

E7500 Series Switch Common User Guide



Published: Feb 2010

ubiQuoss

목차

목차	2
표 목차	14
그림 목차	17
1. 서문	17
1.1. 개요	18
1.2. 적용 규칙	19
1.3. 관련 문서	20
2. E7500 SERIES 스위치시작하기	21
2.1. 편집 및 도움말 기능	22
2.1.1. 명령어 문법의 이해	22
2.1.2. 명령어 문법 도움말(Command Syntax Helper)	23
2.1.3. 단축 명령어 입력	25
2.1.4. 명령어 심볼	25
2.1.5. 명령어 라인 편집 키 및 도움말	26
2.2. 스위치명령어 모드	27
2.3. E7500 SERIES 스위치가동	28
2.4. 사용자 인터페이스	29
2.4.1. 콘솔 연결	29
2.4.2. 텔넷 연결	30
2.4.3. SNMP Network Manager 를 통한 연결	30
2.5. 사용자 관리	31
2.5.1. 사용자 등록 및 삭제 설정	31
2.5.2. 패스워드 설정	32
2.6. AAA (AUTHENTICATION, AUTHORIZATION, ACCOUNTING)	34
2.6.1. 인증 (Authentication)	34
2.6.2. 사용자 인증	35
2.6.3. Enable password 인증	36
2.6.4. 권한 (Authorization)	36
2.6.5. EXEC 실행 권한	37
2.6.6. 명령 실행 권한	38
2.6.7. 계정(Accounting)	39
2.6.8. 세션 접속 관리	39
2.6.9. 명령 실행 내역 관리	39
2.6.10. Privilege level 설정	40

2.7.	서버 설정	40
2.7.1.	RADIUS 서버 설정.....	41
2.7.2.	TACACS+ 서버 설정	42
2.8.	HOSTNAME 설정	43
2.9.	SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL).....	43
2.9.1.	SNMP 환경 설정	44
2.9.2.	Community 설정	44
2.9.3.	Trap host 설정.....	45
2.9.4.	SNMPv3 설정	47
2.10.	ACL (ACCESS CONTROL LIST)	50
2.10.1.	액세스 리스트 생성 규칙.....	50
2.10.2.	표준 IP 액세스 리스트 설정.....	50
2.10.2.1.	모든 액세스 허용	50
2.10.2.2.	모든 액세스 거부	51
2.10.2.3.	특정 호스트에서의 액세스만 허용	51
2.10.2.4.	특정 네트워크에서의 액세스만 허용.....	51
2.10.2.5.	특정 네트워크에서의 액세스만 거부.....	51
2.10.3.	텔넷 연결에 액세스 리스트 설정	52
2.11.	NTP 설정	52
2.11.1.	NTP 개요.....	52
2.11.2.	NTP client mode 설정	52
2.11.3.	NTP Server mode 설정.....	53
2.11.4.	NTP time zone 설정.....	53
2.11.5.	NTP summer time 설정.....	53
2.11.6.	NTP 기타 명령어.....	53
2.11.7.	NTP 설정 예제	54
2.12.	배너 설정	54
3.	인터페이스 환경 설정	57
3.1.	개요	57
3.2.	공통 명령어	57
3.2.1.	Interface name	58
3.2.2.	Interface id	58
3.2.3.	Interface 모드 프롬프트	59
3.2.4.	Description 명령어.....	59
3.3.	인터페이스 정보 및 상태 조회.....	59
3.3.1.	show interface 명령어.....	59
3.3.2.	show interface status 명령어	60
3.3.3.	show idprom 명령어.....	61
3.4.	물리적 포트 환경 설정	64
3.4.1.	Shutdown	65
3.4.2.	Speed and duplex.....	65
3.4.3.	Flow control	65

3.4.4.	Carrier delay	66
3.5.	BROADCAST SUPPRESSION	66
3.6.	PORT MIRRORING	67
3.7.	2 계층 인터페이스 환경 설정	68
3.7.1.	VLAN Trunking.....	68
3.7.2.	2 계층 인터페이스 모드.....	69
3.7.3.	2 계층 인터페이스 기본 설정 값.....	69
3.7.4.	2 계층 인터페이스 설정/해제	69
3.7.5.	Trunk port 설정.....	70
3.7.6.	Access port 설정.....	71
3.8.	PORT GROUP	71
3.8.1.	Port group 개요.....	71
3.8.2.	Port group configuration	72
4.	가상 랜(VLAN)	73
4.1.	VLAN 개관.....	73
4.2.	VLAN 의 유형	75
4.2.1.	포트 기반 VLAN(Port-Based VLANs)	75
4.2.2.	태그 VLAN(Tagged VLANs).....	77
4.2.3.	포트 기반 VLAN 과 태그 VLAN 의 혼합 (Hybrid)	80
4.3.	VLAN 구성.....	80
4.3.1.	VLAN ID.....	80
4.3.2.	Default VLAN	80
4.3.3.	Native VLAN	80
4.4.	VLAN 설정.....	81
4.4.1.	VLAN 설정 명령	81
4.5.	VLAN 설정 예제.....	83
4.6.	VLAN 설정 정보 확인.....	88
5.	IP 환경 설정.....	91
5.1.	개요.....	91
5.2.	네트워크 인터페이스에 IP 주소 할당	91
5.3.	ARP(ADDRESS RESOLUTION PROTOCOL)	93
5.4.	STATIC ROUTES 설정	94
5.5.	IP 설정 예제.....	95
6.	DHCP	99
6.1.	DHCP SERVER 기능 및 설정	99
6.1.1.	DHCP server 기능 개요	99
6.1.2.	DHCP server 기능 활성화.....	101
6.1.3.	DHCP Address Pool	102
6.1.4.	DHCP Network Pool 설정	102
6.1.5.	DHCP Host Pool 설정.....	107

6.1.6.	기타 global 명령어	109
6.2.	DHCP RELAY AGENT 기능 및 설정	109
6.2.1.	DHCP relay agent 개요	109
6.2.2.	DHCP relay 기능 활성화	111
6.2.3.	DHCP Relay Agent 에서 DHCP Server 설정	112
6.2.4.	DHCP Relay Agent Information option(OPTION82) 설정	114
6.2.5.	DHCP Smart Relay 설정	117
6.2.6.	DHCP Relay Agent Verify MAC-Address 설정	119
6.2.7.	DHCP Class 기반 DHCP packet forwarding	120
6.3.	DHCP SNOOPING 기능	123
6.3.1.	DHCP Snooping 기능 개요	123
6.3.1.1.	Trust and Untrust Source	123
6.3.1.2.	DHCP Snooping Binding Database	123
6.3.1.3.	Packet Validation	123
6.3.1.4.	Packet Rate-limit	124
6.3.2.	DHCP Snooping 기능의 활성화	124
6.3.3.	DHCP Snooping Vlan 설정	124
6.3.4.	DHCP Snooping information option(OPTION82) 설정	125
6.3.5.	DHCP Snooping Trust Port 설정	127
6.3.6.	DHCP Snooping max-entry 설정	127
6.3.7.	DHCP Snooping Entry Time 설정	128
6.3.8.	DHCP Snooping Rate-Limit 설정	128
6.3.9.	DHCP Snooping Verify MAC-Address 설정	129
6.3.10.	DHCP Snooping Manual Binding 설정	129
6.4.	DHCP SERVER 모니터링 및 관리	130
6.5.	DHCP RELAY 모니터링 및 관리	131
6.6.	DHCP SNOOPING 모니터링 및 관리	131
6.7.	DHCP 설정 예제	132
6.7.1.	DHCP Network Pool 설정 예제	132
6.7.2.	DHCP Host Pool 설정 예제	133
6.7.3.	DHCP server 모니터링 및 관리 예제	134
6.7.4.	DHCP relay agent 설정	135
6.7.5.	DHCP Snooping 설정 예제	138
7.	RIP	139
7.1.	INFORMATION ABOUT RIP	139
7.2.	HOW TO CONFIGURE RIP	139
7.2.1.	Enabling RIP	140
7.2.2.	Allowing Unicast updates for RIP	140
7.2.3.	Passive interface	141
7.2.4.	Applying Offsets to Routing metrics	141
7.2.5.	Adjusting Timers	141
7.2.6.	Specifying a RIP Version	142

7.2.7.	<i>Applying Distance</i>	142
10.1.1.	<i>Enabling Split Horizon</i>	143
7.3.	CONFIGURATION EXAMPLES FOR RIP	144
7.3.1.	<i>RIP 구성</i>	144
7.3.2.	<i>Offset-list 설정</i>	146
7.3.3.	<i>Passive-interface 설정</i>	146
8.	10 OSPF (OPEN SHORTEST PAHT FIRST)	148
8.1.	OSPF 개요	148
8.1.1.	<i>Link-state Database</i>	149
8.1.2.	<i>Areas</i>	149
8.1.3.	<i>Route Redistribution</i>	150
8.2.	OSPF 설정	151
8.2.1.	<i>OSPF interface parameters</i>	151
8.2.2.	<i>Different Physical Networks</i>	152
8.2.3.	<i>OSPF Area parameters</i>	154
8.2.4.	<i>OSPF NSSA</i>	154
8.2.5.	<i>OSPF Area Route summarization</i>	155
8.2.6.	<i>Redistributed Routes 의 Route Summarization</i>	156
8.2.7.	<i>Virtual Links</i>	156
8.2.8.	<i>Generating a Default Route</i>	156
8.2.9.	<i>Router ID Choice with a Loopback Interface</i>	157
8.2.10.	<i>Default metric</i>	157
8.2.11.	<i>OSPF administrative Distance</i>	158
8.2.12.	<i>Passive interface</i>	158
8.2.13.	<i>Route Calculation Timers</i>	158
8.2.14.	<i>Logging Neighbors Going Up/Down</i>	159
8.2.15.	<i>Blocking LSA Flooding</i>	159
8.2.16.	<i>Ignoring MOSPF LSA Packets</i>	159
8.2.17.	<i>Monitoring and Maintaining OSPF</i>	160
9.	10 라우팅 프로토콜(RIP&OSPF&BGP)	162
9.1.	BGP 개요	162
9.2.	BGP 설정	162
9.1.1.	<i>BGP 프로토콜의 활성화</i>	162
9.1.2.	<i>Neighbor 설정</i>	163
9.1.3.	<i>BGP 필터링 기능</i>	163
9.1.4.	<i>BGP Attribute 설정</i>	168
9.1.5.	<i>Routing Policy 변경</i>	182
9.1.6.	<i>BGP Peer Groups</i>	183
9.1.7.	<i>BGP Multipath</i>	185
9.1.8.	<i>BGP graceful-restart</i>	187
9.1.9.	<i>BGP default-metric</i>	188
9.1.10.	<i>BGP redistribute-internal</i>	188
9.1.11.	<i>BGP Password encryption</i>	188

9.1.12.	<i>BGP disable-adj-out</i>	189
9.1.13.	<i>Use of set as-path prepend Command</i>	189
9.3.	ROUTE FLAP DAMPENING	189
10.	IGMP SNOOPING	191
10.1.	IGMP SNOOPING 개요	191
10.2.	IGMP SNOOPING 설정	192
10.2.1.	<i>Enable IGMP Snooping on a VLAN</i>	192
10.2.2.	<i>Configure IGMP Snooping Functionality</i>	193
10.2.2.1.	IGMP Report-Suppression	193
10.2.2.2.	IGMP Fast-Leave	194
10.2.2.3.	IGMP Mrouter-Port	195
10.2.2.4.	IGMP Access-Group	196
10.2.2.5.	IGMP Group-Limit	197
10.3.	DISPLAY SYSTEM AND NETWORK STATISTICS	198
11.	IP 멀티캐스트 라우팅	199
11.1.	IP 멀티캐스트 라우팅 개요	199
11.2.	IGMP 개요	200
11.3.	PIM-SM 개요	200
11.4.	IP 멀티캐스트 라우팅 설정	201
11.4.1.	<i>Enable IP 멀티캐스트 라우팅</i>	201
11.4.2.	<i>Enable IGMP and PIM on an interface</i>	202
11.4.3.	<i>Configure Multicast Functionality</i>	203
11.4.3.1.	<i>Router-Guard IP Multicast</i>	203
11.4.3.2.	<i>Multicast Traffic Forwarding-TTL-Limit</i>	204
11.4.3.3.	<i>Static Multicast Route Path</i>	204
11.4.3.4.	<i>Global Multicast Group-Limit</i>	205
11.4.3.5.	<i>Multicast Load-Split</i>	206
11.4.3.6.	<i>Multicast Route-Limit</i>	206
11.4.4.	<i>Configure IGMP Functionality</i>	207
11.4.4.1.	<i>IGMP Version</i>	207
11.4.4.2.	<i>IGMP Access-Group</i>	208
11.4.4.3.	<i>IGMP Query-Interval</i>	208
11.4.4.4.	<i>IGMP Last-Member-Query-Count</i>	209
11.4.4.5.	<i>IGMP Last-Member-Query-Interval</i>	210
11.4.4.6.	<i>IGMP Immediate-Leave</i>	211
11.4.4.7.	<i>IGMP Group Limit</i>	212
11.4.4.8.	<i>IGMP Global Limit</i>	212
11.4.4.9.	<i>IGMP Minimum-Version</i>	213
11.4.4.10.	<i>IGMP Querier-Timeout</i>	213
11.4.4.11.	<i>IGMP Query-Max-Response-Time</i>	214
11.4.4.12.	<i>IGMP Rate</i>	215
11.4.4.13.	<i>IGMP Robustness-Variable</i>	216
11.4.4.14.	<i>IGMP Static-Group</i>	216
11.4.4.15.	<i>IGMP SSM-MAP</i>	219
11.4.5.	<i>Configure PIM-SM Functionality</i>	221
11.4.5.1.	<i>PIM Hello-Interval</i>	221

11.4.5.2.	<i>PIM Hello-Holdtime</i>	221
11.4.5.3.	<i>PIM DR-Priority</i>	222
11.4.5.4.	<i>PIM Propagation-Delay</i>	223
11.4.5.5.	<i>PIM Exclude-Genid</i>	223
11.4.5.6.	<i>PIM Neighbor-Filter</i>	224
11.4.5.7.	<i>PIM BSR-Border</i>	224
11.4.5.8.	<i>PIM JP-Timer</i>	225
11.4.5.9.	<i>PIM Access-Group</i>	225
11.4.5.10.	<i>PIM Accept-Register</i>	226
11.4.5.11.	<i>PIM SPT-Threshold</i>	226
11.4.5.12.	<i>PIM Cisco-Register-Checksum</i>	227
11.4.5.13.	<i>PIM BSR-Candidate</i>	228
11.4.5.14.	<i>PIM RP-Candidate</i>	229
11.4.5.15.	<i>PIM RP-Address</i>	230
11.4.5.16.	<i>PIM Register-Source</i>	231
11.4.5.17.	<i>PIM SSM</i>	231
11.4.6.	<i>Display System and Network Statistics</i>	232
12.	시스템 및 통계 모니터링	233
12.1.	상태 모니터링	233
12.2.	시스템 임계치 설정	234
12.2.1.	온도 설정.....	234
12.2.2.	Cpu usage 설정.....	235
12.2.3.	Memory Usage 설정.....	236
12.2.4.	Application memory 사용 display	236
12.3.	포트 통계	236
12.4.	RMON (REMOTE MONITORING)	241
12.4.1.	RMON 개요	241
12.4.2.	RMON 의 Alarm 과 Event 그룹 설정.	243
12.5.	LOGGING.....	246
12.5.1.	시스템 로그 메시지 내용	247
12.5.2.	디폴트 Logging 설정 값.....	247
12.5.3.	Logging 설정 예.....	248
13.	STP(SPANNING TREE PROTOCOL)	250
13.1.	UNDERSTANDING SPANNING-TREE FEATURES	250
13.1.1.	STP Overview	251
13.1.2.	Bridge Protocol Data Units.....	251
13.1.3.	Election of Root Switch	252
13.1.4.	Bridge ID, Switch Priority, and Extended System ID	253
13.1.5.	Spanning-Tree Timers.....	253
13.1.6.	Creating the Spanning-Tree Topology	253
13.1.7.	Spanning-Tree Interface States.....	254
13.2.	UNDERSTANDING RSTP	257
13.1.8.	RSTP Overview.....	257
13.1.9.	Port Roles and the Active Topology	257
13.1.10.	Rapid Convergence	258

13.1.11.	Bridge Protocol Data Unit Format and Processing	259
13.3.	UNDERSTANDING MSTP	260
13.1.12.	MST 영역.....	261
13.1.13.	IST, CST 및 CIST.....	261
13.4.	UNDERSTANDING RPVST+	263
13.5.	CONFIGURING SPANNING-TREE FEATURES	263
13.1.14.	Default STP Configuration	264
13.1.15.	STP Configuration Guidelines.....	264
13.1.16.	Enabling STP	264
13.1.17.	Enable STP in not default Bridge.....	266
13.1.18.	Configuring the Port Priority.....	267
13.1.19.	Configuring the Path Cost.....	269
13.1.20.	Configuring the Switch Priority of a VLAN	271
13.1.21.	Configuring the Hello Time.....	273
13.1.22.	Configuring the Forwarding-Delay Time for a VLAN.....	274
13.1.23.	Configuring the Maximum-Aging Time for a VLAN.....	276
13.1.24.	Changing the Spanning-Tree mode for switch.....	278
13.1.25.	Configuring the Port as Edge Port	280
13.1.26.	Specifying the Link Type to Ensure Rapid Transitions	281
13.6.	CONFIGURING MSTP FEATURES	282
13.1.27.	Instance 생성 및 VLAN 연결	282
13.1.28.	instance and port configuration.....	284
13.7.	CONFIGURING RPVST+ FEATURES	288
13.1.29.	VLAN 생성.....	288
13.1.30.	VLAN and port configuration.....	289
13.8.	DISPLAYING THE SPANNING-TREE STATUS	295
13.9.	CONFIGURING BRIDGE MAC FORWARDING	297
14.	BFD	300
14.1.	UNDERSTANDING BFD	300
14.1.1.	BFD Operation	300
14.1.2.	Benefits of using BFD for Failure Detection.....	301
14.1.3.	BFD Session Type.....	302
14.1.4.	BFD Version Interoperability	302
14.2.	BFD RESTRICTIONS	303
14.3.	DEFAULT BFD CONFIGURATION.....	303
14.4.	CONFIGURING BFD	304
14.4.1.	Configuring BFD session parameters on the interface	304
14.4.2.	Configuring multi-hop BFD session parameters	305
14.4.3.	Configuring BFD support for BGP.....	305
14.4.4.	Configuring BFD support for OSPF	306
14.4.5.	Configuring BFD support for Static routing	308
14.4.6.	Configuring Passive Mode on the Interface	309
14.4.7.	Configuring BFD Echo Mode	309
14.4.8.	Configuring BFD slow timer	310
14.4.9.	Displaying BFD information	310

14.5.	BFD CONFIGURATION SAMPLES	311
14.5.1.	Sample One: Configuring BFD in an OSPF Network	311
14.5.2.	Sample Two: Configuring BFD in an BGP Network	313
14.5.3.	Sample Three: Configuring BFD for static routing	316
15.	LACP	318
15.1.	UNDERSTANDING LINK AGGREGATION CONTROL PROTOCOL	318
15.1.1.	LACP 동작 원리.....	319
15.1.2.	LACPDU 구성	319
15.1.3.	LACP Modes	319
15.1.4.	LACP Parameters	320
15.2.	CONFIGURING 802.3AD LINK AGGREGATION CONTROL PROTOCOL AND STATIC LINK AGGREGATION	321
15.2.1.	Specifying the System Priority	321
15.2.2.	Specifying the Port Priority.....	322
15.2.3.	Specifying the Timeout Value	322
15.2.4.	Configuration LACP and static port group.....	323
15.2.5.	Clearing LACP Statistics	324
15.3.	DISPLAYING 802.3AD STATISTICS AND STATUS	324
16.	IP-OPTION	326
16.1.	IP OPTOIN 개요.....	326
16.2.	IP OPTOIN 명령어	326
17.	VRRP.....	329
17.1.	INFORMATION ABOUT VRRP	329
17.1.1.	VRRP Operation.....	329
17.1.2.	VRRP Benefits	331
17.1.3.	Multiple Virtual Rouer Support	332
17.1.4.	VRRP Router Priority and Preemption.....	332
17.1.5.	VRRP Advertisements.....	333
17.1.6.	VRRP Curcuit failover	333
17.2.	HOW TO CONFIGURE VRRP.....	333
17.2.1.	Enabling VRRP	333
17.2.2.	Disabling VRRP on an Interface	334
17.2.3.	Customizing VRRP	335
17.2.4.	Configuring VRRP circuit failover.....	335
17.3.	CONFIGURATION EXAMPLES FOR VRRP	336
17.3.1.	Configuring VRRP: Example.....	336
17.3.2.	VRRP circuit failover: Example	337
17.3.3.	VRRP Circuit fail-over Verification: Example	337
17.3.4.	Disabling a VRRP Group on an Interface: Example	338
18.	SETTING TIME AND CALENDAR	339
18.1.	UNDERSTANDING TIME SOURCES	339
18.1.1.	Network Time Protocol.....	339
18.1.2.	Hardware Clock.....	340

18.2.	CONFIGURING NTP	340
18.2.1.	Configuring Poll-Based NTP Associations	340
18.2.2.	Configuring NTP Authentication	341
18.2.3.	Configuring the Source IP Address for NTP Packets	342
18.2.4.	Configuring the System as an Authoritative NTP Server	342
18.2.5.	Updating the Hardware Clock	342
18.3.	CONFIGURING TIME AND DATE MANUALLY	343
18.3.1.	Configuring the Time Zone	343
18.3.2.	Configuring Summer Time (Daylight Savings Time)	343
18.3.3.	Manually Setting the Software Clock	344
18.4.	USING THE HARDWARE CLOCK	344
18.4.1.	Setting the Hardware Clock	345
18.4.2.	Setting the Software Clock from the Hardware Clock	345
18.4.3.	Setting the Hardware Clock from the Software Clock	345
18.5.	MONITORING TIME AND CALENDAR SERVICES	345
18.6.	CONFIGURATION EXAMPLES	346
18.6.1.	Clock, Calendar, and NTP Configuration Examples	346
19.	DYNAMIC ARP INSPECTION	347
19.1.	UNDERSTANDING DAI	347
19.1.1.	Understanding ARP	348
19.1.2.	Understanding ARP Spoofing Attacks	348
19.1.3.	Understanding DAI and ARP Spoofing Attacks	350
19.1.4.	Interface Trust States and Network Security	350
19.1.5.	Rate Limiting of ARP Packets	352
19.1.6.	Relative Priority of ARP ACLs and DHCP Snooping Entries	352
19.1.7.	Logging of Dropped Packets	352
19.2.	DEFAULT DAI CONFIGURATION	353
19.3.	DAI CONFIGURATION GUIDELINES AND RESTRICTIONS	353
19.4.	CONFIGURING DAI	354
19.4.1.	Enabling DAI on VLANs	354
19.4.2.	Configuring the DAI Interface Trust State	356
19.4.3.	Applying ARP ACLs for DAI Filtering	357
19.4.4.	Configuring ARP Packet Rate Limiting	357
19.4.5.	Enabling DAI Error-Disabled Recovery	359
19.4.6.	Enabling Additional Validation	360
19.4.7.	Configuring DAI Logging	362
19.4.7.1.	DAI Logging Overview	362
19.4.7.2.	Configuring the DAI Logging Buffer Size	362
19.4.7.3.	Configuring the DAI Logging System Messages	363
19.4.7.4.	Configuring the DAI Log Filtering	364
19.4.8.	Displaying DAI Information	365
19.5.	DAI CONFIGURATION SAMPLES	365
19.5.1.	Sample: Interoperate with DHCP Relay	366
20.	NETFLOW	368
20.1.	NETFLOW OVERVIEW	368

20.1.1.	<i>Netflow 소개</i>	368
20.2.	NETFLOW OVERVIEW.....	369
20.2.1.	<i>Netflow 소개</i>	369
20.2.2.	<i>Netflow deployment</i>	370
20.2.3.	<i>Netflow flow</i>	371
20.2.4.	<i>Netflow packet</i>	371
20.3.	E7500 NETFLOW.....	372
20.3.1.	<i>requirement 및 특성</i>	372
20.3.2.	<i>flow 생성</i>	372
20.3.3.	<i>flow 폐기</i>	372
20.3.4.	<i>제한사항</i>	373
20.3.5.	<i>E7500 Default Netflow configuration</i>	373
20.4.	NETFLOW TRAFFIC 통계 DATA 수집설정.....	373
20.4.1.	<i>Netflow traffic 통계 data 수집설정 명령어 요약</i>	373
20.4.2.	<i>Netflow traffic 통계 data 수집 enable</i>	374
20.4.3.	<i>Flow aging out 시간 설정</i>	374
20.4.4.	<i>최대 flow 개수 지정</i>	375
20.4.5.	<i>Sampled Netflow 기능 설정</i>	375
20.5.	NETFLOW TRAFFIC 통계 DATA 조회	376
20.5.1.	<i>Netflow traffic 통계 data 조회 명령어 요약</i>	376
20.5.2.	<i>flow 조회 명령</i>	376
20.5.3.	<i>flow 폐기명령</i>	378
20.6.	NETFLOW TRAFFIC 통계 DATA 전송 설정.....	378
20.6.1.	<i>Netflow traffic 통계 data 전송설정 명령어 요약</i>	378
20.6.2.	<i>Netflow traffic 통계 data 전송 enable</i>	378
20.6.3.	<i>Netflow traffic 통계 data 전송대상 설정</i>	378
20.6.4.	<i>통계 data 전송시 사용할 source interface 지정</i>	378
20.6.5.	<i>Netflow traffic 통계 data 전송설정 조회</i>	379
21.	QOS 및 ACL	380
21.1.	QOS.....	380
21.1.1.	<i>전역 설정</i>	380
21.1.2.	<i>TX Scheduling 설정</i>	380
21.1.3.	<i>Port trust 모드</i>	382
21.1.4.	<i>DSCP 변환 map 설정</i>	383
21.1.4.1.	DSCP to queue 설정	384
21.1.4.2.	DSCP to COS 설정	384
21.1.4.3.	DSCP to DSCP 설정	385
21.1.5.	<i>COS 변환 map 설정</i>	386
21.1.5.1.	COS to queue 설정	386
21.1.5.2.	COS to DSCP 설정	386
21.1.5.3.	COS to COS 설정	387
21.2.	ACL 설정.....	388

21.2.1.	Standard IP ACL.....	388
21.2.2.	Extended IP ACL.....	389
21.2.3.	MAC ACL	391
21.2.4.	ACL 의 인터페이스 적용	392
21.3.	SERVICE-POLICY 설정	393
21.3.1.	Class-map	393
21.3.2.	Policy-map	394
21.3.3.	Service-policy.....	396
21.4.	COPP	396
21.4.1.	Service-policy on COPP.....	397
21.4.2.	Rate-limit on COPP.....	397
22.	UTILITIES.....	399
22.1.	개 요.....	399
22.2.	상태 DUMP 명령	399
22.2.1.	명령어.....	399
22.3.	COMMAND HISTORY 기능	401
22.4.	OUTPUT POST PROCESSING	401
22.4.1.	output post processing 개요.....	401
22.4.2.	output post processing 예제.....	402
22.4.3.	DDM (Digital Diagnostic Monitoring).....	403
22.4.4.	GBIC DDM Monitoring	403
23.	환경설정 저장 및 소프트웨어 업그레이드	404
23.1.	파일 시스템.....	404
23.2.	IMAGE/CONFIGURATION/BSP DOWN/UP LOAD	407
23.2.1.	FTP 를 통한 Down/Up Load.....	407
23.2.2.	TFTP 를 통한 Down/Up Load.....	409
23.3.	CONFIGURATION 파일 관리	410
23.3.1.	Configuration 파일 저장	410
23.3.2.	Configuration 파일 삭제	411
23.4.	SFE/NETFLOW 소프트웨어 관리	412
23.4.1.	SFE/NETFLOW 소프트웨어 조회	412
23.4.2.	SFE/NETFLOW 소프트웨어 추가	413
23.4.3.	SFE/NETFLOW 소프트웨어 삭제	414
23.5.	BOOT MODE 설정 및 시스템 재시동	416
23.5.1.	Boot Mode 설정.....	416
23.5.2.	시스템 재시동.....	416

표 목차

표 1-1. 문자 표시 규칙	19
표 1-2. 알림 및 경고 아이콘	19
표 2-1. 명령어 구문 심볼	26
표 2-2. 명령어 라인 편집 명령 및 도움말 기능	26
표 2-3. 스위치 명령어 모드	27
표 2-4. 스위치의 명령어 모드 사이의 이동	28
표 2-5. 사용자 등록, 삭제, 관리 명령어	31
표 2-6. ENABLE 패스워드 설정 명령	33
표 2-7. 패스워드 암호화 모드 설정 명령	34
표 2-8. 사용자 인증 설정 명령어	35
표 2-9. PRIVILEGED 모드 사용자 인증 설정 명령어	36
표 2-10. EXEC SHELL 실행 권한 설정 명령어	37
표 2-11. 명령어 실행 권한 설정 명령어	38
표 2-12. 세션 접속 관리 설정 명령어	39
표 2-13. 명령어 실행 내역 설정 명령어	39
표 2-14. PRIVILEGE LEVEL 설정 명령어	40
표 2-15. RADIUS 서버 설정 명령어	41
표 2-16. TACACS+ 서버 설정 명령어	42
표 2-17. HOSTNAME 설정 명령어	43
표 2-18. SNMP 환경 설정 명령	44
표 2-19. SNMP COMMUNITY 설정	45
표 2-20. SNMP TRAP 호스트 설정	46
표 2-21. SNMP 기본 트랩의 ENABLE 설정	46
표 2-22. SNMPV3 설정	47
표 2-23. 액세스 리스트 설정 명령	50
표 2-24. 로그인 배너 및 MOTD 배너 명령어	54
표 3-1. E7500 SERIES 스위치가 지원하는 인터페이스	57
표 3-2. 공통 명령어	57
표 3-3. INTERFACE NAME	58
표 3-4. INTERFACE ID 및 지원 범위	58
표 3-5. 인터페이스 정보 및 상태 관련 명령어	59
표 3-6. 물리적 포트 환경 설정 명령어	64
표 3-7. 2 계층 인터페이스 기본 설정 값	69
표 3-8. 2 계층 인터페이스 설정 및 해제 명령어	69
표 3-9. TRUNK PORT 설정 명령어	70
표 3-10. ACCESS PORT 설정 명령어	71

표 3-11. 포트 그룹 설정 명령어	72
표 4-1. VLAN 설정 명령어	82
표 5-1. 사용 가능한 IP 주소	91
표 5-2. IP 주소 할당 명령어	93
표 5-3. ARP 환경 설정을 위한 명령어	93
표 5-4. STATIC ROUTE 경로 설정 명령어	94
표 5-5. 동적 라우팅 프로토콜의 DEFAULT ADMINISTRATIVE DISTANCES	95
표 8-1. LSA TYPE NUMBER	149
표 8-2. OSPF INTERFACE PARAMETER CLI	151
표 8-3. OSPF NETWORK TYPE CLI	152
표 8-4. P-TO-MULTIPOINT NETWORK, BROADCAST NETWORK 설정	153
표 8-5. NON BROADCAST NETWORK CLI	153
표 8-6. NON BROADCAST NETWORK 설정	153
표 8-7. OSPF AREA PARAMETER CLI	154
표 8-8. OSPF NSSA CLI	155
표 8-9. OSPF AREA ROUTE SUMMARIZATION CLI	155
표 8-10. EXTERNAL ROUTE SUMMARIZATION CLI	156
표 8-11. OSPF VIRTUAL LINK CLI	156
표 8-12. OSPF DEFAULT ROUTE CLI	157
표 8-13. LOOPBACK INTERFACE 설정	157
표 8-14. REFERENCE BANDWIDTH CLI	157
표 8-15. OSPF DISTANCE CLI	158
표 8-16. OSPF PASSIVE INTERFACE CLI	158
표 8-17. OSPF SPF TIMER CLI	159
표 8-18. OSPF ADJACENCY LOG CLI	159
표 8-19. BLOCK LSA CLI	159
표 8-20. IGNORE MOSPF LSA CLI	160
표 8-21. MONITORING OSPF CLI	160
표 8-22. MAINTAINING OSPF CLI	161
표 9-1. ROUTE DAMPENING 에 사용되는 용어	190
표 10-1. IGMP SNOOPING 관련 모니터링 명령어	198
표 11-1. 멀티캐스트 프로토콜	200
표 11-2 IP 멀티캐스트 라우팅 관련 모니터링 명령어	232
표 12-1. 상태 모니터링 명령어	234
표 12-2. 온도 설정 관련 명령어	234
표 12-3. CPU USAGE THRESHOLD 관련 명령어	235
표 12-4. MEMORY USAGE 관련 명령어	236
표 12-5. MEMORY DISPLAY 관련 명령어	236
표 12-6. 포트 통계 조회 명령들	238
표 12-7. 포트 통계 설정 명령	240
표 12-8. 포트 통계 초기화 명령	240

표 12-9. RMON 항목 -----	242
표 12-10. RMON ALARM AND EVENT 설정 명령 -----	243
표 12-11. RMON HISTORY 설정 및 STATISTICS 명령 -----	245
표 12-12. E7500 SERIES 스위치의 로그 레벨 -----	246
표 12-13. 시스템 로그 기본 설정 값 -----	247
표 12-14. 시스템 메시지 로깅 환경 설정 명령 -----	248
표 13-1 SWITCH PRIORITY VALUE AND EXTENDED SYSTEM ID -----	253
표 13-2 SPANNING-TREE TIMERS -----	253
표 13-3 PORT STATE COMPARISON -----	258
표 15-1 LACPDU 에 포함되는 정보 -----	319
표 20-1 NETFLOW V5 RECORD 내용 -----	372
표 21-1. QOS 전역 설정 명령어 -----	380
표 21-2. TX-SCHEDULING MAP 설정 명령어 -----	382
표 21-3. TX-SCHEDULING 설정 명령어 -----	382
표 21-4. PORT TRUST 설정 명령어 -----	383
표 21-5. DSCP-QUEUE MAP 설정 명령어 -----	384
표 21-6. DSCP-COS MAP 설정 명령어 -----	385
표 21-7. DSCP-MUTATION MAP 설정 명령어 -----	385
표 21-8. COS-QUEUE MAP 설정 명령어 -----	386
표 21-9. COS-DSCP MAP 설정 명령어 -----	387
표 21-10. COS-MUTATION MAP 설정 명령어 -----	387
표 21-11. STANDARD IP ACL 설정 명령어 -----	388
표 21-12. EXTENDED IP ACL 설정 명령어 -----	390
표 21-13. STANDARD IP ACL 설정 명령어 -----	391
표 21-14. ACL 의 인터페이스 적용 설정 명령어 -----	392
표 21-15. CLASS-MAP 설정 명령어 -----	393
표 21-16. CLASS-MAP 설정 명령어 -----	395
표 21-17. SERVICE-POLICY 설정 명령어 -----	396
표 21-18. SERVICE-POLICY 의 CONTROL-PLANE 적용 설정 명령어 -----	397
표 21-19. RATE-LIMIT 의 CONTROL-PLANE 적용 설정 명령어 -----	397
표 23-1. 파일 관리를 위한 명령어 -----	405
표 23-2. FTP 를 통한 DOWN/UP LOAD 명령어 -----	407
표 23-3. TFTP 를 통한 DOWN/UP LOAD 명령어 -----	409
표 23-4. CONFIGURATION MANAGEMENT 명령어 -----	410
표 23-5. SFE/NETFLOW 소프트웨어 관리 명령어 -----	412
표 23-6. BOOT MODE 설정 및 시스템 재 시동 명령어 -----	416
표 23-7. BOOT MODE 설정 및 시스템 재 시동 명령어 -----	417

그림 목차

그림 2-1. E7500 SERIES 스위치와 운영 단말 연결	30
그림 4-1. E 7500 SERIES 스위치의 포트 기반 VLAN 구성 예	75
그림 4-2. 두 스위치에 걸쳐서 설정된 단일 포트 기반 VLAN	76
그림 4-3. 두 스위치에 걸쳐서 설정된 두 개의 포트 기반 VLAN	77
그림 4-4. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 물리적 다이어그램	79
그림 4-5. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 논리적 다이어그램	79
그림 4-6. NATIVE VLAN	81
그림 4-7. VLAN 설정 예제 – TAGGED AND UNTAGGED VLAN	87
그림 5-1. 네트워크 설정 예 – 복수 IP ADDRESS	96
그림 5-2. 네트워크 설정 예 – STATIC ROUTE	97
그림 6-1. E7508 를 DHCP SERVER 로 사용	100
그림 6-2. DHCP RELAY AGENT 로서 DHCP SERVER 의 MESSAGE 전달	110
그림 6-3. DHCP RELAY OPTION82	115
그림 6-4. DHCP SMART-RELAY 동작 절차	117
그림 6-5. DHCP CLASS 기반 DHCP PACKET RELAY	121
그림 7-1 RIP 를 설정한 네트워크 예제 설정 및 구성도	144
그림 8-1. OSPF NETWORK	155
그림 11-1. 여러 목적지에 트래픽을 전달하는 방법을 제공하는 멀티캐스팅	199
그림 12-1. RMON MANAGER 와 RMON PROBE	241
그림 13-1 SPANNING-TREE TOPOLOGY	254
그림 13-2 SPANNING-TREE INTERFACE STATES	255
그림 13-3 PROPOSAL AND AGREEMENT HANDSHAKING FOR RAPID CONVERGENCE	259
그림 13-4 VLAN 에 대한 LOAD BALANCE	261
그림 13-5 CST, IST, CIST	262
그림 13-6 CST 에서 인식하는 네트워크	262
그림 13-7 PVST+ SWITCH 와 IEEE 802.1Q 연동	263
그림 14-1 ESTABLISHING A BFD NEIGHBOR RELATIONSHIP	301
그림 14-2 TEARING DOWN AN OSPF NEIGHBOR RELATIONSHIP	301
그림 14-3 BFD SINGLE HOP SESSION	302
그림 14-4 BFD MULTIHOP SESSION	302
그림 17-1 BASIC VRRP TOPOLOGY	330
그림 17-2 LOAD SHARING AND REDUNDANCY VRRP TOPOLOGY	331
그림 20-1 NETFLOW DEPLOYMENT	370
그림 20-2 NETFLOW V5 PACKET FORMAT	371
그림 21-1. POLICY-MAP 의 계층도	395

서문

서문은 본 가이드에 전반적인 개요 및 적용된 규칙들을 설명하고, 시스템 운영에 있어서 유용하게 사용될 수 있는 자료들을 소개한다.

