사 용 자 메 뉴 얼

NK-S_Switch_Manual

MIRAE SIGNAL

www.miraesignal.com

MIRAESIGNAL

목차

1. 제품 설치 34
1.1 설치 준비 34
1.2 랙 환경 설치 34
1.3 선반에 스위치 설치 35
2.4 전원선 연결 35
2.5 DC 전원 연결 (산업용 및 DC전원이 필요한경우) 36
2.6 UTP 및 SFP 연결 방법 36
2.7 콘솔 연결 방법 37
3. 설정 준비하기 38
3.1 스위치의 포트 번호 38
3.2 스위치 시작 전 준비 38
3.3 도움말 확인하기 39
3.4 Command 모드 39
3.5 Commnad 취소 40
3.6 설정 저정하기 40
4. CLI 명령어 규칙 41
4.1 규칙 41
5. 최초 로그인 및 인증 관리 42
5.1 콘솔 및 관리접속 로그인 42
5.2 비밀번호 규칙 설정 44
6. 터미널 설정 46
6.1 VTY 설정 46
6.2 설정 46
6.2.1 라인과 인터페이스의 관계 46
6.3 모니터 및 유지 관리 46

6.4 VTY 구성 예 47
7. 네트워크 관리 구성 48
7.1 SNMP 구성 48
7.1.1 개요 48
7.1.2 SNMP 구성 작업 49
7.1.3 설정 예시 54
7.2 RMON 구성 55
7.2.1 RMON 구성 작업 55
7.3 PDP 설정 59
7.3.1 개요 59
7.3.2 PDP 설정 예시 61
8. SSH 설정 62
9.1 개요 62
8.1.1 SSH 서버 62
8.1.2 SSH 클라이언트 62
8.1.3 기능 62
8.2 설정 62
8.2.1 인증 방법 목록 구성 62
9.2.2 액세스 제어 목록 구성 62
9.2.3 인증 시간 초과 값 구성 63
9.2.4 인증 재시도 시간 구성 63
9.2.5 SSH 서버 활성화 63
9.3 SSH 서버 설정 예시 63
9.3.1 Access control 리스트 63
9.3.2 글로벌 설정 64
9.3.3 인증 실패 및 접속 제한 64
9.4 Telnet 접속 64
9.4.1 Telnet 구성 64
9.4.2 telnet 기능 64

10 AAA 설정 65
10.4 AAA 개요 65
10.1.1 AAA 보안 서비스 65
10.1.2 AAA 사용시 이점 66
10.1.3 AAA 원칙 67
10.1.4 Method 리스트 67
10.5 AAA 구성 프로세스 69
1.2.1 AAA 구성 프로세스 개요 69
10.6 AAA 인증 구성 69
10.7 AAA 인증 구성 작업 70
10.7.1 AAA를 사용하여 로그인 인증 구성 70
10.7.2 권한 수준에 따른 암호 보호 활성화 72
10.7.3 AAA 인증을 위한 메시지 배너 구성 73
10.7.4 AAA 인증 사용자 username-prompt 73
10.7.5 AAA 인증 password-prompt 74
10.7.6 사용자 이름 인증 설정 74
10.7.7 패스워드 활성화 75
10.7.8 패스워드 규칙 설정 75
10.8 AAA 인증 구성 예제 76
10.8.1 RADIUS 인증 예제 76
10.9 AAA 권한 부여 구성 작업 목록 77
10.10 AAA 인증 구성 작업 77
10.10.1 AAA를 사용하여 EXEC 권한 부여 구성 77
10.11 AAA 권한 설정 예시 78
10.11.1 EXEC 로컬 권한 부여 예시 78
10.12 AAA 계정 구성 작업 목록 79
10.13 AAA 계정 구성 작업 79
10.13.1 AAA를 사용하여 계정 연결 구성 80
10.13.2 AAA를 사용하여 네트워크 계정 구성 80

10.13.3 AAA Accounting 업데이트 81
10.13.4 사용자 이름이 비어 있거나 null 값 81
11 RADIUS 설정 82
11.4 개요 82
11.4.1 RADIUS 란 82
11.4.2 RADIUS 동작 83
11.5 RADIUS 설정 순서 84
11.6 RADIUS 구성 작업 목록 84
11.7 RADIUS 구성 작업 84
11.7.1 RADIUS 서버 통신으로 스위치 구성 84
11.7.2 공급업체별 RADIUS 속성을 사용하도록 스위치 구성 85
11.7.3 RADIUS 인증 지정 86
11.7.4 RADIUS 권한 지정 86
11.7.5 RADIUS 계정 지정 86
11.8 RADIUS 설정 예시 86
11.8.1 RADIUS 응용 프로그램 예제 87
12 TACACS+ 설정 88
12.4 TACACS+ 개요 88
12.1.1 TACACS+ 프로토콜의 동작 88
12.5 TACACS+ 구성 프로세스 90
12.6 TACACS+ 구성 작업 목록 90
12.7 TACACS+ 구성 작업 90
12.7.1 ACACS+ 서버 할당 90
12.7.2 TACACS+ 암호화된 비밀 키 설정 91
12.7.3 TACACS+를 인증에 사용하도록 지정 92
12.7.4 TACACS+를 권한 부여에 사용하도록 지정 92
12.7.5 TACACS+를 계정 관리에 사용하도록 지정 92
12.8 TACACS+ 구성 예제 92
12.8.1 TACACS+ 인증 예제 92

12.8.2 TACACS+ 권한 부여 예시 93
12.8.3 TACACS+ 계정 관리 예제 94
12.9 802.1x 설정 목록 95
12.10 802.1.X 설정 작업 95
12.10.1 802.1x Port Authentication 설정 95
12.10.2 802.1x Multiple-host Port Authentication 설정 96
12.10.3 802.1x Re-authentication 설정 97
12.10.4 802.1x Re-authentication 횟수 설정 97
12.10.5 802.1x 전송 주기 설정 97
12.10.6 802.1x 사용자 바인딩 설정 97
12.10.7 802.1x 포트 인증 방식 설정 98
12.10.8 802.1x 포트 인증 유형 선택 98
12.10.9 802.1x 계정 설정 98
12.10.10 802.1x guest-vlan 설정 99
12.10.11 다중 네트워크 카드가 있는 Supplicant 금지 100
12.10.12 802.1x 기본 설정 복구 100
12.10.13 802.1x 인증 구성 및 상태 모니터링 100
12.11 802.1x 설정 예시 101
13 Interface 설정 소개 103
13.4 지원되는 인터페이스 유형 103
13.5 인터페이스 구성 소개 104
14 인터페이스 설정 106
14.4 인터페이스 공통속성 구성 106
14.2.1 설명 추가 106
14.4.1 대역폭 설정 106
14.4.2 시간 지연 설정 106
14.2 인터페이스 모니터링 및 유지 관리 107
14.2.1 인터페이스 상태 확인 107
14.2.2 인터페이스 초기화 및 삭제 107

14.2.3 인터페이스 종료 및 활성화 108
14.3 이더넷 인터페이스 설정 108
14.3.1 이더넷 인터페이스 설정 108
14.3.2 RATE 구성 108
14.3.3 인터페이스의 이중 모드 구성 109
14.3.4 인터페이스에서 Flow Control 구성 109
14.4 논리적 인터페이스 구성 110
14.4.1 Aggregation 인터페이스 구성 110
14.4.2 VLAN 인터페이스 구성 110
14.4.3 인터페이스 설명 예제 111
14.4.4 인터페이스 종료 예제 111
14.5 인터페이스 범위 구성 작업 112
14.5.1 인터페이스 범위의 이해 112
14.5.2 인터페이스 범위 모드 설정 112
14.5.3 설정 예제 112
15 포트 구성 113
15.2 이더넷 인터페이스 구성 113
15.2.1 이더넷 인터페이스 선택 113
15.2.2 Rate 구성 113
15.2.3 인터페이스에서 Flow Control 구성 114
15.2.4 Duplex 모드 설정 114
15.3 Port Isolation 114
15.4 Storm Control 115
15.5 포트 Rate 제한 116
15.6 포트 루프 감지 117
15.7 포트 MAC-address learning 117
15.8 포트 보안 117
15.9 인터페이스의 binding 118
15.10 SVL/IVL 119

15.11 링크 스캔 설정 119
15.11.1 개요 119
15.11.2 링크 스캔 구성 작업 120
15.11.3 설정 예시 120
15.12 포트 링크 상태 확인 구성 120
15.12.1 개요 120
15.12.2 구성 목록 120
15.10.4 설정 예제 121
15.13 시스템 MTU 구성 121
15.13.1 개요 121
15.13.2 구성 목록 121
15.13.3 설정 예시 121
15.14 Port Isolation 121
15.14.1 포트 미러링 구성 121
15.14.2 포트미러링 정보 표시 122
15.14.3 프토 미러링 예제 123
16 MAC 주소 125
16.1 MAC 주소 구성 작업 목록 125
16.2 MAC 주소 구성 작업 125
16.2.1 정적 MAC 주소 구성 125
16.2.2 MAC 주소 Aging 시간 구성 125
16.2.3 Blackhole MAC 주소 구성 126
16.2.4 MAC 주소 테이블 표시 126
16.2.5 동적 MAC 주소 삭제 127
16.3 MAC 액세스 리스트 구성 127
16.4 MAC 액세스 리스트 생성 127
16.5 MAC 액세스 리스트 항목 구성 128
16.6 MAC 액세스 리스트 적용 129
17. VLAN 구성 130

17.1 VLAN 소개 130
17.2 Dot1Q 터널 개요 130
17.2.1 서론 130
17.2.2 Dot1Q 터널 구현 모드 130
17.3 VLAN 구성 작업 목록 132
17.4 VLAN 구성 작업 132
17.4.1 VLAN 추가/삭제 132
17.4.2 스위치 포트 구성 132
17.4.3 VLAN 인터페이스 생성/삭제 133
17.4.4 VLAN 구성 및 상태 모니터링 134
17.4.5 글로벌 Dot1Q 터널 활성화/비활성화 134
17.5 Dot1Q 터널 구성 예제 134
17.5.1 Dot1Q 터널 구성 예제 134
17.6 Private VLAN 소개 136
17.7 Private VLAN의 유형 및 포트 유형 137
17.7.1 기본 VLAN 유형 137
17.7.2 보조 VLAN 유형 137
17.7.3 Private VLAN 포트에서의 포트 유형 137
17.7.4 VLAN 태그의 필드 수정 137
17.8 Private VLAN 구성 작업 목록 137
17.9 Private VLAN 구성 작업 138
17.9.1 Private VLAN 설정 138
17.9.2 Private VLAN 도메인 간 연관성 구성 138
17.9.3 Private VLAN의 2계층 포트를 호스트 포트로 설정 139
17.9.4 Private VLAN의 2계층 포트를 비차단 포트로 설정 139
17.9.5 Private VLAN에서 이그레스 패킷의 관련 필드 수정 140
17.9.6 Private VLAN의 구성 정보 표시 140
17.10 설정 예제 141
17.11 개요 143

17.12 구성 작업 목록 143
17.12.1 GVRP 구성 작업 목록 143
17.13 GVRP 구성 작업 144
17.13.1 GVRP 전체 활성화/비활성화 144
17.13.2 등록된 포트에서만 유효한 동적 VLAN 구성 144
17.13.3 인터페이스에서 GVRP 활성화/비활성화 144
17.13.4 GVRP 모니터링 및 유지보수 144
17.13.5 설정 예제 145
18. IP 프로토콜 구성 147
18.1 IP 개요 147
18.1.1 IP 147
18.2 IP 주소 구성 작업 목록 147
18.3 Configuring IP Address 147
18.3.1 네트워크 인터페이스에서 IP 주소 구성 147
18.3.2 네트워크 인터페이스에서 다중 IP 주소 구성 148
18.3.3 Address Resolution 구성 149
18.3.4 IP 주소 감지 및 유지 관리 152
18.3.5 IP 주소 설정 153
18.4 DHCP 구성 154
18.4.1 DHCP 응용 154
18.4.2 DHCP의 장점 154
18.4.3 DHCP 용어 155
18.5 DHCP 클라이언트 구성 155
18.5.1 DHCP 클라이언트 구성 작업 목록 155
18.5.2 DHCP 클라이언트 구성 작업 155
18.5.3 DHCP 클라이어언트 구성 예제 157
18.6 IP 서비스 구성 158
18.6.1 IP 연결 관리 158
18.6.2 성능 매개변수 구성 160

18.6.3 IP 네트워크 감지 및 유지 관리 161
18.7 액세스 리스트 구성 162
18.7.1 IP 패킷 필터링 162
18.7.2 표준 및 확장 IP 액세스 리스트 생성 163
18.7.3 인터페이스에 액세스 리스트 적용 164
18.7.4 확장 액세스 리스트 예제 165
18.8 물리 포트 기반 IP 액세스 리스트 구성 166
18.8.1 IP 패킷 필터링 166
18.8.2 표준 및 확장 IP 액세스 리스트 생성 166
18.8.3 포트에 ACL 적용 167
18.8.4 확장 액세스 리스트 예제 168
18.9 IP 접근 제어 목록 적용 169
18.9.1 포트에 ACL 적용 169
18.10 IPv6 프로토콜 구성 170
18.11 IPv6 활성화 170
18.11.1 IPv6 주소 설정 170
18.12 IPv6 서비스 설정 172
18.12.1 IPv6 링크 관리 172
18.13 IPv6 ACL 구성 173
18.13.1 IPv6 패킷 필터링 173
18.13.2 IPv6 ACL 설정 174
18.13.3 포트에 ACL 적용하기 175
18.13.4 Pv6 ACL 예제 175
19. STP 구성 177
19.1 STP 소개 177
19.2 STP 구성 작업 목록 178
19.3 STP 구성 작업 179
19.3.1 STP 모드 선택 179
19.3.2 STP 비활성화/활성화 179

19.3.3 포트에서 STP 비활성화/활성화 179
19.3.4 스위치 우선순위 설정 180
19.3.5 Hello Time 설정 180
19.3.6 Max-Age Time 설정 180
19.3.7 Forward Delay Time 설정 180
19.3.8 포트 우선순위 설정 181
19.3.9 경로 비용(Path Cost) 설정 181
19.3.10 STP 상태 모니터링 181
19.3.10 SNMP Trap 설정 182
19.4 VLAN 스패닝 트리 구성 182
19.4.1 개요 182
19.4.2 VLAN STP 구성 작업 183
19.5 RSTP 설정 185
19.6 RSTP 구성 작업 185
19.6.1 스위치 RSTP 활성화/비활성화 185
19.6.2 스위치 우선 순위 설정 185
19.6.3 Forward Delay Time 설정 186
19.6.4 Hello Time 설정 186
19.6.5 Max-Age 설정 187
19.6.6 Path Cost 설정 187
19.6.7 Port Priority 설정 188
19.6.8 Edge Port 설정 188
19.6.9 포트 연결 유형 설정 188
19.6.10 프로토콜 변환 확인 재시작 189
19.7 MSTP 구성 191
19.7.1 MSTP 개요 191
19.7.2 MST 도메인 191
19.7.3 IST, CST, CIST 및 MSTI 191
19.7.4 포트 규정 193

19.7.5 MSTP BPDU 196
19.7.6 안정 상태 (Stable State) 198
19.7.7 홉 카운트 (Hop Count) 198
19.7.8 STP 호환성 (STP Compatibility) 199
19.8 MSTP 구성 작업 목록 199
19.9 MSTP 구성 작업 200
19.9.1 기본 MSTP 구성 200
19.9.2 MSTP 활성화 및 비활성화 200
19.9.3 MST 영역 구성 201
19.9.4 네트워크 루트 구성 202
19.9.5 보조 루트 구성 (Secondary Root) 203
19.9.7 STP 시간 매개변수 구성 204
19.9.8 네트워크 Diameter 구성 205
19.9.9 최대 홉 수 구성 206
19.9.10 포트 우선순위 설정 206
19.9.11 포트 경로 비용 설정 206
19.9.12 엣지 포트 설정 207
19.9.13 포트 연결 유형 설정 207
19.9.14 MST-호환 모드 활성화 208
19.9.15 프로토콜 변환 검사 재시작 209
19.9.16 포트 역할 제한 설정 209
19.9.17 포트 TCN 제한 설정 209
19.9.18 MSTP 정보 확인 210
19.10 STP 선택적 특성 소개 210
19.10.1 포트 패스트(Port Fast) 211
19.10.2 BPDU Guard 212
19.10.3 BPDU 필터 213
19.10.4 Uplink Fast 213
19.10.5 Backbone Fast 215

19.10.6 루트가드 216
19.11 STP 선택적 특성 구성 217
19.11.1 STP 선택적 특성 구성 작업 217
19.11.2 Port Fast 구성 218
19.11.3 BPDU Guard 구성 218
19.11.4 BPDU Filter 구성 219
19.11.5 Uplink Fast 구성 220
19.11.6 Backbone Fast 구성 220
19.11.7 Root Guard 구성 220
19.11.8 Loop Guard 구성 221
19.11.9 Loop Fast 구성 221
19.11.10 Address Table Aging 보호 구성 222
19.11.11 FDB-Flush 구성 223
19.11.12 BPDU Terminal 구성 223
20. Link Aggregation 구성 224
20.1 개요 224
20.2 Link Aggregation 구성 작업 목록 224
20.3 port aggregation 구성 작업 224
20.3.1 집계에 사용되는 논리적 채널 구성 224
20.3.2 물리적 port aggregation 225
20.3.3 port aggregation 후 load balance 방식 선택 226
20.3.4 port aggregation의 구체적인 상태 모니터링 226
21. PDP 및 LLDP 구성 227
21.1 PDP개요 227
21.1 PDP 구성 작업 227
21.1.1 기본 PDP 구성 227
21.1.2 PDP 클록 및 정보 저장 설정 227
21.1.3 PDP 버전 설정 228
21.1.4 스위치에서 PDP 시작 228

21.1.5 포트에서 PDP 시작 228
21.1.6 PDP 모니터링 및 관리 228
21.1.7 PDP 구성 예제 228
21.2 LLDP 설명 229
21.2.1 프로토콜 초기화 230
21.2.2 LLDP 전송 모드 초기화 230
21.2.3 LLDP 수신 모드 초기화 231
21.2.4 LLDP PDU 패킷 구조 설명 231
21.3 LLDP 구성 작업 목록 232
21.4 LLDP 구성 작업 233
21.4.1 LLDP 비활성화/활성화 233
21.4.2 Holdtime 설정 233
21.4.3 Timar 설정 233
21.4.4 Reinit 설정 234
21.4.5 전송할 TLV 구성 234
21.4.6 포트 구성 및 전송할 확장 TLV 선택 235
21.4.7 전송 또는 수신 모드 구성 236
21.4.8 포트의 관리 IP 주소 지정 237
21.4.9 위치 정보 설정 237
21.4.10 포트에 위치 정보 설정 238
21.4.11 Show 관련 명령어 구성 238
21.4.12 삭제 명령어 구성 239
21.4.13 설정 예제 239
22 Backup Link 248
21.2 개요 248
22.1 BackupLink 포트 백업 248
22.1.1 백업 포트 구성 248
22.1.2 포트 상태 제어 249
22.1.3 포트 역할과 상태 249

22.1.4 링크 상태 변경 처리 250
22.1.5 백업 포트의 사전 점유 250
22.1.6 Delay Preemption 251
22.2 VLAN Load Balancing 251
22.2.1 Load Balancing 구성 251
22.2.2 트래픽 공유에서의 포트 상태 제어 252
22.3 MAC 주소 Aging 처리 253
22.3.1 링크의 정상 작동 매커니즘 254
22.3.2 다운링크 장애 처리 매커니즘 254
22.3.3 업링크 장애 처리 매커니즘 255
22.4 BackupLink 구성 가이드라인 258
22.5 BackupLink 구성 작업 258
22.6 BackupLink 설정 258
22.6.1 BackupLink 그룹 구성 258
22.6.2 백업링크 그룹의 Preemption 기능 설정 259
22.6.3 VLAN 로드 밸런싱 설정 259
22.6.4 백업링크 그룹의 MMU 기능 설정 260
22.6.5 MonitorLink 그룹 설정 260
22.7 Fast Ethernet Ring Protection 소개 261
22.8 Fast Ethernet Ring Protection 개념 262
22.8.1 링 노드의 역할 262
22.8.2 링 포트의 역할 262
22.8.3 제어 VLAN(Control VLAN)과 데이터 VLAN(Data VLAN) 263
22.8.4 MAC 주소 테이블의 에이징(Aging) 264
22.8.5 완전한 링 네트워크의 상태 기호 (Symbol) 264
22.9 EAPS 패킷의 종류 264
22.10 Fast Ethernet Ring Protection 메커니즘 265
22.10.1 마스터 노드의 링 감지 및 제어 265
22.10.2 트랜짓 노드의 비정상 링크 알림 265

22.10.3 트랜짓 노드 링크 복구 265
22.11 기본 EAPS 설정 267
22.12 구성 전 요구 사항 267
22.13 MEAPS 구성 작업 268
22.14 Fast Ethernet Ring Protection 구성 268
22.14.1 마스터 노드 구성 268
22.14.2 트랜짓 노드 구성 269
22.14.3 링 포트 구성 269
22.14.4 링 보호 프로토콜 상태 확인 269
22.15 MEAPS 구성 270
22.15.1 설정 예제 270
23 EAPS와 MEAPS 273
23.1 MEAPS의 기본 개념 274
23.1.1 도메인 274
23.1.2 링 275
23.1.3 주요 링 275
23.1.4 하위 링 275
23.1.5 제어 VLAN 275
23.1.6 데이터 VLAN 276
23.1.7 마스터 노드 276
23.1.8 트랜짓 노드 277
23.1.9 엣지 노드와 보조 노드 277
23.1.10 주 포트와 보조 포트 277
23.1.11 트랜짓 포트 278
23.1.12 공통 포트와 엣지 포트 278
23.1.13 MAC 주소 테이블의 에이징 (FLUSH MAC FDB) 279
23.1.14 링의 완전성 플래그 279
23.1.15 EAPS 패킷의 종류 279
23.2 Fast Ethernet 링 보호 메커니즘 280

23.2.1 폴링 메커니즘 280
트랜짓 노드의 비정상 링크 알림 281
23.2.2 주요 링에서 하위 링 프로토콜 패킷의 채널 상태 점검 메커니즘 282
23.3 MEAPS 구성 전 요구 사항 288
23.4 MEAPS 구성 작업 289
23.5 Fast Ethernet 링 보호 구성 289
23.5.1 마스터 노드 구성 289
23.5.2 트랜짓 노드 구성 290
23.5.3 엣지 노드와 이시스턴트 노드 구성 290
23.5.4 서브 링 네트워킹 모드 구성 291
23.5.5 링 포트 구성 292
23.5.6 링 보호 프로토콜 상태 확인 292
23.6 MEAPS 동작 절차 294
23.6.1 정상 상태 (Complete State) 294
23.6.2 링크 다운 295
23.6.3 복구 296
23.6.4 설정 예제 298
24. snooping 구성 307
24.1 IGMP-snooping 구성 작업 307
24.1.1 VLAN의 IGMP-Snooping 활성화/비활성화 308
24.1.2 VLAN의 Static 멀티캐스트 주소 추가/삭제 308
24.1.3 VLAN의 Immediate-Leave 기능 구성 309
24.1.4 포트의 Immediate-Leave 기능 설정 309
24.1.5 VLAN의 Static Routing Interface 설정 309
24.1.6 멀티캐스트 포워딩 테이블 생성을 위한 IPACL 설정 310
24.1.7 등록되지 않은 목적지 주소의 멀티캐스트 메시지를 필터링하는 기능 구성 310
24.1.8 IGMP-snooping의 Router Age Timer 설정 311
24.1.9 IGMP-snooping의 Response Time Timer 설정 311
24.1.10 IGMP-snooping의 Querier 설정 311

24.1.11 IGMP-snooping의 Querier Time Timer 설정 312
24.1.12 IGMP-snooping의 forward-l3-to-mrouter 기능 설정 313
24.1.13 IGMP-snooping의 Sensitive 모드 및 값 설정 313
24.1.14 IGMP-snooping의 v3-leave-check 기능 설정 314
24.1.15 IGMP-snooping의 forward-wrongiif-within-vlan 기능 설정 314
24.1.16 IGMP-snooping의 포트에서 IPACL 기능 설정 314
24.1.17 VLAN에서 IGMP-snooping의 멀티캐스트 필터링 설정 315
24.1.18 IGMP-snooping 포트에서 최대 멀티캐스트 IP 주소 수량 설정 315
24.1.19 IGMP-snooping의 Report-Suppression 기능 설정 315
24.1.20 IGMP-snooping의 Proxy-Leave 기능 설정 316
24.1.21 IGMP-snooping 모니터링 및 유지 관리 316
24.2 IGMP-Proxy 설정 작업 320
24.2.1 IGMP-Proxy 활성화/비활성화 321
24.2.2 VLAN 에이전트 관계 추가/삭제 321
24.2.3 IGMP-Proxy 모니터링 및 유지 관리 322
24.3 MLD-Snooping 개요 322
24.4 MLD-Snooping 멀티캐스트 설정 작업 323
24.4.1 MLD-Snooping 멀티캐스트 활성화/비활성화 323
24.4.2 멀티캐스트 그룹 하드웨어 포워딩 요청 활성화/비활성화 323
24.4.3 VLAN의 static 멀티캐스트 주소 추가/삭제 324
24.4.4 MLD-Snooping 라우터 에이지 타이머 설정 324
24.4.5 MLD-Snooping 응답 시간 타이머 설정 324
24.4.6 MLD-Snooping 쿼리어 설정 325
24.4.7 static 멀티캐스트 라우터 포트 설정 325
24.4.8 Immediate Leave 기능 활성화/비활성화 325
24.4.9 MLD-Snooping 멀티캐스트 모니터링 및 유지 관리 326
24.5 DHCP-Snooping구성 작업 326
24.5.9 DHCP-Snooping 활성화/비활성화 327
24.5.10 VLAN에서 DHCP-Snooping 활성화 327

24.5.11 VLAN에서 DHCP 공격 방지 활성화 327
24.5.12 DHCP trust 인터페이스로 설정 328
24.5.13 바인딩 테이블 빠른 업데이트 기능 활성화/비활성화 328
24.5.14 VLAN에서 DAI(동적 ARP 검사) 활성화 328
24.5.15 ARP trust 인터페이스로 설정 329
24.5.16 VLAN에서 소스 IP 주소 모니터링 활성화 329
24.5.17 소스 IP 주소 모니터링에서 신뢰 인터페이스 설정 329
24.5.18 DHCP-Snooping 옵션 82 설정 330
24.5.19 DHCP-Snooping 옵션 82 패킷 정책 설정 331
24.5.20 인터페이스 바인딩 백업을 위한 TFTP 서버 구성 331
24.5.21 인터페이스 바인딩 백업 파일 이름 구성 332
24.5.22 인터페이스 바인딩 백업 주기 구성 332
24.5.23 인터페이스 바인딩 수동 구성 332
24.5.24 DHCP-Snooping 모니터링 및 유지 관리 333
24.5.25 설정 예제 333
25. QoS 구성 335
25.1 QoS 개요 335
25.1.1 QoS 개념 335
25.1.2 단말 간(end-to-end) QoS 모델 335
25.1.3 QoS 큐잉 알고리즘 336
25.1.4 가중 랜덤 조기 탐지 (WRED) 337
25.2 QoS 구성 작업 목록 338
25.3 QoS 구성 작업 339
25.3.1 글로벌 CoS 우선순위 큐 설정 339
25.3.2 CoS 우선순위 큐의 대역폭 설정 339
25.3.3 CoS 우선순위 큐 스케줄 정책 설정 340
25.3.4 포트의 기본 CoS 값 설정 341
25.3.5 포트의 CoS 우선순위 큐 설정 341
25.3.6 포트 CoS 우선순위 큐 대역폭 설정 342

25.3.7 포트 CoS 우선순위 큐 스케줄 정책 설정 342
25.3.8 DSCP 기반 CoS 우선순위 큐 설정 343
25.3.9 QoS 정책 매핑 생성 343
25.3.10 QoS 정책 매핑 설명 설정 343
25.3.11 QoS 정책 매핑의 데이터 흐름 설정 344
25.3.12 QoS 정책 매핑에서 데이터 흐름의 동작 설정 345
25.3.13 포트에서 QoS 정책 적용 346
25.3.14 글로벌 QoS 정책 적용 347
25.3.15 신뢰 모드(Trust Mode) 구성 347
25.3.17 포트에 QoS 정책 적용 예시 348
26. OAM 구성 349
26.1 OAM 개요 349
26.1.1 OAM 프로토콜 속성 349
26.1.2 OAM 모드 351
26.1.3 OAM 패킷의 구성 요소 352
26.2 OAM 구성 작업 353
26.2.1 인터페이스에서 OAM 활성화 353
26.2.2 OAM 링크 모니터링 구성 354
26.2.3 원격 OAM 엔터티로부터의 장애 알림 구성 355
26.2.4 OAM 프로토콜 정보 표시 356
26.2.5 설정 예제 357
27 CFM 구성 361
27.1 CFM 구서 작업 목록 361
27. 2 CFM 유지 관리 작업 목록 361
27.2.1 유지 관리 도메인 추가 361
27.2.2 유지 관리 연결(MA) 추가 361
27.2.3 MIP(유지 관리 도메인 중간 지점) 추가 361
27.2.4 MEP(유지 관리 연결 종료 지점) 추가 362
27.2.5 CFM 시작 362

27.2.6 루프백 기능 사용 362
27.2.7 링크 추적(Linktrace) 기능 사용 362
27.2.8 설정 예제 362
28. MACFF 구성 364
28.1 MACFF 구성 작업 364
28.1.1 MAC 활성화 / 비활성화 364
1.1.1 VLAN에서 MACFF 활성화 364
28.1.2 VLAN에서 MACFF 기본 AR 구성 365
28.1.3 VLAN에서 MACFF 기타 AR 구성 365
28.1.4 특정 물리 포트에서 MACFF 비활성화 366
28.1.5 MACFF 디버깅 활성화 366
29. Layer-2 Tunnel 프로토콜 구성 367
29.1 개요 367
29.2 Layer-2 Tunnel 프로토콜 구성 367
29.3 구성 예제 367
30. Attack Prevention 369
30.1 필터 개요 369
30.2 필터 모드 369
30.3 공격 방지 구성 작업 371
30.4 공격 방지 구성 371
30.4.1 공격 필터 매개변수 구성 371
30.4.2 공격 방지 유형 구성 372
30.4.3 공격 방지 활성화 372
30.4.4 공격 방지 상태 확인 373
30.4.5 구성 예제 374
30.4.6 Layer-3 네트워크 보호를 위한 IP 필터 사용 374
30.5 DoS 공격 개요 376
30.5.1 DoS 공격 개념 376
30.6 DoS 공격 유형 376

30.7 DoS 공격 방지 구성 작업 377
30.7.1 글로벌 DoS 공격 방지 구성 377
30.7.2 DoS 공격 방지 구성 378
30.7.3 DoS 공격 방지 구성 예시 378
30.8 IP-Attack Prevention 구성 378
30.9 IP 공격 방지 구성 작업 목록 379
30.10 IP-Attack Prevention 구성 379
30.10.1 IP 공격 탐지 매개변수 구성 379
30.10.2 IP attack 탐지 유형 구성 379
30.10.3 IP 공격 방지 기능 활성화 380
30.10.4 IP 공격 방지 구성 예제 380
30.11 네트워크 세그먼트 스캔에 대한 IP Attack 방지 381
30.12 네트워크 세그먼트 스캔에 대한 구성 작업 목록 381
30.12.1 네트워크 세그먼트 스캔에 대한 IP 공격 방지 탐지 매개변수 구성 381
30.12.2 네트워크 세그먼트 스캔 방지 탐지 유형 구성 381
30.12.3 네트워크 세그먼트 스캔에 대한 IP 공격 방지 활성화 382
30.12.4 네트워크 세그먼트 스캔에 대한 IP 공격 방지 예시 382
30.12.5 네트워크 세그먼트 스캔에 대한 IP 공격 방지 탐지 결과 382
30.13 Urpf 개요 383
30.13.1 uRPF (Unicast Reverse Path Forwarding) 383
30.14 Urpf 구성 383
30.14.1 글로벌 설정 모드에서 uRPF 활성화 383
30.14.2 VLAN 인터페이스에서 uRPF 검사 모드 구성 383
31. 라우팅 프로토콜 개요 385
31.1 IP 라우팅 프로토콜 385
31.2 라우팅 프로토콜 선택 385
31.2.1 내부 게이트웨이 라우팅 프로토콜 (Interior Gateway Router Protocol) 385
31.2.2 외부 게이트웨이 라우팅 프로토콜 (Exterior Gateway Routing Protocol) 386
31.3 VRF 구성 387

31.4 VRF 구성 작업 목록 387
31.5 구성 작업 387
31.5.1 인터페이스를 VRF에 연결 387
31.5.2 VRF 대상 VPN 확장 속성 구성 388
31.5.3 VRF 설명 구성 388
2.3.5 VRF 정적 경로 구성 388
31.5.4 VRF 모니터링 389
31.5.5 VRF 유지 관리 389
31.5.6 VRF 구성 예제 389
1.1 exit-address-family31.6 Multi-VRF CE 개요 391
31.6.1 CE 라우트 설정 392
31.6.2 PE 라우트 설정 393
31.7 Multi-VRF CE 구성 394
31.8 MCE 구성 작업 394
31.8.1 VRF 구성 방법 394
31.8.2 VPN 경로 구성 395
31.8.3 PE와 CE 간 BGP 라우트 구성 395
31.8.4 PE와 CE 간 VRF 연결성 테스트 396
31.8.5 MCE 구성 예제 397
31.1 Static 라우팅 구성 406
31.2 Static 라우팅 구성 작업 목록 407
31.2.1 Static 라우팅 구성 407
31.2.2 Static 라우팅 구성 예제 407
31.3 RIP 구성 408
31.4 RIP 구성 작업 목록 408
31.4.1 RIP 구성 작업 409
31.4.3 타이머 조정 410
31.4.4 RIP 버전 번호 지정 411
31.4.5 인터페이스에서 'Passive' 및 'Deaf' 활성화 412

31.4.6 RIP 인증 활성화 412
31.4.7 라우트 요약 금지 413
31.4.8 소스 IP 주소 및 제로-도메인 인증 금지 414
31.4.9 동등 경로의 최대 개수 설정 414
31.4.10 Split-Horizon 활성화 또는 비활성화 415
31.4.11 RIP 모니터링 및 유지 관리 415
31.4.12 RIP 구성 예제 416
31.5 BEIGRP 동적 라우팅 프로토콜 구성 417
31.6 BEIGRP 구성 작업 목록 417
31.6.1 BEIGRP 프로토콜 활성화 418
31.6.2 대역폭 공유 비율 설정 418
31.6.3 BEIGRP 복합 메트릭 계산 계수 조정 419
31.6.4 "Offset"을 사용하여 라우터의 복합 메트릭 조정 419
31.6.5 자동 요약 비활성화 419
31.6.6 BEIGRP 프로세스로 다른 라우트 재배포 419
31.6.7 BEIGRP 기타 파라미터 구성 420
31.6.8 BEIGRP 모니터링 및 유지 관리 422
31.7 OSPF 구성 423
31.8 OSPF 구성 작업 목록 423
31.8.1 OSPF 시작 424
31.8.2 OSPF 인터페이스 매개변수 구성 425
31.8.3 OSPF 네트워크 유형 구성 426
31.8.4 일대다 브로드캐스트 네트워크 구성 426
31.8.5 논브로드캐스트 네트워크 구성 427
31.8.6 OSPF 도메인 구성 428
31.8.7 OSPF의 NSSA 영역 구성 429
31.8.8 OSPF 도메인 내 라우트 요약 구성 430
31.8.9 포워딩 라우터의 요약 구성 430
31.8.10 기본 라우트 생성 430

31.8.11 루프백 인터페이스를 통한 라우터 ID 선택 431
31.8.12 OSPF 관리 거리 구성 431
31.8.13 라우트 계산 타이머 구성 431
31.8.14 온디맨드 링크(On-Demand Link) 구성 432
31.8.15 OSPF 모니터링 및 유지 관리 432
31.8.16 OSPF 포인트 투 멀티포인트 논브로드캐스트 구성 예제 433
31.8.17 가변 길이 서브넷 마스크(VLSM) 구성 예제 434
31.8.18 OSPF 라우트 및 라우트 재분배 구성 예제 435
31.9 OSPFv3 구성 442
31.10 OSPFv3 구성 작업 목록 443
31.10.1 OSPFv3 활성화 443
31.10.2 OSPFv3 인터페이스 매개변수 설정 444
31.10.3 다양한 물리적 네트워크에서 OSPFv3 설정 444
31.10.4 OSPF 네트워크 유형 설정 445
31.10.5 OSPFv3 도메인 매개변수 설정 445
31.10.6 OSPFv3 도메인에서 경로 요약 설정 446
31.10.7 포워딩 경로의 요약 설정 446
31.10.8 기본 경로(디폴트 루트) 생성 447
31.10.9 루프백 인터페이스에서 라우터 ID 선택 447
31.10.10 OSPFv3 관리 거리 설정 447
31.10.11 라우팅 알고리즘 타이머 설정 448
31.10.12 OSPFv3 모니터링 및 유지 관리 448
31.10.13 OSPFv3 라우트 학습 설정 예제 449
31.11 BGP 구성 459
31.11.1 라우터의 BGP 구현 459
31.11.2 BGP 경로 선택 방식 460
31.12 BGP 구성 작업 목록 461
31.12.1 BGP 기본 구성 작업 목록 461
31.12.2 BGP 고급 구성 작업 목록 461

31.13 BGP 구성 작업 462
31.13.1 기본 BGP 기능 구성 462
31.13.2 고급 BGP 기능 구성 468
31.14 BGP 모니터링 및 유지 관리 474
31.14.1 BGP 라우팅 테이블 및 BGP 데이터베이스 삭제 474
31.14.2 라우팅 테이블 및 시스템 통계 정보 표시 475
31.14.3 BGP 정보 추적 475
31.14.4 BGP 라우트 맵 예제 476
31.14.5 Neighbor 구성 예제 477
31.14.6 Neighbor 기반 BGP 라우트 필터링 예제 478
31.14.7 인터페이스 기반 BGP 라우트 필터링 예제 478
31.14.8 프리픽스 리스트를 사용한 라우트 필터링 구성 예제 479
31.14.9 BGP 라우트 애그리게이션 예제 480
31.14.10 BGP 라우트 리플렉터 예제 481
31.14.11 BGP 컨페더레이션 예제 483
31.14.12 BGP 그룹 속성(Route Map) 예제 486
31.15 PBR 구성 489
31.16 PBR 구성 작업 목록 489
31.17 PBR 구성 작업 490
31.17.1 표준 액세스 리스트 생성 490
31.17.2 라우트 맵 생성 490
31.17.3 인터페이스에 라우트 맵 적용 490
31.17.4 PBR 유지 관리 490
31.17.5 PBR 구성 예시 490
31.18 IP-PBR 구성 492
31.18.1 IP-PBR 글로벌 활성화 또는 비활성화 493
31.18.2 ISIS 구성 작업 목록 493
31.18.3 MVC 모니터링 및 유지 관리 494
31.18.4 IP-PBR 구성 예제 494

31.19 스위치 라우팅 프로토콜 고우선순위 구성 496
31.19.1 CPU로 전달되는 라우팅 패킷의 우선순위 향상 활성화 496
32 VRRP 구성 497
32.1 개요 497
32.2 VRRP 구성 작업 목록 497
32.3 VRRP 구성 작업 497
32.3.1 VRRP 가상 IP 주소 구성 497
32.3.2 VRRP 인증 모드 구성 498
32.3.3 VRRP 설명 구성 498
32.3.4 VRRP 우선 순위 프리엠프션(Preemption) 구성 498
32.3.5 VRRP 프로토콜 패킷의 MAC 주소 구성 499
32.3.6 VRRP 우선 순위 구성 499
32.3.7 VRRP 클록 값(타이머) 구성 499
32.3.8 VRRP 모니터링 오브젝트 구성 500
32.3.9 VRRP 모니터링 및 유지 관리 501
32.3.10 VRRP 구성 예제 501
33. 멀티캐스트 개요 504
33.1 멀티캐스트 라우팅 구현 504
33.2 멀티캐스트 라우팅 구성 작업 목록 505
33.2.1 기본 멀티캐스트 구성 작업 목록 505
33.2.2 IGMP 구성 작업 목록 505
33.2.3 PIM-DM 구성 작업 목록 506
33.2.4 PIM-SM 구성 작업 목록 506
34. 기본 멀티캐스트 라우팅 구성 507
34.1 멀티캐스트 라우팅 시작 507
34.2 포트에서 멀티캐스트 기능 시작 507
34.2.1 PIM-DM 시작 507
34.2.2 PIM-SM 시작 507
34.3 TTL 임계값 구성 508

34.4 IP 멀티캐스트 경계 구성 508
34.5 IP 멀티캐스트 헬퍼 구성 509
34.6 Stub 멀티캐스트 라우트 구성 510
34.7 멀티캐스트 라우트 모니터링 및 유지 관리 511
35. IGMP 구성 512
35.1 개요 512
35.2 IGMP 구성 512
35.2.1 현재 IGMP 버전 변경 512
35.2.2 IGMP 쿼리 간격 구성 513
35.2.3 IGMP 쿼리어 간격 구성 513
35.2.4 최대 IGMP 응답 시간 구성 514
35.2.5 마지막 그룹 멤버의 IGMP 쿼리 간격 구성 515
35.2.6 정적 IGMP 구성 515
35.2.7 IGMP Immediate Leave 목록 구성 516
35.3 IGMP 특성 구성 예시 517
36. PIM-DM 구성 521
36.1 PIM-DM 개요 521
36.2 PIM-DM 구성 522
36.2.1 타이머 수정 522
36.2.2 버전 번호 지정 523
36.2.3 상태 갱신 구성 523
36.2.4 필터링 목록 구성 523
36.2.5 DR 우선순위 설정 524
36.2.6 (S,G) 항목 삭제 524
36.3 PIM-SM 구성 525
36.1 PIM-SM 소개 525
36.2 PIM-SM 구성 목록 525
36.2.1 글로벌 멀티캐스트 활성화 526
36.2.2 PIM-SM 시작 526

36.2.3 이웃 필터 목록 구성 527
36.2.4 DR(Designated Router) 선출 529
36.2.5 후보 RP(Candidate RP) 구성 530
36.2.6 후보 BSR(Bootstrap Router) 구성 531
36.2.7 SPT 임계값(SPT-threshold) 구성 532
36.2.8 SSM(Source-Specific Multicast) 구성 533
36.2.9 관리 도메인(sz) 구성 534
36.2.10 등록 패킷의 소스 주소 구성 535
36.2.11 Anycast-RP 구성 535
36.2.12 PIM-SM 로컬 라우팅 항목 표시 536
36.2.13 PIM-SM 라우팅 항목 초기화 537
36.2.14 PIM-SM 디버깅 정보 추적 537
36.3 구성 예제 539
36.3.1 PIM-SM 일반 토폴로지 구성 예시 539
36.3.2 다중 프로토콜 멀티캐스트 혼합 구성 543
37. NTP 구성 544
37.1 개요 544
37.2 NTP 구성 544
37.2.1 장비를 NTP 서버로 구성하기 544
37.2.2 NTP 인증 기능 구성하기 544
37.2.3 NTP 연결 구성하기 544
38. 케이블 진단 546
38.1 이더넷 인터페이스 케이블 진단 활성화 546
38.1.1 케이블 진단 예제 546
39. 광 포트 부가 기능 구성 547
39.1 광 포트 DDM 기능 활성화 547
39.2 광 포트 단일 광섬유 송수신 기능 548
39.3 광 포트 적응형 광 모듈 기능 548
40. Logging 549

40.1 개요 549
40.2 logging on 549
40.3 외부 syslog 서버 연동 549
40.3.1 logging trap 549
40.4 logging buffered 550
40.5 logging console 550
40.6 logging facility 551
40.7 logging monitor 552
40.7.1 logging command 552
40.8 logging history 552
40.9 logging file 553

개정 이력

일자	주요개정 내용	문서 버전
2025-01-13	초판	V_1.0

이 문서는 [미래시그널]의 자산이며, 저작권법 및 기타 지적 재산권 법률에 의해 보호됩니다. 본 매뉴얼의 전부 또는 일부를 [미래시그널]의 사전 서면 동의 없이 복사, 복제, 수정, 배포, 전송하거나 기타의 방법으로 사용하거나 공개하는 것을 금합니다.

본 매뉴얼에 포함된 정보는 사전 고지 없이 변경될 수 있습니다.

■ 보안 스위치 개요

보안 스위치는 네트워크 인프라의 안정성과 보안을 강화하기 위해 설계된 고성능 네트워크 장비입니다. 일반적인 스위치 기능에 고급 보안 기능을 추가함으로써 외부 위협으로 부터 네트워크를 보호하고, 내부 네트워크의 접근 제어 및 트래픽 관리를 효율적으로 수행할 수 있도록 지원합니다. 정보보안이 점점 더 중요해지는 오늘날, 보안 스위치는 기업, 공공기관, 데이터 센터 등 보안이 중요한 환경에서 네트워크의 무결성, 기밀성, 가용성을 유지하는 데 필수적인 역할을 합니다.

이러한 다양한 보안 기능을 통해 보안 스위치는 네트워크 접근 제어를 강화하고, 내부 및 외부 위협으로 부터 네트워크를 보호하며, 안정적이고 안전한 네트워크 운영 환경을 구축합니다. 보안 스위치는 기존 네트워크 스위치의 성능을 유지하면서도, 보안을 강화하여 네트워크 인프라의 신뢰성을 높이는 필수 장비로 자리 잡고 있습니다. 보안이 점점 더 중요해지는 IT 환경에서 보안 스위치는 네트워크 보안의 핵심적인 역할을 담당하며, 기업 및 기관의 정보자산을 보호하는 데 중요한 기여를 하고 있습니다.

1. 제품 설치

1.1 설치 준비

스위치를 설치하기 전에는 안정적인 설치와 운영을 위해 철저한 사전 준비가 필요합니다. 설치 환경 점검, 네트워크 구성 계획, 장비 준비 등 여러 단계를 체계적으로 진행해야 합니다.

1. 설치환경 점검
   - 스위치가 설치될 장소의 물리적 공간과 전원 공급 상태를 확인합니다.
   - 적절한 통풍과 온도 관리가 가능한지 확인하여 장비의 과열을 방지합니다.
   - 랙(Rack) 설치 여부와 랙 마운트 키트 준비 상태를 점검합니다.
2. 네트워크 구성 계획 수립
   - 기존 네트워크 구성도를 검토하고, 스위치가 연결될 위치와 역할을 명확히 합니다.
   - IP 주소, VLAN 설정, 포트 할당 계획을 사전에 수립합니다.
3. 장비 및 부속품 준비
   - 스위치 본체, 전원 케이블, 네트워크 케이블, 랙 마운트 키트 등의 준비 상태를 점검합니다.
   - 펌웨어 버전 확인 및 필요 시 최신 버전으로 업데이트할 준비를 합니다.
4. 보안 설정 계획
   - 관리 계정 및 비밀번호 정책을 사전에 정의합니다.
5. 비상 대응 계획 수립
   - 설치 중 발생할 수 있는 문제를 대비해 복구 절차 및 연락망을 마련합니다.
   - 네트워크 중단 시 빠르게 대응할 수 있도록 사전 테스트 및 백업 계획을 수립합니다.

1.2 랙 환경 설치

19인치 랙에 설치 하기위해 아래의 그림 및 설명을 참고하여 주시기바랍니다.

1. 샤시의 양쪽에 브라켓을 부착하십시오. 드라이버와 나사를 조이고 브라켓을 고정합니다.

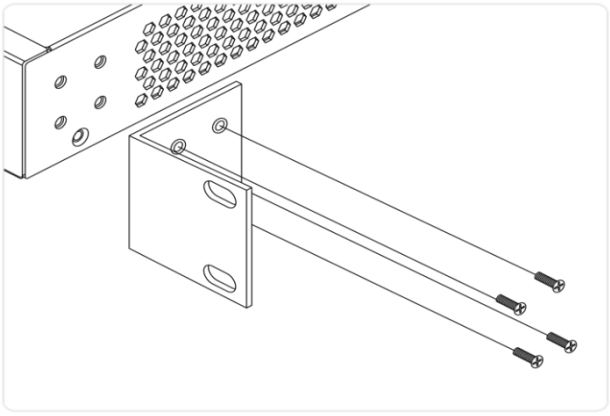


그림 1 스위치에 브라켓 설치

2. 스위치를 랙의 선반위에 놓습니다. 브라켓의 타원형 구멍이 랙 포스트 장착 구멍에 맞춰지도록 밀어 넣으십시오.

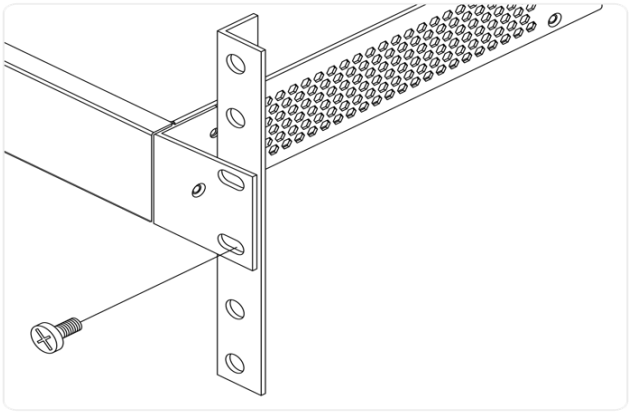


그림 2 랙 포스트에 브라켓 부착

1.3 선반에 스위치 설치

1. 선반등이 견고하게 자리 잡았는지 확인 하십시오.
2. 스위치가 움지이지 않도록 바닥 및 위치를 확인하여 선반위에 올려 놓습니다.

2.4 전원선 연결

1. AC 전원 코드를 스위치의 AC 전원 콘센트에 연결 합니다.
2. AC 전원 코드의 다른 쪽 끝을 AC 전원 콘센트에 연결 합니다.
3. LED의 표시 상태를 확인합니다.

2.5 DC 전원 연결 (산업용 및 DC전원이 필요한경우)

1. DC 젂원 단자에 +, - DC 젂선을 각각 삽입하십시오.
2. DC 젂원이 느슨해 지지 않게 하기 위해 소형 일자 드라이버를 사용하여 터미널 블록 커넥터의 젂면에 있는 와이어 클램프 나사를 조여 주십시오.
3. 블록 커넥터 단자에 커넥터를 삽입하십시오.
4. 전원 LED 를 확인하십시오. 만약 ON 되어 있다면 정상적으로 연결 된 것입니다.

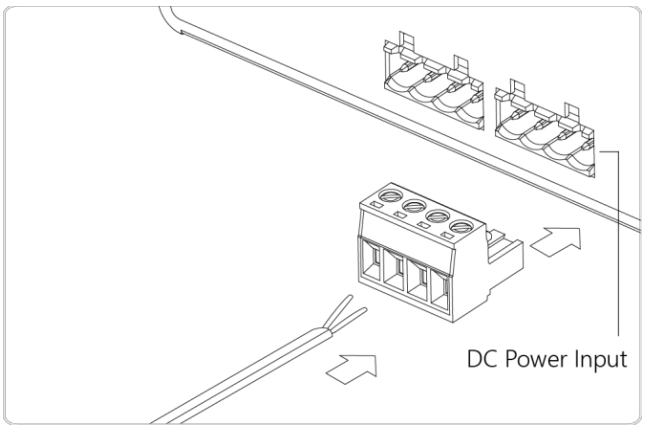


그림 3 DC전원 연결

2.6 UTP 및 SFP 연결 방법

1. UTP 케이블 연결 방법
   - 케이블 준비: Cat5e, Cat6 또는 Cat6a UTP 케이블을 준비합니다.
   - 포트 확인: 스위치의 RJ-45 포트와 연결할 장치의 네트워크 포트를 확인합니다.
   - 케이블 연결: 스위치의 RJ-45 포트에 UTP 케이블 한쪽 끝을 연결하고, 다른 쪽 끝은 PC, 라우터, 서버 또는 다른 네트워크 장치의 포트에 연결합니다.
   - LED 상태 점검: 연결 후 포트의 링크 상태 LED가 점등되는지 확인하여 정상 연결 여부를 확인합니다. 녹색 또는 주황색 LED는 정상 연결을 의미합니다.
   - 네트워크 테스트: 핑(Ping) 명령어 등을 통해 연결 상태를 최종적으로 확인합니다.
2. SFP 모듈 설치 및 연결 방법
   - 모듈 준비: 스위치에 적합한 SFP 모듈(SX, LX, DAC 등)을 준비합니다.
   - 포트 청소: 먼지나 이물질이 없는지 SFP 슬롯을 확인합니다.
   - SFP 모듈 삽입: SFP 모듈을 슬롯에 부드럽게 삽입합니다. 삽입 시 클릭 소리가 나며 고정됩니다.

- 케이블 연결: 광케이블(LC/SC 타입) 또는 DAC 케이블을 SFP 모듈에 연결합니다.
- LED 상태 점검: 연결 후 링크 상태 LED를 확인하여 정상 연결을 확인합니다.
- 트래픽 테스트: 네트워크 장비 간 연결 상태를 테스트합니다.

2.7 콘솔 연결 방법

1. 콘솔 케이블 연결 방법
   - 콘솔 케이블 준비: RJ-45 to USB 또는 RJ-45 to RS-232 콘솔 케이블을 준비합니다.
   - 스위치 연결: 콘솔 케이블의 RJ-45 커넥터를 스위치의 콘솔 포트에 연결합니다.
   - PC 연결: 케이블의 USB 또는 RS-232 커넥터를 PC의 해당 포트에 연결합니다.
   - 드라이설치: USB 타입 연결 시, 필요한 드라이버가 설치되어 있는지 확인합니다.
   - 터미널 프로그램 실행: PuTTY, Tera Term, SecureCRT 등 터미널 프로그램을 실행합니다.
   - 포트 설정: COM 포트를 확인하고, 다음과 같은 기본 설정을 입력합니다.

     속도(Baud rate): 9600

     데이터 비트(Data bits): 8

     패리티(Parity): None

     정지 비트(Stop bits): 1

     흐름 제어(Flow control): None

연결 확인: 연결 후 Enter 키를 눌러 CLI(Command Line Interface) 화면이 출력되는지 확인합니다.

3. 설정 준비하기

사용자가 처음으로 스위치를 구성하기 전에 다음과 같은 준비 작업에 대해 설명합니다.

- 스위치의 포트 번호
- 스위치 시작 전 준비
- 도움말 확인 방법
- Command 모드
- Command 취소
- 설정 저장

3.1 스위치의 포트 번호

스위치의 물리적 포트는 <타입><슬롯>/<포트> 형식으로 번호가 지정됩니다. 타입과 이름의 매핑 테이블은 다음과 같습니다.

인터페이스 유형	이름	간략화된 이름
10M Ethernet	Ethernet	e
100M fast Ethernet	FastEthernet	f
1000M Ethernet	GigaEthernet	g
10000M Ethernet	TGigaEthernet	tg

확장 슬롯 번호는 포트를 표시하고 설정하기 위해 번호 0으로 시작해야 합니다. 기타 확장 슬롯은 왼쪽에서 오른쪽으로 순서대로 번호가 매겨지며, 1부터 시작합니다.

같은 확장 슬롯 내의 포트는 아래에서 위로, 그리고 왼쪽에서 오른쪽 순서에 따라 1부터 번호가 매겨집니다. 만약 슬롯에 하나의 포트만 있다면, 해당 포트 번호는 1입니다.

참고: 각 유형의 모듈에서 포트는 반드시 아래에서 위로, 왼쪽에서 오른쪽 순서로 연속적으로 번호가 지정되어야 합니다.

3.2 스위치 시작 전 준비

스위치를 구성하기 전에 다음 준비 작업을 수행합니다.

① 매뉴얼의 요구 사항에 따라 스위치의 하드웨어를 설정합니다.

② PC 단말기 시뮬레이션 프로그램을 구성합니다. 터미널 연결을 위한 PC 프로그램을 설정합니다. (putty 등)

③ 네트워크 망에서 사용할 IP주소를 미리 계획합니다.

3.3 도움말 확인하기

명령어 입력을 도울 수 있도록 물음표(?)와 방향 키를 사용하십시오

- 물음표 입력 : 현재 사용 가능한 명령어 목록이 표시됩니다.

  Switch> ?

- 일부 문자 입력 후 물음표 사용 : 입력한 문자로 시작하는 사용 가능한 명령어 목록이 표시됩니다.

  Switch> s?

- 명령어 입력 후 물음표 사용 : 명령어의 설정 목록이 표시됩니다.

  Switch> show ?

- 방향 키 사용 : 위쪽 방향 키를 누르면 이전에 입력한 명령어가 표시됩니다. 계속 위쪽 방향 키를 누르면 더 많은 이전 명령어가 표시됩니다. 이후 아래쪽 방향 키를 누르면 현재 명령어 아래의 다음 명령어가 표시됩니다.

3.4 Command 모드

스위치의 명령줄 인터페이스(Command Line Interface)는 여러 모드로 구분됩니다. 각 명령 모드는 서로 다른 그룹웨어를 구성할 수 있도록 설계되었습니다. 현재 사용 가능한 명령어는 사용자가 위치한 명령 모드에 따라 달라집니다.

다른 명령 모드에서 물음표(?)를 입력하면 사용할 수 있는 명령어 목록을 확인할 수 있습니다. 일반적인 명령 모드는 다음 표에 나와 있습니다:

Command 모드	Login 모드	프롬프트	Exit 모드
시스템 모니터링모드	전원이 켜진 후 Ctrl-p 를 입력하세요.	monitor#	실행 종료.
유저 모드	로그인	Switch>	exit 또는 quit 명령어를 실행하세요.
Privileged Mode	사용자 모드에서 enter 또는 enable 을 입력합니다.	Switch#	exit 또는 quit 명령어를 실행하세요.

Global Config Mode	관리 모드에서 config 를 입력합니다.	Switch_config#	exit, quit 또는 Ctrl-z 를 실행하여 관리 모드로 바로 돌아가십시오.
포트 설정 모드	구성 모드에서 인터페이스 명령(예: 인터페이스 g1/1)을 입력합니다.	Switch_config_g1/1#	exit, quit 또는 Ctrl-z 를 실행하여 관리 모드로 바로 돌아가십시오.

각 명령 모드는 일부 명령의 하위 집합에는 적합하지 않을 수 있습니다. 명령어를 입력할 때 문제가 발생하면, 프롬프트를 확인하고 물음표(?)를 입력하여 사용 가능한 명령어 목록을 확인하십시오.

문제는 잘못된 명령 모드에서 실행하거나 명령어를 잘못 입력했을 때 발생할 수 있습니다.

다음과 같은 경우에는 인터페이스 프롬프트의 변경 사항과 해당 명령 모드에 주의하세요.

Switch> enable

Switch# config

Switch_config# interface g1/1

Switch_config_g1/1# exit

Switch_config# exit

Switch#

3.5 Commnad 취소

명령어를 취소하거나 기본 속성으로 복원하려면 대부분의 명령어 앞에 **"no"** 키워드를 추가하십시오. 예시는 다음과 같습니다:

no <명령어>

3.6 설정 저정하기

시스템이 재시작 되거나 갑작스럽게 전원이 꺼질 경우를 대비하여 설정을 저장해야 합니다. 설정을 저장하면 원래 구성을 신속하게 복구할 수 있습니다.

관리 모드 또는 오피스 구성 모드에서 write 명령어를 실행하여 구성을 저장할 수 있습니다.

4. CLI 명령어 규칙

4.1 규칙

구문	의미
Bold	명령줄에서 변경 없이 입력해야 하는 키워드를 나타내며, 명령줄에서 굵은 글씨로 표시됩니다.
{italic}	명령줄에서 실제 값으로 대체해야 하는 매개변수를 나타내며, 중괄호 안에 이탤릭체로 표시됩니다.
<italic>	명령줄에서 실제 값으로 대체해야 하는 매개변수를 나타내며, 꺾쇠 괄호 안에 이탤릭체로 표시됩니다.
[ ]	대괄호 안에 있는 선택적 매개변수를 나타냅니다.
{ x | y | ... }	두 개 이상의 옵션에서 하나의 옵션을 선택할 수 있음을 의미합니다.
[x | y | ...]	두 개 이상의 옵션에서 하나의 옵션을 선택하거나 아무것도 선택하지 않을 수 있음을 의미합니다.
{ x | y | ... } *	* 두 개 이상의 옵션에서 적어도 하나의 옵션을 선택하거나 모든 옵션을 선택해야 함을 의미합니다.
[x | y | ...] *	* 두 개 이상의 옵션에서 여러 옵션을 선택하거나 아무것도 선택하지 않을 수 있음을 의미합니다.
&<1-n>	&<1-n> "&" 기호 앞의 매개변수를 1~n번 입력할 수 있음을 의미합니다.
#	# "#" 기호로 시작하는 줄이 설명 줄임을 의미합니다.

5. 최초 로그인 및 인증 관리

5.1 콘솔 및 관리접속 로그인

제품은 로컬(콘솔)과 원격관리(SSH, Telnet)의 명령어 CLI가 동일 합니다.

콘솔 프로그램 : Putty (속도 : 9600bps, 데이터비트 8, 패리티 없음, 정지 비트 1)

1. PC와 제품의 콘솔 포트를 시리얼 케이블로 연결합니다.

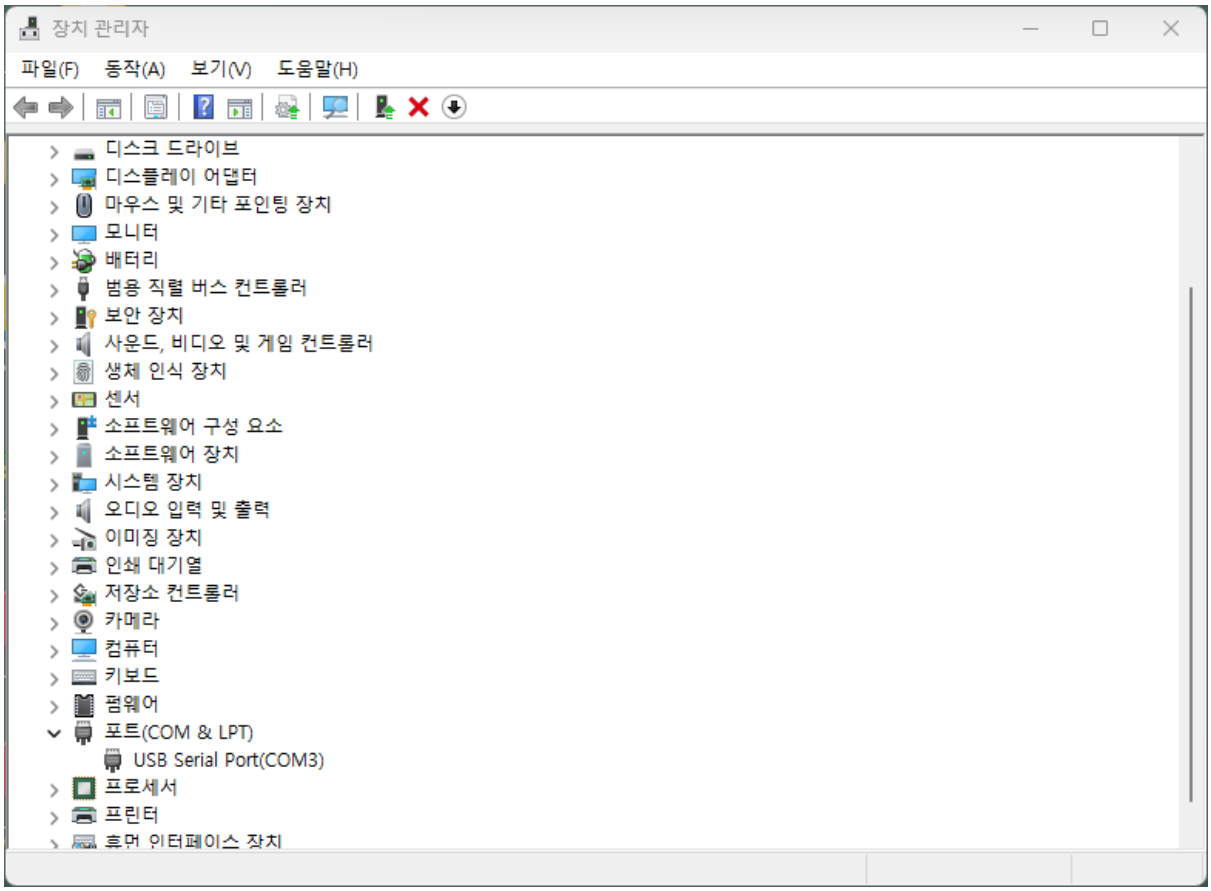


그림 4 장치관리자에서 COM 포트 확인

2. 장치관리자에서 현재 사용하고 있는 COM포트를 확인합니다.
3. Putty 및 다른 접속 프로그램등을 실행합니다.

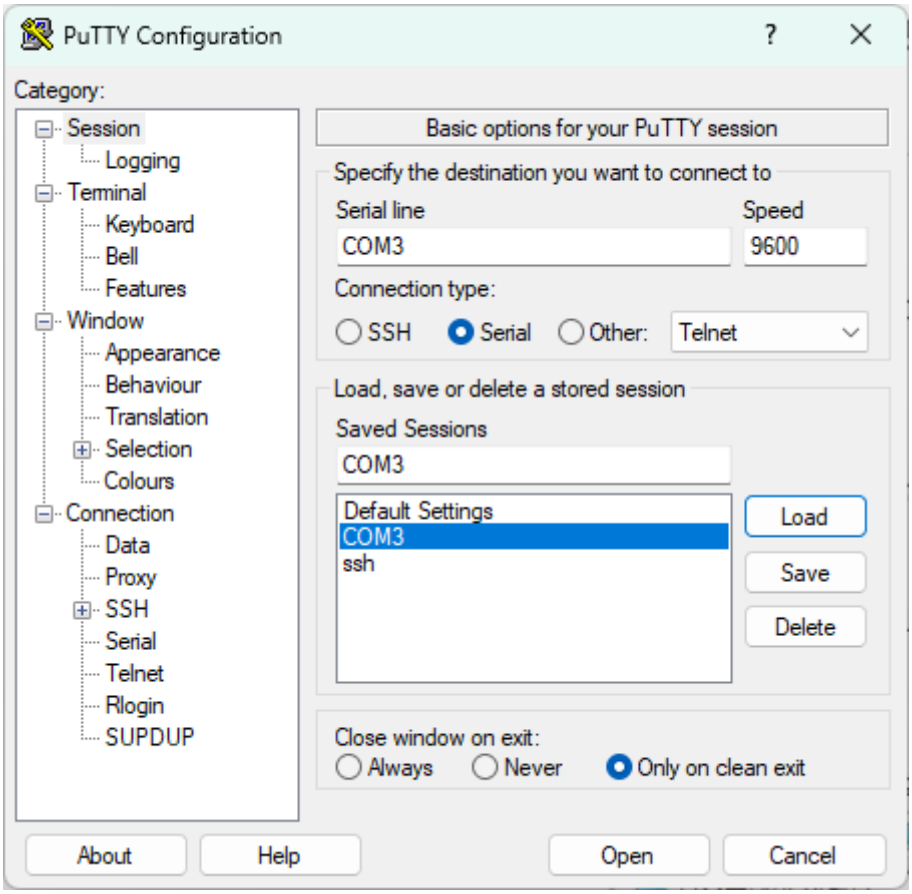


그림 5 Putty 접속

4. 기본 관리자 계정 및 암호

   admin / Mirae12%^

5. SSH 및 Telnet 접속은 콘솔 접속 후 SSH 활성화 후 접속 할 수 있습니다.
6. 최초 접속 시 강제로 비밀번호를 변경 해야 합니다.

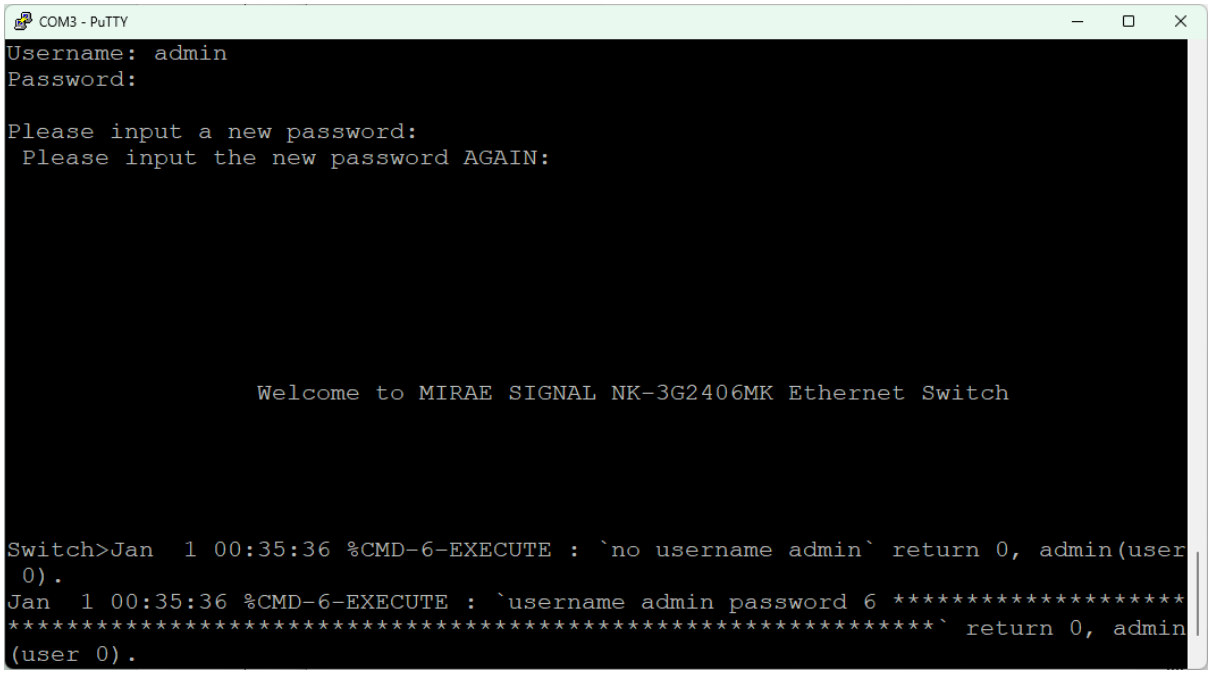


그림 6 비밀번호 강제 변경

5.2 비밀번호 규칙 설정

최초 로그인 시 아래의 정해진 규칙에 따라 비밀번호를 변경해야 합니다.

구분	내용
준수 사항	9자리 이상의 길이 설정 가능
	숫자, 대문자(영문), 소문자(영문), 특수문자 중에서 3가지 이상의 조합으로 입력 가능
금지 항목	사용자 계정(ID)과 동일한 패스워드 설정 금지
	동일한 문자·숫자의 연속적인 반복입력 금지
	키보드상의 연속된 문자 또는 숫자의 순차적 입력금지
	직전 사용된 패스워드 재사용 금지
	3개월 이내 사용된 패스워드 재사용 금지

위의 내용으로 알맞게 비밀번호를 변경하여 접속할 수 있습니다.

비밀 번호 규칙 설정 변경 및 확인 방법

명령어	설명
enable	운용모드를 변경합니다.

config	설정 모드로 진입합니다.
Switch_config#localpass default	스위치의 로컬 패스워드를 설정하거나 변경하는 명령어입니다.
Switch_config_localpass_default#min-length 9	9자리이상 사용
Switch_config_localpass_default#element number lower-letter upper-letter special-character	숫자, 소문자, 대문자, 특수문자 사용합니다.
Switch_config_localpass_default#non-user	사용자 계정과 동일한 패스워드 금지
Switch_config_localpass_default#non-repeat	동일한 연속된 문자 반복금
Switch_config_localpass_default#non-seqlisting	키보드상의 연속된 문자 금지
Switch_config_localpass_default#non-history	직전암호 사용금지
Exit	설정 모드에서 이전으로 되돌아갑니다.
Switch_config#local pass-group default	설정 후 입력되는 사용자 계정에 대한 비밀번호에 그룹 규칙을 적용
Switch_config#local pass-group default#show run	설정된 규칙을 확인 합니다.

6. 터미널 설정

6.1 VTY 설정

시스템은 line 명령을 사용하여 터미널 매개변수를 구성합니다. 명령을 통해 터미널이 표시하는 너비와 높이를 구성할 수 있습니다.

6.2 설정

시스템에는 네 가지 유형의 라인이 있습니다: 콘솔(console), AID, 비동기(asynchronous) 및 가상 터미널(virtual terminal).

이들 라인의 개수는 시스템마다 다를 수 있습니다. 올바른 구성을 위해 소프트웨어 및 하드웨어 구성 가이드를 참조하세요.

라인 우형	인터페이스	설명	넘버링
CON(CTY)	Console	구성을 위해 시스템에 로그인합니다.	0
VTY	Virtual , asynchronous	시스템의 동기 포트(예: 이더넷 및 직렬 포트)의 Telnet, X.25 PAD, HTTP 및 Rlogin 을 연결하려면	1 ~ 32

6.2.1 라인과 인터페이스의 관계

1. 동기 인터페이스와 VTY 라인의 관계

가상 터미널 라인은 시스템에 액세스하기 위한 동기 인터페이스를 제공합니다. VTY 라인을 통해 시스템에 연결하면 실제로 인터페이스의 가상 포트에 연결됩니다. 각 동기 인터페이스에는 여러 개의 가상 포트가 있을 수 있습니다.

예를 들어, 여러 Telnet이 인터페이스(이더넷 또는 직렬 인터페이스)에 연결되는 경우 VTY 구성을 위해 다음 단계를 수행해야 합니다.

- 라인 구성 모드에 로그인합니다.
- 터미널 매개변수를 구성합니다.

VTY 구성의 경우 2.4 "VTY 구성 예"를 참조하십시오.

6.3 모니터 및 유지 관리

VTY 구성을 확인하려면 show line을 실행하세요.

6.4 VTY 구성 예

다음은 모든 VTY(가상 터미널)에서 화면당 라인 수 제한을 취소하고 추가 프롬프트 없이 설정하는 방법을 보여줍니다

config#line vty 0 4 (최대 5개의 동시 접속)_

config_line# exec-timeout 300 (300초 이후에 세션 접속 종료)

7. 네트워크 관리 구성

7.1 SNMP 구성

7.1.1 개요

SNMP 시스템은 다음과 같은 부분으로 구성됩니다.

- SNMP management side (NMS)
- SNMP agent (AGENT)
- Management information base (MIB)

SNMP는 애플리케이션 계층에서 작동하는 프로토콜입니다. SNMP 관리 측과 에이전트 간의 패킷 형식을 제공합니다.

SNMP 관리 측은 네트워크 관리 시스템(CiscoWorks와 같은 NMS)의 일부가 될 수 있습니다. 에이전트와 MIB는 시스템에 저장됩니다. 시스템에서 SNMP를 구성하기 전에 네트워크 관리 측과 에이전트 간의 관계를 정의해야 합니다.

SNMP 에이전트에는 MIB 변수가 포함되어 있습니다. SNMP 관리 측은 이러한 변수의 값을 확인하거나 수정할 수 있습니다. 관리 측은 에이전트에서 변수 값을 가져오거나 변수 값을 에이전트에 저장할 수 있습니다. 에이전트는 MIB에서 데이터를 수집합니다. MIB는 장치 매개변수와 네트워크 데이터의 데이터베이스입니다. 에이전트는 또한 관리 측의 로딩이나 데이터 구성 요청에 응답할 수 있습니다. SNMP 에이전트는 관리 측에 트랩을 보낼 수 있습니다. 트랩은 네트워크의 특정 상태를 나타내는 알람 정보를 NMS에 보냅니다. 트랩은 부적절한 사용자 인증, 재시작, 링크 계층 상태(활성화 또는 비활성화), TCP 연결 종료, 인접 시스템과의 연결 끊김 또는 기타 중요한 이벤트를 지적할 수 있습니다.

1. SNMP notification

일부 특수 이벤트가 발생하면 시스템은 SNMP 관리 측에 'inform'을 보냅니다. 예를 들어, 에이전트 시스템이 비정상적인 조건을 감지하면 관리 측에 정보를 보냅니다.

SNMP 알림은 트랩(trap) 또는 정보 요청(inform request)으로 처리되어 전송될 수 있습니다.

트랩을 수신하는 측에서는 응답을 보내지 않기 때문에, 트랩이 실제로 수신되었는지 확신할 수 없습니다. 따라서 트랩은 신뢰성이 낮습니다.

반면, 정보 요청(inform request)을 수신한 SNMP 관리 측은 이 정보를 회신하기 위해 SNMP가 에코 역할을 하는 PDU를 사용합니다. 관리 측에서 "정보 요청"을 수신하지 못하면 에코가 전송되지 않습니다.

수신 측이 응답을 보내지 않으면 "정보 요청"을 다시 전송할 수 있습니다. 이를 통해 알림이 목적지에 도달할 수 있습니다.

정보 요청이 더 신뢰성이 높기 때문에, 시스템과 네트워크의 리소스를 더 많이 소모합니다.

트랩은 전송 후 바로 삭제되지만, "정보 요청"은 에코를 수신하거나 요청이 타임아웃될 때까지 메모리에 저장되어야 합니다.

또한, 트랩은 한 번만 전송되지만, "정보 요청"은 여러 번 재전송될 수 있습니다.

"정보 요청"의 재전송은 네트워크 통신량을 증가시키고 네트워크에 더 많은 부하를 야기합니다.

따라서, 트랩과 정보 요청은 신뢰성과 리소스 간의 균형을 제공합니다.

2. SNMP Version

- SNMPv1 : 간단한 네트워크 관리 프로토콜, RFC1157에 정의된 완전한 인터넷 표준입니다.
- SNMPv2C : RFC1901에 정의된 인터넷 테스트 프로토콜인 SNMPv2의 그룹 기반 관리 프레임워크입니다.
- SNMPv3 : RFC3410에 정의된 간단한 네트워크 관리 프로토콜 버전 3입니다.

SNMPv1은 그룹 기반 보안 형식을 사용합니다. IP 주소 액세스 제어 목록과 비밀번호를 사용하여 에이전트 MIB에 액세스할 수 있는 관리 측 그룹을 정의합니다.

SNMPv3는 네트워크를 통해 패킷을 인증하고 암호화하는 것을 결합하여 장치에 대한 보안 액세스를 제공합니다.

SNMPv3에서 제공되는 보안 기능은 다음과 같습니다.

- 메시지 무결성 : 패킷이 전송 중에 변조되지 않았는지 확인합니다.
- 인증 : 메시지가 유효한 출처에서 온 것인지 확인합니다.
- 암호화 : 패킷의 내용을 암호화하여 허가되지 않은 출처에서 패킷이 보이지 않도록 방지합니다.

SNMPv3는 보안 모델과 보안 수준을 모두 제공합니다. 보안 모델은 사용자가 접속하는 그룹에 대해 설정된 인증 전략입니다. 보안 수준은 보안 모델 내에서 허용되는 보안 수준입니다. 보안 모델과 보안 수준의 조합은 SNMP 패킷을 처리할 때 사용되는 보안 메커니즘을 결정합니다. 세 가지 보안 모델, 즉 인증 및 암호화, 인증 및 암호화 없음, 인증 없음을 사용할 수 있습니다.

SNMP 에이전트를 관리 작업 스테이션이 지원하는 SNMP 버전으로 구성해야 합니다. 에이전트는 많은 관리 측과 통신할 수 있습니다.

7.1.2 SNMP 구성 작업

- SNMP 뷰 구성

- SNMP 커뮤니티에 대한 액세스 제어 생성 또는 수정
- 시스템 관리자의 연락 방법 및 시스템 위치 구성
- SNMP 에이전트 데이터 패킷의 최대 길이 정의
- SNMP 상태 모니터링
- SNMP 트랩 구성
- SNMP 바인딩 소스 주소 구성
- SNMPv3 그룹 구성
- SNMPv3 사용자 구성
- SNMPv3 EngineID 구성

1. SNMP view 설정

SNMP 뷰는 MIB에 대한 액세스 권한(포함 또는 제외)을 조절하는 것입니다. 다음 명령어를 사용하여 SNMP 뷰를 구성합니다.

명령어	설명
snmp-server view name oid] [exclude | include]	OID 가 지정한 MIB 의 서브트리 또는 테이블을 SNMP 뷰의 이름에 추가하고, SNMB 뷰의 이름에 개체 식별자의 액세스 권한을 지정합니다. Exclude: 액세스 거부 Include: 액세스 허용

SNMP 뷰에서 액세스할 수 있는 하위 집합은 MIB 객체를 " Include "하고 " Exclude " 객체로 구분된 나머지 객체입니다. 구성되지 않은 객체는 기본적으로 액세스할 수 없습니다.

SNMP 보기를 구성한 후에는 SNMP 그룹 이름 구성에 SNMP 보기를 구현하여 그룹 이름이 액세스할 수 있는 개체의 하위 집합을 제한할 수 있습니다.

2. SNMP 커뮤니티에 대한 액세스 제어 생성 또는 수정

SNMP 커뮤니티 문자열을 사용하여 SNMP 관리 측과 에이전트 간의 관계를 정의할 수 있습니다. 커뮤니티 문자열은 에이전트에 로그인하기 위해 액세스 시스템에서 사용하는 비밀번호와 유사한 역할을 합니다.

SNMP 관리 측의 IP 주소에 대한 액세스 목록을 커뮤니티 문자열로 사용할 수 있도록 허용합니다.

지정된 커뮤니티가 액세스할 수 있는 MIB 객체 하위 집합의 MIB 뷰 정의합니다.

접근 가능한 MIB 객체를 읽고 쓸 수 있는 권한을 가진 커뮤니티 지정합니다.

글로벌 구성 모드에서 다음 명령어를 사용하여 커뮤니티 문자열을 구성하십시오

명령어	설명
snmp-server community string [view view-name] [ro | rw] [word]	그룹 액세스 문자열을 정의합니다.

하나 이상의 그룹 문자열을 구성할 수 있습니다.
지정된 커뮤니티 문자열을 제거하려면 no snmp-server community 명령어를 실행하십시오.

커뮤니티 문자열 구성 방법에 대한 자세한 내용은 "SNMP 명령어" 섹션을 참조하십시오.

3. 시스템 관리자 연락 방법 및 시스템 위치 구성

SysContact와 sysLocation은 MIB의 시스템 그룹에서 관리 변수로, 각각 제어 노드의 담당자 식별자와 실제 위치를 정의합니다. 이 정보는 구성 파일을 통해 액세스할 수 있습니다.

글로벌 구성 모드에서 다음 명령어를 사용할 수 있습니다.

명령어	설명
snmp-server contact text	노드의 문자열을 설정합니다.
snmp-server location tex	노드 위치에 대한 문자열을 설정합니다.

4. SNMP 에이전트 데이터 패킷의 최대 길이 정의

SNMP 에이전트가 요청을 수신하거나 응답을 보낼 때 데이터 패킷의 최대 길이를 구성할 수 있습니다.
글로벌 구성 모드에서 다음 명령어를 사용하십시오

명령어	설명
snmp-server packetsize byte-count	데이터 패킷의 최대 길이를 설정합니다.

5. SNMP 상태 모니터링

다음 명령을 글로벌 구성 모드에서 실행하여 SNMP

출력/입력 통계(불법 커뮤니티 문자열 항목, 실수 수 및 요청 변수 포함)를 모니터링할 수 있습니다.

명령어	설명

show snmp	SNMP 상태를 모니터링 합니다.

6. SNMP 트랩 구성

다음 명령을 사용하여 SNMP 트랩을 보내도록 시스템을 구성합니다(두 번째 작업은 선택 사항입니다)

- 트랩을 보내도록 시스템 구성

호스트로 트랩을 보내도록 시스템을 구성하려면 글로벌 구성 모드에서 다음 명령을 실행하세요.

명령어	설명
snmp-server host host community-string [trap-type]	랩 메시지의 수신자를 지정합니다.
snmp-server host host [traps|informs]{version {v1 | v2c | v3 {auth | noauth | priv } }}community-string [trap-type]	랩 메시지의 수신자, 버전 번호 및 사용자 이름을 지정합니다. 참고: SNMPv3 트랩의 경우 호스트가 트랩 메시지를 수신하도록 구성되기 전에 호스트에 대한 SNMP 엔진 ID 를 구성해야 합니다.

시스템이 시작되면 SNMP 에이전트가 자동으로 실행됩니다. 모든 유형의 트랩이 활성화됩니다. snmp-server host 명령을 사용하여 어떤 호스트가 어떤 종류의 트랩을 수신할지 지정할 수 있습니다.

일부 트랩은 다른 명령을 통해 제어해야 합니다. 예를 들어, 인터페이스가 열리거나 닫힐 때 SNMP 링크 트랩을 보내려면 인터페이스 구성 모드에서 snmp trap link-status를 실행하여 링크 트랩을 활성화해야 합니다. 이러한 트랩을 닫으려면 인터페이스 구성 명령 snmp trap link-stat를 실행합니다.

호스트가 트랩을 수신할 수 있도록 snmp-server host 명령을 구성해야 합니다.

- 트랩의 실행 매개변수 수정

선택 항목으로, 트랩이 발생하는 소스 인터페이스, 메시지의 큐 길이 또는 각 호스트에 대한 재전송 간격 값을 지정할 수 있습니다. 트랩의 실행 매개변수를 수정하려면 글로벌 구성 모드에서 다음 선택 명령을 실행할 수 있습니다.

명령어	설명

snmp-server trap-source interface	트랩이 발생하는 소스 인터페이스를 지정하고 메시지의 소스 IP 주소를 설정합니다.
snmp-server queue-length length	트랩이 있는 각 호스트에 대한 메시지의 큐 길이를 생성합니다. 기본값: 10
snmp-server trap-timeout seconds	전송 대기열에서 트랩을 재전송하는 빈도를 정의합니다. 기본값: 30 초

7. SNMP 바인딩 소스 주소 구성

SNMP 메시지의 소스 주소를 설정하려면 글로벌 구성 모드에서 다음 명령을 실행하세요.

명령어	설명
snmp source-addr ipaddress	SNMP 메시지의 소스 주소를 설정합니다.

8. SNMPv3 그룹 구성

다음 명령을 실행하여 그룹을 구성합니다.

명령어	설명
snmp-server group [groupname {v1 | v2c |v3 [auth | noauth | priv]}][read readview][write writeview] [notify notifyview] [access access-list]	SNMPv3 그룹을 구성합니다. 기본적으로 인터넷의 하위트리에 있는 모든 항목만 읽을 수 있습니다.

9. SNMPv3 사용자 구성

다음 명령을 실행하여 로컬 사용자를 구성할 수 있습니다. 관리자가 장치에 로그인하려면 장치에 구성된 사용자 이름과 비밀번호를 사용해야 합니다. 사용자의 보안 수준은 사용자가 속한 그룹의 보안 수준보다 높거나 같아야 합니다. 그렇지 않으면 사용자는 인증에 실패하게 됩니다.

명령어	설명
snmp-server user username groupname {v1 | v2c | v3 [encrypted] [auth {md5 |	로컬 SNMPv3 사용자를 구성합니다.

sha} auth-password]} [access access-list]	

다음 명령을 실행하여 원격 사용자를 구성할 수 있습니다. 장치가 원격 제어 스테이션에 트랩을 보내야 하는 경우 제어 스테이션이 ID 인증을 수행하는 경우 원격 사용자를 구성해야 합니다. 원격 사용자의 사용자 이름과 비밀번호는 제어 스테이션의 사용자 이름과 비밀번호와 동일해야 합니다.

그렇지 않으면 제어 스테이션이 트랩을 수신할 수 없습니다.

명령어	설명
snmp-server user username groupname remote ip-address Configures a remote SNMPv3 user. - 16 -Basic Configuration [udp-port port] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access access-list]	원격 SNMPv3 사용자를 구성합니다. 참고: 원격 사용자를 구성하기 전에 IP 주소의 제어 스테이션에 대한 원격 SNMP 엔진 ID 를 구성해야 합니다.

10. SNMPv3 엔진 ID 구성

SNMP 엔진 ID는 SNMP 엔진을 식별하는 것입니다. 기존 SNMP 관리자 및 에이전트는 SNMPv3 프레임의 SNMP 엔진의 일부입니다.

명령어	설명
snmp-server engineID remote ip-address [udp-port port-number] engineid-string	원격 SNMP 엔진을 구성합니다.

7.1.3 설정 예시

1. 예시

snmp-server community public RO

snmp-server community private RW

snmp-server host 192.168.10.2 public

모든 MIB 변수를 읽을 수만 있는 커뮤니티 문자열을 public으로 설정하는 방법.

모든 MIB 변수를 읽고 쓸 수 있는 커뮤니티 문자열을 비공개로 설정하는 방법.

커뮤니티 문자열 public을 사용하여 시스템에서 MIB 변수를 읽을 수 있습니다. 커뮤니티 문자열 private을 사용하여 시스템에서 MIB 변수를 읽고 쓰기 가능한 MIB 변수를 쓸 수도 있습니다.

위의 명령은 시스템에서 트랩을 보내야 할 때 192.168.10.2로 트랩을 보내도록 커뮤니티 문자열 public을 지정합니다. 예를 들어, 시스템의 포트가 다운 상태일 때 시스템은 192.168.10.2로 링크 다운 트랩 정보를 보냅니다.

2. 예시

snmp-server engineID remote 10.0.0.3 80000523015a000003

snmp-server group getter v3 auth

snmp-server group setter v3 priv write v-write

snmp-server user get-user getter v3 auth sha 12345678

snmp-server user set-user setter v3 encrypted auth md5 12345678 snmp-server user notifier getter remote 90.0.0.3 v3 auth md5 abcdefghi snmp-server host 90.0.0.3 informs version v3 auth notifier

snmp-server view v-write internet included

위의 예는 SNMPv3를 사용하여 장치를 관리하는 방법을 보여줍니다. 그룹 getter는 장치 정보를 검색할 수 있고, 그룹 setter는 장치를 설정할 수 있습니다. 사용자 get-user는 그룹 getter에 속하고, 사용자 set-user는 그룹 setter에 속합니다.

사용자 get-user의 경우 보안 수준은 authenticate이지만 encrypt는 아니고, 비밀번호는 12345678이며, sha 산술을 사용하여 비밀번호를 요약합니다.

사용자 set-user의 경우 보안 수준은 authenticate 및 encrypt이고, 비밀번호는 12345678이며, md5 산술을 사용하여 비밀번호를 요약합니다.

장치에서 주요 이벤트가 발생하면 username notifier를 사용하여 관리자의 호스트 10.0.0.3에 inform 메시지를 보냅니다.

7.2 RMON 구성

7.2.1 RMON 구성 작업

RMON 구성 작업에는 다음이 포함됩니다.

- 스위치에 대한 RMON 알람 기능 구성

- 스위치에 대한 RMON 이벤트 기능 구성
- 스위치에 대한 RMON 통계 기능 구성
- 스위치에 대한 RMON 기록 기능 구성
- 스위치의 RMON 구성 표시

1. 스위치에 대한 RMON 알람 구성

명령줄이나 SNMP NMS를 통해 RMON 알람 기능을 구성할 수 있습니다. SNMP NMS를 통해 구성하는 경우 스위치의 SNMP를 구성해야 합니다. 알람 기능이 구성된 후, 장치는 시스템에서 일부 통계 값을 모니터링할 수 있습니다. 다음 표는 RMON 알람 기능을 설정하는 방법을 보여줍니다.

명령어	설명
configure	Config 모드로 진입합니다.
rmon alarm index variable interval {absolute | delta} rising-threshold value [eventnumber] falling-threshold value [eventnumber] [owner string]	알람 항목을 추가합니다. index 는 알람 항목의 인덱스입니다. 유효 범위는 1~65535 입니다. variable 은 모니터링되는 MIB 의 객체입니다. 시스템에서 유효한 MIB 객체여야 합니다. Integer, Counter, Gauge 또는 TimeTicks 유형의 객체만 감지할 수 있습니다. interval 은 샘플링을 위한 시간 섹션입니다. 단위는 초입니다. 유효 값은 1~4294967295 입니다. absolute 는 MIB 객체의 값을 직접 모니터링하는 데 사용됩니다. delta 는 두 샘플링 사이의 MIB 객체 값 변경을 모니터링하는 데 사용됩니다. value 는 알람이 생성될 때의 임계값입니다. eventnumber 는 임계값에 도달할 때 생성되는 이벤트의 인덱스입니다. eventnumber 는 선택 사항입니다. owner 문자열은 알람에 대한 정보를 설명합니다.
Exit	Config 모드에서 관리모드로 돌아갑니다.
write	설정 값을 저장합니다.

RMON 알람 항목이 구성된 후, 장치는 간격 후에 변수로 지정된 oid의 값을 가져옵니다. 가져온 값은 알람 유형(절대 또는 델타)에 따라 이전 값과 비교됩니다. 가져온 값이 이전 값보다 크고 rising-threshold로 지정된 임계값을 초과하는 경우, 인덱스가 eventnumber인 이벤트(eventnumber의 값이 0이거나 인덱스가 eventnumber인 이벤트가 이벤트 테이블에 없는 경우, 이 벤트는 발생하지 않음)가 발생합니다. 변수로 지정된 oid를 가져올 수 없는 경우, 이 줄의 알람

항목의 상태는 무효로 설정됩니다. rmon alarm을 여러 번 실행하여 동일한 인덱스로 알람 항목을 구성하는 경우, 마지막 구성만 적용됩니다. no rmon alarm index를 실행하여 인덱스가 index인 알람 항목을 취소할 수 있습니다.

2. 스위치에 대한 RMON 이벤트 구성

RMON 이벤트를 구성하는 단계는 다음 표를 참고하십시오

명령어	설명
configure	Config 모드로 진입합니다.
rmon event index [description string] [log] [owner string] [trap community]	이벤트 항목을 추가합니다. index 는 이벤트 항목의 인덱스를 의미합니다. 유효 범위는 1~65535 입니다. Description 은 이벤트에 대한 정보를 의미합니다. log 는 이벤트가 발생할 때 로그 테이블에 정보를 추가하는 것을 의미합니다. trap 은 이벤트가 트리거될 때 트랩 메시지가 생성됨을 의미합니다. 커뮤니티는 커뮤니티의 이름을 의미합니다. owner string 은 알람에 대한 정보를 설명 합니다.
Exit	Config 모드에서 관리모드로 돌아갑니다.
write	설정 값을 저장합니다.

RMON 이벤트를 구성한 후, RMON 알람이 트리거될 때 해당 RMON 이벤트 항목의 eventLastTimeSent 도메인을 sysUpTime으로 설정해야 합니다. RMON 이벤트에 로그 속성을 설정하면 메시지가 로그 테이블에 추가됩니다. RMON 이벤트에 트랩 속성을 설정하면 커뮤니티 이름으로 트랩 메시지가 전송됩니다.

동일한 인덱스를 가진 이벤트 항목을 구성하기 위해 여러 번 RMON event 명령을 실행하면, 마지막으로 실행한 구성만 유효합니다.
특정 인덱스를 가진 이벤트 항목을 취소하려면 no rmon event index 명령을 실행하면 됩니다.

3. 스위치에 대한 RMON 통계 구성

RMON 통계 그룹은 장치의 모든 포트에서 통계 정보를 모니터링하는 데 사용됩니다. RMON 통계를 구성하는 단계는 다음과 같습니다.

명령어	설명
configure	Config 모드로 진입합니다.

interface iftype ifid	포트 모드로 들어갑니다. iftype 은 포트의 유형을 의미합니다. ifid 는 인터페이스의 ID 를 의미합니다.
rmon collection stat index [owner string]	포트에서 통계 기능을 활성화합니다. index 는 통계의 인덱스를 의미합니다. owner 문자열은 통계에 대한 정보를 설명합니다.
Exit	글로벌 오피스 모드로 돌아갑니다.
Exit	관리모드로 돌아갑니다.
write	설정 값을 저장합니다.

RMON collection stat를 여러 번 실행하여 동일한 인덱스로 통계 항목을 구성하는 경우 마지막 구성만 유효합니다. no rmon collection stats index를 실행하여 인덱스가 index인 통계 항목을 취소할 수 있습니다.

4. 스위치에 대한 RMON 기록

명령어	설명
configure	Config 모드로 진입합니다.
interface iftype ifid	포트 모드로 들어갑니다. iftype 은 포트의 유형을 의미합니다. ifid 는 인터페이스의 ID 를 의미합니다.
rmon collection history index [buckets bucket-number] [interval second] [owner owner-name	포트에서 기록 기능을 활성화합니다. index 는 기록 항목의 인덱스를 의미합니다. 기록 항목에서 수집한 모든 데이터 중에서 최신 버킷 번호 항목을 저장해야 합니다. 이더넷의 기록 항목을 탐색하여 이러한 통계 값을 얻을 수 있습니다. 기본값은 50 개 항목입니다. second 는 통계 데이터를 매번 얻는 간격을 의미합니다. 기본값은 1800 초입니다. owner 문자열은 기록 항목에 대한 일부 정보를 설명하는 데 사용됩니다..
Exit	글로벌 오피스 모드로 돌아갑니다.
Exit	관리모드로 돌아갑니다.

write	설정 값을 저장합니다.

RMON 기록 항목이 추가되면 장치는 지정된 포트에서 2초마다 통계 값을 가져옵니다. 통계 값은 정보의 일부로 기록 항목에 추가됩니다. rmon collection history index를 여러 번 실행하여 동일한 인덱스로 기록 항목을 구성하는 경우 마지막 구성만 유효합니다. no rmon history index를 실행하여 인덱스가 index인 기록 항목을 취소할 수 있습니다.

5. 스위치의 RMON 구성 표시

명령어	설명
show rmon [alarm] [event] [statistics] [history]	rMon 구성 정보를 표시합니다. alarm: 알람 항목의 구성을 표시합니다. event: 이벤트 항목의 구성을 표시하고, 이벤트 발생으로 생성되어 로그 테이블에 포함된 항목을 표시합니다. statistics: 통계 항목의 구성과 장치가 포트에서 수집한 통계 값을 표시합니다. history: 히스토리 항목의 구성과 장치가 포트에서 최근 지정된 간격으로 수집한 통계 값을 표시합니다.

7.3 PDP 설정

7.3.1 개요

PDP는 네트워크 장치를 감지하는 데 특별히 사용되는 2계층 프로토콜입니다. PDP는 네트워크 관리 서비스(NMS)에서 이미 알려진 장치의 모든 인접 장치를 감지하는 데 사용됩니다. PDP를 사용하면 SNMP 에이전트 주소와 인접 장치 유형을 알 수 있습니다. PDP를 통해 인접 장치가 감지된 후 NMS는 SNMP를 통해 인접 장치를 요구하여 네트워크 토폴로지를 얻을 수 있습니다.

당사 스위치는 PDP를 통해 인접 장치를 감지할 수 있지만 SNMP를 통해 인접 장치를 요구할 수는 없습니다. 따라서 이러한 스위치는 네트워크의 가장자리에 위치해야 합니다. 그렇지 않으면 전체 네트워크 토폴로지를 얻을 수 없습니다.

스위치의 PDP는 이더넷과 같은 모든 SANP에서 구성할 수 있습니다.

1. 스위치의 기본 PDP 구성

기능	기본 설정
PDP 글로벌 구성 상태	비활성화
PDP 포트 구성 상태	비활성화

PDP 클럭(메시지 전송 주파수)	60 초
PDP 정보 저장	180 초
PDP 버전	2

2. PDP 정보 저장 시간 설정

PDP가 메시지를 보내는 빈도와 PDP 정보 저장 시간을 설정하려면 글로벌 구성 모드에서 다음 명령을 실행하세요.

명령어	설명
pdp timer seconds	PDP 가 메시지를 보내는 빈도를 설정합니다.
pdp holdtime seconds	PDP 정보 저장 시간을 설정합니다.

3. PDP 버전 설정

PDP 버전을 설정하려면 글로벌 구성 모드에서 다음 명령을 실행하세요.

명령어	설명
pdp version {1|2}	PDP 버전을 설정 합니다.

4. 스위치에서 PDP 활성화

PDP는 기본 구성에서 활성화되지 않습니다. PDP를 사용하려면 글로벌 구성 모드에서 다음 명령을 실행하세요.

명령어	설명
pdp run	PDP 를 활성화 합니다.

5. 스위치 포트에서 PDP 활성화

PDP는 기본 구성에서 활성화되지 않습니다. 스위치에서 PDP가 활성화된 후 인터페이스 구성 모드에서 다음 명령을 실행하여 포트에서 PDP를 활성화할 수 있습니다.

명령어	설명
pdp enable	PDP 스위치 포트에서 활성화 합니다.

6. PDP 관리 및 모니터링

PDP를 모니터링하려면 관리 모드에서 다음 명령을 실행하세요.

명령어	설명
show pdp traffic	스위치가 수신하고 보내는 PDP 메시지 수를 표시합니다.
show pdp neighbor [detail]	PDP 를 통해 스위치가 감지한 주변 장치를 표시합니다.

7.3.2 PDP 설정 예시

1. 예시

config# pdp run

config# int f0/0

config_f0/0#pdp enable

2. 예시

PDP 정보 저장 시간 설정

config#pdp timer 30

config#pdp holdtime 90

3. PDP 버전 셋팅

config#pdp version 1

4. PDP 정보 모니터링

config#show pdp neighbors

코드 : R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r – Repeater

장치 ID 로컬 인터페이스 홀드타임 기능 플랫폼 포트 ID

8. SSH 설정

9.1 개요

8.1.1 SSH 서버

SSH 서버를 통해 SSH 클라이언트와 장치 간에 안전하고 암호화된 통신 연결을 만들 수 있습니다. 연결에는 telnet과 같은 기능이 있습니다. SSH 서버는 암호화 알고리즘을 지원합니다.

8.1.2 SSH 클라이언트

SSH 클라이언트는 ssh 프로토콜에서 실행되는 애플리케이션입니다. SSH 클라이언트는 인증 및 암호화를 제공할 수 있으므로 SSH 클라이언트는 통신 장치 또는 SSH 서버를 지원하는 장치 간의 안전한 통신을 보장하며, 이러한 장치가 안전하지 않은 네트워크 조건에서 실행되더라도 마찬가지입니다. SSH 클라이언트는 des, 3des 및 blowfish를 포함한 암호화 알고리즘을 지원합니다.

8.1.3 기능

SSH 서버와 SSH 클라이언트를 지원합니다. 둘 다 Shell 애플리케이션만 지원합니다.

8.2 설정

8.2.1 인증 방법 목록 구성

SSH 서버는 로그인 인증 모드를 채택합니다. SSH 서버는 기본적으로 기본 인증 방법 목록을 사용합니다.

인증 방법 목록을 구성하려면 글로벌 구성 명령 모드에서 다음 명령을 실행하세요.

명령어	설명
Ip sshd auth_method STRING	인증 방법 목록을 구성합니다.

9.2.2 액세스 제어 목록 구성

장치의 SSH 서버에 대한 액세스를 제어하려면 SSH 서버에 대한 액세스 제어 목록을 구성해야 합니다.

글로벌 구성 모드에서 다음 명령을 실행하여 액세스 제어 목록을 구성합니다.

명령어	설명
Ip sshd access-class STRING	접근 제어 목록을 구성합니다.

9.2.3 인증 시간 초과 값 구성

클라이언트와 서버 간에 연결이 설정된 후, 설정된 시간 내에 인증을 승인할 수 없으면 서버는 연결을 끊습니다.

글로벌 구성 모드에서 다음 명령을 실행하여 구성 시간 초과 값을 구성합니다.

명령어	설명
Ip sshd timeout <60-65535>	인증 시간 초과 값을 구성합니다

9.2.4 인증 재시도 시간 구성

실패한 인증 횟수가 최대 횟수를 초과하면 SSH 서버는 새 연결이 설정되지 않는 한 인증을 재시도할 수 없습니다. 인증을 재시도하는 최대 횟수는 기본적으로 5회, 300초 입니다.

글로벌 구성 모드에서 다음 명령을 실행하여 인증을 재시도하는 최대 횟수를 구성합니다.

명령어	설명
Ip sshd timeout <60-65535>	인증을 재시도하는 최대 횟수를 구성합니다.

9.2.5 SSH 서버 활성화

SSH 서버는 기본적으로 비활성화되어 있습니다. SSH 서버가 활성화되면 디바이스는 RSA 비밀번호 쌍을 생성한 다음 클라이언트의 연결 요청을 수신합니다.

SSH 서버를 활성화하려면 글로벌 구성 모드에서 다음 명령을 실행하세요.

명령어	설명
Ip sshd enable	SSH 서버를 활성화 합니다.

9.3 SSH 서버 설정 예시

다음 구성은 IP 주소가 192.168.0.40인 호스트만 SSH 서버에 액세스할 수 있도록 허용합니다. 로컬 사용자 데이터베이스는 사용자 ID를 구별하는 데 사용됩니다.

9.3.1 Access control 리스트

ip access-list standard ssh-acl

permit 192.168.0.40

9.3.2 글로벌 설정

aaa authentication login ssh-auth local

ip sshd auth-method ssh-auth

ip sshd access-class ssh-acl

ip sshd enable

9.3.3 인증 실패 및 접속 제한

사용자가 SSH를 통해 접속 시 설정된 계정과 암호를 정확히 입력하지 않은 경우 장비 접속을 제한 할 수 있습니다.

글로벌 설정 모드에서 아래의 명령어를 실행하여 변경 할 수 있습니다.

ip sshd auth-retries 5(제한 횟수)

ip sshd silence-period 300(제한 시간)

9.4 Telnet 접속

9.4.1 Telnet 구성

Telnet(TELecommunication NETwork)은 원격지의 컴퓨터나 네트워크 장비에 접속하여 명령을 입력하고 제어할 수 있도록 하는 네트워크 프로토콜입니다. 원격 호스트에 접속하여 터미널 세션을 제공하며, TCP/IP 프로토콜을 기반으로 동작합니다.

글로벌 구성모드에서 다음 명령을 실행하여 Telnet을 활성화 및 비활성호 ㅏ합니다.

명령어	설명
Ip telnet enable	텔넷을 활성화합니다.
No ip telnet enable	텔넷을 비활성화 합니다.

9.4.2 telnet 기능

명령어	설명
Ip telnet source-interface	특정 인터페이스를 Telnet 접속의 소스로 지정합니다.
ip telnet access-class	IP 액세스 리스트를 사용하여 Telnet 접속 필터링
ip telnet access-class	Telnet 서버가 대기할 포트 지정 (기본값: 23)

ip telnet script	Telnet 스크립트 지정
Ip telnet attack-defense	Telnet 접속 제한 및 시간 제한
Ip telnet max-user	Telnet 동시 접속 가능 최대 사용자 수 설정

10 AAA 설정

10.4 AAA 개요

액세스 제어는 네트워크와 서비스에 대한 접근을 제어하는 방법입니다. 인증(Authentication), 권한 부여(Authorization), 계정 관리(Accounting, AAA) 네트워크 보안 서비스는 라우터나 액세스 서버에서 액세스 제어를 설정하기 위한 기본 프레임워크를 제공합니다.

10.1.1 AAA 보안 서비스

AAA는 세 가지 독립적인 보안 기능을 일관된 방식으로 구성하기 위한 아키텍처 프레임워크입니다. AAA는 다음과 같은 서비스를 모듈 방식으로 수행할 수 있도록 제공합니다.

- Authentication : 사용자를 식별하는 방법을 제공하며, 로그인 및 비밀번호 대화, 챌린지와 응답, 메시징 지원, 그리고 선택한 보안 프로토콜에 따라 암호화를 포함합니다.

인증(Authentication)은 사용자가 네트워크 및 네트워크 서비스에 접근하기 전에 신원을 확인하는 방식입니다.

AAA 인증을 구성하려면 인증 방법을 정의한 이름이 지정된 리스트를 생성하고, 이를 다양한 인터페이스에 적용합니다.

이 메서드 리스트는 수행할 인증 유형과 실행 순서를 정의하며, 정의된 인증 방법이 실행되기 전에 반드시 특정 인터페이스에 적용되어야 합니다.

단, 예외적으로 기본 메서드 리스트(이름이 "default")는 별도로 정의된 메서드 리스트가 없는 경우 자동으로 모든 인터페이스에 적용됩니다.

정의된 메서드 리스트는 기본 메서드 리스트를 우선하여 적용됩니다.

로컬(Local), 라인 비밀번호(Line Password), 및 활성화(Enable) 인증을 제외한 모든 인증 방법은 반드시 AAA를 통해 정의되어야 합니다.

AAA 보안 서비스를 통해 구현되지 않는 인증 방법을 포함하여 모든 인증 방법을 구성하는 방법에 대한 자세한 내용은 "인증 구성" 장을 참조하세요.

- Authorization : 원격 액세스 제어 방법을 제공하며, 여기에는 1회성 권한 부여 또는 각 서비스별 권한 부여, 사용자별 계정 목록과 프로필, 사용자 그룹 지원, 그리고 IP, IPX,

ARA, Telnet 지원이 포함됩니다.

AAA 권한 부여는 사용자가 수행할 수 있는 작업을 설명하는 속성 집합을 구성함으로써 작동합니다. 이러한 속성은 특정 사용자에 대한 데이터베이스에 저장된 정보와 비교되며, 결과는 AAA로 반환되어 사용자의 실제 권한과 제한 사항을 결정합니다.

데이터베이스는 액세스 서버나 라우터에 로컬로 저장될 수도 있고, RADIUS 또는 TACACS+와 같은 보안 서버에 원격으로 호스팅될 수도 있습니다.

RADIUS 및 TACACS+와 같은 원격 보안 서버는 사용자와 적절한 속성-값(AV) 쌍을 연관시켜 특정 권한을 부여합니다.

모든 권한 부여 방법은 반드시 AAA를 통해 정의되어야 합니다.

인증과 마찬가지로, AAA 권한 부여는 권한 부여 방법을 정의한 이름이 지정된 리스트를 생성하고 이를 다양한 인터페이스에 적용하여 구성합니다.

AAA를 사용한 권한 부여 구성에 대한 자세한 내용은 "권한 부여 구성" 을 참조하세요.

- Accounting : 사용자 ID, 시작 및 종료 시간, 실행된 명령(예: PPP), 패킷 수, 바이트 수와 같은 정보를 수집하고 이를 billing, auditing, reporting에 사용하기 위해 보안 서버로 전송하는 방법을 제공합니다.

Accounting은 사용자가 접근하는 서비스와 소비하는 네트워크 리소스의 양을 추적할 수 있도록 합니다. AAA accounting이 활성화되면, 네트워크 액세스 서버는 사용자 활동을 accounting record의 형태로 RADIUS 또는 TACACS+ 보안 서버(구현된 보안 방법에 따라 다름)로 보고합니다.

각 accounting record는 accounting AV(Attribute-Value) 쌍으로 구성되며, 액세스 제어 서버에 저장됩니다. 이 데이터는 이후 네트워크 관리, 클라이언트 과금, 또는 감사(auditing)를 위해 분석될 수 있습니다.

모든 accounting 방법은 반드시 AAA를 통해 정의되어야 합니다.
인증(Authentication) 및 권한 부여(Authorization)와 마찬가지로, AAA accounting은 accounting 방법을 정의한 이름이 지정된 리스트를 생성하고 이를 다양한 인터페이스에 적용하여 구성합니다.

AAA를 사용하여 accounting을 구성하는 방법에 대한 자세한 내용은 "계정 설정" 을 참조하세요.

10.1.2 AAA 사용시 이점

AAA는 다음과 같은 이점을 제공합니다.

- 접근 구성에 대한 유연성과 제어 향상
- 확장성

- RADIUS, TACACS+, Kerberos와 같은 표준화된 인증 방법 지원
- 다중 백업 시스템 지원

10.1.3 AAA 원칙

AAA는 사용자가 라인별(사용자별) 또는 서비스별(IP, IPX, VPDN 등)로 원하는 유형의 인증(Authentication)과 권한 부여(Authorization)를 동적으로 구성할 수 있도록 설계되었습니다.
사용자는 메서드 리스트를 생성하여 원하는 인증 및 권한 부여 유형을 정의한 후, 해당 메서드 리스트를 특정 서비스나 인터페이스에 적용합니다.

10.1.4 Method 리스트

메서드 리스트는 사용자를 인증하는 데 사용되는 인증 방법을 정의하는 순차적인 리스트입니다. 메서드 리스트를 사용하면 하나 이상의 보안 프로토콜을 지정할 수 있어, 초기 인증 방법이 실패할 경우를 대비한 백업 시스템을 보장할 수 있습니다.

소프트웨어는 메서드 리스트에 나열된 첫 번째 방법을 사용하여 사용자를 인증하며, 해당 방법이 응답하지 않을 경우 다음 인증 방법으로 이동합니다. 이 과정은 리스트에 나열된 인증 방법 중 하나와 성공적으로 통신이 이루어지거나, 리스트가 모두 소진되어 인증이 실패할 때까지 계속됩니다.

소프트웨어는 이전 인증 방법에서 응답이 없을 경우에만 리스트에 나열된 다음 인증 방법으로 시도합니다. 그러나 인증이 어느 시점에서든 실패하는 경우(즉, 보안 서버 또는 로컬 사용자 이름 데이터베이스가 사용자 접근을 거부하는 응답을 보낼 경우), 인증 프로세스는 중단되며 다른 인증 방법은 시도되지 않습니다.

다음 그림은 RADIUS 서버(R1, R2)와 TACACS+ 서버(T1, T2)를 포함한 일반적인 AAA 네트워크 구성을 보여줍니다.

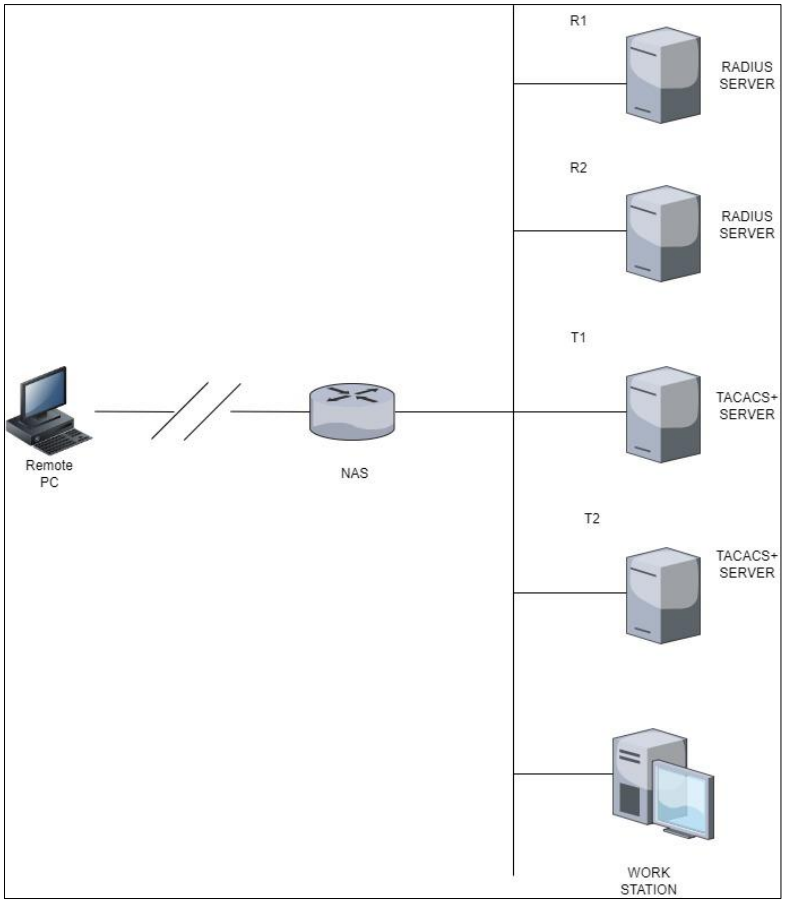


그림 7 AAA 네트워크 구성

시스템 관리자가 인증 정보를 조회할 메서드 리스트를 정의했다고 가정해 보겠습니다. 이 리스트에서는 R1을 먼저 조회하고, 그다음 R2, T1, T2, 마지막으로 액세스 서버의 로컬 사용자 이름 데이터베이스를 조회하도록 설정되었습니다.

원격 사용자가 네트워크에 접속을 시도하면, 네트워크 액세스 서버는 먼저 R1에 인증 정보를 요청합니다.

R1이 사용자를 인증하면 PASS 응답을 네트워크 액세스 서버로 전송하며, 사용자는 네트워크에 접근할 수 있습니다.

- R1이 FAIL 응답을 반환하면, 사용자는 접근이 거부되고 세션이 종료됩니다.
- R1이 응답하지 않으면, 네트워크 액세스 서버는 이를 ERROR로 처리하고 R2에 인증 정보를 요청합니다.

이 과정은 나머지 지정된 인증 방법에 대해 계속 진행되며, 사용자가 인증되거나 거부되거나, 세션이 종료될 때까지 반복됩니다.

모든 인증 방법이 오류를 반환할 경우, 네트워크 액세스 서버는 세션을 실패로 처리하고 세션을 종료합니다.

FAIL 응답은 ERROR와 본질적으로 다릅니다.

- FAIL: 사용자가 해당 인증 데이터베이스에 정의된 기준을 충족하지 못해 인증에 실패했음을 의미합니다. FAIL 응답이 반환되면 인증 프로세스는 즉시 종료됩니다.
- ERROR: 보안 서버가 인증 요청에 대해 응답하지 않았음을 의미합니다. 따라서 실제로 인증 시도가 이루어지지 않았습니다.

오직 ERROR가 감지된 경우에만 AAA가 메서드 리스트에 정의된 다음 인증 방법으로 넘어갑니다.

10.5 AAA 구성 프로세스

먼저 구현하려는 보안 솔루션의 종류를 결정해야 합니다. 특정 네트워크에서 발생할 수 있는 보안 위험을 평가하고, 무단 접근 및 공격을 방지하기 위한 적절한 방법을 선택해야 합니다. AAA를 구성하기 전에 기본적인 구성 절차를 숙지해야 합니다.

1.2.1 AAA 구성 프로세스 개요

- 보안 서버를 사용하기로 결정한 경우, 먼저 RADIUS, TACACS+와 같은 보안 프로토콜 매개변수를 구성하십시오.
- AAA 인증 명령어를 사용하여 인증을 위한 방법 리스트를 정의하십시오.
- 필요하면 특정 인터페이스나 라인에 방법 리스트를 적용하십시오.
- (선택 사항) aaa authorization 명령어를 사용하여 권한 부여를 구성하십시오.
- (선택 사항) aaa accounting 명령어를 사용하여 계정 관리를 구성하십시오.

10.6 AAA 인증 구성

- AAA를 사용하여 로그인 인증 구성
- AAA를 사용하여 PPP 인증 구성
- 권한 수준에서 암호 보호 활성화
- AAA 인증을 위한 메시지 배너 구성
- AAA 인증 사용자 이름 프롬프트
- AAA 인증 암호 프롬프트

- 사용자 이름 인증 설정
- 암호 활성화
-

10.7 AAA 인증 구성 작업

AAA 인증을 구성하려면 다음 구성 프로세스를 수행하십시오.

① 별도의 보안 서버를 사용하기로 결정한 경우 RADIUS, TACACS+, Kerberos와 같은 보안 프로토콜 매개변수를 구성합니다.

② AAA 인증 명령을 사용하여 인증을 위한 방법 목록을 정의합니다.

③ 필요한 경우 특정 인터페이스나 줄에 메서드 목록을 적용합니다.

10.7.1 AAA를 사용하여 로그인 인증 구성

AAA 보안 서비스는 다양한 로그인 인증 방법을 용이하게 합니다. 지원되는 로그인 인증 방법 중 어떤 것을 사용하기로 결정하든 AAA 인증을 활성화하려면 aaa authentication login 명령을 사용합니다. aaa authentication login 명령을 사용하면 로그인 시 시도되는 인증 방법 목록을 하나 이상 만들 수 있습니다. 이러한 목록은 login authentication line configuration 명령을 사용하여 적용됩니다.

AAA를 사용하여 로그인 인증을 구성하려면 글로벌 구성 모드에서 다음 명령을 사용하십시오.

명령어	설명
aaa authentication login {**default** | *list-name*}*method1* [*method2...*]	AAA를 활성화합니다.
line { **console** | **vty** } *line-number* [*ending-line-number*]	라인의 구성 모드로 들어갑니다.
login authentication {**default** | *list-name*}	인증 목록을 라인 또는 라인 세트에 적용합니다. (라인 구성 모드에서)

list-name은 생성 중인 목록의 이름을 지정하는 데 사용되는 문자열입니다. method 인수는 인증 알고리즘에서 시도할 실제 메서드를 참조합니다. 추가 인증 메서드는 이전 메서드가 실패하지 않고 오류를 반환하는 경우에만 사용됩니다. 모든 메서드가 오류를 반환하더라도 인증이 성공하도록 하려면 명령줄에서 마지막 메서드로 none을 지정하십시오.

예를 들어, 인증이 (이 예에서) TACACS+ 서버가 오류를 반환하더라도 성공하도록 지정하려면 다음 명령어를 입력하십시오.

aaa authentication login default group radius

주의 : none 키워드는 로그인하는 사용자가 모두 인증에 성공하도록 허용하므로, 반드시 백업 인증 방법으로만 사용해야 합니다.

다음 표에는 지원되는 로그인 인증 방법이 나열되어 있습니다.

키워드	설명
enable	인증을 위해 비밀번호를 사용합니다.
group name	인증을 위해 서버 그룹을 사용합니다.
group radius	인증에 RADIUS 를 사용합니다.
group tacacs+	인증을 위해 tacacs+ 그룹을 사용합니다.
line	인증을 위해 라인 비밀번호를 사용합니다.
local	인증을 위해 로컬 사용자 이름 데이터베이스를 사용합니다.
localgroup	인증을 위해 로컬 그룹 사용자 이름 데이터베이스를 사용합니다.
local-case	대소문자를 구분하는 로컬 사용자 이름 인증을 사용합니다.
none	조건 없이 인증을 통과합니다.

① Enable Password를 사용한 로그인 인증

aaa authentication login 명령을 enable method 키워드와 함께 사용하여 enable 암호를 로그인 인증 방법으로 지정합니다.

예를 들어, 다른 방법 목록이 정의되지 않은 경우 로그인 시 사용자 인증 방법으로 enable 암호를 지정하려면 다음 명령을 입력하십시오

aaa authentication login default enable

② 라인 패스워드를 이용한 로그인 인증

line method 키워드와 함께 aaa authentication login 명령을 사용하여 line password를 로그인 인증 방법으로 지정합니다. 예를 들어, 다른 방법 목록이 정의되지 않은 경우 로그인 시 사용자 인증 방법으로 line password를 지정하려면 다음 명령을 입력합니다.

aaa authentication login default line

로그인 인증 방법으로 라인 비밀번호를 사용하려면 먼저 라인 비밀번호를 정의해야 합니다.

③ 로컬 비밀번호를 사용한 로그인 인증

로컬 메서드 키워드와 함께 aaa authentication login 명령을 사용하여 Cisco 라우터 또는 액세스 서버가 인증을 위해 로컬 사용자 이름 데이터베이스를 사용하도록 지정합니다. 예를 들어, 다른 메서드 목록이 정의되지 않은 경우 로그인 시 사용자 인증 방법으로 로컬 사용자 이름 데이터베이스를 지정하려면 다음 명령을 입력합니다.

aaa authentication login default local

④ 그룹 RADIUS를 사용한 로그인 인증

aaa authentication login 명령을 group radius 메서드와 함께 사용하여 RADIUS를 로그인 인증 메서드로 지정합니다. 예를 들어, 다른 메서드 목록이 정의되지 않은 경우 로그인 시 사용자 인증 메서드로 RADIUS를 지정하려면 다음 명령을 입력합니다.

aaa authentication login default group radius

RADIUS를 로그인 인증 방법으로 사용하려면 RADIUS 보안 서버와의 통신을 활성화해야 합니다.

10.7.2 권한 수준에 따른 암호 보호 활성화

aaa authentication enable default 명령을 사용하여 사용자가 권한 있는 EXEC 명령 수준에 액세스할 수 있는지 여부를 확인하는 데 사용되는 일련의 인증 방법을 만듭니다. 최대 4개의 인증 방법을 지정할 수 있습니다. 추가 인증 방법은 이전 방법이 실패하지 않고 오류를 반환하는 경우에만 사용됩니다. 모든 방법이 오류를 반환하더라도 인증이 성공하도록 지정하려면 명령줄에서 마지막 방법으로 none을 지정합니다.

글로벌 구성 모드에서 다음 명령을 사용하세요.

명령어	설명
aaa authentication enable default method1 [method2...]	특권 EXEC 수준을 요청하는 사용자의 사용자 ID와 비밀번호 확인을 활성화합니다.

방법 인수는 인증 알고리즘이 입력된 순서대로 시도하는 실제 방법 목록을 참조합니다.

키워드	주의
enable	인증을 위해 비밀번호를 사용합니다.
group group-name	인증을 위해 서버 그룹을 사용합니다.
group radius	인증에 RADIUS를 사용합니다.

line	인증을 위해 라인 비밀번호를 사용합니다.
local	인증을 위해 로컬 사용자 이름 데이터베이스를 사용합니다.

10.7.3 AAA 인증을 위한 메시지 배너 구성

AAA는 구성 가능하고 개인화된 로그인 및 로그인 실패 배너 사용을 지원합니다. 사용자가 AAA를 사용하여 인증받기 위해 시스템에 로그인할 때 표시될 메시지 배너와 어떤 이유로든 인증이 실패할 때 표시될 메시지 배너를 구성할 수 있습니다.

① 로그인 배너 구성

사용자가 로그인할 때마다 표시되는 배너를 구성하려면(로그인에 대한 기본 메시지를 대체) 글로벌 구성 모드에서 다음 명령을 사용합니다.

명령어	설명
aaa authentication banner *delimiter text-string delimiter*	개인화된 로그인 배너를 만듭니다.

② 로그인 실패 배너 구성

사용자가 로그인에 실패할 때마다 표시되는 메시지를 구성하려면(로그인 실패에 대한 기본 메시지를 대체) 글로벌 구성 모드에서 다음 명령을 사용합니다.

명령어	설명
aaa authentication fail-message *delimiter text-string delimiter*	사용자가 로그인에 실패할 때 표시되는 메시지를 만듭니다.

③ 지침

로그인 배너를 생성하려면 구분 문자(delimiting character)를 구성해야 합니다. 이 문자는 시스템에 다음 텍스트 문자열이 배너로 표시될 것임을 알리며, 텍스트 문자열 뒤에 다시 반복되어 배너의 끝을 나타냅니다. 구분 문자는 확장 ASCII 문자 집합의 임의의 단일 문자일 수 있습니다. 하지만 한 번 구분 문자로 정의되면, 그 문자는 배너를 구성하는 텍스트 문자열 내에서 사용할 수 없습니다.

10.7.4 AAA 인증 사용자 username-prompt

사용자에게 사용자 이름 입력을 요청할 때 표시되는 텍스트를 변경하려면 글로벌 구성 모드에서

다음의 명령어를 입력하십시오

aaa authentication username-prompt

기본 사용자 이름 프롬프트 텍스트로 되돌리려면 이 명령의 no 형식을 사용하십시오.

aaa authentication username-prompt 명령은 원격 TACACS+ 서버에서 제공하는 대화 내용을 변경하지 않습니다.

글로벌 구성 모드에서 다음 명령어를 사용하여 구성하십시오

명령어	설명
aaa authentication username-prompt *text-string*	사용자가 사용자 이름을 입력하라는 요청을 받을 때 표시될 텍스트 문자열.

10.7.5 AAA 인증 password-prompt

사용자에게 비밀번호를 묻는 메시지가 표시될 때 표시되는 텍스트를 변경하려면 글로벌 구성 모드에서 aaa authentication password-prompt 명령을 사용합니다. 기본 비밀번호 프롬프트 텍스트로 돌아가려면 이 명령의 no 형식을 사용합니다.

aaa authentication password-prompt 명령은 원격 TACACS+ 서버에서 제공하는 대화 상자를 변경하지 않습니다. 다음 명령을 사용하여 글로벌 구성 모드에서 구성합니다.

명령어	설명
aaa authentication password-prompt *text-string*	text-string 사용자에게 비밀번호를 입력하라는 메시지가 표시될 때 표시되는 텍스트 문자열입니다.

10.7.6 사용자 이름 인증 설정

사용자 이름 기반 인증 시스템을 생성할 수 있으며, 이는 다음과 같은 상황에서 유용합니다

- TACACS를 지원할 수 없는 네트워크를 위해 TACACS와 유사한 사용자 이름 및 암호화된 비밀번호 인증 시스템을 제공하기 위해 사용합니다.
- 특수한 로그인 사례를 제공하기 위해 사용됩니다. (엑세스 목록 확인, 비밀번호 검증 없음, 로그인시 자동명령 실행)

사용자 이름 인증을 설정하려면, 시스템 구성에 따라 필요한 경우 글로벌 구성 모드에서 다음 명령어를 사용하십시오.

no 옵션을 사용하면 사용자 이름을 삭제할 수 있습니다.

username name {nopassword | password password | password encryption-type encrypted-password}

username name [autocommand command]

username name [callback-dialstring telephone-number]

username name [callback-rotary rotary-group-number]

username name [callback-line [tty | aux] line-number [ending-line-number]]

username name [noescape] [nohangup]

username name [privilege level]

username name [user-maxlinks number]

no username name

10.7.7 패스워드 활성화

여러 권한 레벨에 대한 접근을 제어하기 위해 로컬 비밀번호를 설정하려면 글로벌 구성 모드에서 enable password 명령을 사용하십시오.

비밀번호 요구 사항을 제거하려면 이 명령의 no 옵션을 사용하십시오.

enable password { [encryption-type] encrypted-password} [level level]

no enable password [level level]

10.7.8 패스워드 규칙 설정

구분	내용
준수 사항	9자리 이상의 길이 설정 가능
	숫자, 대문자(영문), 소문자(영문), 특수문자 중에서 3가지 이상의 조합으로 입력 가능
금지 항목	사용자 계정(ID)과 동일한 패스워드 설정 금지
	동일한 문자·숫자의 연속적인 반복입력 금지
	키보드상의 연속된 문자 또는 숫자의 순차적 입력금지
	직전 사용된 패스워드 재사용 금지
	3개월 이내 사용된 패스워드 재사용 금지

보안 요구사항의 내용으로 아래의 설정을 통해 패스워드 규칙설정을 만들 수 있습니다.

글로벌 구성모드에서 아래의 명령어를 조합하여 만들 수 있습니다.

Switch_config#localpass default

the illegal password will be disabled [Y/N] ? y

Switch_config_localpass_default#min-length 9 (9자리이상 사용)

Switch_config_localpass_default#element number lower-letter upper-letter special-character (숫자, 소문자, 대문자, 특수문자 사용)

Switch_config_localpass_default#non-user (사용자 계정과 동일한 패스워드 금지)

Switch_config_localpass_default#non-repeat (동일한 연속된 문자 반복금지)

Switch_config_localpass_default#non-seqlisting (키보드상의 연속된 문자 금지)

Switch_config_localpass_default#non-history (직전암호 사용금지)

Exit

Switch_config#local pass-group default (위 설정 후 입력되는 사용자 계정에 대한 비밀번호에 그룹 규칙을 적용)

10.8 AAA 인증 구성 예제

10.8.1 RADIUS 인증 예제

다음 예에서는 RADIUS를 사용하여 인증 및 허가를 받도록 스위치를 구성하는 방법을 보여줍니다.

aaa authentication login radius-login group radius local

aaa authorization network radius-network radius

line vty

login authentication radius-login

RADIUS 인증 및 권한 부여 구성의 줄은 다음과 같이 정의됩니다.

- aaa authentication login radius-login radius local 명령은 로그인 프롬프트에서 인증을 위해 RADIUS를 사용하도록 라우터를 구성합니다. RADIUS가 오류를 반환하면 사용자는 로컬 데이터베이스를 사용하여 인증됩니다.
- aaa authentication ppp radius-ppp radius 명령은 사용자가 아직 로그인하지 않은 경우 CHAP 또는 PAP를 사용하여 PPP 인증을 사용하도록 소프트웨어를 구성합니다. EXEC 기능이 사용자를 인증한 경우 PPP 인증은 수행되지 않습니다.
- aaa 인증 네트워크 반경-네트워크 반경 명령은 네트워크 인증, 주소 할당 및 기타 액세스 목록에 대해 RADIUS를 쿼리합니다.

- 로그인 인증 radius-login 명령은 3번째 줄에 대한 radius-login 방법 목록을 활성화합니다.
-

10.9 AAA 권한 부여 구성 작업 목록

- AAA를 사용하여 EXEC 권한 부여 구성

10.10 AAA 인증 구성 작업

AAA 인증을 구성하려면 다음 구성 프로세스를 수행하십시오.

① 별도의 보안 서버를 사용하기로 결정한 경우 RADIUS, TACACS+, Kerberos와 같은 보안 프로토콜 매개변수를 구성합니다.

② AAA 인증 명령을 사용하여 인증에 대한 방법 목록을 정의합니다.

③ 필요한 경우 특정 인터페이스나 줄에 메서드 목록을 적용합니다.

