로 자동 생성되며, 삭제할 수 없습니다.

VLAN 내 데이터 프레임 유형

VLAN 환경에서 전송되는 데이터 프레임은 다음 세 가지 유형으로 구분됩니다.

- Untagged Frame
  → VLAN 태그가 없는 일반 이더넷 프레임
- VID = 0인 Tagged Frame
  → VLAN ID는 없지만, QoS 정보(802.1p)를 포함하는 프레임
- VID ≠ 0인 Tagged Frame
  → 실제 VLAN ID를 포함하는 프레임 (일반적인 VLAN 트래픽)



스위치 내부 프레임 처리 방식

스위치 내부에서는 모든 데이터 프레임이 Tagged 상태로 처리됩니다.

프레임이 스위치로 유입될 때 처리 방식은 다음과 같습니다.

1) Untagged 프레임 입력 시
   → 스위치는 해당 프레임에 VLAN 태그를 추가합니다.
   → 이때 포트의 기본 VLAN(PVID) 값을 VID로 설정합니다.
2) VID = 0인 Tagged 프레임 입력 시
   → 스위치는 VLAN ID를 새로 할당하여 VID 값을 설정합니다.
   → 이 경우에도 일반적으로 포트의 PVID가 적용됩니다.
   ※ VID 0은 VLAN 정보가 아닌 QoS 정보만 포함하는 특수 케이스입니다.
3) ID ≠ 0인 Tagged 프레임 입력 시
   → 프레임은 변경 없이 그대로 처리됩니다.

7.1.3. VLAN 포트 멤버십 유형

스위치는 포트 기반 VLAN과 802.1Q 기반 VLAN을 지원합니다.

하나의 VLAN은 다음 두 가지 유형의 포트 멤버로 구성될 수 있습니다.

- Untagged 포트
- Tagged 포트

하나의 VLAN에는 Untagged와 Tagged 포트가 함께 포함될 수 있습니다.

VLAN과 포트 관계

- 하나의 VLAN은
  → 포트가 없을 수도 있고
  → 하나 이상의 포트를 포함할 수도 있습니다.
- 포트가 VLAN에 속할 때, 해당 포트는
  → Untagged 멤버 또는
  → Tagged 멤버로 동작합니다.

포트 멤버십 특징

- 하나의 포트는 여러 VLAN에 속할 수 있습니다.
- 포트가 두 개 이상의 VLAN에서 Tagged 멤버로 동작하면
  → 해당 포트는 Trunk 포트라고 합니다.
- 하나의 포트는
  → 일부 VLAN에서는 Untagged 멤버
  → 다른 VLAN에서는 Tagged 멤버로 동시에 동작할 수 있습니다.

7.1.4. 포트의 기본 VLAN (PVID)

각 포트는 하나의 기본 VLAN(Default VLAN)만 가질 수 있으며, 이를 PVID(Port VLAN ID)라고 합니다.

PVID는 다음과 같은 경우에 VLAN을 결정하는 기준으로 사용됩니다.

- Untagged 프레임이 포트로 유입될 때
- VID = 0인 Tagged 프레임이 유입될 때

이 경우, 해당 프레임은 포트의 PVID 값을 기준으로 VLAN이 지정됩니다.

기본적으로 모든 포트의 PVID는 VLAN 1로 설정되어 있습니다.

7.1.5. 포트의 VLAN 모드

포트는 VLAN 설정 시 다음 세 가지 모드를 지원합니다.

- ACCESS 모드
- TRUNK 모드
- HYBRID 모드

포트에 VLAN을 설정하기 전에 반드시 해당 포트의 VLAN 모드를 먼저 지정해야 합니다.

1) ACCESS 모드
   ACCESS 포트는 사용자 단말과 직접 연결되는 포트입니다.
   - 하나의 VLAN에만 속할 수 있음
   - 해당 VLAN의 Untagged 멤버로 동작
   - PVID = 해당 VLAN (사용자가 지정)

   즉, 일반 PC, 프린터, 서버 연결 포트에 사용
2) TRUNK 모드
   TRUNK 포트는 스위치 간 연결(Uplink)에 사용됩니다.
   - 하나 이상의 VLAN에 속할 수 있음
   - 모든 VLAN이 Tagged 멤버로 동작
   - Untagged VLAN 없음
   - 기본 VLAN(PVID)은 VLAN 1 (변경 불가)

   스위치 ↔ 스위치, 스위치 ↔ L3 장비 연결에 사용
3) HYBRID 모드
   HYBRID 포트는 TRUNK와 유사하지만 더 유연한 구조를 가집니다.
   - 여러 VLAN에 속할 수 있음
   - VLAN별로 Tagged 또는 Untagged 설정 가능
   - PVID 변경 가능

   Access + Trunk 혼합 형태 (특정 장비, IP Phone 환경 등)

모드	**VLAN 개수**	**Tagged**	**Untagged**	**PVID 변경**
ACCESS	1개	X	O	가능
TRUNK	여러 개	O	X	불가 (VLAN 1 고정)
HYBRID	여러 개	O	O	가능

7.1.6. VLAN Trunk

두 개 이상의 VLAN에서 Tagged 멤버로 동작하는 포트를 VLAN Trunk 포트라고 합니다.

Trunk 포트를 통해 스위치 간 연결을 구성하면, 여러 VLAN을 하나의 물리 링크로 동시에 전달할 수 있습니다.

동작 개념

- Trunk 포트는 여러 VLAN 트래픽을 Tagging(802.1Q)하여 전달합니다.
- 서로 다른 스위치 간에도 동일한 VLAN을 확장할 수 있습니다.
- 하나의 링크로 여러 VLAN을 전달하므로 효율적인 네트워크 구성이 가능합니다.

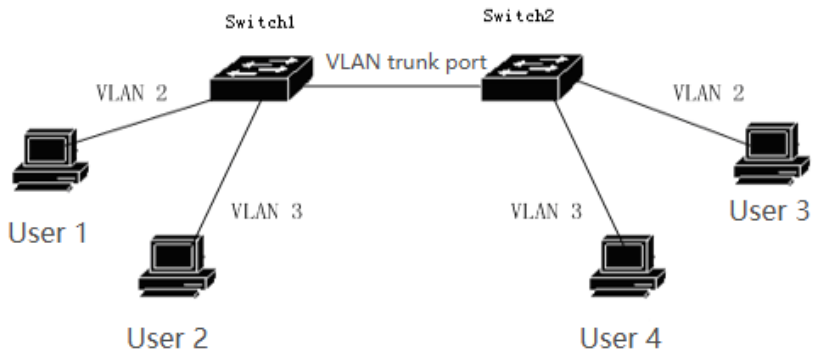
동작 예시

두 개의 스위치가 Trunk 포트로 연결되어 있고, 각 스위치에 VLAN 2와 VLAN 3이 구성되어 있다고 가정합니다.

- VLAN 2: User1 ↔ User3 → 통신 가능
- VLAN 3: User2 ↔ User4 → 통신 가능
- VLAN 2 ↔ VLAN 3 간 → 통신 불가 (L3 필요)

즉,

- 같은 VLAN끼리는 다른 스위치에 있어도 통신 가능
- 다른 VLAN끼리는 같은 스위치에 있어도 통신 불가



7.1.7. VLAN 내 트래픽 전달 방식 (Forwarding of Traffic within a VLAN)

스위치는 포트로 패킷을 수신하면 다음 절차에 따라 Layer 2 forwarding을 수행합니다.

전체 처리 흐름

- 패킷이 속한 VLAN 결정
- 패킷 유형 판단 (Broadcast / Multicast / Unicast)
- 출력 포트 결정
- 출력 시 Tagging 여부 결정

- 패킷 전송

1) VLAN 결정 방식
   패킷이 어떤 VLAN에 속하는지는 다음 기준으로 판단합니다.
   - Tagged 프레임 (VID ≠ 0)
     → 태그에 포함된 VID 값이 해당 VLAN
   - Untagged 또는 VID = 0 프레임
     → 포트의 PVID가 해당 VLAN
2) 패킷 유형 판단
   - Broadcast
     → 목적지 MAC: FF:FF:FF:FF:FF:FF
   - Multicast
     → Broadcast가 아니고, 목적지 MAC의 특정 비트(멀티캐스트 비트)가 1
   - Unicast
     → 위 두 가지가 아닌 경우
3) 출력 포트 결정
   Broadcast 패킷
   → 해당 VLAN의 모든 멤버 포트로 전송
   Multicast 패킷
   - L2 Multicast 테이블 조회
     → 매칭되면 해당 포트로 전달
   - 매칭 없을 경우
     Unregistered 모드 → Broadcast처럼 처리
     Registered 모드 → Drop
   Unicast 패킷
   - MAC 테이블 조회
     → 매칭되면 해당 포트로 전달
   - 매칭 없을 경우 (Unknown Unicast)
     → Broadcast처럼 Flooding
4) 출력 시 Tag 처리
   출력 포트의 VLAN 멤버십에 따라 Tag 여부 결정
   - Untagged 포트
     → Tag 제거 후 전송
   - Tagged 포트
     → VLAN Tag 유지 후 전송 (VID 포함)

핵심 요약

- VLAN 기준으로 forwarding 수행
- MAC 테이블 기반으로 포트 결정

- Unknown 트래픽은 Flooding
- Tagged / Untagged 처리로 VLAN 유지

7.2. VLAN 설정

이 절에서는 VLAN 설정 방법을 상세히 설명하며, 주요 내용은 다음과 같습니다.

- VLAN 생성 및 삭제
- 포트 VLAN 모드 설정
- ACCESS 모드 VLAN 설정
- TRUNK 모드 VLAN 설정
- HYBRID 모드 VLAN 설정
- VLAN 서브넷 설정
- VLAN 정보 조회

7.2.1. VLAN 생성 및 삭제

VLAN을 생성하거나 삭제하기 위해서는 먼저 Global Configuration Mode에서 VLAN 설정 모드로 진입해야 합니다.

스위치는 기본적으로 VLAN 1이 생성되어 있으며, VLAN 1은 삭제할 수 없습니다.

VLAN 생성 / 삭제 명령어

명령어	설명	CLI 모드
vlan <vlan-id>	VLAN을 생성합니다. 이미 존재하는 경우 아무 동작도 하지 않습니다.(범위: 2 ~ 4094)	VLAN Configuration Mode
no vlan <vlan-id>	VLAN을 삭제합니다. 존재하지 않는 경우 아무 동작도 하지 않습니다.(범위: 2 ~ 4094)	VLAN Configuration Mode

7.2.2. 포트의 VLAN 모드 설정

포트에 VLAN을 설정하기 전에 먼저 포트의 VLAN 모드를 지정해야 합니다.

기본값은 ACCESS 모드입니다.

VLAN 모드 설정 명령어

명령어	설명	CLI 모드
switchport mode access	포트를 ACCESS 모드로 설정합니다. 실행 시 VLAN 1의 Untagged 멤버가 되며, PVID는 1입니다.	Interface Configuration Mode
switchport mode trunk	포트를 TRUNK 모드로 설정합니다. 실행 시 VLAN 1의 Tagged 멤버가 되며, PVID는 1입니다.	Interface Configuration Mode
no switchport trunk	TRUNK 모드를 해제하고 기본값인 ACCESS 모드로 복귀합니다.	Interface Configuration Mode
switchport mode hybrid	포트를 HYBRID 모드로 설정합니다. 실행 시 VLAN 1의 Untagged 멤버가 되며, PVID는 1입니다.	Interface Configuration Mode
no switchport hybrid	HYBRID 모드를 해제하고 기본값인 ACCESS 모드로 복귀합니다.	Interface Configuration Mode

7.2.3. ACCESS 모드에서 VLAN 설정

포트의 VLAN을 설정하기 전에 해당 포트를 ACCESS 모드로 지정해야 합니다.

ACCESS 모드에서는 포트가 기본적으로 VLAN 1의 Untagged 멤버이며, PVID는 1입니다.

ACCESS 모드 VLAN 설정 명령어

명령어	설명	CLI 모드
switchport access vlan <vlan-id>	포트를 지정한 VLAN의 Untagged 멤버로 설정합니다. 동시에 포트의 PVID도 해당 VLAN으로 변경됩니다.(범위: 2 ~ 4094)	Interface Configuration Mode
no switchport access vlan	포트 VLAN 설정을 초기화합니다. VLAN 1의 Untagged 멤버로 복귀하며, PVID도 1로 설정됩니다.	Interface Configuration Mode

7.2.4. TRUNK 모드에서 VLAN 설정

포트를 TRUNK 모드로 설정한 후 VLAN을 구성해야 합니다.

TRUNK 모드에서는 포트가 기본적으로 VLAN 1의 Tagged 멤버이며, 기본 VLAN(PVID)은 1입니다.

TRUNK 모드 VLAN 설정 명령어

명령어	설명	CLI 모드
switchport trunk native vlan <vlan-id>	포트의 기본 VLAN(PVID)을 설정합니다.(범위: 2 ~ 4094)	Interface Configuration Mode
switchport trunk allowed vlan all	포트를 모든 VLAN의 Tagged 멤버로 설정합니다.이후 생성되는 VLAN도 자동 포함됩니다.	Interface Configuration Mode
switchport trunk allowed vlan none	VLAN 1을 제외한 모든 VLAN의 Tagged 멤버에서 제외합니다.	Interface Configuration Mode
switchport trunk allowed vlan add <vlan-list>	지정한 VLAN을 Tagged 멤버로 추가합니다.(예: 1, 2-4, 1,3,5)	Interface Configuration Mode
switchport trunk allowed vlan remove <vlan-list>	지정한 VLAN을 Tagged 멤버에서 제거합니다.	Interface Configuration Mode

동작 정리

- TRUNK 포트는 여러 VLAN을 동시에 전달
- 모든 트래픽은 Tagged 상태로 전송
- Allowed VLAN 리스트 기반으로 트래픽 허용/차단
- Native VLAN(PVID)은 Untagged 트래픽 처리 기준

7.2.5. HYBRID 모드에서 VLAN 설정

트를 HYBRID 모드로 설정한 후 VLAN을 구성해야 합니다.

HYBRID 모드에서는 기본적으로 포트가 VLAN 1의 Untagged 멤버이며, PVID는 1입니다.

HYBRID 모드 VLAN 설정 명령어

명령어	설명	CLI 모드
switchport hybrid native vlan <vlan-id>	포트를 지정한 VLAN의 Untagged 멤버로 설정하고, PVID를 해당 VLAN으로 변경합니다.(범위: 2 ~ 4094)	Interface Configuration Mode
no switchport hybrid native vlan	기본 VLAN 설정을 해제하고 PVID를 VLAN 1로 복구합니다.	Interface Configuration Mode

명령어	설명	CLI 모드
switchport hybrid allowed vlan all	VLAN 1을 제외한 모든 VLAN을 Tagged 멤버로 설정합니다.신규 VLAN도 자동 포함됩니다.	Interface Configuration Mode
switchport hybrid allowed vlan none	VLAN 1을 제외한 모든 VLAN에서 멤버십을 제거하고 기본 상태로 복구합니다.	Interface Configuration Mode
switchport hybrid allowed vlan add <vlan-list> egress-tagged enable	지정한 VLAN을 **Tagged 멤버**로 추가합니다.	Interface Configuration Mode
switchport hybrid allowed vlan add <vlan-list> egress-tagged disable	지정한 VLAN을 **Untagged 멤버**로 추가합니다.	Interface Configuration Mode
switchport hybrid allowed vlan remove <vlan-list>	지정한 VLAN에서 포트를 제거합니다.기본 VLAN 포함 시 PVID는 VLAN 1로 복귀합니다.	Interface Configuration Mode

동작 정리

- HYBRID 포트는 Tagged + Untagged 혼합 구성 가능
- VLAN별로 egress 시 Tag 여부 개별 설정 가능
- PVID 변경 가능 → Access처럼도 사용 가능
- Trunk처럼 여러 VLAN 처리 가능

7.2.6. VLAN 정보 조회

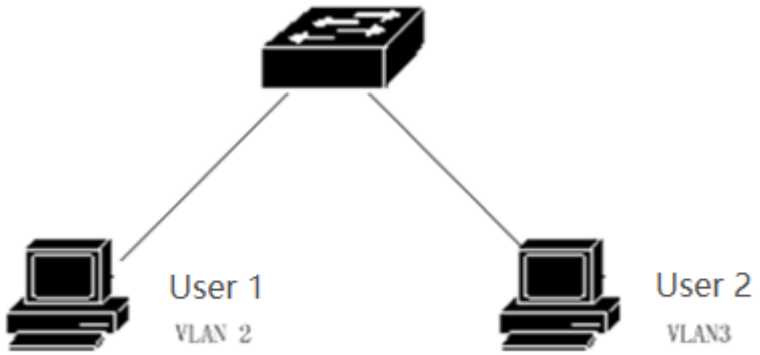
다음 명령어를 사용하여 VLAN 관련 설정 및 상태 정보를 확인할 수 있습니다.

명령어	설명	CLI 모드
show vlan [vlan-id]	파라미터 없이 실행 시 전체 VLAN 정보를 표시합니다. vlan-id 지정 시 해당 VLAN 정보만 표시합니다.(범위: 1 ~ 4094)	Normal / Privileged Mode
show interface	모든 포트의 VLAN 관련 정보(모드, PVID 등)를 표시합니다.	Normal / Privileged Mode
show running-config	현재 설정을 조회하여 VLAN 설정 내용을 확인합니다.	Privileged Mode

7.3. VLAN 설정 예시

7.3.1. 포트 기반 VLAN (Port-based VLAN)

1) 구성 (Configuration)
두 명의 사용자(User 1, User 2)가 있으며,
서로 다른 네트워크 환경 및 기능을 사용하기 때문에 서로 다른 VLAN에 속해야 합니다.
- User 1 → VLAN 2 → 포트 ge1/1 연결
- User 2 → VLAN 3 → 포트 ge1/2 연결



설정 방법

① VLAN 생성

```
Switch# config t
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 3
```

② 포트를 VLAN에 할당

```
Switch# config t

Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode access
Switch(config-ge1/1)# switchport access vlan 2
Switch(config-ge1/1)# exit

Switch(config)# interface ge1/2
Switch(config-ge1/2)# switchport mode access
Switch(config-ge1/2)# switchport access vlan 3
```

2) 동작 확인 및 디버깅
설정 이후 서로 다른 VLAN 간 통신이 되지 않는 것은 정상 동작입니다.

(VLAN 간 통신은 반드시 Layer 3 라우팅 필요)

문제 발생 시 확인 사항

같은 VLAN 내에서도 통신이 되지 않는 경우 다음을 점검합니다.

show vlan

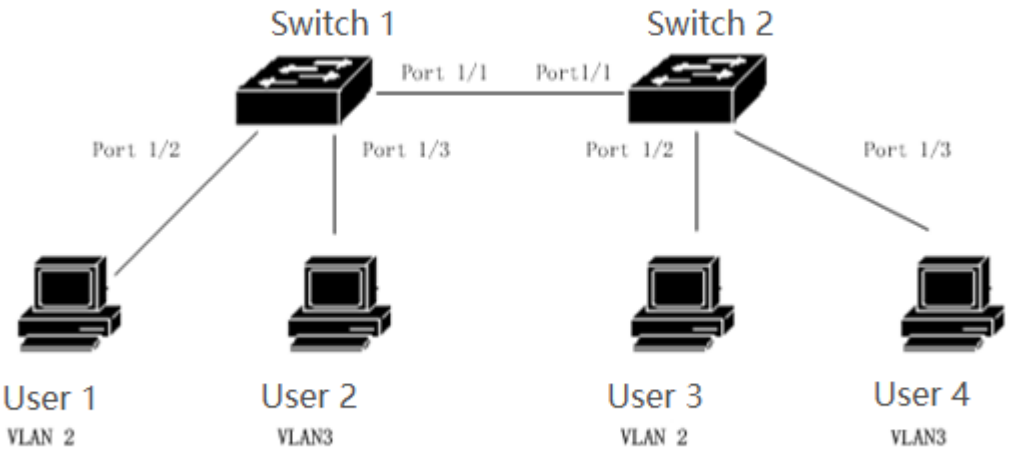
→ 전체 VLAN 및 포트 멤버 확인

show vlan <vlan-id>

→ 특정 VLAN에 포트가 정상적으로 포함되어 있는지 확인

7.3.2. 802.1Q 기반 VLAN 설정 예시

1) 구성



두 개의 스위치가 연결되어 있고, 각 스위치에 2개의 VLAN이 구성되어 있습니다.

사용자	VLAN	연결 포트	스위치	업링크 포트
User1	VLAN 2	ge1/2	Switch1	ge1/1
User2	VLAN 3	ge1/3	Switch1	ge1/1

사용자	VLAN	연결 포트	스위치	업링크 포트
User3	VLAN 2	ge1/2	Switch2	ge1/1
User4	VLAN 3	ge1/3	Switch2	ge1/1

두 스위치는 ge1/1 포트로 TRUNK 연결

Switch 1 설정

Switch# config t

Switch(config)# vlan database

Switch(config-vlan)# vlan 2

Switch(config-vlan)# vlan 3

Switch(config)# interface ge1/1

Switch(config-ge1/1)# switchport mode trunk

Switch(config-ge1/1)# switchport trunk allowed vlan add 2

Switch(config-ge1/1)# switchport trunk allowed vlan add 3

Switch(config)# interface ge1/2

Switch(config-ge1/2)# switchport mode access

Switch(config-ge1/2)# switchport access vlan 2

Switch(config)# interface ge1/3

Switch(config-ge1/3)# switchport mode access

Switch(config-ge1/3)# switchport access vlan 3

Switch 2 설정

Switch# config t

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 3

Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3

Switch(config)# interface ge1/2
Switch(config-ge1/2)# switchport mode access
Switch(config-ge1/2)# switchport access vlan 2

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode access
Switch(config-ge1/3)# switchport access vlan 3
```

동작 결과

- VLAN 2: User1 ↔ User3 → 통신 가능
- VLAN 3: User2 ↔ User4 → 통신 가능
- VLAN 2 ↔ VLAN 3 → 통신 불가 (L3 필요)
  즉, 같은 VLAN은 스위치가 달라도 통신 가능

2) 장애 시 점검 (Debug)
   같은 VLAN인데 통신이 안 될 경우 다음을 확인합니다.

   ① Access 포트 VLAN 설정 확인
   PC 연결 포트가 올바른 VLAN에 속해 있는지
   포트 모드가 ACCESS인지 확인
   ② Trunk 포트 설정 확인
   업링크 포트(ge1/1)가 TRUNK 모드인지

VLAN 2, 3이 allowed VLAN에 포함되어 있는지

7.4. MAC / IP 서브넷 / 프로토콜 기반 VLAN

7.4.1. 개요

일반적인 VLAN은 포트 기반으로 구성되지만, 보다 유연한 네트워크 구성을 위해 MAC / IP / Protocol 기반으로 VLAN을 동적으로 분류할 수도 있습니다.

1) MAC 기반 VLAN
   MAC 기반 VLAN은 패킷의 Source MAC 주소를 기준으로 VLAN을 결정합니다.

   - 포트에서 Untagged 또는 VID=0 패킷 수신 시
   - Source MAC을 기준으로 VLAN을 판단
   - 해당 VLAN으로 자동 할당 후 전달

   특정 단말(MAC) 기준으로 VLAN 고정 가능

2) IP 서브넷 기반 VLAN
   IP 기반 VLAN은 Source IP 주소 + 서브넷을 기준으로 VLAN을 결정합니다.

   - 포트에서 Untagged 패킷 수신 시
   - Source IP를 기준으로 VLAN 판단
   - 해당 VLAN으로 자동 할당 후 전달

   특정 네트워크 대역(서브넷)을 VLAN으로 분리할 때 사용

3) 프로토콜 기반 VLAN
   프로토콜 기반 VLAN은 패킷의 프로토콜 타입에 따라 VLAN을 결정합니다.

   지원 예:
   IP
   IPv6
   IPX 등

   프로토콜별로 VLAN 분리 가능 (예: Voice / Data 분리)

핵심 차이

방식	기준	활용
MAC 기반	MAC 주소	단말 기반 VLAN
IP 기반	IP/서브넷	네트워크 대역 기반
Protocol 기반	프로토콜	서비스/트래픽 분리

7.4.2. MAC / IP 서브넷 / 프로토콜 기반 VLAN 설정

이 기능을 사용하기 전에 해당 VLAN이 미리 생성되어 있어야 합니다.

MAC 기반 VLAN 명령어

명령어	설명	CLI 모드
mac-vlan mac WORD vlan <1-4094>	Source MAC 기준으로 VLAN을 생성합니다.	VLAN Configuration Mode
no mac-vlan mac WORD	특정 MAC 기반 VLAN을 삭제합니다.	VLAN Configuration Mode
no mac-vlan	모든 MAC 기반 VLAN을 삭제합니다.	VLAN Configuration Mode
mac-vlan enable	인터페이스에서 MAC 기반 VLAN 기능을 활성화합니다.	Interface Configuration Mode
mac-vlan disable	인터페이스에서 MAC 기반 VLAN 기능을 비활성화합니다.	Interface Configuration Mode
show mac-vlan	MAC 기반 VLAN 설정을 조회합니다.	Privileged Mode

IP 서브넷 기반 VLAN 명령어

명령어	설명	CLI 모드
ip-subnet-vlan ip A.B.C.D A.B.C.D vlan <1-4094>	Source IP + Subnet 기준 VLAN 생성	VLAN Configuration Mode

명령어	설명	CLI 모드
no ip-subnet-vlan ip A.B.C.D A.B.C.D	특정 IP 기반 VLAN 삭제	VLAN Configuration Mode
no ip-subnet-vlan	모든 IP 기반 VLAN 삭제	VLAN Configuration Mode
ip-subnet-vlan enable	인터페이스에서 IP 기반 VLAN 기능 활성화	Interface Configuration Mode
ip-subnet-vlan disable	인터페이스에서 IP 기반 VLAN 기능 비활성화	Interface Configuration Mode
show ip-subnet-vlan	IP 기반 VLAN 설정 조회	Privileged Mode

프로토콜 기반 VLAN 명령어

명령어	설명	CLI 모드
protocol-vlan ether-type (ip | ipv6 | ipx | ... | <0-65535>) vlan <1-4094>	프로토콜 기준 VLAN 생성	Interface Configuration Mode
no protocol-vlan ether-type (ip | ipv6 | ipx | ... | <0-65535>)	특정 프로토콜 VLAN 삭제	Interface Configuration Mode
no protocol-vlan	모든 프로토콜 VLAN 삭제	Interface Configuration Mode
show protocol-vlan	프로토콜 VLAN 설정 조회	Privileged Mode

상태 확인 명령어

명령어	설명	CLI 모드
show vlan-partition interface IFNAME	인터페이스에 적용된 MAC / IP 기반 VLAN 상태 확인	Privileged Mode

핵심 정리

- MAC / IP / Protocol VLAN은 패킷 기준 자동 VLAN 할당 (Dynamic VLAN)
- 반드시 인터페이스에서 enable 해야 동작

- 기존 Port-based VLAN과 혼합 설계 가능하지만 충돌 주의 필요

7.5. Voice VLAN

7.5.1. Voice VLAN 개요

Voice VLAN은 사용자 음성 데이터 트래픽을 위해 별도로 구성하는 VLAN입니다.

Voice VLAN을 분리하고, 음성 장비가 연결된 포트를 Voice VLAN에 포함시키면 음성 데이터에 대해 QoS(Quality of Service) 파라미터를 설정할 수 있습니다.

이를 통해 음성 패킷의 우선순위를 높이고 통화 품질을 보장할 수 있습니다.

장비는 포트로 유입되는 패킷의 Source MAC 주소에서 OUI 필드를 확인하여 해당 트래픽이 음성 데이터인지 판단할 수 있습니다.

Source MAC 주소가 시스템에 설정된 음성 장비 OUI 주소와 일치하는 경우, 해당 패킷은 Voice 트래픽으로 간주되며 Voice VLAN으로 분류되어 전송됩니다.

사용자는 OUI 주소를 직접 설정하거나, 시스템에 기본으로 등록된 OUI 주소를 기준으로 사용할 수 있습니다.

번호	OUI 주소	제조사
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	00d0-1e00-0000	Pingtel phone
5	0060-b900-0000	Philips/NEC phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3Com phone

IP Phone이 연결된 포트는 수동으로 Voice VLAN에 추가합니다.

이후 시스템은 패킷의 Source MAC을 확인하여 OUI 주소와 매칭합니다.

매칭에 성공하면 시스템은 ACL rule을 적용하고, 해당 패킷에 우선순위를 설정합니다.

7.5.2. Voice VLAN 설정

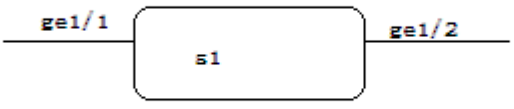
Voice VLAN을 구성하기 전에 해당 VLAN을 먼저 생성해야 합니다.

OUI 설정 (Global)

명령어	설명	CLI 모드
voice-vlan oui WORD mask WORD	사용자 OUI를 설정합니다.	Global Configuration Mode
voice-vlan oui WORD mask WORD description WORD	OUI를 설정하고 이름을 지정합니다.	Global Configuration Mode
no voice-vlan oui WORD mask WORD	특정 OUI 설정을 삭제합니다.	Global Configuration Mode
no voice-vlan oui description WORD	이름으로 OUI 설정을 삭제합니다.	Global Configuration Mode
no voice-vlan oui	모든 사용자 OUI 설정을 삭제합니다.	Global Configuration Mode

7.5.3. Voice VLAN 설정 예시

특정 OUI(0009.ca00.0000)를 가진 음성 트래픽을 포트 ge1/1로 유입 → ge1/2로 VLAN 2 Tag를 붙여 전송하는 구성입니다.



구성 개념

- ge1/1 → IP Phone 연결 (Hybrid)
  Voice 트래픽 → VLAN 2 (Untagged 입력 → 내부에서 VLAN 2로 분류)

- ge1/2 → 상위 스위치 연결 (Trunk)
  VLAN 2 → Tagged 상태로 전달

Switch S1 설정

Switch# configure terminal

! VLAN 생성

Switch(config)# vlan database

Switch(config-vlan)# vlan 2

Switch(config-vlan)# exit

! 사용자/전화기 포트

Switch(config)# interface ge1/1

Switch(config-ge1/1)# switchport mode hybrid

Switch(config-ge1/1)# switchport hybrid allowed vlan add 2 egress-tagged disable

Switch(config-ge1/1)# voice vlan 2 enable

! 업링크 포트

Switch(config)# interface ge1/2

Switch(config-ge1/2)# switchport mode trunk

Switch(config-ge1/2)# switchport trunk allowed vlan add 2

Switch(config-ge1/2)# exit

! OUI 설정 (음성 장비 식별)

Switch(config)# voice-vlan oui 0009.ca00.0000 mask ffff.ff00.0000

동작 흐름

- ge1/1에서 패킷 유입

- Source MAC OUI 검사
- OUI 매칭 → Voice 트래픽으로 인식
- VLAN 2로 자동 할당
- ge1/2 Trunk 포트로 전달 시 Tag 2 부여

핵심 요약

- Hybrid 포트 → 단말(PC + IP Phone) 혼합 환경 대응
- Trunk 포트 → VLAN 전달
- OUI → 음성 장비 자동 인식
- Voice VLAN → 자동 분류 + QoS 적용 구조

7.6. VLAN 매핑 (VLAN Mapping)

7.6.1. 개요

VLAN Mapping 기능은 패킷에 포함된 VLAN Tag(VID) 값을 다른 VLAN ID로 변환하는 기능입니다.

즉, 스위치에서 들어오거나 나가는 트래픽의 VLAN ID를 다른 VLAN으로 재매핑할 수 있습니다.

주요 기능

1:1 VLAN Mapping

→ 특정 VLAN ID를 다른 VLAN ID로 변환

예시

VLAN 10 → VLAN 100 변환

VLAN 20 → VLAN 200 변환

사용 목적

- 서로 다른 VLAN 정책을 사용하는 네트워크 간 연동
- 고객망/사업자망 VLAN 변환 (Service VLAN)
- VLAN ID 충돌 해결
- Multi-tenant 환경 분리

설정 전 조건

VLAN Mapping을 사용하려면 매핑할 VLAN들이 미리 생성되어 있어야 합니다.

7.6.2. VLAN 매핑 설정

VLAN Mapping은 포트 단위(Interface)에서 설정하며, 지정한 VLAN ID를 다른 VLAN ID로 변환합니다.

VLAN 매핑 명령어

명령어	설명	CLI 모드
vlan-mapping vlan <1-4094> map-vlan <1-4094>	포트에서 특정 VLAN을 다른 VLAN으로 매핑합니다.(예: VLAN 10 → VLAN 100)	Interface Configuration Mode
no vlan-mapping vlan <1-4094>	특정 VLAN 매핑을 삭제합니다.	Interface Configuration Mode
no vlan-mapping	포트에 설정된 모든 VLAN 매핑을 삭제합니다.	Interface Configuration Mode
vlan-mapping enable	해당 포트에서 VLAN 매핑 기능을 활성화합니다.	Interface Configuration Mode
vlan-mapping disable	해당 포트의 VLAN 매핑 기능을 비활성화합니다.	Interface Configuration Mode
show vlan-mapping	전체 VLAN 매핑 설정을 조회합니다.	Privileged Mode

동작 예시

vlan-mapping vlan 10 map-vlan 100

→ 포트로 들어오는 VLAN 10 트래픽을 VLAN 100으로 변환하여 전달

핵심 동작 흐름

- 패킷 수신 (VLAN Tag 포함)
- 매핑 규칙 확인
- VLAN ID 변환 (Rewrite)

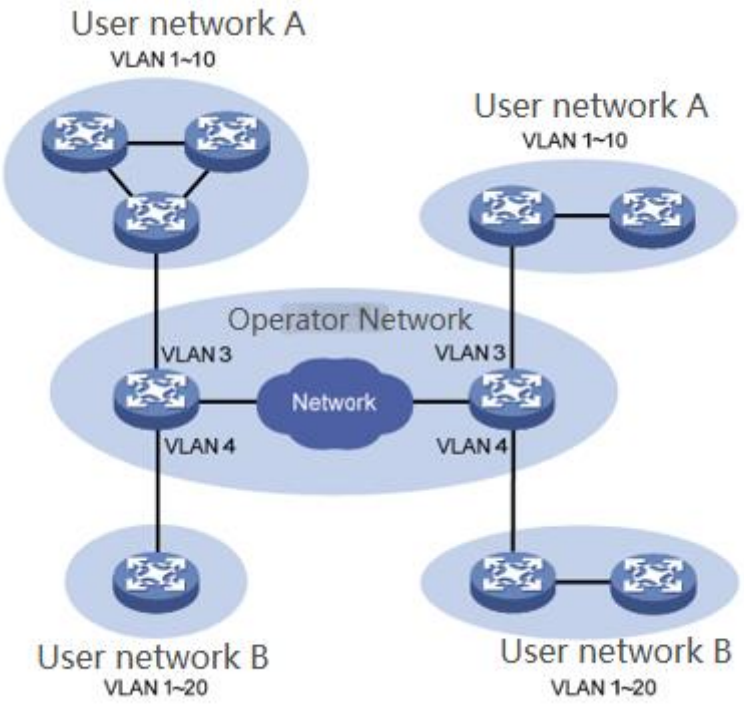
- 변환된 VLAN으로 forwarding

7.7. QinQ

7.7.1. QinQ 개요

QinQ는 장비에서 제공하는 간단하고 유연한 Layer 2 VPN 기술입니다.

이 기능은 사업자망 경계 장비에서 사용자 사설망 패킷에 외부 VLAN Tag를 추가로 캡슐화하여, 패킷이 2개의 VLAN Tag를 가진 상태로 사업자 백본망(Public Network)을 통과할 수 있도록 합니다.



Public Network에서는 장비가 외부 VLAN Tag만 기준으로 패킷을 forwarding합니다.

또한 패킷의 Source MAC 주소는 외부 VLAN Tag가 속한 VLAN의 MAC 주소 테이블에 학습됩니다.

반면 사용자의 사설망 VLAN Tag는 전송 과정에서 패킷의 데이터 영역처럼 취급되어 그대로 전달됩니다.

QinQ 기능을 사용하면 사업자는 하나의 VLAN을 이용하여 여러 VLAN을 포함하는 사용자 네트워크를 수용할 수 있습니다.

예를 들어,

- 사용자 네트워크 A의 사설 VLAN: VLAN 1 ~ 10
- 사용자 네트워크 B의 사설 VLAN: VLAN 1 ~ 20
- 사업자가 사용자 네트워크 A에 할당한 VLAN: VLAN 3

- 사업자가 사용자 네트워크 B에 할당한 VLAN: VLAN 4

사용자 네트워크 A의 VLAN Tag가 포함된 패킷이 사업자망으로 들어오면, 외부에 VLAN ID 3의 VLAN Tag가 추가됩니다.

사용자 네트워크 B의 VLAN Tag가 포함된 패킷이 사업자망으로 들어오면, 외부에 VLAN ID 4의 VLAN Tag가 추가됩니다.

이 방식으로 서로 다른 사용자 네트워크의 트래픽은 Public Network 내에서 완전히 분리됩니다.

두 사용자 네트워크의 VLAN 범위가 서로 겹치더라도 Public Network에서는 혼동 없이 전송할 수 있습니다.

QinQ의 장점

QinQ 기능을 사용하면 네트워크에서 최대 4094 × 4094개의 VLAN을 제공할 수 있어, Metro Ethernet 환경에서 요구되는 대규모 VLAN 수요를 충족할 수 있습니다.

QinQ는 주로 다음 문제를 해결합니다.

- Public Network의 VLAN ID 자원 부족 문제 완화
- 사용자가 자신의 사설 VLAN ID를 자유롭게 설계 가능
  → Public Network VLAN ID와 충돌하지 않음
- 소규모 MAN 또는 기업 네트워크에 간단한 Layer 2 VPN 솔루션 제공

QinQ 유형

QinQ는 다음 두 가지 방식으로 구분됩니다.

1) Basic QinQ
   Basic QinQ는 포트 기반 방식으로 동작합니다.
   포트에서 Basic QinQ 기능을 활성화하면, 해당 포트로 수신되는 패킷에 포트의 기본 VLAN(PVID)에 해당하는 VLAN Tag가 추가됩니다.

   동작 방식은 다음과 같습니다.
   - Tagged 패킷 수신 시
     → 외부 VLAN Tag가 추가되어 Double-Tag 패킷이 됨
   - Untagged 패킷 수신 시
     → 포트 기본 VLAN Tag가 추가된 Tagged 패킷이 됨

2) Flexible QinQ
   Flexible QinQ는 Basic QinQ보다 더 유연한 방식이며, 포트 + VLAN 조합을 기준으로 동작합니다.

Basic QinQ 기능을 모두 지원하면서도, 동일 포트에서 수신되는 패킷이라도 VLAN ID에 따라 서로 다른 동작을 수행할 수 있습니다.
예를 들어, 서로 다른 Inner VLAN ID를 가진 패킷에 대해 각각 다른 Outer VLAN Tag를 추가할 수 있습니다.

7.7.2. QinQ 설정

QinQ는 인터페이스 단위에서 설정하며, 포트를 업링크(사업자) / 고객 포트로 구분하고, 필요 시 VLAN 매핑을 구성합니다.

QinQ 관련 명령어

명령어	설명	CLI 모드
qinq tpid WORD	포트에서 사용하는 TPID 값을 설정합니다.(기본값: 0x8100)	Interface Configuration Mode
no qinq tpid	TPID 값을 기본값으로 복원합니다.	Interface Configuration Mode
qinq uplink	해당 포트를 **업링크 포트(사업자망 방향)**로 설정합니다.	Interface Configuration Mode
no qinq uplink	업링크 설정을 해제합니다.	Interface Configuration Mode
qinq customer	해당 포트를 **고객 포트(사용자망 방향)**로 설정합니다.	Interface Configuration Mode
no qinq customer	고객 포트 설정을 해제합니다.	Interface Configuration Mode
qinq outer-vid <1-4094> inner-vid VLAN_ID	특정 Inner VLAN을 지정된 Outer VLAN로 매핑합니다.	Interface Configuration Mode
no qinq outer-vid <1-4094> [inner-vid VLAN_ID]	VLAN 매핑 설정을 삭제합니다.	Interface Configuration Mode
show qinq	전체 QinQ 설정 상태를 조회합니다.	Privileged Mode

동작 구조

- Customer Port
  → 고객 VLAN(Inner VLAN) 유입
- Uplink Port
  → Outer VLAN Tag 추가 후 전달
- Outer VLAN (S-VLAN
)→ 사업자망에서 사용하는 VLAN
- Inner VLAN (C-VLAN)
  → 고객망 VLAN

예시 개념

Inner VLAN 10 → Outer VLAN 100

Inner VLAN 20 → Outer VLAN 200

→ 고객 VLAN을 사업자 VLAN으로 캡슐화하여 전달

7.7.3. QinQ 설정 예시

구성 개념

Switch B 기준으로:

- ge1/1 → Public Network (사업자망)
- ge1/2 → 사용자 장비 (PC + IP Phone)

트래픽 분리 정책:

- IP Phone (VLAN 500) → Outer VLAN 100으로 전달
- PC (VLAN 600) → Outer VLAN 200으로 전달

즉,

- C-VLAN 500 → S-VLAN 100
- C-VLAN 600 → S-VLAN 200

Switch B 설정

Switch# configure terminal

! Outer VLAN 생성 (사업자 VLAN)

```
Switch(config)# vlan database
Switch(config-vlan)# vlan 100
Switch(config-vlan)# vlan 200
Switch(config-vlan)# exit

! 업링크 포트 (Public Network 방향)
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 100
Switch(config-ge1/1)# switchport trunk allowed vlan add 200
Switch(config-ge1/1)# qinq uplink

! 고객 포트 (PC + IP Phone)
Switch(config)# interface ge1/2
Switch(config-ge1/2)# switchport mode hybrid
Switch(config-ge1/2)# switchport hybrid allowed vlan add 100 egress-tagged disable
Switch(config-ge1/2)# switchport hybrid allowed vlan add 200 egress-tagged disable
Switch(config-ge1/2)# qinq customer

! QinQ 매핑 설정
Switch(config-ge1/2)# qinq outer-vid 100 inner-vid 500
Switch(config-ge1/2)# qinq outer-vid 200 inner-vid 600
```

설정 결과 확인

```
Switch# show qinq

ifname    tpid      mode        outer-vid    inner-vid
ge1/1     0x8100    uplink      -            -
```

ge1/2	0x8100	customer	100	500
ge1/2	0x8100	customer	200	600

동작 흐름

ge1/2에서 패킷 유입

Inner VLAN 확인

- 500 → Voice
- 600 → Data

QinQ 매핑 적용

- 500 → Outer 100
- 600 → Outer 200

Double Tagging 수행

ge1/1 통해 Public Network로 전달

핵심 요약

- 고객 VLAN(C-VLAN)과 사업자 VLAN(S-VLAN) 완전 분리
- 하나의 포트에서 여러 VLAN 정책 처리 가능
- Voice / Data를 서로 다른 S-VLAN으로 분리 가능

8. QoS 설정 (Quality of Service)

이 장에서는 QoS의 개념과 설정 방법을 설명하며, 주요 구성은 다음과 같습니다.

- QoS 개요
- QoS 설정
- QoS 설정 예시

QoS 개념 한 줄 정리

QoS는 네트워크 트래픽을 우선순위 기반으로 제어하여

중요한 서비스(예: 음성, 영상)가 지연 없이 처리되도록 보장하는 기술입니다.

왜 QoS가 필요한가

- 트래픽이 동일하게 처리되면
  → 혼잡 시 Voice / Video 품질 급격히 저하
- QoS 적용 시
  → 중요한 트래픽에 우선순위 + 대역폭 보장

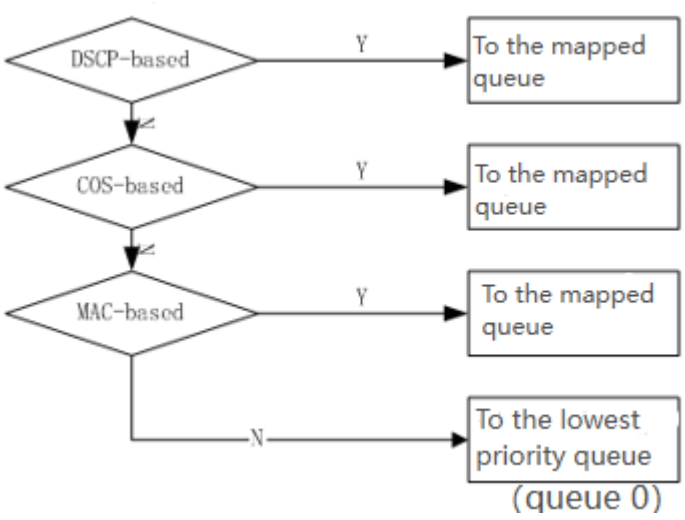
QoS 핵심 기능

- Classification (분류) → 트래픽 식별
- Marking (마킹) → CoS / DSCP 값 설정
- Queuing (큐잉) → 우선순위 큐 처리
- Policing / Shaping → 트래픽 제어

8.1. QoS 개요 (QoS Introduction)

QoS(Quality of Service)는 스위치를 통과하는 트래픽 중 중요한 트래픽에 우선순위를 부여하여

네트워크 대역폭을 효율적으로 사용하고, 예측 가능한 성능을 보장하는 기술입니다.



QoS 동작 기본 원리

스위치에서는 입력 포트에서 결정된 우선순위 정보가

출력 포트에서 어떤 큐(Queue)를 사용할지 결정합니다.

즉,

패킷 → 분류 → 우선순위 → 큐 → 스케줄링 → 전송

이 흐름으로 처리됩니다.

QoS 지원 방식

스위치는 다음 3가지 QoS 방식을 지원합니다.

- CoS 기반 QoS (802.1p)
  → VLAN Tag의 Priority 필드 사용 (기본 활성화)
- DSCP 기반 QoS (DiffServ)
  → IP 헤더 기반 QoS (포트별 설정 가능)
- MAC 기반 QoS
  → MAC 주소 기준 (MAC Binding 기능과 연동)

포트당 하나의 QoS 방식만 적용 가능

Priority Queue 구조

- 총 8개의 큐 (0 ~ 7)
- Queue 7 = 최고 우선순위
- Queue 0 = 최저 우선순위

스케줄링 방식 (Queue Scheduling)

QoS에서 핵심은 큐를 어떻게 처리하느냐입니다.

1) SP (Strict Priority)
   항상 높은 큐부터 먼저 처리
   예: 7 → 6 → 5 → ... → 0
   Voice 트래픽에 적합
   낮은 큐 starvation 발생 가능
2) RR (Round Robin)
   모든 큐를 순서대로 동일하게 처리
   공평하지만 우선순위 개념 약함
3) WRR (Weighted Round Robin)
   큐마다 가중치를 부여하여 처리
   높은 큐는 더 많은 패킷 전송
4) WDRR (Weighted Deficit Round Robin)
   WRR보다 더 유연한 방식
   트래픽 크기까지 고려하여 처리
   대규모 트래픽 환경에 적합

QoS Profile (QosProfile)

QoS 설정을 단순화하기 위해 QosProfile 개념을 사용합니다.

QosProfile	**CoS 값**	**Queue**
Qp0	0	0
Qp1	1	1
Qp2	2	2
Qp3	3	3
Qp4	4	4
Qp5	5	5
Qp6	6	6

QosProfile	CoS 값	Queue
Qp7	7	7

CoS 값 = Queue 매핑 (1:1)

핵심 요약

- QoS = 우선순위 기반 트래픽 제어 기술
- CoS / DSCP / MAC 기반 분류
- 8개 큐 + 다양한 스케줄링 방식
- Voice → 높은 우선순위 (Queue 6~7)

8.1.1. CoS 기반 QoS (802.1p)

CoS 기반 QoS는 VLAN Tag 내부의 Priority 필드(802.1p)를 이용하여

패킷의 우선순위를 결정하는 방식입니다.

기본적으로 모든 포트에서 활성화되어 있음

동작 방식

스위치는 포트로 유입되는 패킷을 다음과 같이 처리합니다.

1) VLAN Tag가 있는 경우 (VID ≠ 0)
   VLAN Tag 내 CoS 값(0~7)을 추출
   해당 값에 따라 우선순위 큐(Queue) 결정
2) VLAN Tag가 없는 경우 (Untagged)
   또는
   VID = 0인 경우
   - 포트의 PVID를 기반으로 VLAN 설정
   - 포트의 기본 우선순위(Default Priority) 적용
   - 해당 우선순위로 Queue 결정

핵심 흐름

패킷 수신

→ VLAN Tag 확인

→ CoS 값 추출 또는 기본값 적용

→ Queue 매핑

→ 스케줄링 후 전송

특징

- Layer 2 기반 QoS
- VLAN Tag 필수 (Tagged 환경에서 효과적)
- 단하고 빠름 (하드웨어 처리)

실무 예시

- Voice VLAN → CoS 6 또는 7 설정
- 일반 데이터 → CoS 0 ~ 3 사용

IP Phone에서 자동으로 CoS 값 설정되는 경우 많음

8.1.2. DSCP 기반 QoS (Layer 3 QoS)

DSCP 기반 QoS는 IP 헤더의 DSCP(Differentiated Services Code Point) 값을 이용하여 패킷의 우선순위를 결정하는 방식입니다.

CoS가 L2라면, DSCP는 L3 QoS 핵심 방식입니다.

동작 방식

포트에서 DSCP 기반 QoS가 활성화되면, 스위치는 다음과 같이 동작합니다.

- 포트로 유입되는 IP 패킷 수신
- IP 헤더에서 DSCP 값 추출 (0~63)
- DSCP → Queue 매핑 테이블 조회
- 해당 Queue로 패킷 분류
- 스케줄링 후 전송

특징

- Layer 3 기반 QoS
- VLAN 여부와 관계없이 동작 (Untagged 환경에서도 적용 가능)
- 라우터 / L3 스위치 환경에서 필수

CoS vs DSCP 차이

구분	CoS	DSCP
계층	L2	L3
위치	VLAN Tag	IP Header
범위	0~7	0~63
사용 환경	스위치 내부	End-to-End QoS

실무 기준 값

- Voice (VoIP)
  → DSCP 46 (EF, Expedited Forwarding)
- Video
  → DSCP 34 (AF41 등)
- 일반 데이터
  → DSCP 0

핵심 정리

- DSCP = End-to-End QoS 표준
- IP 기반 트래픽 제어 가능
- WAN / MPLS / ISP 환경에서 필수

8.1.3. MAC 기반 QoS

MAC 기반 QoS는 목적지 MAC 주소 + VLAN 정보를 기준으로

패킷의 우선순위를 결정하는 방식입니다.

동작 방식

패킷이 스위치로 들어오면 다음과 같이 처리됩니다.

- 패킷 수신
- 목적지 MAC + VLAN(VID) 기준으로 L2 테이블 조회
- 해당 MAC 엔트리가 존재하면
- 해당 엔트리에 설정된 QoS(Queue 매핑) 정보 확인
- 지정된 우선순위 큐로 패킷 전달

특징

- Layer 2 기반 QoS
- 특정 장비(MAC 단위) 기준으로 우선순위 지정 가능
- MAC Binding 기능과 연동

사용 목적

- 특정 서버, 장비, 단말에 대해 고정 우선순위 부여
- 네트워크 장비/중요 시스템 트래픽 보호
- 책 기반 QoS 적용

CoS / DSCP / MAC QoS 비교

방식	기준	특징
CoS	VLAN Tag	L2, 기본 활성
DSCP	IP Header	L3, 표준 QoS
MAC	MAC 주소	장비 기반 QoS

핵심 정리

- MAC QoS = 특정 장비 우선 처리용 QoS
- 일반 트래픽보다 정밀한 제어 가능
- 설정은 MAC Binding과 같이 사용되는 경우 많음

8.1.4. Policy 기반 QoS

Policy 기반 QoS는 단순히 CoS/DSCP 값만 보는 것이 아니라,

사용자가 정의한 조건(Class) + 처리 방식(Action)을 조합하여 트래픽을 제어하는 고급 QoS 방식입니다.

핵심 구성 요소

Policy 기반 QoS는 3가지 요소로 구성됩니다.

1) Class (분류)
   → 어떤 트래픽을 제어할 것인지 정의
   예:
   - 특정 IP
   - 특정 MAC
   - 특정 포트
   - 특정 프로토콜

2) Policy (정책)
   → Class들을 묶어서 정책 구성

3) Action (동작)
   → 해당 트래픽에 대해 어떤 처리를 할 것인지 정의
   예:
   - 우선순위 변경 (CoS / DSCP)
   - Queue 지정
   - Rate 제한 (Policing)

동작 흐름

- 패킷이 포트로 유입
- Class 조건과 비교하여 매칭
- 매칭되면 → 해당 Policy Action 적용
- 매칭되지 않으면 → 기본 QoS 정책 적용
- 최종 Queue 결정 후 전송

특징

- 매우 정교한 트래픽 제어 가능
- 특정 서비스/사용자/트래픽별 정책 적용 가능
- 기업망 / 데이터센터 / ISP에서 활용

예시 개념

- VoIP 트래픽 → DSCP 46 설정 + 최고 우선순위
- CCTV 트래픽 → 중간 우선순위
- 일반 사용자 트래픽 → 낮은 우선순위

핵심 정리

- Policy QoS = 조건 기반 QoS (Rule 기반 제어)
- CoS / DSCP보다 훨씬 유연함
- 실제 QoS 설계의 핵심

8.2. QoS 설정 (Default Configuration)

8.2.1. QoS 기본 설정 (Default Configuration)

스위치의 QoS 기본 동작은 다음과 같이 정의됩니다.

이 값들은 QoS 정책을 따로 구성하지 않아도 기본적으로 적용되는 동작 기준입니다.

기본 구성 항목

항목	기본값	설정 가능 여부
큐 개수	8개 (0~7)	❌
기본 스케줄링	WRR	✅
SP (Strict Priority)	비활성화	✅
RR (Round Robin)	비활성화	✅
WDRR	비활성화	✅

Queue Weight (WRR 기준)

- QP0 → 1
- QP1 → 2
- QP2 → 4
- QP3 → 8

- QP4 → 16
- QP5 → 32
- QP6 → 64
- QP7 → 127

높은 큐일수록 더 많은 트래픽 처리 가능

CoS → Queue 매핑 (고정)

CoS	Queue
0	QP0
1	QP1
2	QP2
3	QP3
4	QP4
5	QP5
6	QP6
7	QP7

CoS는 1:1 매핑 (변경 불가)

DSCP → Queue 매핑 (설정 가능)

DSCP 범위	Queue
0 ~ 7	QP0
8 ~ 15	QP1
16 ~ 23	QP2
24 ~ 31	QP3
32 ~ 39	QP4

DSCP 범위	Queue
40 ~ 47	QP5
48 ~ 55	QP6
56 ~ 63	QP7

DSCP는 범위 기반 매핑, 사용자 설정 가능

인터페이스 기본 상태

- DSCP 기반 QoS → 비활성화
- CoS 기반 QoS → 기본 활성화
- 기본 CoS 값 → 0

핵심 요약

- 기본은 WRR 기반 QoS
- CoS는 자동 적용 / DSCP는 별도 활성화 필요
- Queue 7이 최우선 (Voice용)

8.2.2. QoS 스케줄링 방식 설정

스위치는 기본적으로 WRR(Weighted Round Robin) 방식으로 동작합니다.

필요에 따라 포트별로 다른 스케줄링 방식을 설정할 수 있습니다.

설정 명령어

명령어	설명	CLI 모드
`qos sched {rr	sp	wrr

스케줄링 방식 설명

1) SP (Strict Priority)
   → 높은 큐부터 먼저 처리 (7 → 0 순서)

→ Voice 트래픽에 매우 적합
낮은 큐 트래픽이 밀릴 수 있음 (starvation)

2) RR (Round Robin)
→ 모든 큐를 동일하게 순환 처리
→ 공평하지만 우선순위 의미 약함

3) WRR (Weighted Round Robin) (기본값)
→ 큐별 가중치에 따라 처리
→ 실무에서 가장 많이 사용

4) WDRR (Weighted Deficit Round Robin)
→ WRR보다 더 정교한 방식
→ 패킷 크기까지 고려
→ 고밀도 트래픽 환경에 적합

실무 추천

- 일반 환경 → WRR 유지
- Voice 중요 환경 → SP + WRR 혼합 구성
- 트래픽 다양 / 대용량 → WDRR 고려

8.2.3. Queue Weight 설정

Queue Weight는 각 우선순위 큐가 한 번의 라운드에서 얼마나 많은 패킷을 처리할지를 결정하는 값입니다.

→ WRR / WDRR 스케줄링에서 핵심 파라미터입니다.

설정 명령어

명령어	설명	CLI 모드
qos qosprofile {qp0~qp7} weight <1-127>	해당 큐의 Weight를 설정합니다.	Interface Configuration Mode
no qos qosprofile {qp0~qp7} weight	큐 Weight를 기본값으로 복구합니다.	Interface Configuration Mode

동작 개념

- Weight 값이 높을수록 → 더 많은 패킷 전송
- Weight 값이 낮을수록 → 전송 비율 감소

예시

- QP7 = 100
- QP0 = 10

→ QP7이 QP0보다 약 10배 더 많은 트래픽 처리

중요한 설정 원칙

낮은 우선순위 큐의 Weight가 높은 우선순위 큐보다 크면 안 됩니다

→ 그렇지 않으면 QoS 의미가 깨짐

기본 Weight (참고)

- QP0: 1
- QP1: 2
- QP2: 4
- QP3: 8
- QP4: 16
- QP5: 32
- QP6: 64
- QP7: 127

우선순위가 높을수록 Weight도 큼

실무 예시

- Voice (QP6~7) → 높은 Weight 유지
- Video → 중간 Weight
- Data → 낮은 Weight

핵심 정리

- Weight = 트래픽 처리 비율 제어
- WRR/WDRR에서만 의미 있음
- QoS 튜닝 핵심 파라미터

8.2.4. DSCP ↔ QosProfile 매핑 설정

DSCP 기반 QoS를 사용할 때는 DSCP 값(0~63)을 어떤 우선순위 큐(Qp0~Qp7)로 보낼지 정의해야 합니다.

이 매핑이 실제로 출력 Queue를 결정하는 핵심 로직입니다.

설정 명령어

명령어	설명	CLI 모드
qos dscp-map-qp <0-63> qosprofile {qp0~qp7}	특정 DSCP 값을 지정한 QosProfile(큐)로 매핑	Interface Configuration Mode
no qos dscp-map-qp <0-63> *(또는 기본 복구 명령)*	DSCP 매핑을 기본값으로 복구	Interface Configuration Mode

제공된 문서의 no qos qosprofile ... weight는 Weight 복구 명령으로 보이며, DSCP 매핑 복구는 장비에 따라 no qos dscp-map-qp <value> 형태로 사용됩니다.

동작 개념

- 패킷 유입
- IP Header에서 DSCP 값 추출
- 설정된 DSCP → QosProfile 매핑 확인
- 해당 Queue(Qp0~Qp7)로 분류
- 스케줄링 후 전송

실무 권장 매핑 예시

! Voice (EF)

qos dscp-map-qp 46 qosprofile qp7

! Video (AF41)

qos dscp-map-qp 34 qosprofile qp5

! 일반 데이터

qos dscp-map-qp 0 qosprofile qp0

Voice는 최상위 큐, Video는 중상위, Data는 기본 큐로 분리

핵심 포인트

- DSCP = L3 QoS 기준값, QosProfile = 큐 선택 기준
- 매핑이 없으면 기본 범위 매핑이 적용됨
- End-to-End QoS 설계에서 가장 중요한 설정

8.2.5. 포트 DSCP 기반 QoS 설정

DSCP 기반 QoS를 실제로 적용하려면 인터페이스에서 기능을 활성화해야 합니다.

이 기능은 물리 포트에서만 가능하며, TRUNK 포트나 L3 인터페이스에서는 설정할 수 없습니다.

명령어	설명	CLI 모드
qos dscp-based	해당 포트에서 DSCP 기반 QoS를 활성화합니다.	Interface Configuration Mode
no qos dscp-based	DSCP 기반 QoS를 비활성화합니다.	Interface Configuration Mode

동작 흐름

- 포트에서 패킷 수신
- DSCP 값 추출 (IP Header)
- DSCP → QosProfile 매핑 적용
- Queue 결정
- 스케줄링 후 전송

중요한 제약 사항

- QoS는 포트당 하나의 방식만 적용 가능
  → CoS / DSCP / MAC 중 선택
- DSCP QoS는 IP 패킷에만 적용 가능
  → L2 트래픽에는 적용되지 않음

실무 적용 예