1.1. 개요

본 가이드는 E7500 Series 3 계층 스위치 하드웨어를 설치한 다음 네트워크 환경을 설정하고 운영하는 데 필요한 정보를 제공함을 목적으로 한다.

본 가이드는 이더넷 기반의 네트워크 운영자 및 관련 엔지니어를 대상으로 한다. 네트워크 운영자는 본 가이드를 통하여 최적의 네트워크를 구성하고 보다 효율적으로 운영 관리할 수 있다. 또한 네트워크 운영 중 발생할 수 있는 문제를 해결하는 방법을 제공한다. 따라서 다음 항목들에 대한 기본적인 지식을 가지고 있다는 전제한다.

- 근거리 통신망(Local Area Networks, LAN) 및 메트로 네트워크(Metro Area Network, MAN)
- 이더넷, 고속 이더넷, 기가비트 이더넷 개념
- 이더넷 스위칭 및 브리징 개념
- 라우팅 개념
- TCP/IP 프로토콜 개념
- Routing Information Protocol (RIP) and Open Shortest Path First (OSPF)
- Simple Network Management Protocol (SNMP)

**Notice**

E7500 Series 스위치 하드웨어의 설치 및 초기 설정과 관련된 정보는 각 시스템의 하드웨어 설치 가이드를 참고하기 바란다.



1.2. 적용 규칙

다음의 <오류! 참조 원본을 찾을 수 없습니다.>과 <표 1-2>는 본 가이드에서 사용된 문자 표시 규칙 및 아이콘들을 설명한다.

표 1-1. 문자 표시 규칙

문자 표시 규칙	설명
Screen displays	<ul style="list-style-type: none"> 명령 수행 등의 결과로 운영 단말에 표현되는 정보 CLI 명령어 문법
Screen displays bold	<ul style="list-style-type: none"> 운영자가 운영 단말에 직접 입력한 명령어
[Key] 입력	<ul style="list-style-type: none"> 키보드의 키 입력을 나타내는 경우 [Enter] 또는 [Ctrl]과 같이 대괄호와 함께 사용 둘 이상의 키를 동시에 입력하는 경우 [Ctrl] + [z]와 같이 키를 "+"로 연결하여 표현
<i>이탤릭체</i>	<ul style="list-style-type: none"> 강조하는 부분이나 문장에서 새로 정의될 때 사용 시스템 명령어 문법에서 사용자가 입력해야 하는 파라미터

표 1-2. 알림 및 경고 아이콘

아이콘	종류	설명
	Notice	<ul style="list-style-type: none"> 중요한 기능이나 특징, 명령어, Tip
	Warning	<ul style="list-style-type: none"> 사람에 대한 상해, 데이터 손실, 또는 시스템 손상을 가져올 수 있는 위험

1.3. 관련 문서

E7500 Series 스위치 매뉴얼은 다음과 같이 구성된다. 본 장비에 대한 추가 적인 정보는 다음의 매뉴얼들을 통하여 알 수 있다.

매뉴얼 종류	주요 내용
<i>Hardware Installation Guide</i>	<ul style="list-style-type: none">■ 스위치 하드웨어 설치■ 초기 운용 환경 설정
<i>User Guide</i>	<ul style="list-style-type: none">■ 서비스 제공을 위한 운용 환경 설정■ 시스템 운용 관리 및 유지보수■ 문제 해결(Trouble shooting)

**Notice**

E7500 Series 스위치를 포함한 (주)유비쿼스 네트워크스의 제품에 대한 최신 문서 및 관련 정보들은 홈페이지(<http://www.ubiquoss.com>)를 통하여 다운로드 받거나 서비스를 요청할 수 있다.

본 문서는 E7500 Series 에 대한 통합 매뉴얼이다.

2

E7500 Series 스위치
시작하기

본 장은 시스템 운영자가 E7500 Series 3 계층 스위치의 운용 환경을 처음 설정할 때 필요한 정보를 제공한다. 스위치 시작의 개요는 다음과 같다.

- 편집 및 도움말 기능
- 스위치 명령어 모드의 이해
- 스위치 가동
- E7500 Series 스위치 사용자 인터페이스
- 시스템 로그인과 패스워드 설정
- SNMP 환경설정
- 스위치의 파일 및 환경 설정의 보기와 저장
- 액세스 리스트
- 텔넷 클라이언트

2.1. 편집 및 도움말 기능

본 장은 명령어 편집기의 편집 기능과 도움말 기능에 대하여 설명한다.

2.1.1. 명령어 문법의 이해

다음은 운영자가 시스템 운영을 위한 명령어를 입력하는 단계를 설명한다. 명령어 인터페이스 사용에 대한 자세한 정보는 다음 장에 설명된다.

명령어 라인 인터페이스를 사용하기 위하여 다음의 단계를 거치도록 한다.

- 1) 명령어 프롬프트에서 명령어를 입력하기 전에, 먼저 적절한 권한을 가지고 있는 프롬프트 수준에 있는지 먼저 확인하라. 대부분의 환경 설정 관련 명령어들은 시스템 운영자 수준의 권한을 필요로 한다.
- 2) 수행하고자 하는 명령어를 입력하라. 만약 명령어가 추가적인 명령어(sub-command) 또는 파라미터 값을 입력할 필요가 없으면 3 단계로 간다.
 - a. 만약 명령어가 파라미터를 가지고 있으면 파라미터 이름 및 값을 입력하라.
 - b. 명령어에 따르는 파라미터에 따라서 숫자, 문자열, 또는 주소 등이 값으로 설정된다.
- 3) 명확하게 명령어 입력을 완료 하였으면, [Return]키를 눌러서 명령을 실행한다.

**Notice**

명령어를 입력하고 실행했을 때 "% Command incomplete." 메시지를 받을 때가 있다. 이는 명령어 실행에 필요한 파라미터가 제대로 입력되지 않았음을 의미하며, 입력한 명령은 실행되지 않는다. 이 때 위쪽 화살표를 누르게 되면 마지막에 입력한 명령이 표시된다.

다음은 명령어 파라미터를 제대로 입력하지 않은 경우를 보여준다.

```
Switch# show 
% Incomplete command.
Switch #
```

2.1.2. 명령어 문법 도움말(Command Syntax Helper)

E7500 Series 스위치의 CLI는 명령어 문법 도움말 기능을 자체적으로 내장하고 있다. 시스템 운영자는 명령어 입력 중 완전한 문법을 모르는 경우, 어느 위치에서든지 '?'를 쳐서 도움말을 제공받을 수 있다. E7500 Series 스위치는 다음과 같은 두 가지 도움말 기능을 제공한다.

- 전체 도움말 기능
 - 가능한 파라미터 및 값의 리스트에 대한 전체 도움말을 제공한다. 입력한 명령어 다음에 한 칸 공백을 둔다.
- 부분 도움말 기능
 - 운영자가 축약된 파라미터를 입력한 후, 이에 해당하는 파라미터에 대한 도움말을 제공한다. 입력한 명령어 다음에 공백을 두지 않는다.

다음은 전체 도움말 기능을 show 명령어로 실행해본 결과이다.

show 명령어 다음에 공백 문자와 함께 '?'를 입력하면 운영자가 입력 할 수 있는 파라미터 및 값의 리스트가 출력된다. 그리고 "Switch# show" 프롬프트 상태에서 커서가 깜박이면서 운영자의 입력을 대기한다. 운영자 입력에서 '?'는 화면에 표시되지 않는다.

```
Switch# show ?
  access-list      List IP access lists
  arp              Internet Protocol (IP)
  bfd              BFD information
  bgp              Border Gateway Protocol (BGP)
  bootvar          Boot and related environment variable
  bridge           Bridge information
  cal              CAL show
  calendar          Display the hardware calendar
  class-map        Class map entry
  cli              Show CLI tree of current mode
  clock            Display the system clock
  command          shell command
  cpu              cpu status and configuration
  debugging        Debugging functions (see also 'undebug')
  disk1:           disk1: file system
  dot1x            IEEE 802.1X Port-Based Access Control
  environment      Temperature and FAN status information
  etherchannel     EtherChannel information
  flash:           display information about flash: file system
  flowcontrol      IEEE 802.3x Flow Control
  fm-status        Show the current status
  history          Display the session command history
  hosts            IP domain-name, lookup style and nameservers
  idprom           show IDPROMs for FRUs
  inet-service     Display enabled internet services
  interface        IP interface status and configuration
  ip               Internet Protocol (IP)
  ipv6            Internet Protocol version 6 (IPv6)
```

lacp	LACP commands
lacp-counter	LACP commands
list	Show command lists
logging	Show the contents of logging buffers
mac-access-list	List MAC access lists
mac-address-table	MAC forwarding table
memory	Memory information
mirror	Port Mirroring
mls	mls global commands
module	Module Info
nsm	NSM
ntp	Network time protocol
policy-map	Policy map entry
port	port commands
port-mib	Port-Mib Count
power	Switch Power
pppoe	Point-to-Point over Ethernet (PPPoE)
privilege	Display your current level of privilege
processes	Active process statistics
redundancy	Redundancy Facility (RF) information
reload	Scheduled reload information
rmon	Remote Monitoring Protocol (RMON)
route-map	route-map information
router-guard	Multicast Router-Guard Commands
router-id	Router ID
running-config	Current Operating configuration
service	Setup miscellaneous service
service-policy	Service Policy entry
slot	Slot Info
snmp	Show snmp statistics
spanning-tree	spanning-tree Display spanning tree information
startup-config	Contents of startup configuration
system	Display the system information
tech-support	Show system information for Tech-Support
uptime	Display elapsed time since boot
usbflash:	usbflash: file system
users	Display information about terminal lines
version	System software status
virtual-servers	Virtual-servers
vlan	Display VLAN information
vrrp	VRRP information
whoami	Display information about the current user

```
Switch #show_
```

부분 도움말 기능을 show 명령어를 통하여 보면 다음과 같다. show 명령어 입력 후 공백 없이 '?'를 입력하면 다음과 같이 show 명령어에 대한 설명이 표시되고 커서가 깜박이면서 다음 명령 입력을 기다린다.

```
Switch# show?
  show Show running system information
Switch# show_
```

위 예에서 운영자는 포트의 상태를 알고 싶지만 정확한 명령을 모른다고 하자. 그러면 'p'를 치고 공백 없이 '?'를 치면 'p'로 시작하는 서브 명령어의 리스트가 다음과 같이 출력된다. 물론 운영자가 입력한 명령은 다시 표시가 되면서 커서가 깜박이면서 입력을 대기한다.

```
Switch# show p?
  policy-map  Policy map entry
  port        port commands
  port-mib    Port-Mib Count
  power       Switch Power
  pppoe       Point-to-Point over Ethernet (PPPoE)
  privilege   Display your current level of privilege
  processes   Active process statistics
Switch# show p_
```

2.1.3. 단축 명령어 입력

E7500 Series 스위치의 CLI는 명령어 및 파라미터를 다 입력하지 않고, 단축 명령어를 통한 실행을 지원한다. 일반적으로 명령어의 첫 두세 글자를 입력하여 단축 명령을 수행한다.



Notice 단축 명령을 사용할 때, 시스템 운영자는 E7500 Series 스위치가 명령어를 구분하여 인식할 수 있도록 충분히 입력해야 한다. "% Ambiguous command"라는 메시지를 받을 때가 있다. 이것은 해당 모드에 입력한 문자와 prefix가 같은 하나 이상의 명령어가 있음을 의미한다.

```
Switch# show i_
% Ambiguous command: "show i"
Switch# show i?
  idprom      show IDPROMs for FRUs
  inet-service Display enabled internet services
  interface   IP interface status and configuration
  ip          Internet Protocol (IP)
  ipv6        Internet Protocol version 6 (IPv6)
Switch# show i_
```

2.1.4. 명령어 심볼

본 가이드에서 설명하는 시스템 명령어 문법에는 다양한 심볼이 사용된다. 명령어 심볼은 명령어 수행을 위해서 파라미터들이 어떻게 입력되어야 하는지를 설명한다. 시스템 명령어 문법에 적용된 심볼 및 각각의 심볼이 의미하는 바는 다음 <표 2-1>과 같다.

표 2-1. 명령어 구문 심볼



심볼	이름	설명
<>:	Angle brackets	<ul style="list-style-type: none"> 명령어 문법에서 하나의 변수 또는 값을 의미한다. 이렇게 표현된 파라미터는 반드시 입력을 해야 한다. 예를 들어, 다음과 같은 명령어가 있을 때 <code>access-list <1-99> (deny permit) address</code> 표준 IP access control list 번호는 <1-99> 사이의 값으로 반드시 입력해야 한다.
{ }:	Braces	<ul style="list-style-type: none"> 명령어 문법에서 사용되는 파라미터 또는 값의 리스트 시스템 운영자는 리스트에 포함된 항목 중에서 최소한 하나 이상을 입력해야 한다. 예를 들어, 다음과 같은 명령어가 있을 때 <code>router {rip ospf}</code> 시스템 운영자는 라우팅 프로토콜로서 RIP 또는 OSPF 중의 하나를 반드시 명시해야 한다.
[]:	Square brackets	<ul style="list-style-type: none"> 명령어 문법에서 사용되는 파라미터 또는 값의 리스트 시스템 운영자는 리스트에 포함된 항목 중에서 필요한 항목을 선택적으로 입력한다. 경우에 따라서는 하나도 입력을 하지 않을 수도 있다. 예를 들어, 다음과 같은 명령어가 있을 때 <code>show interface [ifname]</code> 인터페이스의 이름을 정의하지 않을 수도 있다.
:	Vertical bar	<ul style="list-style-type: none"> 파라미터 리스트에서 상호 배타적인 항목들을 표현
<i>Italic 체</i>		<ul style="list-style-type: none"> 입력할 변수들
Bold 체		<ul style="list-style-type: none"> 운영자가 입력해야 하는 명령어
A.B.C.D		<ul style="list-style-type: none"> IP 주소 또는 서브넷 마스크를 의미
A.B.C.D/M		<ul style="list-style-type: none"> IP prefix 를 의미 (예. 192.168.0.0/24)

2.1.5. 명령어 라인 편집 키 및 도움말

E7500 Series 스위치는 Emacs 와 유사한 편집 기능을 제공한다. <표 2-2>는 운영 단말이 제공하는 명령어 라인 편집 명령 및 도움말 기능을 설명한다.

표 2-2. 명령어 라인 편집 명령 및 도움말 기능

명령어	설명
[Ctrl] + [A]	<ul style="list-style-type: none"> 커서를 줄의 처음으로 이동

[Ctrl] + [E]	■ 커서를 줄의 끝으로 이동
[Ctrl] + [B]	■ 커서를 한 단어 뒤로 이동
[Ctrl] + [F]	■ 커서를 한 글자 앞으로 이동
Backspace	■ 커서 앞의 한 글자를 삭제
[Ctrl] + [K]	■ 현재 커서로부터 줄의 끝까지 문자를 삭제
[Ctrl] + [U]	■ 현재 커서로부터 줄의 처음까지 문자를 삭제
Tab	<ul style="list-style-type: none"> ■ 명령어의 일부분을 치고 [tab]을 치면 그 prompt 에서 같은 prefix 를 가진 명령어가 여러 개 있을 경우 리스트를 표시 ■ 한 개의 명령어만 있을 경우 명령어 나머지 부분을 완성
[Ctrl] + [P] 또는 	■ 마지막 입력 명령어부터 차례 대로 20 개까지의 명령어 입력에 대한 이력을 표시
[Ctrl] + [N] 또는 	■ 다음 명령어를 표시
?	<ul style="list-style-type: none"> ■ prompt 상에서 사용 가능한 명령어의 리스트와 설명을 표시 ■ 명령어 다음에 '?'를 쳤을 경우, 해당 명령어 다음에 입력해야 할 파라미터 리스트를 표시 ■ 부분적인 명령어에 바로 붙여서 '?'를 입력했을 경우 같은 prefix 를 가진 명령어의 리스트를 표시
Return 또는 Spacebar 또는 Q	<ul style="list-style-type: none"> ■ -- More -- 에서 Return 키를 누르면 다음 한 line 이 표시 ■ Spacebar 를 누르면 다음 페이지가 표시되며, Q 를 누르면 종료하고 prompt 상태로 전환

2.2. 스위치명령어 모드

E7500 Series 스위치는 <표 2-3>와 같이 다양한 스위치 명령어 모드를 지원한다. 각 스위치 명령어 모드마다 운영자에게 주어지는 권한에는 차이가 있다.

표 2-3. 스위치 명령어 모드

모드	프롬프트	설명
User 모드	Switch >	■ 보통 통계 정보를 디스플레이
Privileged 모드	Switch #	■ 시스템 설정을 출력하거나 시스템 관리 명령을 사용
Config 모드	Switch (config) #	■ 스위치의 환경 설정 값을 글로벌 하게 변경
Interface 모드	Switch(config-if-fal/1) # Switch(config-if-vlan1) #	■ 인터페이스의 환경 설정을 변경

Router 모드	Switch(config-rip) # Switch(config-ospf) #	■ RIP 이나 OSPF 등의 라우팅 프로토콜의 환경 설정을 변경
DHCP pool 모드	Switch(config-dhcp) #	■ DHCP 주소 pool 을 설정



Notice

명령어 프롬프트는 각 모드를 나타내는 문자열 앞에 E7500 Series 스위치의 이름을 호스트 이름으로 사용한다. 본 가이드에서는 'Switch' 프롬프트를 공통의 호스트 이름으로서 사용한다.

시스템 운영자는 E7500 Series 스위치의 환경을 설정 할 때, 여러 가지 종류의 프롬프트를 접하게 된다. 프롬프트는 환경 설정 모드에서 운영자가 현재 어느 위치에 와 있는 지를 알려준다. 스위치의 환경 설정을 변경하기 위해서는 반드시 프롬프트를 체크 해야만 한다. <표 2-4>은 스위치의 명령어 모드 사이의 이동 방법을 설명한다.

표 2-4. 스위치의 명령어 모드 사이의 이동

명령어	설명
enable	<ul style="list-style-type: none"> ■ User 모드에서 Privileged 모드로 이동 ■ Privileged 모드의 password 를 입력할 필요
disable	<ul style="list-style-type: none"> ■ Privileged 모드에서 User 모드로 이동
configure terminal	<ul style="list-style-type: none"> ■ Privileged 모드에서 Config 모드로 이동
interface ifname	<ul style="list-style-type: none"> ■ Config 모드에서 Interface 모드로 이동
router {rip ospf}	<ul style="list-style-type: none"> ■ Config 모드에서 Router 모드로 이동
exit	<ul style="list-style-type: none"> ■ 이전의 모드로 이동
end	<ul style="list-style-type: none"> ■ 어느 모드에서든 Privileged 모드로 이동 ■ User 모드에서는 이동하지 않는다.
ip dhcp pool name	<ul style="list-style-type: none"> ■ Config 모드에서 DHCP pool 설정 모드로 이동

2.3. E7500 Series 스위치가동

E7500 Series 스위치는 처음 가동될 때, 자체 테스트를 실행하고 플래시 메모리로부터 OS 이미지를 찾아서 메모리에 로드 하여 시스템을 시작한다. 시스템 부팅이 완료되면 플래시 메모리에 저장되어 있는 이전 환경 설정 값(startup-config)을 로딩한다.



Notice

E7500 Series 스위치는 시스템 안정성을 위하여 Primary 및 Secondary 등 두 개의 OS 이미지를 관리한다. 기본적으로 Primary OS 이미지가 로드 되도록 설정되어 있으며, 운영자는 스위치의 boot 모드 또는 privileged 모드에서 이를 변경할 수 있다.

2.4. 사용자 인터페이스

시스템 운영자는 스위치의 환경을 설정하고, 환경 설정을 검증하고, 통계 정보 수집 등 다양한 시스템 운영 유지 보수의 목적으로 스위치에 접속할 수 있다. 스위치에 접속하기 위한 가장 기본적인 방법은 E7500 Series 스위치가 제공하는 별도의 콘솔 포트를 통하여 직접 접속하는 것이다(*Out-of-band management*).

스위치로 연결하는 또 다른 방법은 원격지에서 텔넷 프로그램을 이용하는 것이다. 원격지에서 텔넷 연결을 위한 별도의 포트를 지원하지는 않고 서비스 포트를 통하여 접속하도록 한다(*In-band management*).

운영자는 아래의 방법을 사용하여 E7500 Series 스위치를 관리할 수 있다.

- 콘솔 포트에 터미널을 연결해서 CLI 접속.
- TCP/IP 기반 네트워크에서 텔넷 연결을 사용하여 CLI 접속.
- SNMP Network Manager 를 통해서 관리.

E7500 Series 스위치는 운영 관리를 위하여 다음과 같이 동시 접속 연결을 지원한다.

- 1 개의 콘솔 연결
- 최대 10 개의 텔넷 연결

2.4.1. 콘솔 연결

시스템에 내장된 CLI 는 RJ-45 형태의 이더넷 포트를 통하여 접속이 가능하다. 이를 위하여 운영 단말 (또는 terminal emulation 소프트웨어가 탑재된 워크스테이션)은 9 핀, RS-232 DB9 포트를 지원해야 한다. 콘솔 포트는 E7500 Series 스위치의 경우 후면의 SGIM(Switching, Gigabit ethernet I/O & Management Module) 모듈에 탑재된다.

>과 같이 E7500 Series 스위치가 제공하는 콘솔 포트에 운영 단말을 연결한다. 일단 연결이 설정되면, 프롬프트가 나오고 로그인 프로세스를 수행한다.

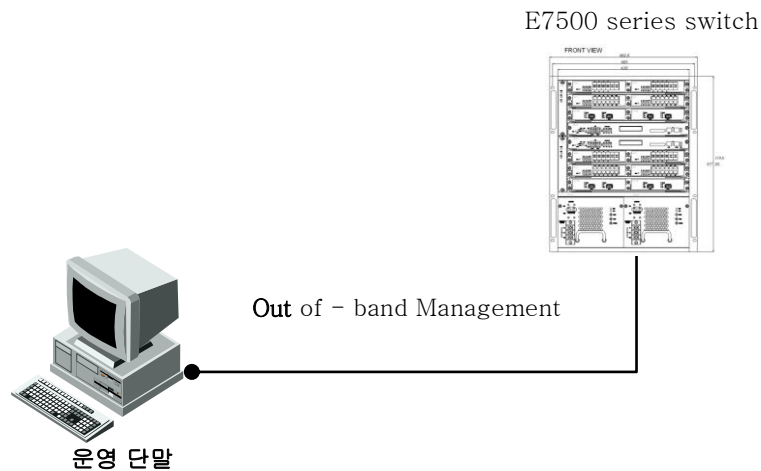


그림 2-1. E7500 Series 스위치와 운영 단말 연결

**Notice**

운영 단말의 설정 방법 및 콘솔 포트 핀 설정은 E7500 Series 스위치하드웨어 설치 가이드를 참조하기 바란다.

2.4.2. 텔넷 연결

시스템 운영자는 TCP/IP 및 텔넷 접속 기능을 가지고 있는 워크스테이션을 통하여 E7500 Series 스위치에 접속할 수 있다. 텔넷을 사용하기 위하여, 운영자는 ID 및 패스워드를 설정하여야 하며, 스위치는 적어도 하나 이상의 IP 주소를 가지고 있어야 한다.

텔넷 {<ipaddress> | <hostname>} [<port_number>]

텔넷 연결이 성공적으로 설정되며 사용자 패스워드를 입력하라는 프롬프트가 뜨고, 텔넷 사용자 패스워드를 입력하면 스위치의 *User* 모드로 들어가게 된다.

또한 시스템 보안을 위하여 액세스 리스트를 사용하여 텔넷에 연결하는 사용자를 제한할 수 있다. 이는 <[2.10 ACL\(Access Control List\)](#)>절을 참조하라.

2.4.3. SNMP Network Manager 를 통한 연결

네트워크 관리자(Network Manager)는 SNMP(Simple Network Management Protocol)를 이용해 E7500 Series 스위치를 관리할 수 있다.

**Notice**

SNMP 에 대한 추가적인 정보는 <[2.9. SNMP\(Simple Network Management Protocol\)](#)>절을 참조하라.

2.5. 사용자 관리

2.5.1. 사용자 등록 및 삭제 설정

시스템 운영자는 E7500 series 스위치를 설정 및 관리하기 위해서 콘솔 포트나 텔넷을 통해 시스템에 접속할 수 있다. 사용자 및 패스워드를 설정하여 시스템에 접속하는 사용자를 관리할 수 있으며 **privilege level** 설정으로 등록할 사용자의 권한을 설정할 수 있다.

새로 등록된 사용자는 **privilege level** 을 기본값인 1로 가지며, **user** 모드 명령을 실행할 수 있다. **User** 모드에서 “**enable**” 명령을 수행하면 **privileged** 모드로 진입 가능하다.

다음은 각 **privilege level** 에 대한 설명이다.

- Privilege level 0은 *non-privileged* 상태를 나타낸다.
- Privilege level 1-14는 user 모드 명령을 수행할 수 있다.
- Privilege level 15는 privilege 모드 명령을 수행할 수 있다.

표 2-5. 사용자 등록, 삭제, 관리 명령어

명령어	설명	모드
username name {nopassword password [0 7] password secret [0 5] password}	사용자를 등록한다. <ul style="list-style-type: none"> ■ nopassword: 로그인 시 패스워드 입력이 요구되지 않는다. ■ password or secret: 로그인 시 패스워드 입력이 요구되며 password 와 secret 은 암호화 방식에 따라 구분된다. 0 – 암호화 하지 않음. 5 – MD5 암호화 7 – DES 암호화 	Config
no username name	등록된 사용자를 삭제한다. 사용자가 root 인 경우 패스워드는 초기화 값으로 변경된다.	Config
username name privilege <0-15>	사용자의 privilege level 을 변경한다.	Config
username name access-class <1-99>	사용자에 대해 access-list 를 적용한다. <ul style="list-style-type: none"> ■ <1-99> : IP standard access list 	Config
no username name access-class	사용자에 적용된 access-list 를 해제한다.	Config
username name user-maxlinks value	해당 사용자로 접속 가능한 최대 session 수를 설정한다.	Config
no username name user-maxlinks value	해당 사용자로 접속 가능한 최대 session 수를 초기화 값으로 변경한다.	Config

	■ Default: 32 개	
username name unlimited-session-ip A.B.C.D	Session 접속 수를 제한 받지 않는 사용자 및 IP 주소를 설정한다.	Config
no username name unlimited-session-ip	Session 접속 수를 제한 받지 않는 사용자 설정을 해제한다.	Config

사용자 추가

아래 예제는 사용자 등록 및 사용자의 패스워드와 `privilege level` 을 설정한다. 'testuser1' 사용자는 로그인 시 패스워드 입력 프롬프트가 출력되지 않으며 시스템에 접속할 수 있다. 'testuser2'와 'testuser3' 사용자는 로그인 시 설정한 패스워드를 입력함으로써 시스템에 접속 가능하며, `enable` 명령을 통해 `privileged` 모드로 진입할 수 있다.

```
Switch# configure terminal
Switch# configure terminal
Switch(config)# username testuser1 nopassword
Switch(config)# username testuser2 password testpw
Switch(config)# username testuser3 privilege 15 password testpw
Switch(config)# end
Switch # show running-config
!
username testuser1 nopassword
username testuser2 password 0 testpw
username testuser3 privilege 15 password 0 testpw
!
Switch#
```

아래는 `privilege level` 이 15 인 'testuser3'가 로그인하여 `privileged` 모드로 진입하는 경우이다.

```
Ubiquoss L3 Switch

Switch login: testuser3
Password: testuser3

Hello.

Switch> enable
Switch#
```



Notice aaa authorization exec 명령이 설정되어 있고, `privilege level` 이 15 이상인 사용자의 경우 로그인 후 `user` 모드가 아닌 `privileged` 모드로 진입한다.

2.5.2. 패스워드 설정

E7500 series 스위치는 시스템 보안을 위해 사용자 및 `enable` 패스워드를 설정할 수 있다. 사용자 패스워드 설정은 <2.10. ACL(Access Control List)>를 참고하라.

- 사용자 패스워드

- 콘솔이나 텔넷을 통해 사용자 모드로 액세스 할 때 사용
- Enable 패스워드
- Privileged 모드의 보안을 목적으로 사용

표 2-6. Enable 패스워드 설정 명령

명령어	설명	모드
enable password {password [0 7] password secret [0 5] password}	Privileged 모드로 진입하기 위한 패스워드를 설정한다. <ul style="list-style-type: none"> ■ password or secret: Privileged 모드 진입 시 패스워드 입력이 요구되며 password 와 secret 은 암호화 방식에 따라 구분된다. 0 – 암호화 하지 않음. 5 – MD5 암호화 7 – DES 암호화 	Config
no enable password	Privileged 모드로 진입하기 위한 패스워드 설정을 해제한다.	Config

Enable password 설정

Privileged 모드로 진입할 때 패스워드를 입력하도록 설정한다.

```
Switch# configure terminal
Switch(config)# enable password testpw
Switch(config)# end
Switch# show running-config
!
enable password 0 testpw
!
```

아래와 같이 설정한 패스워드를 입력하면 privileged 모드로 진입할 수 있다.

```
Ubiquoss L3 Switch

Switch login: root
Password:

Hello.

Switch>enable
Password: testpw
Switch#
```

E7500 series 스위치는 암호화하지 않은 패스워드를 설정한 경우 show running-config 명령으로 설정한 패스워드를 볼 수 있는 문제를 방지하기 위해서 패스워드 암호화 모드를 지원한다. 패스워드 암호화 모드는 service password-encryption 명령으로 설정할 수 있다.

표 2-7. 패스워드 암호화 모드 설정 명령

. 명령어	설명	모드
<code>service password-encryption</code>	시스템에 설정된 패스워드가 암호화되어 보여지도록 패스워드 암호화 모드를 설정한다.	Config
<code>no service password-encryption</code>	패스워드가 암호화 모드를 해제한다.	Config

**Notice**

“no service password-encryption” 명령은 보안을 위해 기존에 암호화된 패스워드를 암호화 되기 전의 문자열로 되돌리지는 않는다. 암호화 모드를 해제한 이후에 설정되는 패스워드만 암호화 하지 않도록 설정한다.

패스워드 암호화 모드 설정

패스워드 암호화 모드를 설정하면 기존에 추가되었던 패스워드가 암호화되어 출력된다.

```
Switch# configure terminal
Switch(config)# service password-encryption
Switch(config)# end
Switch# show running-config
!
enable password 7 xxEp88GxHJIgc
username testuser1 nopassword
username testuser2 password 7 XX1LtbDbOY4
username testuser3 privilege 15 password 7 XX1LtbDbOY4
!
Switch#
```

2.6. AAA (Authentication, Authorization, Accounting)

2.6.1. 인증 (Authentication)

시스템 보안을 위해 시스템에 접속하는 사용자에게 대한 인증이 필요하다. E7500 series 스위치는 로그인 시도하는 사용자에게 대한 인증과 privileged 모드로 진입할 때 enable 패스워드에 대한 인증을 수행한다.

다음은 E7500 series 스위치에서 제공하는 인증 방법으로 Local 시스템의 사용자 정보를 통한 인증과 인증 프로토콜인 RADIUS 및 TACACS+를 통한 인증 방법을 제공한다.

- Local
- RADIUS
- TACACS+

위와 같은 인증 방법은 한 가지 이상 설정될 수 있으며 여러 인증 방법을 설정했을 경우 설정한 순서대로 인증을 시도하게 된다. 사용자는 인증에 대한 성공 또는 실패에 대한 결과를 얻지 못하는 경우에 다른 인증 방법으로 인증을 시도할 수 있도록 여러 인증 방법을 설정해야 한다. **Local** 시스템으로 인증을 시도하는 경우 로그인 또는 **privileged** 모드로 진입하기를 원하는 사용자에게 대한 정보가 **local** 시스템에 없다면 **local** 인증 방법 다음으로 설정된 인증 방법으로 인증을 시도한다. 마찬가지로 **RADIUS** 또는 **TACACS+** 서버로 인증을 시도하는 경우 해당 서버와 시스템이 연결되지 않는 경우 또는 서버에 사용자에게 대한 정보가 없는 경우 등으로 인해 인증 결과를 수신하지 못했다면 다음으로 설정된 인증 방법으로 인증을 시도하게 된다.

Local 인증은 항상 활성화된 상태이며 인증 설정을 명시하지 않은 경우 기본적으로 **Local** 인증 방법으로 사용자 인증을 수행한다.

2.6.2. 사용자 인증

시스템에 접속하기 위해 로그인하는 사용자에게 대해 사용자 이름과 패스워드로 인증을 시도한다. **Local** 시스템의 사용자 정보 또는 **RADIUS** 및 **TACACS+** 서버를 통한 인증이 가능하며 **local** 시스템을 통해 인증하기 위해서는 먼저 사용자를 등록해야 한다. **Local** 시스템의 사용자 등록은 <[2.5.1 사용자 등록 및 삭제 설정](#)>를 참조하라.

표 2-8. 사용자 인증 설정 명령어

명령어	설명	모드
aaa authentication login default {local radius tacacs+}	로그인 시 입력된 사용자 이름 및 패스워드에 인증한다.	Config
no aaa authentication login default	로그인할 때의 사용자 인증 방법을 초기값으로 변경한다. ■ Default: Local	Config
aaa authentication login template-user name	RADIUS 또는 TACACS+ 서버로 인증하는 경우 dummy 사용자를 지정할 수 있다. Dummy 사용자는 local 시스템에 등록되어 있어야 한다.	Config
no aaa authentication login template-user	Dummy 사용자 지정을 해제한다.	Config
aaa authentication login authen-type (chap pap)	TACACS+ 서버로 인증하는 경우 인증메시지를 chap 또는 pap 방식으로 전송한다. ■ Default: Ascii	Config
no aaa authentication login authen-type	TACACS+ 서버로 인증하는 경우 인증메시지를 ascii 방식으로 전송한다.	Config

사용자 인증 설정

아래의 예제에서 사용자가 로그인을 시도하는 경우 먼저 TACACS+ 서버로 인증을 시도하며 TACACS+ 서버에서 응답을 받지 못한 경우 RADIUS 서버로 인증을 시도한다. 마찬가지로 RADIUS 서버에서 응답을 받지 못한 경우 디폴트로 제공하는 local 방식을 통해 인증을 시도한다.

```
Switch# configure terminal
Switch(config)# aaa authentication login default tacacs+ radius
Switch(config)# end
Switch#
```

2.6.3. Enable password 인증

사용자가 privileged 모드로 진입을 원할 때 enable 패스워드로 인증할 수 있다. Local 로 인증하는 경우 시스템에 설정한 enable 패스워드를 통해 인증을 수행하며, RADIUS 또는 TACACS+ 서버를 통해 인증을 수행할 수도 있다. Local 로 인증할 때 local 시스템에 enable 패스워드가 설정되지 않은 경우 인증은 항상 성공하게 되므로 privileged 모드로 인증을 수행하기 위해서는 적절한 enable 패스워드를 설정해야 한다. Local 시스템의 enable 패스워드 설정은 <[2.5.2 패스워드 설정](#)>을 참조하라.