10.10.1 AAA를 사용하여 EXEC 권한 부여 구성

aaa authorization 명령을 사용하여 권한을 활성화합니다.

aaa authorization exec 명령을 사용하여 사용자가 EXEC Shell 을 실행할 수 있는지 확인하기 위해 권한을 실행합니다. 이 기능은 자동 명령 정보와 같은 사용자 프로필 정보를 반환할 수 있습니다.

line configuration 명령 login authorization을 사용하여 이러한 목록을 적용합니다. 글로벌 구성 모드에서 다음 명령을 사용합니다.

명령어	설명
aaa authorization exec {**default** | *list-name*}*method1* [*method2...*]	global 권한 목록을 만듭니다.
line [**console** | **vty**] *line-number* [*ending-line-number*]	라인의 구성 모드로 들어갑니다.
login authorization {**default** | *list-name*}	권한 부여 목록을 라인 또는 라인 세트에 적용합니다. (라인 구성 모드에서)

키워드 list-name은 권한 부여 방법 목록의 이름을 지정하는 데 사용되는 문자열입니다.

키워드 method는 권한 부여 프로세스 중에 실제 방법을 지정합니다. 목록을 사용하면 권한 부여에 사용할 하나 이상의 보안 프로토콜을 지정하여 초기 방법이 실패할 경우 백업 시스템을 확보할 수 있습니다. 시스템은 나열된 첫 번째 방법을 사용하여 특정 네트워크 서비스에 대한 사용자

를 권한 부여합니다. 해당 방법이 응답하지 않으면 시스템은 방법 목록에 나열된 다음 방법을 선택합니다. 이 프로세스는 나열된 권한 부여 방법과 성공적으로 통신하거나 정의된 모든 방법이 소진될 때까지 계속됩니다. 지정된 모든 방법이 응답하지 않고도 시스템이 EXEC 셸을 입력하기를 원하는 경우 명령줄에서 마지막 권한 부여 방법으로 none을 지정해야 합니다.

기본 매개변수를 사용하여 기본 목록을 설정하면 기본 목록이 모든 인터페이스에 자동으로 적용됩니다. 예를 들어 다음 명령을 사용하여 exec에 대한 기본 권한 부여 방법으로 radius를 지정합니다.

aaa authorization exec default group radius

주의 : 메서드 목록이 정의되지 않은 경우 로컬 권한 부여 서비스를 사용할 수 없으며 권한 부여가 통과할 수 있습니다.

다음 표는 현재 지원되는 EXEC 권한 부여 모드를 나열합니다.

키워드	설명
group WORD	서버 그룹을 사용하여 인증을 수행합니다.
group radius	RADIUS 인증을 사용합니다.
group tacacs+	tacacs+ 권한을 사용합니다.
local	로컬 데이터베이스를 사용하여 인증을 수행합니다.
if-authenticated	인증된 사용자에게 필요한 모든 기능을 자동으로 부여합니다.
none	무조건 승인으로 진행 됩니다.

10.11 AAA 권한 설정 예시

10.11.1 EXEC 로컬 권한 부여 예시

aaa authentication login default local

aaa authorization exec default local

!

username exec1 password 0 abc privilege 15

username exec2 password 0 abc privilege 10

username exec3 nopassword

username exec4 password 0 abc user-maxlinks 10

username exec5 password 0 abc autocommand telnet 192.168.10.1

!

RADIUS 인증 구성의 라인은 다음과 같이 정의할 수 있습니다.

- aaa authentication login default local 명령은 로그인 인증의 기본 방법 목록을 정의합니다. 이 방법 목록은 모든 로그인 인증 서버에 자동으로 적용됩니다.
- aaa authorization exec default local 명령은 exec authorization의 기본 메서드 목록을 정의합니다. 메서드 목록은 exec shell을 입력해야 하는 모든 사용자에게 자동으로 적용됩니다.
- 사용자 이름은 exec1이고, 로그인 비밀번호는 abc이며, EXEC 권한 수준은 15(가장 높은 수준)입니다. 즉, 권한 수준이 15인 사용자 exec1이 exec 셸에 로그인하면 모든 명령을 확인하고 수행할 수 있습니다.
- 사용자 이름은 exec2이고, 로그인 비밀번호는 abc이고, EXEC 권한 수준은 10입니다. 즉, 권한 수준이 10인 사용자 exec2가 EXEC 셸에 로그인하면 권한 수준이 10 미만인 명령을 확인하고 수행할 수 있습니다.
- 사용자 이름은 exec3이고, 로그인에는 비밀번호가 필요하지 않습니다.
- 사용자 이름은 exec4이고, 로그인 비밀번호는 abc이고, 사용자의 최대 링크 수는 10입니다.
- 사용자 이름은 exec5이고, 로그인 비밀번호는 abc이며, 사용자는 exec 셸에 로그인하자마자 telnet 192.16.10.1 을 실행합니다.

10.12 AAA 계정 구성 작업 목록

- AAA를 사용하여 연결 계정 구성
- AAA를 사용하여 네트워크 계정 구성

10.13 AAA 계정 구성 작업

AAA 계정을 구성하려면 다음 구성 프로세스를 수행하십시오.

① 별도의 보안 서버를 사용하기로 결정한 경우 RADIUS, TACACS+, Kerberos와 같은 보안 프로토콜 매개변수를 구성합니다.

② AAA 계정 명령을 사용하여 회계에 대한 방법 목록을 정의합니다.

③ 필요한 경우 특정 인터페이스나 줄에 메서드 목록을 적용합니다.

10.13.1 AAA를 사용하여 계정 연결 구성

aaa accounting 명령을 사용하여 AAA Accounting을 활성화합니다.

네트워크 액세스 서버에서 이루어진 모든 아웃바운드 연결에 대한 계정 정보를 제공하는 방법 목록을 만들려면 aaa accounting connection 명령을 사용합니다.

명령어	설명
aaa accounting connection {**default** | *list-name*} {{{**start-stop** | **stop-only**} **group** *groupname}* | **none**}	global accounting 목록을 만듭니다.

키워드 list-name은 설정 목록의 모든 문자열을 명명하는 데 사용됩니다. 키워드 method는 프로세스 중에 채택된 실제 방법을 지정합니다.

다음 표는 현재 지원되는 연결 방법이 나열되어 있습니다.

키워드	설명
group WORD	서버 그룹을 사용하여 작업을 수행합니다.
group radius	RADIUS 를 accounting 에 사용합니다.
none	인터페이스에 대한 accounting 서비스를 비활성화합니다.
stop-only	요청된 사용자 프로세스가 끝나면 "중지" 레코드 accounting 알림을 보냅니다.
start-stop	RADIUS 또는 TACACS+는 요청된 프로세스가 시작될 때 "시작" accounting 알림을 보내고, 프로세스가 끝날 때 "중지" accounting 알림을 보냅니다.

10.13.2 AAA를 사용하여 네트워크 계정 구성

aaa accounting 명령을 사용하여 AAA Accounting을 활성화합니다.

SLIP, PPP, NCP 및 ARAP 세션에 대한 회계 정보를 제공하는 방법 목록을 만들려면 글로벌 구성 모드에서 aaa accounting network 명령을 사용하십시오.

명령어	설명
aaa accounting network {**default** | *list-name*} {{{**start-stop** | **stop-only**} **group** *groupname}* | **none**}	global accounting 목록을 만듭니다.

키워드 list-name은 설정 목록의 모든 문자열을 명명하는 데 사용됩니다. 키워드 method는 회계 프로세스 중에 채택된 실제 방법을 지정합니다.

다음 표는 현재 지원되는 네트워크 accounting 방법을 나열합니다.

키워드	설명
group WORD	서버 그룹을 사용하여 작업을 수행합니다.
group radius	RADIUS 를 accounting 에 사용합니다.
none	인터페이스에 대한 accounting 서비스를 비활성화합니다.
stop-only	요청된 사용자 프로세스가 끝나면 "중지" 레코드 accounting 알림을 보냅니다.
start-stop	RADIUS 또는 TACACS+는 요청된 프로세스가 시작될 때 "시작" accounting 알림을 보내고, 프로세스가 끝날 때 "중지" accounting 알림을 보냅니다.

10.13.3 AAA Accounting 업데이트

주기적인 중간 계정 기록을 계정 관리 서버로 전송하려면 글로벌 구성 모드에서 aaa accounting update 명령을 사용합니다. 중간 계정 업데이트를 비활성화하려면 이 명령의 no 옵션을 사용하십시오.

명령어	설명
aaa accounting update [**newinfo**] [**periodic** *number*]	AAA accounting 업데이트를 활성화 합니다.

newinfo 키워드를 사용하면, 새로운 계정 관리 정보가 보고될 때마다 중간 계정 기록이 계정 관리 서버로 전송됩니다.

예를 들어, IP 제어 프로토콜(IPCP)이 원격 피어와의 IP 주소 협상을 완료할 경우, 중간 계정 기록에는 협상된 원격 피어의 IP 주소가 포함됩니다.

periodic 키워드를 사용하면, 중간 계정 기록이 지정된 주기(숫자 인수로 정의됨)에 따라 정기적으로 전송됩니다.

이 중간 계정 기록에는 해당 시점까지 사용자가 생성한 모든 계정 정보가 포함됩니다.

newinfo와 periodic 키워드를 함께 사용하면, 새로운 계정 관리 정보가 있을 때마다 중간 계정 기록이 계정 관리 서버로 전송되고, 동시에 지정된 주기에 따라 계정 기록이 정기적으로 전송됩니다. 예를 들어, aaa accounting update newinfo periodic number 명령어를 구성하면, 현재 로그인된 모든 사용자는 주기적인 중간 계정 기록을 생성하며, 새로운 사용자는 newinfo 알고리즘에 따라 계정 기록을 생성합니다.

10.13.4 사용자 이름이 비어 있거나 null 값

사용자 이름 문자열이 NULL인 사용자에 대해 AAA 시스템이 계정 기록을 전송하지 않도록 하려면 글로벌 구성 모드에서 aaa accounting suppress null-username 명령을 사용하십시오.

NULL 사용자 이름에 대한 기록 전송을 허용하려면 이 명령의 no 옵션을 사용하십시오

11 RADIUS 설정

이 장에서는 RADIUS(Remote Authentication Dial-In User Service) 보안 시스템을 설명하고, 작동을 정의하며, RADIUS 기술을 사용하기에 적합한 네트워크 환경과 부적절한 네트워크 환경을 식별합니다. "RADIUS 구성 작업 목록" 섹션에서는 AAA(authentication, authorization, and accounting) 명령 집합으로 RADIUS를 구성하는 방법을 설명합니다.

11.4 개요

11.4.1 RADIUS 란

RADIUS는 네트워크를 무단 접근으로부터 보호하는 분산 클라이언트/서버 시스템입니다.

RADIUS 구현에서 RADIUS 클라이언트는 스위치에서 실행되며, 사용자 인증 및 네트워크 서비스 접근 정보를 포함한 중앙 RADIUS 서버로 인증 요청을 보냅니다.

RADIUS는 높은 수준의 보안을 요구하면서도 원격 사용자에게 네트워크 접근을 제공해야 하는 다양한 네트워크 환경에서 구현되었습니다.

다음과 같은 접근 보안이 필요한 네트워크 환경에서 RADIUS를 사용하십시오.

- RADIUS는 다양한 벤더의 액세스 서버를 사용하는 네트워크에서 유용합니다. 예를 들어, 여러 벤더의 액세스 서버가 단일 RADIUS 서버 기반의 보안 데이터베이스를 공유하는 경우가 있습니다. IP 기반 네트워크에서 여러 벤더의 액세스 서버를 사용하는 경우, 다이얼인(dial-in) 사용자는 RADIUS 서버를 통해 인증됩니다. 이 RADIUS 서버는 Kerberos 보안 시스템과 함께 작동하도록 맞춤화되어 있습니다.
- 사용자가 단일 서비스에만 접근해야 하는 네트워크에서 RADIUS를 사용할 수 있습니다.
- RADIUS를 통해 사용자가 단일 호스트, Telnet과 같은 단일 유틸리티, 또는 PPP(Point-to-Point Protocol)와 같은 단일 프로토콜에 접근할 수 있도록 제어할 수 있습니다. 예를 들어, 사용자가 로그인하면 RADIUS는 이 사용자가 IP 주소 10.2.3.4를 사용하여 PPP를 실행할 권한이 있음을 확인하고, 정의된 액세스 목록을 시작합니다.
- 리소스 계정 관리가 필요한 네트워크에서 RADIUS를 사용할 수 있습니다. RADIUS 계정 관리 기능은 RADIUS 인증이나 권한 부여와 독립적으로 사용할 수 있습니다. RADIUS 계정 관리 기능은 서비스 시작 및 종료 시 데이터를 전송하여 세션 동안 사용된 리소스(예: 시간, 패킷, 바이트 등)의 양을 나타냅니다.
  예를 들어, 인터넷 서비스 제공자(ISP)는 특수한 보안 및 과금 요구를 충족하기 위해

RADIUS 접근 제어 및 계정 관리 소프트웨어의 프리웨어 버전을 사용할 수 있습니다. RADIUS는 다음과 같은 네트워크 보안 상황에서는 적합하지 않습니다.

- 다중 프로토콜 엑세스 환경
- NetWare Asynchronous Services Interface (NASI)를 지원하지 않습니다.
- X.25PAD 연결
- Switch-to-switch 상황 RADIUS는 양방향 인증을 제공하지 않습니다.
- 다양한 서비스를 사용하는 네트워크. RADIUS는 일반적으로 사용자를 하나의 서비스 모델에 바인딩합니다.

11.4.2 RADIUS 동작

사용자가 RADIUS를 사용하여 액세스 서버에 로그인하고 인증을 시도할 때, 다음 단계가 진행됩니다.

① 사용자에게 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다.

② 사용자 이름과 암호화된 비밀번호는 네트워크를 통해 RADIUS 서버로 전송됩니다.

③ 사용자는 RADIUS 서버로부터 다음 응답 중 하나를 받습니다.

- ACCEPT: 사용자가 인증되었습니다.
- REJECT: 사용자가 인증되지 않아 사용자 이름과 비밀번호를 다시 입력하라는 메시지가 표시되거나 액세스가 거부됩니다.
- CHALLENGE: RADIUS 서버에서 챌린지를 발행합니다. 챌린지는 사용자로부터 추가 데이터를 수집합니다.
- CHANGE PASSWOR: RADIUS 서버에서 사용자에게 새 비밀번호를 선택하라는 요청을 보냅니다.

  ACCEPT 또는 REJECT 응답은 EXEC 또는 네트워크 권한 부여에 사용되는 추가 데이터와 함께 제공됩니다. RADIUS 권한을 사용하기 전에 먼저 RADIUS 인증을 완료해야 합니다. ACCEPT 또는 REJECT 패킷에 포함된 추가 데이터는 다음으로 구성됩니다.

  사용자가 액세스할 수 있는 서비스에는 Telnet, rlogin 또는 로컬 영역 전송(LAT) 연결, PPP, 직렬 회선 인터넷 프로토콜(SLIP) 또는 EXEC 서비스가 포함됩니다.

  호스트 또는 클라이언트 IP 주소, 액세스 목록 및 사용자 시간 초과를 포함한 연결 매개변수.

11.5 RADIUS 설정 순서

스위치 또는 액세스 서버에서 RADIUS를 구성하려면 다음 작업을 수행해야 합니다.

- aaa authentication 글로벌 구성 명령을 사용하여 RADIUS 인증에 대한 메서드 목록을 정의합니다. aaa authentication 명령 사용에 대한 자세한 내용은 "인증 구성" 장을 참조하십시오.
- 정의된 메서드 목록을 사용할 수 있도록 하려면 라인 및 인터페이스 명령을 사용합니다. 자세한 내용은 "인증 구성" 장을 참조하십시오.
- aaa authorization global 명령을 사용하여 특정 사용자 기능을 인증할 수 있습니다. aaa authorization 명령 사용에 대한 자세한 내용은 "인증 구성" 장을 참조하십시오.
- aaa accounting 명령을 사용하여 RADIUS 연결에 대한 계정을 활성화할 수 있습니다. aaa accounting 명령 사용에 대한 자세한 내용은 "계정 구성" 장을 참조하십시오.

11.6 RADIUS 구성 작업 목록

- 스위치에서 RADIUS 서버 통신으로 구성
- 공급업체별 RADIUS 속성을 사용하도록 스위치 구성
- RADIUS 인증 지정
- RADIUS 권한 지정
- RADIUS 계정 지정

11.7 RADIUS 구성 작업

11.7.1 RADIUS 서버 통신으로 스위치 구성

RADIUS 호스트는 일반적으로 Livingston, Merit, Microsoft 또는 기타 소프트웨어 제공업체의 RADIUS 서버 소프트웨어를 실행하는 다중 사용자 시스템입니다.

RADIUS 서버와 Cisco 라우터는 공유 비밀 텍스트 문자열(shared secret text string)을 사용하여 비밀번호를 암호화하고 응답을 교환합니다.

AAA 보안 명령을 사용하도록 RADIUS를 구성하려면, RADIUS 서버 데몬을 실행 중인 호스트와 라우터가 공유하는 비밀 텍스트(키) 문자열을 지정해야 합니다.

서버별 RADIUS 서버 통신을 구성하려면 글로벌 구성 모드에서 다음 명령어를 사용하십시오.

명령어	설명
radius-server host *ip-address* [**auth-port** *port-number*][**acct-port** *portnumber*]	원격 RADIUS 서버 호스트의 IP 주소 또는 호스트 이름을 지정하고 인증 및 계정 대상 포트 번호를 할당합니다.
radius-server key *string*	라우터와 radius 사이에 사용되는 공유 비밀 텍스트 문자열을 지정합니다.

라우터와 RADIUS 서버 간의 글로벌 통신 설정을 구성하려면 글로벌 구성 모드에서 다음 radius-server 명령을 사용하세요.

명령어	설명
radius-server retransmit *retries*	각 RADIUS 요청을 서버로 전송하는 횟수를 지정합니다.
radius-server timeout *seconds*	RADIUS 요청에 대한 응답을 스위치가 다시 전송하기 전에 기다리는 시간(초)을 지정합니다..
radius-server deadtime *minutes*	인증 요청에 응답하지 않는 RADIUS 서버가 RADIUS 인증 요청으로 인해 무시되는 시간(분)을 지정합니다.

11.7.2 공급업체별 RADIUS 속성을 사용하도록 스위치 구성

인터넷 엔지니어링 태스크 포스(IETF) 초안 표준은 네트워크 액세스 서버와 RADIUS 서버 간에 * 벤더별 속성(attribute 26)을 사용하여 벤더별 정보를 통신하는 방법을 명시합니다. 벤더별 속성(Vendor-Specific Attributes, VSAs)은 일반적인 사용에는 적합하지 않은 벤더 고유의 확장 속성을 지원할 수 있도록 합니다.

벤더 ID 및 VSAs에 대한 자세한 내용은 RFC 2138(Remote Authentication Dial-In User Service, RADIUS)를 참조하십시오.

네트워크 액세스 서버가 VSAs를 인식하고 사용할 수 있도록 구성하려면, 글로벌 구성 모드에서 다음 명령어를 사용하십시오.

명령어	설명
radius-server vsa send [authentication]]	네트워크 액세스 서버가 RADIUS IETF 속성 26 에 의해 정의된 VSAs(벤더별 속성)를 인식하고 사용할 수 있도록 활성화합니다.

11.7.3 RADIUS 인증 지정

RADIUS 서버를 식별하고 RADIUS 인증 키를 정의한 후, RADIUS 인증을 위한 방법 목록(method lists)을 정의해야 합니다.

RADIUS 인증은 AAA를 통해 처리되므로, aaa authentication 명령을 입력하여 RADIUS를 인증 방법으로 지정해야 합니다.

자세한 내용은 "Configuring Authentication"(인증 구성) 장을 참조하십시오.

11.7.4 RADIUS 권한 지정

AAA 권한 부여(Authorization)를 통해 사용자의 네트워크 접근을 제한하는 매개변수를 설정할 수 있습니다.
RADIUS를 사용한 권한 부여는 원격 액세스 제어를 위한 한 가지 방법으로, 다음을 포함합니다.

- 단회성(one-time) 권한 부여 또는 서비스별 권한 부여
- 사용자별 계정 목록 및 프로필
- 사용자 그룹 지원
- IP, IPX, ARA, Telnet 지원

RADIUS 권한 부여는 AAA를 통해 처리되므로, aaa authorization 명령을 사용하여 RADIUS를 권한 부여 방법으로 지정해야 합니다.

자세한 내용은 "Configuring Authorization"(권한 구성) 장을 참조하십시오.

11.7.5 RADIUS 계정 지정

AAA 계정 관리 기능을 사용하면 사용자가 액세스하는 서비스와 소비하는 네트워크 리소스의 양을 추적할 수 있습니다.

RADIUS 계정 관리는 AAA를 통해 처리되므로, aaa accounting 명령을 사용하여 RADIUS를 계정 관리 방법으로 지정해야 합니다.

자세한 내용은 "Configuring Accounting"(계정 관리 구성) 장을 참조하십시오.

11.8 RADIUS 설정 예시

다음 예는 RADIUS를 사용하여 라우터를 인증 및 권한 부여하도록 구성하는 방법을 보여줍니다.

aaa authentication login use-radius group radius local

이 예제의 RADIUS 인증 및 권한 부여 구성에 사용된 각 라인은 다음과 같이 정의됩니다.

라우터가 로그인 프롬프트에서 RADIUS를 인증 방법으로 사용하도록 구성합니다. RADIUS가 오류를 반환하는 경우, 사용자는 로컬 데이터베이스를 통해 인증됩니다. 여기서 use-radius는 **방법 목록(method list)**의 이름이며, RADIUS를 우선적으로 사용한 뒤 로컬 인증을 지정합니다.

RADIUS 인증, 권한 부여, 및 계정 관리 예제

다음은 AAA 명령 세트를 사용하여 RADIUS를 일반적으로 구성하는 방법의 예제입니다.

radius-server host 1.2.3.4

radius-server key myRaDiUSpassWoRd

username root password AlongPassword

aaa authentication login admins radius local

line vty 1 16

login authentication admins

이 예제의 RADIUS 인증, 권한 부여, 및 계정 관리 구성에 사용된 각 라인은 다음과 같이 정의됩니다

radius-server host 명령어: RADIUS 서버 호스트의 IP 주소를 정의합니다.

radius-server key 명령어: 네트워크 액세스 서버와 RADIUS 서버 호스트 간에 공유되는 비밀 텍스트 문자열을 정의합니다.

aaa authentication login admins group radius local 명령어

admins"라는 인증 방법 목록(method list)을 정의합니다.

이 목록은 RADIUS 인증을 우선적으로 사용합니다.

11.8.1 RADIUS 응용 프로그램 예제

다음 예제에서는 AAA 명령어를 통해 일반 구성을 정의하는 방법을 보여줍니다.

radius-server host 1.2.3.4

radius-server key myRaDiUSpassWoRd

username root password AlongPassword

aaa authentication login admins radius local

line vty 1 16

login authentication admins

위의 예에서 각 명령줄은 고유한 의미를 갖습니다. 다음 내용을 참조하세요.

명령어 radius-server host는 RADIUS 서버의 IP 주소를 정의합니다.

명령어 radius-server key는 네트워크 액세스 서버와 RADIUS 서버 간의 공유 핀을 정의합니다.

명령어 aaa authentication login admins radius local은 인증 방법 list admins를 정의하는데, 먼저 RADIUS를 인증 방법으로 지정한 다음 RADIUS 서버가 응답하지 않으면 로컬 인증을 사용합니다.

명령어 login authentication admins는 방법 list admins를 로그인 인증 방법으로 지정합니다.

12 TACACS+ 설정

12.4 TACACS+ 개요

TACACS+는 액세스 보안 제어 프로토콜로, 사용자에 대한 네트워크 액세스 서버의 접근 권한을 중앙에서 검증합니다. 네트워크 액세스 서버와 TACACS+ 서비스 프로그램 간의 정보 교환이 암호화되므로 통신의 안전성이 보장됩니다.
네트워크 액세스 서버에 TACACS+를 구성하여 사용하기 전에, TACACS+ 서버에 접근하고 이를 구성해야 합니다. TACACS+는 독립적이고 모듈화된 인증(Authentication), 권한 부여(Authorization), 계정 관리(Accounting)을 제공합니다.

인증(Authentication): TACACS+는 여러 가지 인증 방식을 지원합니다(예: ASCII, PAP, CHAP 등). 사용자 이름과 비밀번호를 제공한 후, 서비스 유형, ID 번호 등의 추가 질문을 통해 사용자와의 대화를 처리할 수 있는 기능을 제공합니다. 또한, TACACS+ 인증 서비스는 사용자의 화면에 정보를 전송하는 기능을 지원합니다. 예를 들어, 회사의 비밀번호 만료 정책에 따라 사용자가 비밀번호를 변경해야 한다는 알림을 표시할 수 있습니다.

권한 부여(Authorization): TACACS+는 서비스 시간 동안 사용자의 서비스 제한 사항을 세부적으로 제어할 수 있습니다. 여기에는 자동 명령 설정, 접근 제어, 대화 유지 시간 등이 포함됩니다. 또한, 사용자가 실행할 수 있는 명령어를 제한할 수도 있습니다.

계정 관리(Accounting): TACACS+는 생성, 감사, 또는 네트워크 리소스 사용 상태를 계산하기 위한 정보를 수집하고 전송합니다. 네트워크 관리자는 계정 관리 기능을 통해 사용자 활동을 추적하거나 보안 감사를 수행하며, 정보를 제공합니다. 계정 관리 기능은 사용자 인증, 세션 시작 및 종료 시간, 실행된 명령어, 전송된 패킷 수 및 바이트 수 등을 기록합니다.

12.1.1 TACACS+ 프로토콜의 동작

사용자가 TACACS+를 사용하는 네트워크 액세스 서버에 로그인하고 ASCII 형식으로 간단한 인증을 요청하면 일반적인 상황에서 다음과 같은 프로세스가 발생할 수 있습니다.

연결이 구축되면 네트워크 액세스 서버는 TACACS+ 서비스 프로그램과 통신하여 사용자 이름 프

롬프트를 얻은 다음 사용자에게 제공합니다. 사용자가 사용자 이름을 입력하고 네트워크 액세스 서버는 TACACS+ 서비스 프로그램과 다시 통신하여 비밀번호 프롬프트를 얻습니다. 사용자에게 비밀번호 프롬프트를 표시합니다. 사용자가 비밀번호를 입력한 다음 비밀번호가 TACACS+ 서비스 프로그램으로 전송됩니다.

주의 : TACACS+는 사용자를 식별하기에 충분한 정보를 수집할 때까지 서버 프로그램과 사용자 간의 모든 대화를 허용합니다. 일반적으로 사용자 이름과 비밀번호를 묻는 조합으로 수행되지만 ID 번호와 같은 다른 항목을 포함할 수도 있습니다. 이 모든 것은 TACACS+ 서버 프로그램의 제어를 받습니다.

네트워크 액세스 서버는 마침내 TACACS+ 서버에서 다음 응답 중 하나를 받습니다.

ACCEPT	사용자가 인증을 통과하면 서비스가 시작됩니다. 네트워크 액세스 서버가 서비스 인증을 요구하도록 구성된 경우, 이 순간에 인증이 시작됩니다.
REJECT	사용자가 인증을 통과하지 못했습니다. 사용자는 추가 액세스가 거부되거나 다시 액세스하라는 메시지가 표시될 수 있습니다. TACACS+ 서버의 처리에 따라 달라집니다.
ERROR	인증 중에 오류가 발생하고, 원인은 서버에 있을 수 있습니다. 또한 서버와 네트워크 액세스 서버 간의 네트워크 연결에서 발생할 수도 있습니다. ERROR 응답이 수신되면 일반적으로 네트워크 액세스는 사용자를 식별하기 위한 다른 방법을 시도합니다.
CONTINUE	사용자에게 추가 인증 정보를 입력하라는 메시지가 표시됩니다.

PAP 로그인은 ASCII 로그인과 유사하지만, 차이점은 네트워크 액세스 서버의 사용자 이름과 비밀번호가 사용자에 의해 입력되지 않고 PAP 메시지에 포함된다는 점입니다. 따라서 사용자에게 관련 정보를 입력하라는 메시지가 표시되지 않습니다.

CHAP 로그인은 주요 부분에서 유사합니다. 인증이 완료된 후, 네트워크 액세스 서버가 사용자 권한 부여를 요청하면 사용자는 권한 부여 단계로 이동해야 합니다. 그러나 TACACS+ 권한 부여가 처리되기 전에 TACACS+ 인증이 먼저 완료되어야 합니다.

TACACS+ 권한 부여를 처리해야 하는 경우, TACACS+ 서버 프로그램과 다시 통신해야 하며, ACCEPT(허용) 또는 REJECT(거부)라는 권한 부여 응답으로 돌아갑니다.

ACCEPT 응답으로 돌아올 경우, 사용자의 EXEC 또는 NETWORK 대화와 관련된 세부 사항을 지정하고 사용자가 접근할 수 있는 서비스를 확인하기 위해 사용되는 AV(속성-값(Attribute-Value)) 데이터가 포함될 수 있습니다.

12.5 TACACS+ 구성 프로세스

TACACS+를 지원하도록 구성하려면 다음 작업을 수행해야 합니다.

① tacacs-server 명령 사용

- TACACS+ 서버의 하나 이상의 IP 주소를 지정합니다.

② tacacs key 명령 사용

- 네트워크 액세스 서버와 TACACS+ 서버 간에 교환되는 모든 정보를 암호화할 비밀 키를 설정합니다.
- 동일한 비밀 키가 TACACS+ 서버 프로그램에서도 구성되어야 합니다.

③ 글로벌 구성 명령 aaa authentication 사용

- TACACS+를 사용하여 인증을 수행하는 방법 테이블을 정의합니다.
- aaa authentication 명령에 대한 자세한 내용은 "인증 구성(Authentication Configuration)"을 참조하십시오.

④ line 및 interface 명령 사용

- 정의된 방법 테이블을 인터페이스 또는 라인에 적용합니다.
- 관련 정보는 "인증 구성(Authentication Configuration)"을 참조하십시오.

12.6 TACACS+ 구성 작업 목록

- TACACS+ 서버 할당
- TACACS+ 암호화된 비밀 키 설정
- 인증에 TACACS+ 사용 할당
- 권한 부여에 TACACS+ 사용 할당
- 계정에 TACACS+ 사용 할당

12.7 TACACS+ 구성 작업

12.7.1 ACACS+ 서버 할당

tacacs-server 명령은 TACACS+ 서버의 IP 주소를 지정하는 데 사용할 수 있습니다.

TACACS+는 설정된 순서대로 호스트를 검색하므로, 우선순위가 다른 서버를 구성할 때 유용합니다.

TACACS+ 호스트를 지정하려면 글로벌 구성 모드에서 다음 명령어를 사용하십시오.

명령어	설명
tacacs-server host ip-address **[single-connection| multi-connection] [port** integer] [timeout integer] [**key** string]	TACACS+ 서버의 IP 주소와 관련 기능을 할당합니다.

tacacs-server 구성하기 위해 명령어를 사용하십시오.

- single-connection 키워드 사용 : 단일 연결 방식을 지정합니다. 이를 통해 서버 프로그램이 더 많은 TACACS+ 작업을 효율적으로 처리할 수 있습니다. multi-connection 은 여러 TCP 연결 방식을 채택합니다.
- port 매개변수 사용 : TACACS+ 서버 프로그램에서 사용하는 TCP 포트 번호를 지정합니다. 기본 포트 번호는 49입니다.
- timeout 매개변수 사용 : 서버로부터 응답을 기다리는 OLT의 시간 상한을 지정합니다 (단위: 초).
- key 매개변수 사용 : 메시지 암호화 및 복호화를 위한 비밀 키를 지정합니다.

주의 : tacacs-server 명령을 사용하여 호스트에 연결한 후, timeout 명령으로 정의된 시간 초과 값을 적용하여, tacacs-server timeout 명령으로 설정된 전역 시간 초과 값을 덮어씁니다.

또한, tacacs-server 명령으로 지정된 암호화 비밀 키를 사용하여, 글로벌 구성 명령어 tacacs-server key로 설정된 기본 비밀 키를 덮어씁니다.

따라서 이 명령은 네트워크 보안을 강화하기 위해 고유한 TACACS+ 연결을 구성하는 데 사용됩니다.

12.7.2 TACACS+ 암호화된 비밀 키 설정

TACACS+ 메시지의 암호화 비밀 키를 설정하려면 글로벌 구성 모드에서 다음 명령어를 사용하십시오

명령어	설명
tacacs-server key *keystring*	TACACS+ 서버에서 사용되는 암호화 비밀 키와 일치하는 암호화 비밀 키를 설정합니다.

주의 : 암호화를 성공적으로 수행하려면 동일한 비밀 키를 TACACS+ 서버 프로그램에서도 구성해야 합니다.

12.7.3 TACACS+를 인증에 사용하도록 지정

TACACS+ 서버를 지정하고 관련 암호화 비밀 키를 정의한 후, TACACS+ 인증을 위한 방법 테이블을 정의해야 합니다.

TACACS+ 인증은 AAA를 통해 처리되므로, aaa authentication 명령을 사용하여 TACACS+를 인증 방법으로 지정해야 합니다.

자세한 내용은 "Authentication Configuration"(인증 구성)을 참조하십시오.

12.7.4 TACACS+를 권한 부여에 사용하도록 지정

AAA 권한 부여는 사용자의 네트워크 접근 제한을 설정하는 매개변수를 구성하는 데 도움을 줍니다. TACACS+ 권한 부여는 명령어, 네트워크 연결, EXEC 대화 등의 서비스에 적용될 수 있습니다.

TACACS+ 권한 부여는 AAA를 통해 처리되므로, aaa authorization 명령을 사용하여 TACACS+를 권한 부여 방법으로 지정해야 합니다.

자세한 내용은 "Authorization Configuration"(권한 부여 구성)을 참조하십시오.

12.7.5 TACACS+를 계정 관리에 사용하도록 지정

AAA 계정 관리는 사용자의 현재 서비스와 소비된 네트워크 리소스의 양을 추적할 수 있습니다.

TACACS+ 계정 관리는 AAA를 통해 처리되므로, aaa accounting 명령을 사용하여 TACACS+를 계정 관리 방법으로 지정해야 합니다.

자세한 내용은 "Accounting Configuration"(계정 관리 구성)을 참조하십시오.

12.8 TACACS+ 구성 예제

이 장에는 TACACS+ 구성 예제가 포함되어 있습니다.

12.8.1 TACACS+ 인증 예제

다음은 TACACS+를 사용하여 로그인 인증을 구성하는 예제입니다.

```
aaa authentication login test group tacacs+ local
tacacs-server host 1.2.3.4
tacacs-server key testkey
line vty 0
login authentication test
```

예제 설명

- aaa authentication 명령은 vty0에서 사용되는 test 인증 방법 테이블을 정의합니다.
- tacacs+ 키워드는 인증이 TACACS+를 통해 처리됨을 의미합니다.
- 인증 중 TACACS+가 응답하지 않을 경우, local 키워드는 네트워크 액세스 서버의 로컬 데이터베이스를 사용하여 인증을 수행함을 나타냅니다.
- tacacs-server host 명령은 TACACS+ 서버의 IP 주소를 1.2.3.4로 지정합니다.
- tacacs-server key 명령은 공유 암호화 비밀 키를 testkey로 정의합니다.

다음은 TACACS+를 로그인 인증으로 구성할 때 보안 프로토콜을 사용하는 예제입니다. 이 경우 default 방법 테이블이 사용되며, test는 사용되지 않습니다.

aaa authentication login default group tacacs+ local

tacacs-server host 1.2.3.4

tacacs-server key goaway

예제 설명

- aaa authentication 명령은 로그인 인증 시 기본 인증 방법 테이블인 default를 정의합니다.
- 인증이 필요한 경우, tacacs+ 키워드는 TACACS+를 통해 인증이 수행됨을 나타냅니다.
- TACACS+가 응답하지 않을 경우, local 키워드는 네트워크 액세스 서버의 로컬 데이터베이스를 사용하여 인증을 수행함을 나타냅니다.
- tacacs-server host 명령은 TACACS+ 서버 프로그램의 IP 주소를 1.2.3.4로 지정합니다.
- tacacs-server key 명령은 공유 암호화 비밀 키를 goaway로 정의합니다.

12.8.2 TACACS+ 권한 부여 예시

aaa authentication login default group tacacs+ local

aaa authorization exec default group tacacs+

tacacs-server host 10.1.2.3

tacacs-server key goaway

예제 설명

- aaa authentication 명령은 로그인 인증 시 기본 인증 방법 테이블인 default를 정의합니다. 인증이 필요한 경우, tacacs+ 키워드는 인증이 TACACS+를 통해 수행됨을 의미합니

다. TACACS+가 응답하지 않을 경우, local 키워드는 네트워크 액세스 서버의 로컬 데이터베이스를 사용하여 인증을 수행함을 나타냅니다.

- aaa authorization 명령은 TACACS+를 사용하여 네트워크 서비스 권한을 부여합니다.
- tacacs-server host 명령은 TACACS+ 서버의 IP 주소를 10.1.2.3으로 지정합니다.
- tacacs-server key 명령은 공유 암호화 비밀 키를 goaway로 정의합니다.

12.8.3 TACACS+ 계정 관리 예제

다음은 TACACS+를 로그인 인증 및 계정 관리 방법으로 사용하는 구성 예제입니다.

```
aaa authentication login default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
```

예제 설명

- aaa authentication 명령: 로그인 인증 시 기본 인증 방법 테이블 default를 정의합니다. tacacs+ 키워드는 인증이 TAC ACS+를 통해 수행됨을 나타냅니다. TACACS+가 응답하지 않을 경우, local 키워드는 네트워크 액세스 서버의 로컬 데이터베이스를 사용하여 인증을 수행하도록 지정합니다.
- aaa accounting 명령: 네트워크 서비스의 계정 관리를 TACACS+를 사용하여 수행합니다. 이 예제에서는 서비스 시작 및 종료 시간에 대한 정보를 TACACS+ 서버에 기록하고 전송합니다.
- tacacs-server host 명령: TACACS+ 서버의 IP 주소를 10.1.2.3으로 지정합니다.
- tacacs-server key 명령: 공유 암호화 비밀 키를 goaway 로 정의합니다.

12.9 802.1x 설정 목록

- 802.1x 포트 인증 설정
- 802.1x 다중 호스트 포트 인증 설정
- 802.1x 재인증 설정
- 802.1x 재인증 횟수 설정
- 802.1x 데이터 전송 주기 설정
- 802.1x 사용자 바인딩 설정
- 802.1x 포트 인증 방식 설정
- 802.1x 포트 인증 유형 선택
- 802.1x 계정 관리 설정
- 802.1x 게스트 VLAN 설정
- 다중 네트워크 어댑터를 사용하는 클라이언트 금지
- 802.1x 기본 설정으로 복구
- 802.1x 인증 설정 및 상태 모니터링

12.10 802.1.X 설정 작업

12.10.1 802.1x Port Authentication 설정

802.1x는 포트에 대한 세 가지 제어 방법을 정의합니다. 필수 인증 승인, 필수 인증 거부 및 802.1x 인증 시작입니다.

필수 인증 승인은 포트가 이미 인증을 통과했음을 의미합니다. 포트는 더 이상 인증이 필요하지 않으며 모든 사용자가 포트를 통해 data 액세스 제어를 수행할 수 있습니다. 인증 방법은 포트에서 기본값으로 설정됩니다. 필수 인증 거부는 어떤 종류의 방법이 적용되든 포트 인증이 통과되지 않음을 의미합니다. 어떤 사용자도 포트를 통해 데이터 액세스 제어를 수행할 수 없습니다.

802.1x 인증 시작은 포트가 802.1x 인증 프로토콜을 실행해야 함을 의미합니다. 802.1x 인증은 포트에 액세스하는 사용자에게 적용됩니다. 인증을 통과한 사용자만 포트를 통해 데이터 액세스 제어를 수행할 수 있습니다. 802.1x 인증이 시작된 후 AAA 인증 방법을 설정해야 합니다.

802.1x를 설정하기 전에 다음 명령을 실행하여 802.1x 기능을 활성화하십시오.

명령어	설명
dot1x enable	802.1x 기능을 활성화 합니다.

다음 명령을 실행하여 802.1x 인증을 시작하세요.

명령어	설명
dot1x port-control auto	포트에서 802.1x 프로토콜 제어 방법을 설정합니다.
aaa authentication dot1x {default |list name} method1 [method2...]	802.1x 의 AAA 인증을 설정합니다.

포트 설정 모드에서 다음 명령 중 하나를 실행하여 802.1x를 선택하세요.

명령어	설명
dot1x port-control auto	포트에서 802.1x 인증 방법을 시작합니다.
dot1x port-control force-authorized	필수 포트 인증을 승인합니다.
dot1x port-control force-unauthorized	필수 포트 인증을 거부합니다.
dot1x port-control misc-mab	802.1x 하이브리드 인증을 활성화합니다.

12.10.2 802.1x Multiple-host Port Authentication 설정

802.1x 인증은 단일 호스트 사용자 인증을 위한 것입니다. 이 경우 스위치는 한 사용자만 인증 및 액세스 제어를 수행하도 록 허용합니다. 이전 사용자가 인증 및 액세스를 종료하지 않는 한 다른 사용자는 인증 및 액세스할 수 없습니다. 포트가 802.1x를 지원하지 않는 스위치 장치를 통해 여러 호스트를 연결하는 경우 여러 포트 액세스 기능을 시작하여 모든 호스트 사용자가 액세스할 수 있도록 할 수 있습니다.

포트가 802.1x의 다중 호스트 인증으로 설정된 후, 스위치는 다른 호스트 사용자를 인증합니다. 인증이 승인되면 호스트는 스위치를 통해 액세스할 수 있습니다(호스트의 MAC 주소는 제어에 사용됨). 이론적으로 802.1x는 호스트 사용자 수를 제한할 수 없습니다. 스위치가 사용자의 MAC 주소를 통해 사용자 인증을 제어하기 때문에 호스트 사용자 수는 스위치의 MAC 주소 테이블 크기에 따라 제한됩니다. 802.1x 다중 호스트 인증을 활성화하려면 인터페이스 설정 모드에서 다음 명령을 실행하세요.

명령어	설명
dot1x authentication multiple-hosts	802.1x 다중 호스트 포트 인증을 설정합니다. 한 사용자가 인증을 통과하는 경우에만 포트가 설정됩니다.
dot1x authentication multiple-auth	802.1x 다중 호스트 포트 인증을 설정합니다. 각 사용자는 인증과 관련이 없습니다.

12.10.3 802.1x Re-authentication 설정

인증이 통과된 후에도 클라이언트에 대한 인증은 클라이언트 인증의 합법성을 보장하기 위해 매 설정된 간격마다 수행됩니다. 이 경우 re-authentication 기능을 활성화해야 합니다. 재인증이 시작된 후 인증 요청이 주기적으로 호스트로 전송됩니다.

다음 명령을 실행하여 re-authentication 기능을 설정합니다.

명령어	설명
dot1x re-authentication	re-authentication 기능을 활성화 합니다.
dot1x timeout re-authperiod *time*	re-authentication 기능의 기간을 설정합니다.

12.10.4 802.1x Re-authentication 횟수 설정

인증이 실패하면 스위치는 인증을 활성화하기 위해 요청/ID 패킷을 다시 보냅니다. re-authentication 시간이 특정 숫자를 초과하고 여전히 응답이 없으면 인증이 중단됩니다.

re-authentication 의 최대 횟수를 설정하려면 인터페이스 설정 명령에서 다음 명령을 실행하세요.

명령어	설명
dot1x reauth-max time	re-authentication 의 최대 횟수를 설정합니다.

12.10.5 802.1x 전송 주기 설정

802.1x 인증 과정에서 데이터 텍스트가 호스트로 전송됩니다. 데이터 전송은 802.1x 전송주기를 제어하여 호스트 응답이 성공하도록 할 수 있습니다.

다음 명령을 실행하여 전송 주기를 설정합니다.

명령어	설명
dot1x reauth-max *time*	802.1x 의 메시지 전송 주기를 설정합니다.

12.10.6 802.1x 사용자 바인딩 설정

802.1x 인증이 수행되면 포트 액세스의 보안을 보장하기 위해 사용자를 특정 포트에 바인딩할 수 있습니다.

인터페이스 설정 모드에서 다음 명령을 실행하여 802.1x 사용자 바인딩을 시작합니다.

명령어	설명
dot1x timeout tx-period *time*	포트에 바인딩된 사용자를 설정합니다.

12.10.7 802.1x 포트 인증 방식 설정

802.1x 인증은 다른 포트에서 다른 방법으로 수행할 수 있습니다. 기본 설정에서 802.1x 인증은 기본 방법을 채택합니다.

인터페이스 설정 모드에서 다음 명령을 실행하여 802.1x 인증 방법을 설정합니다.

명령어	설명
dot1x authentication method *yyy*	802.1x 인증 방법을 설정합니다.

12.10.8 802.1x 포트 인증 유형 선택

802.1x 인증 유형을 선택할 수 있습니다. 802.1x 인증 유형은 AAA가 Chap 인증 또는 Eap 인증을 사용하는지 여부를 결정합니다. Eap 인증은 md5-challenge 모드와 eap-tls 모드를 지원합니다. MD5에서 요구하는 챌린지는 Chap 인증이 채택될 때 로컬에서 생성되는 반면, 챌린지는 eap 인증이 채택될 때 인증 서버에서 생성됩니다. 각 포트는 하나의 인증 유형만 채택합니다. 기본적으로 글로벌 설정의 인증 유형이 채택됩니다. 포트가 인증 유형으로 설정되면 기본값을 재개하기 위해 No 명령을 실행하지 않는 한 포트는 인증 유형을 사용합니다.

Eap-tls는 전자 인증서를 인증 보증으로 사용하고 변환 계층 보안(tls)의 핸드셰이크 규칙을 준수합니다. 따라서 높은 보안이 보장됩니다.

글로벌 설정 모드에서 다음 명령을 실행하여 인증 유형을 설정합니다.

명령어	설명
dot1x authen-type {**chap**|**eap**}	chap 또는 eap 를 선택합니다

인터페이스 설정 모드에서 다음 명령을 실행합니다.

명령어	설명
dot1x authentication type {**chap**|**eap**}	글로벌 모드에서 chap, eap 또는 설정된 인증 유형을 선택합니다.

12.10.9 802.1x 계정 설정

802.1x 인증과 802.1x 계정 관리는 동시에 수행할 수 있습니다. 작동 메커니즘은 다음과 같습니다: dot1x 인증이 승인된 후, 인증 인터페이스에서 계정 관리 기능이 활성화되었는지 판단합니다. 계정 관리 기능이 활성화된 경우, AAA 인터페이스를 통해 계정 요청을 전송합니다. AAA 모듈이 요청 성공 응답 메시지를 반환하면, AAA 인터페이스는 텍스트를 전달할 수 있습니다.

계정 관리는 AAA 모듈에 설정된 다양한 계정 관리 방식을 채택할 수 있습니다. 자세한 내용은

AAA 설정을 참조하십시오.

계정 관리가 시작된 후, dot1x는 정확한 계정 정보를 얻기 위해 주기적으로 업데이트 메시지를 AAA 인터페이스를 통해 서버로 전송합니다. 서로 다른 AAA 설정에 따라, AAA 모듈은 업데이트 메시지를 전송할지 여부를 결정합니다.

동시에, 클라이언트가 비정상적인 경우 스위치가 이를 알 수 있도록 dot1x 재인증 기능을 활성화해야 합니다.

다음 명령어를 인터페이스 설정 모드에서 실행하여 dot1x 계정 관리를 활성화하고 계정 관리 방식을 설정하십시오

명령어	설명
dot1x accounting enable	dot1x 계정을 활성화 합니다.
dot1x accounting method {*method name*}	계정설정 방법을 구성합니다. 기본값은 default 입니다.

업데이트 구성 정보를 표시하려면 글로벌 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
aaa accounting update periodic <30-120>	레코드 업데이트 정보를 전송하는 시간 간격(초)

12.10.10 802.1x guest-vlan 설정

게스트 VLAN은 클라이언트가 응답하지 않을 때 관련 포트에 일부 접근 권한(예: 클라이언트 소프트웨어 다운로드)을 제공합니다. 게스트 VLAN은 시스템에서 구성된 VLAN 중 하나가 될 수 있습니다. 설정된 게스트 VLAN이 조건을 충족하지 못하면 포트는 게스트 VLAN에서 작동할 수 없습니다.

참고: 인증에 실패한 경우 접근 권한이 부여되지 않습니다.

다음 명령어를 글로벌 모드에서 실행하여 게스트 VLAN을 활성화하십시오.

명령어	설명
Dot1x guest-vlan	모든 포트에서 guest-vlan 을 활성화합니다.

각 포트의 게스트 VLAN ID가 기본적으로 0으로 설정되어 있으면, 글로벌 모드에서 게스트 VLAN이 활성화되더라도 게스트 VLAN은 작동하지 않습니다. 포트 구성 모드에서 게스트 VLAN ID를 설정해야만 게스트 VLAN이 작동할 수 있습니다.

다음 명령어를 포트 구성 모드에서 실행하여 게스트 VLAN ID를 설정하십시오

명령어	설명
Dot1x guest-vlan {id(1-4094)}	모든 포트에서 guest-vlan 의 vlan ID 를 활성화합니다.

12.10.11 다중 네트워크 카드가 있는 Supplicant 금지

에이전트를 방지하기 위해 여러 네트워크 어댑터가 있는 Supplicant를 금지합니다. 802.1x 프로토콜에서 **Supplicant(서플리컨트)**는 네트워크에 연결을 시도하고 인증을 요청하는 클라이언트 장치를 의미합니다. 주로 컴퓨터, 스마트폰, 또는 네트워크에 연결하려는 기타 디바이스를 지칭합니다.

포트 구성 모드에서 다음 명령을 실행합니다.

명령어	설명
dot1x forbid multi-network-adapter	여러 개의 네트워크 어댑터를 사용하는 것을 금지합니다.

12.10.12 802.1x 기본 설정 복구

다음 명령을 실행하여 모든 글로벌 구성을 기본 구성으로 다시 시작하세요.

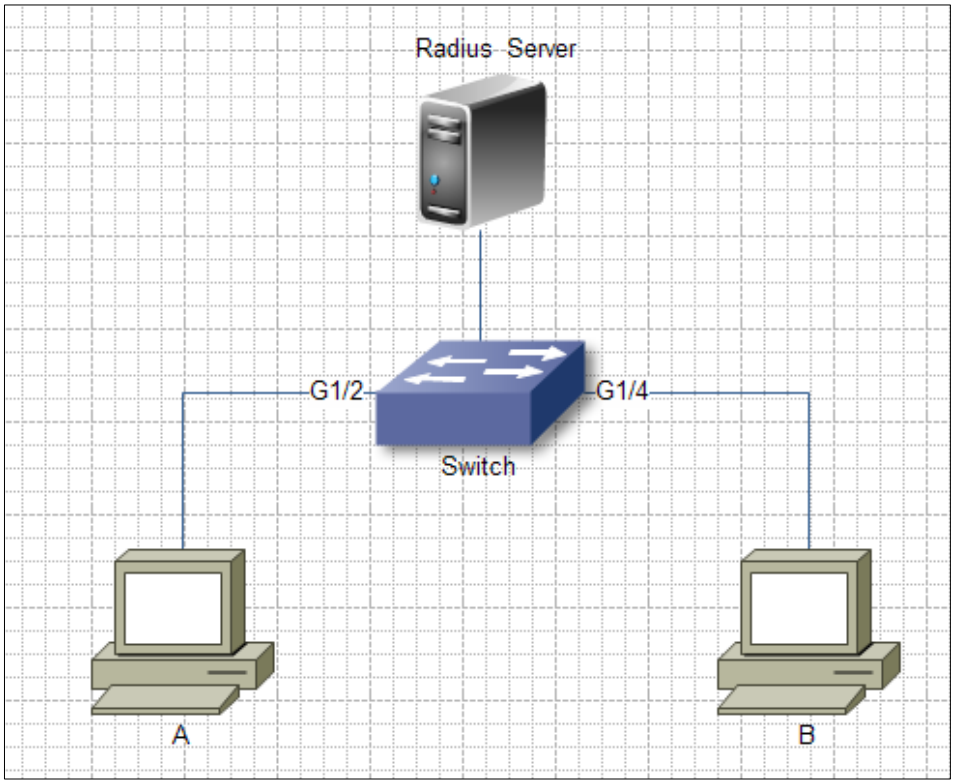
명령어	설명
dot1x default	모든 글로벌 구성을 기본 구성으로 다시 시작합니다.

12.10.13 802.1x 인증 구성 및 상태 모니터링

802.1x 인증의 구성 및 상태를 모니터링하고 어떤 802.1x 매개변수를 조정해야 할지 결정하려면 관리 모드에서 다음 명령을 실행하세요.

명령어	설명
show dot1x { *interface|statistics|misc-mab-db* }	802.1x 인증의 구성과 상태를 모니터링합니다.

12.11 802.1x 설정 예시



호스트 A는 스위치의 포트 G1/2에 연결됩니다.

호스트 B는 포트 G1/4에 연결됩니다.

호스트 C는 포트 G1/6에 연결됩니다.

RADIUS 서버 호스트의 IP 주소는 192.168.20.2이고, RADIUS 키는 TST입니다.

- 포트 G1/2

  원격 RADIUS 인증 방식을 사용합니다.

  사용자 바인딩 및 재인증 기능을 적용합니다.

- 포트 G1/4

  EAP 유형의 로컬 인증 방식을 사용합니다.

  다중 호스트 모드와 게스트 VLAN을 활성화합니다.

- 글로벌 설정

  username switch password 0 TST

username TST password 0 TST

aaa authentication dot1x TST-G1/2 group radius

aaa authentication dot1x TST-G1/4 local

aaa authentication dot1x TST-G1/6 group radius

aaa accounting network dot1x_acc start-stop group radius

dot1x enable

dot1x re-authentication

dot1x timeout re-authperiod 10

dot1x guest-vlan

interface VLAN1

ip address 192.168.20.24 255.255.255.0

!

vlan 1-2

radius-server host 192.168.20.2 auth-port 1812 acct-port 1813

radius-server key TST

- G1/2 포트 설정

interface GigaEthernet1/2

dot1x port-control auto

dot1x authentication method TST-G1/2

dot1x user-permit radius-TST

dot1x accounting enable

dot1x accounting method dot1x_acc

- G1/4 포트 설정

Interface GigaEthernet1/4

dot1x authentication multiple-hosts

dot1x port-control auto

dot1x authentication method TST-G1/4

dot1x guest-vlan 2

13 Interface 설정 소개

이 섹션은 스위치에서 지원하는 다양한 인터페이스 유형에 대해 학습하고, 각 인터페이스 유형별 구성 정보를 참조할 수 있도록 돕습니다. 이 섹션에서 사용된 모든 인터페이스 명령어에 대한 자세한 설명은 '인터페이스 구성 명령어'를 참조하십시오. 이 섹션에 등장하는 기타 명령어는 매뉴얼의 다른 부분을 참조하십시오.

소개에는 모든 인터페이스 유형에 적용할 수 있는 통신 정보가 포함되어 있습니다.

13.4 지원되는 인터페이스 유형

인터페이스 유형에 대한 정보는 아래 표를 참조하십시오.

인터페이스 유형	작업	참고
이더넷 인터페이스	고속 이더넷 인터페이스를 구성합니다. 기가비트 이더넷 인터페이스를 구성합니다.	이더넷 인터페이스 구성
논리적 인터페이스	Aggregation 인터페이스 VLAN 인터페이스	논리적 인터페이스 구성

스위치에서 지원하는 두 가지 주요 인터페이스 유형은 이더넷 인터페이스와 논리적 인터페이스입니다.

- 이더넷 인터페이스는 장치의 표준 통신 인터페이스와 스위치에 설치된 인터페이스 카드 또는 모듈에 따라 달라집니다.
- 논리적 인터페이스는 해당 물리적 장치가 없는 인터페이스로, 사용자가 수동으로 생성합니다.

스위치에서 지원되는 이더넷 인터페이스:

- 고속 이더넷 인터페이스
- 기가비트 이더넷 인터페이스

스위치에서 지원되는 논리적 인터페이스:

- 집계 인터페이스
- VLAN 인터페이스

13.5 인터페이스 구성 소개

다음 설명은 모든 인터페이스의 구성 과정에 적용됩니다. 글로벌 구성 모드에서 인터페이스를 구성하려면 다음 단계를 따르십시오.

① interface 명령 실행

- interface 명령을 실행하여 인터페이스 구성 모드에 들어가 인터페이스 구성을 시작합니다.
- 이때 스위치 프롬프트는 'config_'에 구성할 인터페이스의 축약형이 추가된 형태로 바뀝니다.
- 이러한 인터페이스는 번호를 기준으로 사용됩니다. 번호는 초기 설치 시(출고 시) 또는 시스템에 인터페이스 카드를 추가할 때 할당됩니다.

② show interface 명령 실행

- show interface 명령을 실행하여 해당 장치에서 지원하는 인터페이스를 표시하고 상태를 확인합니다.
- 각 장치가 지원하는 인터페이스는 고유한 상태 정보를 제공합니다.

예를 들어, 장치에서 지원하는 인터페이스 상태는 다음과 같이 나타날 수 있습니다

```
Switch_config#show interface g0/2


GigaEthernet0/2 is administratively down, line protocol is down
  Hardware is Giga-Combo-FX, address is 00e0.0f8d.e0e1 (bia 00e0.0f8d.e0e1)
  MTU 1500 bytes, BW 10000 kbit, DLY 10 usec
  Encapsulation ARPA
  port info 1 0 2 1
  Auto-duplex, Auto-speed
  flow-control off
    Received 0 packets, 0 bytes
    0 broadcasts, 0 multicasts
    0 discard, 0 error, 0 PAUSE
    Transmitted 0 packets, 0 bytes
    0 broadcasts, 0 multicasts
```

0 discard, 0 error, 0 PAUSE

참고: 인터페이스 유형과 인터페이스 번호 사이에는 공백을 추가하지 않아도 됩니다.

예: g0/2 또는 g 0/2 모두 올바른 형식입니다.

③ 인터페이스 구성 모드에서 인터페이스 구성 명령을 설정할 수 있습니다. 다양한 명령어를 사용하여 인터페이스에서 실행될 프로토콜과 애플리케이션 프로그램을 정의할 수 있습니다. 이러한 명령어는 사용자가 인터페이스 구성 모드를 종료하거나 다른 인터페이스로 전환할 때까지 유지됩니다.

④ 인터페이스 구성이 완료되면 인터페이스 모니터링 및 유지 관리 에 나오는 show 명령어를 사용하여 인터페이스 상태를 테스트하십시오.

14 인터페이스 설정

14.4 인터페이스 공통속성 구성

다음 내용은 모든 유형의 인터페이스에서 실행할 수 있는 명령어를 설명하며, 인터페이스의 공통 속성을 구성합니다. 구성할 수 있는 인터페이스의 공통 속성에는 인터페이스 설명, 대역폭, 지연 시간 등이 포함됩니다.

14.2.1 설명 추가

관련 인터페이스에 대한 설명을 추가하면 해당 인터페이스에 첨부된 내용을 기억하는 데 도움이 됩니다. 이 설명은 인터페이스의 용도를 식별하는 참고용으로만 사용되며, 인터페이스의 어떤 기능에도 영향을 미치지 않습니다. 이 설명은 다음 명령어 출력에 나타납니다: show running-config 및 show interface 인터페이스에 설명을 추가하려면 인터페이스 구성 모드에서 다음 명령어를 사용하십시오.

명령어	설명
description *string*	현재 구성된 인터페이스에 설명을 추가합니다.

인터페이스 설명 추가와 관련된 예제는 '인터페이스 설명 예제' 섹션을 참조하십시오.

14.4.1 대역폭 설정

대역폭 정보를 사용하여 작업 결정을 내립니다. 인터페이스에 대역폭을 설정하려면 다음 명령어를 사용하십시오.

명령어	설명
bandwidth *kilobps*	현재 구성된 인터페이스의 대역폭을 설정합니다.

대역폭은 단순히 라우팅 매개변수일 뿐이며, 실제 물리적 인터페이스의 통신 속도에는 영향을 미치지 않습니다.

14.4.2 시간 지연 설정

상위 프로토콜은 시간 지연 정보를 사용하여 작업 결정을 내립니다. 인터페이스에 시간 지연을 구성하려면 인터페이스 구성 모드에서 다음 명령어를 사용하십시오.

명령어	설명
delay *tensofmicroseconds*	현재 구성된 인터페이스의 시간 지연을 설정합니다.

시간 지연 설정은 단순히 정보 매개변수일 뿐이며, 이 명령어를 사용해도 실제 인터페이스의 시간 지연을 조정할 수는 없습니다.

14.2 인터페이스 모니터링 및 유지 관리

다음 작업은 인터페이스를 모니터링하고 유지 관리하는 데 사용할 수 있습니다:

- 인터페이스 상태 확인
- 인터페이스 초기화 및 삭제
- 인터페이스 종료 및 활성화

14.2.1 인터페이스 상태 확인

스위치는 소프트웨어 및 하드웨어 버전 번호, 인터페이스 상태를 포함한 인터페이스 정보와 관련된 여러 명령어를 표시할 수 있습니다. 아래 표는 일부 인터페이스 모니터링 명령어를 나열합니다. 이러한 명령어에 대한 설명은 '인터페이스 구성 명령어' 섹션을 참조하십시오.

명령어	설명
show interface [**type** [slot|port]]	인터페이스 상태를 표시 합니다.
show running-config	현재 설정을 표시 합니다.
show version	메모리 정보, 소프트웨어 버전 등을 표시합니다.

14.2.2 인터페이스 초기화 및 삭제

논리적 인터페이스를 동적으로 생성 및 삭제할 수 있습니다. 이 작업은 서브 인터페이스 및 채널화된 인터페이스에도 적용됩니다.

글로벌 구성 모드에서 다음 명령어를 사용하여 인터페이스를 초기화하거나 삭제하십시오.

명령어	설명
no interface [**type** [slot|port]]	물리적 인터페이스를 초기화하거나 가상 인터페이스를 삭제합니다.

14.2.3 인터페이스 종료 및 활성화

인터페이스가 종료되면 해당 인터페이스의 모든 기능이 비활성화되며, 모든 모니터링 명령어 출력에서 사용할 수 없는 인터페이스로 표시됩니다. 이 정보는 동적 라우팅 프로토콜을 통해 다른 스위치로 전송될 수 있습니다.

인터페이스 구성 모드에서 다음 명령어를 사용하여 인터페이스를 종료하거나 활성화하십시오.

명령어	설명
shutdown	인터페이스를 종료합니다.
no shutdown	인터페이스를 활성화합니다.

show interface 명령과 show running-config 명령을 사용하여 인터페이스가 종료되었는지 확인할 수 있습니다. 종료된 인터페이스는 show interface 명령 디스플레이에서 'administratively down'으로 표시됩니다. 자세한 내용은 'Interface Shutdown Example'의 다음 예를 참조하십시오.

14.3 이더넷 인터페이스 설정

이 섹션에서는 이더넷 인터페이스 설정 절차를 설명합니다. 자세한 구성에는 다음 단계가 포함되며, 그 중 1단계는 필수이고 다른 단계는 선택 사항입니다.

14.3.1 이더넷 인터페이스 설정

이더넷 인터페이스 구성 모드로 들어가려면 글로벌 구성 모드에서 다음 명령을 실행하세요.

명령어	설명
interface gigaethernet [*slot*|*port*]	기가비트 이더넷 인터페이스 구성 모드로 들어갑니다.

show interface gigaethernet [slot|port] 명령은 기가비트 이더넷 인터페이스의 상태를 보여주는 데 사용할 수 있습니다.

14.3.2 RATE 구성

이더넷 속도는 자동 협상(auto-negotiation)을 통해 설정할 수 있을 뿐만 아니라, 인터페이스 구성을 통해서도 실현할 수 있습니다.

명령어	설명

show interface gigaethernet [*slot*|*port*]	빠른 이더넷 속도를 10M, 100M, 1000M 또는 자동 협상으로 설정합니다.
show interface gigaethernet [*slot*|*port*]	기본 설정을 재개합니다. 속도는 자동 협상입니다.

참고 :

- 광 인터페이스의 속도는 모델에 따라 다릅니다.
- 예: GE-FX의 속도는 기본적으로 1000M이지만, 구성에 따라 100M로 지정할 수도 있습니다.
- FE-FX의 속도는 100M입니다.
- 광 인터페이스 속도 명령 뒤에 auto 매개변수가 있을 경우, 자동 협상 기능이 활성화됩니다.
- Auto 매개변수가 없는 경우, 광 인터페이스 속도는 고정되며 협상할 수 없습니다.
- 기가비트 포트는 자동 모드에서 10M, 100M, 1000M을 지원합니다.
- 구체적인 설정은 각 포트의 프롬프트 메시지에 따라야 합니다.

14.3.3 인터페이스의 이중 모드 구성

기본적으로 이더넷 인터페이스는 반이중(half-duplex) 또는 전이중(full-duplex)을 자동으로 협상합니다. 기가비트 인터페이스의 이중 모드는 항상 자동(auto)입니다.

명령어	설명
duplex {**full**|**half**|**auto**}	이더넷 인터페이스의 이중 모드를 설정합니다.
No duplex	기본 설정을 재개합니다. 속도는 자동 협상입니다.

14.3.4 인터페이스에서 Flow Control 구성

인터페이스가 전이중 모드일 때, 흐름 제어는 802.3X에서 정의된 PAUSE 프레임을 통해 구현됩니다. 반이중 모드에서는 백 프레셔(back pressure) 방식으로 구현됩니다.

명령어	설명
flow-control *on/off /auto*	인터페이스에서 흐름 제어를 활성화하거나 비활성화합니다.

no flow-control	기본 설정으로 복원합니다. 기본값은 인터페이스에서 흐름 제어를 사용하지 않는 것입니다.

14.4 논리적 인터페이스 구성

이 섹션은 논리적 인터페이스를 구성하는 방법을 설명합니다. 다음 구성 내용이 포함됩니다:

- Aggregation 인터페이스 구성
- VLAN 인터페이스 구성

14.4.1 Aggregation 인터페이스 구성

단일 이더넷 인터페이스의 대역폭이 부족할 경우, Aggregation 인터페이스가 필요합니다

Aggregation 인터페이스는 동일한 속도의 여러 전이중 인터페이스를 묶어 대역폭을 크게 향상시킬 수 있습니다.

명령어	설명
Interface port-aggregator *number*	aggregation 인터페이스를 설정합니다.

14.4.2 VLAN 인터페이스 구성

VLAN 인터페이스는 스위치에서 라우팅 인터페이스 역할을 합니다.

글로벌 구성 모드에서 VLAN 명령은 시스템에 2계층 VLAN을 추가하지만, 해당 VLAN 내에서 목적지 주소가 자신인 IP 패킷을 처리하는 방법은 정의하지 않습니다.

VLAN 인터페이스가 없으면 이러한 패킷은 삭제됩니다. VLAN 인터페이스를 정의하려면 다음 명령어를 실행하십시오:

명령어	설명
Interface vlan *number*	VLAN 인터페이스를 구성합니다.

14.4.3 인터페이스 설명 예제

다음은 인터페이스와 관련된 설명을 추가하는 방법을 보여줍니다.
이 설명은 구성 파일과 인터페이스 명령 출력에 나타납니다.

interface vlan 1

ip address 192.168.1.23 255.255.255.0

14.4.4 인터페이스 종료 예제

다음은 이더넷 인터페이스 0/1을 종료하는 방법을 보여줍니다.

interface GigaEthernet0/1

shutdown

다음은 인터페이스를 활성화하는 방법을 보여줍니다:

interface GigaEthernet0/1

no shutdown

14.5 인터페이스 범위 구성 작업

14.5.1 인터페이스 범위의 이해

인터페이스 작업을 구성하는 과정에서 동일한 유형의 포트에 동일한 속성을 설정해야 하는 경우가 있습니다.

각 포트를 반복적으로 구성하는 것을 피하기 위해 인터페이스 범위 구성 모드를 제공합니다. 이 모드를 사용하면 동일한 유형과 슬롯 번호를 가진 포트에 동일한 구성 매개변수를 설정할 수 있습니다.

참고 : 인터페이스 범위 모드에 진입할 때, 이 모드에 포함된 모든 인터페이스는 이미 설정되어 있어야 합니다.

14.5.2 인터페이스 범위 모드 설정

다음 명령어를 실행하여 인터페이스 범위 모드로 진입하십시오.

명령어	설명
interface range *type slot/<port1-port2 | port3>*[, *<port1-port2|port3>*]	범위 모드에 진입합니다. 이 모드에 포함된 모든 포트는 다음 조건을 충족해야 합니다: ① 슬롯 번호는 slot으로 설정됩니다. ② 하이픈(-) 앞뒤의 포트 번호는 port1에서 port2 사이여야 하며, 또는 port3과 같아야 합니다. ③ port2는 반드시 port1보다 작아야 합니다. ④ 하이픈(-) 또는 쉼표(,) 앞뒤에 공백이 없어야 합니다

14.5.3 설정 예제

다음 명령어를 통해 슬롯 0과 고속 이더넷 포트 1, 2, 3, 4를 포함한 인터페이스 구성 모드로 진입합니다

switch_config# interface range gigaEthernet 0/1-4

switch_config_if_range#

15 포트 구성

15.2이더넷 인터페이스 구성

이 섹션은 이더넷 인터페이스를 구성하는 방법을 설명합니다. 스위치는 10Mbps 이더넷과 100Mbps 고속 이더넷을 지원합니다.

자세한 구성은 아래와 같습니다. 1.1.1 섹션에서 설명된 단계는 필수이며, 다른 섹션에서 설명된 단계는 선택 사항입니다.

15.2.1 이더넷 인터페이스 선택

글로벌 구성 모드에서 다음 명령어를 실행하여 이더넷 인터페이스 구성 모드로 진입하십시오.

명령어	설명
interface gigaethernet [slot|port]	기가비트 이더넷 인터페이스 구성 모드로 들어갑니다.

show interface fastethernet 명령을 실행하여 fastEthernet 인터페이스의 상태를 표시할 수 있습니다. show interface gigaethernet 명령을 실행하여 기가비트 이더넷 인터페이스의 상태를 표시할 수 있습니다.

15.2.2 Rate 구성

이더넷 속도는 자동 협상(auto-negotiation) 또는 인터페이스 구성을 통해 설정할 수 있습니다. 이더넷 속도를 구성하려면 다음 명령어를 실행하십시오.

명령어	설명
Speed {**10**|**100**|**auto**} (T port) **Speed** {**100**|**1000**|**auto**} (SFP port)	고속 이더넷의 속도를 10M, 100M, 1000M 또는 자동 협상으로 설정합니다.
No speed	기본 설정(자동 협상)을 다시 시작합니다.

참고 : 광 인터페이스의 속도는 고정되어 있습니다.

- GBIC 및 GE-FX의 속도는 1000M입니다.
- FE-FX의 속도는 100M입니다.

  속도 명령 뒤에 auto 매개변수가 있는 경우, 광 인터페이스에서 자동 협상(auto-negotiation) 기능을 활성화할 수 있음을 의미합니다.

그렇지 않으면 광 인터페이스에서 자동 협상 기능을 활성화할 수 없습니다.

15.2.3 인터페이스에서 Flow Control 구성

인터페이스가 전이중 모드일 경우, 흐름 제어는 802.3X에서 정의된 PAUSE 프레임을 통해 구현됩니다. 인터페이스가 반이중 모드일 경우, 흐름 제어는 백 프레셔(back pressure) 방식을 통해 구현됩니다.

명령어	설명
flow-control {on | off | auto}	인터페이스에서 흐름 제어를 활성화하거나 비활성화합니다.
no flow-control	기본 설정으로 복원합니다. 기본 설정에서는 흐름 제어가 비활성화되어 있습니다.

15.2.4 Duplex 모드 설정

기본적으로 이더넷 인터페이스는 자동, 반이중 또는 전이중일 수 있습니다. 기가비트 콤보 SFP/TX 포트는 속도 1000과 강제 이중 모드를 동시에 지원하지 않습니다.

명령어	설명
duplex {full | half | auto}	듀플렉스 모드를 설정합니다.
No duplex	기본 설정을 재개합니다. 듀플렉스 모드는 자동 협상입니다.

15.3 Port Isolation

일반적으로 데이터 패킷은 스위치의 서로 다른 포트 간에 전달될 수 있습니다. 그러나 특정 상황에서는 포트 간의 흐름을 차단해야 할 필요가 있으며, 이를 제어하기 위해 포트 격리 기능이 제공됩니다. 그룹 기반이 아닌 격리의 경우, 격리된 포트 간에는 데이터 통신이 이루어지지 않지만, 격리되지 않은 포트 간 및 격리된 포트와 격리되지 않은 포트 간에는 데이터 패킷이 정상적으로 전달될 수 있습니다.

그룹 기반 격리의 경우, 동일 그룹 내의 격리된 포트 간에는 데이터 통신이 불가능하지만, 그룹 외부의 포트와는 데이터 통신이 가능합니다.

주의할 점은, 포트 격리 기능은 2계층 메시지에서 작동하며 그룹 기반 격리는 지원하지 않는다는 점입니다.

비그룹에 따른 격리

명령어	설명
config	글로벌 구성 모드로 진입
interface g0/1	구성할 인터페이스로 진입
[no] **switchport protected**	포트 격리 기능 활성화/비활성화
exit	글로벌 구성 모드로 돌아가기
exit	관리 구성 모드로 돌아가기

그룹에 따른 격리

명령어	설명
config	글로벌 구성 모드로 진입
[no] **port-protected** *group-id*	격리 그룹 모드를 생성하고 활성화합니다. group-id 는 구성할 격리 그룹 ID 를 의미합니다.
[no] **description** *word*	그룹에 대한 설명입니다. Word 는 그룹의 문자열을 나타냅니다.
exit	글로벌 구성 모드로 돌아갑니다.
interface g0/1	구성할 인터페이스로 진입합니다.
[no] **switchport protected** *group-id*	격리 그룹 추가/제거를 수행합니다. group-id 는 구성된 격리 그룹 ID 를 나타냅니다.
exit	글로벌 구성 모드로 돌아갑니다.
exit	관리 구성 모드로 돌아가기

15.4Storm Control

스위치 포트는 지속적인 비정상 유니캐스트(MAC 주소 위치 확인 실패), 멀티캐스트 또는 브로드캐스트 메시지로 인해 공격받을 수 있습니다. 이는 스위치 포트뿐만 아니라 스위치 전체의 장애를 초래할 수 있습니다. 이러한 현상을 방지하기 위해 제어 메커니즘이 제공됩니다.

스톰 컨트롤 기능은 스위치로 들어오는 다양한 유형의 메시지에 대해 수용 가능한 속도를 인그레스에서 설정할 수 있도록 합니다.

명령어	설명
config	글로벌 구성 모드로 진입
interface g0/1	구성할 인터페이스 입력
[no] **storm-control** {**broadcast** | **multicast** | **unicast**} **threshold** *count*	포트의 스톰 제어 기능 구성. 유니캐스트는 알 수 없는 유니캐스트에 대해 작동한다는 것을 의미합니다. 멀티캐스트는 멀티캐스트에 대해 작동한다는 것을 의미합니다. 브로드캐스트는 브로드캐스트에 대해 작동한다는 것을 의미합니다. 카운트는 구성할 임계값을 의미합니다.
exit	글로벌 구성 모드로 돌아갑니다.
exit	관리 구성 모드로 돌아가기

15.5포트 Rate 제한

포트 속도 제한은 포트로 들어오고 나가는 트래픽의 속도를 제한하는 데 사용됩니다.

관리 모드에 진입한 후 다음 명령어를 사용하여 포트의 흐름 속도를 제한하십시오.

명령어	설명
config	글로벌 구성 모드로 진입
interface g0/1	구성할 인터페이스 입력
[no] **switchport rate-limit** {*band* | **Bandwidth** *percent* } { **ingress** | **egress**}	포트의 스톰 제어 기능 구성. 유니캐스트는 알 수 없는 유니캐스트에 대해 작동한다는 것을 의미합니다. 멀티캐스트는 멀티캐스트에 대해 작동한다는 것을 의미합니다. 브로드캐스트는 브로드캐스트에 대해 작동한다는 것을 의미합니다. 카운트는 구성할 임계값을 의미합니다.
exit	글로벌 구성 모드로 돌아갑니다.
exit	관리 구성 모드로 돌아가기

15.6포트 루프 감지

루프 감지 기능은 포트에 루프가 있는지 감지하는 데 사용됩니다. 포트에서 전송되는 루프 감지 메시지의 시간 간격을 구성할 수 있습니다. 다음 명령을 사용하여 관리 모드로 들어간 후 포트에서 전송되는 루프 감지 메시지의 시간 간격을 설정합니다.

명령어	설명
config	글로벌 구성 모드로 진입
Interface g0/1	구성할 인터페이스 입력
[no] **keepalive [***second* **]**	포트에서 전송된 루프 감지 메시지의 시간 간격 구성. 두 번째는 메시지를 전송하는 시간 간격입니다.
exit	글로벌 구성 모드로 돌아갑니다.
exit	관리 구성 모드로 돌아가기

15.7포트 MAC-address learning

포트 MAC address learning 은 포트 MAC address learning 을 활성화/비활성화하는 데 사용됩니다. 구성 방법은 다음과 같습니다.

명령어	설명
config	글로벌 구성 모드로 진입
interface g0/1	구성할 인터페이스 입력
[no] **switchport disable-learning**	포트 MAC address learning 을 구성합니다. 포트 MAC address learning 기능을 활성화/비활성화합니다.
exit	글로벌 구성 모드로 돌아갑니다.
exit	관리 구성 모드로 돌아가기

15.8포트 보안

포트의 보안은 MAC 주소에 따라 포트에 접근하여 제어합니다. 포트의 보안에는 동적 보안 모드, 정적 수락 모드, 정적 거부 모드의 세 가지 모드가 있습니다. 동적 보안 모드에서는 포트에서 학습할 수 있는 최대 MAC 주소 수량을 구성할 수 있습니다. 스위치에서 일부 포트의 최대 MAC 주소를 학습한 경우 MAC 주소는 learning 되지 않습니다. 그동안 스위치는 모든 DLF 메시지를 삭

제합니다. 정적 보안 모드에서는 포트에서 정적 보안 MAC 주소를 구성할 수 있습니다. 정적 수락 모드에서는 소스 MAC이 안전한 MAC 주소인 메시지만 들어올 수 있고 다른 메시지는 삭제됩니다. 정적 거부 모드에서는 소스 MAC이 안전한 MAC 주소인 메시지는 삭제되고 다른 메시지는 들어올 수 있습니다.

명령어	설명
config	글로벌 구성 모드로 진입
interface g0/1	구성할 인터페이스 입력
[no] **switchport port-security mode** {**dynamic | static** *accept/reject* | **sticky**}	포트의 보안 모드 구성. Dynamic 은 동적 보안 모드를 의미합니다. static accept 는 정적 수락 모드를 의미합니다. static reject 는 정적 거부 모드를 의미합니다.
[no] **switchport port-security dynamic maximum** *num*	최대 learning 가능 MAC 주소 구성
[**no**] **switchport port-security static mac-address** *H.H.H*	정적 보안 주소 구성
[**no**] **switchport port-security sticky** {**maximum** *sticky_number* | **mac-address** *H.H.H* | **aging-time** *aging_time* }	포트 MAC 주소 스티키 구성. maximum sticky_number 는 최대 스티키 MAC 주소 수량을 의미합니다. mac-address H.H.H 는 스티키 MAC 주소를 수동으로 구성하는 것을 의미합니다. aging-time aging_time 은 스티키 MAC 주소의 에이징 시간을 수동으로 구성하는 것을 의미합니다.
exit	글로벌 구성 모드로 돌아갑니다.
exit	관리 구성 모드로 돌아가기

15.9 인터페이스의 binding

이 스위치는 인터페이스에서 IP 주소와 MAC 주소로 동시에 바인딩되거나 IP 주소 또는 MAC 주소로만 바인딩될 수 있습니다. IP 및 ARP 메시지에 작동합니다.

관리 모드로 들어간 후 다음 명령을 사용하여 구성을 수행합니다.

명령어	설명

config	글로벌 구성 모드로 진입
interface g0/1	구성할 인터페이스 입력
[no] **switchport port-security bind|block** {**ip|arp|both-arp-ip** *A.B.C.D* **| mac** *H.H.H* }	인터페이스의 바인딩 기능 구성. Bind 는 바인딩 요구 사항을 준수하는 메시지만 통과시키고 다른 메시지는 통과시키지 않습니다. Block 은 바인딩 요구 사항을 준수하는 메시지만 거부하고 다른 메시지는 통과시킵니다. Ip 는 바인딩 요구 사항을 준수하는 IP 메시지에만 작동함을 의미합니다. Arp 는 바인딩 요구 사항을 준수하는 arp 메시지에만 작동함을 의미합니다. both-arp-ip 는 바인딩 요구 사항을 준수하는 ip 및 arp 메시지에 작동함을 의미합니다.
exit	글로벌 구성 모드로 돌아갑니다.
exit	관리 구성 모드로 돌아가기

15.10 SVL/IVL

스위치는 공유(SVL)/독립(IVL) VLAN 학습 모드로 구성할 수 있습니다. 기본적으로 포트는 모두 IVL 모드입니다.

이 스위치는 인터페이스에서 IP 주소와 MAC 주소로 동시에 바인딩되거나 IP 주소 또는 MAC 주소로만 바인딩될 수 있습니다. IP 및 ARP 메시지에 작동합니다.

관리 모드로 들어간 후 다음 명령을 사용하여 구성을 수행합니다.

명령어	설명
config	글로벌 구성 모드로 진입
[no]**vlan shared-learning**	SVL/IVL 설정
exit	관리 구성 모드로 돌아가기

15.11 링크 스캔 설정

15.11.1 개요

포트의 스캐닝 시간 간격을 구성하면 포트의 작동/중단 상태를 빠르게 스캔할 수 있습니다.

15.11.2 링크 스캔 구성 작업

- 포트 스캐닝 시간 간격 구성.

포트의 스캐닝 시간 간격을 설정할 때 글로벌 구성 모드에서 다음 명령을 사용합니다.

명령어	설명
[no] Link scan {normal *interval* **| fast** *interval***}**	모드는 광 포트의 스캐닝 모드를 선택하는 것을 의미합니다. Normal 은 표준 링크 스캐닝 모드를 의미합니다. Fast 는 빠른 링크 스캐닝 모드를 의미합니다. 빠름 모드는 주로 rstp 와 같은 서비스 프로토콜에 적용됩니다. Interval 포트의 스캐닝 시간 간격을 구성하는 것을 의미합니다.

15.11.3 설정 예시

표준 스캐닝 간격을 20밀리초로 구성

link scan normal 20

15.12 포트 링크 상태 확인 구성

15.12.1 개요

포트의 향상된 링크 상태 검사를 구성하면 포트의 링크 상태를 빠르게 스캔할 수 있습니다.

15.12.2 구성 목록

- 포트의 향상된 링크 상태 검사를 활성화/비활성화합니다.

포트의 향상된 링크 상태 확인하려면 인터페이스 구성 모드에서 다음 명령을 사용합니다.

명령어	설명
[no] switchport enhanced-link	포트의 향상된 링크 상태 확인을 활성화/비활성화 합니다.

15.10.4 설정 예제

인터페이스 g0/1의 향상된 링크 상태 검사를 활성화합니다.

Switch_config#interface g0/1

Switch_config_g0/1#switchport enhanced-link

15.13 시스템 MTU 구성

15.13.1 개요

시스템 MTU 구성

15.13.2 구성 목록

- 시스템 MTU 구성

글로벌 구성 모드에서 다음 명령을 사용하세요.

명령어	설명
[no] system mtu *mtu*	시스템 MTU 값 구성

15.13.3 설정 예시

시스템 MTU 2000바이트 구성

Switch_config#system mtu 2000

15.14 Port Isolation

- 포트 미러링 구성
- 포트 미러링 정보 표시

15.14.1 포트 미러링 구성

포트 미러링을 구성하면 스위치의 한 포트를 사용하여 포트 그룹의 트래픽을 관찰할 수 있습니다.

명령어	설명
config	글로벌 구성 모드로 진입

mirror session *session_number* {**destination** {**interface** *interface-id*} { **rspan** *vid tpid*} | **source** {**interface** *interface-id* [, | -] rx | tx | both] }	포트 미러링을 구성합니다. session-number는 포트 미러링의 번호입니다. destination은 미러링의 대상 포트입니다. 원격 미러링 태그의 Vid입니다. 원격 미러링 태그의 tpid입니다. source는 미러링의 소스 포트입니다. rx는 미러링의 입력 데이터를 의미합니다. Tx는 미러링의 출력 데이터를 의미합니다. both는 미러링의 입력 및 출력 데이터를 의미합니다.
exit	글로벌 구성 모드로 돌아가기
write	설정을 저장합니다.

15.14.2 포트미러링 정보 표시

포트 미러링의 구성 정보를 표시하려면 show 명령어를 실행합니다.

명령어	설명
show mirror [**session** *session_number]*	포트 미러링에 대한 구성 정보를 표시합니다.

15.14.3 프토 미러링 예제

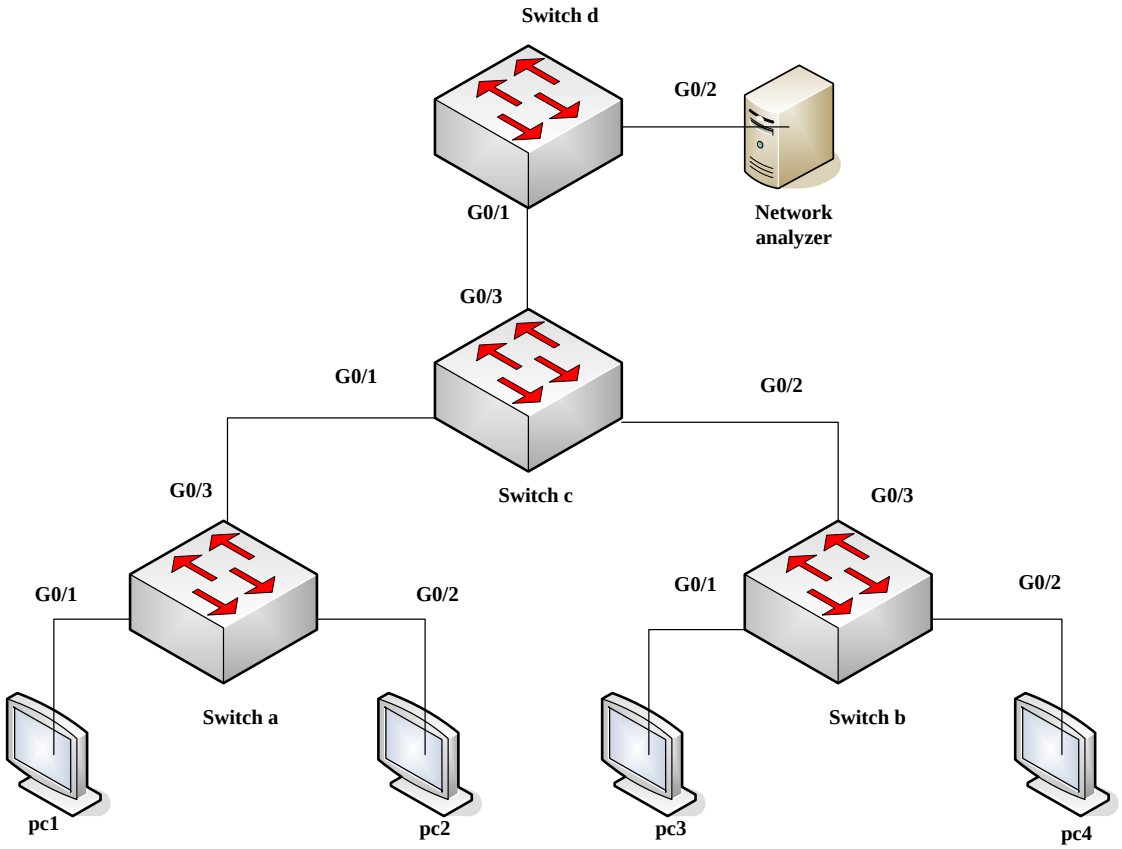


그림 8 네트워크 토폴로지

Switch A

mirror session 1 destination interface g0/3 rspan 100 0x8100

mirror session 1 source interface g0/1 both

Switch B

mirror session 1 destination interface g0/3 rspan 1000 0x8100

mirror session 1 source interface g0/1 both

Switch C

interface GigaEthernet0/1

 switchport mode trunk

!

interface GigaEthernet0/2

 switchport mode trunk

```
!
interface GigaEthernet0/3
 switchport mode trunk
!
vlan 1,100,1000
Switch D
mirror session 1 destination interface g0/2
mirror session 1 source interface g0/1 both
```

16 MAC 주소

16.1MAC 주소 구성 작업 목록

- 정적 MAC 주소 구성
- MAC 주소 Aging 시간 구성
- Blackhole MAC 주소 구성
- MAC 주소 테이블 표시
- 동적 MAC 주소 삭제

16.2MAC 주소 구성 작업

16.2.1 정적 MAC 주소 구성

정적 MAC 주소 항목은 스위치에 의해 Aging 되지 않는 MAC 주소 항목이며 수동으로만 삭제할 수 있습니다. 작업 프로세스 중 실제 요구 사항에 따라 정적 MAC 주소를 추가하고 삭제할 수 있습니다. 다음 명령을 사용하여 정적 MAC 주소를 추가하고 삭제합니다.

명령어	설명
configure	글로벌 구성 모드로 진입
[no] mac address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*	정적 MAC 주소 항목을 추가/삭제합니다. Mac-addr는 MAC 주소를 나타냅니다. Vlan-id는 VLAN 번호를 나타냅니다. 유효한 값은 1~4094입니다. Interface-id는 인터페이스 이름을 나타냅니다.
exit	EXEC 모드로 돌아가기
write	설정을 저장합니다.

16.2.2 MAC 주소 Aging 시간 구성

지정된 에이징 시간 동안 동적 MAC 주소가 사용되지 않으면 스위치는 MAC 주소 테이블에서 이 MAC 주소를 삭제합니다. 스위치 MAC 주소의 에이징 시간은 필요에 따라 구성할 수 있습니다. 기본 에이징 시간은 300초입니다.

다음과 같이 특권 모드에서 MAC 주소의 에이징 시간을 구성합니다.

명령어	설명
configure	포트 미러링에 대한 구성 정보를 표시합니다.
mac address-table aging-time [**0 | 10-1000000**]	MAC 주소의 에이징 시간을 구성합니다. 0 은 MAC 주소의 에이징이 없음을 나타냅니다. 유효한 값은 10~1000000 초입니다.
exit	관리구성 모드로 돌아가기
write	설정을 저장합니다.

16.2.3 Blackhole MAC 주소 구성

Blackhole MAC 주소 테이블 항목은 통신이 허용되지 않고 수동으로만 삭제할 수 있는 항목을 말합니다. 블랙홀 MAC 주소는 스위치 사용의 실제 필요에 따라 추가 및 제거할 수 있습니다. 다음 명령을 구성하여 Blackhole MAC 주소를 추가 및 제거합니다.

명령어	설명
config	포트 미러링에 대한 구성 정보를 표시합니다.
[no] mac address-table blackhole*mac-addr* **vlan** *vlan-id*	Blackhole MAC 주소 항목을 추가/삭제합니다. mac-addr 는 MAC 주소를 나타냅니다. Vlan-id 는 VLAN 번호를 나타냅니다. 유효한 값은 1~4094 입니다.
exit	관리구성 모드로 돌아가기
write	설정을 저장합니다.

16.2.4 MAC 주소 테이블 표시

운영 프로세스에서 디버깅과 관리가 필요하므로 스위치 MAC 주소 테이블의 내용을 알고 싶은 경우 show 명령을 사용하여 스위치 MAC 주소 테이블의 내용을 표시합니다.

명령어	설명
show mac address-table [dynamic [interface *interface-id* | **vlan** *vlan-id***]** | **static | brief | multicast | interface** *interface-id* **| vlan** *vlan-id* **| H.H.H | blackhole]**	Dynamic 은 동적으로 획득하는 MAC 주소를 나타냅니다. Interface-id 는 인터페이스 이름을 나타냅니다. Vlan-id 는 VLAN 번호를 나타냅니다. 유효한 값은 1~4094 입니다.

	Static 은 정적 MAC 주소 테이블을 나타냅니다. Brief 는 MAC 주소의 간략한 정보를 나타냅니다. Multicast 는 멀티캐스트 MAC 주소 테이블을 나타냅니다. Interface 는 인터페이스 MAC 주소 테이블을 나타냅니다. Vlan 은 VLAN 의 MAC 주소 테이블을 나타냅니다. H.H.H 는 특정 주소를 나타냅니다. Blackhole 은 BLACKHOLE MAC 주소 테이블을 나타냅니다.

16.2.5 동적 MAC 주소 삭제

MAC 주소는 어떤 상황에서는 지워야 합니다. 다음 명령을 사용하여 권한 모드에서 동적 MAC 주소를 삭제합니다.

명령어	설명
clear mac address-table dynamic [address *mac-addr* | **interface** *interface-id* **| vlan** *vlan-id*]	동적 MAC 주소 항목을 삭제합니다. Dynamic 은 동적으로 획득하는 MAC 주소를 나타냅니다. Mac-addr 은 MAC 주소입니다. Interface-id 는 인터페이스 이름을 나타냅니다. Vlan-id 는 VLAN 번호를 나타냅니다. 유효한 값은 1~4094 입니다.

16.3 MAC 액세스 리스트 구성

MAC 액세스 리스트 구성은 다음 항목들을 포함합니다

- MAC 액세스 리스트 생성
- MAC 액세스 리스트 항목 구성
- MAC 액세스 리스트 적용

16.4 MAC 액세스 리스트 생성

MAC 액세스 리스트는 포트에 적용하기 전에 먼저 생성되어야 합니다. MAC 액세스 리스트가 생

성되면 MAC 액세스 리스트 구성 모드로 진입하며, 이 모드에서 MAC 액세스 리스트 항목을 구성할 수 있습니다.

권한 모드(privilege mode)로 진입한 후, 아래 단계에 따라 MAC 액세스 리스트를 추가하거나 삭제할 수 있습니다.

명령어	설명
config	글로벌 구성 모드로 진입
[**no**] **mac access-list** *name*	MAC 액세스 리스트를 추가하거나 삭제하려면 이 명령어를 실행합니다. name은 MAC 액세스 리스트의 이름을 나타냅니다.

16.5 MAC 액세스 리스트 항목 구성

MAC 액세스 리스트 구성 모드에서 특정 소스 MAC 주소나 모든 소스 MAC 주소, 특정 목적지 MAC 주소나 모든 목적지 MAC 주소를 허용하거나 거부하도록 지정할 수 있습니다. 동일한 항목은 한 MAC 액세스 리스트에서 한 번만 구성할 수 있습니다.

MAC 액세스 리스트 구성 모드로 진입한 후 아래 단계에 따라 MAC 액세스 리스트 항목을 설정합니다.

명령어	설명
[**no**] {**permit	deny**} {**any**	**host** *src-mac-addr	src-mac-addr src-mac-mask* } {**any**	**host** *dst-mac-addr	dst-mac-addr dst-mac-mask*}[**arp** [{*any	src-ip-addr*} {*any	dst-ip-addr* }]	*ethertype |cos value*]	any: 모든 MAC 주소와 일치합니다. src-mac-addr: 소스 MAC 주소를 나타냅니다. src-mac-mask: 소스 MAC 마스크를 나타냅니다. dst-mac-addr: 목적지 MAC 주소를 나타냅니다. dst-mac-mask: 목적지 MAC 마스크를 나타냅니다. arp: ARP 패킷과 일치합니다. src-ip-addr: 소스 IP 주소를 나타냅니다. dst-ip-addr: 목적지 IP 주소를 나타냅니다. ethertype: 일치하는 이더넷 패킷의 유형을 나타냅니다. cos value: 패킷 헤더에 표시된 우선순위 값(Class of Service)을 나타냅니다.

exit	글로벌 구성모드로 돌아갑니다.
exit	EXEC 모드로 돌아갑니다.
write	설정을 저장합니다.

- MAC 리스트 구성 예제

Switch_config#mac access-list 1

Switch-config-macl#permit host 1.1.1 any

Switch-config-macl#permit host 2.2.2 any

위의 구성은 소스 MAC 주소를 비교하는 것으로, 마스크(mask)가 동일합니다. 구성은 성공적으로 완료되었습니다.

16.6 MAC 액세스 리스트 적용

생성된 MAC 리스트는 임의의 물리적 포트에 적용할 수 있습니다. 한 포트에는 하나의 MAC 리스트만 적용할 수 있지만, 동일한 MAC 리스트를 여러 포트에 적용하는 것은 가능합니다.

권한 모드(privilege mode)로 진입한 후 아래 단계를 따라 MAC 리스트를 구성합니다.

명령어	설명
config	글로벌 구성 모드로 들어갑니다.
interface g0/1	구성될 포트로 들어갑니다.
[**no**] **mac access-group** *name*	생성된 MAC 목록을 포트에 적용하거나 적용된 MAC 목록을 포트에서 삭제합니다. NameMAC: MAC 액세스 목록의 이름
exit	글로벌 구성 모드로 돌아갑니다.
exit	EXEC 모드로 돌아갑니다.
write	설정을 저장합니다.

17.VLAN 구성

17.1 VLAN 소개

VLAN(Virtual Local Area Network)은 하나 이상의 LAN에 걸쳐 있는 논리적으로 네트워크화된 장치 그룹으로, 물리적으로 다른 LAN 세그먼트에 있더라도 동일한 네트워크에 연결된 것처럼 통신하도록 구성됩니다. 1999년에 IEEE는 VLAN 구현 프로젝트를 표준화하기 위해 IEEE 802.1Q 프로토콜 표준 초안을 제정하였습니다. VLAN은 물리적 연결 대신 논리적 기반이기 때문에 사용자 관리, 대역폭 할당 및 리소스 최적화에 매우 유연합니다.

VLAN의 주요 유형:

- 포트 기반 VLAN: 각 물리적 스위치 포트는 VLAN 세트의 멤버십을 지정하는 액세스 리스트로 구성됩니다.
- 802.1Q 트렁크 모드: 인터페이스에서 지원됩니다.
- 액세스 모드: 단일 VLAN에 속하며 태그 없는 이더넷 프레임을 송수신합니다.

포트 기반 VLAN에서는 VLAN 하위 세트에 포트를 할당합니다. VLAN 하위 세트에 하나의 VLAN만 포함되면 포트는 액세스 포트로, 여러 VLAN이 포함되면 트렁크 포트로 동작합니다. 기본 VLAN은 PVID(Port VLAN ID)로 설정됩니다.

17.2 Dot1Q 터널 개요

17.2.1 서론

Dot1Q 터널은 IEEE 802.1ad에서 정의된 802.1Q 캡슐화 기반 터널 프로토콜입니다. 개인 네트워크의 VLAN 태그를 공용 네트워크의 VLAN 태그로 캡슐화하여 ISP 백본 네트워크를 통과할 수 있도록 합니다. 이를 통해 2계층 VPN 터널이 간단하고 관리하기 쉽게 제공됩니다. 이 프로토콜은 정적 구성으로 구현되며, 주요 애플리케이션은 기업 네트워크 및 소규모 MAN(Metropolitan Area Network) 네트워크입니다.

Dot1Q 터널의 주요 기능:

- Dot1Q 터널 전체 활성화 지원
- 고객 VLAN(CVLAN)과 서비스 제공 VLAN(SPVLAN) 간의 변환 지원
- 업링크 포트 구성 지원

17.2.2 Dot1Q 터널 구현 모드

Dot1Q 터널은 다음 두 가지 모드로 구현할 수 있습니다

포트 기반 Dot1Q 터널과 내부 CVLAN 태그 분류 기반 Dot1Q 터널입니다.

① 포트 기반 Dot1Q

이 장치의 포트가 패킷을 수신하면, 해당 패킷에 VLAN 태그가 포함되어 있는지와 관계 없이 스위치는 이 포트의 기본 VLAN 태그를 패킷에 추가합니다. 수신된 패킷에 이미 VLAN 태그가 있는 경우, 해당 패킷은 이중 태그(Double-Tagged) 패킷이 됩니다. 수신된 패킷이 태그가 없는(Untagged) 상태라면, 기본 VLAN 태그가 추가됩니다.

따라서, VLAN 태그가 포함된 패킷은 이중 태그가 되고, 태그가 없는 패킷에는 기본 VLAN 태그가 추가됩니다. 즉, 수신된 패킷이 VLAN 태그를 포함하면 이중 태그가 되고, 포함하지 않으면 기본 VLAN 태그가 추가됩니다.

단일 VLAN 태그를 가진 패킷의 구조는 다음과 같습니다

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

이중 VLAN 태그를 가진 패킷의 구조는 다음과 같습니다

DA (6B)	SA (6B)	**ETYPE(8100) (2B)**	**SPVLAN Tag (2B)**	ETYPE (8100) (2B)	CVLAN Tag (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

② 내부 CVLAN 태그 기반 Dot1Q 터널

Dot1Q 터널의 내부 CVLAN 태그(CVLAN ID 영역)를 기준으로 서비스를 분배합니다. CVLAN 영역은 SPVLAN ID로 변환될 수 있으며, 변환 방식에는 Flat VLAN 변환과 QinQ VLAN 변환 두 가지가 있습니다. QinQ VLAN 변환 모드에서는 동일한 사용자가 서로 다른 CVLAN ID를 사용해 다양한 서비스를 이용할 때, 각 CVLAN ID에 따라 서비스를 분배합니다. 예를 들어 대역폭 서비스의 CVLAN ID 범위는 101~~200, VoIP 서비스는 201~~300, IPTV 서비스는 301~400으로 설정할 수 있습니다. PE 장치가 사용자 데이터를 수신하면 CVLAN ID 범위에 따라 SPVLAN 태그를 추가합니다. 예를 들어, 대역폭 서비스에는 SPVLAN ID 1000을, IPTV 서비스에는 SPVLAN ID 3000을 추가합니다. Flat VLAN 변환 모드와 QinQ VLAN 변환 모드의 차이점은 Flat VLAN 변환 모드에서는 SPVLAN 태그가 CVLAN 태그의 외부 계층에 추가되지 않고 CVLAN 태그를 직접 교체한다는 점입니다. 반면, QinQ VLAN 변환 모드에서는 SPVLAN 태그가 CVLAN 태그 외부에 추가됩니다.

17.3 VLAN 구성 작업 목록

- VLAN 추가/삭제
- 스위치 포트 구성
- VLAN 인터페이스 생성/삭제
- VLAN 구성 및 상태 모니터링
- Dot1Q 터널 활성화/비활성화

17.4 VLAN 구성 작업

17.4.1 VLAN 추가/삭제

VLAN은 동일한 요구 사항을 가진 호스트 그룹으로, 논리적 네트워크를 형성합니다. VLAN 간 데이터 통신은 라우터 또는 브리지를 통해 이루어져야 합니다. 다음 명령어를 사용하여 VLAN을 구성할 수 있습니다

명령어	설명
vlan vlan-id	VLAN 구성 모드로 진입합니다.
name str	VLAN 이름을 설정합니다.
Exit	VLAN 구성 모드를 종료하고 VLAN을 생성합니다.
vlan vlan-range	여러 VLAN을 동시에 생성합니다.
no vlan vlan-id | vlan-range	하나 또는 둘이상의 VLAN을 삭제합니다.

VLAN은 VLAN 관리 프로토콜 GVRP를 통해 동적 추가 및 삭제를 수행할 수 있습니다.

17.4.2 스위치 포트 구성

스위치의 포트는 다음과 같은 모드를 지원합니다.

액세스 모드, 릴레이 모드, VLAN 터널 모드, VLAN 변환 터널 모드, VLAN 터널 업링크 모드

- 액세스 모드: 포트가 하나의 VLAN에만 속하며, 태그가 없는 이더넷 프레임만 송수신합니다.
- 릴레이 모드: 포트가 다른 스위치와 연결되며, 태그가 포함된 이더넷 프레임을 송수신할 수 있습니다.

- VLAN 변환 터널 모드: 릴레이 모드를 기반으로 하는 하위 모드로, 수신한 패킷의 VLAN 태그를 기준으로 VLAN 변환 테이블을 조회하여 해당 SPVLAN을 얻습니다. 이후 스위칭 칩은 원래 태그를 SPVLAN으로 교체하거나, 원래 태그의 외부 계층에 SPVLAN 태그를 추가합니다. 패킷이 포트를 통해 전달될 때 SPVLAN 태그는 원래 태그로 교체되거나 강제로 제거됩니다. 이를 통해 스위치는 네트워크에 액세스하는 다양한 VLAN 분할을 생략하고, 같은 클라이언트의 다른 서브넷에 연결된 포트로 변경 없이 투명하게 전달합니다.
- VLAN 터널 업링크 모드: 릴레이 모드를 기반으로 하는 하위 모드로, 패킷이 포트를 통해 전달될 때 SPVLAN이 설정되어야 합니다. 패킷이 태그가 없는(untagged) 범위에 포함되면, 모든 패킷은 변경 없이 전달됩니다. 포트에서 패킷을 수신할 경우, TPID를 확인하며, 차이가 있거나 태그가 없는 패킷인 경우 SPVLAN 태그가 외부 계층 태그로 추가됩니다.

각 포트는 기본 VLAN과 PVID(Port VLAN ID)를 가지며, 포트에서 VLAN 태그가 없는 데이터는 해당 VLAN의 데이터 패킷으로 간주됩니다.

트렁크 모드는 포트를 여러 VLAN에 속하도록 설정할 수 있으며, 포트를 통해 전달되는 패킷의 유형(태그 포함 여부)과 포트가 속한 VLAN 목록을 구성할 수 있습니다.

스위치 포트를 구성하려면 다음 명령어를 실행합니다.

명령어	설명
switchport pvid *vlan-id*	스위치 포트의 pvid 를 구성합니다.
switchport mode {access | trunk | dot1q-translating-tunnel | dot1q-tunnel-uplink }	스위치의 포트 모드를 구성합니다.
switchport trunk vlan-allowed ...	스위치 포트의 vlan-allowed 범위를 구성합니다.
switchport trunk vlan-untagged ...	스위치 포트의 vlan-allowed 범위를 구성합니다.

이 기능이 활성화되면, 동적 VLAN은 해당 동적 VLAN이 등록된 포트에서만 유효합니다. 이 명령어가 활성화된 후, 특정 포트가 동적 VLAN을 등록하지 않은 경우 해당 포트는 트렁크 포트이더라도 동적 VLAN의 구성원이 되지 않습니다.

17.4.3 VLAN 인터페이스 생성/삭제

VLAN 인터페이스는 네트워크 관리 기능이나 3계층 라우팅 기능을 구현하기 위해 생성할 수 있습니다. VLAN 인터페이스를 사용하여 IP 주소와 서브넷 마스크를 지정할 수 있습니다.

다음 명령어를 실행하여 VLAN 인터페이스를 구성합니다.

명령어	설명
[no] interface vlan *vlan-id*	VLAN 인터페이스를 생성하거나 삭제합니다.

17.4.4 VLAN 구성 및 상태 모니터링

EXEC 모드에서 다음 명령어를 실행하여 VLAN 구성 및 상태를 확인할 수 있습니다.

명령어	설명
show vlan [id *x* **| interface** *intf* **| dot1q-tunnel [interface** *intf***]|mac-vlan | subnet |protocol-vlan |dot1q-translating-tunnel**	VLAN 또는 Dot1Q 터널의 구성 및 상태를 확인 합니다.
show interface vlan x	VLAN 포트 또는 SuperVLAN 포트의 상태를 표시 합니다.

17.4.5 글로벌 Dot1Q 터널 활성화/비활성화

Dot1Q 터널을 글로벌로 활성화한 후, 포트는 기본적으로 Dot1Q 터널의 다운링크 포트로 설정되며, 수신된 패킷에 SPVLAN 태그가 추가됩니다.

Dot1Q 터널을 활성화하는 명령어는 다음과 같습니다.

명령어	설명
dot1q-tunnel	스위치에서 글로벌 Dot1Q 터널을 구성합니다.

17.5 Dot1Q 터널 구성 예제

17.5.1 Dot1Q 터널 구성 예제

다음은 Dot1Q 터널을 적용하는 일반적인 솔루션을 보여줍니다.

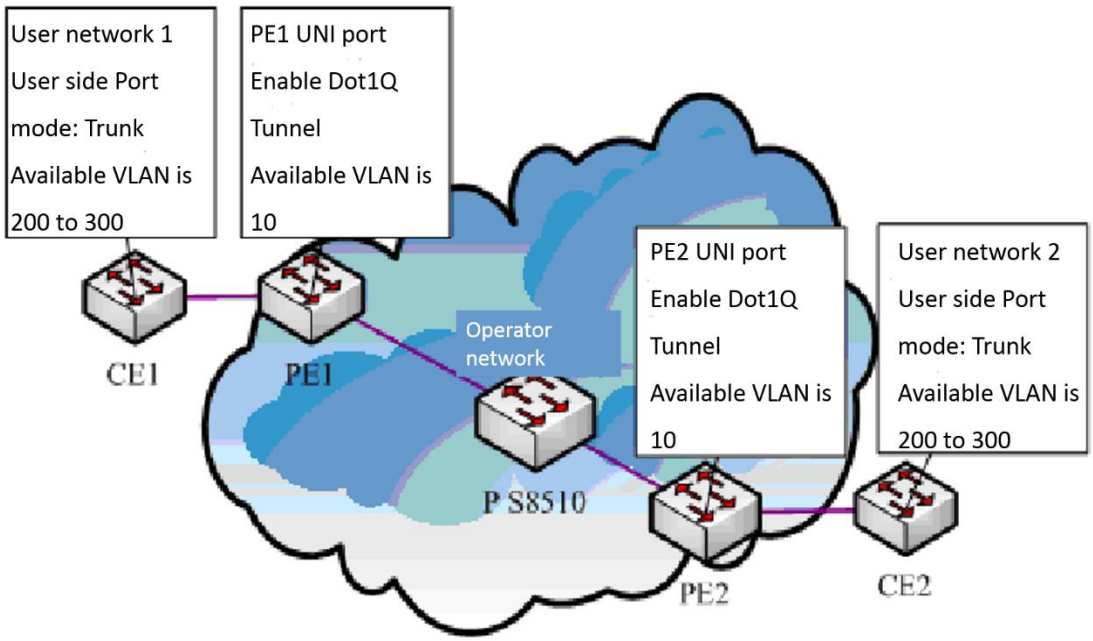


그림 9 Dot1q 터널 설정

위 그림에서 CE1의 F0/1 포트는 PE1의 F0/1 포트(또는 G0/1 포트)에 연결되고, PE1은 S8510의 F0/2 포트(또는 G0/2 포트)에 연결됩니다. PE2는 S8510의 F0/2 포트(또는 G0/2 포트)에 연결되며, PE2의 F0/1 포트(또는 G0/1 포트)는 CE1의 F0/1 포트에 연결됩니다.

PE 장치의 포트는 VLAN 10의 액세스 포트로 설정되며, Dot1Q 터널이 활성화됩니다. 반면 CE 장치의 포트는 VLAN 200~300 범위의 트렁크 VLAN을 필요로 하여 CE와 PE 간 링크가 비대칭 링크로 구성됩니다.

이 경우, 공용 네트워크는 사용자에게 VLAN ID 10 하나만 할당하면 됩니다. 사용자 네트워크에서 계획된 사설 네트워크 VLAN ID의 개수와 관계없이, 공용 네트워크에서 새로 할당된 VLAN ID(10)는 태그가 포함된 패킷이 ISP 백본 네트워크에 진입할 때 강제로 삽입됩니다.

이 패킷들은 공용 네트워크의 VLAN ID를 통해 백본 네트워크를 통과하며, 백본 네트워크의 반대편에 있는 PE 장치에 도달합니다. PE 장치는 공용 네트워크의 VLAN 태그를 제거하고 사용자 패킷을 복원하여 최종적으로 CE 장치로 전달합니다.

결과적으로, 백본 네트워크를 통해 전달되는 패킷은 두 개의 802.1Q 태그 헤더를 가지게 됩니다. 하나는 공용 네트워크 태그이고, 다른 하나는 사설 네트워크 태그입니다.

패킷 전달의 세부 흐름은 다음과 같습니다

① CE1의 이그레스 포트가 트렁크 포트이기 때문에, 사용자가 PE1으로 전송하는 모든 패킷에는 사설 네트워크의 VLAN 태그(200~300 범위)가 포함됩니다. 이러한 패킷 중 하나의 구조는 아래의 표를 참고해 주십시오.

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

② 패킷이 PE1에 들어오면, PE1은 Dot1Q 터널의 인그레스 포트가 액세스 포트로 설정되어 있으므로 사설 네트워크의 VLAN 태그를 무시하고, 기본 VLAN 10 태그를 해당 패킷에 삽입합니다. 이러한 패킷의 구조는 아래의 표를 참고해 주십시오.

DA (6B)	SA (6B)	ETYPE(8100) (2B)	SPVLAN Tag (2B)	ETYPE (8100) (2B)	CVLAN Tag (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

③ 백본 네트워크에서는 패킷이 트렁크 VLAN 10을 따라 포트를 통해 전달됩니다. 사설 네트워크의 태그는 투명 상태로 유지되며, 이러한 패킷은 PE2에 도달할 때까지 그대로 유지됩니다.

④ PE2는 CE2와 연결된 포트가 VLAN 10의 액세스 포트임을 인식하고, 802.1Q 규격에 따라 VLAN 10 태그 헤더를 제거합니다. 그런 다음, 사용자 초기 패킷을 복원하여 CE2로 전송합니다. 이러한 패킷의 구조는 아래의 표를 참고해주십시오.

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

흐름을 보면, Dot1Q 터널은 신호 처리 없이 정적 구성을 통해 터널을 유지할 수 있으므로 매우 간결합니다.

- 설정 예시

Switch_config#dot1q-tunnel

Switch_config_g0/1#switchport pvid 10

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#switchport trunk vlan-untagged 1-9,11-4094

17.6 Private VLAN 소개

Private VLAN 은 ISP 가 직면한 VLAN 응용 문제를 해결합니다. ISP 가 각 사용자에게 VLAN 을 제공할 경우, 장치가 지원할 수 있는 최대 4094 개의 VLAN 이 ISP 가 지원할 수 있는 사용자 수를 제한하게 됩니다.

17.7 Private VLAN의 유형 및 포트 유형

17.7.1 기본 VLAN 유형

- 기본 VLAN(primary VLAN): 이는 비차단 포트(promiscuous port)와 연관되며, Private VLAN에는 단 하나의 기본 VLAN만 존재합니다. 기본 VLAN 내 모든 포트는 기본 VLAN의 멤버로 간주됩니다.

17.7.2 보조 VLAN 유형

- isolate VLAN(isolated VLAN): 동일한 격리 VLAN에 있는 두 포트 간에는 2계층 통신이 불가능합니다. Private VLAN 내에는 단 하나의 격리 VLAN만 존재할 수 있으며, isolate VLAN은 기본 VLAN과 연관되어야 합니다.
- community VLAN(community VLAN): 동일한 커뮤니티 VLAN 내의 두 포트 간에는 2계층 통신이 가능합니다. 그러나 다른 커뮤니티 VLAN에 있는 포트와는 통신할 수 없습니다. 하나의 Private VLAN은 여러 개의 커뮤니티 VLAN을 포함할 수 있으며, 커뮤니티 VLAN은 기본 VLAN과 연관되어야 합니다.

17.7.3 Private VLAN 포트에서의 포트 유형

- Promiscuous 포트: 기본 VLAN에 속하며, 동일한 Private VLAN 내의 보조 VLAN에 있는 격리 포트 및 커뮤니티 포트를 포함한 모든 포트와 통신할 수 있습니다.
- Isolated 포트: Isolated VLAN의 호스트 포트입니다. 동일한 Private VLAN 내에서, Isolated 포트는 다른 포트(비차단 포트를 제외하고)와 2계층에서 완전히 Isolated 됩니다. 따라서 격리 포트에서 수신된 트래픽은 비차단 포트로만 전달됩니다.
- 커뮤니티 포트: 커뮤니티 VLAN의 호스트 포트입니다. Private VLAN 내에서 동일한 커뮤니티 VLAN에 속한 커뮤니티 포트 간에는 2계층 통신이 가능하며, 비차단 포트와도 통신할 수 있습니다. 그러나 다른 VLAN의 커뮤니티 포트 및 격리 VLAN의 격리 포트와는 통신할 수 없습니다.

17.7.4 VLAN 태그의 필드 수정

이 기능을 통해 VLAN 태그의 VLAN ID 및 우선순위를 수정할 수 있으며, Private VLAN의 이그레스(egress) 패킷이 태그를 포함할지 여부를 결정할 수 있습니다.

17.8 Private VLAN 구성 작업 목록

- Private VLAN 구성

- Private VLAN 도메인의 연관성 구성
- Private VLAN의 2계층 포트를 호스트 포트로 구성
- Private VLAN의 2계층 포트를 비차단(promiscuous) 포트로 구성
- Private VLAN에서 이그레스 패킷의 관련 필드 수정
- Private VLAN 구성 정보 표시

17.9 Private VLAN 구성 작업

Private VLAN 피어(peer)가 동작하기 위한 조건은 다음과 같습니다:

- 기본 VLAN이 있어야 합니다.
- 보조 VLAN이 있어야 합니다.
- 기본 VLAN과 보조 VLAN 간의 연관성이 설정되어야 합니다.
- 기본 VLAN에 비차단(promiscuous) 포트가 있어야 합니다.

17.9.1 Private VLAN 설정

VLAN을 Private VLAN으로 설정하려면 다음 명령어를 사용합니다.

명령어	설명
vlan *vlan-id*	VLAN 모드로 들어갑니다.
private-vlan {primary|community|isolated}	private-VLAN 의 기능을 구성합니다.
no private-vlan {primary|community|isolated}	private-VLAN 의 기능을 삭제합니다.
show vlan private-vlan	private-VLAN 의 구성을 표시합니다.
exit	VLAN 구성 모드를 종료합니다.

17.9.2 Private VLAN 도메인 간 연관성 구성

기본 VLAN(primary VLAN)과 보조 VLAN(secondary VLAN)을 연관시키려면 다음 명령어를 실행합니다

명령어	설명
vlan *vlan-id*	기본 VLAN 구성 모드로 들어갑니다.

private-vlan association {*svlist* | **add** *svlist* | **remove** *svlist*}	연관될 보조 VLAN 을 설정합니다.
no private-vlan association	현재 기본 VLAN 과 모든 보조 VLAN 간의 모든 연관을 지웁니다.
exit	VLAN 구성 모드를 종료합니다.

17.9.3 Private VLAN의 2계층 포트를 호스트 포트로 설정

Private VLAN 의 2 계층 포트를 호스트 포트로 설정하려면 다음 명령어를 실행합니다.

명령어	설명
Interface *interface*	인터페이스 구성 모드로 진입합니다.
switchport mode private-vlan host	2 계층 포트를 호스트 포트 모드로 설정합니다.
no switchport mode	2 계층 포트의 Private VLAN 모드 구성을 삭제합니다.
switchport private-vlan host-association *p_vid s_vid*	2 계층 호스트 포트를 Private VLAN 과 연관시킵니다.
no switchport private-vlan host-association	2 계층 호스트 포트와 Private VLAN 간의 연관성을 제거합니다.
exit	인터페이스 구성 모드를 종료합니다.

17.9.4 Private VLAN의 2계층 포트를 비차단 포트로 설정

Private VLAN의 2계층 포트를 비차단(promiscuous) 포트로 설정하려면 다음 명령어를 실행합니다

명령어	설명
Interface *interface*	인터페이스 구성 모드로 진입합니다.
switchport mode private-vlan host	2 계층 포트를 비차단 포트 모드로 설정합니다.
no switchport mode	2 계층 포트의 Private VLAN 모드 구성을 삭제합니다.
switchport private-vlan host-association *p_vid s_vid*	2 계층 비차단 포트를 Private VLAN 과 연관시킵니다.
no switchport private-vlan host-association	2 계층 비차단 포트와 Private VLAN 간의 연관성을 제거합니다.
exit	인터페이스 구성 모드를 종료합니다.

17.9.5 Private VLAN에서 이그레스 패킷의 관련 필드 수정

Private VLAN에서 이그레스(egress) 패킷의 관련 필드를 수정하려면 다음 명령어를 실행합니다.

명령어	설명
Interface *interface*	인터페이스 구성 모드로 진입합니다.
switchport private-vlan tag-pvid *vlan-id*	이그레스 패킷의 태그에서 VLAN ID 필드를 설정합니다.
switchport private-vlan tag-pri *pri*	이그레스 패킷의 태그에서 우선순위(priority) 필드를 설정합니다.
[no] switchport private-vlan untagged	이그레스 패킷에 태그 포함 여부를 설정합니다.
exit	인터페이스 구성 모드를 종료합니다.

17.9.6 Private VLAN의 구성 정보 표시

글로벌, 인터페이스, 또는 VLAN 구성 모드에서 다음 명령어를 실행하여 Private VLAN과 2계층 포트의 구성 정보를 확인할 수 있습니다.

명령어	설명
show vlan private-vlan	Private VLAN 의 구성을 표시합니다.
show vlan private-vlan interface *interface*	Private VLAN 내 2 계층 포트의 구성을 표시합니다.

17.10 설정 예제

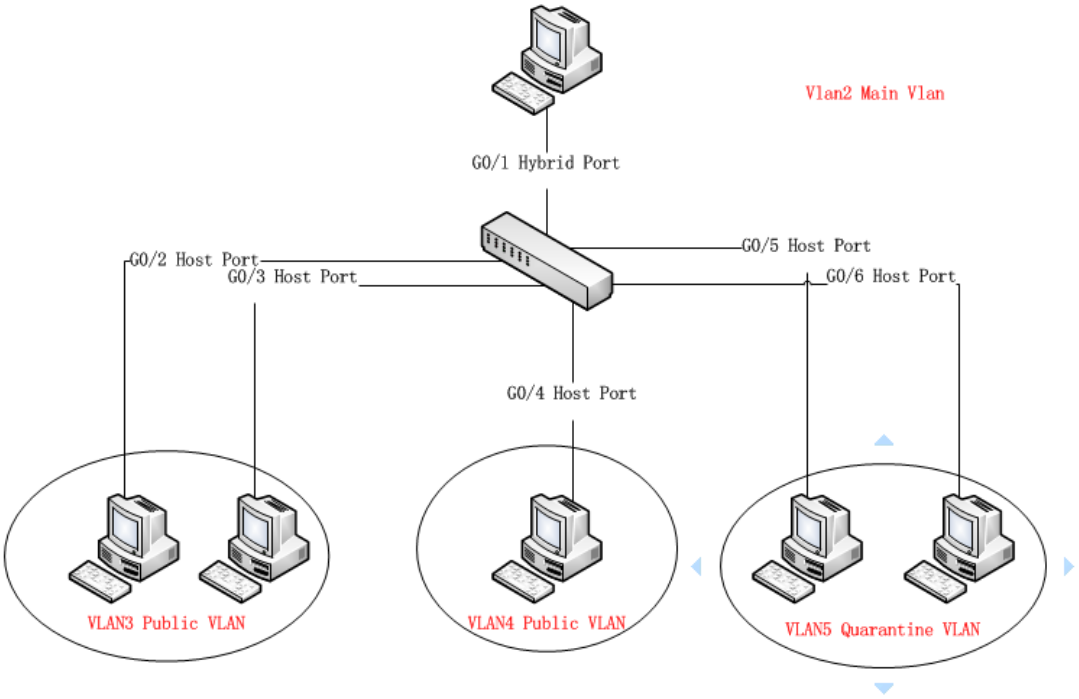


그림 10 Private VLAN 설정

Private VLAN의 정의에 따르면, 비차단 포트 G0/1과 모든 서브-VLAN 도메인의 호스트 포트 간에는 2계층(L2) 통신이 가능합니다. 따라서 커뮤니티 VLAN 3의 호스트 포트 G0/2와 G0/3 간에도 L2 통신이 가능합니다. 그러나 이들은 다른 보조 VLAN의 호스트 포트와는 L2 통신을 할 수 없습니다.

한편, 격리 VLAN 5의 포트 G0/5와 G0/6 간에는 L2 통신이 불가능하지만, 두 포트는 비차단 포트 G0/1과는 L2 통신이 가능합니다.

스위치에서 입력해야 할 명령어는 아래를 참고하여 주시기 바랍니다.

Switch_config#interface GigaEthernet0/1

Switch_config_g0/1#switchport mode private-vlan promiscuous

Switch_config_g0/1#switchport private-vlan mapping 2 3-5

Switch_config_g0/1#switchport pvid 2

Switch_config#interface GigaEthernet0/2

Switch_config_g0/2#switchport mode private-vlan host

Switch_config_g0/2#switchport private-vlan host-association 2 3

Switch_config_g0/2#switchport pvid 3

Switch_config#interface GigaEthernet0/3

Switch_config_g0/3#switchport mode private-vlan host

Switch_config_g0/3#switchport private-vlan host-association 2 3

Switch_config_g0/3#switchport pvid 3

Switch_config#interface GigaEthernet0/4

Switch_config_g0/4#switchport mode private-vlan host

Switch_config_g0/4#switchport private-vlan host-association 2 4

Switch_config_g0/4# switchport pvid 4

Switch_config#interface GigaEthernet0/5

Switch_config_g0/5#switchport mode private-vlan host

Switch_config_g0/5#switchport private-vlan host-association 2 5

Switch_config_g0/5#switchport pvid 5

Switch_config#interface GigaEthernet0/6

Switch_config_g0/5#switchport mode private-vlan host

Switch_config_g0/5#switchport private-vlan host-association 2 5

Switch_config_g0/5#switchport pvid 5

Switch_config#vlan 2

Switch_config_vlan2#private-vlan primary

Switch_config_vlan2#private-vlan association 3-5

Switch_config#vlan 3

Switch_config_vlan3#private-vlan community

```
Switch_config#vlan 4
Switch_config_vlan4#private-vlan community

Switch_config#vlan 5
Switch_config_vlan5#private-vlan isolated

Switch_config#show vlan private-vlan
Primary    Secondary   Type              Ports
---------- ----------- ----------------- ----------------------------------------
2          3           community         g0/1, g0/2, g0/3
2          4           community         g0/1, g0/4
2          5           isolated          g0/1, g0/5, g0/6
```

17.11 개요

GVRP(GARP VLAN Registration Protocol)는 IEEE 802.1Q 표준을 준수하는 VLAN pruning 및 802.1Q 트렁크 포트에서의 동적 VLAN 생성을 제공하는 GARP(GARP VLAN Registration Protocol) 애플리케이션입니다. GVRP를 사용하면 스위치 간에 VLAN 구성 정보를 교환하고, 불필요한 브로드캐스트 및 알 수 없는 유니캐스트 트래픽을 가지치기 하며, 802.1Q 트렁크 포트를 통해 연결된 스위치에서 동적으로 VLAN을 생성하고 관리할 수 있습니다.

17.12 구성 작업 목록

17.12.1 GVRP 구성 작업 목록

- GVRP 전체 활성화/비활성화
- 인터페이스에서 GVRP 활성화/비활성화
- GVRP 모니터링 및 유지보수

17.13 GVRP 구성 작업

17.13.1 GVRP 전체 활성화/비활성화

글로벌 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
[no] gvrp	GVRP 를 전역적으로 활성화하거나 비활성화합니다. 기본적으로 비활성화되어 있습니다.

17.13.2 등록된 포트에서만 유효한 동적 VLAN 구성

글로벌 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
[no] gvrp dynamic-vlan-pruning	등록된 포트에서만 동적 VLAN 이 유효하도록 활성화/비활성화합니다.

이 기능이 활성화되면, 동적 VLAN은 해당 동적 VLAN이 등록된 포트에서만 유효합니다. 이 명령어가 활성화된 후, 특정 포트가 동적 VLAN을 등록하지 않은 경우 해당 포트는 트렁크 포트이더라도 동적 VLAN의 구성원이 되지 않습니다.

17.13.3 인터페이스에서 GVRP 활성화/비활성화

인터페이스 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
[no] gvrp	인터페이스 GVRP 를 활성화하거나 비활성화합니다.

포트가 활성 GVRP 참가자가 되려면 GVRP를 먼저 전체적으로 활성화해야 하며, 해당 포트는 802.1Q 트렁크 포트여야 합니다. 기본적으로 GVRP는 활성화 상태입니다.

17.13.4 GVRP 모니터링 및 유지보수

EXEC 모드에서 다음 작업을 수행합니다.

명령어	설명
show gvrp statistics [**interface** port_list]	GVRP 통계를 표시합니다.
show gvrp status	GVRP 의 전체 상태 정보를 표시합니다.

[**no**] **debug gvrp** [**packet** | **event**]	GVRP 데이터 패킷 및 이벤트 디버그 스위치를 활성화하거나 비활성화합니다. 특정 스위치를 지정하지 않으면 모든 디버그 스위치가 활성화되거나 비활성화됩니다.

- GVRP 통계 정보 표시 예제

switch#show gvrp statistics interface Ethernet0/1

GVRP statistics on port Ethernet0/1

GVRP Status: Enabled

GVRP Failed Registrations: 0

GVRP Last Pdu Origin: 0000.0000.0000

GVRP Registration Type: Normal

- GVRP 전체 상태 정보 표시 예제

switch#show gvrp status

GVRP is enabled

17.13.5 설정 예제

네트워크 연결은 다음과 같습니다. 스위치 A와 스위치 B의 VLAN 구성 정보를 동일하게 만들기 위해 스위치 A와 스위치 B에서 GVRP를 활성화할 수 있습니다. 구성 방법은 다음과 같습니다.



① 스위치 A와 스위치 B를 연결하는 인터페이스 1을 트렁크 모드로 구성:

Switch_config_g0/1# switchport mode trunk

② 스위치 A에서 GVRP를 전체적으로 활성화:

Switch_config#gvRP

③ 스위치 A의 인터페이스 1에서 GVRP를 활성화:

Switch_config_g0/1#gvrp

④ 스위치 A에서 VLAN 10, VLAN 20, VLAN 30 구성:

Switch_config#vlan 10,20,30

⑤ 스위치 A와 스위치 B를 연결하는 인터페이스 2를 트렁크 모드로 구성:

Switch_config_g0/2# switchport mode trunk

⑥ 스위치 B에서 GVRP를 전체적으로 활성화:

Switch_config#gvrp

⑦ 스위치 B의 인터페이스 2에서 GVRP를 활성화:

Switch_config_g0/2#gvrp

⑧ 스위치 B에서 VLAN 40, VLAN 50, VLAN 60 구성:

Switch_config#vlan 40,50,60

구성을 완료한 후, 스위치 A와 스위치 B 모두에서 VLAN 구성 정보가 각각 표시됩니다. 결과적으로, 두 스위치 모두 VLAN 10, VLAN 20, VLAN 30, VLAN 40, VLAN 50, VLAN 60을 포함합니다.

18. IP 프로토콜 구성

18.1 IP 개요

18.1.1 IP

인터넷 프로토콜(IP)은 네트워크에서 텍스트 형식으로 데이터를 교환하는 프로토콜입니다. IP는 주소 지정, 단편화, 재조합 및 다중화와 같은 기능을 수행합니다. 기타 IP 프로토콜(IP 프로토콜군)은 IP를 기반으로 합니다. IP는 네트워크 계층에서 동작하는 프로토콜로, 라우팅에 사용되는 주소 정보 및 제어 정보를 포함합니다. 전송 제어 프로토콜(TCP) 역시 IP를 기반으로 합니다. TCP는 연결 지향 프로토콜로, 데이터 전송에서 데이터 및 정보의 형식을 규정합니다. 또한 TCP는 데이터가 성공적으로 도달했음을 확인하는 방법을 제공합니다. TCP는 수신된 데이터를 각각의 애플리케이션에 전송할 수 있으므로, 하나의 시스템에서 여러 애플리케이션이 동시에 통신하는 것을 허용합니다. IP 주소 지정(예: 주소 결정 프로토콜)은 "IP 주소 지정 구성" 섹션에서 설명됩니다. ICMP, HSRP, IP 통계 및 성능 매개변수와 같은 IP 서비스는 "IP 서비스 구성" 섹션에서 설명됩니다.

18.2 IP 주소 구성 작업 목록

IP 구성을 위해 반드시 필요한 기본 요구 사항은 라우팅 스위치의 네트워크 인터페이스에 IP 주소를 설정하는 것입니다.
이렇게 설정해야 네트워크 인터페이스가 활성화되고, IP 주소가 다른 시스템과 통신할 수 있습니다. 또한 IP 네트워크 마스크를 확인해야 합니다.

IP 주소를 구성하려면 다음 작업을 완료해야 하며, 첫 번째 작업은 필수이고 나머지는 선택 사항입니다. 네트워크에서 IP 주소를 설정하는 방법은 "IP 주소 지정 예시" 섹션을 참조하십시오.

IP 주소 구성 작업 목록:

- 네트워크 인터페이스에서 IP 주소 구성
- 네트워크 인터페이스에서 다중 IP 주소 구성
- 주소 결정(Address Resolution) 구성
- IP 주소 감지 및 유지 관리

18.3 Configuring IP Address

18.3.1 네트워크 인터페이스에서 IP 주소 구성

IP 주소는 IP 메시지가 전송되는 목적지를 결정합니다.
일부 IP 특별 주소는 예약되어 있으며, 호스트 IP 주소 또는 네트워크 주소로 사용할 수 없습니다.

아래 표는 IP 주소 범위, 예약된 IP 주소 및 사용 가능한 IP 주소를 보여줍니다.