```
interface ge1/1
 qos dscp-based
```

해당 포트에서 들어오는 트래픽을 DSCP 기준으로 우선순위 처리

8.2.6. 포트 사용자 우선순위 설정 (CoS 값)

포트에 들어오는 Untagged 트래픽에 대해 기본 CoS(802.1p) 값을 지정할 수 있습니다.

즉, VLAN Tag가 없는 트래픽에도 기본 우선순위를 강제 부여하는 기능입니다.

명령어	설명	CLI 모드
qos user-priority <0-7>	포트의 기본 CoS 값을 설정합니다.	Interface Configuration Mode
no qos user-priority	CoS 값을 기본값(0)으로 복구합니다.	Interface Configuration Mode

동작 방식

- -Tagged 트래픽
  → 패킷의 CoS 값을 그대로 사용
- Untagged / VID=0 트래픽
  → 포트의 user-priority 값 적용

즉, CoS가 없는 트래픽에 기본 우선순위를 부여하는 역할

실무 활용

interface ge1/1

qos user-priority 6

→ 해당 포트로 들어오는 Untagged 트래픽을

Voice 수준 우선순위(CoS 6)로 처리

사용 사례

- IP Phone이 Tag를 안 넣는 경우
- 특정 포트 전체를 고우선 트래픽으로 처리
- Access 포트에서 QoS 강제 적용

핵심 정리

- CoS 기본값 설정 기능
- Untagged 트래픽 QoS 보완
- 간단하지만 효과적인 QoS 방법

8.3. QoS 설정 예시

1) CoS 기반 QoS 설정 (포트 기본 우선순위)

목표:
ge1/3 포트의 기본 CoS 값을 3으로 설정
(CoS 기반 QoS는 기본적으로 활성화 상태)

```
Switch# configure terminal
Switch(config)# interface ge1/3
Switch(config-ge1/3)# qos user-priority 3
Switch(config-ge1/3)# end
```

동작 결과

- Untagged 트래픽 → CoS 3 적용
- Queue → QP3로 전달

기본적인 트래픽 우선순위 설정

2) DSCP 기반 QoS 설정

목표:
DSCP 값 3 → Queue 2(QP2)로 매핑하고
해당 포트에서 DSCP QoS 활성화

```
Switch# configure terminal
Switch(config)# interface ge1/3
Switch(config-ge1/3)# qos dscp-map-qp 3 qosprofile qp2
Switch(config-ge1/3)# qos dscp-based
Switch(config-ge1/3)# end
```

동작 결과

- IP 패킷 DSCP=3 → QP2로 전달
- DSCP 기반 QoS 활성화됨

전체 흐름 비교

구분	기준	적용 대상
CoS 설정	포트 기본값	Untagged 트래픽
DSCP 설정	IP Header	IP 트래픽

핵심 정리

- CoS → 간단한 L2 QoS
- DSCP → 정교한 L3 QoS
- 둘 중 하나만 포트에 적용 가능

8.4. Policy 기반 QoS 설정 예시

이 예제는 특정 MAC 주소 트래픽을 식별 → 우선순위 재설정 → 포트에 적용하는 전체 흐름을 보여줍니다.

1) ACL로 트래픽 식별 (Classification)
   특정 Source MAC을 기준으로 트래픽을 구분합니다.

   ```
   access-list 700 permit host 0000.0000.1111 vid any ip any any
   access-list 701 permit host 0000.0000.2222 vid any ip any any
   access-list 702 permit host 0000.0000.3333 vid any ip any any
   ```

   MAC1 / MAC2 / MAC3 각각을 식별하는 조건

2) QoS Class 정의
   ACL과 매칭하여 트래픽 그룹을 생성합니다.

   ```
   qos class 10 match acl 700
   qos class 11 match acl 701
   ```

qos class 12 match acl 702

Class = "어떤 트래픽인지 정의"

3) QoS Policy 정의 (Action)
각 Class에 대해 우선순위를 설정합니다.

qos policy 10 class 10 remark cos 7
qos policy 10 class 11 remark cos 5
qos policy 10 class 12 remark cos 3

동작 결과

MAC1 → CoS 7 (최고 우선순위)
MAC2 → CoS 5
MAC3 → CoS 3

4) 포트에 정책 적용
interface ge1/2
 qos apply-policy 10
해당 포트로 들어오는 트래픽에 정책 적용

전체 동작 흐름

- 패킷 유입 (ge1/2)
- ACL 매칭 (MAC 기준)
- Class 분류
- Policy 적용 (CoS 재마킹)
- Queue 매핑 후 전송

핵심 정리

- ACL → 트래픽 식별
- Class → 그룹화
- Policy → 처리 정의
- Apply → 실제 적용

9. MSTP 설정 (Multiple Spanning Tree Protocol)

이 장에서는 MSTP의 개념과 설정 방법을 설명하며, 주요 구성은 다음과 같습니다.

- MSTP 개요
- MSTP 설정

- MSTP 설정 예시

MSTP 한 줄 정리

MSTP는 여러 VLAN을 여러 개의 Spanning Tree 인스턴스로 나누어 루프를 방지하면서도 링크를 효율적으로 활용하는 L2 제어 프로토콜입니다.

왜 MSTP가 필요한가

기존 STP / RSTP의 문제:

- 모든 VLAN이 하나의 트리 사용 → 특정 링크만 사용됨
- 나머지 링크는 Block → 대역폭 낭비

MSTP 적용 시:

- VLAN을 여러 Instance로 분리
- 서로 다른 Root / 경로 사용
- → 로드 밸런싱 + 루프 방지 동시에 가능

핵심 개념

Instance (MSTI)

→ VLAN 묶음 단위

Region

→ 동일 MST 설정을 가진 스위치 그룹

Root Bridge

→ 각 Instance별 기준 스위치

동작 예

- VLAN 10,20 → MSTI 1 → 경로 A
- VLAN 30,40 → MSTI 2 → 경로 B

트래픽 분산 가능

핵심 효과

Loop 방지 (STP 기능 유지)

트래픽 분산 (Load Balancing)

빠른 수렴 (RSTP 기반)

9.1. MSTP 소개

해당 스위치는 다음과 같은 Spanning Tree 계열 프로토콜을 지원합니다.

지원 프로토콜

- IEEE 802.1D (STP)
  → 기본 Spanning Tree Protocol
  → 수렴 속도 느림, 단일 트리 구조
- IEEE 802.1W (RSTP)
  → Rapid STP
  → 빠른 수렴 (수 초 내)
  → STP 개선 버전
- IEEE 802.1S (MSTP)
  → Multiple Spanning Tree Protocol
  → 여러 VLAN을 여러 인스턴스로 분리
  → 로드밸런싱 + 빠른 수렴 + 루프 방지

핵심 차이 요약

프로토콜	특징	한계
STP (802.1D)	안정적	느림
RSTP (802.1W)	빠른 수렴	단일 트리
MSTP (802.1S)	다중 트리 + 로드밸런싱	설정 복잡

MSTP 핵심 의미

MSTP = RSTP 기반 + VLAN 그룹화 + 트래픽 분산

9.1.1. MSTP 개요 (Overview)

MSTP는 RSTP 기반의 빠른 수렴 기능을 활용하여

여러 VLAN을 하나의 Spanning Tree Instance(MSTI)로 묶어 처리합니다.

핵심 구조

- 여러 VLAN → 하나의 MST Instance로 그룹화
- 각 Instance → 독립적인 Spanning Tree Topology 구성

즉, VLAN 그룹마다 별도의 트리 구조를 가짐

동작 특징

- 각 MST Instance는 서로 완전히 독립적으로 동작
- Instance마다 다른 Root / 경로 설정 가능
- → 트래픽을 여러 경로로 분산 가능

주요 효과

1) 빠른 수렴 (RSTP 기반)
   → 장애 발생 시 빠르게 경로 재계산
2) Load Balancing
   → VLAN을 Instance로 나누어 여러 링크 활용
3) 확장성 향상
   → VLAN 수가 많아도 Instance 수는 줄일 수 있음

개념 예시

- VLAN 10, 20 → MSTI 1 → 경로 A
- VLAN 30, 40 → MSTI 2 → 경로 B

하나의 링크만 쓰는 것이 아니라 여러 링크를 동시에 활용 가능

핵심 정리

- MSTP = RSTP + VLAN 그룹화 + 멀티 경로
- Instance 단위로 트리 구성
- 대규모 네트워크에서 필수

9.1.2. MST Domain (Multiple Spanning Tree Domain)

MSTP에서 여러 스위치가 하나의 트리 계산에 참여하려면 동일한 MST 설정을 가져야 합니다.

이렇게 동일한 설정을 가진 스위치들의 집합을 MST Domain이라고 합니다.

MST Domain 구성 조건

같은 Domain에 속하려면 다음 3가지가 반드시 동일해야 합니다.

- Domain Name
- Revision Number
- VLAN ↔ MST Instance 매핑 정보

이 정보들은 하나의 Digest 값으로 생성됨

Digest가 같으면 같은 MST Domain

확인 명령

show spanning-tree mst config

→ Domain 정보 및 Digest 확인 가능

MST Domain 특징

- 하나의 Domain = 동일한 MST 정책 공유
- 여러 스위치가 하나의 논리적 STP처럼 동작
- Domain 간에는 RSTP처럼 동작

Instance 관련 제한

- 하나의 Domain당 최대 16개 MST Instance 지원
- VLAN은 Instance에 매핑되어 동작

설계 시 VLAN을 적절히 묶는 것이 중요

핵심 개념 정리

- MST Domain = 같은 설정 가진 스위치 그룹
- Digest = Domain 일치 여부 판단 기준

- Domain 내부 → MSTP 동작
- Domain 간 → RSTP 동작

9.1.3. IST / CIST / CST 개념 정리 (MSTP 핵심 구조)

MSTP를 이해하려면 IST, CIST, CST 3가지를 정확히 구분하는 것이 중요합니다.

1) IST (Internal Spanning Tree)
   - MST Domain 내부에서 동작하는 기본 Spanning Tree
   - Instance 0 (MSTI 0)으로 정의됨
   - 모든 BPDU 송수신의 기준이 되는 트리

   특징
   모든 VLAN은 기본적으로 IST에 속함
   MST Domain 내부의 기본 트리 역할
   다른 MST Instance 정보도 IST BPDU에 포함되어 전달됨

   핵심
   IST = Domain 내부 기본 트리 + BPDU 중심

2) CIST (Common and Internal Spanning Tree)
   - MST Domain 내부 IST + Domain 간 연결 트리까지 포함한 전체 트리

   즉
   - Domain 내부 → IST
   - Domain 간 → CST
   → 이걸 합친 게 CIST

   특징
   - 전체 네트워크 기준의 Root 결정
   - MST Domain을 하나의 큰 스위치처럼 보이게 함

   핵심
   CIST = 전체 네트워크 기준 트리

3) CST (Common Spanning Tree)
   - MST Domain 외부(다른 Domain 간)에서 동작하는 트리

   특징

- 여러 MST Domain을 연결하는 역할
- RSTP / STP 기반으로 동작

핵심
CST = Domain 간 연결 트리

구조 관계 (중요)

MSTP 구조는 이렇게 이해하면 됩니다:

- Domain 내부 → IST
- Domain 간 → CST
- 전체 통합 → CIST

핵심 비교

구분	범위	역할
IST	Domain 내부	기본 트리 (Instance 0)
CIST	전체 네트워크	통합 트리
CST	Domain 간	외부 연결 트리

중요한 포인트

- IST는 모든 MST Instance 정보를 포함하는 핵심 BPDU 역할
- MST Instance(1~15)는 실제 트래픽 분산용
- CIST Root가 전체 네트워크 Root 역할

9.1.4. MSTP Domain 내부 동작 (Intra-domain Operation)

이 내용은 MSTP에서 같은 Domain 내부에서 스위치들이 어떻게 하나의 트리로 수렴(converge)되는지를 설명합니다.

1) IST 기반으로 Domain 전체 연결
   모든 MSTP 스위치는 IST(Instance 0)를 통해 연결됨
   IST가 수렴하면 → Domain 전체의 기본 트리 완성

   IST = Domain 내부의 기준 트리

2) IST Master 선정
IST 수렴 후, Domain 내부에서 IST Master가 결정됩니다.

선정 기준:
가장 낮은 Bridge ID
CST Root까지의 Path Cost가 가장 낮은 스위치

쉽게 말하면
"전체 네트워크 기준 Root에 가장 가까운 스위치"

3) IST Master 역할
- Domain 내부의 대표 Root 역할
- 다른 MST Instance들의 기준점 역할
- Domain과 외부(CST) 연결 시 기준 노드

4) 특수 상황
네트워크에 Domain이 하나만 있는 경우
→ IST Master = CST Root

CST Root가 Domain 외부에 있는 경우
→ Domain 경계(Border)에 있는 스위치가 IST Master

5) 초기 동작 (중요)
스위치가 부팅되면:
자신이 Root라고 주장 (BPDU 전송)
Path Cost = 0으로 시작
모든 MST Instance도 Root라고 주장

이후 더 좋은 BPDU 받으면:
Root 포기
더 우선순위 높은 스위치 따라감

6) Subdomain → 통합 과정
초기에는:
여러 개의 작은 Subdomain 존재 가능

하지만:
더 좋은 BPDU가 전달되면서
점점 하나의 Domain으로 통합됨

결국 하나의 IST Master로 수렴

7) 안정 동작 조건
모든 스위치가 정상 동작하려면:
동일한 IST Master를 인식해야 함
동일한 MST 설정 유지해야 함

다르면 → MST 불일치 / STP 문제 발생

핵심 정리

- IST가 Domain 내부 트리 구성
- IST Master가 Domain 기준 Root
- BPDU 교환으로 하나의 트리로 수렴
- 모든 스위치는 동일한 IST Master를 봐야 정상

9.1.5. MSTP Domain 간 동작 (Interdomain Operation)

네트워크에 여러 MST Domain이 존재하거나 기존 STP(802.1D) 장비가 혼재된 경우, MSTP는 전체를 하나로 묶는 CST(Common Spanning Tree)를 구성합니다.

1) CST 구성 역할
CST는 다음을 모두 포함합니다:
여러 MST Domain
기존 STP 스위치

즉, 전체 네트워크를 하나의 트리로 묶는 최상위 구조

2) MST Domain의 동작 방식
MST Domain 내부 → IST로 연결
MST Domain 외부 → CST로 연결

Domain은 외부에서 보면 하나의 가상 스위치처럼 동작

3) IST와 CST 관계
   - IST는 CST의 일부(서브 트리)처럼 동작
   - IST Root → IST Master
   - IST Master → CST와 연결되는 대표 노드

4) BPDU 동작 방식
   - CST만 BPDU를 송수신
   - MST Instance 정보는
   → BPDU 내부에 포함되어 전달됨

   결과:
   - BPDU 수 감소
   - 처리 효율 증가

5) 파라미터 적용 범위
   CST에서 설정되는 값 (공통 적용)

   hello time
   forward delay
   max-age
   max-hops

   전체 네트워크 기준 동작

   Topology 관련 값 (개별 설정 가능)

   Bridge Priority
   Port Cost
   Port Priority

   👉 CST / MST Instance 각각 설정 가능

6) 다른 프로토콜과의 호환
   MSTP ↔ MSTP → MSTP BPDU 사용
   MSTP ↔ RSTP → RSTP BPDU (Version 3)
   MSTP ↔ STP → 802.1D BPDU

즉, 하위 호환 완벽 지원

핵심 정리

- MST Domain 간 연결 = CST
- Domain은 외부에서 하나의 스위치처럼 보임
- BPDU는 CST 기준으로 동작
- MST Instance는 BPDU에 포함되어 전달

9.1.6. Hop Count

IST와 MST 인스턴스가 스패닝 트리 토폴로지를 계산할 때 사용하는 BPDU에서는 message-age와 maximum-age 정보가 사용되지 않습니다. 대신 루트까지의 경로 계산에는 IP의 TTL과 유사한 hop-count 메커니즘이 사용됩니다.

사용자는 해당 도메인에 대해 최대 hop count 값을 설정할 수 있으며, 이 값은 해당 도메인의 IST와 모든 MST 인스턴스에 적용됩니다. Hop count의 동작 방식은 message-age와 유사한 결과를 가지며(재구성이 발생한 이후 기준), 인스턴스의 루트 스위치는 항상 cost를 0으로 하고 hop-count를 최대값으로 설정한 BPDU(or-M-record)를 전송합니다.

스위치는 BPDU를 수신하면 남아 있는 hop count를 1 감소시키고, 감소된 값을 포함하여 새로운 BPDU를 생성해 전달합니다. 이 값이 0이 되면, 해당 스위치는 BPDU를 폐기하고 해당 포트에 대한 정보를 aging 처리합니다.

도메인 내부에서는 RSTP BPDU에 포함된 message-age와 maximum-age 값이 동일하게 유지되며, 이 값은 도메인 경계 포트를 통해 그대로 전달됩니다.

9.1.7. Boundary Port

Boundary 포트는 MST 도메인을 다음과 같은 다른 스패닝 트리 도메인과 연결하는 포트입니다. RSTP만 사용하는 도메인, 802.1D(STP)만 사용하는 도메인, 또는 서로 다른 MST 설정을 가진 도메인과 연결될 때 해당 포트는 Boundary 포트가 됩니다. 또한, 단일 스패닝 트리 스위치이거나 다른 MST 도메인 설정을 가진 스위치가 지정 스위치로 동작하는 LAN에 연결된 경우에도 Boundary 포트로 간주됩니다.

Boundary 포트에서는 MST 포트의 역할은 중요하지 않으며, 포트 상태는 항상 IST 포트의 상태와 동일하게 강제됩니다. 즉, IST 포트가 forwarding 상태이면 Boundary 포트의 MST 포트도 forwarding 상태가 됩니다. 경계에 위치한 IST 포트는 backup 포트를 제외한 어떤 역할도 가질 수 있습니다.

공유된 Boundary 연결에서는 MST 포트가 blocking 상태에서 forward-delay 시간이 만료될 때까지 대기한 후 learning 상태로 전이되며, 이후 다시 한 번 forward-delay 시간이 지나야 forwarding 상태로 전이됩니다.

Boundary 포트가 point-to-point 연결이고 IST의 root 포트인 경우에는, IST 포트가 forwarding 상태로 전이

되는 즉시 MST 포트도 forwarding 상태로 전이됩니다.

Boundary 포트가 특정 인스턴스에서 forwarding 상태로 전이되면, 모든 인스턴스에서도 forwarding 상태가 되며 이때 topology change가 발생합니다. 또한 IST의 root 포트 또는 designated 포트 역할을 가진 Boundary 포트가 topology change 알림을 수신하면, MSTP 스위치는 해당 포트에서 IST 인스턴스와 활성화된 모든 MST 인스턴스에 대해 topology change를 발생시킵니다.

9.1.8. MSTP와 802.1D STP 간 상호 운용성

MSTP를 실행하는 스위치는 802.1D와의 연동을 위해 내장된 프로토콜 마이그레이션 메커니즘을 지원합니다. 스위치가 특정 포트에서 802.1D 구성의 BPDU를 수신하면, 해당 포트에서는 802.1D BPDU를 전송하게 됩니다. 또한 MSTP 스위치는 도메인의 경계 포트에서 802.1D BPDU를 수신하는 경우와, 다른 도메인의 경계 포트에서 MSTP BPDU 또는 RSTP BPDU를 수신하는 경우를 감지할 수 있습니다.

그러나 스위치가 더 이상 802.1D BPDU를 수신하지 않는다고 해서 자동으로 MSTP 모드로 되돌아가지는 않습니다. 이는 상대 스위치가 연결에서 제거되었는지 여부를 판단할 수 없기 때문이며(상대가 지정 스위치가 아닌 경우), 또한 연결된 스위치가 도메인에 새로 참여했더라도 해당 포트를 계속 Boundary 포트로 유지할 수 있기 때문입니다. 따라서 이러한 경우에는 프로토콜 마이그레이션 과정을 재시작하여 인접 스위치와 다시 협상하도록 해야 합니다.

연결된 다른 스위치들이 모두 RSTP를 사용하는 경우, 이들은 MSTP BPDU와 RSTP BPDU를 모두 처리할 수 있습니다. 따라서 MSTP 스위치는 경계 포트에서 버전 0의 Configuration 및 TCN BPDU 또는 버전 3의 MSTP BPDU를 전송합니다.

Boundary 포트는 단일 스패닝 트리 스위치이거나 다른 MST 설정을 가진 스위치가 지정 스위치로 동작하는 LAN에 연결된 포트를 의미합니다.

9.1.9. Port Role

MSTP는 RSTP의 빠른 수렴 알고리즘을 채택하고 있으며, 여기서는 RSTP를 기반으로 포트 역할과 빠른 수렴에 대해 설명합니다.

RSTP는 포트 역할을 지정하고 활성 토폴로지를 결정함으로써 빠른 수렴을 제공합니다. RSTP는 IEEE 802.1D STP를 기반으로 하며, 우선순위가 높은 스위치를 루트 스위치로 선택합니다. RSTP가 포트 역할을 할당할 때의 유형은 다음과 같습니다.

- Root Port
  스위치가 루트 스위치로 패킷을 전달할 때 가장 최적의 경로 비용을 제공하는 포트입니다.
- Designated Port
  지정 스위치에 연결되는 포트입니다. LAN에서 루트 스위치로 패킷을 전달할 때 가장 낮은 경로 비용을 가지며, 지정 스위치가 LAN에 연결되는 포트를 의미합니다.
- Alternate Port

현재 Root Port에 장애가 발생했을 때 사용할 수 있는 루트로 가는 대체 경로를 제공합니다.

- Backup Port
  지정 포트의 백업 역할을 하는 포트입니다. 두 포트가 point-to-point 루프 형태로 연결되어 있거나, 하나의 스위치가 동일한 LAN 세그먼트에 두 개 이상의 포트를 연결한 경우에만 존재합니다.
- Disable Port
  스패닝 트리 동작에 참여하지 않는 포트로, 포트 역할이 없습니다.
- Master Port
  도메인의 루트에 위치하거나 전체 루트까지 가장 짧은 경로 상에 있는 포트로, 도메인을 전체 루트와 연결하는 포트입니다.

Root Port와 Designated Port는 활성 토폴로지에 포함되며, Alternate Port와 Backup Port는 활성 토폴로지에 포함되지 않습니다.

안정된 토폴로지에서는 RSTP가 모든 Root Port와 Designated Port를 즉시 forwarding 상태로 전환하고, Alternate Port와 Backup Port는 항상 discarding 상태를 유지합니다. 포트 상태는 forwarding과 learning 동작을 제어합니다.

Fast Convergence

RSTP는 스위치 장애, 포트 장애, LAN 장애 발생 시 빠른 복구를 제공하며, edge 포트, 새로운 root 포트, point-to-point 연결에서 빠른 수렴을 지원합니다.

- Edge Port
  포트를 edge 포트로 설정하면 즉시 forwarding 상태로 전환됩니다. 이 포트는 스패닝 트리 계산이 필요 없는 단일 단말 또는 장치에 연결된 경우에만 사용해야 합니다.
- Root Port
  RSTP가 새로운 Root Port를 선택하면 기존 Root Port는 차단되고, 새로운 Root Port는 즉시 forwarding 상태로 전환됩니다.

Topological Change

이 부분은 RSTP와 802.1D가 토폴로지 변경을 처리하는 방식의 차이를 설명합니다.

- Detection (탐지)
  802.1D에서는 blocking과 forwarding 상태 간의 모든 전환이 토폴로지 변경으로 간주되지만, RSTP에서는 blocking에서 forwarding으로 전환될 때만 토폴로지 변경으로 간주합니다. 또한 edge 포트에서의 상태 변화는 토폴로지 변경을 발생시키지 않습니다.
  RSTP 스위치가 토폴로지 변경을 감지하면, TC 정보를 수신한 포트를 제외한 모든 non-edge 포트로 학습된 정보를 플러딩합니다.
- Notification (알림)

802.1D는 TCN BPDU를 사용하지만, RSTP는 이를 사용하지 않습니다. 다만 802.1D와의 호환을 위해 TCN BPDU를 처리하고 생성할 수 있습니다.
RSTP 스위치가 802.1D 스위치로부터 지정 포트에서 TCN 메시지를 수신하면, TCA 플래그가 설정된 802.1D BPDU로 응답합니다.
또한 루트 포트에서 802.1D 스위치로부터 TCA가 설정된 Configuration BPDU를 수신하면 TC-while 타이머가 초기화됩니다. 이 동작은 802.1D 호환을 위해 필요합니다.
RSTP BPDU에는 TCA 플래그가 포함되지 않습니다.

- Propagation (전파)
  RSTP 스위치가 다른 스위치로부터 TC 메시지를 지정 포트 또는 루트 포트에서 수신하면, 수신 포트를 제외한 모든 non-edge 포트, 지정 포트, 루트 포트로 전파합니다. 이때 해당 포트들은 TC-while 타이머를 시작하고 학습 정보를 플러딩합니다.
- Protocol Migration (프로토콜 전환)
  802.1D와의 호환을 위해 RSTP는 포트 단위로 802.1D BPDU와 RSTP BPDU를 선택적으로 전송합니다.
  초기화 시 migrate-delay 타이머가 시작되며, 이 기간 동안 RSTP BPDU를 전송합니다. 이 타이머가 동작 중일 때는 수신된 모든 BPDU를 처리하되 프로토콜 종류는 무시합니다.
  타이머가 종료된 이후 802.1D BPDU를 수신하면 해당 포트는 802.1D 스위치와 연결된 것으로 판단하고 802.1D BPDU를 사용합니다. 반대로, 802.1D BPDU를 사용 중인 포트에서 RSTP BPDU를 수신하면 타이머를 재시작하고 다시 RSTP BPDU를 사용하게 됩니다.

9.1.10. 802.1D Spanning Tree 소개

Spanning Tree Protocol(STP)는 다음과 같은 요소를 기반으로 동작합니다.

- 특정 LAN 내 모든 스위치를 식별하기 위한 고유 그룹 주소(01-80-C2-00-00-00)가 존재하며, 모든 스위치는 이 주소를 인식합니다.
- 각 스위치는 고유한 식별자(Bridge Identifier)를 가집니다.
- 각 스위치의 포트 또한 고유한 Port Identifier를 가집니다.

스패닝 트리 구성을 위해서는 각 스위치의 우선순위, 각 포트의 우선순위, 그리고 각 포트의 경로 비용(path cost)을 함께 고려해야 합니다.

우선순위가 가장 높은 스위치를 루트 스위치(root switch)라고 합니다. 각 스위치 포트는 루트 스위치까지의 경로 비용의 합인 root path cost를 가지며, 이 값이 가장 낮은 포트를 root port라고 합니다. 만약 동일한 root path cost를 가진 포트가 여러 개라면, 우선순위가 높은 포트가 root port가 됩니다.

각 LAN에는 하나의 지정 스위치(designated switch)가 존재하며, 이는 해당 LAN에서 루트까지의 경로 비용이 가장 낮은 스위치입니다. 지정 스위치와 LAN을 연결하는 포트를 지정 포트(designated port)라고 합니다. 하나의 스위치에서 동일 LAN에 두 개 이상의 포트가 연결되어 있다면, 우선순위가 가장 높은 포트가 지정 포트로 선택됩니다.

스패닝 트리 형성을 위한 결정 요소

1) 루트 스위치 결정
   a. 초기에는 모든 스위치가 자신을 루트 스위치로 인식합니다.
   b. 각 스위치는 자신이 연결된 LAN으로 configuration BPDU를 브로드캐스트하며, 이때 root ID와 bridge ID 값은 동일하게 설정됩니다.
   c. 다른 스위치로부터 configuration BPDU를 수신했을 때, 수신한 BPDU의 root ID 값이 현재 스위치가 가지고 있는 값보다 크면 해당 프레임을 무시하고, 더 작으면 root ID, root path cost 등의 값을 갱신한 후 새로운 값으로 BPDU를 다시 전송합니다.

2) Root Port 결정
   a. 스위치에서 root path cost가 가장 낮은 포트가 root port입니다.
   b. 동일한 cost를 가진 포트가 여러 개일 경우, 우선순위가 높은 포트를 root port로 선택합니다.
   c. cost와 우선순위가 모두 동일할 경우, 포트 번호가 가장 낮은 포트가 root port가 됩니다.

3) 지정 스위치(Designated Switch) 결정
   a. 초기에는 모든 스위치가 자신을 지정 스위치로 간주합니다.
   b. 동일 LAN에서 더 낮은 root path cost를 가진 BPDU를 수신하면 해당 스위치는 지정 스위치 역할을 포기합니다.
   c. 동일한 root path cost를 가진 스위치가 여러 개일 경우, 우선순위가 가장 높은 스위치가 지정 스위치로 선택됩니다.
   d. 지정 스위치가 경쟁 상황을 감지하면 configuration BPDU를 다시 전송하여 재선정을 수행합니다.

4) 지정 포트 결정
   - 지정 스위치에서 해당 LAN으로 연결된 포트가 지정 포트가 됩니다.
   - 하나의 스위치에서 동일 LAN에 여러 포트가 연결된 경우, 포트 ID가 가장 낮은 포트가 지정 포트로 선택됩니다.

최종 동작

- Root Port와 Designated Port는 Forwarding 상태
- 나머지 포트는 Blocking 상태

이와 같이 루트 스위치, 루트 포트, 지정 스위치 및 지정 포트를 모두 결정하면 네트워크 전체에 루프가 없는 Spanning Tree 토폴로지가 형성됩니다.

9.2. MSTP 설정

9.2.1. MSTP 기본 설정

다음은 스위치에서 MSTP 관련 기본 설정값입니다.

명령 파라미터	기본값
spanning-tree mst enable (MSTP 활성화)	shut (비활성화 상태)
spanning-tree mst priority (CIST 스위치 우선순위)	32768
spanning-tree mst hello-time (CIST Hello Time)	2초
spanning-tree mst forward-time (CIST Forward Delay)	15초
spanning-tree mst max-age (CIST Max Age)	20초
spanning-tree mst max-hops (CIST Max Hops)	20
instance 1 priority (Instance 우선순위)	32768
spanning-tree mst instance 1 priority (포트 Instance 우선순위)	128
spanning-tree mst instance 1 path-cost (포트 Instance Path Cost)	20000000
spanning-tree mst priority (포트 CIST 우선순위)	128
spanning-tree mst path-cost (포트 CIST Path Cost)	20000000

9.2.2. MSTP 일반 설정

MSTP 시작

시스템은 기본적으로 MSTP가 비활성화(shut) 상태로 시작됩니다.

MSTP를 활성화하는 설정 과정은 다음과 같습니다.

Switch# configure terminal

Switch(config)# spanning-tree mst enable

MSTP를 비활성화하려면 다음 명령을 사용합니다.

Switch# configure terminal

Switch(config)# no spanning-tree mst

max-age 설정

max-age는 모든 인스턴스에 적용되는 설정으로, 스위치가 스패닝 트리 구성 정보를 기다리는 시간(초)을 의미하며, 이 시간이 지나면 재구성을 트리거합니다.

기본값은 20초이며, 설정 범위는 6~40초입니다.

설정 방법:

Switch# configure terminal

Switch(config)# spanning-tree mst max-age <seconds>

max-hops 설정

max-hops는 하나의 도메인 내에서 BPDU가 전달될 수 있는 최대 hop 수를 의미합니다.

이 값을 초과하면 BPDU는 폐기됩니다.

기본값은 20이며, 설정 범위는 1~40입니다.

설정 방법:

Switch# configure terminal

Switch(config)# spanning-tree mst max-hops <hop-count>

forward-time 설정

forward-time은 포트가 discarding → learning → forwarding 상태로 전이될 때 각각 대기하는 시간(초)을 의미합니다.

기본값은 15초이며, 설정 범위는 4~30초입니다.

또한 다음 조건을 만족해야 합니다.

2 × (forward-time - 1) ≥ max-age

설정 방법:

Switch# configure terminal

Switch(config)# spanning-tree mst forward-time <seconds>

hello-time 설정

hello-time은 루트 스위치가 구성 정보를 생성하는 주기를 의미합니다.

기본값은 2초이며, 설정 범위는 1~10초입니다.

다음 조건을 만족해야 합니다.

2 × (hello-time + 1) ≤ max-age

설정 방법:

Switch# configure terminal

Switch(config)# spanning-tree mst hello-time <seconds>

CIST 브리지 우선순위 설정

기본값은 32768이며, 설정 범위는 0~61440입니다.

우선순위 값은 반드시 4096의 배수여야 합니다.

설정 방법:

Switch# configure terminal

Switch(config)# spanning-tree mst priority <priority>

Cisco 호환 설정

이 장비는 IEEE 802.1s 기반 MSTP를 사용하며, MSTI 메시지 길이는 16바이트입니다.

반면 Cisco 장비는 26바이트를 사용합니다.

Cisco 장비와 상호 운용을 위해서는 호환 모드를 활성화해야 합니다.

이 기능이 활성화되면 Domain Name과 Revision Number만 같으면 동일 도메인으로 간주합니다.

기본적으로 비활성화 상태입니다.

Cisco 호환 활성화:

Switch# configure terminal

Switch(config)# spanning-tree mst cisco-interoperability enable

Cisco 호환 비활성화:

Switch# configure terminal

Switch(config)# spanning-tree mst cisco-interoperability disable

Protocol Check Task 초기화

802.1D STP와의 호환을 위해 시스템은 자동으로 상대 장비의 프로토콜을 감지합니다.

하지만 다음과 같은 경우 문제가 발생할 수 있습니다.

예:

- 기존에는 상대 장비가 STP 사용
- 이후 일반 호스트로 변경됨
- 포트를 edge 포트로 설정하려고 함
- 그러나 기존 STP 협상 상태 유지됨

이 경우 프로토콜 감지 작업을 초기화하여 다시 협상해야 합니다.

전체 장비 초기화:

Switch# clear spanning-tree detected protocols

특정 포트 초기화:

Switch# clear spanning-tree detected protocols interface <if-name>

9.2.3. Domain Configuration

두 개 이상의 장비가 동일한 도메인에 속하려면,VLAN–Instance 매핑, Revision Number, Domain Name이 모두 동일해야 합니다.

하나의 도메인은 동일한 MST 설정을 가진 하나 이상의 장비로 구성되며, 각 장비는 RSTP BPDU를 처리할 수 있어야 합니다. 네트워크 내 도메인 수에는 제한이 없지만, 하나의 도메인은 최대 16개의 인스턴스를 지원할 수 있습니다.

Instance 설정은 'Instance Configuration' 항목에서 설명되며, 여기서는 도메인 이름과 Revision Number 설정만 설명합니다.

도메인 이름 설정:

Switch# configure terminal

Switch(config)# spanning-tree mst configuration

Switch(config-mst)# region <region-name>

Revision Number 설정:

Switch# configure terminal

Switch(config)# spanning-tree mst configuration

Switch(config-mst)# revision <revision-num>

9.2.4. Instance Configuration

시스템은 총 16개의 인스턴스를 지원하며, Instance ID 범위는 0 ~ 15입니다.

하나의 VLAN은 동시에 하나의 Spanning Tree Instance에만 할당될 수 있습니다.

기본적으로 시스템에는 Instance 0만 존재하며, 모든 VLAN은 기본적으로 Instance 0에 속합니다.

인스턴스 설정 과정:

Switch# configure terminal

Switch(config)# spanning-tree mst configuration

Switch(config-mst)# instance <instance-id> vlan <vlan-id>

MSTI Bridge 우선순위 설정:

기본값은 32768이며, 설정 범위는 0 ~ 61440입니다.

MSTI 우선순위 값은 반드시 4096의 배수여야 합니다.

설정 과정:

Switch# configure terminal

Switch(config)# spanning-tree mst configuration

Switch(config-mst)# instance <instance-id> priority <priority>

9.2.5. Port configuration

다음은 MSTP와 관련된 포트 설정에 대한 설명입니다. 여기서는 기본적인 설정만 다루며, port fast나 root guard와 같은 기능은 별도로 설명됩니다.

포트를 특정 Instance에 참여시키는 설정 과정:

Switch# configure terminal

Switch(config)# interface <if-name>

Switch(config-if)# spanning-tree mst instance <instance-id>

CIST 포트 우선순위 설정

기본값은 128이며, 설정 범위는 0~240입니다.

우선순위 값은 반드시 16의 배수여야 합니다.

Switch# configure terminal

Switch(config)# interface <if-name>

Switch(config-if)# spanning-tree mst priority <priority>

MSTI 포트 우선순위 설정

기본값은 128이며, 설정 범위는 0~240입니다.

마찬가지로 16의 배수만 설정 가능합니다.

Switch# configure terminal

Switch(config)# interface <if-name>

Switch(config-if)# spanning-tree mst instance <instance-id> priority <priority>

CIST 포트 Path Cost 설정

기본값은 20000000이며, 설정 범위는 1~200000000입니다.

대역폭과 Path Cost의 관계는 다음과 같습니다.

- 100K → 200000000
- 1M → 20000000
- 10M → 2000000
- 100M → 200000
- 1G → 20000
- 10G → 2000
- 100G → 200
- 1T → 20
- 1T 이상 → 2

설정 방법:

Switch# configure terminal

Switch(config)# interface <if-name>

Switch(config-if)# spanning-tree mst path-cost <path-cost>

MSTI 포트 Path Cost 설정

기본값은 20000000이며, 범위는 동일합니다.

Switch# configure terminal

Switch(config)# interface <if-name>

Switch(config-if)# spanning-tree mst instance <instance-id> path-cost <path-cost>

프로토콜 버전 설정

기본적으로 MSTP 패킷을 전송합니다.

설정 범위는 0~3이며, 매핑은 다음과 같습니다.

- 0 → STP
- 2 → RSTP
- 3 → MSTP

Switch# configure terminal

Switch(config)# interface <if-name>

Switch(config-if)# spanning-tree mst force-version <version-id>

연결 타입 설정

포트 연결 방식에 따라 RSTP의 수렴 동작이 달라집니다.

기본값은 point-to-point입니다.

Point-to-Point 설정:

Switch# configure terminal

Switch(config)# interface <if-name>

Switch(config-if)# spanning-tree mst link-type point-to-point

Shared 설정:

Switch# configure terminal

Switch(config)# interface <if-name>

Switch(config-if)# spanning-tree mst link-type shared

연결 타입 동작 설명

Point-to-Point 연결에서는 RSTP의 proposal-agreement 메커니즘을 통해 빠른 수렴이 가능합니다.

스위치가 proposal 메시지를 수신하고 해당 포트가 새로운 root port로 선정되면, 다른 포트들을 모두 동기화(synchronize)합니다. 이 과정에서 forwarding 상태의 지정 포트는 edge 포트가 아닌 경우 blocking 상태로 전환됩니다.

모든 포트가 동기화되면, 스위치는 agreement 메시지를 전송하고, point-to-point 환경에서는 포트가 즉시 forwarding 상태로 전환됩니다.

반면 Shared 연결에서는 기존 802.1D 방식으로 상태 전이가 이루어집니다.

9.2.6. PORTFAST 관련 설정

1) Port Fast
   Port Fast는 access 포트나 trunk 포트를 blocking 상태를 거치지 않고 바로 forwarding 상태로 전환시킵니다.
   즉, listening / learning 단계를 건너뛰기 때문에 ⏱ 즉시 통신 가능하게 됩니다.
   이 기능은 주로 PC, 서버 등 단일 단말 장비 연결 포트에 사용하며,
   스패닝 트리 수렴을 기다리지 않고 네트워크에 바로 접속할 수 있게 합니다.

   설정 방법:
   Switch# configure terminal
   Switch(config)# interface <if-name>
   Switch(config-if)# spanning-tree mst portfast

2) BPDU Filtering
   BPDU Filtering은 포트에서 BPDU 송수신을 차단하는 기능입니다.
   이 기능은 글로벌 설정과 포트별 설정이 가능하며, 동작 방식에 차이가 있습니다.

   글로벌 설정
   - PortFast가 기본 적용된 포트에 대해 BPDU Filtering 적용
   - 기본 상태(portfast default)에 있는 포트에만 영향
     Switch# configure terminal
     Switch(config)# spanning-tree mst portfast bpdu-filter

   포트별 설정

   특정 포트에 대해 강제로 BPDU Filtering 적용

   Switch# configure terminal

Switch(config)# interface <if-name>

Switch(config-if)# spanning-tree mst portfast bpdu-filter enable

동작 특징

해당 포트는 BPDU를 송신하지도, 수신하지도 않음

스패닝 트리 계산에서 사실상 제외됨

핵심 주의사항

- PortFast + BPDU Filtering 조합은 매우 강력하지만 위험함
- 스위치가 연결되면 루프 발생 가능성 있음

반드시 단말(PC, 서버) 연결 포트에서만 사용

3) BPDU Guard

BPDU Guard 기능은 스위치 전체(글로벌) 또는 포트 단위로 설정할 수 있으며, 각각 동작 방식에 차이가 있습니다.

글로벌 설정에서는 spanning-tree mst portfast bpdu-guard 명령을 사용하여, 기본적으로 PortFast가 적용된 포트에 BPDU Guard를 활성화할 수 있습니다.

포트 단위 설정에서는 특정 포트에 대해 BPDU Guard를 개별적으로 활성화할 수 있습니다.

BPDU Guard가 설정된 포트에서 BPDU를 수신하면, 해당 포트는 스패닝 트리에 의해 shutdown 상태로 전환됩니다. 정상적인 구성에서는 PortFast가 적용된 포트는 BPDU를 수신하지 않아야 합니다. 따라서 PortFast 포트에서 BPDU가 수신되는 경우, 이는 허가되지 않은 스위치 연결과 같은 잘못된 구성으로 판단되어 포트가 error-disabled 상태로 진입합니다.

error-disabled 상태란, BPDU Guard가 동작한 포트가 BPDU를 수신했을 때 포트를 비활성화하고, 시스템에 error-disable 기능이 설정되어 있으면 일정 시간이 지난 후 자동으로 포트를 다시 활성화하는 상태를 의미합니다.

글로벌 설정:

Switch# configure terminal

Switch(config)# spanning-tree mst portfast bpdu-guard

포트별 설정:

Switch# configure terminal

Switch(config)# interface <if-name>

Switch(config-if)# spanning-tree mst portfast bpdu-guard enable

error-disable 설정

error-disable 기능 활성화:

Switch# configure terminal

Switch(config)# spanning-tree mst errdisable-timeout enable

error-disable 복구 시간 설정:

Switch# configure terminal

Switch(config)# spanning-tree mst errdisable-timeout interval <seconds>

PortFast와 BPDU Guard는 함께 사용하는 것이 일반적이며, 단말(PC, 서버) 연결 포트에서 비인가 스위치 연결을 차단하는 데 매우 효과적입니다.

9.2.7. Root Guard 관련 설정

서비스 제공자(SP)의 Layer 2 네트워크에는 외부(고객) 스위치와 연결되는 경우가 많습니다. 이러한 환경에서는 스패닝 트리가 재계산되면서 고객 스위치가 Root 스위치로 선출되는 문제가 발생할 수 있습니다.

이 상황을 방지하기 위해, 고객 네트워크와 연결된 포트에 Root Guard를 설정할 수 있습니다.

Root Guard가 설정된 포트에서 스패닝 트리 계산 결과 해당 포트가 Root Port로 선정되려고 하면, 해당 포트는 root-inconsistent 상태(차단 상태)로 전환됩니다. 이를 통해 고객 스위치가 Root 스위치가 되는 것을 방지하고, 루트로 향하는 경로도 차단합니다.

외부(고객) 스위치가 Root 스위치가 되려고 시도하면, 해당 포트는 root-inconsistent 상태로 차단되고, 스패닝 트리는 다른 경로를 통해 새로운 Root 스위치를 다시 선정합니다. 이 과정에서 고객 스위치는 Root가 될 수 없으며, 루트로 향하는 경로도 형성되지 않습니다.

스위치가 MST 모드로 동작하는 경우, Root Guard는 해당 포트를 항상 Designated Port로 유지하도록 강제합니다. 또한 IST 인스턴스에서 Boundary 포트가 Root Guard에 의해 차단되면, 모든 MST 인스턴스에서도 동일하게 차단됩니다.

Boundary 포트는 802.1D 스위치나 다른 MST 도메인 설정을 가진 스위치가 존재하는 LAN에 연결된 포트를 의미합니다.

Root Guard는 해당 포트가 속한 모든 VLAN에 적용됩니다. VLAN은 MST 인스턴스로 묶여 동작할 수 있기 때문에, 결과적으로 해당 Instance 전체에도 영향을 미칩니다.

설정 방법

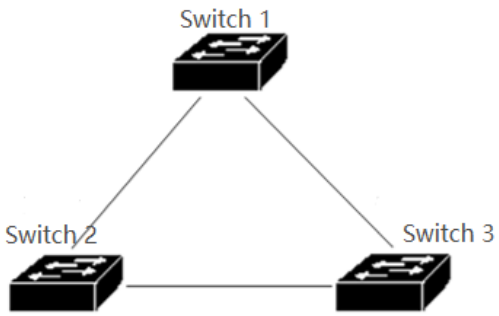
Switch# configure terminal

Switch(config)# interface <if-name>

Switch(config-if)# spanning-tree mst guard root

9.3. MSTP 설정 예제

1) 설정
세 대의 스위치가 링(Ring) 형태로 연결되어 있으며, 루프를 방지하기 위해 각 스위치에서 Spanning Tree Protocol(MSTP)을 활성화해야 합니다. 각 스위치에 대해 개별적으로 다음과 같이 설정을 수행합니다.



Switch 1 설정:
Switch> en
Switch# configure terminal
Switch(config)# spanning-tree mst enable

Switch 2 설정:
Switch> en
Switch# configure terminal
Switch(config)# spanning-tree mst enable

Switch 3 설정:
Switch> en
Switch# configure terminal
Switch(config)# spanning-tree mst enable

2) 디버깅 및 확인
루트 브리지로 어떤 스위치가 선택되었는지 확인하려면 다음 명령을 실행합니다.

Switch# show spanning-tree mst

출력 결과에서 CIST Root 값을 확인하면, 세 스위치 중 MAC 주소가 가장 낮은 스위치가 Root로 선출된 것을 확인할 수 있습니다. 이는 정상적인 동작입니다.
특정 포트의 스패닝 트리 상태를 확인하려면 다음 명령을 사용합니다.

Switch# show spanning-tree mst interface ge1/1

이 명령을 통해 Instance 0(IST) 기준으로 해당 포트의 상태(State)를 확인할 수 있으며, Forwarding / Blocking 등의 상태를 통해 현재 트리 구조를 판단할 수 있습니다.

10. EAPS 설정

이 장에서는 EAPS와 그 설정 방법에 대해 설명하며, 주요 내용은 다음과 같습니다.

- EAPS 소개
- EAPS 기본 개념
- EAPS 프로토콜 소개
- EAPS 설정
- 제약 사항
- 설정 예제

10.1. EAPS 소개

EAPS는 Ethernet Automatic Protection Switching의 약자입니다.

EAPS는 표준 Ethernet과 VLAN 기술을 기반으로 하여 링(Loop) 토폴로지와 장애 복구 메커니즘을 제공합니다.

링 구조에서 장애가 발생할 경우, EAPS는 1초 이내에 데이터 통신을 복구할 수 있는 기능을 제공합니다.

EAPS의 특징은 다음과 같습니다.

- 링에 참여할 수 있는 노드 수에 제한이 없음
- 복구 시간 역시 네트워크 규모에 영향을 받지 않음
- 다른 장비에 의존하지 않음

즉, EAPS 링 내부에는 EAPS 프로토콜을 지원하지 않는 장비가 포함되어도 동작 가능합니다.

10.2. EAPS 기본 개념

다음은 EAPS에서 사용되는 주요 기본 개념입니다.

- EAPS Domain
  네트워크에서 하나의 EAPS 도메인은 독립적인 링 구조로 동작합니다. 여러 개의 노드 장비가 하나의 루프를 구성하며, 하나의 도메인은 마스터 노드와 하나 이상의 트랜짓 노드로 구성됩니다.
- Master Node
  EAPS를 실행하는 스위치 또는 노드 장비로, 도메인 내에서 단 하나만 존재합니다. 링의 제어 및 상태 관리를 담당하는 핵심 장비입니다.
- Transit Node
  마스터 노드를 제외한 나머지 EAPS 노드 장비입니다. 즉, 도메인 내 일반 구성 노드라고 보면 됩니다.
- Primary Port
  EAPS 도메인 내에서 노드 장비를 링으로 연결하는 포트입니다. 각 노드는 하나의 Primary Port만 가질 수 있습니다.
- Secondary Port
  Primary Port와 함께 링을 구성하는 또 다른 연결 포트입니다. 각 노드는 하나의 Secondary Port만 가질 수 있습니다.

결국 각 노드는 링에 연결되기 위해 Primary 1개 + Secondary 1개 = 총 2포트 사용

- Control VLAN
  EAPS 프로토콜 패킷을 전달하는 VLAN입니다. 하나의 도메인에는 오직 1개의 Control VLAN만

존재합니다.

- Protected VLAN
  실제 서비스 트래픽(데이터)이 흐르는 VLAN입니다. 하나 이상의 Protected VLAN이 반드시 존재해야 합니다.

10.3. EAPS 프로토콜 소개

EAPS 도메인은 하나의 링 구조 위에서 동작합니다. 하나의 EAPS 도메인은 1개의 Master 노드와 하나 이상의 Transit 노드로 구성됩니다. 각 EAPS 노드는 동일한 Control VLAN 1개와 여러 개의 Protected VLAN을 가지며, 각각 Primary 포트와 Secondary 포트를 포함합니다. 이 두 포트는 Control VLAN과 모든 Protected VLAN에 동시에 속합니다. 각 노드의 Primary/Secondary 포트를 서로 연결하면 전체적으로 하나의 EAPS 링이 형성됩니다.

정상 상태에서는 도메인 내 모든 Primary 포트와 Secondary 포트가 링크 업 상태일 때, Master 노드의 Secondary 포트를 차단(blocking 상태)하여 루프를 제거합니다. 이로써 서비스 트래픽(Protected VLAN)이 링에서 루프 없이 정상적으로 전달됩니다.

링에서 장애가 발생하면, Master 노드는 즉시 자신의 Secondary 포트를 forwarding 상태로 전환하여 차단을 해제합니다. 그 결과 우회 경로가 열리면서 트래픽이 계속 전달되고, 서비스 통신이 빠르게 복구됩니다.

Transit 노드는 Primary 포트와 Secondary 포트 간에 특별한 역할 차이를 두지 않고 동일하게 처리합니다.

이후에는 EAPS의 장애 감지 및 루프 복구 방식 두 가지에 대해 설명합니다.

10.3.1. Link-Down 알림

Transit 노드에서 Primary 포트나 Secondary 포트 중 하나라도 link down 상태가 되면, 즉시 다른 정상 링크 포트를 통해 Control VLAN으로 link-down 프로토콜 패킷을 Master 노드로 전송합니다.

Master 노드가 link-down 프로토콜 패킷을 수신하면 다음과 같이 동작합니다.

Master 노드는 즉시 정상 상태(complete state)에서 장애 상태(failed state)로 전환하고, 차단되어 있던 Secondary 포트를 forwarding 상태로 변경합니다.

이와 동시에 Layer 2 및 Layer 3 포워딩 정보를 갱신하고, ring-down-flush-fdb 메시지를 전송하여 다른 Transit 노드들에게도 전달합니다.

이를 통해 각 노드는 자신의 포워딩 테이블을 갱신하고, Layer 2 및 Layer 3 정보를 다시 학습하게 됩니다.

Master 노드가 자신의 Primary 포트에서 link down을 감지한 경우에도, link-down 프로토콜을 수신했을 때와 동일한 동작을 수행합니다.

또한 Master 노드가 자신의 Secondary 포트에서 link down을 감지한 경우에도, 즉시 failed 상태로 전환하고 Layer 2/3 포워딩을 갱신하며, ring-down-flush-fdb 프로토콜 패킷을 전송하여 EAPS 도메인 내 다른 Transit 노드들이 포워딩 테이블을 갱신하고 재학습하도록 합니다.

10.3.2. Loop check

Master 노드는 Primary 포트를 통해 주기적으로 health 프로토콜 패킷을 전송합니다.

링이 정상 상태라면, 이 패킷은 링을 한 바퀴 돌아 Secondary 포트로 다시 수신됩니다. 이 경우 Master 노드는 fail period 타이머를 다시 시작하며, 상태는 complete 상태를 유지합니다.

반대로 fail period가 만료될 때까지 health 패킷을 수신하지 못하면, Master 노드는 complete 상태를 벗어나 failed 상태로 전환합니다. 이후 Secondary 포트를 forwarding 상태로 전환하고, Layer 2 및 Layer 3 포워딩 정보를 갱신합니다. 또한 ring-down-flush-fdb 메시지를 전송하여 EAPS 도메인 내 다른 Transit 노드들에게 알리고, 각 노드가 포워딩 테이블을 갱신하고 Layer 2 및 Layer 3 정보를 다시 학습하도록 합니다.

10.3.3. Ring recovery

Master 노드는 링이 complete 상태이든 failed 상태이든 관계없이 Primary 포트를 통해 health 프로토콜 패킷을 전송합니다.

Master 노드가 failed 상태일 때 Secondary 포트에서 health 프로토콜 패킷을 다시 수신하면, 링은 complete 상태로 복구됩니다. 이때 Master 노드는 Secondary 포트를 다시 blocking 상태로 설정하고, Layer 2 및 Layer 3 포워딩 정보를 갱신합니다. 또한 ring-up-flush-fdb 패킷을 전송하여 다른 장비들이 Layer 2/3 포워딩 정보를 갱신하고 다시 학습하도록 알립니다.

Transit 노드의 포트가 link down 상태에서 link up 상태로 복구되고, Master 노드가 링 복구를 감지하기 전까지는 Master 노드의 Secondary 포트가 여전히 forwarding 상태일 수 있습니다. 이 경우 일시적인 링 루프가 발생할 수 있습니다.

이를 방지하기 위해 Transit 노드는 한쪽 포트가 link up 상태이고, 다른 쪽 link down 포트가 다시 link up으로 변경되면 pre-forwarding 상태로 진입합니다. 이 상태에서는 나중에 link up된 포트도 pre-forwarding 상태가 되며, 서비스 트래픽을 전달하지 않습니다. 이를 통해 일시적으로 발생할 수 있는 데이터 루프를 차단합니다.

이후 Master 노드가 링 복구를 확인하고 ring-up-flush-fdb 패킷을 전송하면, Transit 노드는 해당 프로토콜 패킷을 수신한 후 노드 상태를 link-up 상태로 변경하고, pre-forwarding 상태였던 포트를 forwarding 상태로 전환하여 서비스 트래픽의 정상 전달을 재개합니다.

만약 Transit 노드가 ring-up-flush-fdb 프로토콜 패킷을 수신하지 못한 경우, fail time의 2배 시간이 지난 후 pre-forwarding 상태의 포트를 forwarding 상태로 전환합니다.

10.3.4. Extreme 장비와의 EAPS 호환

Extreme사는 EAPS를 최초로 지원한 제조사이며, 본 스위치의 EAPS 프로토콜은 RFC3619 표준을 따릅니다.

다만 Extreme 장비의 EAPS 프로토콜 패킷은 RFC3619 정의와 일부 차이가 있습니다.

이 스위치는 Extreme 장비와 완전히 호환되도록 설계되어 있으며, 호환 기능은 기본적으로 활성화되어 있습니다.

10.3.5. 다중 EAPS 도메인

이 스위치는 최대 16개의 EAPS 도메인을 지원합니다.

10.4. EAPS 설정

EAPS 프로토콜의 기본 설정에는 다음 요소들이 포함됩니다.

- Control VLAN
- Node Mode
- Primary Port
- Secondary Port
- Protected VLAN
- Hello Time
- Fail Time

Hello Time과 Fail Time은 기본값이 설정되어 있으며,

- Hello Time: 1초
- Fail Time: 3초

으로 동작합니다.

10.5. 제약 사항

1) Primary 포트는 EAPS 도메인의 Control VLAN에 속해야 하며, 모든 Protected VLAN의 TRUNK 모드 멤버여야 합니다.
2) EAPS 프로토콜은 MSTP 프로토콜과 동시에 동작할 수 없습니다. MSTP가 활성화되어 있거나 MSTP Instance가 설정되어 있는 경우, EAPS 프로토콜을 활성화할 수 없습니다.
3) 특정 VLAN에서 VLLP 프로토콜이 동작 중인 경우, 해당 VLAN은 EAPS의 Control VLAN 또는 Protected VLAN으로 설정할 수 없습니다.
4) EAPS의 Control VLAN에는 Primary 포트와 Secondary 포트만 포함될 수 있으며, VLAN 모드는 반드시 TRUNK 모드여야 합니다.
5) VLAN이 EAPS 도메인의 Control VLAN으로 설정되어 있고 해당 도메인이 활성화된 경우, 해당 VLAN은 삭제할 수 없으며 포트 멤버를 수정하거나 삭제할 수 없습니다. 또한 Control VLAN에는 Layer 3 인터페이스를 설정할 수 없습니다.
6) Protected VLAN에서 Primary 포트와 Secondary 포트는 반드시 TRUNK 모드여야 합니다. 그 외의 멤버 포트에는 제한이 없습니다.

7) 하나의 포트는 하나의 EAPS 도메인에서만 Primary 포트 또는 Secondary 포트로 설정할 수 있습니다.
8) 동일한 VLAN은 하나의 EAPS 도메인에서만 Control VLAN 또는 Protected VLAN으로 설정될 수 있습니다.
9) 하나의 EAPS 도메인에 속한 모든 노드의 Control VLAN은 반드시 동일해야 합니다.

10.6. EAPS 명령어 간략 소개

APS 도메인을 생성하려면 먼저 VLAN 및 포트 설정이 앞에서 설명한 조건을 만족해야 합니다.

EAPS 설정에는 일정한 순서가 필요합니다.

먼저 EAPS 도메인을 생성한 후, 도메인을 활성화하기 전에 필요한 파라미터를 설정해야 합니다.

그렇지 않으면 EAPS 도메인이 정상적으로 활성화되지 않습니다.

예를 들어 Hello Time을 현재 Fail Time보다 큰 값으로 변경하려는 경우, 먼저 Fail Time을 더 큰 값으로 변경해야 합니다.

그렇지 않으면 설정이 적용되지 않습니다.

그 외의 설정 순서에는 특별한 제한이 없습니다.

EAPS 도메인이 이미 활성화된 상태에서는 다음 항목을 수정할 수 없습니다.

- Control VLAN
- Mode
- Primary Port
- Secondary Port

반면 다음 항목은 도메인이 활성화된 상태에서도 수정할 수 있습니다.

- Protected VLAN
- Fail Timer
- Hello Time
- Extreme 상호 운용성 설정

Primary Port와 Secondary Port는 LACP 포트, 즉 TRUNK 그룹도 사용할 수 있습니다.

10.6.1. EAPS 설정 명령어

다음은 EAPS 도메인을 구성할 때 사용하는 주요 명령어입니다.

명령어	설명	모드
eaps create <ring-id>	EAPS 도메인 생성	Global configuration mode
eaps control-vlan <ring-id> <vlan-id>	EAPS 도메인의 Control VLAN 설정	Global configuration mode
eaps protected-vlan <ring-id> <vlan-id>	EAPS 도메인의 Protected VLAN 추가	Global configuration mode
eaps mode <ring-id> <master|transit>	EAPS 도메인의 노드 동작 모드 설정	Global configuration mode
eaps primary-port <ring-id> <ifname>	EAPS 도메인의 Primary 포트 설정	Global configuration mode
eaps secondary-port <ring-id> <ifname>	EAPS 도메인의 Secondary 포트 설정	Global configuration mode
eaps data-span <ring-id>	링 간 데이터 전달(크로스 링 포워딩) 설정	Global configuration mode
eaps fail-time <ring-id> <secs>	장애 감지 타이머 설정 (기본 3초)	Global configuration mode
eaps hello-time <ring-id> <secs>	헬스 체크 주기 설정 (기본 1초, fail-time보다 작아야 함)	Global configuration mode
eaps extreme-interoperability <ring-id> <enable|disable>	Extreme 장비와의 호환 설정 (기본 활성화)	Global configuration mode
eaps enable <ring-id>	EAPS 도메인 활성화	Global configuration mode
eaps disable <ring-id>	EAPS 도메인 비활성화	Global configuration mode
show eaps	전체 EAPS 도메인 상태 확인	Normal / Privileged mode
show eaps <ring-id>	특정 EAPS 도메인 상세 정보 확인	Normal / Privileged mode

10.7. EAPS 구성 예제 (Single Ring)

3대의 스위치(Switch1, Switch2, Switch3)가 링 구조로 연결되어 있고, EAPS를 통해 VLAN 1 트래픽이 루프 없이 동작하면서, 링 중 하나의 링크가 끊어져도 자동으로 우회 경로가 활성화되도록 구성하는 예제입니다.

전체 구성 개념

Control VLAN: VLAN 2

Protected VLAN: VLAN 1

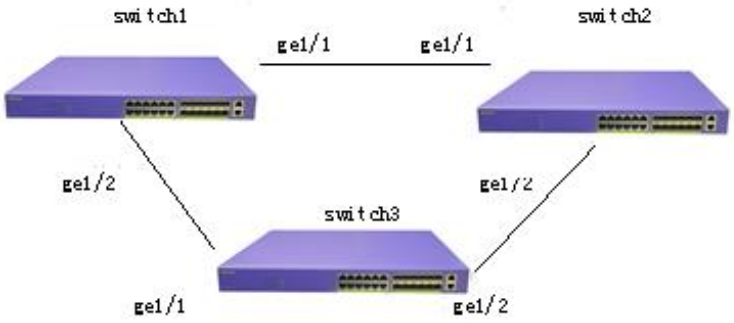
Master: Switch1

Transit: Switch2, Switch3

각 스위치:

Primary: GE1/1

Secondary: GE1/2



Switch1 설정 (Master)

Switch# configure terminal

VLAN 생성

Switch(config)# vlan database

Switch(config-vlan)# vlan 2-3

Switch(config-vlan)# exit

포트 설정

Switch(config)# interface ge1/1

Switch(config-ge1/1)# switchport mode trunk

Switch(config-ge1/1)# switchport trunk native vlan 3

Switch(config-ge1/1)# switchport trunk allowed vlan add 1,2

Switch(config)# interface ge1/2

Switch(config-ge1/2)# switchport mode trunk

Switch(config-ge1/2)# switchport trunk native vlan 3

Switch(config-ge1/2)# switchport trunk allowed vlan add 1,2

EAPS 설정

Switch(config)# eaps create 1

Switch(config)# eaps control-vlan 1 2

Switch(config)# eaps protected-vlan 1 1

Switch(config)# eaps mode 1 master

Switch(config)# eaps primary-port 1 ge1/1

Switch(config)# eaps secondary-port 1 ge1/2

Switch(config)# eaps enable 1

Switch2 설정 (Transit)

Switch# configure terminal

VLAN 생성

Switch(config)# vlan database

Switch(config-vlan)# vlan 2-3

Switch(config-vlan)# exit

포트 설정

Switch(config)# interface ge1/1

Switch(config-ge1/1)# switchport mode trunk

Switch(config-ge1/1)# switchport trunk native vlan 3

Switch(config-ge1/1)# switchport trunk allowed vlan add 1,2

Switch(config)# interface ge1/2

Switch(config-ge1/2)# switchport mode trunk

Switch(config-ge1/2)# switchport trunk native vlan 3

Switch(config-ge1/2)# switchport trunk allowed vlan add 1,2

EAPS 설정

Switch(config)# eaps create 1

Switch(config)# eaps control-vlan 1 2

Switch(config)# eaps protected-vlan 1 1

Switch(config)# eaps mode 1 transit

Switch(config)# eaps primary-port 1 ge1/1

Switch(config)# eaps secondary-port 1 ge1/2

Switch(config)# eaps enable 1

Switch3 설정 (Transit)

Switch# configure terminal

VLAN 생성

Switch(config)# vlan database

Switch(config-vlan)# vlan 2-3

Switch(config-vlan)# exit

포트 설정

Switch(config)# interface ge1/1

Switch(config-ge1/1)# switchport mode trunk

Switch(config-ge1/1)# switchport trunk native vlan 3

Switch(config-ge1/1)# switchport trunk allowed vlan add 1,2

Switch(config)# interface ge1/2

Switch(config-ge1/2)# switchport mode trunk

Switch(config-ge1/2)# switchport trunk native vlan 3

Switch(config-ge1/2)# switchport trunk allowed vlan add 1,2

EAPS 설정

Switch(config)# eaps create 1

Switch(config)# eaps control-vlan 1 2

Switch(config)# eaps protected-vlan 1 1

Switch(config)# eaps mode 1 transit

Switch(config)# eaps primary-port 1 ge1/1

Switch(config)# eaps secondary-port 1 ge1/2

Switch(config)# eaps enable 1

핵심 동작 정리

정상 상태

→ Master(Switch1)의 Secondary 포트 BLOCKING

→ 루프 없음

장애 발생

→ Secondary 포트 FORWARDING 전환

→ 우회 경로 활성화

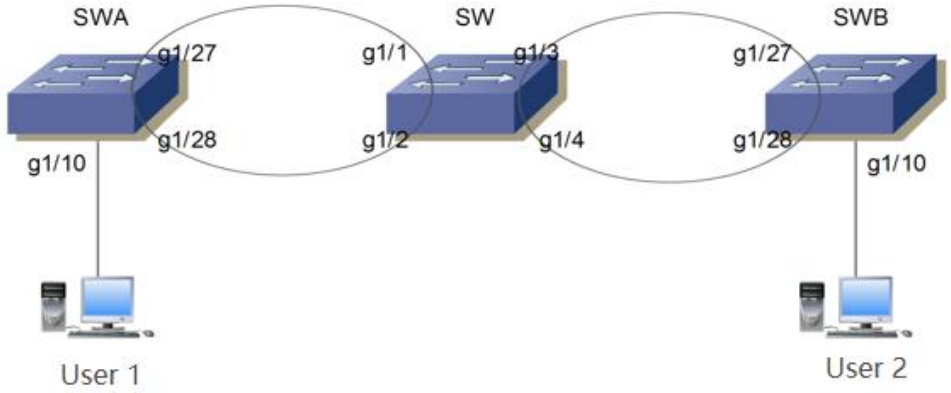
복구

→ 다시 Secondary 포트 BLOCK

→ 정상 링 구조 복귀

10.8. Cross Ring 데이터 포워딩 설정 예제

SWA, SW, SWB 3대의 스위치가 있으며, EAPS 프로토콜을 통해 링을跨跨跨跨 넘어 VLAN 1과 VLAN 2가 서로 통신하도록 구성하는 예제입니다.



SWA 설정

SWA는 Ring 1에 연결되며, Control VLAN은 VLAN 111, Protected VLAN은 VLAN 1과 VLAN 2입니다.

vlan database

vlan 2

vlan 111

interface ge1/10

switchport access vlan 2

interface ge1/27

switchport mode trunk

switchport trunk allowed vlan add 2

switchport trunk allowed vlan add 111

interface ge1/28

switchport mode trunk

switchport trunk allowed vlan add 2

switchport trunk allowed vlan add 111

eaps create 1

eaps mode 1 transit

eaps primary-port 1 ge1/27

eaps secondary-port 1 ge1/28

eaps control-vlan 1 111

eaps protected-vlan 1 1

eaps protected-vlan 1 2

eaps enable 1

SW 설정

SW는 두 개의 EAPS Ring에 동시에 연결됩니다.

Ring 1은 SWA와 연결되며, Control VLAN은 VLAN 111이고 Protected VLAN은 VLAN 1과 VLAN 2입니다.

Ring 2는 SWB와 연결되며, Control VLAN은 VLAN 222입니다.

Ring 간 데이터 포워딩을 위해 가상 Protected VLAN인 VLAN 3333을 사용합니다.

Ring 1과 Ring 2 간 데이터 전달을 위해 eaps data-span 명령을 설정해야 합니다.

vlan database

vlan 2

vlan 111

vlan 222

vlan 3333

interface ge1/1

switchport mode trunk

switchport trunk allowed vlan add 2