표 2-9. Privileged 모드 사용자 인증 설정 명령어

명령어	설명	모드
aaa authentication enable default {enable radius tacacs+}	사용자가 privileged 모드로 진입할 때 enable 패스워드에 대해 인증한다.	Config
no aaa authentication enable default	Enable 패스워드에 대한 인증 방법을 초기값으로 변경한다. <ul style="list-style-type: none"> Default: enable 패스워드(Local 시스템) 	Config

privileged 모드 사용자 인증 설정

아래의 예제에서 사용자가 privileged 모드로 진입을 원하는 경우 enable 패스워드에 대해 먼저 TACACS+ 서버로 인증을 시도한다. TACACS+ 서버에서 응답을 받지 못한 경우 RADIUS 서버로 인증을 시도한다. 마찬가지로 RADIUS 서버에서 응답을 받지 못한 경우 디폴트로 제공하는 local 방식을 통해 인증을 시도한다.

```
Switch# configure terminal
Switch(config)# aaa authentication enable default tacacs+ radius
Switch(config)# end
Switch#
```

2.6.4. 권한 (Authorization)

E7500 series 스위치는 privilege level 을 통해 시스템 자원을 사용할 수 있는 권한을 검사할 수 있다. EXEC shell 을 실행할 때 사용자의 privilege level 과 local 시스템 또는 원격 서버(RADIUS 또는 TACACS+)에 설정한 사용자의 privilege level 을 비교한다. 시스템 자원을 사용하고자 하는 사용자의

privilege level 이 설정한 privilege level 보다 낮은 경우 에러 메시지를 출력하며 실행에 실패하게 된다. 또한 특정 명령을 실행할 때 각 명령의 privilege level 과 설정한 privilege level 을 비교하여 해당 명령의 실행 권한을 local 시스템 또는 원격 서버(TACACS+)을 통해 검사할 수 있다.

인증 서버로 접속이 되지 않거나 인증 서버로부터 결과를 수신하지 못하는 경우를 대비해서 항상 local 시스템을 통한 권한 검사 방법을 추가해야 한다. Local 시스템 권한 검사마저 없는 경우 권한 검사는 항상 실패하게 되며, 이 경우 콘솔을 통한 설정 변경이 필요하다. 콘솔을 통해 시스템에 로그 인한 사용자는 권한을 검사하지 않는다.

2.6.5. EXEC 실행 권한

EXEC shell 은 privileged 모드로 진입할 때 실행되는 사용자 정의 셸이다. EXEC shell 을 실행할 수 있는 권한은 기본적으로 시스템에 등록되어 있는 사용자의 privilege level 로 확인한다. Local 시스템에 등록된 사용자의 privilege level 변경은 <2.5.1. 사용자 추가 및 삭제>를 참조하라. 만약 사용자의 EXEC shell 실행 권한을 local 시스템이 아닌 RADIUS 또는 TACACS+ 서버로 확인할 경우 해당 서버에 권한을 검사할 사용자의 privilege 정보가 설정되어 있어야 한다.

표 2-10. EXEC shell 실행 권한 설정 명령어

명령어	설명	모드
aaa authorization exec default [local radius tacacs+]	EXEC shell 을 실행할 권한을 local 시스템 또는 RADIUS 및 TACACS+ 서버에 설정한 사용자의 privilege level 을 참조하여 검사한다.	Config
no aaa authorization exec default	EXEC shell 을 실행할 권한을 검사하지 않는다.	Config

EXEC shell 실행 권한을 TACACS+ 서버로 검사하도록 설정

아래의 예제는 사용자가 EXEC shell 을 실행시킬 때 TACACS+ 서버에 설정된 사용자의 privilege level 을 참조하여 권한을 검사한다. 또한 TACACS+ 서버로부터 결과를 수신하지 못한 경우 local 시스템으로부터 권한을 검사할 수 있다.

```
Switch# configure terminal
Switch(config)# aaa authorization exec default tacacs+ local
Switch(config)#
Switch#
```

TACACS+ 서버에 'testuser1' 사용자가 등록되어 있고 privilege level 이 15로 설정되어 있는 경우 아래와 같이 로그인 후 EXEC shell 을 실행시킬 수 있다. 이 경우 privilege level 이 15 이상이므로 privileged 모드로 바로 진입할 수 있다.

```
Ubiquoss I3 Switch

Switch login: testuser1
Password: testuser1
```

Hello.

Switch#

2.6.6. 명령 실행 권한

특정 명령을 실행할 때 명령에 주어진 **privilege level**로 명령 실행 권한을 검사할 수 있다. 기본적으로 각 명령의 **privilege level**은 명령이 실행되는 모드의 **privilege level**을 가지며 설정을 통해 변경이 가능하다. **Privilege level** 변경은 <2.6.4 Privilege level 설정>를 참조하라.

E7500 series 스위치는 **local** 시스템 또는 **TACACS+** 서버를 이용해 특정 명령의 실행 권한을 검사할 수 있다. <표 11>과 같이 명령이 실행되는 **privilege level**을 지정하여 권한을 검사할 명령 집합을 설정할 수 있으며, 해당 **privilege level**을 가지는 명령에 대해 **local** 시스템 또는 **TACACS+** 서버로부터 실행 권한을 검사할 수 있다.

표 2-11. 명령어 실행 권한 설정 명령어

명령어	설명	모드
aaa authorization commands <0-15> default (local tacacs+)	해당 privilege level 을 갖는 명령어를 실행하기 위해 local 시스템 또는 TACACS+ 서버로 권한을 검사할 수 있도록 설정한다. <ul style="list-style-type: none"> ▪ <0-15>: privilege level 	Config
no aaa authorization commands <0-15> default	해당 privilege level 을 갖는 명령어를 실행하기 위한 권한을 검사하지 않도록 설정한다. <ul style="list-style-type: none"> ▪ <0-15>: privilege level 	Config

명령어 실행 권한을 TACACS+서버로 검사하도록 설정

아래 예제는 **config** 모드에서 수행하는 **interface** 명령을 실행할 때 **TACACS+** 서버로 명령 실행 권한을 검사하도록 한다. **Interface** 명령을 **privilege level 2**로 설정한 후 **privilege level 2**에 대해 권한 검사를 수행한다.

```
Switch# configure terminal
Switch(config)# privilege config level 2 interface
Switch(config)# aaa authorization commands 2 default tacacs+
Switch(config)# end
Switch#
Switch# show command privilege
COMMAND-MODE          LEVEL      Command
=====
config                 2         interface
Switch#
```

Interface 명령을 실행했을 때 실행 권한이 없는 경우 아래와 같은 에러가 발생한다.

```
Switch (config)# interface Vlan 1
% Command authorization failed
Switch (config)#
```

2.6.7. 계정(Accounting)

E7500 series 스위치는 AAA의 계정 기능을 통해 세션 접속 및 명령 실행 내역을 TACACS+ 서버를 통해 관리할 수 있다.

2.6.8. 세션 접속 관리

시스템에 접속한 내역을 TACACS+ 서버에 기록한다.

표 2-12. 세션 접속 관리 설정 명령어

명령어	설명	모드
aaa accounting exec default (start-stop stop-only) tacacs+	시스템 접속 내역을 TACACS+ 서버로 전송한다. <ul style="list-style-type: none"> start-stop: 세션 시작과 끝을 모두 기록 stop-only: 세션 끝만 기록. 	Config
no aaa accounting exec default	시스템 접속 내역을 TACACS+ 서버로 전송하지 않는다.	Config

세션 접속 내역을 TACACS+ 서버로 전송하도록 설정

```
Switch# configure terminal
Switch(config)# aaa accounting exec default start-stop tacacs+
Switch(config)#
```

2.6.9. 명령 실행 내역 관리

특정 명령을 실행할 때 TACACS+ 서버로 실행 내역을 관리할 수 있다. <표 13> 과 같이 privilege level 을 지정하여 실행 내역을 TACACS+ 서버로 전송할 명령 집합을 설정할 수 있다. 기본적으로 각 명령의 privilege level 은 명령이 실행되는 모드의 privilege level 을 가지며 설정을 통해 변경이 가능하다. Privilege level 변경은 <2.6.4 Privilege level 설정>를 참조하라.

표 2-13. 명령어 실행 내역 설정 명령어

명령어	설명	모드
aaa accounting commands <0-15> default tacacs+	해당 privilege level 을 갖는 명령의 실행 내역을 TACACS+ 서버에 기록한다. <ul style="list-style-type: none"> <0-15>: privilege level. 	Config
no aaa accounting commands <0-15> default	해당 privilege level 을 갖는 명령의 실행 내역을 TACACS+ 서버에 기록하지 않는다. <ul style="list-style-type: none"> <0-15>: privilege level. 	Config

명령어 실행 내역을 TACACS+ 서버로 관리하도록 설정

아래 예제는 EXEC 모드에서 수행하는 모든 **show** 명령의 **privilege level** 을 15 로 변경하고 실행 내역을 TACACS+ 서버로 전송하도록 한다. 또한 기본적으로 **privilege level** 을 15 로 가지는 모든 명령들도 실행 내역을 TACACS+ 서버로 전송한다.

```
Switch# configure terminal
Switch(config)# privilege exec level 15 show
Switch(config)# aaa accounting commands 15 default tacacs+
Switch(config)# end
Switch#
Switch# show command privilege
COMMAND-MODE          LEVEL      Command
=====
config                15        show
Switch#
```

2.6.10. Privilege level 설정

E7500 series 스위치는 **privilege level** 을 통해 특정 명령에 대한 권한(Authorization) 및 계정(Accounting) 기능을 수행할 수 있다. 특정 명령에 대해 **privilege level** 을 설정하지 않는 경우 각 명령은 실행되는 모드의 **privilege level** 을 기본값으로 참조한다.

표 2-14. Privilege level 설정 명령어

명령어	설명	모드
<code>privilege node level <0-15> command</code>	특정 명령에 대해 privilege level 을 부여한다. <ul style="list-style-type: none"> ■ node: 설정할 명령이 실행되는 node ■ <0-15>: privilege level ■ command: privilege level 을 부여할 명령 	Config
<code>no privilege node level <0-15> command</code>	특정 명령에 대한 privilege level 을 초기값으로 변경한다. <ul style="list-style-type: none"> ■ Default: 명령이 실행되는 모드의 privilege level 	Config
<code>show command privilege</code>	설정된 명령들의 privilege level 을 확인할 수 있다.	Privileged

2.7. 서버 설정

E7500 series 스위치는 RADIUS 또는 TACACS+의 원격 서버를 통한 인증, 권한, 계정 관리 기능을 제공한다. 다음은 RADIUS 와 TACACS+ 서버의 설정 방법이다.

2.7.1. RADIUS 서버 설정

표 2-15. RADIUS 서버 설정 명령어

명령어	설명	모드
radius-server host <i>A.B.C.D</i> [key [0 7] <i>key-string</i>]	RADIUS 서버를 설정한다. <ul style="list-style-type: none"> ■ <i>A.B.C.D</i>: RADIUS 서버의 주소 ■ <i>key</i>: 서버에서 사용할 암호 키를 설정한다. 0 – 암호화 하지 않음. 7 – DES 암호화 	Config
no radius-server host <i>A.B.C.D</i>	설정된 RADIUS 서버를 삭제한다. <ul style="list-style-type: none"> ■ <i>A.B.C.D</i>: RADIUS 서버의 주소 	Config
radius-server host <i>A.B.C.D</i> [auth-port <i>PORT</i>]	RADIUS 서버를 설정하며, 서버에서 사용할 auth-port 를 설정한다. <ul style="list-style-type: none"> ■ <i>A.B.C.D</i>: RADIUS 서버의 주소 ■ <i>PORT</i>: auth-port 번호 	Config
no radius-server host <i>A.B.C.D</i> auth-port <i>PORT</i>	서버에서 사용할 auth-port 를 기본값으로 설정 한다. <ul style="list-style-type: none"> ■ Default: 1812 	Config
radius-server key [0 7] <i>key-string</i>	RADIUS 서버에 접속할 때 사용하는 공통 암호 키를 설정한다. Key 가 명시되지 않은 서버는 공통 암호 키를 사용하게 된다.	Config
no radius-server key	공통 암호 키를 삭제한다.	Config
radius-server retransmit <i>count</i>	RADIUS 서버로 AAA 정보를 재전송하는 횟수 를 설정한다. <ul style="list-style-type: none"> ■ <i>count</i>: 재전송 횟수를 설정 	Config
no radius-server retransmit	재전송 횟수를 기본값으로 설정한다. <ul style="list-style-type: none"> ■ Default: 3 회 	Config
radius-server timeout <i>seconds</i>	RADIUS 서버로부터 응답을 기다리는 시간을 설정한다. <ul style="list-style-type: none"> ■ <i>seconds</i>: Timeout 시간을 초 단위로 설정 	Config
no radius-server timeout	응답을 기다리는 시간을 기본값으로 설정한다. <ul style="list-style-type: none"> ■ Default: 5 초 	Config
ip radius source-interface <i>ifname</i>	RADIUS 서버로 전송할 정보의 source IP 주소 를 설정한다. <ul style="list-style-type: none"> ■ <i>ifname</i>: 인터페이스 이름 정보 	Config
no ip radius source- interface	설정된 source IP 주소를 해제한다.	Config

RADIUS 서버 설정

아래 예제는 여러 RADIUS 서버와 공통 암호 키로 test123 을 설정하였다. 192.168.0.1/test123 으로 AAA 정보를 서버로 전송하며 응답을 수신하지 못하는 경우 다음 RADIUS 서버로 전송을 시도 한다.

```
Switch# configure terminal
Switch(config)# radius-server host 192.168.0.1
Switch(config)# radius-server key test123
Switch(config)# radius-server host 192.168.0.2 key lns
Switch(config)# radius-server host 192.168.0.2 auth-port 3000
Switch(config)# end
Switch# show running-config
!
radius-server key test123
radius-server host 192.168.0.1
radius-server host 192.168.0.2 key lns
radius-server host 192.168.0.3 auth-port 3000
!
Switch#
```

2.7.2. TACACS+ 서버 설정

표 2-16. TACACS+ 서버 설정 명령어

명령어	설명	모드
radius-server host <i>A.B.C.D</i> key [<i>0 7</i>] <i>key-string</i>	TACACS+ 서버를 설정한다. <ul style="list-style-type: none"> ■ <i>A.B.C.D</i>: TACACS+ 서버의 주소 ■ <i>key</i>: 서버에서 사용할 암호 키를 설정한다. 0 – 암호화 하지 않음. 7 – DES 암호화 	Config
no radius-server host <i>A.B.C.D</i>	설정된 TACACS+ 서버를 삭제한다. <ul style="list-style-type: none"> ■ <i>A.B.C.D</i>: TACACS+ 서버의 주소 	Config
radius-server host <i>A.B.C.D</i> timeout <i>seconds</i>	TACACS+ 서버로부터 응답을 기다리는 시간을 설정한다. <ul style="list-style-type: none"> ■ <i>seconds</i>: Timeout 시간을 초 단위로 설정 	Config
radius-server host <i>A.B.C.D</i> timeout	응답을 기다리는 시간을 기본값으로 설정한다. <ul style="list-style-type: none"> ■ Default: 5 초 	Config
ip tacacs source-interface <i>ifname</i>	TACACS+ 서버로 전송할 정보의 source IP 주소를 설정한다. <ul style="list-style-type: none"> ■ <i>ifname</i>: 인터페이스 이름 정보 	Config
no ip tacacs source-interface	설정된 source IP 주소를 해제한다.	Config

TACACS+ 서버 설정

아래 예제는 여러 TACACS+ 서버를 설정하다. 192.168.0.1/lns 로 AAA 정보를 서버로 전송하며 응답을 수신하지 못하는 경우 다음 TACACS+ 서버로 전송을 시도 한다.

```
Switch# configure terminal
Switch(config)# tacacs-server host 192.168.0.1 key lns
Switch(config)# tacacs-server host 192.168.0.2 key test123
Switch(config)# end
Switch# show running-config
!
tacacs-server host 192.168.0.1 key lns
tacacs-server host 192.168.0.2 key test123
!
Switch#
```

2.8. Hostname 설정

Hostname 은 시스템을 구별하기 위해 사용될 수 있다. 콘솔 또는 텔넷 화면의 프롬프트는 hostname 과 현재 명령어 모드의 조합으로 이루어져 있으며 E7500 Series 스위치는 기본적으로 시스템의 모델명을 hostname 으로 사용한다.

표 2-17. Hostname 설정 명령어

명령어	설명	모드
hostname <i>string</i>	Hostname 을 변경한다.	Config
no hostname	Hostname 을 초기값으로 변경한다.	Config

Hostname 을 설정하는 절차는 다음과 같다.

```
Switch# configure terminal
Switch(config)# hostname E7500
E7500(config)# end
E7500#
E7500# configure terminal
E7500(config)# no hostname
Switch(config)# end
Switch#
```

2.9. SNMP (Simple Network Management Protocol)

SNMP(Simple Network Management Protocol)는 네트워크 관리자가 SNMP 에이전트가 설치된 장비를 MIB(Management Information Base)을 통해 관리할 수 있도록 한다. E7500 series 스위치에는 SNMPv1, SNMPv2, 그리고 SNMPv3 기능을 제공하는 SNMP 에이전트가 설치되어 있다.

2.9.1. SNMP 환경 설정

다음은 SNMP 에이전트의 시스템 관리자 및 시스템 설치 위치를 지정하는 설정이다.

표 2-18. SNMP 환경 설정 명령

명령어	설명	모드
<code>snmp-server contact <i>string</i></code>	시스템 관리자 정보를 입력한다.	Config
<code>no snmp-server contact</code>	시스템 관리자 정보를 삭제한다.	Config
<code>snmp-server location <i>string</i></code>	장비가 설치된 위치 정보를 입력한다.	Config
<code>no snmp-server location</code>	장비가 설치된 위치 정보를 삭제한다.	Config

시스템 관리자 정보 입력

```
Switch# configure terminal
Switch(config)# snmp-server contact "gil-dong hong. hong@locusnet.com"
Switch(config)# end
Switch# show running-config
!
snmp-server contact "gil-dong hong. hong@locusnet.com"
!
Switch#
```

시스템 구축 위치 입력

```
Switch# configure terminal
Switch(config)# snmp-server location "Wonhyoro-3Ga, Yongsan-gu, Seoul."
Switch(config)# end
Switch# show running-config
!
snmp-server location "Wonhyoro-3Ga, Yongsan-gu, Seoul."
!
Switch#
```

2.9.2. Community 설정

네트워크 관리자는 SNMP 에이전트에 접속하여 SNMP로 관리되는 MIB 정보를 읽거나 쓸 수 있다. SNMP 에이전트에 접속할 때 community로 인증할 수 있으며 community는 아래와 같은 두 가지 접속 타입을 가진다.

- Read-only community
 - 시스템에 읽기 전용으로 접속한다.
- Read-write community
 - 시스템에 읽기 및 쓰기로 접속한다.

표 2-19. SNMP Community 설정

명령어	설명	모드
<pre>snmp-server community string [access-type] view view-name] <1-99>]</pre>	<p>SNMP community 를 설정한다.</p> <ul style="list-style-type: none"> ■ access-type: SNMP 에이전트 접속 타입 ro: read only rw: read write ■ view: MIB 접속 범위를 지정하며, 자세한 내용은 snmp-server view 설정을 참조하라. ■ <1-99>: 접속 호스트에 대해 access-list 를 적용할 수 있다. 	Config
<pre>no snmp-server community string</pre>	SNMP community 를 삭제한다.	Config

SNMP Community 설정

아래 예제는 read-write 접속 타입의 'testcom' community 를 설정한다. 또한 'testcom'으로 접속하는 호스트는 access-list 99 를 참조하여 SNMP 를 통한 접속이 permit 또는 drop 될 수 있다.

```
Switch# configure terminal
Switch(config)# snmp-server community testcom rw 99
Switch(config)# end
Switch# show running-config
!
snmp-server community testcom rw access-class 99
!
Switch#
```

2.9.3. Trap host 설정

시스템에서 발생하는 오류 동작 또는 시스템 상태 변경 등의 이벤트는 네트워크 관리자에게 트랩(trap) 을 통해 제공될 수 있다. E7500 series 스위치는 아래와 같은 버전의 트랩을 제공하며, 기본적으로 트랩 호스트 및 "snmp-server enable traps" 명령으로 트랩을 전송하도록 설정하지 않았다면 트랩은 발생하지 않는다.

- **SNMPv1 Trap**
- **SNMPv2c Trap**
 - 기본적으로 전송되는 트랩 버전이다.
- **SNMPv3 Trap**
 - 인증 및 암호 기능을 제공하며, security model 을 설정할 수 있다.
 - 1) noAuth: 인증 및 암호화를 수행하지 않음.
 - 2) Auth: 인증 수행
 - 3) Priv: 인증 및 암호화를 수행함.

표 2-20. SNMP Trap 호스트 설정

명령어	설명	모드
snmp-server trap-host <i>A.B.C.D</i> [<i>version 1 2c 3 sec-level</i>] <i>community-string</i>	트랩을 전송할 호스트를 설정한다. <ul style="list-style-type: none"> ■ <i>A.B.C.D</i>: 트랩 호스트 주소 ■ <i>version</i>: 전송할 트랩의 버전 (Default: 2c) ■ <i>sec-level</i>: 트랩 버전이 3인 경우 <i>security model</i> 을 설정 ■ <i>community-string</i>: <i>community</i> 설정 	Config
no snmp-server trap-host <i>A.B.C.D</i> [<i>version 1 2c 3 sec-level</i>] <i>community-string</i>	설정된 트랩 호스트를 삭제한다.	Config
snmp-server trap-source <i>ifname</i>	전송할 트랩의 source IP 주소를 설정한다. <ul style="list-style-type: none"> ■ <i>ifname</i>: 인터페이스 이름 정보 	Config
no snmp-server trap-source	설정된 source IP 주소를 해제한다.	Config

표 2-21. SNMP 기본 트랩의 Enable 설정

명령어	설명	모드
snmp-server enable traps alarm [<i>fallingAlarm risingAlarm</i>]	RMON alarm 트랩을 전송하도록 설정한다.	Config
no snmp-server enable traps alarm [<i>fallingAlarm risingAlarm</i>]	RMON alarm 트랩을 전송하지 않도록 설정한다.	Config
snmp-server enable traps envmon [<i>ext-supply fan supply temperature</i>]	시스템 환경 (fan, power 등) 관련 트랩을 전송하도록 설정한다.	Config
no snmp-server enable traps envmon [<i>ext-supply fan supply temperature</i>]	시스템 환경 (fan, power 등) 관련 트랩을 전송하지 않도록 설정한다.	Config
snmp-server enable traps fru- ctrl	모듈, slot 등 실/탈장 가능한 unit 의 상태 변경 시 트랩을 전송하도록 설정한다.	Config
no snmp-server enable traps fru- ctrl	모듈, slot 등 실/탈장 가능한 unit 의 상태 변경 시 트랩을 전송하지 않도록 설정한다.	Config
snmp-server enable traps interface	Linkup, linkdown 트랩을 전송하도록 설정한다.	Config
no snmp-server enable traps	Linkup, linkdown 트랩을 전송하지 않도록	Config

interface	록 설정한다.	
snmp-server enable traps resource [cpu-load-monitor memory-free-monitor]	시스템 자원 관련 트랩을 전송하도록 설 정한다.	Config
no snmp-server enable traps resource [cpu-load-monitor memory-free-monitor]	시스템 자원 관련 트랩을 전송하지 않도 록 설정한다.	Config
snmp-server enable traps snmp [coldStart warmStart authFail]	Cold start, warm start, authentication failure 트랩을 전송하도록 설정한다.	Config
no snmp-server enable traps snmp [coldStart warmStart authFail]	Cold start, warm start, authentication failure 트랩을 전송하지 않도록 설정한 다.	Config



Notice

<표 21> 은 E7500 series 스위치에서 기본적으로 제공하는 트랩의 전송 설정 및 해제 명령을 나타내며 추후에 추가 및 삭제될 수 있다.

SNMP Trap 설정

다음 예제는 192.168.0.1 호스트로 팬, 파워, 온도 등의 환경 관련 트랩 및 linkup/linkdown 트랩이 전송 되도록 설정한다. 트랩 버전은 기본값인 2c 로 전송된다.

```
Switch# configure terminal
Switch(config)# snmp-server host 192.168.0.1 public
Switch(config)# snmp-server enable traps envmon
Switch(config)# snmp-server enable traps snmp
Switch#(config)# end
Switch# show running-config
!
snmp-server enable traps interface
snmp-server enable traps envmon fan supply temperature ext-supply
snmp-server host 192.168.0.1 version 2c public
!
Switch#
```

2.9.4. SNMPv3 설정

E7500 series 스위치는 SNMP 를 통한 시스템 관리에서 더 나은 보완 기능을 제공하기 위해 SNMPv3 를 제공한다. SNMPv3 는 사용자에 대한 인증 및 데이터에 대한 암호화 기능을 제공한다.

표 2-22. SNMPv3 설정

명령어	설명	모드
snmp-server engineID engineid-string	SNMP 에이전트를 유일하게 구분하기 위한 engine ID 를 설정한다.	Config

	SNMP engineID 를 변경하는 경우 기존에 설정한 user 를 다시 설정해야 한다. User 설정은 engine ID 를 이용해 MD5 및 SHA 의 security digest 를 생성하기 때문이다.	
no snmp-server engineID	Engine ID 를 자동으로 생성되는 기본값으로 설정한다. 기본 값은 자사의 enterprise OID(1.3.6.1.4.1.7800)와 시스템의 첫 번째 MAC 주소로 자동 생성한다.	Config
show snmp engineID	Engine ID 를 출력한다.	Privileged
snmp-server group <i>groupname</i> {v1 v2c v3 <i>sec-level</i> } [read <i>read-view</i>] write <i>write-view</i>]	SNMP group 을 설정한다. <ul style="list-style-type: none"> ■ <i>group-name</i>: Group 이름 ■ v1, v2c, v3: Group 버전 ■ <i>sec-level</i>: 트랩 버전이 3 인 경우 security model 을 설정 ■ read: Read view 설정. Read-view 가 명시되지 않은 경우 기본값으로 internet (1.3.6.1)로 설정됨. ■ write: Write view 설정 	Config
no snmp-server group <i>groupname</i> {v1 v2c v3 <i>sec-level</i> }	SNMP group 을 삭제한다	Config
show snmp group	SNMP group 을 출력한다.	Privileged
snmp-server user <i>username</i> <i>groupname</i> {v1 v2c v3 [auth (md5 sha) <i>auth-passwd</i>] [priv (des aes) <i>priv-passwd</i>] [access <1-99>]}	SNMP user 를 설정한다. <ul style="list-style-type: none"> ■ v1, v2c, v3: User 버전 ■ auth: SNMPv3 인 경우 사용자 인증을 수행할 수 있으며 암호화 방법으로 MD5 또는 SHA 를 설정할 수 있다. <i>auth-passwd</i>: 인증을 위한 암호 설정 ■ priv: SNMP PDU 를 암호화할 수 있으며 암호화 방법으로 DES 또는 AES 를 설정할 수 있다. <i>priv-passwd</i>: 암호화를 위한 암호 설정 ■ access: 사용자에게 대해 access-list 를 적용한다. <1-99> : IP standard access list 	Config
no snmp-server user <i>username</i> <i>groupname</i> {v1 v2c v3}	SNMP user 를 삭제한다.	Config
show snmp user	SNMP user 를 출력한다.	Privileged
snmp-server view <i>viewname</i> <i>viewoid</i> {excluded included}	SNMP view 를 설정한다. <ul style="list-style-type: none"> ■ <i>viewoid</i>: User 또는 community 로 읽기/쓰 	Config

기 기능을 수행할 수 있는 MIB의 범위를 지정하며 MIB 이름 또는 OID로 지정 가능.

- `excluded` 또는 `included: viewoid`를 포함하거나 제외하도록 설정

```
no snmp-server view viewname viewoid
```

SNMP view를 삭제한다. Config

SNMP engineID 변경

다음 예제는 시스템의 SNMP engine ID를 변경한다. 기존에 SNMPv3 사용자가 설정되어 있었다면 engine ID를 변경한 후 다시 설정해야 네트워크 관리자가 해당 사용자로 접속할 수 있다.

```
Switch# show snmp engineID
Local SNMP engineID: 0x80001f8880236ed0864b7a760f
Switch#configure terminal
Switch(config)# snmp-server engineID 0x1234567890
Switch(config)# exit
Switch#
Switch# show snmp engineID
Local SNMP engineID: 0x1234567890
Switch#
```

SNMPv3 사용자 설정

다음 예제는 인증과 암호화를 수행하는 'testuser' 사용자를 생성한다. 'testuser'는 'testgroup'에 포함되며 ifEntry(1.3.6.1.2.1.2.2.1)를 읽거나 쓸 수 없는 'testview'를 적용한다.

```
Switch# configure terminal
Switch(config)# snmp-server user testuser testgroup v3 auth md5 mysecretpass
priv des myprivpass
Switch(config)# snmp-server group testgroup v3 priv read testview write
testview
Switch(config)# snmp-server view testview 1.3.6.1 included
Switch(config)# snmp-server view testview 1.3.6.1.2.1.2.2.1 excluded
Switch#(config)# end
Switch# show running-config
!
snmp-server group testgroup v3 priv read readview write writeview
snmp-server view testview 1.3.6.1 included
snmp-server view testview 1.3.6.1.2.1.2.2.1 excluded
!
Switch#
Switch# show snmp user

User name : testuser
Engine ID : 0x80001f8880236ed0864b7a760f
storage-type: nonvolatile          active
Authentication Protocol: MD5
Group-name: testgroup
```



Notice SNMPv3의 패스워드 보안 문제로 user 설정은 “show running-config” 명령으로 출력되지 않는다. 위의 예제와 같이 “show snmp user” 명령으로 확인할 수 있다.

2.10. ACL (Access Control List)

액세스 리스트(Access Control List)를 사용함으로써 네트워크 관리자는 인터넷워크를 통해 전송되는 트래픽에 대해 상당히 세밀한 통제를 할 수 있다. 관리자는 패킷의 전송 상태에 대한 기본적인 통계 자료를 얻을 수 있고 이를 통해 보안 정책을 수립할 수 있다. 또한 인증되지 않은 액세스로부터 시스템을 보호할 수 있다. 액세스 리스트는 스위치를 통해 전달되는 패킷을 허용하거나 거부하기 위해 사용할 수도 있고 Telnet(vty)이나 SNMP를 통한 스위치의 접속에도 적용할 수 있다.

액세스 리스트는 표준 IP 액세스 리스트가 있으며, <1-99>의 번호가 할당 될 수 있다.

표 2-23. 액세스 리스트 설정 명령

명령어	설명	모드
access-list <1-99> {deny permit} address	표준 IP 액세스 리스트를 설정 <ul style="list-style-type: none"> ■ Source address/network 만을 설정 ■ address ::= {any A.B.C.D A.B.C.D host A.B.C.D} 	Config
no access-list <1-99>	액세스 리스트를 삭제	Config

2.10.1. 액세스 리스트 생성 규칙

- 좀더 좁은 범위의 것을 먼저 선언한다.
- 빈번히 조건을 만족시킬만한 것을 먼저 선언한다.
- Access-list 의 마지막에 특별히 ‘permit any’ 를 지정하지 않는 한 기본적으로 ‘deny any’ 가 선언되어 있다.
- Access-list 의 조건을 여러 줄에 선언을 하는데 임의의 줄과 줄 사이의 것을 지우거나 수정할 수 없고, 새로 추가하는 필터는 마지막에 더해진다.

2.10.2. 표준 IP 액세스 리스트 설정

2.10.2.1. 모든 액세스 허용

```
Switch# configure terminal
Switch(config)# access-list 1 permit any
```

```
Switch(config)# end
Switch# show running-config
!
access-list 1 permit any
!
```

2.10.2.2. 모든 액세스 거부

```
Switch# configure terminal
Switch(config)# access-list 1 deny any
Switch(config)# end
Switch# show running-config
!
access-list 1 deny any
!
```

2.10.2.3. 특정 호스트에서의 액세스만 허용

```
Switch# configure terminal
Switch(config)# access-list 1 permit host 192.168.0.3
Switch(config)# end
Switch# show running-config
!
access-list 1 permit host 192.168.0.3
!
```

2.10.2.4. 특정 네트워크에서의 액세스만 허용

```
Switch# configure terminal
Switch(config)# access-list 1 permit 192.168.0.0 255.255.255.0
Switch(config)# end
Switch# show running-config
!
access-list 1 permit 192.168.0.0 255.255.255.0
!
```

2.10.2.5. 특정 네트워크에서의 액세스만 거부

```
Switch# configure terminal
Switch(config)# access-list 1 deny 192.168.0.1 255.255.255.0
Switch(config)# access-list 1 permit any
Switch(config)# end
Switch# show running-config
!
```

```
access-list 1 deny 192.168.0.0 255.255.255.0
access-list 1 permit any
!
```

2.10.3. 텔넷 연결에 액세스 리스트 설정

액세스 리스트는 user 별로 적용되며, 설정된 액세스 리스트는 외부에서 스위치로의 접속을 허용, 제한한다.

192.168.0.0/24 네트워크에서의 접속만을 허용하는 Access list 를 생성하여, 텔넷 접속을 제한하고자 할 때의 절차는 다음과 같다.

```
Switch# configure terminal
Switch(config)# access-list 1 permit 192.168.0.0 255.255.255.0
Switch(config)# username admin access-class 1
Switch# show running-config
!
username admin privilege 15 password 0 admin
username admin access-class 1
!
access-list 1 permit 192.168.0.0 255.255.255.0
!
Switch#
```

2.11. NTP 설정

2.11.1. NTP 개요

NTP (Network Time Protocol)는 네트워크를 통하여 시스템의 시간을 동기화하는 데 사용되는 프로토콜이다. NTP 는 UDP (User Datagram Protocol)위에서 동작하며, 모든 NTP 메시지의 시간 정보는 Greenwich Mean Time 과 동일한 Coordinated Universal Time (UTC)를 사용한다.

2.11.2. NTP client mode 설정

NTP client 모드로 동작하도록 하기 위해서는 global 설정 모드에서 다음의 명령을 사용한다.

명령어	설명
ntp server <i>address</i>	NTP server 를 설정한다. (5 개까지 설정가능)
no ntp server <i>address</i>	NTP server 를 삭제한다.

2.11.3. NTP Server mode 설정

NTP server mode 로 동작하도록 하기 위해서는 global 설정 모드에서 다음의 명령을 사용한다.

명령어	설명
ntp master <i>stratum</i>	NTP master 로 동작하도록 한다.
no ntp master	NTP master 로서의 동작을 멈춘다.

2.11.4. NTP time zone 설정

NTP server 나 client 를 지역에 따라 다른 timezone 을 설정하여 해당 지역에서 현재 사용되는 정확한 시간으로 표시한다.

명령어	설명
ntp timezone plus <i>HH:MM</i>	설정된 Coordinated Universal Time (UTC)에 설정된 시간을 더하여 현재 시간을 표시한다.
ntp timezone minus <i>HH:MM</i>	설정된 Coordinated Universal Time (UTC)에 설정된 시간을 빼서 현재 시간을 표시한다.
no ntp timezone	Coordinated Universal Time (UTC)로 설정한다.

2.11.5. NTP summer time 설정

지역에 따라 summer time(daylight savings time)을 사용하는 곳이 있다. 이는 낮 시간이 긴 여름기간 동안 시간을 한시간 당겨 시간을 효율적으로 쓰고자 하기 위한 것이다.