타입	주소 범위	상태
A	0.0.0.0 1.0.0.0 to 126.0.0.0 127.0.0.0	Reserved 사용가능 Reserved
B	128.0.0.0 to 191.254.0.0 191.255.0.0	사용가능 Reserved
C	192.0.0.0 192.0.1.0 to 223.255.254.0 223.255.255.0	Reserved 사용가능 Reserved
D	224.0.0.0 to 239.255.255.255	Multicast address
E	240.0.0.0 to 255.255.255.254 255.255.255.255	Reserved Broadcast

IP 주소에 대한 공식 설명은 RFC 1166 "Internet Digit"에 명시되어 있습니다. 자세한 내용은 인터넷 서비스 공급자(ISP)에 문의할 수 있습니다. 하나의 인터페이스에는 하나의 기본 IP 주소만 할당됩니다. 인터페이스 구성 모드에서 아래 명령어를 사용해 네트워크 인터페이스의 기본 IP 주소와 네트워크 마스크를 설정합니다.

명령어	설명
ip address *ip-address mask*	인터페이스의 기본 IP 주소를 설정합니다.

마스크는 IP 주소의 일부로, 네트워크를 나타냅니다.

참고 : 스위치는 네트워크 순서에 따라 가장 높은 바이트에서 연속적으로 설정된 마스크만 지원합니다.

18.3.2 네트워크 인터페이스에서 다중 IP 주소 구성

각 인터페이스는 하나의 기본 IP 주소와 여러 개의 보조 IP 주소를 가질 수 있습니다.
다음 두 가지 경우에 보조 IP 주소를 구성해야 합니다.

- 네트워크 세그먼트에서 IP 주소가 부족한 경우
  예를 들어, 특정 논리 서브넷에서 사용 가능한 IP 주소가 254개뿐인데 물리 네트워크에

300개의 호스트를 연결해야 하는 경우입니다.
이 경우, 스위치 또는 서버에서 보조 IP 주소를 구성하여 두 개의 논리 서브넷이 동일한 물리 서브넷을 사용할 수 있도록 합니다.

- 초기 레이어 2 브리지 네트워크에서 서브넷이 나뉘지 않은 경우
  초기 네트워크를 여러 라우트 기반 서브넷으로 나누기 위해 보조 IP 주소를 사용할 수 있습니다.
  구성된 보조 IP 주소를 통해 네트워크 내의 라우팅 스위치는 동일한 물리 네트워크에 연결된 여러 서브넷을 인식할 수 있습니다.
- 두 서브넷이 물리적으로 다른 네트워크에 의해 분리된 경우
  이 경우, 두 서브넷이 물리적으로 분리되어 있지만 논리적으로 연결되도록 네트워크의 주소를 보조 IP 주소로 설정할 수 있습니다.

참고 : 네트워크 세그먼트에서 라우팅 스위치에 보조 IP 주소를 구성하는 경우, 동일한 네트워크 세그먼트에 있는 다른 라우팅 스위치에도 동일하게 구성해야 합니다.

인터페이스 구성 모드에서 아래 명령어를 사용하여 네트워크 인터페이스에 다중 IP 주소를 구성합니다.

명령어	설명
ip address *ip-address mask* **secondary**	트워크 인터페이스에 다중 IP 주소를 구성합니다.

참고 : IP 라우팅 프로토콜이 경로 업데이트 정보를 전송할 때, 보조 IP 주소는 다르게 처리될 수 있습니다.

18.3.3 Address Resolution 구성

IP는 IP 주소 결정 제어와 같은 기능을 수행할 수 있으며 다음 섹션에서는 주소 결정을 구성하는 방법을 설명합니다.

IP 장치는 두 가지 주소를 가질 수 있습니다.

- 로컬 주소 (LAN에서 고유하게 식별되는 로컬 네트워크 세그먼트 또는 장치)
- 네트워크 주소 (장치가 위치한 네트워크를 나타내는 주소)

로컬 주소는 링크 계층의 주소입니다. 로컬 주소는 링크 계층에서 메시지 헤더에 포함되며, 링크 계층에서 장치가 이를 읽고 사용합니다.
이 주소는 일반적으로 MAC 주소라고 불립니다. 이는 링크 계층에서 MAC 서브레이어가 주소를 처리하기 때문입니다.

예를 들어, 호스트가 이더넷에서 다른 장치와 통신하려면 해당 장치의 48비트 MAC 주소(링크 계층의 로컬 주소)를 알아야 합니다.
IP 주소에서 링크 계층의 로컬 주소를 얻는 과정을 주소 결정 프로토콜(ARP)이라고 합니다.
반대로, 링크 계층의 로컬 주소에서 IP 주소를 얻는 과정을 역주소 결정 프로토콜(RARP)이라고 합니다.

시스템은 두 가지 유형의 주소 결정을 사용합니다.

- ARP (Address Resolution Protocol)
- 프록시 ARP (Proxy ARP)

ARP와 프록시 ARP는 각각 RFC 860 및 RFC 1027에 정의되어 있습니다. ARP는 IP 주소를 매체 또는 MAC 주소에 매핑하는 데 사용됩니다. IP 주소가 알려지면, ARP는 해당하는 MAC 주소를 찾습니다. MAC 주소가 확인되면, IP 주소와 MAC 주소 간의 매핑 관계가 ARP 캐시에 저장되어 빠르게 접근할 수 있습니다.그 후, IP 메시지는 링크 계층에서 메시지로 패키징되어 네트워크로 전송됩니다.

- 정적 ARP 캐시 정의

  ARP 및 기타 주소 결정 프로토콜은 IP 주소와 MAC 주소 간의 동적 매핑을 제공합니다. 대부분의 호스트는 동적 주소 결정을 지원하기 때문에 정적 ARP 캐시 항목은 일반적으로 필요하지 않습니다.필요한 경우 글로벌 구성 모드에서 정적 ARP 캐시를 정의할 수 있습니다. 시스템은 정적 ARP 캐시 항목을 사용하여 32비트 IP 주소를 48비트 MAC 주소로 변환합니다.또한, 라우팅 스위치가 다른 호스트의 ARP 요청에 응답하도록 지정할 수도 있습니다. ARP 항목이 영구적으로 존재하지 않도록 활성 기간을 설정할 수 있습니다.다음 두 가지 방법은 정적 IP 주소와 MAC 주소 간의 매핑을 구성하는 방법을 보여줍니다.

글로벌 구성 모드 명령어

명령어	설명
arp ip-address hardware-address vlan	ARP 캐시에 IP 주소를 MAC 주소와 전역적으로 매핑합니다.
arp ip-address hardware-address vlan **alias**	라우팅 스위치가 지정된 IP 주소의 ARP 요청에 대해 라우팅 스위치의 MAC 주소로 응답하도록 지정합니다.

인터페이스 구성 모드 명령어

명령어	설명
arp timeout seconds	ARP 캐시 항목의 타임아웃 시간을 설정합니다.

arp dynamic	인터페이스에서 ARP 동적 학습을 활성화합니다.

상태 확인 및 캐시 관리 명령어

show interfaces – 지정된 인터페이스의 ARP 타임아웃 시간을 표시합니다.

show arp – ARP 캐시의 내용을 확인합니다.

clear arp-cache – ARP 캐시의 모든 항목을 삭제합니다.

- Free ARP 기능 구성

  스위치는 Free ARP 메시지를 전송하여 다른 장치의 IP 주소가 자신의 IP 주소와 충돌하는지 확인할 수 있습니다.

  Free ARP 메시지에는 출발지 IP 주소와 목적지 IP 주소가 모두 스위치의 로컬 주소로 설정됩니다. 메시지의 출발지 MAC 주소는 스위치의 로컬 MAC 주소입니다. 스위치는 기본적으로 Free ARP 메시지를 처리합니다.

  스위치가 장치에서 Free ARP 메시지를 수신하고 해당 메시지의 IP 주소가 자신의 IP 주소와 충돌하는 것을 감지하면, 장치에 ARP 응답을 반환하여 IP 주소 충돌을 알립니다. 또한, 스위치는 로그를 통해 사용자에게 IP 주소 충돌 사실을 알립니다.스위치에서 Free ARP 메시지를 전송하는 기능은 기본적으로 비활성화되어 있습니다.아래 명령어를 사용하여 스위치 포트에서 Free ARP 기능을 구성합니다.

명령어	설명
arp send-gratuitous	인터페이스에서 Free ARP 메시지 전송을 시작합니다.
arp send-gratuitous interval *value*	인터페이스에서 Free ARP 메시지를 전송하는 주기를 설정합니다. 기본 주기는 120 초 입니다.

- ARP 재탐색 및 호스트 이름 매핑 구성

  라우팅 엔트리 게이트웨이에 의존하는 ARP 항목(G로 태그된 항목)은 에이징 시 재탐색이 필요합니다. 이를 통해 하드웨어 서브넷 라우팅의 신속성과 정확성을 보장할 수 있습니다. 재전송 횟수가 많을수록 재탐색 가능성이 높아집니다.

명령어	설명
arp max-gw-retries *number*	재탐색 패킷의 최대 재전송 횟수를 설정합니다. 기본값은 3 입니다.

- ARP 항목 에이징 시 재탐색 설정

기본적으로 라우팅 엔트리에 의존하는 ARP만 에이징 시 재탐색을 수행합니다.
이 명령어를 활성화하면 모든 ARP 항목이 에이징 재탐색 메커니즘을 사용합니다.

명령어	설명
arp retry-allarp	ARP 항목이 에이징될 때 재탐색을 설정합니다.

- 호스트 이름을 IP 주소에 매핑

  IP 주소는 호스트 이름과 매핑될 수 있습니다.
  시스템은 텔넷 또는 핑(ping)할 수 있는 호스트 이름-주소 매핑 캐시를 저장합니다.
  글로벌 모드에서 아래 명령어를 사용해 호스트 이름과 IP 주소 간의 매핑을 설정합니다.

명령어	설명
ip host *name address*	ARP 항목이 에이징될 때 재탐색을 설정합니다.

18.3.4 IP 주소 감지 및 유지 관리

트워크를 감지하고 유지 관리하려면 아래 명령어를 실행합니다.

- 캐시, 목록 및 데이터베이스 지우기

  캐시, 목록 또는 데이터베이스의 모든 내용을 지울 수 있습니다. 일부 내용이 유효하지 않다고 판단되면 이를 삭제할 수 있습니다. 관리 모드에서 아래 명령어를 실행하여 캐시, 목록 및 데이터베이스를 지웁니다.

명령어	설명
clear arp-cache	IP ARP 캐시를 삭제합니다.

- 시스템 및 네트워크 통계 데이터 표시

  시스템은 IP 라우팅 테이블, 캐시 및 데이터베이스와 같은 지정된 통계 데이터를 표시할 수 있습니다.이 정보는 시스템 자원의 사용 현황을 파악하고 네트워크 문제를 해결하는 데 도움이 됩니다.시스템은 네트워크에서 메시지가 실행될 때, 포트의 연결 상태 및 메시지가 경유하는 경로도 표시할 수 있습니다. 관련 명령어는 아래 표에 나와 있으며, 자세한 사용 방법은 "IP 주소 지정 명령어" 장을 참조하십시오.
  관리 모드에서 아래 명령어를 실행합니다.

명령어	설명
show arp	ARP 테이블의 내용을 표시합니다.

show hosts	호스트 이름과 IP 매핑에 대한 캐시 테이블을 표시합니다.
show ip interface *[type number]*	포트 상태를 표시합니다.
ping {host | address}	네트워크 노드의 연결 상태를 테스트합니다.

18.3.5 IP 주소 설정

다음은 VLAN 11 인터페이스에서 IP 주소를 구성하는 예시입니다.

interface vlan 11

ip address 202.96.2.3 255.255.255.0

18.4 DHCP 구성

- 동적 호스트 구성 프로토콜(DHCP) 개요

DHCP는 인터넷에 있는 호스트에게 네트워크 구성 매개변수를 제공하는 데 사용됩니다. 이 프로토콜은 RFC 2131에 자세히 설명되어 있습니다.

DHCP의 주요 기능 중 하나는 인터페이스에 IP를 할당하는 것입니다.

DHCP는 다음 세 가지 IP 할당 메커니즘을 지원합니다.

- 자동 할당
  DHCP 서버는 클라이언트에게 영구적인 IP 주소를 자동으로 할당합니다.
- 동적 할당
  DHCP 서버는 클라이언트가 일정 기간 동안 사용할 수 있는 IP 주소를 할당합니다.
  해당 기간이 지나거나 클라이언트가 더 이상 사용하지 않으면 IP 주소가 회수됩니다.
- 수동 할당
  DHCP 서버 관리자가 IP 주소를 수동으로 지정하고, 이를 DHCP 프로토콜을 통해 클라이언트에 전송합니다.

18.4.1 DHCP 응용

DHCP는 다음과 같은 경우에 적용됩니다. DHCP 클라이언트를 구성하여 이더넷 인터페이스에 IP 주소, 네트워크 세그먼트 및 관련 자원(게이트웨이 등)을 할당할 수 있습니다.

- DHCP에 접근할 수 있는 스위치가 여러 호스트에 연결된 경우,
  스위치는 DHCP 릴레이를 통해 DHCP 서버로부터 IP 주소를 받아 이를 호스트에 배포합니다.

18.4.2 DHCP의 장점

현재 소프트웨어 버전에서는 DHCP 클라이언트 또는 이더넷 인터페이스의 DHCP 클라이언트가 지원됩니다. DHCP의 주요 장점은 다음과 같습니다.

- 설정 속도 향상
- 구성 오류 감소
- DHCP 서버를 통해 장치 포트의 IP 주소 제어

18.4.3 DHCP 용어

DHCP는 서버/클라이언트 모드를 기반으로 합니다. 따라서 DHCP 서버와 DHCP 클라이언트가 동시에 존재해야 합니다.

- DHCP 서버
  IP 주소 및 임대 시간과 같은 DHCP 관련 자원을 배포하고 회수하는 장치입니다.
- DHCP 클라이언트
  로컬 시스템 장치가 사용할 IP 주소 정보를 DHCP 서버에서 받아오는 장치입니다.

동적 DHCP 할당 과정에서 임대 시간이 존재합니다.

- 임대 시간(Lease Time)

  IP의 유효 기간을 의미하며, IP가 할당된 순간부터 시작됩니다.
  임대 시간이 만료되면 DHCP 서버는 IP 주소를 회수합니다.
  클라이언트가 해당 IP를 계속 사용하려면 DHCP 클라이언트가 다시 신청해야 합니다.

18.5 DHCP 클라이언트 구성

18.5.1 DHCP 클라이언트 구성 작업 목록

- IP 주소 획득
- DHCP 서버에 대한 주소 지정
- DHCP 매개변수 구성
- DHCP 모니터링

18.5.2 DHCP 클라이언트 구성 작업

- IP 주소 획득

  VLAN 인터페이스에서 아래 명령어를 실행하여 DHCP 프로토콜을 통해 인터페이스에 IP 주소를 할당 받습니다.

명령어	설명
ip address dhcp	이더넷 인터페이스의 IP 주소를 DHCP 를 통해 설정합니다.

- DHCP 서버 주소 지정

  DHCP 서버의 주소를 알고 있는 경우, 스위치에서 해당 서버의 주소를 지정하여 프로토콜

처리 시간을 단축할 수 있습니다.

글로벌 모드에서 아래 명령어를 실행합니다.

명령어	설명
ip dhcp-server *ip-address*	DHCP 서버의 IP 주소를 지정합니다.

참고 : IP 주소를 획득하는 작업을 수행할 때, 이 명령어는 선택 사항입니다.

- DHCP 매개변수 구성

  실제 요구 사항에 따라 DHCP 통신 매개변수를 조정하려면 글로벌 모드에서 아래 명령어를 실행합니다.

명령어	설명
ip dhcp client minlease *seconds*	허용 가능한 최소 임대 시간을 설정합니다.
ip dhcp client retransmit *count*	DHCP 패킷의 재전송 횟수를 설정합니다.
ip dhcp client select *seconds*	SELECT 단계의 간격을 설정합니다.
ip dhcp client class_identifier *WORD*	공급자의 분류 코드를 지정합니다.
ip dhcp client client_identifier hrd_ether	클라이언트 ID 를 이더넷 유형으로 지정합니다.
ip dhcp client timeout_shut	인터페이스에서 클라이언트 타임아웃 종료를 설정합니다.

참고 : IP 주소를 획득하는 작업을 수행할 때, 이 명령어는 선택 사항입니다.

- DHCP 모니터링

  스위치가 현재 발견한 DHCP 서버에 대한 정보를 확인하려면 EXEC 모드에서 아래 명령어를 실행합니다.

명령어	설명
show dhcp server	스위치에서 인식한 DHCP 서버에 대한 정보를 표시합니다.

현재 스위치에서 사용 중인 IP 주소를 확인하려면 EXEC 모드에서 아래 명령어를 실행합니다.

명령어	설명

show dhcp lease	스위치에서 현재 사용 중인 IP 자원 및 관련 정보를 표시합니다.

또한, 이더넷 인터페이스에 DHCP를 사용해 IP를 할당한 경우, 아래 명령어를 사용해 이더넷 인터페이스가 IP 주소를 성공적으로 획득했는지 확인할 수 있습니다.

show interface

18.5.3 DHCP 클라이어언트 구성 예제

다음 예시는 VLAN 11 인터페이스가 DHCP를 통해 IP 주소를 획득하는 방법을 보여줍니다.

```
!
interface vlan 11
ip address dhcp
```

18.6 IP 서비스 구성

선택적 IP 서비스 구성 작업은 다음과 같습니다.

- IP 연결 관리
- 성능 매개변수 구성
- IP 네트워크 감지 및 유지 관리

위 작업은 필수가 아니며, 필요에 따라 수행할 수 있습니다.

18.6.1 IP 연결 관리

IP 프로토콜은 IP 연결을 제어하고 관리하는 다양한 서비스를 제공합니다. 이러한 서비스는 대부분 ICMP(Internet Control Message Protocol)를 통해 제공됩니다. 라우팅 스위치나 액세스 서버가 IP 메시지 헤더에서 오류를 감지하면, 해당 오류를 알리기 위해 ICMP 메시지가 호스트나 다른 라우팅 스위치로 전송됩니다. ICMP는 RFC 792에 정의되어 있으며, 네트워크 문제를 진단하고 해결하는 데 중요한 역할을 합니다.

IP 연결 상태에 따라 다음과 같은 작업을 수행할 수 있습니다.

- ICMP 도달 불가(Unreachable) 메시지 전송

  시스템이 메시지를 수신했지만 경로가 없거나 다른 이유로 목적지에 전송할 수 없는 경우, 출발지 호스트로 ICMP 도달 불가 메시지가 전송됩니다. 이 기능은 기본적으로 활성화되어 있습니다. 기능이 비활성화된 경우, 인터페이스 구성 모드에서 아래 명령어를 실행하여 ICMP 도달 불가 메시지를 활성화할 수 있습니다.

명령어	설명
ip unreachables	ICMP 도달 불가 메시지를 전송하는 기능을 활성화합니다.

- ICMP 리디렉션(Redirection) 메시지 전송

  호스트가 비효율적인 경로를 선택하는 경우가 있습니다. 라우팅 스위치가 호스트로부터 메시지를 수신하면, 라우팅 테이블을 확인한 후 해당 메시지를 수신한 인터페이스를 통해 같은 네트워크 세그먼트에 있는 다른 라우팅 스위치로 메시지를 전달합니다.
  이 경우, 라우팅 스위치는 호스트에게 ICMP 리디렉션 메시지를 보내, 목적지로 가는 메시지를 자신을 경유하지 않고 다른 라우팅 스위치로 직접 전송하도록 알립니다.

  리디렉션 메시지는 출발지 호스트에게 원래의 경로를 폐기하고 메시지에서 제안하는 더 직접적인 경로를 사용하도록 요청합니다.

많은 호스트 운영 체제는 해당 정보를 기반으로 라우팅 테이블에 호스트 경로를 추가합니다. 그러나 라우팅 스위치는 라우팅 프로토콜을 통해 얻은 정보를 더 신뢰하기 때문에, 리디렉션 메시지를 기반으로 호스트 경로를 추가하지 않습니다. 이 기능은 기본적으로 활성화되어 있으며 인터페이스에서 핫 스탠바이 라우팅 스위치 프로토콜(HSRP)이 구성된 경우, 해당 기능은 자동으로 비활성화됩니다.

하지만 HSRP 구성이 취소되더라도 기능이 자동으로 다시 활성화되지는 않습니다. 인터페이스 구성 모드에서 아래 명령어를 실행해 ICMP 리디렉션 메시지 전송 기능을 활성화할 수 있습니다.

명령어	설명
ip redirects	ICMP 리디렉션 메시지 전송을 허용합니다.

- ICMP 마스크 응답(Mask Response) 메시지 전송

  호스트가 네트워크 마스크를 알아야 하는 경우가 있습니다. 이를 위해 호스트는 ICMP 마스크 요청 메시지를 전송할 수 있습니다. 라우팅 스위치가 호스트의 네트워크 마스크를 확인할 수 있는 경우, ICMP 마스크 응답 메시지를 반환합니다. 라우팅 스위치는 기본적으로 ICMP 마스크 응답 메시지를 전송할 수 있도록 설정되어 있습니다. 인터페이스 구성 모드에서 아래 명령어를 실행해 ICMP 마스크 응답 메시지를 전송할 수 있습니다.

명령어	설명
ip mask-reply	ICMP 마스크 응답 메시지를 전송합니다.

- 경로 MTU 감지(Route MTU Detection) 지원

  시스템은 RFC 1191에서 정의된 IP 경로 MTU 감지 메커니즘을 지원합니다. IP 경로 MTU 감지 메커니즘은 호스트가 서로 다른 경로의 최대 전송 단위(MTU)를 동적으로 찾아 조정할 수 있도록 합니다. 라우팅 스위치가 수신한 IP 메시지의 길이가 메시지를 전달하는 인터페이스에 설정된 MTU보다 클 경우, IP 메시지를 분할해야 합니다. 하지만 IP 메시지의 " 분할 금지(Don't Fragment)" 비트가 설정되어 있으면, 메시지를 분할할 수 없습니다.
  이 경우 메시지는 폐기됩니다.

  라우팅 스위치는 ICMP 메시지를 전송하여, 출발지 호스트에 메시지가 전달되지 못한 이유 , 포워딩 인터페이스의 MTU 값 을 알립니다. 출발지 호스트는 목적지로 전송하는 메시지의 길이를 줄여 경로의 최소 MTU에 맞춥니다. 경로상의 링크가 끊어질 경우, 메시지는 다른 경로를 선택하게 됩니다. 새로운 경로의 최소 MTU는 기존 경로와 다를 수 있습니다. 라우팅 스위치는 새로운 경로의 MTU 값을 출발지 호스트에 다시 알립니다.

IP 메시지는 경로의 최소 MTU에 맞춰 패키징되며, 이를 통해 메시지 분할을 방지하고 전송되는 메시지 수를 줄여 통신 효율을 향상시킬 수 있습니다. IP 경로 MTU 감지를 수행하려면 관련 호스트가 이 기능을 지원해야 합니다. 이 기능을 통해 호스트는 라우팅 스위치에서 통보한 MTU 값에 따라 IP 메시지의 길이를 조정하여, 포워딩 과정에서의 분할을 방지합니다.

- IP 소스 경로(Source Route) 허용

  라우팅 스위치는 수신한 모든 메시지의 IP 헤더를 검사합니다. RFC 791에 정의된 IP 헤더 옵션(엄격 소스 경로, 완화 소스 경로, 경로 기록, 타임스탬프)을 지원합니다. 스위치가 잘못된 옵션을 감지하면, ICMP 매개변수 문제 메시지를 출발지 호스트에 전송하고 해당 메시지를 폐기합니다. 소스 경로에서 문제가 발생한 경우, 라우팅 스위치는 ICMP 도달 불가 메시지(소스 경로 실패)를 출발지 호스트로 전송합니다.

  IP는 출발지 호스트가 메시지를 전송하는 IP 네트워크의 경로를 지정하도록 허용합니다. 이렇게 지정된 경로를 소스 경로라고 합니다. IP 헤더 옵션에서 소스 경로를 선택하여 이를 지정할 수 있습니다. 라우팅 스위치는 해당 옵션에 따라 IP 메시지를 포워딩해야 하며, 보안 요구 사항에 따라 메시지를 폐기할 수도 있습니다. 메시지가 폐기되면, 라우팅 스위치는 출발지 호스트에 ICMP 도달 불가 메시지를 전송합니다. 라우팅 스위치는 기본적으로 소스 경로를 지원합니다. IP 소스 경로가 비활성화된 경우, 글로벌 구성 모드에서 아래 명령어를 실행해 IP 소스 경로를 허용할 수 있습니다.

명령어	설명
ip source-route	IP 소스 경로를 허용합니다.

18.6.2 성능 매개변수 구성

IP 성능을 설정 하려면 아래 명령어를 실행합니다.

- TCP 연결 대기 시간 설정

  라우팅 스위치가 TCP 연결을 수행할 때, 설정된 대기 시간 내에 TCP 연결이 완료되지 않으면 연결 실패로 간주합니다. 라우팅 스위치는 상위 프로그램에 TCP 연결 실패를 알립니다.TCP 연결 대기 시간을 설정할 수 있으며, 시스템의 기본값은 75초입니다.이 설정은 스위치가 직접 생성하는 TCP 연결에만 영향을 미치며, 스위치가 포워딩하는 TCP 연결에는 영향을 주지 않습니다. 글로벌 구성 모드에서 아래 명령어를 실행하여 TCP 연결 대기 시간을 설정합니다.

명령어	설명
ip tcp synwait-time *seconds*	TCP 연결 대기 시간을 설정합니다.

- TCP 윈도우 크기 설정

  기본 TCP 윈도우 크기는 2000바이트입니다. 기본 윈도우 크기를 변경하려면 글로벌 구성 모드에서 아래 명령어를 실행합니다.

명령어	설명
ip tcp window-size *bytes*	TCP 윈도우 크기를 설정합니다.

18.6.3 IP 네트워크 감지 및 유지 관리

네트워크를 감지하고 유지 관리하려면 아래 명령어를 실행합니다.

- 캐시, 목록 및 데이터베이스 지우기

  캐시, 목록 또는 데이터베이스의 모든 내용을 지울 수 있습니다. 데이터베이스에 잘못된 데이터가 포함되어 있는 경우 이를 제거해야 합니다. 아래 명령어를 실행하여 잘못된 데이터를 삭제합니다.

명령어	설명
clear tcp statistics	TCP 통계 데이터를 지웁니다.

- TCP 연결 해제

  TCP 연결을 종료하려면 아래 명령어를 실행합니다.

명령어	설명
clear tcp {**local** host-name port **remote** host-name port | **tcb** address}	clear tcp {로컬 호스트 이름 포트 원격 호스트 이름 포트 | tcb 주소} 지정된 TCP 연결을 지웁니다. TCB 는 TCP 제어 블록을 의미합니다.

- 시스템 및 네트워크 통계 데이터 표시

  시스템은 캐시, 목록 및 데이터베이스의 내용을 표시할 수 있습니다.
  이러한 통계 데이터는 시스템 자원의 사용 현황을 파악하고 네트워크 문제를 해결하는 데 도움이 됩니다. EXEC 모드에서 아래 명령어를 실행합니다.

명령어	설명
show ip access-lists *name*	하나 또는 모든 액세스 목록의 내용을 표시합니다.

show ip sockets	라우팅 스위치의 모든 소켓 정보를 표시합니다.
show ip traffic	IP 프로토콜에 대한 통계 데이터를 표시합니다.
show tcp	모든 TCP 연결 상태 정보를 표시합니다.
show tcp brief	TCP 연결 상태 정보를 간략하게 표시합니다.
show tcp statistics	TCP 통계 데이터를 표시합니다.
show tcp tcb	지정된 TCP 연결 상태 정보를 표시합니다.

- 디버깅 정보 표시

  네트워크에서 문제가 발생한 경우, 디버그 명령어를 실행하여 디버깅 정보를 확인할 수 있습니다. EXEC 모드에서 아래 명령어를 실행합니다. 자세한 내용은 "IP 서비스 명령어" 섹션을 참조하십시오.

명령어	설명
debug arp	ARP 상호 작용 정보를 표시합니다.
debug ip icmp	ICMP 상호 작용 정보를 표시합니다.
debug ip raw	수신/송신된 IP 메시지 정보를 표시합니다.
debug ip packet	IP 상호 작용 정보를 표시합니다.
debug ip tcp	TCP 상호 작용 정보를 표시합니다.
debug ip udp	UDP 상호 작용 정보를 표시합니다..

18.7 액세스 리스트 구성

18.7.1 IP 패킷 필터링

패킷 필터링은 네트워크에서 패킷의 이동을 제어하는 데 도움이 됩니다. 이러한 제어는 특정 사용자나 장치를 통해 네트워크 전송 및 사용을 제한할 수 있습니다. 스위치는 특정 인터페이스에서 패킷을 허용하거나 차단하도록 액세스 리스트 기능을 제공합니다.

액세스 리스트는 다음과 같은 방식으로 사용됩니다.

- 인터페이스에서 패킷 전송 제어
- 가상 터미널 라인 액세스 제어
- 라우팅 업데이트 내용 제한

이 섹션에서는 IP 액세스 리스트를 생성하고 사용하는 방법을 설명합니다.

액세스 리스트 사용 단계

- 액세스 리스트 이름 및 조건을 지정하여 액세스 리스트를 생성합니다.
- 생성한 액세스 리스트를 인터페이스에 적용합니다.

18.7.2 표준 및 확장 IP 액세스 리스트 생성

IP 액세스 리스트는 문자열을 사용하여 생성할 수 있습니다.

참고 : 표준 액세스 리스트와 확장 액세스 리스트는 동일한 이름을 가질 수 없습니다.

표준 엑세스 리스트 생성

글로벌 구성 모드에서 다음 명령어를 실행하여 표준 액세스 리스트를 생성합니다.

명령어	설명
ip access-list standard *name*	이름을 사용해 표준 액세스 리스트를 정의합니다.
deny {*source [source-mask]* | **any**}[**log | location**] or **permit** {*source [source-mask]* | **any**}[**log | location**]	표준 액세스 목록 구성 모드에서 하나 이상의 허용/거부 조건을 지정합니다. 이전 설정은 패킷이 승인되는지 거부되는지를 결정합니다.
Exit	액세스 목록 구성 모드에서 로그아웃합니다.

확장 액세스 리스트 생성

글로벌 구성 모드에서 다음 명령어를 실행하여 확장 액세스 리스트를 생성합니다.

명령어	설명
ip access-list extended *name*	이름을 사용해 확장 액세스 리스트를 정의합니다.
{**deny | permit**} *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**][**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**totallen eq|gt|lt** lentgh] [**ttl eq|gt|lt** time] [**offset-not-zero**] [**offset-zero**] {**deny | permit**} *protocol* **any any** [**precedence** *precedence*] [**tos** *tos*] [**log**][**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**]	확장 가능한 액세스 목록 구성 모드에서 하나 이상의 허용/거부 조건을 지정합니다. 이전 설정은 패킷이 승인되는지 거부되는지를 결정합니다. (우선순위는 IP 패킷의 우선순위를 의미하고 TOS 는 서비스 유형을 의미합니다.)

[**totallen eq|gt|lt** lentgh] [**ttl eq|gt|lt** time] [**offset-not-zero**] [**offset-zero**]	
Exit	액세스 목록 구성 모드에서 로그아웃합니다.

액세스 목록을 원래 만든 후에는 나중에 추가되는 모든 부분을 목록 끝에 넣을 수 있습니다. 즉, 지정된 액세스 목록에 명령줄을 추가할 수 없습니다. 그러나 no permit 및 no deny를 실행하여 액세스 목록에서 항목을 삭제할 수 있습니다.

참고 : 액세스 목록을 만들 때 액세스 목록 끝에는 기본적으로 암묵적 deny 문장이 포함됩니다. 상대 IP 호스트 주소 액세스 목록에서 마스크가 생략된 경우 255.255.255.255가 마스크가 됩니다.

액세스 목록을 만든 후에는 액세스 목록을 경로 또는 인터페이스에 적용해야 합니다. 자세한 내용은 섹션 3.2.3 "인터페이스에 액세스 목록 적용"을 참조하십시오.

18.7.3 인터페이스에 액세스 리스트 적용

액세스 리스트가 생성된 후, 해당 리스트를 인 인터페이스 및 아웃 인터페이스를 포함한 하나 이상의 인터페이스에 적용할 수 있습니다.
인터페이스 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
ip access-group *name* {**in	out**}	인터페이스에 액세스 목록을 적용합니다.

액세스 컨트롤 리스트는 인바운드 또는 아웃바운드 인터페이스에서 사용할 수 있습니다.

패킷이 수신된 후, 패킷의 출발지 주소는 표준 송출 인터페이스 액세스 컨트롤 리스트에 따라 검사됩니다. 확장된 액세스 컨트롤 리스트의 경우, 라우팅 스위치는 목적지 주소도 검사합니다.

만약 액세스 컨트롤 리스트가 목적지 주소를 허용하면, 시스템은 계속해서 패킷을 처리합니다.

그러나 액세스 컨트롤 리스트가 목적지 주소를 금지하면, 시스템은 해당 패킷을 폐기하고 ICMP 도달 불가(Unreachable) 패킷을 반환합니다.

아웃 인터페이스의 표준 액세스 리스트의 경우, 패킷이 수신되거나 제어 인터페이스로 라우팅된 후, 소프트웨어는 액세스 리스트에 따라 패킷의 출발지 주소를 검사합니다. 확장된 액세스 리스트에서는 라우팅 스위치가 수신 측의 액세스 리스트도 검사합니다.

만약 액세스 리스트가 주소를 허용하면, 소프트웨어는 패킷을 전송합니다. 액세스 리스트가 주소를 허용하지 않으면, 소프트웨어는 패킷을 폐기하고 ICMP 도달 불가 메시지를 반환합니다.

지정된 액세스 컨트롤 리스트가 존재하지 않는 경우, 모든 패킷은 통과하도록 허용됩니다.

18.7.4 확장 액세스 리스트 예제

다음 예제는 첫 번째 줄에서 포트 1023보다 큰 목적지 포트로의 새로운 TCP 연결을 허용합니다. 두 번째 줄은 호스트 130.2.1.2의 SMTP 포트(포트 25)로의 새로운 TCP 연결을 허용합니다.

ip access-list extended aaa

permit tcp any 130.2.0.0 255.255.0.0 gt 1023

permit tcp any 130.2.1.2 255.255.255.255 eq 25

interface vlan 10

ip access-group aaa in

다음은 확장 액세스 리스트를 적용하는 또 다른 예제입니다. 네트워크가 인터넷에 연결되어 있고, 이더넷의 모든 호스트가 인터넷의 호스트와 TCP 연결을 생성할 수 있도록 설정하고자 합니다. 그러나 인터넷의 호스트는 메일 호스트의 SMTP 포트를 연결하는 경우를 제외하고는 이더넷의 호스트와 TCP 연결을 생성할 수 없습니다.

SMTP는 한쪽 끝에서 TCP 포트에 연결되고, 다른 쪽에서는 임의의 포트 번호에 연결됩니다. 연결 기간 동안 동일한 두 포트 번호가 사용됩니다. 인터넷에서 들어오는 메일 패킷은 목적지 포트 25를 사용합니다. 송신 패킷은 반대 방향으로 포트 번호를 사용합니다. 실제로 라우팅 스위치 뒤의 보안 시스템은 항상 포트 25에서 메일을 수신합니다. 이는 인바운드 서비스와 아웃바운드 서비스를 독립적으로 제어할 수 있는 이유입니다.

다음 예제에서는 이더넷이 130.20.0.0 주소를 가진 B 클래스 네트워크입니다.

메일 호스트의 주소는 130.20.1.2입니다.

established 키워드는 TCP 프로토콜에만 사용되며, 기존 연결이 생성된 상태를 의미합니다.

ACK 또는 RST 비트가 설정된 TCP 데이터는 일치하며, 해당 패킷은 기존 연결에 속합니다.

ip access-list aaa

permit tcp any 130.20.0.0 255.255.0.0 established

permit tcp any 130.20.1.2 255.255.255.255 eq 25

interface vlan 10

ip access-group aaa in

18.8 물리 포트 기반 IP 액세스 리스트 구성

18.8.1 IP 패킷 필터링

패킷 필터링은 네트워크에서 패킷의 이동을 제어하는 데 도움이 됩니다.
이러한 제어는 특정 사용자나 장치를 통해 네트워크 전송 및 사용을 제한할 수 있습니다.
스위치는 특정 인터페이스에서 패킷을 허용하거나 차단하도록 액세스 리스트 기능을 제공합니다.

액세스 리스트는 다음과 같은 방식으로 사용됩니다.

- 인터페이스에서 패킷 전송 제어
- 가상 터미널 라인 액세스 제어
- 라우팅 업데이트 내용 제한

이 섹션에서는 IP 액세스 목록을 만드는 방법과 이를 사용하는 방법을 설명합니다.

IP 액세스 목록은 IP 주소를 적용하기 위한 허용/금지 조건의 순서 있는 집합입니다. 스위치의 ROS 소프트웨어는 규정에 따라 액세스 목록에서 주소를 하나씩 테스트합니다. 첫 번째 일치는 ROS가 주소를 수락할지 거부할지 여부를 결정합니다. 첫 번째 일치 후 ROS 소프트웨어는 일치 규정을 종료합니다. 따라서 조건의 순서가 중요합니다. 규정과 일치하지 않으면 주소가 거부됩니다.

다음 단계에 따라 액세스 목록을 사용합니다.

- 액세스 목록 이름과 조건을 지정하여 액세스 목록을 만듭니다.
- 포트에 ACL 적용

18.8.2 표준 및 확장 IP 액세스 리스트 생성

IP 액세스 리스트는 문자열을 사용하여 생성합니다.

참고 : 표준 액세스 리스트와 확장 액세스 리스트는 동일한 이름을 가질 수 없습니다.

표준 액세스 리스트 생성

글로벌 구성 모드에서 다음 명령어를 실행하여 표준 액세스 리스트를 생성합니다.

명령어	설명
ip access-list standard *name*	표준 액세스 목록을 정의하려면 이름을 사용합니다.
deny {*source [source-mask]* | **any**} [**log | location**] or **permit** {*source [source-mask]* | **any**} [**log | location**]	표준 액세스 목록 구성 모드에서 하나 이상의 허용/거부 조건을 지정합니다. 이전 설정은 패킷이 승인되는지 거부되는지를 결정합니다.
Exit	액세스 목록 구성 모드에서 로그아웃합니다.

확장 액세스 리스트 생성

글로벌 구성 모드에서 다음 명령어를 실행하여 확장 액세스 리스트를 생성합니다.

명령어	설명
ip access-list extended *name*	표준 액세스 목록을 정의하려면 이름을 사용합니다.
{**deny** **|** **permit**} *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**totallen eq|gt|lt** lentgh] [**ttl eq|gt|lt** time] [**offset-not-zero**] [**offset-zero**] {**deny** **|** **permit**} *protocol* **any any** [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**totallen eq|gt|lt** lentgh] [**ttl eq|gt|lt** time] [**offset-not-zero**] [**offset-zero**]	장 가능한 액세스 목록 구성 모드에서 하나 이상의 허용/거부 조건을 지정합니다. 이전 설정은 패킷이 승인되는지 거부되는지 여부를 결정합니다. 우선 순위는 IP 패킷의 우선순위를 의미하고 TOS 는 서비스 유형을 의미합니다. 프로토콜이 TCP/UDP 인 경우 특정 범위 내에서 단일 또는 14 개 포트 번호를 지정합니다. 자세한 내용은 액세스 목록 구성 예를 참조하십시오.
Exit	액세스 목록 구성 모드에서 로그아웃합니다.

액세스 리스트가 처음 생성된 후, 이후에 추가되는 항목은 목록의 끝에만 추가할 수 있습니다.

즉, 지정된 액세스 리스트의 특정 위치에 명령어를 추가할 수 없습니다.

그러나 no permit 및 no deny 명령어를 실행하여 액세스 리스트에서 항목을 삭제할 수 있습니다.

참고 : 액세스 리스트를 생성할 때, 액세스 리스트의 끝에는 기본적으로 암시적 거부(implicit deny) 문장이 포함됩니다. IP 호스트 주소 액세스 리스트에서 마스크가 생략된 경우, 기본적으로 255.255.255.255가 마스크로 설정됩니다.

액세스 리스트(ACL)가 생성된 후, 반드시 라인 또는 포트에 적용되어야 합니다. 자세한 내용은 " 인터페이스에 액세스 리스트 적용" 섹션을 참조하십시오.

18.8.3 포트에 ACL 적용

ACL이 설정되면 하나 이상의 포트, 인바운드(Ingress) 또는 아웃바운드(Egress) 포트에 적용할 수 있습니다.

아래 명령어를 실행하여 포트에 IPv6 ACL을 적용합니다.

명령어	설명
ip access-group *name*	포트에 ACL 을 적용합니다..

패킷이 수신되면, 표준 송출 인터페이스 액세스 컨트롤 리스트에 따라 패킷의 출발지 주소가 검사됩니다. 확장 액세스 컨트롤 리스트의 경우, 라우팅 스위치는 목적지 주소도 확인합니다.

액세스 리스트가 목적지 주소를 허용한 경우 시스템은 패킷을 계속 처리합니다. 허용하지 않는 경우 시스템은 패킷을 폐기하고 출발지 호스트에 ICMP 패킷을 반환합니다. 지정된 액세스 컨트롤 리스트가 존재하지 않으면, 모든 패킷은 통과됩니다.

18.8.4 확장 액세스 리스트 예제

- TCP/UDP 포트 필터링을 지원하는 포트 기반 IP 액세스 리스트

다음은 액세스 리스트에서 TCP/UDP 포트를 필터링하는 형식입니다.

{deny | permit} {tcp | udp}

source source-mask [{ [src_portrange begin-port end-port] | [{gt | lt } port] }]

destination destination-mask [{ [dst_portrange begin-port end-port] | [{gt | lt } port] }]

[precedence precedence] [tos tos]

- 포트 범위를 지정하여 액세스 리스트를 구성할 때 주의 사항:

  출발지와 목적지에서 모두 포트 범위를 지정하는 방식으로 액세스 리스트를 구성하면 리소스가 많이 소모되어 일부 구성에 실패할 수 있습니다.
  이 경우, 출발지 또는 목적지 중 한 쪽에만 포트 범위를 지정하고 다른 쪽은 단일 포트를 지정해야 합니다.

  포트 범위 필터링을 수행할 경우, 리소스 소모가 큽니다.
  포트 범위 필터링이 과도하게 사용되면, 액세스 리스트는 다른 프로그램을 충분히 지원하지 못할 수 있습니다.

- TCP/UDP 지정 포트 필터링을 지원하는 포트 기반 IP 액세스 리스트

  다음 예제는 TCP를 통해 호스트 130.2.1.2의 SMTP 포트(포트 25)로 새로운 연결을 허용하는 방법을 보여줍니다.

ip access-list extended aaa

permit tcp any 130.2.1.2 255.255.255.255 eq 25

interface g0/1

ip access-group aaa

18.9 IP 접근 제어 목록 적용

18.9.1 포트에 ACL 적용

아래 명령어를 사용하여 설정된 IP 액세스 리스트를 인터페이스에 적용하거나 제거할 수 있습니다.

명령어	설명
config	글로벌 구성 모드로 들어갑니다.
interface g0/1	구성할 포트로 들어갑니다.
[**no**] **{ip | ipv6} access-group** *name*	설정된 IP 액세스 목록을 인터페이스에 적용하거나 인터페이스에서 적용된 IP를 취소합니다. 이름 IP: IP 액세스 목록의 이름입니다.
exit	글로벌 구성 모드로 돌아갑니다.
exit	EXEC 모드로 돌아갑니다.
write	설정을 저장합니다.

글로벌 모드에서 IP 액세스 리스트 적용 또는 해제

글로벌 모드에서 IP 액세스 리스트를 VLAN에 적용하거나 제거하려면 다음 명령어를 사용합니다.

명령어	설명
config	로벌 구성 모드로 들어갑니다.
[**no**] **{ip | ipv6} access-group** *name* **[vlan {***word* **| add** *word* **| remove** *word***}]**	글로벌 모드에서 설정된 IP 액세스 목록을 적용하거나 글로벌 모드에서 적용된 IP를 취소합니다. Egress는 ACL이 아웃바운드 방향으로 적용됨을 의미합니다. Vlan은 ACL이 인바운드 VLAN에 적용됨을 의미합니다. Word는 VLAN 범위 테이블을 의미합니다. Add는 VLAN 범위 테이블을 추가함을 의미합니다. Remove는 VLAN 범위 테이블을 삭제함을 의미합니다.
exit	EXEC 모드로 돌아갑니다.
write	설정을 저장합니다.

참고 : IP 액세스 리스트는 글로벌 모드에서 VLAN에 적용할 수 있지만, 포트 구성 모드에서는

VLAN에 적용할 수 없습니다.

18.10 IPv6 프로토콜 구성

라우터의 IPv6 주소 구성은 VLAN 인터페이스에서만 적용되며, 물리적 인터페이스에서는 적용되지 않습니다.

기본 상태에서는 IPv6 프로토콜이 비활성화되어 있습니다.

VLAN 인터페이스에서 IPv6 프로토콜을 사용하려면, VLAN 인터페이스 구성 모드에서 해당 프로토콜을 활성화해야 합니다.

IPv6 프로토콜을 활성화하려면 IPv6 주소를 설정해야 합니다.

VLAN 인터페이스에서 하나 이상의 IPv6 주소가 설정되면, 해당 VLAN 인터페이스는 IPv6 패킷을 처리하고 다른 IPv6 장치와 통신할 수 있습니다.

IPv6 프로토콜 활성화 작업

- VLAN 인터페이스 구성 모드에서 하나 이상의 IPv6 주소 설정

18.11 IPv6 활성화

18.11.1 IPv6 주소 설정

IPv6 주소는 IPv6 패킷의 목적지를 결정하는 데 사용됩니다. IPv6 주소는 다음 세 가지 유형으로 나뉩니다.

종류	표기형식	설명
유니캐스트 주소	2001:0:0:0:0DB8:800:200C:417A/64	
멀티캐스트 주소	FF01:0:0:0:0:0:0:101	
애니캐스트 주소	2002:0:0:0:0DB8:800:200C:417A/64	

IPv6 활성화를 위한 필수 작업

- VLAN 인터페이스 구성 모드에서 유니캐스트 주소를 설정해야 합니다.
- 설정할 수 있는 유니캐스트 주소는 다음 중 하나 또는 복수일 수 있습니다.
  - ① IPv6 링크-로컬 주소
  - ② 글로벌 IPv6 주소

명령어	설명

ipv6 enable	링크-로컬 주소를 자동으로 설정합니다.
ipv6 address fe80::x link-local	링크-로컬 주소를 수동으로 설정합니다.

참고 : 링크-로컬 주소는 반드시 fe80으로 시작해야 합니다. 기본 프리픽스 길이는 64비트입니다. 수동으로 설정하는 경우 마지막 64비트 값만 지정할 수 있습니다. VLAN 인터페이스당 하나의 링크-로컬 주소만 설정할 수 있습니다. 링크-로컬 주소를 설정하여 IPv6를 활성화한 경우, IPv6는 로컬 링크에서만 작동합니다.

18.12 IPv6 서비스 설정

IPv6가 활성화된 후에는 IPv6가 제공하는 모든 서비스를 설정할 수 있습니다.

설정 가능한 IPv6 서비스는 다음과 같습니다.

- IPv6 링크 관리

18.12.1 IPv6 링크 관리

IPv6는 IPv6 링크를 제어 및 관리하기 위한 다양한 서비스를 제공합니다.
이 서비스에는 다음 항목이 포함됩니다.

- IPv6 MTU 설정

  모든 인터페이스는 기본 IPv6 MTU(Maximum Transmission Unit)를 가지고 있습니다.

  IPv6 패킷의 길이가 MTU를 초과할 경우, 라우터는 해당 IPv6 패킷을 분할(fragmentation)합니다.

특정 인터페이스에서 IPv6 MTU 설정

명령어	설명
ipv6 mtu bytes	특정 인터페이스에서 IPv6 MTU를 설정합니다.

- IPv6 리디렉션 설정

  호스트가 선택한 경로가 최적이 아닐 때가 있습니다.

  이 경우, 스위치가 이 경로에서 패킷을 수신하면, 스위치는 라우팅 테이블에 따라 패킷을 수신한 인터페이스에서 해당 패킷을 전송하고, 이를 호스트와 동일한 네트워크 세그먼트에 속하는 다른 라우터로 포워딩합니다.

  이 조건에서, 스위치는 소스 호스트에게 동일한 목적지 주소로 향하는 패킷을 스위치 자체를 거치지 않고 다른 라우터로 직접 전송하도록 알립니다.

  리디렉션 패킷은 소스 호스트에게 기존 경로를 리디렉션 패킷에 포함된 더 직접적인 경로로 교체하도록 요구합니다.

  많은 호스트의 운영 체제는 라우팅 테이블에 호스트 라우트를 추가합니다.

  그러나, 스위치는 라우팅 프로토콜에서 얻는 정보를 더 신뢰하기 때문에, 이러한 정보에 따라 호스트 라우트를 추가하지 않습니다.

  IPv6 리디렉션은 기본적으로 활성화되어 있습니다.

그러나, 핫 스탠바이 라우터 프로토콜이 인터페이스에서 구성된 경우, IPv6 리디렉션은 자동으로 비활성화됩니다.

핫 스탠바이 라우터 프로토콜이 취소되더라도, 이 기능은 자동으로 활성화되지 않습니다.IPv6 리디렉션을 활성화하려면 다음 명령어를 실행하십시오.

명령어	설명
ipv6 redirects	IPv6가 리디렉션 패킷을 전송하도록 허용합니다.

- IPv6 목적지 도달 불가 설정

  많은 경우, 시스템은 자동으로 목적지 도달 불가(destination-unreachable) 패킷을 전송합니다. 사용자는 이 기능을 비활성화할 수 있습니다. 이 기능이 비활성화되면, 시스템은 ICMP 도달 불가 패킷을 전송하지 않습니다.

  IPv6 목적지 도달 불가 기능을 활성화하려면 다음 명령어를 실행하십시오

명령어	설명
ipv6 unreachables	IPv6가 목적지 도달 불가 패킷을 전송하도록 허용합니다.

- IPv6 ACL 설정

  사용자는 ACL(Access Control List)을 사용하여 VLAN 인터페이스에서 패킷의 수신 및 전송을 제어할 수 있습니다.글로벌 구성 모드에서 VLAN 인터페이스에 ACL을 도입하고 필터링 방향을 지정하면, 해당 VLAN 인터페이스에서 IPv6 패킷이 필터링 됩니다. IPv6 패킷을 필터링하려면 인터페이스 구성 모드에서 다음 명령어를 실행하십시오

명령어	설명
ipv6 access-group *WORD* { in | out }	VLAN 인터페이스에서 수신 방향의 IPv6 패킷을 필터링합니다.

18.13 IPv6 ACL 구성

18.13.1 IPv6 패킷 필터링

IPv6 패킷 필터링은 네트워크에서 패킷의 동작을 제어하는 데 도움이 됩니다. 이러한 제어는 특정 사용자 또는 장치에 의해 네트워크 전송 및 동작을 제한할 수 있습니다. 특정 포트에서 패킷을 허용하거나 차단하려면 **ACL(Access Control List)**을 사용합니다. IPv6 ACL은 다음과 같은 방식으로 사용할 수 있습니다.

- 포트에서의 패킷 전송 제한

- 가상 터미널 라인 액세스 제한
- 라우팅 업데이트 제한

이 장에서는 IPv6 ACL 설정 방법 및 적용 방법에 대해 설명합니다.

IPv6 ACL은 IPv6 주소의 허용/거부를 설정하는 체계적으로 구성된 규칙 집합입니다. 스위치의 ROS(라우팅 운영 체제)는 ACL에서 지정한 규칙에 따라 IPv6 주소를 검사합니다. 첫 번째로 일치하는 규칙에 따라 소프트웨어는 해당 주소를 허용하거나 거부합니다.

첫 번째로 일치하는 규칙 이후에는 추가 규칙이 적용되지 않기 때문에 규칙의 순서가 매우 중요합니다. 일치하는 규칙이 없을 경우, 해당 IPv6 주소는 거부됩니다.

ACL 사용 단계 :

- ACL을 설정하고 ACL 이름 및 조건을 지정합니다.
- ACL을 포트에 적용합니다.

18.13.2 IPv6 ACL 설정

IPv6 ACL은 문자열 형식으로 설정됩니다.

참고 : 표준 ACL과 확장 ACL은 동일할 수 없습니다.

IPv6 ACL을 설정하려면 글로벌 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
IPv6 access-list *name*	이름을 입력하여 IPv6 ACL을 정의합니다.
{**deny** | **permit**} *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]	IPv6 ACL의 구성 모드에서 하나 이상의 활성화/비활성화 조건을 지정합니다. 이는 패킷을 통과시킬지 여부를 결정합니다. (dscp는 IPv6 그룹 헤더 Traffic Class 도메인과 일치시키는 데 사용되고, flow-label은 IPv6 그룹 헤더의 Flow Label 태그 도메인과 일치시키는 데 사용되고, fragments는 그룹 확장 헤더에 none-0 오프셋이 포함된 경우 fragment 그룹과 일치시키는 데 사용되고, log는 로그를 기록할지 여부를 의미하고, routing은 IPv6 그룹 헤더의 경로 확장 헤더의 소스 그룹과 일치시키는 데 사용되고, time-range는 ACL의 시간 범위를 제한하는 데 사용됩니다.)
Exit	ACL 구성 모드를 종료합니다.

ACL을 설정한 후, deny 또는 permit 규칙에 시퀀스(sequence)가 추가되지 않으면, 추가되는 모든 항목은 ACL의 끝에 자동으로 추가됩니다.

다시 말해, deny/permit 규칙의 앞이나 뒤에 **[sequence value]**를 추가하면, 지정된 ACL의 임의

위치에 ACL 명령어를 추가할 수 있습니다.

마찬가지로, ACL에서 항목을 삭제하려면 "no permit" 및 "no deny" 명령어를 사용하거나, "no sequence" 명령어를 사용하여 특정 위치의 규칙을 직접 삭제할 수 있습니다.

참고:

- ACL을 설정할 때, ACL의 기본 끝에는 "deny ipv6 any any" 문이 자동으로 포함됩니다.
- ACL은 설정된 후 반드시 라인(Line) 또는 포트(Port)에 적용되어야 합니다.
  ACL을 포트에 적용하는 방법은 "Apply the ACL to the port" 섹션을 참조하십시오.

18.13.3 포트에 ACL 적용하기

ACL은 하나 이상의 포트 또는 인그레스(ingress)에 적용할 수 있습니다.
다음 명령어는 구성 모드에서 실행됩니다.

명령어	설명
IPv6 access-group *name*	포트에 ACL을 적용합니다.

표준 인그레스 ACL의 경우, 패킷을 수신한 후 소스 주소를 검사합니다.

확장 ACL의 경우, 라우팅 스위치는 대상 주소도 검사합니다. ACL이 해당 주소를 허용하면 소프트웨어는 패킷을 계속 처리합니다. ACL이 주소를 허용하지 않으면 소프트웨어는 패킷을 삭제하고 ICMP 호스트 도달 불가(Host Unreachable) 패킷을 반환합니다. ACL이 지정되지 않은 경우, 모든 패킷은 통과가 허용됩니다.

18.13.4 Pv6 ACL 예제

다음 예제에서는 호스트 A:B:C:D::E에 대한 개별 대상 호스트 연결을 먼저 활성화하고, 호스트 IPv6 소스 프리픽스가 255:255:255::/48인 SMTP 포트(25번)와의 새 TCP 연결을 비활성화합니다.
최종 ACL의 다음 규칙 시퀀스는 이전 규칙보다 앞에 위치합니다.

Switch_config#ipv6 access-list xxcom

Switch_config_ipv6acl#permit any host A:B:C:D::E sequence 20

Switch_config_ipv6acl#deny tcp any 255:255:255::/48 eq 25 sequence 10

Switch_config_ipv6acl#ex

Switch_config#show ipv6 access-lists xxcom

ipv6 access-list xxcom

deny tcp any 255:255:255::/48 eq smtp sequence 10

permit ipv6 any host A:B:C:D::E sequence 20

19. STP 구성

19.1 STP 소개

표준 스패닝 트리 프로토콜(STP)은 IEEE 802.1D에서 정의되며, 여러 브리지로 구성된 LAN 토폴로지를 단일 스패닝 트리로 단순화합니다. 이를 통해 네트워크 루프 발생을 방지하고 네트워크의 안정적인 작동을 보장합니다. STP의 알고리즘과 프로토콜은 랜덤 브리징 LAN을 간단한 연결로 이루어진 활성 토폴로지로 구성합니다. 활성 토폴로지에서는 일부 브리지 포트는 프레임을 전달할 수 있는 상태이며, 다른 포트는 혼잡 상태로 인해 프레임을 전달할 수 없습니다. 혼잡 상태의 포트는 활성 토폴로지에 포함될 수 있습니다. 네트워크에 장치가 추가되거나 제거되거나 비활성화될 때, 포트는 전송 상태로 변경될 수 있습니다.

- STP 토폴로지의 구조는 아래와 같습니다.
- STP 토폴로지에서 하나의 브리지는 루트(root)로 간주됩니다.
- 각 LAN 구간에는 데이터를 루트로 전달하는 브리지 포트가 지정됩니다. 이 포트는 해당 네트워크 구간의 지정 포트(designated port)로 간주됩니다.
- 지정 포트가 위치한 브리지는 해당 LAN의 지정 브리지(designated bridge)로 간주됩니다.
- 루트는 루트와 연결된 모든 네트워크 구간의 지정 브리지로 간주됩니다.

각 브리지의 포트 중 루트에 가장 가까운 포트는 해당 브리지의 루트 포트(root port)로 지정됩니다.

활성 토폴로지에서 데이터 전송 상태가 되는 포트는 루트 포트와 지정 포트입니다. 나머지 포트는 종료되지 않지만 루트 포트나 지정 포트가 아니며, 이를 대기 포트(standby port)라고 부릅니다.

활성 토폴로지의 안정 구조를 결정하는 주요 매개변수

① 각 브리지의 식별자(identifier)

② 각 포트의 경로 비용(path cost)

③ 각 포트의 포트 식별자(port identifier)

우선순위가 가장 높은 브리지(식별자 값이 가장 작은)가 루트로 선택됩니다. 각 브리지의 포트는 루트 경로 비용(root path cost)이라는 속성을 가지며, 이는 루트에서 브리지까지의 모든 포트 경로 비용 합계 중 최소값입니다.

각 네트워크 세그먼트의 지정 포트는 네트워크 세그먼트와 연결되고 최소 경로 비용을 가지는 포트를 의미합니다.

- 루프가 포함된 경우 포트 상태 결정

스위치에서 두 포트가 루프의 일부인 경우, 스패닝 트리의 포트 우선순위와 경로 비용 설정에 따라 어떤 포트가 전송 상태(forwarding state)로 전환되고, 어떤 포트가 차단 상태(blocking state)로 전환될지가 결정됩니다. 스패닝 트리 포트 우선순위 값은 네트워크 토폴로지에서 포트의 위치와 트래픽 전달 가능성을 나타냅니다. 경로 비용(path cost)은 매체 속도를 나타냅니다.

- 지원되는 스패닝 트리 모드

  스위치 표준은 두 가지 스패닝 트리 프로토콜 모드를 지원합니다:

  802.1D STP (Standard Spanning Tree Protocol)

  802.1w RSTP (Rapid Spanning Tree Protocol)

일부 스위치 모델은 VLAN별로 STP 모드를 분배하거나 MSTP(Multiple Spanning Tree Protocol)를 지원할 수 있습니다. 자세한 내용은 2장에서 다루는 'RSTP 구성(Configuring RSTP)'을 참조하세요.

참고 : 802.1D STP와 802.1w RSTP는 이 문서에서 각각 SSTP와 RSTP로 축약하여 사용됩니다. 여기서 SSTP(Single Spanning Tree Protocol)는 단일 스패닝 트리를 의미합니다.

19.2 STP 구성 작업 목록

- STP 모드 선택
- STP 비활성화/활성화
- 포트의 STP 비활성화/활성화
- 스위치 우선순위 설정
- Hello Time 설정
- Max-Age Time 설정
- Forward Delay Time 설정
- 포트 우선순위 설정
- 경로 비용(Path Cost) 설정
- STP 상태 모니터링
- SNMP Trap 구성

19.3 STP 구성 작업

19.3.1 STP 모드 선택

다음 명령어를 실행하여 STP 모드를 설정합니다.

명령어	설명
spanning-tree mode {sstp | pvst | rstp | mstp}	STP 모드를 선택합니다.

19.3.2 STP 비활성화/활성화

스패닝 트리는 기본적으로 활성화되어 있습니다. 네트워크 토폴로지에서 루프가 없다는 확신이 있을 경우에만 STP를 비활성화하십시오.

STP를 비활성화하려면 다음 단계를 따릅니다:

명령어	설명
no spanning-tree	STP 를 비활성화합니다.
spanning-tree	기본 모드(SSTP)로 STP 를 활성화합니다.
spanning-tree mode {**sstp | pvst** | **rstp | mstp**}	특정 STP 모드를 활성화합니다.

19.3.3 포트에서 STP 비활성화/활성화

기본적으로 STP 프로토콜은 모든 스위칭 포트(물리적 포트와 집계 포트)에서 작동합니다. 포트 구성 모드에서 다음 명령어를 사용하여 STP 작동을 비활성화할 수 있습니다:

명령어	설명
no spanning-tree	포트에서 STP 작동을 금지합니다.

STP가 비활성화되면 포트는 계속 포트 할당 및 프레임 전달 상태를 유지하며, BPDU를 전송하지 않습니다. 그러나 모든 STP 모드는 여전히 포트에서 수신된 BPDU에 대해 유형 확인 및 카운팅 작업을 수행합니다. 경계 정보와 토폴로지 정보는 계속 업데이트됩니다.

주의사항:

- no spanning-tree 명령을 실행할 때, 포트가 RSTP/MSTP 모드에서 RootPort, AlternatePort, MasterPort, BackupPort와 같은 역할을 가지고 있다면, 해당 포트가 수신한 프로토콜 정보는 만료되며 DesignatedPort로 전환됩니다.
- SSTP/PVST 모드에서는 포트가 일정 시간 동안 기존 역할을 유지하며, 타이머가 초과되

면 정보가 만료됩니다.

- 모든 STP 모드는 no spanning-tree 포트에서 BpduGuard 기능을 지원합니다.

19.3.4 스위치 우선순위 설정

스위치 우선순위를 설정하여 독립형 스위치나 스택 내의 스위치가 루트 스위치로 선택될 가능성을 높일 수 있습니다.

다음 단계에 따라 스위치 우선순위를 구성합니다.

명령어	설명
spanning-tree sstp priority *value*	SSTP 우선순위 값을 수정합니다.
no spanning-tree sstp priority	SSTP 우선순위를 기본값(32768)으로 복원합니다.

19.3.5 Hello Time 설정

루트 스위치가 STP 데이터 유닛(STP BPDU)을 전송하는 간격을 설정하려면 Hello Time을 구성합니다.

명령어	설명
spanning-tree sstp hello-time *value*	SSTP Hello Time 값을 설정합니다.
no spanning-tree sstp hello-time	SSTP Hello Time을 기본값(2초)으로 복원합니다.

19.3.6 Max-Age Time 설정

스위치는 Max-Age Time 동안 스패닝 트리 구성 메시지(BPDU)를 수신하지 못하면 재구성을 시도합니다.

명령어	설명
spanning-tree sstp max-age *value*	SSTP Max-Age Time을 설정합니다.
no spanning-tree sstp max-age	Max-Age Time을 기본값(20초)으로 복원합니다.

19.3.7 Forward Delay Time 설정

Forward Delay Time은 인터페이스가 STP 학습(Learning) 및 청취(Listening) 상태에서 전송(Forwarding) 상태로 변경되기 전에 대기해야 하는 시간을 결정합니다.

명령어	설명
spanning-tree sstp forward-time *value*	SSTP Forward Delay Time을 설정합니다.
no spanning-tree sstp forward-time	Forward Delay Time을 기본값(15초)으로 복원합니다.

19.3.8 포트 우선순위 설정

루프가 발생하면 스패닝 트리는 포트 우선순위를 사용하여 전송 상태로 전환할 인터페이스를 선택합니다.

- 높은 우선순위(숫자가 낮은 값)를 할당하면 해당 인터페이스가 먼저 선택됩니다.
- 낮은 우선순위(숫자가 높은 값)는 나중에 선택됩니다.
- 모든 인터페이스의 우선순위 값이 같다면, 스패닝 트리는 인터페이스 번호가 가장 낮은 인터페이스를 전송 상태로 설정하고 나머지 인터페이스를 차단합니다.

명령어	설명
spanning-tree port-priority *value*	인터페이스의 포트 우선순위를 설정합니다.
spanning-tree sstp port-priority *value*	SSTP 포트 우선순위를 수정합니다.
no spanning-tree sstp port-priority	포트 우선순위를 기본값(128)으로 복원합니다.

19.3.9 경로 비용(Path Cost) 설정

인터페이스의 경로 비용을 설정하려면 다음 단계를 따르십시오.

명령어	설명
spanning-tree cost *value*	인터페이스의 경로 비용(Path Cost)을 설정합니다.
spanning-tree sstp cost *value*	SSTP 경로 비용을 수정합니다.
no spanning-tree sstp cost	경로 비용을 기본값으로 복원합니다.

19.3.10 STP 상태 모니터링

STP 구성 및 상태를 모니터링하려면 관리 모드에서 다음 명령어를 사용하십시오.

명령어	설명
show spanning-tree	활성 인터페이스의 스패닝 트리 정보를 표시합니다.
show spanning-tree detail	인터페이스의 상세 정보를 요약하여 표시합니다.

show spanning-tree interface	지정된 인터페이스의 스패닝 트리 정보를 표시합니다.

19.3.10 SNMP Trap 설정

STP의 트랩(Trap) 기능을 구성하면, 호스트의 네트워크 관리 소프트웨어를 통해 스위치에서 발생하는 STP 변경 사항을 원격으로 모니터링할 수 있습니다.

STP 프로토콜은 두 가지 유형의 트랩을 지원합니다:

- newRoot: 스위치가 non-root 상태에서 새 루트(newRoot) 상태로 전환될 때 트랩 메시지를 전송합니다.
- topologyChange: non-edge 포트가 비 전송 상태에서 전송 상태로 전환되는 등의 토폴로지 변경을 감지할 때 트랩 메시지를 전송합니다.

주의사항 :

STP 트랩 메시지를 수신하려면 트랩을 지원하는 네트워크 관리 소프트웨어가 필요합니다.

네트워크 관리 소프트웨어에 Bridge-MIB 세트를 가져와야 하며, 해당 OID는 1.3.6.1.2.1.17입니다.

글로벌 구성 모드에서 다음 명령어를 사용합니다.

명령어	설명
spanning-tree management trap **[newroot | topologychange]**	STP 트랩 시작. 트랩 유형이 정의되지 않은 경우 두 가지 종류의 TRAP이 동시에 시작됩니다.
no spanning-tree management trap	STP 트랩을 비활성화합니다.

19.4 VLAN 스패닝 트리 구성

19.4.1 개요

SSTP(Single Spanning Tree Protocol) 모드에서는 네트워크 전체에 단일 스패닝 트리 인스턴스만 존재하며, 스위치 포트의 스패닝 트리 상태가 VLAN에서의 상태를 결정합니다. 네트워크에 여러 VLAN이 존재하는 경우, 단일 스패닝 트리 프로토콜과 VLAN 토폴로지 간의 분리가 네트워크 일부의 정상적인 통신이 차단되는 문제를 일으킬 수 있습니다.

스위치는 특정 수의 VLAN에서 독립적으로 SSTP를 실행하는 것을 지원하며, 이를 통해 포트가 각기 다른 VLAN에서 서로 다른 상태를 가질 수 있도록 합니다. 동시에 VLAN 간 트래픽 균형을 실현할 수 있습니다.

여기서 주의해야 할 점은, 독립적으로 스패닝 트리 프로토콜을 실행할 수 있는 VLAN의 수는 실

제 버전에 따라 다르다는 것입니다. 이 제한을 초과하는 VLAN 토폴로지는 STP에 의해 제어되지 않습니다.

19.4.2 VLAN STP 구성 작업

글로벌 구성 모드에서 SSTP의 속성을 설정하려면 다음 명령어를 따르십시오.

명령어	설명
spanning-tree mode pvst	VLAN별로 STP를 할당하는 모드를 시작합니다.
spanning-tree vlan *vlan-list*	지정된 VLAN에 STP 인스턴스를 할당합니다.
no spanning-tree vlan *vlan-list*	지정된 VLAN에서 스패닝 트리 인스턴스를 제거합니다.
spanning-tree vlan *vlan-list* **priority** *value*	지정된 VLAN에서 스패닝 트리의 우선 순위를 설정합니다.
no spanning-tree *vlan-list* **priority**	VLAN에서 스패닝 트리 우선 순위를 기본값으로 재설정합니다.
spanning-tree vlan *vlan-list* **forward-time** *value*	지정된 VLAN의 Forward Delay를 설정합니다.
no spanning-tree vlan *vlan-list* **forward-time**	지정된 VLAN의 Forward Delay를 기본값으로 재설정합니다.
spanning-tree vlan *vlan-list* **max-age** *value*	지정된 VLAN의 Max-age를 설정합니다.
no spanning-tree vlan *vlan-list* **max-age**	지정된 VLAN의 Max-age를 기본값으로 재설정합니다.
spanning-tree vlan *vlan-list* **hello-time** *value*	지정된 VLAN의 Hello-time을 설정합니다.
no spanning-tree vlan *vlan-list* **hello-time**	지정된 VLAN의 Hello-time을 기본값으로 재설정합니다.

인터페이스 구성 모드에서 포트 속성을 설정하려면 다음 명령어를 따르십시오.

명령어	설명
spanning-tree vlan *vlan-list* **cost**	지정된 VLAN에서 포트 경로 비용(Path Cost)을 설정합니다.
no spanning-tree vlan *vlan-list* **cost**	지정된 VLAN에서 포트 경로 비용을 기본값으로 재설정합니다.

spanning-tree vlan *vlan-list* **port-priority**	지정된 VLAN에서 포트 우선 순위(Port Priority)를 설정합니다.
no spanning-tree vlan *vlan-list* **port-priority**	지정된 VLAN에서 포트 우선 순위를 기본값으로 재설정합니다.

관리 구성 모드에서 지정된 VLAN의 스패닝 트리 상태를 확인하려면 다음 명령어를 사용하십시오.

명령어	설명
show spanning-tree vlan *vlan-list*	VLAN에서 스패닝 트리 상태를 확인합니다.
show spanning-tree pvst instance-list	PVST 인스턴스와 VLAN 간의 관계를 확인합니다.

19.5 RSTP 설정

RSTP 구성 작업 목록

RSTP(Rapid Spanning Tree Protocol) 구성을 위한 주요 작업

- 스위치 RSTP 활성화/비활성화
- 스위치 우선 순위 설정
- Forward Delay 시간 설정
- Hllo Time 설정
- Max-Age 설정
- Path Cost 설정
- 포트 우선 순위 설정
- 엣지 포트(edge port) 설정
- 포트 연결 유형 설정
- 프로토콜 변환 확인 재시작

19.6 RSTP 구성 작업

19.6.1 스위치 RSTP 활성화/비활성화

글로벌 구성 모드에서 다음 명령어를 사용합니다.

명령어	설명
spanning-tree mode rstp	RSTP 활성화
no spanning-tree mode	STP를 기본 모드(SSTP)로 복원

19.6.2 스위치 우선 순위 설정

스위치의 우선 순위를 설정하여 독립형 스위치 또는 스택 내 스위치가 루트 스위치로 선택될 가능성을 높일 수 있습니다.

글로벌 구성 모드에서 다음 명령어를 사용합니다

명령어	설명
spanning-tree rstp priority *value*	RSTP 우선 순위 값을 수정합니다.
no spanning-tree rstp priority	RSTP 우선 순위를 기본값으로 복원합니다.

참고 : 네트워크 내 모든 브리지의 우선 순위 값이 동일하면, MAC 주소가 가장 작은 브리지가 루트 브리지로 선택됩니다. RSTP 프로토콜이 활성화된 상태에서 브리지 우선 순위 값이 변경되면, 스패닝 트리 재계산이 발생합니다. 브리지 우선 순위의 기본값은 32768입니다.

19.6.3 Forward Delay Time 설정

링크 장애가 발생하면 네트워크는 스패닝 트리 구조를 다시 계산해야 합니다. 그러나 최신 구성 메시지가 네트워크 전체에 전달되지 않을 수 있습니다. 새로 선택된 루트 포트와 지정 포트가 데이터를 즉시 전달하기 시작하면 일시적인 경로 루프가 발생할 수 있습니다. 따라서 프로토콜은 상태 전환 메커니즘을 채택합니다. 루트 포트와 지정 포트가 데이터를 전달하기 시작하기 전에 중간 상태를 거치며, 이 중간 상태가 Forward Delay Time 동안 유지된 후 데이터 전달 상태로 전환됩니다. 이 지연 시간은 새로 구성된 메시지가 네트워크 전체에 전달되었는지 확인하는 데 필요합니다.

Forward Delay는 스위치 네트워크의 네트워크 지름(Network Diameter)과 관련이 있습니다. 일반적으로 네트워크 지름이 클수록 Forward Delay Time을 더 길게 설정해야 합니다.

글로벌 구성 모드에서 다음 명령어를 사용합니다

명령어	설명
spanning-tree rstp forward-time *value*	Forward Delay Time을 설정합니다.
no spanning-tree rstp forward-time	Forward Delay Time을 기본값(15초)으로 복원합니다.

참고 : Forward Delay Time을 너무 짧게 설정하면 일시적인 루프 경로가 발생할 수 있습니다. Forward Delay Time을 너무 길게 설정하면 시스템이 연결을 복구하는 데 오랜 시간이 걸릴 수 있습니다. 기본값을 사용하는 것을 권장하며 Forward Delay Time의 기본값은 15초입니다.

19.6.4 Hello Time 설정

적절한 Hello Time 값을 설정하면 네트워크에서 링크 장애를 감지할 수 있으면서도 네트워크 자원을 과도하게 사용하지 않을 수 있습니다.

글로벌 구성 모드에서 다음 명령어를 사용합니다

명령어	설명
spanning-tree rstp hello-time *value*	Hello Time을 설정합니다.
no spanning-tree rstp hello-time	Hello Time을 기본값으로 복원합니다..

참고 : Hello Time 값을 너무 길게 설정하면 링크의 패킷 손실로 인해 브리지가 Hello 메시지를 수신하지 못할 수 있습니다. 이 경우 브리지는 링크가 끊어졌다고 판단하고 스패닝 트리를 다시 계산합니다. Hello Time 값을 너무 짧게 설정하면 브리지가 구성 메시지를 빈번히 전송하게 되어 네트워크 대역폭이 점유되고, 네트워크 및 CPU에 부담을 줄 수 있습니다. 기본값을 사용을 권장하며 Hello Time의 기본값은 2초입니다.

19.6.5 Max-Age 설정

Max-Age는 스위치가 스패닝 트리 구성 메시지를 수신하지 않고 기다리는 시간을 초 단위로 설정하는 값입니다. 이 시간이 지나면 네트워크 재구성을 시도합니다.

글로벌 구성 모드에서 다음 명령어를 사용합니다

명령어	설명
spanning-tree rstp max-age *value*	Max-Age 값을 설정합니다.
no spanning-tree rstp max-age	Max-Age 값을 기본값(20초)으로 복원합니다.

주의사항 : Max-Age 값을 너무 작게 설정하면 스패닝 트리 계산이 자주 발생하여 시스템이 네트워크 차단을 링크 장애로 잘못 인식할 수 있습니다. Max-Age 값을 너무 크게 설정하면 링크 상태를 적시에 감지하지 못할 수 있습니다. 기본값(20초)을 사용하는 것을 권장하며 Max-Age의 기본값은 20초입니다.

19.6.6 Path Cost 설정

스패닝 트리의 Path Cost 기본값은 인터페이스의 매체 속도를 기준으로 결정됩니다. 루프가 발생하면 스패닝 트리는 인터페이스를 Forwarding 상태로 선택할 때 비용(Path Cost)을 기준으로 판단합니다. 우선적으로 선택되기를 원하는 인터페이스에는 낮은 비용 값을, 후순위로 선택되기를 원하는 인터페이스에는 높은 비용 값을 할당할 수 있습니다. 모든 인터페이스의 비용 값이 동일한 경우, 스패닝 트리는 인터페이스 번호가 가장 낮은 인터페이스를 Forwarding 상태로 설정하고 나머지 인터페이스를 차단합니다.

글로벌 구성 모드에서 다음 명령어를 사용합니다

명령어	설명
spanning-tree rstp cost *value*	인터페이스의 Path Cost 값을 설정합니다.
no spanning-tree rstp cost	Path Cost 값을 기본값으로 복원합니다.

참고 : 이더넷 포트의 우선 순위 값을 변경하면 스패닝 트리가 다시 계산될 수 있습니다. 기본값을 사용하는 것이 권장되며, RSTP 프로토콜이 현재 이더넷 인터페이스의 Path Cost를 자동으로 계

산하도록 설정하는 것이 좋습니다. 포트 속도가 10Mbps인 경우: 2000000 포트 속도가 100Mbps 인 경우: 200000

19.6.7 Port Priority 설정

포트 우선 순위는 루프가 발생했을 때 스패닝 트리가 Forwarding 상태로 전환할 인터페이스를 선택하는 데 사용됩니다. 높은 우선 순위(숫자가 낮은 값)를 가진 인터페이스가 먼저 선택되고, 낮은 우선 순위(숫자가 높은 값)를 가진 인터페이스가 후순위로 선택됩니다. 모든 인터페이스의 우선 순위가 동일하다면, 인터페이스 번호가 가장 낮은 포트가 Forwarding 상태로 설정됩니다.

글로벌 구성 모드에서 다음 명령어를 사용합니다

명령어	설명
spanning-tree rstp port-priority *value*	포트의 우선 순위를 설정합니다.
no spanning-tree rstp port-priority	포트의 우선 순위를 기본값으로 복원합니다.

참고 : 이더넷 인터페이스의 우선 순위를 수정하면 스패닝 트리가 다시 계산될 수 있습니다. 기본 이더넷 인터페이스 우선 순위는 128입니다.

19.6.8 Edge Port 설정

Edge Port는 네트워크의 단말 장치에 연결된 포트를 의미합니다. 강제 Edge Port는 링크가 활성화되자마자 즉시 Forwarding 상태로 전환됩니다.

글로벌 구성 모드에서 다음 명령어를 사용합니다

명령어	설명
spanning-tree rstp edge	포트를 Edge Port로 설정합니다.

참고 : 프로토콜이 자동 감지 모드로 설정된 경우, 포트가 일정 시간 동안 BPDU를 수신하지 않으면 해당 포트를 Edge Port로 간주합니다.

19.6.9 포트 연결 유형 설정

RSTP 프로토콜을 사용하는 스위치 간 연결이 포인트-투-포인트(Point-to-Point)로 설정되면 핸드셰이크 메커니즘을 통해 빠르게 토폴로지를 설정할 수 있습니다.

기본적으로 프로토콜은 포트의 듀플렉스 속성을 기준으로 연결 유형을 판단합니다:

포트가 전이중 모드(Full Duplex)로 동작하면 포인트-투-포인트 연결로 간주합니다.

포트가 반이중 모드(Half Duplex)로 동작하면 공유(Shared) 연결로 간주합니다.

만약 포트에 연결된 스위치가 RSTP 또는 MSTP 프로토콜을 사용하는 것이 확인되면, 포트 연결 유형을 포인트-투-포인트로 강제로 설정하여 빠른 핸드셰이크 처리를 보장할 수 있습니다.

글로벌 구성 모드에서 다음 명령어를 사용합니다

명령어	설명
spanning-tree rstp point-to-point **[force-true | force-false | auto]**	지점 간 포트 구성. force-true: 지점 간 유형으로 강제합니다. force-false: none 지점 간 유형으로 강제합니다. 자동: 프로토콜이 자동으로 포트 유형을 감지합니다.

19.6.10 프로토콜 변환 확인 재시작

RSTP 프로토콜은 프로토콜 변환 메커니즘을 통해 기존 802.1D STP 스위치와 협력하여 동작할 수 있습니다. 만약 스위치의 포트 중 하나가 STP 구성 정보를 수신하면, 해당 포트는 STP 메시지만 전송하도록 상태를 변경합니다.

포트가 STP 호환 상태로 전환된 경우, 해당 포트가 더 이상 802.1D STP BPDU를 수신하지 않더라도 RSTP 상태로 자동 복구하지 않습니다. 이 경우 명령어 spanning-tree rstp migration-check를 사용하여 포트의 프로토콜 변환 확인을 시작하고 포트를 RSTP 모드로 복구할 수 있습니다.

글로벌 구성 모드에서 다음 명령어를 사용합니다

명령어	설명
spanning-tree rstp migration-check	모든 포트의 프로토콜 변환 확인 프로세스를 재시작합니다.

스위치 포트 구성 모드에서 다음 명령어를 사용합니다.

명령어	설명
spanning-tree rstp migration-check	현재 포트의 프로토콜 변환 확인 프로세스를 재시작합니다.

이 명령어를 사용하면 프로토콜 변환 상태를 점검하고 RSTP 모드로 복구할 수 있습니다.

19.7 MSTP 구성

19.7.1 MSTP 개요

다중 스패닝 트리 프로토콜(MSTP, Multiple Spanning Tree Protocol)은 브리징된 LAN에서 간단하고 완전한 토폴로지를 생성하는 데 사용됩니다. MSTP는 이전의 스패닝 트리 프로토콜(STP) 및 빠른 스패닝 트리 프로토콜(RSTP)과 호환됩니다.

STP와 RSTP는 모두 단일 STP 토폴로지만 생성할 수 있으며, 모든 VLAN 메시지는 단일 STP를 통해 전달됩니다. STP는 수렴 속도가 느린 단점이 있으나, RSTP는 핸드셰이크 메커니즘을 통해 빠르고 안정적인 네트워크 토폴로지를 보장합니다.

MSTP는 RSTP의 빠른 핸드셰이크 메커니즘을 계승하며, 동시에 서로 다른 VLAN을 서로 다른 STP에 할당하여 네트워크에 여러 개의 토폴로지를 생성할 수 있습니다. MSTP 네트워크에서는 서로 다른 VLAN의 프레임이 서로 다른 경로를 통해 전달될 수 있어 VLAN 데이터의 부하 분산이 가능합니다.

VLAN이 STP에 분배되는 기존 메커니즘과 달리, MSTP는 여러 VLAN이 단일 STP 토폴로지에 할당되도록 허용합니다. 이를 통해 많은 VLAN을 지원하는 데 필요한 STP 수를 효과적으로 줄일 수 있습니다.

19.7.2 MST 도메인

MSTP에서 VLAN과 STP 간의 관계는 MSTP 구성 테이블을 통해 설명됩니다. MSTP 구성 테이블, 구성 이름, 구성 수정 번호로 이루어진 요소는 MST 구성 식별자를 구성합니다.

네트워크에서 동일한 MST 구성 식별자를 가진 상호 연결된 브리지는 동일한 MST 영역(MST Region)으로 간주됩니다. 동일한 MST 영역의 브리지들은 항상 동일한 VLAN 구성을 가지며, VLAN 프레임이 MST 영역 내에서 전송되는 것을 보장합니다.

19.7.3 IST, CST, CIST 및 MSTI

MSTP 네트워크의 구성은 다음과 같은 요소로 설명됩니다:

- IST (Internal Spanning Tree): MST 영역 내에서 작동하는 내부 스패닝 트리.
- CST (Common Spanning Tree): 모든 MST 영역과 802.1D STP 스위치를 포함한 전체 네트워크의 공통 스패닝 트리.
- CIST (Common and Internal Spanning Tree): CST와 IST를 결합한 전체 네트워크의 스패닝 트리.
- MSTI (Multiple Spanning Tree Instance): MST 영역 내에서 VLAN과 연결된 여러 개의 독

립적인 스패닝 트리.

그림에서 MSTP 네트워크의 구조를 보여주며, 여기에는 세 개의 MST 영역과 802.1D STP를 실행하는 스위치가 포함되어 있습니다.

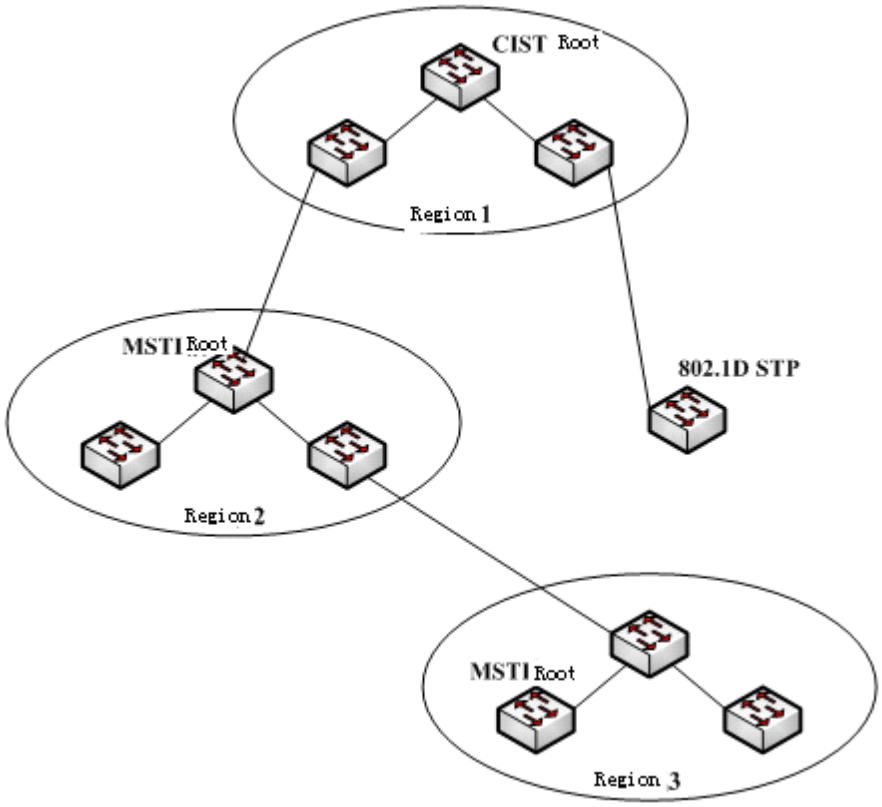


그림 11 MSTP 토폴로지

① CIST (Common and Internal Spanning Tree)

CIST는 모든 단일 스위치와 상호 연결된 LAN으로 구성된 스패닝 트리를 의미합니다. 이 스위치들은 서로 다른 MST 영역에 속할 수 있으며, 기존 STP 또는 RSTP를 실행하는 스위치일 수도 있습니다. MST 영역 내에서 STP 또는 RSTP를 실행하는 스위치는 해당 영역 내의 독립적인 스위치로 간주됩니다.

네트워크 토폴로지가 안정되면, 전체 CIST에서 CIST 루트 브리지가 선택됩니다. 각 MST 영역에서는 해당 영역 중심에서 CIST 루트까지의 최단 경로를 기준으로 내부 CIST 루트 브리지가 선택됩니다.

② CST (Common Spanning Tree)

CST는 각 MST 영역을 단일 스위치로 간주했을 때, 이러한 "단일 스위치"를 연결하는 스패닝 트리를 의미합니다. 그림의 영역 1, 2, 3과 STP 스위치가 네트워크의 CST를 구성하는 예를 보여줍니다.

③ IST (Internal Spanning Tree)

IST는 MST 영역 내에서 작동하는 스패닝 트리로, CIST의 일부를 형성합니다. 즉, IST와 CST가 결합되어 CIST를 구성합니다.

④ MSTI (Multiple Spanning Tree Instance)

일반적으로 No.0 스패닝 트리 인스턴스는 CIST를 지칭하며, 이는 네트워크 전체로 확장될 수 있습니다. No.1부터 시작하는 각 스패닝 트리 인스턴스는 특정 MST 영역에 속하며, 각 인스턴스에 여러 VLAN이 분배될 수 있습니다. 초기 상태에서는 모든 VLAN이 CIST에 할당됩니다.

19.7.4 포트 규정

MSTP에서 포트는 RSTP의 포트와 유사하게 다양한 역할을 수행할 수 있습니다.

① 루트 포트

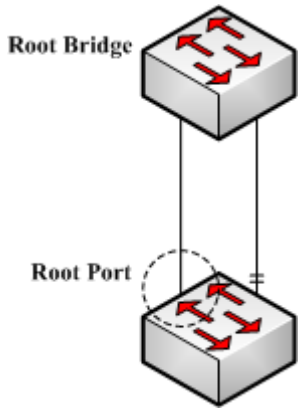


그림 12 루트포트

루트 포트는 현재 스위치와 루트 브리지를 연결하는 경로를 나타내며, 이 경로는 최소 루트 경로 비용을 가집니다.

② 대체 포트(Alternate Port)

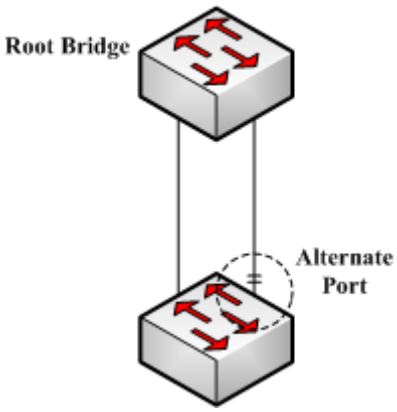


그림 13 대체 포트(Alternate Port)

대체 포트(Alternate Port)는 현재 스위치와 루트 브리지 간의 백업 경로를 제공합니다. 루트 포트가 장애로 인해 작동하지 않을 경우, 대체 포트는 신속하게 새로운 루트 포트로 전환되어 네트워크의 연속성을 유지합니다.

③ 지정 포트(Designated Port)

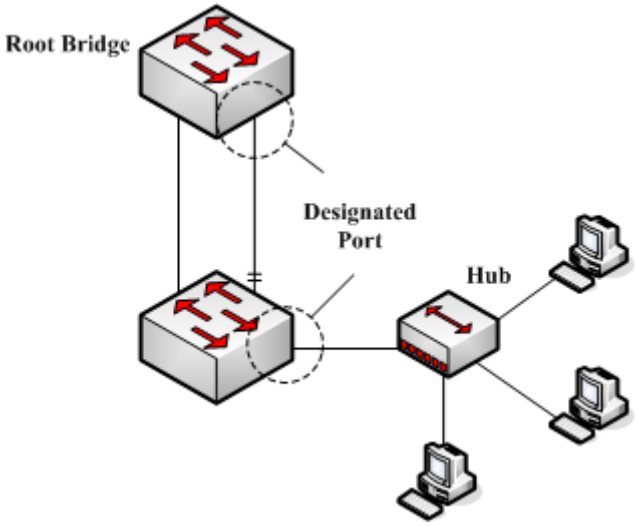


그림 14 지정 포트(Designated Port)

지정 포트(Designated Port)는 다음 영역의 스위치 또는 LAN을 연결할 수 있는 포트입니다. 이는 현재 LAN과 루트 브리지 간의 경로를 제공합니다.

④ 백업 포트

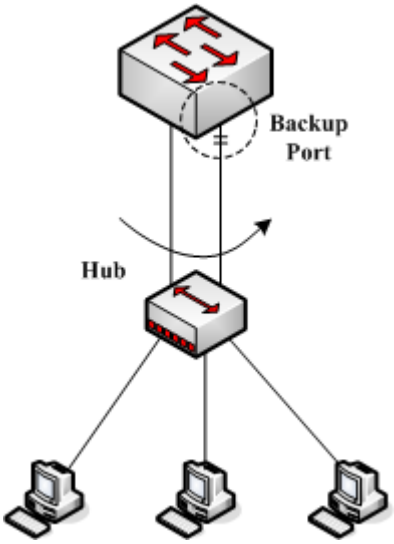


그림 15 백업 포트

두 스위치 포트가 직접 연결되거나 동일한 LAN에 연결된 경우, 우선순위가 낮은 포트가 백업 포트로 설정되고, 나머지 포트는 지정 포트로 설정됩니다. 지정 포트에 장애가 발생하면, 백업 포트가 지정 포트로 전환되어 작업을 계속합니다.

⑤ 마스터 포트

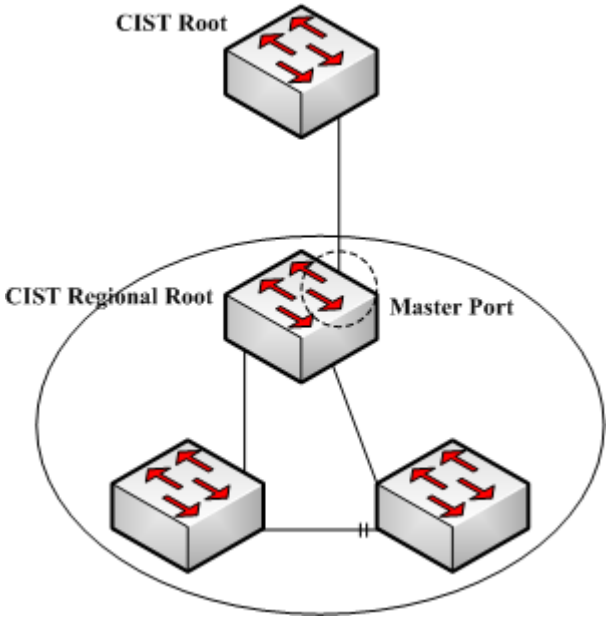


그림 16 마스터 포트

마스터 포트(Master Port)는 MST 영역과 CIST 루트 브리지 간의 최단 경로를 나타냅니다. 마스터 포트는 CIST 영역 내 루트 브리지의 루트 포트입니다.

⑥ 경계 포트(Boundary Port)

CIST와 각 MSTI에서 개념이 약간 다릅니다. MSTI에서 경계 포트는 해당 포트를 통해 스패닝 트리 인스턴스가 확장되지 않음을 의미합니다.

⑦ 엣지 포트

RSTP 또는 MSTP 프로토콜에서 엣지 포트(Edge Port)는 네트워크 호스트에 직접 연결되는 포트를 의미합니다. 이러한 포트는 네트워크에 루프를 유발하지 않고 즉시 Forwarding 상태로 전환될 수 있습니다.

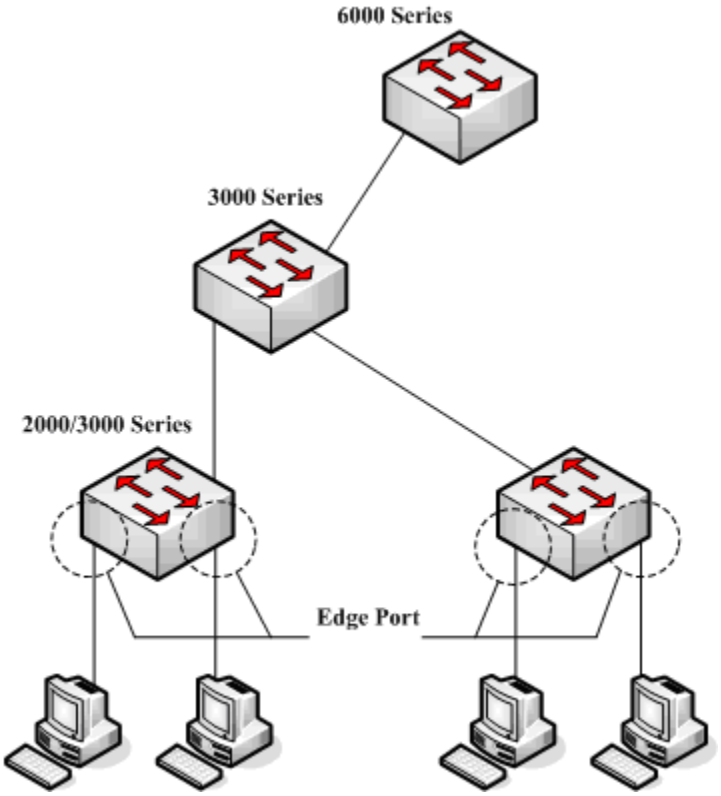


그림 17 엣지 포트

초기 상태에서 MSTP와 RSTP는 모든 포트를 엣지 포트로 간주하지 않으며, 이를 통해 네트워크 토폴로지가 신속하게 생성될 수 있도록 보장합니다. 이 상태에서 포트가 다른 스위치로부터 BPDU를 수신하면 해당 포트는 엣지 상태에서 일반 상태로 복원됩니다. 만약 포트가 802.1D STP BPDU를 수신하면, 포트는 Forwarding 상태로 전환되기 전에 두 배의 Forward Delay 시간을 대기해야 합니다.

19.7.5 MSTP BPDU

STP와 RSTP와 마찬가지로, MSTP를 실행하는 스위치들은 브리지 프로토콜 데이터 유닛(BPDU)을 통해 서로 통신할 수 있습니다. BPDU는 CIST와 MSTI에 대한 모든 구성 정보를 전달할 수 있습니다. 테이블 2.1과 테이블 2.2는 MSTP에서 사용되는 BPDU의 구조를 나타냅니다.

필드 이름	Byte Number
Protocol Identifier	1 - 2
Protocol Version Identifier	3
BPDU Type	4

CIST Flags	5
CIST Root Identifier	6 - 13
CIST External Root Path Cost	14 - 17
CIST Regional Root Identifier	18 - 25
CIST Port Identifier	26 - 27
Message Age	28 - 29
Max Age	30 - 31
Hello Time	32 - 33
Forward Delay	34 - 35
Version 1 Length	36
Version 3 Length	37 - 38
Format Selector	39
Configuration Name	40 - 71
Revision	72 - 73
Configuration Digest	74 - 89
CIST Internal Root Path Cost	90 - 93
CIST Bridge Identifier	94 - 101
CIST Remaining Hops	102
MSTI Configuration Messages	103 ~
MSTI FLAGS	1
MSTI Regional Root Identifier	2 - 9
MSTI Internal Root Path Cost	10 - 13
MSTI Bridge Priority	14
MSTI Port Priority	15
MSTI Remaining Hops	16

19.7.6 안정 상태 (Stable State)

MSTP 스위치는 수신된 BPDU를 기반으로 계산 및 비교 작업을 수행하며, 최종적으로 다음을 보장합니다:

① 네트워크 전체에서 하나의 스위치가 CIST 루트로 선택됩니다.

② 각 스위치와 LAN 세그먼트는 CIST 루트로의 최소 비용 경로를 결정하여 완전한 연결을 보장하고 루프를 방지합니다.

③ 각 MST 영역에서 하나의 스위치가 CIST 지역 루트로 선택됩니다. 이 스위치는 CIST 루트로의 최소 비용 경로를 가집니다.

④ 각 MSTI는 독립적으로 하나의 스위치를 MSTI 지역 루트로 선택할 수 있습니다.

⑤ 영역 내의 각 스위치와 LAN 세그먼트는 MSTI 루트로의 최소 비용 경로를 결정할 수 있습니다.

⑥ CIST의 루트 포트는 CIST 지역 루트와 CIST 루트 간의 최소 비용 경로를 제공합니다.

⑦ CIST의 지정 포트는 해당 LAN에 CIST 루트로의 최소 비용 경로를 제공합니다.

⑧ 대체 포트(Alternate Port)와 백업 포트(Backup Port)는 스위치, 포트 또는 LAN이 작동하지 않거나 제거된 경우 연결을 제공합니다.

⑨ MSTI의 루트 포트는 MSTI 지역 루트로의 최소 비용 경로를 제공합니다.

⑩ MSTI의 지정 포트는 MSTI 지역 루트로의 최소 비용 경로를 제공합니다.

⑪ 마스터 포트(Master Port)는 영역과 CIST 루트를 연결합니다. 영역 내에서 CIST 지역 루트의 CIST 루트 포트는 해당 영역 내 모든 MSTI의 마스터 포트 역할을 수행합니다.

19.7.7 홉 카운트 (Hop Count)

STP 및 RSTP와 달리, MSTP 프로토콜은 BPDU 구성 메시지에서 Message Age와 Max Age를 사용하여 네트워크 토폴로지를 계산하지 않습니다. 대신 MSTP는 Hop Count를 사용하여 네트워크 토폴로지를 계산합니다.

MSTP는 정보 루프를 방지하기 위해 각 스패닝 트리의 홉 카운트 속성과 전송 정보를 연결합니다. BPDU의 홉 카운트 속성은 CIST 지역 루트 또는 MSTI 지역 루트에 의해 지정되며, 각 수신 포트에서 감소합니다. 홉 카운트가 포트에서 0이 되면 해당 정보는 폐기되고, 포트는 지정 포트로 전환됩니다.

19.7.8 STP 호환성 (STP Compatibility)

MSTP는 프로토콜 변환 메커니즘을 통해 기존 STP 스위치와 함께 작동할 수 있습니다. 스위치의 한 포트가 STP 구성 메시지를 수신하면, 해당 포트는 STP 메시지만 전송하게 됩니다. 이와 동시에, STP 정보를 수신한 포트는 경계 포트(Boundary Port)로 간주됩니다.

참고 : 포트가 STP 호환 상태에 있을 경우, 더 이상 STP 메시지를 수신하지 않더라도 자동으로 MSTP 상태로 복원되지 않습니다. 이러한 경우, spanning-tree mstp migration-check 명령을 실행하여 포트가 학습한 STP 메시지를 지우고, 포트를 MSTP 상태로 복원할 수 있습니다.

RSTP 프로토콜을 실행하는 스위치는 MSTP 메시지를 인식하고 처리할 수 있습니다. 따라서 MSTP 스위치가 RSTP 스위치와 함께 작동할 때는 프로토콜 변환이 필요하지 않습니다.

19.8 MSTP 구성 작업 목록

- 기본 MSTP 구성
- MSTP 활성화 및 비활성화
- MSTP 영역 구성
- 네트워크 루트 구성
- 보조 루트 구성
- 브리지 우선 순위 설정
- STP 시간 매개변수 구성
- 네트워크 지름 구성
- 최대 홉 카운트 설정
- 포트 우선 순위 설정
- 포트의 경로 비용(Path Cost) 구성
- 엣지 포트 설정
- 포트 연결 유형 설정
- MST 호환 모드 활성화
- 프로토콜 변환 확인 재시작
- 포트 역할 제한 구성
- 포트 TCN 제한 구성
- MSTP 정보 확인

19.9 MSTP 구성 작업

19.9.1 기본 MSTP 구성

속성	기본 설정
STP mode	SSTP (PVST, RSTP, MSTP는 시작되지 않음).
Area name	MAC 주소의 문자열
Area edit level	0
MST configuration list	모든 VLAN이 CIST(MST00)에 매핑됨
Spanning-tree priority (CIST and all MSTI)	32768
Spanning-tree port priority (CIST and all MSTI)	128
Path cost of the spanning-tree port (CIST and all MSTI)	1000 Mbps: 20000 100 Mbps: 200000 10 Mbps: 2000000
Hello Time	2초
Forward Delay	15초
Maximum-aging Time	20초
Maximum hop count	20

19.9.2 MSTP 활성화 및 비활성화

STP 프로토콜은 기본적으로 PVST 또는 SSTP 모드에서 시작됩니다. 스패닝 트리가 필요하지 않은 경우 실행을 중단할 수 있습니다.

다음 명령어를 실행하여 STP를 MSTP 모드로 설정하십시오

명령어	설명
spanning-tree	기본 모드에서 STP 활성화
spanning-tree mode mstp	MSTP 활성화

다음 명령어를 실행하여 STP를 비활성화하십시오.

명령어	설명

no spanning-tree	STP 비활성화

19.9.3 MST 영역 구성

스위치가 속하는 MST 영역은 세 가지 속성에 따라 결정됩니다: 구성 이름, 수정 번호, VLAN과 MSTI 간의 매핑 관계. 영역 구성 명령을 통해 이 속성들을 설정할 수 있습니다. 이 세 가지 속성 중 하나라도 변경되면 스위치가 속한 MST 영역이 변경됩니다.

초기 상태에서는 MST 구성 이름이 스위치의 MAC 주소로 설정됩니다. 편집 번호는 0이고, 모든 VLAN이 CIST(MST00)에 매핑됩니다. 스위치마다 MAC 주소가 다르기 때문에, MSTP를 실행하는 스위치들은 초기 상태에서 서로 다른 영역에 속합니다.

명령어 spanning-tree mstp instance instance-id vlan vlan-list를 실행하여 새 MSTI를 생성하고 지정된 VLAN을 매핑할 수 있습니다. MSTI가 삭제되면 해당 VLAN은 다시 CIST로 매핑됩니다.

다음 명령어를 실행하여 MST 영역 정보를 설정하십시오

명령어	설명
spanning-tree mstp name *string*	MST 구성 이름을 설정합니다. 문자열은 최대 32자까지 가능하며 대소문자를 구분합니다. 기본값은 MAC 주소 문자열입니다.
no spanning-tree mstp name	MST 구성 이름을 기본값으로 복원합니다.
spanning-tree mstp revision *value*	MST 편집 번호를 설정합니다. 값은 0에서 65535 사이의 숫자로 설정할 수 있으며 기본값은 0입니다.
no spanning-tree mstp revision	MST 편집 번호를 기본값으로 복원합니다.
spanning-tree mstp instance *instance-id* **vlan** *vlan-list*	VLAN을 MSTI에 매핑합니다. MSTI 인스턴스 번호(instance-id)는 1에서 15 사이의 값으로 설정할 수 있습니다. VLAN 목록은 1에서 4094 사이의 VLAN 번호로 지정할 수 있습니다.
no spanning-tree mstp instance *instance-id*	MSTI의 VLAN 매핑을 취소하고 해당 스패닝 트리 인스턴스를 비활성화합니다.

다음 명령어를 실행하여 MSTP 영역의 설정을 확인하십시오

명령어	설명

show spanning-tree mstp region	MSTP 영역의 설정 정보를 확인합니다.

19.9.4 네트워크 루트 구성

MSTP에서는 각 스패닝 트리 인스턴스에 브리지 ID가 있으며, 이는 스위치의 우선 순위 값과 MAC 주소를 포함합니다. 스패닝 트리 토폴로지를 설정할 때 브리지 ID가 상대적으로 작은 스위치가 네트워크 루트로 선택됩니다.

MSTP를 통해 스위치를 네트워크 루트로 설정할 수 있습니다. 명령어 spanning-tree mstp instance-id root primary를 실행하면 스패닝 트리 인스턴스에서 스위치의 우선 순위 값을 기본값보다 충분히 작은 값으로 변경하여 해당 스위치가 스패닝 트리 인스턴스의 루트가 되도록 설정합니다. 일반적으로 이 명령이 실행되면 프로토콜이 현재 네트워크 루트의 브리지 ID를 자동으로 확인하고, 우선 순위 필드를 24576으로 설정하여 현재 스위치를 스패닝 트리의 루트로 만듭니다. 만약 네트워크 루트의 우선 순위 값이 24576보다 작으면, MSTP는 현재 브리지의 우선 순위를 루트의 우선 순위보다 4096만큼 작은 값으로 설정합니다. 여기서 4096은 네트워크 우선 순위 값의 단계 간격입니다. 루트를 설정할 때 diameter 하위 명령을 사용하여 스패닝 트리 네트워크의 네트워크 지름을 지정할 수 있습니다. 이 키워드는 스패닝 트리 인스턴스 ID가 0일 때만 유효합니다. 네트워크 지름이 설정되면 MSTP는 적절한 STP 시간 매개변수를 자동으로 계산하여 네트워크 수렴의 안정성을 보장합니다. 시간 매개변수에는 Hello Time, Forward Delay, Maximum Age가 포함됩니다. 기본 설정을 대체할 새로운 Hello Time을 설정하려면 hello-time 하위 명령을 사용할 수 있습니다.

다음 명령어를 실행하여 스위치를 네트워크 루트로 설정하십시오

명령어	설명
spanning-tree mstp *instance-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	지정된 스패닝 트리 인스턴스에서 스위치를 루트로 설정합니다. nstance-id: 스패닝 트리 인스턴스 번호로, 0에서 15 사이의 값을 가질 수 있습니다. net-diameter: 네트워크 지름을 나타내며 선택적 매개변수입니다. 인스턴스 ID가 0일 때만 유효하며, 2에서 7 사이의 값을 설정할 수 있습니다. seconds: Hello Time의 단위(초)로, 1에서 10 사이의 값을 설정할 수 있습니다.
no spanning-tree mstp *instance-id* **root**	스패닝 트리에서 스위치의 루트 구성을 취소합니다.

다음 명령어를 실행하여 MSTP 메시지를 확인하십시오.

명령어	설명
show spanning-tree mstp [**instance** *instance-id*]	MSTP 메시지를 확인합니다.

19.9.5 보조 루트 구성 (Secondary Root)

네트워크 루트를 설정한 후, 명령어 spanning-tree mstp instance-id root secondary를 실행하여 하나 이상의 스위치를 보조 루트 또는 백업 루트로 설정할 수 있습니다. 루트가 특정 이유로 작동하지 않을 경우, 보조 루트가 네트워크 루트로 전환됩니다.

기본 루트 설정과는 달리, 기본 루트를 설정하는 명령이 실행되면 MSTP는 스위치의 스패닝 트리 우선 순위를 28672로 설정합니다. 다른 스위치의 우선 순위 값이 기본값 32768인 경우, 현재 스위치는 보조 루트가 될 수 있습니다.

보조 루트를 구성할 때 diameter 및 hello-time 하위 명령을 사용하여 STP 시간 매개변수를 업데이트할 수 있습니다. 보조 루트가 기본 루트로 전환되어 작동을 시작하면, 이 매개변수들이 활성화됩니다.

다음 명령어를 실행하여 보조 루트 구성을 확인하십시오.

명령어	설명
spanning-tree mstp *instance-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	지정된 스패닝 트리 인스턴스에서 스위치를 보조 루트로 설정합니다. instance-id: 스패닝 트리 인스턴스 번호로, 0 에서 15 사이의 값을 설정할 수 있습니다. net-diameter: 네트워크 지름을 나타내며 선택적 매개변수입니다. 인스턴스 ID 가 0 일 때만 유효하며, 2 에서 7 사이의 값을 설정할 수 있습니다. seconds: Hello Time 의 단위(초)로, 1 에서 10 사이의 값을 설정할 수 있습니다.
no spanning-tree mstp *instance-id* **root**	스패닝 트리에서 스위치의 루트 구성을 취소합니다.

다음 명령어를 실행하여 MSTP 메시지를 확인하십시오.

명령어	설명
show spanning-tree mstp [**instance** *instance-id*]	MSTP 메시지를 확인합니다.

19.9.6 브리지 우선순위 구성

특정 상황에서는 브리지 우선순위를 직접 설정하여 스위치를 네트워크 루트로 지정할 수 있습니다. 이 경우, root 하위 명령을 실행하지 않고도 스위치를 네트워크 루트로 설정할 수 있습니다. 스패닝 트리 인스턴스마다 스위치의 우선순위 값은 독립적이기 때문에 각 인스턴스에서 개별적으로 우선순위를 설정할 수 있습니다.

브리지 우선순위 설정 명령어

명령어	설명
spanning-tree mstp *instance-id* **priority** *value*	스패닝 트리 인스턴스에서 스위치의 우선순위를 설정합니다. instance-id: 스패닝 트리 인스턴스 번호로, 0 에서 15 사이의 값을 설정할 수 있습니다. value: 브리지 우선순위를 나타내며, 다음 값 중 하나로 설정할 수 있습니다: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440
no spanning-tree mstp *instance-id* **priority**	스위치의 브리지 우선순위를 기본값으로 복원합니다. instance-id: 스패닝 트리 인스턴스 번호로, 0 에서 15 사이의 값을 설정할 수 있습니다.

19.9.7 STP 시간 매개변수 구성

다음은 STP 시간 매개변수입니다:

- Hello Time:

  스위치가 네트워크 루트로 동작할 때, 지정된 포트에 구성 메시지를 전송하는 간격입니다.

- Forward Delay:

  포트가 Blocking 상태에서 Learning 상태로, 그리고 Forwarding 상태로 전환될 때 필요한 시간입니다.

- Max Age:

  스패닝 트리 구성 정보가 유효한 최대 기간입니다.

네트워크 토폴로지 충격을 줄이기 위해 다음 요구사항을 충족해야 합니다

17. 2 x (fwd_delay - 1.0) >= max_age

- max_age >= (hello_time + 1) x 2

다음 명령어를 실행하여 다중 스패닝 트리 프로토콜의 시간 매개변수를 설정하십시오

명령어	설명
spanning-tree mstp hello-time *seconds*	Hello Time 매개변수를 설정합니다. 초 단위 값은 1 에서 10 사이이며 기본값은 2 초입니다.
no spanning-tree mstp hello-time	Hello Time 을 기본값으로 복원합니다.
spanning-tree mstp forward-time *seconds*	Forward Delay 매개변수를 설정합니다. 초 단위 값은 4 에서 30 사이이며 기본값은 15 초입니다.
no spanning-tree mstp forward-time	Forward Delay 를 기본값으로 복원합니다.
spanning-tree mstp max-age *seconds*	Max Age 매개변수를 설정합니다. 초 단위 값은 6 에서 40 사이이며 기본값은 20 초입니다.
no spanning-tree mstp max-age	Max Age 를 기본값으로 복원합니다.

권장 사항 : STP 시간 매개변수는 루트 또는 네트워크 지름을 설정하여 수정하는 것이 좋습니다. 이렇게 하면 시간 매개변수가 정확하게 수정됩니다.

새로 설정된 시간 매개변수는 공식 요구사항을 충족하지 않더라도 유효하며, 구성 중 콘솔에 표시되는 알림에 주의하십시오.

19.9.8 네트워크 Diameter 구성

네트워크 Diameter는 네트워크에서 두 호스트 사이의 최대 스위치 수를 나타내며, 네트워크의 규모를 의미합니다.

명령어 spanning-tree mstp diameter net-diameter를 실행하여 MSTP 네트워크 지름을 설정할 수 있습니다. 매개변수 net-diameter는 CIST에만 유효합니다. 설정 후, 세 가지 STP 시간 매개변수 (Hello Time, Forward Delay, Max Age)가 자동으로 더 적절한 값으로 업데이트됩니다.

다음 명령어를 실행하여 네트워크 Diameter 를 설정하십시오

명령어	설명
spanning-tree mstp diameter *net-diameter*	네트워크(net-diameter)을 설정합니다 net-diameter: 네트워크 지름을 나타내며, 2 에서 7 사이의 값을 가질 수 있습니다. 기본값은 7 입니다.
no spanning-tree mstp diameter	기본값으로 복원합니다.

net-diameter 매개변수는 스위치에 독립적인 설정으로 저장되지 않습니다. 시간 매개변수는 네트워크 지름을 설정할 때 수정되어야만 저장됩니다.

19.9.9 최대 홉 수 구성

다음 명령어를 실행하여 최대 홉 수를 설정하십시오.

명령어	설명
spanning-tree mstp max-hops *hop-count*	최대 홉 수를 설정합니다. hop-count: 최대 홉 수를 나타내며, 1 에서 40 사이의 값을 가질 수 있습니다. 기본값은 20 입니다.
no spanning-tree mstp *hop-count*	최대 홉 수를 기본값으로 복원합니다.

19.9.10 포트 우선순위 설정

스위치의 두 포트 간에 루프가 발생하면, 더 높은 우선순위를 가진 포트가 Forwarding 상태로 전환되고, 낮은 우선순위를 가진 포트는 차단됩니다. 만약 모든 포트가 동일한 우선순위를 가진 경우, 포트 번호가 더 작은 포트가 우선적으로 Forwarding 상태로 전환됩니다.

명령어	설명
spanning-tree mstp *instance-id* **port-priority** *priority*	특정 스패닝 트리 인스턴스의 STP 포트 우선순위를 설정합니다. instance-id: 스패닝 트리 인스턴스 번호(0 ~ 15) priority: 포트 우선순위 값(0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240)
spanning-tree port-priority *value*	모든 스패닝 트리 인스턴스의 포트 우선순위를 설정합니다. value: 포트 우선순위 값(0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240)
no spanning-tree mstp *instance-id* **port-priority**	특정 스패닝 트리 인스턴스의 포트 우선순위를 기본값으로 복원합니다.
no spanning-tree port-priority	모든 스패닝 트리 인스턴스의 포트 우선순위를 기본값으로 복원합니다.

19.9.11 포트 경로 비용 설정

MSTP에서 포트의 경로 비용(Path Cost)은 기본적으로 연결 속도를 기준으로 설정됩니다. 두 스위치 간에 루프가 발생하면, 경로 비용이 적은 포트가 Forwarding 상태로 전환됩니다. 경로 비용이 적을수록 포트 속도는 더 높습니다. 모든 포트의 경로 비용이 동일한 경우, 포트 번호가 작은 포트가 우선적으로 Forwarding 상태로 전환됩니다.

포트 구성 모드에서 다음 명령을 실행하여 포트의 경로 비용을 설정하십시오

명령어	설명

spanning-tree mstp *instance-id* **cost** *cost*	특정 스패닝 트리 인스턴스에서 포트의 경로 비용을 설정합니다. instance-id: 스패닝 트리 인스턴스 번호(0 ~ 15) cost: 포트 경로 비용(1 ~ 200000000)
spanning-tree cost *value*	모든 스패닝 트리 인스턴스에서 포트의 경로 비용을 설정합니다. value: 포트 경로 비용(1 ~ 200000000)
no spanning-tree mstp *instance-id* **cost**	특정 스패닝 트리 인스턴스에서 포트 경로 비용을 기본값으로 복원합니다.
no spanning-tree cost	모든 스패닝 트리 인스턴스에서 포트 경로 비용을 기본값으로 복원합니다.

19.9.12 엣지 포트 설정

엣지 포트는 네트워크의 단말 장치와 연결되는 포트를 의미합니다. 강제 엣지 포트는 링크가 활성화(Link Up)되자마자 즉시 Forwarding 상태로 전환됩니다.

포트 구성 모드에서 다음 명령을 사용하여 MSTP의 엣지 포트를 설정하십시오

명령어	설명
spanning-tree mstp edge	포트를 엣지 포트로 설정합니다.
no spanning-tree mstp edge	엣지 포트의 기본 자동 확인 상태로 복원합니다.

19.9.13 포트 연결 유형 설정

MSTP를 지원하는 스위치 간의 연결이 포인트-투-포인트(Point-to-Point) 방식의 직접 연결일 경우, 스위치들은 핸드셰이크 메커니즘을 통해 빠르게 연결을 설정할 수 있습니다. 포트 연결 유형을 구성할 때, 포트 연결을 포인트-투-포인트 유형으로 설정해야 합니다.

프로토콜은 포트의 듀플렉스 속성에 따라 포인트-투-포인트 연결 여부를 결정합니다.

- 포트가 전이중(Full-Duplex) 모드로 동작하면, 프로토콜은 해당 연결을 포인트-투-포인트로 간주합니다.
- 포트가 반이중(Half-Duplex) 모드로 동작하면, 프로토콜은 해당 연결을 공유(Shared) 연결로 간주합니다.

포트가 RSTP 또는 MSTP 프로토콜을 실행하는 스위치와 연결된 경우, 포트 연결 유형을 포인트-투-포인트로 설정하여 핸드셰이크가 신속하게 설정되도록 보장할 수 있습니다.

포트 구성 모드에서 다음 명령을 실행하여 포트 연결 유형을 설정하십시오.

명령어	설명

spanning-tree mstp point-to-point force-true	포트 연결 유형을 포인트-투-포인트로 설정합니다.
spanning-tree mstp point-to-point force-false	포트 연결 유형을 공유로 설정합니다.
spanning-tree mstp point-to-point auto	포트 연결 유형을 자동으로 확인합니다.
no spanning-tree mstp point-to-point	포트 연결 유형을 기본 설정으로 복원합니다.

19.9.14 MST-호환 모드 활성화

스위치에서 지원하는 MSTP 프로토콜은 IEEE 802.1s를 기반으로 합니다. 다른 MSTP, 특히 Cisco 스위치에서 지원하는 MSTP와 호환되기 위해 MSTP 프로토콜은 MST-호환 모드에서 작동할 수 있습니다. MST-호환 모드에서 실행 중인 스위치는 다른 MSTP의 메시지 구조를 식별하고, 포함된 MST 지역 식별자를 확인하며, MST 지역을 설정할 수 있습니다.

MST-호환 모드와 STP-호환 모드는 MSTP 프로토콜 변환 메커니즘에 기반합니다. 스위치의 포트가 호환 모드에서 BPDU를 수신하면 해당 포트는 자동으로 호환 모드로 전환되며, BPDU를 호환 모드로 전송합니다. 포트를 표준 MST 모드로 복원하려면 spanning-tree mstp migration-check 명령어를 실행하십시오.

글로벌 구성 모드에서 다음 명령어를 실행하여 MST-호환 모드를 활성화하거나 비활성화할 수 있습니다 .

명령어	설명
spanning-tree mstp mst-compatible	스위치의 MST-호환 모드를 활성화합니다.
no spanning-tree mstp mst-compatible	스위치의 MST-호환 모드를 비활성화합니다.

참고: 호환 모드의 주요 기능은 스위치와 다른 MSTP 실행 스위치를 위한 MST 영역을 생성하는 것입니다. 실제 네트워크 환경에서 스위치가 동일한 구성 이름(configuration name)과 수정 번호(revision number)를 가지도록 설정해야 합니다. 다른 MSTP 프로토콜을 실행하는 스위치를 CIST 루트로 구성하는 것이 권장되며, 이를 통해 스위치가 메시지를 수신하여 호환 모드로 전환될 수 있습니다.

MST-호환 모드가 활성화되지 않으면 스위치는 BPDU-호환 메시지를 완전히 해석하지 않고 일반 RSTP BPDU로 처리합니다. 이로 인해 스위치는 연결된 MST-호환 스위치와 동일한 영역에 포함되지 않을 수 있습니다.

호환 모드에 있는 포트는 글로벌 구성 모드에서 호환 모드를 비활성화하더라도 표준 MST BPDU 전송으로 자동 복원되지 않습니다. 이 경우 migration-check 명령어를 실행하여 수동으로 복원해야 합니다.

19.9.15 프로토콜 변환 검사 재시작

MSTP는 프로토콜 변환 메커니즘을 통해 스위치가 기존 STP 스위치와 함께 작동할 수 있도록 지원합니다. 스위치의 한 포트가 STP 구성 메시지를 수신하면 해당 포트는 STP 메시지만 전송하게 됩니다. 이때 STP 정보를 수신한 포트는 경계 포트로 간주됩니다.

참고: 포트가 STP-호환 상태에 있을 때, 해당 포트가 더 이상 STP 메시지를 수신하지 않아도 MSTP 상태로 자동 복원되지 않습니다. 이 경우 spanning-tree mstp migration-check 명령어를 실행하여 포트가 학습한 STP 메시지를 지우고 MSTP 상태로 복원할 수 있습니다.

RSTP 프로토콜을 실행하는 스위치는 MSTP 메시지를 식별하고 처리할 수 있습니다. 따라서 MSTP 스위치가 RSTP 스위치와 함께 작동할 때는 프로토콜 변환이 필요하지 않습니다.

글로벌 구성 모드에서 스위치의 모든 포트에서 감지된 STP 정보를 지우려면 다음 명령어를 실행하십시오.

명령어	설명
spanning-tree mstp migration-check	스위치의 모든 포트에서 감지된 STP 정보를 지웁니다.

포트 구성 모드에서 해당 포트에서 감지된 STP 정보를 지우려면 다음 명령어를 실행하십시오.

명령어	설명
spanning-tree mstp migration-check	해당 포트에서 감지된 STP 정보를 지웁니다.

19.9.16 포트 역할 제한 설정

포트 역할 제한을 설정하면 해당 포트가 루트 포트로 선택되지 않도록 설정할 수 있습니다.

포트 구성 모드에서 다음 명령어를 사용하여 포트 역할 제한을 설정합니다.

명령어	설명
spanning-tree mstp restricted-role	포트가 루트 포트로 선택되지 않도록 설정합니다.

19.9.17 포트 TCN 제한 설정

포트의 TCN(Topology Change Notification) 제한을 설정하면 해당 포트가 토폴로지 변경 정보를

다른 포트로 전파하지 않도록 설정할 수 있습니다.

포트 구성 모드에서 다음 명령어를 사용하여 포트 TCN 제한을 설정합니다:

명령어	설명
spanning-tree mstp restricted-tcn	포트가 토폴로지 변경 정보를 다른 포트로 전파하지 않도록 설정합니다.

19.9.18 MSTP 정보 확인

모니터 명령어, 글로벌 구성 명령어 또는 포트 구성 명령어에서 다음 명령어를 실행하여 MSTP 정보를 확인할 수 있습니다.

명령어	설명
show spanning-tree	포트가 토폴로지 변경 정보를 다른 포트로 전파하지 않도록 설정합니다.
show spanning-tree detail	MSTP 세부 정보를 확인합니다. (SSTP, PVST, RSTP, MSTP 정보도 확인 가능)
show spanning-tree interface *interface-id*	STP 인터페이스 정보를 확인합니다. (SSTP, PVST, RSTP, MSTP 정보도 확인 가능)
show spanning-tree mstp	모든 MST 인스턴스를 확인합니다.
show spanning-tree mstp region	MST 지역 구성을 확인합니다.
show spanning-tree mstp instance *instance-id*	특정 MST 인스턴스 정보를 확인합니다.
show spanning-tree mstp detail	MST 세부 정보를 확인합니다.
show spanning-tree mstp interface *interface-id*	MST 포트 구성을 확인합니다.
show spanning-tree mstp protocol-migration	포트의 프로토콜 변환 상태를 확인합니다.

19.10 STP 선택적 특성 소개

스위치의 스패닝 트리 프로토콜 모듈은 7개의 추가 기능(선택적 기능이라고 함)을 지원합니다. 이러한 기능은 기본적으로 구성되어 있지 않습니다. 각 스패닝 트리 프로토콜 모드에서 선택적 특성에 대한 지원 조건은 아래와 같습니다.

Optional Characteristic	Single STP	PVST	RSTP	MSTP
Port Fast	Yes	Yes	No	No
BPDU Guard	Yes	Yes	Yes	Yes

BPDU Filter	Yes	Yes	No	No
Uplink Fast	Yes	Yes	No	No
Backbone Fast	Yes	Yes	No	No
Root Guard	Yes	Yes	Yes	Yes
Loop Guard	Yes	Yes	Yes	Yes

19.10.1 포트 패스트(Port Fast)

Port Fast는 액세스 또는 트렁크 포트로 구성된 인터페이스가 차단 상태에서 전송 상태로 즉시 전환되도록 하며, 청취(Listening) 및 학습(Learning) 상태를 우회합니다. 이 기능은 단일 워크스테이션 또는 서버에 연결된 인터페이스에서 사용할 수 있으며, 해당 장치가 스패닝 트리의 수렴을 기다리지 않고 네트워크에 즉시 연결할 수 있도록 합니다.

단일 워크스테이션 또는 서버에 연결된 인터페이스는 브리지 프로토콜 데이터 단위(BPDU)를 수신하지 않아야 합니다. Port Fast가 활성화된 인터페이스는 스위치가 재시작될 때 스패닝 트리 상태 변경의 정상적인 사이클을 거칩니다. Port Fast가 스위치에 연결된 포트에 구성된 경우, 루프가 생성될 가능성이 있습니다.

Port Fast 기능은 글로벌 구성 모드 또는 포트 구성 모드에서 설정할 수 있습니다.

글로벌 모드에서 구성하면 모든 포트가 Port Fast 포트로 간주되어 빠르게 전송 상태로 전환됩니다. 그러나 이 경우 루프가 생성될 가능성이 더 커질 수 있습니다. 네트워크 루프가 생성되지 않도록 Port Fast 기능을 설정할 때는 BPDU Guard 또는 BPDU Filter 기능을 사용하여 포트를 보호할 수 있습니다.

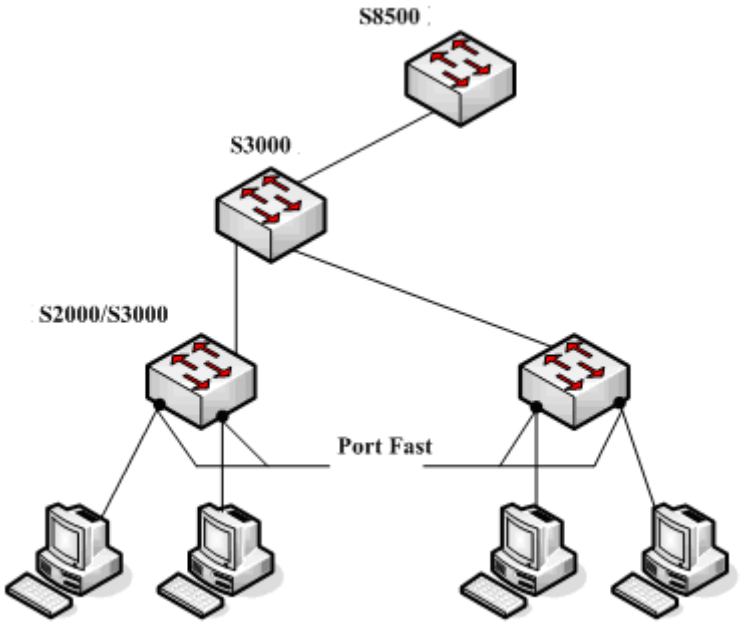


그림 18 Port Fast

참고 : 빠른 수렴을 제공하는 스패닝 트리 프로토콜인 RSTP 및 MSTP는 인터페이스를 즉시 전송 상태로 전환할 수 있으므로 Port Fast 기능을 사용할 필요가 없습니다.

19.10.2 BPDU Guard

Port Fast가 활성화된 포트가 BPDU를 수신하면, 이는 네트워크 구성에 문제가 있음을 나타낼 수 있습니다. BPDU Guard 기능은 포트가 BPDU를 수신한 후 이를 수동적으로 보호합니다.

BPDU Guard는 스패닝 트리 프로토콜에 따라 다르게 작동합니다. SSTP/PVST 모드에서는 BPDU Guard가 활성화된 Port Fast 포트가 BPDU를 수신하면 해당 포트는 강제로 종료(shutdown)되며, 사용자가 수동으로 복구를 구성해야만 다시 활성화할 수 있습니다.

RSTP/MSTP 모드에서는 BPDU Guard가 설정된 일반 포트가 BPDU를 수신하면 일정 시간 동안 차단(Blocking) 상태로 전환됩니다.

BPDU Guard는 Port Fast 없이 독립적으로 구성할 수 있습니다. 모든 스패닝 트리 프로토콜 모드에서 BPDU Guard가 설정된 포트는 여전히 BPDU를 전송하고, BPDU를 수신 및 처리합니다. RSTP/MSTP 모드에서는 포트에 BPDU Guard를 설정하면 스위치에 연결된 장치가 BPDU를 수신하지 못하도록 방지할 수 있습니다. BPDU Guard는 글로벌 또는 포트 모드에서 구성할 수 있습니다. 글로벌 모드에서는 spanning-tree portfast bpduguard 명령어를 사용해도 포트에서 BPDU 전송을 막을 수는 없습니다. 복잡한 네트워크에서 BPDU Guard 기능을 잘못 사용하면 루프가 발생할 수 있으므로 주의가 필요합니다.

19.10.3 BPDU 필터

BPDU 필터링 기능은 스위치에서 전역으로 활성화하거나 각 인터페이스별로 활성화할 수 있습니다. 그러나 이 기능은 활성화 방식에 따라 작동 방식에 차이가 있습니다.

SSTP/PVST 모드에서는 BPDU 필터가 구성된 Port Fast 포트가 BPDU를 수신하면, 해당 포트의 BPDU 필터와 Port Fast 기능이 자동으로 비활성화되며, 포트는 일반 포트로 복원됩니다. 포트가 전송(Forwarding) 상태에 도달하기 전에 청취(Listening) 상태와 학습(Learning) 상태를 거쳐야 합니다. BPDU 필터는 글로벌 구성 모드 또는 포트 구성 모드에서 설정할 수 있습니다. 글로벌 구성 모드에서는 spanning-tree portfast bpdufilter 명령어를 실행하여 모든 포트가 BPDU를 전송하지 못하도록 차단할 수 있습니다. 그러나 포트는 계속 BPDU를 수신하고 처리할 수 있습니다.

19.10.4 Uplink Fast

업링크 패스트(Uplink Fast) 기능은 스위치와 루트 브리지 간의 연결이 끊어졌을 때 새로운 루트 포트가 빠르게 전송(Forwarding) 상태로 전환되도록 합니다.

복잡한 네트워크는 항상 여러 계층의 장치를 포함하며, 그림 2에 나타난 것처럼 스위치의 집계 계층(Aggregation Layer)과 액세스 계층(Access Layer)은 상위 계층과 중복 연결을 가지고 있습니다. 이러한 중복 연결은 루프를 방지하기 위해 STP에 의해 일반적으로 차단됩니다.