```
switchport trunk allowed vlan add 111

interface ge1/2
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 111

interface ge1/3
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 222
switchport trunk allowed vlan add 3333

interface ge1/4
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 222
switchport trunk allowed vlan add 3333

eaps create 1
eaps mode 1 master
eaps primary-port 1 ge1/1
eaps secondary-port 1 ge1/2
eaps control-vlan 1 111
eaps protected-vlan 1 1
eaps protected-vlan 1 2
eaps data-span 1
eaps enable 1
```

eaps create 2

eaps mode 2 transit

eaps primary-port 2 ge1/3

eaps secondary-port 2 ge1/4

eaps control-vlan 2 222

eaps protected-vlan 2 3333

eaps data-span 2

eaps enable 2

SWB 설정

SWB는 Ring 2에 연결되며, Control VLAN은 VLAN 222, Protected VLAN은 VLAN 1과 VLAN 2입니다.

vlan database

vlan 2

vlan 222

interface ge1/10

switchport access vlan 2

interface ge1/27

switchport mode trunk

switchport trunk allowed vlan add 2

switchport trunk allowed vlan add 222

interface ge1/28

switchport mode trunk

switchport trunk allowed vlan add 2

switchport trunk allowed vlan add 222

eaps create 2

eaps mode 2 master

eaps primary-port 2 ge1/27

eaps secondary-port 2 ge1/28

eaps control-vlan 2 222

eaps protected-vlan 2 1

eaps protected-vlan 2 2

eaps enable 2

VLAN 1과 VLAN 2가 서로 통신하도록 설정한 후, 필요에 따라 EAPS Node Mode는 변경할 수 있습니다.

※ 여기서 VLAN 3333은 Ring 간 데이터 전달을 위한 가상 Protected VLAN으로 사용됩니다.

11. ERPS 설정

11.1. ERPS 개요

ERPS는 Ethernet Ring Protection Switching의 약자로, ITU-T에서 정의한 G.8032 표준 기반 링 보호 프로토콜입니다.

이 프로토콜은 이더넷 링 구조에서 발생할 수 있는 루프(Loop)를 방지하고, 장애 발생 시 빠른 복구를 제공하기 위해 설계되었습니다.

링 구조가 정상일 때는 하나의 링크를 차단하여 브로드캐스트 스톰과 같은 루프 문제를 방지합니다.

그리고 링 내 특정 링크에 장애가 발생하면, 차단되어 있던 경로를 즉시 열어 노드 간 통신을 빠르게 복구합니다.

11.2. ERPS 기술 소개

11.2.1. ERPS Ring

ERPS 링은 최소 링(minimum ring) 원칙을 기반으로 구성됩니다.

즉, 하나의 ERPS 링은 가능한 한 가장 작은 단위의 링 구조로 설계되어야 합니다.

ERPS 링은 다음과 같이 구분됩니다.

- Main Ring: 완전히 닫힌(Closed) 링 구조
- Sub Ring: 닫히지 않은(Open) 링 또는 추가로 구성된 보조 링

이러한 링 구성은 모두 명령어를 통해 설정해야 합니다.

ERPS 링 상태 (State)

각 ERPS 링은 총 5가지 상태를 가집니다.

- Idle 상태
  모든 물리 링크가 정상적으로 연결된 상태입니다.
- Protection 상태
  링 내 하나 이상의 링크가 단절된 상태로, 보호 동작이 수행되는 상태입니다.
- Manual Switch 상태
  관리자가 수동으로 링의 상태를 변경한 상태입니다.
- Forced Switch 상태
  강제로 트래픽 경로를 변경한 상태입니다.
- Pending 상태
  상태 전환 중에 있는 중간 단계 상태입니다.

11.2.2. ERPS Node

ERPS 링에 참여하는 Layer 2 스위칭 장비를 Node라고 합니다.

각 Node에서 동일한 ERPS 링에 참여할 수 있는 포트는 최대 2개이며, 하나는 RPL 포트, 다른 하나는 일반

Ring 포트로 구성됩니다.

전체 구조에서 Node 역할은 다음 두 가지로 구분할 수 있습니다.

- Intersecting Node
  여러 ERPS 링에 동시에 속하는 Node를 의미합니다.
- Non-intersecting Node
  하나의 ERPS 링에만 속하는 Node를 의미합니다.

ERPS 프로토콜에서 정의하는 주요 Node 모드는 다음과 같습니다.

1) RPL Owner Node
   하나의 ERPS 링에는 RPL Owner Node가 하나만 존재합니다.
   이 역할은 사용자가 직접 설정합니다.
   RPL Owner Node는 루프 방지를 위해 RPL 포트를 차단합니다.
   이후 ERPS 링 내 다른 Node 또는 링크에 장애가 발생했다는 메시지를 수신하면, 차단되어 있던 RPL 포트를 자동으로 해제합니다.
   이를 통해 해당 포트가 다시 트래픽을 송수신할 수 있게 되어, 서비스 트래픽이 중단되지 않도록 보장합니다.
2) RPL Neighbour Node
   RPL Neighbour Node는 RPL Owner Node의 RPL 포트와 직접 연결된 Node를 의미합니다.
   정상 상태에서는 루프 방지를 위해 RPL Owner Node의 RPL 포트와 RPL Neighbour Node의 RPL 포트가 모두 차단됩니다.
   ERPS 링에 장애가 발생하면 두 RPL 포트가 모두 차단 해제되어 트래픽 전달에 사용됩니다.
3) Ordinary Ring Node
   Ordinary Ring Node는 ERPS 링에서 RPL Owner Node와 RPL Neighbour Node를 제외한 일반 Node입니다.
   Ordinary Ring Node의 RPL 포트는 일반 Ring 포트와 특별한 차이가 없습니다.
   Ordinary Ring Node의 Ring 포트는 직접 연결된 링크 상태를 감시하며, 링크 상태가 변경되면 해당 정보를 다른 Node에 즉시 전달합니다.

11.2.3. Link 및 Channel

1) RPL (Ring Protection Link): 각 ERPS 링에는 하나의 RPL만 존재하며, 이는 RPL Owner 노드의 RPL 포트가 위치한 링크를 의미합니다. Ethernet 링이 Idle 상태일 때, RPL 링크는 blocking 상태에 있으며 데이터 패킷을 전달하지 않아 루프 생성을 방지합니다.
2) Sub-ring link: Sub-ring에 속한 링크로, 교차 링(intersecting ring) 구조에서 sub-ring에 의해 제어되

는 링크를 의미합니다.

3) RAPS (Ring Auto Protection Switch) 가상 채널: 교차 링 구조에서, 교차 노드 간 경로 중 sub-ring에 속하지 않지만 sub-ring 프로토콜 메시지를 전달하기 위해 사용되는 경로를 sub-ring의 RAPS 가상 채널이라고 합니다.

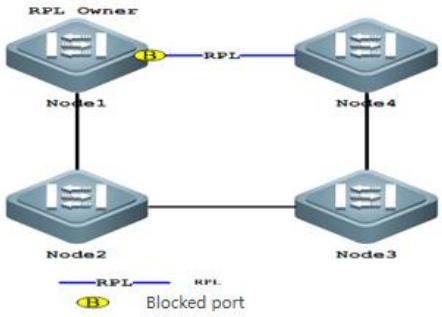
11.2.4. ERPS VLAN

ERPS에는 두 가지 유형의 VLAN이 있습니다.

1) RAPS VLAN: ERPS 프로토콜 메시지를 전달하는 데 사용됩니다. ERPS 링에 연결된 장비의 모든 포트는 RAPS VLAN에 속하며, ERPS 링에 연결된 포트만 이 VLAN에 참여할 수 있습니다. 서로 다른 링은 서로 다른 RAPS VLAN을 사용해야 합니다. 또한 RAPS VLAN 인터페이스에는 IP 주소를 설정할 수 없습니다.
2) Data VLAN: RAPS VLAN과 반대로, 데이터 VLAN은 데이터 패킷을 전달하는 데 사용됩니다. Data VLAN에는 ERPS 링 포트와 비 ERPS 링 포트가 모두 포함될 수 있습니다.

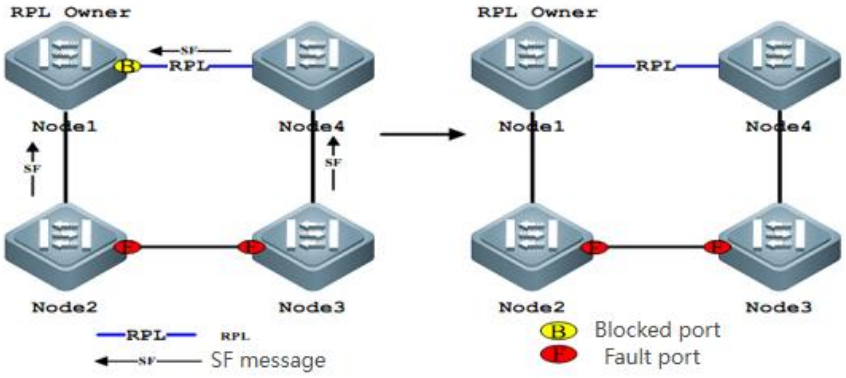
11.3. ERPS 동작 원리

11.3.1. Normal State



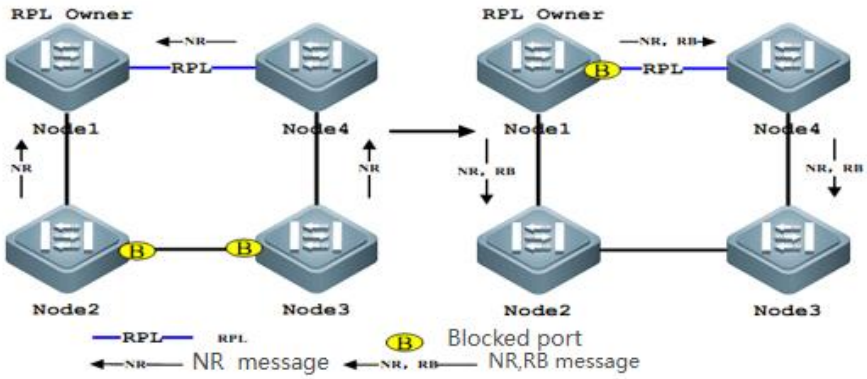
1) 모든 노드는 물리적으로 링 형태의 토폴로지로 연결됩니다.
2) 루프 보호 프로토콜은 RPL 링크를 차단함으로써 루프가 생성되지 않도록 합니다. 위 그림에서 Node1과 Node4 사이의 링크가 RPL 링크입니다.
3) 인접한 노드 간 각 링크에 대해 장애 감지를 수행합니다.

11.3.2. Link failure



1) 장애가 발생한 링크에 인접한 노드는 해당 링크를 차단하고, RAPS(SF) 메시지를 사용하여 링 내 다른 노드들에게 장애를 보고합니다. 위 그림과 같이 Node2와 Node3 사이의 링크에 장애가 발생했다고 가정하면, Node2와 Node3은 holdoff 타이머가 만료된 후 해당 링크를 차단하고, 각각 링 네트워크의 각 노드로 RAPS(SF) 메시지를 전송합니다.
2) RAPS(SF) 메시지는 RPL Owner 노드가 RPL 포트를 개방하도록 트리거합니다. 또한 이 메시지는 모든 노드가 각자의 MAC 엔트리를 갱신하도록 하며, 이후 노드들은 보호 상태(protection state)로 진입합니다.

11.3.3. Link Recovery

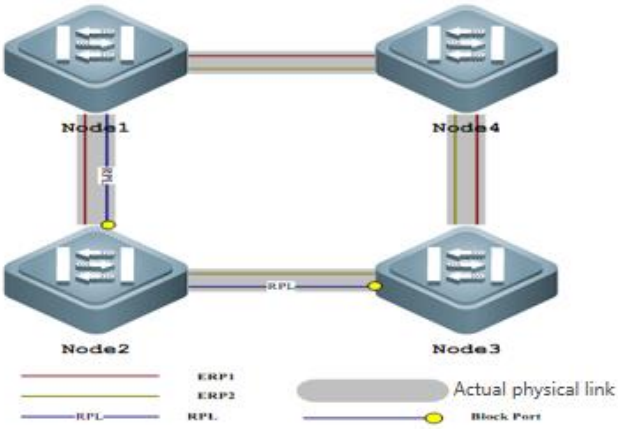


1) 장애가 복구되면, 해당 장애에 인접한 노드는 계속해서 차단 상태를 유지하면서 로컬 장애가 없음을 알리는 RAPS(NR) 메시지를 전송합니다.
2) Guard 타이머가 만료된 후, RPL Owner 노드는 첫 번째 RAPS(NR) 메시지를 수신하면 WTR(Wait-To-Restore) 타이머를 시작합니다.
3) WTR 타이머가 만료되면, RPL Owner 노드는 RPL을 다시 차단하고 RAPS(NR, RB) 메시지를 전송합니다.
4) 다른 노드들은 해당 메시지를 수신한 후 각자의 MAC 테이블을 갱신하고, RAPS(NR) 메시지를 보내

던 노드는 주기적인 메시지 전송을 중단하며 기존에 차단되어 있던 포트를 개방합니다. 이후 링 네트워크는 원래의 정상 상태로 복구됩니다.

11.4. ERPS 기술 특징

11.4.1. ERPS Load Balancing



동일한 물리적 링 네트워크에 여러 개의 Instance와 여러 개의 ERPS Ring을 구성하고, 서로 다른 ERPS Ring이 서로 다른 VLAN 트래픽(Protected VLAN)을 전달하도록 설정할 수 있습니다.

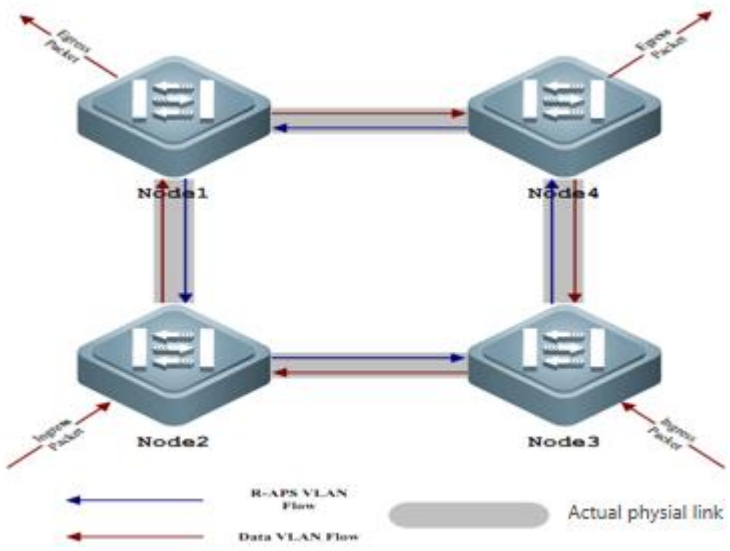
이를 통해 링 네트워크 내에서 VLAN별 데이터 트래픽 토폴로지를 서로 다르게 구성할 수 있으며, 결과적으로 트래픽 부하 분산을 실현할 수 있습니다.

위 그림과 같이 하나의 물리적 링 네트워크가 두 개의 Instance와 두 개의 ERPS Ring에 대응됩니다. 두 ERPS Ring이 보호하는 VLAN은 서로 다릅니다.

ERP 1에서는 Node2가 RPL Owner Node이고, ERP 2에서는 Node3이 RPL Owner Node입니다.

설정을 통해 서로 다른 VLAN이 각각 다른 링크를 차단하도록 구성할 수 있으며, 이를 통해 하나의 링에서 부하 분산을 구현할 수 있습니다.

11.4.2. 높은 보안성

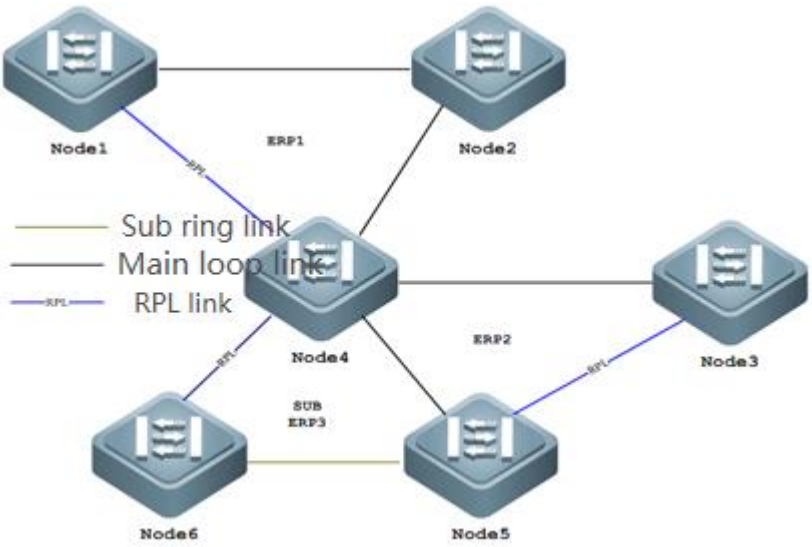


ERPS에는 두 가지 유형의 VLAN이 있습니다. 하나는 RAPS VLAN이고, 다른 하나는 Data VLAN입니다.

RAPS VLAN은 ERPS 프로토콜 메시지를 전달하는 용도로만 사용됩니다. ERPS는 RAPS VLAN에서 수신된 프로토콜 메시지만 처리하며, Data VLAN에서 유입되는 어떠한 프로토콜 공격 메시지도 처리하지 않습니다.

이를 통해 ERPS의 보안성을 향상시킬 수 있습니다.

11.4.3. 다중 링 접점/교차 지원



위 그림과 같이 ERPS는 하나의 노드(Node4)에 여러 개의 링을 접점(tangency) 또는 교차(intersection) 형태로 연결하는 것을 지원합니다. 이를 통해 네트워크 구성의 유연성을 크게 향상시킬 수 있습니다.

11.5. ERPS 프로토콜 명령어

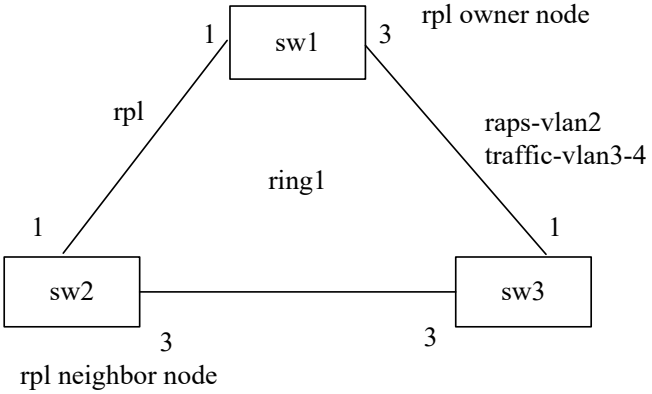
명령어	설명	모드
erps predefine configuration (ring-node | rpl-owner-node)	ERPS 사전 정의 구성 활성화	Global Configuration Mode
no erps predefine configuration	ERPS 사전 정의 구성 비활성화	Global Configuration Mode
erps <1-8>	ERPS 인스턴스 생성	Global Configuration Mode
no erps <1-8>	ERPS 인스턴스 삭제	Global Configuration Mode
node-role (interconnection | none-interconnection)	ERPS 링에서 노드 역할 설정 (교차/비교차)	ERPS Mode
ring <1-32>	ERPS 링 생성	ERPS Mode
no ring <1-32>	ERPS 링 삭제	ERPS Mode
ring <1-32> ring-mode (major-ring | sub-ring)	ERPS 링 모드 설정 (메인 링 / 서브 링)	ERPS Mode
ring <1-32> node-mode (rpl-owner-node | rpl-neighbor-node | ring-node)	ERPS 링 노드 모드 설정 (RPL Owner / Neighbor / 일반 노드)	ERPS Mode
ring <1-32> raps-vlan <2-4094>	ERPS 링 프로토콜 VLAN 설정	ERPS Mode
no ring <1-32> raps-vlan	ERPS 링 프로토콜 VLAN 삭제	ERPS Mode
ring <1-32> traffic-vlan <1-4094>	ERPS 링 데이터 VLAN 설정	ERPS Mode
no ring <1-32> traffic-vlan <1-4094>	ERPS 링 데이터 VLAN 삭제	ERPS Mode
ring <1-32> (rpl-port | rl-port) IFNAME	ERPS 링 포트 설정 (RPL 포트 또는 일반 링 포트)	ERPS Mode
no ring <1-32> (rpl-port | rl-port)	ERPS 링 포트 설정 제거	ERPS Mode
ring <1-32> revertive-behaviour (revertive |	ERPS 링 복구 동작 설정 (복구형 /	ERPS Mode

명령어	설명	모드
non-revertive)	비복구형)	
ring <1-32> hold-off-time <0-10000>	ERPS 링 Hold-off 타이머 설정	ERPS Mode
no ring <1-32> hold-off-time	Hold-off 타이머 기본값 복구	ERPS Mode
ring <1-32> guard-time <10-2000>	ERPS 루프 보호 타이머 설정	ERPS Mode
no ring <1-32> guard-time	루프 보호 타이머 기본값 복구	ERPS Mode
ring <1-32> wtr-time <1-12>	ERPS 링 WTR(복구 대기) 시간 설정	ERPS Mode
no ring <1-32> wtr-time	WTR 기본값 복구	ERPS Mode
ring <1-32> wtb-time <1-10>	ERPS 링 WTB 시간 설정	ERPS Mode
no ring <1-32> wtb-time	WTB 기본값 복구	ERPS Mode
ring <1-32> raps-send-time <1-10>	ERPS 프로토콜 메시지 전송 주기 설정	ERPS Mode
no ring <1-32> raps-send-time	전송 주기 기본값 복구	ERPS Mode
ring <1-32> (enable | disable)	ERPS 링 활성화 / 비활성화	ERPS Mode
ring <1-32> forced-switch IFNAME	ERPS 링 포트 강제 전환	ERPS Mode
ring <1-32> clear forced-switch	강제 전환 해제	ERPS Mode
ring <1-32> manual-switch IFNAME	ERPS 링 포트 수동 전환	ERPS Mode
ring <1-32> clear manual-switch	수동 전환 해제	ERPS Mode
ring <1-32> clear recovery	수동 복구 (비복구 모드 또는 WTR/WTB 이전 복구)	ERPS Mode
show erps	전체 ERPS 인스턴스 및 링 요약 확인	Privileged Mode
show erps <1-8>	특정 ERPS 인스턴스 및 링 상세 정보 확인	Privileged Mode

11.6. ERPS 대표 적용 예제

11.6.1. Single Ring Example

아래 그림과 같이 sw1, sw2, sw3 노드가 하나의 ERPS 단일 링(ring1)을 구성합니다. 각 노드의 포트 1과 포트 3이 ERPS 링 포트로 사용되며, 프로토콜 VLAN은 2, 데이터 VLAN은 3과 4입니다. sw1은 RPL Owner 노드이고, sw2는 RPL Neighbor 노드입니다. sw1과 sw2 사이의 링크는 RPL 링크입니다.



1) SW1 설정

```
Switch> enable
Switch# configure terminal

# ERPS 프로토콜 및 데이터 VLAN 생성
Switch(config)# vlan database
Switch(config-vlan)# vlan 2-4
Switch(config-vlan)# exit

# 링 포트를 trunk 모드로 설정하고 VLAN 추가
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)# exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
```

```
Switch(config-ge1/3)# exit

# ERPS 인스턴스 및 링 설정
Switch(config)# erps 1
Switch(config-erps-1)# ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)# exit
```

2) SW2 설정

```
Switch> enable
Switch# configure terminal

# VLAN 생성
Switch(config)# vlan database
Switch(config-vlan)# vlan 2-4
Switch(config-vlan)# exit

# 포트 설정
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)# exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)# exit

# ERPS 설정
```

```
Switch(config)# erps 1
Switch(config-erps-1)# ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)# exit
```

3) SW3 설정

```
Switch> enable
Switch# configure terminal

# VLAN 생성
Switch(config)# vlan database
Switch(config-vlan)# vlan 2-4
Switch(config-vlan)# exit

# 포트 설정
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)# exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)# exit

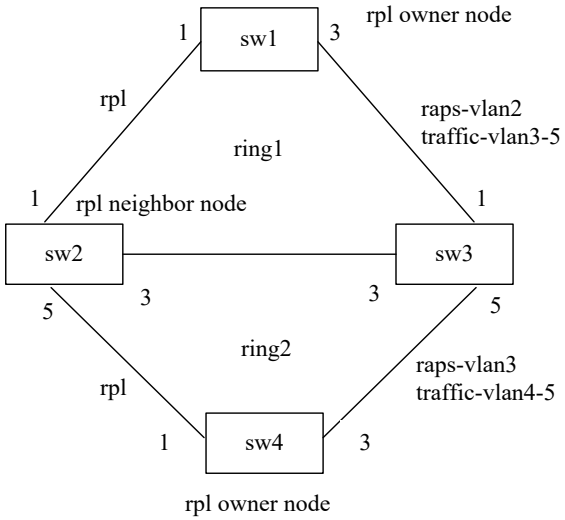
# ERPS 설정
Switch(config)# erps 1
Switch(config-erps-1)# ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
```

```
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)# exit
```

11.6.2. Multi-loop 예제 (번역)

아래 그림과 같이 sw1, sw2, sw3 노드는 ERPS 메인 링 ring1을 구성합니다. 각 노드의 포트 1과 3은 메인 링 ring1의 링 포트로 사용됩니다. 메인 링 ring1의 프로토콜 VLAN은 2이고, 데이터 VLAN은 3, 4, 5입니다. sw1 노드는 메인 링 ring1의 RPL owner 노드이며, sw2 노드는 RPL neighbor 노드입니다. sw1과 sw2 사이의 링크는 메인 링 ring1의 RPL 링크입니다.

sw2, sw3, sw4 노드는 ERPS 서브링 ring2를 구성합니다. sw2와 sw3의 포트 5, 그리고 sw4의 포트 1과 3이 서브링 ring2의 링 포트로 사용됩니다. 서브링 ring2의 프로토콜 VLAN은 3이고, 데이터 VLAN은 4와 5입니다. sw4 노드는 서브링 ring2의 RPL owner 노드이며, sw2와 sw4 사이의 링크는 서브링 ring2의 RPL 링크입니다.



1) SW1 설정

```
Switch>enable
Switch#configure terminal

# VLAN 생성
```

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-5
Switch(config-vlan)#exit

# 포트 설정
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)#exit

# ERPS 설정
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

2) SW2 설정

```
Switch>enable
Switch#configure terminal

Switch(config)#vlan database
```

```
Switch(config-vlan)#vlan 2-5
Switch(config-vlan)#exit

Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)#exit

Switch(config)# interface ge1/5
Switch(config-ge1/5)# switchport mode trunk
Switch(config-ge1/5)# switchport trunk allowed vlan add 3
Switch(config-ge1/5)# switchport trunk allowed vlan add 4
Switch(config-ge1/5)# switchport trunk allowed vlan add 5
Switch(config-ge1/5)#exit

Switch(config)#erps 1
Switch(config-erps-1)# node-role interconnection

# 메인 링
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
```

서브 링
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode ring-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port ge1/5
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit

3) SW3 설정
Switch>enable
Switch#configure terminal

Switch(config)#vlan database
Switch(config-vlan)#vlan 2-5
Switch(config-vlan)#exit

Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)#exit

Switch(config)# interface ge1/5
Switch(config-ge1/5)# switchport mode trunk
Switch(config-ge1/5)# switchport trunk allowed vlan add 3
Switch(config-ge1/5)# switchport trunk allowed vlan add 4
Switch(config-ge1/5)# switchport trunk allowed vlan add 5
Switch(config-ge1/5)#exit

```
Switch(config)#erps 1
Switch(config-erps-1)# node-role interconnection

Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable

Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode ring-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port ge1/5
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit
```

4) SW4 설정

```
Switch>enable
Switch#configure terminal

Switch(config)#vlan database
Switch(config-vlan)#vlan 3-5
Switch(config-vlan)#exit

Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)#exit
```

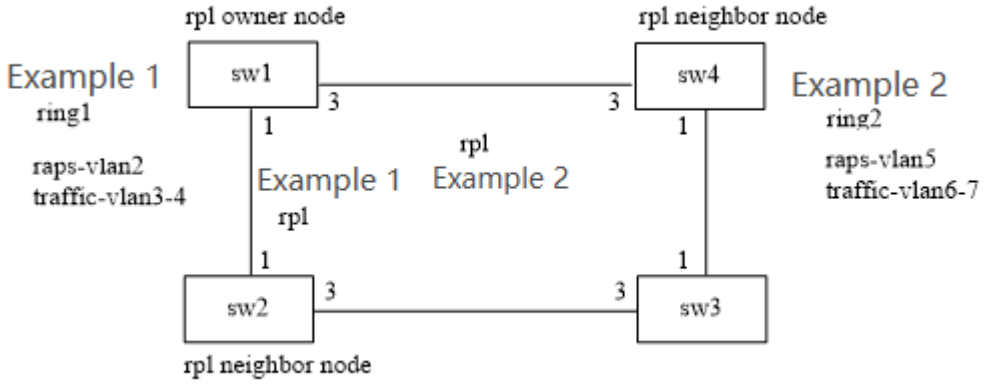
```
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)#exit

Switch(config)#erps 1
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode rpl-owner-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 1
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port ge1/1
Switch(config-erps-1)# ring 2 rl-port ge1/3
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit
```

11.6.3. Multi-Instance Load Balancing Example

아래 그림과 같이 sw1, sw2, sw3, sw4 노드는 ERPS 인스턴스 1의 단일 링 ring1을 구성합니다. 각 노드의 포트 1과 3이 ERPS 링 포트로 사용됩니다. 링의 프로토콜 VLAN은 2이고, 데이터 VLAN은 3과 4입니다. sw1 노드는 RPL owner 노드이고, sw2 노드는 RPL neighbor 노드입니다. sw1과 sw2 사이의 링크는 RPL 링크입니다.

또한 sw1, sw2, sw3, sw4 노드는 ERPS 인스턴스 2의 단일 링 ring2를 구성합니다. 각 노드의 포트 1과 3이 ERPS 링 포트로 사용됩니다. 링의 프로토콜 VLAN은 5이고, 데이터 VLAN은 6과 7입니다. sw1 노드는 RPL owner 노드이며, sw4 노드는 RPL neighbor 노드입니다. sw1과 sw4 사이의 링크는 RPL 링크입니다.



1) 설정 예제 1

SW1 설정

```
Switch>enable
Switch#configure terminal

Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit

Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit

Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

SW2, SW3, SW4 설정

→ 동일한 방식으로 VLAN 및 trunk 구성 후

→ node-mode만 각각 rpl-neighbor-node 또는 ring-node로 설정

→ 나머지 구성은 동일하게 적용됨

2) 설정 예제 2

SW1 설정

```
Switch>enable
Switch#configure terminal

Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit

Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)# switchport trunk allowed vlan add 6
Switch(config-ge1/1)# switchport trunk allowed vlan add 7
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)# switchport trunk allowed vlan add 6
Switch(config-ge1/3)# switchport trunk allowed vlan add 7
Switch(config-ge1/3)#exit

Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode rpl-owner-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 1
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port ge1/3
Switch(config-erps-2)# ring 2 rl-port ge1/1
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
```

SW2, SW3, SW4 설정

→ 동일한 방식으로 VLAN 및 trunk 구성

→ node-mode를 ring-node 또는 rpl-neighbor-node로 설정

→ 나머지 구성 동일

12. AAA 설정

이 장에서는 스위치에서 802.1X와 RADIUS를 구성하여 비인가 사용자의 네트워크 접근을 방지하는 방법을 설명합니다. 802.1X 클라이언트와 HyperBoss의 사용 방법은 각각의 매뉴얼을 참고하십시오. 본 장에서는 다음 내용을 포함합니다.

- 802.1X 소개
- RADIUS 소개
- 802.1X 설정
- RADIUS 설정

AAA는 Authentication, Authorization, Accounting의 약자입니다.

이는 인증, 권한 부여, 과금 기능을 구성하기 위한 일관된 프레임워크를 제공합니다.

AAA 설정은 일종의 네트워크 보안 관리이며, 여기서의 보안은 주로 접근 제어를 의미합니다.

예를 들어 다음과 같은 내용을 포함합니다.

- 어떤 사용자가 네트워크에 접근할 수 있는가
- 접근 가능한 사용자에게 어떤 서비스를 제공할 것인가
- 네트워크 자원을 사용하는 사용자에 대해 어떻게 과금할 것인가
- Authentication (인증): 사용자가 네트워크에 접근 가능한지 확인
- uthorization (권한 부여): 인증된 사용자가 이용할 수 있는 서비스 정의
- Accounting (과금): 사용자의 네트워크 자원 사용 내역 기록

네트워크 장비 업체들은 802.1X 클라이언트, 인증을 지원하는 다양한 스위치, 그리고 HyperBoss 인증/과금 시스템을 포함한 AAA 솔루션을 제공합니다.

802.1X 클라이언트는 사용자 PC에 설치되며, 네트워크 접근 시 인증을 수행해야 합니다. 인증이 완료된 사용자만 네트워크를 사용할 수 있습니다.

스위치는 클라이언트로부터 인증 요청을 수신하고, 사용자 이름과 비밀번호를 인증/과금 시스템인 HyperBoss로 전달합니다. 스위치는 실제 인증 처리를 수행하지 않습니다.

HyperBoss는 스위치로부터 전달받은 인증 요청을 기반으로 실제 인증을 수행하며, 인증이 완료된 사용자에 대해 과금 처리를 진행합니다.

- 802.1X 프로토콜은 클라이언트와 스위치 간 통신에 사용되며,
- RADIUS 프로토콜은 스위치와 HyperBoss 간 통신에 사용됩니다.

12.1. 802.1X 소개

802.1X 프로토콜은 포트 기반 접근 제어 및 인증 프로토콜입니다. 여기서 포트는 물리 포트뿐만 아니라 MAC 주소, VLAN ID 등과 같은 논리적인 포트도 포함할 수 있습니다. 네트워크 스위치는 MAC 주소 기반으로 802.1X 프로토콜을 구현합니다.

802.1X는 Layer 2 프로토콜입니다. 따라서 인증을 수행하는 스위치와 사용자 PC는 동일한 서브넷에 있어야 하며, 프로토콜 패킷은 다른 네트워크 구간을 통과할 수 없습니다.

802.1X 인증은 클라이언트-서버 모델을 사용하며, 모든 사용자를 인증하기 위한 서버가 반드시 필요합니다. 사용자가 인증을 통과하기 전에는 스위치 포트를 통해 인증 트래픽만 통과할 수 있습니다. 인증이 성공적으로 완료된 이후에야 데이터 트래픽이 해당 포트를 통해 전달될 수 있습니다. 즉, 사용자는 네트워크에 접근하기 전에 반드시 인증을 거쳐야 합니다.

이 절에서는 다음 내용을 포함합니다.