명령어	설명
ntp summer-time <i>week day month hh:mm week day month hh:mm</i>	Summer time 이 시작하는 때와 끝나는 때를 지정하여 적용한다.
no ntp summer-time	Summer time 을 적용하지 않는다.

2.11.6. NTP 기타 명령어

명령어	설명
ntp poll-interval <i>number</i>	NTP client mode 로 동작할 시, 설정된 NTP server 로 NTP request message 를 전송하는 간격, 2 의 배수로 동작하며 <4-17>의 범위를 가진다.
show ntp	NTP 에 대한 사항을 보여준다.

2.11.7. NTP 설정 예제

```

Switch#
Switch (config)# ntp server 203.248.240.103
Switch (config)# ntp master 5
Switch (config)# exit
Switch # show ntp
-----
Current time      : Thu Jan 12 20:40:25 2005
-----
NTP master          : enable
NTP stratum         : 5
Poll interval      : 6 (power of 2)
NTP timezone       : GMT
NTP summertime     : none
NTP summertime start : none
NTP summertime end   : none
-----
The list of NTP Server is below.
-----
[1] 203.248.240.103
-----
Switch #

```

2.12. 배너 설정

E7500 series 스위치는 로그인 배너 및 MOTD 배너를 등록할 수 있다. 로그인 배너는 사용자가 시스템에 접속해서 로그인 하기 전에 출력되는 메시지이며, MOTD 배너는 로그인 한 후 EXEC shell을 실행하기 전에 출력되는 메시지이다. 배너를 통해 사용자에게 주의 사항과 같은 메시지를 전달할 수 있다.

표 2-24. 로그인 배너 및 MOTD 배너 명령어

명령어	설명	모드
banner login <i>banner-string</i>	로그인 배너를 등록한다.	Config
banner login default	<ul style="list-style-type: none"> <i>banner-string</i>: 등록할 로그인 배너 메시지로 시작 문자에 대해 동일한 문자가 나올 때까지 로그인 배너로 지정 default: 기본적으로 등록된 로그인 배너 메시지 	
no banner login	시스템에 등록된 로그인 배너를 삭제한다.	Config
banner motd <i>banner-string</i>	MOTD 배너를 등록한다.	Config
banner motd default	<ul style="list-style-type: none"> <i>banner-string</i>: 등록할 MOTD 배너 메시지로 시작 문자 	

에 대해 동일한 문자가 나올 때까지 MOTD 배너로 지정

- **default:** 기본적으로 등록된 MOTD 배너 메시지

no banner motd

시스템에 등록된 MOTD 배너를 삭제한다.

Config

시스템에는 아래와 같은 로그인 배너와 MOTD 배너가 기본적으로 등록되어 있다.

Ubiquoss L3 Switch

<- 로그인 배너

```
Switch login: root
Password:
```

Hello.

<- MOTD 배너

```
Switch >enable
Switch #
```

다음은 로그인 배너를 변경하는 예제이다. 배너는 여러 줄로 입력이 가능하며 다만 시작 문자에 대해 동일한 종료 문자가 나타날 때까지 배너로 등록된다. 아래 예제에서는 ‘.’ 문자에 대해 시작과 종료 문자로 지정하였고, ‘.’ 문자 사이의 공백을 포함한 문자열을 배너로 등록한다.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# banner login .
Enter TEXT message. End with the character '!'.
```

```
Ubiquoss E7508 Switch
```

```
Login Banner TEST!
```

```
^C
```

```
Switch(config)#
Switch(config)#exit
Switch#show running-config
```

```
...
```

```
!
```

```
banner login ^C
```

```
Ubiquoss E7508 Switch
```

```
Login Banner TEST!
```

```
^C
```

```
!
```

```
...
```



Notice

‘show running-config’ 명령으로 등록된 배너를 확인할 때 시작 문자와 종료 문자는 ‘^C’로 지정된다.

위의 예제에서 설정한 로그인 배너는 아래와 같이 출력된다.

Ubiquoss E7508 Switch

Login Banner TEST!

Switch login: root
Password:

Hello.

Switch >

3

인터페이스 환경 설정

3.1. 개요

E7500 Series 스위치가 지원하는 인터페이스는 다음과 같다.

표 3-1. E7500 Series 스위치가 지원하는 인터페이스

구분	종류
Physical interfaces	<ul style="list-style-type: none"> ■ Gigabit Ethernet <ul style="list-style-type: none"> • 1000Base-T • 1000Base-X ■ 10 Gigabit Ethernet <ul style="list-style-type: none"> • 10000Base-X
port-group interfaces	■ Port-group
VLAN Interfaces	■ VLAN
Loopback interface	■ Loopback
Management interface	■ Out of band interface for management

모든 인터페이스 환경 설정은 다음과 같이 진행된다.

- 4) Privileged 모드에서 “**configure terminal**” 명령으로 Config 모드로 진입한다.
- 5) “**interface**” 명령을 사용하여 interface 모드로 진입한다.
- 6) 특정 인터페이스에 대한 configuration 명령을 사용한다.

3.2. 공통 명령어

인터페이스 환경 설정에 공통으로 적용되는 명령어는 다음과 같다.

표 3-2. 공통 명령어

명령어	설명
interface IFNAME	<ul style="list-style-type: none"> ■ Interface 모드로 진입한다. ■ IFNAME: 환경을 설정할 특정 인터페이스의 이름.

- description string**
 - 인터페이스에 대한 설명을 등록한다.
 - *string*: 80 자 이내의 문자열의 인터페이스 설명
- no description**
 - 등록된 인터페이스 설명을 삭제한다.

3.2.1. Interface name

E7500 Series 스위치에서는 인터페이스에 대한 모든 환경 설정에서 interface name을 사용한다. Interface name은 다음과 같이 interface type과id로 구성된다.

표 3-3. Interface name

구분	Interface type	Interface name	예
Physical interface	Gigabit Ethernet	“Gi” + slot_id + port_id	Gi1/1
	10 Gigabit Ethernet	“Te” + slot_id + port_id	Te1/1
Port-group interface	Port group	“po” + port-group id	po1
VLAN interface	VLAN	“vlan” + vlan id	Vlan10
Loopback interface	Loopback	“lo” + id	Loopback0
Management interface	Fast Ethernet	“eth” + id	eth0

3.2.2. Interface id

Interface name은interface type과id로 구성된다. 다음은 E7500 Series 스위치의 interface name 표기 방법과 지원 범위를 나타낸다.

표 3-4. Interface ID 및 지원 범위

Model	Interface Type	ID 구성	ID Range	Name(예)
E7508	Gigabit Ethernet	mod_id + slot_id + port_id	mod_id: 1-6 slot_id: 1-2 port_id: 1-12	Gi1/1/1
	10 Gigabit Ethernet	mod_id + slot_id + port_id	mod_id: 1-6 slot_id: 1-2 port_id: 1-2	Te1/1/2
	Port group	port-group id	1 – 256	po1, po30
	VLAN	vlan id	1 – 4094	Vlan1
	LoopBack	interface id	0 – 3	Loopback0
	management	interface id	0	eth0

3.2.3. Interface 모드 프롬프트

interface 명령을 사용하여 interface 모드로 진입하면 화면상에는 다음과 같은 프롬프트가 나타난다. Interface 모드에서는 인터페이스의 환경을 설정하고 변경할 수 있다.

```
Switch (config-if-Giga1/1/1) #
```

3.2.4. Description 명령어

운영자의 시스템 운영에 대한 편의를 돕기 위해 각 인터페이스에 대한 설명을 등록할 수 있으며, **show interface description** 명령을 사용하여 조회할 수 있다.

3.3. 인터페이스 정보 및 상태 조회

인터페이스의 환경 설정 정보, 상태 정보 및 통계 데이터를 조회하고자 할 경우 다음 명령어를 사용한다.

표 3-5. 인터페이스 정보 및 상태 관련 명령어

명령어	설명	모드
show interface <i>IFNAME</i>	<ul style="list-style-type: none"> 인터페이스의 설정, 상태 및 통계 정보를 출력한다. 	Privileged
show interface status	<ul style="list-style-type: none"> 물리적 인터페이스의 링크 상태, speed, duplex 정보 등을 출력한다. 	Privileged
show interface transceiver [detail]module <1-6>	<ul style="list-style-type: none"> 물리적 인터페이스의 DDM (Digital Diagnostic Monitoring) 정보를 출력한다. 	Privileged
show idprom all	<ul style="list-style-type: none"> 시스템 FRU 정보를 출력한다. 	Privileged
show idprom <i>fru-type</i>	<ul style="list-style-type: none"> <i>all</i>: 모든 FRU 타입 정보를 출력 	
show idprom interface <i>IFNAME</i>	<ul style="list-style-type: none"> <i>fru-type</i>: FRU 타입 별로 정보를 출력 <i>interface IFNAME</i>: 인터페이스 정보를 출력 	



Notice 'show interface transceiver' 명령의 자세한 내용은 **E7500 Series_User Guide_제 18 장_Utilities** 장의 <18.5. DDM>을 참조하라

3.3.1. show interface 명령어

인터페이스에 대한 모든 정보를 확인할 때 **show interface** 명령을 참조한다. 인터페이스의 환경 설정 정보, 링크 상태, 그리고 인터페이스 관련 통계 정보를 출력할 수 있다.

```
Switch# show interface
```

```
Giga2/1/1 is down, line protocol is down (notconnect)
  Hardware is Ethernet, address is 0007.709a.ab10 (bia 0007.709a.ab10)
  index 1101 metric 1 mtu 1500 arp ageing timeout 7200
  Full-duplex, Auto-speed, media type is No Transceiver
  <UP,BROADCAST,MULTICAST>
  VRF Binding: Not bound
  Bandwidth 1g
  VRRP Master of : VRRP is not configured on this interface.
  inet6 1234::22/64
  inet6 fe80::207:70ff:fe9a:ab10/64
  Last clearing of "show interface" counters never
  60 seconds input rate 0 bits/sec, 0 packets/sec
  60 seconds output rate 0 bits/sec, 0 packets/sec
  L2/L3 in Switched: ucast 0 pkt - mcast 0 pkt
  L2/L3 out Switched: ucast 0 pkt - mcast 0 pkt
    0 packets input, 0 bytes
    Received 0 broadcast pkt (0 multicast pkt)
    0 CRC, 0 oversized, 0 dropped
    0 packets output, 0 bytes
    0 collisions
    0 late collisions, 0 deferred
```

```
-- More --
```

3.3.2. show interface status 명령어

모든 물리적 포트의 링크 상태, vlan 정보, 현재 speed/duplex, 그리고 interface type을 출력한다.

```
Switch# show interface status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Gi2/1/1		notconnect	routed	full	auto	No Transceiver
Gi2/1/2		notconnect	routed	full	auto	No Transceiver
Gi2/1/3		notconnect	routed	full	auto	No Transceiver
Gi2/1/4		notconnect	routed	full	auto	No Transceiver
Gi2/1/5		notconnect	routed	full	auto	No Transceiver
Gi2/1/6		notconnect	678	full	auto	1000BaseLX
Gi2/1/7		notconnect	678	full	auto	1000BaseLX
Gi2/1/8		connected	678	full	a-1000	1000BaseLX
Gi2/1/9		notconnect	routed	full	auto	No Transceiver
Gi2/1/10		notconnect	routed	full	auto	No Transceiver
Gi2/1/11		notconnect	routed	full	auto	No Transceiver
Gi2/1/12		notconnect	routed	full	auto	No Transceiver
Gi2/2/1		notconnect	routed	full	auto	1000BaseLX
Gi2/2/2		notconnect	routed	full	auto	1000BaseLX
Gi2/2/3		notconnect	routed	full	auto	1000BaseLX
Gi2/2/4		notconnect	100	full	auto	1000BaseLX

Gi2/2/5	notconnect	100	full	auto	1000BaseLX
Gi2/2/6	notconnect	routed	full	auto	No Transceiver
Gi2/2/7	notconnect	routed	full	auto	No Transceiver
Gi2/2/8	notconnect	routed	full	auto	No Transceiver
Gi2/2/9	notconnect	routed	full	1000	No Transceiver
Gi2/2/10	notconnect	routed	full	auto	No Transceiver
Gi2/2/11	notconnect	routed	full	auto	No Transceiver
Gi2/2/12	connected	routed	full	a-1000	1000BaseLX

3.3.3. show idprom 명령어

show idprom 명령은 시스템의 FRU(Field Replaceable Unit) 정보를 출력한다. E7500 series 스위치는 아래와 같은 FRU 타입에 대해 정보를 출력할 수 있다.

- Chassis
- FAN
- FMU
- Module
- Pfe
- PMU
- Power
- Slot
- Tranceiver

다음은 **show idprom all** 명령으로 시스템의 모든 FRU 타입에 대한 정보를 출력하는 예제이다.

```
Switch# show idprom all
IDPROM for chassis
  Name = 'UbiQuoss Evolution'
  Description = 'UbiQuoss Chassis System'
  SNMP index = '1'

IDPROM for pfe 1
  Name = 'Physical Module Pfe 1'
  Description = 'UbiQuoss Physical Module Pfe 1'
  SNMP index = '2'

IDPROM for module 2
  Name = 'Physical Module 2'
  Description = 'UbiQuoss Physical Module 2'
  SNMP index = '5'

IDPROM for slot 2/1
  Name = 'Physical Slot 2/1'
  Description = 'UbiQuoss Physical Slot 2/1'
  SNMP index = '12'

IDPROM for slot 2/2
  Name = 'Physical Slot 2/2'
```

Description = 'UbiQuoss Physical Slot 2/2'
SNMP index = '13'

IDPROM for pmu 1

Name = 'Container of Power Module 1'
Description = 'Container of Power Module 1'
SNMP index = '30'

IDPROM for pwr 1

Name = 'Power 1'
Description = 'Power 1'
SNMP index = '31'

IDPROM for pmu 2

Name = 'Container of Power Module 2'
Description = 'Container of Power Module 2'
SNMP index = '40'

IDPROM for pwr 2

Name = 'Power 2'
Description = 'Power 2'
SNMP index = '41'

IDPROM for pmu 3

Name = 'Container of Power Module 3'
Description = 'Container of Power Module 3'
SNMP index = '50'

IDPROM for pwr 3

Name = 'Power 3'
Description = 'Power 3'
SNMP index = '51'

IDPROM for pmu 4

Name = 'Container of Power Module 4'
Description = 'Container of Power Module 4'
SNMP index = '60'

IDPROM for pwr 4

Name = 'Power 4'
Description = 'Power 4'
SNMP index = '61'

IDPROM for fmu 1

Name = 'Container of Fan Module 1'
Description = 'Container of Fan Module 1'
SNMP index = '100'

IDPROM for fan 1/1

Name = 'Fan 1/1'
Description = 'Fan 1/1'
SNMP index = '101'

IDPROM for fan 1/2

Name = 'Fan 1/2'
Description = 'Fan 1/2'
SNMP index = '102'

IDPROM for fan 1/3

Name = 'Fan 1/3'
Description = 'Fan 1/3'
SNMP index = '103'

IDPROM for fan 1/4

Name = 'Fan 1/4'
Description = 'Fan 1/4'
SNMP index = '104'

IDPROM for fan 1/5

Name = 'Fan 1/5'
Description = 'Fan 1/5'
SNMP index = '105'

IDPROM for fan 1/6

Name = 'Fan 1/6'
Description = 'Fan 1/6'
SNMP index = '106'

IDPROM for fmu 2

Name = 'Container of Fan Module 2'
Description = 'Container of Fan Module 2'
SNMP index = '110'

IDPROM for fan 2/1

Name = 'Fan 2/1'
Description = 'Fan 2/1'
SNMP index = '111'

IDPROM for fan 2/2

Name = 'Fan 2/2'
Description = 'Fan 2/2'
SNMP index = '112'

IDPROM for fan 2/3

```

Name = 'Fan 2/3'
Description = 'Fan 2/3'
SNMP index = '113'

IDPROM for fan 2/4
Name = 'Fan 2/4'
Description = 'Fan 2/4'
SNMP index = '114'

IDPROM for fan 2/5
Name = 'Fan 2/5'
Description = 'Fan 2/5'
SNMP index = '115'

IDPROM for fan 2/6
Name = 'Fan 2/6'
Description = 'Fan 2/6'
SNMP index = '116'

IDPROM for tranciever 2/2/2
Name = 'Giga2/1/6'
Description = '1000BASE-LX'
SNMP index = '1290'

IDPROM for tranciever 2/2/2
Name = 'Giga2/1/7'
Description = '1000BASE-LX'
SNMP index = '1300'

.....
생략

```

3.4. 물리적 포트 환경 설정

다음은 물리적 포트의 환경 설정에 사용되는 명령어이다.

표 3-6. 물리적 포트 환경 설정 명령어

명령어	설명	모드
shutdown	■ 물리적 포트를 disable/enable	Interface
no shutdown		
speed {10 100 1000}	■ Speed 설정 (단위: Mbps)	Interface
speed auto		
duplex {full half}	■ Duplex 모드 설정	Interface

flowcontrol (send receive) (on off)	▪ flow-control 설정 및 해제	Interface
flowcontrol both		
no flowcontrol		
carrier-delay <0-60>	▪ Carrier-delay 를 sec 단위와 ms 단위로	Interface
carrier-delay msec <0-1000>	설정	



Notice Gpon interface 노드에서는 해당 명령어들이 표시되지 않는다.

3.4.1. Shutdown

물리적 포트를 disable시킨다.

물리적 포트의 shutdown상태를 확인하려면 **show interface** 명령을 사용한다.

```
Switch # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch (config)# interface GigabitEthernet 2/1/1
Switch (config-if-Giga2/1/1)# shutdown          <- disable port
Switch (config-if-Giga2/1/1)# no shutdown       <- enable port
Switch (config-if-Giga2/1/1)#
```

3.4.2. Speed and duplex

E7500 Series 스위치의 각 인터페이스에서 지원하는 speed는 다음과 같다.

type	speed	duplex
1000Base-T	10/100/1000/auto	full/half
	1000	full
1000Base-X	1000/auto	full
	1000	full
10GBase-R	10000	full

Speed 또는 duplex를 설정할 때 다음 사항을 주의하라.

- 10-Gigabit Ethernet 과 1000Base-X Gigabit Ethernet 은 full duplex 만 지원한다.

3.4.3. Flow control

Gigabit Ethernet, 10-Gigabitethernet interface 에 대해서 IEEE 802.3x Flow control 기능을 지원한다.

Flow control 은 interface 의 receive buffer 가 가득 찼을 경우 IEEE 802.3x pause frame 을 반대편 interface 에 전송해서 일정시간 동안 패킷을 보내지 않도록 하는 것을 말한다.

다음은 interface 에 IEEE 802.3x pause frame 을 보내는 설정과 받아서 처리하는 설정을 보여주는 예시이다.

```
Switch# configure terminal
Switch(config)#
Switch(config)# interface Giga2/1/1
Switch(config-if-Giga2/1/1)# flowcontrol send on
Switch(config-if-Giga2/1/1)# flowcontrol receive on
Switch(config-if-Giga2/1/1)# end
Switch# show flowcontrol
Port      Send FlowControl      Receive FlowControl  RxPause TxPause
         admin   oper                admin   oper
-----
Giga2/1/1 on         on                on      off          307    154
Switch#
```

flowcontrol send on 명령은 IEEE 802.3x pause frame 을 보내도록 설정하는 명령이고 **flowcontrol receive on** 는 IEEE 802.3x pause frame 을 받을 경우 일정시간 동안 패킷을 보내지 않도록 설정하는 명령어다. 이러한 설정을 확인하기 위해서 **show flowcontrol (IFNAME)** 명령을 사용한다. 설정을 해제할 경우에는 **no flowcontrol** 명령을 사용한다.

3.4.4. Carrier delay

Interface 에 link up/down event 가 발생할 경우 carrier delay 설정을 통해서 설정 한 시간 보다 작은 시간 사이에 link 가 up -> down -> up 이 될 경우 down 을 인식하지 않도록 설정 할 수 있다.

```
Switch# configure terminal
Switch(config)#
Switch(config)# interface Giga2/1/1
Switch(config-if-Giga2/1/1)# carrier-delay msec 500
Switch(config-if-Giga2/1/1)# end
Switch#
```

설정을 해지하기 위해서는 **no carrier-delay** 명령을 사용한다.

3.5. Broadcast suppression

Broadcast suppression이란 broadcast storm으로 인한 시스템의 과부하를 방지하기 위하여 브로드캐스트 트래픽이 시스템에 유입되는 것을 제한하는 기능을 말한다. Broadcast storm은broadcast/multicast 패킷이 서브넷에 flooding되어 과다한 트래픽으로 인한 네트워크의 성능을 저하시키는 현상을 말하며 프로토콜 스택 구현상의 오류나 네트워크 환경 설정의 오류가 이런 현상을 유발시킬 수 있다.

{OFFICIAL_PRODUCT_NAME}는input port의 packet을 양을 측정하여 이를 설정된 threshold와 비교 그 이상의 트래픽은 시스템에 유입 시키지 않고 폐기한다.

명령어	설명	모드
storm-control (broadcast multicast unicast)	<ul style="list-style-type: none"> ■ Multicast, broadcast, unicast,packet 을 suppression 	Interface
storm-control level LEVEL no storm-control level	<ul style="list-style-type: none"> ■ broadcast suppression rate 을 설정 	Interface

{OFFICIAL_PRODUCT_NAME}에서는 Broadcast suppression 을 설정하기 위해서 먼저 rate 을 설정해야 한다. 그 후 해당 트래픽에 대한 설정을 한다.

다음은 storm-control 설정에 관한 예시이다.

```
Switch # configure terminal
Switch(config) #
Switch(config) # int GigabitEthernet 2/1/3
Switch(config-if-Giga2/1/3) # storm-control level 50
Switch(config-if-Giga2/1/3) # storm-control broadcast
Switch(config-if-Giga2/1/3) # storm-control multicast
Switch# show interface counters storm-control
Port          TotalLevel % UMB UcastDiscards McastDiscards BcastDiscards
-----
.....
Gi2/1/1       0.00          0          0          0
Gi2/1/2       0.00          0          0          0
Gi2/1/3       50.00        **          0          0
Gi2/1/4       0.00          0          0          0
.....
Switch#
```

설정을 해지할 경우 no storm-control 명령을 사용한다.

3.6. Port mirroring

Port mirroring은 특정 port(source port)의 입출력 트래픽을 운용자가 설정한 목적지 포트에 mirroring하는 기능으로 원하는 포트의 모든 패킷을 감시할 수 있다.

{OFFICIAL_PRODUCT_NAME}는 rx, tx 트래픽을 각각 여러 소스 포트로부터 1개의 port로 mirroring할 수 있다.

명령어	설명	모드
mirror interface IFNAME direction (receive transmit both)	<ul style="list-style-type: none"> ■ mirroring 될 port(source port)와 입출력 패킷을 지정 	Interface
no mirror interface IFNAME direction (receive transmit)	<ul style="list-style-type: none"> ■ mirroring 될 port 를 해지 	Interface

다음은 port mirroring 에 대한 예시이다.

```
Switch# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# int GigabitEthernet 6/1/1
Switch(config-if-Giga6/1/1)# mirror interface gi6/1/2 direction receive
Switch(config-if-Giga6/1/1)# mirror interface gi6/1/3 direction receive
Switch(config-if-Giga6/1/1)# mirror interface gi6/1/4 direction receive
Switch(config-if-Giga6/1/1)# end
Switch# show mirror
Mirror Test Port Name: Giga6/1/1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: Giga6/1/2
Mirror Test Port Name: Giga6/1/1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: Giga6/1/3
Mirror Test Port Name: Giga6/1/1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: Giga6/1/4
Switch#
```



Notice Port mirroring 은 netflow 와 동시에 동작 할 수 없다. Netflow 가 enable 되어있는 경우 config 모드 에서 **no mls netflow** 명령 설정 후에 설정해야 한다.

3.7. 2 계층 인터페이스 환경 설정

2계층 인터페이스는 2계층 스위칭 모드(IEEE 802.3 Bridged VLAN)로 동작하는 인터페이스로서 E7500 Series 스위치에서는 물리적 포트와 port-group 이 2계층 스위칭 모드로 동작한다. 이 절에서는 2계층 인터페이스의 설명과 물리적 포트와 port-group을 2계층 인터페이스로 설정하는 명령어와 그 적용 예를 보여준다.

3.7.1. VLAN Trunking

트렁크(trunk)란 이더넷 스위치와 다른 네트워킹 장비(router, switch) 사이의 point-to-point 링크로서 단일 링크에 복수의 VLAN 트래픽을 전송할 수 있으며 이를 통하여 VLAN을 전체 네트워크에 확장할 수 있다.

E7500 Series 스위치는 모든 이더넷 인터페이스에 802.1Q trunking encapsulation을 지원하며 single ethernet interface 또는 port-trunk interface에 trunk을 설정할 수 있다.

3.7.2. 2 계층 인터페이스 모드

E7500 Series 스위치가 지원하는 2 계층 인터페이스 모드에는 다음과 같이 trunk 모드와 access 모드가 있다.

표 7. E7500 Series 스위치가 지원하는 2 계층 인터페이스 모드

모드	설명
switchport mode access	<ul style="list-style-type: none"> non trunking mode. native vlan 만 설정 가능
switchport mode hybrid	<ul style="list-style-type: none"> 하나의 native vlan 설정과 다수의 tagged, untagged VLAN 설정 가능
switchport mode trunk	<ul style="list-style-type: none"> trunking mode. 하나의 native VLAN 과 다수의 tagged VLAN 설정 가능

3.7.3. 2 계층 인터페이스 기본 설정 값

E7500 Series 스위치는 물리적 포트 또는 port-group이 layer2 interface로 설정될 때 다음과 같은 기본(default) 설정 값을 가진다.

표 3-7. 2 계층 인터페이스 기본 설정 값

항목	설정 값
interface mode	switchport mode access
native vlan	VLAN 1

3.7.4. 2 계층 인터페이스 설정/해제

2 계층 인터페이스로 설정 및 해제하기 위한 명령어는 다음과 같다.

표 3-8. 2 계층 인터페이스 설정 및 해제 명령어

명령어	설명	모드
switchport	Layer2 interface 설정	interface
no switchport	Layer2 interface 해제	interface

인터페이스가 최초로 2 계층 인터페이스로 설정되면 2 계층 인터페이스 기본 설정 값을 가지게 되며 2 계층 인터페이스 설정이 해제되면 VLAN 설정 값은 모두 해제되지만 다시 switchport 명령을 통해 2 계층 인터페이스가 되면 기존의 설정들이 복원된다.



Notice

E7500 Series 스위치의 초기 설정은 모든 물리적 포트가 3 계층 인터페이스로 되어 있다.

3.7.5. Trunk port 설정

물리적 포트 또는 port-group 인터페이스를 2계층 트렁크 포트(layer2 trunk port)로 설정하기 위한 명령어는 다음과 같다.

표 3-9. Trunk port 설정 명령어

명령어	설명	모드
switchport mode trunk	■ trunk mode 설정	Interface
switchport trunk native <1-4094>	■ trunk port native VLAN 설정	Interface
no switchport trunk native	■ trunk port native VLAN 을 default 로 설정	Interface
switchport trunk allowed vlan add <2-4094>	■ trunk port tagged VLAN 등록	Interface
switchport trunk remove <2-4094>	■ trunk port tagged VLAN 삭제	Interface
switchport trunk remove all		

다음은 물리적 포트를 2계층 트렁크 포트로 설정하는 예이다.

```
Switch# configure terminal
Switch(config)# interface gi2/1/1
Switch(config-if-gi2/1/1)# switchport ! layer2 interface set
Switch(config-if-gi2/1/1)# switchport mode trunk ! trunk port set
Switch(config-if-gi2/1/1)# switchport trunk native 2 ! native vlan set
Switch(config-if-gi2/1/1)# switchport trunk add 3 ! tagged vlan 등록
Switch(config-if-gi2/1/1)# switchport trunk add 4
Switch(config-if-gi2/1/1)# end
```

다음은 port-group 인터페이스를 2계층 트렁크 포트로 설정하는 예이다.

```
Switch# configure terminal
Switch(config)# interface po2
Switch(config-if-po2)# switchport ! layer2 interface set
Switch(config-if-po2)# switchport mode trunk ! trunk port set
Switch(config-if-po2)# switchport trunk native 2 ! native VLAN set
Switch(config-if-po2)# switchport trunk add 3 ! tagged vlan 등록
Switch(config-if-po2)# switchport trunk add 4
Switch(config-if-po2)# end
```

3.7.6. Access port 설정

물리적 포트 또는 port-group 인터페이스를 2계층 access port로 설정하기 위한 명령어는 다음과 같다.

표 3-10. Access port 설정 명령어

명령어	설명	모드
switchport mode access	▪ access mode 설정	Interface
switchport access vlan <1-4094>	▪ native vlan 설정	Interface
no switchport access vlan	▪ native vlan 을 default 로 set(VLAN 1)	Interface

다음은 물리적 포트를 2계층 access port로 설정하는 예이다.

```
Switch# configure terminal
Switch(config)# interface gi2/1/1
Switch(config-if-gi2/1/1)# switchport ! layer2 interface set
Switch(config-if-gi2/1/1)# switchport mode access ! access port set
Switch(config-if-gi2/1/1)# switchport access vlan 5 ! native vlan set
```

다음은 port-group 인터페이스를 2계층 access port로 설정하는 예이다.

```
Switch# configure terminal
Switch(config)# interface po2
Switch(config-if-po2)# switchport ! layer2 interface set
Switch(config-if-po2)# switchport mode access ! access port set
Switch(config-if-po2)# switchport access vlan 5 ! native vlan set
```



Notice VLAN 에 설정에 관련된 보다 자세한 설명은 가상랜(VLAN) 매뉴얼을 참조하라.

3.8. Port group

3.8.1. Port group 개요

Port group 이란 여러 물리적 포트를 하나의 logical group으로 묶어서 대역폭을 확장하고 링크 이중화를 확보하기 위해 사용한다. E7500 Series 스위치에서 port group 인터페이스는 2계층 인터페이스로 사용될 수 있다.

E7500 Series 스위치의 모델 별 설정 가능한 port group 수는 다음과 같다.

모델	port group 수	그룹 당 최대 port
E7500 Series	256	8

3.8.2. Port group configuration

Port group 설정을 위한 명령어는 다음과 같다.

표 3-11. 포트 그룹 설정 명령어

명령어	설명	모드
Channel-group <1-256> mode on	<ul style="list-style-type: none"> 해당 interface 를 Port group 에 포함시키고 Port group interface 를 생성한다. 	interface
no port-group ifname	<ul style="list-style-type: none"> port-group 을 삭제한다 	config
port-channel load-balance src-dst-mac	<ul style="list-style-type: none"> load-balance 시 MAC 주소를 참조. 	config
port-channel load-balance src-dst-ip	<ul style="list-style-type: none"> load-balance 시 ip field 를 참조. 	config
port-channel load-balance src-dst-port	<ul style="list-style-type: none"> load-balance 시 tcp/udp port 참조 	config
no channel group	<ul style="list-style-type: none"> 해당 interface 를 Port group 에서 제외시킨다. 	Interface *
no interface Channel-group <1-256>	<ul style="list-style-type: none"> 해당 Port group interface 를 삭제한다. Port group 에 멤버가 없을 경우 수행된다. 	config
show etherchannel	<ul style="list-style-type: none"> port group 설정 출력 	Privileged



Notice Port group 에 설정에 관련된 보다 자세한 설명은 LACP 매뉴얼을 참조하라.

4

가상 랜(VLAN)

가상 LAN(이하 VLAN)은 네트워크 사용자와 리소스를 논리적으로 그룹화한 것이다. 이들 사용자와 리소스는 스위치의 포트에 연결되어 있다. VLAN 을 구축함으로써 많은 시간을 소모하는 네트워크 관리 작업이 용이해지며 브로드캐스트 트래픽을 제어함으로써 네트워크의 효율도 증가한다.

이 장에서는 다음의 내용들을 다룬다:

- VLAN 개관
- VLAN 의 유형
- VLAN 설정
- VLAN 설정 정보 보기(Displaying VLAN Settings)

4.1. VLAN 개관

물리적으로 동일 LAN 상에 위치하여 통신하는 것처럼 보이는 장치들의 그룹을 “가상 LAN(VLAN)”이란 용어로 표현한다. VLAN 은 어떤 기능, 조직 혹은 응용에 의해 논리적으로 구분되어 다른 VLAN 으로 트래픽이 흘러가는 것을 방지하고, 같은 VLAN 의 장비에게로만 트래픽을 송신하여 네트워크의 성능을 향상시키는 브로드캐스트 도메인이다. 즉 VLAN 을 사용하면 VLAN 세그먼트(segment)가 하드웨어의 물리적인 연결에 의해 구분되지 않고, 관리자가 만든 논리적인 그룹에 의해 유연하게 구분되어진

다.

VLAN 정의

VLAN은 물리적 연결 혹은 지역적인 위치에 따른 구분보다는 기능, 프로젝트 그룹, 응용 등과 같은 조직적인 기준에 의해 논리적으로 구분된 스위칭 네트워크이다. 예를 들어 특정 작업그룹에 의해 사용되는 모든 워크스테이션과 서버는 그들의 물리적인 네트워크 연결과 상관없이 같은 VLAN으로 연결될 수 있다. 장비와 케이블의 이동이나 재배치 없이 소프트웨어 설정을 통해 네트워크를 재설정하는 것이 가능하다.

VLAN을 스위치의 집합으로 정의된 브로드캐스트 도메인으로 생각할 수 있다. VLAN은 하나의 브리지 도메인으로 연결되는 다수의 종단 시스템(호스트 혹은 브리지와 라우터 같은 네트워크 장비)으로 구성된다. VLAN은 전통적인 LAN 구성에서 라우터에 의해 제공되는 분할(segmentation) 서비스를 제공하기 위해 사용된다. VLAN은 확장성, 보안, 네트워크 관리 기능을 제공한다. VLAN형상에서 라우터는 브로드캐스트 필터링, 보안, 주소 축약, 그리고 트래픽 흐름 제어를 제공한다. 정의된 그룹내의 스위치는 두 VLAN 사이에서 브로드캐스트 프레임뿐 아니라 어떠한 프레임도 전달하지 않는다.

VLAN의 장점

VLAN을 사용하면 다음과 같은 장점이 있다:

■ 트래픽 제어

전통적인 네트워크에서는 각 장비의 데이터 수신 여부와 상관없이 모든 네트워크 장비로 전송되는 브로드캐스트 트래픽 때문에 혼잡을 발생시킨다. VLAN내의 모든 장치는 같은 브로드캐스트 도메인에 속해 있는 구성원이며 모든 브로드캐스트 패킷을 수신한다. 반면 다른 VLAN에 속하는 스위치의 포트로는 브로드캐스트 트래픽이 전송되지 않는다. 따라서 VLAN을 사용하면 브로드캐스트 트래픽이 인접 네트워크로 퍼져나가는 것을 방지하고 네트워크의 효율을 증가시킬 수 있다.

■ 네트워크 보안 강화

전통적인 네트워크에서는 네트워크에 접근하는 누구라도 네트워크 리소스에 접근할 수 있다. 또한, 사용자가 허브를 통하여 네트워크 분석기를 접속하게 되면 네트워크의 모든 흐름을 볼 수 있게 된다. 하지만 VLAN을 사용하면 VLAN에 포함된 장비들은 오직 같은 VLAN의 구성원들과 통신할 수 있으며, 스위치 포트에 컴퓨터를 접속하는 것으로는 더 이상 모든 네트워크 리소스에 접근할 수 없다. 만약 VLAN A에 속한 장비가 다른 VLAN B의 장비와 통신해야 한다면, 트래픽은 반드시 라우팅 장비를 거쳐야 한다.

■ 유연한 네트워크 관리

전통적인 네트워크에서 네트워크 관리자는 장비의 이동과 변경에 많은 시간을 소비했다. 만약 장비가 다른 서브 네트워크로 옮겨간다면, 각 종단장치의 IP 주소를 수동으로 변경해야 한다. 시스템 운영자는 VLAN을 통하여 논리적인 네트워크 구성함으로써 이러한 문제점을 해결할 수 있다.

4.2. VLAN 의 유형

Premier 8700 Series 스위치는 최대 4094 개의 VLAN 을 지원한다. VLAN 은 다음의 기준에 따라 생성 된다:

- 물리적 포트(Physical port)
- 802.1Q 태그(tag)
- 포트기반 VLAN 과 tag 기반 VLAN 의 결합 (Hybrid)

4.2.1. 포트 기반 VLAN(Port-Based VLANs)

포트 기반 VLAN 에서는 스위치의 하나 또는 그 이상의 포트 그룹에 VLAN 이름이 할당된다. 포트 기반 VLAN 에 할당된 스위치 포트를 access 포트라 부른다. 하나의 access 포트는 오직 하나의 포트 기반 VLAN 에만 속한다. 기본적으로 모든 포트는 VLAN 1(default VLAN)의 access 포트에 할당된다.