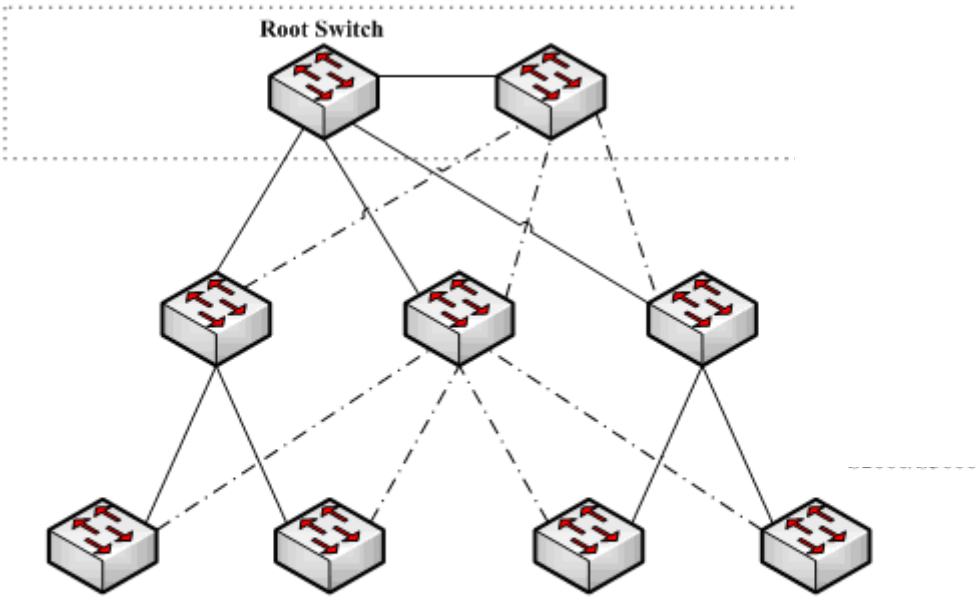


그림 19 스위치 네트워크 토폴로지

스위치와 상위 계층 간의 연결이 끊어졌다고 가정해 봅시다(이를 "직접 링크 장애(Direct Link Failure)"라고 합니다). 이 경우 STP는 중복 라인에서 대체 포트(Alternate Port)를 루트 포트로 선택합니다. 하지만 대체 포트가 전송(Forwarding) 상태로 전환되기 전에 청취(Listening) 상태와 학습(Learning) 상태를 거쳐야 합니다.

만약 글로벌 구성 모드에서 spanning-tree uplinkfast 명령어를 실행하여 Uplink Fast 기능이 구성되어 있다면, 새로운 루트 포트가 직접 전송 상태로 전환되어 스위치와 상위 계층 간의 연결이 신속하게 복원됩니다.

그림 3은 Uplink Fast 기능의 작동 원리를 보여줍니다. 스위치 C가 스위치 B와 연결하는 포트는 초기 상태에서는 대기 포트(Standby Port)로 설정됩니다. 스위치 C와 루트 스위치 A 간의 연결이 끊어지 이전의 대체 포트가 새로운 루트 포트로 선택되고 즉시 전송을 시작합니다.

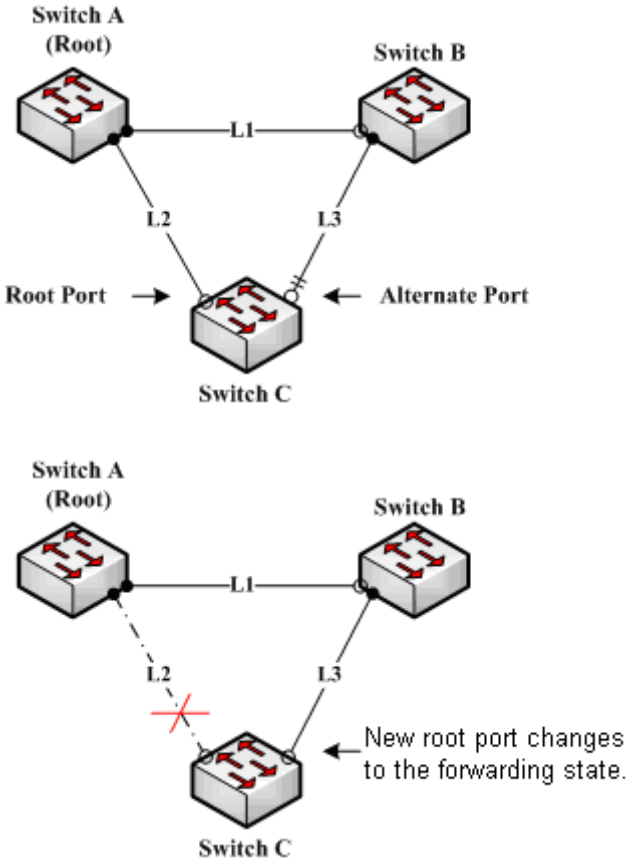


그림 20 Uplink Fast

참고 : Uplink Fast 기능은 느리게 수렴하는 SSTP 및 PVST에 적합합니다. RSTP와 MSTP 모드에서는 Uplink Fast 기능 없이도 새로운 루트 포트가 빠르게 전송(Forwarding) 상태로 전환될 수 있습니다.

19.10.5 Backbone Fast

백본 패스트(Backbone Fast) 기능은 업링크 패스트(Uplink Fast) 기술을 보완하는 역할을 합니다. 업링크 패스트 기술은 지정된 스위치로의 직접 연결이 끊어졌을 때 중복 연결이 신속히 작동하도록 합니다. 반면, 백본 패스트 기술은 상위 계층 네트워크에서 간접 링크의 네트워크 단절을 감지하고 포트 상태 변경을 가속화합니다.

그림 4에서 스위치 C와 루트 스위치 A 간의 L2 연결은 스위치 C와 루트 스위치 A 간의 직접 링크로 간주됩니다. 이 연결이 끊어지면 업링크 패스트 기능으로 문제를 해결할 수 있습니다. 스위치 A와 스위치 B 간의 L1 연결은 스위치 C의 간접 링크로 간주됩니다. 간접 링크가 끊어진 경우 이를 간접 장애(Indirect Failure)라고 하며, 이는 백본 패스트 기능에 의해 처리됩니다.

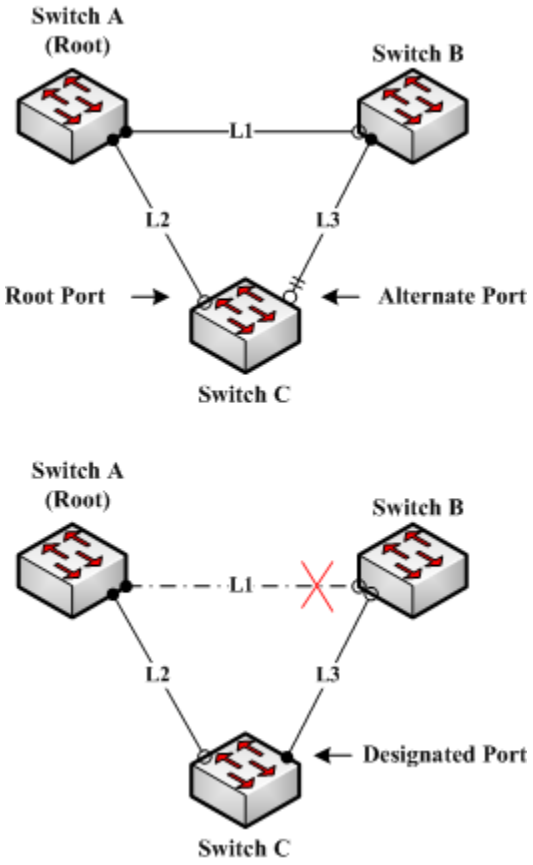


그림 21 Backbone Fast

스위치 C의 브리지 우선순위가 스위치 B보다 높다고 가정해 봅시다. L1이 끊어졌을 때, 스위치 B는 브리지 우선순위가 루트 우선순위로 사용되므로 스위치 C로 BPDU를 전송하는 스위치로 선택됩니다. 그러나 스위치 C는 BPDU에 포함된 정보가 자신의 정보보다 우선하지 않다고 판단합니다.

백본 패스트(Backbone Fast)가 활성화되지 않은 경우, 스위치 C와 스위치 B 간의 포트는 브리지 정보를 기다리는 동안 타이머 만료(Aging) 후 지정 포트(Designated Port)로 전환됩니다. 이 과정은 일반적으로 몇 초가 걸립니다.

글로벌 구성 모드에서 spanning-tree backbonefast 명령어를 실행하여 백본 패스트 기능이 설정된 경우, 스위치 C의 대체 포트(Alternate Port)가 더 낮은 우선순위를 가진 BPDU를 수신하면, 스위치 C는 해당 포트의 간접 링크 및 루트 스위치로 연결된 경로가 끊어졌다고 간주합니다. 스위치 C는 정보 만료를 기다리지 않고 해당 포트를 즉시 지정 포트로 업데이트합니다.

백본 패스트 기능이 활성화된 후, 낮은 우선순위의 BPDU가 다른 포트에서 수신되면 스위치는 다음과 같은 동작을 수행합니다

- 대체 포트가 메시지를 수신한 경우, 해당 포트는 지정 포트로 업데이트됩니다.
- 루트 포트가 낮은 우선순위의 메시지를 수신했으며 대기 포트가 없는 경우, 스위치는 루트 스위치로 전환됩니다.

주의할 점은 백본 패스트 기능이 정보 만료(Aging) 시간을 단축할 뿐이라는 점입니다. 새로운 지정 포트는 상태 변경 순서를 따라야 하며, 청취(Listening) 상태, 학습(Learning) 상태를 거쳐 최종적으로 전송(Forwarding) 상태로 전환됩니다.

참고 : 백본 패스트 기능은 업링크 패스트(Uplink Fast)와 유사하게 SSTP 및 PVST 모드에서만 효과적입니다.

19.10.6 루트가드

루트 가드 기능은 높은 우선순위의 BPDU를 수신하여 포트가 루트 포트로 전환되는 것을 방지합니다.

서비스 제공자(SP)의 2계층 네트워크는 SP가 소유하지 않은 스위치와의 여러 연결을 포함할 수 있습니다. 이러한 토폴로지에서는 스패닝 트리가 재구성되어 고객 네트워크의 스위치를 루트 스위치로 선택할 가능성이 있습니다(그림 17-8 참조). SP 스위치의 고객 네트워크 연결 인터페이스에서 루트 가드를 활성화하면 이러한 상황을 방지할 수 있습니다.

스패닝 트리 계산으로 인해 고객 네트워크의 인터페이스가 루트 포트로 선택되면, 루트 가드는 해당 인터페이스를 루트 불일치(root-inconsistent, 차단) 상태로 전환하여 고객 스위치가 루트 스위치가 되거나 루트로 가는 경로에 포함되지 않도록 합니다. 네트워크 외부의 스위치가 루트 스위치가 되면, 해당 인터페이스는 차단 상태(root-inconsistent)가 되며 스패닝 트리는 새로운 루트 스위치를 선택합니다. 고객의 스위치는 루트 스위치가 되지 않으며 루트로 가는 경로에도 포함되지 않습니다.

MST(Multiple Spanning-Tree) 모드에서 스위치가 작동 중인 경우, 루트 가드는 해당 인터페이스를 지정 포트로 강제 설정합니다. 루트 가드로 인해 내부 스패닝 트리(IST) 인스턴스에서 경계 포트

가 차단되면, 해당 인터페이스는 모든 MST 인스턴스에서도 차단됩니다. 경계 포트(boundary port)는 IEEE 802.1D 스위치 또는 다른 MST 지역 구성을 가진 스위치와 연결된 LAN에 연결된 인터페이스를 의미합니다. 루트 가드가 활성화된 인터페이스는 해당 인터페이스가 속한 모든 VLAN에 적용됩니다. VLAN은 그룹화되어 MST 인스턴스에 매핑될 수 있습니다.

이 기능은 spanning-tree guard root 인터페이스 구성 명령어를 사용하여 활성화할 수 있습니다.

참고 : 루트 가드 기능은 SSTP/PVST와 RSTP/MSTP 모드에서 다르게 동작하며 STP/PVST 모드에서는 루트 포트가 항상 루트 가드에 의해 차단됩니다. RSTP/MSTP 모드에서는 높은 수준의 BPDU를 수신해야 루트 포트가 차단됩니다. 이전에 루트 역할을 수행했던 포트는 차단되지 않습니다.

루프 가드는 단방향 링크로 인해 대체 포트(Alternate Port) 또는 루트 포트(Root Port)가 지정 포트(Designated Port)로 전환되는 것을 방지합니다. 이 기능은 스위치 네트워크 전체에서 활성화했을 때 가장 효과적입니다. 루프 가드는 대체 포트와 루트 포트가 지정 포트로 전환되는 것을 방지하며, 스패닝 트리는 루트 포트 또는 대체 포트에서 BPDU를 전송하지 않습니다.

이 기능은 spanning-tree loopguard default 글로벌 구성 명령어를 사용하여 활성화할 수 있습니다.

- VST+ 또는 Rapid-PVST+ 모드에서 스위치가 작동 중인 경우, 루프 가드는 대체 포트와 루트 포트가 지정 포트로 전환되는 것을 방지하며, 스패닝 트리는 루트 포트나 대체 포트에서 BPDU를 전송하지 않습니다.
- MST 모드에서 루프 가드가 모든 MST 인스턴스에서 인터페이스를 차단한 경우, 비경계 포트(Nonboundary Port)에서는 BPDU가 전송되지 않습니다. 경계 포트(Boundary Port)에서는 루프 가드가 인터페이스를 모든 MST 인스턴스에서 차단합니다.

참고 : 루프 가드 기능은 SSTP/PVST와 RSTP/MSTP 모드에서 다르게 작동합니다. SSTP/PVST 모드에서는 지정 포트가 항상 루프 가드에 의해 차단됩니다. RSTP/MSTP 모드에서는 BPDU 수신이 불가능하여 지정 포트로 전환될 때만 포트가 차단됩니다.루프 가드는 낮은 우선순위의 BPDU를 수신하여 지정 역할을 부여받은 포트를 차단하지 않습니다.

19.11 STP 선택적 특성 구성

19.11.1 STP 선택적 특성 구성 작업

- Port Fast 구성
- BPDU Guard 구성
- BPDU Filter 구성
- Uplink Fast 구성

- Backbone Fast 구성
- Root Guard 구성
- Loop Guard 구성
- Loop Fast 구성
- Address Table Aging 보호 구성
- FDB-Flush 구성
- BPDU Terminal 구성

19.11.2 Port Fast 구성

Port Fast 기능이 활성화된 인터페이스는 스패닝 트리의 표준 Forward-Time 지연을 기다리지 않고 즉시 전송(Forwarding) 상태로 전환됩니다. 이 기능은 다른 스패닝 트리 모드에서는 유효하지 않습니다.

글로벌 구성 모드에서 Port Fast 기능을 구성하려면 다음 명령어를 사용하십시오

명령어	설명
spanning-tree port fast default	Port Fast 기능을 전역으로 활성화합니다. 모든 인터페이스에 적용됩니다.
no spanning-tree portfast default	Port Fast 기능을 전역으로 비활성화합니다. 인터페이스 구성에는 영향을 미치지 않습니다.

참고 : Port Fast 기능은 호스트에 연결된 인터페이스에만 적용됩니다. Port Fast 기능을 글로벌로 구성할 때 BPDU Guard 또는 BPDU Filter를 동시에 구성해야 합니다.

인터페이스 구성 모드에서 Port Fast 기능을 구성하려면 다음 명령어를 사용하십시오.

명령어	설명
spanning-tree portfast	해당 인터페이스에서 Port Fast 기능을 활성화합니다.
no spanning-tree portfast	해당 인터페이스에서 Port Fast 기능을 비활성화합니다. 글로벌 구성에는 영향을 미치지 않습니다.

19.11.3 BPDU Guard 구성

BPDU Guard 기능은 포트가 BPDU를 수신한 후 포트를 수동적으로 보호하며, 포트는 여전히 BPDU를 전송합니다. BPDU Guard는 사용하는 스패닝 트리 프로토콜에 따라 다르게 동작합니다.

SSTP/PVST 모드: BPDU Guard가 설정된 Port Fast 포트가 BPDU를 수신하면 해당 포트는 강제로 종료(shut down)되며, 사용자가 수동으로 복구를 구성해야만 다시 활성화됩니다.

RSTP/MSTP 모드: BPDU Guard가 설정된 일반 포트가 BPDU를 수신하면 해당 포트는 일정 시간 동안 차단(Blocking) 상태로 전환됩니다.

글로벌 구성 모드에서 BPDU Guard를 활성화하려면 다음 명령어를 사용하십시오.

명령어	설명
spanning-tree portfast bpduguard	BPDU Guard 기능을 활성화합니다. 모든 인터페이스에 적용됩니다.
no spanning-tree portfast bpduguard	BPDU Guard 기능을 비활성화합니다..

참고 : Port Fast 기능을 전역으로 활성화하면 브로드캐스트 스톰이 발생할 가능성이 있습니다. 이를 방지하기 위해 BPDU Guard 또는 BPDU Filter를 함께 구성해야 합니다.

인터페이스 구성 모드에서 BPDU Guard를 활성화하려면 다음 명령어를 사용하십시오.

명령어	설명
spanning-tree bpduguard enable	해당 인터페이스에서 BPDU Guard 기능을 활성화합니다.
spanning-tree bpduguard disable	해당 인터페이스에서 BPDU Guard 기능을 비활성화합니다. 글로벌 구성에는 영향을 미치지 않습니다.
no spanning-tree bpduguard	해당 인터페이스에서 BPDU Guard 기능을 비활성화합니다. 글로벌 구성에는 영향을 미치지 않습니다.

19.11.4 BPDU Filter 구성

SSTP/PVST 모드에서는 인터페이스가 BPDU를 전송하지 않도록 BPDU 필터링을 활성화해야 하며, 이는 Port Fast 포트를 보호하는 또 다른 방법입니다.

글로벌 구성 모드에서 BPDU 필터를 활성화하려면 다음 명령어를 사용하십시오.

명령어	설명
spanning-tree portfast bpdufilter	BPDU 필터 기능을 전역으로 활성화합니다. 모든 인터페이스에 적용됩니다.
no spanning-tree portfast bpdufilter	BPDU 필터 기능을 전역으로 비활성화합니다.

19.11.5 Uplink Fast 구성

Uplink Fast 기능은 스위치와 네트워크 루트 브리지 간의 연결이 중단되었을 때 새로운 루트 포트가 빠르게 전송(Forwarding) 상태로 전환되도록 합니다. Uplink Fast 기능은 SSTP/PVST 모드에서만 유효합니다.

글로벌 구성 모드에서 Uplink Fast를 활성화하려면 다음 명령어를 사용하십시오.

명령어	설명
spanning-tree uplinkfast	Uplink Fast 기능을 활성화합니다.
no spanning-tree uplinkfast	Uplink Fast 기능을 비활성화합니다.

19.11.6 Backbone Fast 구성

Backbone Fast 기능은 Uplink Fast 기술을 보완합니다. Uplink Fast는 지정된 스위치와의 직접 연결이 끊어졌을 때 중복 연결을 빠르게 작동시킵니다. 반면 Backbone Fast는 상위 계층 네트워크에서 직접 연결되지 않은 네트워크 장애를 감지하고 포트 상태 변경 속도를 높입니다.

Backbone Fast 기능은 SSTP/PVST 모드에서만 유효합니다.

명령어	설명
spanning-tree backbonefast	Backbone Fast 기능을 활성화합니다.
no spanning-tree backbonefast	Backbone Fast 기능을 비활성화합니다.

19.11.7 Root Guard 구성

Root Guard 기능은 높은 우선순위의 BPDU를 수신하여 포트가 루트 포트가 되는 것을 방지합니다. Root Guard 기능은 SSTP/PVST와 RSTP/MSTP 모드에서 다르게 동작합니다. SSTP/PVST 모드에서는 Root Guard에 의해 루트 포트가 항상 차단됩니다. RSTP/MSTP 모드에서는 더 높은 우선순위의 BPDU를 수신했을 때만 루트 포트가 차단됩니다. 이전에 루트 역할을 수행한 포트는 차단되지 않습니다.

인터페이스에서 Root Guard를 활성화하려면 다음 명령어를 사용하십시오:

명령어	설명
spanning-tree guard root	인터페이스에서 Root Guard 기능을 활성화합니다.
no spanning-tree guard	인터페이스에서 Root Guard 및 Loop Guard 기능을 비활성화합니다.
spanning-tree guard none	인터페이스에서 Root Guard 및 Loop Guard 기능을 비

	활성화합니다.

19.11.8 Loop Guard 구성

Loop Guard 기능은 루트 포트(Root Port) 또는 대체 포트(Alternate Port)가 지정 포트(Designated Port)로 전환된 후에도 루프를 방지합니다. BPDU를 수신하지 못해 발생할 수 있는 루프를 방지합니다. Loop Guard 기능은 SSTP/PVST와 RSTP/MSTP 모드에서 다르게 동작합니다. SSTP/PVST 모드에서는 지정 포트가 항상 Loop Guard에 의해 차단됩니다. RSTP/MSTP 모드에서는 BPDU를 수신하지 못하여 지정 포트로 전환된 경우에만 해당 포트가 차단됩니다. 낮은 우선순위의 BPDU를 수신하여 지정 역할이 부여된 포트는 Loop Guard에 의해 차단되지 않습니다.

글로벌 구성 모드에서 Loop Guard를 활성화하려면 다음 명령어를 사용하십시오:

명령어	설명
spanning-tree loopguard default	Loop Guard 기능을 전역으로 활성화합니다. 모든 인터페이스에 적용됩니다.
no spanning-tree loopguard default	Loop Guard 기능을 전역으로 비활성화합니다.

인터페이스 구성 모드에서 Loop Guard를 활성화하려면 다음 명령어를 사용하십시오:

명령어	목적
spanning-tree guard loop	해당 인터페이스에서 Loop Guard 기능을 활성화합니다.
no spanning-tree guard	해당 인터페이스에서 Root Guard 및 Loop Guard 기능을 비활성화합니다.
spanning-tree guard none	해당 인터페이스에서 Root Guard 및 Loop Guard 기능을 비활성화합니다.

19.11.9 Loop Fast 구성

주의 : 이 장의 구성 명령은 기술 엔지니어의 지시에 따라 사용해야 합니다.

Loop Fast 기능은 특정 네트워크 환경에서 네트워크의 수렴 성능을 제한적으로 개선하는 데 사용됩니다. 예를 들어, 여러 대의 스위치로 구성된 링 네트워크의 모든 포트에서 이 기능을 활성화할 수 있습니다.

글로벌 구성 모드에서 Loop Fast를 구성하려면 다음 명령어를 사용하십시오:

명령어	목적

spanning-tree loopfast	글로벌 구성 모드에서 모든 포트에 대해 Loop Fast 기능을 활성화합니다.
no spanning-tree loopfast	글로벌 구성 모드에서 Loop Fast 기능을 비활성화합니다.

포트 구성 모드에서 Loop Fast를 구성하려면 다음 명령어를 사용하십시오:

명령어	목적
spanning-tree loopfast	해당 포트에서 Loop Fast 기능을 활성화합니다.
no spanning-tree loopfast	모든 포트에서 Loop Fast 구성을 취소합니다.
spanning-tree loopfast disable	해당 포트에서 Loop Fast 기능을 비활성화합니다.

참고 : 글로벌 구성 모드에서 Loop Fast를 활성화한 경우, 포트에서도 이 기능이 유효합니다.

19.11.10 Address Table Aging 보호 구성

네트워크 토폴로지가 빈번하게 변경되는 환경에서 address table aging 보호를 구성하면, 스패닝 트리 프로토콜이 MAC 주소 테이블을 자주 업데이트하여 통신에 영향을 미치는 것을 방지할 수 있습니다.

빠른 수렴을 지원하는 스패닝 트리 프로토콜(RSTP, MSTP 등)은 토폴로지 변경을 감지하면 스위치의 MAC 주소 테이블에 있는 오래된 주소를 삭제하고 새로운 주소를 빠르게 업데이트하여 통신이 신속히 복구되도록 보장합니다. 기본 구성에서는 XXCOM 스위치가 MAC 주소 테이블의 빠른 aging(Fast Aging)를 통해 이 작업을 수행합니다. 대부분의 스위치 모델에서 MAC 주소 테이블의 빠른 aging는 1초 이내에 완료되며, CPU 기능에 거의 영향을 미치지 않습니다.

address table aging 보호 기능이 활성화되면, STP 프로토콜은 첫 번째 aging 작업 후 타이머 보호를 시작합니다. 타이머가 만료되기 전(기본값은 15초)에는 추가 aging이 실행되지 않습니다. 네트워크 토폴로지가 15초 이내에 변경되면, 프로토콜은 타이머 만료 후 두 번째 aging을 실행합니다.

참고 : no spanning-tree fast-aging 명령어를 사용하여 STP 프로토콜의 주소 aging을 완전히 비활성화할 수 있습니다. 이 구성을 실행하기 전에 네트워크에 루프가 없는지 반드시 확인해야 합니다. 그렇지 않으면 네트워크 토폴로지가 변경된 후 단말 장치가 서로 통신을 재개하는 데 5분 이상의 시간이 소요될 수 있습니다.

글로벌 구성 모드에서 address table aging 보호 기능을 구성하려면 다음 명령어를 사용하십시오

명령어	목적

spanning-tree fast-aging	주소 테이블의 aging 기능을 활성화하거나 비활성화합니다.
spanning-tree fast-aging protection	주소 테이블의 aging 보호 기능을 활성화하거나 비활성화합니다.
spanning-tree fast-aging protection time	address table aging 보호 시간을 설정합니다. 보호 시간 동안 스패닝 트리는 한 번만 aging을 실행합니다. 기본값은 15초입니다.

위 명령어 앞에 no를 추가하여 해당 설정을 비활성화할 수 있습니다.

19.11.11 FDB-Flush 구성

스위치의 빠른 스패닝 트리 프로토콜(RSTP 및 MSTP)은 기본적으로 FDB-Flush 방식이 아닌 주소 테이블의 (Fast Aging) 방식을 사용하여 오래된 MAC 주소를 제거합니다.

글로벌 구성 모드에서 FDB-Flush를 구성하려면 다음 명령어를 사용하십시오.

명령어	목적
spanning-tree fast-aging flush-fdb	FDB-Flush를 활성화합니다.
no spanning-tree fast-aging flush-fdb	FDB-Flush를 비활성화합니다.

FDB-Flush는 (Fast Aging) 기능과 독립적으로 작동합니다. no spanning-tree fast-aging 명령어를 설정한 상태에서도 FDB-Flush를 구성할 수 있습니다. 그러나 (Fast Aging Protection) 기능은 FDB-Flush에 유효하지 않습니다.

19.11.12 BPDU Terminal 구성

기본적으로, 스위치는 스패닝 트리가 실행되지 않을 때 수신한 BPDU를 전달합니다. BPDU Terminal 기능은 스패닝 트리가 실행되지 않을 때 BPDU 전달을 비활성화할 수 있습니다.

글로벌 구성 모드에서 BPDU Terminal을 구성하려면 다음 명령어를 사용하십시오.

명령어	목적
spanning-tree bpdu-terminal	BPDU Terminal을 활성화합니다.
no spanning-tree bpdu-terminal	BPDU Terminal을 비활성화합니다

20. Link Aggregation 구성

20.1 개요

Link Aggregation 란 동일한 속성을 가진 여러 물리적 포트를 묶어 논리적 채널을 형성하는 것을 의미합니다. port aggregation 방법에는 두 가지가 있습니다:

- 정적 집계: 물리적 포트가 집계 조건을 충족하는지 여부에 관계없이 물리적 포트를 논리적 포트에 정적으로 집계합니다.
- LACP(동적 집계): port aggregation가 반대쪽 포트와 협상한 후, LACP 협상이 완료된 물리적 포트만 논리적 채널에 집계됩니다.

지원되는 기능:

정적 집계 제어

- 물리적 포트를 논리적 포트에 바인딩(연결)합니다. 해당 포트가 실제로 논리적 포트와 연결될 수 있는지 여부와 상관없이 설정 가능합니다.

LACP 동적 협상 제어

- LACP 협상이 완료된 물리적 포트를 논리적 포트에 바인딩합니다. 협상이 완료되지 않은 포트는 논리적 포트에 바인딩되지 않습니다.
- port aggregation의 흐름 분배

Link Aggregation 후, 집계된 포트의 데이터 흐름은 각 물리적 포트에 고르게 분배됩니다.

20.2 Link Aggregation 구성 작업 목록

- 집계에 사용되는 논리적 채널 구성
- 물리적 port aggregation
- port aggregation 후 load balance 모드 선택
- port aggregation의 구체적인 상태 모니터링

20.3 port aggregation 구성 작업

20.3.1 집계에 사용되는 논리적 채널 구성

모든 물리적 포트를 하나로 묶기 전에 논리적 포트를 생성해야 합니다. 논리적 포트는 바인딩된 물리적 포트로 구성된 채널을 제어하는 데 사용됩니다.

논리적 채널을 구성하려면 다음 명령어를 사용하십시오.

명령어	설명
interface port-aggregator id	집계된 논리적 채널을 구성합니다

20.3.2 물리적 port aggregation

여러 물리적 포트를 논리적 채널로 집계하려면 정적 집계 또는 LACP 프로토콜을 사용할 수 있습니다.

정적 집계를 사용하는 경우

- 물리적 포트의 링크 상태가 업(up)이어야 합니다.
- 집계 포트와 물리적 포트의 VLAN 속성이 동일해야 합니다.
- 현재 포트가 집계 조건을 충족하지 않더라도, 연결된 물리적 포트가 집계 조건에 부합하지 않더라도 포트를 논리적 채널에 집계할 수 있습니다.

LACP 프로토콜을 사용하는 경우:

- 포트와 해당 포트에 연결된 피어(peer) 간에 협상이 완료된 후 집계가 수행됩니다.
- 포트의 링크 상태는 업(up)이어야 하며, 협상 결과 전이중(Full-Duplex) 모드로 설정되어야 합니다.
- 집계 과정에서 모든 물리적 포트의 속도는 동일해야 합니다. 예를 들어, 첫 번째 물리적 포트가 성공적으로 집계되었다면, 두 번째 물리적 포트의 속도는 첫 번째 포트와 동일해야 합니다.
- 모든 물리적 포트의 VLAN 속성(PVID, 트렁크 속성, 허용 VLAN 범위, 비태그 VLAN 범위)은 집계된 포트와 동일해야 합니다.

LACP의 집계 모드:

- Active 모드: 스위치가 적극적으로 집계 협상 프로세스를 시작합니다.
- Passive 모드: 스위치가 수동적으로 집계 협상 프로세스를 수락합니다.
- Passive 모드에서는 양쪽 포트가 모두 협상 프로세스를 시작하지 않기 때문에, 양쪽 포트가 Passive 모드를 사용할 경우 집계는 실패합니다.

물리적 포트를 집계하려면 다음 명령어를 사용하십시오.

명령어	설명
aggregator-group *agg-id* **mode** { **lacp** | **static** }	물리적 포트의 집계 옵션을 구성합니다.

20.3.3 port aggregation 후 load balance 방식 선택

모든 물리적 포트를 집계한 후, 모든 포트가 데이터 트래픽을 공유할 수 있도록 load balance 방식을 선택할 수 있습니다. 스위치는 최대 6가지 load balance 전략을 제공합니다:

- src-mac

  소스 MAC 주소에 따라 데이터 트래픽을 분배합니다. 동일한 MAC 주소 속성을 가진 메시지는 동일한 물리적 포트를 통해 전달됩니다.

- dst-mac

  목적지 MAC 주소에 따라 데이터 트래픽을 분배합니다. 동일한 MAC 주소 속성을 가진 메시지는 동일한 물리적 포트를 통해 전달됩니다.

- both-mac

  소스와 목적지 MAC 주소에 따라 데이터 트래픽을 분배합니다. 동일한 MAC 주소 속성을 가진 메시지는 동일한 물리적 포트를 통해 전달됩니다.

- src-ip

  소스 IP 주소에 따라 데이터 트래픽을 분배합니다. 동일한 IP 주소 속성을 가진 메시지는 동일한 물리적 포트를 통해 전달됩니다.

- dst-ip

  목적지 IP 주소에 따라 데이터 트래픽을 분배합니다. 동일한 IP 주소 속성을 가진 메시지는 동일한 물리적 포트를 통해 전달됩니다.

- both-ip

  소스와 목적지 IP 주소에 따라 데이터 트래픽을 분배합니다. 동일한 IP 주소 속성을 가진 메시지는 동일한 물리적 포트를 통해 전달됩니다.

load balance 방식을 구성하려면 다음 명령어를 사용하십시오.

명령어	설명
aggregator-group load-balance	load balance 방식을 구성합니다.

20.3.4 port aggregation의 구체적인 상태 모니터링

EXEC 모드에서 port aggregation 상태를 모니터링하려면 다음 명령어를 사용하십시오.

명령어	설명
show aggregator-group [id] {detail|brief|summary}	port aggregation의 상태를 표시합니다.

21.PDP 및 LLDP 구성

21.1 PDP개요

PDP(Port Discovery Protocol)는 네트워크 장비를 발견하기 위한 프로토콜로, 알려진 장비의 모든 이웃 장치를 찾는 데 사용됩니다. PDP를 통해 네트워크 관리 프로그램은 SNMP를 사용하여 인접 장치를 쿼리하고 네트워크 토폴로지를 획득할 수 있습니다. 우리 회사의 스위치는 인접 장치를 발견할 수 있지만, SNMP 쿼리를 허용하지 않습니다. 따라서 스위치는 네트워크 가장자리에만 배치해야 하며, 그렇지 않으면 완전한 네트워크 토폴로지를 얻을 수 없습니다.

PDP는 모든 SNAP(예: 이더넷)에서 설정할 수 있습니다.

21.1 PDP 구성 작업

- 기본 PDP 구성
- PDP 클록 및 정보 저장 설정
- PDP 버전 설정
- 스위치에서 PDP 시작
- 포트에서 PDP 시작
- PDP 모니터링 및 관리

21.1.1 기본 PDP 구성

기능	기본 설정
글로벌 구성 모드	기본적으로 비활성화됨
인터페이스 구성 모드	활성화됨
PDP 클록(패킷 전송 주기)	60초
PDP 정보 저장 시간	180초
PDP 버전	2

21.1.2 PDP 클록 및 정보 저장 설정

PDP 패킷 전송 주기와 PDP 정보 저장 시간을 설정하려면 글로벌 구성 모드에서 다음 명령어를 사용하십시오:

명령어	설명

pdp timer seconds	PDP 패킷 전송 주기를 설정합니다.
pdp holdtime seconds	PDP 정보 저장 시간을 설정합니다.

21.1.3 PDP 버전 설정

PDP 버전을 설정하려면 글로벌 구성 모드에서 다음 명령어를 사용하십시오

명령어	설명
pdp version {1|2}	PDP 버전을 설정합니다.

21.1.4 스위치에서 PDP 시작

PDP를 활성화하려면 글로벌 구성 모드에서 다음 명령어를 사용하십시오:

명령어	설명
pdp run	스위치에서 PDP를 시작합니다.

21.1.5 포트에서 PDP 시작

기본적으로 포트에서 PDP를 활성화하려면 포트 구성 모드에서 다음 명령어를 사용하십시오:

명령어	설명
pdp enable	스위치 포트에서 PDP를 시작합니다.

21.1.6 PDP 모니터링 및 관리

PDP를 모니터링하려면 EXEC 모드에서 다음 명령어를 사용하십시오:

명령어	설명
show pdp traffic	수신 및 전송된 PDP 패킷 수를 표시합니다.
show pdp neighbor [detail]	PDP로 발견된 이웃 장치를 표시합니다.

21.1.7 PDP 구성 예제

예제 1: PDP 시작

Switch_config# pdp run

Switch_config# int g0/1

Switch_config_g0/1# pdp enable

예제 2: PDP 클록 및 정보 저장 설정

Switch_config# pdp timer 30

Switch_config# pdp holdtime 90

예제 3: PDP 버전 설정

Switch_config# pdp version 1

예제 4: PDP 모니터링

Switch_config# show pdp neighbor

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater

Device-ID	Local-Intf	Hldtme	Port-ID	Platform	Capability
Switch	Gig0/1	169	Gig0/1	COM, RISC	R S

21.2 LLDP 설명

LDP (Link Layer Discovery Protocol)**는 IEEE 802.1AB 표준으로, 네트워크 문제를 쉽게 감지하고 네트워크 토폴로지를 유지 관리하도록 돕습니다. LLDP는 인접 장치가 상태 정보를 다른 장치에 알리도록 하며, 모든 장치의 각 포트는 자체 정의된 정보를 저장합니다. 필요 시, 인접 장치에 직접 업데이트된 정보를 전송할 수도 있습니다. 장치는 정보를 표준 SNMP MIB에 저장하며, 네트워크 관리 시스템은 MIB에서 2계층의 현재 연결 상태를 쿼리할 수 있습니다.

LLDP는 네트워크 요소나 트래픽을 구성하거나 제어하지 않고, 2계층의 구성을 단순히 보고합니다. LLDP는 이웃 탐색 프로토콜로, 스위치, 라우터, WAP(무선 액세스 포인트)와 같은 이더넷 네트워크 장치에 표준 방법을 설정합니다. 이더넷 장치는 LLDP를 통해 자신의 존재를 다른 노드에 알리고, 인접 장치의 탐색 정보를 저장할 수 있습니다. 장치의 구성 및 식별 정보를 포함한 모든 정보가 프로토콜을 통해 알림으로 전송될 수 있습니다. LLDP는 보편적인 알림 정보 세트, 알림 전송 프ㅇ토콜, 그리고 모든 알림 정보를 저장하는 방법을 정의합니다.

장치는 LAN 데이터 패킷을 통해 여러 알림을 전송할 수 있으며, 전송 형식은 TLV (Type-Length-Value)입니다.

TLV의 유형

필수 TLV

- Chassis ID TLV
- Port ID TLV

- Time To Live TLV

선택적 TLV

- Port Description
- System Name
- System Description
- System Capabilities
- Management Address

확장 TLV

- DOT1 (Port VLAN ID, Protocol VLAN ID, VLAN Name, Protocol Identity)
- DOT3 (MAC/PHY 구성/상태, MDI를 통한 전력 공급, 링크 집계, 최대 프레임 크기)
- MED (MED Capability, Network Policy, Location Identification, Extended Power-via-MDI, Inventory 정보: 하드웨어/펌웨어/소프트웨어 버전, 일련 번호, 제조사 이름, 모델명, 자산 ID)

LLDP의 특성

LLDP는 단방향 프로토콜입니다.

- LLDP 에이전트는 연결된 MSAP(Multiple Spanning Tree Access Port)를 통해 상태 정보와 기능을 전송하거나, 이웃 장치의 현재 상태 정보 또는 기능 정보를 수신합니다.
- 그러나 LLDP 에이전트는 프로토콜을 통해 피어에서 정보를 요청할 수는 없습니다.
- 메시지 교환 중에는 전송과 수신이 서로 영향을 주지 않습니다. 메시지 전송만, 수신만, 또는 둘 다 구성할 수 있습니다.

21.2.1 프로토콜 초기화

LLDP는 세 가지 모드로 작동할 수 있습니다. 전송 전용(transmit-only), 수신 전용(receive-only) 전송 및 수신(transmit-and-receive) 기본 모드는 전송 및 수신(transmit-and-receive)입니다.

21.2.2 LLDP 전송 모드 초기화

LLDP를 인터페이스 모드에서 전송 전용(transmit-only)으로 설정합니다. 전송 전용 모드에서는 로컬 시스템의 하나 이상의 정보 요소(관리 객체)의 상태 또는 값이 변경되거나 전송 타이머가 만료되었을 때 인터페이스가 LLDP 패킷을 전송합니다. 해당 기능이 비활성화되면 인터페이스는 LLDP 패킷을 전송하지 않습니다.

21.2.3 LLDP 수신 모드 초기화

LLDP를 인터페이스 모드에서 수신 전용(receive-only)으로 설정합니다. 수신 전용 모드에서는 인터페이스가 이웃으로부터 LLDP 패킷을 수신하고 TLV를 원격 MIB에 저장할 수 있습니다. 해당 기능이 비활성화되면 인터페이스는 LLDP 패킷을 폐기합니다.

21.2.4 LLDP PDU 패킷 구조 설명

LLDP PDU는 순서대로 다음과 같은 구조를 가집니다: 앞부분에는 세 가지 필수 TLV가 포함되고, 중간에는 하나 이상의 선택적 TLV가 포함되며, 마지막에는 LLDPUD TLV가 위치합니다. 그림 1에 이 구조가 나타나 있습니다.

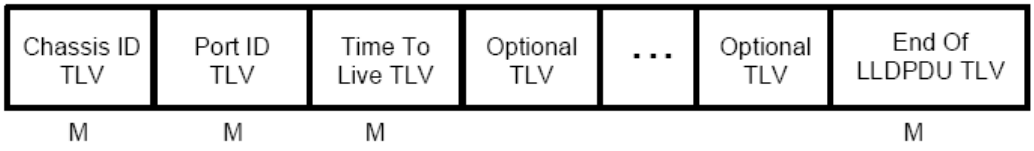


그림 22 LLDP PDU 포멧

- LDP PDU의 시작 부분에는 세 가지 필수 TLV가 순서대로 포함되어야 합니다.
  - ① Chassis ID TLV
  - ② Port ID TLV
  - ③ Time To Live TLV
- 네트워크 관리에서 선택한 선택적 TLV는 임의 순서로 나열될 수 있습니다
  - ① Port Description
  - ② System Name
  - ③ System Description
  - ④ System Capabilities
  - ⑤ Management Address
- 확장 TLV (DOT1 포함)
  - ① Port VLAN ID
  - ② Protocol VLAN ID
  - ③ VLAN Name

④ Protocol Identity

- DOT3 확장
  - ① MAC/PHY Configuration/Status
  - ② Power Via MDI
  - ③ Link Aggregation
  - ④ Max Frame Size
- MED TLV는 기본적으로 전송되지 않습니다. LLDP 패킷에서 MED TLV를 수신했을 때만 MED TLV가 포함된 LLDP 패킷이 전송됩니다.
  - ① MED Capability (MED TLV가 추가된 경우 필수 TLV입니다.)
  - ② Network Policy
  - ③ Location Identification
  - ④ Extended Power-via-MDI
  - ⑤ Inventory (Hardware Revision, Firmware Revision, Software Revision, Serial Number, Manufacturer Name, Model Name, Assert ID 포함)

21.3 LLDP 구성 작업 목록

- LLDP 비활성화/활성화
- Holdtime 설정
- Timer 설정
- Reinit 설정
- 전송할 TLV 구성
- 전송 또는 수신 모드 구성
- 포트 관리 IP 주소 지정
- MIB 데이터베이스로 트랩 알림 전송
- Show 관련 명령어 구성
- 삭제 명령어 구성

21.4 LLDP 구성 작업

21.4.1 LLDP 비활성화/활성화

LLDP가 활성화되면 로컬 포트는 주기적으로 LLDP 프레임을 전송하여 반대쪽 장치에 로컬 정보를 알립니다.

LLDP를 활성화/비활성화 하려면 글로벌 구성 모드에서 다음 명령어를 실행하십시오.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
lldp run	LLDP를 활성화합니다.
No lldp run	LLDP를 비활성화합니다.

참고:

LLDP 기능이 활성화된 경우에만 수신된 LLDP 메시지를 처리할 수 있습니다. LLDP 기능이 비활성화된 상태에서는 LLDP 프레임이 직접 전달됩니다.

21.4.2 Holdtime 설정

일반적으로 원격 장치 정보는 MIB에서 Aging되기 전에 업데이트됩니다. 하지만 전송 과정에서 업데이트 프레임이 손실될 수 있기 때문에 MIB의 정보도 Aging 가능성이 있습니다. 이를 방지하기 위해 TTL 값을 설정하여 노후화 시간 동안 LLDP 프레임이 여러 번 전송되도록 할 수 있습니다. LLDP 메시지의 전송 시간 초과(timeout) 시간을 설정하려면 Holdtime 값을 수정해야 합니다.

글로벌 구성 모드에서 LLDP Holdtime을 설정하려면 다음 명령어를 사용하십시오.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
lldp holdtime time	LLDP의 전송 시간 초과 시간을 설정합니다. 범위: 0 ~ 65535초, 기본값: 120초
no lldp holdtime	LLDP의 시간 초과 값을 기본값(120초)으로 복원합니다.

참고 : 다음 LLDP 프레임을 수신할 때 이전 이웃 정보가 Aging으로 인해 손실되지 않도록 하려면, 시간 초과 값은 LLDP 패킷 전송 간격보다 길어야 합니다.

21.4.3 Timar 설정

LLDP의 타이머를 구성하여 스위치가 메시지를 전송하는 간격을 제어할 수 있습니다.

글로벌 구성 모드에서 LLDP Timer를 설정하려면 다음 명령어를 사용하십시오

명령어	설명
config	글로벌 구성 모드로 진입합니다.
lldp timer time	LLDP 메시지 전송 간격을 설정합니다. 범위: 5 ~ 65534 초, 기본값: 30초
no lldp timer	LLDP 전송 간격을 기본값(30초)으로 복원합니다.

21.4.4 Reinit 설정

LLDP 정보는 로컬 시스템에서 하나 이상의 정보 요소(관리 객체)의 상태 또는 값이 변경되고 전송 타이머가 만료되었을 때 자동으로 전송됩니다.

단일 정보 변경마다 LLDP 프레임이 전송되기 때문에 연속적인 정보 변경이 발생하면 많은 LLDP 프레임 전송이 트리거될 수 있습니다. 이는 각 프레임에서 하나의 변경만 보고하기 때문입니다.

이 문제를 방지하기 위해 네트워크 관리에서는 두 개의 연속 LLDP 프레임 전송 간의 대기 시간을 정의합니다. LLDP의 Reinit을 구성하여 스위치가 연속적으로 두 메시지를 전송하는 간격을 제어할 수 있습니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
lldp reinit time	연속적인 메시지 전송 간격을 설정합니다. 범위: 2 ~ 5 초, 기본값: 2초
no lldp reinit	연속 메시지 전송 간격을 기본값 2초로 복원합니다.

21.4.5 전송할 TLV 구성

LLDP에서 전송할 TLV를 선택하려면 tlv-select를 구성할 수 있습니다. 기본적으로 모든 TLV가 전송됩니다.

글로벌 구성 모드에서 TLV를 추가하려면 다음 명령어를 사용하십시오

명령어	설명
config	글로벌 구성 모드로 진입합니다.
lldp tlv-select management-address	선택 사항. 관리 주소 TLV를 전송합니다. 관리 주소는 일반적으로 사용하기 쉬운 3계층 IP 주소입니다.
lldp tlv-select port-description	선택 사항. 포트 설명 TLV를 전송합니다. 포트 설명은 숫자 또는 문자로 구성됩니다.
lldp tlv-select system-capabilities	선택 사항. 시스템 성능 TLV를 전송합니다. 시스템 성능은 스위치나 라우터와 같은 패킷 전송 시스템을 의

	미합니다.
lldp tlv-select system-description	선택 사항. 시스템 설명 TLV를 전송합니다. 시스템 설명은 숫자와 문자로 구성된 텍스트로, 시스템 전체 이름, 하드웨어 버전, 소프트웨어 버전, 네트워크 소프트웨어를 포함해야 합니다.
lldp tlv-select system-name	선택 사항. 시스템 이름 TLV를 전송합니다. 시스템 이름은 시스템 관리자(예: 스위치 이름)의 이름이어야 합니다.

21.4.6 포트 구성 및 전송할 확장 TLV 선택

LLDP에서 dot1-tlv-select, dot3-tlv-select, 또는 med-tlv-select를 사용하여 포트에서 전송할 확장 TLV를 선택할 수 있습니다. 기본적으로 DOT1 및 DOT3 TLV는 전송되며, MED TLV는 전송되지 않습니다.

포트 구성 모드에서 전송할 TLV를 추가하려면 다음 명령어를 사용하십시오

명령어	설명
config	글로벌 구성 모드로 진입합니다.
interface intf-type intf-id	인터페이스 구성 모드로 진입합니다.
lldp dot1-tlv-select port-vlan-id	선택 사항. 802.1에서 정의된 TLV를 전송하며 포트의 PVID를 알립니다.
lldp dot1-tlv-select protocol-vlan-id	선택 사항. 802.1에서 정의된 TLV를 전송하며 포트의 PPVID를 알립니다.
lldp dot1-tlv-select vlan-name	선택 사항. 802.1에서 정의된 TLV를 전송하며 포트의 VLAN 이름을 알립니다.
Lldp dot3-tlv-select macphy-confg	선택 사항. 802.3에서 정의된 TLV를 전송하며 다음을 알립니다. a) 물리 계층에서의 비트 속도 및 통신 모드(듀플렉스) b) 현재 듀플렉스 상태와 설정된 비트 속도 c) 정이 초기 연결 단계에서 자동 협상 결과인지, 수동 설정인지 여부를 표시
lldp dot3-tlv-select power	선택 사항. 802.3에서 정의된 TLV를 전송하며 비전원 시스템이 링크를 통해 전력 공급을 허용하는지 알립니다.
lldp dot3-tlv-select link-aggregation	선택 사항. 802.3에서 정의된 TLV를 전송하며 링크가 집계 가능한 경우 포트를 식별합니다.
lldp dot3-tlv-select max-frame-size	선택 사항. 802.3에서 정의된 TLV를 전송하며 포트에서 최대 프레임 크기를 지정합니다.

lldp med-tlv-select network-policy	선택 사항. MED에서 정의된 TLV를 전송하며 VLAN 구성 오류 및 2계층, 3계층 속성을 진단합니다.
lldp med-tlv-select location	선택 사항. MED에서 정의된 TLV를 전송하며 위치 정보를 알립니다. a) IETF 3825[6]에서 정의된 좌표 기반 LCI b) IETF 부록 B에서 정의된 도시 주소 LCI c) 긴급 호출 서비스의 ELIN 코드
lldp med-tlv-select power-management	선택 사항. MED에서 정의된 TLV를 전송하며 전원 공급 정보를 알립니다.
lldp med-tlv-select inventory	선택 사항. MED에서 정의된 TLV를 전송하며 상세한 인벤토리 속성을 알립니다.
lldp dot1-tlv-select protocol-identity	선택 사항. 802.1 에서 정의된 TLV 를 전송하며 포트의 프로토콜 식별 정보를 알립니다.

21.4.7 전송 또는 수신 모드 구성

LLDP는 세 가지 모드로 작동할 수 있습니다.

- 전송 전용(transmit-only)
- 수신 전용(receive-only)
- 전송 및 수신(transmit-and-receive)

기본적으로 LLDP는 전송 및 수신(transmit-and-receive) 모드로 작동합니다. 다음 명령어를 사용하여 LLDP의 작동 모드를 수정할 수 있습니다.

포트 구성 모드에서 전송 전용 또는 수신 전용 모드를 활성화/비활성화하려면 다음 명령어를 사용하십시오

명령어	설명
config	글로벌 구성 모드로 진입합니다.
interface intf-type intf-id	인터페이스 구성 모드로 진입합니다.
lldp transmit	포트의 전송 모드를 활성화합니다.
lldp receive	포트의 수신 모드를 활성화합니다.

참고 : 위의 모드 외에도 포트를 전송 전용(transmit-only) 모드 또는 수신 전용(receive-only) 모드로 설정할 수 있습니다.

21.4.8 포트의 관리 IP 주소 지정

포트 구성 모드에서 LLDP 패킷이 전송되는 포트의 관리 IP 주소를 임의로 설정할 수 있습니다. 이 관리 주소는 해당 포트와 관련된 IP 주소여야 하며, 이를 통해 해당 포트의 정상적인 통신이 보장됩니다.

포트 구성 모드에서 관리 IP 주소를 설정하려면 다음 명령어를 사용하십시오.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
interface intf-type intf-id	인터페이스 구성 모드로 진입합니다.
lldp management-ip A.B.C.D	포트의 관리 IP 주소를 설정합니다.

참고 : no lldp management-ip 명령어를 사용하면 포트의 관리 IP 주소를 기본값으로 복원할 수 있습니다. 기본 관리 주소는 해당 포트의 PVID와 연결된 VLAN 인터페이스의 IP 주소입니다. 해당 VLAN 인터페이스가 존재하지 않으면 관리 주소는 0.0.0.0이 됩니다.

21.4.9 위치 정보 설정

명령어	설명
config	글로벌 구성 모드로 진입합니다.
location elin identifier id WORD	ELIN 정보를 설정합니다. id는 ELIN 식별 번호이며, WORD는 10~25바이트 범위의 ELIN 정보를 나타냅니다
location civic identifier id	위치 구성 모드로 진입합니다.
language WORD	언어를 설정합니다.
state WORD	주(도) 이름을 설정합니다.
county WORD	군(county) 이름을 설정합니다.
city WORD	도시 이름을 설정합니다.
division WORD	구역(division) 이름을 설정합니다.
neighborhood WORD	동네(neighborhood) 이름을 설정합니다.
street WORD	거리 이름을 설정합니다.
leading-street-dir WORD	주요 거리의 방향을 설정합니다.
trailing-street-suffix WORD	작은 거리의 접미사를 설정합니다.
street-suffix WORD	거리의 접미사를 설정합니다. 예
number WORD	번지 번호를 설정합니다.
street-number-suffix WORD	번지 번호의 접미사를 설정합니다.

landmark WORD	랜드마크를 설정합니다.
additional-location WORD	추가 위치를 설정합니다.
name WORD	거주자 정보를 설정합니다.
postal-code WORD	우편번호를 설정합니다.
building WORD	건물 정보를 설정합니다.
unit WORD	단위(unit) 정보를 설정합니다.
floor WORD	층(floor) 정보를 설정합니다.
room WORD	방(room) 정보를 설정합니다.
type-of-place WORD	장소 유형을 설정합니다.
postal-community WORD	우체국 이름을 설정합니다.
post-office-box WORD	우편함 번호를 설정합니다.
additional-code WORD	추가 코드를 설정합니다.
country WORD	국가 이름을 설정합니다.
script WORD	문자 체계를 설정합니다.

명령어 앞에 no를 입력하면 삭제할 수 있습니다.

21.4.10 포트에 위치 정보 설정

다음 명령어를 사용하면 포트의 위치 정보를 설정하고 TLV에 위치 정보를 포함시킬 수 있습니다.

포트 구성 모드에서 위치 정보를 설정하려면 다음 명령어를 사용하십시오.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
interface intf-type intf-id	인터페이스 구성 모드로 진입합니다.
location civic id	civic ID의 위치 정보를 설정합니다.
location elin id	ELIN ID의 위치 정보를 설정합니다.

21.4.11 Show 관련 명령어 구성

Show 명령어를 사용하면 LLDP 모듈이 수신한 이웃 정보, 통계 및 포트 상태를 확인할 수 있습니다.

EXEC 모드 또는 글로벌 구성 모드에서 다음 명령어를 사용하십시오.

명령어	설명
Show lldp errors	LLDP 모듈의 오류 정보를 표시합니다.

Show lldp interface interface-name	포트 상태 정보를 표시합니다. 전송 모드와 수신 모드가 포함됩니다.
Show lldp neighbors	이웃에 대한 요약 정보를 표시합니다.
Show lldp neighbors detail	이웃에 대한 상세 정보를 표시합니다.
Show lldp traffic	수신 및 전송된 통계 정보를 모두 표시합니다.
Show location elin	ELIN 위치 정보를 표시합니다.
Show location civic	Civic 위치 정보를 표시합니다.

21.4.12 삭제 명령어 구성

수신된 이웃 목록과 모든 통계 정보를 삭제하려면 다음 명령어를 사용하십시오.

EXEC 모드에서 다음 명령어를 실행하십시오

명령어	설명
clear lldp counters	모든 통계 데이터를 삭제합니다.
clear lldp table	수신된 모든 이웃 정보를 삭제합니다.

21.4.13 설정 예제

- 네트워크 환경 요구사항

두 스위치를 연결하는 포트에 LLDP 프로토콜을 구성해야 합니다.

- 네트워크 토폴로지

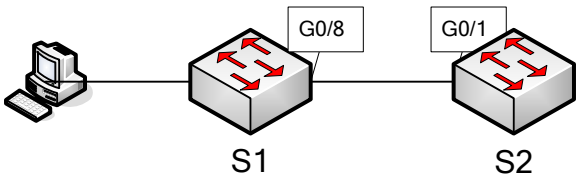


그림 23 네트워크 토폴로지

- 기본 구성

Configuring switch S1:

Switch_config#lldp run

Switch_config#

Configuring switch S2:

Switch_config#lldp run

Switch_config#

B의 정보는 약 1분 후 스위치 A에 표시됩니다. MED-TLV 정보는 기본적으로 전송되지 않습니다.S1:

Switch_config#show lldp neighbors
Capability Codes:
(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone
(W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID	Local-Intf	Hldtme	Port-ID	Capability
Switch	Gig0/8	99	Gig0/1	B

Total entries displayed: 1
Switch_config#show lldp neighbors detail

chassis id: 00e0.0fac.32ff
port id: Gig0/1
port description: GigaEthernet0/1
system name: Switch

system description: SWITCH Software, Version 4.1.0B
Serial: S24090103
Compiled: 2011-9-21 9:24:8 by WRL

Time remaining: 96
system capabilities: R B
enabled capabilities: B
Management Address:
IP: 90.0.0.21

Port VLAN ID: 1
PPVID: 1
VLAN 1 name: Default
Auto Negotiation: supported,enabled
Physical media capabilities:
1000baseX(FD)
1000baseX(HD)
100baseTX(FD)
100baseTX(HD)

Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:
MDI power support --
PSE MDI power support: support
Port class: PSE
PSE MDI power state: enabled
PSE pairs selection control ability: can not be controlled
PSE power pair: signal
Power Classification: Class 0
Link Aggregation:
Aggregation capability: capable of being aggregated
Aggregation status: not currently in aggregation
Maximum frame size: 1500

Total entries displayed: 1

- TLV 구성

스위치 S1 설정

Switch_config# lldp run

Switch_config#

스위치 S2 설정

Switch_config# lldp run

Switch_config# no lldp tlv-select system-name

Switch_config# int g0/8

Switch_config_g0/8# no lldp dot1-tlv-select port-vlan-id

Switch_config_g0/8# no lldp dot3-tlv-select max-frame-size

Switch_config_g0/8#

스위치 S1: LLDP 요약 정보

Switch_config# show lldp neighbors

Capability Codes:

(R)Router, (B)Bridge, (C)DOCSIS Cable Device, (T)Telephone

(W)WLAN Access Point, (P)Repeater, (S)Station, (O)Other

Device-ID	Local-Intf	Hldtme	Port-ID	Capability
Switch	Gas0/8	92	Gig0/1	R B

Total entries displayed: 1

스위치 S1: LLDP 상세 정보

Switch_config# show lldp neighbors detail

chassis id: 00e0.0fac.32ff

port id: Gig0/1

port description: GigaEthernet0/1

system name: -- not advertised

system description: XXCOM(tm) SWITCH Software, Version 4.1.0B

Serial: S24090103

Copyright by Shanghai Baud Data Communication CO. LTD.

Compiled: 2011-9-21 9:24:8 by WRL

Time remaining: 95

system capabilities: R B

enabled capabilities: B

Management Address:

IP: 90.0.0.21

Port VLAN ID -- not advertised

PPVID: 1

VLAN 1 name: Default

Auto Negotiation: supported, enabled

Physical media capabilities:

1000baseX(FD)

1000baseX(HD)

100baseTX(FD)

100baseTX(HD)

Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:

MDI power support --

PSE MDI power support: support

Port class: PSE

PSE MDI power state: enabled

PSE pairs selection control ability: can not be controlled

PSE power pair: signal

Power Classification: Class 0

Link Aggregation:

Aggregation capability: capable of being aggregated

Aggregation status: not currently in aggregation

Total entries displayed: 1

스위치 S2는 system-name, port-vlan-id, max-frame-size TLV를 비활성화했기 때문에, 이 정보는 S1의 LLDP 출력에서 표시되지 않습니다. MED-TLV 정보는 기본적으로 전송되지 않습니다.

- 위치 정보 구성

스위치 S1 구성

Switch_config# lldp run

Switch_config#

스위치 S2 구성

Switch_config# lldp run

```
Switch_config# location elin identifier 1 1234567890      // ELIN 정보 설정
Switch_config# location civic identifier 1                // 위치 구성 모드 진입
Switch_config_civic# language English                     // 언어 설정
Switch_config_civic# city Shanghai                        // 도시 설정
Switch_config_civic# street Curie                         // 거리 이름 설정
Switch_config_civic# script EN                            // 문자 체계 설정
Switch_config_civic# quit                                 // 위치 구성 모드 종료

Switch_config# int g0/8
Switch_config_g0/8# location elin 1                       // 포트에 ELIN ID 지정
Switch_config_g0/8# location civic 1                      // 포트에 Civic ID 지정

Switch_config_g0/8# show location elin                    // ELIN 설정 정보 표시
elin information:
   elin 1: 1234567890
total: 1

Switch_config_g0/8# show location civic                   // Civic 설정 정보 표시
civic address information:
   identifier: 1
   City: Shanghai
   Language: English
   Script: EN
   Street: Curie
-----------------------------------
total: 1
Switch_config_g0/8#
```

스위치 S2 상세 정보

```
Switch_config# show lldp neighbors detail

chassis id: 00e0.0fac.32ff
port id: Gig0/1
port description: GigaEthernet0/1
system name: Switch

system description: SWITCH Software, Version 4.1.0B
Serial: S24090103
Compiled: 2011-9-21 9:24:8 by WRL

Time remaining: 109
system capabilities: R B
enabled capabilities: B
Management Address:
    IP: 90.0.0.21

Port VLAN ID: 1
Auto Negotiation: supported, enabled
Physical media capabilities:
    1000baseX(FD)
    1000baseX(HD)
    100baseTX(FD)
    100baseTX(HD)
Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:
  MDI power support --
    PSE MDI power support: support
```

Port class: PSE

PSE MDI power state: enabled

PSE pairs selection control ability: can not be controlled

PSE power pair: signal

Power Classification: Class 0

MED Information:

MED Codes:

(CA)Capabilities, (NP)Network Policy, (LI)Location Identification

(PS)Power via MDI – PSE, (PD)Power via MDI – PD, (IN)Inventory

Hardware Revision: 0.4.0

Software Revision: 4.1.0B

Serial Number: S24090103

Manufacturer Name:

Model Name: SWITCH

Asset ID: S24090103

Capabilities: CA, NP, LI, PS, IN

Device type: Network Connectivity

Network Policy: Voice

Policy: Unknown

Power requirements:

Type: PSE Device

Source: Unknown

Priority: Low

Value: 150 (0.1 Watts)

Civic address location:

Language: English

City: Shanghai

Street: Curie

Script: EN

ELIN location:

ELIN: 1234567890

Total entries displayed: 1

Switch_config#

22 Backup Link

21.2 개요

이중 업링크 네트워킹(Dual-Uplink Networking)은 일반적인 네트워킹 방식입니다. 아래 그림에서 볼 수 있듯이, DUT(Device Under Test)는 스위치 B와 스위치 C를 통해 스위치 D로 이중 업스트림 연결을 구성합니다.

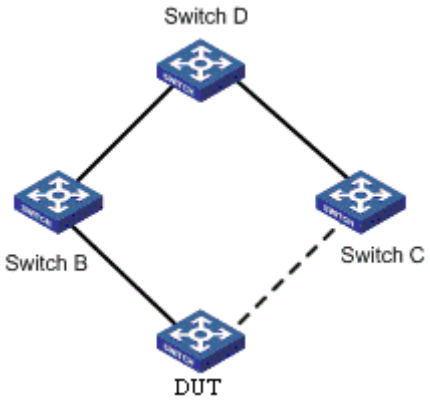


그림 24 Dual 업링크 네트워크

이중 업링크 네트워킹은 링크 백업을 제공할 수 있지만, 네트워크에 루프가 발생하면 브로드캐스트 폭풍이 발생합니다. 따라서 루프를 방지하기 위한 조치가 필요합니다. 일반적으로 루프는 STP(Spanning Tree Protocol)를 통해 제거할 수 있습니다. 그러나 STP는 시간이 오래 걸리면 더 많은 트래픽 손실이 발생하므로, STP는 빠른 복구 시간이 요구되는 네트워킹 환경에는 적합하지 않습니다. BackupLink는 링크 계층 인터페이스 한 쌍을 통해 링크 백업을 제공하며, STP의 느린 수렴 문제를 해결합니다. 하나의 BackupLink 포트 그룹에서 하나는 Primary Port(기본 포트)로, 다른 하나는 Alternate Port(대체 포트)로 구성됩니다. STP 프로토콜을 사용하지 않는 경우에도 BackupLink는 링크의 중복성과 백업을 보장할 수 있습니다.

22.1 BackupLink 포트 백업

22.1.1 백업 포트 구성

BackupLink의 기본 기능은 하나의 스위치 포트를 다른 스위치 포트의 백업으로 설정하는 것입니다. 이때, 두 백업 포트 중 하나만 전송 상태(Forwarding State)에 있게 됩니다. 두 백업 포트는 동일한 장치에 연결될 수도 있고, 서로 다른 장치에 연결될 수도 있습니다.

참고 :

- 서로 백업 수 있는 두 포트는 다음과 같을 수 있습니다.
  ① 두 개의 물리적 포트

② 두 개의 집합 포트

③ 하나의 물리적 포트와 하나의 집합 포트

- 백업 포트는 다음과 같은 기능이 설정된 포트에 구성할 수 없습니다.
  ① 링크 집계(Link Aggregation)
  ② 포트 보안(Port Security)
  ③ EAPS (Ethernet Automatic Protection Switching)
  ④ 기타 네트워크 보호 기능
- 하나의 포트에 이미 백업 포트가 설정된 경우, 이 포트는 다른 포트의 백업으로 구성될 수 없습니다.
- 백업 포트로 설정된 포트에는 다음 기능을 구성할 수 없습니다.
  ① 링크 집계(Link Aggregation)
  ② 포트 보안(Port Security)
  ③ EAPS (Ethernet Automatic Protection Switching)
  ④ 기타 네트워크 보호 기능
- BackupLink가 설정된 포트에서는 물리 계층의 링크 상태 감지 최적화를 활성화할 수 있습니다. 이를 통해 수렴 성능을 향상시킬 수 있습니다.

22.1.2 포트 상태 제어

업 기능이 구성된 포트는 STP 모듈에서 제거되어야 합니다. BackupLink는 포트의 상태를 모든 VLAN [1-4094]에서 제어합니다. 이러한 VLAN은 서로 다른 MST (Multiple Spanning Tree) 또는 STG (Spanning Tree Group)에 속할 수 있습니다.

22.1.3 포트 역할과 상태

구성 명령어를 사용하면 서로 백업하는 두 포트의 기본 역할을 지정할 수 있습니다.

참고 :

- 초기 상태에서 Active 포트와 Backup 포트의 링크 상태가 Linkup인 경우
  Active 포트는 전송 상태에 있고, Backup 포트는 차단 상태에 있습니다.
- 초기 상태에서 한 포트의 링크 상태가 Linkdown인 경우
  다른 포트는 역할에 관계없이 전송 상태로 전환됩니다.

- 특정 시점에 Backup 포트가 전송 상태이고 Active 포트가 차단 상태인 경우

  Backup 포트 구성을 해당 포트에 반복적으로 수행하면 Backup 포트는 강제로 차단 상태로 전환되며, Active 포트는 전송 상태를 복구합니다.

22.1.4 링크 상태 변경 처리

기본 포트 백업 기능에서 링크 상태 변경 처리는 다음 요구사항을 충족해야 합니다:

- Active 포트가 Linkdown 상태이고 Backup 포트도 Linkdown 상태인 경우.

  링크가 끊어지며 데이터 프레임을 전달할 수 없습니다.

- Active 포트가 Linkdown 상태이고 Backup 포트가 Linkup 상태이지만 전송 상태가 아닌 경우

  Backup 포트가 전송 상태로 전환됩니다.

- Active 포트가 Linkup 상태이고 Backup 포트가 Linkdown 상태인 경우

  Active 포트가 전송 상태로 전환됩니다.

- Active 포트가 Linkup 상태이고 Backup 포트가 Linkup 상태이면서 전송 상태인 경우:

  사전 점유(preemption) 모드가 비활성화된 상태에서는 Active 포트가 차단 상태를 유지하며, 데이터 프레임은 Backup 포트를 통해 전달됩니다.

- Active 포트가 Linkup 상태이고 Backup 포트가 Linkup 상태이면서 전송 상태인 경우:

사전 점유(preemption) 모드가 활성화된 상태에서는 다른 전략에 따라 전송 포트와 차단 포트가 결정됩니다. 자세한 내용은 1.2.5를 참조하십시오.

22.1.5 백업 포트의 사전 점유

BackupLink는 포트 사전 점유(preemption)를 지원해야 합니다. A와 B가 한 쌍의 백업 포트라고 가정했을 때 포트 A가 전송 상태에 있고, 포트 B가 LinkDown 상태에서 복구되어 차단 상태인 경우, 포트 B가 사전 점유 조건을 충족하면 포트 B가 전송 상태로 전환되고 포트 A는 차단 상태가 됩니다.

사전 점유 기능은 명령어를 통해 활성화해야 하며, 기본적으로 비활성화되어 있습니다.

사전 점유는 각 백업 포트 쌍마다 독립적으로 설정해야 합니다. 또한, 서로 다른 백업 포트 그룹은 서로 다른 사전 점유 모드를 사용할 수 있습니다.

사전 점유 모드

- 포트 역할 기반 사전 점유

① 백업 포트를 구성할 때 지정된 역할에 따라 사전 점유가 수행됩니다.

② 만약 Backup 포트가 전송 상태에 있고 Active 포트가 LinkUp 상태인 경우, Backup 포트는 차단 상태로 전환되고 Active 포트가 전송 상태로 설정됩니다.

- 포트 대역폭 기반 사전 점유

① 백업 포트는 대역폭을 기준으로 전송 상태의 사전 점유를 지원해야 합니다.

② 대역폭이 작은 포트는 항상 차단 상태가 됩니다.

주의사항 : 같은 백업 포트 그룹에서 사전 점유 기능을 설정할 때는 다음 요구사항을 충족해야 합니다. 사전 점유 기능은 백업 그룹 내의 어느 포트에서든 설정되면 적용되지만, 이 설정이 삭제되면 기능은 비활성화됩니다. 전 점유 기능은 백업 그룹의 두 포트 모두에 설정할 수 있습니다. 단, 사전 점유 모드와 지연 파라미터는 반드시 일치해야 합니다. 점유 파라미터가 일치하지 않는 두 포트는 백업 포트로 설정할 수 없습니다.

22.1.6 Delay Preemption

포트의 경우 지연 시간을 설정해야 합니다. 만약 포트 B가 포트 A의 전송 상태를 Delay Preemption할 수 있는 조건을 충족하면, 지연 시간 이후에 사전 점유가 완료됩니다. 지연 시간 사전 점유는 명령어를 통해 설정해야 합니다. "0"으로 설정하면 유효한 지연 시간으로 간주되며, 즉시 사전 점유를 의미합니다.

22.2 VLAN Load Balancing

BackupLink의 VLAN Load Balancing 기능은 BackupLink 포트 그룹의 두 포트가 서로 다른 VLAN의 트래픽을 동시에 전송할 수 있도록 합니다. 예를 들어, BackupLink 포트 그룹이 VLAN 1100의 트래픽을 처리하도록 구성된 경우, 한 포트는 VLAN 150의 트래픽을 전송하고 다른 포트는 VLAN 51~100의 트래픽을 전송합니다. 만약 한 포트가 Linkdown 상태로 전환되면, 다른 포트가 모든 트래픽을 전송합니다.

22.2.1 Load Balancing 구성

VLAN Load Balancing은 백업 포트에만 구성됩니다. 사용자는 명령어를 통해 VLAN 그룹을 지정하며, 백업 포트는 해당 VLAN 그룹에서 우선적으로 전송 상태로 전환됩니다. 따라서 VLAN 트래픽 공유는 포트에 백업 기능이 먼저 설정된 경우에만 작동합니다.

참고 : 서로 다른 BackupLink 그룹에서는 동일한 VLAN 그룹이 설정될 수 있거나 VLAN 세그먼트가 겹칠 수 있습니다. 하지만 VLAN 세그먼트가 겹치는 경우 시스템은 이를 서로 다른 MST (STG)

로 할당합니다. 따라서 일부 그룹의 포트가 동작하게 되면 해당 포트는 모든 MST (STG)에서 상태 변화가 발생하게 됩니다. 따라서 일반적으로 VLAN 그룹이 겹치지 않는 것을 선택하는 것이 좋습니다.

22.2.2 트래픽 공유에서의 포트 상태 제어

- 지정된 VLAN에 대해 새로운 MST (STG) 생성

  서로 다른 VLAN에서 포트 상태를 구분하여 설정하려면, 사용자가 트래픽 공유 명령어로 지정한 VLAN을 새로운 MST (STG)에 할당해야 합니다. BackupLink는 L2 모듈에서 제공하는 인터페이스를 통해 사용자가 지정한 VLAN을 확인해야 합니다. 만약 지정된 VLAN이 다른 프로토콜 모듈(MSTP에서 특정 MST에 할당되었거나 EAPS의 제어 VLAN으로 구성됨)에서 이미 사용 중이라면, 이 VLAN은 더 이상 VLAN 트래픽 공유에 사용할 수 없습니다. 이러한 경우 사용자의 구성 오류로 처리되어야 합니다.

- 동일한 VLAN이 여러 백업 포트 그룹에서 사용되는 경우

  BackupLink는 서로 다른 백업 포트 그룹에서 동일한 VLAN이 구성되는 경우를 처리할 수 있어야 합니다. 예:

  P1과 P2가 서로 백업 관계에 있고, P2에서 VLAN v의 트래픽 공유가 구성됨

  P3과 P4가 서로 백업 관계에 있고, P4에서 VLAN v가 구성됨

  이 경우:

  ① 설정이 로드되는 동안 VLAN v에 대해 MST를 할당하는 작업만 수행하면 됩니다.

  ② 모든 백업 포트 그룹에서 VLAN v 트래픽 공유 구성이 삭제된 경우, VLAN v는 기본 MST로 복원되어야 합니다.

- MST 생성 후 포트 상태 갱신

  VLAN의 MST 수정은 시스템의 STG 테이블에서 일부 포트 상태를 부정확하게 만들 수 있습니다. 이 경우:

  ① L2는 BackupLink를 제외한 프로토콜 모듈에 포트 상태 설정 갱신을 알립니다.

  ② BackupLink 모듈의 각 백업 포트 그룹은 모든 VLAN에서 상태를 능동적으로 갱신합니다.

- 포트 상태 설정

  VLAN 트래픽 공유를 구성한 후, 백업 포트의 상태 설정은 다음 규칙을 따라야 합니다

  ① 백업 관계에 있는 두 포트가 모두 Link Down 상태인 경우, VLAN [1-4094]의 상

태는 Blocking으로 설정됩니다.

② 두 포트 중 하나만 Link Up 상태인 경우, 해당 포트는 모든 VLAN에서 Forwarding 상태로 설정됩니다.

③ 두 포트가 모두 Link Up 상태인 경우:

Active 역할로 선택된 포트는 트래픽 공유 VLAN에서 Blocking 상태로, 다른 VLAN에서는 Forwarding 상태로 설정됩니다.

Backup 역할로 선택된 포트는 트래픽 공유 VLAN에서 Forwarding 상태로, 다른 VLAN에서는 Blocking 상태로 설정됩니다.

22.3 MAC 주소 Aging 처리

BackupLink는 업링크 네트워크에 루프가 존재하는 경우를 처리하기 위해 업링크의 토폴로지 변경 알림을 지원해야 합니다.

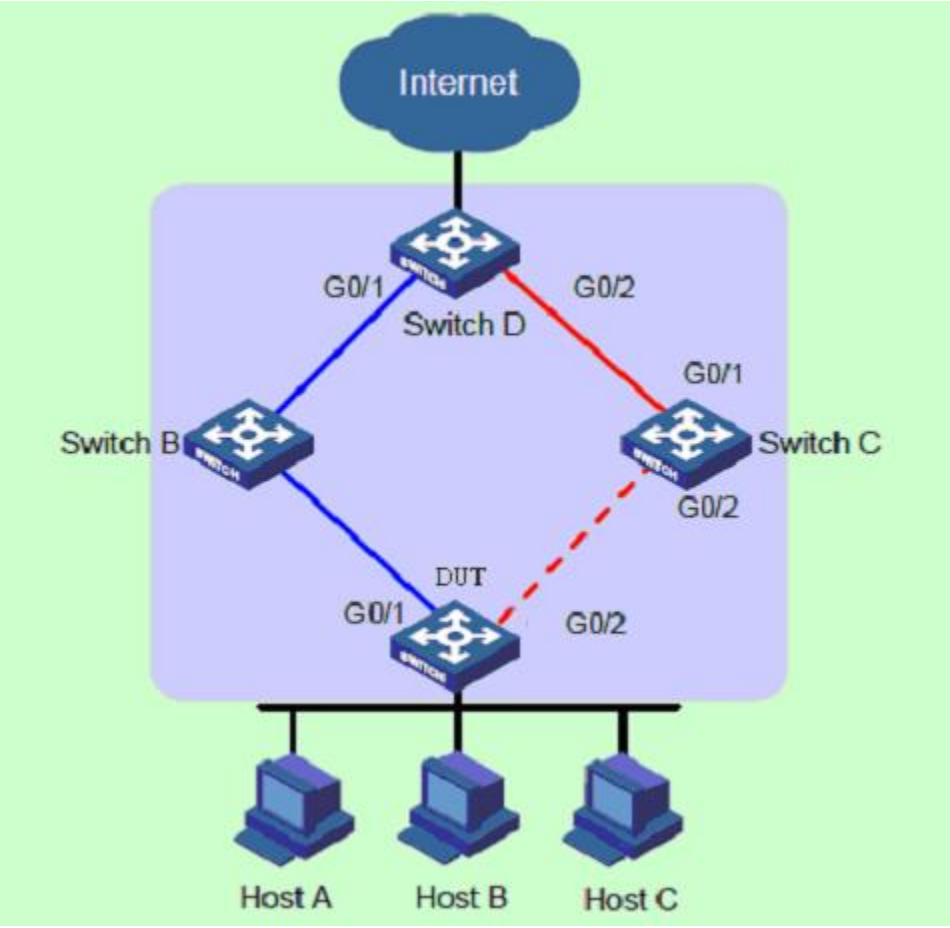


그림 25 backuplink

22.3.1 링크의 정상 작동 매커니즘

DUT의 "GigaEthernet0/1" 포트는 기본 포트이며, "GigaEthernet0/2" 포트는 백업 포트입니다. 이중 업링크가 정상 작동 상태일 때, 기본 포트는 전송 상태에 있고 해당 링크는 기본 링크입니다. 백업 포트는 차단 상태에 있고 해당 링크는 보조 링크입니다. 데이터는 파란색 선으로 표시된 링크를 따라 전송되며, 네트워크에 루프가 존재하지 않아 브로드캐스트 Strom을 방지할 수 있습니다.

22.3.2 다운링크 장애 처리 매커니즘

DUT의 기본 링크에 장애가 발생하면, 기본 포트인 "GigaEthernet0/1"은 대기 상태로 전환되고, 백업 포트인 "GigaEthernet0/2"는 전송 상태로 전환됩니다. 이 시점에서 네트워크 장치의 MAC 주소 포워딩 테이블 항목과 ARP 테이블 항목이 잘못될 수 있으므로, MAC 및 ARP 정보를 빠르게 업데이트하여 트래픽을 신속하게 전환하고 트래픽 손실을 방지하는 메커니즘이 필요합니다. 현재 두 가지 업데이트 메커니즘이 존재합니다:

- 링크 업데이트 패킷 MMU를 통해 테이블 항목을 장치에 알림

  이 방식에서는 업스트림 장치(위 그림에서 Switch D, Switch B 및 선택적으로 Switch C)가 BackupLink의 MMU 기능을 지원하고 MMU 패킷 상황을 인식해야 합니다. 빠른 링크 전환을 달성하려면 DUT에서 MMU 패킷 전송 기능을 활성화하고, 이중 업링크 네트워크의 업스트림 장치 포트에서 MMU 패킷 수신 및 처리 기능을 활성화해야 합니다.

  DUT의 링크 전환이 발생하면 새로운 기본 링크, 즉 "GigaEthernet0/2" 포트에서 MMU 패킷이 전송됩니다. 업스트림 장치가 MMU 패킷을 수신하면, 해당 패킷의 제어 VLAN이 패킷을 수신한 포트에 설정된 수신 제어 VLAN 목록에 포함되어 있는지 판단합니다. 만약 포함되어 있지 않으면 장치는 패킷을 처리하지 않고 바로 전달합니다. 하지만 포함되어 있는 경우, 장치는 MMU 패킷에 포함된 VLAN Bitmap 데이터를 추출하고 해당 VLAN에서 학습된 MAC 및 ARP 항목을 삭제합니다.

  그 후, Switch D가 DUT를 목적지로 하는 데이터 패킷을 수신하면 2계층 포워딩이 필요한 패킷은 2계층 브로드캐스팅 방식으로 전달됩니다. 3계층 포워딩이 필요한 패킷은 ARP 탐지 방식을 사용해 ARP 항목을 업데이트한 후 패킷을 전송합니다. 이를 통해 데이터 트래픽이 올바르게 전송될 수 있습니다.

- 트래픽을 통해 자동으로 항목 업데이트

  이 방법은 BackupLink를 지원하지 않는 장치(다른 벤더의 장치를 포함)와 연결된 경우에 적용되며, 업스트림 트래픽이 트리거되는 상황에서 작동합니다.

  DUT에서 업스트림 트래픽이 발생하지 않으면, Switch D는 여전히 잘못된 MAC 및 ARP

항목을 기반으로 포트 "GigaEthernet0/1"을 통해 DUT로의 데이터 패킷을 전송하려 하지만, 패킷은 DUT에 도달하지 못하고 트래픽이 단절됩니다. 이때, MAC 또는 ARP 항목이 자동으로 aging되기 전까지는 문제가 해결되지 않습니다. DUT가 업스트림 트래픽을 전송하는 경우에도, 잘못된 MAC 및 ARP 항목 때문에 트래픽은 자동으로 aging되고 재학습되기 전까지 전송되지 않습니다. 업스트림 트래픽이 포트 "GigaEthernet0/2"를 통해 Switch D에 도달하면, Switch D는 자체 MAC 및 ARP 항목을 업데이트합니다. 이후 Switch D가 다시 DUT를 목적지로 하는 패킷을 수신하면, "GigaEthernet0/2" 포트를 통해 전송되며 패킷은 Switch C를 거쳐 DUT에 도달하게 됩니다.

참고 : MMU 패킷을 통해 장치에 항목 업데이트를 알리는 메커니즘에서는 항목이 자동으로 aging 될 때까지 기다릴 필요가 없으므로, 항목 업데이트 시간을 크게 단축할 수 있습니다.

22.3.3 업링크 장애 처리 매커니즘

위 에서 설명된 네트워킹 환경에서는 BackupLink 기능이 DUT의 링크 중복 백업을 위해 사용됩니다. GigaEthernet0/1은 기본 포트이며, GigaEthernet0/2는 보조 포트입니다.

기본 포트 GigaEthernet0/1의 링크에 장애가 발생하면, 트래픽은 GigaEthernet0/2 보조 포트의 링크로 밀리초 단위의 짧은 시간에 전환되어, 효율적이고 신뢰할 수 있는 링크 백업 및 빠른 수렴 성능을 제공합니다. 그러나 Switch B의 업링크 포트 GigaEthernet0/1이 연결된 링크에 장애가 발생했을 때, DUT에서 BackupLink 그룹을 구성한 경우에는, GigaEthernet0/1이 연결된 링크 자체에 장애가 없으므로 BackupLink 그룹 내에서 링크 전환이 발생하지 않습니다.

실제로 DUT의 트래픽은 GigaEthernet0/1 포트를 통해 Switch D로 업링크되지 못해 트래픽이 중단됩니다.

이 문제를 해결하기 위해 BackupLink는 업링크 토폴로지 변경에 따라 로컬 링크를 변경하는 "MonitorLink" 메커니즘을 지원해야 합니다.

MonitorLink는 업링크를 모니터링하여 다운링크가 업링크와 동기화되도록 하며, BackupLink의 백업 역할을 향상시킵니다.

- MonitorLink 개념 소개

  MonitorLink 그룹은 하나 이상의 업스트림 포트와 다운스트림 포트로 구성됩니다.

  다운스트림 포트의 상태는 업스트림 포트 상태의 변화에 따라 달라집니다.

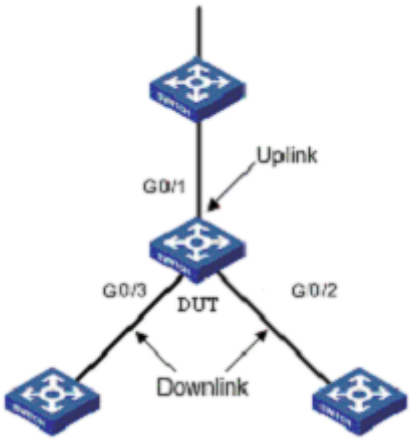


그림 26 모니터링크 그룹 개념

위 그림에서 DUT의 세 개의 포트(GigaEthernet0/1, GigaEthernet0/2, GigaEthernet0/3)는 하나의 MonitorLink 그룹을 형성합니다.

- Uplink Port

  MonitorLink 그룹의 Uplink Port는 이더넷 포트(전기 또는 광) 또는 집합 인터페이스일 수 있습니다. 그림 3에서 DUT의 GigaEthernet1/1 포트는 MonitorLink 그룹의 Uplink Port로 구성되어 있습니다.

Uplink Port에 장애가 발생하면 MonitorLink 그룹의 상태가 DOWN으로 전환되며, 모든 Downlink Port가 비활성화됩니다. 만약 Uplink Port가 지정되지 않으면 Uplink Port에 장애가 발생한 것으로 간주되며, 이 경우에도 모든 Downlink Port가 비활성화됩니다.

- Downlink Port

  Downlink Port는 MonitorLink 그룹에서 모니터 역할을 하며, 명령어를 통해 지정되는 또 다른 포트 역할입니다. MonitorLink 그룹의 Downlink Port는 이더넷 포트(전기 또는 광) 또는 집합 인터페이스일 수 있습니다. 위 그림에서 DUT의 두 포트(GigaEthernet0/2, GigaEthernet0/3)는 MonitorLink 그룹의 Downlink Port로 구성되어 있습니다.

- MonitorLink 작동 메커니즘

  아래 네트워킹 환경에서 DUT에 BackupLink 그룹이 구성되어 있어 호스트가 신뢰할 수 있는 인터넷 액세스를 할 수 있습니다.

  GigaEthernet0/1은 Primary Port로 전송 상태에 있습니다.

  GigaEthernet0/2는 Secondary Port로 설정되어 있습니다.

  MonitorLink는 Uplink Port의 상태를 모니터링하여, Uplink Port의 장애가 Downlink Port의 상태로 반영되도록 합니다.

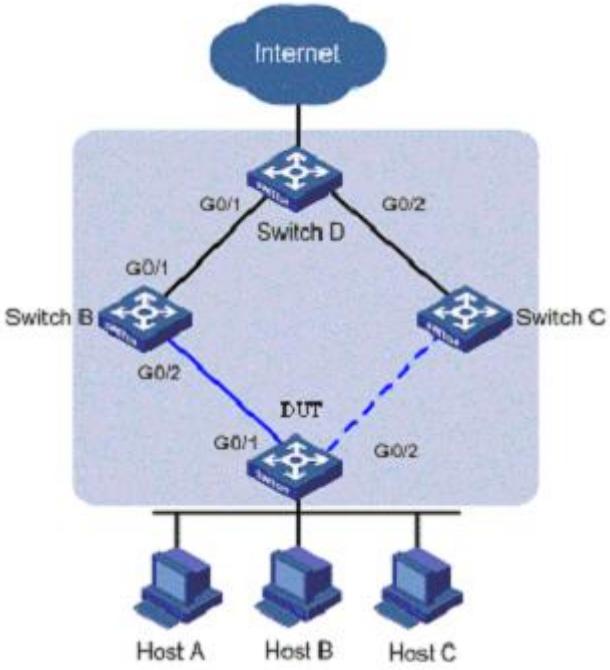


그림 27 모니터링크 운영 매커니즘

DUT의 트래픽이 Switch B의 포트 "GigaEthernet1/1"에 연결된 링크 장애로 인해 업링크되지 못하는 문제를 방지하기 위해, Switch B에 MonitorLink 그룹이 구성되었습니다.

포트 "GigaEthernet0/1"은 Uplink Port로 지정되고, 포트 "GigaEthernet0/2"는 Downlink Port로 지정되었습니다.

Switch B의 Uplink Port인 "GigaEthernet0/1"이 연결된 링크에 장애가 발생하면, MonitorLink 그룹은 해당 그룹의 Downlink Port인 "GigaEthernet0/2"를 강제로 비활성화합니다. 이로 인해 DUT의 BackupLink 그룹에서 링크 전환이 트리거됩니다. Switch B의 Uplink Port "GigaEthernet0/1"이 장애에서 복구되면 Downlink Port "GigaEthernet0/2"도 활성화됩니다. 이때, DUT의 BackupLink 그룹이 역할 사전 점유(preemption) 모드로 구성되어 있는 경우, DUT의 BackupLink 그룹에서 다시 링크 전환이 트리거됩니다. 그렇지 않은 경우에는 다음 링크 전환이 발생할 때까지 기다려야 합니다.

결과적으로, MonitorLink 기술과 BackupLink 기술의 결합은 효율적이고 신뢰할 수 있는 링크 백업과 빠른 성능을 제공합니다.

22.4 BackupLink 구성 가이드라인

BackupLink 프로토콜을 구성하기 전에 다음 가이드라인을 읽어보시기 바랍니다:

- 기본 포트(Ethernet 포트 또는 링크 집합 포트)는 BackupLink의 백업 포트로 구성될 수 있습니다. 그러나 기본 포트와 백업 포트는 동일한 포트일 수 없습니다.
- 하나의 포트는 오직 하나의 BackupLink 그룹에만 속할 수 있습니다. 백업 포트는 하나의 기본 포트에만 백업 포트로 지정될 수 있으며, 기본 포트는 다른 BackupLink 그룹에 속할 수 없습니다.
- BackupLink 그룹 내의 포트는 링크 집합 포트의 멤버가 될 수 없습니다. 그러나 링크 집합 포트와 물리적 포트, 물리적 포트와 물리적 포트, 또는 링크 집합 포트와 링크 집합 포트는 BackupLink 그룹의 멤버가 될 수 있습니다.
- BackupLink의 기본 포트와 백업 포트는 유형이 다를 수 있습니다. Fast Ethernet 포트, Gigabit 포트 또는 링크 집합 포트일 수 있지만, 두 포트 모두 유사한 특성을 가져야 합니다. 따라서 기본 포트에 장애가 발생하면 백업 포트가 유사한 방식으로 데이터 트래픽을 전송할 수 있습니다.
- VLAN Load Balancing 기능과 BackupLink 사전 점유(preemption) 기능은 동시에 사용할 수 없습니다.

22.5 BackupLink 구성 작업

- BackupLink 그룹 구성
- BackupLink 그룹의 사전 점유 기능 구성
- VLAN을 위한 Load Balancing 구성
- BackupLink 그룹의 MMU 기능 구성
- MonitorLink 그룹 구성

22.6BackupLink 설정

22.6.1 BackupLink 그룹 구성

다음 단계를 따라 BackupLink 그룹을 구성합니다

명령어	설명
Switch#config	스위치 구성 모드로 진입합니다.
Switch#**config**	BackupLink 그룹을 구성합니다. id는 BackupLink 그룹

	인스턴스 번호입니다.
Switch_config#**backup-link-group** *id*	포트 구성 모드로 진입합니다.
Switch_config#**interface** *interface-type interface-number*	BackupLink 그룹 포트 역할을 구성합니다. id는 BackupLink 그룹 인스턴스 번호입니다.
Switch_config_g1/1#**backup-link-group** *id* **active[backup]**	포트 구성 모드에서 나갑니다.
Switch_config_g1/1#**exit**	명령 완료 후 대기 상태로 돌아갑니다.
Switch_config#	

참고 : no backup-link-group id 명령어를 사용하여 BackupLink 그룹 구성과 포트 구성을 삭제할 수 있습니다. BackupLink 그룹이 생성되지 않은 상태에서 포트에 BackupLink 그룹을 직접 구성하면, 시스템이 자동으로 BackupLink 그룹을 생성합니다.

22.6.2 백업링크 그룹의 Preemption 기능 설정

백업링크 그룹의 Preemption 기능을 아래 단계에 따라 설정합니다.

명령어	설명
Switch#config	스위치 구성 모드로 진입합니다.
Switch_config#**backup-link-group** *id* {**preemption-mode [forced | bandwidth] {delay** *value***}**}	백업링크 그룹의 Preemption 기능 설정 Preemption 기능을 백업링크 그룹에 대해 구성합니다. id: 백업링크 그룹 인스턴스 번호 value: 지연 시간 (초)

참고 : backup-link-group id {preemption-mode [forced | bandwidth] {delay value}} 명령을 사용하여 백업링크 그룹을 직접 생성할 수 있습니다.

22.6.3 VLAN 로드 밸런싱 설정

VLAN 로드 밸런싱을 아래 단계에 따라 설정합니다.

명령어	설명
Switch#**config**	스위치 구성 모드로 진입합니다.
Switch_config#**interface** *interface-type interface-number*	포트 구성 모드로 진입합니다.
Switch_config_g1/2#**share-load vlan** *vlanmap*	VLAN 로드 밸런싱을 설정합니다. - vlanmap: VLAN 값

Switch_config_g1/2#**exit**	포트 구성 모드에서 나옵니다.
Switch_config#	

참고 : share-load vlan vlanmap 명령은 백업 포트에만 사용 가능합니다. 따라서 VLAN 로드 밸런싱을 설정하기 전에 해당 포트를 백업 포트로 구성해야 합니다. 서로 다른 BackupLink 그룹 간에는 동일한 VLAN 그룹을 설정하거나 VLAN 세그먼트가 중첩될 수 있습니다. 하지만 중첩된 VLAN 세그먼트를 설정하면, 시스템이 이를 서로 다른 MST(Multiple Spanning Tree) 또는 STG(Spanning Tree Group)로 자동 할당합니다.이로 인해 특정 그룹의 포트를 운영할 때, 해당 포트의 상태가 모든 MST(STG)에서 변경될 수 있습니다. 따라서 일반적으로 VLAN 그룹을 로드 밸런싱용으로 구성할 때, 중첩되지 않은 VLAN 그룹을 선택하는 것이 좋습니다.

22.6.4 백업링크 그룹의 MMU 기능 설정

백업링크 그룹에 대한 MMU 기능을 아래 단계에 따라 설정합니다.

명령어	설명
Switch#**config**	스위치 구성 모드로 진입합니다.
Switch_config#**interface** *interface-type interface-number*	포트 구성 모드로 진입합니다.
Switch_config_g1/2#**backup-link-group mmu transmit [receive]**	MMU 전송(수신) 기능을 설정합니다

.

Switch_config_g1/2#exit 포트 구성 모드에서 나옵니다.

참고: transmit으로 설정된 포트는 반드시 백업링크 그룹의 포트여야 하며, 먼저 해당 포트를 Active 또는 Backup으로 설정해야 합니다. receive 기능을 설정하는 경우, 해당 포트를 백업링크 그룹에 별도로 설정할 필요는 없습니다.

22.6.5 MonitorLink 그룹 설정

MonitorLink 그룹을 아래 단계에 따라 설정합니다.

명령어	설명
Switch#**config**	스위치 구성 모드로 진입합니다.
Switch_config#**monitor-link-group** *id*	MonitorLink 그룹을 설정합니다. - id: MonitorLink 그룹 인스턴스 번호
Switch_config#**interface** *interface-type interface-number*	포트 구성 모드로 진입합니다.

Switch_config_g1/1#**monitor-link-group** *id* **uplink[downlink]**	MonitorLink 그룹의 포트 역할을 설정합니다. - id: MonitorLink 그룹 인스턴스 번호
Switch_config_g1/1#**exit**	포트 구성 모드에서 나옵니다.
Switch_config#	

참고:

no monitor-link-group id 명령어를 사용하여 MonitorLink 그룹 구성 및 포트 구성을 삭제할 수 있습니다.

MonitorLink 그룹이 생성되지 않은 상태에서 포트에 대해 MonitorLink 그룹 포트 역할을 직접 설정하면, 시스템이 자동으로 MonfitorLink 그룹을 생성합니다.

22.7 Fast Ethernet Ring Protection 소개

이더넷 링 보호 프로토콜은 링형 이더넷 토폴로지를 구성하기 위해 설계된 특별한 링크 계층 프로토콜입니다. 이 프로토콜은 완전한 링 토폴로지에서 하나의 링크를 차단하여 데이터 루프가 생성되어 브로드캐스트 폭풍이 발생하는 것을 방지합니다. 만약 링크가 손상되면, 프로토콜은 즉시 이전에 차단된 링크를 복구하여 링 네트워크의 노드 간 통신이 가능하도록 합니다.

링 보호 프로토콜과 STP(Spanning Tree Protocol)는 모두 링크 계층에서 토폴로지를 제어하는 데 사용됩니다.

- STP는 모든 종류의 복잡한 네트워크에 적합하며, 네트워크 토폴로지의 변화를 홉 단위로 전파합니다.
- 링 보호 프로토콜은 링형 토폴로지에 특화되었으며, 네트워크 토폴로지 변화를 확산 메커니즘(pervasion mechanism)을 통해 전파합니다.

따라서 링형 네트워크에서 링 보호 프로토콜의 수렴 속도는 STP보다 더 빠릅니다. 정상적인 네트워크에서 링 보호 프로토콜은 50ms 이내에 네트워크 통신을 복구할 수 있습니다.

참고 : EAPS(Ethernet Automatic Protection Switching)를 사용하면 하나의 스위치를 다수의 물리적 링의 노드로 설정하여 복잡한 토폴로지를 구성할 수 있습니다.

22.8Fast Ethernet Ring Protection 개념

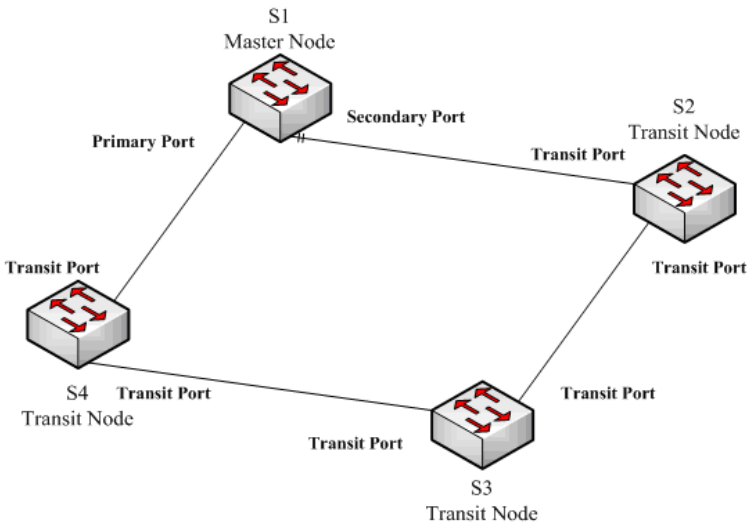


그림 28 EAPS 구성

22.8.1 링 노드의 역할

이더넷 링의 각 스위치는 링 노드입니다. 링 노드는 마스터 노드와 트랜짓 노드로 분류됩니다.

이더넷 링에서 하나의 스위치만 마스터 노드 역할을 수행할 수 있으며, 나머지 스위치들은 트랜짓 노드로 작동합니다.

- 마스터 노드:
  - ① 링의 토폴로지가 완전한지 여부를 확인합니다.
  - ② 루프백(Loopback)을 제거합니다.
  - ③ 다른 스위치가 토폴로지 정보를 업데이트하도록 제어합니다.
- 트랜짓 노드:
  - ① 로컬 포트의 상태만 점검하며, 유효하지 않은 링크를 마스터 노드에 알립니다.

각 노드의 역할은 사용자가 설정을 통해 지정할 수 있습니다. 그러나 동일한 링 내의 각 스위치는 하나의 역할만 가질 수 있습니다.

예를 들어, 그림 1.1에서 스위치 S1은 링 네트워크의 마스터 노드이고, 스위치 S2, S3, S4는 트랜짓 노드입니다.

22.8.2 링 포트의 역할

EAPS(Ethernet Automatic Protection Switching) 프로토콜은 각 스위치가 링 네트워크와 연결하기

위해 두 개의 포트를 필요로 합니다. 링 네트워크의 각 포트는 설정을 통해 다음 역할 중 하나로 지정될 수 있습니다.

- Primary Port (주 포트):
  ① 주 포트는 마스터 노드에서만 설정할 수 있습니다.
  ② 마스터 노드는 주 포트를 통해 링 감지 패킷을 전송합니다.
- Secondary Port (보조 포트):
  ① 보조 포트는 마스터 노드에서만 설정할 수 있습니다.
  ② 마스터 노드는 보조 포트를 통해 링 감지 패킷을 수신하고 링 네트워크의 토폴로지가 완전한지 판단합니다.
  ③ 토폴로지가 완전한 경우, 보조 포트에서 데이터 패킷을 차단하여 루프백 발생을 방지합니다.
  ④ 링 네트워크의 링크가 끊어질 경우, 마스터 노드는 보조 포트를 열어 데이터 패킷을 전달합니다.
- Transit Port (트랜짓 포트):
  ① 트랜짓 포트는 트랜짓 노드에서만 설정할 수 있습니다.
  ② 트랜짓 노드가 링 네트워크에 연결되는 두 포트는 모두 트랜짓 포트입니다.

각 링 포트는 스위치의 노드 역할과 제어 VLAN이 설정된 후 하나의 포트 역할만 가질 수 있습니다. 예를 들어, 그림 1.1에서 마스터 노드 S1이 트랜짓 노드 S4와 연결된 포트는 주 포트이며, S1이 S2와 연결된 포트는 보조 포트입니다. S2, S3, S4의 링 네트워크 연결 포트는 모두 트랜짓 포트입니다.

참고 : 하나의 스위치를 여러 링에 포함하려면, 스위치가 다른 링과 서로 다른 물리적 포트를 통해 연결되어야 합니다.

22.8.3 제어 VLAN(Control VLAN)과 데이터 VLAN(Data VLAN)

제어 VLAN은 마스터 노드와 트랜짓 노드 간에 프로토콜 패킷을 전송하기 위해 사용되는 전용 VLAN입니다. 사용자는 설정을 통해 제어 VLAN을 지정하며, 링의 포트도 제어 VLAN에 추가합니다. 이를 통해 프로토콜 패킷이 정상적으로 전달되도록 보장합니다.

일반적으로 링 네트워크의 각 포트는 제어 VLAN에서 전달 상태(Forwarding State)를 유지하며, 링 네트워크에 속하지 않은 포트는 제어 VLAN의 패킷을 전달할 수 없습니다.

참고 : 스위치의 각 링에 대해 다른 제어 VLAN을 지정할 수 있습니다. 제어 VLAN은 링 네트워크의 제어 패킷 전송만을 위해 사용되며, L2/L3 통신에는 사용되지 않습니다. 예를 들어, 제어

VLAN에 해당하는 VLAN 포트가 생성되더라도, 해당 VLAN 포트의 IP 주소는 다른 장치에서 핑(Ping)이 되지 않습니다.

제어 VLAN을 제외한 나머지 VLAN은 모두 데이터 VLAN으로 간주됩니다. 데이터 VLAN은 일반적인 서비스 패킷이나 관리 패킷을 전송하는 데 사용됩니다.

참고 : 데이터 VLAN은 정상적인 L2/L3 통신에 사용할 수 있습니다. 예를 들어, 데이터 VLAN에 해당하는 VLAN 포트를 생성하고, 동적 라우팅 프로토콜을 설정할 수 있습니다

22.8.4 MAC 주소 테이블의 에이징(Aging)

이더넷 링 보호 프로토콜은 토폴로지가 변경될 때 스위치의 MAC 주소 테이블 에이징 시간을 제어하여 데이터 패킷을 올바른 링크로 전달합니다.

일반적으로 MAC 주소가 테이블에서 에이징되는 기본 시간은 300초입니다. 링 보호 프로토콜은 MAC 주소 테이블의 에이징을 단시간 내에 제어할 수 있습니다.

22.8.5 완전한 링 네트워크의 상태 기호 (Symbol)

마스터 노드와 트랜짓 노드는 현재 링 네트워크가 완전한지 여부를 "COMPLETE" 상태 기호를 통해 표시할 수 있습니다. 마스터 노드에서는 모든 링 네트워크의 링크가 정상이고, 주 포트가 전달 상태이며 보조 포트가 차단 상태일 때 "COMPLETE" 상태가 참이 됩니다. 링 네트워크의 상태 기호는 사용자가 현재 네트워크의 토폴로지 상태를 판단하는 데 도움을 줍니다.

22.9EAPS 패킷의 종류

EAPS 패킷은 아래와 같이 분류됩니다.

패킷 종류	설명
Loopback Detection (HEALTH)	마스터 노드에서 전송되며 링 네트워크의 토폴로지가 완전한지 여부를 감지합니다.
LINK-DOWN	링에서 링크가 끊어졌음을 나타내는 패킷으로, 트랜짓 노드에서 전송됩니다.
RING-DOWN-FLUSH-FDB	링 네트워크의 장애가 감지된 후 마스터 노드에서 전송되며, 트랜짓 노드의 MAC 주소 에이징 테이블 정보를 포함합니다.
RING-UP-FLUSH-FDB	링 네트워크의 장애가 복구된 후 마스터 노드에서 전송되며, 트랜짓 노드의 MAC 주소 에이징 테이블 정보를 포함합니다.

EAPS 패킷은 링 네트워크의 상태를 관리하고 복구를 지원하기 위해 중요한 정보를 전달합니다.

22.10 Fast Ethernet Ring Protection 메커니즘

22.10.1 마스터 노드의 링 감지 및 제어

마스터 노드는 주 포트를 통해 제어 VLAN으로 HEALTH 패킷을 주기적으로 전송합니다(주기는 설정 가능). 정상적인 경우, 이 HEALTH 패킷은 링 네트워크의 모든 노드를 통과한 후 마스터 노드의 보조 포트로 도달합니다. 보조 포트는 초기 상태에서 모든 데이터 VLAN을 차단합니다. HEALTH 패킷을 계속 수신하면 보조 포트는 데이터 VLAN을 차단하며 루프를 방지합니다.

보조 포트가 일정 시간(설정 가능) 동안 HEALTH 패킷을 수신하지 못하면, 링 네트워크가 비정상으로 간주됩니다. 이때 마스터 노드는 보조 포트의 데이터 VLAN 차단을 해제하고, 로컬 MAC 주소 테이블을 에이징하며, RING-DOWN-FLUSH-FDB 패킷을 전송하여 다른 노드에 이를 알립니다.

링 네트워크가 복구되고 마스터 노드가 보조 포트를 통해 HEALTH 패킷을 수신하면, 마스터 노드는 즉시 보조 포트에서 데이터 VLAN을 차단하고, 로컬 토폴로지 정보를 갱신하며, RING-UP-FLUSH-FDB 패킷을 통해 다른 노드에 MAC 주소 테이블을 에이징하도록 보고합니다.

관련 명령을 사용하여 Hello-time 노드 및 Fail-time 노드에서 주 포트의 HEALTH 패킷 전송 간격과 보조 포트의 HEALTH 패킷 대기 시간을 설정할 수 있습니다.

22.10.2 트랜짓 노드의 비정상 링크 알림

트랜짓 노드의 트랜짓 포트가 비정상 상태가 되면, 다른 트랜짓 포트를 통해 즉시 LINK-DOWN 패킷을 전송하여 다른 노드에 알립니다.

정상적인 경우, 이 패킷은 다른 트랜짓 노드를 통과한 후 마스터 노드의 한 포트에 도달합니다.

마스터 노드가 LINK-DOWN 패킷을 수신하면, 링 네트워크가 비정상 상태로 간주됩니다. 마스터 노드는 보조 포트의 데이터 VLAN 차단을 해제하고, 로컬 MAC 주소 테이블을 에이징하며, RING-DOWN-FLUSH-FDB 패킷을 전송하여 다른 노드에 알립니다.

22.10.3 트랜짓 노드 링크 복구

트랜짓 포트가 복구된 후 즉시 데이터 VLAN 패킷을 전송하지 않고, Pre-Forwarding 상태로 진입합니다.

- Pre-Forwarding 상태의 트랜짓 포트는 제어 VLAN에서 제어 패킷만 전송하고 수신합니다.

링 네트워크에서 트랜짓 포트 하나만 비정상 상태였고, 해당 포트가 Pre-Forwarding 상태로 진입

한 경우, 마스터 노드의 보조 포트는 주 포트로부터 다시 HEALTH 패킷을 수신할 수 있습니다.

- 이때 마스터 노드는 보조 포트에서 데이터 VLAN을 다시 차단하고, MAC 주소 테이블 에이징 알림을 전송합니다.
- Pre-Forwarding 상태의 트랜짓 포트가 MAC 주소 테이블 에이징 알림을 수신하면, 해당 포트를 Forwarding 포트로 변경하고 로컬 MAC 주소 테이블을 에이징합니다.

트랜짓 노드가 마스터 노드로부터 MAC 주소 테이블 에이징 알림을 수신하지 못하면, 마스터 노드로의 링크가 비정상이라고 판단하여 Pre-Forwarding 포트를 자동으로 Forwarding 포트로 전환합니다.

관련 명령을 사용하여 Pre-Forward-Time 노드를 통해 트랜짓 포트가 Pre-Forwarding 상태를 유지하는 시간을 설정할 수 있습니다.

22.11 기본 EAPS 설정

참고 : Fast Ethernet 보호 프로토콜과 STP(Spanning Tree Protocol)는 함께 설정할 수 없습니다. STP를 비활성화한 후, spanning-tree bpdu-terminal 명령을 실행하는 것이 권장됩니다. 이를 통해 링 노드에서 BPDU(Bridge Protocol Data Unit)가 전달되지 않도록 하여 브로드캐스트 폭풍을 방지할 수 있습니다.

Ethernet 링 보호 프로토콜과 STP의 기본 설정은 다음과 같습니다.

항목	기본 설정
Spanning tree protocol	spanning-tree mode rstp
Fast Ethernet Ring Protection	구성 없음

기본적으로 STP가 활성화된 상태이며, Fast Ethernet 링 보호 프로토콜은 설정되지 않은 상태로 시작합니다.

22.12 구성 전 요구 사항

MEAPS(Master Ethernet Automatic Protection Switching)를 구성하기 전에 아래 내용을 확인해주기 바랍니다.

- 링 보호 프로토콜의 중요한 기능 중 하나는 브로드캐스트 폭풍을 방지하는 것입니다. 따라서 링 링크가 다시 연결되기 전에 모든 링 노드가 구성되었는지 확인해야 합니다. 구성이 완료되지 않은 상태에서 링 네트워크가 연결되면 브로드캐스트 폭풍이 발생할 가능성이 높습니다.
- EAPS는 STP와 잘 호환되지만, EAPS로 제어되는 포트는 STP의 영향을 받지 않습니다.
- 링 보호 프로토콜은 하나의 스위치에 여러 링 네트워크를 구성할 수 있습니다.
- 링 제어 VLAN을 구성하면, 해당 시스템 VLAN이 자동으로 생성됩니다.
- 각 링의 포트는 해당 링의 제어 VLAN에서 오는 패킷을 전달할 수 있지만, 다른 포(Trunk 모드 포트 포함)는 제어 VLAN의 패킷을 전달할 수 없습니다.
- 기본적으로 마스터 노드의 Fail-time은 Hello-time의 세 배로 설정됩니다. 이는 패킷 지연으로 인해 링 보호 프로토콜에 충격이 가지 않도록 합니다. Hello-time을 수정하면 Fail-time도 적절히 수정해야 합니다.

- 기본적으로 트랜짓 노드의 Pre-Forward-Time은 마스터 노드의 Hello-time의 세 배로 설정됩니다. 이는 마스터 노드가 링 네트워크 복구를 감지하기 전에 트랜짓 포트가 Pre-

Forwarding 상태로 들어가지 않도록 보장합니다. 만약 마스터 노드의 Hello-time이 트랜짓 노드의 Pre-Forward-Time보다 길게 설정되면, 루프백이 쉽게 발생하며 브로드캐스트 폭풍이 유발될 수 있습니다.

- 물리 인터페이스, Fast Ethernet 인터페이스, Gigabit Ethernet 인터페이스 및 집계 인터페이스는 모두 링 인터페이스로 설정할 수 있습니다.그러나 물리 인터페이스에 링크 집계(Link Aggregation), 802.1X, 또는 포트 보안(Port Security)이 이미 구성되어 있다면, 해당 물리 인터페이스를 링 인터페이스로 설정할 수 없습니다.

22.13 MEAPS 구성 작업

- 마스터 노드 구성
- 트랜짓 노드 구성
- 링 포트 구성
- 링 보호 프로토콜 상태 확인

22.14 Fast Ethernet Ring Protection 구성

22.14.1 마스터 노드 구성

명령어	설명
Switch#config	스위치 구성 모드로 진입합니다.
Switch_config#ether-ring *id*	노드를 설정하고, 노드 구성 모드로 진입합니다. id: 인스턴스 ID
Switch_config_ring#control-vlan *vlan-id*	제어 VLAN을 구성합니다. vlan-id: 제어 VLAN의 ID
Switch_config_ring#master-node	노드 유형을 마스터 노드로 설정합니다.
Switch_config_ring#hello-time *value*	이 단계는 선택 사항입니다. 마스터 노드가 HEALTH 패킷을 전송하는 주기를 설정합니다. value: 1~10초 범위의 시간 값, 기본값은 1초
Switch_config_ring#fail-time *value*	이 단계는 선택 사항입니다. 보조 포트가 HEALTH 패킷을 대기하는 시간을 설정합니다. value: 3~30초 범위의 시간 값, 기본값은 3초
Switch_config_ring#exit	현재 설정을 저장하고 노드 구성 모드를 종료합니다.

참고 : no ether-ring id 명령을 사용하여 이더넷 링의 노드 설정 및 포트 설정을 삭제할 수 있습니다.

22.14.2 트랜짓 노드 구성

스위치를 링 네트워크의 트랜짓 노드로 설정하려면 다음 단계를 따르십시오.

명령어	설명
Switch#config	스위치 구성 모드로 진입합니다.
Switch_config#ether-ring *id*	노드를 설정하고, 노드 구성 모드로 진입합니다. id: 인스턴스 ID
Switch_config_ring#control-vlan *vlan-id*	제어 VLAN을 구성합니다. vlan-id: 제어 VLAN의 ID
Switch_config_ring#transit-node	노드 유형을 마스터 노드로 설정합니다.
Switch_config_ring#pre-forward-time *value*	이 단계는 선택 사항입니다. 트랜짓 포트에서 Pre-Forward 상태를 유지하는 시간을 설정합니다. value: 3~30초 범위의 시간 값, 기본값은 3초
Switch_config_ring#exit	현재 설정을 저장하고 노드 구성 모드를 종료합니다.

22.14.3 링 포트 구성

스위치의 포트를 이더넷 링의 포트로 설정하려면 다음 단계를 따르십시오.

명령어	설명
Switch#config	스위치 구성 모드로 진입합니다.
Switch_config#interface *intf-name*	인터페이스 구성 모드로 진입합니다. intf-name: 인터페이스 이름
Switch_config_intf#ether-ring *id* **{primary-port | secondary-port | transit-port }**	이더넷 링의 포트 유형을 설정하며, 링의 노드 ID도 함께 지정해야 합니다.
Switch_config_intf#exit	현재 설정을 저장하고 노드 구성 모드를 종료합니다.

참고 : no ether-ring id {primary-port | secondary-port | transit-port} 명령을 사용하여 이더넷 링의 포트 설정을 취소할 수 있습니다.

22.14.4 링 보호 프로토콜 상태 확인

다음 명령을 실행하여 링 보호 프로토콜의 상태를 확인할 수 있습니다.

명령어	설명
show ether-ring *id*	링 보호 프로토콜 및 이더넷 링 포트의 요약 정보를

	확인합니다. id: 이더넷 링의 ID
show ether-ring *id* **detail**	링 보호 프로토콜 및 이더넷 링 포트의 상세 정보를 확인합니다.
show ether-ring *id* **interface** *intf-name*	이더넷 링 포트 또는 일반 포트의 상태를 확인합니다. intf-name: 인터페이스 이름

22.15 MEAPS 구성

22.15.1 설정 예제

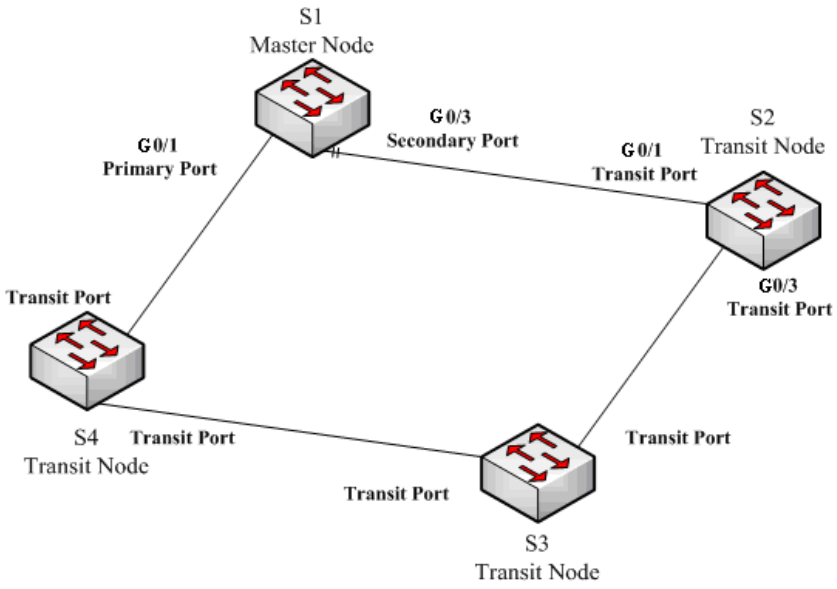


그림 29 MEAPS 구성

링 네트워크에서 S1(마스터 노드)과 S2(트랜짓 노드) 구성

- 스위치 S1 구성 (마스터 노드)
- STP 비활성화 및 이더넷 링 노드 설정

  S1_config#no spanning-tree

  S1_config#ether-ring 1

  S1_config_ring1#control-vlan 2

  S1_config_ring1#master-node
- 시간 관련 매개변수 설정

  S1_config_ring1#hello-time 2

S1_config_ring1#fail-time 6

- 노드 구성 모드 종료

S1_config_ring1#exit

- 주 포트와 보조 포트 설정

S1_config#interface gigaEthernet 0/1

S1_config_g0/1#ether-ring 1 primary-port

S1_config_g0/1#exit

S1_config#interface gigaEthernet 0/3

S1_config_g0/3#ether-ring 1 secondary-port

S1_config_g0/3#exit

- 제어 VLAN 생성

S1_config#vlan 2

S1_config_vlan2#exit

- 포트모드 설정

S1_config#interface range g0/1 , 3

S1_config_if_range#switchport mode trunk

S1_config_if_range#exit

- 스위치 S2 구성 (트랜짓 노드)
- STP 비활성화 및 이더넷 링 노드 설정

S2_config#no spanning-tree

S2_config#ether-ring 1

S2_config_ring1#control-vlan 2

S2_config_ring1#transit-node

- Pre-Forward 시간 설정

S2_config_ring1#pre-forward-time 8

- 노드 구성 모드 종료

S2_config_ring1#exit

- 트랜짓 포트 설정

S2_config#interface gigaEthernet 0/1

S2_config_g0/1#ether-ring 1 transit-port

S2_config_g0/1#exit

S2_config#interface gigaEthernet 0/3

S2_config_g0/3#ether-ring 1 transit-port

S2_config_g0/3#exit

- 제어 VLAN 생성

S2_config#vlan 2

S2_config_vlan2#exit

- 포트 모드 설정

S2_config#interface range gigaEthernet 0/1 , 3

S2_config_if_range#switchport mode trunk

S2_config_if_range#exit

참고 :

- S2와 동일한 방식으로 다른 트랜짓 노드를 구성합니다.

제어 VLAN은 링 네트워크의 모든 노드에서 동일한 ID로 구성해야 합니다.

23 EAPS와 MEAPS

EAPS(Ethernet Automatic Protection Switching)는 이더넷 링의 링크 계층에서 동작하는 특화된 프로토콜입니다.

- EAPS 작동 원리:
  - ① 이더넷 링이 완전한 상태일 때, 데이터 루프백으로 인해 브로드캐스트 스톰이 발생하는 것을 방지해야 합니다.
  - ② 반면, 이더넷 링의 링크가 끊어지면 백업 링크를 신속히 활성화하여 링 내 서로 다른 노드 간의 통신을 복구해야 합니다.
  - ③ 스위치의 역할(마스터 노드 또는 트랜짓 노드)은 사용자가 설정을 통해 지정합니다.
- MEAPS(Master Ethernet Automatic Protection Switching):
  - ① MEAPS는 EAPS를 확장한 프로토콜로, 단일 링뿐만 아니라 2단계 다중 링 구조(Level-2 Multi-Ring Structure)도 지원합니다.
  - ② 다중 링 구조:

    집계 계층(Aggregation Layer): 중앙에 위치하며, 빠른 스위칭을 위해 집계 장비를 통해 이더넷 링을 구성합니다.

    접속 계층(Access Layer): 외곽에 위치하며, 접속 장비를 통해 연결됩니다.
  - ③ 서로 다른 계층의 링은 접점(Tangency) 또는 교차(Intersection) 방식으로 연결됩니다.

특정 토폴로지 구조: MEAPS의 구체적인 토폴로지는 아래 그림과 같이 구성됩니다. (그림 참조)

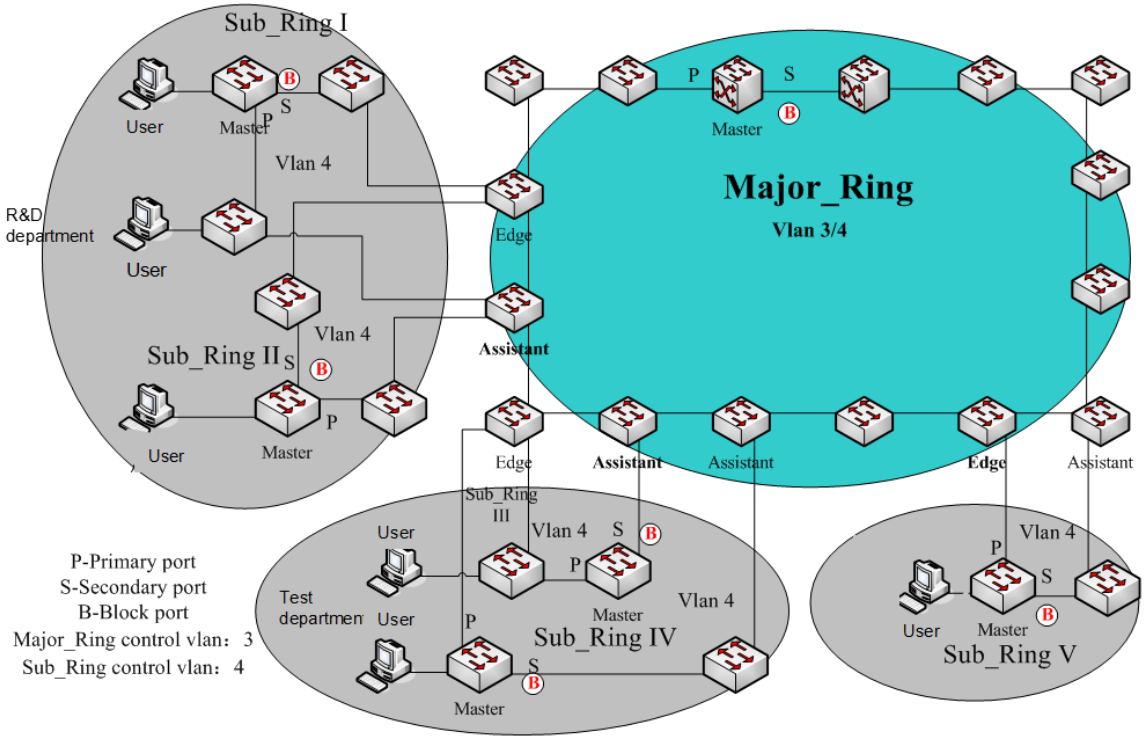


그림 30 MEAPS 구조

링 보호 프로토콜과 STP는 모두 링크 계층에서 토폴로지 제어에 사용됩니다.

STP는 다양한 복잡한 네트워크에 적합하며, 네트워크 토폴로지 변경을 홉 단위로 전파합니다.

링 보호 프로토콜은 링형 토폴로지에 특화되어 있으며, 네트워크 토폴로지 변경을 확산 방식으로 전파합니다. 이 때문에 링 네트워크에서 링 보호 프로토콜의 수렴 속도가 STP보다 빠릅니다. 정상적인 네트워크 환경에서 링 보호 프로토콜은 50ms 이내에 네트워크 통신을 복구할 수 있습니다.

23.1MEAPS의 기본 개념

23.1.1 도메인

도메인은 이더넷 루프백 보호 프로토콜의 보호 범위를 지정하며, 정수로 구성된 ID로 표시됩니다. 동일한 보호 데이터를 지원하고 동일한 제어 VLAN을 사용하는 스위치 그룹은 상호 연결되어 하나의 도메인을 형성할 수 있습니다.

하나의 도메인은 하나의 링만 포함할 수도 있고, 서로 교차하는 여러 링을 포함할 수도 있습니다. 그림 2를 참조하십시오.

MEAPS 도메인은 MEAPS 링, 제어 VLAN, 마스터 노드, 트랜짓 노드, 엣지 노드, 보조 엣지 노드로 구성됩니다.

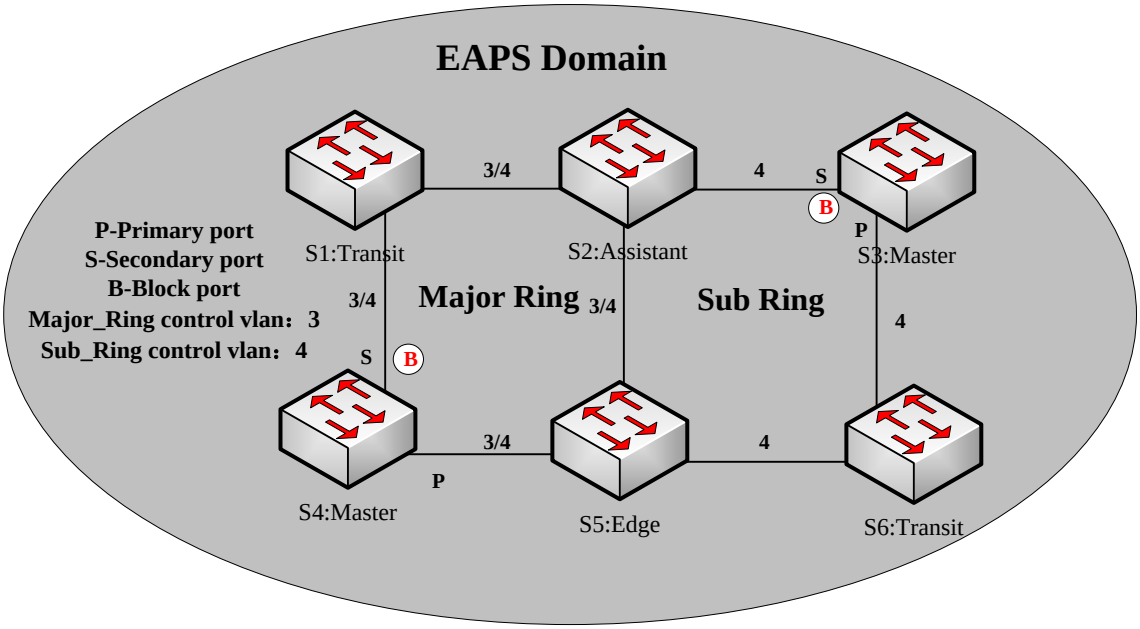


그림 31 MEAPS

23.1.2 링

링은 물리적으로 링형 이더넷 토폴로지에 해당하며, 상호 연결된 스위치 그룹으로 구성됩니다. 하나의 MEAPS 도메인은 하나의 MEAPS 링만 포함할 수도 있고, 서로 교차하는 여러 링을 포함할 수도 있습니다.

23.1.3 주요 링

도메인에 여러 개의 링이 포함된 경우, 주요 링을 제외한 링을 하위 링이라고 합니다.
주요 링에 있는 각 노드의 주 포트와 보조 포트는 메인 제어 VLAN과 서브 제어 VLAN에 동시에 추가되어야 합니다. 그림 2를 참조하십시오.

23.1.4 하위 링

도메인에 여러 개의 링이 포함된 경우, 그중 하나를 주요 링으로 선택해야 합니다.
하위 링에 있는 각 노드의 주 포트와 보조 포트는 서브 제어 VLAN에 추가되어야 합니다. 그림 2를 참조하십시오.

23.1.5 제어 VLAN

제어 VLAN은 데이터 VLAN과 대조되는 개념으로, MEAPS에서 제어 VLAN은 MEAPS 패킷을 전송하는 데 사용됩니다.

각 MEAPS는 메인 제어 VLAN과 서브 제어 VLAN, 두 개의 제어 VLAN을 사용합니다.

주요 링이나 하위 링을 구성할 때 메인 제어 VLAN을 지정해야 합니다.
구성 시 메인 제어 VLAN만 지정하면 되며, 메인 제어 VLAN ID보다 1 높은 ID를 가진 VLAN이 서브 제어 VLAN으로 자동 설정됩니다.
주요 링은 메인 제어 VLAN과 서브 제어 VLAN에 동시에 추가되지만, 하위 링은 서브 제어 VLAN에만 추가됩니다. 각 포트 옆의 번호 3과 4를 참조하십시오.

주요 링의 프로토콜 패킷은 메인 제어 VLAN을 통해 전송되며, 하위 링의 프로토콜 패킷은 서브 제어 VLAN을 통해 전송됩니다.
주요 링에서 서브 제어 VLAN은 주요 링의 데이터 VLAN 역할을 합니다.
스위치의 이더넷 링에 연결된 포트는 제어 VLAN에 속하며, 이더넷 링에 연결된 포트만 제어 VLAN에 추가될 수 있습니다.

참고 : 주요 링의 MEAPS 포트는 메인 제어 VLAN과 서브 제어 VLAN 모두에 속해야 합니다. 하위 링의 MEAPS 포트는 서브 제어 VLAN에만 속합니다 주요 링은 하위 링의 논리적 노드로 간주되며, 하위 링의 패킷은 주요 링을 통해 투명하게 전송됩니다. 주요 링의 패킷은 주요 링 내에서만 전송됩니다.

23.1.6 데이터 VLAN

데이터 VLAN은 제어 VLAN과 구분되며, 데이터 패킷을 전송하는 데 사용됩니다. 데이터 VLAN에는 MEAPS 포트와 비-MEAPS 포트가 모두 포함될 수 있습니다. 하나의 도메인은 하나 이상의 데이터 VLAN을 보호할 수 있습니다.

도메인 내에서 링 보호 프로토콜에 의해 계산된 토폴로지는 해당 도메인의 데이터 VLAN에만 영향을 미칩니다.
데이터 VLAN이 생성되지 않아도 링 상태 기계의 동작에는 영향을 미치지 않습니다. MEAPS 포트는 MEAPS 모듈에 의해 제어되고, 비-MEAPS 포트는 STP 모듈에 의해 제어됩니다.

참고 : MSTP 모듈과 유사한 처리 방식을 사용할 수 있습니다. 기본 STP 인스턴스에서 포트의 상태는 포트의 링크 상태에 따라 결정되며, VLAN 설정과는 상관이 없습니다.

23.1.7 마스터 노드

마스터 노드는 링의 정책 수립과 제어를 담당합니다. 각 링에는 하나의 마스터 노드만 존재할 수 있습니다.
마스터 노드는 링의 토폴로지가 완전한지 적극적으로 확인하고, 루프백을 제거하며, 다른 스위치

가 토폴로지 정보를 업데이트하도록 제어합니다.
그림에서 S3은 하위 링의 마스터 노드이고, S4는 주요 링의 마스터 노드입니다.

23.1.8 트랜짓 노드

이더넷 상의 모든 스위치 중 마스터 노드를 제외한 스위치들은 트랜짓 노드로 간주됩니다.
트랜짓 노드는 링의 로컬 포트 상태만 확인하며, 비정상 링크를 마스터 노드에 알립니다.
그림에서 S1, S2, S5, S6이 모두 트랜짓 노드입니다.

23.1.9 엣지 노드와 보조 노드

하위 링과 주요 링이 교차하면 두 개의 교차 지점이 생기며, 이 지점에 인접한 두 스위치를 각각 엣지 노드와 보조 노드라고 합니다. 두 노드는 모두 하위 링에 속합니다. 엣지 노드와 보조 노드로 설정될 스위치를 선택하는 데 특별한 제한은 없지만, 두 스위치는 각각 엣지 노드와 보조 노드로 설정되어야 합니다. 엣지 노드와 보조 노드는 하위 링에서의 역할이며, 주요 링에서는 트랜짓 노드 또는 마스터 노드로 동작합니다.
그림에서 S2는 보조 노드이고, S5는 엣지 노드입니다.

23.1.10 주 포트와 보조 포트

마스터 노드가 이더넷 링에 접근하는 두 포트를 주 포트와 보조 포트라고 합니다. 두 포트의 역할은 사용자에 의해 설정됩니다.