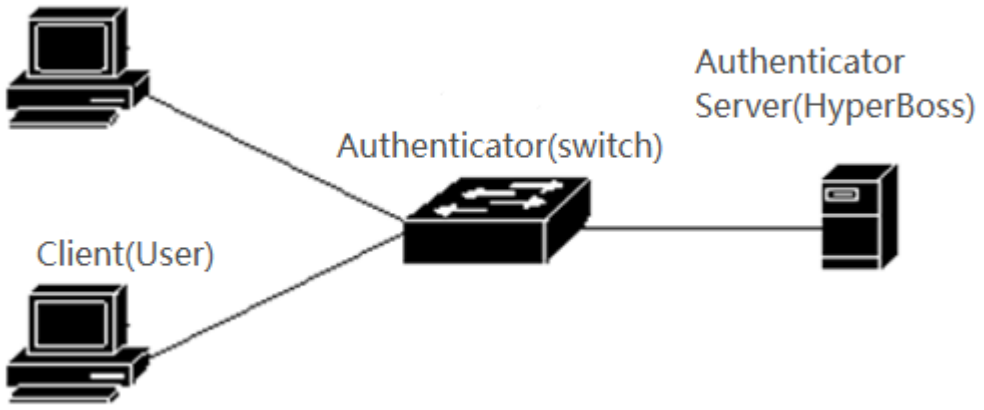
- 802.1X 장비 구성
- 프로토콜 패킷 소개
- 프로토콜 동작 흐름
- 802.1X 포트 상태

12.1.1. 802.1X 장비 구성

802.1X 장비는 다음 세 가지 요소로 구성됩니다.

- 클라이언트(Supplicant System)
- 인증 시스템(Authenticator System)
- 인증 서버(Authentication Server System)

아래 그림은 802.1X 장비 구성을 나타냅니다.



802.1X 장비

클라이언트는 네트워크 접근을 요청하는 장비를 의미하며, 일반적으로 사용자 PC와 같은 사용자 단말 시스템입니다. 사용자 단말에는 802.1X 클라이언트 소프트웨어가 설치되어 있어야 하며, 이 소프트웨어는 802.1X 프로토콜의 클라이언트 부분을 구현합니다. 클라이언트는 802.1X 인증 요청을 시작하여 인증 서버가 자신의 사용자 이름과 비밀번호를 인증하도록 요청합니다. 인증이 성공하면 사용자는 네트워크에 접근할 수 있습니다.

인증 시스템은 인증을 수행하는 장비를 의미하며, 예를 들어 스위치가 이에 해당합니다. 인증 시스템은 사용자의 논리 포트 상태, 즉 MAC 주소 상태를 기준으로 사용자의 네트워크 접근 가능 여부를 제어합니다. 사

용자의 논리 포트 상태가 unauthorized이면 사용자는 네트워크에 접근할 수 없습니다. 반대로 사용자의 논리 포트 상태가 authorized이면 사용자는 네트워크에 접근할 수 있습니다.

인증 시스템은 클라이언트와 인증 서버 사이의 중계 역할을 합니다. 인증 시스템은 사용자의 식별 정보를 요청하고, 사용자의 식별 정보를 인증 서버로 전달하며, 인증 서버가 보낸 인증 결과를 클라이언트로 전달합니다.

인증 시스템은 사용자와 가까운 쪽에서는 802.1X 프로토콜의 서버 역할을 수행해야 하며, 인증 서버와 가까운 쪽에서는 RADIUS 프로토콜의 클라이언트 역할을 수행해야 합니다. 인증 시스템의 RADIUS 클라이언트는 802.1X 클라이언트가 보낸 EAP 정보를 RADIUS 패킷에 캡슐화하여 인증 서버로 전송합니다. 또한 인증 서버가 보낸 RADIUS 프로토콜 패킷에서 EAP 정보를 역캡슐화한 후, 802.1X 서버 기능을 통해 802.1X 클라이언트로 전달합니다.

인증 서버는 실제로 사용자를 인증하는 장비를 의미합니다. 인증 서버는 인증 시스템이 전달한 사용자의 식별 정보를 수신하여 검증합니다. 인증이 성공하면 인증 서버는 인증 시스템에 권한을 부여하고 사용자가 네트워크에 접근할 수 있도록 허용합니다. 인증이 실패하면 인증 서버는 인증 시스템에 사용자 인증 실패를 알리고, 해당 사용자의 네트워크 접근을 차단합니다.

인증 서버는 EAP로 확장된 RADIUS 프로토콜을 통해 인증 시스템과 통신합니다. 네트워크에서는 사용자 인증 및 과금을 위해 HyperBoss 인증/과금 시스템을 제공합니다.

12.1.2. 프로토콜 패킷 소개

802.1X 프로토콜에서 네트워크 상으로 전달되는 인증 데이터 스트림은 EAPOL(EAP Over LAN) 프레임 형식을 사용합니다. 모든 사용자 식별 정보(사용자 이름, 비밀번호 포함)는 EAP(Extensible Authentication Protocol)에 캡슐화되며, 이 EAP는 다시 EAP 프레임에 캡슐화됩니다. 사용자 이름은 EAP 내에서 평문으로 존재하고, 비밀번호는 MD5 방식으로 암호화되어 저장됩니다.

	Octet Number
PAE Ethernet Type	1-2
Protocol Version	3
Packet Type	4
Packet Body Length	5-6
Packet Body	7-N

EAPOL 프레임 형식은 다음과 같습니다.

PAE Ethernet Type은 EAPOL을 위한 이더넷 프로토콜 타입으로 값은 0x888E입니다. Protocol Version은 EAPOL 버전 번호로 값은 1입니다. Packet Type은 EAPOL 프레임 유형을 나타냅니다. Packet Body Length는 EAPOL 프레임 내용의 길이이며, Packet Body는 실제 EAPOL 프레임의 내용을 의미합니다.

스위치는 다음 세 가지 유형의 EAPOL 프로토콜 프레임을 사용합니다.

- EAPOL-Start: Packet Type 값이 1인 경우로, 인증 시작 프레임입니다. 사용자가 인증이 필요할

때 클라이언트가 먼저 생성하여 스위치로 전송합니다.

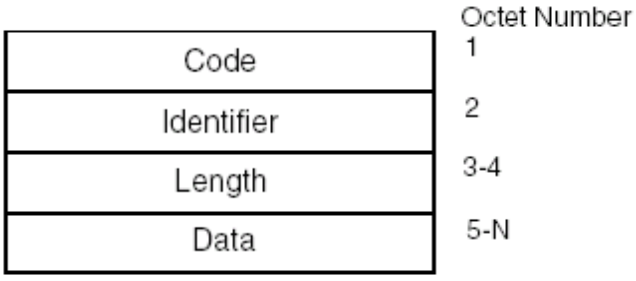
- EAPOL-Logoff: Packet Type 값이 2인 경우로, 로그오프 요청 프레임입니다. 사용자가 네트워크 사용을 종료할 때 스위치에 통보하기 위해 전송됩니다.
- EAP-Packet: Packet Type 값이 0인 경우로, 실제 인증 정보를 전달하는 프레임입니다.

EAP 패킷 형식은 다음과 같습니다.

Code는 EAP 패킷 유형을 의미하며 Request, Response, Success, Failure가 있습니다. Identifier는 Request와 Response를 매칭하기 위한 식별자입니다. Length는 헤더를 포함한 EAP 패킷의 길이입니다. Data는 EAP 패킷의 실제 데이터입니다.

EAP 패킷은 다음 네 가지 유형으로 구분됩니다.

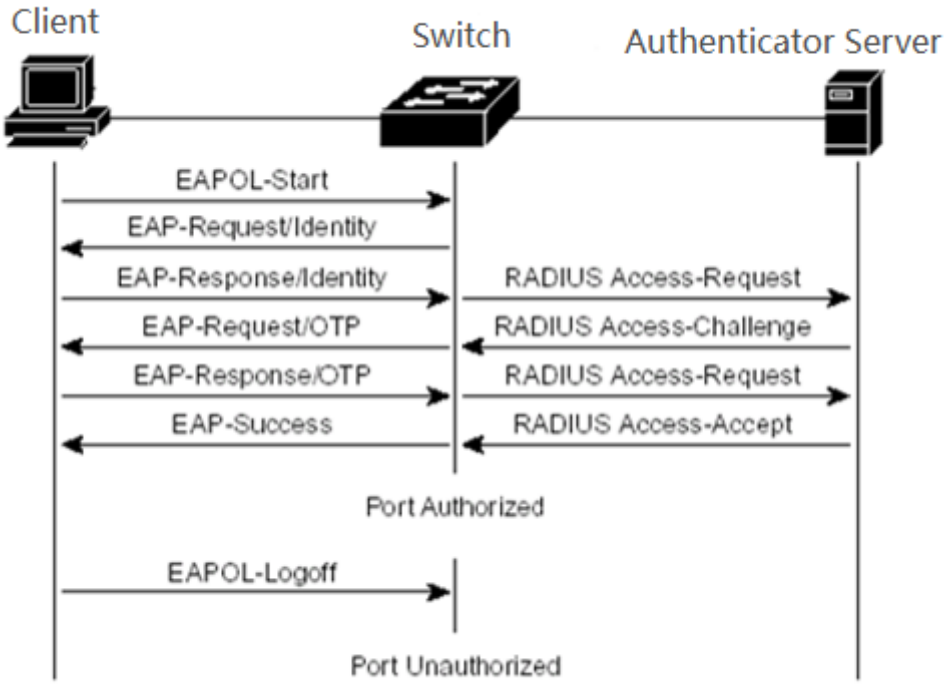
- EAP-Request: Code 값이 1이며, 스위치가 클라이언트에게 사용자 이름 또는 비밀번호 입력을 요청할 때 사용됩니다.
- EAP-Response: Code 값이 2이며, 클라이언트가 사용자 이름 또는 비밀번호를 스위치로 전달할 때 사용됩니다.
- EAP-Success: Code 값이 3이며, 스위치가 클라이언트에게 인증 성공을 알릴 때 사용됩니다.
- EAP-Failure: Code 값이 4이며, 스위치가 클라이언트에게 인증 실패를 알릴 때 사용됩니다.



EAP packet format

12.1.3. 프로토콜 동작 흐름

스위치에서 802.1X가 활성화되고 포트 상태가 Auto일 경우, 해당 포트에 접속하는 모든 사용자는 네트워크 접근 전에 반드시 인증을 수행해야 합니다. 프로토콜 상호작용은 아래와 같습니다.



클라이언트가 시작하는 인증 프로토콜 상호작용

사용자가 네트워크에 접근하려고 하면, 클라이언트는 먼저 스위치로 EAPOL-Start를 전송하여 인증을 요청합니다. 스위치는 이 요청을 수신한 후 사용자 이름을 요구하는 EAP-Request를 전송합니다.

클라이언트는 EAP-Response로 사용자 이름을 응답하고, 스위치는 이 EAP 정보를 추출하여 RADIUS 패킷에 캡슐화한 뒤 인증 서버로 전달합니다.

인증 서버는 사용자 비밀번호를 요구하고, 이에 따라 스위치는 다시 클라이언트에게 EAP-Request를 전송하여 비밀번호 입력을 요청합니다.

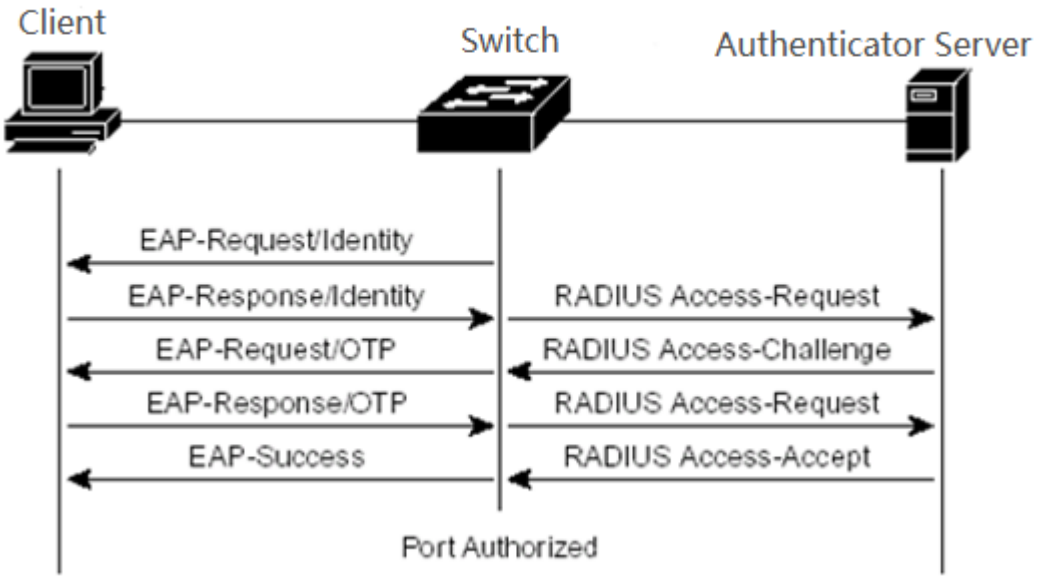
클라이언트는 비밀번호를 포함한 EAP-Response를 전송하고, 스위치는 이를 다시 RADIUS 패킷으로 캡슐화하여 인증 서버로 전달합니다.

인증 서버는 사용자 이름과 비밀번호를 기반으로 인증을 수행합니다. 인증이 성공하면 인증 서버는 스위치에 이를 통보하고, 스위치는 클라이언트에게 EAP-Success를 전송하며 사용자의 논리 포트를 authorized 상태로 변경합니다. 클라이언트가 EAP-Success를 수신하면 인증이 완료된 것이며, 사용자는 네트워크를 사용할 수 있습니다.

사용자가 네트워크 사용을 종료하면, 클라이언트는 스위치로 EAPOL-Logoff를 전송합니다. 스위치는 사용자의 논리 포트를 unauthorized 상태로 변경하며, 이후 사용자는 네트워크에 접근할 수 없습니다.

클라이언트의 비정상 종료를 방지하기 위해 스위치는 재인증(re-authentication) 메커니즘을 제공합니다. 재인증 주기는 스위치에서 설정할 수 있습니다.

설정된 시간이 경과하면 스위치는 재인증을 수행합니다. 인증이 성공하면 사용자는 계속 네트워크를 사용할 수 있으며, 인증이 실패하면 네트워크 접근이 차단됩니다.



재인증을 위한 프로토콜 상호작용

12.1.4. 802.1X 포트 상태

여기서 말하는 포트 상태는 스위치의 물리 포트 상태를 의미합니다. 스위치의 물리 포트는 네 가지 상태를 가질 수 있습니다: N/A, Auto, Force-authorized, Force-unauthorized. 스위치에서 802.1X가 활성화되지 않은 경우 모든 포트는 N/A 상태입니다. 포트를 Auto, Force-authorized 또는 Force-unauthorized 상태로 설정하려면 반드시 802.1X 기능이 활성화되어 있어야 합니다.

스위치 포트가 N/A 상태일 경우, 해당 포트에 연결된 모든 사용자는 인증 없이 네트워크에 접근할 수 있습니다. 이때 스위치는 해당 포트로부터 수신한 802.1X 프로토콜 패킷을 모두 폐기합니다.

포트가 Force-authorized 상태일 경우에도 모든 사용자는 인증 없이 네트워크에 접근할 수 있습니다. 포트에서 EAPOL-Start 패킷을 수신하면 스위치는 EAP-Success 패킷을 응답으로 전송하며, 그 외의 802.1X 프로토콜 패킷은 모두 폐기합니다.

포트가 Force-unauthorized 상태일 경우, 해당 포트에 연결된 모든 사용자는 네트워크에 전혀 접근할 수 없습니다. 인증 요청 또한 통과할 수 없으며, 스위치는 해당 포트에서 수신한 모든 802.1X 프로토콜 패킷을 폐기합니다.

포트가 Auto 상태일 경우, 해당 포트에 연결된 모든 사용자는 네트워크에 접근하기 전에 반드시 인증을 수행해야 합니다. 일반적으로 사용자 인증이 필요한 경우 포트를 Auto 상태로 설정합니다.

또한 스위치 포트가 Auto 상태로 설정되면 ARP 스푸핑 방지 기능이 함께 활성화됩니다. 이 기능은 인증 과

정에서 클라이언트가 제공한 정보와 일치하는 경우에만 패킷을 전달하도록 제어합니다. 즉, IP 패킷의 출발지 MAC과 IP가 인증 시 제공된 정보와 일치하고, ARP 패킷의 Sender IP와 MAC이 인증 정보와 일치할 경우에만 포워딩이 허용되며, 그렇지 않은 경우 해당 패킷은 폐기됩니다.

이 기능을 사용할 때는 클라이언트가 고정 IP 주소를 사용해야 합니다. 만약 DHCP를 통해 IP를 동적으로 할당받는 경우에는 DHCP Snooping 기능을 활성화하여 동일한 기능을 구현할 수 있습니다. 보다 자세한 내용은 IP-MAC 바인딩 설정을 참고하면 됩니다.

12.2. RADIUS 소개

사용자 인증 시, 스위치와 인증 서버 간의 상호작용에는 EAP 확장을 지원하는 RADIUS 프로토콜이 사용됩니다. RADIUS 프로토콜은 클라이언트/서버 모델을 사용하며, 스위치는 RADIUS 클라이언트를 구현해야 하고 인증 서버는 RADIUS 서버를 구현해야 합니다.

스위치와 인증 서버 간 통신의 보안을 보장하고, 비인가 스위치 또는 비인가 인증 서버와의 통신을 방지하기 위해 스위치와 인증 서버는 서로를 인증해야 합니다. 이를 위해 스위치와 인증 서버는 동일한 키를 사용해야 합니다.

스위치 또는 인증 서버가 RADIUS 프로토콜 패킷을 전송할 때, 모든 프로토콜 패킷은 해당 키를 기반으로 HMAC 알고리즘을 사용하여 message digest를 생성합니다. 스위치와 인증 서버가 RADIUS 프로토콜 패킷을 수신하면, 동일한 키를 사용하여 각 패킷의 message digest를 검증합니다.

검증에 성공하면 정상적인 RADIUS 프로토콜 패킷으로 판단하고, 검증에 실패하면 비정상적인 RADIUS 프로토콜 패킷으로 간주하여 폐기합니다.

이 절에서는 다음 내용을 포함합니다.

- 프로토콜 패킷 소개
- 프로토콜 동작 흐름
- 사용자 인증 방식

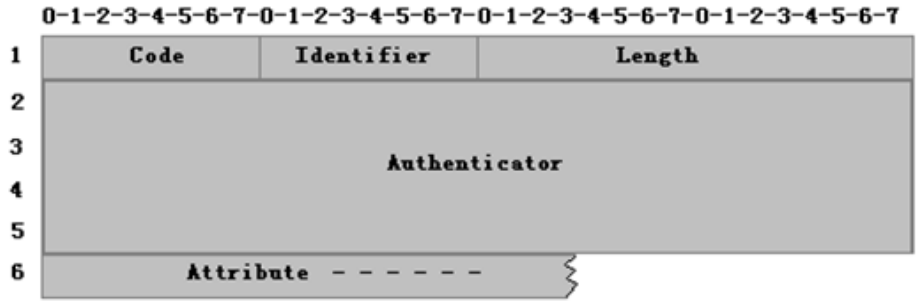
12.2.1. 프로토콜 패킷 소개

RADIUS는 UDP 기반 프로토콜입니다. RADIUS는 인증 정보와 과금 정보를 캡슐화할 수 있습니다. 초기 RADIUS 인증 포트는 1645였으며, 현재는 1812 포트를 사용합니다. 초기 RADIUS 과금 포트는 1646이었으며, 현재는 1813 포트를 사용합니다.

RADIUS는 UDP 기반으로 동작하기 때문에 timeout 재전송 메커니즘이 필요합니다. 또한 인증 시스템과 RADIUS 서버 간 통신 신뢰성을 높이기 위해 일반적으로 두 대의 RADIUS 서버를 사용하며, 이를 통해 standby server 메커니즘을 구성합니다.

RADIUS 메시지 형식은 아래 그림과 같습니다. Code는 RADIUS 프로토콜 메시지 유형을 의미합니다. Identifier는 request와 reply를 매칭하기 위해 사용됩니다. Length는 메시지 헤더를 포함한 전체 메시지 길이를 의미합니다. Authenticator는 16바이트 문자열이며, request packet에서는 난수로 사용되고, reply packet에

서는 MD5로 생성된 message digest로 사용됩니다. Attribute는 RADIUS 패킷 내의 속성을 의미합니다.



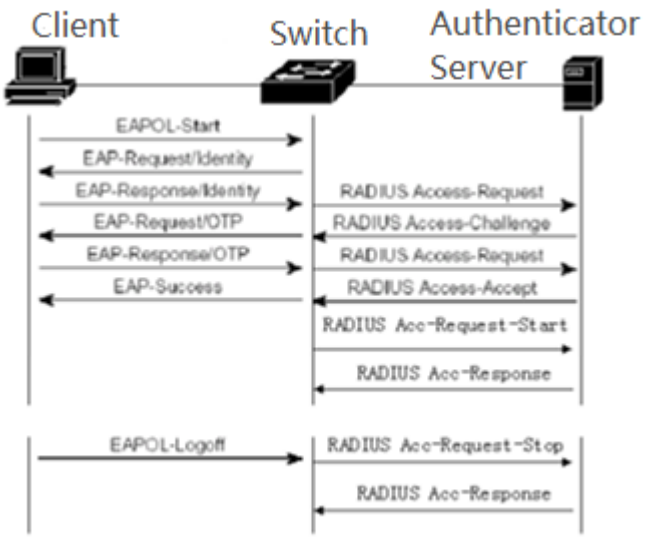
RADIUS message format

네트워크에서는 다음과 같은 RADIUS 프로토콜 패킷을 사용합니다.

a. Access-Request: Code 값은 1입니다. 인증 시스템에서 인증 서버로 전송하는 인증 요청 패킷이며, 사용자 이름과 비밀번호가 이 패킷에 캡슐화됩니다.
b. Access-Accept: Code 값은 2입니다. 인증 서버에서 인증 시스템으로 전송하는 응답 패킷이며, 사용자 인증이 성공했음을 나타냅니다.
c. Access-Reject: Code 값은 3입니다. 인증 서버에서 인증 시스템으로 전송하는 응답 패킷이며, 사용자 인증이 실패했음을 나타냅니다.
d. Access-Challenge: Code 값은 11입니다. 인증 서버에서 인증 시스템으로 전송하는 응답 패킷이며, 비밀번호 등 사용자로부터 추가 정보가 필요함을 나타냅니다.
e. Accounting-Request: Code 값은 4입니다. 인증 시스템에서 인증 서버로 전송하는 과금 요청 패킷이며, 과금 시작 패킷과 과금 종료 패킷을 포함합니다. 과금 정보는 이 패킷에 캡슐화됩니다.
f. Accounting-Response: Code 값은 5입니다. 인증 서버에서 인증 시스템으로 전송하는 과금 응답 패킷이며, 과금 정보가 정상적으로 수신되었음을 나타냅니다.

12.2.2. 프로토콜 동작 흐름

사용자가 인증을 시작하면, 인증 시스템은 RADIUS 프로토콜을 통해 인증 서버와 상호작용합니다. 인증 시스템이 RADIUS 과금 패킷을 전송하지 않는 경우의 프로토콜 흐름은 아래 그림과 같으며, 일반적으로 사용자가 인증에 성공하거나 네트워크에서 로그오프할 때 인증 시스템은 RADIUS 과금 패킷을 인증 서버로 전송합니다. 이에 대한 프로토콜 흐름도는 아래 그림과 같습니다.



사용자 인증 과정에서, 스위치는 사용자 이름을 Access-Request 메시지에 캡슐화하여 인증 서버로 전송합니다. 인증 서버는 사용자 비밀번호를 요청하는 Access-Challenge 메시지로 응답합니다. 이에 따라 스위치는 클라이언트 사용자에게 비밀번호 입력을 요청하고, 클라이언트는 비밀번호를 EAP에 캡슐화하여 전송합니다.

스위치는 이 EAP 정보를 수신한 후 이를 다시 Access-Request 메시지에 캡슐화하여 인증 서버로 전송합니다. 인증 서버는 사용자 이름과 비밀번호를 기반으로 인증을 수행합니다. 인증이 성공하면 인증 서버는 스위치로 Access-Accept 메시지를 전송하고, 스위치는 이 메시지를 수신한 후 클라이언트에게 인증 성공을 통보합니다.

동시에 스위치는 과금 시작을 알리기 위해 Accounting-Request 메시지를 인증 서버로 전송하며, 인증 서버는 이에 대해 Accounting-Response 메시지를 반환합니다.

사용자가 더 이상 네트워크를 사용하지 않을 경우, 클라이언트는 스위치에 로그오프를 알립니다. 스위치는 인증 서버로 Accounting-Request 메시지를 전송하여 과금 종료를 통보하며, 이 패킷에는 과금 정보가 포함됩니다. 인증 서버는 이에 대해 Accounting-Response 메시지를 반환합니다.

12.2.3. 사용자 인증 방식

RADIUS에는 다음과 같은 세 가지 사용자 인증 방식이 있습니다.

PAP(Password Authentication Protocol)

사용자는 사용자 이름과 비밀번호를 평문으로 스위치에 전달합니다. 스위치는 RADIUS 프로토콜 패킷을 통해 사용자 이름과 비밀번호를 RADIUS 서버로 전달합니다. RADIUS 서버는 데이터베이스를 검색하여 동일한 사용자 이름과 비밀번호가 존재하면 인증 성공으로 판단하고, 그렇지 않으면 인증 실패로 판단합니다.

CHAP(Challenge Handshake Authentication Protocol)

사용자가 네트워크 접근을 요청하면, 스위치는 사용자에게 16바이트 난수를 생성하여 전달합니다. 사용자는

이 난수, 비밀번호 및 기타 필드를 암호화하여 응답값을 생성한 후, 사용자 이름과 응답값을 스위치로 전송합니다. 스위치는 사용자 이름, 응답값, 원래의 16바이트 난수를 RADIUS 서버로 전달합니다. RADIUS 서버는 사용자 이름을 기준으로 데이터베이스에서 사용자 측 암호화에 사용된 동일한 비밀번호를 조회한 후, 전달받은 16바이트 난수를 기준으로 암호화 연산을 수행하고 그 결과를 전달받은 응답값과 비교합니다. 두 값이 같으면 인증 성공으로 판단하고, 다르면 인증 실패로 판단합니다.

EAP(Extensible Authentication Protocol)

이 인증 방식에서는 스위치가 실제 인증 과정에 직접 참여하지 않고, 사용자와 RADIUS 서버 사이에서 전달 역할만 수행합니다. 사용자가 네트워크 접근을 요청하면, 스위치는 사용자 이름을 요청하고 이를 RADIUS 서버로 전달합니다. RADIUS 서버는 사용자를 위해 16바이트 난수를 생성하고 이를 저장합니다. 사용자는 이 난수, 비밀번호 및 기타 필드를 암호화하여 응답값을 생성한 후, 사용자 이름과 응답값을 스위치로 전송합니다. 스위치는 해당 응답값을 RADIUS 서버로 전달합니다. RADIUS 서버는 사용자 이름을 기준으로 데이터베이스에서 사용자 측 암호화에 사용된 비밀번호와 동일한 값을 조회하고, 저장된 16바이트 난수를 기준으로 암호화 연산을 수행한 뒤, 그 결과를 전달받은 응답값과 비교합니다. 두 값이 같으면 인증 성공으로 판단하고, 다르면 인증 실패로 판단합니다.

이 네트워크의 인증 및 과금 솔루션은 EAP 사용자 인증 방식을 사용합니다.

12.3. 802.1X 설정

이 절에서는 802.1X 설정 방법을 상세히 설명합니다. 주요 내용은 다음과 같습니다.

- 802.1X 기본 설정
- 802.1X 활성화 및 비활성화
- 802.1X 포트 상태 설정
- 재인증(Recertification) 메커니즘 설정
- 포트에 연결 가능한 최대 호스트 수 설정
- 재전송 간격 및 재전송 횟수 설정
- 포트를 전송 포트로 설정
- 802.1X 클라이언트 버전 설정
- 클라이언트 버전 검사 여부 설정
- 인증 방식 설정
- 클라이언트 타이밍 패킷 검사 여부 설정
- 802.1X 정보 확인

12.3.1. 802.1X 기본 설정

스위치의 802.1X 기본 설정은 다음과 같습니다.

- 802.1X는 기본적으로 비활성화 상태입니다.
- 모든 포트 상태는 N/A입니다.
- 재인증(Recertification) 기능은 비활성화되어 있으며, 재인증 주기는 3600초입니다.

- 모든 포트의 최대 접속 가능 호스트 수는 100입니다.
- EAP-Request 재전송 타임아웃은 30초입니다.
- 타임아웃 발생 시 EAP-Request 재전송 횟수는 3회입니다.
- 사용자 인증 실패 후 대기 시간은 60초입니다.
- 서버 타임아웃 재전송 간격은 10초입니다.

스위치는 모든 설정을 기본값으로 되돌릴 수 있는 명령어를 글로벌 설정 모드에서 제공합니다.

12.3.2. 802.1X 활성화 및 비활성화

802.1X 설정의 첫 단계는 기능을 활성화하는 것입니다. 글로벌 설정 모드에서 다음 명령어를 입력하면 802.1X를 활성화할 수 있습니다.

```
Switch(config)# dot1x
```

802.1X를 비활성화하면 모든 포트는 다시 N/A 상태로 돌아갑니다. 글로벌 설정 모드에서 다음 명령어를 입력하면 802.1X를 비활성화할 수 있습니다.

```
Switch(config)# no dot1x
```

12.3.3. 802.1X 포트 상태 설정

802.1X 포트 상태를 설정하기 전에 반드시 802.1X 기능을 먼저 활성화해야 합니다.

해당 포트에 연결된 모든 사용자가 인증 후에만 네트워크에 접근하도록 하려면 포트를 Auto 상태로 설정해야 합니다.

인터페이스 설정 모드에서 다음 명령어를 사용하면 포트 ge1/1을 Auto 상태로 설정할 수 있으며, 이때 ARP 스푸핑 방지 기능도 함께 활성화됩니다.

```
Switch(config-ge1/1)# dot1x control auto
```

ARP 스푸핑 방지 설정이 실패하는 경우는 다음과 같은 원인이 있을 수 있습니다.

- 시스템 CFP 리소스가 부족한 경우
- 해당 인터페이스에 ACL 필터링이 설정된 경우
- 해당 인터페이스에 DHCP Snooping 기능이 활성화된 경우

- 해당 인터페이스가 Layer 3 인터페이스이거나 트렁크 인터페이스인 경우

포트 ge1/1을 Force-authorized 상태로 설정하는 명령어는 다음과 같습니다.

Switch(config-ge1/1)# dot1x control force-authorized

포트 ge1/1을 Force-unauthorized 상태로 설정하는 명령어는 다음과 같습니다.

Switch(config-ge1/1)# dot1x control force-unauthorized

포트 ge1/1을 N/A 상태로 설정하는 명령어는 다음과 같습니다.

Switch(config-ge1/1)# no dot1x control

주의

포트에 MAC 주소 바인딩이 설정되어 있는 경우에는 해당 포트를 Auto, Force-authorized, Force-unauthorized 상태로 설정할 수 없습니다.

12.3.4. 재인증(Recertification) 메커니즘 설정

클라이언트가 비정상적으로 오프라인되는 상황을 스위치나 인증 서버가 감지하지 못하는 문제를 방지하기 위해, 스위치는 재인증(재인증 주기 기반 인증) 기능을 제공합니다. 설정된 주기마다 스위치가 다시 인증을 수행합니다.

글로벌 설정 모드에서 다음 명령어를 사용하면 재인증 기능을 활성화할 수 있습니다.

Switch(config)# dot1x reauthenticate

재인증 기능을 비활성화하려면 다음 명령어를 사용합니다.

Switch(config)# no dot1x reauthenticate

재인증 주기(간격)를 설정하려면 다음 명령어를 사용합니다.

Switch(config)# dot1x timeout re-authperiod <interval>

주의

재인증 주기를 너무 짧게 설정하면 인증 트래픽이 과도하게 발생하여 스위치 CPU 자원과 네트워크 대역폭을 불필요하게 많이 소모할 수 있습니다.

12.3.5. 포트 최대 접속 호스트 수 설정

스위치의 각 포트는 동시에 접속할 수 있는 최대 호스트 수를 제한할 수 있습니다. 이 기능은 하나의 포트를 통해 여러 장비를 연결하여 불법적으로 네트워크에 접근하는 것을 방지하는 데 사용됩니다.

기본값은 100이며, 최대 설정값도 100입니다.

만약 최대 접속 호스트 수를 0으로 설정하면 해당 포트는 모든 사용자 접근을 차단합니다.

인터페이스 설정 모드에서 다음 명령어를 사용하여 포트 ge1/1의 최대 접속 호스트 수를 설정할 수 있습니다.

Switch(config-ge1/1)# dot1x support-host <number>

12.3.6. 재전송 간격 및 재전송 횟수 설정

802.1X 프로토콜은 동작 과정에서 사용하는 타이머(간격)와 재전송 횟수가 표준으로 정의되어 있습니다. 스위치는 기본적으로 이 표준 값을 사용하며, 일반적인 환경에서는 해당 값을 변경하지 않는 것이 권장됩니다.

각 항목의 의미는 다음과 같습니다.

- tx-period: 스위치가 EAP-Request 패킷을 재전송하는 간격
- max-req: EAP-Request 패킷 재전송 최대 횟수
- quiet-period: 인증 실패 후 재인증까지 대기하는 시간
- server-timeout: RADIUS 서버로 패킷 재전송 간격
- supp-timeout: 클라이언트(EAP) 요청 재전송 간격

글로벌 설정 모드에서 다음 명령어를 사용하여 각 값을 설정할 수 있습니다.

Switch(config)# dot1x timeout tx-period <interval>

Switch(config)# dot1x max-req <number>

Switch(config)# dot1x timeout quiet-period <interval>

Switch(config)# dot1x timeout server-timeout <interval>

Switch(config)# dot1x timeout supp-timeout <interval>

12.3.7. 포트를 전송 포트(Transmit Port)로 설정

스위치에서 802.1X 인증을 사용하지 않더라도, 동일 서브넷 내의 다른 스위치에서 802.1X 인증을 수행하는 경우가 있습니다. 이때 클라이언트와 인증 스위치 사이에 위치한 스위치의 포트를 전송 포트(transmit port)로 설정하면, EAPOL 인증 패킷을 그대로 전달(포워딩)하여 다른 스위치에서 클라이언트 인증이 가능하도록 할 수 있습니다.

즉, 이 기능은 해당 스위치가 인증을 직접 수행하지 않고 인증 트래픽을 중계하는 역할을 하도록 만드는 설정입니다.

인터페이스 설정 모드에서 다음 명령어를 사용하면 포트 ge1/1을 전송 포트로 설정할 수 있습니다.

Switch(config-ge1/1)# dot1x transmit-port

전송 포트 설정을 해제하려면 다음 명령어를 사용합니다.

Switch(config-ge1/1)# no dot1x transmit-port

12.3.8. 802.1X 클라이언트 버전 설정

802.1X 클라이언트의 최소 허용 버전을 설정할 수 있습니다.

설정된 버전보다 낮은 클라이언트는 인증이 거부되며, 해당 버전 이상인 경우에만 인증이 허용됩니다.

스위치의 기본 클라이언트 버전은 2.0입니다.

글로벌 설정 모드에서 다음 명령어를 사용하여 클라이언트 버전을 설정할 수 있습니다.

Switch(config)# dot1x client-version <string>

12.3.9. 802.1X 클라이언트 버전 검사 설정

802.1X 클라이언트의 버전 검사 여부를 설정할 수 있습니다.

버전 검사가 활성화되어 있으면, 스위치는 인증 과정에서 먼저 클라이언트의 버전을 확인한 후 인증을 진행합니다.

기본값은 버전 검사 활성화(체크함) 상태입니다.

글로벌 설정 모드에서 다음 명령어를 사용하여 클라이언트 버전 검사를 활성화할 수 있습니다.

```
Switch(config)# dot1x check-version open
```

12.3.10. 인증 방식 설정

스위치에서 802.1X 패킷에 대해 사용할 인증 방식(authentication mode)을 설정할 수 있습니다.

클라이언트가 시작하는 인증 방식은 크게 일반 인증과 확장 인증(extended authentication)으로 구분됩니다. 스위치는 특정 인증 방식을 우선적으로 사용하도록 설정할 수 있습니다.

클라이언트가 사용하는 인증 방식이 스위치에 설정된 방식과 일치하지 않을 경우, 일정 횟수 인증 실패 이후 클라이언트는 다른 인증 방식으로 자동 전환하여 다시 인증을 시도합니다.

글로벌 설정 모드에서 다음 명령어를 사용하면 스위치의 인증 방식을 확장 인증(extended)으로 설정할 수 있습니다.

```
Switch(config)# dot1x extended
```

12.3.11. 클라이언트 타이밍 패킷 검사 설정

스위치가 클라이언트의 주기적인 802.1X 패킷(타이밍 패킷)을 검사할지 여부를 설정할 수 있습니다.

일반적으로 인증이 완료된 이후, 스위치는 클라이언트에게 일정 주기로 802.1X 패킷을 전송하도록 요구합니다. 하지만 모든 클라이언트가 인증 후에 이러한 주기적인 패킷을 전송하는 것은 아닙니다. 따라서 이 기능을 통해 스위치가 해당 타이밍 패킷을 검사할지 여부를 설정할 수 있습니다.

글로벌 설정 모드에서 다음 명령어를 사용하면 클라이언트의 타이밍 패킷 검사를 활성화할 수 있습니다.

```
Switch(config)# dot1x check-client
```

12.3.12. 802.1X 정보 확인

다음 명령어를 사용하면 일반 모드 또는 privileged 모드에서 802.1X 관련 정보를 확인할 수 있습니다.

Switch# show dot1x

이 명령어는 802.1X 전체 설정 정보를 출력합니다.

모든 포트의 설정 상태까지 포함한 전체 구성 정보를 확인할 수 있습니다.

Switch# show dot1x interface

이 명령어는 각 포트에 접속된 사용자 정보를 출력합니다.

즉, 포트별로 어떤 사용자가 인증되어 있는지 확인할 수 있습니다.

12.4. RADIUS 설정

이 절에서는 스위치에서 RADIUS를 구성하는 방법을 설명하며, 주요 내용은 다음과 같습니다.

- RADIUS 기본 설정
- 인증 서버 IP 주소 설정
- Shared Secret(공유 키) 설정
- 과금(Accounting) 활성화 및 비활성화
- RADIUS 포트 및 속성(Attribute) 설정
- RADIUS 로밍 설정
- RADIUS 정보 확인

12.4.1. RADIUS 기본 설정

스위치의 RADIUS 기본 설정은 다음과 같습니다.

- Primary 인증 서버와 Backup 인증 서버의 IP 주소는 설정되어 있지 않습니다. 즉, 기본 IP 주소는 0.0.0.0입니다.
- Shared Secret은 설정되어 있지 않습니다. 즉, Shared Secret 문자열은 비어 있습니다.
- Accounting(과금)은 기본적으로 활성화되어 있습니다.
- RADIUS 인증 UDP 포트는 1812, Accounting UDP 포트는 1813입니다.
- RADIUS Attribute 값은 다음과 같습니다.

NASPort: 0xc353
NASPortType: 0x0f
NASPortServer: 0x02

12.4.2. 인증 서버 IP 주소 설정

스위치와 RADIUS 인증 서버 간 통신을 위해서는 인증 서버의 IP 주소를 스위치에 설정해야 합니다.

실제 운영 환경에서는 보통

- Primary(주 인증 서버)
- Backup(보조 인증 서버)
- 를 함께 구성합니다.

Primary 서버와 통신이 불가능해지면, 스위치는 자동으로 Backup 서버로 전환하여 인증을 계속 수행할 수 있습니다.

글로벌 설정 모드에서 다음 명령어를 사용하여 Primary 인증 서버를 설정합니다.

Switch(config)# radius-server host <ip-address>

다음 명령어를 사용하여 Backup 인증 서버를 설정합니다.

Switch(config)# radius-server option-host <ip-address>

12.4.3. Shared Secret 설정

스위치와 인증 서버 간에는 상호 인증(mutual authentication)이 필요하며, 이를 위해 양쪽에 동일한 Shared Secret(공유 키)를 설정해야 합니다.

스위치에 설정한 키와 인증 서버(RADIUS 서버)에 설정한 키가 일치하지 않으면 인증이 정상적으로 이루어지지 않습니다.

글로벌 설정 모드에서 다음 명령어를 사용하여 스위치의 Shared Secret을 설정할 수 있습니다.

Switch(config)# radius-server key <string>

12.4.4. 과금(Accounting) 활성화 및 비활성화

스위치에서 Accounting이 비활성화되어 있으면, 사용자 인증이 성공하거나 사용자가 로그오프할 때 RADIUS Accounting 패킷을 인증 서버로 전송하지 않습니다.

일반적으로 실무 환경에서는 사용자 사용 이력 추적 및 과금/로그 목적을 위해 Accounting을 활성화하는 것이 기본입니다.

글로벌 설정 모드에서 다음 명령어를 사용하면 Accounting을 활성화할 수 있습니다.

```
Switch(config)# radius-server accounting
```

Accounting을 비활성화하려면 다음 명령어를 사용합니다.

```
Switch(config)# no radius-server accounting
```

12.4.5. RADIUS 포트 및 속성(Attribute) 설정

일반적으로 RADIUS의 포트 및 Attribute 설정은 기본값을 그대로 사용하는 것이 권장됩니다. 특별한 연동 요구사항(타 장비, 특정 AAA 서버 정책 등)이 있는 경우에만 변경하는 것이 좋습니다.

글로벌 설정 모드에서 다음 명령어를 사용하여 RADIUS 인증 UDP 포트를 변경할 수 있습니다.

```
Switch(config)# radius-server udp-port <port-number>
```

다음 명령어를 사용하면 RADIUS Attribute 값을 설정할 수 있습니다.

```
Switch(config)# radius-server attribute nas-portnum <number>
Switch(config)# radius-server attribute nas-porttype <number>
Switch(config)# radius-server attribute service-type <number>
```

12.4.6. RADIUS 로밍 설정

클라이언트에 대해 MAC / IP / VLAN 바인딩이 적용된 상태에서 사용자가 다른 위치(포트/VLAN)로 이동하면, 기존 바인딩 정보와 불일치하게 되어 802.1X 인증이 실패할 수 있습니다.

이때 RADIUS 로밍(roaming) 기능을 활성화하면, 기존 바인딩 정보를 무시하고 클라이언트의 이동 상황에서

도 802.1X 인증을 계속 수행할 수 있습니다.

글로벌 설정 모드에서 다음 명령어를 사용하면 RADIUS 로밍을 활성화할 수 있습니다.

Switch(config)# radius-server roam

RADIUS 로밍을 비활성화하려면 다음 명령어를 사용합니다.

Switch(config)# no radius-server roam

12.4.7. RADIUS 정보 확인

다음 명령어를 사용하면 일반 모드 또는 privileged 모드에서 RADIUS 설정 정보를 확인할 수 있습니다.

Switch# show radius-server

이 명령어를 통해 다음과 같은 정보를 확인할 수 있습니다.

- 인증 서버(Primary / Backup) 설정 상태
- Shared Secret 설정 여부
- Accounting 활성화 여부
- RADIUS 포트 및 Attribute 설정 값

12.5. 설정 예제 (번역)

02.1X 프로토콜을 활성화하고, 포트 ge1/1을 Auto 상태로 설정하며, Primary 인증 서버를 198.168.80.111로 설정하고, Shared Key를 abcdef로 설정하는 구성입니다.

Switch#

Switch# dot1x

Switch# configure terminal

Switch(config)# radius-server host 198.168.80.111

Switch(config)# radius-server key abcdef

Switch(config)# interface ge1/1

Switch(config-ge1/1)# dot1x control auto

12.6. TACACS+ 소개

TACACS+는 인증(Authentication)과 권한 부여(Authorization)를 통해 보다 엄격한 사용자 권한 관리를 제공합니다. 단순히 사용자의 로그인 여부만 확인하는 것이 아니라, 사용자가 실행할 수 있는 명령까지 제어할 수 있습니다.

TACACS+ 인증이 활성화되면, 사용자가 스위치에 접근할 때 반드시 TACACS+ 서버를 통해 사용자 이름과 비밀번호를 검증해야 합니다. 인증이 성공해야만 스위치에 접근할 수 있습니다.

TACACS+는 사용자 권한을 두 가지로 구분합니다.

- 일반 사용자 (Ordinary user) → CLI의 일반 모드만 접근 가능
- 특권 사용자 (Privileged user) → CLI의 모든 모드 접근 가능

또한 명령어 실행 권한도 TACACS+ 서버 기준으로 제어됩니다.

사용자가 명령어(enable, end, exit 제외)를 입력하면, TACACS+ 서버에서 권한 검증을 수행하고, 실패 시 해당 명령은 실행되지 않습니다.

TACACS+ 적용 범위는 다음과 같습니다.

- Telnet / SSH 접속 → 사용자 인증 + 명령 권한 제어
- Console 접속 → 제어하지 않음
- Web 로그인 → 인증은 수행하지만 명령 권한 제어는 없음

SSH 접속의 경우, 특권 사용자만 접근 가능합니다.

기본적으로 스위치는 TACACS+ 기능이 비활성화되어 있으며, 이 경우 Telnet, SSH, Web 로그인은 내장 사용자 관리 기능을 사용합니다.

TACACS+를 활성화하면 기존 로컬 계정 설정은 유지되지만 실제 인증에는 사용되지 않습니다.

명령어	설명	모드
tacacsplus enable	TACACS+ 기능 활성화	Global configuration
tacacsplus disable	TACACS+ 기능 비활성화	Global configuration
tacacsplus host <server-ip>	Primary 서버 설정 (IPv4/IPv6 지원)	Global configuration
tacacsplus option-host <server-ip>	Backup 서버 설정	Global configuration
tacacsplus key WORD	Shared Key 설정 (서버와 동일해야 함)	Global configuration

명령어	설명	모드
tacacsplus auth-type (PAP|CHAP)	인증 방식 선택 (기본: PAP)	Global configuration
show tacacsplus	TACACS+ 설정 확인	Global configuration
no tacacsplus host	Primary 서버 삭제	Global configuration
no tacacsplus key	Shared Key 삭제	Global configuration

13. GMRP 설정

이 장에서는 GMRP 설정과 관련된 내용을 설명하며, 다음과 같은 항목을 포함합니다.

- GMRP 소개
- GMRP 설정
- GMRP 정보 확인

13.1. GMRP 소개

GMRP(GARP Multicast Registration Protocol)는 GARP 기반의 멀티캐스트 등록 프로토콜로, 스위치 내에서 멀티캐스트 그룹 정보를 유지하고 동기화하는 역할을 합니다.

GMRP를 지원하는 모든 스위치는 다른 스위치로부터 멀티캐스트 등록 정보를 수신할 수 있으며, 이를 기반으로 로컬 멀티캐스트 정보를 동적으로 업데이트하고 다시 다른 스위치로 전파합니다. 이러한 정보 교환 메커니즘을 통해 동일한 스위칭 네트워크 내의 모든 GMRP 장비는 일관된 멀티캐스트 정보를 유지할 수 있습니다.

호스트가 특정 멀티캐스트 그룹에 참여하려고 할 때, GMRP Join 메시지를 전송합니다.

스위치는 이 Join 메시지를 수신한 포트를 해당 멀티캐스트 그룹에 등록합니다.

동시에 해당 포트가 속한 VLAN 내로 Join 메시지를 브로드캐스트하여, 동일 VLAN 내의 멀티캐스트 소스가 멤버 존재를 인지할 수 있도록 합니다.

이후 멀티캐스트 소스가 데이터를 전송하면, 스위치는 해당 멀티캐스트 그룹에 속한 멤버가 연결된 포트로만 트래픽을 전달합니다.

13.2. GMRP 설정

GMRP의 주요 설정 항목은 다음과 같습니다.

- GMRP 활성화
- GMRP 상태 확인

설정 시 중요한 점은, 포트 단위 GMRP를 활성화하기 전에 반드시 글로벌 GMRP를 먼저 활성화해야 한다는 것입니다.

즉, 설정 순서는 다음과 같이 이해하시면 됩니다.

Global GMRP ON → Interface GMRP ON

13.2.1. GMRP 활성화 설정

명령어	설명	설정 모드
set gmrp enable | disable	모든 VLAN에 대해 GMRP 전역 활성화/비활성화	Global Configuration Mode
set gmrp enable vlan <vlan-id>	특정 VLAN에 대해 GMRP 활성화	Global Configuration Mode
set gmrp registration {fixed | forbidden | normal} <if-name>	인터페이스의 멀티캐스트 등록 모드 설정	Global Configuration Mode
set gmrp timer {join | leave | nleaveall} <time-value>	GMRP 타이머 값 설정	Global Configuration Mode
set port gmrp enable <if-name>	포트 GMRP 기능 활성화	Global Configuration Mode

명령어	설명	설정 모드
set port gmrp disable <if-name>	포트 GMRP 기능 비활성화	Global Configuration Mode

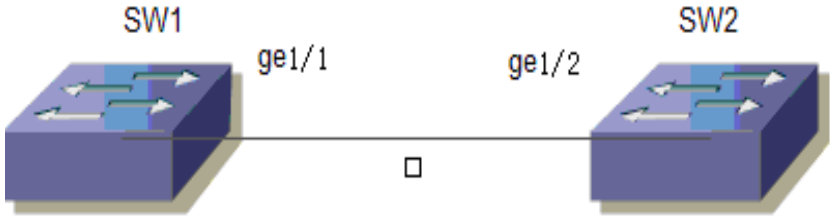
13.2.2. GMRP 정보 확인

설정 완료 후에는 privileged 모드에서 show 명령어로 GMRP 동작 상태를 확인하고, 설정이 제대로 적용되었는지 검증할 수 있습니다.

명령어	설명	모드
show gmrp configuration	GMRP 설정 정보 확인	Privileged Mode
show gmrp machine	GMRP 상태 머신 정보 확인	Privileged Mode
show gmrp statistics vlanid	특정 VLAN의 GMRP 통계 정보 확인	Privileged Mode
show gmrp timer <ifname>	특정 포트의 타이머 정보 확인	Privileged Mode

13.3. GMRP 대표 설정 예제

1) 네트워크 요구사항
   스위치 간 멀티캐스트 정보의 동적 등록 및 업데이트를 위해 GMRP를 활성화해야 합니다.
2) 구성 개요



두 대의 스위치(SW1, SW2)에서 각각 GMRP를 활성화하고, 특정 포트에서 GMRP를 동작시키는 구성입니다.

설정 절차

SW1 설정

Switch(config)# set gmrp enable

Switch(config)# set port gmrp enable ge1/1

- 글로벌 GMRP 활성화
- ge1/1 포트에서 GMRP 활성화

SW2 설정

Switch(config)# set gmrp enable

Switch(config)# set port gmrp enable ge1/2

- 글로벌 GMRP 활성화
- ge1/2 포트에서 GMRP 활성화

14. IGMP SNOOPING 설정

네트워크에서 동일한 데이터를 여러 수신자에게 유니캐스트 방식으로 전송하면, 수신자 수만큼 패킷을 복제해야 하기 때문에 트래픽이 선형적으로 증가합니다. 이로 인해 서버, 스위치/라우터, 그리고 네트워크 대역폭에 큰 부하가 발생하고 전체 효율이 크게 저하됩니다.

이러한 문제를 해결하기 위해, 화상회의, VOD(Video on Demand), 그룹 통신과 같은 멀티포인트 서비스 환경에서는 멀티캐스트 방식이 널리 사용됩니다. 멀티캐스트는 하나의 데이터 스트림을 여러 수신자가 공유함으로써 네트워크 자원을 효율적으로 사용할 수 있게 해줍니다.

스위치는 멀티캐스트 트래픽을 효율적으로 처리하기 위해 IGMP Snooping 기능을 제공합니다.

IGMP Snooping은 네트워크 상의 IGMP 패킷을 모니터링하여, IP 멀티캐스트 그룹과 MAC 주소를 동적으로 학습하고, 필요한 포트로만 멀티캐스트 트래픽을 전달하도록 합니다.

이 장에서는 IGMP Snooping의 개념과 설정 방법을 설명하며, 다음과 같은 내용을 포함합니다.

- IGMP Snooping 소개
- IGMP Snooping 설정
- IGMP Snooping 설정 예제

14.1. IGMP Snooping 소개

전통적인 네트워크에서는 멀티캐스트 패킷이 동일 서브넷 내에서 브로드캐스트처럼 처리(flooding)되기 때문에, 불필요한 트래픽 증가와 네트워크 혼잡을 유발하기 쉽습니다.

스위치에서 IGMP Snooping을 활성화하면, 스위치는 IGMP 패킷을 감시하여 IP 멀티캐스트 MAC 주소를 동적으로 학습하고, 해당 멀티캐스트 그룹에 속한 출력 포트 리스트를 유지합니다.

그 결과, 멀티캐스트 트래픽은 필요한 포트로만 전달되며 네트워크 트래픽을 크게 줄일 수 있습니다.

이 절에서는 다음과 같은 내용을 포함합니다.

- IGMP Snooping 동작 과정
- Layer 2 동적 멀티캐스트
- 그룹 가입(Join)
- 그룹 탈퇴(Leave)

14.1.1. IGMP Snooping 동작 과정

IGMP Snooping은 스위치를 통과하는 IGMP 패킷을 감시하는 Layer 2 네트워크 프로토콜입니다. 스위치는 IGMP 패킷의 수신 포트, VLAN ID, 멀티캐스트 주소를 기준으로 멀티캐스트 그룹을 유지하고, 이후 해당 그룹 정보를 기반으로 멀티캐스트 패킷을 전달합니다. 이때 멀티캐스트 그룹에 가입된 포트만 멀티캐스트 데이터 스트림을 수신할 수 있으므로, 네트워크 트래픽을 줄이고 대역폭을 절약할 수 있습니다.

멀티캐스트 그룹은 멀티캐스트 그룹 주소, 멤버 포트, VLAN ID, Age time으로 구성됩니다.

IGMP Snooping 멀티캐스트 그룹은 학습 과정을 통해 생성됩니다. 스위치의 포트가 IGMP Report 패킷을 수신하면, IGMP Snooping은 새로운 멀티캐스트 그룹을 생성하고 해당 IGMP Report 패킷을 수신한 포트를 멀티캐스트 그룹에 추가합니다.

스위치가 IGMP Query 패킷을 수신했을 때, 이미 해당 멀티캐스트 그룹이 존재한다면 IGMP Query를 수신한 포트도 해당 멀티캐스트 그룹에 가입됩니다. 만약 멀티캐스트 그룹이 존재하지 않으면 IGMP Query 패킷은 단순히 전달됩니다.