예를 들면, <그림 4-1>의 E7500 series 에서 1/7, 1/8 포트는 VLAN A 의 access 포트이고 2/1, 2/2, 2/7,2/8 포트는 VLAN B 의 access 포트에 할당된다. 그리고 1/5, 1/6, 1/9, 1/10, 2/5, 2/6, 2/9, 2/10 포트는 VLAN C 의 access 포트에 정의한다.

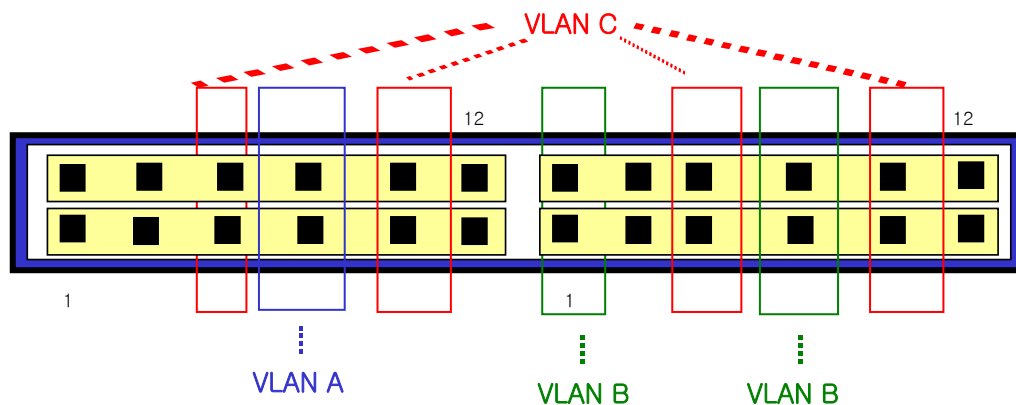


그림 4-1. E 7500 Series 스위치의 포트 기반 VLAN 구성 예

서로 다른 VLAN 의 구성원들이 통신하기 위해서는, 비록 그들이 물리적으로 같은 I/O 모듈의 일부분이더라도 프레임은 스위치에 의해 라우팅 되어야 한다. 이것은 각각의 VLAN 이 유일한 IP 주소를 가진 라우터 인터페이스로 설정되어야 함을 의미한다.

포트 기반 VLAN 으로 스위치 묶기

포트 기반 VLAN 으로 두 스위치를 묶으려면, 다음의 작업을 해야 한다.

- 7) 각 스위치에서 VLAN 에 대한 access 포트를 할당한다.
- 8) 각 스위치에서 VLAN 에 할당된 access 포트 중 하나씩을 사용하여 두 스위치를 케이블로 연결한다. 여러 개의 VLAN 을 연결하려면, 각각의 VLAN 마다 케이블로 스위치를 연결해야 한다.

<그림 2>는 서로 다른 2 개의 E7500 SERIES 를 하나의 VLAN 으로 묶는 방법을 보여준다. 먼저 스위치 1 의 4 개의 포트는 VLAN A 로 포함되도록 할당되어 있다. 또한 스위치 2 의 4 개 포트도 VLAN A 의 access 포트로 할당되어 있다. 두 스위치는 <그림 2>와 같이 상호 연결하여 하나의 브로드캐스트 도메인을 형성한다.

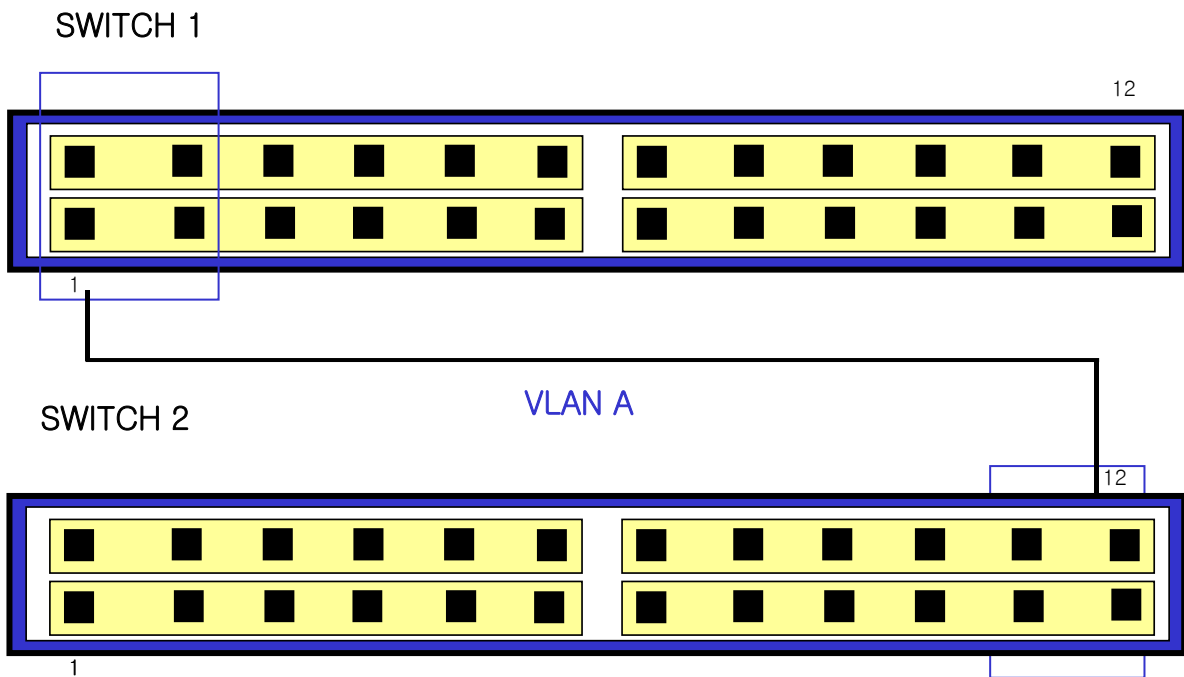


그림 4-2. 두 스위치에 걸쳐서 설정된 단일 포트 기반 VLAN

두 개의 스위치에 걸쳐서 설정되는 다수의 포트 기반 VLAN 을 생성하려면, 각각의 VLAN 에 대해서 스위치 1 의 포트와 스위치 2 의 포트가 반드시 케이블로 연결되어야 한다. 그리고 각 스위치에서 적어도 하나의 포트는 각 VLAN 의 access 포트로 할당되어 있어야 한다.

<그림 4-3>은 두 개의 E7500 SERIES 에 걸쳐서 설정되는 두 개의 VLAN 을 보여준다. 스위치 1 에서 포트 1/1, 1/2, 1/3, 1/4 포트는 VLAN A 의 access 포트이고 2/1, 2/2, 2/3, 2/4 까지의 포트는 VLAN B 의 access 포트로 할당되어 있다.

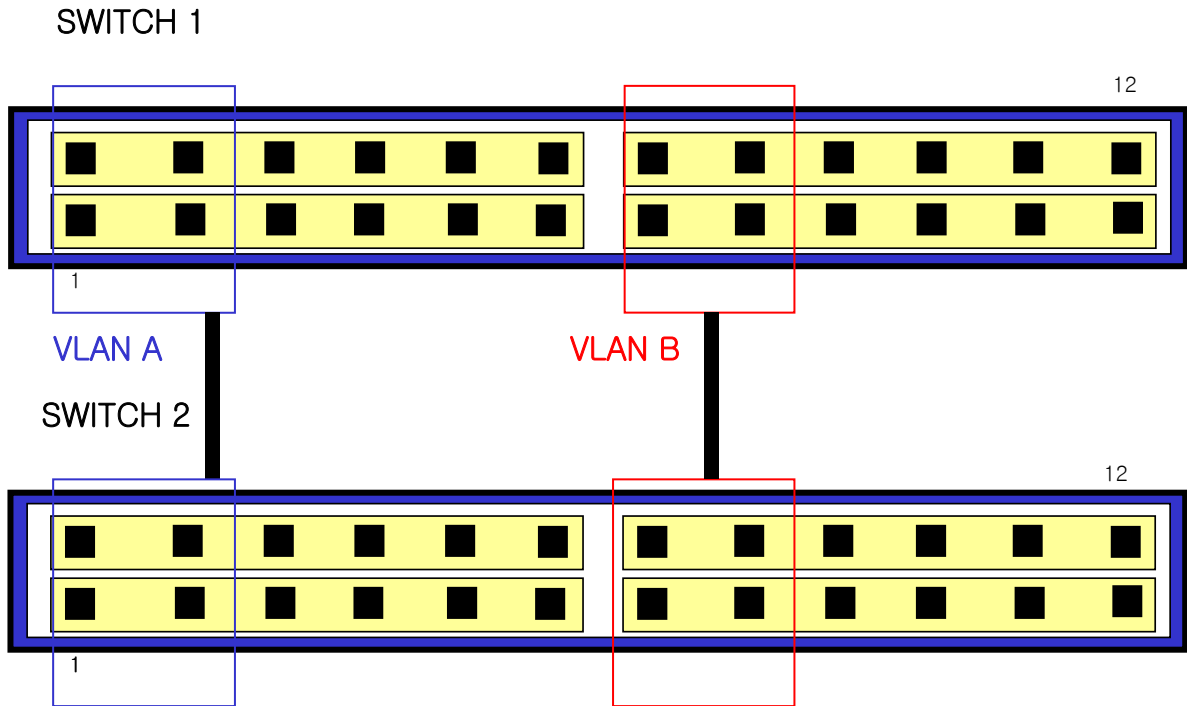


그림 4-3. 두 스위치에 걸쳐서 설정된 두 개의 포트 기반 VLAN

VLAN A는 스위치 1의 포트 13과 스위치 2의 포트 1의 연결을 통해 스위치 1과 스위치 2를 묶는다. VLAN B는 스위치 1의 포트 20과 스위치 2의 포트 11 사이를 연결하여 스위치 1과 스위치 2를 묶는다.

이런 설정 방법을 사용하면, 여러 개의 스위치를 데이지 체인(daisy-chain)으로 연결하는 다중 VLAN을 생성할 수 있다. 각 스위치는 각각의 VLAN의 연결을 위한 전용 access 포트를 가지며, 전용 access 포트는 다음 스위치에서 VLAN의 access 포트와 연결된다.

4.2.2. 태그 VLAN(Tagged VLANs)

태깅(tagging)은 Ethernet 프레임에 태그(tag)라는 표지(marker)를 삽입하는 작업이다. 태그에는 각각의 VLAN을 식별하기 위한 VLANid가 포함된다.



Notice

802.1Q 태그 프레임을 사용하면 IEEE 802.3/Ethernet 프레임의 최대 크기인 1,518 바이트보다 약간 큰 프레임을 발생시킬 수 있다. 이것은 802.1Q를 지원하지 않는 다른 장비의 프레임 에러 카운터에 영향을 줄 수 있으며, 또한 경로상에 802.1Q를 지원하지 않는 브리지와 라우터가 존재한다면 네트워크 연결 문제를 야기할 수 있다.

태그 VLAN의 사용(Uses of Tagged VLANs)

태그는 여러 스위치를 묶는 VLAN을 생성하기 위해 가장 일반적으로 사용되는 방법이다. 태그를 사용

하면, 여러 개의 VLAN 이 하나 이상의 트렁크를 사용하여 프레임을 송수신할 수 있다.

<그림 4-3>에서 설명한 것처럼 포트 기반 VLAN 에서는 각 VLAN 별로 하나의 포트를 할당하여 두 스위치를 연결해야 한다. 하지만 태그 VLAN 을 사용하면 하나의 트렁크만을 사용하여 두 스위치를 묶는 여러 개의 VLAN 을 생성할 수 있다.

태그 VLAN 의 또 다른 장점은 하나의 포트가 여러 VLAN 의 멤버가 될 수 있다는 점이다. 태그 VLAN 은 서버처럼 다수의 VLAN 에 속하는 장비를 사용하는 경우에 특히 유용하다. 이 경우 장비는 반드시 IEEE 802.1Q 태그를 지원하는 네트워크 인터페이스 카드(NIC)을 장착해야 한다.

VLAN 태그의 할당(Assigning a VLAN Tag)

각 VLAN 은 생성할 때 VLANid 를 할당 받는다. 포트가 태그 VLAN 의 트렁크 포트로 할당되어 사용될 때, 포트는 802.1Q VLAN 태그가 붙은 프레임을 사용한다. 이 경우 태그 VLAN 의 VLANid 가 프레임의 태그로 사용된다.

VLAN 의 모든 포트에 반드시 태그가 붙는 것은 아니다. 포트로 수신된 프레임이 스위치 외부로 전달(forward)될 때, 스위치는 프레임에 대한 각 목적지 포트가 태그가 붙은 프레임을 사용하는지 혹은 태그가 붙지 않은 프레임을 사용하는지를 결정한다. 스위치는 VLAN 에 대한 포트 설정에 따라 프레임에 태그를 추가하거나 삭제한다.



Notice

VLAN 이 설정되지 않은 포트로 그 VLAN 의 태그 프레임이 수신되면, 프레임은 폐기된다. 예를 들어 VLANid 가 10, 20 의 멤버인 포트로 VLANid 가 30 인 프레임이 수신된다면 스위치는 그 프레임을 버린다.

<그림 4-4>는 태그가 붙은 프레임과 태그가 붙지 않은 프레임을 사용하는 네트워크의 물리적인 구성을 보여준다.

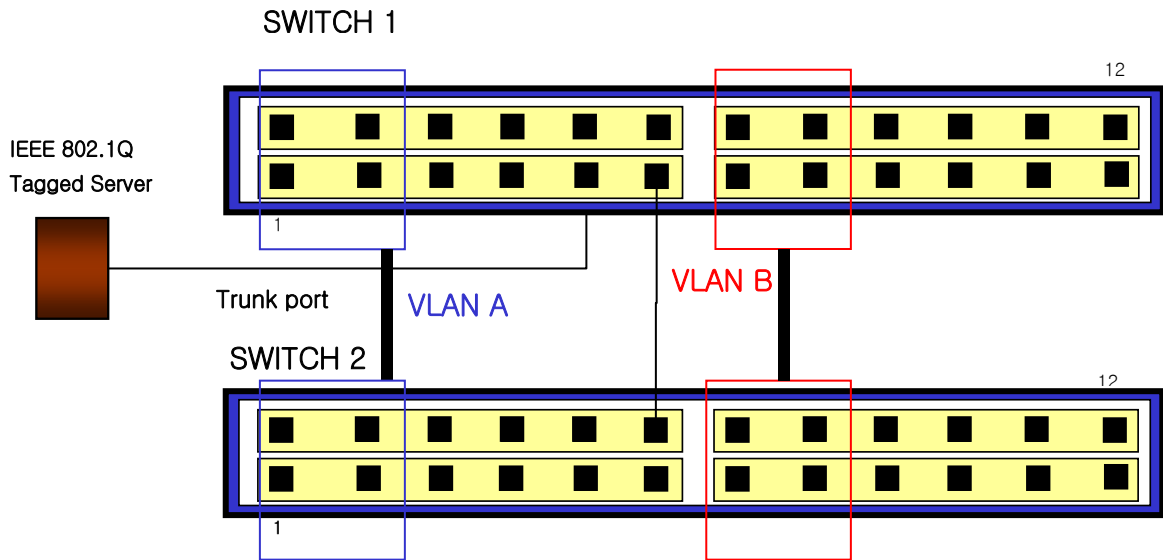


그림 4-4. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 물리적 다이어그램

<그림 4-5>는 동일한 네트워크의 논리적인 다이어그램을 보여준다.

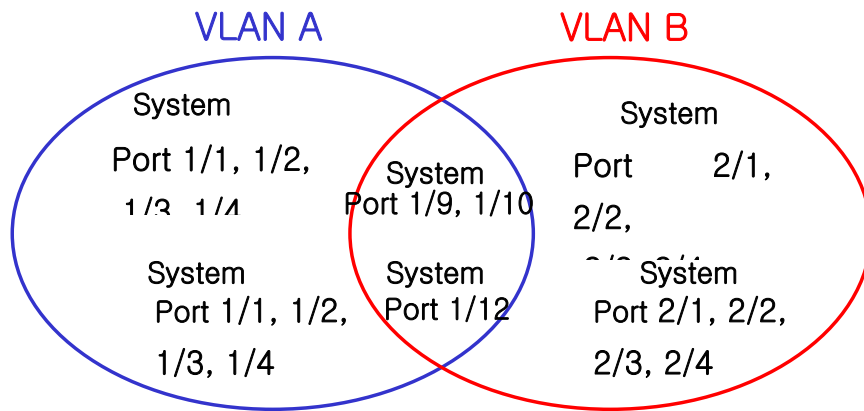


그림 4-5. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 논리적 다이어그램

<그림 4-4>와 <그림 4-5>에서:

- 각 스위치의 트렁크 포트(Tagged ports)는 VLAN A 와 VLAN B 의 트래픽을 전송한다.
- 각 스위치의 트렁크 포트는 태그가 붙은 프레임을 전송한다.
- 시스템 1 의 포트 17 와 연결된 서버는 802.1Q 태그를 지원하는 네트워크 인터페이스 카드를 장착하고 있으며 VLAN A 와 VLAN B 의 멤버이다.
- 다른 단말들은 태그가 붙지 않은 프레임을 송수신한다.

프레임이 스위치를 지나갈 때, 스위치는 목적지 포트에 대해 태그가 붙은 프레임을 사용할지 태그가 붙지 않은 프레임을 사용할지를 결정한다. 서버로부터 송수신되는 모든 프레임과 트렁크 포트에 송수신되는 프레임에는 태그가 붙는다. 하지만 네트워크의 다른 장치로 송수신되는 프레임에는 태그가 붙지 않는다.

4.2.3. 포트 기반 VLAN 과 태그 VLAN 의 혼합 (Hybrid)

Hybrid 유형의 VLAN 은 포트 기반의 VLAN 과 태그 VLAN 의 기능을 혼합한 형태이다. Hybrid VLAN 은 포트 기반의 VLAN 과 같이 해당 포트에 들어오는 프레임의 VLAN id 를 결정하고 태그 VLAN 과 같이 태그를 붙여서 송신하거나 태그를 붙이지 않고 송신 하는 것을 결정 할 수 있다.

4.3. VLAN 구성

4.3.1. VLAN ID

VLAN 을 식별하기 위한 VLAN id 의 값으로 1 부터 4,094 사이의 숫자를 사용할 수 있다. 스위치가 초기화되었을 때 기본적으로 하나의 VLAN 이 생성되어져 있으며(*default VLAN*), 이 VLAN 이 VLAN id 의 값으로 1 을 사용한다. 따라서 새로 만들어지는 VLAN 은 VLAN id 의 값으로 1 을 사용할 수 없다.

VLAN id 는 태그 VLAN 의 멤버인 포트가 트렁크 모드에서 동작할 때 프레임에 붙이는 태그로 사용된다. VLAN id 를 잘못 설정했을 경우에 원하지 않는 VLAN 으로 프레임 송신이 발생할 수 있으므로, 전체 네트워크 구성을 잘 고려하여 VLAN id 를 결정해야 한다.

4.3.2. Default VLAN

스위치에는 다음과 같은 특성을 가지는 *default VLAN* 이 설정되어 있다.

- Default VLAN 은 VLANid 값으로 1 을 사용한다.
- 스위치 초기 상태에서 모든 포트는 *native VLAN* 으로 *default VLAN* 이 설정되어 있다.

4.3.3. Native VLAN

각 물리적 포트는 PVID(Port VLAN ID)를 가지고 있다. 모든 802.1Q 포트에는 자신의 *native VLAN ID* 가 PVID 의 값으로 할당된다. 태그가 붙지 않은 모든 프레임은 PVID 값이 나타내는 VLAN 으로 송신된다. 포트에 태그가 붙은 프레임을 수신했을 경우에는 프레임의 태그를 그대로 사용한다. 하지만 태그가 붙지 않은 프레임이 수신된다면, 프레임에 포함된 PVID 값을 태그로 간주한다.

<그림 6>처럼 태그가 붙지 않은 프레임과 PVID 가 붙은 프레임이 공존하는 것이 허용되므로, VLAN

을 지원하는 브리지나 end station 과 VLAN 을 지원하지 못하는 브리지나 end station 들이 케이블로 연결될 수 있다.

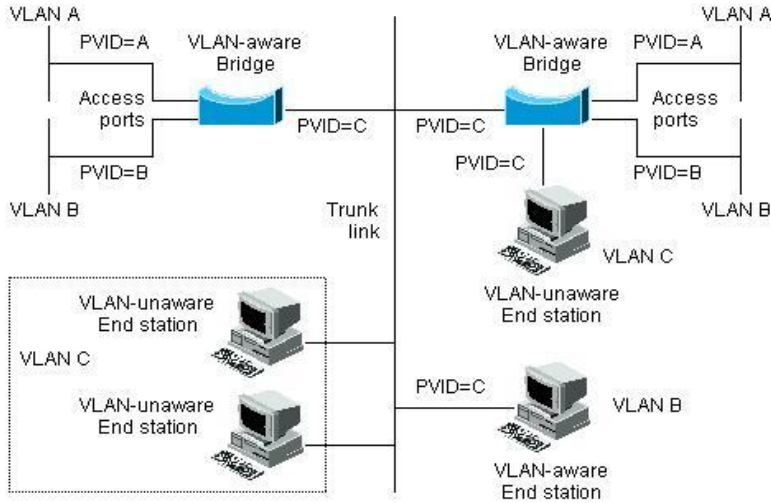


그림 4-6. Native VLAN

예를 들어 <그림 6>의 하단 부분에서처럼 두 end station 이 중앙의 트렁크 링크에 연결된 상태를 생각해 보자. 그들은 VLAN 을 인식하지 못하지만, VLAN 을 인식하는 브리지의 PVID 가 VLAN C 와 동일하게 하므로 VLAN C 에 포함될 것이다. VLAN 을 인식하지 못하는 end station 은 태그가 붙지 않은 프레임만 송신하므로, VLAN 을 인식하는 브리지 장비가 이러한 태그가 붙지 않은 프레임을 수신했을 경우, 이를 VLAN C 로 송신한다.

4.4. VLAN 설정

본 절에서는 E7500 SERIES 에 VLAN 을 설정에 사용되는 명령들을 설명한다. VLAN 설정은 다음의 단계로 진행된다.

- 1) 생성된 VLAN 과 관련된 값을 설정한다.
- 2) 포트가 할당될 VLAN 의 종류에 따라 포트의 모드를 설정한다.
- 3) VLAN 에 하나 이상의 포트를 할당한다. VLAN 에 포트를 추가할 때, 802.1Q 태그의 사용 여부를 결정한다.

4.4.1. VLAN 설정 명령

<표 4-1>은 VLAN 설정에 사용되는 명령들을 설명한다.

표 4-1. VLAN 설정 명령어

명령어	설명	모드
<code>vlan database</code>	<ul style="list-style-type: none"> VLAN database 모드로 진입. 	config
<code>vlan <i>vlanid</i></code>	<ul style="list-style-type: none"> Vlanid 에 해당하는 vlan 을 생성 1 은 default VLAN 의 값으로 사용 <i>vlanid</i> : 2 부터 4094 사이의 값을 사용한다 	vlan database
<code>vlan <i>vlanid</i> name WORD (state (enable disable))</code>	<ul style="list-style-type: none"> Vlanid 에 해당하는 vlan 을 생성 WORD 에 해당하는 vlan ascii 값을 설정 vlan 의 상태를 enable disable 할 수 있다. 	vlan database
<code>vlan <i>vlanid</i> bridge <1-256> name WORD (state (enable disable))</code>	<ul style="list-style-type: none"> Vlanid 에 해당하는 vlan 을 생성 WORD 에 해당하는 vlan ascii 값을 설정 생성하는 vlan 을 bridge 에 만든다. vlan 의 상태를 enable disable 할 수 있다. 	
<code>switchport</code>	<ul style="list-style-type: none"> 포트의 type 을 L2 로 변경한다. L2 포트로 변경되면 default 로 access 모드에 VLAN 1 의 멤버가 된다. 	Interface
<code>switchport mode {access hybrid trunk}</code>	<ul style="list-style-type: none"> 포트의 VLAN 타입을 설정한다. access – 포트를 access 모드(포트 기반 VLAN)로 설정한다. 설정된 포트는 태그가 붙지 않은 프레임을 송수신하는 단일 VLAN 의 인터페이스로 동작한다. Hybrid – 포트를 hybrid 로 설정한다. trunk – 포트를 트렁크(태그 VLAN)로 설정한다. 설정된 포트는 태그가 붙은 프레임을 송수신한다. 태그가 붙지 않은 프레임의 경우 native VLAN id 로 인식한다. 	Interface
<code>switchport access vlan <i>vlanid</i></code>	<ul style="list-style-type: none"> 포트를 VLAN 의 access 포트로 설정한다. 모드가 access 로 설정되면, 설정된 포트는 VLAN 의 멤버 포트로 동작한다. <i>vlanid</i> : 2 부터 4094 사이의 값을 사용한다. 	Interface
<code>Switchport hybrid vlan <i>vlanid</i></code>	<ul style="list-style-type: none"> 설정된 포트는 VLAN 의 멤버 포트로 동작한다. 수신되는 프레임이 untagged 일 경우 vlan id 에 해당하는 프레임으로 인식하도록 설정한다. <i>vlanid</i> : 2 부터 4094 사이의 값을 사용한다. 	Interface

명령어	설명	모드
switchport trunk allowed vlan (add all except) vlanid	<ul style="list-style-type: none"> 포트를 VLAN의 트렁크 포트로 설정한다. 특정 VLAN을 트렁크 포트로 설정하려면 add, 설정된 VLAN을 모두 설정하려면 all, 특정 vlan만 제외하려면 except 명령을 사용한다. vlanid : 2부터 4094 사이의 값을 사용한다. 	Interface
switchport trunk native vlanid	<ul style="list-style-type: none"> 포트가 802.1Q 트렁크 모드, 즉 태그 VLAN의 트렁크 포트일 때, 태그가 붙지 않고 송수신되는 트래픽을 위한 native VLAN을 설정한다. native VLAN을 설정하지 않으면 default VLAN(VLANid = 1)이 native VLAN으로 설정 vlanid : 2부터 4094 사이의 값을 사용한다. 	Interface
switchport trunk (remove none) vlanid	<ul style="list-style-type: none"> 포트를 명시한 VLAN의 멤버에서 제외시킨다. vlanid : 2부터 4094 사이의 값을 사용한다. none: 모든 VLAN으로부터 멤버에서 제외 	Interface

4.5. VLAN 설정 예제

다음의 예제에서는 VLANid가 1000을 생성하고, VLAN에 IP 주소 132.15.121.1을 할당하고, 두 포트를 VLAN에 할당한다.

```
shu#
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#vlan database
shu(config-vlan)#vlan 1000
shu(config-vlan)#exit
shu(config)#interface Vlan 1000
shu(config-if-Vlan1000)#ip address 132.15.121.1/24
shu(config-if-Vlan1000)#interface GigabitEthernet 6/1/2
shu(config-if-Giga6/1/2)#switchport
shu(config-if-Giga6/1/2)#switchport mode access
shu(config-if-Giga6/1/2)#switchport access vlan 1000
shu(config-if-Giga6/1/2)#interface GigabitEthernet 6/1/3
shu(config-if-Giga6/1/3)#switchport
shu(config-if-Giga6/1/3)#switchport mode access
shu(config-if-Giga6/1/3)#switchport access vlan 1000
shu(config-if-Giga6/1/3)#end
shu#show vlan
```

VLAN Name	Status	Ports
1 default	active	Gi6/1/1

```

2    VLAN0002                active
3    VLAN0003                active
4    VLAN0004                active
5    VLAN0005                active
6    VLAN0006                active
7    VLAN0007                active
8    VLAN0008                active
9    VLAN0009                active
10   VLAN0010                active
11   VLAN0011                active
12   VLAN0012                active
100  VLAN0100                active
1000 VLAN1000                active      Gi6/1/2  Gi6/1/3

...

shu#

```

다음의 예제에서는 태그 기반 Vlanid 로 2000 을 할당하고, 두 포트를 트렁크 포트로 VLAN 에 추가한다.

```

shu#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
shu(config)#vlan database
shu(config-vlan)#vlan 2000
shu(config-vlan)#exit
shu(config)#interface GigabitEthernet 6/1/4
shu(config-if-Giga6/1/4)#switchport
shu(config-if-Giga6/1/4)#switchport mode trunk
shu(config-if-Giga6/1/4)#switchport trunk allowed vlan add 2000
shu(config-if-Giga6/1/4)#interface GigabitEthernet 6/1/5
shu(config-if-Giga6/1/5)#switchport
shu(config-if-Giga6/1/5)#switchport mode trunk
shu(config-if-Giga6/1/5)#switchport trunk allowed vlan add 2000
shu(config-if-Giga6/1/5)#end
shu#show vlan all

```

Bridge	VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
-	-	-	-	-
0	1	default	ACTIVE	Gi6/1/1 (u) Gi6/1/4 (u) Gi6/1/5 (u)
0	2	VLAN0002	ACTIVE	
0	3	VLAN0003	ACTIVE	
0	4	VLAN0004	ACTIVE	
0	5	VLAN0005	ACTIVE	
0	6	VLAN0006	ACTIVE	
0	7	VLAN0007	ACTIVE	
0	8	VLAN0008	ACTIVE	
0	9	VLAN0009	ACTIVE	

0	10	VLAN0010	ACTIVE	
0	11	VLAN0011	ACTIVE	
0	12	VLAN0012	ACTIVE	
0	100	VLAN0100	ACTIVE	
0	1000	VLAN1000	ACTIVE	Gi6/1/2 (u) Gi6/1/3 (u)
0	2000	VLAN2000	ACTIVE	Gi6/1/4 (t) Gi6/1/5 (t)

shu#

다음의 예제에서는 Vlanid 로 3000, 4000 을 할당하고, 두 포트를 hybrid 포트로 3000 에 추가하고 4000 에 태그포트로 추가한다.

```
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#vlan database
shu(config-vlan)#vlan 3000
shu(config-vlan)#vlan 4000
shu(config-vlan)#exit
shu(config)#interface GigabitEthernet 6/1/6
shu(config-if-Giga6/1/6)#switchport
shu(config-if-Giga6/1/6)#switchport mode hybrid
shu(config-if-Giga6/1/6)#switchport hybrid vlan 3000
shu(config-if-Giga6/1/6)#switchport hybrid allowed vlan add 4000 egress-tagged
enable
shu(config-if-Giga6/1/6)#interface GigabitEthernet 6/1/7
shu(config-if-Giga6/1/7)#switchport
shu(config-if-Giga6/1/7)#switchport mode hybrid
shu(config-if-Giga6/1/7)#switchport hybrid vlan 3000
shu(config-if-Giga6/1/7)#switchport hybrid allowed vlan add 4000 egress-tagged
enable
shu(config-if-Giga6/1/7)#end
shu#show vlan all
```

Bridge	VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
-				
0	1	default	ACTIVE	Gi6/1/1 (u) Gi6/1/4 (u) Gi6/1/5 (u)
0	2	VLAN0002	ACTIVE	
0	3	VLAN0003	ACTIVE	
0	6	VLAN0006	ACTIVE	
0	7	VLAN0007	ACTIVE	
0	8	VLAN0008	ACTIVE	
0	9	VLAN0009	ACTIVE	
0	10	VLAN0010	ACTIVE	
0	11	VLAN0011	ACTIVE	
0	12	VLAN0012	ACTIVE	
0	100	VLAN0100	ACTIVE	
0	1000	VLAN1000	ACTIVE	Gi6/1/2 (u) Gi6/1/3 (u)
0	2000	VLAN2000	ACTIVE	Gi6/1/4 (t) Gi6/1/5 (t)
0	3000	VLAN3000	ACTIVE	Gi6/1/6 (u) Gi6/1/7 (u)
0	4000	VLAN4000	ACTIVE	Gi6/1/6 (t) Gi6/1/7 (t)

```
shu#
```

다음 예제는 VLANid 가 120 인 sales 란 VLAN 을 생성한다. VLAN 은 태그가 붙은 포트(트렁크 포트)와 태그가 붙지 않은 포트(access 포트)를 모두 포함한다. 포트 1 과 포트 2 에는 태그가 붙고, 포트 3 과 포트 4 에는 태그가 붙지 않는다. 명시적으로 설정하지 않는다면 포트에는 태그가 붙지 않는다.

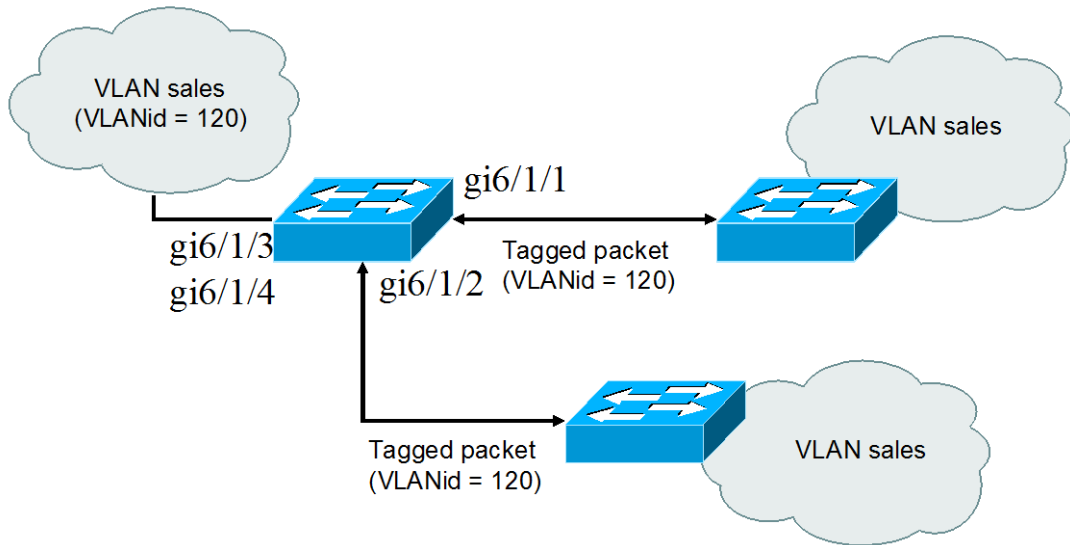


그림 4-7. VLAN 설정 예제 – Tagged and Untagged VLAN

```

shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#vlan database
shu(config-vlan)#vlan 120
shu(config-vlan)#exit
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#switchport
shu(config-if-Giga6/1/1)#switchport mode trunk
shu(config-if-Giga6/1/1)#switchport trunk allowed vlan add 120
shu(config-if-Giga6/1/1)#interface GigabitEthernet 6/1/2
shu(config-if-Giga6/1/2)#switchport
shu(config-if-Giga6/1/2)#switchport mode trunk
shu(config-if-Giga6/1/2)#switchport trunk allowed vlan add 120
shu(config-if-Giga6/1/2)#interface GigabitEthernet 6/1/3
shu(config-if-Giga6/1/3)#switchport
shu(config-if-Giga6/1/3)#switchport access vlan 120
shu(config-if-Giga6/1/3)#interface GigabitEthernet 6/1/4
shu(config-if-Giga6/1/4)#switchport
shu(config-if-Giga6/1/4)#switchport access vlan 120
shu(config-if-Giga6/1/4)#end
shu#show vlan all

```

Bridge	VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
0	1	default	ACTIVE	Gi6/1/1 (u) Gi6/1/2 (u) Gi6/1/5 (u)
0	120	VLAN0120	ACTIVE	Gi6/1/1 (t) Gi6/1/2 (t) Gi6/1/3 (u) Gi6/1/4 (u)

```

shu#

```

다음은 스위치의 포트 1 을 포트 기반 VLAN *Marketing* 과 태그 VLAN *Engineering* 의 멤버로 설정하는 예제이다. VLAN *Marketing* 의 VLANid 는 200 이며, VLAN *Engineering* 의 VLANid 는 400 이다.

```
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#vlan database
shu(config-vlan)#vlan 200
shu(config-vlan)#vlan 400
shu(config-vlan)#exit
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#switchport mode trunk
shu(config-if-Giga6/1/1)#switchport trunk allowed vlan add 200
shu(config-if-Giga6/1/1)#switchport trunk native vlan 200
shu(config-if-Giga6/1/1)#switchport trunk allowed vlan add 400
shu(config-if-Giga6/1/1)#end
shu#show vlan all
Bridge          VLAN ID  Name                State  Member ports
              (u)-Untagged, (t)-Tagged
-----
-
0                1        default             ACTIVE  Gi6/1/1 (t)
0                100      VLAN0100            ACTIVE
0                120      VLAN0120            ACTIVE  Gi6/1/1 (t)
0                200      VLAN0200            ACTIVE  Gi6/1/1 (u)
0                400      VLAN0400            ACTIVE  Gi6/1/1 (t)
shu#
```

포트 *gi6/1/1* 으로 태그가 붙지 않은 프레임이 수신되면 스위치는 VLAN *marketing* 의 멤버 포트에 프레임을 전달한다.