주 포트는 정상 상태일 때 전송 상태에 있습니다. 이 포트는 마스터 노드의 데이터 VLAN 패킷을 전송하고, 제어 VLAN의 제어 패킷을 수신 및 전송합니다. 마스터 노드는 주 포트를 통해 제어 VLAN으로 루프백 감지 패킷을 전송합니다.
주 포트가 비정상 상태에서 복구되면, 마스터 노드는 제어 VLAN으로 주소 에이징 알림을 즉시 전송한 후 주 포트를 통해 루프백 감지 패킷 전송을 시작합니다.

보조 포트는 정상 상태일 때 전송 또는 차단 상태에 있을 수 있습니다. 마스터 노드는 보조 포트를 통해 링 감지 패킷을 수신하고, 이를 통해 링 네트워크의 토폴로지가 완전한지 판단합니다.
토폴로지가 완전한 경우, 마스터 노드는 보조 포트에서 데이터 패킷을 차단하여 루프백 발생을 방지합니다. 링 네트워크의 링크가 끊어지면, 마스터 노드는 보조 포트를 열어 데이터 패킷을 전송합니다.

참고 : 포트는 노드의 주 포트 또는 보조 포트로 설정될 수 있으며, 동시에 두 역할을 가질 수는 없습니다.

23.1.11 트랜짓 포트

트랜짓 노드가 이더넷 링에 접근하는 두 포트는 모두 트랜짓 포트입니다. 두 포트의 역할은 사용자가 설정을 통해 지정할 수 있습니다.

트랜짓 포트는 정상 상태일 때 전송 상태 또는 프리포워딩 상태에 있습니다.
트랜짓 포트는 제어 VLAN에서 제어 패킷을 수신하며, 동시에 이 패킷을 제어 VLAN의 다른 포트로 전달합니다.
트랜짓 포트가 비정상 상태에서 복구되면 먼저 프리포워딩 상태로 진입하며, 이 상태에서는 제어 패킷만 수신 및 전송하고 데이터 VLAN은 차단합니다.
트랜짓 노드가 주소 테이블 에이징 알림을 수신한 후 트랜짓 포트는 전송 상태로 전환됩니다.

참고 : 포트는 노드의 주 포트 또는 트랜짓 포트로 설정될 수 있으며, 설정 후 다시 변경할 수 없습니다.

23.1.12 공통 포트와 엣지 포트

엣지 노드와 보조 노드는 하위 링과 주요 링이 교차하는 지점입니다. 이 지점에서 이더넷에 접속하는 두 포트 중 하나는 공통 포트이며, 이는 하위 링과 주요 링의 공용 포트 역할을 합니다. 다른 하나는 하위 링 내의 엣지 포트입니다. 두 포트의 역할은 사용자가 설정을 통해 지정합니다.

공통 포트는 주요 링 포트에 속하며, 상태는 주요 링 포트의 상태에 의해 결정됩니다. 공통 포트 자체는 별도의 동작이나 알림 기능을 가지지 않습니다. 공통 포트에 연결된 링크가 변경되더라도 공통 포트가 위치한 하위 링 노드에는 알림이 전달되지 않습니다. 공통 포트의 존재 목적은 링의 완전성을 보장하는 데 있습니다.

엣지 노드의 엣지 포트는 정상 상태일 때 전송 상태 또는 프리포워딩 상태에 있습니다. 이 포트의 기본 동작은 트랜짓 포트와 유사하지만 주요 링의 완전성을 감지하기 위해 엣지 헬로 패킷을 주요 링 포트로 전송하는 추가 기능이 있습니다.

보조 노드의 엣지 포트는 전송 상태, 프리포워딩 상태 또는 엣지 프리포워딩 상태일 수 있습니다. 보조 노드의 엣지 포트는 트랜짓 포트와 동일한 특성을 가지지만 엣지 프리포워딩 상태라는 추가 상태가 있습니다. 엣지 포트가 전송 상태이고 해당 주요 링 포트가 엣지 헬로 패킷을 수신하지 못한 경우, 엣지 포트는 엣지 프리포워딩 상태로 전환됩니다. 이 상태에서는 제어 패킷만 수신 및 전송하며 데이터 VLAN은 차단됩니다. 주요 링 포트가 다시 엣지 헬로 패킷을 수신하면 엣지 포트는 원래 상태로 복귀합니다.

엣지 노드와 보조 노드의 엣지 포트는 주요 링의 완전성을 감지하는 데 사용됩니다. 이에 대한 자세한 내용은 다음 장에서 다룰 하위 링 프로토콜 패킷의 채널 상태 점검 메커니즘을 참조하십시오.

참고 : 각 포트는 노드에서 단 하나의 엣지 포트로만 설정될 수 있으며, 설정 후 다시 구성할 수 없습니다. 공통 포트는 주요 링의 포트에서만 설정할 수 있으며, 주요 링 포트가 없는 포트에는 구성할 수 없습니다.

23.1.13 MAC 주소 테이블의 에이징 (FLUSH MAC FDB)

이더넷 링 보호 프로토콜은 토폴로지가 변경될 때 스위치의 MAC 주소 테이블 에이징을 제어하여 데이터 패킷을 올바른 링크로 전송할 수 있습니다. 일반적으로 MAC 주소가 테이블에서 에이징되는 기본 시간은 300초입니다.
링 보호 프로토콜은 MAC 주소 테이블의 에이징을 짧은 시간 내에 제어할 수 있습니다.

23.1.14 링의 완전성 플래그

마스터 노드와 트랜짓 노드는 상태 기호 "COMPLETE"를 통해 현재 링 네트워크가 완전한지 여부를 나타낼 수 있습니다.

마스터 노드에서는 모든 링 네트워크 링크가 정상이고, 주 포트가 전송 상태이며 보조 포트가 차단 상태일 때만 "COMPLETE" 상태가 참으로 표시됩니다.
트랜짓 노드에서는 두 트랜짓 포트가 모두 전송 상태일 때만 "COMPLETE" 상태가 참으로 표시됩니다.

링 네트워크의 상태 기호는 사용자가 현재 네트워크의 토폴로지 상태를 판단하는 데 도움을 줍니다.

23.1.15 EAPS 패킷의 종류

패킷 종류	설명
Ring Detection (HEALTH)	마스터 노드에서 전송되며, 링 네트워크의 토폴로지가 완전한지 감지합니다.
link interruption (LINK-DOWN)	링에서 링크가 끊어진 경우를 나타내며, 트랜짓 노드에서 전송됩니다.
MAC address aging table of the transit node (RING-DOWN-FLUSH-FDB)	링 네트워크의 중단이 감지된 후 마스터 노드에서 전송되며, 트랜짓 노드의 MAC 주소 에이징 테이블을 포함합니다.
Ring resume aging address table (RING-UP-FLUSH-FDB)	링 네트워크의 중단이 복구된 후 마스터 노드에서 전송되며, 트랜짓 노드의 MAC 주소 에이징 테이블을 포함합니다.

Ring completeness detection (EDGE-HELLO)	엣지 노드의 엣지 포트에서 결정되며, 엣지 노드와 대응하는 주요 링 포트에서 전송되어 주요 링의 완전성을 감지합니다.

23.2 Fast Ethernet 링 보호 메커니즘

23.2.1 폴링 메커니즘

주 포트는 HEALTH 패킷을 제어 VLAN으로 전송합니다. 정상적인 경우, HEALTH 패킷은 링의 모든 노드를 통과하여 최종적으로 마스터 노드의 보조 포트에 도달합니다.

보조 포트는 초기 상태에서 모든 데이터 VLAN을 차단합니다. HEALTH 패킷을 지속적으로 수신하면 보조 포트는 데이터 VLAN을 차단하여 루프백을 방지합니다.
만약 보조 포트가 주 포트로부터 일정 시간(구성 가능) 동안 HEALTH 패킷을 수신하지 못하면, 링 네트워크가 비정상 상태로 간주됩니다. 이 경우 마스터 노드는 다음 작업을 수행합니다.

- 보조 포트에서 데이터 VLAN 차단 해제
- 로컬 MAC 주소 테이블 에이징
- RING-DOWN-FLUSH-FDB 패킷 전송으로 다른 노드에 알림

반면, 마스터 노드가 보조 포트에서 데이터 VLAN이 열려 있는 상태로 HEALTH 패킷을 수신하면, 링 네트워크가 복구된 것으로 간주됩니다. 이 경우 마스터 노드는 다음 작업을 수행합니다.

- 보조 포트에서 데이터 VLAN 차단
- 로컬 토폴로지 정보 업데이트
- RING-UP-FLUSH-FDB 패킷 전송으로 다른 노드가 MAC 주소 테이블을 에이징하도록 보고

다음 그림에서 마스터 노드인 S4는 HELLO 패킷을 주기적으로 전송합니다. 루프백 문제가 없으면 HELLO 패킷은 마스터 노드의 보조 포트에 도달하며, 마스터 노드는 보조 포트가 속한 데이터 VLAN의 데이터 전달을 차단하여 루프백 발생을 방지합니다.

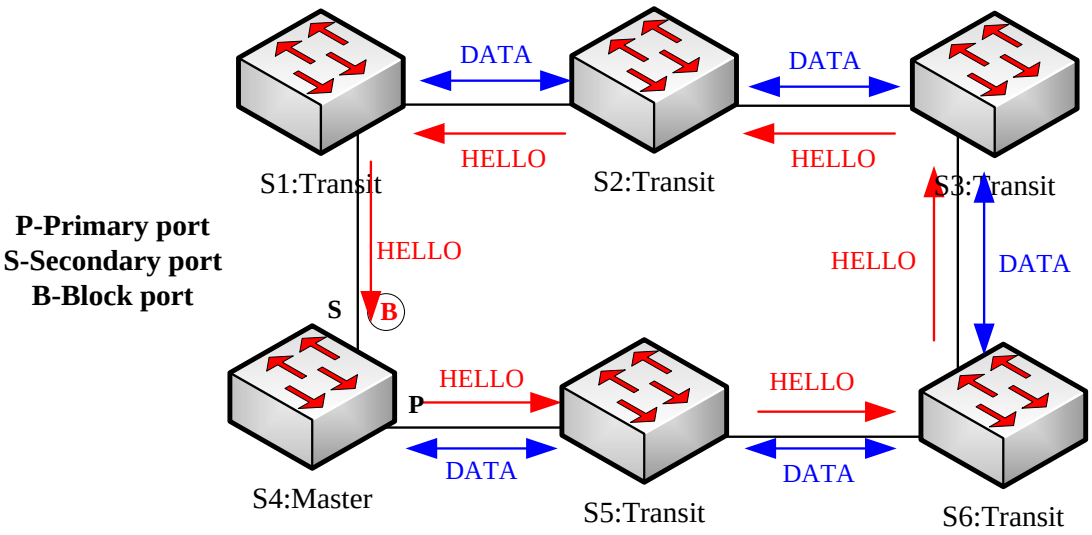


그림 32 폴링 메커니즘

참고 : Hello-time 노드와 Fail-time 노드에서 관련 명령어를 구성하여 주 포트가 HEALTH 패킷을 전송하는 간격과 보조 포트가 HEALTH 패킷을 대기하는 시간 제한을 수정할 수 있습니다.

트랜짓 노드의 비정상 링크 알림

링크 상태 변경 알림 메커니즘은 폴링 메커니즘보다 빠르게 링 네트워크 토폴로지 변화를 처리할 수 있습니다.

트랜짓 노드의 트랜짓 포트가 비정상 상태가 되면 다른 트랜짓 포트에서 즉시 LINK-DOWN 패킷을 전송하여 다른 노드에 이를 알립니다. 정상적인 경우 이 패킷은 다른 트랜짓 노드를 통과한 후 마스터 노드의 포트 중 하나에 도달합니다.

마스터 노드가 LINK-DOWN 패킷을 수신하면 링 네트워크가 비정상 상태라고 판단합니다. 이 경우 마스터 노드는 다음 작업을 수행합니다. 보조 포트에서 데이터 VLAN 차단을 해제합니다.

로컬 MAC 주소 테이블을 에이징합니다. RING-DOWN-FLUSH-FDB 패킷을 전송하여 다른 노드에 알립니다.

노드 S3과 S6 사이의 링크에서 문제가 발생한 경우를 예로 들면 S3과 S6은 문제가 발생했음을 감지한 후 해당 링크와 연결된 포트를 차단합니다. 이후 각각 다른 포트를 통해 LINK-DOWN 패킷을 전송합니다. 마스터 노드는 LINK-DOWN 패킷을 수신한 후 루프백에서 문제가 발생했음을 인식하고 더 이상 Fail-time을 대기하지 않고 즉시 조치를 취합니다.

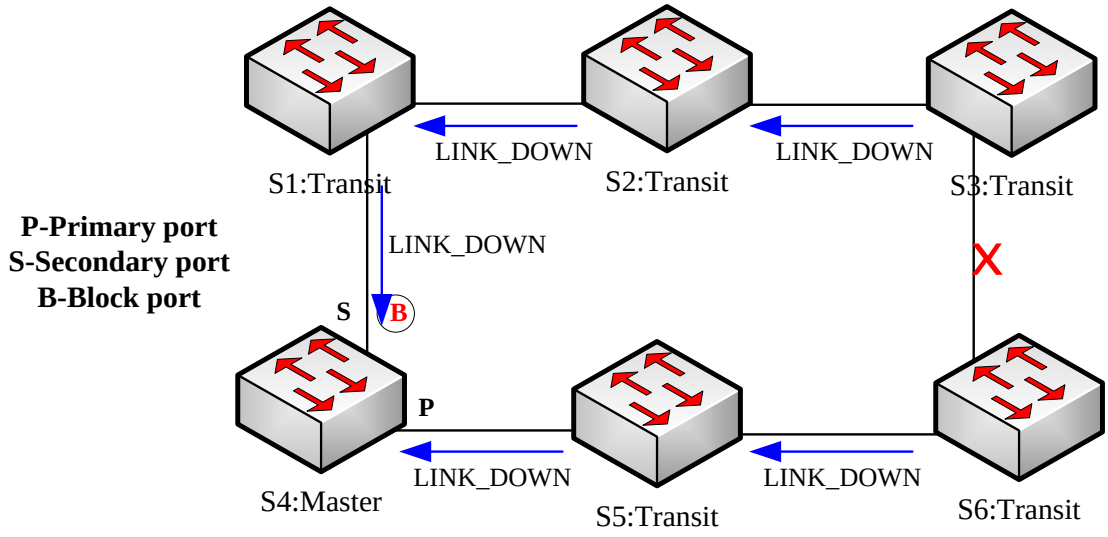


그림 33 링크 상태 변경 알림

트랜짓 포트가 복구된 후에는 즉시 데이터 VLAN의 패킷을 전송하지 않고 프리포워딩 상태로 진입합니다. 프리포워딩 상태의 트랜짓 포트는 제어 VLAN에서 제어 패킷만 전송하고 수신합니다.

링 네트워크에서 하나의 트랜짓 포트만 비정상 상태였다가 프리포워딩 상태로 진입한 경우, 마스터 노드의 보조 포트는 주 포트에서 HEALTH 패킷을 다시 수신할 수 있습니다. 이 경우 마스터 노드는 다시 보조 포트에서 데이터 VLAN을 차단하고, 외부로 주소 테이블 에이징 알림을 전송합니다. 프리포워딩 상태의 트랜짓 포트가 주소 테이블 에이징 알림을 수신하면, 해당 포트를 전송 상태로 변경하고 로컬 MAC 주소 테이블을 에이징합니다.

트랜짓 노드가 마스터 노드로부터 주소 테이블 에이징 알림을 수신하지 못하면, 마스터 노드와 연결된 링크가 비정상이라고 판단하여 프리포워딩 포트를 자동으로 전송 상태로 전환합니다.

참고 : pre-forward-time 노드를 통해 관련 명령을 구성하여 트랜짓 포트가 프리포워딩 상태를 유지하는 시간을 수정할 수 있습니다.

23.2.2 주요 링에서 하위 링 프로토콜 패킷의 채널 상태 점검 메커니즘

주요 링의 포트는 주요 링의 제어 VLAN과 하위 링의 제어 VLAN에 동시에 추가됩니다.
따라서 하위 링의 프로토콜 패킷은 주요 링이 제공하는 채널을 통해 엣지 노드와 보조 노드의 엣지 포트 사이에서 브로드캐스트됩니다.
이러한 경우, 주요 링 전체가 하위 링의 하나의 노드(가상 트랜짓 노드와 유사)처럼 동작합니다.
아래 그림을 참조하십시오.

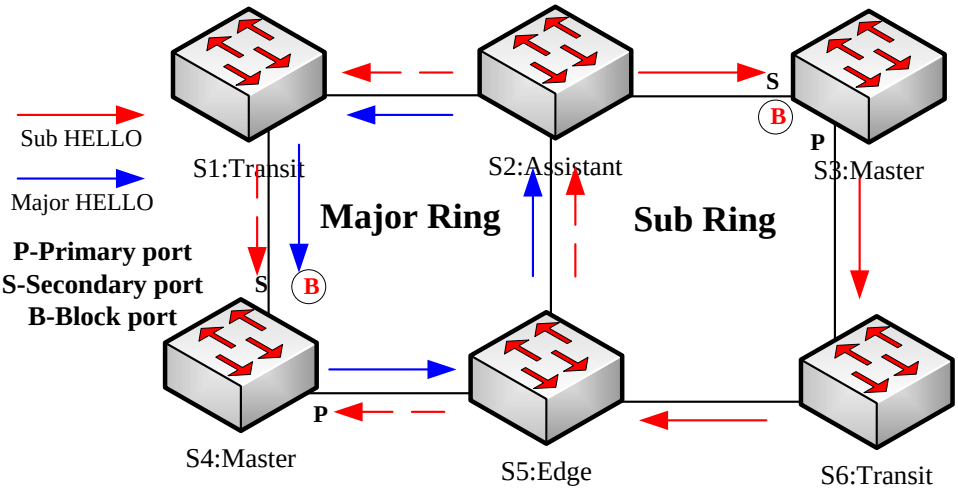


그림 34 주요 링과 하위 링의 교차

주요 링의 링크에 문제가 발생하고 엣지 노드와 보조 노드 사이의 하위 링 프로토콜 패킷 채널이 중단되면, 하위 링의 마스터 노드는 자신이 전송한 HELLO 패킷을 수신할 수 없습니다. 이 경우 Fail Time이 초과되며, 하위 링의 마스터 노드는 Failed 상태로 전환되고 보조 포트를 엽니다.

위 과정은 일반적인 네트워킹에서 효과적으로 보호 기능을 제공합니다. 이는 브로드캐스트 루프백을 방지할 뿐만 아니라 백업 링크의 기능도 보장합니다. 실제 네트워킹에서는 듀얼 홈 네트워킹 모드가 자주 사용됩니다. 아래 그림과 같이 듀얼 홈 네트워킹에서 하위 링 I과 하위 링 II는 엣지 노드와 보조 노드를 통해 상호 연결되어 큰 링을 형성합니다. 주요 링에 문제가 발생하면 모든 하위 링 마스터 노드의 보조 포트가 열리고, 큰 링에서 브로드캐스트 루프(화살표로 표시됨)가 형성됩니다.

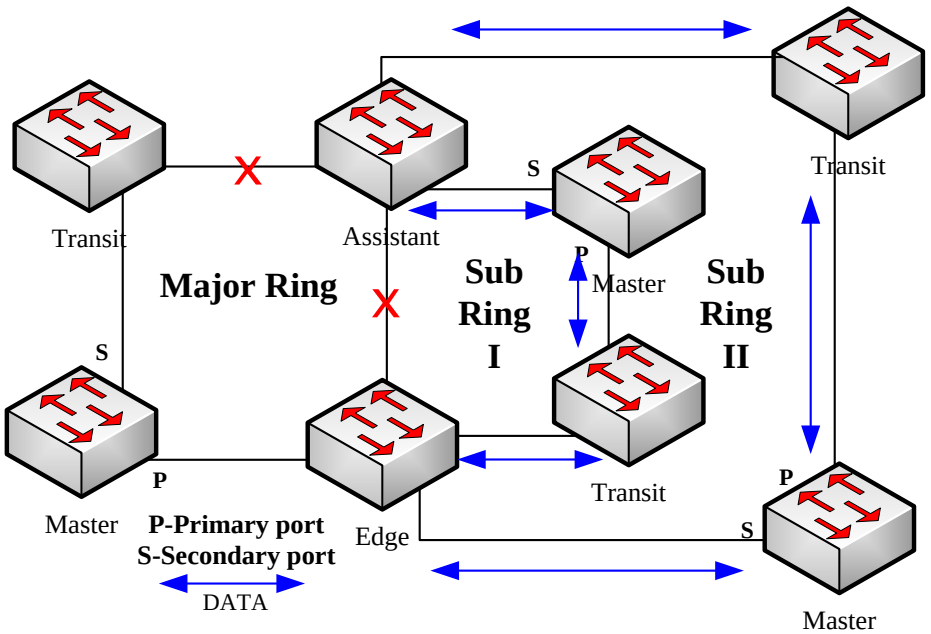


그림 35듀얼 홈 네트워킹 모드에서 발생하는 브로드캐스트 스톰

주요 링에서 하위 링 프로토콜 패킷의 채널 상태 점검 메커니즘은 듀얼 홈 링 문제를 해결하기 위해 도입되었습니다. 이 메커니즘은 엣지 노드와 보조 노드 사이 주요 링의 채널 링크 상태를 모니터링하며, 엣지 노드와 보조 노드의 협력이 필요합니다.

이 메커니즘의 목적은 하위 링의 마스터 노드의 보조 포트가 열리기 전에 엣지 노드의 엣지 포트를 차단하여 데이터 루프가 발생하지 않도록 하는 것입니다. 엣지 노드는 메커니즘의 트리거 역할을 하며, 보조 노드는 메커니즘의 리스너이자 결정자 역할을 합니다.

엣지 노드로부터의 알림 메시지가 수신되지 않으면, 엣지 포트는 즉시 차단 상태가 되며, 알림 메시지가 다시 수신될 때까지 차단 상태를 유지합니다. 주요 링에서 문제가 발생했을 때 이 메커니즘이 작동한 결과는 아래 그림에 표시되어 있습니다.

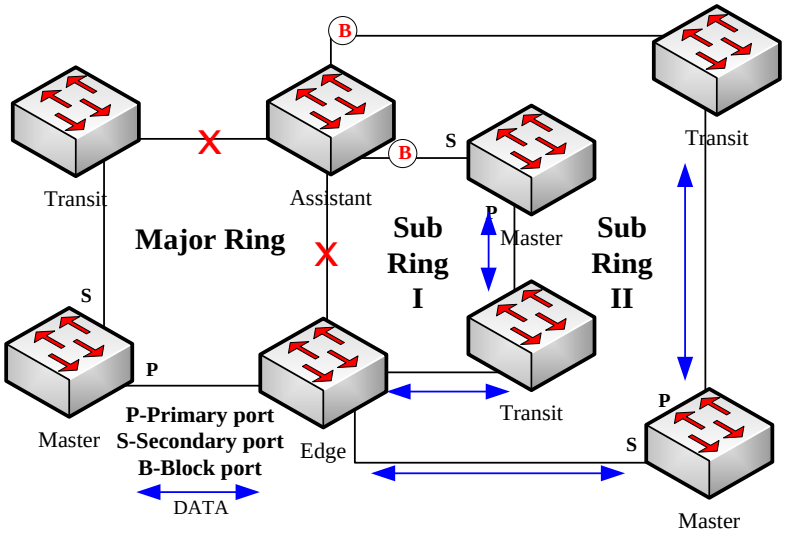


그림 36 채널 상태 점검 메커니즘의 결과

특히 주의해야 할 점은, 하위 링의 마스터 노드에서 보조 포트가 열리기 전에 보조 노드의 엣지 포트가 차단되어야 한다는 점입니다. 그렇지 않으면 브로드캐스트 스톰이 발생할 수 있습니다.

이 메커니즘의 전체 과정은 다음과 같습니다.

1. 엣지 노드와 보조 노드 사이 주요 링의 채널 상태를 점검합니다.
   하위 링의 엣지 노드는 주요 링의 두 포트를 통해 주기적으로 Edge-Hello 패킷을 전송합니다. 이 패킷은 주요 링의 모든 노드를 순차적으로 통과한 뒤 최종적으로 보조 노드에 도달합니다. 아래 그림을 참조하십시오.
   보조 노드가 규정된 시간 내에 Edge-Hello 패킷을 수신할 수 있다면 해당 채널이 정상임을 나타냅니다. 그렇지 않으면 채널이 중단되었음을 나타냅니다. Edge-Hello 패킷은 하위 링의 제어 패킷이지만, 주요 링의 포트를 통해 전송 및 수신되며 하위 링으로 전달되어 처리됩니다.

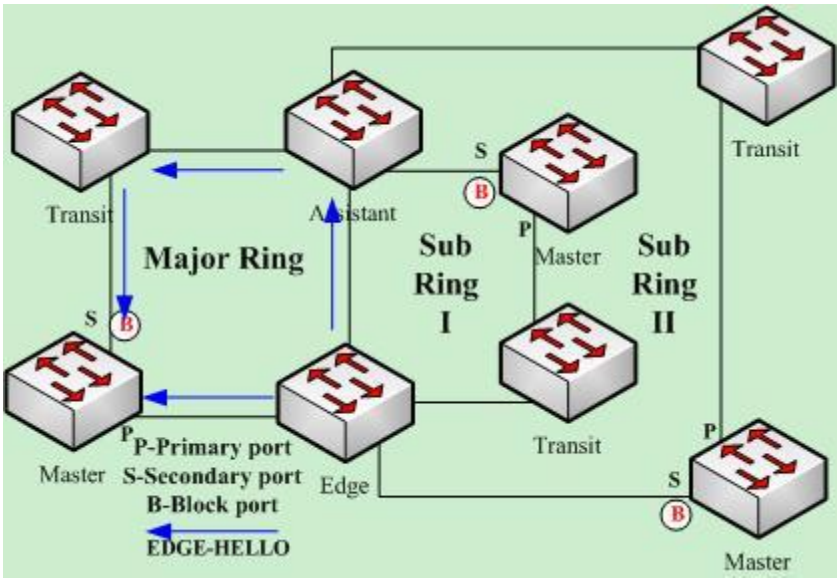


그림 37 엣지 노드와 보조 노드 사이 주요 링의 채널 상태 점검

2. 채널이 중단될 경우 엣지 노드는 엣지 포트를 차단합니다.

   보조 노드가 Edge Fail Time 동안 Edge-Hello 패킷을 수신하지 못하면, 보조 노드는 하위 링 프로토콜 패킷(Edge-Hello 패킷)의 채널이 중단되었다고 판단합니다.
   이 경우 보조 노드는 즉시 엣지 포트를 Edge-Preforwarding 상태로 변경하며, 데이터 패킷의 전달을 차단합니다. 단, 제어 패킷은 계속 수신 및 전달합니다.
   보조 노드는 또한 LINK-DOWN 패킷을 마스터 노드로 전송하여, 마스터 노드가 보조 포트를 열어 링의 모든 노드 간 통신 중단을 방지할 수 있도록 합니다.

참고 : 엣지 포트가 먼저 Edge-Preforwarding 상태로 전환되고 마스터 노드가 보조 포트를 여는 순서가 보장되려면 다음 조건을 충족해야 합니다.

엣지 노드가 Edge-Hello 패킷을 전송하는 주기(Edge Hello Time)가 마스터 노드가 Hello 패킷을 전송하는 주기(Hello Time)보다 작아야 합니다.

보조 노드의 Edge Fail Time은 마스터 노드의 Fail Time보다 작아야 합니다.

일반적으로 Fail Time은 Hello Time의 세 배이며, Edge Fail Time 역시 Edge Hello Time의 세 배입니다.

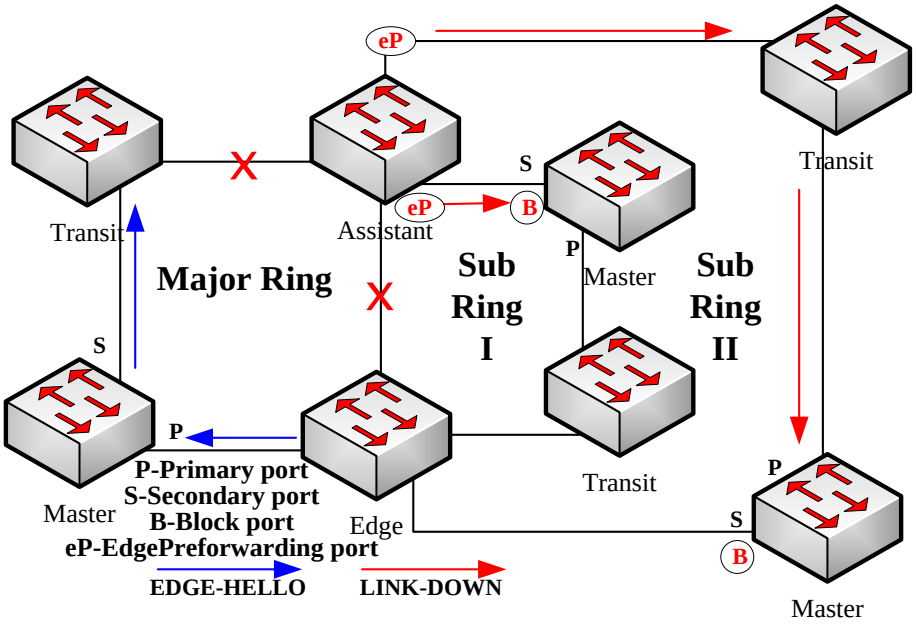


그림 38 채널 중단 시 엣지 노드에 의해 엣지 포트 차단

3. 채널 복구

주요 링의 링크와 엣지 노드와 보조 노드 간의 통신이 복구되면 하위 링 프로토콜 패킷의 채널도 정상 기능으로 복구됩니다.

이 경우, 하위 링의 마스터 노드는 자신이 전송한 Hello 패킷을 다시 수신하고 Complete 상태로 전환합니다. 마스터 노드는 보조 포트를 차단하고 RING-UP-FLUSH-FDB 패킷을 링으로 전송하여 모든 노드에 이를 알립니다.

동시에 보조 노드의 엣지 포트 상태는 Edge-Preforwarding에서 Forwarding으로 전환되며, 링 내 모든 노드 간 원활한 통신이 보장됩니다.

아래 그림은 채널이 복구되고 링의 통신이 정상적으로 복구된 상태를 보여줍니다.

참고 : 엣지 노드가 차단된 엣지 포트를 열기 전에, 하위 링의 마스터 노드에서 보조 포트가 차단되어 브로드캐스트 스톰을 방지해야 합니다.

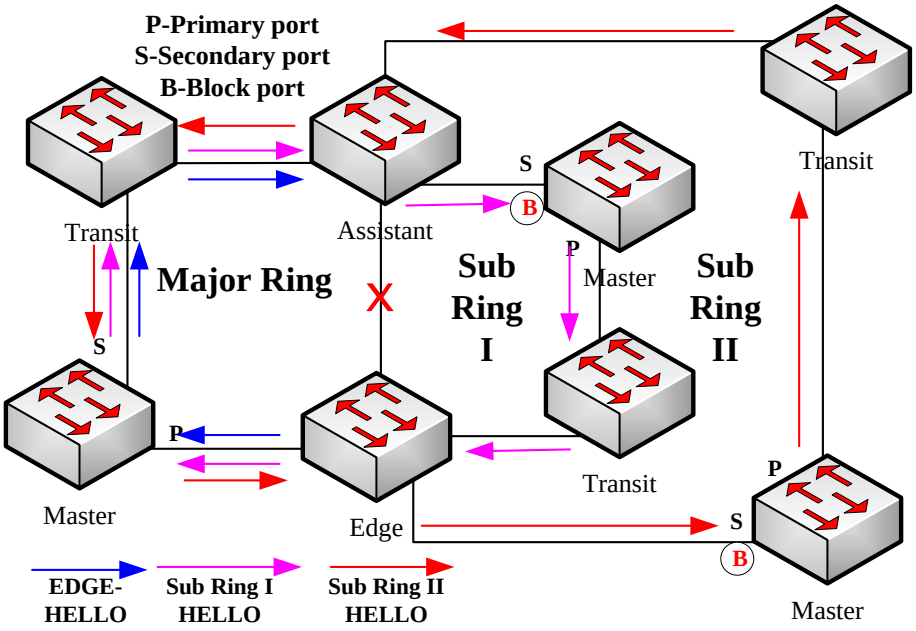

P-Primary port
S-Secondary port
B-Block port
Transit
Assistant
S
B
Transit
Major Ring
Sub Ring I
P
Master
Sub Ring II
S
P
Master
Edge
Transit
P
S
B
Master
EDGE-HELLO
Sub Ring I HELLO
Sub Ring II HELLO

그림 39 채널 복구

23.3 MEAPS 구성 전 요구 사항

MEAPS를 구성하기 전에 아래 항목을 주의 깊게 확인하십시오.

- 링 보호 프로토콜의 중요한 기능 중 하나는 브로드캐스트 스톰을 방지하는 것입니다. 링 링크를 다시 연결하기 전에 모든 링 노드가 구성되었는지 확인해야 합니다. 예를 들어, EAPS를 구성할 때는 마스터 노드와 모든 트랜짓 노드를 구성한 후 네트워크 케이블과 마스터 노드의 보조 포트를 연결해야 합니다. ERPS를 구성할 때는 모든 링 노드가 구성될 때까지 최소 하나의 링크를 연결하지 않은 상태로 유지해야 합니다.
- 링 보호 프로토콜을 스위치의 STP와 호환되도록 설정하려면 관련 구성을 통해 가능합니다. 사용자는 "no spanning-tree", SSTP, RSTP, PVST 또는 MSTP 모드를 설정할 수 있습니다.
- 링 노드의 인스턴스가 설정된 후에는 현재 링 노드를 삭제한 다음 다시 설정하지 않는 한 노드의 기본 정보를 변경할 수 없습니다. 시간 매개변수는 예외입니다.
- 구성된 노드를 확인하려고 show 명령을 실행했을 때 노드의 상태가 init으로 표시되면, 이는 노드의 구성이 완료되지 않았음을 의미하며, 따라서 노드를 시작할 수 없습니다. 이 경우 기본 정보를 수정하거나 추가하여 노드 구성을 완료해야 합니다.
- 링 보호 프로토콜은 스위치에서 여러 링 네트워크 구성을 지원합니다.
- 링의 제어 VLAN을 구성하면 자동으로 해당 VLAN이 생성되며, 사용자가 수동으로 설정할 필요는 없습니다.
- 각 링의 포트는 해당 링의 제어 VLAN에서 오는 패킷을 전달할 수 있지만, 다른 포트(Trunk 모드 포트 포함)는 제어 VLAN의 패킷을 전달할 수 없습니다.
- 기본적으로 마스터 노드의 Fail-time은 Hello-time의 세 배로 설정됩니다. 이는 패킷 지연으로 인한 링 보호 프로토콜의 충격을 방지하기 위한 것입니다. Hello-time이 수정되면 Fail-time도 이에 맞게 수정해야 합니다.
- 기본적으로 트랜짓 노드의 Pre-Forward-Time은 마스터 노드의 Hello-time의 세 배로 설정됩니다. 이는 트랜짓 포트가 Pre-Forwarding 상태로 진입하기 전에 마스터 노드가 링 네트워크의 복구를 감지할 수 있도록 보장합니다. 마스터 노드의 Hello-time이 트랜짓 노드의 Pre-Forward-Time보다 길게 설정되면 루프백이 발생하기 쉽고, 이로 인해 브로드캐스트 스톰이 유발됩니다.
- 사용자는 Edge Hello Time과 Edge Fail Time을 설정할 수 없습니다. 이 값들은 각각 Hello Time과 Fail Time의 1/3로 자동 결정됩니다.
- 물리 인터페이스, Fast-Ethernet 인터페이스, Gigabit-Ethernet 인터페이스, 그리고 집계 인터페이스는 모두 링 인터페이스로 설정할 수 있습니다. 그러나 물리 인터페이스에 이미

링크 집계, 802.1X 또는 포트 보안이 구성된 경우 해당 물리 인터페이스를 링 인터페이스로 설정할 수 없습니다.

- 이 프로토콜은 기존 EAPS와 기능적으로 유사하지만 링의 토폴로지가 더 높은 확장성과 유연성을 제공합니다. 따라서 MEAPS와 EAPS는 부분적으로 호환되며, MEAPS 링과 EAPS 링 간에 교차 구성을 수행할 수 있습니다.

23.4 MEAPS 구성 작업

- 마스터 노드 구성
- 트랜짓 노드 구성
- 엣지 노드와 보조 노드 구성
- 링 포트 구성
- 링 보호 프로토콜 상태 확인

23.5 Fast Ethernet 링 보호 구성

23.5.1 마스터 노드 구성

스위치를 링 네트워크의 마스터 노드로 설정하려면 다음 단계를 따르십시오.

명령어	설명
Switch#**config**	스위치 구성 모드로 진입합니다.
Switch_config#**mether-ring** *id1* **domain** *id2*	노드를 설정하고 노드 구성 모드로 진입합니다. id1: 노드의 인스턴스 ID id2: 도메인의 인스턴스 ID (0일 경우 생략 가능)
Switch_config_ring1#**master-node**	필수. 노드 유형을 마스터 노드로 설정합니다.
Switch_config_ring1#**major-ring[sub-ring]**	필수. 노드 레벨을 주요 링 또는 하위 링으로 설정합니다.
Switch_config_ring1#**control-vlan** *vlan-id*	필수. 제어 VLAN을 설정하고 VLAN "id" 및 VLAN "id+1"을 생성합니다. vlan-id: 제어 VLAN ID
Switch_config_ring1#**hello-time** *value*	선택 사항. 마스터 노드가 HEALTH 패킷을 전송하는 주기를 설정합니다. value: 1~10초 범위의 시간 값, 기본값은 3초
Switch_config_ring1#**fail-time** *value*	선택 사항. 보조 포트가 HEALTH 패킷을 대기하는 시간을 설정합니다. value: 3~30초 범위의 시간 값, 기본값은 9초

Switch_config_ring1#**exit**	현재 설정을 저장하고 노드 구성 모드를 종료합니다.

참고 : no mether-ring id domain id2 명령을 사용하여 링의 노드 설정과 노드의 포트 설정을 삭제할 수 있습니다. 주요 링과 하위 링은 동일한 VLAN, 즉 주요 링 제어 VLAN으로 구성해야 합니다. 구성 후 주요 링에서는 주요 링 제어 VLAN과 하위 링 제어 VLAN이 동시에 생성됩니다.
하위 링에서는 하위 링 제어 VLAN이 생성되며, 주요 링 제어 VLAN은 금지됩니다.

23.5.2 트랜짓 노드 구성

다음 단계를 따라 스위치를 링 네트워크의 트랜짓 노드로 구성합니다.

명령어	설명
Switch# config	스위치 구성 모드로 진입합니다.
Switch_config#**mether-ring** *id1* **domain** *id2*	노드를 설정하고 노드 구성 모드로 진입합니다. id1: 노드 ID id2: 도메인 인스턴스 ID (0일 경우 생략 가능)
Switch_config_ring1# **transit -node**	필수. 노드 유형을 트랜짓 노드로 설정합니다.
Switch_config_ring1#**major-ring[sub-ring]**	필수. 노드 레벨을 주요 링 노드(major ring) 또는 하위 링 노드(sub-ring)로 설정합니다.
Switch_config_ring1#**control-vlan** *vlan-id*	필수. 제어 VLAN을 설정하고 VLAN "id" 및 VLAN "id+1"을 생성합니다. vlan-id: 제어 VLAN ID
Switch_config_ring1#**pre-forward-time** *value*	선택. 트랜짓 포트에서 프리-포워드(pre-forward) 상태를 유지하는 시간을 설정합니다. value: 3~30초 사이의 값 (기본값: 9초)
Switch_config_ring#exit	현재 설정을 저장하고 노드 구성 모드에서 나갑니다.
Switch_config#	

참고 : 이 단계에 따라 구성 완료 후, 노드는 링 네트워크에서 트랜짓 역할을 수행하도록 준비됩니다. 필요한 경우 각 설정의 세부사항을 점검하세요.

23.5.3 엣지 노드와 이시스턴트 노드 구성

다음 단계를 따라 스위치를 링 네트워크의 마스터 노드로 구성합니다.

명령어	설명
Switch# **config**	스위치 구성 모드로 진입합니다.

Switch_config#**mether-ring** *id1* **domain** *id2*	노드를 설정하고 노드 구성 모드로 진입합니다. id1: 노드의 인스턴스 ID id2: 도메인 인스턴스 ID (0일 경우 생략 가능)
Switch_config_ring1#**edge-node[assistant-node]**	필수. 노드 유형을 엣지 노드로 설정합니다.
Switch_config_ring1#**sub-ring**	이 단계는 생략할 수 있습니다. 엣지 노드는 반드시 서브 링 노드여야 합니다.
Switch_config_ring1#**control-vlan** *vlan-id*	필수. 제어 VLAN을 설정하고 VLAN "id" 및 VLAN "id+1"을 생성합니다. vlan-id: 제어 VLAN ID
Switch_config_ring1#**pre-forward-time** *value*	선택. 엣지 포트의 프리-포워드(pre-forward) 상태를 유지하는 시간을 설정합니다. value: 3~30초 사이의 값 (기본값: 9초)
Switch_config_ring1#**exit**	현재 설정을 저장하고 노드 구성 모드에서 나갑니다.

참고 : 엣지 노드 구성: 엣지 노드는 반드시 서브 링 노드로 설정해야 하며, 이를 통해 네트워크의 접점 역할을 수행합니다. 어시스턴트 노드 옵션: 어시스턴트 노드는 필요에 따라 추가적으로 설정할 수 있습니다.

23.5.4 서브 링 네트워킹 모드 구성

다음 단계를 따라 스위치를 링 네트워크의 마스터 노드로 구성합니다.

명령어	설명
Switch# **config**	스위치 구성 모드로 진입합니다.
Switch_config#**mether-ring** *id1* **domain** *id2*	노드를 설정하고 노드 구성 모드로 진입합니다. id1: 노드의 인스턴스 ID id2: 도메인 인스턴스 ID (0일 경우 생략 가능)
Switch_config_ring1#**edge-node[assistant-node]**	필수. 노드 유형을 엣지 노드로 설정합니다.
Switch_config_ring1#**sub-ring**	이 단계는 생략할 수 있습니다. 엣지 노드는 반드시 서브 링 노드여야 합니다.
Switch_config_ring1#**control-vlan** *vlan-id*	필수. 제어 VLAN을 설정하고 VLAN "id" 및 VLAN "id+1"을 생성합니다.
Switch _config_ring2#**single-subring-mode**	
Switch_config_ring1#**pre-forward-time** *value*	필수. 명령어 없이도 링 구성을 완료할 수 있지만, 서브 링 네트워킹 모드는 활성화되지 않습니다. 서브 링

	네트워킹 모드에서는 주요 링에서 서브 링 프로토콜 패킷 채널 감지 메커니즘이 작동하지 않으며, 이중 호밍 네트워킹(dual homing networking)은 사용할 수 없습니다. 이 명령은 엣지 노드 및 어시스턴트 노드에서만 유효합니다.
Switch_config_ring1#**exit**	선택. 엣지 포트의 프리-포워드(pre-forward) 상태를 유지하는 시간을 설정합니다. value: 3~30초 사이의 값 (기본값: 9초)
Switch_config#	현재 설정을 저장하고 노드 구성 모드에서 나갑니다.

23.5.5 링 포트 구성

다음 단계를 따라 스위치의 포트를 이더넷 링의 포트로 구성합니다

명령어	설명
Switch# config	스위치 구성 모드로 진입합니다.
Switch_config#interface *intf-name*	인터페이스 구성 모드로 진입합니다.)
Switch_config_intf#mether-ring *id1* **domain** *id2* **primary-port [secondary-port | transit-port | common-port | edge-port]**	이더넷 링의 포트 유형을 설정합니다. id1: 노드의 인스턴스 ID id2: 도메인 인스턴스 ID (0일 경우 생략 가능)
Switch_config_intf#exit	인터페이스 구성 모드에서 나갑니다.

참고 : 링 포트 구성을 삭제하려면 다음 명령어를 실행합니다. no mether-ring id1 domain id2 primary-port [secondary-port | transit-port | common-port | edge-port]

23.5.6 링 보호 프로토콜 상태 확인

다음 명령어를 실행하여 링 보호 프로토콜의 상태를 확인합니다.

명령어	설명
show mether-ring	링 보호 프로토콜 및 링 포트에 대한 요약 정보를 확인합니다.
show mether-ring *id1* **domain** *id2*	특정 링 보호 프로토콜 및 링 포트에 대한 요약 정보를 확인합니다. id1: 노드의 인스턴스 ID id2: 도메인 인스턴스 ID (0일 경우 생략 가능)
show mether-ring *id1* **domain** *id2* **detail**	특정 링 보호 프로토콜 및 이더넷 링 포트에 대한 상세 정보를 확인합니다.

show mether-ring *id1* **domain** *id2* **interface** *intf-name*	특정 링 포트 또는 공통 포트의 상태를 확인합니다.

23.6 MEAPS 동작 절차

MEAPS는 단일 링 또는 2단계 다중 링 구조를 지원하기 위해 세 가지 보호 메커니즘을 채택합니다. 다음 섹션에서는 정상 상태에서 링크 다운 상태, 그리고 복구 상태를 거쳐 다시 정상 상태로 돌아가는 과정까지의 MEAPS 작동 세부 사항과 MEAPS 토폴로지 변화를 대표적인 예를 통해 설명합니다.

23.6.1 정상 상태 (Complete State)

링의 정상 상태는 단일 링에 대해 권장되며, 폴링(polling) 메커니즘에 의해 모니터링되고 유지됩니다.

- 정상 상태의 특징

  링의 모든 링크가 UP 상태에 있으며, 이는 마스터 노드의 상태로 표현됩니다.

- broadcast storm

  broadcast storm을 방지하기 위해 마스터 노드는 자신의 보조 포트(secondary port)를 차단합니다.

- Hello 패킷 전송

  마스터 노드는 주 포트(primary port)를 통해 주기적으로 Hello 패킷을 전송합니다.

  이 Hello 패킷은 순차적으로 트랜짓 노드(transit node)를 통과한 후, 마침내 마스터 노드의 보조 포트로 되돌아옵니다.

- 정상 상태에서의 링 토폴로지

  주요 링(major ring)과 두 개의 하위 링(sub ring) 모두 정상 상태를 유지합니다.

  주요 링의 Hello 패킷은 주요 링에서만 브로드캐스트됩니다.

  하위 링의 Hello 패킷은 주요 링을 통해 투명하게(transparently) 전달되며, 하위 링으로 되돌아와 하위 링의 마스터 노드 보조 포트로 도착합니다.

정상 상태를 나타내는 링 구조는 아래 그림에 설명되어 있습니다.

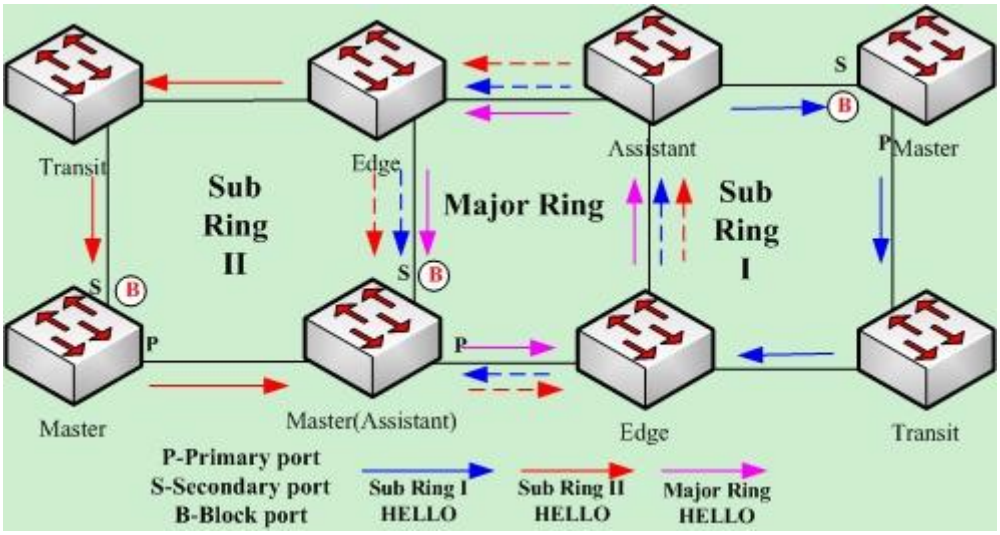


그림 40 링 상태

23.6.2 링크 다운

링의 링크 다운 상태는 폴링 메커니즘, 링크 상태 변경 알림, 그리고 서브 링 프로토콜 패킷의 채널 상태 확인 메커니즘에 의해 결정됩니다. 이 상태 역시 단일 링에서만 적용되는 것으로 권장됩니다.

링 내의 일부 링크가 링크 다운 상태가 되면, 링은 정상 상태에서 문제가 발생한 상태(troubled state)로 전환됩니다. 이는 곧 링크 다운 상태를 의미합니다.

링크 다운이 발생하면 폴링 메커니즘과 링크 상태 변경 알림 메커니즘이 동시에 작동합니다. 링크 다운이 발생한 트랜짓 노드는 반대쪽 포트의 Up 포트를 통해 링크 다운 패킷을 마스터 노드로 전송합니다. 동시에 폴링 메커니즘은 Fail Time을 통해 링의 상태를 신속하게 감지하고 변경합니다.

서브 링 프로토콜 채널에서 문제가 발생하면, 이 문제는 주요 링에서 서브 링 프로토콜 패킷의 채널 상태 확인 메커니즘에 의해 처리됩니다. 아래 그림과 같이 주요 링 및 공통 링크의 문제 알림 메시지는 주요 링 내에서만 전송되며, 최종적으로 마스터 노드로 전달됩니다. 서브 링 2의 링크 문제 알림 메시지는 서브 링의 마스터 노드로 전송되고, 이 메시지는 주요 링을 통해 투명하게 전달될 수 있습니다.

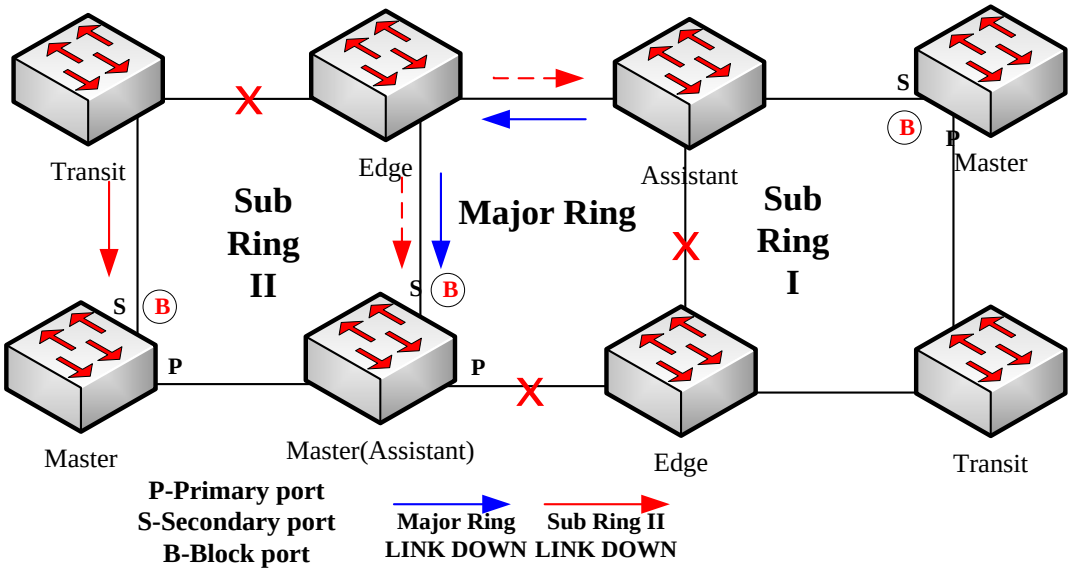


그림 41 링 노드 문제 알림

마스터 노드가 링크 다운 패킷을 수신하면 상태가 Failed 상태로 변경됩니다. 동시에 보조 포트가 열리고, FDB 테이블이 갱신되며, RING-DOWN-FLUSH-FDB 패킷이 두 포트에서 전송되어 모든 노드에 이를 알립니다. 아래 그림에서 볼 수 있듯이, 주요 링의 마스터 노드는 주요 링의 트랜짓 노드에 FDB 갱신을 알립니다. 서브 링 1에서는 채널에 문제가 발생하여 어시스턴트 노드의 엣지 포트가 차단됩니다. 서브 링 2의 마스터 노드는 서브 링의 트랜짓 노드들에게 FDB 갱신을 알린 뒤, 주요 링에서 투명하게 전송을 수행합니다.

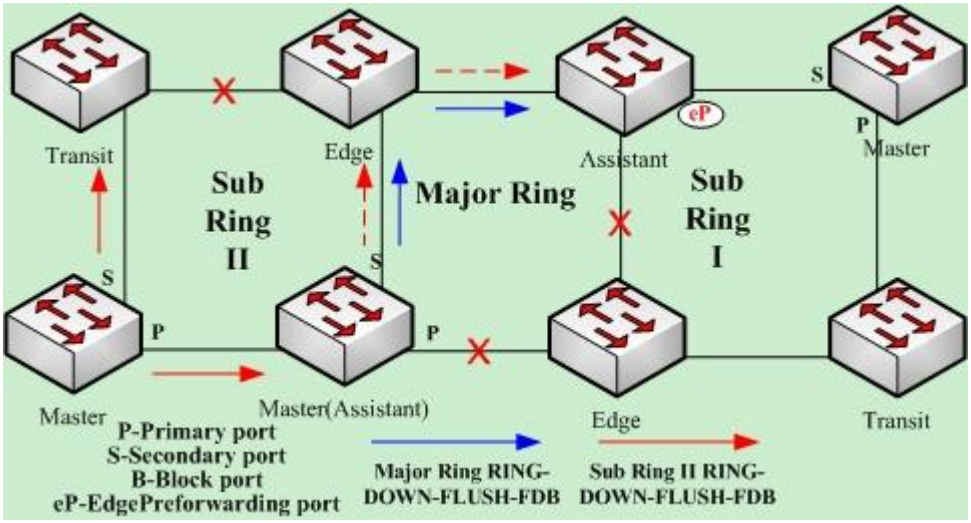


그림 42 링이 문제를 전송하고 FDB를 갱신

23.6.3 복구

트랜짓 노드의 포트가 복구되면 해당 트랜짓 노드는 Preforwarding 상태로 전환됩니다. 트랜짓

노드의 포트가 복구될 때의 처리 절차는 아래 그림에 나와 있습니다.

주요 링의 링크가 복구되면서, 주요 링의 링크와 연결된 트랜짓 노드는 Preforwarding 상태로 전환됩니다. 이 상태에서 트랜짓 노드는 데이터 패킷을 차단하지만, 제어 패킷의 Hello 패킷은 통과시킵니다. 마찬가지로 서브 링 2의 트랜짓 노드도 Preforwarding 상태로 전환됩니다.

서브 링 1의 Hello 패킷이 엣지 노드에 도달하려 할 때, 복구된 트랜짓 노드가 주요 링의 제어 패킷만 통과하도록 허용하기 때문에, 서브 링 1의 Hello 패킷은 주요 링의 데이터 패킷처럼 간주되어 전달될 수 없습니다.

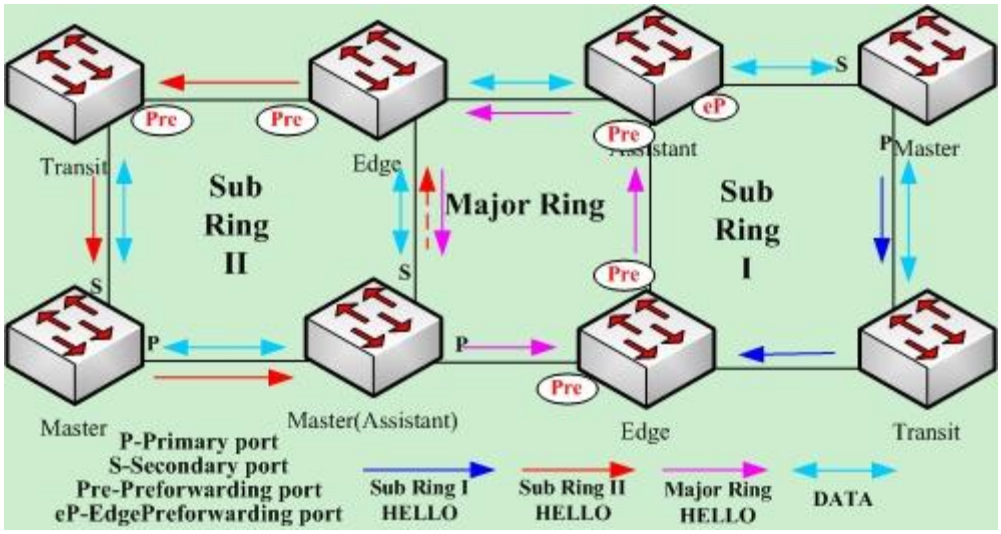


그림 43 링의 링크 복구와 트랜짓 노드의 Preforwarding 상태 전환

트랜짓 포트는 Preforwarding 상태에서 제어 패킷을 전송할 수 있으므로, 마스터 노드의 보조 포트는 주 포트에서 전송된 Hello 패킷을 수신할 수 있습니다. 이에 따라 마스터 노드는 상태를 Complete로 전환하고, 보조 포트를 차단하며, RING-UP-FLUSH-FDB 패킷을 주 포트에서 전송합니다.

트랜짓 노드가 RING-UP-FLUSH-FDB 패킷을 수신하면, 트랜짓 노드는 Link-Up 상태로 전환되어 차단된 포트를 열고 FDB 테이블을 갱신합니다.

링 복구 절차는 아래 그림에 나와 있습니다. 주요 링의 마스터 노드는 Complete 상태로 전환되며, 보조 포트를 차단하고, RING-UP-FLUSH-FDB 패킷을 주요 링의 모든 트랜짓 노드로 전송합니다. 이를 통해 트랜짓 노드들은 Link-Up 상태로 전환되고, 차단된 포트를 열며 FDB 테이블을 갱신합니다.

서브 링 2의 트랜짓 노드와 마스터 노드도 이와 동일한 변화를 겪습니다. 서브 링 1에서는 서브 링 프로토콜 패킷의 채널이 복구됨에 따라, 마스터 노드의 보조 포트가 주 포트로부터 Hello 패킷을 수신할 수 있습니다. 이에 마스터 노드는 Complete 상태로 전환되며, 보조 포트를 차단하고, RING-UP-FLUSH-FDB 패킷을 전송합니다. 이 과정에서 어시스턴트 노드는 엣지 포트를 열게 되고,

서브 링 1은 정상 상태로 복구됩니다.

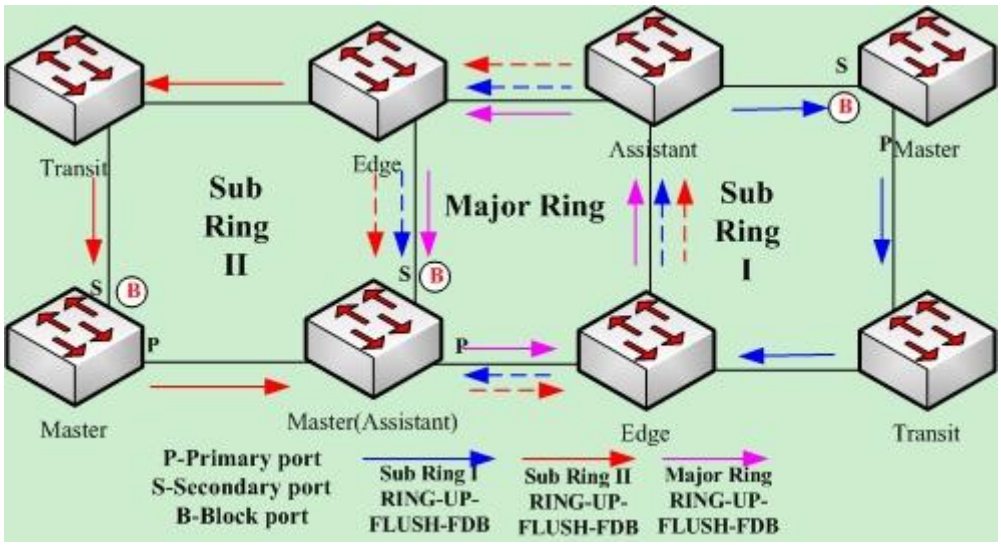


그림 44 링 복구

물론, Preforwarding 상태에 있는 트랜짓 노드가 RING-UP-FLUSH-FDB 패킷을 수신하지 못하고 Fail Time을 초과하는 경우, 트랜짓 노드는 차단된 트랜짓 포트를 열고 데이터 통신을 재개합니다.

23.6.4 설정 예제

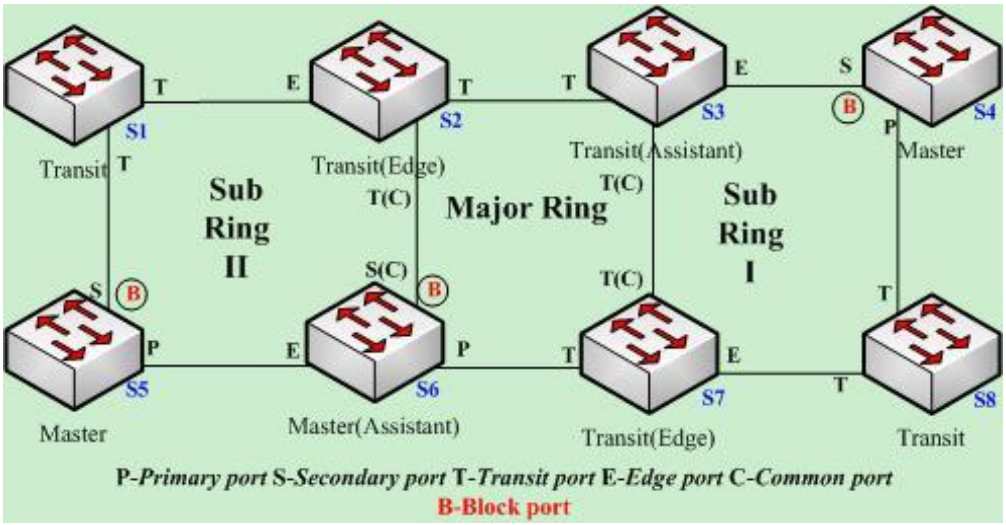


그림 45 MEAPS 예제

그림과 같이 마스터 노드 S1과 트랜짓 노드 S2를 다음과 같이 구성합니다.

다른 노드의 설정은 S2의 설정과 동일합니다.

- 스위치 S1 구성

  서브링 트랜짓 노드, 노드 2 설정

Switch_config#mether-ring 2 domain 1

Switch_config_ring2#transit-node

Switch_config_ring2#sub-ring

Switch_config_ring2#control-vlan 2

- 시간 관련 매개변수 설정

  Switch_config_ring2#pre-forward-time 12

- 노드 구성 모드 종료

  Switch_config_ring2#quit

- 노드 2의 트랜짓 포트 설정 명령어

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 2 domain 1 transit-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 2 domain 1 transit-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

- 스위치 S2 구성

Switch_config#mether-ring 1 domain 1

Switch_config_ring1#transit-node

Switch_config_ring1#major-ring

Switch_config_ring1#control-vlan 2

- 시간 관련 매개변수 설정 명령어

  Switch_config_ring1#pre-forward-time 12

- 노드 구성 모드 종료

  Switch_config_ring1#quit

- 노드 1의 트랜짓 포트 설정 명령어

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 1 domain 1 transit-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 1 domain 1 transit-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

- 서브 링 엣지 노드, 노드 2 설정 명령어

Switch_config#mether-ring 2 domain 1

Switch_config_ring2#edge-node

Switch_config_ring2#sub-ring (이 단계는 생략 가능)

Switch_config_ring2#control-vlan 2

- 시간 관련 매개변수 설정 명령어

Switch_config_ring2#pre-forward-time 12

- 노드 구성 모드 종료

Switch_config_ring2#quit

- 노드 2의 공통 포트와 엣지 포트 설정 명령어

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 2 domain 1 common-port

Switch_config_g0/2#quit

Switch_config#interface gigaEthernet 0/3

Switch_config_g0/3#mether-ring 2 domain 1 edge-port

Switch_config_g0/3#switchport mode trunk

Switch_config_g0/3#quit

- 스위치 S3 구성

Switch_config#mether-ring 1 domain 1

Switch_config_ring1#transit-node

Switch_config_ring1#major-ring

Switch_config_ring1#control-vlan 2

- 시간 관련 매개변수 설정 명령어

Switch_config_ring1#pre-forward-time 12

Switch_config_ring1#quit

- 노드 1의 트랜짓 포트 설정

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 1 domain 1 transit-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 1 domain 1 transit-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

- 서브 링 어시스턴트 노드, 노드 4 설정 명령어

Switch_config#mether-ring 4 domain 1

Switch_config_ring4#assistant-node

Switch_config_ring4#sub-ring

Switch_config_ring4#control-vlan 2

- 시간 관련 매개변수 설정 명령어

Switch_config_ring4#pre-forward-time 12

Switch_config_ring4#quit

- 노드 4의 공통 포트와 엣지 포트 설정

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 4 domain 1 common-port

Switch_config_g0/2#quit

Switch_config#interface gigaEthernet 0/3

Switch_config_g0/3#mether-ring 4 domain 1 edge-port

Switch_config_g0/3#switchport mode trunk

Switch_config_g0/3#quit

- 스위치 S4 구성

Switch_config#mether-ring 4 domain 1

Switch_config_ring4#master-node

Switch_config_ring4#sub-ring

Switch_config_ring4#control-vlan 2

- 시간 관련 매개변수 설정 명령어

Switch_config_ring4#hello-time 4

Switch_config_ring4#fail-time 12

Switch_config_ring4#quit

- 노드 4의 주 포트와 보조 포트 설정

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 4 domain 1 primary-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 4 domain 1 secondary-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

- 스위치 S5 구성

Switch_config#mether-ring 2 domain 1

Switch_config_ring2#master-node

Switch_config_ring2#sub-ring

Switch_config_ring2#control-vlan 2

- 시간 관련 매개변수 설정 명령어

Switch_config_ring2#hello-time 4

Switch_config_ring2#fail-time 12

Switch_config_ring2#quit

- 노드 2의 주 포트와 보조 포트 설정

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 2 domain 1 primary-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 2 domain 1 secondary-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

- 스위치 S6 구성

Switch_config#mether-ring 1 domain 1

Switch_config_ring1#master-node

Switch_config_ring1#major-ring

Switch_config_ring1#control-vlan 2

- 시간 관련 매개변수 설정 명령어

Switch_config_ring1#hello-time 4

Switch_config_ring1#fail-time 12

Switch_config_ring1#quit

- 노드 1의 주 포트와 보조 포트 설정

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 1 domain 1 primary-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 1 domain 1 secondary-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

- 서브 링 어시스턴트 노드, 노드 2 설정 명령어

Switch_config#mether-ring 2 domain 1

Switch_config_ring2#assistant-node

Switch_config_ring2#sub-ring

Switch_config_ring2#control-vlan 2

Switch_config_ring2#pre-forward-time 12

- 노드 구성 모드 종료

Switch_config_ring2#quit

- 노드 2의 공통 포트와 엣지 포트 설정

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 2 domain 1 common-port

Switch_config_g0/2#quit

Switch_config#interface gigaEthernet 0/3

Switch_config_g0/3#mether-ring 2 domain 1 edge-port

Switch_config_g0/3#switchport mode trunk

Switch_config_g0/3#quit

- 스위치 S7 구성

Switch_config#mether-ring 1 domain 1

Switch_config_ring1#transit-node

Switch_config_ring1#major-ring

Switch_config_ring1#control-vlan 2

- 시간 관련 매개변수 설정 명령어

Switch_config_ring1#pre-forward-time 12

Switch_config_ring1#quit

- 노드 1의 트랜짓 포트 설정

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 1 domain 1 transit-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 1 domain 1 transit-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

- 서브 링 엣지 노드, 노드 4 설정 명령어

Switch_config#mether-ring 4 domain 1

Switch_config_ring4#edge-node

Switch_config_ring4#sub-ring

Switch_config_ring4#control-vlan 2

- 시간 관련 매개변수 설정 명령어

Switch_config_ring4#pre-forward-time 12

Switch_config_ring4#quit

- 노드 4의 공통 포트와 엣지 포트 설정

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 4 domain 1 common-port

Switch_config_g0/2#quit

Switch_config#interface gigaEthernet 0/3

Switch_config_g0/3#mether-ring 4 domain 1 edge-port

Switch_config_g0/3#switchport mode trunk

Switch_config_g0/3#quit

- 스위치 S8 구성

Switch_config#mether-ring 4 domain 1

Switch_config_ring4#transit-node

Switch_config_ring4#sub-ring

Switch_config_ring4#control-vlan 2

- 시간 관련 매개변수 설정 명령어

Switch_config_ring4#pre-forward-time 12

Switch_config_ring4#quit

- 노드 4의 트랜짓 포트 설정

Switch_config#interface gigaEthernet 0/1

Switch_config_g0/1#mether-ring 4 domain 1 transit-port

Switch_config_g0/1#switchport mode trunk

Switch_config_g0/1#quit

Switch_config#interface gigaEthernet 0/2

Switch_config_g0/2#mether-ring 4 domain 1 transit-port

Switch_config_g0/2#switchport mode trunk

Switch_config_g0/2#quit

24. snooping 구성

24.1 IGMP-snooping 구성 작업

IGMP-snooping의 작업은 VLAN과 그룹 주소 간의 관계를 유지하고 멀티캐스트 변경 사항에 따라 실시간으로 업데이트하여, 스위치가 멀티캐스트 그룹의 토폴로지 구조에 따라 데이터를 전달할 수 있도록 하는 것입니다.

IGMP-snooping의 주요 기능은 다음과 같습니다.

- IGMP 메시지 수신.
- VLAN과 그룹 주소 간 관계 테이블 유지.
- 호스트와 라우터의 IGMP 엔터티를 동일한 상태로 유지하여 브로드캐스트 발생 방지.

참고:

- IGMP-snooping은 IGMP의 query 메시지와 report 메시지를 수신하여 위 기능을 실현합니다. 따라서 IGMP-snooping이 멀티캐스트 라우터와 함께 작동할 때만 제대로 동작할 수 있습니다. 즉, 스위치는 라우터로부터 주기적으로 IGMP query 정보를 수신해야 합니다.
- IGMP-snooping의 라우터 에이지 타이머는 IGMP-snooping에 연결된 멀티캐스트 라우터의 그룹 쿼리 주기보다 긴 값으로 설정해야 합니다. 각 VLAN에서 멀티캐스트 라우터 정보를 확인하려면 show ip igmp-snooping 명령어를 실행할 수 있습니다.

IGMP-snooping 구성 작업 목록

- VLAN의 IGMP-snooping 활성화/비활성화
- VLAN의 정적 멀티캐스트 주소 추가/삭제
- VLAN의 즉시 종료(immediate-leave) 구성
- VLAN의 정적 라우팅 인터페이스 구성
- 멀티캐스트 포워딩 테이블 생성을 위한 IPACL 구성
- 등록된 목적지 주소가 없는 멀티캐스트 메시지 필터링 기능 구성
- IGMP-snooping의 라우터 에이지 타이머 구성
- IGMP-snooping의 응답 시간 타이머 구성
- IGMP-snooping 쿼리어(Querier) 구성
- IGMP-snooping의 쿼리어 시간 타이머 구성
- IGMP-snooping의 forward-l3-to-mrouter 데이터 포워딩을 라우터 포트로 구성
- IGMP-snooping의 민감 모드(sensitive mode) 및 값 구성

- IGMP-snooping의 v3-leave-check 기능 구성
- IGMP-snooping의 forward-wrongiif-within-vlan 기능 구성
- IGMP-snooping 포트의 IPACL 기능 구성
- IGMP-snooping 포트에서 최대 멀티캐스트 IP 주소 수량 구성
- IGMP-snooping 모니터링 및 유지 관리
- IGMP-snooping 구성 예제

24.1.1 VLAN의 IGMP-Snooping 활성화/비활성화

글로벌 구성 모드에서 다음 구성을 진행합니다.

명령어	설명
ip igmp-snooping [**vlan** *vlan_id*]	VLAN의 IGMP-snooping을 활성화합니다.
no ip igmp-snooping [**vlan** *vlan_id*]	기본 설정으로 되돌립니다.

참고 :

- VLAN을 지정하지 않으면, 시스템의 모든 VLAN(나중에 생성된 VLAN 포함)을 활성화하거나 비활성화할 수 있습니다.
- 기본 설정에서 모든 VLAN의 IGMP-snooping이 활성화되어 있으며, 이는 ip igmp-snooping 명령어를 실행한 것과 동일합니다.
- IGMP-snooping은 최대 16개의 VLAN에서 실행할 수 있습니다.

VLAN3에서 IGMP-snooping을 활성화하려면 먼저 no ip igmp-snooping 명령어를 실행하여 모든 VLAN의 IGMP-snooping을 비활성화한 후, ip igmp-snooping vlan 3을 구성하고 설정을 저장해야 합니다.

24.1.2 VLAN의 Static 멀티캐스트 주소 추가/삭제

IGMP를 지원하지 않는 호스트도 static 멀티캐스트 주소를 구성하여 해당 멀티캐스트 메시지를 수신할 수 있습니다.

글로벌 구성 모드에서 다음 구성을 진행합니다.

명령어	설명
ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*	VLAN의 static 멀티캐스트 주소를 추가합니다.
no ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D*	VLAN의 tatic 멀티캐스트 주소를 삭제합니다.

interface *intf*	

24.1.3 VLAN의 Immediate-Leave 기능 구성

Immediate-leave 기능을 구성하면, 스위치가 leave 메시지를 수신한 후 해당 포트를 멀티캐스트 그룹의 포트 목록에서 바로 삭제할 수 있습니다. 이로 인해 타이머를 활성화하여 다른 호스트가 멀티캐스트 그룹에 참여하기를 기다릴 필요가 없습니다.

하지만 동일한 포트의 다른 호스트가 동일한 그룹에 속해 있고, 해당 사용자들이 그룹에서 나가기를 원하지 않을 경우, 이러한 사용자들의 멀티캐스트 통신이 영향을 받을 수 있습니다. 이런 상황에서는 immediate-leave 기능을 활성화하지 않는 것이 좋습니다.

글로벌 구성 모드에서 다음 구성을 진행합니다.

명령어	설명
ip igmp-snooping vlan *vlan_id* **immediate-leave**	VLAN의 immediate-leave 기능을 구성합니다.
no ip igmp-snooping vlan *vlan_id* **immediate-leave**	VLAN의 immediate-leave를 기본값으로 설정합니다.

24.1.4 포트의 Immediate-Leave 기능 설정

포트에 immediate-leave 기능을 설정하면, 스위치는 leave 메시지를 수신한 후 해당 포트를 멀티캐스트 그룹의 포트 목록에서 바로 삭제할 수 있습니다. 이로 인해 타이머를 활성화하여 다른 호스트가 멀티캐스트 그룹에 참여하기를 기다릴 필요가 없습니다.

하지만 동일한 포트의 다른 호스트가 동일한 그룹에 속해 있고, 해당 사용자들이 그룹에서 나가기를 원하지 않을 경우, 이러한 사용자들의 멀티캐스트 통신이 영향을 받을 수 있습니다. 이런 상황에서는 immediate-leave 기능을 활성화하지 않는 것이 좋습니다.

포트의 immediate-leave 설정은 VLAN의 immediate-leave 설정과 동시에 작동합니다.

인터페이스 구성 모드에서 다음 설정을 진행합니다.

명령어	설명
ip igmp-snooping immediate-leave	포트의 immediate-leave 기능을 구성합니다.
no ip igmp-snooping immediate-leave	포트의 immediate-leave 를 기본값으로 설정합니다..

포트의 immediate-leave 기능은 기본적으로 비활성화되어 있습니다.

24.1.5 VLAN의 Static Routing Interface 설정

Static Routing Interface를 구성하여 멀티캐스트 패킷을 라우팅 포트로 전송합니다. 스위치는

VLAN 내 모든 라우팅 포트로 멀티캐스트 리포트 패킷을 전송합니다.

명령어	설명
ip igmp-snooping vlan *vlan_id* **mrouter interface** *intf*	VLAN의 static 라우팅 포트를 추가합니다.
no ip igmp-snooping vlan *vlan_id* **mrouter interface** *intf*	VLAN 의 static 라우팅 포트를 삭제합니다.

24.1.6 멀티캐스트 포워딩 테이블 생성을 위한 IPACL 설정

글로벌 구성 모드에서 다음 명령어를 실행하여 IPACL을 설정합니다. 이를 통해 IGMP report 패킷 수신 후 멀티캐스트 포워딩 테이블 생성 시의 규칙과 제한 사항을 구성할 수 있습니다.

명령어	설명
ip igmp-snooping policy *word*	멀티캐스트 포워딩 테이블 생성을 위한 IPACL을 추가합니다.
no ip igmp-snooping policy	멀티캐스트 포워딩 테이블 생성을 위한 IPACL 을 삭제합니다.

24.1.7 등록되지 않은 목적지 주소의 멀티캐스트 메시지를 필터링하는 기능 구성

등록된 목적지 주소를 찾을 수 없는 멀티캐스트 메시지(DLF, Destination Lookup Failure)는 스위치 칩에 IGMP-snooping을 통해 등록되지 않은 목적지 주소를 가리킵니다. 기본 처리 방식은 VLAN의 모든 포트로 메시지를 전송(broadcast)하는 것입니다.

구성을 통해 이러한 처리 방식을 변경할 수 있으며, 등록되지 않은 목적지 주소를 가지는 모든 멀티캐스트 메시지를 삭제하도록 설정할 수 있습니다.

명령어	설명
ip igmp-snooping dlf-drop	목적지를 찾을 수 없는 멀티캐스트 메시지를 삭제합니다.
no ip igmp-snooping dlf-drop	기본 설정(전달)을 복원합니다. (해당 메시지가 VLAN 내에서 브로드캐스트됨)

참고:

1. 이 속성은 모든 VLAN에 대해 구성됩니다.
2. 스위치의 기본 메시지 처리 방식은 전달(forward)이며, 이 유형의 메시지는 VLAN 내에서 브로드캐스트됩니다.

24.1.8 IGMP-snooping의 Router Age Timer 설정

Router Age Timer는 IGMP 쿼리어(Queryer)의 존재 여부를 모니터링하는 데 사용됩니다. IGMP 쿼리어는 쿼리 메시지를 전송하여 멀티캐스트 주소를 유지합니다. IGMP-snooping은 IGMP 쿼리어와 호스트 간의 통신을 통해 작동합니다.

글로벌 구성 모드에서 다음 설정을 진행합니다.

명령어	설명
ip igmp-snooping timer router-age *timer_value*	IGMP-snooping의 Router Age 값을 설정합니다.
no ip igmp-snooping timer router-age	IGMP-snooping 의 Router Age 기본값을 복원합니다.

참고:

- Timer를 설정하는 방법은 IGMP 쿼리어의 쿼리 주기 설정을 참조해야 합니다.
- Timer 값은 쿼리 주기보다 작게 설정할 수 없습니다. Timer를 쿼리 주기의 3배로 설정하는 것이 권장됩니다.
- IGMP-snooping의 Router Age 기본값은 260초입니다.

24.1.9 IGMP-snooping의 Response Time Timer 설정

Response Time Timer는 IGMP 쿼리어가 쿼리 메시지를 전송한 후, 호스트가 멀티캐스트를 보고하는 데 걸리는 최대 시간을 의미합니다. Timer가 만료된 후에도 보고 메시지가 수신되지 않으면, 스위치는 멀티캐스트 주소를 삭제합니다.

글로벌 구성 모드에서 다음 설정을 진행합니다

명령어	설명
ip igmp-snooping timer response-time timer_value	IGMP-snooping의 Response Time 값을 설정합니다.
no ip igmp-snooping timer response-time	IGMP-snooping 의 Response Time 기본값을 복원합니다.

참고 : Timer 값이 너무 작으면 멀티캐스트 통신이 불안정해질 수 있으며 기본값은 15초 입니다.

24.1.10 IGMP-snooping의 Querier 설정

멀티캐스트 라우터가 IGMP-snooping이 활성화된 VLAN에 존재하지 않을 경우, IGMP-snooping의 querier 기능을 사용하여 멀티캐스트 라우터를 모방하여 정기적으로 IGMP 쿼리 메시지를 전송할

수 있습니다.

이 기능은 글로벌 기능으로, IGMP-snooping이 글로벌 활성화된 VLAN에서 설정하거나 비활성화할 수 있습니다.

LAN에 멀티캐스트 라우터가 없고 멀티캐스트 트래픽이 라우팅을 필요로 하지 않는 경우, 스위치의 자동 쿼리 기능을 IGMP-snooping을 통해 활성화하여 IGMP-snooping이 정상적으로 작동할 수 있도록 할 수 있습니다.

글로벌 구성 모드에서 다음 설정을 진행합니다.

명령어	설명
[**no**] **ip igmp-snooping querier [address** *[ip_addr]*	IGMP-snooping의 querier를 구성합니다. 선택적 매개변수 address는 쿼리 메시지의 소스 IP 주소를 지정합니다.

참고 : 기본적으로 IGMP-snooping의 querier 기능은 비활성화되어 있습니다. 쿼리 메시지의 기본 소스 IP 주소는 10.0.0.200입니다. querier 기능이 활성화된 경우, 멀티캐스트 라우터가 VLAN에 존재하면 이 기능은 비활성화됩니다. 멀티캐스트 라우터의 타이머가 만료되면 querier 기능이 자동으로 활성화됩니다.

24.1.11 IGMP-snooping의 Querier Time Timer 설정

Querier Time Timer는 스위치가 로컬 IGMP querier로서 쿼리 메시지를 전송하는 시간 간격을 설정합니다. Timer가 만료되면 VLAN 내에서 쿼리 메시지를 브로드캐스트합니다.

글로벌 구성 모드에서 다음 설정을 진행합니다.

명령어	설명
ip igmp-snooping querier querier-timer *timer_value*	IGMP-snooping의 Querier Time 값을 설정합니다.
no ip igmp-snooping querier querier-timer	IGMP-snooping 의 Querier Time 을 기본값으로 복원합니다.

참고 : 기본적으로 IGMP-snooping querier는 비활성화되어 있으며, 쿼리 메시지의 기본 전송 간격은 200초입니다. Querier 기능이 활성화된 경우, querier-timer 값을 너무 길게 설정하면 안 됩니다. 서브넷 내 다른 스위치에서 querier 기능이 활성화된 경우, querier-timer가 다른 스위치의 router-age보다 길면 서브넷에서 querier 선택이 불안정해질 수 있습니다.

24.1.12 IGMP-snooping의 forward-l3-to-mrouter 기능 설정

forward-l3-to-mrouter 기능은 L3 멀티캐스트가 활성화된 환경에서 멀티캐스트 데이터가 모든 다운스트림 포트로 브로드캐스트되는 대신, PIM-SM 메시지로 등록된 멀티캐스트 라우터 포트로만 전송되도록 설정합니다.

이 기능은 다음과 같은 상황에서 주로 사용됩니다:

- 여러 스위치가 L3 멀티캐스트를 계단식으로 연결(cascading)하여 사용하고, 업스트림 장치가 멀티캐스트 라우터 프로토콜을 통해 다운스트림 VLAN 포트를 학습할 때.
- 업스트림과 다운스트림 장치 간에 IGMP 메시지가 상호작용하지 않는 경우. 이 경우 업스트림 장치의 snooping은 다운스트림 장치와 연결된 물리적 포트를 학습할 수 없습니다.
- 업스트림 장치가 멀티캐스트 트래픽을 전달할 때, VLAN의 모든 물리적 포트로 트래픽을 전송하게 되는 문제를 방지합니다.

이 기능이 활성화되면 데이터 메시지는 다운스트림 장치와 연결된 물리적 포트로만 전달되며, 다운스트림 VLAN 전체로 브로드캐스트되지 않습니다.

글로벌 구성 모드에서 다음 설정을 진행합니다.

명령어	설명
[no] ip igmp-snooping forward-l3-to-mrouter	IGMP-snooping의 forward-l3-to-mrouter 기능을 설정 또는 비활성화합니다.

참고 : 기본적으로 IGMP-snooping의 forward-l3-to-mrouter 기능은 비활성화되어 있습니다. 이 명령어는 데이터 메시지를 멀티캐스트 라우터 포트로 전달할 수 있지만, 스위칭 칩은 소스 데이터 포트에 대한 제한 기능을 제공합니다. 따라서 데이터 메시지는 소스 데이터 포트로 전달되지 않으며, PIM-SM에 의해 등록된 다운스트림 라우터 포트로만 전달됩니다.

24.1.13 IGMP-snooping의 Sensitive 모드 및 값 설정

Sensitive 모드가 활성화되면, 트렁크 모드 포트가 종료될 때 활성 상태의 mrouter의 router-age 시간을 sensitive 값으로 설정하고 빠르게 쿼리 메시지를 전송합니다.

글로벌 구성 모드에서 다음 설정을 진행합니다.

명령어	설명
[**no**] **ip igmp-snooping sensitive** [value [3-30]]	IGMP-snooping의 sensitive 모드 및 값을 설정합니다. 값은 현재 활성 상태의 mrouter의 router-age 시간입니다.

참고 : 본적으로 IGMP-snooping의 sensitive 모드는 비활성화되어 있습니다. Sensitive 모드에서 설정된 sensitive 값은 한 번만 router-age를 업데이트하는 데 사용됩니다. 이후 router-age는 구성된 기본값으로 복원됩니다.

24.1.14 IGMP-snooping의 v3-leave-check 기능 설정

v3-leave-check 기능이 활성화되면, v3 leave 메시지를 수신한 후 특별한 쿼리 메시지를 전송합니다. 비활성화된 경우, 추가 작업은 수행되지 않습니다.

글로벌 구성 모드에서 다음 설정을 진행합니다.

명령어	설명
[no] ip igmp-snooping v3-leave-check	IGMP-snooping의 v3-leave-check 기능을 설정합니다. v3 leave 메시지 수신 후 특별한 쿼리 메시지를 전송합니다.

24.1.15 IGMP-snooping의 forward-wrongiif-within-vlan 기능 설정

forward-wrongiif-within-vlan 기능이 활성화되면, 잘못된 VLAN 인터페이스 포트로부터 수신된 멀티캐스트 데이터 메시지를 소스 VLAN 내의 그룹 멤버 포트로 L2 포워딩합니다. 비활성화된 경우, 메시지는 삭제됩니다.

글로벌 구성 모드에서 다음 설정을 진행합니다.

명령어	설명
[no] ip igmp-snooping forward-wrongiif-within-vlan	GMP-snooping의 forward-wrongiif-within-vlan 기능을 설정하고 VLAN 내 관련 그룹 멤버 포트로 메시지를 전달합니다.

참고 : ip igmp-snooping forward-wrongiif-within-vlan 명령은 L3 멀티캐스트가 활성화된 경우에만 의미가 있습니다.

24.1.16 IGMP-snooping의 포트에서 IPACL 기능 설정

포트에서 IGMP-snooping의 IPACL 기능이 활성화되면, 특정 멀티캐스트 IP 주소 메시지를 처리하거나 무시할지 IPACL을 통해 결정할 수 있습니다.

인터페이스 포트 구성 모드에서 다음 설정을 진행합니다.

명령어	설명
ip igmp-snooping policy *word*	포트에서 처리해야 할 멀티캐스트 메시지의 IPACL을 추가합니다.

no ip igmp-snooping policy	포트에서 처리해야 할 멀티캐스트 메시지의 IPACL을 삭제합니다.

24.1.17 VLAN에서 IGMP-snooping의 멀티캐스트 필터링 설정

VLAN에서 IGMP-snooping의 멀티캐스트 필터링이 활성화되면, 필터링 목록에 포함된 멀티캐스트 그룹 리포트 요청만 허용되고 VLAN의 그룹에 추가됩니다. 목록에 없는 요청은 삭제되며 그룹에 추가되지 않습니다.

글로벌 구성 모드에서 다음 설정을 진행합니다.

명령어	설명
ip igmp-snooping vlan *value* **filter** *vlanid-list*	VLAN에서 IGMP-snooping의 멀티캐스트 필터링을 설정합니다. vlanid-list는 "," 및 "-"로 연결된 VLAN ID 목록을 나타냅니다. ","와 "-" 뒤에는 반드시 공백이 있어야 합니다.
ip igmp-snooping vlan *value* **filter** *vlanid-list*	VLAN에서 멀티캐스트 필터링을 제거합니다.

24.1.18 IGMP-snooping 포트에서 최대 멀티캐스트 IP 주소 수량 설정

IGMP-snooping 포트에서 최대 멀티캐스트 IP 주소 수량을 설정하면, IGMP-snooping이 포워딩 항목을 생성할 때 해당 포트에 적용된 그룹 수가 설정된 최대 수량을 초과했는지 판단합니다. 초과하면 해당 포트의 항목이 생성되지 않습니다.

인터페이스 포트 구성 모드에서 다음 설정을 진행합니다.

명령어	설명
[no] ip igmp-snooping limit [value [1-2048]]	IGMP-snooping 포트에서 최대 멀티캐스트 IP 주소 수량을 설정합니다. 기본 최대값은 2048입니다.

24.1.19 IGMP-snooping의 Report-Suppression 기능 설정

명령어	설명
[**no] ip igmp-snooping report-suppression [max-number value** [1-5]]	IGMP-snooping의 report-suppression 기능과 최대 보고 전달 수를 설정합니다.

참고 : max-number 키워드가 생략되면 기본 전달 수는 1입니다.

24.1.20 IGMP-snooping의 Proxy-Leave 기능 설정

명령어	설명
[no] ip igmp-snooping proxy-leave	IGMP-snooping의 proxy-leave 기능을 설정합니다.

이 기능은 같은 VLAN 내에서 모든 멤버가 멀티캐스트 그룹을 완전히 떠난 후에만 상위 장치로 leave 메시지를 전송합니다.

24.1.21 IGMP-snooping 모니터링 및 유지 관리

명령어	설명
show ip igmp-snooping	IGMP-snooping 구성 정보를 표시합니다.
show ip igmp-snooping timer	IGMP-snooping의 타이머 정보를 표시합니다.
show ip igmp-snooping group	IGMP-snooping의 멀티캐스트 그룹 정보를 표시합니다.
show ip igmp-snooping group interface	특정 포트에서 IGMP-snooping의 멀티캐스트 그룹 정보를 표시합니다.
show ip igmp-snooping statistics [message|packet|hardware|vlan vlanid]	IGMP-snooping의 통계 정보를 표시합니다.
show ip igmp-snooping vlan	IGMP-snooping의 VLAN 정보를 표시합니다.
[no] debug ip igmp-snooping [packet | timer | event | error]	IGMP-snooping의 패킷, 타이머, 이벤트, 또는 오류 디버그 출력 스위치를 활성화하거나 비활성화합니다. 디버그 스위치를 지정하지 않으면 모든 디버그 스위치가 활성화되거나 비활성화됩니다.

IGMP-snooping 실행 중인 VLAN 정보를 표시합니다.

switch # show ip igmp-snooping

Global IGMP snooping configuration:

Globally enable : Enabled

VLAN nodes : 1,50,100,200,400,500

Dlf-frames filtering : Disabled

Sensitive : Disabled

Querier : Enabled

Querier address : 10.0.0.200

Querier interval : 140 s

Router age : 260 s

Response time : 15 s

vlan_id	Immediate-leave	Ports	Router Ports
1	Disabled	5-10	SWITCH(querier);
50	Disabled	1-4	SWITCH(querier);
100	Disabled	NULL	SWITCH(querier);G0/1(static);
200	Disabled	NULL	SWITCH(querier);
400	Disabled	NULL	SWITCH(querier);
500	Disabled	NULL	SWITCH(querier);

IGMP-snooping의 멀티캐스트 그룹 정보를 표시합니다.

switch# show ip igmp-snooping group

The total number of groups 2

Vlan	Group	Type	Port(s)
1	226.1.1.1	IGMP	G0/1 G0/3
1	225.1.1.16	IGMP	G0/1 G0/3

포트에 추가된 IGMP-snooping 멀티캐스트 그룹 정보를 표시합니다.

Switch#show ip igmp-snooping group interface g0/4

Number of joined groups: 1

Vlan	Group	Mode	Source Num

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

2 230.1.1.1 Exclude 0

IGMP-snooping 타이머 정보를 표시합니다.

switch#show ip igmp-snooping timers

vlan 1 router age : 251

vlan 1 multicast address 0100.5e00.0809 response time : 1

IGMP-snooping 통계 정보를 표시합니다.

Switch_config#show ip igmp-s statistics

IGMP Snooping Message Statistics

L2 main messages sent OK : 75

L2 main messages sent failed : 0

L2 packets received : 72

L2 packets sent : 72

L2 packets sent failed : 0

L2 link-status messages : 3

IGMP Snooping messages received: 79

IGMP packet messages received : 72

IGMP Snooping Packet Statistics

Received packets : 72

IGMP packets : 29

M-routing protocol packets : 0

Other packets : 43

Received IGMP general queries : 0

Received IGMPv2 specific queries : 0

Received IGMPv3 g specific queries : 0

Received IGMPv3 gs specific queries: 0

Received IGMPv1 reports : 0

Received IGMPv2 reports : 0

Received IGMP leaves : 0

Received IGMPv3 reports : 29

Flooded queries : 0

Forwarded and proxy-sent reports : 0

Forwarded and proxy-sent leaves : 0

IGMP Snooping Hardware Operation Statistics

Total : 0 Total number of hardware operations

Succeeded : 0 Number of successful hardware operations

Failed : 0 Number of failed hardware operations

Report/leave processing: 0 Number of hardware operations processing report and leave

Response timer expiring: 0 Number of hardware operations in response to timer aging

Group creating/updating: 0 Number of hardware operations resulting from creating and updating groups

Group deleting : 0 Number of hardware operations caused by deleting a group

IGMP-snooping의 VLAN 정보를 표시합니다.

Switch_config#show ip igmp-snooping vlan

vlan_id	Immediate-leave	Ports	Router Ports
1	Disabled	7-30	
2	Disabled	NULL	

IGMP-snooping의 메시지 타이머를 디버그합니다.

switch#debug ip igmp-snooping packet

Jan 1 02:22:28 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:

Jan 1 02:22:28 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.

Jan 1 02:22:29 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:

Jan 1 02:22:29 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.

Jan 1 02:22:38 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:

Jan 1 02:22:38 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.

Jan 1 02:22:39 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:

Jan 1 02:22:39 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.

Jan 1 02:23:11 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:

Jan 1 02:23:11 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.

Jan 1 02:23:12 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:

Jan 1 02:23:12 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.

IGMP-snooping의 메시지 타이머 디버그를 수행합니다.

switch#debug ip igmp-snooping timer

Jan 1 02:30:36 IGMP-snooping: Vlan 1 router on interface (null) expiry.

Jan 1 02:30:36 IGMP-snooping: Vlan 100 router on interface (null) expiry.

Jan 1 02:30:36 IGMP-snooping: Vlan 200 router on interface (null) expiry.

Jan 1 02:30:36 IGMP-snooping: Vlan 400 router on interface (null) expiry.

Jan 1 02:30:36 IGMP-snooping: Vlan 500 router on interface (null) expiry. Inquerying the response timer expiry

24.2 IGMP-Proxy 설정 작업

IGMP Proxy는 멀티캐스트 사용자가 위치한 VLAN이 다른 VLAN의 멀티캐스트 소스를 수신할 수 있도록 합니다. IGMP Proxy는 레이어 2에서 독립적으로 실행되며, 다른 멀티캐스트 라우팅 프로토콜 없이 작동합니다. IGMP Proxy는 프록시된 VLAN의 IGMP 패킷을 프록시하는 VLAN으로 전송하고, 이러한 IGMP 패킷에 따라 에이전트 VLAN의 멀티캐스트 사용자 하드웨어 포워드 테이블

을 유지 관리합니다.

IGMP Proxy는 VLAN을 두 가지로 나눕니다: 프록시된 VLAN과 프록시하는 VLAN입니다.

다운스트림 멀티캐스트 VLAN은 프록시된 VLAN으로 설정할 수 있으며, 업스트림 멀티캐스트 VLAN은 프록시하는 VLAN으로 설정할 수 있습니다.

IGMP Proxy는 IGMP Snooping을 기반으로 하지만, 두 기능은 독립적으로 작동합니다. IGMP Proxy를 활성화하거나 비활성화하더라도 IGMP Snooping에는 영향을 미치지 않으며, IGMP Snooping이 활성화된 경우에만 IGMP Proxy가 작동합니다.

다음 조건이 충족되지 않으면 IGMP Proxy는 사용할 수 없습니다.

- L3 스위치
- IP 멀티캐스트 라우팅을 동시에 활성화하지 않음
- VLAN이 다운스트림 VLAN 및 업스트림 VLAN으로 동시에 작동하지 않도록 설정

IGMP-Proxy 설정 작업

- IGMP-Proxy 활성화/비활성화
- VLAN 에이전트 관계 추가/삭제
- IGMP-Proxy 모니터링 및 유지 관리

24.2.1 IGMP-Proxy 활성화/비활성화

다음 명령어를 글로벌 설정 모드에서 실행합니다.

명령어	설명
ip igmp-proxy enable	IGMP Proxy를 활성화합니다.
no ip igmp-proxy enable	기본 설정으로 되돌립니다.

IP 멀티캐스트 라우팅이 활성화된 후에는 IGMP Proxy를 활성화할 수 없습니다. IP 멀티캐스트 라우팅이 활성화되면, 이전에 활성화된 IGMP Proxy는 자동으로 종료됩니다. 반면, ip multicast-routing이 비활성화되어도 IGMP Proxy는 자동으로 활성화되지 않습니다.

24.2.2 VLAN 에이전트 관계 추가/삭제

다음 명령어를 글로벌 설정 모드에서 실행합니다.

명령어	설명
ip igmp-proxy agent-vlan *avlan_map* **client-vlan**	에이전트 VLAN(avlan_map)을 추가하여 지정된

map c*vlan_map*	VLAN(cvlan_map)을 관리합니다.
no ip igmp-proxy agent-vlan a*vlan_map* **client-vlan map** c*vlan_map*	에이전트 관계를 삭제합니다.

참고 :

- 에이전트 VLAN(avlan_map)이 먼저 지정되지 않은 상태에서는 지정된 VLAN(cvlan_map)을 설정할 수 없습니다. 마찬가지로, 지정된 VLAN(cvlan_map)이 먼저 설정되지 않으면 에이전트 VLAN(avlan_map)을 설정할 수 없습니다.
- 지정된 VLAN과 에이전트 VLAN 모두 IGMP Snooping의 제어를 받아야 합니다.

24.2.3 IGMP-Proxy 모니터링 및 유지 관리

다음 명령어를 EXEC 모드에서 실행합니다.

명령어	설명
show ip igmp-proxy	IGMP Proxy에 대한 정보를 표시합니다.
[**no**] **debug ip igmp-proxy** *[error / event / packet]*	IGMP Proxy 디버그 스위치를 활성화하거나 비활성화합니다.

24.3 MLD-Snooping 개요

MLD 스누핑(MLD Snooping)의 역할은 VLAN 내 IPv6 그룹 주소의 포워딩 관계를 유지하고, 멀티캐스트 그룹의 변화에 따라 동기화하여 데이터가 멀티캐스트 그룹의 토폴로지에 따라 포워딩되도록 하는 것입니다.

주요 기능은 다음과 같습니다.

- MLD 스누핑 패킷을 모니터링
- 그룹 주소와 VLAN 간의 테이블 유지
- MLD 스누핑 호스트와 MLD 스누핑 라우터의 동기화
- 불필요한 브로드캐스트 문제 해결

L2 장치에서 MLD 스누핑이 실행되지 않은 경우, 멀티캐스트 데이터는 2계층에서 브로드캐스트됩니다.

반면, MLD 스누핑이 실행 중인 경우, 알려진 멀티캐스트 그룹의 데이터는 지정된 수신자로만 전송되고, 알려지지 않은 멀티캐스트 데이터는 삭제됩니다.

참고:

MLD 스누핑은 MLD 스누핑의 Query 및 Report 패킷을 모니터링하여 위의 문제를 해결합니다. 따라서 멀티캐스트 라우터가 존재해야 MLD 스누핑이 정상 작동합니다. 즉, 스위치는 주기적으로 라우터로부터 MLD 스누핑 쿼리 메시지를 수신해야 합니다.
이와 관련하여 MLD 스누핑의 라우터 에이지 타이머(router age timer) 설정은 연결된 멀티캐스트 라우터의 그룹 쿼리 주기보다 커야 합니다. 각 VLAN에서 멀티캐스트 라우터 정보를 보려면 show ipv6 mld-snooping 명령어를 사용하세요.

24.4 MLD-Snooping 멀티캐스트 설정 작업

- MLD 스누핑 활성화/비활성화
- 멀티캐스트 그룹의 하드웨어 포워딩 요청 활성화/비활성화
- VLAN의 static 멀티캐스트 주소 추가/삭제
- MLD 스누핑 라우터 에이지 타이머 설정
- MLD 스누핑 응답 시간 타이머 설정
- static 멀티캐스트 라우터 포트 설정
- Immediate Leave 기능 설정
- MLD 스누핑 모니터링 및 유지 관리

24.4.1 MLD-Snooping 멀티캐스트 활성화/비활성화

다음 명령어를 글로벌 설정 모드에서 실행합니다.

명령어	설명
ipv6 mld-snooping	MLD 스누핑 멀티캐스트를 활성화합니다.
no ipv6 mld-snooping	MLD 스누핑 멀티캐스트를 비활성화합니다.

참고:

MLD 스누핑이 활성화된 후 멀티캐스트 패킷을 찾을 수 없으면, 등록되지 않은 대상 주소의 멀티캐스트 패킷은 삭제됩니다.

24.4.2 멀티캐스트 그룹 하드웨어 포워딩 요청 활성화/비활성화

다음 명령어를 글로벌 설정 모드에서 실행합니다.

명령어	설명

ipv6 mld-snooping solicitation	멀티캐스트 그룹의 하드웨어 포워딩 요청을 활성화합니다.
no ipv6 mld-snooping solicitation	하드웨어 포워딩 요청을 비활성화합니다.

24.4.3 VLAN의 static 멀티캐스트 주소 추가/삭제

MLD 스누핑 프로토콜을 지원하지 않는 일부 호스트가 해당 그룹 패킷을 수신하도록 설정할 수 있습니다. 다음 명령어를 글로벌 설정 모드에서 실행합니다.

명령어	설명
ipv6 mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf_name*	VLAN의 static 멀티캐스트 주소를 추가합니다.
no ipv6 mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf_name*	VLAN의 static 멀티캐스트 주소를 삭제합니다.

24.4.4 MLD-Snooping 라우터 에이지 타이머 설정

라우터 에이지 타이머는 MLD 스누핑 쿼리 당사자의 존재를 모니터링하는 데 사용됩니다.
다음 명령어를 글로벌 설정 모드에서 실행합니다.

명령어	설명
ipv6 mld-snooping timer router-age *timer_value*	MLD 스누핑 라우터 에이지를 설정합니다.
no ipv6 mld-snooping timer router-age	기본 라우터 에이지 설정으로 되돌립니다.

참고 :

- 이 타이머 설정은 MLD 쿼리 주기보다 커야 합니다.
- 권장 설정은 쿼리 주기의 3배입니다.
- 기본값: 260초

24.4.5 MLD-Snooping 응답 시간 타이머 설정

다음 명령어를 글로벌 설정 모드에서 실행합니다.

명령어	설명
ipv6 mld-snooping timer response-time *timer_value*	MLD 스누핑 라우터 에이지를 설정합니다.
no ipv6 mld-snooping timer response-time	기본 라우터 에이지 설정으로 되돌립니다.

참고:

- 타이머 값이 너무 작으면 멀티캐스트 통신이 불안정해질 수 있습니다.
- 기본값: 10초

24.4.6 MLD-Snooping 쿼리어 설정

멀티캐스트 라우터가 없는 경우, 쿼리어(Querier)를 활성화해 가상 멀티캐스트 라우터 역할을 수행할 수 있습니다.
다음 명령어를 글로벌 설정 모드에서 실행합니다.

명령어	설명
[**no**] **ipv6 mld-snooping querier [address** *[ip_addr]***]**	MLD 스누핑 쿼리어를 설정합니다.

참고:

- VLAN에 멀티캐스트 라우터가 존재하면 쿼리어는 비활성화됩니다.
- 라우터가 타임아웃되면 쿼리어는 자동으로 활성화됩니다.

24.4.7 static 멀티캐스트 라우터 포트 설정

포트를 static 멀티캐스트 라우터 포트로 구성하면, 해당 포트로 모든 MLD 스누핑 Report 및 Done 메시지가 전달됩니다.
다음 명령어를 글로벌 설정 모드에서 실행합니다.

명령어	설명
ipv6 mld-snooping vlan *WORD* **mrouter** interface *inft_name*	해당 VLAN에서 MLD 스누핑을 위한 static 멀티캐스트 라우터 포트를 설정합니다.
no ipv6 mld-snooping vlan *WORD* **mrouter** interface *inft_name*	해당 VLAN에서 MLD 스누핑의 static 멀티캐스트 라우터 포트를 삭제합니다.

24.4.8 Immediate Leave 기능 활성화/비활성화

Immediate Leave 기능은 멀티캐스트 그룹에서 호스트가 빠르게 나갈 수 있도록 합니다.
다음 명령어를 글로벌 설정 모드에서 실행합니다.

명령어	설명
ipv6 mld-snooping vlan *WORD* **immediate-leave**	Immediate Leave 기능을 활성화합니다.
no ipv6 mld-snooping vlan *WORD* **immediate-leave**	기본 설정으로 되돌립니다.

24.4.9 MLD-Snooping 멀티캐스트 모니터링 및 유지 관리

다음 명령어를 EXEC 모드에서 실행합니다.

명령어	설명
show ipv6 mld-snooping	MLD 스누핑 설정을 확인합니다.
show ipv6 mld-snooping timer	MLD 스누핑 타이머 상태를 확인합니다.
show ipv6 mld -snooping groups	MLD 스누핑 멀티캐스트 그룹을 확인합니다.
show ipv6 mld-snooping statistics	MLD 스누핑 통계 정보를 확인합니다.
show ipv6 mld-snooping vlan	VLAN 내 MLD 스누핑 설정을 확인합니다.
show ipv6 mld-snooping mac	MLD 스누핑으로 기록된 멀티캐스트 MAC 주소를 확인합니다.

24.5 DHCP-Snooping구성 작업

DHCP-Snooping은 DHCP 패킷을 판별하여 위조된 DHCP 서버가 DHCP 서비스를 제공하는 것을 방지하고, MAC 주소와 IP 주소 간의 바인딩 관계를 유지하는 기능입니다.

L2 스위치는 MAC 주소와 IP 주소 간의 바인딩 관계에 따라 DAI(Dynamic ARP Inspection) 및 IP 소스 가드 기능을 수행할 수 있습니다.

DHCP-Snooping은 주로 DHCP 패킷을 모니터링하고 MAC-IP 바인딩 목록을 동적으로 유지합니다.

L2 스위치는 MAC-IP 바인딩 관계를 충족하지 않는 패킷을 필터링하여, 불법 사용자로부터의 네트워크 공격을 방지합니다.

DHCP-Snooping 구성 작업 목록

- DHCP-Snooping 기능 활성화/비활성화
- 특정 VLAN에서 DHCP-Snooping 활성화
- 인터페이스를 DHCP trust 인터페이스로 설정
- 특정 VLAN에서 DAI 활성화
- 인터페이스를 ARP trust 인터페이스로 설정
- 특정 VLAN에서 소스 IP 주소 모니터링 활성화
- 소스 IP 주소 모니터링을 위한 trust 인터페이스 설정
- DHCP Snooping을 대기 TFTP 서버에 바인딩
- DHCP-Snooping 바인딩 백업 파일 이름 구성
- DHCP-Snooping 바인딩 백업 주기 구성

- 바인딩 관계 수동 설정 또는 추가
- DHCP-Snooping 모니터링 및 유지 관리
- DHCP-Snooping 구성 예제

24.5.9 DHCP-Snooping 활성화/비활성화

다음 명령어를 글로벌 구성 모드에서 실행합니다.

명령어	설명
ip dhcp-relay snooping	DHCP-Snooping을 활성화합니다.
no ip dhcp-relay snooping	기본 설정으로 되돌립니다.

이 명령어는 글로벌 구성 모드에서 DHCP-Snooping을 활성화하는 데 사용됩니다.
이 명령어가 실행된 후, 스위치는 모든 DHCP 패킷을 모니터링하고 해당 바인딩 관계를 형성합니다.

참고 : 클라이언트가 이 명령어 실행 전에 스위치로부터 주소를 할당받은 경우, 스위치는 해당 바인딩 관계를 추가할 수 없습니다.

24.5.10 VLAN에서 DHCP-Snooping 활성화

VLAN에서 DHCP-Snooping이 활성화되면, 해당 VLAN 내에서 trust되지 않은 물리적 포트로 수신된 모든 DHCP 패킷이 합법적으로 검사됩니다.

VLAN 내에서 trust되지 않은 포트로부터 수신된 DHCP 응답 패킷은 삭제되어, 위조되거나 잘못 구성된 DHCP 서버가 주소 할당 서비스를 제공하는 것을 방지합니다.

trust되지 않은 포트에서 수신된 DHCP 요청 패킷의 하드웨어 주소 필드가 해당 패킷의 MAC 주소와 일치하지 않는 경우, 스위치는 이를 DHCP DoS 공격을 위한 위조 패킷으로 판단하고 삭제합니다.

다음 명령어를 글로벌 구성 모드에서 실행합니다.

명령어	설명
ip dhcp-relay snooping vlan *vlan_id*	특정 VLAN에서 DHCP-Snooping을 활성화합니다.
no ip dhcp-relay snooping vlan *vlan_id*	특정 VLAN에서 DHCP-Snooping을 비활성화합니다.

24.5.11 VLAN에서 DHCP 공격 방지 활성화

특정 VLAN에서 공격 방지 기능을 활성화하려면, 해당 VLAN에서 허용되는 최대 DHCP 클라이언트 수를 설정하고 "선착순(First come, first serve)" 원칙을 적용해야 합니다.

특정 VLAN의 사용자 수가 최대 값에 도달하면, 새로운 클라이언트는 주소를 할당받을 수 없습니다.

명령어	설명
ip dhcp-relay snooping vlan *vlan_id* **max-client** *number*	특정 VLAN에서 DHCP 공격 방지 기능을 활성화합니다.
no ip dhcp-relay snooping vlan *vlan_id* **max-client**	특정 VLAN에서 DHCP 공격 방지 기능을 비활성화합니다.

24.5.12 DHCP trust 인터페이스로 설정

인터페이스를 DHCP trust 인터페이스로 설정하면, 해당 인터페이스에서 수신된 DHCP 패킷은 검사되지 않습니다.

명령어	설명
dhcp snooping trust	인터페이스를 DHCP trust 인터페이스로 설정합니다.
no dhcp snooping trust	인터페이스를 DHCP distrust 인터페이스로 되돌립니다.

기본값: 인터페이스는 기본적으로 비trust 인터페이스로 설정됩니다.

24.5.13 바인딩 테이블 빠른 업데이트 기능 활성화/비활성화

이 기능은 기본적으로 비활성화되어 있습니다. 기능이 비활성화된 상태에서 포트가 클라이언트 A에 바인딩되어 있으면, 클라이언트 A가 오프라인 상태라도 다른 포트에서 동일한 MAC 주소로 DHCP 요청을 보내면 이를 위조 MAC 공격으로 간주합니다. 기능이 활성화되면, 위와 같은 상황이 발생하지 않습니다. 클라이언트가 포트를 자주 변경하거나, DHCP 서버에서 분배한 주소 임대 기간을 짧게 설정할 수 없는 경우 이 기능을 활성화하는 것이 권장됩니다.

명령어	설명
ip dhcp-relay snooping rapid-refresh-bind	바인딩 테이블의 빠른 업데이트 기능을 활성화합니다.
no ip dhcp-relay snooping rapid-refresh-bind	바인딩 테이블의 빠른 업데이트 기능을 비활성화합니다.

24.5.14 VLAN에서 DAI(동적 ARP 검사) 활성화

VLAN의 모든 물리 포트에서 동적 ARP 모니터링을 수행하면, 수신된 ARP 패킷의 소스 MAC 주소와 소스 IP 주소가 설정된 MAC-IP 바인딩 관계와 일치하지 않을 경우 해당 ARP 패킷은 폐기됩니다. 인터페이스의 바인딩 관계는 DHCP에 의해 동적으로 설정되거나 수동으로 구성할 수 있습니다. 물리 인터페이스에 IP 주소와 바인딩된 MAC 주소가 없는 경우, 스위치는 모든 ARP 패킷의

포워딩을 거부합니다.

명령어	설명
ip arp inspection vlan *vlanid*	VLAN의 모든 distrust 포트에서 동적 ARP 모니터링을 활성화합니다.
no ip arp inspection vlan *vlanid*	VLAN의 모든 distrust 포트에서 동적 ARP 모니터링을 비활성화합니다.

24.5.15 ARP trust 인터페이스로 설정

ARP 모니터링은 trust 된 인터페이스에서는 활성화되지 않습니다. 인터페이스는 기본적으로 distrust 상태입니다.

명령어	설명
arp inspection trust	인터페이스를 ARP trust 인터페이스로 설정합니다.
no arp inspection trust	인터페이스를 ARP distrust 인터페이스로 되돌립니다.

24.5.16 VLAN에서 소스 IP 주소 모니터링 활성화

VLAN에서 소스 IP 주소 모니터링이 활성화되면, 해당 VLAN의 모든 물리 포트에서 수신된 IP 패킷의 소스 MAC 주소와 소스 IP 주소가 설정된 MAC-IP 바인딩 관계와 일치하지 않을 경우 해당 패킷이 폐기됩니다. 인터페이스의 바인딩 관계는 DHCP에 의해 동적으로 설정되거나 수동으로 구성할 수 있습니다. 물리 인터페이스에 IP 주소와 바인딩된 MAC 주소가 없는 경우, 스위치는 해당 물리 인터페이스에서 수신된 모든 IP 패킷의 포워딩을 거부합니다.

명령어	설명
ip verify source vlan *vlanid*	VLAN의 모든 distrust 인터페이스에서 소스 IP 주소 확인을 활성화합니다.
no ip verify source vlan *vlanid*	VLAN의 모든 인터페이스에서 소스 IP 주소 확인을 비활성화합니다.

참고 : DHCP 패킷(즉, IP 패킷)은 글로벌 스누핑이 구성되어 있는 경우 포워딩됩니다.

24.5.17 소스 IP 주소 모니터링에서 신뢰 인터페이스 설정

소스 IP 주소 신뢰 인터페이스에서는 소스 주소 감지 기능이 활성화되지 않습니다.

명령어	설명
ip-source trust	인터페이스를 trust 소스 IP 주소 인터페이스로 설정합니다.

no ip-source trust	인터페이스를 distrust 소스 IP 주소 인터페이스로 되돌립니다..

24.5.18 DHCP-Snooping 옵션 82 설정

옵션 82는 서버로 로컬 정보를 전송하여 클라이언트에게 주소를 할당하는 데 도움을 줍니다.

명령어 (글로벌 구성 모드에서 실행)

명령어	설명
ip dhcp-relay snooping information option	DHCP-Snooping이 DHCP 패킷을 포워딩할 때 기본 형식으로 옵션 82를 포함합니다.
no ip dhcp-relay snooping information option	DHCP-Snooping이 DHCP 패킷을 포워딩할 때 옵션 82를 포함하지 않습니다.

옵션 82 형식 지정 (글로벌 구성 모드에서 실행)

명령어	설명
ip dhcp-relay snooping information option format {snmp-ifindex/manual/hn-type / cm-type/ [host]/hw-type}	DHCP-Snooping이 DHCP 패킷을 포워딩할 때 옵션 82의 형식을 지정합니다.
no ip dhcp-relay snooping information option format {snmp-ifindex/manual/hn-type /cm-type/[host]/hw-type}	DHCP-Snooping이 옵션 82를 포함하지 않도록 설정합니다.

수동 모드에서 옵션 82 설정 (회로 ID)

명령어	설명
dhcp snooping information circuit-id string [STRING]	수동 형식으로 옵션 82를 설정할 때, 문자열로 회로 ID를 설정합니다.
dhcp snooping information circuit-id **hex [***xx-xx-xx-xx-xx-xx***]**	수동 형식으로 옵션 82를 설정할 때, 16진수로 회로 ID를 설정합니다.
no dhcp snooping information circuit-id	수동으로 설정된 옵션 82의 회로 ID를 삭제합니다.

수동 모드에서 옵션 82 설정 (원격 ID)

명령어	설명
dhcp snooping information remote-id string [STRING]	수동 형식으로 옵션 82를 설정할 때, 문자열로 원격 ID를 설정합니다.
dhcp snooping information remote-id hex [xx-xx-xx-xx-	수동 형식으로 옵션 82를 설정할 때, 16진수로 원격 ID

xx-xx]	를 설정합니다.
no dhcp snooping information remote-id	수동으로 설정된 옵션 82의 원격 ID를 삭제합니다.

수동 모드에서 옵션 82 설정 (벤더 전용)

명령어	설명
dhcp snooping information vendor-specific string STRING	수동 형식으로 옵션 82를 설정할 때, 문자열로 벤더 전용 정보를 설정합니다.
dhcp snooping information vendor-specific hex [*xx-xx-xx-xx-xx-xx***]**	수동 형식으로 옵션 82를 설정할 때, 16진수로 벤더 전용 정보를 설정합니다.
no **dhcp snooping information vendor-specific**	수동으로 설정된 옵션 82의 벤더 전용 정보를 삭제합니다.

이 설정은 DHCP 패킷에 옵션 82를 추가하여 네트워크에서 클라이언트의 출처를 추적하고 DHCP 요청을 보다 안전하게 관리할 수 있도록 합니다.

24.5.19 DHCP-Snooping 옵션 82 패킷 정책 설정

DHCP 요청 패킷이 옵션 82를 포함하여 수신된 경우, 해당 패킷에 대한 정책을 설정할 수 있습니다. 정책은 다음과 같습니다.

"Drop" 정책 : 옵션 82가 포함된 요청 패킷을 폐기합니다.

명령어	설명
dhcp snooping information drop	옵션 82를 포함한 요청 패킷을 폐기합니다.

"Append" 정책 : 옵션 82가 포함된 요청 패킷을 추가합니다.

명령어	설명
dhcp snooping information append	포트에서 옵션 82를 추가하는 기능을 활성화합니다.
dhcp snooping information append first-subop9-param { hex *xx-xx-xx-xx-xx-xx* **| vlanip | hostname }**	옵션 82 벤더 전용 서브옵션 9의 첫 번째 매개변수를 설정합니다.
dhcp snooping information append second-subop9-param { hex *xx-xx-xx-xx-xx-xx* **| vlanip | hostname }**	옵션 82 벤더 전용 서브옵션 9의 두 번째 매개변수를 설정합니다.

24.5.20 인터페이스 바인딩 백업을 위한 TFTP 서버 구성

스위치 구성이 재부팅되면 이전에 구성된 인터페이스 바인딩이 손실됩니다. 이 경우, 해당 인터페이스에는 바인딩 관계가 존재하지 않습니다. 소스 IP 주소 모니터링이 활성화된 경우, 스위치는 모든 IP 패킷의 포워딩을 거부합니다. TFTP 서버를 인터페이스 바인딩 백업용으로 구성하면, 바인

딩 관계가 TFTP 프로토콜을 통해 서버에 백업됩니다.

스위치가 재시작된 후, 스위치는 TFTP 서버에서 자동으로 바인딩 목록을 다운로드하여 네트워크가 정상적으로 운영되도록 보장합니다.

명령어	설명
ip dhcp-relay snooping database-agent *ip-address*	인터페이스 바인딩을 백업할 TFTP 서버의 IP 주소를 구성합니다.
no ip dhcp-relay snooping database-agent *ip-address*	인터페이스 바인딩 백업용 TFTP 서버 구성을 취소합니다.

24.5.21 인터페이스 바인딩 백업 파일 이름 구성

인터페이스 바인딩 관계를 백업할 때, 해당 파일 이름이 TFTP 서버에 저장됩니다.
이렇게 하면 여러 스위치가 동일한 TFTP 서버에 자신의 인터페이스 바인딩 관계를 각각 백업할 수 있습니다.

명령어	설명
ip dhcp-relay snooping db-file name [timestamp]	인터페이스 바인딩 백업 파일의 이름을 구성합니다.
no ip dhcp-relay snooping db-file	인터페이스 바인딩 백업 파일 이름 구성을 취소합니다.

24.5.22 인터페이스 바인딩 백업 주기 구성

인터페이스에서 MAC-IP 바인딩 관계는 동적으로 변경됩니다. 따라서 일정 간격으로 바인딩 관계가 업데이트되었는지 확인해야 합니다. 바인딩 관계가 업데이트(추가 또는 삭제)되면, 해당 정보를 다시 백업해야 합니다. 기본 백업 주기는 30분입니다.

명령어	설명
ip dhcp-relay snooping write-immediately	바인딩 정보가 변경될 때 DHCP Snooping 즉시 백업을 구성합니다.
ip dhcp-relay snooping write-time *num*	인터페이스 바인딩 백업 주기를 기본 설정으로 되돌립니다.
no ip dhcp-relay snooping write-time	인터페이스 바인딩 백업 주기를 구성합니다. (단위: 분)

24.5.23 인터페이스 바인딩 수동 구성

호스트가 DHCP를 통해 주소를 할당받지 않은 경우, 스위치의 인터페이스에 바인딩 항목을 추가하여 호스트가 네트워크에 액세스할 수 있도록 할 수 있습니다. no ip source binding MAC IP 명령어를 사용하여 해당 바인딩 목록에서 항목을 삭제할 수 있습니다.

주의 :수동으로 구성된 바인딩 항목은 동적으로 구성된 바인딩 항목보다 우선순위가 높습니다.

수동으로 구성된 바인딩 항목과 동적으로 구성된 바인딩 항목이 동일한 MAC 주소를 가질 경우, 수동 항목이 동적 항목을 덮어쓰며 인터페이스 바인딩 항목은 MAC 주소를 고유 인덱스로 사용합니다.

명령어	설명
ip source binding *MAC IP* interface *name vlan-id*	인터페이스에서 수동으로 바인딩을 구성합니다.
no ip source binding *MAC IP vlan-id*	인터페이스 바인딩 항목을 삭제합니다.

24.5.24 DHCP-Snooping 모니터링 및 유지 관리

명령어	설명
show ip dhcp-relay snooping	DHCP-Snooping 구성 정보를 표시합니다.
show ip dhcp-relay snooping binding	인터페이스에서 유효한 주소 바인딩 항목을 표시합니다.
show ip dhcp-relay snooping binding all	DHCP-Snooping으로 생성된 모든 바인딩 항목을 표시합니다.
[**no**] **debug ip dhcp-relay** [snooping | binding | event | all]	DHCP 릴레이 스누핑 바인딩 또는 이벤트의 스위치를 활성화하거나 비활성화합니다.

24.5.25 설정 예제

VLAN 1에서 DHCP 스누핑을 활성화하여 프라이빗 네트워크 A에 연결합니다.

Switch_config#ip dhcp-relay snooping

Switch_config#ip dhcp-relay snooping vlan 1

VLAN 2에서 DHCP 스누핑을 활성화하여 프라이빗 네트워크 B에 연결합니다.Switch_config#ip dhcp-relay snooping

Switch_config#ip dhcp-relay snooping vlan 2

DHCP 서버에 연결된 인터페이스를 DHCP 신뢰 인터페이스로 설정합니다.

Switch_config_g0/1#dhcp snooping trust

옵션 82 인스턴스를 수동으로 구성합니다.

interface GigaEthernet0/1

dhcp snooping information circuit-id hex 00-01-00-05

dhcp snooping information remote-id hex 00-e0-0f-13-1a-50

dhcp snooping information vendor-specific hex 00-00-0c-f8-0d-01-0b-78-69-61-6f-6d-69-6e-37-

```
31-31-34
 dhcp snooping information append
 dhcp snooping information append first-subop9-param hex 61-62-63-61-62-63
!
interface GigaEthernet0/2
dhcp snooping trust
arp inspection trust
   ip-source trust
!
!
!
ip dhcp-relay snooping
ip dhcp-relay snooping vlan   1-100
ip arp inspection vlan   1
ip verify source vlan   1
ip dhcp-relay snooping information option format manual
```

25. QoS 구성

25.1 QoS 개요

25.1.1 QoS 개념

일반적으로 스위치는 베스트 에포트(best-effort) 방식으로 동작하며, 모든 트래픽을 동등하게 처리하고 가능한 모든 트래픽을 전달하려고 합니다. 따라서 혼잡이 발생하면 모든 트래픽이 동일한 확률로 폐기될 수 있습니다. 하지만 실제 네트워크에서는 서로 다른 트래픽이 서로 다른 중요성을 가지며, 스위치의 QoS 기능은 각 트래픽의 중요도에 따라 서로 다른 서비스를 제공하며 중요한 트래픽은 더 나은 서비스를 받게 됩니다.

트래픽의 중요도를 분류하는 주요 방법은 다음과 같습니다.

- 802.1Q 프레임 헤더의 태그

  2바이트 크기의 태그 중 3비트가 패킷의 우선순위를 나타냅니다.

  8개의 우선순위가 있으며, 0은 가장 낮은 우선순위, 7은 가장 높은 우선순위를 의미합니다.

- IP 패킷 헤더의 DSCP 필드

  IP 헤더의 TOS(서비스 유형) 필드 하위 6비트를 사용합니다.

실제 네트워크에서는 엣지 스위치가 트래픽의 중요도에 따라 서로 다른 우선순위를 부여하고, 우선순위에 따라 다른 서비스가 제공됩니다.

이 방식은 단말 간(end-to-end) QoS를 실현하는 방법입니다.

또한 네트워크에서 특정 속성을 가진 패킷(예: MAC 레이어 또는 L3 정보 기준)을 스위치가 특별히 처리하도록 설정할 수 있습니다. 이러한 동작을 한 번의 홉(one-leap) 동작이라고 합니다. 스위치의 QoS 기능은 제한된 네트워크 대역폭을 최적화하여 전체 네트워크 성능을 크게 향상시킵니다.

25.1.2 단말 간(end-to-end) QoS 모델

서비스 모델은 단말 간 QoS 기능을 설명하며, 네트워크가 특정 통신 서비스를 한 단말에서 다른 단말로 전송하는 능력을 의미합니다.
QoS 소프트웨어는 두 가지 서비스 모델을 지원합니다.

- 베스트 에포트(Best-Effort) 서비스

  베스트 에포트 서비스는 단순한 서비스 모델입니다. 이 모델에서는 애플리케이션이 허가나 사전 네트워크 알림 없이 필요한 시점에 원하는 양의 데이터를 보낼 수 있습니다. 베스트 에포트 서비스에서는 네트워크가 허용하는 경우 데이터를 전송할 수 있으나, 신뢰

성, 지연, 처리량에 대한 보장은 없습니다. 베스트 에포트 서비스가 구현된 스위치의 QoS는 기본적으로 선착순 처리(First Come, First Served, FCFS) 방식으로 작동합니다.

- 차등 서비스(Differentiated Service)

  차등 서비스에서는 특정 서비스를 네트워크에서 전송하려면 각 패킷에 적절한 QoS 태그를 지정해야 합니다. 이 태그 지정은 다양한 방식으로 구현될 수 있으며, 예를 들어 IP 데이터 패킷에서 IP 우선순위 상태를 설정하는 방식이 있습니다. 스위치는 이러한 QoS 규칙을 사용해 트래픽을 분류하고 지능형 큐잉(intelligent queuing)을 수행합니다.

스위치의 QoS는 다음과 같은 큐잉 메커니즘을 제공합니다.

- 엄격 우선순위(Strict Priority, SP)
- 가중 라운드 로빈(Weighted Round Robin, WRR)
- 부족 라운드 로빈(Deficit Round Robin, DRR)
- 선착순 처리(First-Come-First-Served, FCFS)

25.1.3 QoS 큐잉 알고리즘

각 큐잉 알고리즘은 QoS를 구현하는 중요한 기반이며 스위치의 QoS는 다음과 같은 알고리즘을 제공합니다.

- 엄격 우선순위(Strict Priority) : 이 알고리즘은 가장 높은 우선순위의 트래픽에 먼저 서비스를 제공하고, 그 다음으로 높은 우선순위의 트래픽에 서비스를 제공합니다.우선순위가 높은 트래픽에는 매우 좋은 서비스를 제공하지만, 낮은 우선순위의 트래픽은 서비스를 받지 못하고 영구적으로 대기 상태에 빠질 수 있는 단점이 있습니다.
- 가중 라운드 로빈(Weighted Round Robin, WRR) : WRR은 엄격 우선순위 알고리즘에서 발생하는 낮은 우선순위의 트래픽이 무시되는 문제를 해결하기 위한 효과적인 방법입니다.WRR은 각 우선순위 큐에 일정한 대역폭을 할당하고, 높은 우선순위에서 낮은 우선순위 순서로 서비스를 제공합니다. 가장 높은 우선순위 큐가 할당된 대역폭을 모두 사용한 후, 다음 우선순위 큐에 서비스가 제공됩니다.
- 가중 공정 큐잉(Weighted Fair Queuing, WFQ)

  WFQ는 트래픽의 우선순위에 따라 패킷을 분류하고, 각 트래픽의 가중치에 따라 출구 대역폭을 설정합니다. 가중치가 클수록 더 많은 대역폭이 할당됩니다. 이를 통해 우선순위 서비스의 공정성이 보장되고, 서로 다른 우선순위 서비스 간의 가중치 차이를 반영합니다.
- 선착순 처리(First-Come-First-Served, FCFS)

FCFS 알고리즘은 스위치에 도착한 순서대로 패킷에 서비스를 제공합니다. 스위치에 먼저 도착한 패킷이 먼저 처리 됩니다.

25.1.4 가중 랜덤 조기 탐지 (WRED)

- 혼잡 회피와 기존 패킷 손실 메커니즘

  과도한 혼잡은 네트워크 자원에 손상을 줄 수 있으므로, 이를 해결하기 위한 조치가 필요합니다. 혼잡 회피는 네트워크 자원을 모니터링하여 적극적으로 패킷을 폐기하고 네트워크 흐름을 조절하는 방식으로, 네트워크 과부하를 해결하는 일종의 흐름 제어 방법입니다. 기존의 혼잡 해결 방식은 큐 길이가 임계값에 도달하면 모든 수신 패킷을 폐기하는 방법입니다. 그러나 TCP 패킷의 경우, 대량의 패킷 손실은 TCP 타임아웃을 유발하여 TCP 시작 속도를 늦추고 혼잡 회피 상태로 진입하게 됩니다. 이러한 현상을 TCP 글로벌 동기화(TCP Global Synchronization)라고 합니다.

- WRED (Weighted Random Early Detection)

  WRED 알고리즘은 TCP 글로벌 동기화 방지를 위해 도입됩니다. WRED는 사용자가 큐 임계값을 설정할 수 있도록 합니다.

  큐 길이가 설정된 임계값보다 작으면 패킷이 폐기되지 않습니다. 큐 길이가 임계값을 초과하면 패킷이 랜덤하게 폐기됩니다. WRED는 랜덤 폐기 방식을 사용하므로, 여러 TCP 연결이 동시에 전송 속도를 늦추는 상황을 방지합니다. 이로 인해 TCP 글로벌 동기화를 피할 수 있습니다. 특정 TCP 연결에서 패킷이 폐기되고 전송 속도가 느려지더라도, 다른 TCP 연결은 상대적으로 높은 전송 속도를 유지할 수 있습니다. 따라서 언제든지 일부 TCP 연결은 고속으로 패킷을 전송할 수 있으며, 이는 대역폭 사용 효율을 보장하는 데 도움이 됩니다. WRED는 패킷이 출력 큐에 진입할 때 작동하며, 패킷 크기를 확인하여 범위에 따라 서로 다른 처리를 수행합니다. WRED의 주요 매개변수는 Start, Slope, 폐기 우선순위(Drop Priority)입니다.

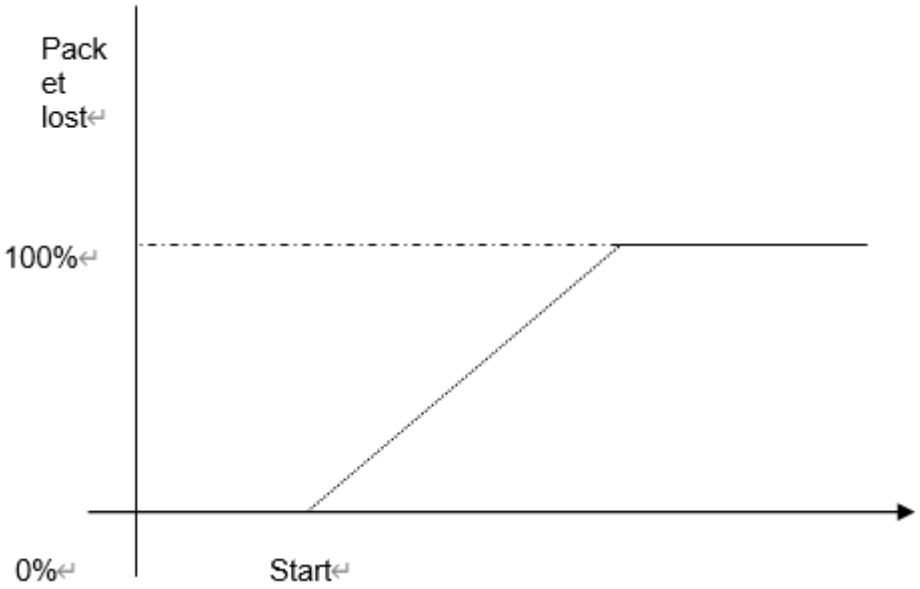


그림 46 평균 큐 길이

- 큐 길이가 start 값보다 작으면 패킷이 폐기되지 않습니다.
- 큐 길이가 start 값보다 크면, 수신된 패킷이 랜덤하게 폐기되기 시작합니다. 큐가 길어질수록 폐기율이 증가합니다.
- 패킷 손실률은 큐 길이가 증가함에 따라 높아집니다.