IGMP Snooping은 IGMPv2의 Leave 메커니즘도 지원합니다. IGMP Snooping에서 fast-leave가 enable로 설정되어 있으면, IGMPv2 Leave 패킷을 수신한 포트는 즉시 멀티캐스트 그룹에서 탈퇴합니다. fast-leave-timeout이 설정되어 있는 경우에는, 해당 시간이 만료된 후 멀티캐스트 그룹에서 탈퇴합니다.

IGMP Snooping에는 두 가지 업데이트 메커니즘이 있습니다. 하나는 앞에서 설명한 Leave 메커니즘이고, 다른 하나는 Age time을 이용하여 만료된 멀티캐스트 그룹을 삭제하는 방식입니다. 멀티캐스트 그룹이 IGMP Snooping에 등록되면 가입 시간이 기록됩니다. 해당 그룹이 설정된 Age time보다 오래 스위치에 유지되면,

스위치는 해당 멀티캐스트 그룹을 삭제합니다.

포트가 Leave 프로토콜 패킷을 수신하면, 해당 포트는 즉시 멀티캐스트 그룹에서 삭제될 수 있는데, 이 경우 네트워크 데이터 스트림의 연속성에 영향을 줄 수 있습니다. 왜냐하면 해당 포트 하단에 HUB 또는 IGMP Snooping 기능이 없는 네트워크 장비가 연결되어 있을 수 있고, 그 하위에 여러 멀티캐스트 수신 장비가 연결되어 있을 수 있기 때문입니다. 이때 하나의 장비가 Leave를 전송하면, 같은 하위 장비에 연결된 다른 장비들의 멀티캐스트 수신에도 영향을 줄 수 있습니다.

Fast-leave-timeout 메커니즘은 이러한 문제를 방지하기 위한 기능입니다. 이 기능을 통해 Leave 대기 시간을 설정할 수 있으며, 포트가 Leave 패킷을 수신하더라도 즉시 그룹에서 삭제하지 않고 Fast-leave-timeout 시간 동안 대기한 후 멀티캐스트 그룹에서 제거합니다. 이를 통해 네트워크 멀티캐스트 스트림의 연속성을 보장할 수 있습니다.

14.1.2. Layer 2 동적 멀티캐스트

Layer 2 하드웨어 멀티캐스트 포워딩 테이블의 멀티캐스트 MAC 주소 엔트리는 IGMP Snooping을 통해 동적으로 학습될 수 있습니다. 즉, IP 멀티캐스트 MAC 주소는 IGMP Snooping을 통해 자동으로 학습됩니다.

스위치에서 IGMP Snooping이 비활성화된 경우, Layer 2 멀티캐스트 포워딩 테이블은 비등록(unregistered) 포워딩 모드로 동작합니다. 이 상태에서는 멀티캐스트 MAC 주소를 동적으로 학습할 수 없고, 포워딩 테이블에도 엔트리가 존재하지 않으며, 모든 Layer 2 멀티캐스트 트래픽이 브로드캐스트처럼 처리됩니다.

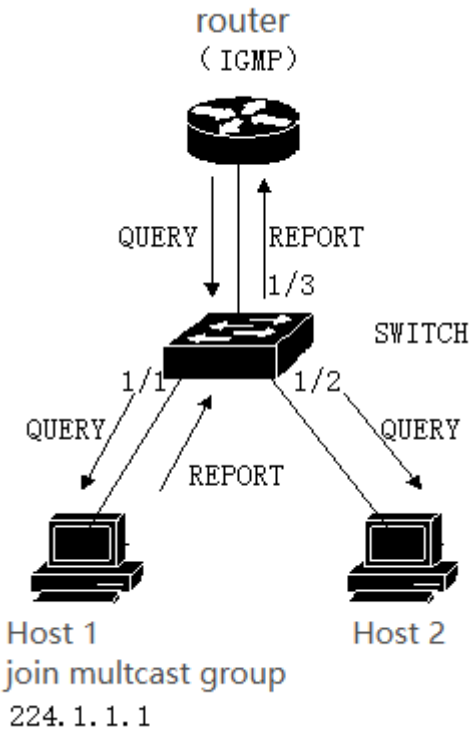
반대로, 네트워크에 멀티캐스트 환경이 존재할 때 IGMP Snooping을 활성화하면, Layer 2 포워딩 테이블은 등록(register) 포워딩 모드로 동작하게 됩니다. 이때 스위치는 네트워크 상의 IGMP 패킷을 모니터링하여 멀티캐스트 MAC 주소를 학습할 수 있습니다. 그리고 Layer 2 멀티캐스트 포워딩 테이블에 등록된 엔트리와 일치하는 트래픽만 전달됩니다.

14.1.3. 그룹 가입 (Join a Group)

호스트가 멀티캐스트 그룹에 가입하려고 할 때, 해당 호스트는 가입하고자 하는 멀티캐스트 그룹 주소를 포함한 IGMP Report 패킷을 전송합니다.

스위치가 IGMP Query 패킷을 수신하면, 동일 VLAN에 속한 모든 다른 포트로 해당 패킷을 전달합니다. 이후 멀티캐스트 그룹에 가입하려는 포트 아래의 호스트는 IGMP Query 패킷을 수신하고, 이에 대한 응답으로 IGMP Report 패킷을 다시 전송합니다.

스위치가 IGMP Report 패킷을 수신하면, Layer 2 멀티캐스트 엔트리를 생성합니다. 그리고 IGMP Query 패킷을 수신한 포트와 IGMP Report 패킷을 수신한 포트를 해당 멀티캐스트 엔트리의 출력 포트로 등록합니다.



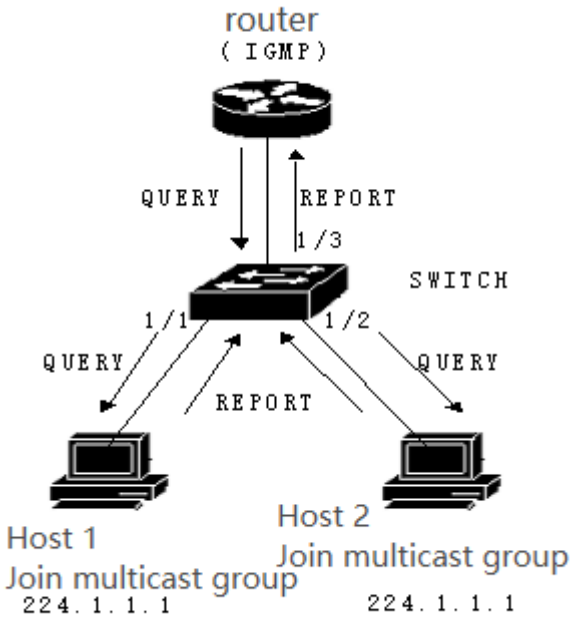
위 그림과 같이 모든 장비는 하나의 서브넷에 있으며, 해당 서브넷의 VLAN은 2라고 가정합니다. 라우터는 IGMPv2 프로토콜을 실행하며 IGMP Query 패킷을 주기적으로 전송합니다.

Host 1은 멀티캐스트 그룹 224.1.1.1에 가입하려고 합니다. 스위치가 포트 1/3에서 IGMP Query 패킷을 수신하면, 스위치는 해당 포트를 기록하고 이 패킷을 포트 1/1과 1/2로 전달합니다.

Host 1은 IGMP Query 패킷을 수신한 후 IGMP Report 패킷을 응답으로 전송합니다. 반면 Host 2는 멀티캐스트 그룹에 가입하지 않으므로 IGMP Report 패킷을 전송하지 않습니다.

스위치가 포트 1/1에서 IGMP Report 패킷을 수신하면, 해당 패킷을 Query 포트인 1/3으로 전달하고, Layer 2 멀티캐스트 엔트리를 생성합니다. 단, 해당 엔트리가 기존에 존재하지 않는다고 가정합니다.

Layer 2 멀티캐스트 주소	**VLAN ID**	**출력 포트 목록**
01:00:5e:01:01:01	2	1/1, 1/3



위 그림의 조건은 앞의 Figure 1과 동일합니다. Host 1은 이미 멀티캐스트 그룹 224.1.1.1에 가입한 상태이며, 이제 Host 2도 같은 멀티캐스트 그룹 224.1.1.1에 가입하려고 합니다.

Host 2가 IGMP Query 패킷을 수신한 후 IGMP Report 패킷을 응답으로 전송하면, 스위치는 포트 1/2에서 해당 IGMP Report 패킷을 수신합니다. 이후 스위치는 이 패킷을 Query 포트인 1/3으로 전달하고, 포트 1/2를 기존 Layer 2 멀티캐스트 엔트리에 추가합니다.

이후 Layer 2 멀티캐스트 엔트리는 다음과 같이 변경됩니다.

Layer 2 멀티캐스트 주소	**VLAN ID**	**출력 포트 목록**
01:00:5e:01:01:01	2	1/1, 1/2, 1/3

14.1.4. 그룹 탈퇴 (Leave a Group)

안정적인 멀티캐스트 환경을 유지하기 위해 IGMP를 사용하는 장비(예: 라우터)는 주기적으로 IGMP Query 패킷을 전송합니다. 멀티캐스트 그룹에 가입했거나 가입하려는 호스트는 이 Query를 수신하면 IGMP Report 패킷으로 응답합니다.

호스트가 멀티캐스트 그룹을 탈퇴하는 방법은 두 가지가 있습니다.

- Active Leave (능동 탈퇴) → 호스트가 라우터로 IGMP Leave 패킷을 전송
- Passive Leave (수동 탈퇴) → Query를 받아도 Report를 보내지 않음

이에 대응하여 스위치에서 포트가 Layer 2 멀티캐스트 엔트리에서 빠지는 방식도 두 가지입니다.

1) Timeout 방식 탈퇴
   일정 시간 동안 해당 포트에서 IGMP Report가 수신되지 않으면, 스위치는 해당 포트를 멀티캐스트 엔트리에서 제거합니다. 그리고 해당 엔트리에 남은 포트가 없으면, 멀티캐스트 엔트리 자체도 삭제됩니다.
2) IGMP Leave 수신 기반 탈퇴
   스위치에서 fast-leave 기능이 활성화되어 있는 경우, 포트가 IGMP Leave 패킷을 수신하면 즉시 해당 포트를 멀티캐스트 엔트리에서 제거합니다. 마찬가지로, 엔트리에 포트가 없으면 엔트리는 삭제됩니다.

14.1.5. IGMP Querier

일반적으로 Layer 3 멀티캐스트 장비(라우터)가 있는 네트워크에서는 해당 장비가 IGMP Querier(질의자) 역할을 수행합니다. 이 경우 Layer 2 스위치는 IGMP 패킷을 단순히 모니터링하면서 멀티캐스트 포워딩 테이블을 생성/유지하면 됩니다.

하지만 네트워크에 Layer 3 멀티캐스트 장비가 없는 경우에는 IGMP Query를 생성하는 장비가 없기 때문에, Layer 2 스위치에서 IGMP Querier 기능을 활성화해야 합니다. 이때 스위치는 IGMP 메시지를 모니터링하는 역할뿐 아니라, 직접 Query를 생성하여 멀티캐스트 그룹 관리까지 수행하게 됩니다.

동작 방식

IGMP Querier 기능을 활성화한 Layer 2 장비는 다음과 같은 역할을 수행합니다.

- 주기적으로 IGMP Query 메시지 전송
- 호스트가 응답하는 IGMP Report 메시지 수신 및 유지 관리
- 이를 기반으로 Layer 2 멀티캐스트 포워딩 테이블 생성 및 유지

또한 Query 메시지와 관련된 주요 파라미터는 설정을 통해 조정할 수 있습니다.

주요 설정 항목

① Querier 활성화
특정 VLAN에서 IGMP Querier 기능을 활성화할 수 있습니다.
② IGMP 버전 지정
Querier가 사용하는 IGMP 버전(v1 / v2 / v3)을 설정할 수 있습니다.
③ Source IP 설정
Querier가 전송하는 Query 메시지에 포함될 Source IP 주소를 설정합니다.
④ Query 전송 주기 설정

Query 메시지를 주기적으로 전송하는 간격을 설정합니다.

14.1.6. IGMP Snooping 멀티캐스트 필터링

IGMP Snooping을 사용하는 장비는 멀티캐스트 트래픽의 범위와 부하를 제어할 수 있으며, 비정상적이거나 허용되지 않은 멀티캐스트 스트림을 차단하는 데 효과적입니다.

글로벌 설정에서 멀티캐스트 필터링 규칙을 정의하고, 이를 인터페이스에 적용하면 특정 멀티캐스트 그룹에 대한 가입(Join)을 허용하거나 제한할 수 있습니다.

14.2. IGMP Snooping 설정

14.2.1. IGMP Snooping 기본 설정

IGMP Snooping의 기본 설정은 다음과 같습니다.

- IGMP Snooping은 기본적으로 비활성화 상태이며, Layer 2 하드웨어 멀티캐스트 포워딩 테이블은 비등록(unregistered) 포워딩 모드로 동작합니다.
- Fast-leave 기능은 기본적으로 비활성화되어 있습니다.
- Fast-leave-timeout 기본값은 300초입니다.
- 멀티캐스트 그룹의 Report 포트 Age Time 기본값은 400초입니다.
- 멀티캐스트 그룹의 Query 포트 Age Time 기본값은 300초입니다.

14.2.2. IGMP Snooping 활성화 및 비활성화

IGMP Snooping은 글로벌 단위 또는 VLAN 단위로 활성화/비활성화할 수 있습니다.

즉, 전체 네트워크에 적용할 수도 있고, 특정 VLAN에만 선택적으로 적용할 수도 있습니다.

글로벌 IGMP Snooping 활성화

Switch# configure terminal

Switch(config)# ip igmp snooping

전체 VLAN에 대해 IGMP Snooping이 동작합니다.

특정 VLAN에 IGMP Snooping 활성화

Switch# configure terminal

Switch(config)# ip igmp snooping vlan <vlan-id>

지정한 VLAN에서만 IGMP Snooping이 동작합니다.

글로벌 IGMP Snooping 비활성화

Switch# configure terminal

Switch(config)# no ip igmp snooping

모든 VLAN에서 IGMP Snooping이 비활성화됩니다.

특정 VLAN IGMP Snooping 비활성화

Switch# configure terminal

Switch(config)# no ip igmp snooping vlan <vlan-id>

특정 VLAN에서만 IGMP Snooping이 비활성화됩니다.

14.2.3. 멀티캐스트 그룹 유지 시간(Lifetime) 설정

IGMP Snooping에서는 멀티캐스트 그룹이 얼마 동안 유지될지(유효 시간)를 설정할 수 있습니다.

이 값은 멀티캐스트 트래픽의 지속성 vs 빠른 정리에 직접적인 영향을 줍니다.

멀티캐스트 그룹(Report 기반) 유지 시간 설정

Switch# configure terminal

Switch(config)# ip igmp snooping group-membership-timeout <interval> vlan <vlan-id>

- 단위: milliseconds (ms)
- 의미: IGMP Report를 기반으로 생성된 멀티캐스트 그룹이 유지되는 시간

Query 기반 그룹 유지 시간 설정

Switch# configure terminal

Switch(config)# ip igmp snooping query-membership-timeout <interval> vlan <vlan-id>

- 단위: milliseconds (ms)

- 의미: IGMP Query 기반으로 유지되는 멀티캐스트 그룹의 유지 시간

14.2.4. Fast-Leave 설정

IGMP Snooping에서 Fast-Leave 기능은 호스트가 멀티캐스트 그룹을 떠날 때 즉시 포트를 제거할지 여부를 결정하는 중요한 옵션입니다.

Fast-Leave 활성화 (특정 VLAN)

Switch# configure terminal

Switch(config)# ip igmp snooping fast-leave vlan <vlan-id>

해당 VLAN에서 IGMP Leave 수신 시 즉시 포트 제거

Fast-Leave 비활성화

Switch# configure terminal

Switch(config)# no ip igmp snooping fast-leave vlan <vlan-id>

Leave 후 일정 시간 유지 (기본 동작)

Fast-Leave 대기 시간 설정

Switch# configure terminal

Switch(config)# ip igmp snooping fast-leave-timeout <interval> vlan <vlan-id>

- 단위: milliseconds
- 의미: Leave 수신 후 대기 후 제거하는 시간

Fast-Leave 대기 시간 기본값 복원

Switch# configure terminal

Switch(config)# no ip igmp snooping fast-leave-timeout vlan <vlan-id>

14.2.5. MROUTER 설정 (정적 멀티캐스트 라우터 포트)

멀티캐스트 라우터가 연결된 포트를 스위치에 정적으로 지정하는 설정입니다.

이 포트는 IGMP Query/Report가 오가는 기준 포트로 사용되며, 멀티캐스트 트래픽이 정상적으로 라우터 방향으로 전달되도록 합니다.

Switch# configure terminal

Switch(config)# interface ge1/6

Switch(config-ge1/6)# ip igmp snooping mrouter vlan <vlan-id>

14.2.6. IGMP Snooping Query 포트 설정 (정적 Query/Mrouter 포트)

IGMP Snooping 환경에서 Query를 전달하거나 수신하는 기준 포트를 수동으로 지정하는 설정입니다.

실제 명령은 mrouter 설정과 동일하며, 해당 포트를 멀티캐스트 라우터(Query 장비) 연결 포트로 지정하는 의미입니다.

Switch# configure terminal

Switch(config)# interface ge1/6

Switch(config-ge1/6)# ip igmp snooping mrouter vlan <vlan-id>

14.2.7. IGMP Snooping Query 기능 설정

VLAN 1에서 IGMP Snooping Query 기능을 활성화하는 설정입니다.

Switch# configure terminal

Switch(config)# ip igmp snooping

Switch(config)# ip igmp snooping querier vlan 1

14.2.8. IGMP Snooping 멀티캐스트 필터링 설정

포트 ge1/1에서 멀티캐스트 주소 235.0.0.1을 차단하는 설정입니다.

Switch# configure terminal

Switch(config)# ip igmp snooping filter-rule 1 deny 235.0.0.1

Switch(config)# interface ge1/1

Switch(config-ge1/1)# ip igmp snooping filter-group 1

14.2.9. IGMP Snooping 정보 확인

IGMP Snooping 관련 설정 및 동작 상태를 확인하는 명령어입니다.

Switch# show ip igmp snooping

→ IGMP Snooping 전체 설정 정보 확인

Switch# show ip igmp snooping vlan <vlan-id>

→ 특정 VLAN의 IGMP Snooping 설정 정보 확인

Switch# show ip igmp snooping age-table group-membership

→ 멀티캐스트 그룹(Report 기반) Aging 정보 확인

Switch# show ip igmp snooping age-table query-membership

→ Query 기반 Aging 정보 확인

Switch# show ip igmp snooping forwarding-table

→ 멀티캐스트 그룹 포워딩 정보 확인

Switch# show ip igmp snooping mrouter

→ Mrouter 포트 정보 확인

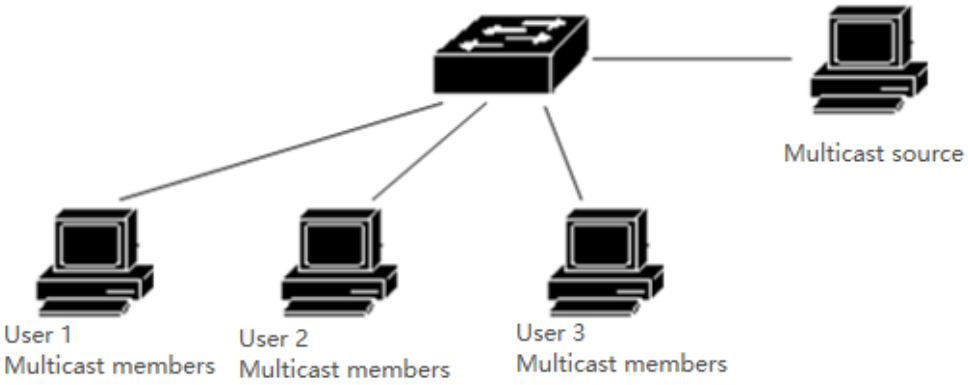
→ Mrouter 포트 정보 확인

→ 전체 설정 확인 (IGMP Snooping 포함)

14.3. IGMP Snooping 예제

14.3.1. 설정 예제

스위치에서 IGMP Snooping 기능을 활성화하고, User1, User2, User3가 특정 멀티캐스트 그룹에 가입할 수 있도록 설정하는 구성입니다.



Switch# configure terminal

Switch(config)# ip igmp snooping

Switch(config)# vlan database

Switch(config-vlan)# vlan 200

Switch(config-vlan)# exit

Switch(config)# interface ge1/1

Switch(config-ge1/1)# switchport mode access

Switch(config-ge1/1)# switchport access vlan 200

Switch(config)# interface ge1/2

Switch(config-ge1/2)# switchport mode access

Switch(config-ge1/2)# switchport access vlan 200

Switch(config)# interface ge1/3

Switch(config-ge1/3)# switchport mode access

Switch(config-ge1/3)# switchport access vlan 200

```
Switch(config)# ip igmp snooping vlan 200
Switch(config)# ip igmp snooping group-membership-timeout 60000 vlan 200
```

15. MVR 설정

이 장에서는 MVR 설정과 관련된 내용을 설명하며, 다음과 같은 항목을 포함합니다.

- MVR 소개
- MVR 설정

15.1. MVR 소개

MVR(Multicast VLAN Registration)은 서비스 제공자 네트워크에서 VOD(Video on Demand)와 같은 멀티캐스트 스트리밍 애플리케이션을 위해 사용되는 기능입니다.

MVR은 특정 포트의 가입자가 멀티캐스트 VLAN 내의 멀티캐스트 스트림을 구독하거나 해지할 수 있도록 하며, 하나의 멀티캐스트 VLAN에서 생성된 데이터 스트림을 다른 VLAN에서도 공유할 수 있도록 합니다.

MVR의 목적은 다음과 같습니다.

- 간단한 설정으로 VLAN 간 멀티캐스트 스트림을 효율적이고 안전하게 전달
- 멀티캐스트 그룹에 대한 동적 가입 및 탈퇴 지원

MVR의 동작은 IGMP Snooping과 유사하며, 두 기능은 동시에 사용할 수 있습니다.

MVR은 설정된 특정 멀티캐스트 그룹에 대해서만 가입/탈퇴를 처리하고, 그 외의 그룹은 IGMP Snooping이 관리합니다.

두 기능의 차이점은 다음과 같습니다.

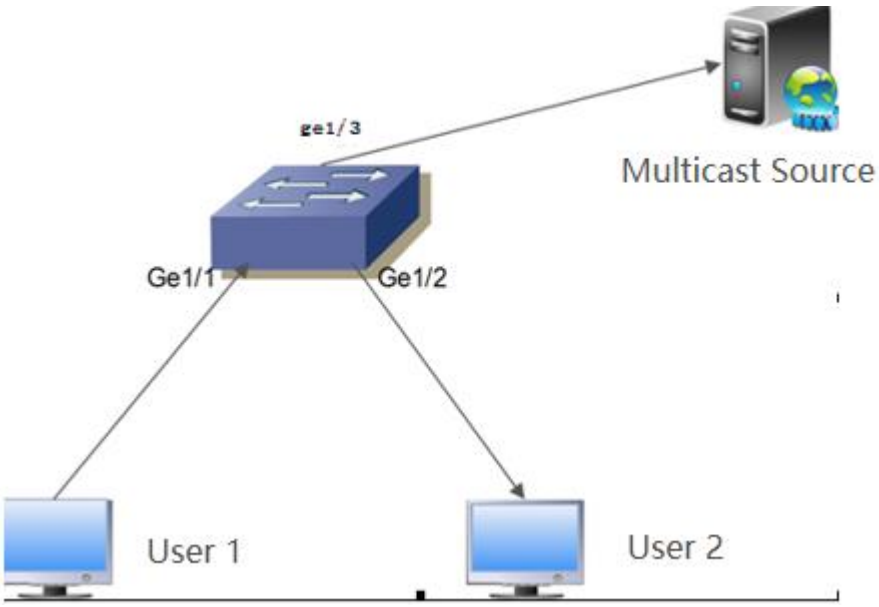
- IGMP Snooping → 멀티캐스트 스트림은 하나의 VLAN 내에서만 전달
- MVR → 멀티캐스트 스트림을 여러 VLAN 간에 전달 가능

15.2. MVR 설정

명령어	설명	모드
mvr (enable|disable)	MVR 글로벌 활성화/비활성화	Global Configuration Mode
no mvr	모든 MVR 설정 삭제	Global Configuration Mode
mvr group A.B.C.D	멀티캐스트 IP 주소 설정	Global Configuration Mode
no mvr group A.B.C.D	멀티캐스트 IP 주소 삭제	Global Configuration Mode
mvr group A.B.C.D <1-256>	연속된 멀티캐스트 그룹 주소 설정	Global Configuration Mode
mvr vlan <1-4094>	멀티캐스트 데이터를 수신할 VLAN 지정	Global Configuration Mode
no mvr vlan	기본 VLAN 1로 복원	Global Configuration Mode
mvr-interface (enable|disable)	인터페이스 MVR 활성화/비활성화	Interface Configuration Mode
show mvr	MVR 설정 정보 확인	Privileged Mode

15.3. MVR 설정 예제

다음과 같은 네트워크에서 User1은 VLAN 10, User2는 VLAN 20에 속해 있으며, 두 사용자는 동일한 멀티캐스트 프로그램(225.1.1.1 ~ 225.1.1.64)을 시청합니다. MVR VLAN은 100으로 구성합니다.



글로벌 설정

VLAN 생성, IGMP Snooping 활성화, MVR VLAN 및 멀티캐스트 그룹 범위 설정, MVR 활성화

Switch# configure terminal

Switch(config)# ip igmp snooping

Switch(config)# mvr enable

Switch(config)# mvr vlan 100

Switch(config)# mvr group 225.1.1.1 64

사용자 포트 설정 (ge1/1, ge1/2)

Switch# configure terminal

Switch(config)# interface ge1/1

Switch(config-ge1/1)# switchport mode hybrid

Switch(config-ge1/1)# switchport hybrid native vlan 10

Switch(config-ge1/1)# switchport hybrid allowed vlan add 100 egress-tagged disable

Switch(config-ge1/1)# mvr enable

Switch# configure terminal

Switch(config)# interface ge1/2

Switch(config-ge1/2)# switchport mode hybrid

Switch(config-ge1/2)# switchport hybrid native vlan 20

Switch(config-ge1/2)# switchport hybrid allowed vlan add 100 egress-tagged disable

Switch(config-ge1/2)# mvr enable

업링크 포트 설정 (ge1/3)

Switch# configure terminal

Switch(config)# interface ge1/3

Switch(config-ge1/3)# switchport access vlan 100

16. DHCP Snooping 설정

동적 접속 환경에서 호스트는 DHCP 서버를 통해 IP 주소와 네트워크 설정 정보를 할당받습니다.

DHCP Snooping은 DHCP 메시지를 감시하여 클라이언트의 IP 주소와 MAC 주소를 동적으로 바인딩함으로써 ARP 공격을 방지하는 기능입니다.

스위치는 DHCP Snooping 기능을 통해 네트워크 상의 DHCP 메시지를 검사하고, 포트 기반으로 ARP 정보를 바인딩하여 비정상적인 ARP 패킷을 차단할 수 있습니다.

또한, DHCP 서버가 연결된 포트를 지정할 수 있으며, 최대 4개의 서버 포트를 설정하여 비인가 DHCP 서버(rogue DHCP server)가 네트워크에 영향을 주는 것을 방지할 수 있습니다.

이 장에서는 DHCP Snooping의 개념과 설정 방법을 설명하며, 다음과 같은 내용을 포함합니다.

- DHCP Snooping 소개
- DHCP Snooping 설정
- DHCP Snooping 설정 예제

16.1. DHCP Snooping 소개

ARP 프로토콜은 단순한 신뢰 기반으로 동작하기 때문에 네트워크 보안에 취약점을 가질 수 있습니다. 공격자가 위조된 MAC 정보를 포함한 ARP 패킷을 전송하면, 호스트는 이를 검증 없이 ARP 캐시 테이블에 반영하게 되고, 정상적인 데이터 트래픽이 공격자에게 전달될 수 있습니다.

이러한 문제를 방지하기 위해, Layer 2 스위치에서 포트 기반의 ARP 정보 바인딩을 수행하면 비정상적인 ARP 공격 패킷을 필터링하여 공격 트래픽이 대상 호스트에 도달하지 못하도록 할 수 있습니다.

또한, 네트워크에 비인가 DHCP 서버가 연결될 경우 IP 주소 할당이 혼란스러워질 수 있습니다. DHCP Snooping은 DHCP 서버가 연결된 물리 포트를 지정하고, 지정되지 않은 포트에서는 DHCP 서버가 전송하는 패킷을 차단함으로써 불법 DHCP 서버의 영향을 줄일 수 있습니다.

이 절에서는 다음과 같은 내용을 포함합니다.

- DHCP Snooping 처리 과정
- DHCP Snooping 바인딩 테이블
- DHCP 서버 물리 포트 바인딩

16.1.1. DHCP Snooping 처리 과정

DHCP Snooping 프로토콜은 DHCP Request, DHCP ACK, DHCP Release 메시지만 가로채어 처리하며, 그 외의 DHCP 메시지는 수신하지 않습니다.

스위치는 이 메시지들을 기반으로 IP 주소와 MAC 주소 간의 매핑 관계를 바인딩합니다.

글로벌 DHCP Snooping 스위치는 DHCP 메시지 수신 기능을 활성화하는 역할을 합니다.

즉, UDP 포트 67번과 68번을 사용하는 IP 메시지를 수신하도록 설정합니다.

16.1.2. DHCP Snooping 바인딩 테이블

DHCP Snooping 바인딩 테이블 엔트리는 MAC 주소를 기준으로 인덱싱되며, 다음 정보를 포함합니다.

- 엔트리 유형

- IP 주소
- MAC 주소
- 인터페이스 정보
- Delay Timer
- Lease Timer

엔트리 유형은 REQ와 ACK 두 가지가 있습니다.

REQ 유형은 DHCP Request 메시지는 수신했지만 DHCP ACK 메시지는 아직 수신하지 않은 상태를 의미합니다. 이때 Delay Timer가 시작되며, 기본 시간은 10초입니다. 10초 이내에 DHCP ACK 메시지를 수신하지 못하면 REQ 유형의 바인딩 테이블 엔트리는 삭제됩니다.

ACK 유형은 DHCP ACK 메시지를 수신한 상태를 의미합니다. 이때 기록되는 IP 주소는 DHCP 서버가 할당한 IP 주소입니다. 이후 Lease Timer가 시작되며, 이 시간은 DHCP ACK 메시지에 포함된 DHCP 서버의 Lease 값을 사용합니다. Lease가 갱신되면 타이머가 다시 시작되고, Lease가 만료되면 해당 바인딩 테이블 엔트리는 삭제됩니다.

인터페이스 정보는 클라이언트가 위치한 인터페이스를 기록합니다. 즉, IP 주소와 MAC 주소의 바인딩 관계가 연결된 포트를 의미합니다.

DHCP Request 메시지를 수신하면 바인딩 테이블 엔트리가 생성됩니다. 이 엔트리는 REQ 유형이며, IP 주소, MAC 주소, 인터페이스 정보를 기록하고 10초 Delay Timer를 시작합니다.

DHCP Request 메시지를 수신했을 때 이미 REQ 유형의 바인딩 테이블 엔트리가 존재하면, 해당 엔트리를 갱신하고 Delay Timer를 다시 시작합니다.

DHCP Request 메시지를 수신했을 때 ACK 유형의 바인딩 테이블 엔트리가 이미 존재하면, 인터페이스 정보를 기록합니다.

DHCP ACK 메시지를 수신했을 때 REQ 유형의 바인딩 테이블 엔트리가 존재하면, DHCP ACK 메시지에 포함된 서버 할당 IP 주소를 기록하고 Delay Timer를 종료한 뒤 Lease Timer를 시작합니다.

DHCP ACK 메시지를 수신했는데 REQ 유형의 바인딩 테이블 엔트리가 없으면, 해당 메시지는 폐기됩니다.

DHCP ACK 메시지를 수신했을 때 ACK 유형의 바인딩 테이블 엔트리가 이미 존재하고 인터페이스가 변경된 경우, 기존 인터페이스의 바인딩 테이블 엔트리를 삭제하고 엔트리를 갱신합니다.

인터페이스는 변경되지 않았지만 서버가 할당한 IP 주소가 변경된 경우에도 기존 인터페이스의 바인딩 테이블 엔트리를 삭제하고 엔트리를 갱신합니다.

인터페이스와 IP 주소가 모두 변경되지 않은 경우에는 Lease 갱신 과정으로 판단하고 Lease Timer를 다시 시작합니다.

Delay Timer가 만료되면 REQ 유형의 바인딩 테이블 엔트리는 삭제됩니다.

Lease Timer가 만료되면 ACK 유형의 바인딩 테이블 엔트리는 삭제됩니다.

16.1.3. DHCP Snooping 서버 연결 포트 지정

DHCP Snooping에서는 DHCP 서버가 연결된 물리 포트를 지정할 수 있습니다.

DHCP 메시지는 지정된 포트에서만 수신되며, 지정되지 않은 포트에서 들어오는 DHCP 서버의 메시지는 차단됩니다.

네트워크에 여러 DHCP 서버가 존재할 경우, 지정되지 않은 포트에서 들어오는 DHCP OFFER 메시지는 필터링되므로, 해당 서버는 클라이언트에게 IP 주소를 할당할 수 없습니다.

이와 같이 서버 포트를 지정하면 네트워크에서 IP 주소를 일관되게 할당할 수 있으며, 계획되지 않은 DHCP 서버의 주소 풀로 인해 일부 클라이언트가 정상적으로 네트워크에 접속하지 못하는 문제를 방지할 수 있습니다.

또한, 비인가 DHCP 서버가 네트워크에 연결되어 발생할 수 있는 통신 장애를 줄이는 데에도 도움이 됩니다.

16.2. DHCP Snooping 설정

16.2.1. 기본 설정

- DHCP Snooping은 기본적으로 비활성화 상태입니다.
- DHCP Snooping 바인딩 테이블에서 REQ 유형 엔트리의 기본 Delay Timer 값은 10초입니다.

16.2.2. DHCP Snooping 글로벌 활성화 및 비활성화

DHCP Snooping은 글로벌로 먼저 활성화되어야 인터페이스 단위에서 설정할 수 있습니다. 또한 글로벌 DHCP Snooping을 비활성화하기 전에 모든 인터페이스 설정을 먼저 해제해야 합니다.

글로벌 DHCP Snooping 활성화

Switch# configure terminal

Switch(config)# ip dhcp snooping [IF_LIST]

- [IF_LIST]는 DHCP 서버가 연결된 물리 포트 목록입니다.
- 최대 4개의 포트를 지정할 수 있으며, 쉼표(,)로 구분합니다.
  예: ge1/1, ge1/4, ge1/5

글로벌 DHCP Snooping 비활성화

Switch# configure terminal

Switch(config)# no ip dhcp snooping

16.2.3. 인터페이스 DHCP Snooping 활성화 및 비활성화

포트에서 DHCP Snooping 활성화

Switch# configure terminal

Switch(config)# interface ge1/1

Switch(config-ge1/1)# dhcp snooping

포트에서 DHCP Snooping 비활성화

Switch# configure terminal

Switch(config)# interface ge1/1

Switch(config-ge1/1)# no dhcp snooping

16.2.4. 인터페이스 DHCP Snooping Option82 설정

포트에서 DHCP Snooping Option82 활성화

Switch# configure terminal

Switch(config)# interface ge1/1

Switch(config-ge1/1)# dhcp snooping option82

포트에서 DHCP Snooping Option82 비활성화

Switch# configure terminal

Switch(config)# interface ge1/1

Switch(config-ge1/1)# no dhcp snooping option82

포트의 Option82 circuit-id 설정

Switch# configure terminal

Switch(config)# interface ge1/1

Switch(config-ge1/1)# dhcp snooping option82 circuit-id vlan111

포트의 Option82 circuit-id 삭제

Switch# configure terminal

Switch(config)# interface ge1/1

Switch(config-ge1/1)# no dhcp snooping option82 circuit-id

16.2.5. DHCP Snooping 정보 확인

DHCP Snooping 설정 및 동작 상태를 확인하는 명령어입니다.

Switch# show dhcp snooping

→ DHCP Snooping 설정 정보 확인

Switch# show dhcp snooping binding-table

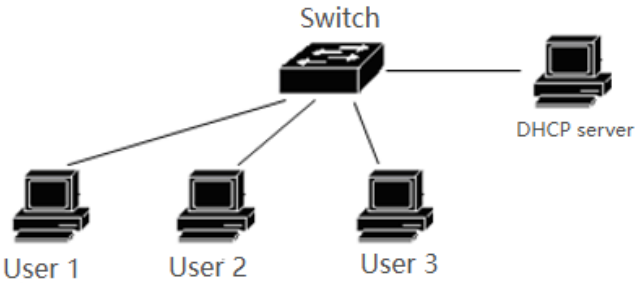
→ DHCP Snooping 바인딩 테이블 정보 확인

Switch# show running-config

→ 전체 설정 확인 (DHCP Snooping 포함)

16.3. DHCP Snooping 설정 예제

Layer 2 스위치에서 DHCP Snooping 기능을 활성화하고, User1, User2, User3가 DHCP 서버를 통해 IP 주소와 네트워크 정보를 동적으로 할당받도록 설정합니다. 또한 각 사용자 포트에서 DHCP Snooping Option82 기능을 활성화하고, circuit-id를 aaa로 설정하며, ARP 정보가 동적으로 바인딩되도록 구성합니다.



Switch# configure terminal

Switch(config)# ip dhcp snooping ge1/5

Switch(config)# interface ge1/1

Switch(config-ge1/1)# dhcp snooping

Switch(config-ge1/1)# dhcp snooping option82

Switch(config-ge1/1)# dhcp snooping option82 circuit-id aaa

Switch(config)# interface ge1/2

Switch(config-ge1/2)# dhcp snooping

Switch(config-ge1/2)# dhcp snooping option82

Switch(config-ge1/2)# dhcp snooping option82 circuit-id aaa

Switch(config)# interface ge1/3

Switch(config-ge1/3)# dhcp snooping

Switch(config-ge1/3)# dhcp snooping option82

Switch(config-ge1/3)# dhcp snooping option82 circuit-id aaa

Switch(config)# end

DHCP Snooping 상태 확인

Switch# show dhcp snooping

출력 예시:

- DHCP Snooping 글로벌 활성화 상태
- DHCP 서버 포트: ge1/5
- 활성화된 인터페이스: ge1/1, ge1/2, ge1/3
- Option82 적용 인터페이스 및 Circuit ID

바인딩 테이블 확인

Switch# show dhcp snooping binding-table

IP	MAC	FLAG	PORT	LEASE
192.168.1.100	xx:xx:xx:34:42:ad	ACK	ge1/1	23:59:58
192.168.1.101	xx:xx:xx:52:13:5d	ACK	ge1/2	23:50:01
192.168.1.102	xx:xx:xx:4d:a2:46	ACK	ge1/3	20:34:45

16.4. DHCP Snooping 설정 문제 해결

DHCP Snooping 설정이 실패하는 경우, 다음과 같은 원인이 있을 수 있습니다.

1) 시스템의 CFP 리소스가 부족한 경우
2) 인터페이스에 ACL 필터링 기능이 설정되어 있어 글로벌 DHCP Snooping 활성화가 실패하는 경우
3) 인터페이스에 IP-MAC 바인딩이 설정되어 있어 글로벌 DHCP Snooping 활성화가 실패하는 경우
4) 현재 인터페이스에 ACL 필터링 기능이 설정된 경우
5) 해당 인터페이스에서 802.1X Anti-ARP Spoofing 기능이 활성화된 경우
6) 설정하려는 인터페이스가 Layer 3 인터페이스이거나 Trunk 인터페이스인 경우

17. DHCP Client 설정

17.1. DHCP Client 소개

DHCP(Dynamic Host Configuration Protocol)는 Client/Server 방식으로 동작하는 프로토콜입니다.

DHCP Client 기능을 사용하면 스위치의 Layer 3 인터페이스가 DHCP 서버로부터 IP 주소와 게이트웨이 정보를 자동으로 할당받을 수 있습니다.

이 절에서는 다음 내용을 포함합니다.

- DHCP Client 설정

17.2. DHCP Client 설정

VLAN1 인터페이스에서 DHCP Client 활성화

Switch(config)# interface vlan1

Switch(config-vlan1)# dhcp client enable

VLAN1 인터페이스 IP 주소 재요청 (Renew)

Switch(config)# interface vlan1

Switch(config-vlan1)# dhcp client renew

VLAN1 인터페이스 IP 주소 해제 (Release)

Switch(config)# interface vlan1

Switch(config-vlan1)# dhcp client release

18. DHCP Relay 설정

이 장에서는 DHCP Relay 설정과 관련된 내용을 설명하며, 다음과 같은 항목을 포함합니다.

- DHCP Relay 소개

- DHCP Relay 설정
- DHCP Relay 설정 예제

18.1. DHCP Relay 소개

DHCP(Dynamic Host Configuration Protocol)는 BOOTP의 확장 버전으로, 네트워크에 연결된 호스트의 TCP/IP 환경을 동적으로 설정하는 프로토콜입니다. DHCP는 서버와 클라이언트 구조로 동작하며, 서버는 IP 주소 및 네트워크 정보를 중앙에서 관리하고 클라이언트 요청에 따라 이를 할당합니다.

DHCP는 다음과 같은 방식으로 주소를 할당합니다.

- 자동 할당(Automatic): 한 번 할당된 IP를 지속적으로 사용
- 동적 할당(Dynamic): IP에 임대(Lease) 기간이 있으며, 만료 시 반납 또는 갱신

DHCP 동작 과정

클라이언트가 네트워크에 처음 접속하면 IP 정보가 없기 때문에 출발지 0.0.0.0, 목적지 255.255.255.255로 Discover 메시지를 브로드캐스트합니다.

서버 응답이 없으면 일정 간격으로 최대 4번까지 재전송합니다.

서버는 Discover를 수신하면 사용 가능한 IP를 선택하여 Offer 메시지로 응답합니다.

네트워크에 여러 DHCP 서버가 있을 경우 클라이언트는 여러 Offer를 받을 수 있으며, 일반적으로 가장 먼저 도착한 Offer를 선택하고 Request 메시지를 브로드캐스트하여 선택한 서버를 알립니다.

클라이언트가 ARP 확인을 통해 해당 IP가 이미 사용 중임을 발견하면 Decline 메시지를 보내고 다시 Discover 과정을 시작합니다.

서버는 Request 메시지를 수신하면 Ack 메시지를 보내 IP 할당을 확정합니다.

이미 IP를 사용 중인 클라이언트는 Discover 과정을 거치지 않고, 임대 기간 만료 전에 Request 메시지로 갱신(Renew)을 요청합니다.

서버는 문제가 없으면 Ack로 승인하고, 문제가 있으면 Nack 메시지로 거부합니다.

클라이언트는 필요 시 Release 메시지를 통해 IP를 반환할 수 있습니다.

또한 클라이언트는

- 부팅 시 Request 전송
- Lease의 50% 시점에 갱신 요청
- Lease의 75% 시점에도 재요청을 수행하며, 응답이 없으면 IP 사용이 제한됩니다.

DHCP Relay 필요성

DHCP Discover 메시지는 브로드캐스트이므로 동일 네트워크에서만 전달되며, 라우터를 통해 다른 네트워크

로 전달되지 않습니다.

클라이언트와 DHCP 서버가 서로 다른 네트워크에 위치할 경우, 클라이언트는 서버에 도달할 수 없습니다. 이를 해결하기 위해 DHCP Relay 기능을 사용하여 라우터 또는 Layer 3 장비가 DHCP 메시지를 대신 전달하도록 합니다.

이 기능을 통해 DHCP는 서로 다른 네트워크 간에서도 정상적으로 동작할 수 있습니다.

18.2. DHCP Relay 설정

DHCP Relay 기능은 주로 인터페이스와 관련되어 있으며, 네트워크 간 DHCP 메시지를 전달하기 위해 인터페이스 모드에서 설정합니다.

DHCP Relay 설정에는 다음과 같은 항목이 포함됩니다.

- 인터페이스에서 DHCP Relay 기능 활성화

18.2.1. 인터페이스 DHCP Relay 기능 활성화

- 모드: 인터페이스 설정 모드
- 명령어:

  dhcp relay <ip-address-1> [ip-address-2]
  → 인터페이스에서 DHCP Relay 기능을 활성화하고, DHCP 서버 IP 주소를 설정

  no dhcp relay
  → 인터페이스에서 DHCP Relay 기능 비활성화

- 기본값
  → DHCP Relay 기능은 기본적으로 비활성화 상태입니다.

18.2.2. DHCP Relay 정보 확인

Switch# show dhcp relay

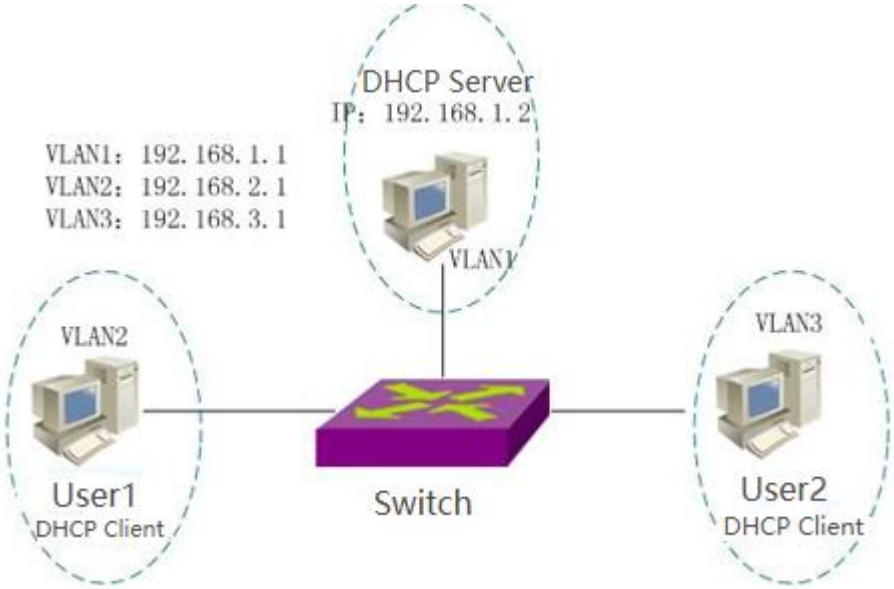
→ DHCP Relay 설정 정보 확인

18.3. DHCP Relay 설정 예제

1) 설정

스위치에서 DHCP Relay 기능을 설정하여, User1과 User2의 DHCP 요청과 DHCP 서버의 응답을 라우팅 및 전달할 수 있도록 구성합니다.

User1과 User2는 서로 다른 네트워크에 있는 DHCP 서버를 통해 IP 주소를 할당받을 수 있습니다.




```
Switch> enable
Switch# configure terminal

Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 3
Switch(config-vlan)# exit

Switch(config)# ip interface vlan 2
Switch(config)# ip interface vlan 3

Switch(config)# interface ge1/2
Switch(config-ge1/2)# switchport access vlan 2

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport access vlan 3
```

```
Switch(config)# interface vlan2
Switch(config-vlan2)# ip address 192.168.2.1/24
Switch(config-vlan2)# dhcp relay 192.168.1.2

Switch(config)# interface vlan3
Switch(config-vlan3)# ip address 192.168.3.1/24
Switch(config-vlan3)# dhcp relay 192.168.1.2
```

2) 확인

```
Switch# show running-config
```

→ 현재 설정 확인

```
Switch# show dhcp relay
```

→ DHCP Relay 설정 정보 확인

19. DHCP Server 설정

이 장에서는 DHCP Server 설정과 관련된 내용을 설명하며, 다음과 같은 항목을 포함합니다.

- DHCP Server 소개
- DHCP Server 설정

- DHCP Server 설정 예제

19.1. DHCP Server 소개

DHCP(Dynamic Host Configuration Protocol)는 BOOTP의 확장 버전으로, 네트워크에 연결된 호스트의 TCP/IP 환경을 동적으로 설정하는 프로토콜입니다. DHCP는 서버와 클라이언트 구조로 동작하며, 서버는 IP 주소와 네트워크 정보를 중앙에서 관리하고 클라이언트 요청에 따라 이를 할당합니다.

DHCP는 다음과 같은 방식으로 주소를 할당합니다.

- 자동 할당: 한 번 할당된 IP 주소를 지속적으로 사용
- 동적 할당: IP 주소에 임대(Lease) 기간이 있으며, 만료 시 반환 또는 갱신

동적 할당은 IP 주소 부족 문제를 효율적으로 해결할 수 있습니다.

DHCP 동작 과정

클라이언트가 처음 네트워크에 접속하면 IP 정보가 없기 때문에 출발지 0.0.0.0, 목적지 255.255.255.255로 Discover 메시지를 브로드캐스트합니다. 서버 응답이 없으면 일정 간격으로 최대 4번까지 재전송합니다.

서버는 Discover를 수신하면 사용 가능한 IP를 선택하여 Offer 메시지로 응답합니다.

여러 DHCP 서버가 있을 경우 클라이언트는 여러 Offer를 받을 수 있으며, 일반적으로 가장 먼저 도착한 Offer를 선택하고 Request 메시지를 브로드캐스트하여 선택한 서버를 알립니다.

클라이언트가 ARP 확인을 통해 해당 IP가 이미 사용 중임을 발견하면 Decline 메시지를 보내고 다시 Discover 과정을 시작합니다.

서버는 Request 메시지를 수신하면 Ack 메시지를 보내 IP 할당을 확정합니다.

이미 IP를 사용 중인 클라이언트는 Discover 과정을 거치지 않고, 임대 기간 만료 전에 Request 메시지로 갱신을 요청합니다. 서버는 문제가 없으면 Ack로 승인하고, 문제가 있으면 Nack 메시지로 거부합니다.

클라이언트는 필요 시 Release 메시지를 통해 IP를 반환할 수 있습니다.

또한 클라이언트는 부팅 시 Request를 전송하고, Lease의 50% 시점과 75% 시점에도 갱신 요청을 수행하며, 응답이 없으면 IP 사용이 제한됩니다.

DHCP Server 역할

DHCP 서버는 Discover, Request, Decline, Release 메시지를 처리하며, 네트워크 내 클라이언트에게 IP 주소를 동적으로 할당합니다. 또한 자체 주소 풀 정보와 클라이언트 할당 정보를 관리합니다.

19.2. DHCP Server 설정

DHCP Server 기능은 Global 모드, Interface 모드, Address Pool 모드에서 설정하며, 기능 활성화, 주소 풀 구성, 글로벌 설정 및 세부 옵션 설정을 포함합니다.

DHCP Server 설정 항목은 다음과 같습니다.

- 글로벌 DHCP Server 기능 활성화
- DHCP 메시지를 수신할 인터페이스 활성화
- 주소 풀(Address Pool) 설정
- 주소 풀 범위 설정
- 서브넷 마스크 설정
- 임대 기간(Lease) 설정
- 기본 게이트웨이 설정
- DNS 서버 설정
- 주소 풀에서 제외할 IP 설정

19.2.1. 글로벌 DHCP Server 기능 활성화

- 모드: Global Configuration Mode
- 명령어:

  ip dhcp server
  → 글로벌 DHCP Server 기능 활성화

  no ip dhcp server
  → 글로벌 DHCP Server 기능 비활성화

- 기본값
  → DHCP Server 기능은 기본적으로 비활성화 상태입니다.

19.2.2. 인터페이스 DHCP Server 메시지 수신 설정

- 모드: Interface Configuration Mode
- 명령어:

  dhcp server listen
  → 인터페이스에서 DHCP Server 메시지 수신 활성화

  no dhcp server listen

→ 인터페이스에서 DHCP Server 메시지 수신 비활성화

- 기본값
  → 인터페이스는 기본적으로 비활성화 상태이며 DHCP Server 메시지를 수신하지 않습니다.

19.2.3. 주소 풀(Address Pool) 설정

- 모드: Global Configuration Mode
- 명령어:

  dhcp server pool <pool-name>
  → 주소 풀 생성 및 주소 풀 설정 모드 진입

  no dhcp server pool <pool-name>
  → 지정된 주소 풀 삭제

- 파라미터
  <pool-name>: 주소 풀 이름으로, 서로 다른 주소 풀을 구분하는 데 사용되며 최대 16자까지 설정 가능
- 기본값
  → 주소 풀은 기본적으로 설정되어 있지 않으며, 주소 풀 이름을 생성하면 별도의 IP 설정 없이도 주소 풀 모드로 진입할 수 있습니다.

19.2.4. 주소 풀 범위 설정

- 모드: Address Pool Configuration Mode
- 명령어:

  range <low-address> <high-address>
  → 주소 풀의 시작 IP와 끝 IP 범위 설정

  no range
  → 주소 풀 범위 삭제

- 파라미터
  <low-address>: 시작 IP 주소 (점 표기 형식)
  <high-address>: 끝 IP 주소 (점 표기 형식)
- 기본값
  → 주소 범위는 기본적으로 설정되어 있지 않으며, 범위를 설정하면 해당 범위 내의 모든 IP에

대해 동적 할당 가능한 엔트리가 생성됩니다.