4.6. VLAN 설정 정보 확인

VLAN 설정 정보를 보려면 다음의 명령을 사용한다.

명령어	설명	모드
show vlans	<ul style="list-style-type: none"> ■ VLAN 와 관련된 다음의 요약 정보를 출력한다. <ul style="list-style-type: none"> • VLANid • 멤버 포트 • VLAN 이 속한 bridge • Spanning-tree 모드 	Exec
show vlan all	<ul style="list-style-type: none"> ■ VLAN 와 관련된 다음의 요약 정보를 출력한다. <ul style="list-style-type: none"> • VLANid • 멤버 포트 • tag, untag 	Exec

show interface trunk (module <1-6>)	<ul style="list-style-type: none"> ■ VLAN 와 관련된 다음의 요약 정보를 출력한다. <ul style="list-style-type: none"> • 포트 • Vlan 모드 • Native vlan, trunk vlan 	Exec
show interface summary vlan	<ul style="list-style-type: none"> ■ VLAN 와 관련된 다음의 요약 정보를 출력한다. <ul style="list-style-type: none"> • Vlan id 	Exec

```
shu#show vlan all
```

Bridge	VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
-				
0	1	default	ACTIVE	Gi6/1/1 (t) Gi6/1/2 (u) Gi6/1/5 (u)
0	2	VLAN0002	ACTIVE	
0	10	VLAN0010	ACTIVE	
0	11	VLAN0011	ACTIVE	
0	12	VLAN0012	ACTIVE	
0	100	VLAN0100	ACTIVE	
0	120	VLAN0120	ACTIVE	Gi6/1/1 (t) Gi6/1/2 (t) Gi6/1/3 (u) Gi6/1/4 (u)
0	200	VLAN0200	ACTIVE	Gi6/1/1 (u)
0	400	VLAN0400	ACTIVE	Gi6/1/1 (t)
0	1000	VLAN1000	ACTIVE	
0	2000	VLAN2000	ACTIVE	Gi6/1/5 (t)
0	3000	VLAN3000	ACTIVE	Gi6/1/6 (u) Gi6/1/7 (u)
0	4000	VLAN4000	ACTIVE	Gi6/1/6 (t) Gi6/1/7 (t)

```
shu#
```

```
shu#show vlan
```

VLAN Name	Status	Ports
1 default	active	Gi6/1/1 Gi6/1/2 Gi6/1/5
120 VLAN0120	active	Gi6/1/1 Gi6/1/2 Gi6/1/3 Gi6/1/4
200 VLAN0200	active	Gi6/1/1
400 VLAN0400	active	Gi6/1/1
1000 VLAN1000	active	
2000 VLAN2000	active	Gi6/1/5
3000 VLAN3000	active	Gi6/1/6 Gi6/1/7
4000 VLAN4000	active	Gi6/1/6 Gi6/1/7

VLAN	MTU	BridgeNo	Stp Enabled	BrdgMode
1	1500	0	Yes	rstp-vlan-bridge
120	1500	0	Yes	rstp-vlan-bridge
200	1500	0	Yes	rstp-vlan-bridge
400	1500	0	Yes	rstp-vlan-bridge

1000	1500	0	Yes	rstp-vlan-bridge
2000	1500	0	Yes	rstp-vlan-bridge
3000	1500	0	Yes	rstp-vlan-bridge
4000	1500	0	Yes	rstp-vlan-bridge

shu#

5

IP 환경 설정

5.1. 개요

본 장에서는 IP 주소를 설정하는 방법을 설명한다.

IP를 설정하기 위해 요구되는 기본 작업은 IP 주소를 네트워크 인터페이스에 할당하는 것이다. IP 주소를 할당함으로써 인터페이스는 **layer 3 interface**로 활성화된다.

E7500 Series 스위치는 다음의 인터페이스에 IP를 할당할 수 있다.

- VLAN interface
- Loopback interface
- Management interface

5.2. 네트워크 인터페이스에 IP 주소 할당

IP 주소는 수신된 IP 데이터그램이 보내질 지역을 식별한다. 어떤 IP 주소들은 특별한 용도로 예약되어 있어 호스트, 서브넷, 네트워크 주소로 사용할 수 없다. <표 5-1>은 IP 주소의 범위를 열거하였고, 어떤 주소들이 예약되었으며 어떤 주소들을 사용할 수 있는지 보여준다.

표 5-1. 사용 가능한 IP 주소

Class	주소 범위	상태
A	0.0.0.0 1.0.0.0 ~ 126.0.0.0	예약 사용가능

	127.0.0.0	예약
B	128.0.0.0 ~ 191.254.0.0	사용가능
	191.255.0.0	예약
C	192.0.0.0	예약
	192.0.1.0 ~ 223.255.255.254	사용 가능
	224.255.255.0	예약
D	224.0.0.0 ~ 239.255.255.255	멀티캐스트 그룹 주소
E	240.0.0.0 ~ 255.255.255.254	예약
	255.255.255.255	브로드캐스트



Notice IP 주소에 대한 공식적인 기술 사항은 RFC1166, Internet Number 를 참고하면 된다.



Notice 네트워크 번호를 할당 받으려면, 당신에게 서비스를 제공하고 있는 ISP(Internet Service Provider)에게 문의하라.

E7500 Series 스위치는 하나의 인터페이스에 복수의 IP 주소를 할당하는 기능을 지원한다. E7500 Series 스위치는 인터페이스 당 최대 10 개의 IP 주소를 설정할 수 있다. 다양한 상황에서 복수개의 IP 주소가 유용하게 사용된다. 다음은 가장 일반적인 응용이다:

- 특정 네트워크 세그먼트를 위한 충분한 호스트 주소가 마련되어 있지 않다. 예를 들어, 300 개의 호스트 주소를 필요로 하는 하나의 물리적인 서브넷 위에, 논리적인 서브넷마다 254 개의 호스트를 허용하도록 서브넷을 구성한다고 가정하자. 라우터나 access 서버에서 복수개의 IP 주소를 사용한다면 하나의 물리적 서브넷을 가지고 두 개의 논리적인 서브넷을 구성할 수 있다.
- 많은 오래된 네트워크들은 계층 2 의 브리지를 사용하여 구성되어 있으며, 서브넷으로 구성되어 있지 않다. 복수개의 주소의 적절한 사용은 서브넷으로의 전환과 라우터 기반 네트워크로 전환을 돕는다. 오래된 브리지 세그먼트에 속한 라우터는 그 세그먼트에 많은 서브넷이 존재한다는 사실을 쉽게 인식할 수 있다.
- 한 네트워크의 두 서브넷은 다른 네트워크에 의해 분리될 수 있다. 복수개의 주소를 사용하는 다른 네트워크에 의해 물리적으로 분리된 서브넷으로부터 하나의 네트워크를 구성할 수 있다. 이 예에서, 첫 네트워크는 확장되거나, 두 번째 네트워크의 상위에 위치한다. 서브넷은 라우터의 하나 이상의 활성화된 인터페이스에 동시에 나타날 수 없다.

네트워크 인터페이스에 IP 주소를 할당하려면, 인터페이스 설정 모드에서 다음의 명령을 사용한다.

표 5-2. IP 주소 할당 명령어

명령어	설명
<code>ip address ipaddress/prefixlen</code>	■ 인터페이스에 사용될 IP 주소를 설정한다.



Notice Prefixlen 란 ip address 중 네트워크를 구분하는 bit length 를 말한다.

5.3. ARP(Address Resolution Protocol)

ARP 테이블의 정보를 확인하려면, `privilege` 모드에서 다음 < 표 5-3>의 명령어를 사용한다. E7500 Series 에서는 Static ARP 설정 및 Proxy ARP 를 설정 할 수 있고

표 5-3. ARP 환경 설정을 위한 명령어

명령어	설명	모드
<code>Show arp</code>	■ ARP 테이블의 엔트리를 출력한다.	Privileged
<code>clear arp-cache</code>	■ ARP 테이블의 엔트리를 삭제한다.	Privileged
<code>Clear arp-cache interface IFNAME</code>	■ 해당 interface 의 ARP 엔트리를 삭제한다	Privileged
<code>arp ip-address MAC</code>	■ ARP 테이블에 static ARP 엔트리를 설정 ■ ip-address: ARP 엔트리의 IP 주소를 나타낸다; ■ MAC: ARP 엔트리의 48bit Ethernet 주소를 나타낸다. ■ alias	config
<code>no arp ip-address</code>	■ 해당 ip address 의 ARP 엔트리를 삭제한다.	config
<code>arp-ageing-timeout <1-3000></code>	■ 해당 interface 의 ARP entry 의 소멸 시간을 설정한다	interface
<code>no arp-ageing- timeout</code>	■ 해당 interface 의 ARP entry 소멸 시간을 default 값으로 설정한다 (default : 7200 sec)	interface

다음은 static ARP 를 설정하고 ARP timeout 을 설정하는 예이다. ARP 설정을 위해서는 설정하는 ip address 를 가지고 있는 interface 가 먼저 존재해야 한다.

```
shu#
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#arp 192.168.1.3 0111.1111.1213
% Interface does not exist
shu(config)#int GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#ip address 192.168.1.3/24
```

```

shu(config-if-Giga6/1/1)#exit
shu(config)#arp 192.168.1.3 0111.1111.1213
shu(config)#end
shu#show arp
Protocol Address      Hardware Addr  Type   Interface
-----
Internet 192.168.1.3    0111.1111.1213 static  Giga6/1/1
Internet 10.1.17.104    0022.1926.2db3 dynamic eth0
Internet 10.1.17.254    0007.7045.a36f dynamic eth0
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#no arp 192.168.1.3
shu(config)#end
shu#show arp
Protocol Address      Hardware Addr  Type   Interface
-----
Internet 10.1.17.254    0007.7045.a36f dynamic eth0
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#arp-ageing-timeout 2000
shu(config-if-Giga6/1/1)#

```

5.4. Static Routes 설정

Static route 는 패킷이 시작점부터 목적지까지의 명시된 경로를 따라 이동하도록 사용자가 정의한 라우팅 경로이다. 만약 라우팅 프로토콜을 사용하여 특정 목적지에 대한 경로를 구성할 수 없다면 static route 는 매우 중요하게 사용된다. 라우팅될 수 없는 패킷들이 보내질 게이트웨이를 명시하는데 유용하다.

Static route 를 설정하려면 Config 모드에서 다음의 명령을 사용한다.

표 5-4. Static route 경로 설정 명령어

명령어	설명
<pre>ip route {destination- prefix mask destination- ipaddress/mask} {gateway- ipaddress null0} [distance-value]</pre>	<ul style="list-style-type: none"> ■ Static route 를 등록한다. ■ destination-prefix : 목적지의 네트워크 번호를 명시한다. ■ mask : 목적지 네트워크의 마스크를 명시한다. ■ gateway-ipaddress : 게이트웨이 장치의 IP 주소를 명시한다. ■ null : null 인터페이스를 게이트웨이로 설정한다. ■ distance-value : 1 부터 255 사이의 숫자를 사용

시스템은 static route 가 지워질 때(global configuration 모드에서 IP route 명령의 no 형식을 사용)까지 기억한다. 하지만 administrative distance 값을 신중하게 할당함으로써 동적 라우팅 정보로 static route 를 중첩할 수 있다. 각 동적 라우팅 프로토콜은 <표 5-5>에 나열한 것처럼 default administrative distance 값을 가진다. Static route 가 동적 라우팅 프로토콜의 정보로 중첩되길 원한다면 static route 의 administrative distance 가 동적 프로토콜의 값보다 더 크면 된다.

표 5-5. 동적 라우팅 프로토콜의 default administrative distances

항목	기본 설정 값
Route Source	Default Distance
Connected interface	0
Static route	1
Exterior Border Gateway Protocol(BGP)	20
OSPF	110
RIP	120
Interior BGP	200
Unknown	255

인터페이스가 다운되었을 때, 그 인터페이스를 통하는 모든 static route 는 IP 라우팅 테이블에서 삭제된다. 또한 static route 에서 forwarding 라우터의 주소를 위해 유용한 다음 홉을 더 이상 찾을 수 없을 때에도 static route 는 IP 라우팅 테이블에서 삭제된다.

static route 정보를 확인하려면 privileged 모드에서 다음의 명령을 사용하라.

명령	목적
show ip route static	■ IP route 정보를 출력한다.

5.5. IP 설정 예제

이 절에서는 IP 주소 설정 예제를 제공한다:

- Assign IP address to network interface
- Creating a Network from Separated Subnets Examples
- ARP
- Static Route

다음의 예제는 스위치의 vlan5 인터페이스에 C 클래스 IP 주소인 192.10.25.1 를 할당한다.

```
Switch(config)# interface vlan5
Switch(config-int-vlan5)# ip address 192.10.25.1/24
```

다음의 예제에서 131.108.0.0 네트워크의 서브넷 1 과 2 는 백본 네트워크에 의해 분리된다. 두 네트워크는 하나의 논리적인 네트워크로 구성된다.

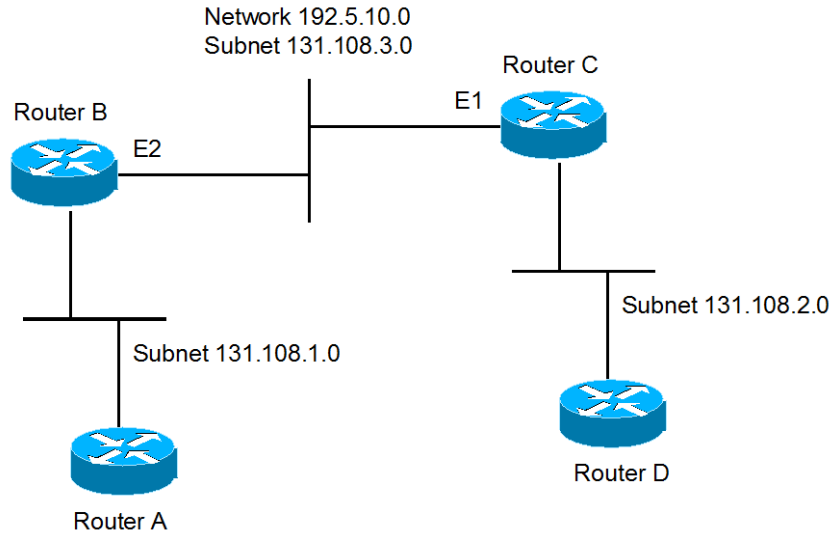


그림 5-1. 네트워크 설정 예 - 복수 IP address

라우터 B 설정

```
Switch(config)# interface vlan2
Switch(config-int-vlan2)# ip address 192.5.10.1/24
Switch(config-int-vlan2)# ip address 131.108.3.1/24
```

라우터 C 설정

```
Switch(config)# interface vlan2
Switch(config-int-vlan2)# ip address 192.5.10.2/240
Switch(config-int-vlan2)# ip address 131.108.3.2/24
```

다음의 예제들은 ARP 테이블의 내용을 확인하는 예제이다.

```
Switch# show arp
```

IP Address	MAC Address	IPF	PORT	RefCnt	Flags
10.1.2.254	0007.7089.1123	vlan2	fa1/1	1	S
10.1.11.46	0006.2bfc.146e	vlan11	fa6/1	1	S
10.1.13.1	0001.0281.f775	vlan13	fa2/1	1	R
10.1.13.190	0000.f083.f6d4	vlan13	fa6/2	1	K

다음의 명령은 ARP 테이블에 static ARP 엔트리를 등록한다.


```
Switch(config)# arp 142.10.52.196 0010.073c.0514 vlan1 fa2/1
Switch# show arp
```

IP Address	MAC Address	IPF	PORT	RefCnt	Flags
142.10.52.196	0010.073c.0514	vlan1	fa2/1	1	P

다음의 명령은 ARP 테이블에서 static ARP 엔트리를 삭제한다.

```
Switch(config)# no arp 142.10.52.196
```

다음의 예제는 20.1.1.0 네트워크에 연결된 호스트가 192.168.2.0 네트워크의 호스트와 통신할 수 있도록 static route 를 설정한다.

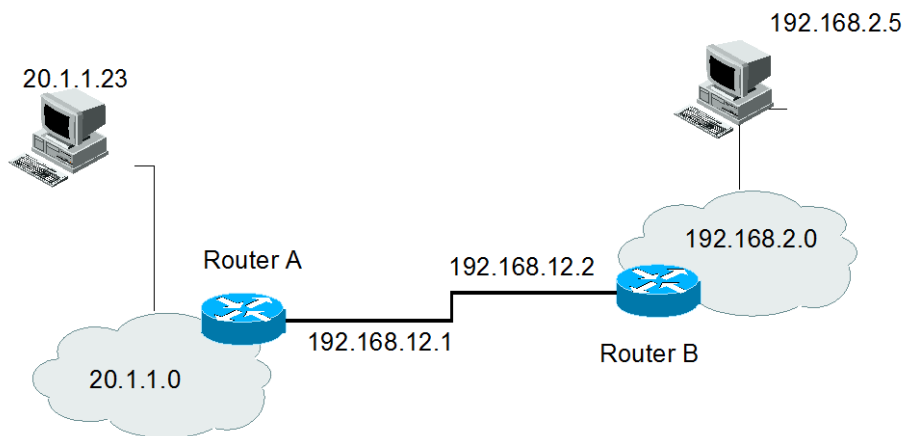


그림 5-2. 네트워크 설정 예 - Static route

라우터 A 설정

```
Switch(config)# ip route 192.168.2.0/24 192.168.12.2
Switch(config)# show ip route static
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route
S>* 192.168.2.0/24 [1/0] via 192.168.12.2 vlan2
Switch(config)#
```

라우터 B 설정

```
Switch(config)# ip route 20.1.1.0/8 192.168.12.1
Switch(config)# show ip route static
Codes: C - connected, S - static, R - RIP, O - OSPF,
       B - BGP, > - selected route, * - FIB route
S 20.1.1.0/8 [1/0] via 192.168.12.1 vlan2
```

Switch(config)#

6

DHCP

6.1. DHCP server 기능 및 설정

문서버전 History

E7508-DHCP-2

마지막 수정 날짜: 2010-02-17

적용가능 장비: E7508

6.1.1. DHCP server 기능 개요

DHCP(Dynamic Host Configuration Protocol)는 IP Network 의 다른 IP Host(DHCP client)들에게 재사용 가능한 IP Address 와 설정 파라미터를 동적으로 할당하는 방법을 제공한다. DHCP 는 규모가 큰 Network 환경과 복잡한 TCP/IP 소프트웨어 설정을 위해 설계되었으며, 이는 IP Network 관리자에게 요구되는 작업을 감소시킨다. Client 가 Server 로부터 수신하는 설정 정보 중 가장 중요한 것은 Client 의 IP Address 이다.

DHCP 는 BOOTP 의 확장이지만 DHCP 와 BOOTP 사이에는 다음과 같은 두 가지 큰 차이점이 있다.

- DHCP 는 Client 가 한정된 시간 동안만 IP Address 를 할당 받도록 하여, 후에 다른 Client 에게 그 IP Address 를 재할당하여 사용할 수 있는 방법을 제공한다.
- DHCP 는 Client 가 TCP/IP Network 에서 동작하기 위해 필요한 추가적인 IP 설정 파라미터들을 설정할 수 있는 방법을 제공한다.

E7508 server 는 스위치에 설정된 Address Pool 로부터 Client 에게로 IP Address 를 할당하고 관리하는 DHCP server 기능을 제공한다. 만약 DHCP server 가 자신의 데이터베이스에서 DHCP 요구를 만족시킬 수 없다면, 관리자에 의해 설정된 하나 이상의 보조 DHCP server 에게로 요구를 전달할 수도 있다.

DHCP server 의 Address 할당 방법

DHCP server 가 Client 에게 IP Address 를 할당하는 방법은 다음과 같다.

- 자동 할당(automatic allocation) – DHCP 가 Client 에게 영구적인 IP Address 를 할당한다.
- 수동 할당(manual allocation) – 관리자에 의해 Client 에게 IP Address 가 할당되며, DHCP 는 Client 에게 IP Address 를 실어 나른다.
- 동적 할당(dynamic allocation) – DHCP 가 제한된 기간 동안만 Client 에게 IP Address 를 할당한다.

사용 가능한 설정 파라미터들은 RFC 2132 에 열거되어 있으며, 주요 파라미터는 다음과 같다.

- Subnet mask
- Router
- Domain
- Domain Name Server(DNS)

E7508 를 DHCP server 로 사용

<그림 6-1>는 DHCP client 가 DHCP server(E7508)에게 IP Address 를 요구했을 때의 기본 절차이다.

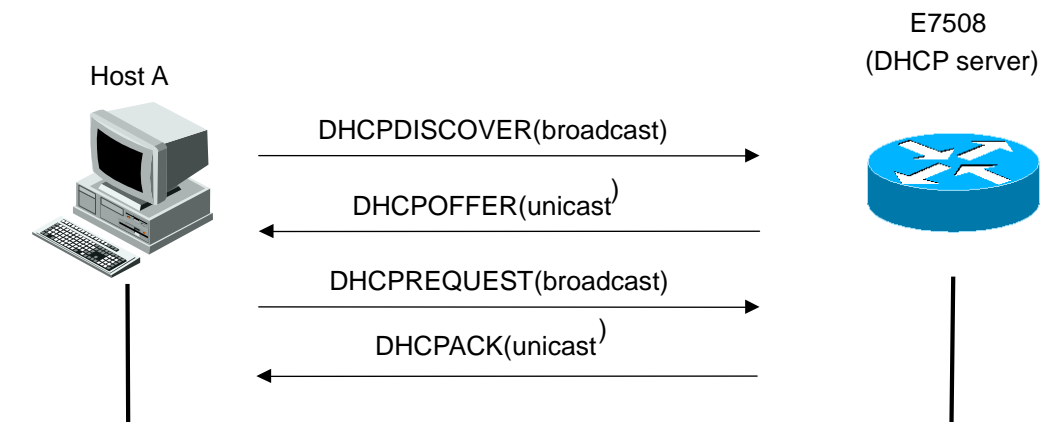


그림 6-1. E7508 를 DHCP server 로 사용

- 4) Client Host A 는 브로드캐스트 message *DHCPDISCOVER* 를 DHCP server 로 전송한다.
- 5) DHCP server 는 IP Address, 도메인 이름, IP Address 의 임대 기간 등의 설정 파라미터를 Client 에게 유니 캐스트 message *DHCPOFFER* 를 사용하여 전송한다.



Notice

DHCP client 는 하나 이상의 DHCP server 로부터 *DHCPOFFER* message 를 받을 수 있다. Client 는 일반적으로 가장 먼저 수신된 하나의 message 만 수용한다. 하지만 DHCP server 의 IP Address 제공 message 인 *DHCPOFFER* message 를 수신했다고 해서 DHCP server 가 Address 할

당을 보장하는 것은 아니다. DHCP server 는 Client 가 다시 공식적으로 Address 할당을 요구할 때까지 Address 사용을 예약한다.

- 6) Client 는 제공된 IP Address 에 대한 형식적인 요청을 DHCP server 에게 브로드캐스트 message *DHCPREQUEST* 를 사용하여 전송한다.
- 7) DHCP server 는 Client 에게 유니 캐스트 message *DHCPACK* 를 전송함으로써 IP Address 가 Client 에게 할당되었음을 확인한다.



Notice

Client 의 공식적인 Address 요청인 *DHCPREQUEST* message 는 이전의 *DHCPDISCOVER* message 를 수신한 모든 DHCP server 에게 브로드캐스트 된다. 이 message 를 받은 DHCP server 는 Client 에게 할당하고자 예약한 Address 를 다른 가입자에게 할당하도록 한다.

DHCP server 의 장점

E7508 server 는 다음의 이점을 제공한다.

- 인터넷 접근 비용의 감소 - 각각의 원격 사이트에서 자동으로 IP Address 할당을 사용함으로써 인터넷 접근 비용을 감소시킬 수 있다. 정적 IP Address 는 자동 IP Address 할당보다 더 높은 비용을 요구한다.
- Client 설정 작업과 비용의 감소 - DHCP 는 설정하기 쉽기 때문에, 장치 설정과 관련된 부담과 비용을 최소화 할 수 있으며, 많은 사람들이 쉽게 쓸 수 있다..
- 중앙 집중적인 관리 - DHCP server 는 여러 서브 Network 에 대한 설정을 관리하므로, 설정 파라미터가 변경되었을 경우 관리자는 오직 하나의 중앙 Server 만 변경하면 된다.

6.1.2. DHCP server 기능 활성화

기본적으로 스위치의 DHCP server 기능은 비활성화 되어 있다. global 설정 mode 에서 다음의 명령을 사용하여 DHCP server 기능을 활성화 시킬 수 있다.

명령	설명
<code>service dhcp</code>	<ul style="list-style-type: none"> ■ 스위치의 DHCP server 기능을 활성화 ■ DHCP server 기능을 비활성 시키려면, 이 명령의 no 형태를 사용

다음의 예제는 DHCP server 기능을 활성화 시킨다.

```
Router# configure terminal
```

```
Router(config)# service dhcp
Router# show running-config
!
. . .
service dhcp server
. . .
!
```

6.1.3. DHCP Address Pool

E7508 server 는 Network Pool 과 Host Pool 의 두 가지 Pool 을 지원한다.

- Network Pool – automatic 또는 dynamic allocation 을 위한 Pool 을 구성하며, 여러 개의 Network Pool 을 하나의 group 으로 구성하면, 서로 다른 서브넷 간에 IP Pool 을 공유할 수 있다.
- Host Pool – manual allocation 을 위한 Pool 을 구성하며, 하나의 Host Pool 에는 공통 정보를 갖는 여러 개의 Host 를 설정할 수 있다.

6.1.4. DHCP Network Pool 설정

문자열(예를 들어 “ubiquoss”) 또는 정수(예를 들어 0)를 이름으로 사용하여 DHCP Network Pool 을 설정할 수 있다. 또한 DHCP 네트워크 Pool 설정은 IP Network Address, 기본 라우터 등의 파라미터를 설정할 수 있는 DHCP 네트워크 Pool 설정 mode 로 진입한다. DHCP 네트워크 Pool 을 설정하기 위해서는 다음 절에서 요구되는 작업들을 완료해야 한다.



Notice 여러 개의 서로 다른 Network Pool 을 하나의 그룹으로 설정할 수 있으며, 하나의 VLAN 에 속하는 여러 개의 서브넷은 반드시 같은 그룹으로 구성하여야 한다.

DHCP Network Pool 이름 설정 및 DHCP 설정 mode 진입

DHCP 네트워크 Pool 이름을 설정하거나 DHCP Pool 설정 mode 로 진입하기 위해 global 설정 mode 에서 다음 명령을 사용한다.

명령어	설명
<code>ip dhcp pool name</code>	<ul style="list-style-type: none"> ■ DHCP Network Pool 을 위한 이름을 생성 ■ “config-dhcp#” 프롬프트로 식별되는 DHCP 네트워크 Pool 설정 mode 로 진입

다음의 예제는 DHCP Network Pool 이름을 ‘network_pool1’ 로 설정하는 예제이다. DHCP Network Pool Name 의 최대 길이는 ‘31’자 이다.

```
Router# configure terminal
```

```
Router(config)# ip dhcp pool network_pool1
Router(config-dhcp)# exit
Router# show running-config
. . .
!
ip dhcp pool network_pool1
!
. . .
```

DHCP 서브넷 및 Network 마스크 설정

새로 생성된 DHCP Address Pool 을 위한 IP Address 와 Server Network 의 마스크를 설정하기 위해 DHCP Network Pool 설정 mode 에서 다음의 명령을 사용한다.

명령어	설명
network <i>network-number/prefix-length</i>	<ul style="list-style-type: none"> DHCP 네트워크 Pool 내의 포함될 서브 Network 번호와 마스크를 설정

다음 예제는 DHCP Subnet 과 Network mask 를 100.0.0.0/24 로 설정하는 예제이다.

```
Router# configure terminal
Router(config)# ip dhcp pool network_pool1
Router(config-dhcp)# network 100.0.0.0/24
Router# show running-config
. . .
!
ip dhcp pool network_pool1
network 100.0.0.0/24
!
. . .
```

Network Pool 에서 할당 할 IP Address 범위 설정

DHCP Network Pool 내에서 Client 들에게 할당할 Address 범위를 지정한다. 하나의 네트워크 내에는 비연속적인 여러 개의 Address 범위를 지정할 수 있다.

명령어	설명
range <i>lowest-address highest-address</i>	<ul style="list-style-type: none"> 서브넷에서 클라이언트들에게 할당할 Address 범위를 지정한다. 이 명령어는 DHCP Subnet 및 Network Mask 를 설정한 이후에 설정해야 한다.

다음의 예제는 Network Pool 에서 할당 할 IP Address 범위를 100.0.0.1~100 으로 설정하는 예제이다.

```
Router# configure terminal
Router(config)# ip dhcp pool network_pool1
Router(config-dhcp)# range 100.0.0.1 100.0.0.100
Router# show running-config
```

```

. . .
!
ip dhcp pool network_pool1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
!
. . .

```

Client 를 위한 기본 라우터 설정

DHCP client 가 부팅된 후, Client 는 자신의 기본 라우터로 packet 을 전송한다. 기본 라우터의 IP Address 는 Client 와 동일한 서브 Network 상에 존재해야 한다. DHCP client 를 위한 기본 라우터를 설정하기 위해, DHCP Network Pool 설정 mode 에서 다음의 명령을 사용한다.

명령어	설명
<code>default-router address</code>	■ DHCP client 를 위한 기본 라우터의 IP Address 를 명시

다음의 예제는 DHCP server 에서 Client 를 위한 기본 라우터로 100.0.0.1 을 설정한다.

```

Router# configure terminal
Router(config)# ip pool network_pool1
Router(config-dhcp)# default-router 100.0.0.1
Router(config-dhcp)# exit
Router# show running-config
. . .
!
ip dhcp pool network_pool1
default-router 100.0.0.1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
!
. . .

```

Client 를 위한 DNS IP Server 설정

DHCP client 가 Host 이름을 IP Address 로 변환할 필요가 있을 경우, Client 는 DNS IP Server 에게 질의한다. DHCP client 가 이용할 수 있는 DNS IP Server 를 설정하기 위해 DHCP Pool 설정 mode 에서 다음의 명령을 사용한다.

명령	설정
<code>dns-server address</code>	<ul style="list-style-type: none"> ■ DHCP client 가 이용할 수 있는 DNS Server 의 IP Address 를 설정 ■ 명령어 입력시마다 새로운 DNS Server IP 가 삽입된다.

다음의 예제는 DHCP server 에서 Client 를 위한 DNS Server 로 200.0.0.1, 200.0.0.2 을 설정한다.

```

Router# configure terminal
Router(config)# ip dhcp pool network_pool1

```



```

Router(config-dhcp)# dns-server 200.0.0.1
Router(config-dhcp)# dns-server 200.0.0.2
Router(config-dhcp)# exit
Router# show running-config
. . .
!
ip dhcp pool network_pool1
dns-server 200.0.0.1
dns-server 200.0.0.2
default-router 100.0.0.1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
!
...

```

Client 를 위한 도메인 이름 설정

DHCP client 의 도메인 이름은 Client 를 일반적인 Network 의 그룹 속에 포함시킨다. Client 를 위한 도메인 이름 문자열을 설정하기 위해 DHCP Pool 설정 mode 에서 다음의 명령을 사용한다.

명령어	설명
domain-name <i>domain</i>	■ Client 를 위한 도메인 이름을 명시

다음의 예제는 DHCP server 에서 Client 를 위한 도메인 이름을 “ubiquoss.com”으로 설정하는 예제이다.

```

Router# configure terminal
Router(config)# ip dhcp pool network_pool1
Router(config-dhcp)# domain-name ubiquoss.com
Router(config-dhcp)# exit
Router# show running-config
. . .
!
ip dhcp pool network_pool1
dns-server 200.0.0.1 200.0.0.2
domain-name ubiquoss.com
default-router 100.0.0.1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
!
...

```

네트워크 Pool 을 위한 그룹 설정

여러 개의 DHCP 네트워크 Pool 을 Network 그룹 속에 포함시킬 수 있으며, 같은 그룹으로 구성된 네트워크 Pool 은 IP Pool 을 서로 공유할 수 있다.

명령어	설명
-----	----

```
group group-name
```

- 그룹 이름을 명시

**Notice**

하나의 interface 에 여러 개의 IP address 를 설정 시, 이는 반드시 같은 그룹 이름으로 각 Network Pool 을 구성하여야 한다.

다음의 예제는 서로 다른 Network Pool 을 “ubiquoss_pool”로 묶는 예제이다.

```
Router# configure terminal
Router(config)# ip dhcp pool network_pool1
Router(config-dhcp)# group ubiquoss_pool
Router(config-dhcp)# exit
Router# show running-config
. . .
!
ip dhcp pool network_pool1
dns-server 200.0.0.1 200.0.0.2
domain-name ubiquoss.com
default-router 100.0.0.1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
group ubiquoss_pool
!
. . .
```

Address 임대 기간 설정

기본적으로 DHCP server 에 의해 할당된 각각의 IP Address 는 한 시간 동안 임대된다. IP Address 의 할당 기간을 변경하기 위해서 DHCP Address Pool mode 에서 다음의 명령을 사용한다.

명령어	설명
lease {days [hours] [minutes]}	<ul style="list-style-type: none"> ■ 임대 기간을 명시 ■ 기본값은 한 시간으로 설정 ■ infinite: Host 에게 영구적으로 IP Address 를 임대하는 자동 할당방식으로 설정

다음의 예제는 Address 임대 기간은 ‘20’ 분으로 설정하는 예제이다.

```
Router(config)# ip dhcp pool network_pool1
Router(config-dhcp)# lease 0 0 20
Router(config-dhcp)# exit
Router# show running-config
. . .
!
ip dhcp pool network_pool1
dns-server 200.0.0.1 200.0.0.2
lease 0 0 20
domain-name ubiquoss.com
default-router 100.0.0.1
network 100.0.0.0/24
```

```

range 100.0.0.1 100.0.0.100
group ubiquoss_pool
!
...

```

6.1.5. DHCP Host Pool 설정

수동 바인딩은 IP Address 와 Client 의 MAC(Media Access Control) Address 사이의 매핑이다. Client 의 IP Address 는 Network 관리자에 의해서 수동으로 할당되거나 DHCP server 의 Pool 로부터 자동으로 할당될 수 있으며, Host Pool 은 수동 Address 할당을 위한 특별한 형태의 Address 할당 형태이다. DHCP Host Pool 설정은 IP, MAC 등의 파라미터를 설정할 수 있는 DHCP Host Pool 설정 mode 로 진입한다. DHCP Host Pool 을 설정하기 위해서는 다음 절에서 요구되는 작업들을 완료해야 한다.



Notice

하나의 Host Pool 은 공통된 파라미터를 적용하기 원하는 Client 들을 위한 Pool 이다. 하나의 Host Pool 에는 여러 개의 Host 를 설정할 수 있으며, 한 번의 파라미터 설정으로 해당 Pool 내의 모든 Host 들에게 파라미터를 적용할 수 있다.

DHCP Host Pool 이름 설정 및 DHCP 설정 mode 진입

DHCP Host Pool 이름을 설정하거나 DHCP Pool 설정 mode 로 진입하기 위해 global 설정 mode 에서 다음 명령을 사용한다.

명령어	설명
<code>ip dhcp pool name</code>	<ul style="list-style-type: none"> ■ DHCP Host Pool 을 위한 이름을 생성 ■ “config-dhcp#” 프롬프트로 식별되는 DHCP Host Pool 설정 mode 로 진입

다음의 예제는 DHCP Host Pool 이름을 ‘host_pool1’로 설정하는 예제이다. DHCP Host Pool Name 의 최대 길이는 ‘31’자 이다.

```

Router# configure terminal
Router(config)# ip dhcp pool host_pool1
Router(config-dhcp)# exit
Router# show running-config
. . .
!
ip dhcp pool host-pool
!
. . .