25.2 QoS 구성 작업 목록

일반적으로 ONU는 각 패킷을 최대한 전달하려고 노력하며, 혼잡이 발생하면 모든 패킷이 동일한 확률로 폐기됩니다. 그러나 실제로는 각 패킷의 중요도가 다르며, 상대적으로 중요한 패킷은 더 나은 서비스를 받아야 합니다. QoS는 중요도가 다른 패킷에 서로 다른 우선순위 서비스를 제공하는 메커니즘으로, 이를 통해 네트워크 성능이 향상되고 자원을 효율적으로 사용할 수 있습니다.

이 장에서는 ONU에서 QoS를 설정하는 방법을 설명합니다.

- 글로벌 cos 우선순위 큐 설정
- cos 우선순위 큐의 대역폭 설정
- cos 우선순위 큐의 스케줄 정책 설정
- 포트의 기본 cos 값 설정
- 포트의 cos 우선순위 큐 설정
- 포트의 cos 우선순위 큐 대역폭 설정
- 포트의 cos 우선순위 큐 스케줄 정책 설정

- dscp 기반 cos 우선순위 큐 설정
- QoS 정책 매핑 생성
- QoS 정책 매핑 설명 설정
- QoS 정책 매핑의 데이터 흐름 일치 설정
- QoS 정책 매핑 데이터 흐름의 동작 설정
- 포트에서 QoS 정책 적용
- 글로벌 QoS 정책 적용
- Trust 모드 구성
- QoS 정책 매핑 테이블 표시

25.3 QoS 구성 작업

25.3.1 글로벌 CoS 우선순위 큐 설정

QoS 우선순위 큐 설정 작업은 IEEE 802.1p에서 정의한 8개의 CoS 값을 스위치의 우선순위 큐에 매핑하는 것입니다. 이 스위치 시리즈는 8개의 우선순위 큐를 제공합니다. 스위치는 각 큐에 따라 서로 다른 스케줄 정책을 적용하여 QoS를 구현합니다. 글로벌 모드에서 CoS 우선순위 큐를 설정하면 모든 포트의 CoS 우선순위 큐 매핑에 영향을 미칩니다. L2 포트에서 우선순위 큐가 설정되면, 해당 우선순위 큐는 해당 L2 포트에서만 동작합니다.

아래 관리 모드로 진입한 후 명령어를 순서대로 실행하여 CoS 우선순위 큐를 설정합니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
[**no**] **cos map** *quid cos1..cosn*	CoS 우선순위 큐를 설정합니다. uid는 CoS 우선순위 큐의 ID를 나타냅니다. cos1..cosn은 IEEE 802.1p에서 정의한 CoS 값입니다.
exit	EXEC 모드로 돌아갑니다.
write	설정을 저장합니다.

25.3.2 CoS 우선순위 큐의 대역폭 설정

우선순위 큐의 대역폭은 각 우선순위 큐에 할당되는 대역폭 비율을 의미하며, CoS 우선순위 큐의 스케줄 정책이 WRR(Weighted Round Robin) 또는 WFQ(Weighted Fair Queuing)로 설정된 경우에 구성됩니다. 이 스위치 시리즈는 총 8개의 우선순위 큐를 제공합니다.

이 명령어를 실행하면 모든 인터페이스의 우선순위 큐 대역폭에 영향을 미칩니다. 큐 스케줄링 모드가 WRR 또는 WFQ로 설정된 경우에만 유효합니다. WRR/WFQ 스케줄 정책이 사용될 때 CoS 우선순위 큐의 대역폭 가중치를 결정합니다.

아래 명령어를 순서대로 실행하여 CoS 우선순위 큐의 대역폭을 설정합니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
[**no**] **scheduler weight bandwidth** *weight1...weightn*	CoS 우선순위 큐의 대역폭을 설정합니다. weight1...weightn은 WRR/DRR 방식의 8개 CoS 큐의 가중치입니다.
exit	EXEC 모드로 돌아갑니다.
write	설정을 저장합니다.

25.3.3 CoS 우선순위 큐 스케줄 정책 설정

스위치의 각 포트에는 여러 개의 출력 큐가 있습니다.
이 스위치 시리즈는 8개의 우선순위 큐를 제공하며, 출력 큐는 다음 네 가지 스케줄링 모드를 사용할 수 있습니다.

- SP (Strict Priority):

  높은 우선순위 큐에 패킷이 있는 경우, 낮은 우선순위 큐의 패킷은 전송되지 않습니다. 높은 우선순위 큐가 비어 있을 때만 낮은 우선순위 큐의 패킷이 전송됩니다.

- WRR (Weighted Round Robin):

  각 우선순위 큐에 일정한 대역폭을 할당하고, 높은 우선순위에서 낮은 우선순위 순서로 서비스를 제공합니다.

- WFQ (Weighted Fair Queuing):

  트래픽의 우선순위에 따라 각 큐에 일정한 대역폭을 할당하는 방식입니다.

- FCFS (First-Come-First-Served):

  패킷이 도착한 순서대로 전송하는 방식으로, 먼저 도착한 패킷이 먼저 서비스됩니다.

아래 명령어를 사용하여 CoS 우선순위 큐의 스케줄 정책을 설정합니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
[**no**] **scheduler policy** { **sp** | **wrr|wfq|fcfs** }	sp: SP(Strict Priority) 스케줄 정책 사용 wrr: WRR(Weighted Round Robin) 스케줄 정책 사용 wfq: WFQ(Weighted Fair Queuing) 스케줄 정책 사용

	fcfs: FCFS(First-Come-First-Served) 스케줄 정책 사용
exit	EXEC 모드로 돌아갑니다.
write	설정을 저장합니다.

25.3.4 포트의 기본 CoS 값 설정

스위치 포트가 태그 없는 데이터 프레임을 수신하면, 스위치는 해당 프레임에 기본 CoS 우선순위를 추가합니다. 포트의 기본 CoS 값을 설정하는 것은 포트에서 수신한 **태그 없는 프레임(untagged frame)**에 지정된 CoS 값을 부여하는 작업입니다.

아래 명령어를 사용하여 포트의 기본 CoS 값을 설정합니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
interface g0/1	설정할 포트로 진입합니다.
[**no**] **cos default** *cos*	수신된 태그 없는 프레임의 CoS 값을 설정합니다.
exit	글로벌 구성 모드로 돌아갑니다.
exit	EXEC 모드로 돌아갑니다.
write	설정을 저장합니다.

25.3.5 포트의 CoS 우선순위 큐 설정

L2 포트에서 우선순위 큐를 설정하면 해당 포트에서 해당 큐가 사용됩니다. 그렇지 않은 경우, 글로벌 CoS 우선순위 큐를 구성해야 합니다.

아래 명령어를 사용하여 포트의 CoS 우선순위 큐를 설정합니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
interface g0/1	설정할 포트로 진입합니다.
[**no**] **cos map** *quid cos1..cosn*	CoS 우선순위 큐를 설정합니다. quid는 CoS 우선순위 큐의 ID를 의미합니다. quid는 CoS 우선순위 큐의 ID를 의미합니다.
exit	글로벌 구성 모드로 돌아갑니다.
exit	EXEC 모드로 돌아갑니다.
config	설정을 저장합니다.

25.3.6 포트 CoS 우선순위 큐 대역폭 설정

L2 포트에서 우선순위 큐 대역폭을 설정하면, 해당 포트에서 설정된 대역폭이 사용됩니다. 그렇지 않은 경우, 글로벌 우선순위 큐 대역폭을 구성해야 합니다.

아래 명령어를 사용하여 포트의 CoS 우선순위 큐 대역폭을 설정합니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
interface g0/1	설정할 포트로 진입합니다.
[**no**] **scheduler weight bandwidth** *weight1...weightn*	CoS 우선순위 큐의 대역폭을 설정합니다. weight1...weightn은 WRR/DRR 방식의 8개 CoS 큐의 가중치입니다.
exit	글로벌 구성 모드로 돌아갑니다.
exit	EXEC 모드로 돌아갑니다.
write	설정을 저장합니다.

25.3.7 포트 CoS 우선순위 큐 스케줄 정책 설정

L2 포트에서 우선순위 큐 스케줄 정책을 설정하면, 해당 포트에서 설정된 스케줄 정책이 사용됩니다. 그렇지 않은 경우, 글로벌 우선순위 큐 스케줄 정책을 구성해야 합니다.

아래 명령어를 사용하여 포트의 CoS 우선순위 큐 스케줄 정책을 설정합니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
interface g0/1	설정할 포트로 진입합니다.
[**no**] **scheduler policy** { **sp** | **wrr|wfq** }	CoS 우선순위 큐의 스케줄 정책을 설정합니다. p는 SP(Strict Priority) 스케줄 정책을 사용함을 의미합니다. wrr는 WRR(Weighted Round Robin) 스케줄 정책을 사용함을 의미합니다. wfq는 WFQ(Weighted Fair Queuing) 스케줄 정책을 사용함을 의미합니다. drr는 DRR(Deficit Round Robin) 스케줄 정책을 사용함을 의미합니다.
exit	글로벌 구성 모드로 돌아갑니다.
exit	EXEC 모드로 돌아갑니다.
write	설정을 저장합니다.

25.3.8 DSCP 기반 CoS 우선순위 큐 설정

DSCP 값을 기반으로 CoS 큐를 다시 매핑하고, DSCP 값을 수정하며 혼잡 비트를 변경합니다.

아래 명령어를 사용하여 포트의 기본 CoS 값을 설정합니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
[**no**]**dscp map** *word* { **cos** *cos-value* } dscp	DSCP 범위 테이블을 기반으로 CoS 우선순위를 매핑합니다. word는 DSCP 범위 테이블을 나타냅니다. cos-value는 매핑된 우선순위 CoS 값을 설정합니다.
exit	글로벌 구성 모드로 돌아갑니다.
exit	EXEC 모드로 돌아갑니다.
config	설정을 저장합니다.

25.3.9 QoS 정책 매핑 생성

트래픽 분류는 특정 규칙을 적용해 특정 속성을 가진 패킷을 식별하고, 해당 패킷에 대해 지정된 동작을 수행하는 것을 의미합니다. 아래 명령어를 사용하여 QoS 정책을 설정하고 새로운 QoS 정책 매핑을 생성합니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
[no] policy-map *name*	QoS 정책 매핑 구성 모드로 진입합니다. name은 정책의 이름을 나타냅니다
exit	글로벌 구성 모드로 돌아갑니다.
exit	EXEC 모드로 돌아갑니다.
write	설정을 저장합니다.

25.3.10 QoS 정책 매핑 설명 설정

아래 명령어를 사용하여 QoS 정책 매핑의 설명을 설정합니다.

이 설정은 이전 설정을 덮어씁니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
[no] policy-map *name*	QoS 정책 매핑 구성 모드로 진입합니다. name은 정책의 이름을 나타냅니다
description description-text	QoS 정책의 설명을 설정합니다.

	description-text는 정책을 설명하는 텍스트입니다.
exit	글로벌 구성 모드로 돌아갑니다.
exit	EXEC 모드로 돌아갑니다.
write	설정을 저장합니다.

25.3.11 QoS 정책 매핑의 데이터 흐름 설정

QoS 데이터 흐름의 분류 규칙은 관리자가 관리 요구 사항에 따라 구성하는 필터링 규칙을 의미합니다.이 규칙은 간단하게 ToS 필드로 트래픽의 우선순위를 구분하거나, MAC 주소, IP 소스 주소, 목적지 주소, 애플리케이션 포트 ID 등 링크 계층, 네트워크 계층 및 전송 계층 정보를 기반으로 패킷을 분류할 수 있습니다. 일반적으로 분류 기준은 패킷 헤더에 한정되며, 패킷 본문을 기준으로 분류하는 경우는 드뭅니다.

아래 명령어를 사용해 관리 구성 모드로 진입한 후 정책 데이터 흐름을 설정하고, 이전 설정을 대체합니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
no]policy-map name	QoS 정책 매핑 구성 모드로 진입합니다. name은 정책의 이름을 나타냅니다.
description description-text	QoS 정책의 설명을 설정합니다. description-text는 정책을 설명하는 텍스트입니다.
classify {any | cos cos | icos icos | vlan vlanid | ivlan ivlanid | ethernet-type ethernet-type | precedence precedence-value | dscp dscp-value | tos tos-value | diffserv diffserv-value | ip ip-access-list | ipv6 ipv6-access-list | mac mac-access-list } no classify { cos | icos | vlan | ivlan | ethernet-type | precedence | dscp | tos | diffserv | ip | ipv6 | mac }	모든 패킷과 일치합니다. 0~7 사이의 일치된 COS 값을 구성합니다. icos는 0~7 사이의 일치된 내부 COS 값을 나타냅니다. vlanid는 1~4094 사이의 일치된 VLAN을 나타냅니다. ivlanid는 1~4094 사이의 일치된 내부 VLAN을 나타냅니다. ethernet-type은 0x0600~0xFFFF 사이의 일치된 패킷 유형을 나타냅니다. precedence-value는 0~7 사이의 IP 패킷의 tos에 있는 우선순위 필드를 나타냅니다. dscp-value는 0~63 사이의 IP 패킷의 tos에 있는 dscp 필드를 나타냅니다. tos-value는 0~15 사이의 IP 패킷의 tos에 있는 대기 시간, 처리량, 안정성 및 비용 필드를 나타냅니다. diffserv-value는 전체 tos 필드를 나타냅니다. Ip-access-list는 일치하는 IP 액세스 목록의 이름을 나

	타냅니다. 이름은 1~20자입니다. Ipv6-access-list는 일치하는 IPv6 액세스 목록의 이름을 나타냅니다. 이름은 1~20자입니다. 일치하는 MAC 액세스 목록의 이름을 구성합니다. 이름은 1~-20자입니다.
exit	글로벌 구성 모드로 돌아갑니다.
exit	EXEC 모드로 돌아갑니다.
write	설정을 저장합니다.

25.3.12 QoS 정책 매핑에서 데이터 흐름의 동작 설정

데이터 흐름에 대한 동작을 정의하는 것은 필터링 규칙에 따라 데이터 흐름에 특정 동작을 적용하는 것을 의미합니다. 이 동작에는 대역폭 제한, 폐기(drop), 업데이트 등이 포함됩니다. 아래 명령어를 사용하여 관리 모드에서 정책의 동작을 설정하고, 데이터 흐름과 일치하도록 구성합니다.

이 설정은 이전 설정을 덮어씁니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
[no]policy-map name	QoS 정책 매핑 구성 모드로 진입합니다. name은 정책의 이름을 나타냅니다.
description description-text	max-band는 점유된 최대 대역폭을 나타냅니다: 1-163840. 단위: 64Kbps 폴리싱을 구성합니다. Cos: 일치하는 흐름 COS 값을 구성합니다. 유효한 범위는 0~7입니다. drop은 일치하는 패킷을 삭제하는 것을 의미합니다. dscp-value: 일치하는 DSCP 필드를 dscp-value 0~63으로 설정합니다. precedence-value는 IP 패킷의 tos(tos의 5~7)에 있는 우선순위 필드를 나타내며 범위는 0~7입니다. Forward: 일치하는 패킷에 대해 아무런 작업도 수행하지 않습니다. ICOS: 일치하는 COS 필드를 cos-value 0~7로 설정합니다. ivlanID는 1~4094 범위의 내부 vlan ID를 대체하거나 추가하는 데 사용됩니다. session-value는 1~4 범위의 미러링을 설정하는 데 사용됩니다.

	queue-value는 1~8 범위의 매핑 대기열을 설정하는 데 사용됩니다. Interface-id: 일치하는 흐름의 이그레스 포트를 리디렉션합니다. stat-packet은 통계에 있는 패킷 수를 나타냅니다. stat-byte는 통계에 있는 바이트 수를 의미합니다. vlanID는 1~4094 범위의 외부 vlan ID를 대체하거나 추가하는 데 사용됩니다. copy-to-cpu는 CPU에 메시지를 보내는 것을 의미합니다.
classify {**any** | **cos** *cos* | **icos** *icos* | **vlan** *vlanid* | **ivlan** *ivlanid* | **ethernet-type** *ethernet-type* | **precedence** *precedence-value* | **dscp** *dscp-value* | **tos** *tos-value* | **diffserv** *diffserv-value* | **ip** *ip-access-list* | **ipv6** *ipv6-access-list* | **mac** *mac-access-list* } **no classify** { **cos** | **icos** | **vlan** | **ivlan** | **ethernet-type** | **precedence** | **dscp** | **tos** | **diffserv** | **ip** | **ipv6** | **mac** }	글로벌 구성 모드로 돌아갑니다.
exit	EXEC 모드로 돌아갑니다.
exit	설정을 저장합니다.

25.3.13 포트에서 QoS 정책 적용

QoS 정책은 포트에 적용될 수 있으며, 하나의 포트에 여러 QoS 정책을 적용할 수 있습니다. 또한 동일한 QoS 정책을 여러 포트에 적용하는 것도 가능합니다. 동일한 포트에서 먼저 적용된 정책이 이후에 적용된 정책보다 우선순위를 가집니다. 패킷에 두 개의 정책이 설정되고 해당 동작이 충돌하는 경우, 먼저 일치하는 정책의 동작이 적용됩니다.

포트에 QoS 정책이 적용되면, 스위치는 기본적으로 이 포트에 허용되지 않은 다른 데이터 흐름을 차단하는 정책을 추가합니다. 포트에서 모든 정책이 삭제되면, 스위치는 해당 포트에서 기본 차단 정책을 자동으로 제거합니다.

아래 명령어를 사용하여 QoS 정책을 포트에 적용합니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
interface g0/1	설정할 포트로 진입합니다.
[**no**] **qos policy** *name* { **ingress**|**egress**}	QoS 정책 매핑 구성 모드로 진입합니다. name은 정책의 이름을 나타냅니다.

exit	포트에 QoS 정책을 적용합니다. name은 QoS 정책 매핑의 이름을 나타냅니다. ingress는 ingress에 영향을 미치는 것을 의미합니다.
exit	글로벌 구성 모드로 돌아갑니다.

25.3.14 글로벌 QoS 정책 적용

아래 명령어를 사용하여 QoS 정책을 글로벌로 적용합니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
[**no**] **qos policy** *name* **ingress**	QoS 정책을 글로벌로 적용합니다. name은 QoS 정책 매핑의 이름을 나타냅니다. ingress는 수신 방향에 정책을 적용합니다.
exit	글로벌 구성 모드로 돌아갑니다.

25.3.15 신뢰 모드(Trust Mode) 구성

글로벌 구성 모드에서 신뢰 모드를 설정할 때, cos, dscp, untrust 세 가지 옵션이 있습니다. 선택한 옵션에 따라 데이터는 해당 큐에 매핑됩니다. untrust를 선택하는 경우, 패킷의 우선순위는 기본적으로 큐에 매핑됩니다.

아래 명령어를 사용하여 신뢰 모드를 구성합니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
[**no**] **qos trust** { cos | dscp | untrust }	글로벌 구성 모드에서 신뢰 모드 구성. Untrust는 어떤 모드도 신뢰하지 않음을 의미합니다..
exit	EXEC 모드로 돌아갑니다.

25.3.16 QoS 정책 매핑 테이블 표시

show 명령어를 사용하여 모든 QoS 정책 매핑 또는 지정된 일부 QoS 정책 매핑을 표시할 수 있습니다. 아래 명령어를 사용하여 관리 모드에서 QoS 정책 매핑 테이블을 확인합니다.

명령어	설명
show policy-map [*policy-map-name* | *interface* | *global*]	지정된 QoS 정책 맵 전체 또는 일부를 표시합니다. policy-map-name은 QoS 매핑 테이블의 이름을 나타냅니다.

	interface는 포트에 적용된 QoS 정책을 나타냅니다. global은 글로벌 애플리케이션의 QoS 정책을 나타냅니다.
[no] qos trust { cos | dscp | untrust }	글로벌 구성 모드에서 신뢰 모드 구성. Untrust는 어떤 모드도 신뢰하지 않음을 의미합니다..

25.3.17 포트에 QoS 정책 적용 예시

다음 예시는 포트 g0/2에서 IP 액세스 리스트에 일치하는 QoS 정책을 구성하는 방법을 보여줍니다.

ip access-list extended ipacl

permit ip 192.168.20.2 255.255.255.255 192.168.20.210 255.255.255.255

policy-map pmap

classify ip ipacl

action drop

interface g0/2

qos policy pmap ingress

26.OAM 구성

26.1 OAM 개요

EFM OAM(IEEE 802.3ah)은 단일 링크에서 점대점(point-to-point) 링크 장애 및 성능 감지 기능을 제공합니다. 그러나, EFM OAM은 EVC(Ethernet Virtual Circuit)에 적용할 수 없으므로 종단 간(terminal-to-terminal) 이더넷 모니터링은 불가능합니다.

또한, OAM PDU(Protocol Data Unit)는 다른 인터페이스로 전달되지 않으며, IEEE 802.3ah에서 규정된 이더넷 OAM은 속도가 느린 프로토콜입니다.

- 최대 전송 속도: 초당 10프레임
- 최소 전송 속도: 초당 1프레임

26.1.1 OAM 프로토콜 속성

- 이더넷 OAM 장치 및 속성 지원

  이더넷 OAM 연결 과정은 Discovery(탐색) 단계로 불립니다.

  이 단계에서 OAM 엔터티는 원격 장치의 OAM 엔터티를 발견하고, 안정적인 세션이 설정됩니다. 탐색 단계 동안, 연결된 이더넷 OAM 엔터티는 OAM 모드, OAM 설정 정보 및 로컬 노드에서 지원하는 이더넷 OAM 기능을 OAM PDU를 통해 상호 교환합니다.만약 루프백(loopback) 설정, 단방향 링크 감지(unidirectional link detection) 및 링크 이벤트 설정이 두 단말의 OAM에서 통과되면, 이더넷 OAM 프로토콜은 링크 계층에서 작동을 시작합니다.

- 링크 모니터링

  이더넷 OAM은 Event Notification OAM PDU를 통해 링크를 모니터링합니다.

  링크에 문제가 발생하고 로컬 링크에서 이를 감지하면, Event Notification OAM PDU를 원격 이더넷 OAM에 전송하여 정상적인 링크 이벤트를 보고합니다.

  관리자는 링크 모니터링을 통해 네트워크 상태를 실시간으로 파악할 수 있습니다.

정상적인 링크 이벤트	정의
오류 신호의 주기적 이벤트	신호 수 N을 주기로 지정합니다. N개의 신호를 수신했을 때 오류 신호가 정의된 임계값을 초과합니다.
오류 프레임 이벤트	단위 시간 동안 오류 프레임 수가 정의된 임계값을 초과합니다.
오류 프레임의 주기적 이벤트	프레임 수 N을 주기로 지정합니다. N개의 프레임을 수신했을 때 오류 프레임이 임계값을 초과합니다.

오류 프레임의 2차 프레임	지정된 M초 동안 오류 프레임의 초과 횟수가 정의된 임계값을 초과합니다.

- 원격 장애 표시 (Remote Trouble Indication)

이더넷에서는 물리적 네트워크 통신이 지속되면서 네트워크 성능이 저하되는 경우와 같이 장애를 확인하는 것이 어렵습니다.
OAM PDU는 플래그 영역(flag domain)을 정의하여 이더넷 OAM 엔터티가 상대 엔터티(peer)로 장애 정보를 전송할 수 있도록 합니다.

이 플래그는 다음과 같은 긴급 링크 이벤트를 나타낼 수 있습니다.

- 링크 장애(Link Fault):
  물리 계층에서 로컬 DTE(데이터 종단 장치)의 수신 방향이 무효함을 감지합니다.
  장애가 발생하면 일부 물리 계층 장치는 단방향 작동을 지원하며, 원격 OAM에서 장애 알림을 허용합니다.
- Dying Gasp:
  복구할 수 없는 로컬 오류(예: OAM 종료)가 발생하면, 인터페이스가 error-disabled 상태로 전환되고 이후 종료됩니다.
- 치명적 이벤트(Critical Event):
  불확실한 치명적 이벤트가 발생합니다. (치명적 이벤트는 제조업체에 의해 정의됩니다.)

이더넷 OAM 연결 동안 Information OAM PDU는 지속적으로 전송됩니다.
로컬 OAM 엔터티는 Information OAM PDU를 통해 로컬에서 발생하는 중요한 링크 이벤트를 원격 OAM 엔터티에 보고할 수 있습니다.
이를 통해 관리자는 링크 상태를 동적으로 파악하고, 장애 발생 시 신속하게 문제를 처리할 수 있습니다.

- 원격 루프백 (Remote Loopback)

OAM은 선택적으로 링크 계층 수준의 루프백(loopback) 모드를 제공합니다.
비-OAM-PDU 루프백을 통해 오류 위치를 확인하고 링크 성능 테스트를 수행할 수 있습니다.

원격 루프백은 OAM 연결이 생성된 이후에만 실현됩니다.
OAM 연결이 설정된 후, 활성 모드의 OAM 엔터티가 원격 루프백 명령을 트리거하고 상대 엔터티가 해당 명령에 응답합니다.

원격 단말이 루프백 모드에 들어가면, OAM PDU 패킷과 Pause 패킷을 제외한 모든 패킷은 이전 경로를 따라 다시 전송됩니다.

이를 통해 오류 위치 확인 및 링크 성능 테스트를 수행할 수 있습니다.

원격 DTE가 원격 루프백 모드에 있을 때, 로컬 또는 원격 통계 데이터를 무작위로 조회하고 비교할 수 있습니다.
조회 작업은 루프백 프레임이 원격 DTE로 전송되기 전, 중, 후에 모두 수행될 수 있습니다.

정기적인 루프백 검사는 네트워크 오류를 신속하게 감지합니다.
구간별 루프백 검사는 네트워크 오류를 특정 구간에서 파악하고 제거하는 데 도움이 됩니다.

- MIB 변수 쿼리

802.3 표준에서 설명하는 모든 MIB 변수에 대한 순환 쿼리(round query)를 수행할 수 있습니다.

26.1.2 OAM 모드

장치는 두 가지 모드(액티브 모드와 패시브 모드)를 통해 OAM 연결을 수행할 수 있습니다.
각 모드에서의 장치 기능은 표 2에서 비교됩니다.

액티브 모드의 OAM 엔터티만 연결 프로세스를 트리거할 수 있으며, 패시브 모드의 OAM 엔터티는 상대 OAM 엔터티로부터의 연결 요청을 기다려야 합니다.원격 OAM 탐색 프로세스가 완료된 후, 원격 엔터티가 액티브 모드일 경우 로컬 엔터티는 액티브 모드에서 모든 OAM PDU 패킷을 전송할 수 있습니다. 그러나 원격 엔터티가 패시브 모드인 경우, 액티브 모드의 로컬 엔터티는 일부 동작이 제한됩니다. 이는 액티브 모드 장치가 패시브 원격 엔터티에서 전송된 원격 루프백 명령 및 변수 요청에 반응하지 않기 때문입니다.

기능	액티브 모드	패시브 모드
이더넷 OAM 탐색 프로세스 초기화	YES	NO
OAM 탐색 초기화 프로세스에 응답	YES	YES
정보 OAM PDU 패킷 전송	YES	YES
이벤트 알림 OAM PDU 패킷 전송 허용	YES	YES
변수 요청 OAM PDU 패킷 전송 허용	YES	NO
변수 응답 OAM PDU 패킷 전송 허용	YES	YES
프백 제어 OAM PDU 패킷 전송 허용	YES	NO
루프백 제어 OAM PDU 응답	YES	YES
특정 OAM PDU 전송 허용	YES	YES

이 표는 액티브 모드와 패시브 모드 간의 주요 차이점을 보여줍니다.
액티브 모드는 모든 OAM PDU 패킷을 전송할 수 있는 반면, 패시브 모드는 특정 패킷 전송에 제한이 있습니다.

이더넷 OAM 연결이 설정된 후, 두 단말의 OAM 엔터티는 정보 OAM PDU 패킷을 주고받으며 연결을 유지합니다. 상대 OAM 엔터티로부터 5초 이내에 정보 OAM PDU 패킷을 수신하지 못하면, 연결이 타임아웃되어 새로운 OAM 연결을 다시 설정해야 합니다.

26.1.3 OAM 패킷의 구성 요소

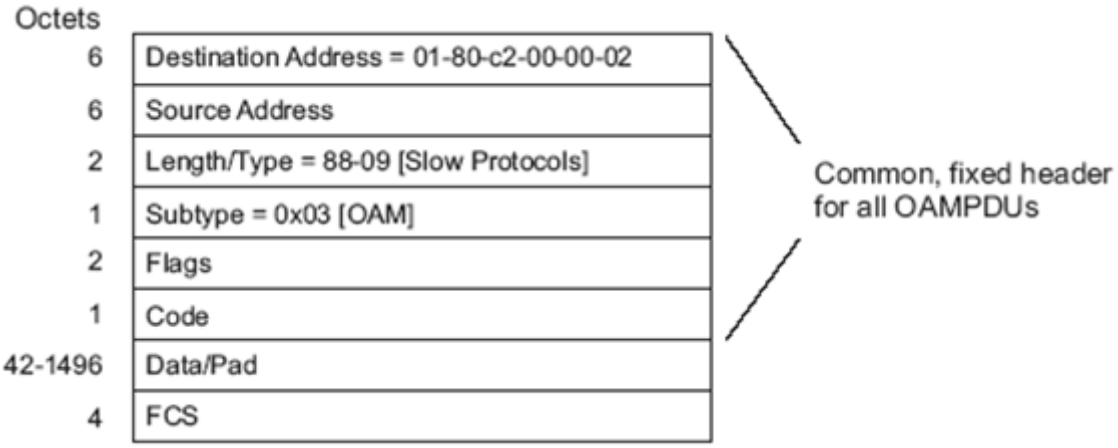


그림 47 OAM 패킷의 구성 요소

- 목적지 주소 (Destination Address) : 이더넷 OAM 패킷의 목적지 MAC 주소입니다.
- 출발지 주소 (Source Address) : 이더넷 OAM 패킷의 출발지 MAC 주소입니다. 패킷을 전송하는 단말 포트의 MAC 주소이며, 유니캐스트 MAC 주소입니다.
- 길이/타입 (Length/Type) : 항상 Type 인코딩 방식을 사용합니다. 이더넷 OAM 패킷의 프로토콜 타입은 0x8809입니다.
- 서브타입 (Subtype) : 이더넷 OAM 패킷의 프로토콜 서브타입은 0x03입니다.
- 플래그 (Flags) : 이더넷 OAM 엔터티의 상태를 나타내는 영역입니다.
- 코드 (Code) : OAM PDU(OAM Protocol Data Unit) 패킷의 유형을 나타내는 영역입니다.
- 데이터/패드 (Data/Pad) : OAM PDU 데이터와 패딩 값을 포함하는 영역입니다.
- FCS (Frame Check Sequence) : 프레임의 체크섬으로, 데이터 전송의 무결성을 검증하는 역할을 합니다.

코드	OAMPDU
00	정보 (Information)
01	이벤트 알림 (Event Notification)
02	변수 요청 (Variable Request)

03	변수 응답 (Variable Response)
04	루프백 제어 (Loopback Control)
05-FD	예약됨 (Reserved)
FE	사용자 정의 (Organization Specific)
FF	예약됨 (Reserved)

26.2 OAM 구성 작업

26.2.1 인터페이스에서 OAM 활성화

다음 명령어를 실행하여 OAM을 활성화합니다.

명령어	설명
config	글로벌 설정 모드로 진입합니다.
interface intf-type intf-id	인터페이스 설정 모드로 진입합니다.
ethernet oam	인터페이스에서 이더넷 OAM을 활성화합니다.
ethernet oam [**max-rate** oampdus | **min-rate** seconds | **mode** {**active** | **passive**} | **timeout** seconds]	● max-rate 매개변수 초당 전송되는 OAM PDU의 최대 수를 설정합니다. 범위: 1~10 기본값: 10 ● min-rate 매개변수 OAM PDU의 최소 전송 속도를 설정합니다. 단위: 초 범위: 1~10 기본값: 1초 ● mode {active | passive} 매개변수 OAM 모드를 설정합니다. 두 인터페이스 간 OAM 연결은 최소 하나의 인터페이스가 액티브 모드일 때만 설정됩니다. ● timeout 매개변수 OAM 연결의 타임아웃 시간을 설정합니다. 범위: 1~30초 기본값: 1초

no ethernet oam 명령어를 실행하면 OAM 기능이 비활성화됩니다. aggregation interface에 속하는

물리적 인터페이스에서는 원격 OAM 루프백을 활성화할 수 없습니다.

26.2.2 OAM 링크 모니터링 구성

OAM 링크 모니터링에서는 상한(High Threshold) 및 하한(Low Threshold)을 설정할 수 있습니다. 아래 절차는 인터페이스에서 OAM 링크 모니터링을 구성하는 단계입니다.

명령어	설명
config	글로벌 설정 모드로 진입합니다.
interface intf-type intf-id	인터페이스 설정 모드로 진입합니다.
ethernet oam link-monitor negotiation-supported	인터페이스에서 이더넷 OAM을 활성화합니다.
ethernet oam link-monitor symbol-period {threshold {high { symbols **|none} | low** {symbols}**} | window** symbols**}**	오류 신호의 주기적 이벤트의 높음 및 낮음 임계값을 설정하여 오류 링크 이벤트를 트리거합니다. 임계값 높음 매개변수는 높은 임계값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 1에서 65535까지이며 기본값은 없음입니다. 임계값 낮음 매개변수는 낮은 임계값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 0에서 65535까지이며 기본값은 1입니다. 창 매개변수는 라운드 쿼리 기간의 창 크기를 구성하는 데 사용됩니다. 창 크기의 단위는 100M 신호의 번호입니다. 창 크기는 1000M 이더넷 인터페이스에서 10에서 600까지이며 기본값은 10입니다. 100M 이더넷 인터페이스에서는 창 크기가 1에서 60까지이며 기본값은 1입니다.
ethernet oam link-monitor frame {threshold {high { symbols **|none} | low** {symbols}**} | window** symbols**}**	오류 프레임 이벤트의 높음 및 낮음 임계값을 설정하여 오류 프레임의 링크 이벤트를 트리거합니다. 임계값 높음 매개변수는 높은 임계값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 1에서 65535까지이며 기본값은 없음입니다. 임계값 낮음 매개변수는 낮은 임계값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 0에서 65535까지이며 기본값은 1입니다. 창 매개변수는 라운드 쿼리 기간의 창 크기를 구성하는 데 사용됩니다. 단위는 초입니다. 범위는 1에서 60까지이며 기본값은 1입니다.
ethernet oam link-monitor frame-period	낮은 임계값을 구성하는 데 사용됩니다. 단위는 신호

{threshold {high { symbols **|none}	low** {symbols}**}	window** symbols**}**	번호입니다. 범위는 0에서 65535까지이며 기본값은 1입니다. 창 매개변수는 라운드 쿼리 기간의 창 크기를 구성하는 데 사용됩니다. 창 크기의 단위는 14881 프레임의 개수입니다. 창 크기는 1000M 이더넷 인터페이스에서 100에서 6000까지이며, 이 경우 기본값은 100입니다. 100M 이더넷 인터페이스에서는 창 크기가 10에서 600까지이며, 이 경우 기본값은 10입니다.
ethernet oam link-monitor frame-seconds {threshold {high { symbols **|none}	low** {symbols}**}	window** symbols**}**	오류 프레임의 두 번째 이벤트에 대한 높음 및 낮음 임계값을 설정하여 오류 프레임의 두 번째 링크 이벤트를 트리거합니다. 임계값 높음 매개변수는 높은 임계값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 1에서 900까지이며 기본값은 없음입니다. 임계값 낮음 매개변수는 낮은 임계값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 0에서 900까지이며 기본값은 1입니다. 창 매개변수는 라운드 쿼리 기간의 창 크기를 구성하는 데 사용됩니다. 단위는 초입니다. 범위는 10에서 900까지이며 기본값은 60입니다.
ethernet oam link-monitor receive-crc {threshold {high { symbols **|none}	low** {symbols}**}	window** symbols**}**	오류 CRC 프레임 이벤트의 높음 및 낮음 임계값을 설정하여 CRC 체크섬 오류의 링크 이벤트를 트리거합니다. 임계값 높음 매개변수는 높은 임계값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 1에서 65535까지이며 기본값은 없음입니다. 임계값 낮음 매개변수는 낮은 임계값을 구성하는 데 사용됩니다. 단위는 신호 번호입니다. 범위는 0에서 65535까지이며 기본값은 1입니다. 창 매개변수는 라운드 쿼리 기간의 창 크기를 구성하는 데 사용됩니다. 단위는 초입니다. 범위는 1에서 180까지이며 기본값은 10입니다.

26.2.3 원격 OAM 엔터티로부터의 장애 알림 구성

인터페이스에서 error-disable 동작을 구성할 수 있습니다.
로컬 인터페이스는 다음과 같은 경우에 **errdisabled** 상태로 진입합니다.

- 로컬 인터페이스에서 정상 링크 이벤트의 상한 임계값이 초과된 경우

- 로컬 인터페이스에 연결된 원격 인터페이스가 errdisabled 상태로 진입한 경우
- 로컬 인터페이스에 연결된 원격 인터페이스에서 관리자가 OAM 기능을 비활성화한 경우

아래 표는 인터페이스에서 원격 OAM 장애 알림을 구성하는 절차를 보여줍니다.

명령어	설명
config	글로벌 설정 모드로 진입합니다.
interface intf-type intf-id	인터페이스 설정 모드로 진입합니다.
ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action error-disable-interface	인터페이스에서 원격 OAM 장애의 트리거 동작을 구성합니다. critical-event 매개변수는 지정되지 않은 치명적 이벤트가 발생했을 때 인터페이스가 errdisabled 상태로 진입하도록 활성화하는 데 사용됩니다. dying-gasp 매개변수는 다음과 같은 경우 로컬 인터페이스가 errdisabled 상태로 진입하도록 활성화하는 데 사용됩니다. 로컬 인터페이스에서 정상 링크 이벤트의 상한 임계값이 초과된 경우 로컬 인터페이스에 연결된 원격 인터페이스가 errdisabled 상태로 진입한 경우 로컬 인터페이스에 연결된 원격 인터페이스에서 관리자가 OAM 기능을 비활성화한 경우 link-fault 매개변수는 수신기가 신호 손실을 감지했을 때 인터페이스가 errdisabled 상태로 진입하도록 활성화하는 데 사용됩니다.

스위치는 LINK FAULT 패킷 및 Critical Event 패킷을 생성할 수 없습니다. 그러나, 이러한 패킷이 원격 단말에서 수신되면 정상적으로 처리됩니다. 라우터는 Dying Gasp 패킷을 송수신할 수 있습니다. 로컬 포트가 errdisabled 상태로 진입하거나, 관리자가 포트를 종료하거나, 로컬 포트의 OAM 기능이 관리자에 의해 비활성화되면, Dying Gasp 패킷이 로컬 포트에 연결된 원격 단말로 전송됩니다.

26.2.4 OAM 프로토콜 정보 표시

명령어	설명
show ethernet oam discovery interface [intf-type intf-id**]**	모든 인터페이스 또는 지정된 인터페이스에서 OAM 탐색 정보를 표시합니다.

show ethernet oam statistics {pdu | link-monitor | remote-failure} interface [intf-type intf-id**]**	모든 인터페이스 또는 지정된 인터페이스에서 OAM 통계 정보를 표시합니다.
show ethernet oam configuration interface [intf-type intf-id**]**	모든 인터페이스 또는 지정된 인터페이스에서 OAM 설정 정보를 표시합니다.
show ethernet oam runtime interface [intf-type intf-id**]**	모든 인터페이스 또는 지정된 인터페이스에서 OAM 실행 상태 정보를 표시합니다.

참고 :

- pdu 매개변수는 OAM 패킷의 코드 도메인 값에 따라 OAM 패킷을 분류하고 집계합니다.
- link-monitor 매개변수는 정상 링크 이벤트의 상세 통계 정보를 표시합니다.
- remote-failure 매개변수는 원격 장애에 대한 상세 통계 정보를 표시합니다.

26.2.5 설정 예제

네트워크 환경 요구사항

사용자 액세스 측에서 오류 프레임을 수신하는 스위치에 대한 정보를 캡처하려면, 두 스위치가 연결된 인터페이스에서 OAM 프로토콜을 구성해야 합니다.

네트워크 토폴로지

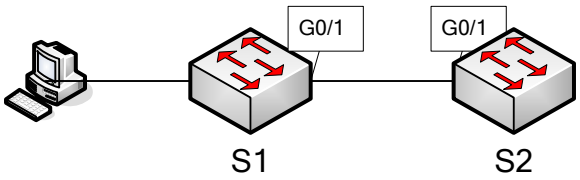


그림 48 네트워크 토폴로지

설정

Configuring switch S1:

Switch_config_g0/1#ethernet oam

Switch_config_g0/1#ethernet oam mode passive

Switch_config_g0/1#ethernet oam link-monitor frame threshold low 10

Switch_config_g0/1#ethernet oam link-monitor frame window 30

Switch_config_g0/1#show ethernet oam configuration int g0/1

GigaEthernet0/1

General

Admin state : enabled

Mode : passive

PDU max rate : 10 packets/second

PDU min rate : 1 seconds/packet

Link timeout : 1 seconds

High threshold action: no action

Remote Failure

Link fault action : no action

Dying gasp action : no action

Critical event action: no action

Remote Loopback

Is supported : not supported

Loopback timeout : 2

Link Monitoring

Negotiation : supported

Status : on

Errored Symbol Period Event

Window : 10 * 100M symbols

Low threshold : 1 error symbol(s)

High threshold : none

Errored Frame Event

Window : 30 seconds

Low threshold : 10 error frame(s)

High threshold : none

Errored Frame Period Event

Window : 100 * 14881 frames

Low threshold : 1 error frame(s)

High threshold : none

Errored Frame Seconds Summary Event

Window : 60 seconds

Low threshold : 1 error second(s)

High threshold : none

Errored CRC Frames Event

Window : 1 seconds

Low threshold : 10 error frame(s)

High threshold : none

Configuring switch S2: Switch_config_g0/1#ethernet oam

Switch_config_g0/1#show ethernet oam statistics link-monitor int g0/1

GigaEthernet0/1

Local Link Events:

Errored Symbol Period Event:

No errored symbol period event happened yet.

Errored Frame Event:

No errored frame event happened yet.

Errored Frame Period Event:

No errored frame period event happened yet.

Errored Frame Seconds Summary Event:

No errored frame seconds summary event happened yet.

Errored CRC Frames Event:

No errored CRC frame event happened yet.

Remote Link Events:

Errored Symbol Period Event:

No errored symbol period event happened yet.

Errored Frame Event:

No errored frame event happened yet.

Errored Frame Period Event:

No errored frame period event happened yet.

Errored Frame Seconds Summary Event:

No errored frame seconds summary event happened yet.

Errored CRC Frames Event:

No errored CRC frame event happened yet.

27 CFM 구성

27.1 CFM 구서 작업 목록

- 유지 관리 도메인 추가
- 유지 관리 연결(MA) 추가
- MIP(유지 관리 도메인 중간 지점) 추가
- MEP(유지 관리 연결 종료 지점) 추가
- CFM 시작

27. 2 CFM 유지 관리 작업 목록

- 루프백 기능 사용
- 링크 추적(Linktrace) 기능 사용

27.2.1 유지 관리 도메인 추가

명령어	설명
ethernet cfm md mdnf *{string}* *<char_string>* [**level** *<0-7>* / **creation** *<MHF_creation_type>* / **sit** *<sender_id_type>* / **ip** *<IP_address>*]	유지 관리 도메인이 추가된 후 시스템은 유지 관리 도메인 구성 모드로 진입합니다.

27.2.2 유지 관리 연결(MA) 추가

명령어	설명
ma manf *{string}* *<char_string>* **ci** *{100ms / 1s / 10s / 1min / 10min}* **meps** *<mepids>* [**vlan** *<1-4094>* / **creation** *<MHF_creation_type>* / **sit** *<sender_id_type>* / **ip** *<IP_address>*]	이름이 char_string인 유지 관리 연결(MA)을 추가합니다.

27.2.3 MIP(유지 관리 도메인 중간 지점) 추가

명령어	설명
ethernet cfm mip add level *<0-7>* [**vlan** *<1-4094>*]	지정된 물리 인터페이스에 VLAN 및 계층 MIP를 추가합니다.

27.2.4 MEP(유지 관리 연결 종료 지점) 추가

명령어	설명
ethernet cfm mep add mdnf *{string} <char_string>* **manf** *{string} <char_string>* **mepid** *<1-8191>* **rmepid** *<1-8191>* [**direction** *{up / down}* **| ip** *<ip_address>* **| lap** *{all / mac / rCCM / eCCM / xcon / none}*]	지정된 유지 관리 도메인 및 MEP를 물리 인터페이스에 추가합니다.

27.2.5 CFM 시작

명령어	설명
ethernet cfm {*enable*}	CFM을 시작합니다.

27.2.6 루프백 기능 사용

명령어	설명
ethernet cfm loopback mdnf *{string} <char_string>* **manf** *{string} <char_string>* **mepid** *<1-8191>* **mac** *<AA:BB:CC:DD:EE:FF>* **number** *<1-64>*	지정된 MEP를 사용하여 자체 루프백을 수행합니다.

27.2.7 링크 추적(Linktrace) 기능 사용

명령어	설명
ethernet cfm linktrace mdnf *{string} <char_string>* **manf** *{string} <char_string>* **mepid** *<1-8191>* **mac** *<AA:BB:CC:DD:EE:FF>* [**ttl** *{1-255}* / **fdb-only** *{yes}*]	Uses a designated MEP to conduct loopback towards itself.

27.2.8 설정 예제

사용자는 이름이 customer이고 계층이 5인 유지 관리 도메인을 추가하고, vlan1에 대해 customer1 유지 관리 연결을 설정하고자 합니다. 유지 관리 연결의 CCM 전송 간격은 1초이며, MEP1, MEP2, MEP2009가 포함됩니다. 마지막으로, 물리적 포트 1에 MEP ID가 2009이고 원격 MEP가 2008인 MEP를 추가합니다.

Switch_config#ethernet cfm md mdnf string customer level 5

Switch_config_cfm#ma manf string customer1 vlan 1 ci 1s meps 1-2,2009

Switch_config_cfm#interface g0/1

Switch_config_g0/1#ethernet cfm mep add mdnf string customer manf string customer1 mepid 2009 rmep 2008 direction down lap all

Switch_config_g0/1#exit

Switch_config#ethernet cfm enable

28. MACFF 구성

28.1 MACFF 구성 작업

MACFF는 스위치에서 동일 VLAN의 다운링크 포트 간 패킷 교환을 차단하여, 이러한 패킷이 DHCP 서버를 통해 클라이언트의 기본 게이트웨이로 할당되고 다시 다운링크 포트로 전송되도록 합니다. MACFF는 다운링크 포트 간 ARP 패킷을 캡처하여 ARP 학습을 방지하고, 게이트웨이의 MAC 주소로 응답함으로써 모든 다운링크 포트 간의 패킷이 게이트웨이를 통해 전달되도록 합니다.

참고 : MACFF는 DHCPR 스누핑을 지원해야 합니다. 따라서 MACFF를 활성화하기 전에 DHCPR 스누핑이 정상적으로 작동하는지 확인해야 합니다. 게이트웨이에서 ICMP 리디렉션은 기본적으로 비활성화되어 있습니다. MACFF가 활성화된 스위치에는 VLAN 관리 주소가 구성되어야 합니다.

구성 작업 목록

- MACFF 활성화 또는 비활성화
- VLAN에서 MACFF 활성화
- VLAN에서 MACFF의 기본 AR(주소 확인) 구성
- VLAN에서 MACFF의 기타 AR 구성
- 특정 물리적 포트에서 MACFF 비활성화

28.1.1 MAC 활성화 / 비활성화

명령어	설명
macff enable	MACFF를 활성화합니다.
no macff enable	기본 설정으로 되돌립니다.

이 명령어는 글로벌 구성 모드에서 MACFF를 활성화하는 데 사용되며 명령어를 실행하면 스위치가 모든 ARP 패킷을 감지합니다.

참고 : 이 명령어를 구성하기 전에 DHCP-Snooping이 활성화되어 있어야 하며 명령어를 실행하기 전에 클라이언트가 스위치에서 주소를 할당받은 경우, 스위치는 해당 바인딩 관계를 추가할 수 없습니다.

1.1.1 VLAN에서 MACFF 활성화

VLAN에서 MACFF가 활성화되면, 모든 VLAN의 DHCP-Snooping distrust 물리 포트에서 수신된

ARP 패킷이 모니터링됩니다. ARP 패킷의 대상 IP 주소가 해당 ARP 패킷을 수신한 물리 포트에 위치한 DHCP 클라이언트의 IP 주소인 경우, 해당 ARP 패킷은 폐기됩니다. 또한 ARP 응답 패킷인 경우에도 폐기됩니다.

다른 DHCP 클라이언트, 기본 게이트웨이 또는 다른 서비스 주소에서 요청이 발생하면, 해당 요청에 대한 응답으로 해당 MAC 주소가 ARP 요청에 응답하게 됩니다.

참고 : MACFF가 활성화된 VLAN에는 관리 주소가 구성되어야 하며, 해당 VLAN에서 DHCP-Snooping도 활성화되어 있어야 합니다.

명령어	설명
macff vlan *vlan_id* **enable**	VLAN에서 MACFF를 활성화합니다.
no macff vlan *vlan_id* **enable**	VLAN에서 MACFF를 비활성화합니다.

28.1.2 VLAN에서 MACFF 기본 AR 구성

클라이언트에서 수동으로 주소를 설정하거나(DHCP 서버가 기본 경로 옵션3을 구성하지 않은 경우), 스위치는 자동으로 기본 AR을 MACFF의 기본 게이트웨이로 설정합니다.

기본 AR은 하나만 설정할 수 있습니다.

명령어	설명
macff vlan *vlan_id* **default-ar** *A.B.C.D*	VLAN에서 MACFF의 기본 AR을 설정합니다.
no macff vlan *vlan_id* **default-ar** *A.B.C.D*	VLAN에서 MACFF의 기본 AR을 삭제합니다.

참고 : 이 명령어를 구성하기 전에, ip source binding xx-xx-xx-xx-xx-xx A.B.C.D interface name 명령어를 실행하여 스위치에 클라이언트 바인딩 테이블을 추가할 수 있습니다. 이 작업을 수행하지 않으면, MACFF는 수동으로 구성된 클라이언트를 불법 클라이언트로 간주하며 해당 클라이언트에 서비스를 제공하지 않습니다.

28.1.3 VLAN에서 MACFF 기타 AR 구성

MACFF에서 기타 AR이 구성되면, DHCP 클라이언트는 DHCP 서버에서 할당된 기본 게이트웨이를 거치지 않고 직접 해당 AR에 액세스할 수 있습니다.
이 기능은 클라이언트 네트워크 세그먼트에 있는 일부 서버나 기타 서비스 주소에 적용할 수 있습니다.

명령어	설명
macff vlan *vlan_id* **other_ar** *A.B.C.D*	VLAN에서 MACFF의 기타 AR을 구성합니다.
no macff vlan *vlan_id* **other_ar** *A.B.C.D*	VLAN에서 MACFF의 기타 AR을 삭제합니다.

28.1.4 특정 물리 포트에서 MACFF 비활성화

특정 물리 포트에서 MACFF를 비활성화하면, 해당 포트의 패킷은 격리되지 않으며 ARP 패킷도 모니터링되지 않습니다. 인터페이스 모드에서 아래의 명령어를 실행하십시오.

명령어	설명
macff disable	물리 포트에서 MACFF를 비활성화합니다.
no macff disable	물리 포트에서 MACFF를 활성화합니다. (기본값)

28.1.5 MACFF 디버깅 활성화

명령어	설명
debug macff	MACFF 디버깅을 활성화합니다.
no debug macff	MACFF 디버깅을 비활성화합니다.

29. Layer-2 Tunnel 프로토콜 구성

29.1개요

레이어 2 프로토콜 터널은 스위치의 두 단말에 연결된 사용자가 스위치를 통해 자신만의 네트워크에서 지정된 레이어 2 프로토콜 패킷을 투명하게 전송할 수 있도록 합니다.

이 과정에서 스위치의 레이어 2 프로토콜 모듈에 영향을 받지 않으며, 스위치는 단순한 투명 전송 매체 역할을 수행합니다.

29.2Layer-2 Tunnel 프로토콜 구성

명령어	설명
interface *<intf_name>*	글로벌 구성 모드로 진입합니다.
[**no**] **l2protocol-tunnel** *[stp]*	스위치 포트의 인터페이스 구성 모드로 진입합니다.
no spanning-tree	해당 스위치 포트에서 터널 기능을 활성화할 L2 프로토콜(STP)을 설정합니다.
exit	포트에서 STP를 비활성화합니다.
write	글로벌 모드로 돌아갑니다.
interface *<intf_name>*	설정을 저장합니다.

참고 : 이 명령어는 터널 기능이 활성화된 포트에서 STP를 비활성화하여, STP 패킷 전송으로 터널에 접속된 장치에 영향을 주지 않도록 합니다.

29.3 구성 예제

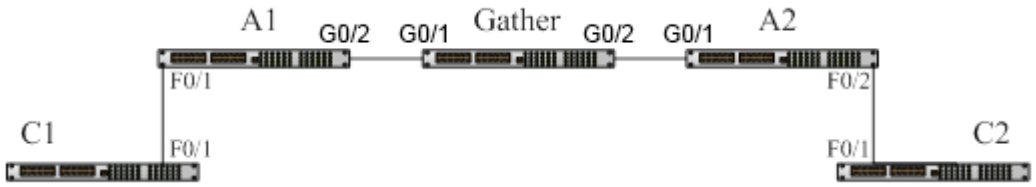


그림 49 네트워크 토폴로지

A1/A2/Gather는 코어 네트워크에 속합니다. C1/C2는 클라이언트의 두 지점에 위치한 스위치를 나타냅니다.

클라이언트는 두 네트워크를 독립적인 네트워크로 관리하기를 원합니다. 즉, 코어 네트워크는 클라이언트에게 투명한 전송 채널처럼 동작해야 합니다.

STP 투명 전송을 실현하기 위해, 클라이언트는 각 스위치에서 다음과 같은 설정을 수행해야 합니다.

- 스위치 A1의 g0/2 포트, 스위치 Gather의 g0/1 포트, 스위치 A2의 g0/1 포트를 각각 트렁크 모드로 설정합니다.

스위치 A1의 f0/1 포트와 스위치 A2의 f0/2 포트를 액세스 모드로 설정하고, STP를 비활성화한 후 두 포트에서 STP 프로토콜의 터널 기능을 활성화합니다.

30. Attack Prevention

30.1 필터 개요

네트워크 대역폭의 합리적인 사용을 보장하기 위해, 이 스위치 시리즈는 악의적인 트래픽이 네트워크 대역폭을 과도하게 점유하는 것을 방지하는 기능을 제공합니다.
필터는 스위치 인터페이스가 수신한 패킷을 식별하고 패킷 유형에 따라 계산합니다.
현재의 공격 방식에 따라, 필터는 호스트가 일정 시간 동안 전송하는 ARP, IGMP 또는 IP 메시지의 수를 계산합니다. 이 수가 임계값을 초과하면 스위치는 해당 호스트에 서비스를 제공하지 않습니다.

필터는 출발지 주소를 차단하여 특정 호스트의 패킷을 제한합니다.

- ARP 공격의 경우, 필터는 출발지 MAC 주소를 차단합니다.
- Ping 스캔 및 TCP/UDP 스캔과 같은 IP 공격의 경우, 필터는 출발지 IP 주소를 차단합니다.

30.2 필터 모드

필터 모드는 스위치가 공격 출처를 지정하는 방식을 결정합니다. 필터에는 두 가지 모드가 있습니다.

- 출발지 주소 차단 시간 (Raw)
  Raw 모드에서는 공격 출처가 확인된 후 일정한 차단 시간 동안 공격 출처에서 오는 패킷이 폐기됩니다.
  차단 시간이 종료되면 공격 출처에 대한 제한이 해제되고 새로운 계산이 시작됩니다.
  이 모드에서는 출발지 주소에서 오는 모든 패킷이 차단됩니다.
  예를 들어, 공격 출처의 MAC 주소가 차단되면 ARP, ICMP, DHCP 및 기타 모든 유형의 패킷이 폐기됩니다.
- 출발지 주소 차단 폴링 (Hybrid)
  공격 출처가 차단된 후에도 스위치는 해당 출처에서 오는 패킷을 계속 계산하여 폴링 간격이 끝나기 전에 패킷 수가 임계값을 초과하는지 감지합니다.
  패킷 수가 임계값을 초과하면 차단 상태가 유지됩니다.
  그렇지 않으면 차단이 해제됩니다.

하이브리드 모드에서는 공격 출처를 처음 감지했을 때의 패킷 수와 폴링 중 임계값을 독립적으로 구성할 수 있습니다.
지속적인 패킷 계산을 위해, 하이브리드 모드에서는 출발지 주소가 차단된 상태에서도 패킷 유형이 일치하는지 확인합니다.
예를 들어, 호스트의 MAC 주소가 ARP 공격으로 인해 차단되면, 해당 호스트에서 발생하는 IP 패

킷은 계속 전송됩니다.
단, 호스트가 IP 공격의 출처로도 확인된 경우에는 차단됩니다.

필터 모드 선택 지침

- 공격 출처에 대한 엄격한 제한을 설정하고 스위치 CPU의 부담을 줄이고자 한다면 Raw 모드를 사용하십시오.
- 공격이 종료된 후 호스트와의 통신을 빠르게 재개하고 유연하게 공격 출처를 제어하고자 한다면 Hybrid 모드를 사용하십시오.

스위치가 하이브리드 모드에서 지원할 수 있는 필터 수는 제한적입니다.
필터 수가 부족한 경우, Raw 모드가 자동으로 적용됩니다.

30.3 공격 방지 구성 작업

지정된 시간 동안 호스트가 전송하는 IGMP, ARP 또는 IP 메시지 수가 임계값을 초과하면, 해당 호스트가 네트워크를 공격하는 것으로 간주합니다.

다음과 같은 구성 작업을 수행할 수 있습니다.

- 공격 필터 매개변수 구성
- 공격 방지 유형 구성
- 공격 방지 기능 활성화
- 공격 방지 상태 확인

30.4 공격 방지 구성

30.4.1 공격 필터 매개변수 구성

글로벌 구성 모드에서 아래 명령어를 실행하여 필터의 매개변수를 구성합니다.

명령어	설명
Switch# **config**	글로벌 구성 모드로 들어갑니다.
Switch_config# **filter period** *time*	공격 필터 기간을 시간으로 설정합니다. 단위는 초입니다.
Switch_config# **filter threshold** **[arp | bpdu | dhcp | igmp | ip | icmp | icmpv6]** *value*	공격 필터 임계값을 값으로 설정합니다.
Switch_config# **filter block-time** *time*	공격 소스가 감지될 때 공격 소스에 대한 서비스 중단 시간(블록 시간)을 설정합니다. 단위는 초입니다.
Switch_config# **filter polling period** *time*	하이브리드 모드에서 필터 폴링 기간을 설정합니다. 단위는 초입니다.
Switch_config# **filter polling threshold** **[arp | bpdu | dhcp | igmp | ip | icmp | icmpv6]** *value*	하이브리드 모드에서 필터 폴링 임계값을 설정합니다.
Switch_config# **filter polling auto-fit**	공격 소스 필터에 적응하는 폴링 필터의 기간 및 임계값에 해당하는 매개변수를 설정합니다. 이 명령은 기본적으로 효율적입니다. 폴링 기간은 공격 필터 기간과 동일하고 폴링 패킷 임계값은 공격 필터 패킷 임계값의 3/4와 같습니다.
Switch_config# **filter shutdown-action**	시 모드에서 공격을 감지하면 포트를 종료합니다.

30.4.2 공격 방지 유형 구성

글로벌 및 인터페이스 구성 모드에서 다음 명령을 사용하여 공격 필터 유형을 구성합니다.

명령어	설명
config	글로벌 구성 모드로 들어갑니다.
filter dhcp	글로벌 구성 모드에서 DHCP 패킷 공격 필터를 활성화합니다.
filter icmp	ICMP 패킷 공격 필터를 활성화합니다.
icmpv6	ICMPv6 패킷 공격 필터를 활성화합니다.
filter igmp	IGMP 패킷 공격 필터를 활성화합니다.
filter ip source-ip	로벌 구성 모드에서 IP 공격 필터를 활성화합니다.
interface intf-name	인터페이스 구성 모드로 들어갑니다.
filter arp	인터페이스에서 ARP 패킷 공격 필터를 활성화합니다.
filter bpdu	인터페이스에서 BPDU 패킷 공격 필터를 활성화합니다.
filter dhcp	인터페이스에서 DHCP 패킷 공격 필터를 활성화합니다.
filter icmp	인터페이스에서 ICMP 패킷 공격 필터를 활성화합니다.
filter icmpv6	인터페이스에서 ICMPv6 패킷 공격 필터를 활성화합니다.
filter ip source-ip	인터페이스에서 IP 패킷 공격 필터를 활성화합니다.

ARP 공격은 호스트 MAC 주소 + 출발지 포트의 조합을 공격 출처로 간주합니다. 즉, 동일한 MAC 주소를 가진 패킷이라도 서로 다른 포트에서 들어오는 경우, 해당 패킷은 누적되지 않습니다. IGMP 공격 및 IP 공격은 호스트의 IP 주소와 출발지 포트를 공격 출처로 간주합니다.

- IGMP 공격 방지와 IP 공격 방지는 동시에 활성화할 수 없습니다.
- IP, ICMP, ICMPv6 및 DHCP 필터는 글로벌 및 인터페이스 구성 모드에서만 적용됩니다.

30.4.3 공격 방지 활성화

모든 공격 방지 매개변수를 설정한 후, 공격 방지 기능을 활성화할 수 있습니다.
공격 방지 기능이 시작되면 일부 프로세서 자원이 사용됩니다.

명령어	설명
config	글로벌 구성 모드로 들어갑니다.
filter enable	공격 방지 기능을 활성화합니다..

filter mode [raw | hybrid]	필터 모드를 원시 또는 하이브리드로 설정합니다.

30.4.4 공격 방지 상태 확인

공격 방지 기능이 시작된 후, 아래 명령어를 사용해 공격 방지 상태를 확인할 수 있습니다.

명령어	설명
show filter	공격 방지 상태를 확인합니다.
show filter summary	필터의 매개변수 구성 및 요약 정보를 확인합니다.

30.4.5 구성 예제

아래 그림과 같이, 스위치에서 ARP 공격 필터를 구성하여 LAN을 보호합니다.

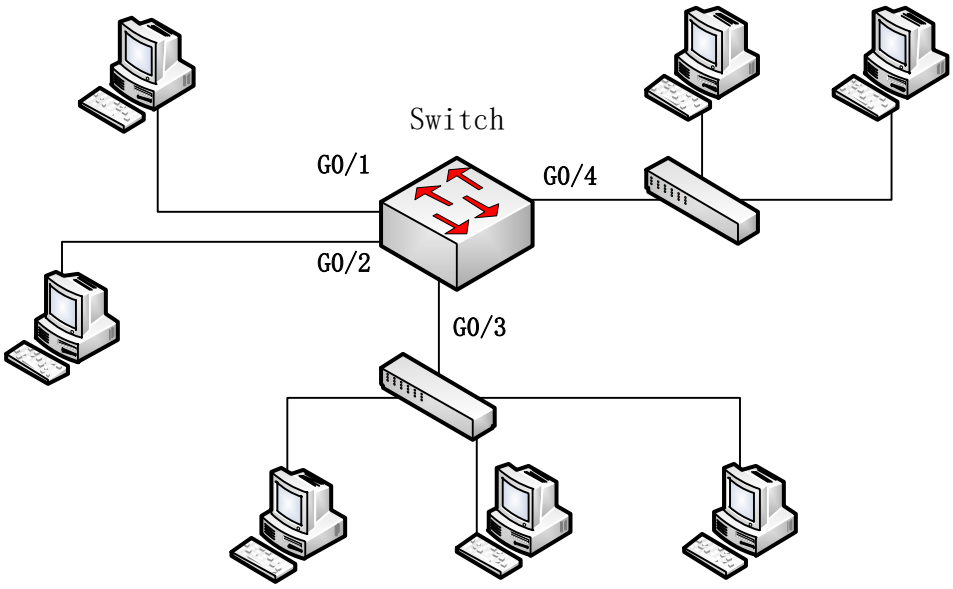


그림 50 네트워크 토폴로지

필터의 매개변수를 설정합니다. 호스트가 10초 동안 100개 이상의 ARP 메시지를 전송하면 공격 출처로 간주됩니다.

Switch# config

Switch_config# filter period 10

Switch_config# filter threshold arp 100

개의 포트에서 ARP 공격 필터를 설정하는 명령어 예시입니다.

Switch_config# interface range g0/1 - 4

Switch_config_intf# filter arp

Switch_config_intf# exit

Switch_config# filter mode raw

Switch_config# filter enable

30.4.6 Layer-3 네트워크 보호를 위한 IP 필터 사용

스위치가 여러 LAN, 서버 및 인터넷에 연결된 경우, IP 패킷 공격 방지는 서브넷 간 IP 스캔 및 BitTorrent와 같은 대규모 네트워크 연결을 차단할 수 있습니다.

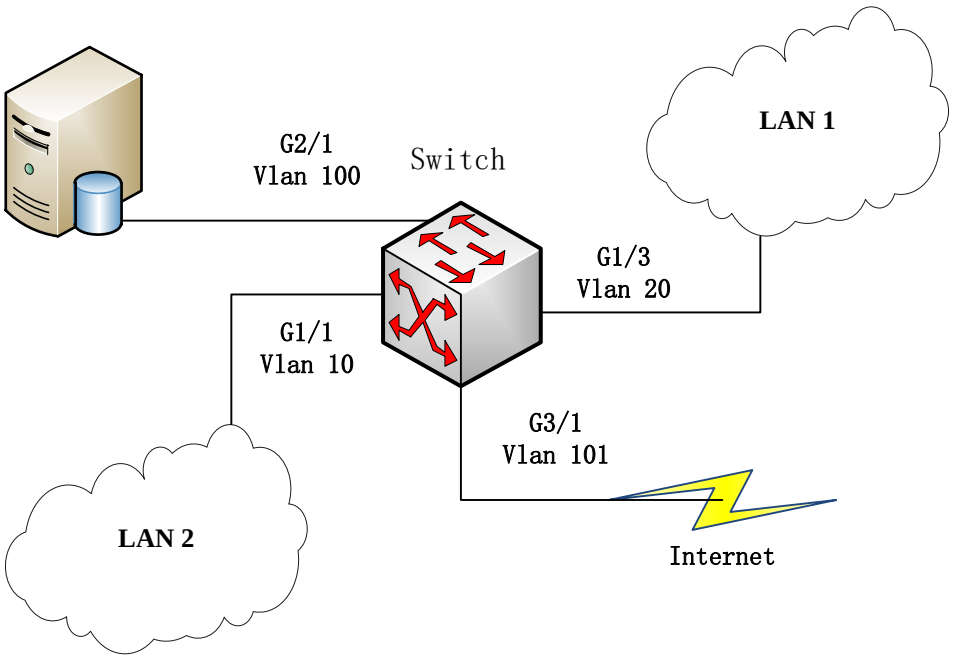


그림 51 네트워크 토폴로지

필터의 매개변수를 설정합니다. 1분 동안 300개 이상의 ARP 메시지를 보내는 호스트는 공격 소스로 간주됩니다.

Switch# config

Switch_config# filter period 60

Switch_config# filter threshold ip 300

글로벌 구성 모드와 인터페이스 모드에서 IP 패킷 필터를 활성화합니다. 서버와 외부 네트워크를 연결하는 인터페이스는 구성할 필요가 없습니다.

Switch_config# filter ip source-ip

Switch_config# interface g1/1

Switch_config_g1/1# filter ip source-ip

Switch_config_g1/1# interface g1/3

Switch_config_g1/3# filter ip source-ip

Switch_config_g1/3# exit

Switch_config#

필터 활성화:

Switch_config# filter enable

30.5DoS 공격 개요

30.5.1 DoS 공격 개념

DoS(서비스 거부) 공격은 네트워크 서비스 거부 공격이라고도 합니다.

일반적인 DoS 공격에는 네트워크 대역폭 공격과 연결성 공격이 포함되며 DoS 공격은 해커들이 자주 사용하는 네트워크 공격 방식으로, 궁극적인 목표는 네트워크를 마비시켜 합법적인 사용자에게 정상적인 네트워크 서비스를 중단시키는 것입니다. DoS 공격 방지를 위해 스위치는 다양한 공격 방지 방법을 제공합니다. 이 방법들은 Ping Flood, SYN Flood, Land Attack, Teardrop 및 비정상 플래그를 포함한 TCP 패킷과 같은 공격을 차단하는 데 사용됩니다. 스위치가 공격을 받으면, 공격 유형을 판단하고 해당 공격 패킷을 별도로 처리해야 합니다.

예를 들어, 공격 패킷을 CPU로 전송하거나 폐기(drop)하여 네트워크 성능 저하를 방지합니다.

30.6 DoS 공격 유형

해커들은 서버를 공격하기 위해 다양한 유형의 DoS 공격 패킷을 만듭니다.
다음은 일반적인 DoS 공격 패킷 유형입니다.

- Ping of Death
  Ping of Death는 비정상적인 Ping 패킷으로, 패킷 크기가 ICMP 임계값을 초과한다고 주장합니다.
  이로 인해 TCP/IP 스택이 손상되고 결국 수신 호스트가 다운됩니다.

- Tear Drop
  Tear Drop 공격은 TCP/IP 스택에서 신뢰된 IP 프래그먼트의 패킷 헤더에 포함된 정보를 악용합니다.
  IP 프래그먼트는 원본 패킷의 어느 부분이 포함되어 있는지를 나타내는 정보를 포함하고 있습니다.
  일부 TCP/IP 스택은 오버랩된 오프셋을 포함하는 위조된 프래그먼트를 수신하면 손상됩니다.

- SYN Flood
  표준 TCP 연결은 세 번의 핸드셰이크 과정을 거쳐야 합니다.
  클라이언트가 서버에 SYN 메시지를 전송하고, 서버는 SYN-ACK 메시지를 반환하며, 클라이언트는 SYN-ACK 메시지를 수신한 후 서버에 ACK 메시지를 전송하여 TCP 연결이 완료됩니다.

SYN Flood는 두 호스트 간의 TCP 프로토콜 스택 초기화 핸드셰이크 절차에서 DoS 공격을 유발합니다.

SYN-ACK 메시지를 받은 후, 공격자는 출발지 주소를 위조해 ACK 응답을 보내지 않아 서버가 ACK 메시지를 대기 상태로 유지하게 만듭니다.
공격자가 지속적으로 연결 요청을 보내면, 서버의 TCP 연결 큐가 가득 차게 되고 네트워크 대역폭이 급격히 감소해 정상적인 네트워크 서비스가 불가능해집니다.

- Land Attack
  공격자는 출발지 주소와 목적지 주소가 동일한 서비스 주소로 설정된 특별한 SYN 메시지를 생성합니다. 이 SYN 메시지는 서버가 자신에게 SYN-ACK 메시지를 보내도록 유도하고, 서버는 자신에게 ACK 메시지를 보내 연결을 생성합니다.
  이러한 연결은 타임아웃될 때까지 유지되며, 다수의 연결이 발생하면 서버가 마비됩니다.
  Land Attack은 IP Land와 MAC Land로 분류됩니다.

30.7 DoS 공격 방지 구성 작업

30.7.1 글로벌 DoS 공격 방지 구성

글로벌 DoS 공격 방지 구성은 글로벌 모드에서 DoS 공격 방지 하위 기능을 설정하는 것을 의미합니다. 각 하위 기능은 서로 다른 유형의 DoS 공격 패킷을 방지합니다.

- DoS IP 하위 기능 – LAND 공격 방지
- DoS ICMP 하위 기능 – Ping of Death 공격 방지

실제 요구 사항에 따라 해당 하위 기능을 설정할 수 있으며 DoS 공격 방지 기능은 EXEC 모드에서 구성합니다.

명령어	설명
config	글로벌 구성 모드로 진입합니다.
[**no**] **dos enable {all | icmp** ***icmp-value*** **| ip | l4port | mac | tcpflags | tcpfrag** ***tcpfrag-value*** **| tcpsmurf | icmpsmurf | ipsmurf }**	모든 유형의 DoS 공격 패킷을 차단하도록 all을 구성합니다. icmp-value보다 긴 ICMP 패킷을 PING 공격으로부터 차단하도록 icmp를 구성합니다. 이 중 icmp-value는 ICMP 패킷의 최대 길이, 즉 0-1023바이트를 의미합니다. 소스 IP가 대상 IP와 같은 IP 패킷을 차단하도록 ip를 구성합니다. 소스 포트 ID가 대상 포트 ID인 TCP/UDP 패킷을 차단하도록 l4port를 구성합니다. 소스 MAC이 대상 MAC과 같은 패킷을 차단하도록 mac를 구성합니다.

	불법 TCP 플래그가 포함된 TCP 패킷을 차단하도록 tcpflags를 구성합니다. 최소 TCP 헤더가 tcpfrag-value인 감지 대상 TCP 패킷을 차단하도록 tcpfrag를 구성합니다. 대상 주소가 boardcast 주소인 TCP 패킷을 차단하도록 tcpsmurf를 구성합니다. 목적지 주소가 boardcast 주소인 ICMP 패킷을 차단하도록 icmpsmurf를 구성합니다. 목적지 주소가 boardcast 주소인 IP 패킷을 차단하도록 ipsmurf를 구성합니다.
exit	

30.7.2 DoS 공격 방지 구성

show 명령어를 사용하여 DoS 공격 방지 구성을 확인할 수 있습니다.

아래 명령어를 EXEC 모드에서 실행하여 설정된 DoS 공격 방지 기능을 확인합니다.

명령어	설명
show dos	DoS 공격 방지 구성을 표시합니다.

30.7.3 DoS 공격 방지 구성 예시

아래 예시는 불법 플래그가 포함된 TCP 패킷 공격을 방지하도록 구성하고, 사용자의 설정을 확인하는 방법을 보여줍니다.

config

dos enable tcpflags

show dos

다음 예시는 글로벌 모드에서 출발지 IP와 목적지 IP가 동일한 IP 패킷 공격을 방지하는 방법을 보여줍니다.

config

dos enable ip

30.8 IP-Attack Prevention 구성

네트워크 대역폭의 효율적인 사용을 보장하기 위해, 당사의 스위치는 IP 공격 방지(IP-Attack Prevention) 기능을 제공하여 악성 IP 트래픽이 네트워크 대역폭을 점유하는 것을 차단합니다. 일

반적인 공격 유형에 대해, 특정 시간 동안 ICMP, IGMP, 또는 IP 패킷을 과도하게 전송하는 호스트에 통신 제한을 가하고, 해당 호스트에는 네트워크 서비스를 제공하지 않습니다. 이 구성을 통해 악성 패킷이 대량으로 대역폭을 소비해 발생하는 네트워크 혼잡 문제를 방지할 수 있습니다.

30.9 IP 공격 방지 구성 작업 목록

호스트가 지정된 시간 내에 IGMP, ICMP, 또는 IP 패킷을 과도하게 전송할 경우, 네트워크에서 공격이 발생했다고 간주합니다.

사용자는 다음을 선택할 수 있습니다:

- 공격 방지 유형 (ICMP, IGMP, 또는 IP)
- 적용 포트
- 공격 탐지 매개변수

구성 작업은 다음과 같습니다:

- IP 공격 방지 유형 구성
- IP 공격 탐지 매개변수 구성

30.10 IP-Attack Prevention 구성

30.10.1 IP 공격 탐지 매개변수 구성

명령어	설명
ip verify log-enable	공격 탐지 시스템 로그 활성화/비활성화
ip verify filter *time*	공격 소스가 식별되면 해당 서비스 중지. 단위는 초이며, 기본 시간은 180초

30.10.2 IP attack 탐지 유형 구성

명령어	설명
ip verify icmp ping-flood *value*	ping 패킷 수신 제한. *value*는 탐지 임계값을 의미
ip verify icmp ping-sweep *time*	ping 스캔 제한. *time*은 탐지 주기로, 단위는 초
ip verify tcp syn-flood *value*	TCP SYN 패킷 수신 제한. *value*는 탐지 임계값을 의미
ip verify tcp syn-sweep *time*	TCP SYN 포트 스캔 제한. *time*은 탐지 주기로, 단위는 초
ip verify tcp fin-scan *time*	TCP Stealth FIN 스캔 제한. *time*은 탐지 주기로, 단위는 초

ip verify tcp rst-flood *value*	TCP RST 패킷 수신 제한. *value*는 탐지 임계값을 의미
ip verify udp udp-flood *value*	UDP 패킷 수신 제한. *value*는 탐지 임계값을 의미
ip verify udp udp-sweep *time*	UDP 스캔 제한. *time*은 탐지 주기로, 단위는 초
ip verify attack Xmas-Tree *time*	Xmas-Tree 스캔 공격 필터링. *time*은 탐지 주기로, 단위는 초
ip verify attack Null-scan *time*	Null 스캔 공격 필터링. *time*은 탐지 주기로, 단위는 초
ip verify attack Land	Land 공격 필터링
ip verify attack Smurf	Smurf 공격 필터링
ip verify attack WinNuke	WinNuke 공격 필터링
ip verify attack TearDrop	TearDrop 공격 필터링
ip verify attack Fraggle	Fraggle 공격 필터링

30.10.3 IP 공격 방지 기능 활성화

모든 공격 방지 매개변수가 구성되면 공격 방지 기능을 활성화할 수 있습니다. 공격 방지 기능은 소량의 프로세서 공간을 사용합니다.

명령어	설명
ip verify enable	공격 탐지 활성화/비활성화. 이 명령어를 사용하지 않으면 공격 탐지가 비활성화되며, 차단된 모든 공격 소스가 차단 해제됩니다.

30.10.4 IP 공격 방지 구성 예제

포트 스캔 공격 방지 기능을 활성화하려면 다음과 같이 구성할 수 있습니다.
어떤 호스트가 15초 이내에 한 번 이상의 스캔 단위로 포트를 스캔하면 공격으로 간주되며, 10분 동안 네트워크 서비스가 차단됩니다.

ip verify icmp ping-sweep 15

ip verify tcp syn-sweep 15

ip verify udp udp-sweep 15

ip verify enable

ip verify log-enable

ip verify filter 600

30.11 네트워크 세그먼트 스캔에 대한 IP Attack 방지

직접 연결된 라우트에 다량의 스캔 패킷을 보내는 악의적인 공격을 방지하기 위해, 스위치는 직접 연결된 라우트의 도달 불가능한 주소에 대해 소프트웨어 캐시를 생성하여 CPU 사용률을 증가시킵니다. 직접 네트워크 세그먼트 스캔에 대한 IP 공격 방지 기능은 이러한 공격을 처리하여 CPU 사용률을 줄이는 데 도움이 됩니다.

30.12 네트워크 세그먼트 스캔에 대한 구성 작업 목록

스위치 VLAN에서 불완전한 ARP 수가 일정 수를 초과하면, 스위치가 직접 네트워크 세그먼트 스캔으로부터 공격을 받은 것으로 간주합니다.
지정된 시간 간격 내에 도달 불가능한 IP 패킷 수가 임계값을 초과하면, 공격이 발생한 것으로 간주되며, 기록 및 출력하여 사용자에게 알립니다.
사용자는 직접 네트워크 세그먼트 스캔 공격 방지 기능의 동작 모드 및 공격 탐지 매개변수를 선택할 수 있습니다. 구성 작업은 다음을 포함합니다:

- 직접 네트워크 세그먼트 스캔에 대한 IP 공격 방지 탐지 매개변수 구성
- 직접 네트워크 세그먼트 스캔 방지 탐지 유형 구성

참고 : ip verify ip-sweep action rate-limit-attacker 명령은 ip verify ip-sweep action rate-limit 명령을 덮어씁니다. 그렇지 않으면 먼저 no ip verify ip-sweep action rate-limit-attacker를 구성하여 ip verify ip-sweep action rate-limit을 설정해야 합니다. 덮어쓸 때 시간 및 패킷 매개변수는 그대로 유지됩니다.

30.12.1 네트워크 세그먼트 스캔에 대한 IP 공격 방지 탐지 매개변수 구성

명령어	설명
ip verify filter *time*	공격원이 식별되었을 때 해당 공격원의 서비스를 중지합니다. 조정 단위는 초이며, 기본 시간은 180초입니다.

30.12.2 네트워크 세그먼트 스캔 방지 탐지 유형 구성

명령어	설명
ip verify ip-sweep action rate-limit	IP 패킷 수를 제한합니다.
ip verify ip-sweep action rate-limit *time packets*	제한 시간 동안 허용되는 최대 IP 패킷 수를 설정하여 IP 패킷 수를 제한합니다.
ip verify ip-sweep action rate-limit-attacker	공격자로 정의된 IP 패킷 수만 제한합니다.

ip verify ip-sweep action rate-limit-attacker *time packets*	제한 시간 동안 공격자로 정의된 IP 패킷의 최대 허용 수를 설정합니다.
ip verify ip-sweep action no-cache	직접 연결된 네트워크 세그먼트의 알려지지 않은 호스트에 대한 캐시 생성을 금지합니다.

30.12.3 네트워크 세그먼트 스캔에 대한 IP 공격 방지 활성화

모든 매개변수가 구성되면 직접 네트워크 세그먼트 스캔에 대한 IP 공격 방지 기능을 활성화할 수 있습니다. 공격 방지 기능은 소량의 프로세서 공간을 차지한다는 점에 유의해야 합니다.

명령어	설명
ip verify ip-sweep detect unknown-host	직접 연결된 네트워크에서 알려지지 않은 호스트의 IP 스캔에 대한 공격 방지 기능을 활성화/비활성화합니다.

30.12.4 네트워크 세그먼트 스캔에 대한 IP 공격 방지 예시

직접 네트워크 세그먼트 스캔에 대한 IP 공격 방지를 활성화하려면 다음과 같이 구성할 수 있습니다. 즉, 감지된 공격자는 2초마다 200개의 IP 패킷만 전달할 수 있으며, 알려지지 않은 직접 네트워크 세그먼트 호스트의 캐시를 방지합니다. 또한, 전체 테스트 결과는 10분마다 초기화됩니다.

ip verify filter 600

ip verify ip-sweep detect unknown-host

ip verify ip-sweep action no-cache

ip verify ip-sweep action rate-limit 2 200

30.12.5 네트워크 세그먼트 스캔에 대한 IP 공격 방지 탐지 결과

Jan 1 00:07:14 Unknown-host (connected network sweep) attack detected

Jan 1 00:07:14 Action rate-limit-attacker is being used.

Jan 1 00:07:14 Action no-cache is being used.

Jan 1 00:07:14 Connected network sweep attacker 100.1.1.2 detected, VLAN 100, port g2/1

Jan 1 00:07:14 [SLOT 2]Connected network sweep attacker 100.1.1.2 detected, VLAN 100, port g2/1

직접 네트워크 세그먼트 스캔 공격 및 rate-limit-attacker와 action no-cache 방어 방법이 활성화된 경우, VLAN 100, 물리 포트 g2/1, IP 주소 100.1.1.2에서 공격자의 IP 네트워크 세그먼트 스캔 공격이 감지되었습니다. 가능한 빨리 조치해 주시기 바랍니다.

30.13 Urpf 개요

30.13.1 uRPF (Unicast Reverse Path Forwarding)

uRPF(Unicast Reverse Path Forwarding)은 장치가 패킷을 포워딩하기 전에 출발지 주소가 로컬 라우팅 테이블에 존재하는지 확인하는 메커니즘입니다. 이는 출발지 주소 스푸핑(Source Address Spoofing)을 검사하고, DOS 공격을 방지하는 데 유용합니다.
uRPF는 Strict 모드와 Loose 모드 두 가지 방식이 있습니다.

- Strict 모드: 출발지 주소에 대한 라우팅 테이블 항목이 존재하고, 해당 경로의 출구 인터페이스(egress interface)가 패킷이 수신된 인터페이스와 동일한 경우에만 허용합니다.
- Loose 모드: 패킷을 포워딩하기 전에 라우팅 테이블에 경로가 존재하는지만 확인합니다.

30.14 Urpf 구성

30.14.1 글로벌 설정 모드에서 uRPF 활성화

uRPF를 사용하려면 글로벌 설정 모드에서 uRPF를 활성화해야 합니다.

명령어	설명
[no] urpf check	글로벌 설정 모드에서 uRPF 체크를 활성화/비활성화합니다.

30.14.2 VLAN 인터페이스에서 uRPF 검사 모드 구성

VLAN 인터페이스에서 uRPF 검사 모드(Strict 모드 또는 Loose 모드)를 설정합니다.

- Strict 모드에서는 패킷의 출발지 주소를 통해 FIB 테이블에서 라우팅 가능 여부와 동시에 패킷의 인그레스 포트(ingress port)가 다음 홉 인터페이스와 일치하는지를 확인합니다.
- Loose 모드에서는 출발지 주소를 FIB 테이블에서 확인하여 라우팅 가능한지만 검사합니다.

uRPF를 구성한 후에는 경로 필터링도 지원됩니다. 기본 경로(default route)가 설정된 경우, uRPF가 출발지 주소를 FIB 테이블에서 검사할 때 모든 출발지 주소가 일치하는 항목을 찾을 수 있습니다. 기본적으로 uRPF 검사에서 FIB에서 찾은 경로가 기본 경로인 경우, 항목이 존재하지 않는 것으로 간주되어 패킷이 드롭됩니다.

참고 : 글로벌 설정 모드에서 uRPF 검사를 활성화해야 uRPF가 작동합니다.

VLAN 인터페이스에서 uRPF 모드를 구성하려면 인터페이스 설정 모드에서 다음 명령어를 실행합니다.

명령어	설명
[no] urpf check *strict/loose [uncheck-default-route]*	VLAN 인터페이스에서 uRPF 검사 모드를 구성합니다.

	uncheck-default-route는 기본적으로 비활성화되어 있습니다.

참고 : uncheck-default-route를 활성화하면, 패킷의 출발지 주소가 FIB 테이블에서 일치하는 항목을 찾을 경우, 해당 항목이 기본 경로(default route)인지 여부와 상관없이 패킷이 허용됩니다. 기본 설정에서는(uncheck-default-route 비활성화) FIB 테이블에서 출발지 주소가 기본 경로로 매칭될 경우, uRPF 검사는 실패하고 패킷이 드롭됩니다.

31. 라우팅 프로토콜 개요

31.1 IP 라우팅 프로토콜

우터는 여러 IP 동적 라우팅 프로토콜을 구현합니다. 이 장에서는 각 프로토콜에 대해 설명합니다. IP 라우팅 프로토콜은 내부 게이트웨이 라우팅 프로토콜(IGP)과 외부 게이트웨이 라우팅 프로토콜(EGP) 두 가지로 분류됩니다. 당사 라우터는 RIP, OSPF, BGP 및 BEIGRP를 지원합니다. RIP, OSPF, BGP 및 BEIGRP는 실제 필요에 따라 개별적으로 구성할 수 있습니다.

당사 라우터는 여러 라우팅 프로토콜을 동시에 구성할 수 있으며, 메모리가 충분한 경우 무제한 OSPF 프로세스, 하나의 BGP 프로세스, 하나의 RIP 프로세스 및 무제한 BEIGRP 프로세스를 지원합니다.

redistribute 명령어를 사용하면 현재 라우팅 프로토콜의 데이터베이스에 다른 라우터 프로토콜을 주입할 수 있어 여러 라우팅 프로토콜을 연동할 수 있습니다.

IP 동적 라우팅 프로토콜을 구성하려면 해당 프로세스를 시작하고, 해당 네트워크 인터페이스 및 특정 동적 라우팅 프로세스를 연결해야 합니다. 이를 통해 라우팅 프로세스가 실행될 인터페이스를 지정합니다. 이를 위해 구성 명령어에 대한 관련 문서를 참조해야 합니다.

이 문서에서 라우팅 장치는 스위치를 지칭합니다.

31.2 라우팅 프로토콜 선택

라우팅 프로토콜 선택은 복잡한 과정입니다. 라우팅 프로토콜을 선택할 때는 다음과 같은 요소를 고려해야 합니다.

- 네트워크의 규모와 복잡성
- VLSM(가변 길이 서브넷 마스크) 지원 필요 여부
- 네트워크 트래픽
- 보안 요구 사항
- 신뢰성 요구 사항
- 정책
- 기타

31.2.1 내부 게이트웨이 라우팅 프로토콜 (Interior Gateway Router Protocol)

내부 게이트웨이 라우팅 프로토콜은 단일 자율 시스템(Autonomous System) 내에서 사용됩니다.

모든 IP 내부 게이트웨이 라우팅 프로토콜은 시작될 때 특정 네트워크(예: network)를 구성해야 합

니다.

각 라우팅 프로세스는 네트워크에서 다른 라우터의 업데이트 메시지를 수신하고, 동시에 자신의 라우팅 정보를 네트워크에 방송합니다.

당사 라우터가 지원하는 내부 게이트웨이 라우팅 프로토콜은 다음과 같습니다.

- RIP
- OSPF
- BEIGRP

31.2.2 외부 게이트웨이 라우팅 프로토콜 (Exterior Gateway Routing Protocol)

외부 게이트웨이 라우팅 프로토콜은 서로 다른 autonomous system 간에 라우팅 정보를 교환하는 데 사용됩니다.

라우팅을 교환하기 위해서는 일반적으로 해당 neighbor, 도달 가능한 네트워크 및 로컬 autonomous system 번호를 구성해야 합니다.

당사 라우터가 지원하는 외부 게이트웨이 라우팅 프로토콜은 BGP입니다.

31.3 VRF 구성

VPN의 핵심 요소 중 하나는 데이터를 안전하게 보호하고 격리하는 것입니다. VPN에 속하지 않은 스테이션 간의 통신은 방지되어야 합니다.

PE(Provider Edge) 장치에서 로컬 인터페이스를 통해 전송된 VPN 사용자 경로를 구별하기 위해, PE 장치에 가상 라우트를 생성합니다. 각 가상 라우트는 자체 라우팅 테이블 및 포워딩 테이블을 가집니다. 이 라우팅 테이블과 포워딩 테이블을 VRF(VPN Routing and Forwarding 인스턴스)라고 합니다. 하나의 VRF는 동일한 스테이션과 관련된 라우팅 테이블, 인터페이스(서브 인터페이스), 라우팅 인스턴스 및 라우팅 정책을 포함합니다. PE에서는 동일한 VPN에 속하는 물리 포트 또는 논리 포트가 하나의 VRF에 대응됩니다.

31.4 VRF 구성 작업 목록

VRF를 구성하려면 다음 작업을 수행해야 합니다.

- VRF 테이블 생성
- VRF에 인터페이스 연결
- VRF의 대상 VPN 확장 속성 구성
- VRF 설명 구성
- VRF 정적 경로 구성
- VRF 모니터링
- VRF 유지 관리
- VRF 구성 예제

31.5구성 작업

글로벌 구성 모드에서 VPN 라우팅 및 포워딩 테이블을 생성하려면 아래와 같이 설정 합니다.

명령어	설명
PE_config#**ip vrf** ce	VRF 구성 모드에 진입하여 VRF 테이블을 정의합니다.
PE_config_vrf_ce#**rd** *ASN:nn or IP-address:nn*	VRF의 라우팅 태그를 지정하고, VRF 라우팅 및 포워딩 테이블을 생성합니다.
PE_config_vrf_ce#**route-target** [**export** | **import** | **both**] *ASN:nn or IP-address:nn*	VRF 입력을 생성하고 대상 VPN 확장 속성을 출력합니다.

31.5.1 인터페이스를 VRF에 연결

인터페이스를 VRF에 연결하려면 아래와 같이 설정합니다.

명령어	설명
PE_config#**interface vlan** 1	인터페이스 구성 모드로 진입합니다.
PE_config_v1#**ip vrf forwarding** *vrf-name*	인터페이스를 VRF에 연결합니다.
PE_config_v1#**ip address** *ip-address subnet-mask*	인터페이스의 IP 주소를 설정합니다.

31.5.2 VRF 대상 VPN 확장 속성 구성

VRF의 대상 VPN 확장 속성을 구성하려면 아래와 같이 설정합니다.

명령어	설명
PE_config#**ip vrf** ce	VRF의 구성 모드로 들어갑니다.
PE_config_vrf_ce#**rd** *ASN:nn or IP-address:nn*	VRF 라우팅 태그를 구성하고 VRF 테이블을 만듭니다.
PE_config_vrf_ce#**route-target** [**export** | **import** | **both**]*ASN:nn or IP-address:nn*	VRF의 입력과 출력 대상 확장 속성을 구성합니다.
PE_config_vrf_ce#**import map** *WORD*	VRF 라우팅 테이블에 추가하는 경로의 경로 맵 필터를 구성합니다.
PE_config_vrf_ce#**export map** *WORD*	경로 맵 조건을 준수하는 대상 VPN 확장 속성을 VRF의 출력 대상 VPN 확장 속성에 추가합니다.

로컬 경로를 다른 PE 라우팅 장치에 게시하기 전에, 입구 PE는 직접 스테이션에서 학습한 모든 경로에 경로 대상 속성을 추가합니다. 경로에 연결된 대상 값은 출력 대상 확장 속성에 구성된 VRF 값을 기반으로 합니다.

다른 PE가 로컬 VRF에 게시한 원격 경로를 설치하기 전에, 입구 PE 경로 장치의 모든 VRF는 하나의 입력 대상 확장 속성으로 구성됩니다. VPN-IPv4에서 생성한 라우팅 대상 속성이 VRF 입력 대상과 일치할 때까지 PE 라우팅 장치는 특정 VRF에만 설치할 수 있습니다.

31.5.3 VRF 설명 구성

VRF 설명을 구성하려면 아래와 같이 설정합니다.

명령어	설명
PE_config#**ip vrf** ce	VRF 구성 모드에 진입합니다.
PE_config_vrf_ce#**rd** *ASN:nn or IP-address:nn*	VRF 라우팅 태그를 설정하고 VRF 테이블을 생성합니다.
PE_config_vrf_ce# **description** LINE	VRF에 대한 설명을 설정합니다.

2.3.5 VRF 정적 경로 구성

VRF 정적 경로를 구성하려면 아래와 같이 설정합니다.

명령어	설명
PE_config#**ip vrf** ce	VRF 구성 모드로 들어갑니다.
PE_config_vrf_ce#**rd** *ASN:nn or IP-address:nn*	VRF 라우팅 태그를 구성하고 VRF 테이블을 만듭니다.
PE_config_vrf_ce#**exit**	VRF 구성 모드를 종료합니다.
PE_config#**ip route** [**vrf** vrf-name] dest mask { type num | nexthop } [distance]	VRF 정적 경로를 구성합니다.

31.5.4 VRF 모니터링

VRF를 모니터링하고 VRF 통계를 확인하려면 아래와 같이 설정합니다.

명령어	설명
PE#**show ip vrf**	VRF 및 관련 포트 정보를 표시합니다.
PE#**show ip vrf** [{**brief** | **detail** | **interfaces**}] *vrf-name*	VRF 구성 및 관련 포트 정보를 표시합니다.
PE#**show ip route vrf** *vrf-name*[A.B.C.D | all | beigrp | bgp | ospf | rip | connect | static | summary]	VRF 라우팅 테이블의 라우팅 정보를 표시합니다.

31.5.5 VRF 유지 관리

VRF를 유지 관리하고, 관리 모드에서 주요 라우팅 테이블 및 VRF 라우팅 테이블의 변경 사항과 VRF 구성 정보를 추적하려면 아래와 같이 설정합니다.

명령어	설명
PE#**debug ip routing**	주요 라우팅 테이블에서 경로의 추가, 삭제 및 변경 사항을 추적합니다.
PE #**debug ip routing message**	VRF가 수신 및 전송한 정보를 추적합니다.
PE #**debug ip routing vrf** *vrf-name*	지정된 VRF 라우팅 테이블의 추가, 삭제 및 변경 사항을 추적합니다.

31.5.6 VRF 구성 예제

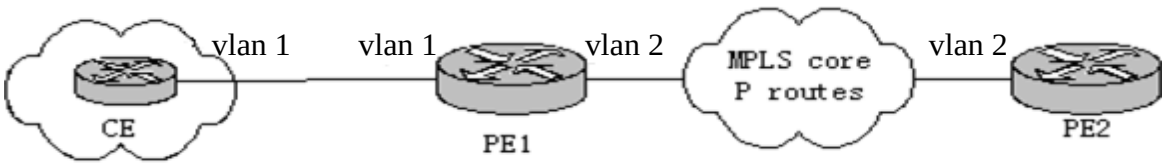


그림 52 네트워크 토폴로지

Routing device CE:

```
interface loopback 0
ip address 22.1.1.1 255.255.255.0
!
interface vlan 1
ip address 170.168.20.152 255.255.255.0
!
router ospf 1
network 170.168.20.0 255.255.255.0 area 0
network 22.1.1.0 255.255.255.0 area 0
!
Routing device PE1:
ip vrf pe1
rd 1:1
route-target 1:1
!
interface vlan 1
ip vrf forwarding pe1
ip address 170.168.20.153 255.255.255.0
!
interface vlan 2
ip address 176.168.20.152 255.255.255.0
!
router ospf 1 vrf pe1
 network 170.168.20.0 255.255.255.0 area 0
!
router bgp 1
neighbor 176.168.20.154 remote-as 2
 address-family vpnv4
 neighbor 176.168.20.154 activate
```

```
 exit-address-family
 address-family ipv4 vrf pe1
 no synchronization
 redistribute ospf 1
 exit-address-family
Routing device PE2:
ip vrf pe2
rd 1:1
route-target 1:1
!
interface loopback 0
ip vrf forwarding pe2
ip address 44.1.1.1 255.255.255.0
!
interface vlan 2
 ip address 176.168.20.154 255.255.255.0
!
router bgp 2
neighbor 176.168.20.153 remote-as 1
address-family vpnv4
neighbor 176.168.20.153 activate
exit-address-family
address-family ipv4 vrf pe2
no synchronization
redistribute connected
```

1.1 exit-address-family

31.6 Multi-VRF CE 개요

가상 사설망(VPN)은 여러 클라이언트 네트워크가 ISP에서 제공하는 대역폭을 안전하게 공유할 수 있는 방법을 제공합니다. 일반적으로 하나의 VPN은 ISP 라우터에서 공용 라우팅 테이블을 공유하는 클라이언트 네트워크 그룹으로 구성됩니다. 각 클라이언트 네트워크는 ISP 네트워크 장치의 인터페이스에 연결되며, ISP 장치는 각 인터페이스를 VPN 라우팅 테이블에 연결합니다. 하나의 VPN 라우팅 테이블은 **VRF(VPN Routing/Forwarding table)**이라고도 합니다.

VRF는 일반적으로 Provider Edge(PE) 장치에 배포되며, 대표적으로 MPLS VRF VPN이 있습니다. PE는 여러 VPN을 지원하며, 각 VPN은 독립적인 IP 주소 공간을 가지므로 서로 다른 VPN 간에 IP 주소가 중복될 수 있습니다. 서로 다른 클라이언트의 VPN은 PE의 다른 인터페이스에 연결되며, PE는 패킷이 들어오는 포트에 따라 확인해야 할 라우팅 테이블을 구분합니다.

Multi-VRF CE는 여러 클라이언트 네트워크를 연결하는 작업을 PE에서 CE로 이전하는 것을 의미하며, CE와 PE 간에는 물리적인 링크 하나만 필요합니다. 이를 통해 PE의 포트 자원이 절약됩니다. CE는 각 VPN에 대해 VRF 라우팅 테이블을 유지합니다. 클라이언트 네트워크에서 전송된 패킷은 먼저 CE에서 포워딩되고, 이후 ISP 네트워크를 거쳐 PE로 전달됩니다.

MCE(멀티 VRF CE) 역할을 하는 스위치는 서로 다른 클라이언트 네트워크를 다른 포트를 통해 연결하고, 이 포트를 VPN 라우팅 테이블에 연결합니다. 스위치는 VLAN 포트에서만 VRF 설정을 지원합니다.

MCE 기능은 대규모 MPLS-VRF VPN 네트워크의 가장자리에 주로 배포됩니다. 멀티 VRF CE, MPLS 라벨 스위칭 및 MPLS 제어 계층 기능은 서로 독립적입니다.

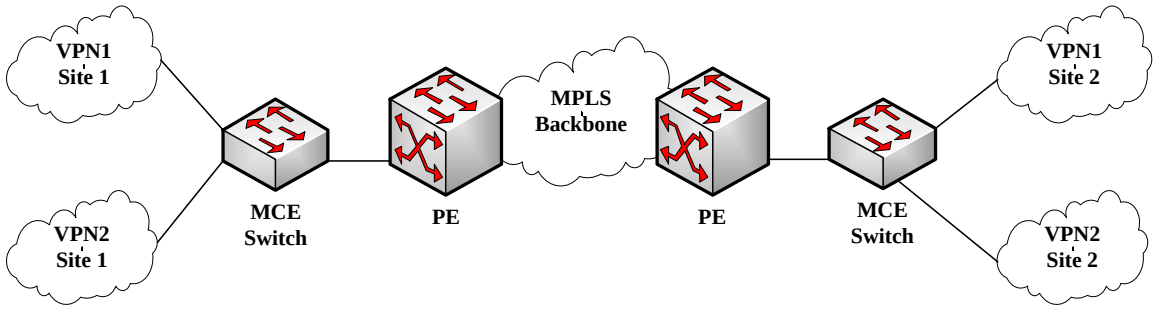


그림 53 MPLS-VRF VPN 네트워크

31.6.1 CE 라우트 설정

멀티 VRF CE(MCE) 스위치는 여러 동적 라우팅 프로토콜을 통해 CE와 라우트를 설정할 수 있습니다. CE는 라우터 또는 이더넷 스위치일 수 있습니다. 지원되는 라우팅 프로토콜은 OSPF, RIP, BEIGRP입니다. MCE 스위치는 정적 라우팅(static routing) 구성도 지원합니다.

MCE 스위치는 일반적으로 서로 다른 VPN에 속하는 CE를 연결하기 위해 다양한 VLAN 포트를

필요로 합니다. VPN 연결에 사용되는 VLAN 포트는 반드시 VRF에 연동되어야 합니다. CE는 VRF를 지원할 필요가 없습니다.

31.6.2 PE 라우트 설정

MCE 스위치는 하나 또는 여러 개의 PE에 연결될 수 있습니다. 하지만 MCE와 연결된 PE는 모두 VRF가 구성되어 있어야 합니다. MCE는 CE에서 학습한 라우트를 PE에 제공하고, PE로부터 원격 클라이언트 네트워크의 라우트를 학습합니다.

MCE와 PE 간의 VRF 라우트는 BGP, OSPF, RIP, BEIGRP와 같은 동적 라우팅 프로토콜을 통해 설정할 수 있습니다. 물론 VRF 라우트는 정적으로 설정할 수도 있습니다.

일반적으로 MCE와 PE는 서로 다른 자율 시스템(AS)에 속합니다. 따라서 **MCE와 PE 간 VRF 라우트를 EBGP(Exterior Border Gateway Protocol)**를 통해 설정하는 방법이 이 문서의 주요 포인트입니다.

31.7 Multi-VRF CE 구성

기능	기본 구성
VRF	구성 없음. 모든 라우트는 기본 라우팅 테이블에 추가됩니다.
VRF의 VPN 확장성	라우팅 (RD)이 없습니다. 입/출력 라우팅 타겟(RT)이 없습니다.
최대 VRF 라우트 수	10,240
VRF 포트	해당 사항 없음. VLAN 포트는 VRF에 연동되지 않으며, 포트의 라우트는 기본 라우팅 테이블에 추가됩니다.
IP Express Forwarding	하드웨어 IP 라우팅이 비활성화되어 있습니다.

31.8 MCE 구성 작업

- VRF 구성
- VPN 라우트 구성
- PE와 CE 간 BGP 라우트 구성
- PE와 CE 간 VRF 연결성 테스트

31.8.1 VRF 구성 방법

다음 단계를 참조하여 하나 또는 여러 개의 VRF를 구성하십시오.

기능	기본 구성
Switch# config	스위치 구성 모드로 들어갑니다.
Switch_config# ip vrf *vrf-name*	VRF를 생성하고 VRF 구성 모드로 들어갑니다. vrf-name: 최대 31자의 VRF 이름
Switch_config_vrf# rd *route-distinguisher*	VRF의 경로 구분자를 설정합니다. route-distinguisher: 경로 구분자를 의미합니다. 자율 도메인 ID와 난수, 또는 IP와 난수로 구성됩니다.
Switch_config_vrf# route-target **{ export | import | both }** *route-target-extened-community*	입력/출력 VRF 객체의 확장된 VPN 속성을 생성합니다. route-target-extended-community: 자율 도메인 ID와 난수, 또는 IP와 난수로 구성됩니다.
Switch_config_vrf# **exit**	VRF 구성 모드를 종료합니다.
Switch_config# interface *intf-name*	인터페이스 구성 모드로 들어갑니다. intf-name: 인터페이스 이름을 의미합니다.

Switch_config_intf# ip vrf forwarding *vrf-name*	L3 인터페이스를 VRF와 연관시킵니다. vfi-name: VRF의 이름을 의미합니다.
Switch_config_intf# exit	인터페이스 구성 모드를 종료합니다.
Switch_config# **ip exf**	IP 하드웨어 라우팅을 활성화합니다.
Switch_config# show ip vrf **[brief | detail | interface] [** *vrf-name* **]**	RF 정보를 탐색합니다.
Switch_config#no ip vrf *vrf-name*	구성된 VRF와 VRF와 L3 인터페이스 간의 관계를 삭제합니다. vfi-name: VRF의 이름을 의미합니다.
Switch_config_intf# no ip vrf forwarding **[** *vrf-name* **]**	L3 인터페이스와 VRF 간의 관계를 삭제합니다.

31.8.2 VPN 경로 구성

MCE와 고객 장치(CE) 간 라우트는 BGP, OSPF, RIP, BEIGRP 또는 정적 라우트(static route) 설정을 통해 구성할 수 있습니다.

다음은 OSPF 구성 예시이며, 다른 라우팅 프로토콜 구성도 유사한 방식으로 진행됩니다.

참고 : MCE에서 클라이언트 네트워크와 연결하기 위한 라우트를 구성할 때, 라우팅 프로토콜의 VRF 속성을 지정해야 합니다. 고객 장치(CE)에서는 VRF를 구성할 필요가 없습니다.

기능	기본 구성
Switch# config	스위치 구성 모드로 들어갑니다.
Switch_config# router ospf *process-id* **vrf** *vrf-name*	OSPF-VRF 경로를 시작하고 구성 모드로 들어갑니다. OSPF 네트워크, 마스크 및 영역 ID를 정의합니다.
Switch_config_ospf# network *network-number* *network-mask* **area** *area-id*	OSPF 네트워크, 마스크 및 영역 ID를 정의합니다.
Switch_config_ospf# **redistribute bgp** *ASN*	지정된 BGP 네트워크를 OSPF 네트워크로 전달합니다.
Switch_config_ospf# **exit**	OSPF 구성 모드를 종료합니다.
Switch_config# **show ip ospf**	OSPF 프로토콜에 대한 정보를 탐색합니다.
Switch_config# **no router ospf** *process-id*	OSPF-VRF 라우팅 구성을 삭제합니다.

31.8.3 PE와 CE 간 BGP 라우트 구성

다음 구성 명령어를 참조하여 PE와 CE 간 BGP 라우트를 설정하십시오.

기능	기본 구성
Switch# **config**	스위치 구성 모드로 들어갑니다.
Switch_config# **router bgp** *autonomous-system-number*	자율 시스템 번호를 지정하여 BGP 프로토콜을 시작하고 BGP 구성 모드로 들어갑니다.
Switch_config_bgp# **bgp log-neighbor-changes**	BGP 이웃 변경에 대한 기록을 시작합니다.
Switch_config_bgp# **address-family ipv4 vrf** *vrf-name*	VRF 주소 패밀리 구성 모드로 들어갑니다.
Switch_config_bgp_af# **redistribute ospf** *ospf-process-id*	OSPF 라우팅 정보를 BGP 네트워크로 전달합니다.
Switch_config_bgp_af# **network** *network-number/prefix-length*	BGP에서 분배하는 네트워크 번호와 마스크 길이를 구성합니다.
Switch_config_bgp_af# **neighbor** *address* **remote-as** *ASN*	BGP 이웃과 이웃의 자율 시스템 번호를 구성합니다.
Switch_config_bgp_af# **exit-address-family**	address-family를 종료 합니다.
Switch_config_bgp# **exit**	BGP 구성 모드를 종료합니다.
Switch_config# **show ip bgp vpnv4** **[all | rd | vrf]**	BGP-VRF 라우팅 정보를 탐색합니다.
Switch_config# **no router bgp** *ASN*	BGP 라우팅 구성을 삭제합니다.

31.8.4 PE와 CE 간 VRF 연결성 테스트

PE와 CE 간 VRF 연결성을 확인하려면 VRF 옵션을 사용하여 PING 명령어를 실행하십시오.

기능	기본 구성
Switch# **ping –vrf** *vrf-name ip-address*	VRF 내 주소로 PING을 수행하여 연결성을 확인합니다.

31.8.5 MCE 구성 예제

그림은 간단한 VRF 네트워크를 보여줍니다.

S1과 S2는 Multi-VRF CE 스위치입니다. S11, S12, S13은 VPN1에 속하며, S21, S22는 VPN2에 속합니다. 이 장치들은 모두 클라이언트 장치(CE)입니다. OSPF 라우트는 CE와 클라이언트 장치 간에 구성되며, BGP 라우트는 CE와 PE 간에 구성됩니다.

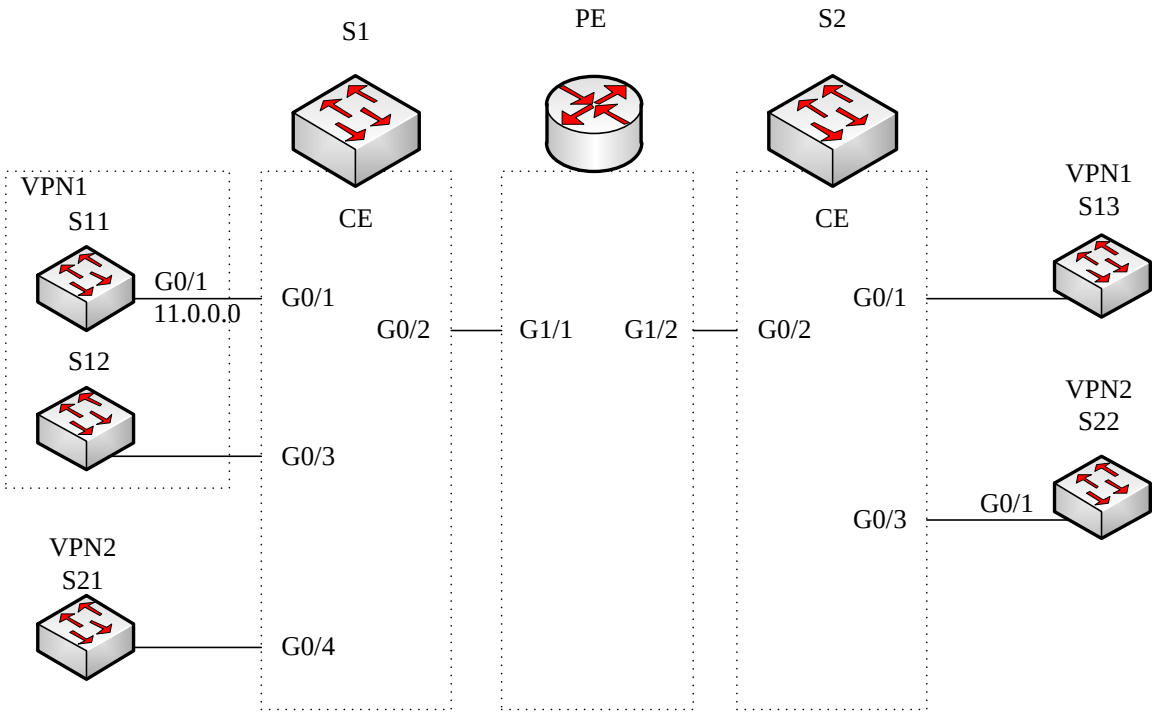


그림 54 MCE 설정 예제

- S11 설정

CE를 연결하는 물리적 인터페이스의 VLAN 속성을 설정합니다.

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 11

Switch_config_g0/1# exit

Sets the IP address and the VLAN interface.

Switch_config# interface VLAN11

Switch_config_v11# ip address 11.0.0.2 255.0.0.0

Switch_config_v11# exit

CE와 고객 장치 간의 라우팅 프로토콜을 설정합니다.

Switch_config# router ospf 101

Switch_config_ospf_101# network 11.0.0.0 255.0.0.0 area 0

Switch_config_ospf_101# exit

- MCE-S1

VPN1 및 VPN2에 대해 VRF를 생성하고, 라우트 구분자(RD)와 라우트 타겟(RT)을 설정합니다.

Switch# config

Switch_config# ip vrf vpn1

Switch_config_vrf_vpn1# rd 100:1

Switch_config_vrf_vpn1# route-target export 100:1

Switch_config_vrf_vpn1# route-target import 100:1

Switch_config_vrf_vpn1# exit

Switch_config# ip vrf vpn2

Switch_config_vrf_vpn2# rd 100:2

Switch_config_vrf_vpn2# route-target export 100:2

Switch_config_vrf_vpn2# route-target import 100:2

Switch_config_vrf_vpn2# exit

루프백 포트를 구성하고, 루프백 포트의 주소를 BGP 프로토콜의 라우터 ID로 사용합니다.

Switch_config# interface loopback 0

Switch_config_l0# ip address 101.0.0.1 255.255.255.255

Switch_config_l0# exit

S1은 F0/1 포트를 통해 S11에 연결되고, G0/4 포트를 통해 S21에 연결되며, G0/2 포트를 통해 PE에 연결됩니다.

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 11

Switch_config_g0/1# exit

Switch_config# interface gigaEthernet 0/4

Switch_config_g0/4# switchport pvid 15

Switch_config_g0/4# exit

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# switchport mode trunk

Switch_config_g0/2# exit

스위치의 L3 VLAN 포트를 설정하고, VLAN 포트에 VRF를 바인딩하고 IP 주소를 설정합니다.

Switch_config# interface VLAN11

Switch_config_v11# ip vrf forwarding vpn1

Switch_config_v11# ip address 11.0.0.1 255.0.0.0

Switch_config_v11# exit

Switch_config# interface VLAN15

Switch_config_v15# ip vrf forwarding vpn2

Switch_config_v15# ip address 15.0.0.1 255.0.0.0

Switch_config_v15# exit

Switch_config# interface VLAN21

Switch_config_v21# ip vrf forwarding vpn1

Switch_config_v21# ip address 21.0.0.2 255.0.0.0

Switch_config_v21# exit

Switch_config# interface VLAN22

Switch_config_v22# ip vrf forwarding vpn2

Switch_config_v22# ip address 22.0.0.2 255.0.0.0

Switch_config_v22# exit

CE와 클라이언트 장치 간 OSPF 라우트 구성

Switch_config# router ospf 1 vrf vpn1

Switch_config_ospf_1# network 11.0.0.0 255.0.0.0 area 0

Switch_config_ospf_1# redistribute bgp 100

Switch_config_ospf_1# exit

Switch_config# router ospf 2 vrf vpn2

Switch_config_ospf_2# network 15.0.0.0 255.0.0.0 area 0

Switch_config_ospf_2# redistribute bgp 100

Switch_config_ospf_2# exit

Switch_config# router bgp 100

Switch_config_bgp# bgp log-neighbor-changes

Switch_config_bgp# address-family ipv4 vrf vpn1

Switch_config_bgp_vpn1# no synchronization

Switch_config_bgp_vpn1# redistribute ospf 1

Switch_config_bgp_vpn1# neighbor 21.0.0.1 remote-as 200

Switch_config_bgp_vpn1# exit-address-family

Switch_config_bgp# address-family ipv4 vrf vpn2

Switch_config_bgp_vpn2# no synchronization

Switch_config_bgp_vpn2# redistribute ospf 2

Switch_config_bgp_vpn2# neighbor 22.0.0.1 remote-as 200

Switch_config_bgp_vpn2# exit-address-family

Switch_config_bgp# exit

Switch_config# vlan 1,11-12,21-22

Switch_config# ip exf

VLAN11 및 VLAN15는 고객 장치(CE)와 연결되어 있으며, 각각 VPN1 및 VPN2에 속합니다. VLAN21 및 VLAN22는 PE와 연결되어 있으며, VRF가 각각 VPN1 및 VPN2로 바인딩됩니다. OSPF 라우트는 CE와 고객 장치 간 라우팅을 담당하며, BGP 라우트는 PE와 CE 간 라우트를 설정합니다.

- PE 구성

VPN1 및 VPN2에 대해 VRF를 생성하고, RD 및 RT 값을 설정합니다.

Switch# config

Switch_config# ip vrf vpn1

Switch_config_vrf_vpn1# rd 200:1

Switch_config_vrf_vpn1# route-target export 200:1

Switch_config_vrf_vpn1# route-target import 200:1

Switch_config_vrf_vpn1# exit

Switch_config# ip vrf vpn2

Switch_config_vrf_vpn2# rd 200:2

Switch_config_vrf_vpn2# route-target export 200:2

Switch_config_vrf_vpn2# route-target import 200:2

Switch_config_vrf_vpn2# exit

루프백 인터페이스를 라우터 식별자로 설정

Switch_config# interface loopback 0

Switch_config_l0# ip address 102.0.0.1 255.255.255.255

Switch_config_l0# exit

PE와 CE를 연결하는 물리 인터페이스 설정

Switch_config# interface gigaEthernet 1/1

Switch_config_g1/1# switchport mode trunk

Switch_config_g1/1# exit

Switch_config# interface gigaEthernet 1/2

Switch_config_g1/2# switchport mode trunk

Switch_config_g1/2# exit

PE의 L3 VLAN 인터페이스 설정 (S1 및 S2 연결)

Switch_config# interface VLAN21

Switch_config_v21# ip vrf forwarding vpn1

Switch_config_v21# ip address 21.0.0.1 255.0.0.0

Switch_config_v21# exit

Switch_config# interface VLAN22

Switch_config_v22# ip vrf forwarding vpn2

Switch_config_v22# ip address 22.0.0.1 255.0.0.0

Switch_config_v22# exit

Switch_config# interface VLAN31

Switch_config_v31# ip vrf forwarding vpn1

Switch_config_v31# ip address 31.0.0.1 255.0.0.0

Switch_config_v31# exit

Switch_config# interface VLAN32

Switch_config_v32# ip vrf forwarding vpn2

Switch_config_v32# ip address 32.0.0.1 255.0.0.0

Switch_config_v32# exit

PE에서 EBGP 설정

Switch_config# router bgp 200

Switch_config_bgp# bgp log-neighbor-changes

VPN1에 대한 BGP 구성

Switch_config_bgp# address-family ipv4 vrf vpn1

Switch_config_bgp_vpn1# no synchronization

Switch_config_bgp_vpn1# neighbor 21.0.0.2 remote-as 100

Switch_config_bgp_vpn1# neighbor 31.0.0.2 remote-as 300

Switch_config_bgp_vpn1# exit-address-family

VPN2에 대한 BGP 구성

Switch_config_bgp# address-family ipv4 vrf vpn2

Switch_config_bgp_vpn2# no synchronization

Switch_config_bgp_vpn2# neighbor 22.0.0.2 remote-as 100

Switch_config_bgp_vpn2# neighbor 32.0.0.2 remote-as 300

Switch_config_bgp_vpn2# exit-address-family

Switch_config_bgp# exit

VLAN 생성 및 서브넷 라우팅 포워딩 활성화

Switch_config# vlan 1,21-22,31-32

Switch_config# ip exf

VRF는 PE에서 VPN1 및 VPN2를 구분하기 위해 설정됩니다. BGP는 PE와 CE 간 및 PE와 S2 간의 라우트를 설정하는 데 사용됩니다.

VLAN21 및 VLAN22는 S1과 PE 간의 인터페이스이며, VLAN31 및 VLAN32는 S2와 PE 간 인터페이스입니다. ip exf 명령을 사용하여 서브넷 라우팅 전달을 활성화하고 하드웨어 기반 IP 라우팅을 지원합니다.

이 설정을 통해 PE는 다중 VPN을 처리하고, CE와의 연결성을 유지하며 VRF 기반 라우팅을 수행합니다.

- MCE-S2 구성

VPN1 및 VPN2에 대한 VRF를 생성하고 RD 및 RT를 설정합니다.

Switch# config

Switch_config# ip vrf vpn1

Switch_config_vrf_vpn1# rd 300:1

Switch_config_vrf_vpn1# route-target export 300:1

Switch_config_vrf_vpn1# route-target import 300:1

Switch_config_vrf_vpn1# exit

Switch_config# ip vrf vpn2

Switch_config_vrf_vpn2# rd 300:2

Switch_config_vrf_vpn2# route-target export 300:2

Switch_config_vrf_vpn2# route-target import 300:2

Switch_config_vrf_vpn2# exit

루프백 인터페이스를 구성하고, BGP 프로토콜의 라우터 ID로 사용할 IP 주소를 설정합니다.

Switch_config# interface loopback 0

Switch_config_l0# ip address 103.0.0.1 255.255.255.255

Switch_config_l0# exit

물리 인터페이스 설정

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 41

Switch_config_g0/1# exit

Switch_config# interface gigaEthernet 0/3

Switch_config_g0/3# switchport pvid 46

Switch_config_g0/3# exit

Switch_config# interface gigaEthernet 0/2

Switch_config_g0/2# switchport mode trunk

Switch_config_g0/2# exit

L3 VLAN 포트 설정 및 VRF 바인딩

Switch_config# interface VLAN41

Switch_config_v41# ip vrf forwarding vpn1

Switch_config_v41# ip address 41.0.0.1 255.0.0.0

Switch_config_v41# exit

Switch_config# interface VLAN46

Switch_config_v46# ip vrf forwarding vpn2

Switch_config_v46# ip address 46.0.0.1 255.0.0.0

Switch_config_v46# exit

Switch_config# interface VLAN31

Switch_config_v31# ip vrf forwarding vpn1

Switch_config_v31# ip address 31.0.0.2 255.0.0.0

Switch_config_v31# exit

Switch_config# interface VLAN32

Switch_config_v32# ip vrf forwarding vpn2

Switch_config_v32# ip address 32.0.0.2 255.0.0.0

Switch_config_v32# exit

OSPF 라우트 설정

Switch_config# router ospf 1 vrf vpn1

Switch_config_ospf_1# network 41.0.0.0 255.0.0.0 area 0

Switch_config_ospf_1# redistribute bgp 300

Switch_config_ospf_1# exit

Switch_config# router ospf 2 vrf vpn2

Switch_config_ospf_2# network 46.0.0.0 255.0.0.0 area 0

Switch_config_ospf_2# redistribute bgp 300

Switch_config_ospf_2# exit

PE와 CE 간 EBGP 구성

Switch_config# router bgp 300

Switch_config_bgp# bgp log-neighbor-changes

Switch_config_bgp# address-family ipv4 vrf vpn1

Switch_config_bgp_vpn1# no synchronization

Switch_config_bgp_vpn1# redistribute ospf 1

Switch_config_bgp_vpn1# neighbor 31.0.0.1 remote-as 200

Switch_config_bgp_vpn1# exit-address-family

Switch_config_bgp# address-family ipv4 vrf vpn2

Switch_config_bgp_vpn2# no synchronization

Switch_config_bgp_vpn2# redistribute ospf 2

Switch_config_bgp_vpn2# neighbor 32.0.0.1 remote-as 200

Switch_config_bgp_vpn2# exit-address-family

Switch_config_bgp# exit

Switch_config# vlan 1,31-32,41,46

Switch_config# ip exf

- S22 구성

CE의 G0/1 포트를 VLAN46에 할당하고, S22와 S2를 F0/1 인터페이스를 통해 연결합니다.

Switch_config# interface gigaEthernet 0/1

Switch_config_g0/1# switchport pvid 46

Switch_config_g0/1# exit

VLAN46 인터페이스에 IP 주소를 설정합니다.

Switch_config# interface VLAN46

Switch_config_v46# ip address 46.0.0.2 255.0.0.0

Switch_config_v46# exit

OSPF 103 프로세스를 설정하고, VLAN46 네트워크를 OSPF 영역 0에 추가합니다.

Switch_config# router ospf 103

Switch_config_ospf_103# network 46.0.0.0 255.0.0.0 area 0

Switch_config_ospf_103# exit

- VRF 연결성 테스트

S1에서 VPN1의 VRF를 사용해 S11(11.0.0.2)로 PING을 실행하여 연결성을 확인합니다.

Switch# ping -vrf vpn1 11.0.0.2

!!!!!

--- 11.0.0.2 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 0/0/0 ms

결과 설명:

PING 패킷 5개가 전송 및 수신되었으며, 패킷 손실이 없습니다.

S1과 S11 간 VRF 연결성이 정상적으로 작동하고 있습니다.

S1에서 VPN1의 VRF를 사용해 PE(21.0.0.1)로 PING을 실행하여 연결성을 확인합니다.

Switch# ping -vrf vpn1 21.0.0.1

!!!!!

--- 21.0.0.1 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 0/0/0 ms

31.1 Static 라우팅 구성

Static 라우팅은 관리자가 직접 설정하는 특별한 라우팅 구성입니다. 구조가 비교적 단순한 네트워크에서는 네트워크 상호 운용성을 위해 Static 라우트를 설정하는 것만으로 충분합니다.

Static 라우트를 적절히 설정하고 사용하면 네트워크 성능을 향상시킬 수 있으며, 중요한 네트워크 애플리케이션에 대역폭을 보장할 수 있습니다.

Static 라우팅의 단점은 네트워크 토폴로지 변경에 자동으로 적응하지 못한다는 점입니다.

네트워크 장애 또는 토폴로지 변경이 발생하면 라우트가 도달할 수 없게 되어 네트워크가 중단될 수 있습니다.

이 경우 관리자가 직접 Static 라우트 구성을 수정해야 합니다.

기본 경로(Default Route) 는 라우터가 일치하는 라우팅 테이블 항목을 찾을 수 없을 때 사용됩니다.

- 패킷의 목적지 주소가 라우팅 테이블의 어떤 항목과도 일치하지 않으면, 기본 경로를 선택합니다.
- 기본 경로가 없고, 패킷의 목적지가 라우팅 테이블에 존재하지 않을 경우, 해당 패킷은 폐기됩니다.

기본 경로는 Static 라우트로 설정할 수 있으며, 네트워크 0.0.0.0/0의 형태로 라우팅 테이블에 나타납니다.

31.2 Static 라우팅 구성 작업 목록

Static 라우팅을 구성하려면 다음 작업이 필요합니다.

- 관련 인터페이스의 물리적 매개변수 구성
- 관련 인터페이스의 링크 계층 속성 구성
- 관련 인터페이스의 IP 주소 구성

31.2.1 Static 라우팅 구성

Static 라우팅을 활성화하려면 글로벌 구성 모드에서 다음 단계를 수행해야 합니다.

명령어	설명
ip route *A.B.C.D mask* {next-hop | interface} [distance] [tag tag] [global] [description]	Static 라우트 구성

31.2.2 Static 라우팅 구성 예제

네트워크 세그먼트 10.0.0.0/8으로 패킷을 전달하는 포트가 interface vlan 1인 경우,
구성 명령어는 다음과 같습니다.

ip route 10.0.0.0 255.0.0.0 vlan 1

31.3 RIP 구성

경로 정보 프로토콜(Route Information Protocol, RIP)은 비교적 오래되었지만 여전히 많이 사용되는 내부 게이트웨이 프로토콜(Interior Gateway Protocol, IGP)입니다. 주로 소규모 네트워크에서 사용됩니다. RIP는 전통적인 거리 벡터 라우팅 프로토콜(Distance Vector Routing Protocol)로, RFC 1058에 정의되어 있습니다.

RIP는 UDP 패킷을 브로드캐스트하여 라우팅 정보를 교환합니다. 라우터는 30초마다 라우팅 정보를 업데이트하여 전송합니다.
만약 180초 이내에 인접 라우터로부터 업데이트 정보가 수신되지 않으면, 해당 인접 라우터에서 온 라우팅 테이블 내 경로는 '사용 불가(Unusable)'로 표시됩니다.
그 후 추가로 120초 동안 업데이트가 수신되지 않으면, 해당 경로는 라우팅 테이블에서 삭제됩니다. RIP는 홉 카운트(Hop Count)를 메트릭(metric)으로 사용하여 경로를 측정합니다. 홉 카운트는 출발지에서 목적지까지 패킷이 통과하는 라우터의 수를 나타냅니다. 네트워크에 직접 연결된 경로의 메트릭 값은 '0'이며, 도달할 수 없는 네트워크의 메트릭 값은 '16'입니다.
RIP에서 사용되는 메트릭 범위는 상대적으로 작기 때문에 대규모 네트워크에는 적합하지 않습니다. 라우터에 기본 경로(Default Route)가 설정된 경우, RIP는 0.0.0.0이라는 가상 네트워크로 해당 경로를 광고합니다. 사실, 0.0.0.0 네트워크는 존재하지 않으며, RIP에서 기본 경로 기능을 실현하기 위해 사용됩니다.
RIP가 기본 경로를 학습했거나, 라우터에서 기본 게이트웨이가 설정되어 있고 기본 메트릭이 구성된 경우, 라우터는 기본 네트워크를 광고합니다.

RIP는 지정된 네트워크 인터페이스에 업데이트를 전송합니다. 해당 인터페이스의 네트워크가 지정되지 않은 경우, 해당 네트워크는 RIP 업데이트에서 제외됩니다.

당사 라우터의 RIP-2는 다음 기능을 지원합니다.

- 라우트 요약(Route Summary)
- CIDR(Classless Inter-Domain Routing)
- VLSM(가변 길이 서브넷 마스크)

31.4 RIP 구성 작업 목록

RIP를 구성하려면 다음 작업이 필요합니다. RIP를 활성화하는 것이 첫 번째 작업이며, 나머지는 선택 사항입니다.

- RIP 시작
- RIP 라우트 업데이트 메시지의 유니캐스트 활성화
- 경로 메트릭에 오프셋(offset) 적용

- 타이머 조정
- RIP 버전 번호 지정
- RIP 인증 활성화
- 인터페이스의 'Passive' 및 'Deaf' 기능 활성화
- 라우트 요약 금지
- 출발지 IP 주소 인증 금지
- 스플릿 호라이즌(Split-Horizon) 활성화 또는 비활성화
- RIP 구성 예제

31.4.1 RIP 구성 작업

RIP를 활성화하려면 글로벌 구성 모드에서 다음 단계를 설정하십시오.

명령어	설명
router rip *process-id* [**vrf** *vrf-name*]	RIP 라우팅 프로세스를 활성화하고 라우터 구성 모드에 진입합니다.

RIP 인스턴스가 활성화된 후, 해당 인스턴스와 연관된 인터페이스만 RIP 네트워크 세그먼트를 생성하고 라우팅 정보를 교환할 수 있습니다.
인스턴스를 인터페이스에 연결해야 합니다. 인터페이스 구성 모드에서 아래와 같이 설정합니다.

명령어	설명
router rip *process-id* **enalbe**	인터페이스를 process-id 인스턴스에 연결합니다.

RIP 인스턴스로 인터페이스를 활성화하려면 다음 조건을 충족해야 합니다.

- 인터페이스가 RIP 인스턴스와 연결되어 있어야 합니다.
- 인터페이스에 유효한 IP 주소가 있어야 합니다.
- 인터페이스 상태가 up이어야 합니다.

추가 사항 :

- 인터페이스에서 RIP 인스턴스가 활성화되었을 때, 해당 인스턴스의 VRF와 인터페이스에 지정된 VRF가 일치하지 않으면 해당 인터페이스는 RIP 활성 인터페이스가 될 수 없습니다.
- 인터페이스 VRF를 수정해야 RIP가 정상 작동합니다.

- RIP 인스턴스가 생성되지 않은 상태에서 인터페이스가 RIP 인스턴스와 연결되면, 인터페이스에 지정된 VRF(지정된 경우)와 함께 RIP 인스턴스가 생성됩니다.

제한 사항 :

- 각 인터페이스는 하나의 RIP 인스턴스에만 속할 수 있습니다.