19.2.5. 주소 풀 서브넷 마스크 설정

- 모드: Address Pool Configuration Mode
- 명령어:

  subnet-mask <address>
  → 주소 풀의 서브넷 마스크 설정

- 파라미터
  <address>: 서브넷 마스크 (점 표기 형식, 가변 길이 가능)
- 기본값
  → 255.255.255.0 (24비트 마스크)

19.2.6. 주소 풀 Lease(임대 기간) 설정

- 모드: Address Pool Configuration Mode
- 명령어:

  lease [<days> <hours> <minutes> | infinite]
  → 주소 풀의 임대 기간 설정

- 파라미터
  <days>: 일 (0~999)
  <hours>: 시간 (0~23)
  <minutes>: 분 (0~59)
  infinite: 무제한 임대
- 기본값
  → 8일

19.2.7. 주소 풀 기본 게이트웨이 설정

- 모드: Address Pool Configuration Mode
- 명령어:

  default-router <ip-address>
  → 주소 풀의 기본 게이트웨이 설정

no default-router
→ 주소 풀 기본 게이트웨이 삭제

- 파라미터
  <ip-address>: 기본 게이트웨이 IP 주소 (점 표기 형식, 주소 풀과 동일 네트워크 대역이어야 함)
- 기본값
  → 기본 게이트웨이는 설정되어 있지 않음

19.2.8. 주소 풀 DNS 서버 설정

- 모드: Address Pool Configuration Mode
- 명령어:

  dns-server <ip-address1> [ip-address2]
  → 주소 풀의 DNS 서버 설정

  no dns-server
  → 주소 풀 DNS 서버 설정 삭제

- 파라미터
  <ip-address1>, <ip-address2>: DNS 서버 IP 주소 (점 표기 형식)
  → 최대 2개의 DNS 서버를 한 번의 명령으로 설정 가능
- 주의사항
  → DNS 서버를 두 개 설정할 경우 반드시 한 줄에서 함께 입력해야 함
  → 명령을 다시 입력하면 기존 DNS 설정은 덮어쓰기 됨
- 기본값
  → DNS 서버는 설정되어 있지 않음

19.2.9. 주소 풀 수동 제외 주소 설정

- 모드: Address Pool Configuration Mode
- 명령어:

  exclude-address <ip-address>
  → 특정 IP 주소를 주소 풀에서 제외

  exclude-address <low-address> <high-address>
  → 연속된 IP 주소 범위를 주소 풀에서 제외

no exclude-address <ip-address>
→ 제외된 특정 IP 주소 복원

no exclude-address <low-address> <high-address>
→ 제외된 IP 주소 범위 복원

no exclude-address all
→ 모든 제외 주소 복원

- 파라미터
  <ip-address>: 제외할 단일 IP 주소 (점 표기 형식)
  <low-address>, <high-address>: 제외할 IP 범위의 시작과 끝 주소
- 설명
  → 제외된 주소는 DHCP에서 동적으로 할당되지 않음
  → 범위 내 이미 제외된 주소는 별도 메시지 없이 건너뜀
- 기본값
  → 수동 제외 주소는 설정되어 있지 않음

19.2.10. Option82 설정

- 모드: Address Pool Configuration Mode
- 명령어:

  option82 circuit-id <circuit-id>
  → Option82의 circuit-id 설정

- 파라미터
  <circuit-id>: 문자열, 최대 64자까지 설정 가능

19.2.11. 할당된 주소 테이블 엔트리 삭제

- 모드: EXEC Mode
- 명령어:

  clear dhcp server address [ip-address | all]
  → 특정 IP 주소 또는 전체 DHCP 할당 테이블 엔트리 삭제

19.2.12. 충돌 감지 주소 엔트리 삭제

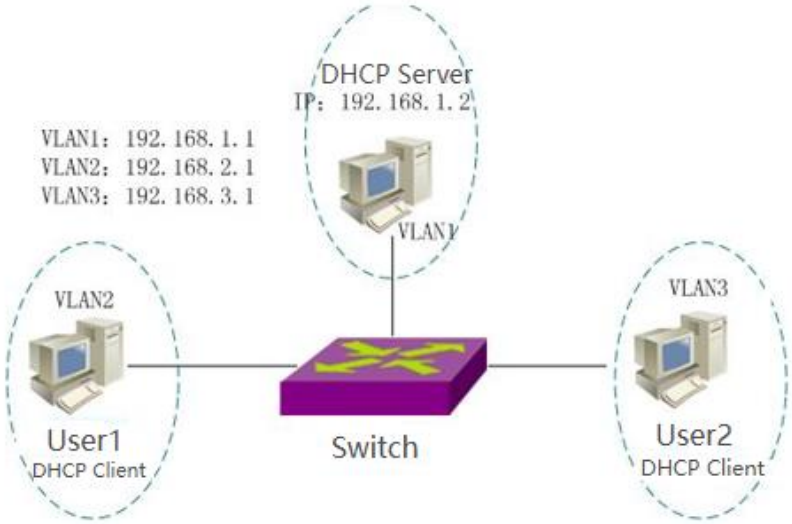
- 모드: EXEC Mode

- 명령어:

clear dhcp server address conflict [ip-address | all]
→ 충돌로 인해 자동 제외된 주소를 삭제
→ 특정 IP 주소 또는 전체 충돌 주소 삭제 가능

19.3. DHCP Server 설정 예제

1) 설정
스위치를 DHCP 서버로 구성하여 VLAN1, VLAN2, VLAN3의 서로 다른 네트워크에 대해 각각 주소 풀을 설정하고, 각 VLAN에 속한 클라이언트에게 해당 네트워크 대역의 IP 주소를 할당합니다.



Switch> enable
Switch# configure terminal

Switch(config)# ip dhcp server

Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 3
Switch(config-vlan)# exit

Switch(config)# ip interface vlan 2
Switch(config)# ip interface vlan 3

Switch(config)# interface ge1/2

```
Switch(config-ge1/2)# switchport access vlan 2

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport access vlan 3

Switch(config)# interface vlan2
Switch(config-vlan2)# ip address 192.168.2.1/24
Switch(config-vlan2)# dhcp server listen

Switch(config)# interface vlan3
Switch(config-vlan3)# ip address 192.168.3.1/24
Switch(config-vlan3)# dhcp server listen

Switch(config)# interface vlan1
Switch(config-vlan1)# dhcp server listen

Switch(config)# dhcp server pool a
Switch(config-dhcp)# range 192.168.2.1 192.168.2.20
Switch(config-dhcp)# lease 2 0 0
Switch(config-dhcp)# default-router 192.168.2.1
Switch(config-dhcp)# dns-server 1.1.1.1 2.2.2.2
Switch(config-dhcp)# exclude-address 192.168.2.10
Switch(config-dhcp)# exit

Switch(config)# dhcp server pool b
Switch(config-dhcp)# range 192.168.3.2 192.168.3.20
Switch(config-dhcp)# default-router 192.168.3.1
Switch(config-dhcp)# exit

Switch(config)# dhcp server pool c
Switch(config-dhcp)# range 192.168.1.2 192.168.1.20
Switch(config-dhcp)# default-router 192.168.1.1
Switch(config-dhcp)# exit
```

2) 확인

```
Switch# show running-config
```

→ 전체 설정 확인

```
Switch# show dhcp server
```

→ DHCP 서버 글로벌 설정 확인

Switch# show dhcp server pool [pool-name]
→ 특정 주소 풀 설정 확인

Switch# show dhcp server address
→ 할당된 IP 주소 테이블 확인

20. ACL 설정

실제 네트워크 환경에서 관리자는 네트워크 접근 보안에 많은 관심을 가집니다. 스위치는 ACL(Access Control List) 필터링 기능을 지원하여 네트워크 접근 보안을 제공합니다. ACL 규칙을 설정하면, 스위치는 해당 규칙에 따라 입력되는 트래픽을 필터링하여 접근을 제어할 수 있습니다.

이 장에서는 ACL 설정 방법을 설명하며, 다음과 같은 내용을 포함합니다.

- ACL 리소스 라이브러리 소개
- ACL 필터링 소개
- ACL 리소스 풀 설정
- ACL 필터링 설정
- ACL 설정 예제

20.1. ACL 리소스 라이브러리 소개

ACL(Access Control List) 리소스 라이브러리는 여러 개의 접근 제어 규칙 그룹으로 구성된 집합입니다. ACL 리소스 라이브러리 자체는 데이터 포워딩을 직접 제어하는 기능은 없으며, 충돌하는 규칙들을 정렬한 규칙 집합입니다. 이후 ACL 리소스 풀을 애플리케이션에서 참조하면, 해당 애플리케이션이 ACL 규칙에 따라 데이터 포워딩을 제어하게 됩니다. ACL은 포트 접근 제어, 서비스 접근 제어, QoS 등 다양한 기능에 적용될 수 있습니다.

ACL 리소스 라이브러리는 다음과 같은 유형의 규칙 그룹으로 구성됩니다.

- 표준 IP ACL: 그룹 번호 1~99, 1300~1999
- 확장 IP ACL: 그룹 번호 100~199, 2000~2699
- IP-MAC ACL: 그룹 번호 700~799
- ARP ACL: 그룹 번호 1100~1199

각 ACL 그룹 내부에서는 규칙 간 충돌이 발생할 경우 자동으로 우선순위가 정렬됩니다. 사용자가 ACL 규칙을 설정하면, 시스템은 해당 규칙을 적절한 위치에 자동으로 삽입합니다.

실제 동작 시, 패킷이 스위치를 통과할 때 스위치는 각 규칙의 필드와 패킷의 해당 필드를 비교합니다. 여러 규칙이 동시에 완전히 일치할 경우, 가장 먼저 완전히 일치하는 규칙이 적용됩니다. 해당 규칙의 permit 또는 deny에 따라 패킷이 전달되거나 차단됩니다.

여기서 "완전 일치"란 규칙의 필드 값이 패킷의 해당 필드 값과 정확히 동일한 경우를 의미합니다. ACL 규칙과 완전히 일치하지 않으면 permit 또는 deny 동작은 수행되지 않습니다.

스위치 내부에서는 동일한 그룹에 속한 규칙들이 자동으로 정렬됩니다. 이 정렬 과정은 비교적 복잡하며, 범위가 넓은 규칙은 뒤로, 범위가 좁은 규칙은 앞으로 배치됩니다.

규칙의 범위는 제약 조건의 수에 의해 결정됩니다.

- 제약 조건이 적을수록 → 매칭 범위가 넓음
- 제약 조건이 많을수록 → 매칭 범위가 좁음

이 제약 조건은 주로 다음 요소에 의해 결정됩니다.

- 주소의 Wildcard 값
- 비주소 필드 (프로토콜 타입, IP 프로토콜, 포트 등)

Wildcard는 비트 문자열로 구성됩니다.

- IP 주소는 4바이트

- MAC 주소는 6바이트

Wildcard에서

- 1 → 해당 비트는 매칭하지 않음
- 0 → 해당 비트는 반드시 매칭

즉, Wildcard에서 0이 많을수록 더 많은 조건을 요구하므로 규칙의 범위가 좁아집니다. 반대로 1이 많을수록 조건이 적어져 범위가 넓어집니다.

규칙 정렬 예시

포트 접근 제어 예시를 통해 규칙 정렬의 필요성을 설명합니다.

요구사항:

- 192.168.1.0/24 대역은 허용
- 10.10.0.0/16 대역은 차단

설정 예:

access-list 1 permit 192.168.1.0 0.0.0.255 (Rule 1)

access-list 1 deny 10.10.10.0 0.0.255.255 (Rule 2)

이 두 규칙은 서로 충돌합니다. Rule 1의 주소 범위가 Rule 2의 범위에 포함되기 때문입니다.

올바른 동작을 위해서는 다음 순서가 되어야 합니다.

Rule 1 → Rule 2

스위치는 이 순서를 자동으로 정렬합니다. 사용자가 어떤 순서로 입력하더라도 내부적으로는 위와 같이 정렬됩니다.

패킷 처리 예:

- 192.168.1.1 → Rule 1 먼저 매칭 → 허용
- 10.10.10.1 → Rule 2 매칭 → 차단

만약 정렬 기능이 없다면 Rule 2가 먼저 적용되어 Rule 1이 무시되는 문제가 발생할 수 있습니다.

Wildcard 예시 설명

- Rule 2: 0.0.255.255 → 16비트만 비교 → 범위 넓음
- Rule 1: 0.0.0.255 → 24비트 비교 → 범위 좁음

따라서 Rule 1이 먼저, Rule 2가 나중에 위치합니다.

확장 ACL에서는 다음 요소들도 정렬 기준에 포함됩니다.

- IP 프로토콜
- 포트 번호

기본 원칙은 동일합니다.

조건이 많을수록 앞쪽, 조건이 적을수록 뒤쪽 배치

ACL 필터링 항목

ACL에서 지원하는 주요 필터링 필드는 다음과 같습니다.

- 출발지 IP 주소
- 목적지 IP 주소
- IP 프로토콜 (TCP, UDP, OSPF 등)
- 출발지 포트
- 목적지 포트

20.2. ACL 필터링 소개

ACL 필터링은 스위치의 입력 포트(Ingress Port)에서 수행되며, 해당 포트로 들어오는 데이터 흐름에 대해 규칙 매칭을 통해 필터링을 수행합니다. ACL 필터링은 스위치의 라인 속도(line-rate)로 처리되므로 데이터 포워딩 성능에는 영향을 주지 않습니다.

스위치 포트에 ACL 필터링이 설정되지 않은 경우, 해당 포트로 들어오는 모든 트래픽은 규칙 매칭 없이 그대로 전달됩니다. 반대로 포트에 ACL 필터링이 설정된 경우, 해당 포트로 들어오는 모든 트래픽은 ACL 규칙과 비교됩니다.

매칭된 규칙이 permit이면 트래픽은 전달됩니다.

deny이면 트래픽은 차단되고 폐기됩니다.

포트에 ACL 필터링을 설정할 때 하나 이상의 ACL 규칙 그룹을 선택할 수 있습니다. 선택된 규칙 그룹은 해당 포트의 CFP(Content Flow Processor)에 적용됩니다. 만약 규칙 그룹 내에 모든 IP 트래픽을 허용하거나 차단하는 규칙이 없는 경우, CFP에 적용될 때 모든 IP를 차단하는 규칙이 자동으로 추가됩니다. ACL 리소스가 변경되면 CFP에 적용된 규칙도 자동으로 업데이트됩니다.

예를 들어, 다음과 같은 규칙이 하나만 있는 경우:

```
access-list 1 permit 192.168.1.0 0.0.0.255
```

내부적으로는 "모든 IP 차단" 규칙이 자동으로 추가되어 실제로는 두 개의 규칙이 적용됩니다. 따라서

192.168.1.0 ~ 192.168.1.255 범위만 허용되고, 나머지 트래픽은 모두 차단됩니다.

또 다른 예로, 다음과 같은 두 개의 규칙이 있는 경우:

access-list 1 deny 192.168.1.0 0.0.0.255

access-list 1 permit any

이미 모든 트래픽을 허용하는 규칙이 있으므로 추가적인 숨겨진 규칙은 생성되지 않습니다. 이 경우 192.168.1.0 ~ 192.168.1.255 대역만 차단되고, 나머지 트래픽은 모두 허용됩니다.

다음과 같은 상황을 가정할 수 있습니다.

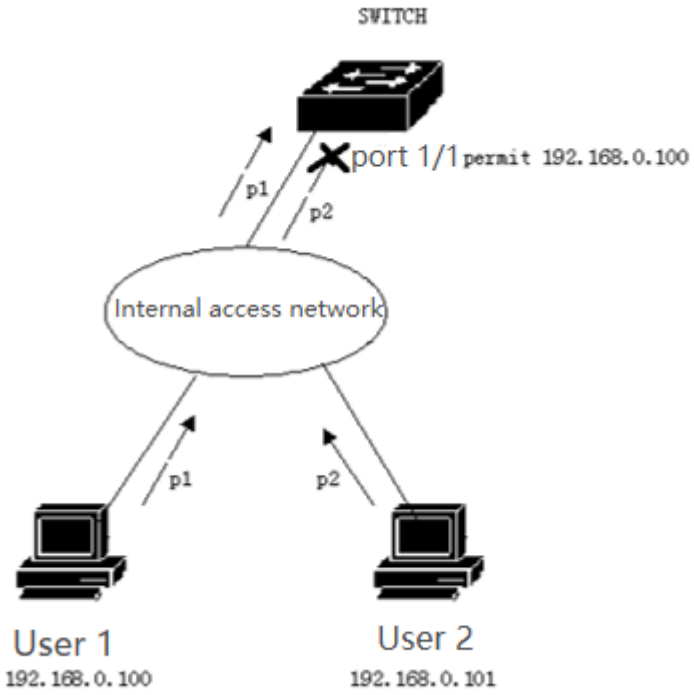
스위치의 포트 1/1에 다음 규칙이 포함된 ACL 그룹 1이 적용되어 있습니다.

access-list 1 permit 10.10.10.100

포트 1/1 아래에 두 사용자가 연결되어 있을 때:

사용자1: 10.10.10.100

사용자2: 10.10.10.101



이 경우 사용자1의 트래픽만 허용되고, 사용자2의 트래픽은 차단됩니다. 즉, 사용자1의 트래픽(P1)은 전달되고, 사용자2의 트래픽(P2)은 포트에서 폐기됩니다.

여러 포트에서 ACL 필터링을 사용하는 경우, 동일한 ACL 규칙 그룹을 여러 포트에 적용하여 동일한 필터링 정책을 사용할 수 있습니다.

하나 또는 여러 개의 ACL 규칙 그룹이 포트에 적용되더라도 규칙은 자동으로 정렬되며, 서로 다른 그룹 간에도 정렬이 적용됩니다.

또한, 포트가 참조하고 있는 ACL 규칙 그룹이 변경되면 해당 포트는 자동으로 변경 사항을 반영하며, 별도의 재설정 없이도 적용됩니다.

20.3. ACL 리소스 풀 설정

스위치는 기본적으로 어떤 ACL 규칙도 설정되어 있지 않습니다.

스위치의 리소스 풀은 다음 네 가지 ACL 규칙 유형을 지원합니다.

- 표준 IP ACL
- 확장 IP ACL
- IP-MAC ACL
- ARP ACL

ACL 설정은 위 네 가지 규칙 유형을 기준으로 구성됩니다.

표준 IP ACL (Standard IP Rules)

표준 IP ACL은 출발지 IP 주소를 기준으로 패킷 포워딩을 제어합니다.

access-list <groupId> {deny | permit} <source>

- groupId: ACL 그룹 번호
  → 1~99, 1300~1999 사용 가능
- deny / permit: 매칭 시 차단 또는 허용
- source: 출발지 IP

출발지 IP 입력 방식:

- A.B.C.D wildcard → 네트워크 대역 지정
- any → 모든 IP (A.B.C.D 255.255.255.255와 동일)
- host A.B.C.D → 특정 IP (A.B.C.D 0.0.0.0과 동일)

Wildcard 의미:

- 0 → 반드시 일치
- 1 → 무시

확장 IP ACL (Extended IP Rules)

확장 ACL은 표준 ACL을 확장하여 다음 항목을 기준으로 제어합니다.

- 출발지 IP
- 목적지 IP
- 프로토콜 (TCP, UDP 등)
- 포트 번호

access-list <groupId> {deny | permit} <protocol> <source> [eq <srcPort>] <destination> [destPort] <tcp-flag>

- groupId: 100~199, 2000~2699
- protocol: TCP, UDP 또는 숫자 (TCP=6 등), 전체는 ip 또는 0
- srcPort: TCP/UDP일 때 출발지 포트 지정
- destPort: 목적지 포트
- tcp-flag: TCP 플래그 (ack, fin, psh, rst, syn, urg)

IP 입력 방식은 표준 ACL과 동일합니다.

IP-MAC ACL

IP-MAC ACL은 MAC 주소 + IP 주소를 동시에 제어합니다.

access-list <groupId> {deny | permit} <src-mac> ip <src-ip> <dst-ip>

- groupId: 700~799
- src-mac: 출발지 MAC
- src-ip: 출발지 IP
- dst-ip: 목적지 IP

MAC 입력 방식:

- HHHH.HHHH.HHHH wildcard → MAC 범위 지정
- any → 전체 MAC
- host → 특정 MAC

IP 입력 방식:

- wildcard / any / host 동일

ARP ACL

ARP ACL은 ARP 패킷의 동작을 제어합니다.

access-list <groupId> {deny | permit} arp {arp-type} <sender-mac> <sender-ip>

- groupId: 1100~1199
- arp-type
- any → 전체
- reply → ARP 응답
- request → ARP 요청
- sender-mac: ARP 송신 MAC
- sender-ip: ARP 송신 IP

MAC/IP 입력 방식은 위와 동일합니다.

추가 명령어

show access-list [groupId]

→ ACL 규칙 확인

→ groupId 입력 시 해당 그룹만 표시

no access-list <groupId>

→ 해당 그룹의 ACL 전체 삭제

20.4. Time-based ACL (시간 기반 ACL)

시간 기반 ACL은 특정 시간 구간에만 ACL 규칙이 적용되도록 설정하는 기능입니다. 사용자는 특정 시간대에만 필터링이 동작하도록 설정할 수 있으며, 그 외 시간에는 해당 ACL 규칙이 적용되지 않습니다.

이를 위해 먼저 하나 이상의 시간 범위(time-range)를 정의하고, 이후 ACL 규칙에서 해당 시간 범위를 참조하면, 지정된 시간에만 ACL이 동작합니다.

ACL 규칙에서 참조한 시간 범위가 아직 설정되지 않은 경우에도 규칙 생성은 가능하지만, 실제 동작은 해당 시간 범위가 설정되고 시스템 시간이 그 범위에 포함될 때부터 적용됩니다.

시간 범위 설정 방식

시간 범위는 두 가지 방식으로 설정할 수 있습니다.

1) 상대 시간(Relative Time)
   → 특정 요일/시간 반복 (예: 매일 09:00~18:00)
2) 절대 시간(Absolute Time)
   → 특정 날짜/시간 범위 (예: 2025-01-01 09:00 ~ 2025-01-01 18:00)

시간 범위 설정 명령어

time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59>

→ 시간만 기준으로 상대 시간 설정

time-range WORD cycle-time days from <0-6> to <0-6>

→ 요일 기준 상대 시간 설정 (0~6: 일~토)

time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59> days from <0-6> to <0-6>

→ 시간 + 요일 함께 설정

time-range WORD utter-time from <year> <month> <day> <hour> <min> to <year> <month> <day> <hour> <min>

→ 절대 시간 설정

시간 범위 삭제

no time-range WORD cycle-time

→ 상대 시간 삭제

no time-range WORD utter-time

→ 절대 시간 삭제

no time-range WORD

→ 특정 시간 범위 전체 삭제

no time-range

→ 모든 시간 범위 삭제

시간 범위 확인

show time-range WORD cycle-time

→ 상대 시간 확인

show time-range WORD utter-time

→ 절대 시간 확인

show time-range WORD

→ 특정 시간 범위 전체 확인

show time-range

→ 전체 시간 범위 확인

ACL에 시간 적용

time-acl <ACL번호> time-range WORD

→ 특정 ACL에 시간 범위 적용

no time-acl <ACL번호> time-range WORD

→ ACL에서 시간 적용 해제

show time-acl <ACL번호> time-range

→ ACL에 적용된 시간 확인

show time-acl all time-range

→ 전체 ACL 시간 적용 확인

시간 범위 동작 규칙

1) 여러 개의 상대 시간 설정 → OR 조건
   → 하나라도 해당되면 동작
2) 여러 개의 절대 시간 설정 → OR 조건
   → 하나라도 해당되면 동작
3) 상대 시간 + 절대 시간 함께 설정 → AND 조건
   → 둘 다 만족해야 동작
4) 제한 사항
   - 최대 256개의 시간 범위 정의 가능
   - 하나의 시간 범위에 최대 256개의 시간 설정 가능
   - 하나의 ACL 규칙에 최대 256개의 시간 범위 적용 가능

ACL이 인터페이스에 적용될 때, 연결된 시간 조건도 함께 적용됩니다.

20.5. ACL 필터링 설정

기본적으로 스위치의 모든 포트에는 ACL 필터링이 적용되어 있지 않습니다.

명령어 목록:

access-group <groupId>

- 모드: Layer 2 인터페이스 설정 모드
- 파라미터:
  groupId: 포트에 바인딩할 ACL 그룹 번호
- 기능: ACL 포트 필터링 설정

참고:

위 명령어 설정이 실패하거나 적용되지 않는 경우, 다음과 같은 원인이 있을 수 있습니다.

- ACL 그룹 내 규칙 수가 너무 많은 경우
- 하드웨어 리소스가 부족한 경우
- 다른 애플리케이션에서 리소스를 이미 사용 중인 경우

ACL 포트 필터링 설정 확인:

show acccess-group

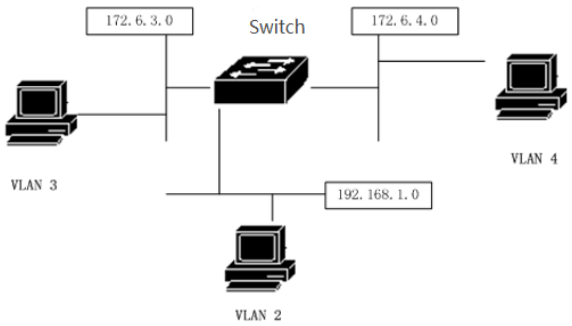
현재 포트와 ACL 포트 필터링 관련 설정 삭제:

no acl-group <groupId>

20.6. ACL 설정 예제

스위치가 3개의 서브넷에 연결되어 있으며, ACL을 통해 출발지 주소가 192.168.1.0 네트워크인 트래픽은 차단하고, 그 외의 트래픽은 허용하도록 설정합니다.

192.168.1.0 대역은 스위치의 포트 1/1에 연결되어 있습니다.



다음과 같이 스위치에 설정합니다:

```
Switch# config t
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 3

Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode access
Switch(config-ge1/1)# switchport access vlan 2

Switch(config)# interface vlan2
Switch(config-vlan2)# ip add 192.168.1.1/24

Switch(config)# interface ge1/2
Switch(config-ge1/2)# switchport mode access
Switch(config-ge1/2)# switchport access vlan 3

Switch(config)# interface vlan3
Switch(config-vlan2)# ip add 172.16.3.1/24

Switch(config)# access-list 10 deny 192.168.1.0 0.0.0.255
Switch(config)# access-list 10 permit any

Switch(config)# interface ge1/1
Switch(config-ge1/1)# access-group 10
Switch(config-ge1/1)# exit

Switch(config)# interface ge1/2
Switch(config-ge1/2)# access-group 10
```

20.7. ACL 설정 문제 해결

ACL 설정이 실패하는 경우, 다음과 같은 원인이 있을 수 있습니다.

1) Access Control List를 설정하기 전에 모든 IP가 정상적으로 통신되는지 먼저 확인한 후 ACL을 추가해야 합니다. 이 ACL은 출발지 주소가 192.168.1.0 대역인 IP 트래픽이 스위치를 통과하는 것을 차단합니다. 서브넷 wildcard 작성 방식에 주의해야 합니다. show access-list 명령어를 사용하여 ACL 목록을 확인하고, 출발지 주소와 목적지 주소를 반대로 입력하지 않았는지 확인해야 합니다. 또한 기본 ACL의 마지막에는 암시적인 deny any 문장이 존재합니다. 다른 트래픽을 통과시키려면 permit any 문장을 추가해야 하며, 그렇지 않으면 통과하지 못합니다.
2) 시스템에 Static IP-MAC Binding이 설정되어 있는 경우
3) 현재 인터페이스에서 DHCP Snooping 프로토콜이 활성화되어 있는 경우.
4) 시스템 CFP 리소스가 부족한 경우.

21. 기본 TCP/IP 설정

네트워크 관리 기능을 갖는 Layer 2 스위치는 다른 장비와의 통신을 위해 TCP/IP 프로토콜에 대한 기본 네

트워크 설정이 필요합니다.

이 장에서는 다음과 같은 내용을 포함합니다.

- VLAN 인터페이스 설정
- ARP 설정
- 정적 라우팅 설정
- IP 라우팅 설정 예제

21.1. VLAN 인터페이스 설정

스위치에서 각 Layer 3 인터페이스는 하나의 VLAN에 연결되며, 이러한 Layer 3 인터페이스를 VLAN 인터페이스라고 합니다. VLAN 인터페이스의 생성과 삭제는 수동으로 수행되며, 스위치에서는 최대 4094개의 VLAN을 생성할 수 있지만 실제로는 최대 32개의 서브넷만 구성할 수 있습니다. 서브넷 인터페이스는 사용자 요구에 따라 생성할 수 있으며, 수동으로 삭제하거나 해당 VLAN이 삭제될 때 함께 삭제됩니다.

각 VLAN 인터페이스는 이름을 가지며, 이름은 "VLAN" 문자열 뒤에 VLAN ID가 붙는 형태입니다. 예를 들어 VLAN 1의 인터페이스는 vlan1, VLAN 4094의 인터페이스는 vlan4094입니다.

VLAN 인터페이스는 포트와 마찬가지로 관리 상태와 링크 상태를 가집니다. 현재 스위치는 VLAN 인터페이스의 관리 상태 설정은 지원하지 않으며, 인터페이스가 생성되면 항상 UP 상태입니다. 링크 상태는 해당 VLAN에 속한 포트 상태에 따라 결정되며, VLAN 내에 하나라도 RUNNING 상태의 포트가 있으면 VLAN 인터페이스도 RUNNING 상태가 됩니다. 모든 포트가 RUNNING이 아니면 VLAN 인터페이스도 RUNNING 상태가 아닙니다.

VLAN 인터페이스에는 IP 주소를 설정할 수 있으며, 해당 인터페이스가 연결된 네트워크의 프리픽스(서브넷 마스크)를 함께 지정합니다. 현재 스위치는 하나의 VLAN 인터페이스에 하나의 IP 주소만 설정할 수 있습니다. IP 주소를 설정하기 전에 VLAN을 생성하고 해당 포트를 VLAN에 추가해야 합니다.

기본적으로 스위치에는 VLAN1 인터페이스가 존재하며, 기본 IP 주소는 10.10.10.1/24입니다. 사용자는 이 IP를 변경할 수 있습니다. VLAN1을 제외한 다른 VLAN 인터페이스에는 기본적으로 IP가 설정되어 있지 않습니다.

VLAN 인터페이스 IP 설정 명령어

Ip interface vlan <2-4094>

→ VLAN 인터페이스 생성 (Global Configuration Mode)

No Ip interface vlan <2-4094>

→ VLAN 인터페이스 삭제 (Global Configuration Mode)

ip address <ip-prefix>

→ VLAN 인터페이스에 IP 주소 설정 (Interface Configuration Mode)

→ 형식: A.B.C.D/M

→ 기존 IP가 있을 경우 먼저 삭제 후 설정해야 함

no ip address [ip-prefix]

→ VLAN 인터페이스 IP 삭제 (Interface Configuration Mode)

→ 지정 시 기존 설정과 동일해야 함

VLAN 인터페이스 확인 명령어

show interface [if-name]

→ VLAN 인터페이스 정보 확인 (IP, MAC, 상태 등)

→ if-name 생략 시 전체 인터페이스 표시

show running-config

→ 현재 설정 확인 (VLAN 인터페이스 포함)

설정 예제

VLAN3 인터페이스에 193.1.1.0/24 네트워크를 구성하고, IP 주소를 193.1.1.1로 설정 후 확인:

switch(config)# interface vlan3

switch(config-vlan3)# ip address 193.1.1.1/24

switch(config-vlan3)# end

switch# show interface vlan3

21.2. ARP 설정

ARP(Address Resolution Protocol)는 IP 주소를 해당하는 MAC 주소로 매핑해주는 프로토콜입니다. 동일 VLAN 내에서 이더넷 프레임을 전송할 때, 목적지는 48비트 MAC 주소를 기준으로 결정되며, 수신 장비는 목적지 MAC 주소를 기준으로 패킷 수신 여부를 판단합니다.

두 개의 인접한 네트워크에 있는 호스트 A와 B가 스위치를 통해 통신하는 경우를 가정하면, 호스트 A는 호스트 B에게 데이터를 전송하기 전에 먼저 ARP 요청 메시지를 스위치의 연결 인터페이스로 전송합니다. 이후 ARP 응답을 수신하면 해당 인터페이스로 데이터 패킷을 전송합니다. 스위치는 이 데이터를 수신한 후, 호스트 B를 찾기 위해 ARP 요청을 브로드캐스트하고, 호스트 B로부터 ARP 응답을 받으면 해당 데이터를 호스트 B에게 전달합니다.

스위치는 ARP 캐시(ARP 테이블)를 가지고 있으며, 여기에는 직접 연결된 네트워크의 IP 주소와 MAC 주소 매핑 정보가 저장됩니다. ARP 테이블의 각 엔트리는 일정한 유효 시간을 가지며, 기본값은 20분입니다. 해당 시간 동안 특정 IP 주소로부터 ARP 요청 또는 응답 메시지를 받지 못하면 해당 ARP 엔트리는 삭제됩니다.

이 절에서는 다음 내용을 포함합니다.

- Static ARP 설정
- ARP 바인딩 설정
- ARP 정보 조회

21.2.1. 정적 ARP 설정

ARP 테이블에는 두 가지 유형의 ARP 엔트리가 존재합니다. 하나는 정적 ARP이고, 다른 하나는 동적 ARP입니다.

정적 ARP는 사용자가 명령어를 통해 직접 설정하는 ARP 테이블 엔트리입니다. 시스템에서 자동으로 갱신되거나 삭제되지 않으며, 사용자가 직접 관리해야 합니다.

동적 ARP는 시스템이 ARP 요청 또는 응답 패킷을 기반으로 자동으로 학습하는 엔트리입니다. 시스템이 자동으로 생성, 삭제, 갱신을 수행하며, 사용자 개입 없이 실시간으로 유지됩니다. 단, 사용자가 수동으로 동적 ARP 엔트리를 삭제할 수는 있습니다.

스위치는 기본적으로 정적 ARP 엔트리가 설정되어 있지 않습니다. 또한 VLAN 인터페이스가 삭제되거나 해당 인터페이스의 서브넷 IP가 변경되면, 기존 서브넷에 속한 정적 및 동적 ARP 엔트리는 모두 삭제됩니다.

정적 ARP 설정 명령어

arp <ip-address> <mac-address>

→ 정적 ARP 엔트리 설정

→ 첫 번째 파라미터: IP 주소 (해당 서브넷에 속해야 함)

→ 두 번째 파라미터: MAC 주소 (유니캐스트 MAC이어야 함)

→ MAC 주소 형식: HHHH.HHHH.HHHH (예: 5491.AFB1.7825)

no arp <ip-address>

→ 해당 IP에 대한 ARP 엔트리 삭제

21.2.2. ARP 정보 확인

ARP 정보를 확인하는 명령어는 다음 표와 같습니다.

Command	Description	CLI Mode
show arp	ARP 테이블의 엔트리 정보를 확인합니다. 모든 ARP 테이블 엔트리를 포함합니다.	Normal mode, Privileged mode
show running-config	현재 시스템 설정을 확인합니다. ARP 설정 내용을 확인할 수 있습니다.	Privileged Mode

21.3. 정적 라우팅 설정

정적 라우팅은 사용자가 직접 정의한 경로로, 패킷이 출발지에서 목적지까지 특정 경로를 따라 전달되도록 합니다. 라우팅이 불가능한 패킷은 기본 경로(Default Route)를 설정하여 게이트웨이로 전달할 수 있습니다.

정적 라우팅은 관리자가 수동으로 설정하며, 네트워크 구조가 단순한 환경에 적합합니다. 라우팅 업데이트가 없기 때문에 네트워크 대역폭을 추가로 소모하지 않는다는 장점이 있습니다.

기본 라우트(Default Route) 또한 정적 라우트의 한 형태입니다. 이는 일치하는 경로가 없을 때만 사용되는 경로로, 라우팅 테이블에서는 0.0.0.0/0 형태로 표시됩니다. 목적지에 대한 경로가 없고 기본 라우트도 없는 경우, 패킷은 폐기되며 ICMP Unreachable 메시지가 반환됩니다.

스위치에는 동일 목적지에 대해 여러 개의 정적 라우트를 설정할 수 있지만, 실제 포워딩에는 하나의 경로만 사용됩니다. 기본적으로 스위치에는 정적 라우트가 설정되어 있지 않습니다.

Command	Description	CLI Mode
ip route <ip-prefix> <nexthop-address>	정적 라우트 설정. <ip-prefix>는 네트워크 주소와 프리픽스 길이, <nexthop-address>는 다음 홉 IP	Global Configuration Mode
ip route <ip-address> <mask-address> <nexthop-address>	위 명령과 동일 기능. 네트워크 주소 + 서브넷 마스크 + 다음 홉 IP로 설정	Global Configuration Mode
no ip route <ip-prefix> [nexthop-	정적 라우트 삭제. 다음 홉 미지정 시 해당 네트워	Global

Command	Description	CLI Mode
address]	크 전체 삭제, 지정 시 해당 경로만 삭제	Configuration Mode
no ip route <ip-address> <mask-address> [nexthop-address]	위 삭제 명령과 동일 기능	Global Configuration Mode

라우팅 정보 확인 명령어

Command	Description	CLI Mode
show ip route [<ip-address> | <ip-prefix>]	활성화된 라우트 확인 (전체/특정/대역별 조회 가능)	Normal mode, Privileged mode
show ip route database	전체 라우트 정보 확인 (활성 + 비활성 포함)	Normal mode, Privileged mode
show running-config	현재 설정 확인 (정적 라우트 포함)	Privileged Mode

설정 예제

목적지 네트워크 200.1.1.0/24, 다음 홉 10.1.1.2 설정:

Switch(config)# ip route 200.1.1.0 255.255.255.0 10.1.1.2

또는

Switch(config)# ip route 200.1.1.0/24 10.1.1.2

정적 라우트 삭제:

Switch(config)# no ip route 200.1.1.0/24

또는

Switch(config)# no ip route 200.1.1.0/24 10.1.1.2

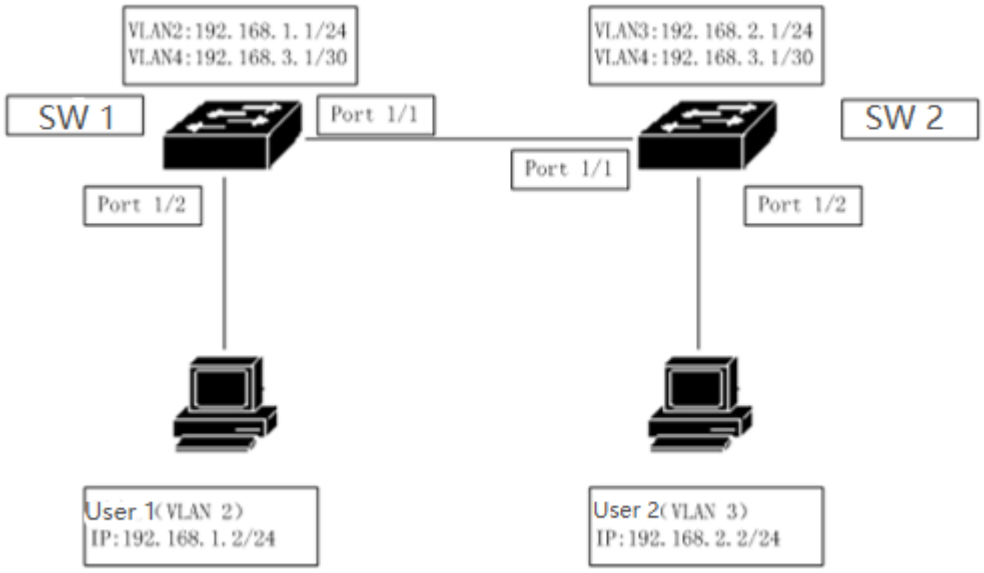
또는

Switch(config)# no ip route 200.1.1.0 255.255.255.0

또는

Switch(config)# no ip route 200.1.1.0 255.255.255.0 10.1.1.2

21.4. TCP/IP 기본 설정 예제



그림에서 Switch 1은 Layer 2 스위치이고, Switch 2는 Layer 3 스위치입니다.

21.4.1. 3계층 인터페이스 설정

스위치 1에서 VLAN2에 대한 Layer 3 인터페이스를 구성하고, IP 주소를 192.168.1.1/24로 설정합니다.

설정은 다음과 같습니다:

Switch# config t

Switch(config)# vlan database

Switch(config-vlan)# vlan 2

Switch(config-vlan)# exit

Switch(config)# interface ge1/2

Switch(config-ge1/2)# switch access vlan 2

Switch(config)# ip interface vlan 2

Switch(config)# interface vlan2

Switch(config-vlan2)# ip add 192.168.1.1/24

21.4.2. 정적 라우트 설정

User 2가 Switch 1에 접근하기 위해서는 Switch 2의 라우팅 기능을 통해야 합니다.

Switch 1 설정:

Switch# config t

Switch(config)# ip route 192.168.2.0 255.255.255.0 192.168.3.2

Switch 2 설정:

Switch# config t

Switch(config)# ip route 192.168.1.0/24 192.168.3.1

21.4.3. ARP 설정

VLAN 2에서 User1만 접근할 수 있도록 User1에 대한 정적 ARP를 설정합니다.

User1의 MAC 주소는 00:00:00:00:00:01이라고 가정합니다.

Switch 1 설정:

Switch# config t

Switch(config)# arp 192.168.1.2 0000.0000.0001

22. SNMP 설정

스위치는 원격 관리 기능을 위해 SNMP(Simple Network Management Protocol)를 제공합니다.

이 장에서는 SNMP 설정 방법을 설명하며, 다음과 같은 내용을 포함합니다.

- SNMP 소개

- SNMP 설정
- SNMP 설정 예제

22.1. SNMP 소개

SNMP(Simple Network Management Protocol)는 가장 널리 사용되는 네트워크 관리 프로토콜로, 네트워크 장비를 원격에서 관리하기 위한 표준 방식입니다. SNMP는 다음과 같은 다섯 가지 관리 기능을 제공합니다.

- 장애 관리 (Fault Management)
- 금 관리 (Accounting Management)
- 구성 관리 (Configuration Management)
- 성능 관리 (Performance Management)
- 보안 관리 (Security Management)

또한 네트워크 관리 애플리케이션과 네트워크 관리 에이전트 간 통신을 위한 정보 형식을 제공합니다.

SNMP 구성 요소

SNMP는 다음 네 가지 요소로 구성됩니다.

- 관리 스테이션 (Management Station)
- 관리 에이전트 (Management Agent)
- 관리 정보 베이스 (MIB: Management Information Base)
- 네트워크 관리 프로토콜

스위치에서는 관리 에이전트가 서버 역할을 하며, 관리 스테이션이 스위치에 접근할 수 있도록 합니다. 관리 정보는 MIB 형태로 구성되어 저장됩니다.

SNMP 동작 방식

SNMP는 다음 세 가지 기본 동작을 제공합니다.

- GET: 관리 스테이션이 에이전트로부터 특정 객체의 값을 조회
- SET: 관리 스테이션이 에이전트의 객체 값을 설정
- TRAP: 에이전트가 이벤트 발생 시 관리 스테이션으로 알림 전송

TRAP 메시지는 스위치에서 이벤트가 발생했을 때 자동으로 전송되며, 다음과 같은 내용을 포함할 수 있습니다.

- cold start / warm start
- 포트 link up / link down
- 인증 실패
- STP 상태 변화 등

SNMP 버전

현재 SNMP는 세 가지 버전을 지원합니다.

- SNMPv1
- SNMPv2
- SNMPv3

버전이 올라갈수록 기능과 보안이 강화됩니다. 스위치는 세 가지 버전을 모두 지원하며, TRAP 메시지도 이 중 하나의 버전으로 전송될 수 있습니다.

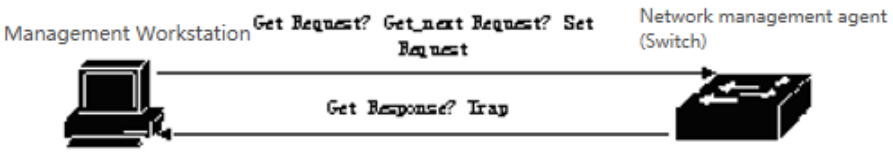
지원 MIB

스위치는 RFC 표준 MIB, BRIDGE MIB, 그리고 제조사 고유 MIB를 지원하며, SNMP를 통해 전체 관리가 가능합니다. 대표적으로 다음과 같은 MIB를 지원합니다.

- RFC 1213
- RFC 1493
- RFC 1724
- RFC 1850
- RFC 1907
- RFC 2233
- RFC 2571 ~ 2575
- RFC 2674 등

SNMP 통신 구조

관리 스테이션은 Get Request, GetNext Request, GetBulk Request, Set Request 등의 SNMP 메시지를 통해 스위치의 MIB 값을 조회하거나 설정할 수 있습니다.



스위치의 관리 에이전트는 이에 대해 Get Response 메시지를 반환합니다. 또한 스위치에서 특정 이벤트가 발생하면, 관리 에이전트가 관리 스테이션으로 TRAP 메시지를 능동적으로 전송합니다.

22.2. SNMP 설정

SNMP 설정에는 스위치의 커뮤니티 설정, TRAP 수신 대상 설정, 그리고 SNMP 시스템 정보 설정이 포함됩니다. 기본적으로 스위치에는 public이라는 읽기 전용(RO) 커뮤니티가 설정되어 있으며, 최대 8개의 커뮤니티를 구성할 수 있습니다. TRAP 수신 대상은 기본적으로 설정되어 있지 않습니다.

Command	**Description**	**CLI Mode**
snmp community <community-name> {ro | rw}	네트워크 관리 접근을 위한 커뮤니티 이름 설정. 인터랙티브 명령으로, 커뮤니티 이름과 읽기/쓰기 권한을 설정	Global Configuration Mode
no snmp community <community-name>	지정된 SNMP 커뮤니티 삭제	Global Configuration Mode
snmp trap <notify-name> host <ipaddress> version {1 | 2c | 3}	SNMP TRAP 전송 대상 설정 또는 수정. notify-name은 고유값이며, host는 TRAP 수신 IP, version은 SNMP 버전 지정. 기본 포트는 162	Global Configuration Mode
no snmp trap <notify-name>	지정된 SNMP TRAP 설정 삭제	Global Configuration Mode
snmp system information <contact | location | name> <information-string>	시스템 정보 설정 (관리자 연락처, 위치, 장비 이름 등)	Global Configuration Mode
no snmp system information <contact | location | name>	시스템 정보 삭제	Global Configuration Mode
show snmp community	현재 설정된 커뮤니티 및 권한 정보 확인	Normal / Privileged Mode
show snmp trap	TRAP 대상 IP 및 SNMP 버전 정보 확인	Normal / Privileged Mode
show snmp system information	SNMP 시스템 정보 확인	Normal / Privileged Mode

22.3. SNMP 설정 예제

22.3.1. 설정

읽기/쓰기 권한을 가진 private 커뮤니티를 설정합니다.

SNMP TRAP 이름을 test로 설정하고, 목적지 IP를 10.10.10.10, SNMP 버전은 1로 설정합니다.

시스템 정보로 연락처, 위치, 이름을 설정합니다.

스위치 설정은 다음과 같습니다:

```
Switch# config t
Switch(config)# snmp community private rw
Switch(config)# snmp trap test host 10.10.10.10 version 1
Switch(config)# snmp system information contact E-mail:networks@abc.com
Switch(config)# snmp system information location Shenzhen
Switch(config)# snmp system information name switch
```

23. RMON 설정

이 장에서는 RMON(Remote Monitoring) 설정과 관련된 내용을 설명하며, 다음과 같은 항목을 포함합니다.

- RMON 소개
- RMON 설정
- RMON 설정 예제

23.1. RMON 소개

RMON(Remote Monitoring)은 표준 네트워크 모니터링 규격으로, 네트워크의 특정 구간 또는 전체 네트워크의 트래픽을 모니터링하는 데 사용됩니다. 현재 가장 널리 사용되는 네트워크 관리 표준 중 하나입니다. RMON은 SNMP MIB의 확장 개념으로, MIB II 표준을 확장한 중요한 기능이며, SNMP가 원격 장비를 보다 효과적이고 능동적으로 모니터링할 수 있도록 합니다.

RMON 모니터링 시스템은 두 가지 구성 요소로 이루어집니다.

- Probe(에이전트 또는 모니터)
- 관리 스테이션

RMON 에이전트는 네트워크 정보를 RMON MIB에 저장하며, 이 에이전트는 라우터나 스위치와 같은 네트워크 장비에 직접 내장되어 있습니다. 관리 스테이션은 SNMP를 통해 RMON 데이터를 수집합니다.

장비는 RMON에서 가장 일반적으로 사용되는 다음 네 가지 그룹을 지원합니다.

1) Statistics 그룹
   각 인터페이스에 대한 통계 정보를 제공합니다. 대부분의 객체는 카운터 형태이며, 인터페이스에서 수집된 정보를 기록합니다.
2) History 그룹
   지정된 인터페이스의 데이터를 일정한 시간 간격으로 샘플링하여 저장합니다.
3) Alarm 그룹
   모든 인터페이스의 특정 데이터를 일정 주기로 샘플링하고, 설정된 임계값과 비교하여 조건을 만족하면 이벤트를 발생시킵니다.
4) Event 그룹
   이벤트를 정의하며, 로그 기록 또는 TRAP 전송을 선택할 수 있습니다.

23.2. RMON 설정

RMON 명령어는 네 가지 그룹 설정과 설정 조회, 데이터 조회로 구성됩니다.

Command	**Description**	**CLI Mode**
rmon statistics <1-100> (owner WORD|)	지정된 번호로 통계(Statistics) 그룹을 포트에 설정. 인터랙티브 명령으로, 사용자 입력에 따라 시퀀스 번호와 owner를 설정 (owner는 선택사항). 시퀀스 번호 범위: 1~100	Port Configuration Mode
no rmon statistics <1-100>	지정된 번호의 통계 그룹 설정 삭제	Port Configuration Mode
rmon history <1-100> buckets <1-100> interval <1-3600> (owner WORD|)	지정된 번호로 History 그룹 설정. 인터랙티브 명령으로 시퀀스 번호, 저장 개수, 샘플링 주기, owner 입력. 시퀀스 번호: 1~100, buckets:	Port Configuration Mode

Command	Description	CLI Mode
	1~100, interval(초): 1~3600	
no rmon history <1-100>	지정된 번호의 History 그룹 설정 삭제	Port Configuration Mode
rmon alarm <1-60> WORD <1-3600> (absolute|delta) rising-threshold <1-2147483647> <1-60> falling-threshold <1-2147483647> <1-60> (owner WORD|)	지정된 번호로 Alarm 그룹 설정. 인터랙티브 명령으로 시퀀스 번호, 모니터링 대상(OID), 샘플링 주기, 비교 방식, 상/하한 임계값 및 이벤트 번호, owner 입력. 시퀀스 번호: 1~60, interval(초): 1~3600, threshold 범위: 1~2147483647	Global Configuration Mode
no rmon alarm <1-60>	지정된 번호의 Alarm 그룹 설정 삭제	Global Configuration Mode
rmon event <1-60> (log|log-trap WORD|none|trap WORD) (description WORD|) (owner WORD|)	지정된 번호로 Event 그룹 설정. 인터랙티브 명령으로 시퀀스 번호, 이벤트 타입, 커뮤니티명, 설명, owner 입력. 시퀀스 번호: 1~60. 이벤트 타입: log, log-trap, none, trap	Global Configuration Mode
no rmon event <1-60>	지정된 번호의 Event 그룹 설정 삭제	Global Configuration Mode
show rmon (statistics|history-control|alarm|event) config	RMON 설정 정보 확인. 인터랙티브 방식으로 조회 대상 선택	Global Configuration Mode
show rmon statistics-data interface IFNAME	특정 인터페이스의 Statistics 데이터 확인	Global Configuration Mode
show rmon history-data interface IFNAME	특정 인터페이스의 History 데이터 확인	Global Configuration Mode

23.3. RMON 설정 예제

포트 ge1/1에서 통계(Statistics) 그룹 설정을 활성화하고, 시퀀스 번호는 10, owner는 tereco로 설정합니다.

포트 ge1/8에서 History 그룹 데이터 수집을 활성화하며, 시퀀스 번호는 2, 최대 80개의 데이터를 저장하고, 샘플링 간격은 1분(60초)으로 설정합니다. owner는 설정하지 않습니다.

시퀀스 번호 1의 이벤트는 로그(log)로 기록하며 owner는 없습니다.

시퀀스 번호 3의 이벤트는 TRAP을 전송하도록 설정하며, 커뮤니티 이름은 public이고 owner는 없습니다.

시퀀스 번호 5의 Alarm 그룹을 설정하여 각 포트의 수신 바이트 수를 모니터링합니다. 30초 단위로 샘플링하며, 바이트 수가 1000을 초과하면 TRAP(이벤트 3)을 전송하고, 10 미만이면 로그(이벤트 1)를 기록합니다. owner는 설정하지 않습니다.

스위치 설정은 다음과 같습니다:

Switch# configure terminal

Switch(config)# interface ge1/1

Switch(config-ge1/1)# rmon statistics 10 owner tereco

Switch(config-ge1/1)# exit

Switch(config)# interface ge1/8

Switch(config-ge1/8)# rmon history 2 buckets 80 interval 60

Switch(config-ge1/8)# exit

Switch(config)# rmon event 1 log

Switch(config)# rmon event 3 trap public

Switch(config)# rmon alarm 5 1.3.6.1.2.1.2.2.1.10 30 delta rising-threshold 1000 3 falling-threshold 10 1

24. 클러스터 설정

스위치는 클러스터 관리 기능을 제공하며, 이를 통해 하나의 장비에서 여러 네트워크 장비를 그룹으로 관리할 수 있습니다.

이 장에서는 클러스터 관리 설정 방법을 설명하며, 다음과 같은 내용을 포함합니다.

- 클러스터 관리 소개
- 관리 장비 설정
- 멤버 장비 설정
- 클러스터 관리 조회 및 유지보수
- 클러스터 관리 설정 예제

24.1. 클러스터 관리 소개

24.1.1. 클러스터 정의

클러스터는 하나의 장비처럼 관리할 수 있는 네트워크 장비들의 집합입니다.

클러스터 관리의 목적은 여러 곳에 분산되어 있는 다수의 네트워크 장비를 중앙에서 관리하는 문제를 해결하는 것입니다.

클러스터의 장점은 공인 IP 주소를 절약하고, 설정 및 관리 작업을 단순화할 수 있다는 점입니다. 네트워크 관리자는 클러스터 내 하나의 스위치에만 공인 IP 주소를 설정하면, 클러스터에 포함된 다른 스위치들도 관리하고 유지보수할 수 있습니다.

공인 IP 주소를 설정하고 관리 기능을 수행하는 스위치를 Command Switch라고 하며, 관리 대상이 되는 다른 스위치들을 Member Switch라고 합니다. Command Switch와 Member Switch가 함께 하나의 클러스터를 구성합니다.

클러스터는 다음 세 가지 프로토콜을 통해 클러스터 내 스위치를 설정하고 관리합니다.

- NDP(Neighbor Discovery Protocol)
- NTDP(Neighbor Topology Discovery Protocol)
- Cluster(Cluster Management Protocol)

클러스터의 동작 과정에는 토폴로지 수집과 클러스터의 생성 및 유지 관리가 포함됩니다. 토폴로지 수집 과정과 클러스터 유지 과정은 비교적 독립적으로 동작하며, 토폴로지 수집 과정은 클러스터가 생성되기 전에 시작됩니다.

동작 원리는 다음과 같습니다.

- 모든 장비는 NDP를 통해 인접 장비의 정보를 획득합니다. 여기에는 인접 장비의 소프트웨어 버전, 호스트 이름, MAC 주소, 포트 이름 등의 정보가 포함됩니다.
- 관리 장비는 NTDP를 통해 사용자가 지정한 hop count 범위 내의 장비 정보와 각 장비 간 연결 정보를 수집하고, 수집된 토폴로지 정보에서 클러스터 후보 장비를 결정합니다.
- 관리 장비는 NTDP를 통해 수집한 후보 장비 정보를 기반으로, 후보 장비를 클러스터에 추가하거나 기존 멤버 장비를 클러스터에서 제거하는 작업을 수행합니다.