```

표 2. Host Pool 설정 명령어

명령어	설명
<code>default-router address</code>	<ul style="list-style-type: none"> DHCP client 를 위한 기본 라우터의 IP Address 를 명시
<code>dns-server address1 address2 address3</code>	<ul style="list-style-type: none"> DHCP client 가 이용할 수 있는 DNS Server 의 IP Address 를 설정 DHCP client 하나의 IP Address 만 요구하지만, 명령 라인에서 최대 3 개의 IP Address 를 설정할 수 있다.
<code>domain-name domain</code>	<ul style="list-style-type: none"> Client 를 위한 도메인 이름을 명시
<code>host ipaddr/prefix-len</code>	<ul style="list-style-type: none"> 하나의 Host Pool 내에서 설정할 수동 바인딩 IP 의 네트워크



Notice

Pool 생성 후 `host` 명령의 입력, `network` 명령의 입력에 따라서 `host pool` 또는 `network pool` 로 설정되고 이외 공통적인 명령은 설정 방법이 동일하다.

DHCP 수동 바인딩을 위한 Client 설정

Host Pool 내에 수동 바인딩을 제공할 Client 들을 생성한다.

명령어	설명
<code>host ip-address netmask</code>	<ul style="list-style-type: none"> Client 에게 할당할 IP Address 와 제공할 Network 마스크 를 설정한다. "<code>config-dhcp #</code>" 프롬프트로 식별되는 DHCP Host 설정 <code>mode</code> 로 진입

표 3. 수동 바인딩 명령어

명령어	설명
<code>hardware-address hardware-address</code>	<ul style="list-style-type: none"> Client 의 하드웨어 Address 를 명시

다음의 예제는 Mac Address 가 00:11:22:33:44:55 인 가입자 단말에게 IP 110.0.0.1 을 할당하는 예제이다. 이 명령어는 'network A.B.C.D' 명령어 이후에 설정해야 한다.

```
Router# configure terminal
Router(config)# ip dhcp pool host_pool1
Router(config-dhcp)# host 110.0.0.1/24
Router(config-dhcp)# hardware-address 0011.2233.4455
Router(config-dhcp)# exit
Router# show running-config
. . .
!
```

```
ip dhcp pool host_pool1
  host 110.0.0.1/24
  hardware-address 0011.2233.4455
!
```

6.1.6. 기타 global 명령어

표 4. global 명령어 리스트

명령어	설명
ip dhcp max-lease {days [hours] [minutes] infinite}	<ul style="list-style-type: none"> DHCP client 에서 Lease time 에 대한 요청이 있는 경우, DHCP server 는 max-lease time 값 이상의 임대시간을 DHCP client 에게 할당하지 않는다. Premier 스위치는 1 일 을 기본 값으로 갖는다.

다음은 max-lease time 을 '2'일로 설정하는 예제이다.

```
Router(config)# ip dhcp max-lease 2
Router# show running-config
!
. . .
ip dhcp max-lease 2
. . .
!
```

6.2. DHCP relay agent 기능 및 설정

6.2.1. DHCP relay agent 개요

- DHCP relay 는 서로다른 subnet 상에 위치한 DHCP client, DHCP server 사이에서 DHCP packet 을 forwarding 해주는 host 이다. IP 망에서의 일반적인 packet forwarding 과는 달린 relay agent 는 DHCP packet 을 RX 하면 RX 받은 packet 에 몇몇 field 가 추가되거나 변경된 packet 을 생성하여 Forwarding 한다. DHCP relay agent 는 gateway address 에 값을 기록 (DHCP packet 의 giaddr field)하고 relay agent information option (option82)를 DHCP packet 에 삽입하여 server 에 전달하도록 설정할 수 있다.

E7508 을 DHCP relay agent 로 설정하면 아래와 같이 DHCP client, DHCP server 간 DHCP packet 을 forwarding 한다.

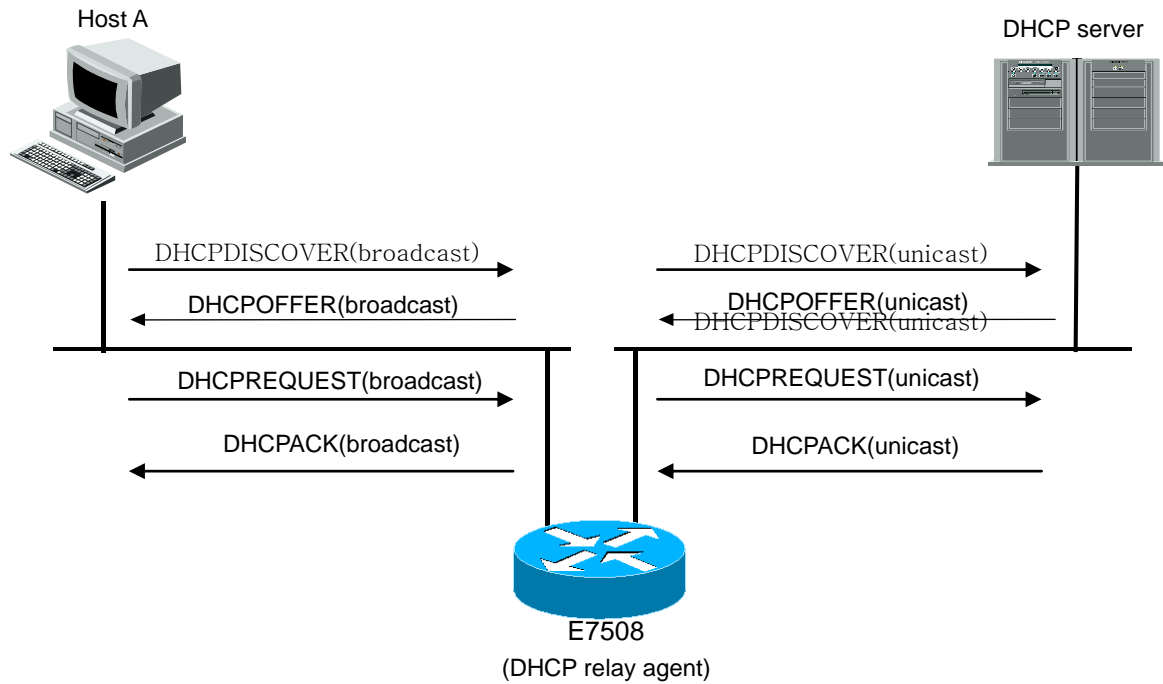


그림 6-2. DHCP relay agent 로서 DHCP server 의 message 전달

- 1) DHCP client 는 IP 를 요청하기 위해 DHCP DISCOVER message 를 broadcast 로 전송한다.
- 2) DHCP relay agent 는 DHCP client 의 IP 요청 message 를 수신하여 DHCP server 에게 해당 message 를 unicast 로 전달한다.
- 3) DHCP relay agent 로부터 message 를 수신한 DHCP server 는 client 의 IP address, default gateway 등의 정보를 가진 DHCP OFFER message 를 unicast 로 DHCP relay agent 에게 unicast 로 전송한다.(이때의 destination IP 로는 giaddr field 에 기록된 IP 를 사용한다.)



Notice

일반적으로 DHCP server 는 DHCP DISCOVERY/REQUEST message 의 giaddr field 가 설정되어있다면 server 가 가진 address pool 중 giaddr 과 같은 subnet 에 속하는 address pool 에서 IP address 를 선택하여 이를 offer 하거나 할당하는 DHCP OFFER/ACK message 를 relay agent 에게 전송하고 giaddr 에 해당하는 address pool 이 없는 경우 응답하지 않지만 이는 DHCP 의 RFC (RFC 2131)에서 강제 하는 사항은 아니다.

- 4) DHCP relay agent 는 수신한 DHCPOFFER message 를 client 에게 broadcast 로 전송한다.
- 5) DHCP server 와 client 사이의 DHCPREQUEST 와 DHCPACK message 도 동일한 과정을 통해 DHCP relay agent 에 의해 전달된다.

6.2.2. DHCP relay 기능 활성화

기본적으로 스위치의 DHCP relay agent 는 비활성화 되어 있다. global 설정 mode 에서 다음의 명령을 사용하여 DHCP relay agent 를 활성화 할 수 있다.

명령	설명
service dhcp relay	<ul style="list-style-type: none"> ■ Router 의 DHCP relay 기능을 활성화 ■ DHCP relay 기능을 비활성화 하려면, 이 명령의 no 형태를 사용
	<div style="display: flex; align-items: center;"> <div style="background-color: #0056b3; color: white; padding: 5px; margin-right: 10px;">i</div> <div> <p>Notice E7508 의 DHCP relay 는 .DHCP server 와 같이 설정될 경우의 동작을 보장하지않는다. 이는 반대의 경우에도 마찬가지다.</p> </div> </div>

DHCP Relay agent 를 통해서 DHCP packet 을 forwarding 하려면 router 의 switching chip 이 packet 을 forwarding 하지않고 CPU 로 packet 을 trap 해서 relay agent 가 packet 을 처리할수 있도록 설정할 필요가 있다.

다음은 가입자가 Vlan10 에 속한 port 에 연결되어있고 gi1/1/1 을 통해 DHCP server 가 연결되어있을 때 DHCP relay agent 를 활성화하는 예제이다.

```
Router#config terminal
Router(config)#class-map dhcp_user_class
Router(config-cmap)#match protocol udp
Router(config-cmap)#match layer4 source-port 68
Router(config-cmap)#exit
Router(config)#class-map dhcp_server_class
Router(config-cmap)#match protocol udp
Router(config-cmap)#match layer4 source-port 67
Router(config-cmap)#end
Router#show class-map

CLASS-MAP-NAME: dhcp_user_class (match-all)
  Match Source Port: 68
  Match Protocol: udp

CLASS-MAP-NAME: dhcp_server_class (match-all)
  Match Source Port: 67
  Match Protocol: udp

Router#config terminal
Router(config)#policy-map dhcp_user_map
Router(config-pmap)#class dhcp_user_class
Router(config-pmap-c)#trap-cpu
Router(config-pmap-c)#exit
Router(config-pmap)#exit
```

```
Router(config)#policy-map dhcp_server_map
Router(config-pmap)#class dhcp_user_class
Router(config-pmap-c)#trap-cpu
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#int vlan10
Router(config-if-Vlan10)#service-policy input dhcp_user_map
Router(config-if-Vlan10)#int gil/1/1
Router(config-if-Gigal/1/1)service-policy input dhcp_user_map
Router(config-if-Gigal/1/1)end
Router#show policy-map
```

```
POLICY-MAP-NAME: dhcp_user_map
State: attached
```

```
CLASS-MAP-NAME: dhcp_user_class (match-all)
Trap-cpu
```

```
POLICY-MAP-NAME: dhcp_server_map
State: attached
```

```
CLASS-MAP-NAME: dhcp_server_class (match-all)
Trap-cpu
```

```
Router#show service-policy
Interface Gigal/1/1 : input dhcp_server_map
Interface Vlan10 : input dhcp_user_map
Router# configure terminal
Router(config)# service dhcp relay
Router(config)# exit
Router# show ip dhcp relay
```

```
DHCP relay : Enabled
DHCP Smart Relay feature : Disabled
DHCP Smart Relay retry count : 3
DHCP server-id based relay : Disabled
Verification of MAC address : Enabled
Insertion of option 82 : Disabled
DHCP Option82 Management-IP : 0.0.0.0
DHCP maximum hop count : 10
```

```
DHCP helper-address is configured on following servers:
none
```

6.2.3. DHCP Relay Agent 에서 DHCP Server 설정

DHCP relay agent 가 작동하기 위해서는 DHCP client 로 부터 온 DHCP DISCOVER/REQUEST message 를 forwarding 할 DHCP server 를 설정해야 한다. relay agent 는 DHCP packet 을 RX 한 interface 별로 forwarding 할 server 를 설정하거나 packet 을 RX 한 interface 에 무관하게 forwarding

할 server 를 설정할 수 있다.

DHCP message 를 RX 한 interface 별로 DHCP server 를 설정하려면 다음의 명령을 사용한다.

명령어	설명
ip dhcp helper-address address	<ul style="list-style-type: none"> ■ interface 에서 RX 한 DHCP DISCOVER/REQUEST message 를 forwarding 할 DHCP server 의 IP address 를 설정 ■ interface 에서 수신한 DHCP packet 만 지정된 server 로 forwarding 함. ■ 설정을 해제하려면 명령의 no 형태를 사용

DHCP message 를 RX 한 interface 와 관계없이 DHCP server 를 설정하려면 다음의 명령을 사용한다.

명령어	설명
ip dhcp-server address	<ul style="list-style-type: none"> ■ DHCP relay agent 가 DHCP DISCOVER/REQUEST message 를 forwarding 할 DHCP server 의 IP address 를 설정 ■ 설정을 해제하려면 명령의 no 형태를 사용



Notice

E7508 의 DHCP relay Agent 는 helper-address 를 최대 256 개까지 설정 가능하다.

다음은 DHCP relay agent 에서 server 주소를 지정하는 예제이다.

```
Router#configure terminal
Router(config)#service dhcp relay
Router(config)#ip dhcp-server 192.168.0.254
Router(config)#exit
Router#show ip dhcp relay
```

```
DHCP relay : Enabled
DHCP Smart Relay feature : Disabled
DHCP Smart Relay retry count : 3
DHCP server-id based relay : Disabled
Verification of MAC address : Enabled
Insertion of option 82 : Disabled
DHCP Option82 Management-IP : 0.0.0.0
DHCP maximum hop count : 10
```

```
DHCP helper-address is configured on following servers:
 192.168.0.254
```

```
Router#configure terminal
Router(config)#interface vlan1
```

```
Router (config-if-vlan1)#ip dhcp helper-address 100.0.0.1
Router(config)#end
Router#show ip dhcp relay
DHCP relay : Enabled
DHCP Smart Relay feature : Disabled
DHCP Smart Relay retry count : 3
DHCP server-id based relay : Disabled
Verification of MAC address : Enabled
Insertion of option 82 : Disabled
DHCP Option82 Management-IP : 0.0.0.0
DHCP maximum hop count : 10
```

```
DHCP helper-address is configured on following servers:
 192.168.0.254, 100.0.0.1(vlan1)
```

6.2.4. DHCP Relay Agent Information option(OPTION82) 설정

일반적으로 DHCP protocol 에 의한 IP address 의 할당은 gateway IP address (DHCP packet 의 giaddr field)나 packet 을 RX 한 interface 의 IP address 에 의해 결정되지만 network 구성에 따라 IP 할당이나 가입자별 network 이용정책 설정을 위한 추가적인 정보가 요구되는 경우가 있다.

E7508 DHCP relay agent 는 client 에서 RX 한 DHCP packet(DHCP DISCOVER/REQUEST message)를 DHCP server 로 forwarding 할 때, packet 을 RX 한 E7508 의 port/Interface 정보를 포함할 수 있도록 relay agent 가 DHCP relay agent information option 을 client 로 부터 받은 packet 에 삽입할 수 있는 기능을 제공한다. server 는 이 정보를 가입자의 IP 할당, 가입자에 대한 access controll 수행, QoS 및 보안정책 설정등에 이용할 수 있다.

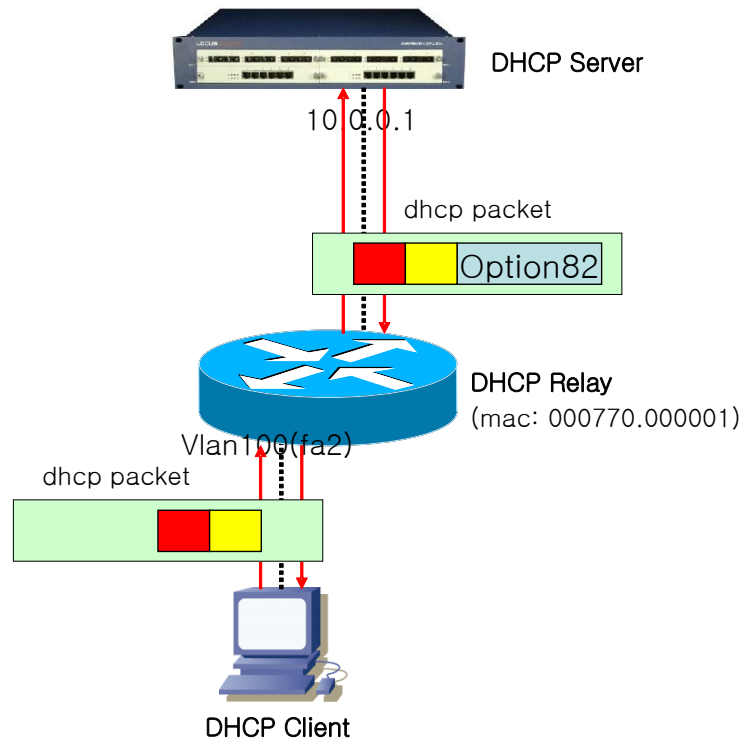


그림 6-3. DHCP Relay Option82

위 그림에서처럼 DHCP relay agent information option 은 DHCP relay agent 와 DHCP server 사이에서만 사용된다. relay agent 는 client 가 전송한 packet 을 server 로 forwarding 할 때 DHCP relay agent information option 를 삽입하며, server 가 전송한 packet 을 client 에게 forwarding 할 때 DHCP relay agent information option 를 제거한다.

DHCP relay agent information option 기능의 활성화

E7508 DHCP relay agent 에서 relay agent information option 기능을 활성화시키기 위해서는 다음의 명령을 사용한다.

명령어	설명
ip dhcp relay agent information option	<ul style="list-style-type: none"> ■ DHCP relay agent information option 기능을 활성화 ■ 기본적으로, 이 특성은 비활성화 되어 있다. ■ router 에서 relay agent information option 을 삽입하지 않으려면 이명령의 no 형식을 사용한다.

다음은 DHCP relay agent 의 relay agent information option 삽입 기능을 활성화 시키는 예제이다.

```
Router# configure terminal
Router(config)# ip dhcp relay agent information option
Router(config)# exit
Router#
Router# show ip dhcp relay
```

```

DHCP relay : Enabled
DHCP Smart Relay feature : Disabled
DHCP Smart Relay retry count : 3
DHCP server-id based relay : Disabled
Verification of MAC address : Enabled
Insertion of option 82 : Enabled
DHCP relay agent information option policy : replace
DHCP Option82 Management-IP : 0.0.0.0
DHCP maximum hop count : 10
    
```

DHCP helper-address is configured on following servers:
192.168.0.254

Relay agent information option reforwarding 정책 설정

기본적으로, E7508의 relay agent information option reforwarding 정책은 DHCP client(또는 DHCP relay agent)로부터 수신한 packet에 기존의 relay agent information option이 이미 삽입되어 있는 경우 router의 relay agent information option으로 이를 대체한다. 기본 정책을 변경하기 원한다면, global 설정 mode에서 다음의 명령을 사용한다.

명령어	설명
ip dhcp relay agent information option policy {drop keep replace}	<ul style="list-style-type: none"> ■ 기본 값은 replace이다. ■ drop : relay agent information option이 삽입되어 있는 packet은 폐기한다. ■ keep : 기존의 relay agent information option을 유지하며, 기존의 relay agent information option이 없으면 router의 relay agent information option을 삽입한다. ■ replace : 기존의 relay agent information option을 router의 relay agent information option으로 대체한다. ■ 기본 설정으로 돌아가려면 이 명령의 no 형태를 사용한다.

다음의 예제는 DHCP Relay Information Option reforwarding 설정을 Drop으로 설정한다.

```

Router# configure terminal
Router(config)# ip dhcp relay agent information option policy drop
Router(config)# exit
Router# show ip dhcp relay

DHCP relay : Enabled
DHCP Smart Relay feature : Disabled
DHCP Smart Relay retry count : 3
DHCP server-id based relay : Disabled
Verification of MAC address : Enabled
Insertion of option 82 : Enabled
DHCP relay agent information option policy : drop
DHCP Option82 Management-IP : 0.0.0.0
DHCP maximum hop count : 10
    
```

DHCP helper-address is configured on following servers:
192.168.0.254

6.2.5. DHCP Smart Relay 설정

E7508 DHCP relay agent 는 기본적으로 DHCP client 로 부터 DHCP packet 을 받은 interface 의 primary IP address 를 DHCP packet 의 giaddr field 로 설정하여 DHCP server 로 packet 을 forwarding 한다.

일반적인 network 구성에서 giaddr field 에 설정된 IP 는 server 가 client 에게 IP address 를 할당하는데 사용할 address pool 을 결정하기위해 참조되고 server 가 relay agent 로부터 forwarding 받은 packet 에 대한 응답을 전송할때 destination IP 로 사용된다.

smart-relay 기능은 router 가 client 로부터 DHCP packet 을 RX 받은 interface 에 두개 이상의 IP 가 설정되어 있고 relay agent 가 interface 에 설정된 IP address 중 하나를 사용하여 giaddr field 를 설정하여 server 로 forwarding 한 DHCP DISCOVER/REQUEST message 에 대한 응답이 일정횟수이상 오지않는다면 interface 에 설정된 다른 IP address 를 giaddr field 에 설정하고 DHCP DISCOVER/REQUEST message 를 forwarding 하여 client 가 server 의 다른 address pool 또는 다른 server 를 통해 IP address 를 할당받을수 있게 하는 기능이다.

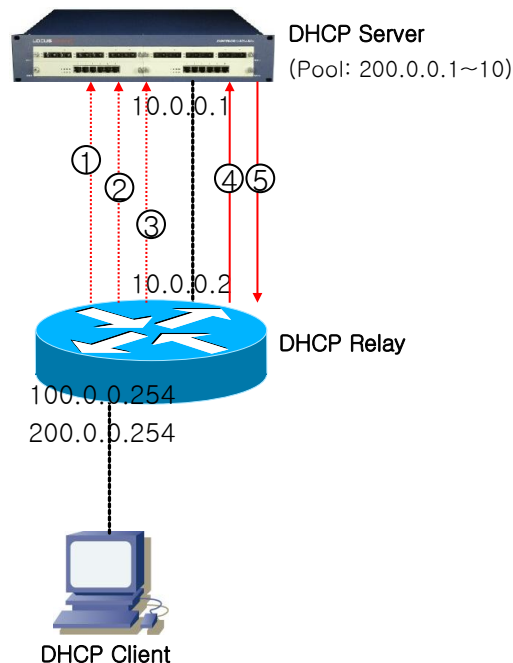


그림 6-4. DHCP Smart-Relay 동작 절차

- 8) client 로부터 DHCP DISCOVER/REQUEST message 를 수신한 relay agent 는 giaddr field 에 DHCP packet 을 RX 한 interface 의 primary IP 인 '100.0.0.254'를 삽입하여 packet 을 server 에게

forwarding 한다.(1) server 에 설정된 address pool 중 giaddr field 의 IP 와 같은 subnet 상의 address pool 이 없으므로 server 는 relay agent 가 보낸 message 에 응답하지 않는다.

- 9) DHCP OFFER/ACK message 를 받지 못한 client 는 다시 한번 IP 를 요청한다. 이 message 를 수신한 relay agent 는 그 client 에서 giaddr field 값으로 100.0.0.254 를 사용한 IP 요청 시도횟수를 기억한다.
- 10) IP 요청 시도 횟수가 3 회(기본설정) 이상이면 (2) (3)('4' 번 packet), relay agent 는 다음부터는 giaddr 를 '200.0.0.254'로 변경하여 server 로 message 를 forwarding 한다.(4) server 에 설정된 address pool 중 200.0.0.254 와 같은 network 에 속한 pool 이 있으므로 server 로부터 정상적으로 응답을 받는다.(5)



Notice

E7508 DHCP relay agent 는 smart-relay 에 사용하기 위해 interface 당 최대 500 개의 client 의 IP 요청 시도횟수를 유지하기 위해 내부적인 database 를 사용한다. 만약 한 interface 상에 IP 할당을 요청했으나 server 로 부터 응답을 받지 못한 client 가 500 개 이상 존재한다면 relay agent 는 database 를 삭제한다.

DHCP smart-relay 를 활성화 하기 위해 아래의 명령을 사용한다.

명령어	설명
ip dhcp smart-relay	<ul style="list-style-type: none"> ■ DHCP smart-relay 기능을 활성화 ■ 기본적으로, 이 특성은 비활성화 되어 있다. ■ 해제하기 위해서는 이 명령의 no 형식을 사용한다.

DHCP relay agent 가 giaddr field 에 설정할 IP address 를 변경하는 client 의 IP 요청 시도횟수는 아래의 명령어로 설정할 수 있다.

명령어	설명
ip dhcp smart-relay retry <1-10>	<ul style="list-style-type: none"> ■ <1-10> giaddr field 에 설정할 IP 를 relay agent 가 변경하는 client 의 IP 요청 시도횟수 ■ 기본값은 3 이다. ■ 기본값으로 돌아가기 위해서는 이 명령의 no 형식을 사용한다.

다음은 DHCP Smart-Relay 기능을 설정하는 예제이다.

```
Router# configure terminal
Router(config)# ip dhcp smart-relay
Router(config)# ip dhcp smart-relay retry 5
Router(config)# exit
Router# show ip dhcp relay

DHCP relay : Enabled
DHCP Smart Relay feature : Enabled
DHCP Smart Relay retry count : 5
DHCP server-id based relay : Disabled
Verification of MAC address : Enabled
```

```

Insertion of option 82      : Enabled
DHCP relay agent information option policy : drop
DHCP Option82 Management-IP  : 0.0.0.0
DHCP maximum hop count      : 10

DHCP helper-address is configured on following servers:
192.168.0.254
    
```

6.2.6. DHCP Relay Agent Verify MAC-Address 설정

DHCP relay agent 는 IP 요청을 시작한 DHCP client 를 인식하기 위한 수단으로 DHCP packet 의 field 중 다음 세가지를 사용한다.

- 1) source MAC address
- 2) client hardware address(chaddr field)
- 3) client identifier option (option61)

E7508 DHCP relay agent 는 악의적인 client 로부터의 IP 할당요청을 막기위해 DHCP DISCOVER message 의 위 세 field 를 검사하여 세 field 가 동일하지 않을 경우 DHCP DISCOVER message 를 server 로 forwarding 하지않도록 설정할 수 있다.

client hardware address 또는 client Identifier option 이 변조된 DHCP DISCOVER message 를 drop 하기 위해 다음 명령어를 사용한다.

명령어	설명
ip dhcp relay verify mac-address	<ul style="list-style-type: none"> ■ DHCP DHCP DISCOVER message 의 client hardware address 또는 client Identifier option 이 변조된 경우, 이 message 를 server 로 forwarding 하지 않는다. ■ 기본적으로, 이 특성은 활성화 되어 있다. ■ 비활성화 시키기 위해서는 이 명령어의 no 형식을 사용하면 된다.

다음은 DHCP relay agent verify MAC-address 기능 설정을 해제하는 예제이다.

```

Router# configure terminal
Router(config)# no ip dhcp relay verify mac-address
Router(config)# exit
Router# show ip dhcp relay

DHCP relay      : Enabled
DHCP Smart Relay feature : Enabled
DHCP Smart Relay retry count : 3
DHCP server-id based relay : Disabled
Verification of MAC address : Disabled
Insertion of option 82      : Enabled
DHCP relay agent information option policy : drop
DHCP Option82 Management-IP  : 0.0.0.0
    
```

```
DHCP maximum hop count      : 10
```

```
DHCP helper-address is configured on following servers:  
192.168.0.254
```

6.2.7. DHCP Class 기반 DHCP packet forwarding

E7508 DHCP relay agent 는 client 로부터 RX 한 DHCP DISCOVER/REQUEST message 에 options 60, 77, 124 또는 125 가 삽입되었다면 (packet 이 수신된 Network/DHCP option/option 값)과 DHCP message 를 RX 한 interface 가 속한 subnet 에 따라 DHCP message 를 forwarding 할 server 를 선택 하는 기능을 가지고 있다. 이 기능은 ip dhcp-server, ip dhcp helper-address 명령어와 같이 client 로 부터 RX 한 DHCP message 를 어떤 DHCP server 로 forwarding 할지 선택하는 기능이다.



Notice

E7508 DHCP relay agent 는 RX 한 DHCP DISCOVER/REQUEST message 가 relay agent 에 설정된 DHCP class 중 하나로 분류되어 message 를 forwarding 할 DHCP server 를 알게 되면 그 server 로만 message 를 forwarding 하고 ip dhcp-server, ipdhcp helper-address 명령에 의해 지정된 server 로는 message 를 forwarding 하지 않는다.

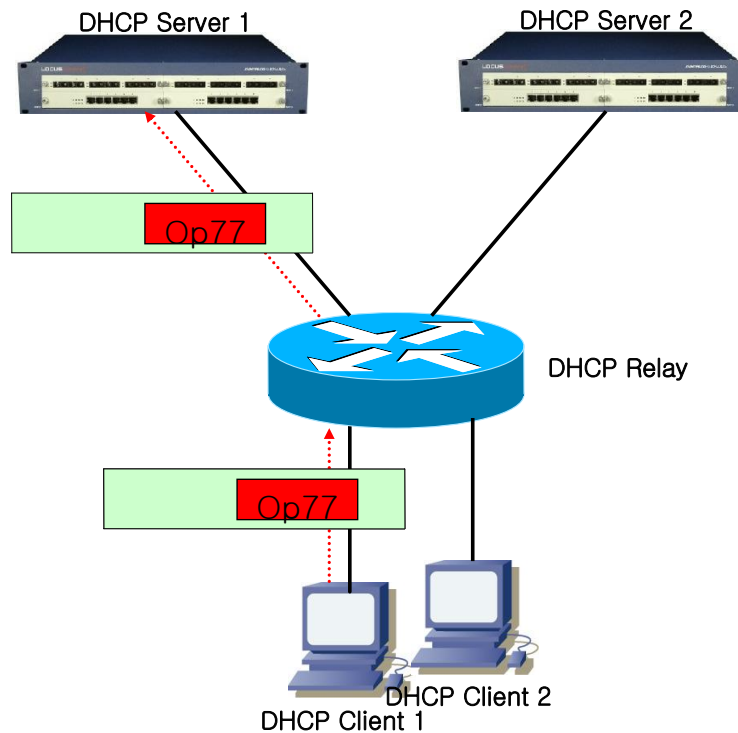


그림 6-5. DHCP Class 기반 DHCP packet Relay

DHCP Class 설정

E7508 DHCP relay agent 에서 DHCP class 를 설정하기 위해 다음의 명령어를 사용한다.

명령어	설명
<code>ip dhcp class class-name</code>	<ul style="list-style-type: none"> ■ DHCP Class Name 지정 ■ “(dhcp-class)#” 로 식별되는 DHCP class 설정 mode 로 진입 ■ class 를 삭제하기 위해서는 이 명령의 no 형식을 사용.
<code>option <1-255> {ascii hex} WORD</code>	<ul style="list-style-type: none"> ■ client 가 보낸 DHCP message 가 이 class 로 분류되기 위해 가지고 있어야 할 option-option value 를 설정한다. ■ <1-255>: DHCP option 번호 ■ {ascii hex}: DHCP option 값 형식 (ascii 문자열, hexadecimal) ■ WORD: option 값,



Notice

- 형식이 hexadecimal 일 경우 반드시 짝수개의 digit 를 사용해야 한다.
EX) ip dhcp option 60 hex 1 -> 설정안됨

ip dhcp option 60 hex 01 -> 설정됨

다음은 DHCP Class “test” 를 설정하는 예제이다. client 로 부터 RX 된 DHCP DISCOVER/REQUEST message 중 option 77 을 가지고 그 값이 ascii 문자열 77 인 message 는 이 class 로 분류된다.

```
Router(config)# configure terminal
Router(config)# ip dhcp class test
Router(dhcp-class)# option 77 ascii ubiquoss
```

DHCP Relay-Pool 설정

E7508 DHCP relay agent 의 DHCP relay-pool 은 DHCP client 로 부터 RX 한 DHCP DISCOVER/REQUEST message 가 분류된 class, message 를 RX 한 interface 가 속한 subnet 을 보고 message 를 forwarding 할 DHCP server 를 선택하는데 사용된다. 아래의 명령어를 통해 DHCP relay-pool 을 설정할 수 있다.

명령어	설명
ip dhcp relay-pool WORD	<ul style="list-style-type: none"> ■ DHCP relay-pool 을 생성하고 “(dhcp-pool)#” 로 식별되는 DHCP relay-pool 모드로 진입 ■ WORD: relay-pool 의 이름 ■ relay-pool 을 삭제하려면 이 명령의 no 형식을 사용한다.
relay source A.B.C.D/M	<ul style="list-style-type: none"> ■ relay-pool 의 subnetwork 를 설정 ■ DHCP DISCOVER/REQUEST message 를 RX 한 interface 가 여기서 지정된 subnetwork 에 속하면 message 가 어떤 DHCP class 로 분류되는지 찾는다. ■ 이 명령의 no 형식을 사용하여 설정을 해제할 수 있다.
class class-name	<ul style="list-style-type: none"> ■ 이 relay-pool 에 설정된 server 로 message 가 forwarding 되려면 client 가 보낸 DHCP DISCOVER/REQUEST message 가 어떤 DHCP class 로 분류되어야 하는지 설정한다. ■ 하나이상의 class 를 지정할 수 있으며 해제하려면 이 명령의 no 형식을 사용한다.
relay target A.B.C.D/M	<ul style="list-style-type: none"> ■ DHCP DISCOVER/REQUEST message 를 forwarding 할 server 를 설정한다. ■ 이 명령의 no 형식을 사용하여 설정을 해제할 수 있다.

이전 예제에나온 “test” DHCP class 를 설정한후 다음 예제에서 나오는 DHCP relay-pool “test-pool”을 설정하면 DHCP relay agent 는 subnetwork ‘100.0.0.0/24’ 에 속한 IP address 를 가진 interface 가 RX 한 DHCP DISCOVER/REQUEST message 중 DHCP Option 77 을 가지고 그 option 값으로 ascii 문자열 “ubiquoss”를 포함한 message 를 DHCP server 200.0.0.254 로 forwarding 한다.

```
Router(config)# ip dhcp relay-pool test
Router(config-dhcp)# relay source 100.0.0.0/24
Router(config-dhcp)# exit
Router(config-dhcp)# class test
Router(config-class)# relay target 200.0.0.254
Router(config-class)# exit
Router(config)# service dhcp relay
```

6.3. DHCP Snooping 기능

6.3.1. DHCP Snooping 기능 개요

DHCP snooping 기능은 DHCP client와 DHCP server 간에 교환되는 DHCP message 들을 보고 DHCP server에서 생성되는 것과 유사한 address binding table을 작성한다. 이 binding table은 DAI에서 악의적인 사용자를 차단하기 위해 database로 사용된다. 또한 snoop은 설정에 따라 client-server 간에 주고받는 message를 통제할 수 있다. snoop은 DHCP relay agent와 같이 활성화될 수 있으며 DHCP server와는 같이 사용될 수 없다.

6.3.1.1. Trust and Untrust Source

DHCP Snooping은 traffic sources가 trusted인지 untrusted인지 구분한다. untrusted sources는 traffic 공격 또는 다른 적대적인 행동을 할지 모른다. 그러한 공격을 막기 위해, DHCP Snooping은 untrusted source로부터 message를 필터링할 수 있다.

6.3.1.2. DHCP Snooping Binding Database

DHCP Snooping은 DHCP Message를 가로챈 정보를 사용하여 database를 동적으로 만들고 유지한다. Database는 DHCP Snooping이 활성화되어 있는 Vlan의 untrusted host에 관한 entry를 포함한다. Database Entry는 DHCP server, Client로부터 받은 모든 DHCP message를 Validation check 후 추가하고, Validation check 값은 state 항목에 기록한다. 또한 동일한 DHCP client로부터 시작된 일련의 정상 DHCP message는 가장 최근의 message 1개만 Database Entry에 기록된다. IP Address lease time이 경과되거나 host로부터 DHCPRELEASE message를 받았을 때는 state 항목에 time expired, released로 기록되며, Database의 Entry가 최대값을 넘었을 때는 가장 오래된 Invalid Entry가 삭제되고, 새로운 Entry가 추가된다.

DHCP Snooping binding database는 host의 MAC Address, Client Hardware Address, Client Identifier, leased IP address, lease time, received time, State, Vlan ID, host가 연결된 interface port 정보를 포함한다.