RIP 라우터의 단일 브로드캐스트 업데이트 및 그룹화 허용

RIP는 브로드캐스트 방식의 프로토콜입니다. 라우팅 업데이트가 비브로드캐스트 네트워크에 접근하도록 하려면, 라우터를 구성하여 정보 교환이 가능하도록 설정해야 합니다.

이를 위해 라우터 구성 모드에서 다음 명령어를 사용합니다.

명령어	설명
neighbor *ip-address*	라우팅 정보를 교환할 neighbor 라우터를 정의합니다.

또한, 라우팅 정보를 교환할 수 있는 인터페이스를 제어하려면 ip rip passive 명령어를 사용하여 특정 인터페이스에서 라우팅 업데이트 전송을 차단할 수 있습니다. 필요한 경우, "IP 라우터 구성에서 프로토콜 독립 명령어" 장의 "라우팅 정보 필터링"에서 관련 논의를 참조하십시오.

31.4.2 경로 메트릭에 오프셋 적용

Offset List는 RIP로 학습된 인바운드 및 아웃바운드 경로에 오프셋을 추가하는 데 사용됩니다.
또한, 액세스 리스트 또는 인터페이스를 사용하여 Offset List를 제한할 수 있습니다.
경로 메트릭을 증가시키려면 라우터 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
offset-list {*interface-type number* | * } {**in**|**out**} *access-list-name offset*	경로 메트릭의 오프셋을 늘립니다.

31.4.3 타이머 조정

라우팅 프로토콜은 여러 타이머를 사용하여 라우팅 업데이트 전송 빈도, 라우터가 유효하지 않다고 간주되는 시간 및 기타 매개변수를 결정합니다.

이러한 타이머를 조정하여 라우팅 프로토콜의 성능을 네트워크 요구 사항에 더 적합하게 조정할 수 있습니다.

라우팅 프로토콜을 조정하여 모든 종류의 IP 라우팅 계산에서 수렴 시간을 단축하고, 백업 라우터로 빠르게 전환하여 복구 시간을 최소화할 수 있습니다.

타이머를 조정하려면 라우터 구성 모드에서 다음 명령어를 사용합니다.

명령어	설명
timers holddown *value*	라우팅 테이블에서 특정 경로를 삭제하는 데 걸리는 시간(초 단위)을 조정합니다.
timers expire *value*	라우터가 유효하지 않다고 선언되는 시간(초 단위)을 조정합니다.
timers update *value*	라우터 업데이트 전송 주기(초 단위)를 조정합니다.
timers trigger *value*	트리거 업데이트 간격(초 단위)을 조정합니다.
timers peer *value*	피어 타임아웃 간격(초 단위)을 조정합니다.

31.4.4 RIP 버전 번호 지정

라우터의 RIP-2는 인증(Authentication), 비밀번호 관리, 경로 요약(Route Summary), CIDR 및 VLSM을 지원합니다.
기본적으로 라우터는 RIPv1 및 RIPv2 업데이트를 수신할 수 있으며, RIPv1 업데이트만 전송합니다.
구성을 통해 라우터가 RIPv1 또는 RIPv2 업데이트만 수신 및 전송하도록 설정할 수 있습니다.
이를 위해 라우터 구성 모드에서 다음 명령어를 사용합니다.

명령어	설명
version {1 | 2}	RIPv1 또는 RIPv2의 업데이트만 보내고 받도록 라우터를 구성합니다.

위 작업은 RIP의 기본 동작을 제어하는 명령어입니다. 특정 인터페이스에서 이 기본 동작을 변경하려면 인터페이스 구성 모드에서 다음 명령어를 사용합니다.

RIP-1 또는 RIP-2 업데이트 전송 설정 (인터페이스 모드)

명령어	설명
ip rip send version 1	인터페이스에서 RIPv1 업데이트만 전송하도록 설정합니다.
ip rip send version 2	인터페이스에서 RIPv2 업데이트만 전송하도록 설정합니다.
ip rip send version compatibility	RIPv2 업데이트를 브로드캐스트 방식으로 전송합니다.
ip rip v1demand	요청이 있을 때 RIPv1 패킷을 전송합니다.
ip rip v2demand	요청이 있을 때 RIPv2 패킷을 전송합니다.

RIP-1 및 RIP-2 업데이트 수신 설정 (인터페이스 모드)

명령어	설명

ip rip receive version 1	인터페이스에서 RIPv1 업데이트만 수신하도록 설정합니다.
ip rip receive version 2	인터페이스에서 RIPv2 업데이트만 수신하도록 설정합니다.
ip rip receive version 1 2	인터페이스에서 RIPv1 및 RIPv2 업데이트를 모두 수신하도록 설정합니다.

31.4.5 인터페이스에서 'Passive' 및 'Deaf' 활성화

기본적으로 RIP가 활성화된 인터페이스는 라우팅 업데이트를 송수신할 수 있습니다. RIP 프로토콜을 유연하게 적용하기 위해 인터페이스의 패시브 및 디프 상태를 설정할 수 있습니다. 인터페이스 구성 모드에서 다음 명령어를 사용하여 구성합니다.

명령어	설명
ip rip passive	해당 인터페이스에서 RIP 프로토콜 패킷을 전송하지 않습니다.
ip rip deaf	인터페이스에서 RIP 프로토콜 패킷을 수신하지 않습니다.

31.4.6 RIP 인증 활성화

RIP-1은 인증을 지원하지 않습니다.
RIP-2 패킷을 송수신할 때 인터페이스에서 RIP 인증을 활성화할 수 있습니다.
RIP가 활성화된 인터페이스에서는 여러 인증 모드를 지원합니다.

- 평문(plaintext) 인증
- MD5 인증
- 동적 인증(MD5 및 SHA1)

RIP-2 패킷은 기본적으로 평문 인증을 사용합니다.

참고 : 보안을 고려하는 경우, RIP 패킷에서 평문 인증을 사용하지 않는 것이 좋습니다.
이유는 암호화되지 않은 인증 키가 RIP-2 패킷과 함께 전달되기 때문입니다.
보안이 크게 고려되지 않는 환경(예: 잘못된 설정의 호스트가 라우팅에 참여하지 않는 경우)에서는 평문 인증이 가능합니다.

RIP 평문 인증 구성

인터페이스 구성 모드에서 다음 명령어를 사용합니다.

명령어	설명
ip rip authentication simple	인터페이스에서 평문 인증을 구성합니다.

ip rip password *string*	평문 인증 키를 설정합니다.

RIP MD5 인증 구성

인터페이스 구성 모드에서 다음 명령어를 사용합니다.

명령어	설명
ip rip authentication md5	인터페이스에서 인증을 구성합니다.
ip rip md5-key *key-ID* **md5** *key*	인증 키 및 인증 ID를 설정합니다.

RIP 동적 인증 구성

인터페이스 구성 모드에서 다음 명령어를 사용합니다.

명령어	설명
ip rip authentication dynamic	인터페이스에서 동적 인증 을 구성합니다.
ip rip dynamic-key *key-ID* { **md5 | sha1** } *key xxxx-xx-xx-xx:xx xx:xx*	동적 인증 키와 인증 ID를 구성합니다.

RIP 인증 설정 커밋

RIP 인증을 구성한 후, 인터페이스 구성 모드에서 다음 명령어를 사용하여 설정을 커밋합니다.

명령어	설명
ip rip authentication commit	인증에 실패하면, 피어와 해당 피어에서 학습된 라우트를 무효화합니다.

31.4.7 라우트 요약 금지

기본적으로 RIP-2는 자동 라우트 요약을 지원하여, 분류된 네트워크(Classful Network)의 경계를 넘어설 때 RIP-2 라우트를 요약합니다.
RIP-1은 항상 자동 라우트 요약 기능이 활성화되어 있습니다.

서브넷이 분리된 경우, 해당 서브넷을 알리기 위해 라우트 요약을 금지해야 합니다.
라우트 요약이 금지되면, 분류된 네트워크의 경계를 넘을 때 라우터는 서브넷 및 호스트의 라우트 정보를 전송합니다.

라우터 구성 모드에서 다음 명령어를 사용하여 자동 요약을 금지할 수 있습니다.

명령어	설명
no auto-summary	자동 라우트 요약을 금지합니다.

31.4.8 소스 IP 주소 및 제로-도메인 인증 금지

기본적으로 라우터는 수신된 라우트 업데이트의 소스 IP 주소를 인증합니다. 이 주소가 유효하지 않은 경우, 라우터는 해당 업데이트를 거부합니다. 라우터가 업데이트를 수신해야 하지만, 수신 측에서 해당 "network" 또는 "neighbor" 구성이 없을 경우, 이 기능을 활성화해야 합니다.
하지만 일반적으로 이 명령어는 사용하지 않는 것이 권장됩니다.

라우터 구성 모드에서 다음 명령어를 사용하여 수신 라우트 업데이트에서 소스 IP 주소 인증 기능을 비활성화할 수 있습니다.

소스 IP 주소 인증 금지

명령어	설명
no validate-update-source	수신 RIP 라우터 업데이트의 소스 IP 주소 인증을 금지합니다.

제로-도메인 인증 금지

기본적으로 라우터는 버전 1에서 수신된 라우팅 항목의 제로-도메인을 인증합니다.

해당 필드가 제로-도메인 인증을 통과하지 못하면, 라우팅 항목이 폐기됩니다. 인증이 비활성화된 경우, 피어에서 잘못된 라우팅 정보를 학습할 수 있습니다.

다음 명령어를 사용하여 수신된 RIP 라우터 업데이트의 제로-도메인 인증을 비활성화할 수 있습니다.

명령어	설명
no check-zero-domain	수신된 RIP 라우터 업데이트의 제로-도메인 인증을 금지합니다.

31.4.9 동등 경로의 최대 개수 설정

기본적으로, 로컬 RIP 라우팅 테이블은 최대 4개의 동등 경로(Equivalent Routes)를 포함할 수 있습니다. 나 또는 여러 동일 네트워크 세그먼트에서 여러 neighbor으로부터 라우팅 정보를 학습하여 동등 경로를 생성할 때, 해당 네트워크 세그먼트에서 동등 경로의 수가 현재 최대 개수를 초과하면, RIP 데이터베이스에 추가되지 않습니다.

라우터 구성 모드에서 다음 명령어를 사용하여 로컬 RIP 라우팅 테이블의 동등 경로 최대 개수를 설정합니다.

명령어	설명
maximum-nexthop *number*	RIP 라우팅 테이블의 동등 경로 최대 개수를 설정합니다.

No maximum-nexthop	RIP 라우팅 테이블에서 기본 동등 경로 최대 개수로 복원합니다.

31.4.10 Split-Horizon 활성화 또는 비활성화

일반적으로, IP 네트워크에 연결된 라우터는 거리 벡터 라우팅 프로토콜(Distance Vector Routing Protocol)을 사용할 때, 우팅 루프 가능성을 줄이기 위해 Split-Horizon을 사용합니다. 라우팅 정보가 수신된 인터페이스로 다시 광고되지 않도록 방지합니다. 방식은 여러 라우터 간의 통신(특히 루프가 발생할 가능성이 있을 때)을 최적화합니다. 그러나, 프레임 릴레이(FR)와 같은 비브로드캐스트 네트워크에서는 수평 분할을 비활성화해야 하는 경우가 있습니다.

인터페이스에 보조 IP 주소가 구성된 경우 경로 업데이트의 소스 IP 주소는 모든 보조 IP 주소를 포함하지 않을 수 있습니다.

명령어	설명
ip rip split-horizon {simple | poisoned}	Split-Horizon 활성화
no ip rip split-horizon {simple | poisoned}	Split-Horizon 비활성화

31.4.11 RIP 모니터링 및 유지 관리

RIP를 모니터링 및 유지 관리하면 네트워크 통계 정보를 확인할 수 있습니다.
이 정보에는 RIP 프로토콜 매개변수 설정, 네트워크 활용도, 실시간 네트워크 통신 추적 등이 포함됩니다. 이러한 데이터는 네트워크 리소스 사용 상태를 판단하고, 네트워크 문제를 해결하며, 노드의 가용성을 확인하는 데 도움이 됩니다.

관리 통계 모드에서 다음 명령어를 사용하여 다양한 라우트 통계 정보를 표시할 수 있습니다.

명령어	설명
show ip rip	모든 RIP의 현재 상태를 표시합니다.
Show ip rip *process-id*	지정된 RIP의 현재 상태를 표시합니다.
show ip rip *process-id* **database**	RIP의 모든 라우트를 표시합니다.
show ip rip *process-id* **protocol**	RIP 프로토콜의 관련 정보를 모두 표시합니다.
Show ip rip *process-id* **interface**	지정된 RIP의 모든 인터페이스 및 상태를 표시합니다.
show ip rip *process-id* **peer**	지정된 RIP의 모든 피어(peer) 및 상태를 표시합니다.

관리 모드에서 다음 명령어를 사용하여 라우트 프로토콜 정보를 추적할 수 있습니다.

명령어	설명
debug ip rip database	라우팅 테이블에 삽입, 라우팅 테이블에서 삭제, 경로 변경 등 RIP 라우팅의 절차 정보를 추적합니다.
debug ip rip packet [send | receive]	RIP 프로토콜 메시지를 추적합니다.

debug ip rip message	타이머 시간 초과 등 RIP 이벤트를 추적합니다.

참고 : RIP 프로토콜의 상태 및 동작을 실시간으로 추적하고, 네트워크에서 발생하는 문제를 진단하는 데 매우 유용합니다.

디버그 명령어는 시스템 리소스를 많이 사용할 수 있으므로, 필요한 경우에만 사용하고 완료 후 비활성화하는 것이 좋습니다.

31.4.12 RIP 구성 예제

Router A

interface vlan1

ip address 192.168.20.81 255.255.255.0

ip rip 1 enable

!

interface loopback 0

ip address 10.1.1.1 255.0.0.0

ip rip 1 enable

!

router rip 1

!

Router B

interface vlan1

ip address 192.168.20.82 255.255.255.0

ip rip 1 enable

!

interface loopback 0

ip address 20.1.1.1 255.0.0.0

ip rip 1 enable

!

router rip 1

31.5BEIGRP 동적 라우팅 프로토콜 구성

BEIGRP에서 사용되는 기술은 거리 벡터 라우팅 프로토콜과 유사합니다.

- 라우터는 직접 연결된 neighbor으로부터 제공된 정보만으로 라우팅 결정을 수행합니다.
- 라우터는 자신이 사용하는 라우팅 정보만 직접 연결된 neighbor에게 제공합니다.

하지만, BEIGRP는 거리 벡터 라우팅 프로토콜과 몇 가지 주요 차이점이 있어 더 많은 장점을 제공합니다.

- BEIGRP는 모든 neighbor으로부터 수신한 모든 경로를 토폴로지 테이블에 저장하며, 지금까지의 최적 경로만 저장하는 것은 아닙니다.
- 목적지에 접근할 수 없고 대체 경로가 없는 경우, BEIGRP는 neighbor에게 쿼리를 전송할 수 있습니다.
  이를 통해 BEIGRP의 수렴 속도는 최상의 링크 상태(Link-State) 프로토콜과 경쟁할 수 있습니다.

BEIGRP의 우수성을 보장하는 핵심 기술은 DUAL(Diffused Update Algorithm)입니다.

- DUAL은 항상 적극적으로 작동하며, 목적지에 도달할 수 없고 대체 경로(실현 가능한 대체 경로)가 없는 경우 neighbor에게 쿼리를 보냅니다.
- BEIGRP의 수렴 과정은 소극적으로 타이머 만료를 기다리는 것이 아니라 능동적으로 이루어지기 때문에 수렴 속도가 매우 빠릅니다.

BEIGRP는 EIGRP의 요구 사항에 맞게 설계된 특정 라우팅 프로토콜로, IP에 직접 기반을 두고 있습니다. BEIGRP는 다음 요구 사항을 충족합니다.

- "Hello" 메시지를 통해 새로운 neighbor을 동적으로 발견하고, 기존 neighbor이 사라지는 것을 감지합니다.
- 모든 데이터 전송은 신뢰성을 보장합니다.
- 전송 프로토콜은 유니캐스트 및 멀티캐스트 데이터 전송을 허용합니다.
- 전송 프로토콜 자체가 네트워크 상태 변화와 neighbor의 응답에 적응할 수 있습니다.
- BEIGRP는 필요에 따라 대역폭 점유율을 제한할 수 있습니다.

BEIGRP는 빠른 수렴 속도와 안정성 덕분에 대규모 네트워크에서도 효율적으로 사용될 수 있는 강력한 라우팅 프로토콜입니다.

31.6BEIGRP 구성 작업 목록

BEIGRP 구성을 완료하려면 다음 작업을 수행해야 합니다.

이 중 BEIGRP 활성화는 필수이며, 나머지는 필요에 따라 설정할 수 있습니다.

- BEIGRP 프로토콜 활성화
- 대역폭 공유 비율 설정
- BEIGRP 복합 거리(메트릭) 계산 계수 조정
- "offset"을 사용하여 라우터의 복합 거리 조정
- 자동 요약 비활성화
- 다른 라우트 재배포
- 사용자 정의 라우트 요약
- 기타 BEIGRP 파라미터 구성
- 수평 분할(Split-Horizon) 비활성화
- BEIGRP 모니터링 및 유지 관리

31.6.1 BEIGRP 프로토콜 활성화

BEIGRP 프로세스를 생성하려면 다음 명령어를 실행해야 합니다.

명령어	설명
router beigrp *as-number*	글로벌 구성 모드에서 BEIGRP 프로세스를 추가합니다.
network *network-number network-mask*	라우터 구성 모드에서 해당 BEIGRP 프로세스에 주소를 추가합니다.

구성 완료 후:

- BEIGRP는 해당 주소에 속하는 모든 인터페이스에서 실행됩니다.
- "Hello" 메시지를 통해 새 neighbor을 발견하고, "update"를 통해 초기 라우팅 상호 작용을 수행합니다.

31.6.2 대역폭 공유 비율 설정

기본적으로 BEIGRP는 최대 50%의 대역폭을 사용할 수 있습니다.
다른 데이터의 정상적인 상호 작용을 보장하거나, 실제 상황과 맞지 않는 대역폭을 조정해야 할 경우 이 값을 변경할 수 있습니다.
이와 같은 상황에서 인터페이스 구성 모드에서 다음 명령어를 사용하여 설정합니다.

명령어	설명

31.6.3 BEIGRP 복합 메트릭 계산 계수 조정

특정 상황에서는 BEIGRP 복합 메트릭의 계산 계수를 조정해야 하며, 이는 라우터의 라우팅 정책에 영향을 미칩니다. EIGRP의 기본 계산 계수는 대부분의 네트워크에서 적합하지만, 일부 특정 조건에서는 조정이 필요할 수 있습니다. 그러나 이러한 조정은 네트워크 전반에 큰 변화를 초래할 수 있으므로, 반드시 숙련된 엔지니어가 수행해야 합니다.

라우터 구성 모드에서 다음 명령어를 사용하여 조정합니다.

명령어	설명
metric weights *k1 k2 k3 k4 k5*	EIGRP 복합 메트릭의 계산 계수를 조정합니다.

31.6.4 "Offset"을 사용하여 라우터의 복합 메트릭 조정

Offset List를 사용하여 인바운드 또는 아웃바운드 라우트에 오프셋을 추가할 수 있습니다. 한 특정 조건을 충족하는 라우트의 복합 메트릭만 조정할 수 있습니다. 접근 방식의 목적은 라우터의 라우팅 결과에 영향을 주어, 원하는 결과를 얻는 것입니다. 구성 과정에서, 액세스 리스트 또는 인터페이스를 선택적으로 지정하여 오프셋을 적용할 라우트를 명확히 정의할 수 있습니다.

다음 명령어를 사용하여 오프셋 리스트를 적용합니다.

명령어	설명
offset{*type number* | *} {**in** | **out**} *access-list-name offset*	오프셋 목록을 적용합니다.

31.6.5 자동 요약 비활성화

기본적으로 BEIGRP의 자동 요약(Auto-Summary)은 비활성화되어 있으며, 현재는 지원되지 않습니다.

명령어	설명
no auto-summary	자동 요약 기능을 비활성화합니다.

31.6.6 BEIGRP 프로세스로 다른 라우트 재배포

재배포(redistribute) 작업 규칙:

- 정적(static) 및 연결된(connected) 라우트를 재배포할 때 "default-metric" 명령어를 반드시 구성할 필요는 없습니다.

  관련 파라미터(대역폭, 지연, 신뢰도, 부하, MTU 등)는 해당 인터페이스에서 자동으로 가져옵니다.

- 다른 BEIGRP 프로세스의 라우트를 재배포할 때도 "default-metric" 명령어를 구성할 필요

가 없습니다. 련 파라미터는 재배포된 BEIGRP 프로세스에서 자동으로 가져옵니다.

- RIP, OSPF와 같은 다른 프로토콜의 라우트를 재배포할 경우 "default-metric" 명령어 구성이 필요합니다. 련 파라미터는 "default-metric" 설정을 통해 유효화됩니다. default-metric" 명령어 없이 이러한 라우트를 재배포하면, 재배포가 작동하지 않습니다.

RIP 및 BEIGRP 프로토콜을 동시에 실행하는 라우터에서 RIP 라우트를 BEIGRP 프로토콜로 가져와야 하는 경우, 다음 명령어를 구성해야 합니다.

명령어	설명
default-metric *bandwidth delay reliability loading mtu*	재배포에 필요한 기본 파라미터를 설정합니다.
redistribute *protocol [process]* [**route-map** *name*]	BEIGRP 프로토콜로 라우트를 재배포합니다.

31.6.7 BEIGRP 기타 파라미터 구성

다양한 네트워크 환경에 적응하고 BEIGRP가 보다 효과적이고 완벽하게 작동하도록 하기 위해, 다음과 같은 파라미터를 조정해야 할 수 있습니다.

- BEIGRP가 "hello" 메시지를 전송하는 시간 간격 및 neighbor 라우터의 타임아웃 시간 조정
- 수평 분할(Split-Horizon) 비활성화

① BEIGRP "hello" 메시지 전송 간격 및 neighbor 타임아웃 시간 조정

BEIGRP "hello" 프로토콜은 BEIGRP의 올바른 작동을 보장하기 위해 세 가지 목표를 수행합니다.

- 새로운 neighbor 라우터를 자동으로 발견합니다.
- neighbor의 설정을 확인하고, 호환 모드로 구성된 라우터와만 통신을 허용합니다.
- neighbor의 가용성을 지속적으로 유지하며, neighbor의 사라짐을 감지합니다.

라우터는 BEIGRP가 실행 중인 모든 인터페이스에서 "hello" 멀티캐스트 패킷을 전송합니다.
모든 BEIGRP 지원 라우터는 이러한 멀티캐스트 그룹을 수신하므로 모든 neighbor을 자동으로 발견할 수 있습니다.

- Hello 타이머: 라우터 인터페이스에서 BEIGRP "hello" 메시지를 전송하는 주기를 설정합니다.
- Hold 타이머: 지정된 neighbor으로부터 데이터가 수신되지 않을 경우, neighbor가 비활성 상태로 간주되기까지의 대기 시간을 설정합니다.

neighbor 라우터로부터 BEIGRP 패킷을 수신할 때마다 Hold 타이머는 리셋됩니다.

네트워크 유형 및 대역폭에 따라 "hello" 타이머의 기본값은 달라집니다.

인터페이스 유형		Hello timer (second)	Hold timer (second)
LAN 인터페이스	Any	5	15
WAN 인터페이스	HDLC or PPP	5	15
	NBMA interface, bandwidth<=T1	60	180
	NBMA interface, bandwidth>T1	5	15
	The point-to-point sub-interface of NBMA interface	5	15

Hello 프로토콜에서 타이머의 기본값 차이는 서로 다른 IP 서브넷에 연결된 BEIGRP neighbor들이 서로 다른 hello 및 hold 타이머를 사용할 수 있다는 결과를 초래할 수 있습니다. 이 문제를 해결하기 위해 각 라우터의 hello 패킷은 자체 hold 타이머를 지정하며, 모든 BEIGRP 라우터는 해당 neighbor의 hello 그룹에 지정된 hold 타이머를 사용하여 해당 neighbor의 타임아웃을 결정합니다. 이를 통해 동일한 WAN 토폴로지에서 서로 다른 neighbor 오류 감지 타이머가 나타날 수 있습니다. 그러나 특정 상황에서는 타이머의 기본값이 요구사항을 충족하지 않을 수 있습니다. hello 메시지를 전송하는 시간 간격을 조정하려면 다음 명령어를 사용하십시오:

명령어	설명
ip beigrp hello-interval *seconds*	이 인터페이스에서 hello 메시지를 전송하는 시간 간격 조정

neighbor의 타임아웃 타이머를 조정하려면 다음 명령어를 사용하십시오.

명령어	설명
ip beigrp hold-time *seconds*	neighbor 의 타임아웃 시간을 조정

② 수평 분할(Split-Horizon) 비활성화

일반적으로 split-horizon을 사용합니다. 이는 한 인터페이스에서 얻은 라우팅 정보를 동일한 인터페이스로 다시 브로드캐스트하는 것을 방지하여 라우트 루프(Route Loop)를 방지합니다. 하지만 특정 상황에서는 이것이 최적의 선택이 아닐 수 있으며, 이러한 경우 다음 명령어를 사용하여 split-horizon을 비활성화할 수 있습니다.

명령어	설명
no ip beigrp split-horizon	(Split-Horizon) 비활성화

31.6.8 BEIGRP 모니터링 및 유지 관리

모든 neighbor와의 neighbor십을 초기화하려면 다음 명령어를 사용하십시오:

명령어	설명
clear ip beigrp neighbors [*as-number*	*interface*]	모든 neighbor 와의 neighbor 십 초기화

BEIGRP의 다양한 통계 정보를 확인하려면 다음 명령어를 실행하십시오.

명령어	설명
show ip beigrp interface [*interface*] *[as-number*]	인터페이스 정보 표시
show ip beigrp neighbors [*as-number*	*interface*]	정보 표시
show ip beigrp topology [*as-number*	**all-link	summary	active**]	토폴로지 정보 표시

31.7OSPF 구성

OSPF(Open Shortest Path First)는 IETF의 OSPF 워킹 그룹에서 개발한 IGP(Interior Gateway Protocol) 라우팅 프로토콜입니다. IP 네트워크를 위해 설계된 OSPF는 IP 서브넷 및 외부 라우트 정보 라벨을 지원하며, 메시지 인증과 IP 멀티캐스트를 허용합니다.

당사의 OSPF 구현은 OSPF V2 사양(RFC2328 참조)을 준수합니다. 주요 기능은 다음과 같습니다.

- Stub Area – Stub Area를 지원합니다.
- Route Redistribution – 특정 라우팅 프로토콜에서 형성되고 학습된 모든 라우트는 다른 라우팅 프로토콜 도메인으로 재분배될 수 있습니다.
- autonomous system 내에서 OSPF는 RIP에서 학습한 라우트를 입력할 수 있으며, OSPF에서 학습한 라우트도 RIP으로 재분배될 수 있습니다.
- autonomous system 간에서 OSPF는 BGP에서 학습한 라우트를 입력할 수 있으며, OSPF 라우트도 BGP로 주입될 수 있습니다.
- Authentication – 영역 내 인접 라우터 간에 일반 텍스트(plaintext) 및 MD5 인증을 지원합니다.
- Router Interface Parameters – 설정 가능한 매개변수는 다음과 같습니다:
    ① 송출 비용(outgoing cost)
    ② 재전송 간격(retransmission interval)
    ③ 인터페이스 전송 지연(interface transmission delay)
    ④ 라우터 우선순위(router priority)
    ⑤ 라우터 스위칭 오프 간격(router switching-off interval) 판단
    ⑥ Hello 메시지 간격
    ⑦ 인증 비밀번호(authentication password)
- NSSA Area – RFC 1587 참조
- OSPF – 가상 회선(virtual circuit)에서의 OSPF는 RFC 1793을 참조합니다.

31.8OSPF 구성 작업 목록

OSPF는 하나의 영역(area) 내 모든 라우터, ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router) 간에 라우팅 데이터를 교환해야 합니다. 구성을 단순화하기 위해 인증 없이 기본 매개변수(default parameters)로 모든 라우터를 작동시킬 수 있습니다. 하지만 특정 매개변수를 변경하려는 경우, 모든 라우터에서 해당 매개변수가 동일하게 설정되었는지 확인해야 합니다.

OSPF를 구성하려면 다음 작업을 완료하십시오. OSPF 활성화는 필수이며, 그 외의 구성은 선택 사항입니다.

- OSPF 시작
- OSPF 인터페이스 매개변수 구성
- 네트워크 유형에서의 OSPF 구성
- 일대다 브로드캐스트(one-to-multiple broadcast) 네트워크 구성
- 논브로드캐스트(non-broadcasting) 네트워크 구성
- OSPF 도메인 구성
- OSPF의 NSSA 영역 구성
- OSPF 도메인 내 라우트 요약(route summary) 구성
- 포워드(forward) 라우터의 요약 구성
- 기본(default) 라우트 생성
- LOOPBACK 인터페이스를 통한 라우터 ID 선택
- OSPF의 관리 거리(administrative distance) 구성
- 라우트 계산(timer) 구성
- 온디맨드(on-demand) 링크 구성 활성화
- OSPF의 모니터링 및 유지 관리

또한, 라우트 재분배(route redistribution) 구성에 대해서는 "IP 라우팅 프로토콜의 프로토콜 독립적 기능 구성(Protocol-independent Feather Configurations of IP Routing Protocol)"의 "Route Redistribution" 관련 내용을 참조하십시오.

31.8.1 OSPF 시작

다른 라우팅 프로토콜과 마찬가지로, OSPF를 활성화하려면 OSPF 라우팅 프로세스를 생성하고, 해당 프로세스를 실행할 IP 주소 범위를 할당하며, 해당 IP 주소 범위와 관련된 영역 ID(area ID)를 할당해야 합니다. 글로벌 구성 모드에서 다음 명령어를 사용합니다.

명령어	설명
router ospf *process-id*	OSPF 라우팅 프로토콜을 활성화하고 라우터 구성 모드로 진입합니다.
network *address mask* **area** *area-id*	OSPF 가 실행되는 인터페이스 및 해당 인터페이스의 영역 ID 를 구성합니다.

31.8.2 OSPF 인터페이스 매개변수 구성

OSPF를 구현하는 동안, 필요에 따라 인터페이스와 관련된 OSPF 매개변수를 변경할 수 있습니다. 매개변수를 변경하지 않아도 되지만, 연결된 네트워크의 모든 라우터에서 특정 매개변수가 동일하게 설정되어야 합니다. 인터페이스 구성 모드에서 다음 명령어를 사용하여 인터페이스 매개변수를 구성합니다

명령어	설명
ip ospf authentication	OSPF 인터페이스에서 패킷 송수신을 위한 인증 방식을 구성합니다.
ip ospf cost *cost*	패킷을 포워딩하기 위한 OSPF 인터페이스의 메트릭(metric)을 구성합니다.
ip ospf retransmit-interval *seconds*	동일 OSPF 인터페이스에 속한 neighbor 간에 LSA 재전송에 소요되는 시간을(초 단위로) 구성합니다.
ip ospf transmit-delay *seconds*	OSPF 인터페이스에서 LSA 전송에 소요되는 예상 시간을(초 단위로) 구성합니다.
ip ospf priority *number*	라우터가 DR(Designated Router)이 될 수 있는 우선순위를 구성합니다.
ip ospf hello-interval *seconds*	OSPF 인터페이스에서 hello 패킷을 전송하는 시간 간격을 구성합니다.
ip ospf dead-interval *seconds*	설정된 시간 내에 neighbor 로부터 hello 패킷을 수신하지 못할 경우, 해당 neighbor 를 종료된 것으로 간주합니다.
ip ospf password *key*	OSPF 의 간단한 패스워드 인증을 사용하는 경우, 인접 라우터에 대한 인증 비밀번호를 구성합니다.
ip ospf passive	해당 인터페이스에서 hello 메시지를 전송하지 않도록 설정합니다.
ip ospf mtu-ignore	포트에서 패킷의 MTU 값을 확인하지 않도록 설정합니다.

OSPF 네트워크 유형

OSPF는 네트워크의 물리적 매체를 다음 세 가지 유형으로 나눕니다:

- 브로드캐스트 네트워크(broadcast network) – 이더넷(Ethernet), 토큰 링(Token Ring), FDDI
- 논브로드캐스트 멀티액세스 네트워크(non-broadcast multi-access network) – SMDS, 프레임 릴레이(Frame Relay), X.25
- 포인트 투 포인트 네트워크(point-to-point network) – HDLC, PPP

네트워크를 브로드캐스트 네트워크 또는 논브로드캐스트 멀티액세스 네트워크로 구성할 수 있습니다.

31.8.3 OSPF 네트워크 유형 구성

네트워크의 물리적 매체 유형에 관계없이, 네트워크를 브로드캐스트(broadcasting) 네트워크 또는 논브로드캐스트(non-broadcasting), 멀티액세스(multi-access) 네트워크로 구성할 수 있습니다. 이 기능을 사용하면 물리적 브로드캐스트 네트워크를 논브로드캐스트 멀티액세스 네트워크로, 또는 논브로드캐스트 네트워크(X.25, 프레임 릴레이(Frame Relay), SMDS)를 브로드캐스트 네트워크로 유연하게 구성할 수 있습니다.

이 기능은 neighbor 구성 작업을 줄여줍니다. 자세한 정보는 OSPF 논브로드캐스트 네트워크 구성 관련 내용을 참조하십시오.

논브로드캐스트 멀티액세스 네트워크를 브로드캐스트 네트워크 또는 논브로드캐스트 네트워크로 구성한다는 것은 모든 라우터 간에 가상 링크(virtual link)가 존재한다고 가정하거나, 전체 메시(full-mesh) 네트워크로 구성되어 있다고 가정하는 것입니다. 그러나 비용 문제로 인해 전체 메시 네트워크는 일반적으로 비현실적이며, 부분 메시(partially full-mesh) 네트워크로 구성됩니다. 이러한 경우, 포인트 투 멀티포인트(point-to-multipoint) 네트워크로 구성할 수 있습니다.

인접하지 않은 라우터 간에도 가상 링크를 통해 라우팅 정보를 교환할 수 있습니다.

OSPF 포인트 투 멀티포인트 인터페이스는 여러 포인트 투 포인트(point-to-point) 네트워크 인터페이스로 정의할 수 있으며, 이를 통해 여러 호스트 라우트(host route)를 생성합니다. OSPF 포인트 투 멀티포인트 네트워크는 논브로드캐스트 멀티액세스 네트워크 및 포인트 투 포인트 네트워크에 비해 다음과 같은 이점을 제공합니다:

- 구성이 간단 – neighbor 구성 명령어가 필요하지 않으며, 하나의 IP만 사용하고 DR(Designated Router)을 생성하지 않습니다.
- 비용 절감 – 전체 메시 네트워크 토폴로지가 필요하지 않기 때문에 비용이 절감됩니다.
- 신뢰성 향상 – 가상 링크가 실패하더라도 연결을 유지할 수 있습니다.

인터페이스 구성 모드에서 다음 명령어를 사용하여 OSPF 네트워크 유형을 구성합니다.

명령어	설명
ip ospf network {broadcast | non-broadcast | {point-to-multipoint [non-broadcast] }}	OSPF 라우팅 프로토콜을 활성화하고 라우터 구성 모드로 진입합니다.

이 장의 마지막 부분에서는 OSPF 포인트 투 멀티포인트 네트워크 구성 예제를 확인할 수 있습니다.

31.8.4 일대다 브로드캐스트 네트워크 구성

포인트 투 멀티포인트(point-to-multipoint) 네트워크 및 브로드캐스트(broadcasting) 네트워크에서

는 neighbor 관계를 별도로 설명할 필요가 없습니다. 하지만 특정 neighbor의 우선순위를 지정하려면 neighbor 명령어를 사용할 수 있습니다.

이 명령어를 사용하기 전에, 일부 OSPF 포인트 투 멀티포인트 프로토콜 트래픽은 멀티캐스트(multicast) 트래픽이라는 점을 유의해야 합니다. 따라서 포인트 투 멀티포인트 인터페이스에서는 neighbor 명령어가 필요하지 않습니다. "hello" 패킷, 업데이트 패킷, 확인 패킷은 모두 브로드캐스트 방식으로 전송됩니다. 특히 멀티캐스트 "hello" 패킷은 모든 neighbor를 동적으로 검색할 수 있습니다.

포인트 투 멀티포인트 네트워크에서 라우터는 모든 neighbor가 동일한 메트릭(metric)을 갖는다고 가정합니다. 이 값은 ip ospf cost 명령어를 통해 구성할 수 있습니다. 하지만 실제로는 각 neighbor의 대역폭이 서로 다르기 때문에, 메트릭 값도 다르게 설정해야 합니다. 이 기능은 포인트 투 멀티포인트 인터페이스에만 적용됩니다.

다음 명령어를 사용하여 인터페이스를 포인트 투 멀티포인트 인터페이스로 구성하고 각 neighbor에 메트릭을 할당합니다

명령어	설명
ip ospf network point-to-multipoint	OSPF 라우팅 프로토콜을 활성화하고 라우터 구성 모드로 진입합니다.
exit	글로벌 구성 모드로 돌아갑니다.
router ospf *process-id*	OSPF 라우터 프로세스를 구성하고 라우터 구성 모드로 진입합니다.
neighbor ip-address **cost** number	특정 neighbor 를 지정하고 메트릭을 할당합니다. 메트릭을 지정하려는 각 neighbor에 대해 이 명령어를 반복 실행합니다.

31.8.5 논브로드캐스트 네트워크 구성

OSPF 네트워크에는 여러 라우터가 존재하기 때문에, 네트워크에 하나의 DR(Designated Router)이 선출되어야 합니다. 브로드캐스트 기능이 구성되지 않은 경우, DR 선출 프로세스를 위해 매개변수를 구성해야 합니다.

이 매개변수는 DR 또는 BDR(Backup Designated Router)이 될 수 있는 라우터에서만 구성됩니다.

라우터 구성 모드에서 다음 명령어를 사용하여 논브로드캐스트 네트워크에 연결된 라우터를 구성합니다.

명령어	설명
neighbor *ip-address* [**priority** *number*] [**poll-interval** *seconds*]	논브로드캐스트 네트워크에 연결된 라우터를 구성합니다.

neighbor 라우터에 대해 다음 매개변수를 지정할 수 있습니다:

- neighbor 라우터의 우선순위(priority)
- 논브로드캐스트 폴링 간격(poll interval)
- neighbor에 접근 가능한 인터페이스

포인트 투 멀티포인트(point-to-multipoint) 논브로드캐스트 네트워크에서는 neighbor 명령어를 사용하여 neighbor 관계를 지정하고, 선택적으로 우선순위를 할당할 수 있습니다.

이전 소프트웨어 버전에서는 일부 사용자가 논브로드캐스트 매체(예: IP over ATM)에서 포인트 투 멀티포인트 연결을 구성했습니다. 이 경우, 라우터는 neighbor 라우터를 동적으로 검색할 수 없었습니다. 이 기능을 통해 포인트 투 멀티포인트 인터페이스에서 neighbor 명령어를 사용할 수 있습니다.

포인트 투 멀티포인트 네트워크에서는 라우터가 모든 neighbor가 동일한 메트릭(metric)을 갖는다고 가정합니다. 이 값은 ip ospf cost 명령어를 통해 구성할 수 있습니다. 하지만 실제로 각 neighbor의 대역폭이 다르기 때문에, 메트릭 값도 달라야 합니다. 이 기능은 포인트 투 멀티포인트 인터페이스에만 적용됩니다.

인터페이스 구성 모드에서 다음 명령어를 사용하여 브로드캐스트를 지원하지 않는 매체에서 포인트 투 멀티포인트 인터페이스를 구성합니다:

명령어	설명
ip ospf network point-to-multipoint non-broadcast	브로드캐스트를 지원하지 않는 매체에서 포인트 투 멀티포인트 인터페이스를 구성합니다.
exit	글로벌 구성 모드로 진입합니다.
router ospf *process-id*	OSPF 라우팅 프로세스를 생성하고 라우터 구성 모드로 진입합니다.
neighbor *ip-address* [**cost** *number*]	OSPF neighbor 를 지정하고 메트릭을 할당합니다. 메트릭을 지정하려는 각 neighbor에 대해 이 명령어를 반복 실행합니다.

31.8.6 OSPF 도메인 구성

구성 가능한 영역(area) 매개변수에는 인증(authentication), Stub 영역 지정, 기본 요약 라우트의 메트릭(metric) 지정이 포함됩니다. 인증은 비밀번호 기반 보호 방식을 사용합니다.

Stub 영역은 외부 라우트를 배포하지 않는 영역입니다. 대신 ABR(Area Border Router)이 기본 외부 라우트를 생성하여 Stub 영역에 전달하고, 이를 통해 자율 시스템(AS)의 외부 네트워크에 접근할 수 있도록 합니다. OSPF Stub 기능을 사용하려면 Stub 영역에서 기본 라우트를 사용해야 합니다.

Stub 영역으로 전송되는 LSA(Link-State Advertisement) 수를 추가로 줄이기 위해 ABR에서 요약 LSA(type 3)의 전송을 금지할 수 있습니다. 이를 통해 Stub 영역으로 들어오는 요약 LSA를 줄일 수 있습니다.

라우터 구성 모드에서 다음 명령어를 사용하여 영역 매개변수를 정의합니다:

명령어	설명
area *area-id* **authentication simple**	OSPF 영역 인증 활성화
area *area-id* **authentication message-digest**	OSPF 에서 인증을 사용하도록 설정
area *area-id* **stub [no-summary]**	Stub 영역을 정의
area *area-id* **default-cost** *cost*	tub 영역에서 기본 라우트의 메트릭을 설정

31.8.7 OSPF의 NSSA 영역 구성

NSSA(Not-So-Stubby Area) 영역은 STUB 영역과 유사하지만, 외부 라우트를 허용한다는 점에서 차이가 있습니다. NSSA 영역에서는 라우트 요약(route summary) 및 패킷 필터링(packet filtration)이 전송 중에도 지원됩니다.
ISP가 서로 다른 라우팅 프로토콜을 사용하는 원격 네트워크와 연결해야 하는 경우, NSSA는 관리를 단순화할 수 있습니다.

NSSA가 적용되지 않은 경우, 기업의 코어 경계 라우터는 OSPF의 STUB 영역에서 작동할 수 없습니다. 이는 원격 네트워크의 라우트가 STUB 영역으로 전달될 수 없기 때문입니다.
RIP와 같은 간단한 라우팅 프로토콜은 광고(advertise)될 수 있지만, 두 가지 라우팅 프로토콜을 유지해야 합니다. NSSA를 사용하면 중앙 라우터와 원격 라우터를 동일한 NSSA 영역에 배치할 수 있으며, 이를 통해 원격 네트워크에서도 OSPF를 적용할 수 있습니다.

NSSA 영역을 사용할 경우, ABR(Area Border Router) 라우터가 생성한 라우트는 NSSA가 구성된 후 NSSA 영역으로 들어갈 수 있습니다.
동일한 영역에 있는 모든 라우터는 자신이 NSSA 영역에 속해 있음을 인식해야 하며, 그렇지 않으면 서로 통신할 수 없습니다. 라우터 간 패킷 전송 혼란을 방지하기 위해 ABR에서 적절한 설정을 사용해야 합니다.

라우터 구성 모드에서 다음 명령어를 실행하여 OSPF의 NSSA 영역을 설정합니다.

명령어	설명
Area *area-id* **nssa** [**no-redistribution**][**no-summary**][**default-information-originate**] [**translate-always**]	OSPF NSSA 영역을 구성합니다.

31.8.8 OSPF 도메인 내 라우트 요약 구성

이 기능은 ABR(Area Border Router)이 요약 라우트(summary route)를 다른 영역으로 브로드캐스트하도록 합니다.
OSPF에서는 ABR이 모든 네트워크를 다른 영역으로 브로드캐스트합니다.
네트워크 번호를 일정한 방식으로 할당하고 연속적으로 구성할 수 있다면, ABR이 요약 라우트를 브로드캐스트하도록 설정할 수 있습니다. 요약 라우트는 특정 범위 내의 모든 네트워크를 포함할 수 있습니다.

라우터 구성 모드에서 다음 명령어를 사용하여 주소 범위를 정의합니다.

명령어	설명
area area-id **range** address mask	라우트 요약을 위한 주소 범위를 정의합니다.

31.8.9 포워딩 라우터의 요약 구성

다른 라우터 영역에서 OSPF 라우터 영역으로 라우트를 배포할 때, 각 라우터는 외부 LSA(external LSA) 형태로 독립적인 브로드캐스트를 수행합니다.
그러나 라우터를 구성하여 특정 주소 범위를 포함하는 하나의 라우트를 브로드캐스트하도록 설정할 수 있습니다.
이 방법은 OSPF 링크 상태 데이터베이스(link state database)의 크기를 줄이는 데 도움이 됩니다.

라우터 구성 모드에서 다음 명령어를 사용하여 라우터 요약을 구성합니다

명령어	설명
summary-address *prefix mask* [not advertise]	배포 라우트를 포함하는 주소와 마스크를 설명하고, 하나의 요약 라우트만 브로드캐스트합니다.

31.8.10 기본 라우트 생성

ASBR(Autonomous System Boundary Router)이 OSPF 라우트 영역으로 진입하는 기본 라우트(default route)를 생성하도록 설정할 수 있습니다.
라우터가 OSPF 도메인으로 진입하는 라우트를 배포하도록 구성하면, 해당 라우터는 자동으로 ASBR로 전환됩니다.
그러나 ASBR은 기본적으로 OSPF 라우트 영역으로 진입하는 기본 라우트를 생성하지 않습니다.

라우터 구성 모드에서 다음 명령어를 사용하여 ASBR이 기본 라우트를 강제로 생성하도록 설정합니다

명령어	설명
default-information originate [**always**] [**route-map** *map-name*]	ASBR 이 OSPF 라우트 영역으로 진입하는 기본 라우트를 강제로 생성합니다.

31.8.11 루프백 인터페이스를 통한 라우터 ID 선택

OSPF는 인터페이스에 구성된 가장 큰 IP 주소를 라우터 ID(router ID)로 사용합니다.

이 IP 주소에 연결된 인터페이스가 DOWN 상태로 전환되거나 IP 주소가 삭제되면, OSPF 프로세스는 새로운 라우터 ID를 다시 계산하고 모든 인터페이스에서 라우팅 정보를 재전송합니다.

루프백(loopback) 인터페이스에 IP 주소를 구성하면, 해당 IP 주소가 라우터 ID로 사용됩니다. 루프백 인터페이스는 DOWN 상태가 되지 않기 때문에 라우팅 테이블이 보다 안정적으로 유지됩니다.

라우터는 가능하면 루프백 인터페이스를 라우터 ID로 사용하며, 모든 루프백 인터페이스 중 가장 큰 IP 주소를 라우터 ID로 선택합니다. 루프백 인터페이스가 없는 경우, 라우터에서 가장 큰 IP 주소를 사용합니다. 특정 인터페이스를 OSPF 라우터 ID로 지정할 수는 없습니다.

글로벌 모드에서 다음 명령어를 사용하여 IP 루프백 인터페이스를 구성합니다.

명령어	설명
interface loopback 0	루프백 인터페이스를 생성하고 인터페이스 구성 모드로 진입합니다.
ip address *ip-address mask*	인터페이스에 IP 주소를 할당합니다.

31.8.12 OSPF 관리 거리 구성

관리 거리(management distance)는 라우팅 정보 소스(예: 라우터 또는 라우터 그룹)의 신뢰 수준을 정의합니다. 일반적으로 관리 거리는 0~255 사이의 정수이며, 값이 높을수록 신뢰 수준이 낮아집니다. 관리 거리가 255인 경우, 해당 라우트 정보 소스는 신뢰할 수 없으며 무시됩니다.

OSPF는 세 가지 관리 거리를 사용합니다:

- intra-area – 영역 내 라우트
- inter-area – 다른 영역으로의 라우트
- external – 다른 라우팅 프로토콜 도메인에서 배포된 라우트

각 라우트 유형의 기본값은 110입니다. 라우터 구성 모드에서 다음 명령어를 사용하여 OSPF의 관리 거리 값을 구성합니다

명령어	설명
distance ospf [**intra-area** *dist1*] [inter-area *dist2*] [**external** *dist3*]	OSPF 의 intra-area, inter-area 및 external 라우트의 관리 거리 값을 변경합니다.

31.8.13 라우트 계산 타이머 구성

OSPF는 토폴로지 변화 정보를 수신한 후 SPF(Shortest Path First) 계산을 시작하기까지의 지연 시

간을 설정할 수 있습니다. 또한, 연속적인 SPF 계산 간의 최소 시간 간격도 구성할 수 있습니다.

라우터 구성 모드에서 다음 명령어를 사용하여 타이머를 설정합니다.

명령어	설명
timers delay *delaytime*	영역 내 라우트 계산의 지연 시간을 설정합니다.
timers hold *holdtime*	영역 내 라우트 계산 간의 최소 시간 간격을 설정합니다.

31.8.14 온디맨드 링크(On-Demand Link) 구성

온디맨드 회선(on-demand circuits)에서의 OSPF는 OSPF 프로토콜을 업그레이드하여, 온디맨드 다이얼링(on-demand dialing) 네트워크 환경에서 더 효율적으로 작동하도록 합니다.
OSPF 프로토콜은 처음 연결이 설정되거나 패킷에 포함된 정보가 변경된 후, 연결된 라우터 간에 정기적으로 HELLO 패킷과 링크 상태 브로드캐스트 갱신 패킷을 교환합니다.
이는 토폴로지가 실제로 변경될 때만 최소 스패닝 트리(minimum spanning tree)가 다시 계산되고 패킷이 전송됨을 의미합니다.

라우터 간 연결이 포인트 투 포인트(point-to-point) 방식인 경우, 한쪽 터미널에서만 구성을 수행해야 합니다. 반대편 터미널의 라우터도 이 기능을 지원해야 합니다.
라우터 간 연결이 포인트 투 멀티포인트(point-to-multipoint) 방식인 경우, 멀티포인트 터미널에서 구성을 수행해야 합니다.

온디맨드 다이얼링은 STUB 영역에서 구성하는 것이 권장됩니다. STUB 영역의 각 라우터에 이 속성이 구성되어 있다면, STUB 영역 외부의 라우터는 온디맨드 다이얼링을 지원하지 않아도 됩니다. 표준 영역에 온디맨드 다이얼링이 구성된 경우, 다른 표준 영역도 이 기능을 지원해야 합니다. 이는 두 번째 유형의 외부 링크 상태 브로드캐스트 패킷이 모든 영역으로 브로드캐스트되기 때문입니다.

브로드캐스트 기반 네트워크에서 이 기능이 구성되면, 링크 상태 브로드캐스트 패킷은 제한되지만 HELLO 패킷은 제한되지 않습니다.
HELLO 패킷은 neighbor 관계를 유지하고 DR(Designated Router)을 선출하는 데 사용되기 때문입니다.

인터페이스 모드에서 다음 명령어를 실행하여 OSPF 온디맨드 다이얼링을 구성합니다:

명령어	설명
ip ospf demand-circuit	OSPF 온디맨드 다이얼링을 구성합니다.

31.8.15 OSPF 모니터링 및 유지 관리

OSPF는 네트워크의 통계 정보를 표시할 수 있으며, IP 라우팅 테이블, 캐시, 데이터베이스 등의

내용을 포함합니다.
이 정보는 네트워크 자원의 활용도를 판단하고, 네트워크 문제를 해결하는 데 도움이 됩니다.
네트워크 노드의 가용성을 파악하고, 데이터 패킷이 네트워크를 통해 전달되는 경로를 확인할 수 있습니다.

다음 명령어를 사용하여 다양한 라우팅 통계 정보를 확인할 수 있습니다

명령어	설명
show ip ospf [*process-id*]	OSPF 라우팅 프로세스의 일반 정보를 표시합니다.
show ip ospf [*process-id*] **database**[**router**| **network**| **summary**| **asbr-summary**| **external**| **database-summary**]{ *link-state-id*| **self-originate**| **adv-router** [*ip-address*]}	OSPF 데이터베이스에 대한 관련 정보를 표시합니다.
show ip ospf border-routers	ABR 및 ASBR 의 내부 라우팅 테이블 항목을 표시합니다.
show ip ospf interface	OSPF 인터페이스 정보를 표시합니다.
show ip ospf neighbor	인터페이스별 OSPF neighbor 정보를 표시합니다.
debug ip ospf adj	OSPF 인접성(adjacent) 설정 과정을 모니터링합니다.
debug ip ospf events	OSPF 인터페이스 및 neighbor 이벤트를 모니터링합니다.
debug ip ospf flood	OSPF 데이터베이스의 플러딩(flooding) 과정을 모니터링합니다.
debug ip ospf lsa-generation	OSPF LSA(링크 상태 광고) 생성 과정을 모니터링합니다.
debug ip ospf packet	OSPF 패킷 메시지를 모니터링합니다.
debug ip ospf retransmission	OSPF 패킷 재전송 과정을 모니터링합니다.
debug ip ospf spf [**intra**| **external**]	OSPF 의 SPF 계산 경로를 감독합니다.
debug ip ospf tree	OSPF SPF 트리(tree) 생성 과정을 모니터링합니다.

31.8.16 OSPF 포인트 투 멀티포인트 논브로드캐스트 구성 예제

Switch A

interface vlan 1

ip address 10.0.1.1 255.255.255.0

ip ospf network point-to-multipoint non-broadcast

!

router ospf 1

network 10.0.1.0 255.0.0.0 area 0

neighbor 10.0.1.3 cost 5

neighbor 10.0.1.4 cost 10

Switch B

interface vlan 1

ip address 10.0.1.3 255.255.255.0

ip ospf network point-to-multipoint non-broadcast

!

router ospf 1

network 10.0.1.0 255.0.0.0 area 0

neighbor 10.0.1.1

neighbor 10.0.1.4 cost 14

Switch C

interface vlan 1

ip address 10.0.1.4 255.255.255.0

ip ospf network point-to-multipoint non-broadcast

!

router ospf 1

network 10.0.1.0 255.0.0.0 area 0

neighbor 10.0.1.1

neighbor 10.0.1.3

31.8.17 가변 길이 서브넷 마스크(VLSM) 구성 예제

OSPF와 정적 라우팅(static routing)은 가변 길이 서브넷 마스크(VLSM, Variable-Length Subnet Mask)를 지원합니다.
VLSM을 사용하면 동일한 네트워크 번호에 대해 서로 다른 인터페이스에서 서로 다른 서브넷 마스크를 사용할 수 있습니다.
이를 통해 IP 주소를 절약하고 네트워크 주소 공간을 보다 효율적으로 사용할 수 있습니다.

다음 예제에서는 30비트 서브넷 마스크를 사용하여 직렬 포트(serial port)의 호스트 주소로 2비트 주소 공간을 예약합니다.
이는 두 개의 호스트 주소가 필요한 포인트 투 포인트(point-to-point) 직렬 링크에 적합합니다.

```
interface vlan 1
ip address 131.107.1.1 255.255.255.0
!
interface serial 1/1
ip address 131.107.254.1 255.255.255.252
!
router ospf 107
network 131.107.0.0 255.255.0.0 area 0.0.0.0
```

31.8.18 OSPF 라우트 및 라우트 재분배 구성 예제

OSPF는 여러 내부 라우터(internal router), ABR(Area Border Router), ASBR(Autonomous System Boundary Router) 간에 정보를 교환해야 합니다.
최소 구성으로도 OSPF 기반 라우터는 기본 매개변수(default parameters)로 작동할 수 있으며, 인증(authentication)이 필요하지 않습니다.

다음은 세 가지 구성 예제입니다:

- 첫 번째 예제는 기본 OSPF 명령어를 연습합니다.
- 두 번째 예제는 하나의 OSPF 자율 시스템(AS) 내에서 내부 라우터, ABR 및 ASBR 구성을 보여줍니다.
- 세 번째 예제는 다양한 OSPF 도구를 사용한 보다 복잡한 구성 사례를 설명합니다.

기본 OSPF 구성 예제

다음 예제는 간단한 OSPF 구성을 보여줍니다.
라우팅 프로세스 90을 활성화하고, VLAN 1을 OSPF 영역 0.0.0.0에 연결합니다.
동시에 RIP를 OSPF로, OSPF를 RIP로 재분배(redistribute)합니다.

```
interface vlan 1
 ip address 130.130.1.1 255.255.255.0
!
router ospf 90
```

```
network 130.130.0.0 255.255.0.0 area 0
redistribute rip 1
!
router rip 1
redistribute ospf 90
```

내부 라우터, ABR 및 ASBR의 기본 구성 예제

영역 10.9.50.0, 2, 3의 마스크는 특정 주소 범위를 지정하지만, 영역 0은 모든 네트워크를 포함합니다.

```
router ospf 109
 network 131.108.20.0 255.255.255.0 area 10.9.50.0
 network 131.108.0.0 255.255.0.0 area 2
 network 131.109.10.0 255.255.255.0 area 3
 network 0.0.0.0 0.0.0.0 area 0
 redistribute static
!
interface vlan 1
ip address 131.108.20.5 255.255.255.0
!
interface vlan 2
ip address 131.108.1.5 255.255.255.0
!
interface vlan 3
ip address 131.108.2.5 255.255.255.0
!
interface vlan 4
 ip address 131.109.10.5 255.255.255.0
!
interface vlan 5
```

ip address 131.109.1.1 255.255.255.0

!

interface vlan 6

ip address 10.1.0.1 255.255.0.0

!

ip route 44.0.0.0 255.0.0.0 VLAN1

구성 명령어 설명

- 네트워크 영역 구성 명령어는 순차적으로 실행됩니다. 따라서 명령어의 순서가 중요합니다.
- 라우터는 각 인터페이스의 주소/마스크 쌍을 순서대로 매칭합니다.
- 자세한 정보는 "OSPF 명령어"의 관련 네트워크 프로토콜 명령어 참조 내용을 확인하십시오.

영역 구성 과정 설명

- 첫 번째 네트워크 영역에서는 영역 ID 10.9.50.0이 인터페이스 서브넷 마스크 131.108.20.0과 함께 구성됩니다.
  따라서 VLAN 1이 매칭되며, VLAN 1은 영역 10.9.50.0에 속하게 됩니다.
- 두 번째 영역에서는 VLAN 1을 제외하고 다른 인터페이스에 대해 동일한 과정을 적용합니다.
  이 과정에서 VLAN 2가 매칭되며, VLAN 2는 영역 2에 연결됩니다.
- 나머지 네트워크 영역에 대해서도 계속해서 매칭이 진행됩니다.

주의: 마지막 네트워크 영역 명령어는 특수한 경우입니다. 이 명령어는 나머지 인터페이스가 모두 영역 0에 연결됨을 의미합니다.

가상 링크 구성 예제

다음 그림을 기준으로 라우터를 구성합니다

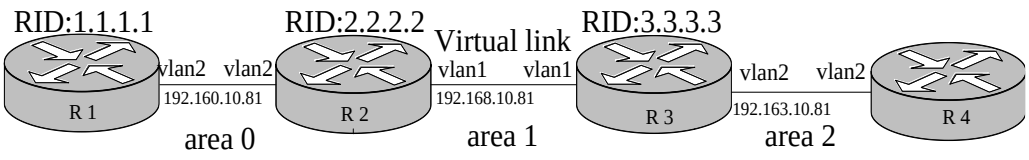


그림 55 네트워크 토폴로지

R1

interface vlan 2

ip address 192.160.10.81 255.255.255.0

!

router ospf 1

router-id 1.1.1.1

network 192.160.10.81 255.255.255.0 area 0

R2

interface vlan 1

ip address 192.168.10.81 255.255.255.0

!

interface vlan 2

ip address 192.160.10.82 255.255.255.0

!

router ospf 192

router-id 2.2.2.2

network 192.168.10.81 255.255.255.0 area 1

network 192.160.10.82 255.255.255.0 area 0

area 1 virtual-link 3.3.3.3

R3

interface vlan 1

ip address 192.168.10.82 255.255.255.0

!

interface vlan 2

ip address 192.163.10.81 255.255.255.0

!

router ospf 192

router-id 3.3.3.3

network 192.168.10.82 255.255.255.0 area 1

network 192.163.10.81 255.255.255.0 area 2

area 1 virtual-link 2.2.2.2

복합 OSPF ABR 라우터 구성 예제

다음 예제는 ABR(Area Border Router) 구성에서 수행해야 할 여러 작업을 보여줍니다.
구성 작업은 다음 두 가지로 나뉩니다.

- 기본 OSPF 구성
- 라우트 재분배

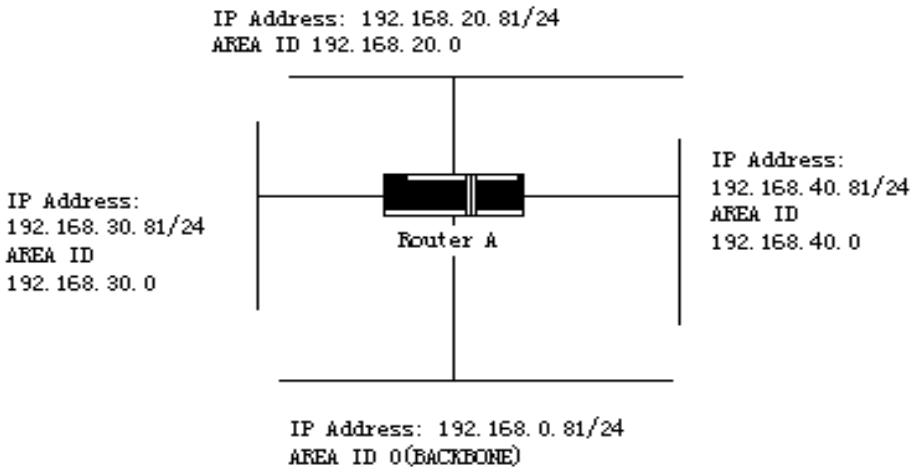


그림 56 네트워크 주소의 범위 및 할당

구성 작업 개요

- 기본 OSPF 구성:
  - ① VLAN 1~4의 주소 범위 설정
  - ② 각 인터페이스에서 OSPF 활성화
  - ③ 각 영역 및 네트워크에 OSPF 인증 비밀번호 설정
  - ④ 링크 상태 가중치(link state weight) 및 기타 인터페이스 매개변수 설정
  - ⑤ Stub 영역에서 36.0.0.0 생성 (인증 및 stub 영역 매개변수 설정은 area 명령어를 사용)
  - ⑥ 백본 영역(Area 0) 설정
- 라우트 재분배:

① IGRP 및 RIP 라우트를 OSPF로 재분배 (metric-type, metric, tag, subnet 포함)

② IGRP 및 OSPF 라우트를 RIP으로 재분배

```
interface vlan 1
 ip address 192.168.20.81 255.255.255.0
 ip ospf password GHGHGHG
 ip ospf cost 10
!
interface vlan 2
ip address 192.168.30.81 255.255.255.0
ip ospf password ijklmnop
ip ospf cost 20
ip ospf retransmit-interval 10
ip ospf transmit-delay 2
ip ospf priority 4
!
interface vlan 3
ip address 192.168.40.81 255.255.255.0
ip ospf password abcdefgh
ip ospf cost 10
!
interface vlan 4
ip address 192.168.0.81 255.255.255.0
ip ospf password ijklmnop
ip ospf cost 20
 ip ospf dead-interval 80
!
router ospf 192
network 192.168.0.0 255.255.255.0 area 0
network 192.168.20.0 255.255.255.0 area 192.168.20.0
```

network 192.168.30.0 255.255.255.0 area 192.168.30.0

network 192.168.40.0 255.255.255.0 area 192.168.40.0

area 0 authentication simple

area 192.168.20.0 stub

area 192.168.20.0 authentication simple

area 192.168.20.0 default-cost 20

area 192.168.20.0 authentication simple

area 192.168.20.0 range 36.0.0.0 255.0.0.0

area 192.168.30.0 range 192.42.110.0 255.255.255.0

area 0 range 130.0.0.0 255.0.0.0

area 0 range 141.0.0.0 255.0.0.0

redistribute rip 1

!

router rip 1

redistribute ospf 192

31.9OSPFv3 구성

OSPFv3(Open Shortest Path First version 3)는 IETF의 OSPF 워킹 그룹에서 IPv6 네트워크를 위해 개발한 IGP(Interior Gateway Protocol) 라우팅 프로토콜입니다.

OSPFv3는 IPv6 서브넷, 외부 라우팅 정보의 마크, 그리고 패킷 인증을 지원합니다.

OSPFv3와 OSPFv2의 공통점

- 라우터 ID 및 영역 ID는 32비트입니다.
- 동일한 유형의 패킷을 사용합니다.
- Hello 패킷, DD(Database Description) 패킷, LSR(Link State Request) 패킷, LSU(Link State Update) 패킷, LSAck(Link State Acknowledgment) 패킷
- Neighbor 검색 및 이웃 생성 메커니즘이 동일합니다.
- LSA 확장 메커니즘 및 LSA 에이징 메커니즘이 동일합니다.

OSPFv3와 OSPFv2의 주요 차이점

- OSPFv3는 링크 기반으로 동작, OSPFv2는 네트워크 세그먼트 기반으로 동작합니다.
- OSPFv3는 동일한 링크에서 여러 인스턴스를 실행할 수 있습니다.
- OSPFv3는 라우터 ID를 통해 이웃을 식별하지만, OSPFv2는 IP 주소를 통해 이웃을 식별합니다.
- OSPFv3는 7가지 클래스의 LSA를 정의합니다.

주요속성	설명
Stub domain	스텁 도메인을 지원합니다.
Route forwarding	모든 라우팅 프로토콜에서 학습하거나 생성된 경로가 다른 라우팅 프로토콜의 도메인으로 전달될 수 있음을 의미합니다. 자율 도메인에서 OSPFv3가 RIPng에서 학습한 경로를 입력할 수 있음을 의미합니다. OSPFv3에서 학습한 경로도 RIPng로 내보낼 수 있습니다. 자율 도메인 사이에서 OSPFv3는 BGP에서 학습한 경로를 가져올 수 있습니다.
Parameters of a routing interface	OSPFv3 경로도 BGP로 내보낼 수 있습니다. 다음은 구성 가능한 인터페이스 매개변수입니다. 출력 비용, 재전송 간격, 인터페이스의 전송 지연, 라우터의 우선 순위, 라우터 종료 판단 간격, 헬로 간격, 인증 키.
Virtual link	가상 링크를 지원합니다.

31.10 OSPFv3 구성 작업 목록

OSPFv3는 도메인 내 라우터, ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router) 간의 라우팅 데이터 전환을 요구합니다.
설정을 단순화하기 위해, 관련 구성을 수행하여 인증 없이 기본 매개변수로 작동하도록 할 수 있습니다.
그러나 특정 매개변수를 변경하려면, 모든 라우터에서 동일한 매개변수를 사용해야 합니다.

OSPFv3를 설정하려면 다음 작업을 수행해야 합니다.
OSPFv3 활성화는 필수 작업이며, 다른 설정은 선택 사항입니다.

- OSPFv3 활성화
- OSPFv3 인터페이스 매개변수 설정
- 다양한 물리적 네트워크에서 OSPFv3 설정
- OSPFv3 도메인의 매개변수 설정
- OSPFv3의 NSSA(Not-So-Stubby Area) 도메인 구성
- OSPFv3 도메인에서 경로 요약(Route Summary) 설정
- 포워딩 경로 요약 설정
- 기본 경로(Static Default Route) 생성
- 루프백 인터페이스에서 라우터 ID 선택
- OSPFv3 관리 거리(Administrative Distance) 설정
- 라우팅 알고리즘 타이머 설정
- OSPFv3 모니터링 및 유지 관리

31.10.1 OSPFv3 활성화

OSPFv3를 활성화하기 전에 IPv6 패킷 포워딩 기능을 먼저 활성화해야 합니다.

OSPFv3를 활성화하려면 OSPFv3 라우팅 프로세스를 생성하고, 해당 프로세스의 라우터 ID를 지정한 후, 인터페이스에서 OSPFv3를 활성화해야 합니다.

글로벌 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
router ospfv3 *process-id*	OSPFv3를 활성화하고, 라우터 구성 모드로 진입합니다.
router-id *router-id*	OSPFv3가 실행 중인 라우터의 라우터 ID를 설정합니

	다.

인터페이스 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
ipv6 ospf *process-id* **area** *area-id* **[instance** *instance-id***]**	인터페이스에서 OSPFv3를 활성화합니다.

참고 : 인터페이스에서 OSPFv3를 활성화하기 전에 OSPFv3 프로세스가 생성되지 않은 경우, OSPFv3 프로세스가 자동으로 생성됩니다.

31.10.2 OSPFv3 인터페이스 매개변수 설정

OSPFv3 구현 과정에서, 인터페이스에 대한 관련 OSPFv3 매개변수를 실제 요구 사항에 따라 수정할 수 있습니다. 모든 매개변수를 변경할 필요는 없지만, 연결된 네트워크의 모든 라우터에서 일부 매개변수는 반드시 일치해야 합니다.

인터페이스 구성 모드에서 다음 명령어를 실행하여 설정합니다.

명령어	설명
ipv6 ospf cost *cost*	OSPFv3 인터페이스에서 전송되는 패킷의 비용을 설정합니다.
ipv6 ospf retransmit-interval *seconds*	LSA 재전송 간격을 설정합니다.
ipv6 ospf transmit-delay *seconds*	OSPFv3 인터페이스에서 LSA 전송 지연 시간을 설정합니다.
ipv6 ospf priority *number*	OSPFv3 DR(Designated Router)의 우선순위를 설정합니다.
ipv6 ospf hello-interval *seconds*	OSPFv3 인터페이스에서 Hello 패킷 전송 간격을 설정합니다.
ipv6 ospf dead-interval *seconds*	일정 시간 동안 이웃 라우터에서 OSPFv3 패킷을 수신하지 못하면 해당 라우터를 종료된 것으로 간주합니다.

31.10.3 다양한 물리적 네트워크에서 OSPFv3 설정

OSPFv3는 물리적 네트워크 매체를 다음 세 가지 유형으로 구분합니다.

- 브로드캐스트 네트워크 (이더넷, 토큰 링, FDDI)
- 비브로드캐스트 다중 액세스 네트워크 (SMDS, 프레임 릴레이, X.25)
- 포인트 투 포인트 네트워크 (HDLC, PPP)

해당 명령어를 사용하여 네트워크를 브로드캐스트 네트워크 또는 비브로드캐스트 다중 액세스 네트워크로 설정할 수 있습니다. 프레임 릴레이 네트워크는 선택적으로 브로드캐스트 기능을 제공합니다.

OSPF는 map 명령어를 통해 브로드캐스트 네트워크에서 작동하도록 구성할 수 있습니다.

31.10.4 OSPF 네트워크 유형 설정

네트워크의 물리적 매체 유형에 관계없이, 네트워크를 브로드캐스트 네트워크, 비브로드캐스트 네트워크 또는 다중 액세스 네트워크로 설정할 수 있습니다.
이러한 방식으로 네트워크를 유연하게 설정할 수 있으며, X.25, 프레임 릴레이, SMDS와 같은 네트워크를 비브로드캐스트 및 다중 액세스 네트워크 또는 브로드캐스트 네트워크로 구성할 수 있습니다.
또한, Neighbor 설정이 간소화됩니다.

비브로드캐스트 및 다중 액세스 네트워크를 설정하는 것은 각 라우터 간에 가상 링크를 설정하거나 풀-메시(Full-Mesh) 네트워크를 가정하는 것입니다. 그러나, 이러한 방식은 비용이 높아 현실적으로 불가능합니다. 대신, 포인트-투-멀티포인트(Point-to-Multipoint) 방식으로 네트워크를 설정할 수 있습니다. 인접하지 않은 라우터 간에는 가상 링크를 통해 라우팅 정보가 교환됩니다.

OSPFv3 포인트-투-멀티포인트 인터페이스는 멀티포인트-투-포인트(Multipoint-to-Point) 인터페이스로 설정할 수 있으며, 이를 통해 호스트의 여러 경로를 설정할 수 있습니다.

OSPFv3 포인트-투-멀티포인트 네트워크의 장점

- 설정이 용이하며, DR(Designated Router)을 생성하지 않습니다.
- 풀-메시 토폴로지가 필요하지 않으며, 구축 비용이 상대적으로 낮습니다.
- 신뢰성이 높습니다.
- 가상 링크에 장애가 발생하더라도 연결이 유지됩니다.

라우터의 기본 네트워크 유형은 브로드캐스트 유형입니다.

31.10.5 OSPFv3 도메인 매개변수 설정

구성 가능한 도메인 매개변수에는 인증, 스텁 영역 지정 및 기본 요약 경로의 가중치 지정이 포함됩니다. 인증은 비밀번호 보호를 기반으로 합니다.

스텁 영역은 외부 라우트가 이 영역으로 배포되지 않음을 의미합니다. 대신, ABR는 스텁 영역으로 들어가는 기본 외부 경로를 생성하여 스텁 영역이 자율 시스템 외부 네트워크와 통신할 수 있도록 합니다. OSPF 스텁이 지원하는 속성을 사용하려면 스텁 영역에서 기본 경로를 사용해야 합니

다. 스텁 영역으로 전달되는 LSA를 더욱 줄이기 위해 ABR에서 요약 기능을 금지할 수 있습니다.

라우터 구성 모드에서 다음 명령어를 실행하여 도메인 매개변수를 설정합니다.

명령어	설명
area *area-id* **stub** [no-summary]	스텁 영역을 정의합니다.
area *area-id* **default-cost** *cost*	스텁 영역의 기본 경로에 대한 가중치를 설정합니다.

백본 영역이 아닌 영역으로서 백본 영역과 직접 연결되지 않거나, 영역이 단절된 경우 OSPFv3 가상 링크를 사용하여 논리적 연결을 설정할 수 있습니다.
가상 링크를 생성하려면, 가상 링크의 두 끝에서 구성을 수행해야 합니다. 한쪽 끝에서만 구성된 경우, 가상 링크는 작동하지 않습니다.

라우터 구성 모드에서 다음 명령어를 실행하여 도메인 매개변수를 설정합니다.

명령어	설명
area *area-id* **virtual-link** *neighbor-ID* [**dead-interval** *dead-value*][**hello-interval** *hello-value*][**retransmit-interval** *retrans-value*][**transmit-delay** *dly-value*]	가상 링크를 설정합니다.

31.10.6 OSPFv3 도메인에서 경로 요약 설정

이 기능을 통해 ABR(Area Border Router)은 다른 영역에 요약 경로를 브로드캐스트할 수 있습니다.
OSPFv3에서는 ABR이 각 네트워크를 다른 영역에 브로드캐스트합니다.
만약 네트워크 ID가 연속적으로 할당되어 있다면, ABR을 설정하여 다른 영역에 요약 경로(summary route)를 브로드캐스트하도록 할 수 있습니다.
이 요약 경로는 특정 범위 내의 모든 네트워크를 포함할 수 있습니다.

명령어	설명
area *area-id* **range** *ipv6-prefix /prefix-length*	요약 경로의 주소 범위를 설정합니다.

31.10.7 포워딩 경로의 요약 설정

다른 라우팅 영역에서 OSPFv3 라우팅 영역으로 경로가 배포될 때, 각 경로는 **외부 LSA(External LSA)**로 개별적으로 브로드캐스트됩니다.

그러나, 라우터에서 특정 경로를 설정하여 주소 범위를 포함하는 경로로 설정할 수 있습니다.

이를 통해 OSPFv3 링크 상태 데이터베이스(LSDB)의 크기를 줄일 수 있습니다.

명령어	설명
summary-prefix *ipv6-prefix /prefix-length*	하나의 요약 경로만 브로드캐스트합니다.

31.10.8 기본 경로(디폴트 루트) 생성

ASBR(Autonomous System Boundary Router)은 OSPFv3 라우팅 영역에 진입하기 위한 기본 경로를 생성해야 합니다.

언제든지 설정을 통해 라우터가 OSPFv3 라우팅 영역에 경로를 배포하도록 활성화할 수 있으며, 이 경로는 자동으로 ASBR이 됩니다.

그러나, ASBR은 기본적으로 OSPFv3 라우팅 영역에 진입하는 기본 경로를 생성하지 않습니다.

31.10.9 루프백 인터페이스에서 라우터 ID 선택

OSPFv3는 최대 IPv4 주소를 라우터 ID로 사용합니다.

만약 해당 IPv4 주소를 사용하는 인터페이스가 다운되거나, IPv4 주소가 삭제되면, OSPF 프로세스는 새 라우터 ID를 재계산하고 모든 인터페이스에서 라우팅 정보를 다시 전송합니다.

루프백 인터페이스에 IPv4 주소가 설정되어 있으면, 라우터는 우선적으로 루프백 인터페이스의 IPv4 주소를 라우터 ID로 사용합니다.

루프백 인터페이스는 절대 다운되지 않으므로, 라우팅 테이블의 안정성이 크게 향상됩니다.

라우터는 먼저 루프백 인터페이스의 주소를 ID로 선택하거나, 모든 루프백 인터페이스에서 최대 IPv4 주소를 라우터 ID로 선택합니다.

만약 루프백 인터페이스가 없으면, 라우터는 기존의 IPv4 주소를 라우터 ID로 사용합니다.

OSPFv3는 특정 인터페이스를 지정하여 라우터 ID로 사용할 수 없습니다.

명령어	설명
interface loopback *num*	루프백 인터페이스를 생성하고 인터페이스 구성 모드로 진입합니다.
ip address *ip-address mask*	인터페이스에 IPv4 주소를 할당합니다.

31.10.10 OSPFv3 관리 거리 설정

관리 거리(Administrative Distance)는 라우팅 정보 소스의 신뢰 수준을 의미합니다.
일반적으로 관리 거리는 0에서 255 사이의 정수입니다.
값이 클수록 신뢰 수준이 낮습니다. 관리 거리가 255이면 해당 라우팅 정보 소스는 신뢰되지 않으며 무시됩니다.

OSPFv3는 세 가지 종류의 관리 거리를 사용합니다.

- 도메인 내(intra-domain) 라우트: 동일한 영역 내의 라우트

- 도메인 간(inter-domain) 라우트: 다른 영역으로 향하는 라우트
- 외부(exterior) 라우트: 다른 라우팅 프로토콜에서 전달된 라우트

각 라우트 유형의 기본값은 110입니다.

31.10.11 라우팅 알고리즘 타이머 설정

토폴로지 변경 정보를 수신하고 SPF(Shortest Path First) 알고리즘을 계산하는 지연 시간을 설정할 수 있습니다.
또한, 두 번의 SPF 알고리즘 실행 간의 최소 간격도 설정할 수 있습니다.

명령어	설명
timers delay *delaytime*	영역에서 라우팅 알고리즘 지연 시간을 설정합니다.
timers hold *holdtime*	영역에서 라우팅 알고리즘 실행 간 최소 간격을 설정합니다.

31.10.12 OSPFv3 모니터링 및 유지 관리

네트워크 통계 정보에는 IP 라우팅 테이블, 캐시 및 데이터베이스의 내용이 포함됩니다.
이 정보는 네트워크 자원의 사용 상태를 파악하고 네트워크 문제를 해결하는 데 유용합니다.

명령어	설명
show ipv6 ospf [*process-id*]	SPFv3 라우팅 프로세스에 대한 일반 정보를 표시합니다.
show ipv6 ospf [*process-id*] **database** **show ipv6 ospf** [*process-id*] **database [router] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [network] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [inter-prefix] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [inter-router] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [external] [adv-router** *router-id***]** **show ipv6 ospf** [*process-id*] **database [link] [adv-**	OSPFv3 데이터베이스에 대한 정보를 표시합니다.

router *router-id*] **show ipv6 ospf** [*process-id*] **database [intra-prefix] [adv-router** *router-id*]	
show ipv6 ospf interface	OSPFv3 인터페이스에 대한 정보를 표시합니다.
show ipv6 ospf neighbor	OSPFv3 이웃에 대한 정보를 표시합니다.
show ipv6 ospf route	OSPFv3에 대한 라우팅 정보를 표시합니다.
show ipv6 ospf topology	OSPFv3 토폴로지를 표시합니다.
show ipv6 ospf virtual-links	OSPFv3의 가상 링크를 표시합니다.
debug ipv6 ospf	모든 OSPFv3 동작을 모니터링합니다.
debug ipv6 ospf events	OSPFv3 이벤트를 모니터링합니다.
debug ipv6 ospf ifsm	OSPFv3 인터페이스의 상태 머신을 모니터링합니다.
debug ipv6 ospf lsa	OSPFv3 LSA에 대한 관련 동작을 모니터링합니다.
debug ipv6 ospf nfsm	OSPFv3 이웃의 상태 머신을 모니터링합니다.
debug ipv6 ospf nsm	관리 모듈이 OSPFv3에 알리는 정보를 모니터링합니다.
debug ipv6 ospf packet	OSPFv3 패킷을 모니터링합니다.
debug ipv6 ospf route	OSPFv3에 대한 라우팅 정보를 모니터링합니다.

31.10.13 OSPFv3 라우트 학습 설정 예제

OSPFv3는 여러 내부 라우터, ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router) 간의 정보 교환이 필요합니다.

최소 설정으로 OSPFv3 기반 라우터는 모든 매개변수가 기본값을 사용하고, 인증 없이 작동합니다.

기본 OSPFv3 구성 예제

다음은 간단한 OSPFv3 설정 예제입니다.

이 예제에서는 프로세스 90을 활성화하고, VLAN 10을 영역 0.0.0.0에 연결하며, OSPFv3를 RIPng에 배포합니다.

```
ipv6 unicast-routing
!
interface vlan 10
 ipv6 address 2001::1/64
 ipv6 enable
 ipv6 ospf 90 area 0
```

```
 ipv6 ospf cost 1
!
router ospfv3 90
 router-id 1.1.1.1
 redistribute rip 1
!
router ripng 1
 redistribute ospf 90
```

여러 OSPFv3 프로세스 구성

다음 예제는 두 개의 OSPFv3 프로세스를 생성하는 방법을 보여줍니다.

```
ipv6 unicast-routing
!
interface vlan 10
 ipv6 address 2001::1/64
 ipv6 enable
 ipv6 ospf 109 area 0 instance 1
 ipv6 ospf 110 area 0 instance 2
!
!
interface vlan 11
 ipv6 address 2002::1/64
 ipv6 enable
 ipv6 ospf 109 area 1 instance 1
 ipv6 ospf 110 area 1 instance 2
!
!
router ospfv3 109
 router-id 1.1.1.1
 redistribute static
```

!

router ospfv3 110

router-id 2.2.2.2

!

참고 : 각 인터페이스는 여러 OSPFv3 프로세스에 속할 수 있습니다.

단, 인터페이스가 여러 OSPFv3 프로세스에 속하는 경우, 각 OSPFv3 프로세스는 다른 인스턴스(instance)에 속해야 합니다.

복합 구성 예제

다음 예제는 단일 OSPFv3 자율 시스템 내에서 여러 라우터를 구성하는 방법을 보여줍니다.

이 예제의 네트워크 토폴로지는 아래 그림과 같습니다.

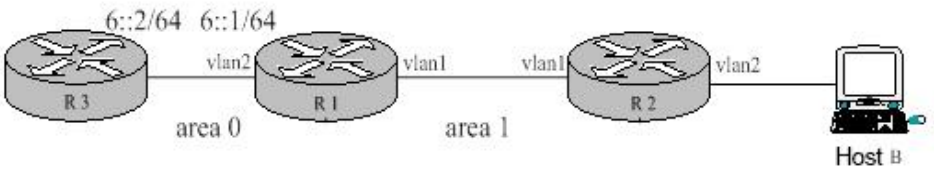


그림 57 네트워크 토폴로지

R1 :

```
interface vlan 1
    ipv6 enable
    ipv6 ospf 1 area 1
!
interface vlan 2
    ipv6 enable
    ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
  router-id 1.1.1.1
  redistribute static
```

!

R2 :

interface vlan 1

ipv6 enable

ipv6 ospf 1 area 1

!

!

router ospfv3 1

router-id 2.2.2.2

!

R2에서 라우팅 테이블 확인

R2#show ipv6 route

O 6::/64[1]

[110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)

O 2001::/64[1] (Forwarding route)

[110,150] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)

C fe80::/10[1]

is directly connected, L,Null0

C fe80::/64[1]

is directly connected, C, VLAN1

C fe80::2e0:fff:fe26:a8/128[1]

is directly connected, L, VLAN1

C ff00::/8[1]

is directly connected, L,Null0

영역 1을 스텁 영역으로 설정

R1 :

interface vlan 1

ipv6 enable

ipv6 ospf 1 area 1

```
!
interface vlan 2
     ipv6 enable
     ipv6 ospf 1 area 0
!
ipv6 route 2001::/64 6::2
!
router ospfv3 1
   router-id 1.1.1.1
   area 1 stub
   redistribute static
!
```

R2 :

```
interface vlan 1
     ipv6 enable
     ipv6 ospf 1 area 1
!
!
router ospfv3 1
   router-id 2.2.2.2
   area 1 stub
!
```

R2에서 라우팅 테이블 확인

```
R2#show ipv6 route
O          ::/0[1]
            [110,11] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)
O          6::/64[1]
            [110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)
C          fe80::/10[1]
```

is directly connected, L,Null0

C fe80::/64[1]

is directly connected, C, VLAN1

C fe80::2e0:fff:fe26:a8/128[1]

is directly connected, L, VLAN1

C ff00::/8[1]

is directly connected, L,Null0

위 결과를 통해, 스텁 영역의 ABR(Area Border Router)은 기본 경로(default route)를 정상적으로 생성하고, 다른 라우터에 이를 알릴 수 있으며, ASE LSA(External Type-5 LSA)가 스텁 영역으로 유입되지 않음을 확인할 수 있습니다.

가상 링크 구성

다음 예제는 단일 자율 OSPFv3 시스템에서 가상 링크를 구성하는 방법을 보여줍니다.

다음 그림은 구성 예제의 네트워크 토폴로지를 나타냅니다.

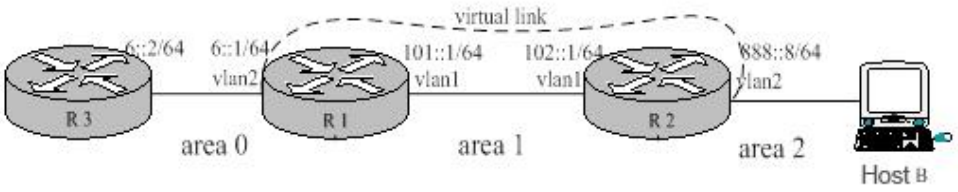


그림 58 네트워크 토폴로지

R1 :

```
interface vlan 1
    ipv6 address 101::1/64
    ipv6 enable
    ipv6 ospf 1 area 1
!
interface vlan 2
    ipv6 address 6::1/64
    ipv6 enable
    ipv6 ospf 1 area 0
!
```

```
ipv6 route 2001::/64 6::2
!
router ospfv3 1
   router-id 200.200.200.1
   area 1 virtual-link 200.200.200.2
   redistribute static
!
R2 :
interface vlan 1
     ipv6 address 101::2/64
     ipv6 enable
     ipv6 ospf 1 area 1
!
interface vlan 2
     ipv6 address 888::8/64
     ipv6 enable
     ipv6 ospf 1 area 2
!
!
router ospfv3 1
   router-id 200.200.200.2
   area 1 virtual-link 200.200.200.1
!
```

OSPFv3 이웃 상태 확인

R1에서 OSPFv3 이웃 상태 확인

```
R1#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID      Pri    State           Dead Time    Interface    Instance ID
200.200.200.2      1    Full/DR         00:00:35     VLAN1        0
```

200.200.200.2 1 Full/ - 00:00:36 VLINK1 0

R2에서 OSPFv3 이웃 상태 확인

R2#show ipv6 ospf neighbor

OSPFv3 Process (1)

Neighbor ID Pri State Dead Time Interface Instance ID

200.200.200.1 1 Full/Backup 00:00:36 VLAN1 0

200.200.200.1 1 Full/ - 00:00:37 VLINK1 0

R1에서 라우팅 테이블 확인

R1#show ipv6 route

C 6::/64[1]

is directly connected, C, VLAN2

C 6::1/128[1]

is directly connected, L, VLAN2

C 101::/64[2]

is directly connected, C, VLAN1

C 101::1/128[2]

is directly connected, L, VLAN1

O 101::2/128[2]

[110,10] via fe80:4::2e0:fff:fe26:a8(on VLAN1)

O 888::/64[2]

[110,20] via fe80:4::2e0:fff:fe26:a8(on VLAN1)

S 2001::/64[1]

[1,0] via 6::2(on VLAN2)

C fe80::/10[2]

is directly connected, L, Null0

C fe80::/64[2]

is directly connected, C, VLAN1

C fe80::2e0:fff:fe26:2d98/128[2]

is directly connected, L, VLAN1

C fe80::/64[1]

is directly connected, C, VLAN2

C fe80::2e0:fff:fe26:2d99/128[1]

is directly connected, L, VLAN2

C ff00::/8[2]

is directly connected, L, Null0

R2에서 라우팅 테이블 확인

R2#show ipv6 route

O 6::/64[1]

[110,20] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)

C 101::/64[1]

is directly connected, C, VLAN1

O 101::1/128[1]

[110,10] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)

C 101::2/128[1]

is directly connected, L, VLAN1

C 888::/64[1]

is directly connected, C, VLAN2

C 888::8/128[1]

is directly connected, L, VLAN2

O 2001::/64[1]

[110,150] via fe80:4::2e0:fff:fe26:2d98(on VLAN1)

C fe80::/10[1]

is directly connected, L, Null0

C fe80::/64[1]

is directly connected, C, VLAN1

C fe80::2e0:fff:fe26:a8/128[1]

is directly connected, L, VLAN1

C fe80::/64[1]

is directly connected, C, VLAN2

C fe80::2e0:fff:fe26:a9/128[1]

is directly connected, L, VLAN2

C ff00::/8[1]

is directly connected, L, Null0

이 설정을 통해 R1과 R2 사이에 OSPFv3 가상 링크가 성공적으로 구성되었으며, 라우팅 테이블을 통해 네트워크가 정상적으로 연결된 것을 확인할 수 있습니다.

31.11 BGP 구성

이 장에서는 BGP(Border Gateway Protocol) 구성 방법에 대해 설명합니다. BGP 명령어에 대한 전체 설명은 "BGP 명령어" 관련 섹션을 참조하십시오.
BGP는 RFC1163, 1267 및 1771에서 정의된 외부 게이트웨이 프로토콜(EGP, Exterior Gateway Protocol)입니다.
BGP는 서로 다른 자율 시스템(AS) 간에 경로 선택 메커니즘을 설정할 수 있으며, 이 메커니즘은 autonomous system 간 루프 없는 라우팅 정보 교환을 자동으로 보장합니다.

31.11.1 라우터의 BGP 구현

BGP에서 각 라우트는 네트워크 번호, 해당 경로가 통과한 autonomous system 목록(AS-path) 및 기타 속성(attribute) 목록을 포함합니다.
라우터 소프트웨어는 RFC1771에서 정의된 BGP v4를 지원합니다.

BGP의 기본 기능은 다른 BGP 시스템과 네트워크 도달 가능성 정보(network reachability information)를 교환하는 것입니다.
이 정보에는 AS-path 정보가 포함되며, 이를 통해 라우팅 루프를 방지하는 AS 연결 그래프(AS connection graph)를 생성할 수 있습니다.
AS 연결 그래프를 사용해 AS 수준 라우팅 정책을 구현할 수 있습니다.

BGP v4는 클래스 없는 도메인 간 라우팅(CIDR, Classless Inter-Domain Routing)을 지원합니다. CIDR은 요약 라우트(summary route)를 생성하여 라우팅 테이블의 크기를 줄이고, 슈퍼넷(super network)을 생성합니다.
CIDR은 BGP에서 네트워크 레벨 개념을 제거하고 IP 프리픽스(prefix) 브로드캐스트를 지원합니다. CIDR 라우트는 OSPF, Enhanced IGRP, ISIS-IP 및 RIP2를 통해 전송할 수 있습니다.

외부 게이트웨이 라우팅과 내부 게이트웨이 라우터의 중요한 차이점은 전자가 더 나은 제어 능력을 가지고 있다는 것입니다.
경로를 제어하기 위해, BGP 구현은 몇 가지 선택적인 방법을 제공합니다:

- 경로를 필터링하기 위해, neighbor를 기반으로 한 access-list, aspath-list, prefix-list를 사용할 수 있으며, 인터페이스를 기반으로 한 access-list, prefix-list를 사용하거나 라우트의 Nexthop 속성을 사용하여 경로를 필터링할 수 있습니다.
- 경로의 속성을 변경하기 위해, route-map을 사용하여 BGP 라우트의 속성(MED, Local preference, route value 등)을 수정할 수 있습니다.
- 내부 게이트웨이 동적 라우팅 프로토콜(OSPF, RIP 등)과 상호 작용하기 위해, 경로를 재분배(redistribute)하여 BGP 라우팅 정보를 자동으로 생성할 수 있습니다. 또한 네트워크 및

애그리게이션(aggregation)을 수동으로 구성하여 BGP 라우트를 생성할 수 있습니다. BGP 라우트를 생성하는 동안 route-map을 사용하여 경로의 속성을 구성할 수 있습니다.

- 시스템 내 BGP 라우트의 우선순위를 제어하기 위해, distance 명령어를 사용하여 BGP 라우트의 관리 거리(administrative distance)를 구성할 수 있습니다.

31.11.2 BGP 경로 선택 방식

BGP의 경로 결정 프로세스는 경로 속성 값(route attribute value)을 비교하는 데 기반을 둡니다. 동일한 네트워크에 여러 경로가 존재할 경우, BGP는 목적지로 가는 최적의 경로를 선택합니다. 다음은 BGP가 최적의 경로를 선택하는 과정을 요약한 것입니다:

- 다음 홉(next hop)에 도달할 수 없는 경우, 해당 경로는 고려되지 않습니다.
- 경로가 내부 경로이고 동기화(synchronization)가 활성화되어 있으며, 경로가 IGP(Interior Gateway Protocol)에 존재하지 않는 경우, 해당 경로는 고려되지 않습니다.
- 최대 우선순위(precedence)를 가진 경로를 우선적으로 선택합니다.
- 모든 경로의 값이 동일하다면, 최대 로컬 우선순위(local precedence)를 가진 경로를 우선적으로 선택합니다.
- 각 경로의 로컬 우선순위가 동일하다면, 로컬 라우터(local router)에서 생성된 경로를 우선적으로 선택합니다.
  예를 들어, network 또는 aggregate 명령어를 사용하거나 IGP 라우트를 재분배(redistribute)하여 로컬 라우터에서 생성된 경로를 의미합니다.
- 로컬 우선순위가 같거나 로컬 라우터에서 생성된 경로가 없을 경우, AS 경로(AS path)가 가장 짧은 경로를 우선적으로 선택합니다.
- AS 경로 길이가 동일하다면, origin 속성 값이 가장 낮은 경로를 우선적으로 선택합니다. (IGP < EGP < INCOMPLETE 순서)
- origin 속성 값이 동일하다면, MED(Multi-Exit Discriminator) 값이 가장 낮은 경로를 우선적으로 선택합니다.
  단, bgp always-compare-med가 활성화되지 않은 경우, 동일한 neighbor AS에서 온 경로에 대해서만 MED 비교가 수행됩니다.
- 모든 경로의 MED 값이 동일하다면, 외부 경로(EBGP)를 내부 경로(IBGP)보다 우선적으로 선택합니다.
  autonomous system 연합(confederation) 내 모든 경로는 내부 경로로 간주되지만, IBGP 연합보다 EBGP 연합 경로를 우선적으로 선택합니다.
- 모든 경로의 연결 속성이 동일하다면, 라우터 ID(router-id)가 작은 경로를 우선적으로 선

택합니다.

31.12 BGP 구성 작업 목록

BGP 구성 작업은 기본 작업과 고급 작업으로 나뉩니다.
기본 작업 중 처음 두 항목은 BGP를 구성하는 데 필수이며, 나머지 기본 작업 항목과 모든 고급 작업은 선택 사항입니다.

31.12.1 BGP 기본 구성 작업 목록

BGP의 기본 구성 작업은 다음과 같습니다:

- BGP 경로 선택 활성화
- BGP neighbor 구성
- BGP 소프트 재구성(soft reconfiguration) 구성
- BGP 연결 재설정(reset)
- BGP와 IGP 간 동기화 구성
- BGP 경로 값(route value) 구성
- neighbor 기반 BGP 경로 필터 구성
- 인터페이스 기반 BGP 경로 필터링 구성
- BGP 업데이트의 nexthop 처리 비활성화

31.12.2 BGP 고급 구성 작업 목록

BGP의 고급 및 선택적 구성 작업은 다음과 같습니다:

- route-map을 사용하여 경로 업데이트를 필터링 및 수정
- 애그리게이트(aggregate) 주소 구성
- BGP 커뮤니티 속성(community attribute) 구성
- autonomous system 연합(confederation) 구성
- 라우트 리플렉터(route reflector) 구성
- 피어(peer) 엔티티 종료
- 멀티홉 외부 피어(multihop external peer) 구성
- BGP 라우트의 관리 거리 구성

- BGP 타이머 조정
- 다른 AS에서 온 경로의 MED 비교
- BGP neighbor의 MD5 인증 구성
- BGP 그레이스풀 리스타트(graceful restart) 구성
- 출력 라우팅 필터링(ORF, Output Routing Filtering) 구성

IP 라우트 선택 프로토콜의 여러 속성 구성에 대한 자세한 내용은
"프로토콜과 독립적인 IP 라우팅 속성 구성" 섹션을 참조하십시오.

31.13 BGP 구성 작업

31.13.1 기본 BGP 기능 구성

- BGP 경로 선택 활성화

  BGP 경로 선택을 활성화하려면, 글로벌 구성 모드에서 다음 명령어를 사용하여 BGP 경로 선택을 활성화합니다.

명령어	설명
router bgp autonomous-system	우터 구성 모드에서 BGP 경로 선택 프로세스를 활성화합니다.
network network-number/masklen [route-map route-map-name]	네트워크를 로컬 자율 시스템으로 태그하고 BGP 목록에 추가합니다.

참고 :

- 외부 게이트웨이 라우팅 프로토콜에서는 network 구성 명령어를 사용하여 IP 네트워크를 구성할 경우, 어떤 네트워크를 알릴지를 제어합니다.
  이는 RIP와 같은 내부 게이트웨이 프로토콜(IGP)과 반대입니다. IGP에서는 network 명령어를 사용하여 업데이트를 보낼 위치를 결정합니다.
- network 명령어는 IGP 경로를 BGP 라우팅 테이블에 가져오는 데 사용됩니다. 사용 가능한 network 명령어의 최대 개수는 라우터 자원(예: RAM 구성)에 의해 결정됩니다.
  선택 사항으로, redistribute 명령어를 사용하여 동일한 효과를 얻을 수 있습니다.

- BGP Neighbor 구성

  BGP는 두 가지 유형의 neighbor를 지원합니다: 내부 neighbor(IBGP)와 외부

neighbor(EBGP)입니다.
내부 neighbor는 같은 AS에 속해 있고, 외부 neighbor는 서로 다른 AS에 속해 있습니다.
일반적으로 외부 neighbor는 서로 인접해 있으며 같은 서브넷을 공유합니다.
하지만 내부 neighbor는 같은 AS 내 어디에나 위치할 수 있습니다.

neighbor 명령어를 사용하여 BGP neighbor를 구성합니다

명령어	설명
neighbor {*ip-address* | *peer-group-name*} **remote-as** *number*	BGP neighbor 를 지정합니다.

BGP neighbor 구성 예제는 이 장 하단의 "BGP neighbor 구성 예제" 섹션을 참조하십시오.

- BGP 소프트 재구성(Soft Reconfiguration) 구성

  일반적으로 BGP neighbor는 연결이 설정될 때 모든 경로를 교환하고, 그 이후에는 업데이트된 경로만 교환합니다.

  따라서 구성된 라우팅 정책이 변경될 경우, 이를 수신한 경로에 적용하려면 BGP 세션을 초기화해야 합니다.

  BGP 세션을 초기화하면 캐시가 무효화되고 네트워크 운영에 큰 영향을 미칩니다.

  소프트 재구성 기능은 BGP 세션을 초기화하지 않고 정책을 구성하고 활성화할 수 있도록 합니다.

  따라서 소프트 재구성을 사용하는 것이 권장됩니다. 현재 소프트 재구성은 각 neighbor에 대해 개별적으로 활성화됩니다.

  neighbor가 생성한 수신 업데이트에 대해 소프트 재구성을 사용하면, 이를 인바운드 소프트 재구성이라고 합니다.

  neighbor로 전송하는 발신 업데이트에 대해 소프트 재구성을 사용하면, 이를 아웃바운드 소프트 재구성이라고 합니다.

  수신 소프트 재구성을 적용하면 새로운 입력 정책이 효과를 가지게 되며,

  발신 소프트 재구성을 적용하면 BGP 세션을 초기화하지 않고 새로운 로컬 출력 정책이 효과를 가지게 됩니다.

  BGP 세션을 초기화하지 않고 새로운 수신 업데이트를 생성하려면, 로컬 BGP 스피커는 현재 수신 정책에 따라 수락되거나 거부된 것과 관계없이 수신한 업데이트를 수정 없이 저장해야 합니다.

  이 과정은 메모리를 많이 소모하므로 피하는 것이 좋습니다.

  반면, 발신 재구성은 추가 메모리 소모가 없으므로 항상 효과적입니다.

BGP 세션의 반대편에서 발신 소프트 재구성을 트리거하면 새로운 로컬 수신 정책이 효과를 가집니다.

수신 소프트 재구성을 허용하려면 BGP가 수락된 모든 라우팅 업데이트를 저장하도록 구성해야 합니다.

발신 재구성은 사전 구성이 필요하지 않습니다.

다음 라우터 구성 명령어를 사용하여 BGP 소프트 재구성을 구성합니다

명령어	설명
Neighbor {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**]	BGP 소프트 재구성을 구성합니다.

BGP 피어 커뮤니티를 지정하기 위해 peer-community-name 매개변수를 사용하는 경우, 해당 커뮤니티의 모든 멤버는 이 명령어의 기능을 상속합니다.

- BGP 연결 재설정

  두 라우터가 BGP neighbor로 정의되면, BGP 연결이 생성되고 라우팅 정보가 교환됩니다.

  BGP 라우팅 정책이나 다른 설정이 변경된 경우, 변경 사항을 적용하려면 BGP 연결을 재설정해야 합니다.

  다음 두 가지 관리 모드 명령어 중 하나를 사용하여 BGP 연결을 재설정할 수 있습니다.

명령어	설명
clear ip bgp *	특정 BGP 연결을 다시 생성합니다.
clear ip bgp *address*	모든 BGP 연결을 재설정합니다.

- BGP와 IGP 간 동기화 구성

  다른 AS가 여러분의 AS를 통해 제3의 AS로 데이터를 전송하도록 허용하는 경우, AS 내부 라우팅 상태와 다른 AS에 브로드캐스트되는 라우팅 정보 간의 동기화는 매우 중요합니다.

  예를 들어, 여러분의 BGP가 AS 내 모든 라우터가 IGP를 통해 해당 경로를 알기 전에 경로를 브로드캐스트하려고 한다면, 일부 라우터가 경로를 모르는 상태에서 AS가 정보를 수신하게 될 수 있습니다. 이러한 상황을 방지하기 위해, BGP는 AS 내 모든 IGP 라우터가 해당 라우팅 정보를 인지할 때까지 기다려야 합니다.

  이를 BGP와 IGP 간 동기화라고 하며, 동기화는 기본적으로 활성화되어 있습니다.

  특정 상황에서는 동기화가 필요하지 않을 수 있습니다.

다른 AS가 여러분의 AS를 통해 데이터를 전송하지 않거나, AS 내 모든 라우터가 BGP를 실행하는 경우 동기화 기능을 비활성화할 수 있습니다.

동기화 기능을 비활성화하면 IGP에서 관리하는 경로 수를 줄이고, BGP의 수렴 속도를 높일 수 있습니다. 동기화를 비활성화하려면 다음 명령어를 사용합니다.

명령어	설명
no synchronization	BGP 와 IGP 간 동기화를 비활성화합니다.

동기화를 비활성화할 경우, clear ip bgp 명령어를 사용하여 BGP 세션을 초기화해야 합니다.

BGP 동기화 예제는 이 장 하단의 "neighbor에 의한 BGP 경로 필터링 예제" 섹션을 참조하십시오.

일반적으로 모든 경로를 IGP로 재분배하는 것은 권장되지 않습니다.

일반적인 설계 방식은 한두 개의 경로만 재분배하여 IGRP에서 외부 경로로 만들거나, BGP 세션이 AS 기본 경로(default route)를 생성하도록 강제하는 것입니다.

BGP가 IGP로 경로를 재분배하는 경우, EBGP를 통해 획득한 경로만 재분배됩니다.

대부분의 경우 IGP를 BGP에 할당하지 않는 것이 좋습니다.

network 명령어를 사용하여 AS 내 네트워크를 나열하면, 해당 네트워크가 브로드캐스트됩니다.

이렇게 나열된 네트워크는 로컬 네트워크(local network)라고 하며, BGP에서 IGP origin 속성을 갖습니다.

이 네트워크들은 메인 IP 라우팅 테이블에 존재하고 유효

해야 합니다.

예를 들어, 직접 연결된 경로, 정적 경로, IGP를 통해 인식된 경로가 이에 해당합니다.

BGP 라우팅 프로세스는 주기적으로 메인 IP 라우팅 테이블을 스캔하여 로컬 네트워크의 존재 여부를 확인하고, 이에 따라 BGP 라우팅 테이블을 업데이트합니다.

BGP가 실제로 경로를 재분배하도록 하려면 매우 신중해야 합니다. 이는 다른 라우터가 BGP를 통해 IGP로 주입한 경로일 수 있기 때문입니다. 이 경우, BGP가 IGP로 정보를 주입하고 다시 BGP로 정보를 반환하는 상황이 발생할 수 있으며 반대의 경우도 발생할 수 있습니다.

- BGP 경로 값(Route Value) 구성

  BGP 경로 값은 라우터에서 BGP 경로 선택 프로세스를 제어하기 위해 설정하는 숫자입니다. 이 값은 라우터에서만 유효한 로컬 값입니다. 값의 범위는 0부터 65535까지입니다. 로컬에서 생성된 BGP 경로의 기본 값은 32768이며, neighbor로부터 획득한 경로의 값은 0입니다. 관리자는 경로 값을 변경하여 라우팅 정책을 구현할 수 있습니다. 다음 라우터 구

성 명령어를 사용하여 BGP 경로 가중치(weight)를 구성합니다.

명령어	설명
neighbor {*ip-address* | *X:X::X:X* } **weight** *weight*	특정 neighbor 로부터 받은 각 경로에 값을 지정합니다.

- BGP 라우트 필터를 NEIGHBOUR 기준으로 설정하기

  라우터 소프트웨어의 BGP 구현에서 지정된 neighbor의 BGP 라우트를 필터링하는 4가지 방법이 있습니다:

  Aspath 리스트 필터를 글로벌 구성 명령어 "ip aspath-list" 및 명령어 "neighbour filter-list" 와 함께 사용합니다.

명령어	설명
ip as-path access-list *aspaths-list-name* {**permit | deny**} *as-regular-expression*	BGP 에 대한 액세스 목록을 정의합니다.
router bgp *autonomous-system*	라우터 구성 모드로 들어갑니다.
neighbor {*ip-address* | *X:X::X:X* } **filter-list** *aspath-list-name* {**in | out** }	BGP 필터를 설정합니다.

액세스 리스트를 글로벌 구성 명령어 "ip access-list" 및 명령어 "neighbour distribute-list"와 함께 사용합니다.

명령어	설명
ip access-list standard *access-list-name*	액세스 목록을 정의합니다.
router bgp *autonomous-system*	라우터 구성 모드로 들어갑니다.
neighbor {*ip-address* | *X:X::X:X* } **distribute-list** *access-list-name* {**in | out** }	BGP 필터를 설정합니다.

프리픽스 리스트를 글로벌 구성 명령어 "ip prefix-list" 및 명령어 "neighbour prefix-list"와 함께 사용합니다.

명령어	설명
ip prefix-list *prefixs-list-name* **{permit |deny}** A.B.C.D/n **ge** x **le** y	접두사 목록을 정의합니다.
router bgp *autonomous-system*	라우터 구성 모드로 들어갑니다.
neighbor {*ip-address* | *X:X::X:X* } **prefix-list** *prefix-list-name* {**in | out** }	BGP 필터를 설정합니다.

Route-map을 글로벌 구성 명령어 "route-map" 및 명령어 "neighbour route-map"와 함께

사용합니다.

Route-map을 사용하면 라우트를 필터링할 뿐만 아니라 라우트 속성을 변경할 수도 있으며, 사용 방법은 이후 장에서 설명됩니다.

neighbor 필터 라우트를 기반으로 하는 예제는 "example of BGP route filtration based on the neighbor"를 참조하십시오.

- 인터페이스 기반 BGP 라우트 필터 구성

  인터페이스 기반 BGP 라우트 필터링은 액세스 리스트와 프리픽스 리스트를 사용하여 수행할 수 있습니다. 라우트의 네트워크 번호와 게이트웨이 주소를 필터링할 수 있습니다.

  라우트의 네트워크 번호를 필터링하기 위해 "access-list" 옵션을 지정하여 액세스 리스트를 사용할 수 있으며, "prefix-list" 옵션을 지정하여 프리픽스 리스트를 사용할 수 있습니다.

  라우트의 "nexthop" 속성을 필터링하기 위해 "gateway" 옵션을 지정하여 액세스 리스트를 사용할 수 있습니다.

  라우트의 네트워크 번호와 "nexthop" 속성을 동시에 필터링할 수도 있지만, "access-list" 옵션과 "prefix-list" 옵션은 동시에 사용할 수 없습니다.

  "*"를 지정하면 모든 인터페이스에서 라우트를 필터링할 수 있습니다.

  인터페이스 기반 BGP 라우트 필터링을 구성하려면 BGP 구성 모드에서 다음 구성을 수행해야 합니다.

명령어	설명
filter interface {**in** | **out**} (**access-list** access-list-name) (**prefix-list** prefix-list-name) (**gateway** access-list-name)	인터페이스에 따라 BGP 경로를 필터링합니다.

인터페이스 기반 라우트 필터링 예제는 "examples of BGP route filtration based on the interface"를 참조하십시오.

- BGP 업데이트의 넥스트홉 처리 비활성화

  neighbor BGP 업데이트의 넥스트홉 처리를 비활성화하도록 구성할 수 있습니다. 이는 비브로드캐스팅 네트워크(FR 또는 X.25 등)에서 유용합니다. FR 또는 X.25 네트워크에서는 BGP neighbor가 동일한 IP 서브넷의 다른 neighbor에 직접 접근하지 못할 수 있습니다. 넥스트홉 처리를 취소하는 방법은 두 가지가 있습니다:

  ① 해당 BGP 연결의 로컬 IP 주소를 사용하여 나가는 라우트의 넥스트홉 주소를 대체합니다.

  ② 라우트 맵을 사용하여 들어오거나 나가는 라우트의 넥스트홉 주소를 지정합니다. (다

른 장을 참조하십시오)

다음 라우터 구성 명령어를 사용하여 넥스트홉 처리를 비활성화하고 나가는 라우트의 넥스트홉 주소를 BGP 연결의 로컬 IP 주소로 대체합니다.

명령어	설명
neighbor {*ip-address* | *X:X::X:X*} **next-hop-self**	BGP neighbor 업데이트를 수행하는 동안 넥스트홉 처리를 비활성화합니다.

이 명령어를 구성하면 현재 라우터가 자신을 라우트의 넥스트홉으로 알리도록 설정됩니다. 따라서 다른 BGP neighbor는 이 네트워크로의 패킷을 현재 라우터로 전달하게 됩니다.
이것은 비브로드캐스팅 네트워크 환경에서 매우 유용합니다. 현재 라우터에서 지정된 neighbor로의 경로가 존재하기 때문입니다.
그러나 브로드캐스팅 네트워크 환경에서는 불필요한 추가 홉을 유발할 수 있으므로 주의해야 합니다.

31.13.2 고급 BGP 기능 구성

1. 라우트 맵을 사용하여 라우트 업데이트 필터링 및 수정

   라우트 맵(route-map)을 사용하여 라우트 업데이트를 필터링하고, 각 neighbor별로 매개변수 속성을 수정할 수 있습니다.
   라우트 맵은 들어오는 업데이트(incoming)와 나가는 업데이트(outgoing) 모두에 적용할 수 있습니다.
   라우트 맵을 통과하는 라우트만이 라우트 업데이트를 수락하거나 전송할 때 처리됩니다.

라우트 맵은 AS 경로, 커뮤니티(community), 네트워크 번호와 일치하는 들어오고 나가는 업데이트를 지원합니다.

AS 경로 일치를 위해서는 명령어 "aspath-list"를 사용해야 하며 커뮤니티 기반 일치는 명령어 "community-list"를 사용해야 합니다. 또한 네트워크 기반 일치는 명령어 "ip access-list"를 사용해야 합니다.

다음 BGP 구성 명령어를 사용하여 라우트 업데이트의 필터링 및 수정을 위한 라우트 맵을 구성할 수 있습니다.

명령어	설명
neighbor {*ip-address* | *X:X::X:X*} **route-map** *route-map-name* **{in | out}**	Apply route-map on incoming or outcoming routes.

라우트 업데이트를 필터링하고 수정하는 라우트 맵 사용 예제는 "Examples of BGP route-map"을

참조하십시오.

2. 애그리게이트 주소 구성

클래스 없는 도메인 간 라우팅(CIDR)은 라우팅 테이블을 최소화하기 위해 애그리게이트 라우팅(및 슈퍼 네트워크)을 생성할 수 있습니다.
BGP에서 애그리게이트 라우팅은 애그리게이트 경로를 BGP로 재분배하거나, 아래 작업 목록에서 설명하는 조건부 애그리게이트 속성을 사용하여 구성할 수 있습니다.
BGP 라우팅 테이블에 최소 하나 이상의 자세한 레코드가 존재하는 경우, 애그리게이트 주소가 BGP 라우팅 테이블에 추가됩니다.

다음 라우터 구성 명령어 중 하나 이상을 사용하여 라우팅 테이블에 애그리게이트 주소를 생성할 수 있습니다

명령어	설명
aggregate *network/len*	BGP 라우팅 테이블에 애그리게이트 주소를 생성합니다.
aggregate *network/len* **summary-only**	요약 주소만 브로드캐스트합니다.
aggregate *network/len* **attribute-map** *map-name*	라우트 맵에 의해 지정된 조건에 따라 애그리게이트 주소를 생성합니다.

BGP 라우트 애그리게이션 사용 예제는 이 장의 하단에 있는 "examples of BGP route aggregation" 섹션을 참조하십시오.

3. BGP 커뮤니티 속성 구성

BGP에서 지원하는 라우팅 정책은 주로 BGP 라우팅 정보의 세 가지 값 중 하나를 기반으로 합니다:

① 라우트의 네트워크 번호

② 라우트의 as_path 속성 값

③ 라우트의 "community" 속성 값

"community" 속성을 통해 라우트를 커뮤니티로 나누고, 커뮤니티 기반 라우팅 정책을 적용하여 라우팅 정보 제어 구성을 단순화할 수 있습니다.

커뮤니티(Community)는 공통 속성을 가진 라우트 그룹을 의미하며, 각 라우트는 여러 커뮤니티에 속할 수 있습니다. AS 관리자는 특정 라우트를 특정 커뮤니티에 속하도록 정의할 수 있습니다.
커뮤니티 속성은 선택적이고 전송 가능한 글로벌 속성으로, 범위는 1부터 4,294,967,200까지입니다.

인터넷 커뮤니티에서 미리 정의된 유명 커뮤니티는 다음과 같습니다:

① No-export — 이 라우트를 EBGP 피어(autonomous system 컨페더레이션 내의 EBGP 피어

포함)에게 광고하지 않습니다.

② No-advertise — 이 라우트를 어떤 피어 에게도 advertise 하지 않습니다.

③ local-as — 이 라우트를 autonomous system 외부로 광고하지 않습니다(autonomous system 컨페더레이션 내 다른 서브-AS 피어에게는 전송 가능).

BGP 스피커는 라우트를 생성, 수락 또는 전송할 때 라우트 커뮤니티 속성을 구성, 추가 또는 수정할 수 있습니다.

라우트를 애그리게이션할 경우, 생성된 애그리게이트는 모든 원본 라우트의 완전한 커뮤니티에서 "community" 속성을 포함합니다.

기본적으로 "community" 속성은 neighbor에게 전송되지 않습니다.

다음 BGP 구성 명령어를 사용하여 neighbor에게 "community" 속성을 전송하도록 지정할 수 있습니다.

명령어	설명
neighbor {*ip-address* | *X:X::X:X* } **send-community**	"커뮤니티" 속성을 보내도록 지정합니다.

라우터에서 커뮤니티 속성을 구성하려면 다음 작업을 수행해야 합니다.

명령어	설명
route-map *map-name sequence-number* {**deny | permit**}	라우팅 맵을 구성합니다.
set community *community-value*	설정 규칙을 구성합니다.
router bgp *autonomous-system*	라우터 구성 모드로 들어갑니다.
neighbor{*ip-address* | *X:X::X:X* } **route-map** *access-list-name* {**in** | **out** }	라우팅 맵을 적용합니다.

커뮤니티 속성을 기반으로 라우팅 정보를 필터링하려면 다음 작업을 수행해야 합니다.

명령어	설명
ip community-list {**expanded | standard** } *community-list-name* {**permit | deny**} *communtiy-expression*	커뮤니티 목록을 정의합니다.
route-map *map-name sequence-number* **{deny | permit}**	라우팅 맵을 구성합니다.
match community *community-list-name*	매칭 규칙을 구성합니다.
router bgp *autonomous-system*	라우터 구성 모드로 들어갑니다.
neighbor {*ip-address* | *peer-group-name*} **route-map** *route-map-name* {**in | out** }	라우팅 맵을 적용합니다.

4. autonomous system 컨페더레이션(Confederation) 구성

IBGP 연결 수를 줄이는 방법은 AS(자율 시스템)를 여러 개의 서브 AS로 나누고, 이를 autonomous system 컨페더레이션으로 구성하는 것입니다. 외부에서 보면 컨페더레이션은 하나의 AS처럼 보입니다.

컨페더레이션 내에서 각 서브 AS는 내부적으로 풀-메시(Full-mesh) 상태이며, 동일한 컨페더레이션 내의 다른 서브 AS와 연결됩니다.

서로 다른 서브 AS 간 피어링된 EBGP 세션이 있더라도, IBGP 피어와 유사하게 라우팅 선택 정보를 교환할 수 있습니다. 구체적으로는 넥스트홉(nexthop), MED, 로컬 우선순위(local precedence) 정보가 유지됩니다.

BGP autonomous system 컨페더레이션을 구성하려면 컨페더레이션 식별자(confederation identifier)를 지정해야 합니다.

컨페더레이션 식별자는 AS 번호이며, 외부에서 보면 컨페더레이션은 컨페더레이션 식별자와 같은 AS 번호를 가진 단일 AS처럼 동작합니다.

다음 BGP 구성 명령어를 사용하여 자율 시스템의 컨페더레이션 식별자를 구성할 수 있습니다.

명령어	설명
bgp confederation identifier *autonomous-system*	autonomous system 의 컨페더레이션 식별자를 구성합니다.

autonomous system 컨페더레이션에 속하는 AS 번호를 지정하려면 다음 BGP 구성 명령어를 사용합니다.

명령어	설명
bgp confederation peers *autonomous-system* [*autonomous-system ...*]	컨페더레이션에 속하는 AS 를 지정합니다.

5. 라우트 리플렉터(Route Reflector) 구성

자율 시스템 컨페더레이션을 구성하는 대신, IBGP 연결 수를 줄이는 또 다른 방법은 라우트 리플렉터를 구성하는 것입니다.

라우트 리플렉터의 내부 피어는 두 그룹으로 나뉩니다:

① 클라이언트 피어(client peers)

② 비클라이언트 피어(non-client peers, 기타 모든 라우터)

③ 라우트 리플렉터는 두 그룹 간 라우트를 반사(reflect)합니다. 라우트 리플렉터와 클라이언

트 피어는 하나의 클러스터(cluster) 를 형성합니다.
비클라이언트 피어는 풀-메시(full-mesh)로 연결되어야 하지만, 클라이언트 피어는 그렇지 않아도 됩니다. 클러스터 내 클라이언트는 클러스터 외부의 IBGP 스피커와 직접 통신하지 않습니다.

라우트 리플렉터가 라우팅 정보를 수신할 때 수행하는 작업은 다음과 같습니다:

① 외부 BGP 스피커로부터 받은 라우트를 모든 클라이언트 및 비클라이언트 피어에 브로드캐스트합니다.

② 비클라이언트로부터 받은 라우트를 모든 클라이언트에게 브로드캐스트합니다.

③ 클라이언트로부터 받은 라우트를 모든 클라이언트 및 비클라이언트 피어에 브로드캐스트합니다. 따라서 클라이언트 피어는 풀-메시로 연결될 필요가 없습니다.

다음 라우터 구성 명령어를 사용하여 로컬 라우터를 리플렉터로 구성하고, neighbor를 라우트 리플렉터 클라이언트로 지정할 수 있습니다

명령어	설명
Neighbor {*ip-address* | *X:X::X:X* } **route-reflector-client**	로컬 라우터를 경로 리플렉터로 구성하고 neighbor 을 클라이언트로 지정합니다.

AS는 여러 라우트 리플렉터를 가질 수 있으며, 라우트 리플렉터가 다른 라우트 리플렉터를 처리하는 방식은 IBGP 스피커를 처리하는 방식과 동일합니다.
일반적으로 하나의 클러스터에는 하나의 라우트 리플렉터가 있으며, 클러스터는 라우트 리플렉터의 라우터 ID로 식별됩니다.
단일 노드 장애를 방지하고冗여성을 증가시키기 위해, 하나의 클러스터에 두 개 이상의 라우트 리플렉터를 구성할 수 있습니다.

이 경우, 클러스터 내 모든 라우트 리플렉터는 4비트 클러스터 ID를 구성하여, 동일 클러스터 내의 라우트 리플렉터가 업데이트 정보를 식별할 수 있도록 해야 합니다.
동일 클러스터에 속하는 모든 라우트 리플렉터는 풀-메시로 연결되어야 하며, 동일한 클라이언트 및 비클라이언트 피어 세트를 가져야 합니다.

클러스터에 두 개 이상의 라우트 리플렉터가 있는 경우, 다음 BGP 구성 명령어를 사용하여 클러스터 ID를 구성할 수 있습니다

명령어	설명
bgp cluster-id *cluster-id*	클러스터 ID 를 구성합니다.

6. 피어 엔티티(Neighbor) 종료

다음 BGP 구성 명령어를 사용하여 BGP neighbor를 종료(shutdown)할 수 있습니다.

명령어	설명
Neighbor {*ip-address* | *X:X::X:X* } **shutdown**	BGP neighbor 을 종료합니다.

이전에 종료된 neighbor를 활성화하려면 다음 BGP 구성 명령어를 사용합니다

명령어	설명
no neighbor {*ip-address* | *X:X::X:X* } **shutdown**	BGP neighbor 을 활성화합니다.

7. 멀티홉 외부 피어 구성

   기본적으로 외부 피어는 직접 연결된 네트워크에 있어야 합니다. 멀티홉 외부 피어를 구성하려면 다음 작업을 수행해야 합니다

명령어	설명
neighbor {*ip-address* | *X:X::X:X* } **ebgp-multihop** ttl	BGP neighbor 멀티홉 외부 피어로 설저합니다.

8. BGP 라우트 관리 거리(Management Distance) 구성

   관리 거리는 서로 다른 라우팅 프로토콜의 우선순위를 측정하는 방식입니다. BGP는 세 가지 서로 다른 관리 거리를 사용합니다: 외부 거리(external distance), 내부 거리(internal distance), 로컬 거리(local distance).

- 외부 BGP에서 얻은 라우트는 외부 거리로 할당됩니다.
- 내부 BGP에서 얻은 라우트는 내부 거리로 설정됩니다.
- 로컬 라우트는 로컬 거리로 지정됩니다.

다음 BGP 구성 명령어를 사용하여 BGP 라우트 관리 거리를 구성할 수 있습니다

명령어	설명
distance bgp {*external-distance*| *internal-distance* |*local-distance*}	BGP 경로 관리 거리를 구성합니다.

BGP 라우트의 관리 거리를 변경하는 것은 위험할 수 있으며, 일반적으로 권장되지 않습니다.
외부 거리는 다른 동적 라우팅 프로토콜의 거리보다 짧아야 하고, 내부 거리는 다른 동적 라우팅 프로토콜보다 길어야 합니다.

9. BGP 타이머 조정

   다음 BGP 구성 명령어를 사용하여 특정 neighbor의 BGP "keepalive" 및 "holdtime" 타이머를 조정할 수 있습니다

명령어	설명

distance bgp {*external-distance*| *internal-distance* |*local-distance*}	지정된 피어 또는 피어 커뮤니티에 대해 "keepalive" 및 "holdtime" 타이머 간격(단위 '초'로 계산)을 설정합니다.

10. 다른 AS에서 온 라우트의 MED 비교

MED는 여러 경로 중 최적의 경로를 선택할 때 고려되는 매개변수입니다. MED 값이 낮은 경로가 더 높은 MED 값을 가진 경로보다 우선적으로 선택됩니다.

기본적으로 최적 경로를 선택하는 과정에서 MED 비교는 동일한 AS에서 온 라우트에만 수행됩니다.

라우트가 어느 AS에서 오든 관계없이, 라우팅 선택에서 MED 비교를 허용할 수 있습니다.

다음 BGP 구성 명령어를 사용하여 위의 목적을 실현할 수 있습니다.

명령어	설명
bgp always-compare-med	다른 AS 에서 온 라우트 간에도 MED 비교를 허용합니다.

31.14 BGP 모니터링 및 유지 관리

관리자는 BGP 라우팅 테이블 또는 기타 데이터베이스의 내용을 표시하거나 삭제할 수 있습니다. 또한 자세한 통계 정보도 확인할 수 있습니다.

- BGP 라우팅 테이블 및 데이터베이스 삭제
- 라우팅 테이블 및 시스템 통계 정보 표시
- BGP 정보 추적

31.14.1 BGP 라우팅 테이블 및 BGP 데이터베이스 삭제

아래 표는 고속 캐시 삭제, 테이블 삭제 또는 BGP 데이터베이스 삭제와 관련된 작업을 나열합니다.

다음 표에 나열된 명령어는 모두 EXEC 모드에서 실행됩니다.

명령어	설명
clear ip bgp *	모든 BGP 연결을 재설정합니다.
clear ip bgp *as-number*	지정된 BGP 연결을 재설정합니다.
clear ip bgp *address*	지정된 neighbor 의 BGP 연결을 재설정합니다.
clear ip bgp *address* soft {**in**|**out**}	지정된 neighbor 의 들어오는 데이터베이스나 나가는 데이터베이스를 삭제합니다.
clear ip bgp *aggregates*	경로 애그리게이션에서 생성된 라우트를 삭제합니다.

clear ip bgp *networks*	포워딩 프로세스에서 생성된 라우트를 삭제합니다.
clear ip bgp *redistribute*	network 명령어에 의해 생성된 라우트를 삭제합니다.

31.14.2 라우팅 테이블 및 시스템 통계 정보 표시

BGP 라우팅 테이블 또는 데이터베이스에 대한 자세한 통계 정보가 표시됩니다. 제공된 정보는 리소스 사용량을 결정하고 네트워크 문제를 해결하는 데 도움이 됩니다.
노드 도달 가능성에 대한 정보도 확인할 수 있습니다. 다양한 라우팅 통계 정보를 표시하려면 다음 명령어를 실행하십시오

명령어	설명
show ip bgp	시스템의 BGP 라우팅 테이블을 표시합니다.
show ip bgp prefix	지정된 접두사 목록과 일치하는 경로를 표시합니다.
show ip bgp community	그룹 속성에 대한 통계 정보를 표시합니다.
show ip bgp regexp *regular-expression*	지정된 정규 표현식과 일치하는 경로를 표시합니다.
show ip bgp *network*	지정된 BGP 경로를 표시합니다.
show ip bgp neighbors *address*	지정된 neighbor 의 TCP 및 BGP 연결에 대한 정보를 표시합니다.
show ip bgp neighbors *[address]* [**received-routes** | **routes** | **advertised-routes**]	특수 BGP neighbors 에서 학습한 경로를 표시합니다.
show ip bgp paths	데이터베이스의 모든 BGP 경로에 대한 정보를 표시합니다.
show ip bgp summary	모든 BGP 연결의 상태를 표시합니다.

31.14.3 BGP 정보 추적

BGP 정보 추적을 통해 BGP 연결 설정 및 라우트 전송/수신 과정을 관찰할 수 있습니다.
이를 통해 문제를 진단하고 해결하는 데 도움이 됩니다.

BGP 정보를 추적하는 명령어는 다음 표에 나와 있습니다.

명령어	설명
debug ip bgp	일반적인 BGP 정보를 추적합니다.
debug ip bgp all	모든 BGP 정보를 추적합니다.
debug ip bgp fsm	BGP 상태 머신(Finite State Machine)을 추적합니다.
debug ip bgp keepalive	BGP 의 KeepAlive 패킷을 추적합니다.
debug ip bgp open	BGP 의 OPEN 패킷을 추적합니다.
debug ip bgp update	BGP 의 UPDATE 패킷을 추적합니다.

31.14.4 BGP 라우트 맵 예제

다음 예제는 neighbor로부터 들어오는 라우트의 속성을 변경하기 위해 라우트 맵(route-map)을 사용하는 방법을 설명합니다.

neighbor 140.222.1.1에서 들어오는 모든 라우트 중 ASPATH 접근 리스트 "aaa" 조건을 충족하는 라우트는 메트릭(metric)을 200으로 설정하고, 로컬 프리퍼런스(local preference) 값을 250으로 설정하며, 해당 라우트를 허용합니다.

그 외의 모든 라우트는 거부됩니다.

```
router bgp 100
 neighbor 140.222.1.1 route-map fix-weight in
 neighbor 140.222.1.1 remote-as 1
!
route-map fix-weight 10 permit
 match as-path aaa
 set local-preference 250
 set weight 200
!
ip as-path access-list aaa permit ^690$
ip as-path access-list aaa permit ^1800
```

다음 예제에서는 라우트 맵 "freddy"의 첫 번째 항목이 자율 시스템 690에서 유래된 모든 라우트의 MED 속성을 127로 설정합니다.

두 번째 항목은 위 조건을 충족하지 않는 라우트를 neighbor 1.1.1.1에 전송하도록 허용합니다.

```
router bgp 100
 neighbor 1.1.1.1 route-map freddy out
!
ip as-path access-list abc permit ^690_
ip as-path access-list xyz permit .*
!
route-map freddy 10 permit
 match as-path abc
```

```
 set metric 127
!
route-map freddy 20 permit
 match as-path xyz
```

다음 예제는 라우트 맵을 사용하여 라우트 재분배(route redistribution)에서 들어오는 라우트를 변경하는 방법을 보여줍니다.

```
router bgp 100
 redistribute rip 1 route-map rip2bgp
!
route-map rip2bgp
 match ip address rip
 set local-preference 25
 set metric 127
 set weight 30000
 set ip next-hop 192.92.68.24
 set origin igp
!
ip access-list standard rip
 permit 131.108.0.0 255.255.0.0
 permit 160.89.0.0 255.255.0.0
 permit 198.112.0.0 255.255.128.0
```

31.14.5 Neighbor 구성 예제

다음 예제에서 BGP 라우터는 AS109에 속하며, 두 개의 네트워크를 생성합니다.

이 라우터에는 세 개의 neighbor가 있습니다

- 첫 번째 neighbor는 외부 AS(다른 AS)입니다.
- 두 번째 neighbor는 내부 AS(동일한 AS 번호)입니다.
- 세 번째 neighbor는 외부 AS입니다.
- router bgp 109

- network 131.108.0.0
- network 192.31.7.0
- neighbor 131.108.200.1 remote-as 167
- neighbor 131.108.234.2 remote-as 109
- neighbor 150.136.64.19 remote-as 99

31.14.6 Neighbor 기반 BGP 라우트 필터링 예제

다음은 neighbor 기반 BGP 경로 필터링 예제입니다. AS-path 접근 리스트 "test1"을 통과하는 라우트는 메트릭 값으로 100이 할당됩니다. AS-path 접근 리스트 "test2"를 통과하는 라우트만이 193.1.12.10으로 전송됩니다.

마찬가지로, AS-path 접근 리스트 "test3"을 통과하는 라우트만 193.1.12.10에서 수락됩니다.

```
router bgp 200
neighbor 193.1.12.10 remote-as 100
neighbor 193.1.12.10 filter-list test1 weight 100
neighbor 193.1.12.10 filter-list test2 out
neighbor 193.1.12.10 filter-list test3 in
!
ip as-path access-list test1 permit _109_
ip as-path access-list test2 permit _200$
ip as-path access-list test2 permit ^100$
ip as-path access-list test3 deny _690$
ip as-path access-list test3 permit .*
```

31.14.7 인터페이스 기반 BGP 라우트 필터링 예제

다음은 인터페이스 기반 라우트 필터링 구성 예제입니다.