클러스터 메시지는 모두 Layer 2 Ethernet 메시지로 구성됩니다. 구체적인 메시지 형식과 동작 방식은 IEEE 및 IETF 표준 기반의 Ethernet 관리 및 네트워크 관리 프로토콜 규격을 참고합니다.

24.1.2. Cluster Role

클러스터 내 각 장비의 위치와 기능에 따라 서로 다른 역할이 형성됩니다. 사용자는 설정을 통해 역할을 지정할 수 있습니다. 전체 역할은 다음과 같습니다.

1) Command Switch
   클러스터에서 전체 클러스터를 설정하고 관리할 수 있는 유일한 스위치이며, 클러스터 내에서 공인 IP 주소를 가진 유일한 스위치입니다.

- Command Switch는 클러스터를 생성합니다.
- Command Switch는 NDP(Neighbor Discovery Protocol)와 NTDP(Neighbor Topology Discovery Protocol) 정보를 수집하여 Candidate Switch를 발견하고 결정합니다.
- Command Switch는 클러스터 유지 관리를 제어하며, Candidate Switch를 클러스터에 추가하거나 Member Switch를 클러스터에서 삭제할 수 있습니다.
- 클러스터가 생성된 후, Command Switch는 클러스터에 대한 관리 채널을 제공합니다.

2) Member Switch
클러스터 내에서 관리 대상이 되는 스위치입니다.
Member Switch는 클러스터에 가입하기 전에는 Candidate 상태입니다.
Member Switch에는 공인 IP 주소가 제공되지 않습니다.
Member Switch의 관리는 Command Switch를 통해 대리 수행됩니다.

3) Candidate Switch
클러스터에 가입할 수 있는 기능은 있지만, 아직 어떤 클러스터에도 가입하지 않은 스위치입니다.
스위치가 Member가 되기 위해서는 먼저 Candidate 상태여야 합니다.

4) Independent Switch
클러스터 기능을 지원하지 않는 스위치입니다.

각 역할은 일정한 규칙에 따라 전환될 수 있습니다.

- Candidate 장비에서 클러스터를 생성할 때, 사용자는 현재 Candidate 장비를 클러스터 관리 장비로 지정합니다. 각 클러스터에는 반드시 하나의 관리 장비만 지정되어야 합니다. 관리 장비가 지정되면, 해당 관리 장비는 관련 정보를 수집하여 Candidate 장비를 검색하고 결정합니다. 사용자는 해당 설정을 통해 Candidate 장비를 클러스터에 추가할 수 있습니다.
- Candidate 장비가 클러스터에 가입하면 Member 장비가 됩니다.
- 클러스터 내 Member 장비가 삭제되면 다시 Candidate 장비로 복원됩니다.
- 관리 장비는 클러스터가 삭제될 때만 Candidate 장비로 복원될 수 있습니다.

24.1.3. NDP 소개

NDP(Neighbor Discovery Protocol)는 직접 연결된 이웃 장비의 정보를 수집하기 위해 사용되며, 연결 포트, 장비 이름, 소프트웨어 버전 등의 정보를 포함합니다. 동작 원리는 다음과 같습니다.

- NDP를 실행하는 장비는 주기적으로 이웃 장비에게 NDP 메시지를 전송합니다. 이 메시지에는 현재 장비의 NDP 정보(장비 이름, 소프트웨어 버전, 연결 포트 등)와 수신 장비에서의 해당 정보 유지 시간(aging time)이 포함됩니다. 또한 이웃 장비로부터 수신한 NDP 메시지는 처리만 하고 다른 곳으로 전달하지는 않습니다.
- NDP를 실행하는 장비는 이웃 장비 정보를 저장하고 관리하기 위해 NDP 이웃 정보 테이블을 유지합니다. 각 이웃 장비마다 하나의 엔트리가 생성됩니다.
- 새로운 이웃 장비가 발견되면(처음으로 NDP 메시지를 수신한 경우) 새로운 엔트리가 추가됩니다.
- 이웃 장비로부터 받은 정보가 기존 정보와 다르면 해당 엔트리가 업데이트됩니다.
- 정보가 동일하면 aging 시간만 갱신됩니다.

- 일정 시간 동안 NDP 메시지를 수신하지 못하면 해당 이웃 엔트리는 자동으로 삭제됩니다.

24.1.4. NTDP 소개

NTDP는 네트워크 내 각 장비의 정보와 장비 간 연결 정보를 수집하는 데 사용됩니다. NTDP는 관리 장비에게 클러스터에 추가할 수 있는 장비 정보를 제공하며, 지정된 hop count 범위 내의 장비 토폴로지 정보를 수집합니다.

NDP는 NTDP에 인접 장비 테이블 정보를 제공합니다. NTDP는 이 인접 정보를 기준으로 NTDP 토폴로지 수집 요청을 전송하고 전달하며, 일정 네트워크 범위 내 각 장비의 NDP 정보와 각 장비와 모든 이웃 장비 간의 연결 정보를 수집합니다. 정보 수집이 완료되면 관리 장비 또는 네트워크 관리자는 필요에 따라 해당 정보를 사용하여 필요한 기능을 수행할 수 있습니다.

Member 장비의 NDP가 이웃 장비의 변경을 감지하면, handshake 메시지를 통해 관리 장비에 이웃 변경 사항을 알립니다. 관리 장비는 NTDP를 시작하여 지정된 토폴로지를 수집할 수 있으며, 이를 통해 NTDP는 네트워크 토폴로지 변경을 즉시 반영할 수 있습니다.

관리 장비는 네트워크 내 토폴로지를 주기적으로 수집할 수 있으며, 사용자는 수동 설정 명령을 통해 토폴로지 수집을 한 번 실행할 수도 있습니다.

관리 장비가 토폴로지 정보를 수집하는 과정은 다음과 같습니다.

- 관리 장비는 NTDP 기능이 활성화된 포트에서 주기적으로 NTDP 토폴로지 수집 요청 메시지를 전송합니다.
- 요청 메시지를 수신한 장비는 즉시 관리 장비로 토폴로지 응답 메시지를 전송하고, NTDP 기능이 활성화된 포트에서 요청 메시지를 복사하여 인접 장비로 전송합니다. 토폴로지 응답 메시지에는 해당 장비의 기본 정보와 모든 인접 장비의 NDP 정보가 포함됩니다.
- 인접 장비는 요청 메시지를 수신하면 동일한 동작을 수행하며, 토폴로지 수집 요청 메시지가 지정된 hop 범위 내 모든 장비로 전파될 때까지 반복됩니다.
- 토폴로지 수집 요청 메시지가 네트워크에 전파될 때, 많은 네트워크 장비가 동시에 요청을 수신하고 토폴로지 응답 메시지를 전송할 수 있습니다. 네트워크 혼잡과 관리 장비의 작업 부하를 방지하기 위해 다음과 같은 방법으로 토폴로지 수집 요청 메시지의 전파 속도를 제어할 수 있습니다.
- 장비는 토폴로지 수집 요청을 수신한 후 즉시 전달하지 않고, 일정 시간 지연한 뒤 NTDP 기능이 활성화된 포트에서 토폴로지 수집 요청 메시지를 전달합니다.
- 동일 장비에서는 첫 번째 포트를 제외하고, NTDP 기능이 활성화된 각 포트가 이전 포트에서 토폴로지 수집 요청 메시지를 전송한 후 일정 시간 지연한 뒤 토폴로지 수집 요청 메시지를 전달합니다.

24.1.5. 클러스터 관리 및 유지보수

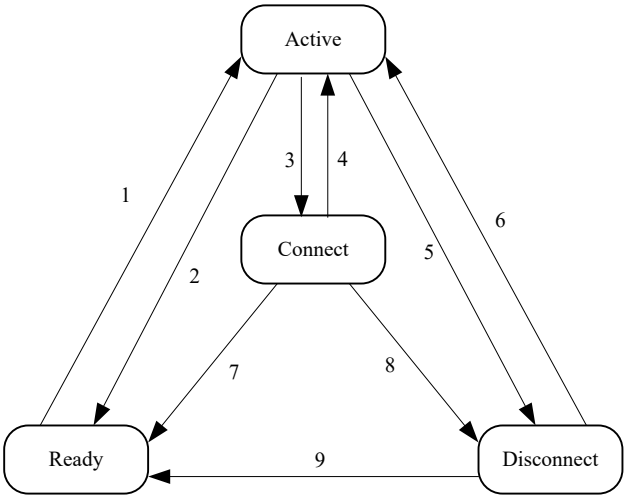
1) Candidate 장비의 클러스터 가입

클러스터를 생성하기 전에, 사용자는 먼저 관리 장비를 지정해야 합니다. 관리 장비는 NDP와 NTDP 프로토콜을 통해 Candidate 장비를 검색하고 결정한 후, 해당 Candidate 장비를 클러스터에 자동으로 추가합니다. 또는 수동 설정을 통해 Candidate 장비를 클러스터에 추가할 수도 있습니다.

클러스터를 생성하기 전에, 사용자는 먼저 관리 장비를 지정해야 합니다. 관리 장비는 NDP와 NTDP 프로토콜을 통해 Candidate 장비를 검색하고 결정한 후, 해당 Candidate 장비를 클러스터에 자동으로 추가합니다. 또는 수동 설정을 통해 Candidate 장비를 클러스터에 추가할 수도 있습니다.

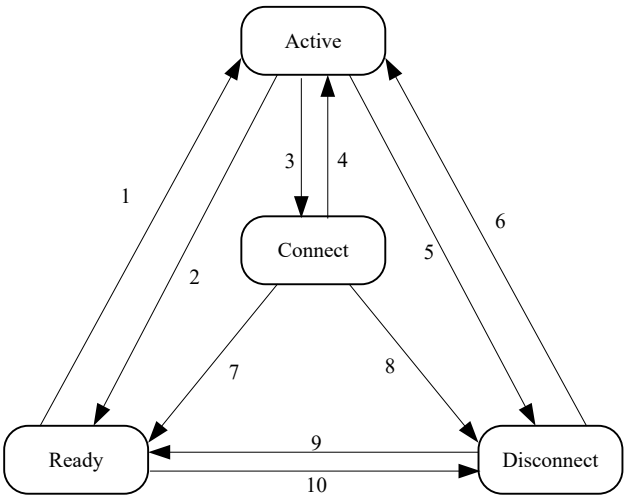
2) 클러스터 내부 통신

클러스터 내부에서 관리 장비는 Member 장비와 handshake 메시지를 통해 실시간으로 통신하며, 두 장비 간 연결 상태를 유지합니다. 관리 장비와 Member 장비 간 연결 상태는 아래 그림과 같습니다.



Command Switch 상태 전이도

1 Member 추가
2 Member 삭제
3 handshake 신호를 3회 연속 수신하지 못함
4 handshake 신호 수신
5 복구 요청 수신
6 복구 중단. 재등록 통과
7 Member 삭제
8 지정된 시간을 초과하여 상태 유지
9 Member 삭제



Member Switch 상태 전이도

1 클러스터 가입
2 클러스터 탈퇴
3 handshake 메시지를 3회 연속 수신하지 못함
4 handshake 메시지 수신
5 가입 요청 수신
6 복구 중단. 재등록 통과
7 클러스터 탈퇴
8 지정된 시간을 초과하여 상태 유지하거나 가입 요청 메시지 수신
9 클러스터 탈퇴
10 설정 복구

Command Switch는 장비의 기본 정보를 수집하고, 해당 장비를 Candidate Switch로 식별합니다. 이 장비는 초기 상태에서 Ready 상태입니다.

어떤 상태에 있든 Member를 삭제하는 작업을 수행하면, 해당 Member Switch는 다시 Ready 상태로 전환되고 Candidate Switch로 식별됩니다.

- 클러스터가 정상적으로 생성되고 Candidate 장비가 클러스터에 가입하여 Member 장비가 되면, 관리 장비는 Member 장비의 상태 정보를 로컬에 저장하고 해당 Member 상태를 Active로 표시합니다. Member 장비 역시 자신의 상태 정보를 로컬에 저장하고 자신의 상태를 Active로 표시합니다.
- 관리 장비와 Member 장비는 일정 주기로 서로 handshake 메시지를 전송합니다. 관리 장비는 Member 장비로부터 handshake 메시지를 수신하면 별도의 응답 없이 Member 장비를 Active 상태로 유지합니다. Member 장비도 마찬가지로 응답하지 않고 자신의 상태를 Active로 유지합니다.
- 관리 장비가 Member 장비로 handshake 메시지를 전송한 후, handshake 메시지 전송 간격의 3배 시간 이내에 Member 장비가 보낸 handshake 메시지를 수신하지 못하면, 로컬에 저장된

Member 장비의 상태를 Active에서 Connect로 전환합니다. 마찬가지로 Member 장비도 관리 장비로 handshake 메시지를 전송한 후, handshake 메시지 전송 간격의 3배 시간 이내에 관리 장비가 보낸 handshake 메시지를 수신하지 못하면 자신의 상태를 Active에서 Connect로 전환합니다.

- 관리 장비가 Connect 상태의 Member 장비로부터 유효 유지 시간 내에 handshake 메시지 또는 관리 메시지를 수신하면, 해당 Member 장비의 상태를 다시 Active로 전환합니다. 그렇지 않으면 Member 장비의 상태를 Disconnect로 전환하며, 이때 관리 장비는 해당 Member가 연결 해제된 것으로 판단합니다. Connect 상태의 Member 장비도 유효 유지 시간 내에 관리 장비가 보낸 handshake 메시지 또는 관리 메시지를 수신하면 자신의 상태를 Active로 전환하고, 그렇지 않으면 Disconnect로 전환합니다.
- 관리 장비와 Member 장비 간 중단되었던 통신이 복구되면, Disconnect 상태의 Member 장비는 클러스터에 다시 가입합니다. 가입이 성공하면 관리 장비에 저장된 Member 장비의 상태와 Member 장비의 로컬 상태는 모두 Active로 복구됩니다.

토폴로지 변경이 발견되면, Member 장비는 해당 변경 정보를 handshake 메시지를 통해 관리 장비로 전달합니다.

24.1.6. Management VLAN

Management VLAN은 클러스터 관리 범위를 제한합니다. Management VLAN을 설정하면 다음 기능을 구현할 수 있습니다.

- 클러스터 관리 메시지(NDP, NTDP, handshake 메시지 포함)를 Management VLAN 내부로 제한하고, 다른 메시지와 분리하여 보안을 향상시킵니다.
- 관리 장비와 Member 장비 간 내부 통신은 Management VLAN을 통해 이루어집니다.

클러스터 관리를 위해서는 관리 장비와 Member/Candidate 장비 사이에 연결된 포트가 Management VLAN을 통과시킬 수 있어야 합니다. 여기에는 Cascade 포트도 포함됩니다. Candidate 장비가 다른 Candidate 장비를 통해 관리 장비에 연결되는 경우, Candidate 장비 간 연결 포트를 Cascade 포트라고 합니다.

따라서 다음 사항을 만족해야 합니다.

- 포트에서 Management VLAN 통과가 허용되지 않으면, 해당 포트에 연결된 장비는 클러스터에 가입할 수 없습니다. 따라서 클러스터를 구성하기 전에 Candidate 장비와 관리 장비를 연결하는 포트 및 Cascade 포트에서 Management VLAN 통과가 허용되어 있는지 확인해야 합니다.
- 관리 장비와 Member/Candidate 장비가 연결된 포트의 기본 VLAN ID, 그리고 Cascade 포트의 기본 VLAN ID가 Management VLAN인 경우에만 Management VLAN 메시지가 Untagged로 통과할 수 있습니다. 그렇지 않은 경우 Management VLAN 메시지는 반드시 Tagged 형태로 통과해야 합니다.

VLAN에 대한 자세한 내용은 VLAN 설정 항목을 참고하십시오.

24.2. 클러스터 설정 소개

클러스터를 설정하기 전에, 사용자는 클러스터 내 각 장비의 역할과 기능을 정의하고, 관련 기능을 설정하며, 클러스터 내 장비 간 통신 방식을 계획해야 합니다.

설정 작업

관리 장비 설정 (Configuration management device)

- 시스템 및 포트의 NDP 기능 활성화
- NDP 파라미터 설정
- 시스템 및 포트의 NTDP 기능 활성화
- NTDP 파라미터 설정
- NTDP 정보 수동 수집 설정
- 클러스터 기능 활성화
- 클러스터 생성
- 클러스터 내부 멤버 간 통신 설정
- 클러스터 멤버 관리 설정

멤버 장비 설정 (Configure Member Device)

- 시스템 및 포트의 NDP 기능 활성화
- 시스템 및 포트의 NTDP 기능 활성화
- NTDP 정보 수동 수집 설정
- 클러스터 기능 활성화

클러스터 멤버 간 상호 접근 설정 (Configure cluster members to access each other)

주의사항

클러스터가 생성된 이후, 관리 장비 또는 멤버 장비에서 NDP 또는 NTDP 기능을 비활성화하더라도 클러스터 자체는 해제되지 않습니다. 다만, 이미 구성된 클러스터의 정상적인 동작에는 영향을 미칠 수 있습니다.

24.3. 관리 장비 설정

24.3.1. 시스템 및 포트의 NDP 기능 활성화

Command	Description	CLI Mode
ndp global enable	전역 NDP 기능을 활성화합니다. 기본값은 전역 비활성화 상태입니다.	Configuration Mode
ndp enable	포트의 NDP 기능을 활성화합니다. 모든 포트는 기본적으로 비활성화 상태입니다.	Interface Configuration Mode

주의사항:

- NDP가 정상적으로 동작하려면 전역 기능과 포트 기능이 모두 활성화되어야 합니다.
- NDP 기능은 Aggregated Port를 지원하지 않습니다.
- 토폴로지 수집 중 클러스터에 가입할 필요가 없는 장비의 정보까지 수집되어 클러스터에 추가되는 것을 방지하기 위해, 클러스터에 가입할 필요가 없는 장비와 연결된 포트에서는 NDP 기능을 비활성화하는 것이 권장됩니다.

24.3.2. NDP 파라미터 설정

Command	Description	CLI Mode
ndp aging-timer <aging-time>	수신 장비에서 유지되는 NDP 메시지의 aging 시간 설정. 기본값은 180초	Configuration Mode
ndp hello-timer <hello-time>	NDP 메시지 전송 주기 설정. 기본값은 60초	Configuration Mode

주의사항:

일반적으로 수신 장비의 NDP 메시지 aging 시간은 NDP 전송 주기보다 작으면 안 됩니다. 그렇지 않으면 NDP 포트 이웃 정보 테이블이 불안정해질 수 있습니다.

24.3.3. 시스템 및 인터페이스의 NTDP 기능 활성화

Command	Description	CLI Mode
ntdp global enable	전역 NTDP 기능을 활성화합니다. 기본값은 전역 비활성화 상태입니다.	Configuration Mode
ntdp enable	포트의 NTDP 기능을 활성화합니다. 모든 포트는 기본적으로 비	Interface Configuration

Command	Description	CLI Mode
	활성화 상태입니다.	Mode

주의사항:

- NTDP가 정상적으로 동작하려면 전역 기능과 포트 기능이 모두 활성화되어야 합니다.
- NTDP 기능은 Aggregated Port를 지원하지 않습니다.
- 토폴로지 수집 시 클러스터에 가입할 필요가 없는 장비의 정보까지 수집되는 것을 방지하기 위해, 해당 장비와 연결된 포트에서는 NTDP 기능을 비활성화하는 것이 권장됩니다.

24.3.4. NTDP 파라미터 설정

Command	Description	CLI Mode
ntdp hop <hop-value>	토폴로지 수집 범위를 설정합니다. 기본적으로 수집되는 토폴로지에서 가장 먼 장비는 수집 장비로부터 최대 3 hop까지입니다.	Configuration Mode
ntdp timer <interval-time>	주기적인 토폴로지 수집 시간 간격을 설정합니다. 기본값은 1분입니다.	Configuration Mode
ntdp timer hop-delay <time>	장비가 토폴로지 수집 요청 메시지를 첫 번째 포트에서 전달하기 전에 대기하는 시간을 설정합니다. 기본값은 200ms입니다.	Configuration Mode
ntdp timer port-delay <time>	현재 장비가 토폴로지 수집 요청 메시지를 각 포트로 전달할 때의 지연 시간을 설정합니다. 기본값은 20ms입니다.	Configuration Mode

24.3.5. NTDP 정보 수동 수집 설정

클러스터가 구성된 이후에는 관리 장비가 주기적으로 토폴로지 정보를 수집합니다. 또한, 클러스터 구성 여부와 관계없이 사용자는 언제든지 설정을 통해 NTDP 정보를 수동으로 수집할 수 있으며, 이를 통해 보다 효과적으로 장비를 실시간 관리 및 모니터링할 수 있습니다.

Command	Description	CLI Mode
ntdp explore	토폴로지 정보를 수동으로 1회 수집	Normal mode, Privileged mode

24.3.6. 클러스터 기능 활성화

Command	Description	CLI Mode
cluster enable	클러스터 기능을 활성화합니다. 기본적으로 클러스터 기능은 비활성화 상태입니다.	Configuration Mode

24.3.7. 클러스터 생성

Management VLAN은 클러스터 관리 범위를 제한합니다. Management VLAN을 설정하면 다음 기능을 구현할 수 있습니다.

- 클러스터 관리 메시지(NDP, NTDP, handshake 메시지 포함)를 Management VLAN 내부로 제한하고, 다른 메시지와 분리하여 보안을 향상시킵니다.
- 관리 장비와 Member 장비 간 내부 통신은 Management VLAN을 통해 이루어집니다.

Command	Description	CLI Mode
cluster management-vlan <vlan-id>	Management VLAN을 지정합니다. 기본값은 VLAN1입니다.	Configuration Mode

주의사항

현재 장비가 클러스터에 속해 있는 경우, Management VLAN을 수정할 수 없습니다.

클러스터에 속하지 않은 경우:

1) VLAN 존재 여부 확인
   → VLAN이 존재하지 않으면 즉시 실패하며, 존재하면 다음 단계로 진행합니다.
2) 모든 인터페이스 재확인
   → 인터페이스가 속한 VLAN과 Management VLAN이 동일하지 않은 경우,
   NDP 및 NTDP 전역 기능을 활성화한 후 다시 비활성화 및 초기화하고, 이후 다시 활성화해야 합니다.
3) 해당 VLAN의 Layer 3 인터페이스 확인
   → 존재하지 않으면 새로 생성합니다.
   → 생성이 실패하더라도 Management VLAN 설정은 완료된 상태입니다.
   → 이 경우 NDP와 NTDP는 동작하지만 클러스터에는 참여할 수 없습니다.
4) 현재 Layer 3 인터페이스의 MAC 주소를 dev_ID로 설정
   → VLAN 설정은 성공했으나 Layer 3 인터페이스 생성이 실패한 경우, vlan1의 MAC 주소를 dev_ID로 사용합니다.

Management VLAN이 설정된 상태에서 사용자가 VLAN Database에서 해당 VLAN을 삭제하면, Management VLAN은 자동으로 VLAN1으로 변경됩니다. 또한 활성화되어 있던 NDP, NTDP, Cluster 전역 기능은 함께 비활성화되고 초기화됩니다.

클러스터를 생성하기 전에, 사용자는 클러스터 내 Member 장비에서 사용할 Private IP 주소 범위를 먼저 설정해야 합니다.

Candidate 장비가 클러스터에 추가될 때, 관리 장비는 해당 범위 내에서 사용 가능한 Private IP를 동적으로 할당하고 Candidate 장비로 전달합니다. 이를 통해 클러스터 내부 통신이 이루어지며, 관리 장비가 Member 장비를 관리 및 유지보수할 수 있습니다.

Command	**Description**	**CLI Mode**
cluster ip-pool <IP/MASK>	관리 장비로 설정할 장비에서, 클러스터 내 Member 장비가 사용할 Private IP 주소 범위를 설정	Configuration Mode

주의사항

- 관리 장비 및 Member 장비의 VLAN 인터페이스 IP와 클러스터 IP 풀은 동일한 네트워크 대역으로 설정할 수 없습니다. 그렇지 않으면 클러스터가 정상적으로 동작하지 않습니다.
- 해당 설정은 장비가 클러스터에 속해 있지 않을 때만 가능합니다.
- Management VLAN을 기준으로 대응되는 Layer 3 인터페이스 존재 여부를 확인합니다.
  → 해당 인터페이스가 없으면 즉시 실패하며, 해당 장비는 Command Switch로 사용할 수 없습니다.
  → Layer 3 인터페이스가 존재하는 경우, 해당 인터페이스를 기준으로 IP Pool의 기본 주소가 설정됩니다.
  → 이 과정에서 설정이 실패하면 IP Pool 설정도 함께 실패합니다.

기본적으로 장비는 관리 장비(Command Switch)가 아니며, 클러스터는 아직 생성되지 않은 상태입니다.

Command	**Description**	**CLI Mode**
cluster build <name>	클러스터를 수동으로 생성하고, 현재 장비를 관리 장비로 설정하며 클러스터 이름을 지정	Configuration Mode
cluster auto-build <name>	클러스터를 자동으로 생성. 지정된 hop 범위 내에서 발견된 모든 Candidate 장비를 자동으로 클러스터에 추가	Configuration Mode
cluster delete <name>	클러스터 삭제	Configuration Mode

Command	Description	CLI Mode
cluster stop auto-add member	자동 클러스터 구성 시 신규 장비의 자동 가입을 중지. 이미 가입된 장비는 클러스터에 유지됨	Configuration Mode

주의사항

- 클러스터를 생성하기 전에만 Management VLAN을 지정할 수 있으며, 클러스터에 가입된 이후에는 Management VLAN을 변경할 수 없습니다. 변경이 필요한 경우, 관리 장비에서 클러스터를 삭제한 후 Management VLAN을 재설정하고 다시 클러스터를 구성해야 합니다.
- 보안을 위해 관리 장비와 Member 장비가 연결된 포트 및 Cascade 포트의 기본 VLAN ID를 Management VLAN으로 설정하지 않는 것이 권장됩니다.
- 관리 장비와 Member 장비가 연결된 포트 및 모든 Cascade 포트의 기본 VLAN ID가 Management VLAN인 경우에만 Management VLAN 메시지를 Untagged로 전송할 수 있습니다. 그렇지 않은 경우, 해당 포트들은 Management VLAN 메시지를 Tagged 형태로 전달하도록 설정해야 합니다. (자세한 설정은 VLAN 항목 참조)
- 클러스터 내 Member 장비의 Private IP 주소 범위는 클러스터가 생성되기 전에만 설정할 수 있으며, 관리 장비에서만 설정 가능합니다. 클러스터가 이미 생성된 이후에는 해당 IP 범위를 변경할 수 없습니다.

24.3.8. 클러스터 내부 Member 상호작용 설정

클러스터 내부에서 관리 장비는 Member 장비와 handshake 메시지를 통해 실시간으로 통신하며, 두 장비 간 연결 상태를 유지합니다.

Handshake 메시지 전송 간격과 장비의 유효 유지 시간은 관리 장비에서 설정할 수 있습니다. 이 설정은 클러스터 내 모든 Member 장비에 동시에 적용됩니다.

Command	Description	CLI Mode
cluster timer <interval-time>	Handshake 메시지 전송 간격 설정. 기본값은 10초	Configuration Mode
cluster holdtime <hold-time>	장비의 유효 유지 시간 설정. 기본값은 60초	Configuration Mode

24.3.9. 클러스터 멤버 관리 설정

사용자는 관리 장비에서 Candidate 장비를 수동으로 클러스터에 추가하거나, 클러스터에 포함된 특정 Member 장비를 수동으로 삭제할 수 있습니다.

클러스터 멤버의 추가/삭제 작업은 반드시 관리 장비에서 수행해야 하며, 그렇지 않을 경우 오류 메시지가 반환됩니다.

Command	Description	CLI Mode
cluster add member mac-address <mac-address>	Candidate 장비를 클러스터에 추가	Configuration Mode
cluster delete member mac-address <mac-address>	클러스터에서 Member 장비 삭제	Configuration Mode

24.4. Member 장비 설정

24.4.1. 시스템 및 포트의 NDP 기능 활성화

시스템 및 포트의 NDP 기능 활성화 항목을 참고하십시오.

24.4.2. 시스템 및 포트의 NTDP 기능 활성화

시스템 및 포트의 NTDP 기능 활성화 항목을 참고하십시오.

24.4.3. NTDP 정보 수동 수집 설정

NTDP 정보 수동 수집 설정 항목을 참고하십시오.

24.4.4. 클러스터 기능 활성화

클러스터 기능 활성화 항목을 참고하십시오.

24.5. 클러스터 멤버 접근 설정

NDP, NTDP 및 클러스터 기능이 정상적으로 설정된 이후에는, 관리 장비를 통해 클러스터 내 Member 장비를 설정, 관리 및 모니터링할 수 있습니다.

관리 장비에서 특정 Member 장비의 운영 인터페이스로 전환하여 해당 장비를 직접 구성할 수 있습니다.

Command	Description	CLI Mode
cluster switch-to member <member-number>	관리 장비 인터페이스에서 지정된 Member 장비 인터페이스로 전환	Normal mode, Privileged mode

주의사항

클러스터 관리 장비와 Member 장비 간 전환은 Telnet 연결을 사용합니다. 전환 시 다음 사항에 유의해야 합니다.

- 전환을 수행하기 전에 대상 장비에서 telnet server enable 명령을 실행하여 Telnet 기능을 활성화해야 합니다. 그렇지 않으면 전환이 실패합니다.
- 관리 장비에서 Member 장비로 전환할 때, 지정한 Member 번호가 존재하지 않으면 오류 메시지가 표시됩니다.
- 대상 장비의 Telnet 접속 사용자 수가 최대치에 도달한 경우, 전환이 실패합니다.

24.6. 클러스터 관리 조회 및 유지보수

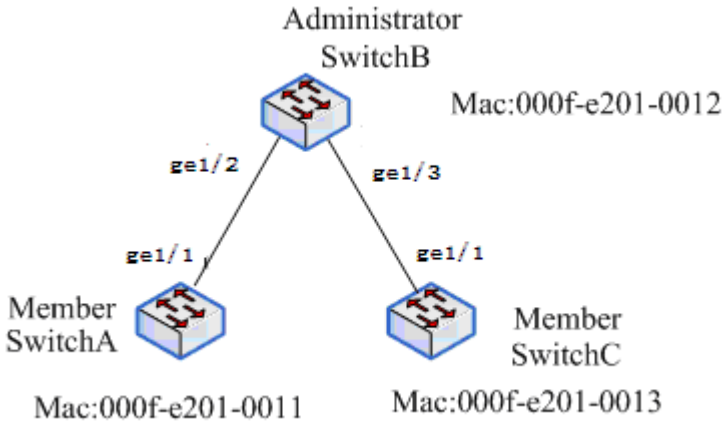
Command	Description	CLI Mode
show ndp [interface <ifname>]	NDP 설정 정보 조회	Normal mode, Privileged mode
reset ndp statistics [interface <ifname>]	NDP 통계 정보 초기화	Configuration View
show ntdp	시스템 NTDP 정보 조회	Normal mode, Privileged mode
show ntdp device-list	NTDP로 수집된 장비 정보 조회	Normal mode, Privileged mode
show ntdp single-device mac-address <mac-address>	지정된 장비의 NTDP 상세 정보 조회	Normal mode, Privileged mode
show cluster	장비가 속한 클러스터의 상태 및 통계 정보 조회	Normal mode, Privileged mode
show cluster topology	클러스터 토폴로지 정보 조회	Normal mode, Privileged mode
show cluster candidates [mac-address <mac-address>]	Candidate 장비 정보 조회	Normal mode, Privileged mode

Command	Description	CLI Mode
show cluster members [<member-number>]	클러스터 Member 장비 정보 조회	Normal mode, Privileged mode

24.7. 클러스터 관리 설정 예제

1) 네트워크 요구사항
세 대의 스위치 A, B, C로 구성된 클러스터를 구성하며, 관리 VLAN은 VLAN 10입니다.
Switch B는 관리 장비(Administrator), Switch A와 Switch C는 Member 장비입니다.
클러스터 전체 주소 풀의 기본 IP는 10.0.0.1이며, 총 8대의 장비를 지원합니다.

2) 네트워크 구성도



3) 설정 절차
Member 장비 SwitchA 설정

Management VLAN 설정
[SwitchA] cluster management-vlan 10
[SwitchA] interface ge1/1
[SwitchA-ge1/1] switch access vlan 10

NDP 기능 활성화 (전역 및 포트)
[SwitchA] ndp global enable
[SwitchA] interface ge1/1
[SwitchA-ge1/1] ndp enable

NTDP 기능 활성화 (전역 및 포트)
[SwitchA] ntdp global enable

[SwitchA] interface ge1/1
[SwitchA-ge1/1] ntdp enable

클러스터 기능 활성화
[SwitchA] cluster enable

Member 장비 SwitchC 설정
Member 장비는 동일한 설정을 사용하므로 SwitchC도 SwitchA와 동일하게 설정합니다.

관리 장비 SwitchB 설정
Management VLAN 설정
[SwitchB] cluster management-vlan 10
[SwitchB] interface ge1/2
[SwitchB-ge1/2] switch access vlan 10
[SwitchB] interface ge1/3
[SwitchB-ge1/3] switch access vlan 10

NDP / NTDP 기능 활성화 (전역 및 포트)
[SwitchB] ndp global enable
[SwitchB] ntdp global enable

[SwitchB] interface ge1/2
[SwitchB-ge1/2] ndp enable
[SwitchB-ge1/2] ntdp enable

[SwitchB] interface ge1/3
[SwitchB-ge1/3] ndp enable
[SwitchB-ge1/3] ntdp enable

NDP 파라미터 설정
[SwitchB] ndp timer aging 200
[SwitchB] ndp timer hello 70

NTDP 파라미터 설정
[SwitchB] ntdp hop 2
[SwitchB] ntdp timer hop-delay 150
[SwitchB] ntdp timer port-delay 15
[SwitchB] ntdp timer 3

클러스터 기능 활성화
[SwitchB] cluster enable

```
# 클러스터 IP 풀 설정
[SwitchB] cluster ip-pool 10.0.0.1 8

# 클러스터 생성 및 자동 가입
[SwitchB] cluster auto-build abc

# 자동 가입 중지 (필요 시)
[SwitchB] cluster stop auto-add member
```

25. SNTP 설정

이 장에서는 SNTP(Simple Network Time Protocol) 설정과 관련된 내용을 설명하며, 다음과 같은 항목을 포함합니다.

- SNTP 소개
- SNTP 설정
- SNTP 정보 조회

25.1. SNTP 소개

현재 인터넷에서는 네트워크 시간 동기화를 위해 일반적으로 NTP(Network Time Protocol)를 사용하며, 또

다른 프로토콜로는 NTP의 단순화된 버전인 SNTP(Simple Network Time Protocol)가 있습니다.

NTP 프로토콜은 다양한 플랫폼과 운영체제를 지원하며, 매우 정교한 알고리즘을 사용하기 때문에 네트워크 지연이나 지터의 영향을 거의 받지 않고 약 1~50ms 수준의 정확도를 제공합니다. 또한 높은 수준의 보안을 위한 인증 기능도 제공합니다. 하지만 NTP는 알고리즘이 복잡하고 시스템 요구사항이 높은 편입니다.

SNTP는 NTP의 단순화된 버전으로, 구현 시 간단한 알고리즘을 사용하여 시간 계산을 수행하므로 성능이 뛰어납니다. 정확도는 일반적으로 약 1초 수준이며, 대부분의 환경에서 요구되는 시간 동기화 요구사항을 충분히 만족할 수 있습니다.

SNTP 메시지는 NTP 메시지와 완전히 동일한 형식을 사용하므로, 스위치에 구현된 SNTP 클라이언트는 NTP 서버와 완전히 호환됩니다.

25.2. SNTP 설정

25.2.1. 기본 SNTP 설정

Item	Default Value
SNTP 상태	Disable (SNTP 서비스 비활성화)
NTP 서버	없음
SNTP 동기화 주기	1800초
로컬 타임존	+8 (동8구)

SNTP 활성화 / 비활성화

설정은 다음과 같습니다:

Switch# configure terminal

→ Global Configuration Mode 진입

Switch(config)# sntp enable

→ SNTP 활성화

Switch(config)# sntp disable

→ SNTP 비활성화

25.2.2. SNTP 서버 주소 설정

SNTP 메시지는 NTP 메시지와 완전히 동일하므로, SNTP Client는 NTP Server와 완전히 호환됩니다. 네트워크에는 다양한 NTP 서버가 존재하므로, 지연이 적은 서버를 선택하는 것이 좋습니다.

NTP 서버 주소는 다음 사이트에서 확인할 수 있습니다.

- ntp.kriss.re.kr
- kr.pool.ntp.org

예: 192.43.244.18 (time.nist.gov)

스위치는 최대 3개의 서버 주소를 설정할 수 있으며, 첫 번째 서버부터 순차적으로 시간 동기화를 시도합니다. 첫 번째 서버 실패 시 두 번째, 그 다음 서버를 사용합니다.

25.2.3. SNTP 동기화 주기 설정

SNTP Client는 NTP Server와 주기적으로 시간 동기화를 수행하여 정확한 시간을 유지합니다.

설정 방법

Switch# configure terminal

Switch(config)# sntp interval 60

→ 시간 동기화 주기 설정 (단위: 초)

→ 설정 범위: 60 ~ 65535초

→ 기본값: 1800초

→ 위 예제에서는 60초로 설정

기본값으로 복구

Switch(config)# no sntp interval

→ 동기화 주기를 기본값인 1800초로 복구

25.2.4. 로컬 타임존 설정

SNTP를 통해 동기화된 시간은 기본적으로 GMT(그리니치 표준시)입니다.

실제 지역 시간에 맞추기 위해서는 로컬 타임존 설정이 필요합니다.

기본적으로 스위치의 타임존은 동경 8구(East +8)로 설정되어 있습니다.

설정 방법

Switch# configure terminal

Switch(config)# sntp time-zone -8

→ 로컬 타임존을 서경 8구(West -8)로 설정

기본값으로 복구

Switch(config)# no sntp time-zone

→ 타임존을 기본값인 동경 8구(East +8)로 복구

25.3. SNTP 정보 조회

SNTP 설정 및 동작 상태를 확인하기 위한 명령어는 다음과 같습니다.

명령어

Switch# show sntp

→ SNTP 상태, 서버 정보, 동기화 주기 등 SNTP 관련 전체 상태 정보 조회

Switch# show running-config

→ 현재 장비에 설정된 전체 구성 확인 (SNTP 설정 포함)

26. System Log 구성

이 장에서는 주로 다음 내용을 포함합니다.

- System Log 소개
- Syslog 구성

26.1. System Log 소개

시스템 로그 모듈은 스위치의 중요한 구성 요소로, 시스템 전체의 동작 상태, 비정상 동작, 사용자 작업 기록 등을 저장하는 역할을 합니다. 이를 통해 관리자는 시스템 상태를 실시간으로 파악하고 모니터링할 수 있습니다.

시스템 로그 모듈은 각 동작 모듈에서 발생하는 모든 로그 정보를 수집하고, 이를 분류, 저장 및 표시하는 기능을 수행합니다.

또한 로그 시스템에는 중요한 디버깅 기능이 포함되어 있습니다. 디버깅 기능을 통해 관리자는 네트워크 동작 상태를 모니터링하고, 장애를 분석 및 진단할 수 있습니다. 필요한 디버깅 항목을 선택하여 로그를 확인함으로써 장비 또는 네트워크의 문제를 보다 쉽게 파악하고 해결할 수 있습니다.

이 절에서는 다음과 같은 내용을 다룹니다.

- 로그 정보 형식
- 로그 저장 방식
- 로그 표시 방법
- 디버깅 도구

26.1.1. 로그 정보 형식

로그 정보 형식은 다음과 같습니다.

Timestamp, priority, module name, log content

Timestamp와 priority 사이에는 공백이 있으며, priority와 module name 사이에는 ": "(콜론 + 공백), module name과 log content 사이에도 ": "가 사용됩니다.

예시:

2006/05/20 13:56:34 Warning: MSTP: Port up notification received for port ge1/2

이 로그에서

- Timestamp: 2006/05/20 13:56:34
- Priority: Warning
- Module Name: MSTP
- Log Content: Port up notification received for port ge1/2

1) Timestamp
   형식: year/month/day hour:minute:second
   시간은 24시간 형식(0~23)을 사용합니다.

   Timestamp는 로그가 생성된 시점을 의미하며, 스위치의 시스템 시간을 기준으로 합니다.
   시스템 시간은 출고 시 설정되어 있으며, 관리자에 의해 변경할 수 있습니다.

또한 장비 전원이 꺼져도 유지됩니다.

2) Priority

Priority는 로그의 중요도를 나타내며, 다음 4단계로 구분됩니다.

Priority	설명
Critical	심각한 오류
Warning	일반 오류, 경고, 중요한 알림
Informational	일반 정보, 진단 정보
Debugging	디버깅 정보

우선순위는 Critical → Warning → Informational → Debugging 순으로 낮아집니다.

3) Module Name

Module Name은 로그를 생성한 모듈을 의미합니다. 주요 모듈은 다음과 같습니다.

Module Name	설명
CLI	명령어 인터페이스 모듈
MSTP	다중 인스턴스 스패닝 트리 프로토콜
VLAN	VLAN 기능 모듈
ARP	ARP 프로토콜 모듈
IP	IP 프로토콜 모듈
ICMP	ICMP 프로토콜 모듈
UDP	UDP 프로토콜 모듈
TCP	TCP 프로토콜 모듈

4) Log Content

Log Content는 로그의 핵심 내용을 나타내는 문장 또는 구문입니다.
관리자는 해당 내용을 통해 시스템에서 어떤 이벤트가 발생했는지 확인할 수 있습니다.

26.1.2. 로그 저장

로그는 일반적으로 다음 세 가지 방식으로 저장됩니다.

- 메모리 저장
- NVM 저장
- 서버 저장

메모리 저장 방식에서는 로그 우선순위에 따라 4개의 로그 테이블이 존재하며, 각 테이블은 하나의 우선순위에 해당하는 로그만 저장합니다.

각 로그 테이블은 최대 1K(약 1024개)의 로그를 저장할 수 있으며, 테이블이 가득 차면 가장 오래된 로그부터 덮어쓰기 됩니다.

이 방식의 단점은 시스템이 재부팅되면 로그가 모두 삭제된다는 점입니다. 따라서 장애 발생 후 원인 분석이 어려울 수 있습니다.

중요 로그(Critical, Warning)는 NVM에 저장할 수 있습니다.

이 경우 재부팅 이후에도 로그가 유지되어 장애 분석에 도움이 됩니다.

하지만 NVM은 저장 용량이 제한적이기 때문에 많은 로그를 저장하기에는 적합하지 않습니다.

가장 효율적인 방법은 SYSLOG 프로토콜을 이용하여 로그를 서버에 저장하는 방식입니다.

이 방식은 로그를 실시간으로 서버에 전송하고, 서버에서 저장 및 표시하므로 대용량 로그 관리가 가능하며 관리 편의성이 높습니다.

단, 현재 시스템은 메모리 저장만 지원하며, NVM 및 서버 저장 방식은 지원하지 않습니다.

26.1.3. 로그 표시

로그 표시 방식은 수동 표시와 실시간 표시 두 가지가 있습니다.

수동 표시는 사용자가 명령어를 입력하여 로그 정보를 확인하는 방식입니다.

실시간 표시는 로그 정보가 생성될 때 해당 로그가 터미널에 바로 출력되는 방식이며, 사용자는 발생한 로그를 즉시 확인할 수 있습니다.

수동 표시 방식에서는 모든 로그 정보를 확인할 수 있습니다. 로그 정보는 가장 최근 로그가 앞에 표시되는 순서로 출력되므로, 사용자는 스위치의 최신 동작 상태를 먼저 확인할 수 있습니다.

실시간 표시 방식에서는 사용자가 터미널 실시간 표시 기능을 활성화해야 합니다.

해당 기능이 활성화되어 있으면 생성된 로그 정보가 로그 테이블에 저장될 뿐만 아니라 터미널에도 출력됩니다.

해당 기능이 비활성화되어 있으면 로그 정보는 터미널에 실시간으로 표시되지 않습니다.

현재 시스템은 Console 터미널로의 실시간 로그 출력만 지원하며, Telnet 터미널로의 실시간 로그 출력은 지원하지 않습니다.

26.1.4. 디버깅 도구

디버깅(Debugging)은 장비 및 네트워크 문제를 진단하기 위한 도구입니다.

시스템 및 각 모듈의 패킷 송수신 과정과 상태 머신의 변화를 추적하여, 관리자가 시스템과 모듈의 동작 과정을 이해하고 모니터링할 수 있도록 합니다.

네트워크나 장비에 이상이 발생했을 경우, 디버깅 도구를 통해 문제를 추적할 수 있습니다.

디버깅 도구는 다양한 디버깅 옵션을 제공하며, 관리자는 필요한 항목만 선택하여 추적할 수 있습니다.

장애 발생 시 관련 디버깅 기능을 활성화하면, 시스템 및 모듈의 동작 흐름을 추적하여 문제 원인을 분석할 수 있습니다.

디버깅 기능이 활성화되면, 관련 로그 정보가 생성되어 해당 로그 테이블에 저장됩니다.

일반적으로 디버깅을 통해 생성되는 로그의 우선순위는 Informational입니다.

또한 터미널 실시간 표시 기능이 활성화된 경우, 디버깅 로그는 터미널에 실시간으로 출력됩니다.

디버깅 기능이 비활성화되면, 관련 로그는 생성되지 않습니다.

26.2. Syslog 구성

- 터미널 실시간 로그 출력 설정
- 로그 정보 확인
- 디버깅 기능 설정
- 디버깅 정보 확인

26.2.1. 터미널 실시간 로그 출력 설정

기본적으로 터미널 실시간 출력 기능은 비활성화되어 있으며, 시스템에서 생성된 로그는 로그 테이블에만 저장되고 터미널에는 표시되지 않습니다.

일부 로그는 이 설정과 관계없이 항상 Console 터미널에 출력됩니다.

현재 시스템은 Console 터미널에서만 실시간 로그 출력이 가능하며, Telnet 터미널에서는 지원되지 않습니다.

또한 write 명령으로 설정을 저장하더라도, 터미널 실시간 출력 설정은 구성 파일에 저장되지 않으며, 장비 재부팅 시 초기화되므로 다시 설정해야 합니다.

Command	설명	CLI Mode
log stdout	터미널 실시간 로그 출력 기능을 활성화합니다.	Configuration Mode
no log stdout	터미널 실시간 로그 출력 기능을 비활성화합니다.	Configuration Mode

26.2.2. 로그 레벨 설정

로그 레벨 설정 명령은 다음과 같습니다.

Command	설명	CLI Mode
log trap <alerts | critical | debugging | emergencies | errors | informational | notifications | warnings>	로그 출력 레벨을 설정합니다.	Configuration Mode

26.2.3. 로그 정보 확인

로그 정보 확인 명령은 다음과 같습니다.

Command	설명	CLI Mode
show log	모든 로그 정보를 표시합니다.	Configuration Mode

26.2.4. 디버깅 스위치 설정

시스템은 다양한 디버깅 스위치를 제공하며, 여러 모듈에 대해 디버깅을 수행할 수 있습니다. 여기서는 주요 명령만 설명하며, 전체 명령 형식은 별도 매뉴얼을 참고해야 합니다.

또한 write 명령으로 설정을 저장하더라도 디버깅 설정은 구성 파일에 저장되지 않으며, 장비 재부팅 시 초기화되므로 다시 설정해야 합니다.

Command	설명	CLI Mode
debug ip ...	IP 패킷 송수신 관련 디버깅 활성화	Privileged Mode
no debug ip ...	IP 패킷 관련 디버깅 비활성화	Privileged Mode

Command	설명	CLI Mode
debug ip icmp ...	ICMP 패킷 디버깅 활성화	Privileged Mode
no debug ip icmp ...	ICMP 패킷 디버깅 비활성화	Privileged Mode
debug ip arp ...	ARP 패킷 디버깅 활성화	Privileged Mode
no debug ip arp ...	ARP 패킷 디버깅 비활성화	Privileged Mode
debug ip udp ...	UDP 패킷 디버깅 활성화	Privileged Mode
no debug ip udp ...	UDP 패킷 디버깅 비활성화	Privileged Mode
debug ip tcp ...	TCP 패킷 디버깅 활성화	Privileged Mode
no debug ip tcp ...	TCP 패킷 디버깅 비활성화	Privileged Mode
debug mstp ...	MSTP 프로토콜 디버깅 활성화	Privileged Mode
no debug mstp ...	MSTP 프로토콜 디버깅 비활성화	Privileged Mode
debug igmp snooping ...	IGMP Snooping 디버깅 활성화	Privileged Mode
no debug igmp snooping ...	IGMP Snooping 디버깅 비활성화	Privileged Mode
debug dhcp snooping ...	DHCP Snooping 디버깅 활성화	Privileged Mode
no debug dhcp snooping ...	DHCP Snooping 디버깅 비활성화	Privileged Mode
no debug all	모든 디버깅 비활성화	Privileged Mode

26.2.5. 디버깅 정보 확인

디버깅 정보 확인 명령은 다음과 같습니다.

Command	설명	CLI Mode
show debug [module]	디버깅 스위치 설정을 확인합니다. 파라미터 미입력 시 전체 모듈, 특정 모듈 입력 시 해당 모듈만 확인합니다. IP 입력 시 IP, ICMP, ARP, UDP, TCP 모듈을 함께 확인합니다.	Normal Mode, Privileged Mode

26.3. SYSLOG 구성

이 장에서는 주로 다음 내용을 포함합니다.

- SYSLOG 소개
- SYSLOG 구성
- SYSLOG 구성 예제

26.3.1. SYSLOG 소개

SYSLOG는 장비 로그 정보 관리를 위한 표준 프로토콜이며, 구조가 단순하여 널리 사용됩니다.

SYSLOG 시스템은 크게 세 부분으로 구분됩니다.

1) 로그 정보 분류
   각 서브 모듈을 정의하여 서로 다른 모듈에서 생성되는 로그 정보를 구분하고, 로그 레벨을 정의하여 장비의 동작 상태를 확인할 수 있도록 합니다.
   장비의 다양한 로그 정보는 이 기준에 따라 수집됩니다.
2) 설정 파일
   수집된 로그 정보를 어떻게 처리할지 정의합니다.
   로그 정보는 로컬에 저장하거나, 네트워크의 지정된 서버로 전송하거나, 지정된 로그인 사용자에게 배포할 수 있습니다.
   설정 파일은 장비에서 생성된 로그 정보를 저장하고 처리하는 방식을 결정합니다.
3) SYSLOG 프로토콜 메시지 전송
   RFC에서 정의한 메시지 형식에 따라 SYSLOG 프로토콜 메시지를 전송합니다.
   스위치 시스템에서 SYSLOG 전체 동작 기준은 System Log 모듈입니다.
   SYSLOG 프로토콜의 첫 번째 부분은 스위치의 각 기능 서브 모듈에서 수행합니다. 각 모듈은 각 레벨의 로그 정보를 System Log 모듈로 전달합니다. Syslog 모듈은 4단계 로그 테이블을 유지합니다.
   SYSLOG 프로토콜의 두 번째 부분은 System Log 모듈이 로그 정보를 통합 분배하는 방식으로 동작합니다.
   첫째, 터미널 출력 설정을 통해 로그 정보를 시리얼 포트 터미널에 실시간 또는 수동으로 표시합니다.
   둘째, 4단계 로그 테이블을 메모리에 저장합니다.
   셋째, 전원 장애 시 중요한 로그 기록이 손실되지 않도록 높은 레벨의 로그 정보를 NVM에 저장합니다.
   넷째, SYSLOG 메시지를 통해 로그를 원격 서버로 전송하여 저장, 수집 및 정리할 수 있습니다.
   System Log 모듈 내 SYSLOG 서브 모듈은 시스템 로그를 서버로 전송하는 세 번째 기능만 구현합니다.

26.3.2. SYSLOG 구성

SYSLOG 구성 명령은 다음 항목을 포함합니다.

- SYSLOG 서버 주소 활성화
- SYSLOG 서버 주소 비활성화
- SYSLOG 프로토콜 활성화

Command	**설명**	**CLI Mode**
syslog open <server-ip>	SYSLOG 서버 주소를 활성화합니다. Parameter: server-ip는 서버 IP 주소입니다.	Configuration Mode
syslog close	SYSLOG 서버 주소를 비활성화합니다.	Configuration Mode
log syslog	SYSLOG 프로토콜을 활성화합니다.	Configuration Mode

26.3.3. SYSLOG 구성 예제

1) 구성
SYSLOG 서버 IP 주소를 192.168.0.201로 설정하고, 스위치를 다음과 같이 설정합니다.
Switch#configure terminal
Switch(config)#syslog open 192.168.0.201
Switch(config)#log syslog

2) 확인
Switch#show syslog
Syslog is opened!
server ip address: 192.168.0.201
udp destination port: 514
severity level: debugging
local device name: switch

27. IPv6 기본 구성

이 장에서는 스위치의 IPv6 기본 기능 설정에 대해 설명합니다.

해당 스위치는 IPv6 L2 포워딩 및 IPv6 ND(Neighbor Discovery) 기능을 지원합니다.

이 장에서는 다음 내용을 포함합니다.

- IPv6 소개
- IPv6 기본 기능 설정
- IPv6 Neighbor Discovery 프로토콜 설정
- IPv6 정보 확인 및 유지보수

27.1. IPv6 소개

IPv6(Internet Protocol Version 6)는 네트워크 계층 프로토콜의 차세대 표준으로, IPng(IP Next Generation)라고도 불립니다.

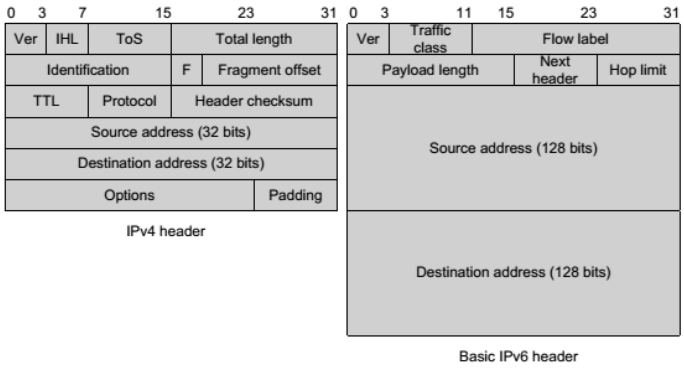
이는 IETF에서 설계한 규격으로, 기존 IPv4를 확장한 업그레이드 버전입니다.

IPv6와 IPv4의 가장 큰 차이점은 IP 주소 길이입니다.

IPv4는 32비트 주소를 사용하는 반면, IPv6는 128비트 주소를 사용하여 훨씬 더 많은 주소 공간을 제공합니다.

27.1.1. IPv6 프로토콜 특징

1) 헤더 구조 단순화
   IPv6는 IPv4 헤더의 일부 필드를 제거하거나 확장 헤더로 이동시켜 기본 헤더 구조를 단순화했습니다.
   고정 길이(40바이트)의 기본 헤더를 사용하여 포워딩 장비의 처리 효율을 향상시킵니다.
   IPv6 주소는 IPv4보다 4배 길지만, 기본 헤더 크기는 옵션 제외 IPv4 헤더(20바이트)의 약 2배 수준입니다.



2) 충분한 주소 공간
   IPv6는 128비트(16바이트)의 주소를 사용하여 약 3.4×10^{38}개의 주소를 제공합니다.
   이는 공인망, 사설망, 계층적 주소 분할 등 다양한 요구를 충분히 만족할 수 있는 규모입니다.
3) 계층적 주소 구조
   IPv6는 계층적 주소 구조를 사용하여 라우팅 검색 속도를 향상시키고,
   라우팅 집약(Route Aggregation)을 통해 라우팅 테이블 크기를 줄여 시스템 자원 사용을 효율화합니다.
4) 자동 주소 설정
   IPv6는 호스트 설정을 단순화하기 위해 두 가지 주소 설정 방식을 지원합니다.
   - Stateful 방식: DHCP 서버 등으로부터 IPv6 주소 및 관련 정보를 할당받음
   - Stateless 방식: 라우터가 제공하는 Prefix와 자신의 MAC 주소를 기반으로 자동 설정

   또한 기본 Prefix(FE80::/10)를 사용하여 링크 로컬 주소를 자동 생성하며, 동일 링크 내 통신이 가

능합니다.

5) 내장 보안 기능
IPv6는 IPSec을 표준 확장 헤더로 포함하여 종단 간 보안(End-to-End Security)을 제공합니다.
이를 통해 보안 표준화와 애플리케이션 간 상호운용성을 향상시킵니다.

6) QoS 지원
IPv6 헤더의 Flow Label 필드를 통해 특정 트래픽 흐름을 식별할 수 있으며,
장비는 이를 기반으로 QoS 처리를 수행할 수 있습니다.

7) 향상된 Neighbor Discovery
IPv6의 Neighbor Discovery는 ICMPv6 메시지를 기반으로 동작합니다.
기존 IPv4의 다음 기능을 대체합니다.
- ARP
- ICMP Router Discovery
- ICMP Redirect

추가적으로 이웃 노드 간 다양한 정보 교환 기능을 제공합니다.

8) 유연한 확장 헤더 구조
IPv6는 IPv4의 옵션 필드를 제거하고 다양한 확장 헤더를 도입했습니다.
이로 인해 처리 효율이 향상되고 프로토콜 확장성이 크게 개선되었습니다.
IPv4 옵션 필드는 최대 40바이트로 제한되지만, IPv6 확장 헤더는 패킷 크기 범위 내에서 유연하게 확장할 수 있습니다.

27.1.2. IPv6 주소 소개

1) IPv6 주소 표현 방식
IPv6 주소는 16비트 단위의 16진수 숫자 8개 그룹으로 구성되며, 각 그룹은 콜론(:)으로 구분됩니다.

예시:
2001:0000:130F:0000:0000:09C0:876A:130B

주소를 간략하게 표현하는 방법은 다음과 같습니다.

① 각 그룹의 앞쪽 0은 생략 가능
→ 2001:0:130F:0:0:9C0:876A:130B
② 연속된 0 그룹은 "::"로 축약 가능
→ 2001:0:130F::9C0:876A:130B

주의사항

"::"는 한 번만 사용할 수 있습니다. 여러 번 사용하면 원래 128비트 주소 복원이 불가능합니다.

IPv6 주소는 다음 두 부분으로 구성됩니다.

- Prefix (네트워크 부분)
- Interface Identifier (호스트 부분)

표기 방식: IPv6주소/Prefix길이

2) IPv6 주소 종류

IPv6 주소는 크게 세 가지로 구분됩니다.

① Unicast 주소
단일 인터페이스를 식별하며, IPv4의 유니캐스트와 동일한 개념입니다.

② Multicast 주소
여러 인터페이스 그룹을 식별하며, 해당 주소로 전송된 패킷은 그룹 전체로 전달됩니다.

③ Anycast 주소
여러 인터페이스 중 가장 가까운(라우팅 기준) 하나로 전달됩니다.

IPv6에는 Broadcast 주소가 없으며, 해당 기능은 Multicast로 대체됩니다.
주요 주소 Prefix는 다음과 같습니다.

주소 타입	포맷 프리픽스 (Binary)	IPv6 프리픽스 표기
Unicast 주소	지정되지 않음	00...0 (128비트) / ::/128
	Loopback 주소	00...1 (128비트) / ::1/128
	Link-local 주소	1111111010
	Site-local 주소	1111111011
	Global Unicast 주소	기타 형식
Multicast 주소	11111111	FF00::/8
Anycast 주소	Unicast 주소 공간에서 사용	Unicast 주소 형식 사용

3) Unicast 주소 유형

- Global Unicast
  IPv4의 공인 IP와 동일 개념, 인터넷 라우팅 가능
- Link-local
  동일 링크 내 통신용 (ND, 자동 설정), 라우터를 통해 전달되지 않음

- Site-local
  사설 네트워크용 주소 (외부 라우팅 불가)
- Loopback
  ::1, 자기 자신 통신용
- Unspecified
  ::, 주소 할당 전 임시 사용 (목적지로 사용 불가)

4) Multicast 주소
특수 목적 Multicast 주소 예시는 다음과 같습니다.

주소	용도
FF01::1	노드 로컬 전체 노드
FF02::1	링크 로컬 전체 노드
FF01::2	노드 로컬 전체 라우터
FF02::2	링크 로컬 전체 라우터
FF05::2	사이트 전체 라우터

또한 Solicited-node 주소가 존재합니다.

형식:

FF02::1:FFXX:XXXX

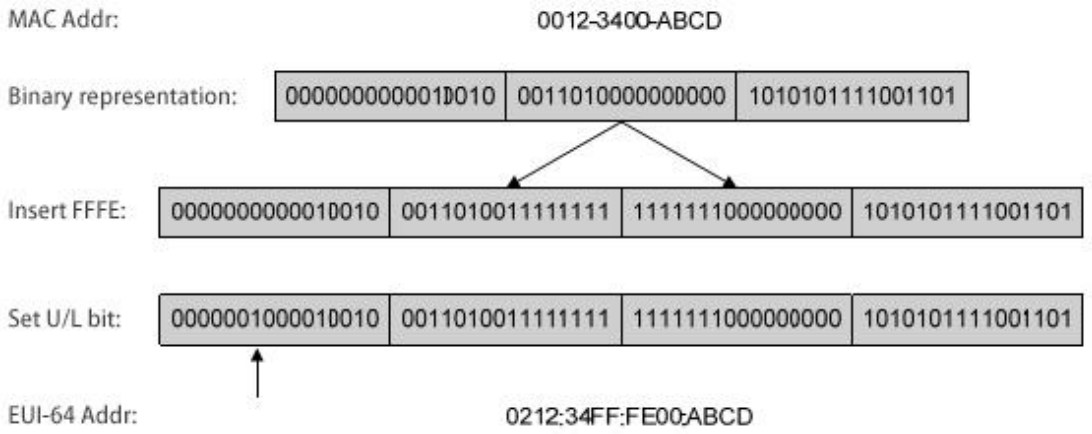
이는

- 이웃 노드 MAC 주소 조회
- 중복 주소 검출(DAD)

에 사용됩니다.

5) EUI-64 기반 인터페이스 ID
IPv6 인터페이스 식별자는 일반적으로 64비트이며, MAC 주소 기반으로 생성됩니다.
생성 방법은 다음과 같습니다.
① MAC 주소(48bit) 중간에 FFFE 삽입
② U/L 비트(7번째 비트)를 1로 변경

이렇게 생성된 값이 IPv6 Interface ID로 사용됩니다.



MAC 주소를 EUI-64 형식 인터페이스 식별자로 변환

27.1.3. IPv6 Neighbor Discovery Protocol 개요

IPv6 Neighbor Discovery Protocol(NDP)은 5가지 ICMPv6 메시지를 사용하여 다음 기능들을 수행합니다.

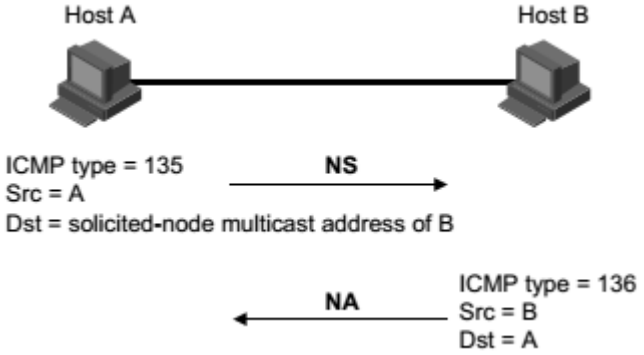
- 주소 해석(Address Resolution)
- 이웃 도달 가능 여부 확인(Neighbor Reachability)
- 중복 주소 검출(Duplicate Address Detection)
- 라우터/프리픽스 탐색(Router/Prefix Discovery)
- 주소 자동 설정(Address Autoconfiguration)
- 리다이렉션(Redirection)

아래 표는 NDP에서 사용하는 ICMPv6 메시지 타입과 기능을 정리한 것입니다.

ICMPv6 메시지	**타입 번호**	**동작**
Neighbor Solicitation	135	이웃의 링크 계층 주소 조회
		이웃 도달 가능 여부 확인
		중복 주소 검출 수행
Neighbor Advertisement	136	NS 메시지에 대한 응답
		링크 계층 정보 변경 시 이웃에게 변경사항 알림
Router Solicitation	133	노드 부팅 후 라우터에 프리픽스 및 설정 정보 요청

ICMPv6 메시지	타입 번호	동작
Router Advertisement	134	RS 메시지에 대한 응답
		주기적으로 프리픽스 및 플래그 정보 전달
Redirect	137	최적의 다음 홉으로 경로 재선택 유도

1) 주소 해석 (Address Resolution)
같은 링크 상의 이웃 노드의 링크 계층 주소를 얻는 기능으로, IPv4의 ARP와 동일한 역할을 합니다.
NS와 NA 메시지를 통해 수행됩니다.



동작 과정:

① 노드 A가 NS 메시지를 멀티캐스트로 전송
출발지: A의 IPv6 주소
목적지: B의 Solicited-node 멀티캐스트 주소
내용: A의 링크 계층 주소 포함

② 노드 B는 해당 메시지가 자신에게 해당되는지 확인 후
→ 자신의 링크 계층 주소를 포함한 NA 메시지를 유니캐스트로 응답

③ 노드 A는 NA 메시지를 통해 B의 링크 계층 주소를 획득

2) 이웃 도달 가능 여부 확인 (Neighbor Reachability)
이웃의 링크 계층 주소를 획득한 후, 해당 노드가 실제로 통신 가능한 상태인지 확인하는 기능입니다.

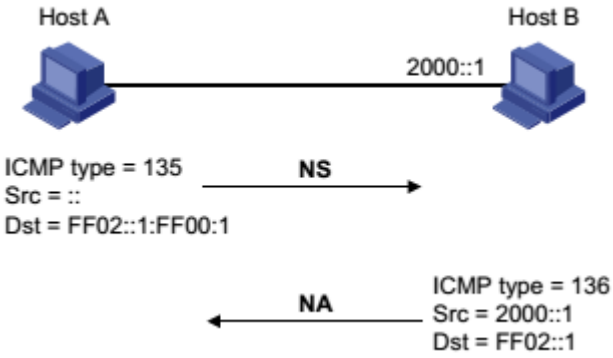
동작 과정:

① NS 메시지를 이웃 IPv6 주소로 전송

② NA 응답 수신 시 → 도달 가능
응답 없을 경우 → 도달 불가로 판단

3) 중복 주소 검출 (Duplicate Address Detection, DAD)
노드가 IPv6 주소를 사용할 때, 해당 주소가 이미 사용 중인지 확인하는 기능입니다. (IPv4의

Gratuitous ARP와 유사)



동작 과정:

① 노드 A가 NS 메시지 전송
출발지: :: (미지정 주소)
목적지: 검사 대상 IPv6 주소의 Solicited-node 멀티캐스트
내용: 검사할 IPv6 주소 포함

② 동일 주소를 사용하는 노드 B가 있으면 NA 메시지 응답

③ NA 수신 시 → 주소 중복
응답 없으면 → 사용 가능

4) 라우터/프리픽스 탐색 및 자동 주소 설정
노드는 RA 메시지를 통해 라우터 및 네트워크 정보를 획득하고, 이를 기반으로 IPv6 주소를 자동 설정합니다.

동작 과정:

① 노드 부팅 시 RS 메시지로 라우터에 정보 요청

② 라우터는 RA 메시지로 프리픽스 정보 응답 (주기적 송신 포함)

③ 노드는 해당 정보를 이용해 IPv6 주소 자동 설정

추가 설명:

프리픽스 정보에는 다음이 포함됨

- 주소 프리픽스
- Preferred Lifetime
- Valid Lifetime

Valid Lifetime 동안 주소 사용 가능

만료 시 자동으로 주소 삭제

5) 리다이렉션 기능 (Redirection)
호스트가 더 효율적인 경로를 사용하도록 유도하는 기능입니다. (IPv4 ICMP Redirect와 동일 개념)

동작 조건:

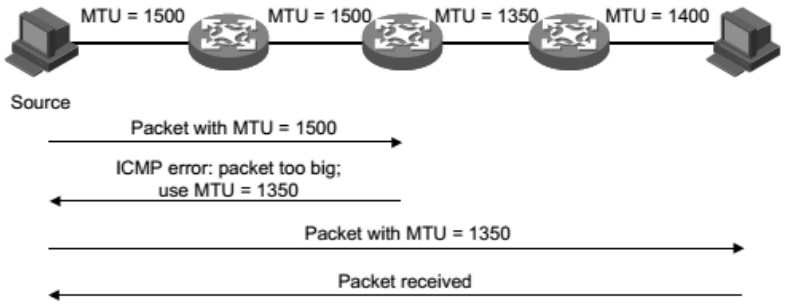
- 수신 인터페이스와 송신 인터페이스가 동일할 경우
- 해당 경로가 ICMP Redirect로 생성된 경로가 아닐 경우
- 기본 경로(Default Route)가 아닐 경우
- 패킷에 Routing Extension Header가 포함되지 않은 경우
-

→ 위 조건 만족 시, 게이트웨이는 ICMPv6 Redirect 메시지를 보내 호스트가 더 적절한 다음 홉을 선택하도록 유도합니다.

27.1.4. IPv6 PMTU Discovery

송신지에서 목적지까지 패킷이 전달되는 경로 상에는 서로 다른 MTU를 가지는 링크들이 존재할 수 있습니다. IPv6에서는 패킷의 길이가 링크의 MTU보다 클 경우, 중간 장비가 아닌 송신 측에서 단편화(Fragmentation)를 수행합니다. 이를 통해 중간 전달 장비의 처리 부담을 줄이고, 네트워크 자원을 보다 효율적으로 사용할 수 있습니다.

PMTU(Path MTU) 탐색 메커니즘의 목적은 송신지에서 목적지까지의 경로 상에서 가장 작은 MTU 값을 찾는 것입니다. PMTU의 동작 과정은 다음과 같습니다.



PMTU 동작 과정

1) 송신 호스트는 자신의 MTU를 기준으로 패킷을 분할한 후 목적지로 전송합니다.
2) 중간 전달 장비가 패킷을 수신하여 전달하는 과정에서,
   해당 패킷을 전달해야 하는 인터페이스의 MTU가 패킷 크기보다 작을 경우,
   패킷을 폐기하고 ICMPv6 오류 메시지를 송신 호스트로 전송합니다.
   이 메시지에는 전달에 실패한 인터페이스의 MTU 값이 포함됩니다.
3) 송신 호스트는 오류 메시지를 수신한 후,
   메시지에 포함된 MTU 값을 기준으로 다시 패킷을 분할하여 전송합니다.
4) 목적지 호스트가 패킷을 정상적으로 수신할 때까지 위 과정을 반복하며,
   이를 통해 송신지에서 목적지까지의 경로 상에서 최소 MTU 값이 결정됩니다.

27.1.5. 프로토콜 규격 (Protocol Specification)

IPv6 기본 기술과 관련된 주요 프로토콜 규격은 다음과 같습니다.

- RFC 1881: IPv6 주소 할당 관리
- RFC 1887: IPv6 유니캐스트 주소 할당 아키텍처
- RFC 1981: IPv6 경로 MTU 탐색(Path MTU Discovery)
- RFC 2375: IPv6 멀티캐스트 주소 할당
- RFC 2460: IPv6(Internet Protocol Version 6) 규격
- RFC 2461: IPv6 이웃 탐색(Neighbor Discovery)
- RFC 2462: IPv6 Stateless 주소 자동 설정
- RFC 2463: IPv6용 ICMP(Internet Control Message Protocol) 규격
- RFC 2464: Ethernet 네트워크에서의 IPv6 패킷 전송
- RFC 2526: 예약된 IPv6 서브넷 Anycast 주소
- RFC 3307: IPv6 멀티캐스트 주소 할당 가이드라인
- RFC 3513: IPv6 주소 구조(Addressing Architecture)
- RFC 3596: IPv6 지원을 위한 DNS 확장

27.2. IPv6 기본 구성 작업 개요

IPv6의 기본 기능 구성에는 다음 항목이 포함됩니다.

- IPv6 기본 기능 구성
- IPv6 Neighbor Discovery Protocol 구성
- PMTU Discovery 구성
- ICMPv6 메시지 송신 설정

27.3. IPv6 기본 기능 구성

27.3.1. IPv6 유니캐스트 주소 구성

IPv6 글로벌 유니캐스트 주소는 수동으로 할당됩니다.

IPv6 링크-로컬 주소는 다음 두 가지 방법으로 생성됩니다.

- 자동 생성: VLAN 포트가 UP 상태가 되면, 장비는 링크-로컬 주소 프리픽스(FE80::/10)와 인터페이스의 링크 계층 주소(MAC 주소)를 기반으로 자동으로 링크-로컬 주소를 생성합니다.
- 수동 설정: 사용자가 직접 IPv6 링크-로컬 주소를 설정합니다.

27.4. IPv6 Neighbor Discovery Protocol 구성

Command	설명	CLI Mode
ipv6 address <ipv6-address>/<prefix-length>	IPv6 주소를 수동으로 설정합니다. 기본적으로 링크-로컬 주소는 VLAN 인터페이스의 MAC 주소를 기반으로 Layer 3 인터페이스에서 자동 생성됩니다.	Configuration Mode

27.4.1. RA 메시지 관련 파라미터 구성

사용자는 실제 환경에 따라 인터페이스에서 RA 메시지 전송 여부와 전송 주기를 설정할 수 있습니다. 또한 RA 메시지에 포함될 다양한 파라미터를 설정하여 호스트에 전달할 수 있으며, 호스트는 RA 메시지를 수신한 후 해당 파라미터를 기반으로 동작합니다.

RA 메시지에서 설정 가능한 주요 파라미터와 의미는 아래와 같습니다.

Parameter	설명
Cur Hop Limit	호스트가 IPv6 패킷을 전송할 때 Hop Limit 필드에 설정되는 값이며, 장비의 응답 메시지에서도 동일하게 사용됩니다.
Prefix Information	동일 링크상의 호스트가 이 정보를 수신하면 Stateless 자동 설정 등의 동작을 수행할 수 있습니다.
Managed address configuration flag bit (M flag)	호스트가 Stateful 자동 설정(DHCP 등)을 통해 IPv6 주소를 획득할지 여부를 결정합니다. 1이면 Stateful 방식, 0이면 Stateless 방식 사용
Other configuration flag bit (O flag)	IPv6 주소 외의 추가 정보를 Stateful 방식으로 획득할지 여부를 결정합니다. 1이면 DHCP 등 사용
Router Lifetime	해당 RA 메시지를 보낸 라우터를 기본 게이트웨이로 사용할 시간
Retrans Timer	NS 메시지 전송 후 응답이 없을 경우 재전송까지 대기 시간
Reachable Time	이웃이 도달 가능하다고 판단된 후 유지되는 시간
Link MTU	링크 상 모든 노드가 동일한 MTU를 사용하도록 지정

Hop Limit 설정

- Command: ipv6 nd cur-hop-limit value
- Mode: VLAN Interface Mode
- 기본값: 64

RA 메시지 송신 활성화

- Command: ipv6 nd send-ra
- Mode: VLAN Interface Mode
- 기본값: RA 메시지 송신 비활성화

RA 메시지 송신 주기 설정

- 최대 간격
  Command: ipv6 nd max-ra-interval value
  기본값: 600초
- 최소 간격
  Command: ipv6 nd min-ra-interval value
  기본값: 198초
- 참고 사항
  실제 전송 간격은 최소값~최대값 사이에서 랜덤하게 결정됨
  최소값은 최대값의 0.75 이하로 설정해야 함

RA 메시지 Prefix 정보 설정

- Command:
  ipv6 nd prefix X:X::X:X/M (valid-lifetime preferred-lifetime (off-link | no-autoconfig))
- Mode: VLAN Interface Mode
- 기본값: 미설정 시 인터페이스 IPv6 주소가 Prefix로 사용됨

M Flag 설정

- Command: ipv6 nd managed-config-flag
- Mode: VLAN Interface Mode
- 기본값: 0 (Stateless 방식)

O Flag 설정

- Command: ipv6 nd other-config-flag
- Mode: VLAN Interface Mode
- 기본값: 0 (Stateless 방식)

Router Lifetime 설정

- Command: ipv6 nd ra-lifetime value
- Mode: VLAN Interface Mode
- 기본값: 1800초

NS 재전송 간격 설정

- Command: ipv6 nd base retrans-timer value
- Mode: Configuration Mode
- 기본값: 1000ms

RA 메시지 내 Retrans Timer 설정

- Command: ipv6 nd retrans-timer value
- Mode: VLAN Interface Mode
- 기본값: 0

이웃 도달 가능 시간 설정 (Global)

- Command: ipv6 nd base reachable-time value
- Mode: Configuration Mode
- 기본값: 30000ms

이웃 도달 가능 시간 설정 (RA 메시지 포함)

- Command: ipv6 nd reachable-time value
- Mode: VLAN Interface Mode
- 기본값: 0

Link MTU 설정

- Command: ipv6 nd link-mtu value
- Mode: VLAN Interface Mode
- 기본값: 0

27.4.2. 중복 주소 검출 시 Neighbor Solicitation 메시지 전송 횟수 설정

인터페이스는 IPv6 주소를 획득한 후, 중복 주소 검출(DAD)을 위해 Neighbor Solicitation(NS) 메시지를 전송합니다. 지정된 시간(ipv6 nd retrans-timer 명령으로 설정됨) 내에 응답을 받지 못하면, 인터페이스는 NS 메

시지를 계속 전송합니다.

설정된 전송 횟수만큼 NS 메시지를 전송한 이후에도 응답이 없을 경우, 해당 IPv6 주소는 사용 가능한 것으로 판단됩니다.

Command	설명	CLI Mode
ipv6 nd dad attempts <value>	중복 주소 검출(DAD) 시 Neighbor Solicitation(NS) 메시지 전송 횟수를 설정합니다. 기본값은 1이며, 값이 0이면 중복 주소 검출 기능이 비활성화됩니다.	Configuration Mode

27.5. IPv6 정적 라우트 설정

IPv6 정적 라우트는 관리자가 목적지 네트워크에 대한 경로를 수동으로 설정할 때 사용됩니다.

Command	설명	CLI Mode
ipv6 route <X:X::X:X/M> (<X:X::X:X> | <ifName>) <distance>	IPv6 정적 라우트를 설정합니다. 목적지 네트워크에 대해 다음 홉 주소 또는 인터페이스를 지정하고, distance 값으로 경로 우선순위를 설정합니다.	Configuration Mode

27.6. IPv6 표시 및 유지보수

위 설정이 완료된 후, 특권 모드(Privileged Mode)에서 show 명령어를 실행하여 IPv6 동작 상태를 확인할 수 있습니다.

표시된 정보를 통해 설정이 정상적으로 적용되었는지 검증할 수 있습니다.

Command	설명	CLI Mode
show ipv6 ndp nc	이웃(Neighbor) 정보를 표시합니다.	Privileged Mode
show ipv6 interface (<ifName>) brief	IPv6 주소가 설정된 인터페이스의 정보를 간략히 표시합니다.	Privileged Mode
show ipv6 route (database)	IPv6 라우팅 정보를 표시합니다.	Privileged Mode

28. MLD SNOOPING 설정

네트워크 환경에서 동일한 데이터를 여러 수신자에게 유니캐스트 방식으로 전송할 경우, 각 수신자마다 패킷을 복제하여 전송해야 하므로 수신자 수가 증가함에 따라 전송해야 하는 패킷 수가 선형적으로 증가합니다. 이는 호스트, 스위치/라우팅 장비, 그리고 네트워크 대역폭 자원에 전체적인 부담을 증가시키며, 결과적으로 전송 효율이 크게 저하됩니다.

최근 다자간 화상회의, 주문형 비디오(VoD), 그룹 통신과 같은 서비스 수요가 증가함에 따라, 자원 활용 효율을 높이기 위한 방법으로 멀티캐스트 전송 방식이 점점 더 중요해지고 있습니다.

스위치는 멀티캐스트 애플리케이션을 지원하기 위해 MLD SNOOPING 기능을 제공합니다.

MLD SNOOPING은 네트워크 상의 MLD 패킷을 감시하여 IPv6 멀티캐스트 MAC 주소를 동적으로 학습하는 기능입니다.

본 장에서는 MLD SNOOPING의 개념 및 설정 방법에 대해 설명하며, 주요 내용은 다음과 같습니다.

- MLD SNOOPING 개요
- MLD SNOOPING 설정
- SNOOPING 설정 예제

28.1. MLD SNOOPING 개요

기존 네트워크에서는 멀티캐스트 패킷이 서브넷 내에서 브로드캐스트처럼 처리되기 때문에, 불필요한 트래픽 증가와 네트워크 혼잡을 유발하기 쉽습니다.

스위치에서 MLD SNOOPING 기능을 활성화하면, 스위치는 IPv6 멀티캐스트 MAC 주소를 동적으로 학습하고 해당 MAC 주소에 대한 출력 포트 목록을 유지합니다. 이를 통해 멀티캐스트 데이터 스트림을 필요한 포트로만 전달하게 되어 네트워크 트래픽을 효과적으로 줄일 수 있습니다.

본 절에서는 다음 내용을 중심으로 설명합니다.

- MLD SNOOPING 동작 과정
- Layer 2 동적 멀티캐스트
- 그룹 가입 (Join)
- 그룹 탈퇴 (Leave)

28.1.1. MLD SNOOPING 동작 과정

MLD SNOOPING은 스위치를 통과하는 MLD 프로토콜 패킷을 모니터링하는 Layer 2 프로토콜입니다. 스위치는 MLD 패킷의 수신 포트, VLAN ID, 멀티캐스트 주소를 기반으로 멀티캐스트 그룹을 유지하며, 이후 해당 정보를 기반으로 패킷을 전달합니다.

멀티캐스트 그룹에 가입된 포트만 멀티캐스트 데이터 스트림을 수신할 수 있으므로, 불필요한 트래픽을 줄이고 네트워크 대역폭을 절약할 수 있습니다.

멀티캐스트 그룹은 다음 정보를 포함합니다.

- 멀티캐스트 그룹 주소
- 멤버 포트
- VLAN ID
- Age 시간

MLD SNOOPING의 멀티캐스트 그룹 생성은 학습 과정(Learning Process)을 통해 이루어집니다.

- 스위치의 포트가 MLD REPORT 패킷을 수신하면
  → 새로운 멀티캐스트 그룹이 생성되고
  → 해당 포트가 그룹에 추가됩니다
- 스위치가 MLD QUERY 패킷을 수신할 경우
  → 이미 해당 멀티캐스트 그룹이 존재하면, 해당 포트도 그룹에 추가됩니다
  → 그룹이 존재하지 않으면, QUERY 패킷은 단순히 전달됩니다

MLD SNOOPING은 MLDv2의 Done 메커니즘도 지원합니다.

- Fast-leave 기능이 활성화된 경우
  → Done 패킷 수신 즉시 해당 포트는 멀티캐스트 그룹에서 제거됩니다
- Fast-leave-timeout이 설정된 경우
  → 설정된 시간 동안 대기한 후 그룹에서 제거됩니다

MLD SNOOPING에는 두 가지 업데이트 방식이 있습니다.

1) Done 메커니즘
2) Age Time 기반 삭제

일반적으로는 Age Time을 기반으로 멀티캐스트 그룹이 삭제됩니다.

- 멀티캐스트 그룹이 생성될 때 가입 시간이 기록됨
- 설정된 Age Time을 초과하면 자동으로 삭제됨

Fast Leave 관련 동작 주의사항

포트가 Done 패킷을 수신하면 해당 포트는 즉시 멀티캐스트 그룹에서 제거됩니다.

하지만 이 경우 네트워크 데이터 흐름의 연속성에 영향을 줄 수 있습니다.

예를 들어:

- 해당 포트에 HUB 또는 MLD SNOOPING 미지원 장비가 연결된 경우
- 하나의 장비에서 Done을 보내면
  → 동일 장비 뒤에 연결된 다른 수신 장비들도 영향을 받을 수 있음

Fast-leave-timeout의 역할

이 문제를 방지하기 위해 Fast-leave-timeout 기능을 사용할 수 있습니다.

- Leave 패킷 수신 후 즉시 제거하지 않고
- 설정된 시간만큼 대기 후 그룹에서 제거

이를 통해 멀티캐스트 데이터 스트림의 연속성을 보장할 수 있습니다.

28.1.2. Layer 2 동적 멀티캐스트

Layer 2 하드웨어 멀티캐스트 포워딩 테이블의 멀티캐스트 MAC 주소 엔트리는 MLD SNOOPING을 통해 동적으로 학습될 수 있습니다. IPv6 멀티캐스트 MAC 주소는 MLD SNOOPING을 통해 자동으로 학습됩니다.

스위치에서 MLD SNOOPING이 비활성화된 경우, Layer 2 하드웨어 멀티캐스트 포워딩 테이블은

Unregistered Forwarding 모드로 동작합니다. 이 상태에서는 멀티캐스트 MAC 주소를 동적으로 학습할 수 없으며, 포워딩 테이블에 엔트리가 존재하지 않습니다. 따라서 모든 Layer 2 멀티캐스트 트래픽은 브로드캐스트처럼 처리됩니다.

반대로, 네트워크에 멀티캐스트 환경이 존재할 경우 트래픽을 효율적으로 제어하기 위해 스위치에서 MLD SNOOPING을 활성화할 수 있습니다. 이때 Layer 2 하드웨어 멀티캐스트 포워딩 테이블은 Registered Forwarding 모드로 동작하게 됩니다.

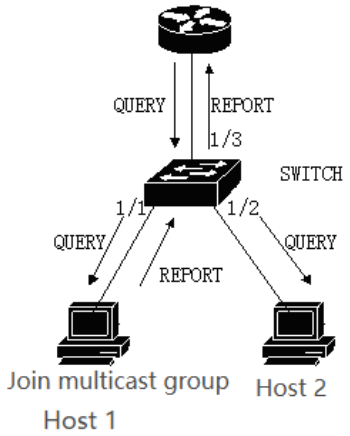
이 모드에서는 스위치가 네트워크 상의 MLD 프로토콜 패킷을 모니터링하여 멀티캐스트 MAC 주소를 학습하며, Layer 2 하드웨어 멀티캐스트 포워딩 테이블에 등록된 엔트리와 일치하는 멀티캐스트 트래픽만 전달됩니다.

28.1.3. 그룹 가입 (Join a group)

호스트가 멀티캐스트 그룹에 가입하려면, 가입하려는 멀티캐스트 그룹을 명시한 MLD REPORT 패킷을 전송합니다.

스위치는 MLD QUERY 패킷을 수신하면 동일 VLAN 내의 다른 모든 포트로 해당 패킷을 전달합니다. 멀티캐스트 그룹에 가입하려는 호스트는 MLD QUERY 패킷을 수신한 후 MLD REPORT 패킷을 응답으로 전송합니다.

스위치가 MLD REPORT 패킷을 수신하면 Layer 2 멀티캐스트 엔트리를 생성하며, MLD QUERY 패킷을 수신한 포트와 MLD REPORT 패킷을 수신한 포트를 해당 멀티캐스트 엔트리의 출력 포트로 추가합니다.



동작 예시

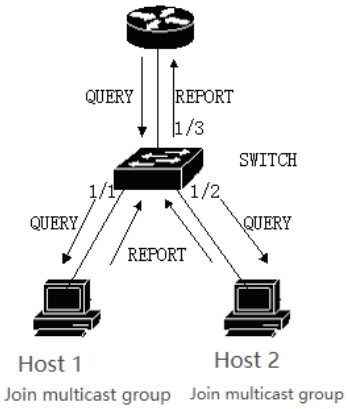
위 그림과 같이 모든 장비가 하나의 서브넷에 있으며, 해당 VLAN은 2라고 가정합니다.

라우터는 MLDv2 프로토콜을 사용하여 주기적으로 MLD QUERY 패킷을 전송합니다.

- Host 1은 멀티캐스트 그룹 ff15::1에 가입하려고 합니다.
- 스위치는 포트 1/3에서 MLD QUERY 패킷을 수신하고, 해당 포트를 기록한 뒤 포트 1/1과 1/2로 패킷을 전달합니다.

- Host 1은 MLD QUERY 패킷을 수신한 후 MLD REPORT 패킷을 전송합니다.
- Host 2는 그룹에 가입하지 않기 때문에 MLD REPORT를 전송하지 않습니다.

스위치는 포트 1/1에서 MLD REPORT 패킷을 수신하면 이를 포트 1/3으로 전달하고, 다음과 같은 Layer 2 멀티캐스트 엔트리를 생성합니다.



Layer 2 multicast addr	VLAN ID	List of output ports
33:33:00:00:00:01	2	1/1, 1/3

이후 동일한 환경에서 Host 1이 이미 그룹에 가입된 상태에서, Host 2도 동일한 멀티캐스트 그룹 ff15::1에 가입하려고 한다고 가정합니다.

- Host 2가 MLD QUERY 패킷을 수신한 후 MLD REPORT 패킷을 전송하면
- 스위치는 포트 1/2에서 해당 패킷을 수신하고, 이를 포트 1/3으로 전달한 후
- 포트 1/2를 기존 멀티캐스트 엔트리에 추가합니다

그 결과, 멀티캐스트 엔트리는 다음과 같이 변경됩니다.

Layer 2 multicast addr	VLAN ID	List of output ports
33:33:5e:00:00:01	2	1/1, 1/2, 1/3

28.1.4. 그룹 탈퇴 (Leave a group)

안정적인 멀티캐스트 환경을 유지하기 위해, MLD를 동작하는 장비(예: 라우터)는 일정 주기로 모든 호스트에게 MLD QUERY 패킷을 전송합니다. 멀티캐스트 그룹에 가입한 호스트 또는 가입하려는 호스트는 이 QUERY를 수신하면 MLD REPORT 패킷으로 응답합니다.

호스트가 멀티캐스트 그룹을 탈퇴하는 방법에는 두 가지가 있습니다.

- 능동적 탈퇴 (Active Leave): 호스트가 라우터로 MLD LEAVE 패킷을 전송

- 수동적 탈퇴 (Passive Leave): 호스트가 QUERY를 수신해도 MLD REPORT를 보내지 않음

호스트의 탈퇴 방식에 따라, 스위치 포트가 Layer 2 멀티캐스트 엔트리에서 제거되는 방식도 두 가지가 있습니다.

- 타임아웃 기반 탈퇴 (Timeout Leaving)
- MLD Done 패킷 수신 기반 탈퇴 (Done Packet Leaving)

동작 방식

- 특정 포트에서 일정 시간 동안 해당 멀티캐스트 그룹에 대한 MLD REPORT 패킷이 수신되지 않으면
  → 해당 포트는 Layer 2 멀티캐스트 엔트리에서 제거됩니다
  → 엔트리에 남은 포트가 없으면 해당 멀티캐스트 엔트리는 삭제됩니다
- 스위치에서 Fast-leave 기능이 활성화된 경우
  → 포트가 멀티캐스트 그룹의 MLD LEAVE(Done) 패킷을 수신하면 즉시 해당 포트를 엔트리에서 제거합니다
  → 엔트리에 포트가 없으면 엔트리는 삭제됩니다

Fast-leave 사용 시 주의사항

Fast-leave 기능은 일반적으로 포트에 단일 호스트가 연결된 경우에 적합합니다.

하나의 포트에 여러 호스트가 연결되어 있는 경우에는, fast-leave-timeout 대기 시간을 설정하여 즉시 제거되지 않도록 해야 합니다.

이를 통해 멀티캐스트 스트림의 연속성과 안정성을 유지할 수 있습니다.

28.2. MLD SNOOPING 설정

28.2.1. MLD SNOOPING 기본 설정

MLD SNOOPING 기능은 기본적으로 비활성화되어 있으며, 이 경우 Layer 2 하드웨어 멀티캐스트 포워딩 테이블은 Unregistered Forwarding 모드로 동작합니다.

기본 설정 값은 다음과 같습니다.

- MLD SNOOPING: 비활성화 (OFF)
- Fast-leave: 비활성화 (OFF)
- Fast-leave-timeout: 300초
- 멀티캐스트 그룹 REPORT 포트의 기본 Age Time: 400초
- 멀티캐스트 그룹 QUERY 포트의 기본 Age Time: 300초

28.2.2. MLD SNOOPING 활성화 및 비활성화

MLD SNOOPING 프로토콜은 전역(Global) 단위로 활성화할 수도 있고, 특정 VLAN에 대해서만 개별적으로 설정할 수도 있습니다.

단, VLAN 단위에서 MLD SNOOPING을 설정하려면 먼저 전역 MLD SNOOPING이 활성화되어 있어야 합니다.

전역 MLD SNOOPING 활성화

Switch# configure terminal

Switch(config)# ipv6 mld snooping

특정 VLAN에서 MLD SNOOPING 활성화

Switch# configure terminal

Switch(config)# ipv6 mld snooping vlan <vlan-id>

전역 MLD SNOOPING 비활성화

Switch# configure terminal

Switch(config)# no ipv6 mld snooping

특정 VLAN에서 MLD SNOOPING 비활성화

Switch# configure terminal

Switch(config)# no ipv6 mld snooping vlan <vlan-id>

28.2.3. Lifetime 설정

멀티캐스트 그룹 Lifetime 설정

멀티캐스트 그룹의 유지 시간을 설정합니다.

Switch# configure terminal

Switch(config)# ipv6 mld snooping group-membership-timeout <interval> vlan <vlan-id>

- interval 값은 밀리초(ms) 단위입니다.

Query 그룹 Lifetime 설정

Query 기반 멤버십의 유지 시간을 설정합니다.

Switch# configure terminal

Switch(config)# ipv6 mld snooping query-membership-timeout <interval> vlan <vlan-id>

- interval 값은 밀리초(ms) 단위입니다.

28.2.4. Fast-leave 설정

특정 VLAN에서 Fast-leave 활성화

Switch# configure terminal

Switch(config)# ipv6 mld snooping fast-leave vlan <vlan-id>

Fast-leave 비활성화

Switch# configure terminal

Switch(config)# no ipv6 mld snooping fast-leave vlan <vlan-id>

Fast-leave 대기 시간 설정

Switch# configure terminal

Switch(config)# ipv6 mld snooping fast-leave-timeout <interval> vlan <vlan-id>

Fast-leave 대기 시간 기본값 복원

Switch# configure terminal

Switch(config)# no ipv6 mld snooping fast-leave-timeout vlan <vlan-id>

28.2.5. MROUTER 설정

정적 Query 포트 설정

Switch# configure terminal

Switch(config)# interface ge1/6

Switch(config-ge1/6)# ipv6 mld snooping mrouter vlan [vlan-id]

28.2.6. VLAN Querier 기능 설정

VLAN 1에서 Querier 기능 활성화

특정 VLAN에서 MLD Querier 기능을 활성화합니다.

Switch# configure terminal

Switch(config)# ipv6 mld snooping querier vlan 1

28.2.7. 정보 확인 (Display Information)

MLD SNOOPING 설정 정보 확인

Switch# show ipv6 mld snooping

특정 VLAN 설정 정보 확인

Switch# show ipv6 mld snooping vlan <vlan-id>

REPORT 기반 멀티캐스트 그룹 Aging 정보 확인

Switch# show ipv6 mld snooping age-table group-membership

QUERY 기반 Aging 정보 확인

Switch# show ipv6 mld snooping age-table query-membership

멀티캐스트 그룹 포워딩 정보 확인

Switch# show ipv6 mld snooping forwarding-table

MROUTER 정보 확인

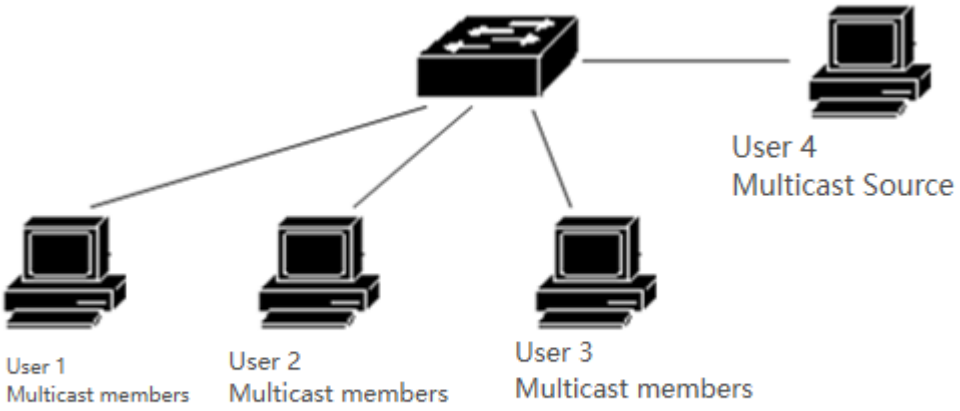
Switch# show ipv6 mld snooping mrouter

시스템 전체 설정 확인 (MLD SNOOPING 포함)

Switch# show running-config

28.3. MLD SNOOPING 설정 예제

스위치에서 MLD SNOOPING 기능을 활성화하고, User 1, User 2, User 3이 특정 멀티캐스트 그룹에 가입할 수 있도록 설정하는 예제입니다.



Switch# config t

Switch(config)# vlan database

Switch(config-vlan)# vlan 200

Switch(config)# ipv6 mld snooping

Switch(config)# interface ge1/1

Switch(config-ge1/1)# switchport mode access

Switch(config-ge1/1)# switchport access vlan 200

Switch(config)# interface ge1/2

Switch(config-ge1/2)# switchport mode access

Switch(config-ge1/2)# switchport access vlan 200

```
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode access
Switch(config-ge1/3)# switchport access vlan 200

Switch(config)# ipv6 mld snooping group-membership-timeout 60000 vlan 200
```

설명

- VLAN 200을 생성하고 해당 VLAN에 사용자 포트를 할당합니다.
- MLD SNOOPING 기능을 전역으로 활성화합니다.
- 각 포트(ge1/1 ~ ge1/3)를 Access 모드로 설정하고 VLAN 200에 연결합니다.
- VLAN 200에서 멀티캐스트 그룹의 유지 시간(Timeout)을 60000ms로 설정합니다.

이를 통해 해당 VLAN에 연결된 사용자들이 멀티캐스트 그룹에 정상적으로 가입하고, 효율적으로 멀티캐스트 트래픽을 수신할 수 있습니다.

29. PoE 설정

본 스위치는 PoE(Power over Ethernet) 기능을 지원하며, 주요 내용은 다음과 같습니다.

- PoE 개요
- PoE 설정

29.1. PoE 개요

PoE(Power over Ethernet, 원격 전원 공급)는 이더넷 인터페이스를 통해 트위스트 페어 케이블을 사용하여 외부 PD(Powered Device) 장비(IP 전화기, 무선 AP, 네트워크 카메라 등)에 전원을 공급하는 기술입니다.

1) PoE의 장점
   - 신뢰성: 중앙 집중식 전원 공급으로 백업이 용이함
   - 간편한 연결: 네트워크 단말에 별도의 전원 공급이 필요 없으며, 하나의 LAN 케이블만으로 전원과 데이터 전송 가능
   - 표준화: IEEE 802.3af 및 802.3at 표준을 준수하며, 글로벌 통합 전원 인터페이스 사용
   - 확장성: IP 전화기, 무선 AP(Access Point), 휴대용 장치 충전기, 카드 리더기, 네트워크 카메라, 데이터 수집 장비 등 다양한 분야에 적용 가능

2) PoE 시스템 구성
   PoE 시스템은 PoE 전원 공급 장치, PSE, PD로 구성됩니다.

PoE 전원 공급 장치

PoE 시스템 전체에 전원을 공급하며, 다음 두 가지 형태로 구분됩니다.

- 외장형 전원 공급
- 내장형 전원 공급

PSE (Power Sourcing Equipment)

PSE는 전원을 공급하는 장비(보드 또는 모듈)입니다.

- 각 PSE는 해당 보드(또는 모듈)의 PoE 인터페이스를 독립적으로 관리
- PoE 인터페이스에 연결된 PD를 탐지, 식별, 분류 및 전원 공급 수행
- PD가 분리되면 전원 공급을 중단

PoE 전원을 지원하는 이더넷 인터페이스는 PoE 인터페이스라고 하며, FE 및 GE 포트를 포함합니다.

PD (Powered Device)

PD는 PSE로부터 전원을 공급받는 장비입니다.

- 표준 PD는 IEEE 802.3af 및 802.3at 규격을 준수
- PoE 전원과 함께 별도의 전원 공급을 동시에 사용할 수 있어 이중화(백업) 구성이 가능

29.2. PoE 설정

PoE 설정은 다음 세 가지 항목으로 구성됩니다.

- 수동 PoE 설정
- PoE 정책 설정
- PD 조회 설정

29.2.1. 수동 PoE 설정

수동 PoE 설정에서는 다음 기능을 수행할 수 있습니다.

- 인터페이스의 PoE 전원 공급 활성화/비활성화
- PoE 상태 정보 확인

Command	설명	CLI Mode
[no] poe enable	인터페이스의 PoE 전원 공급을 활성화 또는 비활성화합니다. 기본적으로 인터페이스의 전원 공급 상태는 활성화(On)입니다.	Interface Configuration Mode
show poe	모든 인터페이스의 PoE 정보를 표시합니다.	User Mode 또는 Privileged Mode

29.2.2. PoE 정책 설정

PoE 정책 설정에서는 다음 기능을 수행할 수 있습니다.

- 인터페이스의 PoE 정책 활성화/비활성화
- 인터페이스의 PoE 정책 항목 설정
- PoE 정책 정보 조회

Command	설명	CLI Mode
[no] poe policy enable	인터페이스의 PoE 정책을 활성화 또는 비활성화합니다. 기본적으로 인터페이스 PoE 정책은 비활성화 상태입니다.	Interface Configuration Mode
[no] poe policy shutdown clock <clock-value> week-day <day-value>	인터페이스에 PoE 정책 항목을 설정하거나 삭제합니다. 이 명령어는 여러 번 설정할 수 있습니다. 기본적으로 PoE 정책 항목은 설정되어 있지 않습니다.<clock-value>는 24시간 형식의 시간 또는 시간 범위를 의미합니다. 예를 들어 1은 1시부터 2시 사이를 의미하며, 20-23은 20시부터 24시 사이를 의미합니다.<day-value>는 요일을 의미하며, 특정 요일 또는 연속된 요일 범위를 지정할 수 있습니다. 예를 들어 3은 수요일, 1-7은 월요일부터 일요일까지를 의미합니다.PoE 정책은 해당 인터페이스의 PoE 정책이 활성화된 경우에만 적용됩니다.	Interface Configuration Mode
show poe policy <if-name>	특정 인터페이스의 PoE 정책 정보를 표시합니다.	User mode 또는 Privileged mode

29.2.3. PD 조회 설정

PD 조회 설정에서는 다음 기능을 수행할 수 있습니다.

- PD의 IP 주소 설정
- PD 조회 주기 설정
- PD 조회 타임아웃 횟수 설정
- PD 재부팅(시작) 시간 설정
- PD 정보 조회

Command	설명	CLI Mode
poe pd-ip-address <ip-address>no poe pd-ip-address	인터페이스에 연결된 PD의 IP 주소를 설정하거나 삭제합니다. 기본적으로 PD의 IP 주소는 설정되어 있지 않습니다.IP 주소가 설정되면 시스템은 해당 주소로 주기적으로 조회를 수행하며, 지정된 횟수만큼 응답이 없을 경우 PoE 제어를 통해 PD를 재시작합니다.	Interface Configuration Mode

Command	설명	CLI Mode
poe pd-query-interval <interval>no poe pd-query-interval	PD 조회 주기를 설정합니다. 기본값은 5초입니다.	Interface Configuration Mode
poe pd-timeout-number <number>no poe pd-timeout-number	PD 조회 타임아웃 횟수를 설정합니다. 기본값은 3회입니다.	Interface Configuration Mode
poe pd-boot-time <time>no poe pd-boot-time	PD의 재시작(부팅) 시간을 설정합니다. 기본값은 120초입니다.	Interface Configuration Mode
show poe pd-information	설정된 모든 PD의 정보를 표시합니다.	User mode 또는 Privileged mode

30. GVRP 설정

본 장에서는 다음 내용을 중심으로 설명합니다.

- GVRP 개요
- GVRP 설정
- GVRP 정보 확인

30.1. GVRP 개요

GVRP는 IEEE 802.1p 표준에 정의된 프로토콜로, 802.1Q VLAN을 제어할 수 있도록 합니다.

GVRP를 지원하는 스위치들은 서로 VLAN 구성 정보를 교환할 수 있으며, 불필요한 브로드캐스트 및 Unknown 유니캐스트 트래픽을 줄이고, 802.1Q 트렁크로 연결된 스위치 간에 VLAN을 동적으로 생성하고 관리할 수 있습니다.

GVRP는 GARP 기반 애플리케이션을 위해 일반 상태 메커니즘을 제공하는 GID와, 공통 정보 전파 메커니즘을 제공하는 GIP를 사용합니다. GVRP는 802.1Q 트렁크 링크에서만 동작합니다.

GVRP는 트렁크 링크에서 활성화된 VLAN만 전달되도록 하여 불필요한 VLAN 트래픽을 제거합니다. 트렁크에 VLAN을 추가하기 위해서는 먼저 스위치로부터 Join 메시지를 수신해야 합니다. 또한 GVRP의 업데이트 정보와 타이머 값은 변경이 가능합니다.

GVRP 포트는 여러 가지 동작 모드를 가지며, 이를 통해 VLAN의 필터링(트리밍) 동작을 제어할 수 있습니다. GVRP는 VLAN 데이터베이스를 기반으로 VLAN을 동적으로 추가하고 관리할 수 있는 기능을 제공합니다.

즉, GVRP는 장비 간 VLAN 정보를 자동으로 전파하는 기능을 제공합니다. 하나의 스위치에 VLAN 정보를 수동으로 설정하면, 네트워크 내의 다른 스위치들은 해당 VLAN 정보를 동적으로 학습할 수 있습니다.

단말 장치는 네트워크 내 어느 스위치에 연결되더라도 원하는 VLAN에 접속할 수 있습니다. 이를 위해 단말 장치에는 GVRP를 지원하는 네트워크 인터페이스 카드(NIC)가 필요합니다. GVRP 지원 NIC는 원하는 VLAN에 가입하도록 설정할 수 있으며, GVRP가 활성화된 스위치에 연결되면 NIC와 스위치 간 통신이 이루어지고 VLAN 연결이 자동으로 구성됩니다.

30.2. GVRP 설정

GVRP의 주요 설정 항목은 다음과 같습니다.

- RP 활성화
- GVRP 상태 확인

설정 작업 시, 먼저 전역(Global) GVRP를 활성화한 후에 포트 단위 GVRP를 활성화할 수 있습니다.

30.2.1. GVRP 설정 활성화

Command	설명	Configuration Mode
set gvrp enable | disable	모든 VLAN에 대해 전역 GVRP를 활성화 또는 비활성화합니다.	Global configuration mode
set gvrp applicant state active | normal	전역 GVRP Applicant 상태를 활성화합니다.	Global configuration mode
set gvrp dynamic-vlan-creation enable | disable	전역 동적 VLAN 생성 기능을 활성화 또는 비활성화합니다.	Global configuration mode
Set gvrp registration {fixed | forbidden | normal} <if-name>	해당 인터페이스의 GVRP 등록 모드를 설정합니다.	Global configuration mode
set gvrp timer {join | leave | nleaveall} <time-value>	GVRP의 각종 타이머 시간을 설정합니다.	Global configuration mode
set port gvrp enable <if-name>	지정한 포트에서 GVRP 기능을 활성화합니다.	Global configuration mode
set port gvrp disable <if-name>	지정한 포트에서 GVRP 기능을 비활성화합니다.	Global configuration mode

30.2.2. GVRP 정보 확인

위 설정이 완료된 후, 특권 모드(Privileged Mode)에서 show 명령어를 실행하여 GVRP의 동작 상태를 확인할 수 있습니다.

표시되는 정보를 통해 설정이 정상적으로 적용되었는지 검증할 수 있습니다.

Command	설명	Configuration Mode
show gvrp configuration	GVRP 설정 정보를 확인합니다.	Privileged mode
show gvrp machine	GVRP 상태 머신 정보를 확인합니다.	Privileged mode

Command	설명	Configuration Mode
show gvrp statistics vlanid	특정 VLAN ID의 GVRP 통계 정보를 확인합니다.	Privileged mode
show gvrp timer <ifname>	특정 포트의 타이머 정보를 확인합니다.	Privileged mode

4MITECH Co.,LTD

본사: 경기도 수원시 영통구 삼성로 274 팩토리월드 711-A호

지사: 서울특별시 강서구 공항대로 213 보타닉파크타워 2차 1002호

연구소: 서울특별시 금천구 가산디지털1로 205-15, SH드림타워 712호

연구소: 충남 천안시 동남구 문암로 76, 백석대학교 본부동 지하1층 B101, B101-1호

W. www.4mitech.co.kr T. 031-211-6561 F. 0505-210-6561