이 예제에서는 인터페이스 vlan1에서 액세스 리스트 "ac1"을 통해 라우트를 필터링합니다.

```
router bgp 122
filter vlan1 in access-list acl
```

다음 예제는 액세스 리스트 "filter-network"를 사용해 라우트의 네트워크 번호를 필터링하고, 동시

에 액세스 리스트 "filter-gateway"를 사용해 vlan1 인터페이스에서 라우트의 게이트웨이 주소를 필터링합니다

router bgp 100

filter vlan1 in access-list filter-network gateway filter-gateway

다음 예제는 프리픽스 리스트 "filter-prefix"를 사용해 라우트의 네트워크 번호를 필터링하고, 동시에 액세스 리스트 "filter-gateway"를 사용해 모든 인터페이스에서 라우트의 게이트웨이 주소를 필터링합니다.

router bgp 100

filter * in prefix-list filter-prefix gateway filter-gateway

31.14.8 프리픽스 리스트를 사용한 라우트 필터링 구성 예제

다음 예제는 기본 경로 0.0.0.0/0을 거부(deny)합니다.

ip prefix-list abc deny 0.0.0.0/0

다음 예제는 프리픽스 35.0.0.0/8과 일치하는 라우트를 허용(permit)합니다.

ip prefix-list abc permit 35.0.0.0/8

다음 예제에서 BGP 프로세스는 프리픽스 길이가 /8에서 /24 사이인 경우만 수락합니다.

router bgp 1

network 101.20.20.0

filter * in prefix max24

!

ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24

다음 구성에서는 라우터가 모든 인터페이스에서 라우트를 필터링하며, 프리픽스 길이가 8에서 24 사이인 경우만 수락합니다.

router bgp 12

filter * in prefix-list max24

!

ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24

기타 프리픽스 리스트 구성 예제

다음 예제는 네트워크 192/8에서 프리픽스 길이가 24 이하인 라우트를 허용합니다.

ip prefix-list abc permit 192.0.0.0/8 le 24

다음 예제는 네트워크 192/8에서 프리픽스 길이가 25 이상인 라우트를 거부합니다

ip prefix-list abc deny 192.0.0.0/8 ge 25

다음 예제는 모든 주소 공간에서 프리픽스 길이가 8보다 크고 24보다 작은 라우트를 허용합니다.

ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24

다음 예제는 모든 주소 공간에서 프리픽스 길이가 25보다 큰 모든 라우트를 거부합니다.

ip prefix-list abc deny 0.0.0.0/0 ge 25

네트워크 10/8에서 라우트를 거부합니다. 클래스 A 네트워크 10.0.0.0/8에서 마스크가 32비트 이하인 경우, 해당 네트워크의 모든 라우트가 거부됩니다

ip prefix-list abc deny 10.0.0.0/8 le 32

다음 예제는 네트워크 204.70.1.24에서 마스크 길이가 25보다 큰 라우트를 거부합니다.

ip prefix-list abc deny 204.70.1.0/24 ge 25

다음 예제는 모든 라우트를 허용합니다

ip prefix-list abc permit any

31.14.9 BGP 라우트 애그리게이션 예제

다음 예제는 BGP에서 애그리게이션 라우트를 생성하는 방법을 설명합니다.

애그리게이션 라우트는 라우트 재분배(redistribution) 또는 조건부 라우트 애그리게이션(conditional route aggregation) 기능을 사용해 생성할 수 있습니다.

다음 예제에서 명령어 redistribute static은 애그리게이션 라우트 193...*를 재분배합니다.

ip route 193.0.0.0 255.0.0.0 null 0

!

router bgp 100

redistribute static

지정된 범위 내에 하나 이상의 라우트가 라우팅 테이블에 존재할 경우, 다음 구성은 BGP 라우팅 테이블에 애그리게이션 라우트를 생성합니다.

애그리게이션 라우트는 해당 AS에서 유래된 것으로 간주되며, 정보 손실 가능성을 나타내는 "atomic" 속성을 가집니다

router bgp 100

aggregate 193.0.0.0/8

다음 예제는 애그리게이션 라우트 193...*를 생성할 뿐만 아니라, 더 구체적인 라우트를 모든 neighbor에게 브로드캐스트하지 않도록 설정합니다.

router bgp 100

aggregate 193.0.0.0/8 summary-only

31.14.10 BGP 라우트 리플렉터 예제

다음은 라우트 리플렉터(route reflector) 구성 예제입니다.

- RTA, RTB, RTC, RTE는 동일한 자율 시스템 AS200에 속합니다.
- RTA는 라우트 리플렉터로 동작하며, RTB와 RTC는 라우트 리플렉터 클라이언트(client)입니다.
- RTE는 일반 IBGP neighbor입니다.
- RTD는 AS100에 속하며, RTA와 EBGP 연결을 생성합니다

RTA 구성

```
interface vlan2
 ip address 2.0.0.1 255.0.0.0
!
interface vlan3
 ip address 3.0.0.1 255.0.0.0
!
interface vlan4
 ip address 4.0.0.1 255.0.0.0
!
interface vlan5
 ip address 5.0.0.1 255.0.0.0
!
router bgp 200
 neighbor 2.0.0.1 remote-as 200     /*RTC IBGP*/
```

```
 neighbor 2.0.0.1 route-reflector-client
 neighbor 3.0.0.1 remote-as 200     /*RTB IBGP*/
 neighbor 3.0.0.1 route-reflector-client
 neighbor 5.0.0.1 remote-as 200     /*RTE IBGP*/
 neighbor 4.0.0.2 remote-as 100     /*RTD EBGP*/
 network 11.0.0.0/8
!
ip route 11.0.0.0 255.0.0.0 2.0.0.12
```

RTB 구성

```
interface vlan3
 ip address 3.0.0.2 255.0.0.0
!
router bgp 200
 neighbor 3.0.0.1 remote-as 200     /*RTA IBGP*/
 network 13.0.0.0/8
!
ip route 13.0.0.0 255.0.0.0 3.0.0.12
```

RTC 구성

```
interface vlan2
 ip address 2.0.0.2 255.0.0.0
!
router bgp 200
 neighbor 2.0.0.1 remote-as 200     /*RTA IBGP*/
 network 12.0.0.0/8
!
ip route 12.0.0.0 255.0.0.0 2.0.0.12
```

RTD 구성

```
interface vlan4
 ip address 4.0.0.2 255.0.0.0
!
router bgp 100
 neighbor 4.0.0.1 remote-as 200     /*RTA EBGP*/
 network 14.0.0.0/8
!
ip route 14.0.0.0 255.0.0.0 4.0.0.12
```

RTE 구성

```
interface vlan5
 ip address 5.0.0.2 255.0.0.0
!
router bgp 200
 neighbor 5.0.0.1 remote-as 200     /*RTA IBGP*/
 network 15.0.0.0/8
!
ip route 15.0.0.0 255.0.0.0 5.0.0.12
```

31.14.11 BGP 컨페더레이션 예제

다음은 BGP 컨페더레이션(confederation) 구성 예제입니다.

- RTA, RTB, RTC는 IBGP로 연결되며, 프라이빗 자율 시스템 AS65010에 속합니다.
- RTE는 프라이빗 자율 시스템 AS65020에 속합니다.
- RTE와 RTA는 컨페더레이션 내부 EBGP 연결을 수립합니다.
- AS65010과 AS65020은 컨페더레이션을 구성하며, 컨페더레이션 식별자는 AS200입니다.
- RTD는 자율 시스템 AS100에 속하며, RTA를 통해 AS200과 EBGP 연결을 수립합니다.

RTA 구성

```
interface vlan1
 ip address 1.0.0.1 255.0.0.0
!
interface vlan2
 ip address 2.0.0.1 255.0.0.0
!
interface vlan4
 ip address 4.0.0.1 255.0.0.0
!
interface vlan5
 ip address 5.0.0.1 255.0.0.0
!
router bgp 65010
 bgp confederation identifier 200
 bgp confederation peers 65020
 neighbor 1.0.0.2 remote-as 65010   /*RTB IBGP*/
 neighbor 2.0.0.2 remote-as 65010   /*RTC IBGP*/
 neighbor 5.0.0.2 remote-as 65020   /*RTE EBGP*/
 neighbor 4.0.0.2 remote-as 100     /*RTD EBGP*/
```

RTB 구성

```
interface vlan1
 ip address 1.0.0.2 255.0.0.0
!
interface vlan3
 ip address 3.0.0.1 255.0.0.0
!
router bgp 65010
 bgp confederation identifier 200
```

```
 bgp confederation peers 65020
 neighbor 1.0.0.1 remote-as 65010   /*RTA IBGP*/
 neighbor 3.0.0.2 remote-as 65010   /*RTC IBGP*/
```

RTC 구성

```
interface vlan2
 ip address 2.0.0.2 255.0.0.0
!
interface vlan3
 ip address 3.0.0.2 255.0.0.0
!
router bgp 65010
 bgp confederation identifier 200
 bgp confederation peers 65020
 neighbor 2.0.0.1 remote-as 65010   /*RTA IBGP*/
 neighbor 3.0.0.1 remote-as 65010   /*RTB IBGP*/
```

RTD 구성

```
interface vlan4
 ip address 4.0.0.2 255.0.0.0
!
router bgp 100
 neighbor 4.0.0.1 remote-as 200   /*RTA EBGP*/
```

RTE 구성

```
interface vlan5
 ip address 5.0.0.2 255.0.0.0
!
router bgp 65020
```

```
 bgp confederation identifier 200
 bgp confederation peers 65010
 neighbor 5.0.0.1 remote-as 65010   /*RTA EBGP*/
```

31.14.12 BGP 그룹 속성(Route Map) 예제

이 예제에서는 neighbor 171.69.232.50의 나가는 업데이트에 "route map set-community"가 적용됩니다

```
router bgp 100
 neighbor 171.69.232.50 remote-as 200
 neighbor 171.69.232.50 send-community
 neighbor 171.69.232.50 route-map set-community out
!
route-map set-community 10 permit
 match ip address aaa
 set community no-export
!
route-map set-community 20 permit
```

커뮤니티 값 200 삽입 예

이 예제에서는 neighbor 171.69.232.90의 나가는 업데이트에 "route map set-community"가 사용됩니다.

```
router bgp 200
 neighbor 171.69.232.90 remote-as 100
 neighbor 171.69.232.90 send-community
 neighbor 171.69.232.90 route-map set-community out
!
route-map set-community 10 permit
 match as-path test1
 set community-additive 200 200
```

```
!
route-map set-community 20 permit
 match as-path test2
!
ip as-path access-list test1 permit 70$
ip as-path access-list test2 permit .*
```

커뮤니티 기반 MED 및 로컬 프리퍼런스 설정 예제

이 예제에서는 neighbor 171.69.232.55에서 들어오는 업데이트에 대해 라우트의 커뮤니티 속성에 따라 MED 및 로컬 프리퍼런스(local preference) 값을 선택적으로 설정합니다.

```
router bgp 200
 neighbor 171.69.232.55 remote-as 100
 neighbor 171.69.232.55 route-map filter-on-community in
!
route-map filter-on-community 10 permit
 match community com1
 set metric 8000
!
route-map filter-on-community 20 permit
 match community com2
 set local-preference 500
!
route-map filter-on-community 30 permit
 set local-preference 50
!
ip community-list standard com1 permit 100 200 300
ip community-list standard com1 permit 900 901
!
ip community-list standard com2 permit 88
```

```
ip community-list standard com2 permit 90
```

31.15 PBR 구성

이 섹션은 PBR(Policy Based Routing, 정책 기반 라우팅) 구성 방법에 대해 설명합니다. PBR은 동적 라우팅 프로토콜 외에도 특정 정책에 따라 IP 패킷을 라우팅할 수 있도록 합니다. 현재 PBR은 IP 패킷의 길이 및 소스 IP 주소에 따라 라우팅하는 정책을 지원합니다. 정책에 일치하는 패킷에 대해 게이트웨이 또는 출력 인터페이스를 설정할 수 있으며, PBR은 로드 밸런싱도 지원합니다.

PBR의 다음 홉을 선택하는 규칙은 다음과 같습니다

- set ip next-hop이 구성되어 있고 게이트웨이가 도달 가능한 경우 해당 게이트웨이가 사용됩니다. 여러 게이트웨이가 구성되어 있는 경우 첫 번째로 도달 가능한 게이트웨이가 사용됩니다. load-balance 키워드가 사용된 경우 이러한 게이트웨이 간에 로드 밸런싱이 수행됩니다.
- set interface가 구성되어 있고 출력 인터페이스가 라우팅 가능(인터페이스 프로토콜이 활성화되고 IP 주소가 구성됨)한 경우 해당 인터페이스가 사용됩니다. 여러 개의 출력 인터페이스가 구성된 경우 첫 번째 라우팅 가능한 인터페이스가 사용됩니다. load-balance 키워드가 사용된 경우 이러한 인터페이스 간에 로드 밸런싱이 수행됩니다. set ip next-hop과 set interface가 모두 구성된 경우 set ip next-hop이 우선 적용됩니다.
- set ip default next-hop 또는 set default interface는 라우팅 조회에 실패한 경우에만 사용됩니다.

다음과 같은 패킷에는 정책 라우팅이 적용되지 않습니다:

- 대상 주소가 로컬 장치인 패킷
- 멀티캐스트 메시지
- 로컬 직접 브로드캐스트 패킷

31.16 PBR 구성 작업 목록

PBR을 사용하려면 다음 구성이 필요합니다:

- 표준 액세스 리스트 생성(선택 사항)
- 라우트 맵 생성
- 인터페이스에 라우트 맵 적용

31.17 PBR 구성 작업

31.17.1 표준 액세스 리스트 생성

표준 액세스 리스트를 생성하려면 다음 단계를 확인합니다.

명령어	설명
ip access-list standard net1	액세스 리스트 구성 모드로 진입합니다.

31.17.2 라우트 맵 생성

라우트 맵을 생성하려면 다음 단계를 따릅니다.

명령어	설명
route-map pbr	경로 맵 구성을 입력합니다.
match ip address *access-list* **match length** *min_length max_length*	일치 정책을 구성합니다.
set ip [**default**] **next-hop** *A.B.C.D* **set** [**default**] **interface** *interface_name*	IP 패킷의 다음 홉 주소 또는 포트를 구성합니다.

31.17.3 인터페이스에 라우트 맵 적용

인터페이스에서 PBR(Policy-Based Routing)을 활성화하려면 다음 단계를 따릅니다.

명령어	설명
interface *interface_name*	인터페이스 구성 모드로 들어갑니다.
ip policy route-map *route-map_name*	인터페이스에 PBR 을 적용합니다.

31.17.4 PBR 유지 관리

EXEC 모드에서 PBR을 유지 관리하려면 다음 단계를 따릅니다.

명령어	설명
debug ip policy	정책 라우팅 적용 결과를 확인합니다.

31.17.5 PBR 구성 예시

```
!
interface Vlan1
 ip address 10.1.1.3 255.255.255.0
 no ip directed-broadcast
```

```
 ip policy route-map pbr
!
interface Vlan2
 ip address 13.1.1.3 255.255.255.0
 no ip directed-broadcast
!
interface Vlan3
 ip address 14.1.1.3 255.255.255.0
 no ip directed-broadcast
!
ip access-list standard net1
 permit 10.1.1.2 255.255.255.255
!
ip access-list standard net2
 permit 10.1.1.4 255.255.255.255
!
ip access-list standard net3
 permit 10.1.1.21 255.255.255.255
!
route-map pbr 10 permit
 match ip address net1
 set ip next-hop 13.1.1.99
!
route-map pbr 20 permit
 match ip address net2
 set ip next-hop 14.1.1.99
!
route-map pbr 30 permit
 match ip address net3
```

set ip next-hop 13.1.1.99 14.1.1.99 load-balance

!

route-map pbr 40 permit

set ip default next-hop 13.1.1.99

구성 설명

정책 라우팅은 인터페이스 vlan1에서 활성화됩니다.

10.1.1.2에서 시작된 패킷의 경우, 13.1.1.99가 다음 홉이 됩니다. 13.1.1.99가 도달 가능한 경우 해당 홉이 사용됩니다. 만약 13.1.1.99가 도달할 수 없는 경우, 목적지 기반 라우팅이 사용됩니다.

10.1.1.21에서 시작된 패킷의 경우, route-map pbr 30이 사용됩니다. load-balance 키워드가 사용되었기 때문에, 13.1.1.99와 14.1.1.99 모두 다음 홉으로 사용됩니다(라우팅 테이블에 13.1.1.99와 14.1.1.99로의 경로가 있는 경우)

31.18 IP-PBR 구성

IP-PBR는 스위치 칩의 하드웨어를 통해 소프트웨어 PBR 기능을 구현합니다.

PBR(Policy Based Routing)은 라우팅 프로토콜이 아닌 특정 정책에 따라 라우팅을 수행하도록 합니다. 소프트웨어 기반 PBR은 여러 정책 및 규칙을 지원하며, 로드 밸런싱도 가능합니다. 정책에 부합하는 패킷에 대해 다음 홉의 IP 주소 또는 포트를 지정할 수 있습니다. PBR은 로드 밸런싱을 지원하며, 정책을 지원하는 패킷에 대해 여러 개의 다음 홉 IP 주소 또는 포트를 적용합니다.

경로 맵(route map)에 의해 지정된 다음 홉 출구의 ARP가 학습된 경우에만, IP-PBR은 해당 출구를 유효한 것으로 간주하고, 해당 규칙이 적용됩니다. 패킷이 IP-PBR 정책을 충족하면 하드웨어는 해당 규칙이 지정한 다음 홉 출구로 패킷을 직접 전달합니다. 이 과정은 CPU의 개입 없이 하드웨어에서 처리됩니다. IP-PBR에 의해 전달되는 패킷은 가장 높은 우선순위를 가지며, IP-PBR 규칙과 일치하지 않는 패킷만 CPU로 전달됩니다.

현재 IP-PBR은 IP ACL 정책 및 다음 홉 IP 주소 정책을 지원합니다. 여러 개의 다음 홉이 구성된 경우, 첫 번째로 유효한 다음 홉이 선택됩니다. IP-PBR은 스위치 칩에 의해 구현되는 동등 라우팅(equivalent routing)도 지원합니다. 하드웨어 기반 동등 라우팅은 추가 구성 없이 작동합니다.

IP-PBR은 다음과 같은 정책 라우팅 명령을 지원합니다

route-map WORD

match ip address WORD

set ip next-hop X.X.X.X [load-balance]

ip policy route-map WORD

IP-PBR은 라우터의 정책 라우팅과 약간 다릅니다. IP-PBR은 유효한 다음 홉을 출구로 선택하며, 유효한 다음 홉이 없는 경우 패킷을 삭제합니다. 반면 라우터의 정책 라우팅은 유효한 다음 홉을 선택하지만, 해당 홉이 ARP를 학습하지 않은 경우 패킷 손실이 발생할 수 있습니다.

여러 시퀀스가 설정된 경우, IP-PBR과 소프트웨어 정책 라우팅 간의 차이를 주의해야 합니다. 소프트웨어 정책 라우팅은 높은 우선순위 시퀀스 경로를 항상 선택합니다. 이는 높은 우선순위 시퀀스에 의해 일치된 IP 주소가 낮은 우선순위 시퀀스와 겹치거나 해당 경로가 유효하지 않더라도 마찬가지입니다. 반면, IP-PBR은 높은 우선순위 시퀀스 경로가 유효하지 않은 경우 낮은 우선순위 시퀀스 경로를 선택합니다.

31.18.1 IP-PBR 글로벌 활성화 또는 비활성화

글로벌 구성 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip pbr	IP-PBR 기능은 기본적으로 비활성화되어 있습니다.
no ip pbr	기본 설정으로 복원합니다.

IP-PBR은 기본적으로 비활성화 상태입니다.

31.18.2 ISIS 구성 작업 목록

IP-PBR을 구성하려면 다음을 수행하십시오:

- ACL을 생성합니다.
- 경로 맵(Route Map)을 생성합니다.
- 포트에 경로 맵을 적용합니다.

ACL 생성

ACL을 생성하려면 글로벌 모드에서 다음 명령을 실행하십시오.

명령어	설명
ip access-list standard *net1*	ACL 구성 모드로 진입하고 ACL을 정의합니다.

경로 맵(Route Map) 생성

경로 맵을 생성하려면 글로벌 모드에서 다음 명령을 실행하십시오.

명령어	설명
route-map *pbr*	경로 맵 구성 모드로 진입합니다.

match ip address *access-list*	매칭 정책을 구성합니다.
set ip next-hop *A.B.C.D*	IP 패킷의 다음 홉 주소를 구성합니다.

IP 수신 포트에 정책 라우팅 적용

IP 수신 포트에 정책 라우팅을 적용하려면 다음 명령을 실행하십시오

명령어	설명
interface *interface_name*	인터페이스 구성 모드로 진입합니다.
ip policy route-map *route-map_name*	포트에 정책 라우팅을 적용합니다.

31.18.3 MVC 모니터링 및 유지 관리

EXEC 모드에서 다음 명령을 실행하십시오

명령어	설명
show ip pbr	RIP 구성 정보를 표시합니다.
show ip policy	IP-PBR이 적용된 포트를 표시합니다.
show ip pbr policy	IP-PBR 동등 라우팅에 대한 정보를 표시합니다.
debug ip pbr	IP-PBR 디버깅 스위치를 활성화하거나 비활성화합니다.

31.18.4 IP-PBR 구성 예제

```
!
ip pbr
!
interface vlan1
ip address 10.1.1.3 255.255.255.0
no ip directed-broadcast
ip policy route-map pbr
!
ip access-list standard ac1
permit 10.1.1.21 255.255.255.255
!
ip access-list standard ac2
```

```
permit 10.1.1.2 255.255.255.255
!
route-map pbr 10 permit
match ip address ac1
set ip next-hop 13.1.1.99
!
route-map pbr 20 permit
match ip address ac2
set ip next-hop 13.1.1.99 14.1.1.99 load-balance
!
```

구성 설명:

스위치는 VLAN1에서 수신된 패킷에 정책 라우팅을 적용합니다.

- 소스 IP가 10.1.1.21인 패킷은 다음 홉이 13.1.1.99로 설정됩니다.
- 소스 IP가 10.1.1.2인 패킷은 route-map pbr 20에 적용됩니다.

set ip next-hop 명령어에 load-balance 매개변수가 포함되어 있어, 스위치 칩은 목적지 IP 주소에 따라 자동으로 13.1.1.99 또는 14.1.1.99를 출구로 선택합니다.

31.19 스위치 라우팅 프로토콜 고우선순위 구성

라우팅 프로토콜을 테스트할 때, FP(Fast Path)를 통해 라우팅 프로토콜 패킷의 CPU 우선순위를 높일 수 있습니다. 이를 통해 시스템이 과부하 상태에서(예: 전송해야 하는 IP 패킷과 같은) 백그라운드 트래픽을 수신할 때도 라우팅 프로토콜 패킷이 정상적으로 수신될 수 있습니다.

CPU로 전달되는 라우팅 패킷의 우선순위를 향상시키기 위해 다음과 같은 구성 작업이 필요합니다.

31.19.1 CPU로 전달되는 라우팅 패킷의 우선순위 향상 활성화

글로벌 구성 모드에서 다음과 같이 구성합니다:

명령어	설명
switch routing-protocol-highpriority	CPU 로 전달되는 라우팅 패킷의 우선순위 향상을 활성화합니다.

32 VRRP 구성

32.1개요

VRRP (Virtual Router Redundancy Protocol)는 기본 정적 라우팅 환경에서 단일 노드 서비스가 원활하게 작동하도록 보장하는 프로토콜입니다. VRRP는 정적으로 지정된 게이트웨이의 단점을 보완합니다.

OLTs(Optical Line Terminals) 그룹은 VRRP를 통해 하나의 가상 OLT로 작동할 수 있습니다. 이 가상 OLT는 외부에서 가상 IP 주소와 가상 MAC 주소를 사용합니다.

VRRP는 OLT 그룹 중 하나를 마스터 OLT로 선택하며, 마스터 OLT는 패킷 포워딩을 담당합니다. 마스터 OLT에 문제가 발생하면 대기(Standby) OLT가 즉시 마스터 OLT의 작업을 인계받습니다.

기본 게이트웨이 주소를 변경할 필요가 없으며, 이 전환 과정은 단말 시스템에 투명하게 이루어집니다.

VRRP는 장애 발생 시 빠르고 효과적인 해결책을 제공합니다.

32.2 VRRP 구성 작업 목록

- 인터페이스에서 VRRP 활성화/비활성화
- VRRP 인증 모드 구성
- VRRP 우선 순위 프리엠프션(preemption) 구성
- VRRP 우선 순위(priority) 구성
- VRRP 타이머(clock) 값 구성
- VRRP 모니터링 및 유지 관리

32.3 VRRP 구성 작업

32.3.1 VRRP 가상 IP 주소 구성

VLAN 인터페이스 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
vrrp [*vrid***] associate** *virtual-address address-mask*	인터페이스에 VRRP 가상 IP 주소를 구성합니다.
no vrrp [*vrid***] associate [***virtual-address address-mask***]**	인터페이스에서 VRRP 가상 IP 주소를 삭제합니다.

VRRP의 가상 주소가 구성되면 가상 OLT가 활성화됩니다.

VRRP의 가상 주소와 포트의 기본 IP 주소는 반드시 동일한 네트워크 세그먼트에 있어야 합니다. 그렇지 않으면 가상 OLT는 Init 상태로 유지됩니다. 가상 IP 주소와 포트의 IP 주소가 일치할 경우, 시스템은 라우팅 OLT의 우선 순위를 자동으로 255로 승격합니다.

32.3.2 VRRP 인증 모드 구성

VLAN 인터페이스 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
vrrp [*vrid***] authentication** *WORD*	VRRP 인증 모드를 단순 텍스트(simple-text)로 구성합니다.
no vrrp [*vrid***] authentication**	VRRP 인증 모드를 기본 설정으로 복원합니다.

단순 텍스트 인증 모드에서는 인증 문자열이 메시지에 평문(clear code)으로 포함되어 전송됩니다. 수신자는 메시지 내 인증 문자열을 확인하여 로컬에서 구성된 인증 문자열과 일치하는지 검사합니다.
인증 문자열은 최대 8자까지 설정할 수 있습니다. 기본적으로 VRRP의 인증 모드는 no-authen(인증 없음)입니다.

32.3.3 VRRP 설명 구성

VLAN 인터페이스 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
vrrp [*vrid***] description** *WORD*	VRRP 설명 정보를 구성합니다.
no vrrp [*vrid***] description**	VRRP 설명 정보를 삭제합니다.

32.3.4 VRRP 우선 순위 프리엠프션(Preemption) 구성

VLAN 인터페이스 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
vrrp [*vrid***] preempt [delay** *second***]**	VRRP 우선 순위 프리엠프션을 구성합니다.
no vrrp [*vrid***] preempt [delay]**	VRRP 우선 순위 프리엠프션 모드를 기본 설정으로 복원합니다.

우선 순위 프리엠프션은 백업 OLT에만 적용됩니다.

백업 OLT가 마스터 OLT로부터 **알림 메시지(announce message)**를 수신하면, 마스터 OLT의 우

선 순위를 확인합니다.

마스터 OLT의 우선 순위가 로컬에서 구성된 우선 순위보다 낮고, 백업 OLT에 프리엠프션이 구성되어 있는 경우, 백업 OLT는 백업 상태에서 마스터 상태로 전환되며 외부로 알림 메시지를 전송합니다.

그렇지 않은 경우, 백업 OLT는 계속 백업 상태를 유지합니다. 기본 상태에서 VRRP의 인증 모드는 **no-authen(인증 없음)**입니다.

32.3.5 VRRP 프로토콜 패킷의 MAC 주소 구성

VLAN 인터페이스 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
vrrp [*vrid*] source-mac-use-system	VRRP 그룹이 시스템 MAC 주소를 사용해 패킷을 전송하도록 구성합니다.
no vrrp [*vrid*] source-mac-use-system	VRRP 그룹이 프로토콜 MAC 주소를 사용해 패킷을 전송하도록 구성합니다.

기본적으로 VRRP 프로토콜 패킷은 프로토콜 MAC 주소를 출발지 주소로 사용하여 전송됩니다.

해당 명령어를 구성하면, VRRP 프로토콜 패킷은 시스템 MAC 주소를 출발지 주소로 사용하여 전송합니다.

32.3.6 VRRP 우선 순위 구성

VLAN 인터페이스 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
vrrp [*vrid*] priority *value* (1~254)	VRRP 우선 순위를 구성합니다.
no vrrp [*vrid*] priority	VRRP 우선 순위를 기본 설정으로 복원합니다.

가상 주소와 포트 주소가 동일할 경우, VRRP는 자동으로 우선 순위 값을 255로 증가시킵니다.

가상 주소 또는 포트 주소가 변경되면, 우선 순위 값은 자동으로 원래 값으로 복원됩니다.

기본 우선 순위 값은 100입니다.

32.3.7 VRRP 클록 값(타이머) 구성

VLAN 인터페이스 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
vrrp [*vrid***] timer advertise { *value* | dsec *value* | csec *value* }**	RRP 클록 값 구성
no vrrp [*vrid***] timer advertise**	RRP 클록 값을 기본값으로 재개합니다.
no vrrp [*vrid***] timer learn**	VRRP 클록을 학습 모드로 구성합니다.

클록 값(clock value)은 가상 라우팅 OLT가 장애로부터 복구하는 데 필요한 최소 시간을 의미합니다.

마스터 라우팅 OLT가 다운되면, 백업 라우팅 OLT는 3*advertisement + skew_time 이후 마스터 OLT 역할을 수행하게 됩니다.

클록 값이 너무 크면 장애를 즉시 해결할 수 없습니다. 따라서, 클록의 기본 값 사용이 권장됩니다.

기본 값은 1초입니다.

32.3.8 VRRP 모니터링 오브젝트 구성

vlan 인터페이스 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
vrrp [*vrid***] track interface** *intf-id value*	VRRP가 로컬 인터페이스 상태를 모니터링하도록 구성
no vrrp [*vrid***] track interface** *intf-id*	기본 설정으로 복원
vrrp [*vrid***] track ip** *ip-address value*	지정된 주소에 대한 정적 라우팅 상태를 VRRP가 모니터링하도록 구성
no vrrp [*vrid***] track ip** *ip-address*	기본 설정으로 복원

VRRP 모니터링 기능을 통해 VRRP 그룹은 링크 상태 변화에 따라 우선순위를 적절하게 조정할 수 있습니다. 이를 통해 마스터 라인 상태에서 백업 라인 상태로 전환할 기회를 제공합니다. 링크 상태의 변화는 VRRP 라우팅 OLT를 우회하는 대상 링크가 연결 가능한지를 의미하며, VRRP OLT 자체의 연결 가능 여부는 의미하지 않습니다.

VRRP는 두 가지 모니터링 오브젝트를 지원합니다.
첫째, 인터페이스 상태를 모니터링합니다. 모니터링하는 포트의 링크 상태가 다운되면, 자체적으로 우선순위를 낮춥니다.
둘째, 지정된 노드의 정적 라우트 상태를 모니터링합니다. 모니터링하는 라우트가 연결 불가능할 경우, 자체적으로 우선순위를 낮춥니다. 지정된 노드의 정적 라우트 상태를 모니터링하려면 BFD(Bidirectional Forwarding Detection) 정적 라우트 감지 기능을 적용해야 합니다.

32.3.9 VRRP 모니터링 및 유지 관리

EXEC 구성 모드에서 다음 명령어를 실행합니다.

명령어	설명
show vrrp { brief | [interface *vlan_intf***] [detail]}**	VRRP 정보를 표시합니다.
debug vrrp [interface *intf-id vrid***] {errors | events | packets | all}**	VRRP 패킷 및 이벤트에 대한 디버그를 활성화하거나 비활성화합니다.
no debug vrrp	VRRP 패킷 및 이벤트에 대한 디버그를 비활성화합니다.

VRRP 정보 표시 예시

Switch_config#show vrrp interface vlan 1 detail

VLAN1 - Group 1

VRRP 상태는 Master입니다.

가상 IP 주소 : 192.168.20.110/24

가상 Mac 주소 : 0000.5e00.0101

현재 우선순위 : 100 (설정 값: 100)

VRRP 타이머 : Advertise 1.0 s (기본값) master_down 3.6 s

VRRP 현재 타이머 : Advertise 1.0 s master_down 0.0 s preempt after 0.0 s

인증 문자열은 설정되어 있지 않습니다.

Preempt는 설정됨 (지연 시간 : 0 s)

Advertise 간격 학습은 설정되어 있지 않습니다.

마스터 라우터 IP : 192.168.20.118, 우선순위 : 100, advertise 간격 : 1.0 s

32.3.10 VRRP 구성 예제

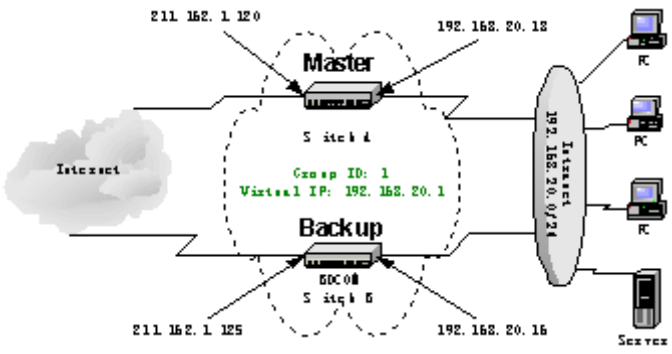


그림 59 네트워크 토폴로지

- OLT 스위치 A 구성

장애 1: 사설 네트워크 인터페이스에 주소를 설정합니다.

Switch_config_v1# ip address 192.168.20.18 255.255.255.0

장애 2: 공용 네트워크 인터페이스에 주소를 설정합니다.

Switch_config_v2# ip address 211.162.1.120 255.255.255.0

장애 3: 사설 네트워크 인터페이스에서 가상 스위치 그룹 1을 구성합니다. 가상 주소는 192.168.20.1이며, 우선순위 값은 120입니다.

Switch_config_v1# vrrp 1 associate 192.168.20.1 255.255.255.0

Switch_config_v1# vrrp 1 priority 120

장애 4: 가상 OLT에 대한 정보를 표시합니다.

Switch_config#show vrrp detail

VLAN1 - Group 1

VRRP 상태는 Master입니다.

가상 IP 주소 : 192.168.20.1/24

가상 Mac 주소 : 0000.5e00.0101

현재 우선순위 : 120 (설정 값: 120)

VRRP 타이머 : Advertise 1.0 s (기본값) master_down 3.6 s

VRRP 현재 타이머 : Advertise 1.0 s master_down 0.0 s preempt after 0.0 s

인증 문자열은 설정되어 있지 않습니다.

Preempt는 설정됨 (지연 시간 : 0 s)

Advertise 간격 학습은 설정되어 있지 않습니다.

마스터 라우터 IP : 192.168.20.18, 우선순위 : 100, advertise 간격 : 1.0 s

- OLT 스위치 B 구성

사설 네트워크 PC 및 서버 구성

사설 네트워크 인터페이스에 주소를 설정합니다.

Switch_config_v1# ip address 192.168.20.16 255.255.255.0

공용 네트워크 인터페이스에 주소를 설정합니다.

Switch_config_v2# ip address 211.162.1.125 255.255.255.0

가상 OLT 그룹 1을 사설 네트워크 인터페이스에서 구성합니다. 가상 주소는 192.168.20.1이며, 우선순위 값은 120입니다.

Switch_config_v1# vrrp 1 associate 192.168.20.1 255.255.255.0

가상 OLT 정보 표시

Switch_config#show vrrp detail

Switch_config#show vrrp interface vlan 1 detail

VLAN1 - Group 1

VRRP 상태는 Backup입니다.

가상 IP 주소 : 192.168.20.1/24

가상 Mac 주소 : 0000.5e00.0101

현재 우선순위 : 100 (설정 값: 100)

VRRP 타이머 : Advertise 1.0 s (기본값) master_down 3.6 s

VRRP 현재 타이머 : Advertise 0.0 s master_down 3.0 s preempt after 0.0 s

인증 문자열은 설정되어 있지 않습니다.

Preempt는 설정됨 (지연 시간 : 0 s)

Advertise 간격 학습은 설정되어 있지 않습니다.

마스터 라우터 IP : 192.168.20.18, 우선순위 : 120, advertise 간격 : 1.0 s

사설 네트워크 PC 및 서버 구성

사설 네트워크의 각 PC와 서버의 기본 게이트웨이를 192.168.20.1로 설정합니다.

33. 멀티캐스트 개요

전통적인 IP 전송 방식은 하나의 호스트가 단일 호스트와 통신하는 유니캐스트(unicast) 또는 모든 호스트와 통신하는 브로드캐스트(broadcast) 방식만을 허용합니다. 멀티캐스트(multicast) 기술은 하나의 호스트가 특정 호스트 그룹에 메시지를 전송할 수 있도록 합니다. 이러한 호스트는 그룹 멤버(group members)라고 합니다.

그룹 멤버에게 전송되는 메시지의 목적지 주소는 D 클래스 주소(224.0.0.0~239.255.255.255)입니다. 멀티캐스트 메시지는 UDP와 유사하게 전송되며, TCP와 같은 신뢰성 있는 전송 및 오류 제어 기능을 제공하지 않습니다.

송신자와 수신자는 멀티캐스트 애플리케이션을 구성합니다. 송신자는 그룹에 참여하지 않고도 멀티캐스트 메시지를 전송할 수 있습니다. 하지만 수신자는 그룹에서 메시지를 받기 전에 반드시 그룹에 가입해야 합니다.

그룹 멤버 간의 관계는 동적입니다. 호스트는 언제든지 그룹에 가입하거나 탈퇴할 수 있습니다. 그룹 멤버의 위치와 수에는 제한이 없으며, 필요하다면 하나의 호스트가 여러 그룹의 멤버가 될 수 있습니다. 따라서 그룹의 상태와 멤버 수는 시간에 따라 변화합니다.

라우터는 PIM-DM(Protocol Independent Multicast - Dense Mode) 및 PIM-SM(Sparse Mode)과 같은 멀티캐스트 라우팅 프로토콜을 실행하여 멀티캐스트 메시지를 전달하기 위한 라우팅 테이블을 유지합니다. 라우터는 직접 연결된 네트워크 세그먼트에서 IGMP(Internet Group Management Protocol)를 통해 그룹 멤버의 상태를 학습합니다. 호스트는 IGMP Report 메시지를 전송하여 지정된 IGMP 그룹에 가입할 수 있습니다.

IP 멀티캐스트 기술은 1 대 N 다중 멀티미디어 애플리케이션에 적합합니다.

참고 : 이 장에서 언급된 "라우터"는 라우팅 프로토콜을 실행하는 L3 스위치, 일반적인 네트워크 환경의 라우터, 그리고 기타 라우팅 프로토콜을 실행하는 장치를 포함합니다.

33.1 멀티캐스트 라우팅 구현

스위치 소프트웨어에서 멀티캐스트 라우팅은 다음과 같은 규칙을 포함합니다:

- IGMP는 LAN에서 라우터와 호스트 간에 실행되며, 그룹 멤버 관계를 추적하는 데 사용됩니다.
- PIM-DM/PIM-SM은 동적 멀티캐스트 라우팅 프로토콜입니다. 이 프로토콜은 스위치 간에 실행되며, 멀티캐스트 라우팅 테이블을 생성하여 멀티캐스트 포워딩을 구현합니다.

아래 그림은 IP 멀티캐스트 애플리케이션에서 사용되는 멀티캐스트 프로토콜을 보여줍니다.

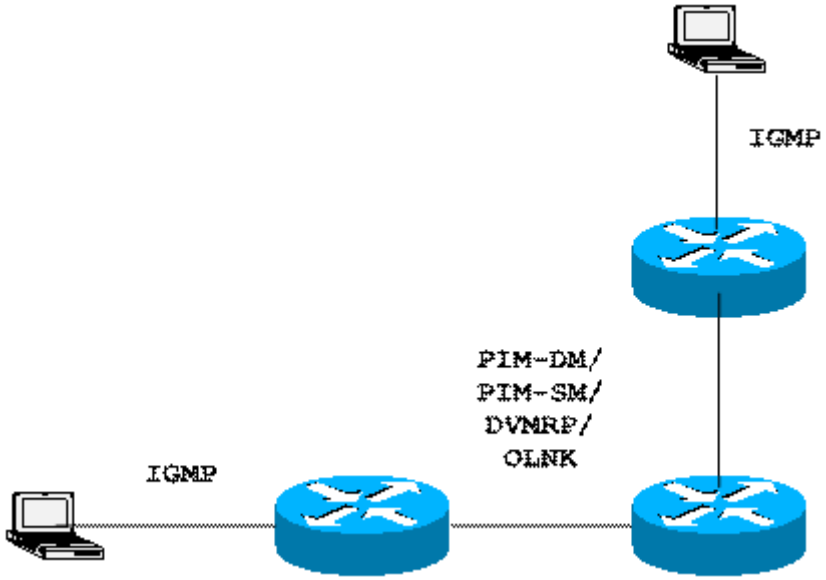


그림 60 네트워크 토폴로지

33.2 멀티캐스트 라우팅 구성 작업 목록

33.2.1 기본 멀티캐스트 구성 작업 목록

- 멀티캐스트 라우팅 시작 (필수)
- TTL 임계값 구성 (선택 사항)
- 빠른 멀티캐스트 포워딩 취소 (선택 사항)
- 정적 멀티캐스트 라우트 구성 (선택 사항)
- 멀티캐스트 경계 구성 (선택 사항)
- 멀티캐스트 헬퍼 구성 (선택 사항)
- Stub 멀티캐스트 라우트 구성 (선택 사항)
- 멀티캐스트 라우트 모니터링 및 유지 관리 (선택 사항)

33.2.2 IGMP 구성 작업 목록

- 현재 IGMP 버전 수정
- IGMP 쿼리 간격 구성
- IGMP 쿼리어(Querier) 간격 구성
- IGMP 최대 응답 시간 구성
- 마지막 IGMP 그룹 멤버의 쿼리 간격 구성

- 정적 IGMP 구성
- IGMP Immediate Leave(Immediate-leave) 목록 구성

33.2.3 PIM-DM 구성 작업 목록

- 타이머 설정
- PIM-DM 버전 지정
- 상태 갱신 구성
- 필터링 목록 구성
- DR(Designated Router) 우선순위 설정
- (S,G) 정보 삭제
-

33.2.4 PIM-SM 구성 작업 목록

- 정적 RP(랜데부 포인트) 구성
- 대기 BSR(부트스트랩 라우터) 구성
- 대기 RP 구성
- PIM-SM 멀티캐스트 라우팅 정보 표시
- PIM-SM에서 수집한 멀티캐스트 라우트 삭제

34. 기본 멀티캐스트 라우팅 구성

참고 : 이 장에서 언급된 "라우터"는 라우팅 프로토콜을 실행하는 L3 스위치, 일반적인 네트워크 환경의 라우터 및 기타 라우팅 프로토콜을 실행하는 장치를 포함합니다.

34.1 멀티캐스트 라우팅 시작

스위치 소프트웨어가 멀티캐스트 메시지를 전달하도록 하려면 멀티캐스트 라우팅을 시작해야 합니다. 글로벌 구성 모드에서 다음 명령어를 실행하여 멀티캐스트 메시지 포워딩을 활성화합니다

명령어	설명
ip multicast-routing	멀티캐스트 라우팅을 시작합니다.

34.2 포트에서 멀티캐스트 기능 시작

멀티캐스트 라우팅 프로토콜이 포트에서 실행될 때, 해당 포트에서 IGMP가 활성화됩니다. 멀티캐스트 라우팅 프로토콜에는 PIM-DM 및 PIM-SM이 포함됩니다. 동일한 포트에서 하나의 멀티캐스트 라우팅 프로토콜만 실행할 수 있습니다. 라우터가 여러 멀티캐스트 도메인에 연결되어 있는 경우, 서로 다른 멀티캐스트 프로토콜을 다른 포트에서 실행할 수 있습니다.

스위치 소프트웨어는 멀티캐스트 경계 라우터(MBR) 역할을 수행할 수 있습니다. 그러나 가능하다면 하나의 스위치에서 여러 멀티캐스트 라우팅 프로토콜을 동시에 실행하지 않는 것이 좋습니다. 일부 멀티캐스트 라우팅 프로토콜은 상호 간섭을 일으킬 수 있기 때문입니다. 예를 들어, PIM-DM(오직 (S, G) 엔트리 지원)과 BIDIR PIM-SM(오직 (*, G) 엔트리 지원)을 동시에 실행하면 혼란이 발생할 수 있습니다.

34.2.1 PIM-DM 시작

다음 명령어를 실행하여 포트에서 PIM-DM을 실행하고 멀티캐스트 덴스 모드(Dense Mode) 기능을 활성화합니다.

명령어	설명
ip pim-dm	PIM-DM이 실행될 포트로 진입하고, 포트 구성 모드에서 PIM-DM 멀티캐스트 라우팅 프로세스를 활성화합니다.

34.2.2 PIM-SM 시작

포트에서 **PIM-SM**을 실행하고 PIM-SM 멀티캐스트를 활성화하려면 다음 작업을 수행합니다.

명령어	설명
ip pim-sm	PIM-SM이 실행될 포트로 진입하고, 포트 구성 모드에서 PIM-SM 멀티캐스트 라우팅 프로세스를 활성화합니다.

34.3 TTL 임계값 구성

ip multicast ttl-threshold 명령어를 사용하여 포트를 통과할 수 있는 멀티캐스트 메시지의 TTL 임계값을 설정합니다.

no ip multicast ttl-threshold 명령어를 실행하면 기본 임계값인 1로 설정됩니다.

명령어	설명
ip multicast ttl-threshold *ttl-value*	포트의 TTL 임계값을 구성합니다.

예시 : 관리자가 포트에서 TTL 임계값을 설정하는 예제입니다

interface vlan1

ip multicast ttl-threshold 200

34.4 IP 멀티캐스트 경계 구성

ip multicast boundary 명령어를 사용하여 포트에 멀티캐스트 경계를 설정합니다.

no ip multicast boundary 명령어를 실행하면 설정된 경계를 취소합니다. 이후에 실행된 명령어는 이전에 설정된 명령어를 대체합니다.

명령어	설명
ip multicast boundary *access-list*	포트에 멀티캐스트 경계를 구성합니다.

예시 : 포트에서 관리 경계를 구성하는 예제입니다.

interface vlan1

ip multicast boundary acl

!

ip access-list standard acl

permit 192.168.20.97 255.255.255.0

34.5 IP 멀티캐스트 헬퍼 구성

ip multicast helper-map 명령어를 실행하여 멀티캐스트 네트워크에서 두 개의 브로드캐스트 네트워크를 연결하는 멀티캐스트 라우트를 사용합니다.

no ip multicast helper-map 명령어를 실행하면 해당 설정이 취소됩니다.

소스 브로드캐스트 네트워크에 연결된 첫 번째 홉 라우터에서 실행합니다.

명령어	설명
interface *type number*	인터페이스 구성 모드로 진입합니다.
ip multicast helper-map broadcast *group-address access-list*	브로드캐스트 메시지를 멀티캐스트 메시지로 변환하도록 구성합니다.
ip directed-broadcast	방향성 브로드캐스트를 허용합니다.
ip forward-protocol [*port*]	메시지 전달을 허용할 포트 번호를 구성합니다.

목적지 브로드캐스트 네트워크에 연결된 마지막 홉 라우터에서 실행합니다.

명령어	설명
interface *type number*	인터페이스 구성 모드로 진입합니다.
ip directed-broadcast	방향성 브로드캐스트를 허용합니다.
ip multicast helper-map *group-address broadcast-address access-list*	멀티캐스트 메시지를 브로드캐스트 메시지로 변환하도록 구성합니다.
ip forward-protocol [port]	메시지 전달을 허용할 포트 번호를 구성합니다.

예시 : IP 멀티캐스트 헬퍼 구성

다음 예시는 ip multicast helper 명령어를 구성하는 방법을 보여줍니다.

아래 구성에서 첫 번째 홉 라우터의 vlan1 포트에 ip directed-broadcast를 설정하여 방향성 메시지를 처리하도록 합니다.

ip multicast helper-map broadcast 230.0.0.1 testacl1 명령어를 사용하여, 소스 주소 192.168.20.97/24에서 포트 번호 4000으로 전송된 UDP 브로드캐스트 메시지를 목적지 주소 230.0.0.1의 멀티캐스트 메시지로 변환하도록 구성합니다.

마지막 홉 라우터의 vlan1 포트에도 ip directed-broadcast를 설정하여 방향성 메시지를 처리하도록 합니다.

ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2 명령어를 사용하여, 소스 주소 192.168.20.97/24에서 포트 번호 4000으로 전송된 목적지 주소 230.0.0.1의 멀티캐스트 메시지를 목적지 주소 172.10.255.255의 브로드캐스트 메시지로 변환합니다.

소스 브로드캐스트 네트워크에 연결된 첫 번째 홉 라우터 구성

```
interface vlan1
ip directed-broadcast
ip multicast helper-map broadcast 230.0.0.1 testacl
ip pim-dm
!
ip access-list extended testacl
   permit udp 192.168.20.97 255.255.255.0 any
!
ip forward-protocol udp 4000
```

목적지 브로드캐스트 네트워크에 연결된 마지막 홉 라우터 구성

```
interface vlan2
ip directed-broadcast
ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2
ip pim-dm
!
ip access-list extended testacl2
   permit udp 192.168.20.97 255.255.255.0 any
!
ip forward-protocol udp 4000
```

34.6 Stub 멀티캐스트 라우트 구성

ip igmp helper-address 및 ip pim-dm neighbor-filter 명령어를 사용하여 Stub 멀티캐스트 라우트를 구성합니다.

Stub 라우터와 호스트가 연결된 포트에서 수행할 작업

명령어	설명
interface *type number*	인터페이스 구성 모드로 진입합니다.
ip igmp helper-address *destination-address*	멀티캐스트 메시지를 중앙 라우터로 전달하기 위해 IGMP 헬퍼 주소를 설정합니다.

중앙 라우터와 Stub 라우터가 연결된 포트에서 수행할 작업

명령어	설명
interface *type number*	인터페이스 구성 모드로 진입합니다.
ip pim-dm neighbor-filter *access-list*	Stub 라우터에서 모든 PIM 메시지를 필터링합니다.

34.7 멀티캐스트 라우트 모니터링 및 유지 관리

- 멀티캐스트 캐시 및 라우팅 테이블 삭제

  특정 캐시나 라우팅 테이블이 유효하지 않은 경우, 내용을 삭제해야 합니다.
  관리 모드에서 다음 명령어를 실행합니다.

명령어	설명
clear ip igmp group [*type number*] [*group-address*	*<cr>*]	IGMP 캐시의 항목을 지웁니다.
clear ip mroute *[*	*group-address*	*source-address]*	멀티캐스트 라우팅 테이블의 항목을 지웁니다.

- 멀티캐스트 라우팅 테이블 및 시스템 통계 정보 표시

  IP 멀티캐스트 라우팅 테이블, 캐시 또는 데이터베이스에 대한 상세 정보는 자원 사용 현황을 파악하고 네트워크 문제를 해결하는 데 도움이 됩니다.
  관리 모드에서 다음 명령어를 실행하여 멀티캐스트 라우트의 통계 정보를 확인합니다.

명령어	설명
show ip igmp groups [*type number*	*group-address*] [**detail**]	IGMP 캐시의 멀티캐스트 그룹에 대한 정보를 표시합니다.
show ip igmp interface [*type number*]	인터페이스의 IGMP 구성 정보를 표시합니다.
show ip mroute mfc	멀티캐스트 전달 캐시를 표시합니다.
show ip rpf [**pim-dm**	**pim-sm**] *source-address*	RPF 정보를 표시합니다.

35.IGMP 구성

35.1 개요

- IGMP

인터넷 그룹 관리 프로토콜(IGMP)은 멀티캐스트 그룹 멤버를 관리하는 데 사용되는 프로토콜입니다. IGMP는 호스트 측과 스위치 측을 포함하는 비대칭 프로토콜입니다. 호스트 측에서 IGMP 프로토콜은 멀티캐스트 그룹 멤버인 호스트가 속한 멀티캐스트 그룹을 보고하는 방법과 호스트가 스위치의 쿼리 메시지에 응답하는 방법을 조절합니다. 라우터 측에서 IGMP 프로토콜은 IGMP 지원 스위치가 로컬 네트워크의 호스트의 멀티캐스트 그룹 멤버 ID를 학습하는 방법과 호스트의 보고 메시지에 따라 저장된 멀티캐스트 그룹 멤버 정보를 수정하는 방법을 조절합니다.

스위치는 IGMP 라우터 프로토콜을 지원하므로 멀티캐스트 라우팅 프로토콜에 현재 네트워크의 멀티캐스트 그룹 멤버에 대한 정보를 제공하고 스위치는 멀티캐스트 메시지를 전달할지 여부를 결정합니다. 간단히 말해서 스위치가 IP 메시지의 멀티캐스트 프로세스를 지원할 수 있도록 하려면 스위치를 멀티캐스트 라우팅 프로토콜과 IGMP 라우터 프로토콜을 지원하도록 구성해야 합니다. 현재, 저희 스위치는 IGMP 라우터 프로토콜과 최신 버전인 버전 3 IGMP를 지원합니다.

IGMP에 대한 독립적인 시작 명령은 없습니다. IGMP-라우터 프로토콜의 기능은 멀티캐스트 라우팅 프로토콜을 통해 시작됩니다.

참고:

이 장에서 언급하는 "라우터"는 라우팅 프로토콜을 실행하는 레이어 3 스위치, 일반 네트워크 환경의 라우터 및 라우팅 프로토콜을 실행하는 다른 장치를 말합니다.

35.2 IGMP 구성

IGMP 라우터(IGMP-Router)의 속성을 구성하는 명령어는 주로 IGMP 파라미터를 조정하는 명령어입니다. 아래에서는 이러한 명령어에 대해 설명합니다. IGMP 명령어에 대한 자세한 내용은 관련 명령어 설명 문서를 참조하세요.

35.2.1 현재 IGMP 버전 변경

현재까지 IGMP 프로토콜은 세 가지 공식 버전이 존재합니다. 해당 RFC는 RFC1112, RFC2236, RFC3376입니다.

- IGMP V1: 멀티캐스트 그룹 멤버를 기록하는 기능만 지원합니다.
- IGMP V2: 특정 멀티캐스트 그룹 멤버를 쿼리하고, IGMP 호스트가 멀티캐스트 그룹을 탈퇴할 때 Leave 메시지를 생성하며, 그룹 멤버 변경 지연 시간을 단축합니다.

- IGMP V3: 멀티캐스트 그룹 멤버 ID를 소스 호스트 주소와 매핑하여 업데이트 및 유지 관리하는 기능이 추가되었습니다.

IGMP V3 라우터 프로토콜은 IGMP V1 및 IGMP V2 호스트와 완벽하게 호환됩니다.
스위치 소프트웨어는 IGMP V1, V2, V3의 IGMP 라우터 프로토콜을 모두 지원합니다.

IGMP-Router 기능 구성

IGMP-Router 기능은 서로 다른 인터페이스에서 구성할 수 있으며, 각 인터페이스에서 다른 버전의 IGMP를 실행할 수 있습니다.

동일한 네트워크에 연결된 여러 포트 중 하나에서만 IGMP-Router 기능을 활성화할 수 있다는 점에 유의하세요.

다음 명령어를 인터페이스 구성 모드에서 실행하여 특정 포트에서 IGMP 라우터 프로토콜 버전을 변경합니다.

명령어	설명
ip igmp version *version_number*	인터페이스 구성 모드로 진입합니다.

35.2.2 IGMP 쿼리 간격 구성

현재 IGMP 라우터 프로토콜의 버전에 관계없이, 멀티캐스트 스위치는 IGMP 라우터 기능이 활성화된 포트에서 일정 시간마다 IGMP General Query 메시지를 전송합니다.
이 메시지는 224.0.0.1 주소로 전송됩니다.

멀티캐스트 스위치의 목적은 IGMP 호스트로부터 리포트(Report) 메시지를 수신해, 네트워크의 각 IGMP 호스트가 어떤 멀티캐스트 그룹에 속하는지 파악하는 것입니다.
이 General Query 메시지를 전송하는 주기를 IGMP 쿼리 간격(Query Interval)이라고 합니다.

- IGMP 쿼리 간격이 너무 크면, 스위치가 IGMP 호스트가 속한 멀티캐스트 그룹 정보를 즉시 받지 못할 수 있습니다.
- IGMP 쿼리 간격이 너무 작으면, 네트워크에서 IGMP 메시지 트래픽이 증가합니다.

다음 명령어를 인터페이스 구성 모드에서 실행하여 포트의 IGMP 쿼리 간격을 수정합니다.

명령어	설명
ip igmp query-interval *time*	현재 인터페이스의 IGMP 쿼리 간격을 수정합니다. (단위: 초)

35.2.3 IGMP 쿼리어 간격 구성

IGMP 라우터 프로토콜 버전 2 및 버전 3에서는, 동일 네트워크에 IGMP 라우터 프로토콜을 실행하는 다른 스위치가 존재하는 경우 쿼리어(Querier)를 선택해야 합니다.

쿼리어는 쿼리 메시지를 전송할 수 있는 스위치(실제로는 IGMP 라우터 프로토콜이 활성화된 스위치의 포트)를 의미합니다.

- 일반적으로 하나의 네트워크에는 하나의 쿼리어만 존재하며, 이 스위치만이 IGMP 쿼리 메시지를 전송합니다.
- IGMP 라우터 V1에서는 쿼리어 선택이 없으며, 멀티캐스트 라우팅 프로토콜에 의해 쿼리 메시지를 보낼 스위치가 결정됩니다.

IGMP 라우터 V2 및 V3는 동일한 쿼리어 선택 메커니즘을 사용합니다:

- 네트워크에서 IP 주소가 가장 작은 스위치가 쿼리어가 됩니다.
- 쿼리어가 아닌 스위치는 쿼리어의 존재를 기록하는 타이머를 유지합니다.
- 타이머가 만료되면, 쿼리어가 아닌 스위치는 쿼리어 역할을 수행하며, 더 작은 IP 주소를 가진 스위치로부터 IGMP 쿼리 메시지를 받을 때까지 쿼리어로 남습니다.

IGMP 라우터 V2에서는 다음 명령어를 사용해 쿼리어 타임아웃 간격을 구성할 수 있습니다.

명령어	설명
ip igmp querier-timeout *time*	다른 쿼리어의 타임아웃 간격을 설정합니다. (단위: 초)

- GMP 라우터 V1에서는 쿼리어 타임아웃 간격이 필요하지 않습니다.
- IGMP 라우터 V3에서는 타임아웃 간격이 프로토콜에 의해 자동으로 결정되므로, 별도로 구성할 수 없습니다.

따라서, 위 명령어는 IGMP 라우터 V2에서만 유효합니다.

35.2.4 최대 IGMP 응답 시간 구성

IGMP 라우터 V2 및 V3에서는 전송되는 IGMP General Query 메시지의 특정 데이터 필드가 IGMP 호스트의 최대 응답 시간을 규정합니다. 즉, IGMP 호스트는 규정된 최대 응답 시간이 만료되기 전에 응답 메시지를 전송하여 General Query 메시지를 수신했음을 나타내야 합니다.

- 최대 응답 시간이 크게 설정되면, 멀티캐스트 그룹 멤버 변경이 지연됩니다.
- 최대 응답 시간이 작게 설정되면, 네트워크 내 IGMP 메시지 트래픽이 증가합니다.

참고 : 최대 IGMP 응답 시간은 IGMP 쿼리 간격보다 짧아야 합니다.
만약 최대 응답 시간이 쿼리 간격보다 크다면, 시스템은 최대 응답 시간을 쿼리 간격에서 1을 뺀 값으로 자동 설정합니다.

IGMP 라우터 V2 및 V3에서는 인터페이스 구성 모드에서 다음 명령어를 실행하여 최대 IGMP 응답 시간을 설정합니다.

명령어	설명
ip igmp query-max-response-time *time*	마지막 그룹 멤버의 IGMP 쿼리 간격을 구성합니다. (단위: 밀리초)

IGMP 라우터 V1에서는 최대 IGMP 응답 시간이 프로토콜 자체에 의해 결정됩니다. 따라서 위 명령어는 IGMP 라우터 V1에서는 사용되지 않습니다.

35.2.5 마지막 그룹 멤버의 IGMP 쿼리 간격 구성

IGMP 라우터 V2 및 V3에서는 특정 멀티캐스트 그룹에 대한 Group Specific Query 메시지가 전송될 때, 마지막 그룹 멤버의 쿼리 간격이 호스트의 최대 응답 시간으로 사용됩니다.
즉, IGMP 호스트는 마지막 그룹 멤버의 최대 응답 시간이 만료되기 전에 응답 메시지를 전송하여 Group Specific Query 메시지를 수신했음을 나타내야 합니다.

- IGMP 호스트가 쿼리 메시지에 응답할 필요가 없다고 판단하면, 간격이 지나면 응답하지 않습니다.
- 이 경우, 멀티캐스트 스위치는 저장된 멀티캐스트 그룹 멤버 정보를 업데이트합니다.
- 마지막 그룹 멤버의 쿼리 간격이 크게 설정되면, 멀티캐스트 그룹 멤버 변경이 지연됩니다.
- 쿼리 간격이 작게 설정되면, 네트워크 내 IGMP 메시지 트래픽이 증가합니다.

IGMP 라우터 V2 및 V3에서는 인터페이스 구성 모드에서 다음 명령어를 실행하여 마지막 그룹 멤버의 IGMP 쿼리 간격을 설정합니다.

명령어	설명
ip igmp last-member-query-interval *time*	마지막 그룹 멤버의 IGMP 쿼리 간격을 설정합니다. (단위: 밀리초)

이 명령어는 IGMP 라우터 V1에서는 사용되지 않습니다.

35.2.6 정적 IGMP 구성

IGMP 라우터 프로토콜에서 규정된 기능 외에도, 스위치는 포트에서 정적 멀티캐스트 그룹 구성을 지원합니다.

IGMP 호스트의 멀티캐스트 그룹 멤버 관계는 변동될 수 있습니다. 예를 들어, IGMP 호스트가 처음에는 멀티캐스트 그룹 group1에 속해 해당 그룹에서 멀티캐스트 메시지를 수신하고 전송합니다. 일정 시간이 지나면, IGMP 호스트는 group2에 속하게 되어 group2에서 메시지를 주고받습니

다. 이후에는 어떤 멀티캐스트 그룹에도 속하지 않을 수 있습니다. 이처럼 멀티캐스트 그룹 할당 정보는 계속해서 변동됩니다.

이러한 동적 멀티캐스트 그룹과 달리, 특정 포트가 정적 멀티캐스트 그룹에 속하도록 구성된 경우, 멀티캐스트 라우팅 프로토콜은 해당 포트를 해당 멀티캐스트 그룹의 메시지를 항상 수신 및 전송하는 포트로 간주합니다.

IGMP 라우터 V3와의 호환성을 높이기 위해, 정적 멀티캐스트 그룹은 지정된 소스 주소에서 멀티캐스트 메시지를 수신하도록 구성할 수 있습니다. 즉, 멀티캐스트 메시지를 수신할 때 소스 필터 기능이 추가됩니다.

인터페이스 구성 모드에서 다음 명령어를 실행하여 포트의 정적 멀티캐스트 그룹을 구성합니다.

명령어	설명
ip igmp static-group { * | *group-address*} {**include** *source-address* | *<cr>* }	포트의 정적 멀티캐스트 그룹 속성을 구성합니다.

35.2.7 IGMP Immediate Leave 목록 구성

스위치 포트에서 IGMP V2가 활성화되어 있고, 해당 포트가 연결된 네트워크에 단 하나의 IGMP 호스트만 존재하는 경우, IGMP Immediate Leave 목록을 구성하여 IGMP 호스트의 Immediate Leave 기능을 구현할 수 있습니다.

IGMP V2 규정에 따르면, 호스트가 특정 멀티캐스트 그룹에서 탈퇴할 때 Leave 메시지를 모든 멀티캐스트 스위치로 전송합니다. 멀티캐스트 스위치는 Leave 메시지를 받은 후 Group Specific 메시지를 전송하여 해당 포트에서 해당 멀티캐스트 그룹으로부터 수신 또는 전송할 멀티캐스트 메시지가 남아 있는지 확인합니다.

Immediate Leave 기능이 구성되어 있으면, IGMP 호스트와 멀티캐스트 스위치 간의 메시지 교환 없이 즉시 그룹에서 탈퇴할 수 있으며, 멀티캐스트 그룹 멤버 ID의 변경이 지연되지 않습니다.

참고 : 해당 명령어는 글로벌 구성 모드와 인터페이스 구성 모드에서 모두 설정할 수 있습니다. 글로벌 구성 모드에서 설정한 명령어의 우선순위가 인터페이스 구성 모드에서 설정한 명령어보다 높습니다.

- 글로벌 구성 모드에서 먼저 명령어를 설정하면, 인터페이스 구성 모드에서 설정한 명령어는 무시됩니다.
- 인터페이스 구성 모드에서 먼저 명령어를 설정한 경우, 글로벌 구성 모드에서 명령어를 설정하면 인터페이스 구성 모드에서 설정한 명령어가 삭제됩니다.

IGMP 라우터 V2에서는 인터페이스 구성 모드에서 다음 명령어를 실행하여 IGMP Immediate Leave 목록을 구성합니다.

명령어	설명
ip igmp immediate-leave group-list *list-name*	IGMP 호스트가 멀티캐스트 그룹에서 Immediate Leave 하도록 액세스 리스트를 구성합니다.
ip access-list standard *list-name*	list-name이라는 이름의 표준 IP 액세스 리스트를 생성합니다.
permit *source-address*	Immediate Leave 기능을 수행할 IGMP 호스트의 IP 주소를 표준 액세스 리스트 구성 모드에서 설정합니다.

35.3 IGMP 특성 구성 예시

- IGMP 버전 변경 예시

상위 버전의 IGMP 라우터 프로토콜은 하위 버전의 IGMP 호스트와 호환됩니다. 하지만 상위 버전의 IGMP 라우터 프로토콜은 하위 버전의 IGMP 라우터 프로토콜과 호환되지 않습니다.

따라서, 현재 네트워크에 하위 버전의 IGMP 라우터 프로토콜을 실행하는 스위치가 존재하는 경우, 동일한 네트워크 세그먼트에서는 상위 버전의 IGMP 라우터 프로토콜을 하위 버전으로 변경해야 합니다.

예를 들어, 네트워크에 IGMP 라우터 V1 및 V2를 실행하는 스위치가 존재하는 경우, 관리자는 IGMP 라우터 V2를 실행하는 스위치의 포트에서 IGMP 라우터 프로토콜 버전을 V1으로 변경해야 합니다.

interface vlan 1

ip igmp version 1

- IGMP 쿼리 간격 구성 예시

다음 예시는 인터페이스 vlan 1에서 IGMP 쿼리 간격을 50초로 수정하는 방법을 보여줍니다.

interface vlan 1

ip igmp query-interval 50

IGMP 라우터 V2 및 V3에서는 동일 네트워크에 동일한 IGMP 라우터 프로토콜을 실행하는 라우터가 여러 대 존재할 경우 쿼리어(Querier)를 선택해야 합니다.

쿼리어는 쿼리 패킷을 전송하는 라우터를 의미하며, 실제로는 IGMP 라우터 프로토콜이 활성화된 특정 포트를 의미합니다.

일반적으로 하나의 네트워크에는 하나의 쿼리어만 존재하며, 해당 라우터만 IGMP 쿼리 메시지를 전송합니다.

IGMP 라우터 V1에서는 멀티캐스트 라우팅 프로토콜이 쿼리 메시지를 전송할 라우터를 지정하므로 쿼리어 선택 문제가 발생하지 않습니다.

IGMP 라우터 V2 및 V3는 동일한 쿼리어 선택 메커니즘을 사용합니다. 네트워크에서 가장 작은 IP 주소를 가진 라우터가 쿼리어가 됩니다.

쿼리어가 아닌 라우터는 쿼리어의 존재 시간을 기록하는 타이머를 유지해야 합니다.

타이머가 만료되면 쿼리어가 아닌 라우터는 쿼리어가 되어 IGMP 쿼리 패킷을 전송하기 시작합니다.

이후 더 작은 IP 주소를 가진 라우터로부터 IGMP 쿼리 패킷을 수신하면 다시 쿼리어가 아닌 상태로 돌아갑니다.

IGMP 라우터 V2에서는 다음 명령어를 사용해 다른 쿼리어의 타임아웃 간격을 구성할 수 있습니다.

명령어	설명
ip igmp querier-timeout *time*	른 쿼리어의 타임아웃 간격을 설정합니다. (단위: 초)

IGMP 라우터 V1에서는 다른 쿼리어의 타임아웃 간격이 필요하지 않습니다. IGMP 라우터 V3에서는 해당 타임아웃 간격이 프로토콜에 의해 자동으로 설정되며, 별도로 구성할 수 없습니다.

따라서, 위 명령어는 IGMP 라우터 V2에서만 유효합니다.

- IGMP 쿼리어 간격 구성 예시

다음 예시는 인터페이스 vlan 1에서 IGMP 쿼리어 간격을 100초로 수정하는 방법을 보여줍니다.

interface vlan 1

ip igmp querier-timeout 100

- 최대 IGMP 응답 시간 구성 예시

다음 예시는 인터페이스 vlan 1에서 최대 IGMP 응답 시간을 15초로 수정하는 방법을 보여줍니다.

interface vlan 1

ip igmp query-max-response-time 15

- 마지막 그룹 멤버의 IGMP 쿼리 간격 구성 예시

다음 예시는 인터페이스 vlan 1에서 마지막 그룹 멤버의 IGMP 쿼리 간격을 2000ms로 수정하는 방법을 보여줍니다.

interface vlan 1

ip igmp last-member-query-interval 2000

- 정적 IGMP 구성 예시

정적 멀티캐스트 그룹의 구성 명령어는 서로 다른 매개변수를 사용하여 다양한 유형의 정적 멀티캐스트 그룹을 정의할 수 있습니다.
다음 예시는 다양한 명령어 매개변수 실행 결과를 보여줍니다.

interface vlan 1

ip igmp static-group *

위 명령어는 인터페이스 vlan 1에서 모든 정적 멀티캐스트 그룹을 구성합니다.
멀티캐스트 라우팅 프로토콜은 모든 IP 멀티캐스트 메시지를 인터페이스 vlan 1로 전달합니다.

interface vlan 1

ip igmp static-group 224.1.1.7

위 명령어는 인터페이스 vlan 1에서 멀티캐스트 그룹 224.1.1.7을 정적으로 구성합니다.
즉, 해당 인터페이스는 멀티캐스트 그룹 224.1.1.7에 속합니다.
멀티캐스트 라우팅 프로토콜은 멀티캐스트 그룹 224.1.1.7로 전송되는 모든 IP 멀티캐스트 메시지를 인터페이스 vlan 1로 전달합니다.

interface vlan 1

ip igmp static-group 224.1.1.7 include 192.168.20.168

위 명령어는 인터페이스 vlan 1에서 멀티캐스트 그룹 224.1.1.7을 정적으로 구성하고, 소스 필터를 192.168.20.168로 설정합니다.

즉, 해당 인터페이스는 멀티캐스트 그룹 224.1.1.7에 속하지만, 192.168.20.168에서 오는 IP 멀티캐스트 메시지만 수신합니다.

멀티캐스트 라우팅 프로토콜은 192.168.20.168에서 수신되고 멀티캐스트 그룹 224.1.1.7로 전송되는 IP 멀티캐스트 메시지를 인터페이스 vlan 1로 전달합니다.

다음 명령어를 인터페이스 구성 모드에서 실행하여, 192.168.20.169에서 전송되고 멀티캐스트 그룹 224.1.1.7로 최종 전송되는 IP 멀티캐스트 메시지를 수신합니다.

ip igmp static-group 224.1.1.7 include 192.168.20.169

위 명령어는 여러 번 실행하여 다른 소스 주소를 정의할 수 있습니다.

ip igmp static-group 224.1.1.7

ip igmp static-group 224.1.1.7 include 192.168.20.168

두 번째 명령어(ip igmp static-group 224.1.1.7 include 192.168.20.168)는 무시됩니다.

- IGMP immediate-leave 목록 구성 예시

다음 예시는 인터페이스 vlan 1에서 immediate-leave 기능을 사용하여, 액세스 리스트에 IGMP 호스트 IP 주소 192.168.20.168을 추가하는 방법을 보여줍니다.

이 구성은 IP 주소 192.168.20.168을 가진 IGMP 호스트가 즉시 탈퇴 기능을 수행할 수 있도록 보장합니다.

```
interface vlan 1
ip igmp immediate-leave imme-leave
!
ip access-list standard imme-leave
permit 192.168.20.168
```

36.PIM-DM 구성

36.1 PIM-DM 개요

프로토콜 독립 멀티캐스트 덴스 모드(Protocol Independent Multicast Dense Mode, PIM-DM)는 덴스 모드에서 동작하는 멀티캐스트 라우팅 프로토콜입니다.

기본적으로, 멀티캐스트 소스가 멀티캐스트 데이터를 전송하기 시작하면 도메인의 모든 네트워크 노드는 해당 데이터를 수신합니다.

따라서 PIM-DM은 브로드캐스트-프루닝(broadcast-pruning) 방식으로 멀티캐스트 패킷을 전달합니다.

멀티캐스트 소스가 데이터를 전송하기 시작하면, 인접한 스위치는 RPF(Reverse Path Forwarding) 인터페이스를 제외한 모든 PIM 활성화 인터페이스로 멀티캐스트 패킷을 전달합니다.

이 방식으로, PIM-DM 도메인의 모든 네트워크 노드는 멀티캐스트 패킷을 수신할 수 있습니다.

멀티캐스트 포워딩을 완료하기 위해, 인접한 스위치는 그룹 G와 소스 S에 대한 (S,G) 멀티캐스트 라우팅 항목을 생성해야 합니다.

(S,G) 라우팅 항목은 멀티캐스트 소스 주소, 멀티캐스트 그룹 주소, 인입 인터페이스, 아웃고잉 인터페이스 목록, 타이머 및 상태 정보를 포함합니다.

특정 네트워크 세그먼트에 멀티캐스트 그룹 멤버가 없으면, PIM-DM은 프루닝(pruning) 정보를 전송하고, 해당 세그먼트를 연결하는 포워딩 인터페이스를 프루닝하여 프루닝 상태를 설정합니다.

프루닝 상태에는 타임아웃 타이머가 설정됩니다. 타이머가 만료되면 프루닝 상태는 다시 포워딩 상태로 전환되며, 멀티캐스트 데이터는 해당 브랜치를 따라 전달됩니다.

프루닝 상태에는 멀티캐스트 소스와 멀티캐스트 그룹에 대한 정보가 포함됩니다.

프루닝된 영역에 멀티캐스트 그룹 멤버가 나타나면, PIM-DM은 상위 네트워크에서 타이머가 만료될 때까지 기다리지 않고 즉시 그래프트(graft) 메시지를 전송하여 프루닝 상태를 포워딩 상태로 전환합니다.

소스 S가 여전히 그룹 G로 데이터를 전송하는 동안, 첫 번째 홉 스위치는 주기적으로 (S,G) 라우팅 항목의 갱신 정보를 초기 브로드캐스트 트리로 전송하여 상태를 갱신합니다.

PIM-DM의 상태 갱신 메커니즘은 하위 네트워크의 상태를 갱신하여 브로드캐스트 트리가 타임아웃되지 않도록 보장합니다.

다중 액세스 네트워크에서 PIM-DM 메커니즘

DR(Designated Router) 선택 외에도, PIM-DM은 다음과 같은 메커니즘을 도입합니다:

- 어서션(assertion) 메커니즘: 중복된 멀티캐스트 패킷이 전달되는 것을 방지하기 위해 유일

한 포워더를 선택합니다.

- Add/Prune 억제 메커니즘: 불필요한 Add/Prune 정보를 줄입니다.
- 프루닝 거부 메커니즘: 잘못된 프루닝 동작을 방지합니다.

PIM-DM 도메인에서 PIM-DM을 실행하는 라우터는 주기적으로 Hello 정보를 전송하여 다음을 수행합니다:

- 인접 PIM 라우터를 검색합니다.
- 리프(leaf) 네트워크 및 리프 라우터를 판단합니다.
- 다중 액세스 네트워크에서 지정 라우터(DR)를 선택합니다.

DR(Designated Router) 선택

IGMP v1과의 호환성을 위해, PIM-DM은 DR 선택을 담당합니다.

해당 인터페이스에서 모든 PIM 인접 라우터가 DR 우선순위를 지원하는 경우, 우선순위가 높은 인접 라우터가 DR로 선택되며 우선순위가 동일한 경우, 인터페이스 IP 주소가 가장 큰 인접 라우터가 DR로 선택됩니다.

여러 라우터의 Hello 메시지에서 우선순위가 표시되지 않은 경우, 인터페이스 IP 주소가 가장 큰 라우터가 DR로 선택됩니다.

스위치의 PIM-DM v2는 다음을 지원합니다.

- 인접 필터 목록
- CIDR(Classless Inter-Domain Routing)
- VLSM(Variable Length Subnet Mask)
- IGMP v1~v3

참고 : 이 장에서 언급된 "라우터"는 라우팅 프로토콜을 실행하는 레이어 3 스위치, 일반 네트워크 환경의 라우터 및 기타 라우팅 프로토콜을 실행하는 장치를 포함합니다.

36.2 PIM-DM 구성

36.2.1 타이머 수정

라우팅 프로토콜은 Hello 메시지 및 상태 갱신(state-refresh) 제어 메시지의 전송 주기를 결정하기 위해 여러 타이머를 사용합니다. Hello 메시지 전송 간격은 인접 관계(neighbor relationship)가 올바르게 생성되는지에 영향을 미칩니다.

다음 명령어를 스위치 구성 모드에서 실행하여 타이머를 조정합니다.

명령어	설명

ip pim-dm hello-interval	인터페이스 및 인접 장치에서 Hello 메시지를 전송하는 간격을 설정합니다. (단위: 초)
ip pim-dm state-refresh origination-interval	소스에 직접 연결된 첫 번째 홉 스위치에서 상태 갱신 메시지를 전송하는 간격을 설정합니다. 이 간격은 업스트림 포트에서만 유효합니다. 이후 스위치에서는 상태 갱신 메시지를 수신하고 처리하는 주기가 됩니다.

36.2.2 버전 번호 지정

라우터의 PIM-DM은 PIM v2만을 지원합니다.
PIM v1은 더 이상 사용되지 않으며, 기본적으로 PIM v2를 지원합니다.여기에서 사용하는 명령어는 이전 스타일과의 호환성을 위한 것입니다.

명령어	설명
ip pim-dm version *version*	인터페이스 및 인접 장치에서 Hello 메시지를 전송하는 간격을 설정합니다. (단위: 초)

36.2.3 상태 갱신 구성

기본적으로 PIM-DM의 상태 갱신 제어 정보는 관리 모드에서 전달됩니다.
인터페이스 구성 모드에서의 설정 명령어는 소스에 직접 연결된 첫 번째 홉 스위치가 주기적으로 상태 갱신 메시지를 전송할 때, 업스트림 포트에만 유효합니다.
이후 스위치에서는 상태 갱신 메시지를 수신하고 처리하는 주기가 됩니다.

명령어	설명
no ip pim-dm state-refresh disable	포트에서 상태 갱신 메시지를 송수신할 수 있도록 허용합니다.
ip pim-dm state-refresh origination-interval	포트에서 상태 갱신 메시지를 송수신하는 간격을 설정합니다.

36.2.4 필터링 목록 구성

PIM-DM은 기본적으로 필터링 목록을 설정하지 않습니다.
여기서 말하는 필터링 목록은 neighbor 필터링 목록과 멀티캐스트 경계 필터링 목록을 포함합니다.
필터링 목록은 인터페이스 구성 모드에서 설정해야 합니다.

- 특정 네트워크 세그먼트의 스위치가 PIM-DM 협상에 참여하지 못하도록 하려면 이웃 필터링 목록을 구성해야 합니다.
- 일부 그룹이 로컬 영역을 통과하는 것을 금지하거나 허용하려면 멀티캐스트 경계 필터링 목록을 구성해야 합니다.

명령어	설명
ip pim-dm neighbor-filter	neighbor 필터링 목록을 구성합니다.
ip multicast boundary	멀티캐스트 경계 필터링 목록을 구성합니다.

36.2.5 DR 우선순위 설정

IGMP v1과의 호환성을 위해 DR(Designated Router) 선택이 필요합니다.
기본적으로 DR의 우선순위는 1로 설정되어 있습니다.

- 인터페이스의 모든 PIM 인접 라우터가 DR 우선순위를 지원하는 경우, 우선순위가 높은 라우터가 DR로 선택됩니다.
- 우선순위가 동일한 경우, 인터페이스 IP 주소가 가장 큰 라우터가 DR로 선택됩니다.
- 여러 라우터의 Hello 메시지에서 우선순위가 표시되지 않은 경우, 인터페이스 IP 주소가 가장 큰 라우터가 DR로 선택됩니다.

명령어	설명
ip pim-dm dr-priority	지정된 포트에서 로컬 DR의 우선순위를 설정합니다.

36.2.6 (S,G) 항목 삭제

일반적으로 로컬 멀티캐스트 라우팅 테이블(MRT)에 있는 (S,G) 항목이나 (S,G)를 통해 전달된 멀티캐스트 메시지의 통계 값을 초기화해야 합니다. 다음 명령어를 관리 모드에서 실행합니다.

명령어	설명
clear ip mroute pim-dm {* | group [source]}	이 명령어는 로컬 멀티캐스트 라우팅 테이블의 모든 항목 또는 일부 항목을 삭제합니다. 멀티캐스트 메시지 전달에 영향을 줄 수 있습니다. 이 명령어는 PIM-DM 멀티캐스트 라우팅 프로토콜에 의해 업스트림 포트에서 생성된 (S,G) 항목만 삭제합니다.
clear ip pim-dm interface	PIM-DM 포트에서 (S,G)를 통해 전달된 멀티캐스트 메시지의 통계 값을 초기화합니다. 이 명령어는 PIM-DM 멀티캐스트 라우팅 프로토콜에 의해 업스트림 포트에서 생성된 (S,G) 항목만 초기화합니다.

36.3 PIM-SM 구성

36.1 PIM-SM 소개

프로토콜 독립 멀티캐스트 스패어 모드(Protocol Independent Multicast Sparse Mode, PIM-SM)는 RIP, OSPF, IS-IS, BGP 등과 같은 유니캐스트 라우팅 프로토콜에 의해 생성된 유니캐스트 라우팅 테이블을 사용하여 IP 멀티캐스트를 위한 경로를 제공합니다.
멀티캐스트 라우팅은 사용된 유니캐스트 라우팅 프로토콜과 무관하며, 해당 멀티캐스트 라우팅 테이블 항목만 생성되면 됩니다.

PIM은 RPF(Reverse Path Forwarding) 메커니즘을 사용하여 멀티캐스트 패킷을 전달합니다.
장치에 멀티캐스트 패킷이 도착하면, 먼저 RPF 검사를 수행합니다.

- RPF 검사가 통과되면, 해당 멀티캐스트 패킷을 전달하기 위해 멀티캐스트 라우팅 테이블 항목이 생성됩니다.
- RPF 검사가 실패하면, 해당 패킷은 폐기됩니다.

PIM은 구현 메커니즘에 따라 다음 두 가지 모드로 구분됩니다:

- 프로토콜 독립 멀티캐스트 덴스 모드(PIM-DM)
- 프로토콜 독립 멀티캐스트 스패어 모드(PIM-SM)

또한, 소스 지정 멀티캐스트(SSM, Source-Specific Multicast) 모델은 PIM-SM의 일부 기술을 사용하여 구현됩니다.

스패어 모드는 덴스 모드와 상대적인 개념입니다.

- 스패어 모드는 호스트가 데이터를 수신하려면 요청해야 합니다.
- 덴스 모드는 호스트가 데이터를 능동적으로 수신합니다.
- 스패어 모드는 일반적으로 규모가 큰 네트워크에서 사용되며, 덴스 모드는 멀티캐스트 멤버가 밀집된 소규모 네트워크에 적합합니다.

참고 : 이 장에서 언급된 "라우터"는 라우팅 프로토콜을 실행하는 레이어 3 스위치, 일반 네트워크 환경의 라우터 및 기타 라우팅 프로토콜을 실행하는 장치를 포함합니다.

36.2 PIM-SM 구성 목록

- 글로벌 멀티캐스트 라우팅 활성화
- pim-sm 시작
- 이웃 필터 목록 구성
- DR(Designated Router) 선출

- RP(Candidate RP) 구성
- BSR(Candidate BSR) 구성
- SPT 임계값(SPT-threshold) 구성
- SSM 구성
- 관리 도메인 구성
- 등록 패킷의 소스 주소 구성
- anycast-rp 구성
- PIM-SM 로컬 라우팅 항목 표시
- pim-sm 디버깅 정보 추적
- PIM-SM 라우팅 항목 초기화

36.2.1 글로벌 멀티캐스트 활성화

ip multicast-routing

no ip multicast-routing

PIM-SM 프로토콜을 사용하려면 구성 모드에서 다음 명령어를 실행합니다.

switch_config# ip multicast-routing

실행 결과

!

ip multicast-routing

!

PIM-SM 프로토콜을 사용하지 않으려면 구성 모드에서 다음 명령어를 실행합니다.

switch_config# no ip multicast-routing

36.2.2 PIM-SM 시작

글로벌 멀티캐스트 라우팅 기능을 활성화한 후, PIM-SM 프로토콜 패킷을 송수신할 수 있도록 PIM-SM을 지원하는 인터페이스를 구성해야 합니다.
각 라우팅 포트는 멀티캐스트 프로토콜을 독점적으로 사용합니다. 즉, 포트에서 다른 멀티캐스트 프로토콜이 활성화되어 있으면 PIM-SM을 구성할 수 없습니다.

PIM-SM이 포트에서 동작하기 위한 사전 조건:

- 포트에 기본 IP 주소가 설정되어 있어야 합니다.
- 포트 프로토콜이 활성 상태(up)여야 합니다.
- 포트에 PIM-SM이 구성되어야 합니다.

switch_config# interface v8

switch_config_v8# ip address 172.17.21.173 255.255.255.0

switch_config_v8# ip pim-sm

구성 완료 후, show running 명령어를 사용하여 결과를 확인합니다.

!

interface VLAN8

ip address 172.17.21.173 255.255.255.0

no ip directed-broadcast

ip pim-sm

!

show ip pim-sm interface 명령어를 사용하여 결과를 확인합니다.

switch# show ip pim-sm interface

Intf	Address	Ver/ Mode	Nbr Count	Hello Intvl	DR Prior	DR Addr
v8	172.17.21.173	V2/S	0	30	1	172.17.21.173

PIM-SM을 포트에서 비활성화하려면 다음 명령어를 사용합니다.

switch_config# interface v8

switch_config_v8# no ip pim-sm

36.2.3 이웃 필터 목록 구성

PIM-SM은 동작 시 이웃 관계를 유지해야 하며PIM-SM은 Hello 정보를 통해 감지 및 관련 파라미터에 대한 협상을 완료합니다. PIM-SM은 모든 PIM 라우터(224.0.0.13)로 주기적으로 멀티캐스트로 Hello 패킷을 전송하고, 수신한 Hello 정보와 합의된 파라미터를 통해 이웃 관계를 설정합니다.

라우터가 Hello 정보를 수신하기 전에 Hello 정보를 전송하면, 해당 라우터는 이웃이 존재하는 것으로 간주합니다. 반대로 Hello 정보를 수신하지 못하면 이웃이 존재하지 않는 것으로 간주됩니다.

해당 인터페이스에서 이웃 필터 목록을 구성하여, Hello 패킷을 확인하고 이웃을 필터링합니다.

이웃 필터 목록이 삭제되거나 금지된 이웃이 해제된 경우, 다음 Hello 주기에서만 이웃 정보를 획득할 수 있습니다.

이웃 접근 목록 구성 단계

- 인터페이스에 기본 IP 주소를 설정합니다.
- 포트 프로토콜이 활성화 상태(up)여야 합니다.
- 인터페이스에서 PIM-SM을 구성합니다.
- 인터페이스에 PIM-SM 표준 접근 목록을 구성하고 이웃을 필터링합니다.

switch_config# interface v9

switch_config_v9# ip address 172.20.21.172 255.255.255.0

switch_config_v9# ip pim-sm

switch_config_v9# ip pim-sm nbr-filter nbr_permit

switch_config_v9# exit

switch_config# ip access-list standard nbr_permit

switch_config_std_nacl# permit 172.20.21.174 255.255.255.0

세그먼트 172.20.21.0/24에서 전송된 Hello 패킷을 허용하고, 이웃 관계를 설정합니다.

R172_config_std_nacl# show ip pim-s nei

PIM-SMv2 Neighbor Table

Neighbor Address	Interface	Uptime/Expires	DR Prior
172.20.21.173	v9	00:15:24/00:01:30	1(DR)

다음과 같이 설정을 변경하면, 인터페이스 v9에서는 172.20.21.174에서 전송된 Hello 패킷만 허용됩니다.

S172_config_std_nacl# permit 172.20.21.174 255.255.255.255

디버그 정보 예시

2004-1-1 00:16:26 PIM-SM: rcvd hello from 172.20.21.173, filter by acl

이전에 설정된 이웃은 타임아웃될 때까지 서서히 만료됩니다.

S172# show ip pim-s nei

PIM-SMv2 Neighbor Table

Neighbor Address	Interface	Uptime/Expires	DR Prior
172.20.21.173	v9	00:17:21/00:00:03	1(DR)

36.2.4 DR(Designated Router) 선출

DR 선출은 각 라우터의 Hello 패킷에 포함된 우선순위와 IP 주소를 비교하여 라우터 세그먼트에서 DR을 선택하는 과정입니다.

DR의 역할

- 호스트 IGMP(v1) 정보에 대한 응답

  호스트가 두 개 이상의 PIM-SM 라우터에 직접 이더넷으로 연결된 경우, DR만이 이러한 정보를 수신하고 (*,G) 조인(join) 패킷을 전송합니다.

  수신 측에서 DR과 어서트(assert) 우승자가 충돌하는 경우, DR이 우선합니다.

- 멀티캐스트 소스에서의 역할

  DR은 원본 등록 패킷을 생성하고 RP(랜데부 포인트)로 등록합니다.

  새로운 이웃이 발견되면, DR은 로컬에 저장된 BSM(부트스트랩 메시지) 패킷을 전송하는 역할을 합니다.

- DR로 승격 시 조건

  로컬 장치가 DR이 되려고 할 경우, DR 우선순위를 높이거나 우선순위가 동일한 경우 IP 주소 값을 기준으로 DR을 결정합니다.

DR 우선순위 구성 단계

- 인터페이스에 기본 IP 주소를 설정합니다.
- 포트 프로토콜이 활성화 상태(up)여야 합니다.
- 인터페이스에서 PIM-SM을 구성합니다.
- 인터페이스에서 ip pim-sm dr-priority 명령어를 사용하여 DR 우선순위를 설정합니다.

interface vlan 10

ip address 192.168.1.1 255.255.255.0

ip pim-sm

ip pim-sm dr-priority 5

36.2.5 후보 RP(Candidate RP) 구성

스위치를 후보 RP로 구성하려면 다음 4단계를 수행해야 합니다.

구성 단계

- 후보 RP가 될 라우팅 포트에 IP 주소를 설정합니다.
- 포트에서 PIM-SM을 활성화합니다.
- 글로벌 구성 모드에서 PIM-SM을 활성화합니다: router pim-sm
- PIM-SM 글로벌 구성 모드에서 후보 RP를 구성합니다: c-rp ***

switch_config# interface loopback1

switch_config_l1# ip address 1.1.1.1 255.255.255.0

switch_config_l1# ip pim-sm

switch_config# router pim-sm

switch_config_ps# c-rp lo1 list rp-range

switch_config_ps# exit

switch_config# ip access-list standard rp-range

switch_config_std_nacl# permit 225.1.1.0 255.255.255.0

switch_config_std_nacl# permit 226.1.1.0 255.255.255.0

위 구성은 후보 RP 주소를 1.1.1.1로 설정하고, 멀티캐스트 그룹 범위 225.1.1.0/24 및 226.1.1.0/24를 지원하도록 설정합니다.

show 명령어를 사용하여 로컬에 구성된 후보 RP 상태와 동작 상태를 확인할 수 있습니다.

switch_config# show ip pim-sm bsr

PIMv2 BSR information:

Candidate-RP: 1.1.1.1 (Loopback1)

Interval of Advertisements: 60 seconds

Next Advertisement will be sent in 00:00:55

switch_config#

스위치의 후보 RP 기능을 비활성화하려면 PIM-SM 구성 모드에서 해당 명령어를 사용하여 설정을 제거합니다.

switch_config# router pim-sm

switch_config_ps# no c-rp loopback1

후보 RP 구성을 제거한 후, show 명령어를 사용해 현재 CRP 상태를 확인할 수 있습니다.

switch_config_ps# exit

switch_config# show ip pim-sm bsr

PIMv2 BSR information:

switch_config#

36.2.6 후보 BSR(Bootstrap Router) 구성

스위치를 후보 BSR로 구성하려면 다음 네 단계로 명령어를 실행합니다.

구성 단계

- 후보 RP가 될 라우팅 포트에 IP 주소를 설정합니다.
- 포트에서 PIM-SM을 활성화합니다.
- 글로벌 구성 모드에서 PIM-SM을 활성화합니다: router pim-sm
- PIM-SM 글로벌 구성 모드에서 후보 BSR을 구성합니다: c-bsr ***

switch_config# interface loopback1

switch_config_l1# ip address 1.1.1.1 255.255.255.0

switch_config_l1# ip pim-sm

switch_config# router pim-sm

switch_config_ps# c-bsr loopback1 30 200

위 구성은 후보 BSR이 EBSR(Elected BSR)로 선택된 후 해시 길이(hash length)를 30으로 설정하고, BSR 선출에서 후보 BSR의 우선순위를 200으로 설정합니다.

show 명령어를 사용해 후보 BSR의 로컬 구성 및 동작 상태를 확인할 수 있습니다.

switch_config_ps# show ip pim-s bsr

PIMv2 BSR information:

I am a Candidate-BSR: Loopback1 in sz 224.0.0.0/4.

CBSR-STM state (0-c,1-p,2-e): 1.

switch_config_ps#

CBSR 상태 전환을 관찰할 수 있습니다. 아래 예시는 EBSR로 선출된 상태입니다.

switch_config_ps# show ip pim-s bsr

PIMv2 BSR information:

I am BSR in sz 224.0.0.0/4

CBSR-STM state (0-c,1-p,2-e): 2.

Address of BSR: 1.1.1.1

BSR Priority: 200

Hash Mask Length: 30

Uptime: 02:54:12

BSR will expire in 00:00:51

switch_config_ps#

후보 BSR 기능을 비활성화하려면 PIM-SM 구성 모드에서 해당 명령어를 실행해 설정을 제거합니다.

switch_config# router pim-sm

switch_config_ps# no c-bsr loopback1

후보 BSR 구성을 삭제한 후, show 명령어를 사용해 현재 후보 BSR 상태를 확인할 수 있습니다.

switch_config_ps# show ip pim-s bsr

PIMv2 BSR information:

I am NCBSR in sz 224.0.0.0/4

NCBSR-STM state (0-NI,1-AA,2-AP): 1

switch_config_ps#

36.2.7 SPT 임계값(SPT-threshold) 구성

스위치에서 데이터가 포워딩될 때, RPT(Rendezvous Point Tree)에서 SPT(Shortest Path Tree)로 전환할지 여부를 판단해야 합니다.이 판단 기준이 spt-threshold(임계값)입니다.기본적으로 수신자가 첫 번째 데이터 패킷을 수신하면 SPT로 전환됩니다.하지만 RPT에서 SPT로 전환하는 임계값을 설정할 수 있으며, 단위는 KB/s입니다. 일반적으로 RPT에서 SPT로 전환되면 다시 RPT로 돌아가지 않습니다.

switch_config# router pim-sm

switch_config_ps# spt-threshold 1000

위 구성은 RPT에서 SPT로 전환하는 임계값을 1000KB/s로 설정합니다.

36.2.8 SSM(Source-Specific Multicast) 구성

SSM 모델은 IGMPv3의 지원이 필요하며, 수신 측의 PIM-SM 장치에서 IGMPv3를 활성화해야 합니다.

SSM 모델은 PIM-SM의 서브셋 기능을 통해 구현됩니다. 시스템은 PIM-SM 및 SSM 기능을 모두 활성화합니다.

PIM-SM을 배포할 때, 모든 비경계(non-boundary) 인터페이스에서 PIM-SM을 활성화하는 것이 권장됩니다.

SSM과 PIM-SM 선택 기준은 멀티캐스트 소스에서 수신자에게 정보를 전송하는 과정에서, PIM-SSM 또는 PIM-SM이 사용되는지는 수신자의 멀티캐스트 그룹 내에 지정된 채널(S, G)이 존재하는지 여부에 따라 결정됩니다.

PIM-SM이 활성화된 인터페이스는 "PIM-SSM" 모델을 채택하는 범위 내의 멀티캐스트 그룹을 PIM-SSM 그룹으로 간주합니다.

PIM-SSM 기본 기능 구성 전 준비 사항

- 먼저 유니캐스트 라우트를 구성해야 합니다.
- 이는 내부 네트워크 계층 간의 상호작용과 사용 가능한 경로를 보장하기 위함입니다.

PIM-SSM 구성 단계

- 인터페이스에서 PIM-SM을 활성화합니다.
- PIM-SM 구성 모드에서 SSM 그룹 주소 범위를 입력합니다.
- PIM-SM의 다른 기능을 구성합니다(선택 사항).

```
switch_config# interface v8
switch_config_v8# ip address 1.1.1.1 255.255.255.0
switch_config_v8# ip pim-sm
switch_config_v8# exit
switch_config# router pim-sm
switch_config_ps# ssm range grp_range
switch_config_ps# exit
switch_config# ip access-list standard grp-range
switch_config_std_nacl# permit 233.1.0.0 255.255.0.0
switch_config_std_nacl#
```

위 구성에서는 기본 SSM 그룹 범위인 232.0.0.0/8 대신 233.1.0.0/8을 그룹 범위로 설정합니다.

SSM을 비활성화하려면 PIM-SM 구성 모드에서 해당 설정에 no 명령어를 사용하여 SSM 관련 구성을 제거합니다.

switch_config# router pim-sm

switch_config_ps# no ssm range grp_range

36.2.9 관리 도메인(sz) 구성

관리 도메인이 없는 메커니즘에서는 하나의 PIM-SM 도메인에 단 하나의 BSR(Bootstrap Router)이 존재합니다.

네트워크 전체는 해당 BSR에 의해 제어됩니다. 보다 효율적인 관리 및 확장성을 위해, PIM-SM 도메인을 여러 개의 관리 도메인으로 분할할 수 있습니다.

각 관리 도메인은 하나의 BSR을 유지하며, 특정 범위의 멀티캐스트 그룹을 처리합니다. 글로벌 도메인은 여전히 하나의 BSR을 유지하며, 나머지 모든 멀티캐스트 그룹을 처리합니다.

관리 도메인 메커니즘

- 각 관리 도메인의 경계는 ZBR(Zone Border Router)로 구성됩니다.
- 관리 도메인 내의 BSR은 해당 범위의 멀티캐스트 그룹을 관리합니다.
- 특정 멀티캐스트 프로토콜 패킷(예: 어서트 메시지 및 BSR 부트스트랩 메시지)은 관리 도메인의 경계를 넘지 않습니다.

관리 도메인 네트워크에서의 동작 방식

- 네트워크에서 멀티캐스트 그룹별로 후보 BSR(C-BSR)을 선택합니다.
- 네트워크 내의 후보 RP(C-RP)는 해당 BSR에만 정보 패킷을 전달합니다.
- BSR은 RP-SET을 요약하여 해당 관리 도메인 내 모든 장치에 정보를 전달합니다.

RP 찾기 방식

- 멀티캐스트 그룹의 RP를 찾으려면 해당 그룹에 대해 가장 긴 접두사(prefix)와 서브넷 마스크를 기반으로 도메인(sz)을 찾습니다.
- 해당 도메인의 RP-SET을 조회하여 RP를 결정합니다.

관리 도메인 구성 단계

- ZBR(관리 도메인 경계 장치)에서 로컬 관리 도메인 그룹 범위를 구성합니다.
- 관리 도메인 내에서 PIM-SM을 구성합니다.
    ① 관리 도메인 경계와 일치하는 대기 BSR(standby BSR) 그룹 범위를 구성합니다.
    ② 대기 BSR을 구성하고, 해당 BSR 포트를 지정합니다.

ZBR에서 관리 도메인 범위 구성

Sa_config_v9# ip pim-sm admin-scope 225.1.1.0 255.255.255.0

도메인 PIM-SM 장치에서 대기 BSR 그룹 범위 및 포트 구성

Sb_config# interface loopback1

Sb_config_l1# ip address 1.1.1.1 255.255.255.0

Sb_config_l1# ip pim-sm

Sb_config# router pim-sm

Sb_config_ps# c-bsr admin-scope 225.1.1.0 255.255.255.0 30 200

Sb_config_ps# c-bsr loopback1 32 250

30, 32는 해시 서브넷 마스크 길이를 의미합니다. 200, 250은 대기 BSR의 우선순위를 나타냅니다.

구성에 불일치가 발생할 경우, 대기 BSR을 설정할 때 지정된 값이 관리 도메인을 구성할 때의 값보다 우선합니다.

36.2.10 등록 패킷의 소스 주소 구성

기본적으로 데이터 소스에서 등록 패킷을 전달하는 DR(Designated Router)은 자신의 주소를 등록 패킷의 소스 주소로 사용합니다.
그러나 DR 장치에서 활성 상태의 PIM-SM 인터페이스 중 어느 것이든 등록 패킷의 소스 주소로 지정할 수 있습니다.

Sb_config# interface loopback1

Sb_config_l1# ip address 1.1.1.1 255.255.255.0

Sb_config_l1# ip pim-sm

Sb_config# router pim-sm

Sb_config_ps# reg-src loopback 1

위 구성은 loopback1의 기본 주소 1.1.1.1을 등록 패킷의 소스 주소로 지정합니다.

36.2.11 Anycast-RP 구성

PIM-SM 도메인에서 단일 RP(Rendezvous Point)는 높은 부하를 가질 수 있습니다. 이러한 부하를 줄이기 위해 여러 개의 동일한 RP를 지정할 수 있습니다.
멀티캐스트 소스 및 수신자는 최신 RP를 기반으로 등록 패킷 및 조인(join) 요청을 전달합니다.

Anycast-RP 구성 시 주의사항

- MSDP(Multicast Source Discovery Protocol) 모듈이 도입되지 않은 경우, Anycast-RP를 구성할 때 이웃(anycast-rp neighbor)을 명확하게 지정해야 합니다.
- 이웃 주소와 RP로 작동하는 포트 주소는 동일할 수 없습니다.

36.2.12 PIM-SM 로컬 라우팅 항목 표시

PIM-SM 멀티캐스트 라우팅 정보를 확인하려면 show ip mroute pim-sm 명령어를 사용합니다.

명령어 형식

show ip mroute pim-sm [group-address] [source-address]

매개변수	설명
group-address	멀티캐스트 그룹 주소
source-address	멀티캐스트 소스 주소

기본값

- 없음

명령어 모드

- EXEC 모드

예제

```
switch# show ip mroute pim-sm
IP PIM-SM Multicast Routing Table:
(source, group)   RP        Uptimer/Expires   Flags
(*, 225.1.1.10), 9.1.1.1, 00:15:14/00:02:37, JOIN|IGMP
Upstream interface: VLAN5, RPF nbr 192.168.100.143
Downstream interface list:
  VLAN2, 00:13:23/00:02:37
(192.166.1.253, 225.1.1.10), 00:15:14/00:02:46 JOIN|IGMP
Upstream interface: VLAN5, RPF nbr 192.168.100.143
Downstream interface list:
  VLAN2, 00:15:14/00:02:46
```

36.2.13 PIM-SM 라우팅 항목 초기화

PIM-SM 멀티캐스트 라우터에 저장된 멀티캐스트 라우팅 정보를 삭제하려면 clear ip mroute pim-sm 명령어를 사용합니다.

명령어 형식

clear ip mroute pim-sm [* | group-address] [source-address]

매개변수	설명
*	PIM-SM이 생성한 모든 멀티캐스트 라우트를 삭제합니다.
group-address	해당 그룹의 멀티캐스트 라우팅을 삭제합니다.
source-address	해당 소스의 멀티캐스트 라우팅을 삭제합니다.

기본값

- 없음

명령어 모드

- EXEC 모드

예제

PIM-SM이 로컬 MRT(멀티캐스트 라우팅 테이블)의 업스트림 포트에서 생성한 모든 라우트를 삭제합니다.

switch# clear ip mroute pim-sm *

PIM-SM이 생성한 멀티캐스트 라우팅 중 그룹 주소가 239.1.1.1인 모든 라우트를 삭제합니다.

switch# clear ip mroute pim-sm 239.1.1.1

PIM-SM이 생성한 업스트림 포트에서 (192.168.20.138, 239.1.1.1) 라우트를 삭제합니다.

switch# clear ip mroute pim-sm 239.1.1.1 192.168.20.131

36.2.14 PIM-SM 디버깅 정보 추적

PIM-SM 패킷 및 상태 머신(state machine) 정보를 추적하려면 debug ip pim-sm 명령어를 사용합니다.

명령어 형식

debug ip pim-sm [hello | jp | register | assert | bsr | timer] [packet]

매개변수	설명

hello	Hello 모듈에서 송수신하는 패킷 정보를 추적합니다.
jp	Join/Prune(JP) 패킷 정보를 추적합니다.
register	등록(register) 패킷 정보를 추적합니다.
assert	assert 패킷 정보를 추적합니다.
bsr	BSR(Bootstrap Router) 패킷 정보를 추적합니다.
time	타이머 정보를 추적합니다.
packet	상태 머신의 동작 정보를 추적합니다.

기본값

- 없음

명령어 모드

- EXEC 모드

예제

Hello 패킷 상호작용 추적

switch# debug ip pim-sm hello

2003-4-21 16:44:00 PIM-SM: VLAN5, Rcv Hello Msg, Source = 192.168.100.143, Destination = 224.0.0.13, len = 34

2003-4-21 16:44:07 PIM-SM: VLAN5, Send Hello Msg, Destination = 224.0.0.13, len = 34

2003-4-21 16:44:08 PIM-SM: VLAN2, Send Hello Msg, Destination = 224.0.0.13, len = 34

2003-4-21 16:44:10 PIM-SM: VLAN2, Rcv Hello Msg, Source = 192.168.21.144, Destination = 224.0.0.13, len = 34

JP(Join/Prune) 패킷 및 상태 변화 추적

switch# debug ip pim-sm jp

switch# PIM-SM: downstream VLAN5, RP = 192.166.100.142, GP = 224.2.127.254

SM state = PS_ST_JP_NI, ev = PS_EV_JP_JOIN.

PIM-SM: downstream VLAN5, RP = 192.166.100.142, GP = 224.2.127.254

SM state = PS_ST_JP_J, ev = PS_EV_JP_PRUNE.

PIM-SM: downstream VLAN5, RP = 192.166.100.142, GP = 239.255.255.250

SM state = PS_ST_JP_NI, ev = PS_EV_JP_JOIN.

PIM-SM: downstream VLAN5, RP = 192.166.100.142, GP = 239.255.255.250

SM state = PS_ST_JP_J, ev = PS_EV_JP_PRUNE.

2003-4-21 16:48:52 PIM-SM: VLAN5, Rcv J/P Msg, Source = 192.168.100.143, Destination = 224.0.0.13, len = 42

PIM-SM: downstream VLAN5, RP = 192.166.100.142, GP = 225.1.1.10

SM state = PS_ST_JP_NI, ev = PS_EV_JP_JOIN.

등록 패킷 상호작용 및 상태 변화 추적

S142# debug ip pim-sm register

S142# 2003-4-21 16:52:19 Line protocol on Interface VLAN5, changed state to up

2003-4-21 16:52:29 PIM-SM: VLAN5, Rcv Register Msg, Source = 192.168.100.143, Destination = 192.166.100.142, len = 57

2003-4-21 16:52:29 PIM-SM: VLAN5 Rcv Register Msg, Source = 192.168.100.143, Destination = 192.166.100.142, len = 57

36.3 구성 예제

36.3.1 PIM-SM 일반 토폴로지 구성 예시

PIM-SM(Protocol Independent Multicast - Sparse Mode)은 멀티캐스트 트래픽을 효율적으로 전송하기 위한 프로토콜입니다.
아래는 PIM-SM을 구성하는 일반적인 토폴로지 예시입니다.

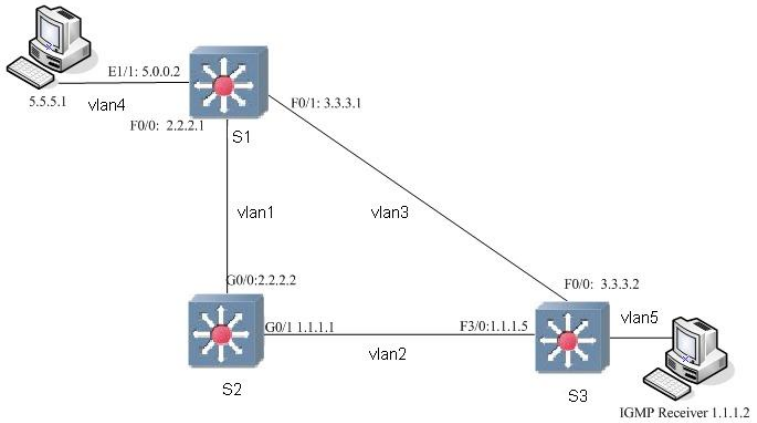


그림 61 네트워크 토폴로지

PIM-SM 일반 토폴로지 구성 예시

모든 라우터에서 멀티캐스트 포워딩 기능 활성화

switch_config# ip multicast-routing

모든 포트에서 PIM-SM 멀티캐스트 포워딩 프로토콜 구성

S1_config_v4# ip pim-sm

S1_config_v3# ip pim-sm

S1_config_v1# ip pim-sm

RP(Rendezvous Point) 구성

동적 RP 구성

동적 RP의 경우, 후보 BSR(C-BSR) 및 후보 RP(C-RP)를 담당하는 라우터에서만 구성합니다. C-BSR과 C-RP는 동일한 장치에서 구성할 필요는 없습니다.

S2_config_l0# ip address 6.6.6.6 255.255.255.0

S2_config_l0# ip pim-sm

S2_config# router pim-sm

S2_config_ps# c-bsr loopback0

S2_config_ps# c-rp loopback0

정적 RP 구성

정적 RP의 경우, 각 PIM 라우터에서 RP 주소를 명시해야 합니다. RP 주소로 사용되는 포트는 반드시 PIM-SM이 활성화되어 있어야 합니다.

S2에서 정적 RP 구성

S2_config_l0# ip address 6.6.6.6 255.255.255.0

S2_config_l0# ip pim-sm

S2_config_ps# static-rp 6.6.6.6

S1 및 S3에서 정적 RP 구성

S1_config_ps# static-rp 6.6.6.6

S3_config_ps# static-rp 6.6.6.6

SSM(Source-Specific Multicast) 기능 활성화

- SSM 기능을 활성화하려면 PIM 도메인 전체에서 동일하게 설정해야 합니다.
- SSM 모델은 IGMPv3 지원이 필요하므로, 수신 측에 연결된 PIM-SM 장치에서 IGMPv3 기능이 활성화되어 있어야 합니다.
- SSM 모델은 PIM-SM 기능의 서브셋으로 구현됩니다.

- PIM-SM을 활성화하면 시스템은 자동으로 SSM 기능도 활성화됩니다.

PIM-SSM 구성 예시

switch_config# interface vlan8

switch_config_v8# ip address 1.1.1.1 255.255.255.0

switch_config_v8# ip pim-sm

switch_config_v8# exit

switch_config# router pim-sm

switch_config_ps# ssm range grp_range

switch_config_ps# exit

switch_config# ip access-list standard grp-range

switch_config_std_nacl# permit 233.1.0.0 255.255.0.0

switch_config_std_nacl#

위 구성에서 SSM 그룹 범위는 기본값인 232.0.0.0/8 대신 233.1.0.0/16으로 설정됩니다. SSM을 비활성화하려면 no 명령어를 사용하여 관련 구성을 삭제합니다.

switch_config_ps# no ssm range grp_range

PIM-SM 구성 예시 (S2는 RP, S3는 DR)

S2: RP(Rendezvous Point) 역할 수행

S3: 1.1.1.0 네트워크 세그먼트에서 DR(Designated Router) 역할 수행

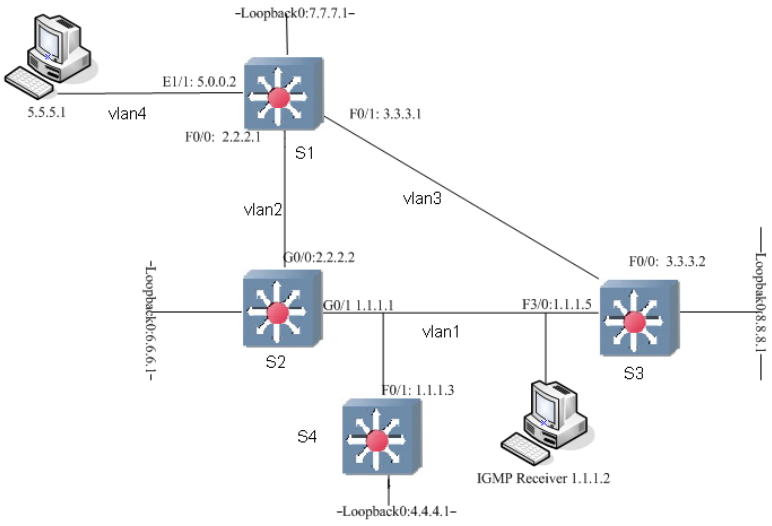


그림 62 네트워크 토폴로지

SSM을 사용한 멀티캐스트 트래픽 포워딩 구성 (233.1.0.0/16 범위)

구성 개요

- SSM(Source-Specific Multicast) 기능을 사용하여 233.1.0.0/16 범위의 멀티캐스트 트래픽을 포워딩하려면, PIM-SM 도메인 내의 모든 라우터에서 구성이 필요합니다.
- 본 예시에서는 S1, S2, S3, S4가 구성 대상입니다.
- IGMPv3를 사용하는 수신자(1.1.1.2)가 (5.5.5.1, 233.1.0.1)에 대한 IGMP 보고서를 전송하면, LAN의 DR(S3)은 RP를 경유하지 않고 직접 소스(5.5.5.1)로 조인합니다.
- 소스 라우터(S1)가 (5.5.5.1, 233.1.0.1) 패킷을 수신하면 RP에 등록하지 않고 직접 SPT(Shortest Path Tree)를 통해 패킷을 포워딩합니다.
- 이 방식은 레지스터 오버헤드를 제거하고, SPT 트리를 사용하여 효율성을 높입니다.

PIM-SM 라우터에서 SSM 범위 설정

switch_config# router pim-sm

switch_config_ps# ssm range grp_range

switch_config_ps# exit

switch_config# ip access-list standard grp-range

switch_config_std_nacl# permit 233.1.0.0 255.255.0.0

동작 방식

- 토폴로지에서 1.1.1.2(IGMP 수신자)가 IGMPv3 보고서를 전송합니다.
- **(5.5.5.1, 233.1.0.1)**을 포함하는 경우, LAN의 DR(Designated Router, S3)은 RP를 경유하지 않고 직접 소스 5.5.5.1에 조인합니다.
- 직접 연결된 S1 라우터가 (5.5.5.1, 233.1.0.1) 패킷을 수신하면, RP에 등록하지 않고 설정된 SPT(Shortest Path Tree)를 따라 패킷을 즉시 포워딩합니다.

이 방식은 레지스터 오버헤드를 줄이고 SPT 트리를 통해 멀티캐스트 트래픽을 보다 효율적으로 전달합니다.

주의 사항

- IGMP 수신자 1.1.1.2가 (*, 233.1.0.1) 형식의 보고서를 전송하는 경우, 해당 보고서는 처리되지 않습니다.
- 이는 해당 그룹 주소가 SSM 범위에 포함되기 때문입니다.
- SSM 범위 내 그룹에 대해서는 지정된 소스에서 전송된 보고서만 처리됩니다.

36.3.2 다중 프로토콜 멀티캐스트 혼합 구성

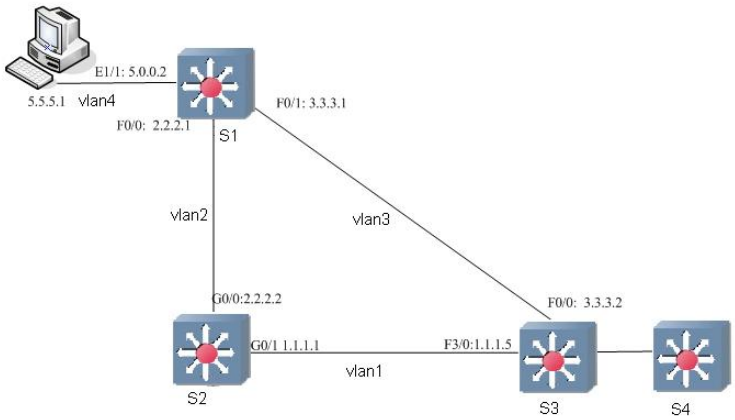


그림 63 네트워크 토폴로지

위 그림과 같이,

- S3의 VLAN1 및 VLAN3에서 ip pim-sm을 구성합니다.
- S1의 VLAN4에서 ip pim-dm을 구성합니다.

S3는 PIM-SM 도메인과 PIM-DM 도메인의 경계, 즉 PMBR(Protocol Multicast Boundary Router) 역할을 수행합니다.

이때, S3는 각 RP에 대해 (**RP) 항목을 생성합니다.
PIM-SM 도메인에서 RP 주소를 사용하는 그룹의 모든 트래픽은 (**RP) 항목을 따라 S3로 흐르고, 이후 S4로 전달됩니다.

따라서, 혼합 구성 기능을 사용할 때는 SSM(Source-Specific Multicast) 기능을 동시에 혼합할 수 없습니다.

37.NTP 구성

37.1개요

Network Time Protocol(NTP)은 분산된 시간 서버와 클라이언트 간에 시간 동기화를 수행하는 컴퓨터 프로토콜입니다. NTP는 매우 정확한 시간 보정 기능을 제공하며, 암호화 인증을 통해 악의적인 프로토콜 공격을 방지할 수 있습니다.

클라이언트와 서버는 UDP(User Datagram Protocol)를 통해 통신하며, 포트 번호는 123입니다.

37.2NTP 구성

37.2.1 장비를 NTP 서버로 구성하기

명령어	설명
ntp master primary	장비에 상위 NTP 서버가 없는 경우, 장비를 원래 NTP 서버(계층 = 1)로 구성합니다.
ntp master secondary	장비에 상위 NTP 서버가 있는 경우 장비를 보조 NTP 서버로 구성합니다. (즉, "ntp server" 명령이 구성되고 지정된 서버에서 시간 동기화가 이루어지지 않는 한 장비는 NTP 클라이언트에 대한 시간 동기화 서비스를 제공할 수 없습니다.)

37.2.2 NTP 인증 기능 구성하기

명령어	설명
ntp authentication enable	인증 기능을 활성화합니다(기본적으로 비활성화되어 있음).
ntp authentication key *keyid* **md5** *password*	NTP 인증 keyid 및 해당 키를 구성합니다.
ntp authentication trusted-key *keyid*	해당 keyid를 신뢰할 수 있는 키로 설정합니다.

37.2.3 NTP 연결 구성하기

명령어	설명
ntp server *ip-address* [**version** *number* | **key** *keyid*]*	NTP 서버의 IP 주소 및 버전 번호, 키 번호를 구성합니다.
ntp peer *ip-address* [**version** *number* | **key** *keyid*]*	장비의 NTP 피어(peer) IP 주소 및 버전 번호, 키 번호를 구성합니다.

사용 지침:

- 장비가 NTP 클라이언트에 시간 서비스를 제공하려면, 해당 장비가 시간 동기화를 완료해야 합니다. 그렇지 않으면, 해당 장비를 서버로 사용하는 클라이언트는 시간 동기화를 수행할 수 없습니다.

NTP 인증을 수행하려면 양측 장비에서 NTP 인증 기능을 동시에 활성화해야 합니다.동일한 keyid 및 key를 구성하고, 해당 keyid를 신뢰할 수 있는 키로 설정해야 합니다.그렇지 않으면, 시간 동기화가 실패합니다.

38.케이블 진단

38.1이더넷 인터페이스 케이블 진단 활성화

인터페이스 모드에서 케이블 진단을 활성화하려면 다음 명령어를 사용합니다.

명령어	설명
cable-diagnostic {**period** | **<cr>**} (TX port)	포트 케이블 점검 주기를 설정합니다. 0으로 설정하면 한 번만 점검합니다.
No cable-diagnostic	포트 케이블 점검을 수행하지 않고 기본 설정으로 복원합니다.

참고 : 진단 결과는 모든 제조사의 케이블에 대한 정확성을 보장하지 않습니다. 테스트 결과는 참고용입니다. 이 명령어는 인터페이스 서비스의 정상적인 사용에 단기간 영향을 미칠 수 있습니다. 실행 후 show interface 명령어를 사용하여 테스트 결과를 확인할 수 있습니다.

38.1.1 케이블 진단 예제

show interface g0/4

.....

Cable Ok (4 pairs)

Pair A Ok, length < 1 metres

Pair B Ok, length < 1 metres

Pair C Ok, length < 1 metres

Pair D Ok, length < 1 metres

.....

케이블 상태 설명:

- OK: 와이어 페어의 양쪽 끝이 정상임을 나타냅니다.
- Open: 와이어 페어가 단선됨을 나타냅니다.
- Short: 와이어 페어가 단락됨을 나타냅니다.
- Crosstalk: 와이어 페어 간에 누화(crosstalk)가 발생했음을 나타냅니다(서로 간섭 발생).

Unknown: 기타 실패 원인을 나타냅니다.

39.광 포트 부가 기능 구성

39.1광 포트 DDM 기능 활성화

글로벌 구성 모드에서 DDM을 활성화하려면 다음 명령어를 사용하십시오.

명령어	설명
ddm {enable}	모든 광 포트에 대해 DDM 검사 기능을 활성화합니다.
no ddm	모든 광 포트에 대해 DDM 검사 기능을 비활성화합니다.

DM 검사 기능을 활성화한 후 show interface xxxx 명령어를 통해 광 모듈의 DDM 정보를 확인할 수 있습니다. 광 모듈이 삽입되지 않은 경우 DDM 정보는 표시되지 않습니다.

참고 : 활성화 후 하드웨어 설계에 따라 CPU 사용률이 약간 증가할 수 있습니다. 검사 정보에는 사양, 파장, 제조업체 정보, 일련 번호, 제조 날짜 등이 포함됩니다. 광 모듈이 디지털 진단 모니터링(DDM) 기능을 지원하는 경우, 수신 광 파워, 전압, 바이어스 전류, 온도 및 관련 임계값 정보도 표시됩니다.

Ddm enable

show int g0/25

.....

Transceiver Info:

SFP,LC,850nm,10000BASE-FX-SR,LOS:yes

MM 80M(50um OM2 fiber) 30M(62.5um OM1 fiber) 300M(50um OM3 fiber)

DDM:YES,Vend:FINISAR,PN:FTLX8571D3BCL-HW

SerialNum:AQN03Y5,Date:2018-04-04

DDM info:

TX power:-9.40 dBm, RX power:-36.99 dBm

SFP temperature:21.00 C,supply voltage :3.40V,Bias Current.:5.00mA

DDM Thresholds:	Low-Alarm	Low-Warning	High-Warning	High-Alarm
TX power(dBm):	-6.00	-5.00	0.50	1.50

RX power(dBm):	-13.00	-12.50	0.50	1.50
SFP temperature(C):	-10	0	75	85
Supply voltage(v):	3.00	3.10	3.50	3.60
Bias Current(mA):	1.00	1.00	100.00	110.00

39.2광 포트 단일 광섬유 송수신 기능

명령어	설명
single-fiber one-way {tx|rx}	포트 단일 파이버(송신 또는 수신) 기능을 활성화합니다.
No single-fiber	포트 단일 파이버 트랜시버 기능을 비활성화합니다.

이 기능을 활성화하면 포트는 즉시 LINK UP 상태가 됩니다. 구성된 기능에 따라 광 모듈의 TX 방향 또는 RX 방향에 광섬유를 삽입할 수 있습니다. 데이터는 단일 방향으로만 흐릅니다.

39.3광 포트 적응형 광 모듈 기능

명령어	설명
fiber-auto-config {full}	광 포트 적응형 광 모듈 기능 구성을 활성화합니다. full 매개변수를 사용하면 장비가 강제 모드로 전환됩니다.
n**o** fiber-auto-config	포트 단일 광섬유 송수신 기능을 비활성화합니다.

이 기능을 활성화하면 포트는 삽입된 광 모듈 유형에 맞게 작동 모드를 전환합니다. 예를 들어, 10기가비트 광 포트에 1기가비트 광 모듈이 삽입되면 기가비트 광 모드로 전환되며, 기가비트 광 포트에 100M 광 모듈이 삽입되면 100M 광 모드로 전환됩니다.

참고 : 10기가비트 포트는 하나의 작동 모드만 있으며, 기가비트 포트는 자동 적응 및 강제 모드 두 가지가 있습니다. 따라서 10기가비트 광 포트에 1기가비트 광 모듈이 삽입되면 기본적으로 기가비트 자동 적응 모드로 전환됩니다. 기가비트 강제 모드로 전환하려면 이 명령어에 full 매개변수를 추가해야 합니다. 100M 포트는 하나의 작동 모드만 있기 때문에 full 매개변수는 필요하지 않습니다. 광-전기 변환 모듈을 사용할 경우, 올바르게 작동하려면 full 매개변수를 반드시 구성해야 합니다.

40. Logging

40.1 개요

스위치 장비에서 로그(logging) 기능을 설정하고 관리하는 방법을 설명합니다. 로그 기능은 장비의 이벤트 및 경고를 기록하여 네트워크 관리자가 문제를 진단하고 보안을 유지하는 데 중요한 역할을 합니다.

40.2 logging on

오류 정보를 기록하려면 logging on 명령어를 실행합니다. 모든 로그 기록을 중지하려면 no logging on 명령어를 실행합니다.

Privileged Mode 에서 clear logging 을 실행하면 모든 로그 기록이 삭제 되며 show logging을명령어를 실행하면 로그 기록을 확인 할 수 있습니다.

명령어	설명
Logging on	로그를 활성화 합니다.
Show logging	로그 기록을 확인합니다.
Clear logging	모든 로그 기록을 삭제 합니다.

40.3 외부 syslog 서버 연동

스위치의 로그를 외부 syslog 서버와 연동할 수 있습니다. 외부 서버가 있는 경우 아래의 명령어를 사용하여 스위치의 로그를 외부로 전송합니다.

명령어	설명
Logging a.b.c.d	사용하는 syslog 서버의 IP주소를 입력합니다.

40.3.1 logging trap

Syslog 서버에 기록되는 로그 정보의 양을 제어하려면 logging trap 명령어를 실행합니다.
Syslog 서버에 로그 정보가 기록되지 않도록 하려면 no logging trap 명령어를 실행합니다. 지정된 로그 수준을 설정하면, 해당 수준 또는 그보다 더 심각한 수준의 로그가 syslog에 기록됩니다.

프롬프트	레벨	설명	로그 정의
emergencies	0	시스템 사용불가	LOG_EMERG
alerts	1	즉시 조치 필요	LOG_ALERT
critical	2	심각한 상태	LOG_CRIT

errors	3	오류 상태	LOG_ERR
warnings	4	경고 상태	LOG_WARNING
notifications	5	정상적인지만 중요한 상태	LOG_NOTICE
informational	6	정보성 메시지만 기록	LOG_INFO
debugging	7	디버깅 메시지	LOG_DEBUG

40.4 logging buffered

위치의 메모리 캐시에 로그 정보를 기록합니다. 메모리 캐시는 순환 방식으로 사용되며, 캐시가 가득 차면 새로운 정보가 이전 정보를 덮어씁니다.

스위치의 메모리 캐시에 기록된 로그 정보를 확인하려면 show logging 명령어를 사용할 수 있습니다.
메모리 부족을 초래할 수 있으므로 너무 큰 메모리를 할당하지 않도록 주의해야 합니다.

스위치의 메모리에 로그 정보를 기록하려면 다음 명령어를 사용합니다. 기본 설정으로 되돌리려면 no 형식의 명령어를 사용합니다.

logging buffered [size | level | dump]

no logging buffered

명령어	설명
logging buffered Size	메모리 캐시 크기 (범위: 4096~2147483647 바이트)
logging buffered alarm-threshold 1-100	설정된 임계값을 초과시 알람 발생

프롬프트	레벨	설명	로그 정의
emergencies	0	시스템 사용불가	LOG_EMERG
alerts	1	즉시 조치 필요	LOG_ALERT
critical	2	심각한 상태	LOG_CRIT
errors	3	오류 상태	LOG_ERR
warnings	4	경고 상태	LOG_WARNING
notifications	5	정상적인지만 중요한 상태	LOG_NOTICE
informational	6	정보성 메시지만 기록	LOG_INFO
debugging	7	디버깅 메시지	LOG_DEBUG

40.5 logging console

콘솔에 표시되는 로그 정보의 양을 제어하려면 logging console 명령어를 실행합니다. 로그 정보

를 콘솔에 표시하지 않도록 하려면 no logging console 명령어를 실행합니다.

콘솔에 표시할 로그 정보를 설정하려면 아래의 표를 참고하십시오.

프롬프트	레벨	설명	로그 정의
emergencies	0	시스템 사용불가	LOG_EMERG
alerts	1	즉시 조치 필요	LOG_ALERT
critical	2	심각한 상태	LOG_CRIT
errors	3	오류 상태	LOG_ERR
warnings	4	경고 상태	LOG_WARNING
notifications	5	정상적인지만 중요한 상태	LOG_NOTICE
informational	6	정보성 메시지만 기록	LOG_INFO
debugging	7	디버깅 메시지	LOG_DEBUG

예로 logging console errers 설정을 적용하면 errors(3)이상의 로그만 콘솔에 표시 됩니다.

40.6 logging facility

특정 오류 정보를 기록하도록 설정하려면 logging facility 명령어를 실행합니다.
기본값인 local7로 복원하려면 no logging facility 명령어를 실행합니다. 이명령어는 로그 정보를 특정 시스템 카테고리에 기록하도록 지정합니다. 기본적으로 local7이 사용되며 필요에 따라 다른 카테고리를 선택할 수도 있습니다.

타입	설명
auth	인증 시스템
cron	Cron 작업 관리자
daemon	시스템 데몬
kern	커널
local0-7	로컬에서 정의된 메시지 저장용
lpr	라인 프린터 시스템
mail	메일 시스템
news	USENET news
sys9	시스템 사용
sys10	시스템 사용
sys11	시스템 사용
sys12	시스템 사용

sys13	시스템 사용
sys14	시스템 사용
syslog	시스템 사용
user	사용자 프로세스
uucp	UNIX-to-UNIX copy 시스템

40.7 logging monitor

터미널 라인에 표시되는 로그 정보의 양을 제어하려면 logging monitor 명령어를 실행합니다.
터미널 라인에 로그 정보를 표시하지 않으려면 no logging monitor 명령어를 실행합니다. 지정된 로그 수준을 설정하면, 해당 수준 또는 그보다 더 심각한 수준의 로그가 터미털 라인에 표시 됩니다. 터미널 라인에 표시되는 로그 정보는 아래의 표를 참고하십시오.

프롬프트	레벨	설명	로그 정의
emergencies	0	시스템 사용불가	LOG_EMERG
alerts	1	즉시 조치 필요	LOG_ALERT
critical	2	심각한 상태	LOG_CRIT
errors	3	오류 상태	LOG_ERR
warnings	4	경고 상태	LOG_WARNING
notifications	5	정상적인지만 중요한 상태	LOG_NOTICE
informational	6	정보성 메시지만 기록	LOG_INFO
debugging	7	디버깅 메시지	LOG_DEBUG

40.7.1 logging command

명령어 실행 기록 기능을 활성화하려면 logging command 명령어를 실행합니다.

이 기능이 활성화되면 입력된 모든 명령어에 대한 로그가 생성되며, 실행된 명령어, 실행 라인, 실행 결과, 로그인 세션 및 로그인 주소 등의 정보가 기록됩니다.

이 기능을 비활성화하려면 no logging command 명령어를 실행합니다.

40.8 logging history

logging history 명령어는 히스토리 로그 테이블에 저장되는 로그의 수준과 설정을 관리하는 기능을 제공합니다.

이 명령어를 사용하여 로그의 심각도(Level 0 ~ 7)를 조정하고, 저장할 로그의 개수 또는 출력 속도를 설정할 수 있습니다.

40.9 logging file

logging file 명령어는 로그 파일에 기록할 로그의 수준(Level)과 추가 설정(보존 기간, 동기화 주기, 알람 임계값 등)을 관리하는 기능을 제공합니다.

이 명령어를 사용하면 로그를 파일로 저장하여 분석 및 추적이 용이 해집니다

레벨 0 ~ 7 까지 지정할 수 있으며 지정될 레벨 이상만 파일로 저장됩니다.

명령어	설명
logging file [lever]	설정한 레벨 이상만 저장
logging file days	로그파일 보존기간
logging file sync-interval	로그 동기와 주기 설정
logging file alarm-threshold	로그 알람 임계값 설정