6.3.1.3. Packet Validation

스위치는 DHCP Snooping이 활성화된 VLAN의 untrusted interface로부터 수신한 DHCP packet의 유효성을 검사한다. 스위치는 다음 상황이 발생하면, DHCP Snooping binding Table의 state 항목에 각각의 내용을 표시한다.

- 스위치가 untrusted interface로부터 source MAC address와 DHCP client Identifier 또는 DHCP client Hardware Address가 일치하지 않는 DHCPDISCOVER packet을 받는다.

6.3.1.4. Packet Rate-limit

DHCP Snooping 은 동일한 DHCP client 로부터 오는 DHCP Packet 에 대하여 Rate-limit 을 수행한다. DHCP Snooping 은 기본적으로 동일한 DHCP client 로부터 오는 동일한 타입의 DHCP Packet 을 초당 2 개까지 허용한다.

6.3.2. DHCP Snooping 기능의 활성화

기본적으로 스위치의 DHCP Snooping 의 기능은 비활성화 되어 있다. global 설정 mode 에서 다음의 명령어를 사용하여 DHCP Snooping 기능을 활성화 시킬 수 있다.



Notice DHCP Snooping 을 활성화할때도 relay agent 기능과 마찬가지로 class-map 과 policy-map 설정을 통해 DHCP packet 이 CPU 로 trap 되도록 해야 한다. 설정방법은 6.2.2 절을 참조하면 된다.

명령	설명
<code>ip dhcp snooping</code>	<ul style="list-style-type: none"> ■ 스위치의 DHCP Snooping 기능을 활성화 ■ DHCP Snooping 기능을 비활성화 하려면, 이 명령의 <code>no</code> 형태를 사용

다음의 예제는 DHCP Snooping 기능을 활성화 하는 예제이다.

```
Router# configure terminal
Router(config)# ip dhcp snooping
Router(config)# exit
Router# show ip dhcp snooping
Router DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 2 pps
Verification of hwaddr field is enabled
Insertion of option 82 is disabled
DHCP snooping is configured on following VLANs:
none
```

6.3.3. DHCP Snooping Vlan 설정

DHCP packet 을 Snooping 할 Vlan 을 설정한다. 설정된 Vlan 이외의 Vlan 을 통과하는 DHCP packet 은 Snooping 되지 않는다.

명령어	설명
<code>ip dhcp snooping vlan <i>vlan_ID</i></code>	<ul style="list-style-type: none"> ■ DHCP packet 을 Snooping 할 Vlan 설정 ■ DHCP Snooping Vlan 삭제는 이 명령의 <code>no</code> 형태를 사용



Notice DHCP Snooping 을 DHCP Relay 와 함께 사용할 경우, DHCP Relay 가 packet 을 forwarding 하게 된다.



Notice DHCP Snooping 을 DHCP Relay 와 함께 사용할 경우, DHCP server 와 연결된 vlan, DHCP client 와 연결된 vlan 양 쪽 모두 Snooping vlan 으로 지정해야 한다.

다음의 예제는 'vlan1'에 DHCP Snooping 기능을 활성화 하는 예제이다.

```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 1
Router(config)# exit
Router# show ip dhcp snooping
Router DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 2 pps
Verification of hwaddr field is enabled
Insertion of option 82 is disabled
DHCP snooping is configured on following VLANs:
vlan1
```

6.3.4. DHCP Snooping information option(OPTION82) 설정

DHCP Snooping 은 DHCP client 로부터의 DHCP request 를 Snooping 할 때, DHCP client 가 연결된 Interface 및 장비에 대한 정보를 포함할 수 있도록 DHCP Snooping information option 기능을 제공한다.

DHCP Snooping information option 기능의 활성화

E7508 Snooping 에서 information option 기능을 활성화시키기 위해서는 다음의 명령을 사용한다.

명령어	설명
ip dhcp snooping information option	<ul style="list-style-type: none"> DHCP Snooping information(option-82 field) 기능을 활성화 기본적으로, 이 특성은 비활성화 되어 있다.

다음의 예제는 DHCP Snooping Information Option 기능을 활성화 시킨다.

```
Router# configure terminal
Router(config)# ip dhcp snooping information option
Router(config)# exit
Router# show ip dhcp snooping
Router DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
```

```
DHCP Packet rate-limit per client: 2 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [drop]
DHCP snooping is configured on following VLANs:
vlan1
```

DHCP Snooping information option reforwarding 정책 설정

기본적으로, E7508 스위치의 DHCP Snooping information 정책은 DHCP client로부터 수신한 packet 내에 information Option 정보가 있으면 packet을 Drop 시킨다. E7508 스위치의 기본 정책을 변경하기 원한다면, global 설정 mode에서 다음의 명령을 사용한다.

명령어	설명
ip dhcp snooping information policy {drop keep replace}	<ul style="list-style-type: none"> ■ 기본 값은 drop 이다. ■ drop : DHCP Snooping information 이 삽입되어 있는 packet 은 폐기한다. ■ keep : 기존의 DHCP Snooping information 을 유지한다. ■ replace : 기존의 DHCP Snooping information 을 Premier router 의 DHCP Snooping information 으로 대체한다.

다음의 예제는 DHCP Snooping Information Option reforwarding 정책을 Keep 으로 설정한다.

```
Router# configure terminal
Router(config)# ip dhcp snooping information policy keep
Router(config)# exit
Router#
Router# show ip dhcp snooping
Router DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 2 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
vlan1
```

6.3.5. DHCP Snooping Trust Port 설정

네트워크 관리자가 신뢰할 수 있는 포트(ex, DHCP server 방향 포트)는 다음의 명령어를 사용하여 Trust Port 로 설정한다. Trust Port 를 설정하면 Host 로부터의 Request packet 이 Trust Port 로만 forwarding 된다.

명령어	설명
ip dhcp snooping trust	<ul style="list-style-type: none"> 지정된 포트를 Trust Port 로 설정한다. Trust Port 에서 수신한 DHCP packet 은 Validation check 하지 않는다. Host 로부터의 Request packet 이 Trust Port 로만 forwarding 된다. 기본적으로, 모든 포트는 untrust 포트이다.

다음은 포트 'gi1/1/1'을 Trust Port 로 설정하는 예제이다.

```
Router(config)# interface gi1/1/1
Router(config-if-Gigal/1/1)# ip dhcp snooping trust
Router(config-if-Gigal/1/1)# end
Router# show ip dhcp snooping interface
```

Interface	Trust State	Max Entry
Gigal/1/1	Trusted	2000

6.3.6. DHCP Snooping max-entry 설정

포트별로 DHCP Snooping max-entry 개수를 설정하기 위해 다음과 같은 명령을 사용한다.

명령어	설명
ip dhcp snooping max-entry <10-10000>	<ul style="list-style-type: none"> 포트별로 DHCP Snooping max-entry 개수를 설정한다. 단, Max entry 개수를 초과하여 binding entry 가 생겨도 기존 entry 중 valid(현재 IP 를 사용중인)한 entry 는 삭제하지 않는다. 기본적으로, 포트별 Max-entry 개수는 2000 개이다.

다음은 'gi1/1/1'의 DHCP Snooping Max-Entry 를 '100'개로 설정하는 예제이다.

```
Router# configure terminal
Router(config)# interface gi1/1/1
Router(config-if-Gigal/1/1)# ip dhcp snooping max-entry 100
Router(config-if-Gigal/1/1)# end
Router# show ip dhcp snooping interface
```

Interface	Trust State	Max Entry
Gigal/1/1	Trusted	100

6.3.7. DHCP Snooping Entry Time 설정

Invalid(현재 IP 를 사용하고 있지 않는)한 DHCP Snooping Binding Entry 를 저장하고 있는 시간을 설정하기 위해 다음의 명령을 사용한다.

명령어	설명
ip dhcp snooping entry-time <5-65535>	<ul style="list-style-type: none"> Invalid(IP 를 현재 사용하고 있지 않는)한 DHCP Snooping Binding Entry 를 저장하고 있는 시간을 설정한다. 단위는 분이다. 기본적으로, 14400 분(10 일)으로 설정된다.

다음의 예제는 DHCP Snooping 의 Entry Time 을 '10 분'으로 설정하는 예제이다.

```
Router# configure terminal
Router(config)# ip dhcp snooping entry-time 10
Router(config)# exit
Router# show ip dhcp snooping
Router DHCP Snooping is enabled
Invalid entry keep time: 10 mins
DHCP Packet rate-limit per client: 100 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
vlan1
```

6.3.8. DHCP Snooping Rate-Limit 설정

동일한 DHCP client 로부터 전송되는 DHCP Packet 의 Rate-limit 를 설정하기 위해 다음의 명령어를 사용한다.

명령어	설명
ip dhcp snooping rate-limit	<ul style="list-style-type: none"> 매 1 초당 동일한 DHCP client 로부터 Packet type 이 같은 DHCP Packet 의 허용 개수를 설정한다. 기본적으로, 초당 2 개의 packet 을 허용한다.

다음 예제는 DHCP Snooping Rate-Limit 를 '100'으로 설정하는 예제이다.

```
Router# configure terminal
Router(config)# ip dhcp snooping rate-limit 100
Router(config)# end
Router#
Router# show ip dhcp snooping
Router DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 100 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
```



```
vlan1
```

6.3.9. DHCP Snooping Verify MAC-Address 설정

DHCP client Identifier 또는 Client HW Address 가 변조된 경우, 이 packet 을 Drop 시키기 위해 다음 명령어를 사용한다.

명령어	설명
ip dhcp snooping verify mac-address	<ul style="list-style-type: none"> ■ DHCP client Identifier 또는 Client HW Address 가 변조된 경우, 이 packet 을 Drop 시킨다. ■ 기본적으로, 이 특성은 활성화 되어 있다.

다음의 예제는 DHCP Snooping Verify Mac-Address 기능 설정을 해제한다.

```
Router# configure terminal
Router(config)# no ip dhcp snooping verify mac-address
Router(config)# exit
Router# show ip dhcp snooping
Router DHCP Snooping is enabled
Invalid entry keep time: 10 mins
DHCP Packet rate-limit per client: 100 pps
Verification of hwaddr field is disabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
vlan1
```

6.3.10. DHCP Snooping Manual Binding 설정

DHCP Snooping Binding Entry 를 수동으로 설정하기 위해 다음과 같은 명령어를 사용한다.

명령어	설명
ip dhcp snooping binding H.H.H vlan <1-4094> A.B.C.D interface IFNAME	<ul style="list-style-type: none"> ■ MAC-Address 가 H.H.H인 DHCP client 를 지정된 Interface 에서 IP A.B.C.D 를 사용하며, lease time 은 Infinite 이다.

다음은 MAC 이 1111.2222.3333 인 가입자가, Vlan 1 의 gi1/1/1 포트에 연결되어 IP 100.0.0.10 을 사용하는 예제이다.

```
Router# configure terminal
Router(config)# ip dhcp snooping binding 1111.2222.3333 vlan 1 100.0.0.10
interface gi1/1/1
Router(config)# exit
Router#
```

```

Router#
Router# show ip dhcp snooping binding
State Codes: (C) - Invalid Client Identifier, (E) - Lease Time Expired
              (H) - Invalid Client HW Address, (R) - Rate Limit Dropped
              (M) - Mac Validation Check Dropped

Mac Address      IP Address      State              Lease(sec)  interface
-----
1111.2222.3333  100.0.0.10     Manual             Infinite    Gigal/1/1
total 4 bindings found

```

6.4. DHCP server 모니터링 및 관리

DHCP server Pool 정보 조회

DHCP server 에 생성된 DHCP Address Pool 정보를 조회하려면, **privileged EXEC mode** 에서 다음의 명령을 사용한다.

명령	목적
show ip dhcp pool	▪ DHCP server 의 DHCP Address Pool 정보를 출력
show ip dhcp pool pool [name]	▪ DHCP server 의 Network Pool 내의 정보 출력

DHCP server 바인딩 정보 조회

DHCP server 에서 Client 에게 제공한 Address 의 바인딩 정보를 조회하려면, **privileged EXEC mode** 에서 다음의 명령을 사용한다.

명령	목적
show ip dhcp binding	▪ DHCP server 에 생성된 모든 바인딩을 출력
show ip dhcp binding detail	▪ DHCP server 에 생성된 모든 바인딩을 좀 더 상세한 형태로 출력

DHCP server 통계 정보 조회

명령	목적
show ip dhcp server statistics	▪ Server 의 통계와 송수신한 message 와 관련된 카운터 정보를 출력

DHCP server 충돌 정보 조회

명령어	목적
<code>show ip dhcp conflict {poolname}</code>	<ul style="list-style-type: none"> DHCP server 에 의해 기록된 모든 Address 충돌을 출력 특정 Pool 에서 발생한 충돌 정보 출력

DHCP server 변수 초기화 명령어

명령어	설명
<code>clear ip dhcp binding {address *}</code>	<ul style="list-style-type: none"> DHCP 데이터베이스로부터 자동 Address 바인딩을 삭제 <code>address</code> 를 명시하면 명시된 IP Address 의 자동 바인딩을, "*"를 사용하면 모든 자동 바인딩을 삭제
<code>clear ip dhcp server statistics</code>	<ul style="list-style-type: none"> DHCP server 의 모든 통계 카운터를 초기화

DHCP server 디버그 명령어

명령어	설명
<code>debug ip dhcp server on</code>	<ul style="list-style-type: none"> DHCP server 의 디버깅 기능을 활성화

6.5. DHCP relay 모니터링 및 관리

표 5. DHCP relay 모니터링 및 관리 명령어

명령어	설명
<code>show ip dhcp helper-address</code>	<ul style="list-style-type: none"> DHCP server 의 목록을 출력
<code>show ip dhcp relay agent information option</code>	<ul style="list-style-type: none"> DHCP relay agent information option 의 활성화 및 reforwarding 정책을 출력
<code>show ip dhcp relay statistics</code>	<ul style="list-style-type: none"> relay 의 통계와 송수신한 message 와 관련된 카운터 정보를 출력
<code>debug ip dhcp relay {events packets}</code>	<ul style="list-style-type: none"> DHCP relay 의 디버깅 기능을 활성화

6.6. DHCP Snooping 모니터링 및 관리

DHCP Snooping 모니터링 및 관리 명령어

명령어	설명
-----	----

show ip dhcp snooping	■ global DHCP Snooping Configuration 을 출력
show ip dhcp snooping binding {IFNAME valid invalid manual}	■ DHCP Snooping Binding Entry 를 출력
show ip dhcp snooping interface	■ Interface 에 설정된 DHCP Snooping Configuration 을 출력
show ip dhcp snooping statistics	■ DHCP Snooping 통계 정보를 출력
show debugging ip dhcp snooping	■ DHCP Snooping debugging 설정 상태를 출력
debug ip dhcp snooping	■ DHCP Snooping 디버깅 기능을 활성화

6.7. DHCP 설정 예제

이 절에서는 다음의 설정 예를 제공한다.

- DHCP Network Pool 설정 예제
- DHCP Host Pool 설정 예제
- DHCP server 모니터링 및 관리 예제
- DHCP relay agent 설정 예제
- DHCP relay agent 모니터링 및 관리 예제

6.7.1. DHCP Network Pool 설정 예제

다음 예제는 192.168.1.0/24 인터페이스에 대한 DHCP Network Pool 을 생성과정이다. Client 의 기본 라우터는 192.168.1.1 로 설정되며, 도메인 이름으로 ubiquoss.com 을 사용한다. Client 의 IP Address 는 하루 동안 임대된다. 할당 Address 범위는 192.168.1.10~192.168.1.100 과 192.168.1.150~192.168.1.230 이다.

```
Router(config)# configure terminal
Router(config)# ip dhcp pool marketing
Router(config-dhcp)# domain-name ubiquoss.com
Router(config-dhcp)# lease 1
Router(config-dhcp)# network 192.168.1.0/24
Router(config-dhcp)# default-router 192.168.1.1
Router(config-dhcp)# range 192.168.1.10 192.168.1.100
Router(config-dhcp)# range 192.168.1.150 192.168.1.230
```

다음의 예제는 하나의 vlan 이 192.168.2.0/24 와 192.168.3.0/24 를 갖는 인터페이스에 대한 Network Pool 및 그룹 설정 과정이다. 192.168.2.0/24 Network 의 default-router 는 192.168.2.1 이며, 할당 Address 범위로 192.168.2.10~192.168.2.240 을 사용하며, 192.168.3.0/24 Network 의 default-router 는

192.168.3.1 이며, 할당 Address 범위는 192.168.3.10~192.168.3.50 과 192.168.3.100~192.168.3.230 을 사용한다. 그리고, DNS Server 는 모두 1.2.3.4 와 1.2.3.5 를 사용한다. 각 Client 는 IP Address 의 임대를 12 시간까지 보장 받는다.

```
Router(config)# configure terminal
Router(config)# ip dhcp pool sales1
Router(config-dhcp)# dns-server 1.2.3.4 1.2.3.5
Router(config-dhcp)# lease 0 12
Router(config-dhcp)# network 192.168.2.0/24
Router(config-dhcp)# default-router 192.168.2.1
Router(config-dhcp)# range 192.168.2.10 192.168.2.240
Router(config-dhcp)# group vlan10
Router(config-dhcp)# exit
Router(config)# ip dhcp pool sales2
Router(config-dhcp)# dns-server 1.2.3.4
Router(config-dhcp)# dns-server 1.2.3.5
Router(config-dhcp)# lease 0 12
Router(config-dhcp)# network 192.168.3.0/24
Router(config-dhcp)# default-router 192.168.3.1
Router(config-dhcp)# range 192.168.3.10 192.168.3.50
Router(config-dhcp)# range 192.168.3.100 192.168.3.230
Router(config-dhcp)# group vlan10
Router(config-dhcp)# exit
```

6.7.2. DHCP Host Pool 설정 예제

다음 예는 192.168.4.0/24 Network 에 속하는 Host Pool 의 구성을 보여준다. default-router 로 192.168.4.1 사용하며, ubiquoss.com 을 domain name 으로, 192.168.4.10 과 192.168.4.11 을 dns-server 로 사용하는 Client 들을 위한 Host Pool 이다. 그리고, Client 의 MAC Address 가 00:01:02:94:77:d7 인 Client 에게 192.168.4.114 의 IP Address 와 255.255.255.0 의 Network 마스크가 할당된다. 수동 바인딩으로 할당된 IP Address 는 영구적으로 사용된다.

```
Router(config)# ip dhcp pool mars
Router(config-dhcp)# default-router 192.168.4.1
Router(config-dhcp)# dns-server 192.168.4.10
Router(config-dhcp)# dns-server 192.168.4.11
Router(config-dhcp)# domain-name ubiquoss.com
Router(config-dhcp)# host 192.168.4.114/13
Router(config-dhcp)# hardware-address 00:01:02:94:77:d7
Router(config-dhcp)# exit
```



Notice

수동 바인딩으로 설정된 Client 에게는 항상 동일한 IP Address 가 할당된다.

6.7.3. DHCP server 모니터링 및 관리 예제

다음은 DHCP server 에 생성된 DHCP Address Pool 정보를 출력하는 예제이다.

```
shu# show ip dhcp pool
Pool network :
network: 44.1.1.0/24
address range(s):
  add: 44.1.1.1 to 44.1.1.200
lease <days:hours:minutes> <0:0:1>
no domain is defined
no dns-servers
no default-routers

Pool host:
host 3.1.1.1/24
hardware Ethernet 11:11:11:11:11:11
no domain is defined
no dns-servers
no default-routers
shu#
```



Notice

show running-config 명령을 사용하면 운영자가 설정한 모든 정보를 볼 수 있다.

다음은 DHCP server 가 Client 에게 할당한 IP Address 를 보여주는 예제이다.

```
Router# show ip dhcp binding
IP address      Hardware address  Lease expiration  Type
192.168.4.114   00:01:02:94:77:d7 Infinite          Maunal
192.168.3.10    02:c7:f8:00:04:22 Wed Mar 12 06:27:39 2003 Automatic
```

다음은 DHCP server 가 Client 에게 할당한 IP Address 를 자세히 보여주는 예제이다.

```
Router(Config)# show ip dhcp binding detail
-----
TYPE                : Manual
IP addr             : 192.168.4.114
HW addr             : 00:01:02:94:77:d7
Client ID           : -
Host Name           : -

Lease                : Infinite
-----
```

```

TYPE                : Manual
IP addr             : 192.168.4.115
HW addr             : 00:01:02:94:77:d8
Client ID           : -
Host Name           : -
Lease               : Infinite

```

```

-----
TYPE                : Manual
IP addr             : 192.168.4.116
HW addr             : 00:01:02:94:77:d9
Client ID           : -
Host Name           : -
Lease               : Infinite

```

```

-----
total 3 bindings found

```

다음은 Client에게 이미 바인딩된 IP Address를 DHCP server가 사용할 수 있도록(다른 Client의 IP Address로 사용하도록 시도), DHCP server의 바인딩 정보를 삭제하는 예제이다..

```

Router(Config)# clear ip dhcp binding 192.168.3.10
Router(Config)# show ip dhcp binding
IP address          Hardware address      Lease expiration      Type
192.168.4.114      00:01:02:94:77:d7      Infinit               Maunal

```

다음은 DHCP server의 통계자료를 보여주는 예제이다.

```

Router# show ip dhcp server statistics
Message                               Received
Malformed messages                    0
BOOTREQUEST                           0
DHCPDISCOVER                          200
DHCPREQUEST                           178
DHCPDECLINE                           0
DHCPRELEASE                           0
DHCPINFORM                            0
ICMPECHO
Message                               Sent
BOOTREPLY                             0
DHCPOFFER                             190
DHCPACK                               172
DHCPNAK                               6

```

6.7.4. DHCP relay agent 설정

다음의 예제는 스위치의 DHCP relay agent가 Client의 요구를 전달한 DHCP server를 설정하는 예제이다. Client의 요구를 만족시키는 DHCP Address Pool이 없을 경우 스위치는 다른 서브 Network

에 위치한 DHCP server 로 Client 의 요구를 전달한다.

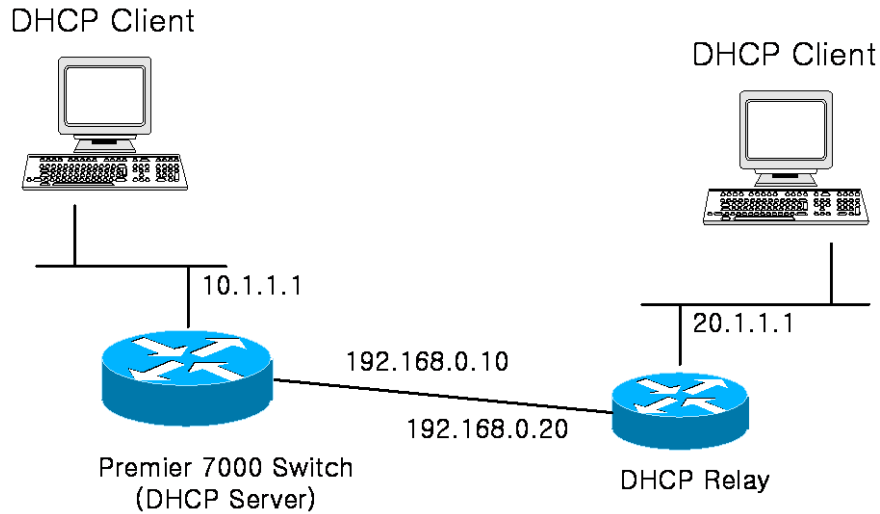


그림 3. 예제 Network – DHCP Relay agent 환경 설정

```
Router(config)# configure terminal
Router(config)# ip dhcp-server 10.1.1.2
Router(config)# service dhcp relay
Router (config)# end
Router# show ip dhcp helper-address
Server's IP address : 10.1.1.2
Router #
Router # show ip dhcp relay statistics
```

```
Destination(Server)    Value
Client-packets relayed  8
Client-packets errored  0
```

```
Destination(Client)    value
Server-packets relayed  6
Server-packets errored  0
Giaddr errored         0
Corrupt agent options  0
Missing agent options  0
Bad circuit id         0
Missing circuit id     0
```



Notice

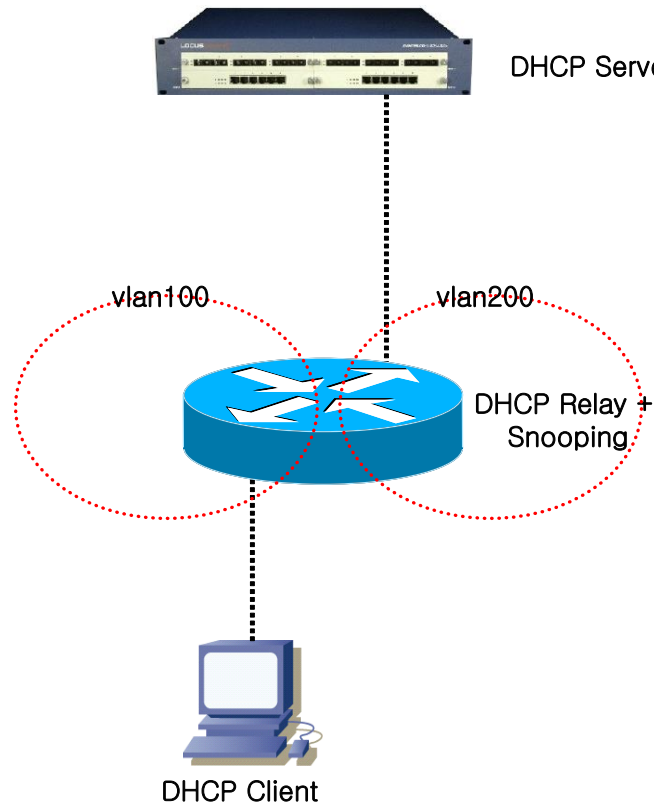
다른 서브 Network 에 위치한 DHCP server 로 DHCP message 를 전달하려 면, 해당 Network 에 대한 라우팅 경로 정보가 설정되어 있어야 한다.

Client-packets relayed	DHCP client 가 TX 한 packet 을 DHCP server 로 forwarding 하는데 성공함
Client-packets errored	DHCP client 가 TX 한 packet 을 DHCP server 로 forwarding 하는데 실패함
Server-packets relayed	DHCP server 가 TX 한 packet 을 DHCP client 로 forwarding 하는데 성공함
Server-packets errored	DHCP server 가 TX 한 packet 을 DHCP client 로 forwarding 하는데

	실패함
Giaddr errored	DHCP server로부터 RX 한 DHCP Packet 에 giaddr 가 없음
Corrupt agent options	DHCP relay agent 또는 snoop의 DHCP information option 삽입 기능이 enable 되어 있을 때, DHCP server로부터 RX 한 DHCP packet의 Option82 정보에 오류가 있음(DHCP Option82의 Length field값과 실제 DHCP Option82 Length 가 서로 다름)
Missing agent options	DHCP relay agent 또는 snoop의 DHCP information option 삽입 기능이 enable 되어 있을 때, DHCP server로부터 RX 한 DHCP packet에 Option82 정보가 없음
Bad circuit id	DHCP relay agent 또는 snoop의 DHCP information option 삽입 기능이 enable 되어 있을 때, DHCP server로부터 RX 한 DHCP packet Option82 정보 중 circuit id(가입자 Interface 정보)에 오류가 있음 (DHCP packet에 있는 option82 의 circuit id를 통해 장비에서 circuit id에 해당하는 port를 찾을수 없음.)
Missing circuit id	DHCP relay agent 또는 snoop의 DHCP information option 삽입 기능이 enable 되어 있을 때, DHCP relay(snoop)은 이전에 DHCP Request packet을 받았을 때 RX한 port에 해당하는 circuit id를 buffering하는데 이 buffer에 없는 circuit id를 포함한 DHCP packet을 DHCP server로부터 받았다.

6.7.5. DHCP Snooping 설정 예제

다음 예제는 DHCP Server 와 DHCP Client 사이에 위치한 E7508 를 DHCP Snoop 으로 사용한 예제이다. Premier 8700 DHCP Snoop 은 Switch 를 통하는 DHCP 패킷을 Snooping 하여 DHCP Snooping Binding Entry 를 생성한다. 예제 화면은 gi1/1/1 port 에 물린 DHCP Client(0000.864a.c185) 가 DHCP Server 100.0.0.254 로 DHCP Request 패킷을 보내 IP 100.0.0.100 을 받은것을 보여준다.



```
Router# configure terminal
Router(config)# ip dhcp snooping vlan 100
Router(config)# ip dhcp snooping vlan 200
Router(config)# ip dhcp snooping
Router(config)# ip dhcp-server 100.0.0.254
Router(config)# service dhcp relay
Router# show ip dhcp snooping binding
State Codes: (C) - Invalid Client Identifier, (E) - Lease Time Expired
              (H) - Invalid Client HW Address, (D) - Rate Limit Dropped

   MacAddress      IpAddress      State      Lease(sec)   VlanId      Port
   -----      -
0000.864a.c185    100.0.0.100    Ack        87           100         Giga1/1/1
```

7 RIP

(Routing Information Protocol)

이 장에서는 RIP (Routing Information Protocol)를 설정하는 방법에 대해 설명한다. RIP는 오래된 방법이지만 여전히 규모가 작은 네트워크의 IGP (Interior Gateway Protocol)로 사용된다.

7.1. Information about RIP

RIP는 오래되었지만 여전히 작은 네트워크에서 사용되는 interior gateway protocol이다. RIP는 고전적인 distance-vector 방식의 라우팅 프로토콜이다.

RIP는 라우팅 정보를 교환하기 위하여 User Datagram Protocol (UDP) 데이터 패킷을 브로드캐스트하는 방식을 사용한다. 기본적으로 라우팅 정보는 30초마다 advertisement 된다. 만약 스위치가 180초 혹은 그 이상의 시간동안 다른 스위치로부터 업데이트를 수신하지 못할 경우, 이는 쓸모없는 스위치에서 제공된 라우트 정보라고 표시를 해둔다. 만약 240초 이후까지 여전히 업데이트가 없을 경우 스위치는 이 라우팅 엔트리를 모두 제거한다.

RIP에서 사용하는 metric은 hop count이다. Hop count는 라우트까지 지나는 라우터의 수이다. Connected 네트워크는 0의 metric 값을 가지고 도달 불가능한 라우트의 metric은 16 값을 가진다, 이처럼 작은 metric 범위를 사용하기 때문에 큰 네트워크를 위한 라우팅 프로토콜로는 부적합하다.

스위치는 다른 장비로부터의 update를 통하여 default 네트워크를 수신할 수도 있고 default 네트워크를 생성할 수도 있다. 이러한 경우에, default 네트워크는 RIP와 다른 RIP neighbor를 통하여 advertisement 된다.

7.2. How to Configure RIP

RIP를 설정하기 위해서는 다음 장에서 설명되어 있는 작업을 수행하라.

- Enabling RIP
- Allowing Unicast Updates for RIP
- Passive interface
- Applying Offsets to Routing Metrics
- Adjusting Timers
- Specifying a RIP version
- Applying Distnace
- Enabling Split Horizon

7.2.1. Enabling RIP

RIP 를 동작시키려면 다음과 같이 설정하면 된다.

	Command or Action	Purpose
Step 1	Configure terminal 예제: Switch# configure terminal	Global configuration 모드로 진입한다
Step 2	router rip 예제: Switch(config)# router rip	RIP 라우팅 설정 모드로 진입한다.
Step 3	network ip-address/prefix-len 예제: Switch(config-router)# network 33.1.1.0/24	RIP 를 통하여 다른 라우터에게 광고하려는 네트워크를 지정한다.
Step 4	end 예제: Switch(config-router)# end	privileged EXEC 모드로 돌아간다

7.2.2. Allowing Unicast updates for RIP

일반적으로 RIP 는 broadcast 프로토콜이기 때문에, RIP 라우팅 을 nonbroadcast 네트워크로 도달하게 update 를 하려면, 다음의 명령을 router configuration mode 에서 실행해야 한다.

Command or Action	Purpose
neighbor ip-address 예제: Switch(config-router)# neighbor 3.3.3.2	라우팅 정보를 교환할 Neighboring 을 맺을 스위치를 정의한다.

7.2.3. Passive interface

Update 라우팅 정보를 교환하는 특정 인터페이스의 update 라우팅 정보의 전송을 **disable** 할 수 있다. **passive-interface** 명령을 router configuration 모드에서 사용한다.

Command or Action	Purpose
passive-interface IFNAME 예제: Switch(config-router)# passive-interface gi2/1/1	Passive interface 를 설정한다.

7.2.4. Applying Offsets to Routing metrics

Offset list 는 RIP 를 통해 얻은 라우트에 대한 incoming 과 outgoing metric 을 증가시키기 위한 메커니즘이다. Access list 과 offset list 로 조절할 수 있다. 라우팅 metric 의 값을 증가시키기 위해서는 router configuration 모드에서 다음의 명령을 사용하라.

Command or Action	Purpose
offset-list access-list-name {in out} metric IFNAME 예제: Switch (router-config)# offset-list aa in 5 gi2/1/1	라우팅 metric 에 offset 을 적용한다.

7.2.5. Adjusting Timers

라우팅 프로토콜은 여러가지의 타이머를 사용한다. 네트워크 관리자는 관리하는 네트워크에 적합하도록 라우팅 프로토콜 수행능력을 변경하는 타이머 값을 조정할 수 있다. 다음의 타이머 조정을 할 수 있다.

- Routing table update timer (default 30 초)
- Routing information timeout timer (180 초)
- Garbage collection timer (120 초)

Timer 값을 조정하기 위해서는 router configuration 모드에서 다음의 명령을 사용하라.

Command or Action	Purpose
timer basic update invalid holddown 예제: Switch(config-router)# timer basic 30 120 120	라우팅 프로토콜 타이머값을 조정한다.

7.2.6. Specifying a RIP Version

한 버전으로 패킷을 송수신 하도록 설정하기 위해서는 **router configuration** 모드에서 다음의 명령을 수행하여야 한다.

Command or Action	Purpose
version {1 2}	RIP의 버전을 변경하여 설정한다.
예제: Switch(config-router)# version 2	

특정 인터페이스에서 전송하는 RIP 버전을 조정하기 위해서는 인터페이스의 **configuration** 모드에서 다음의 명령을 사용한다.

Command or Action	Purpose
ip rip send version VERSION	인터페이스는 오직 RIP 해당 버전 패킷만 전송하도록 설정한다.
예제: Switch(config-if-Giga2/1/1)# ip rip send version 1 Switch(config-if-Giga2/1/1)# ip rip send version 2 Switch(config-if-Giga2/1/1)# ip rip send version 1 2	Note version 1 과 2 를 설정 했을 경우, version 1 2 를 모두 지원한다.

인터페이스로 수신할 패킷의 버전을 제어하기 위해서는, 다음의 명령을 인터페이스 **configuration** 모드에서 실행한다.

Command or Action	Purpose
ip rip receive version VERSION	인터페이스는 오직 RIP 해당 버전 패킷만 수신 하도록 설정한다.
예제: Switch(config-if-Giga2/1/1)# ip rip receive version 1 Switch(config-if-Giga2/1/1)# ip rip receive version 2 Switch(config-if-Giga2/1/1)# ip rip receive version 1 2	Note version 1 과 2 를 설정 했을 경우, version 1 2 를 모두 지원한다.

7.2.7. Applying Distance

Administrative distance 는 routing information source 에 대한 신뢰성 정도를 나타낸다. 일반적으로 큰 값이 낮은 신뢰도를 의미한다. RIP 의 Administrative distance 기본값은 120 이다.

Administrative distance 값을 조정하기 위해서는 **router configuration** 모드에서 다음의 명령을 사용하라.

Command or Action	Purpose
distance VALUE A.B.C.D/M 예제: Switch(config-router)# distance 90 10.1.1.1/24	Administrative distance 값을 변경한다.

10.1.1. Enabling Split Horizon

Distance-vector 라우팅은 라우팅 loop 의 가능성을 줄이기 위하여 **split horizon** 메커니즘을 함께 사용한다. Split horizon 을 enable 하려면 다음과 같은 명령을 interface configuration 모드에서 수행한다.

Command or Action	Purpose
ip rip split-horizon [poisoned] 예제: Switch(config-if-Giga2/1/1)# ip rip split-horizon poisoned	Split horizon poisoned 를 enable 한다.

7.3. Configuration Examples for RIP

7.3.1. RIP 구성

그림 1 과 같은 네트워크 구성도를 통하여 RIP 프로토콜의 구성 예를 살펴본다.

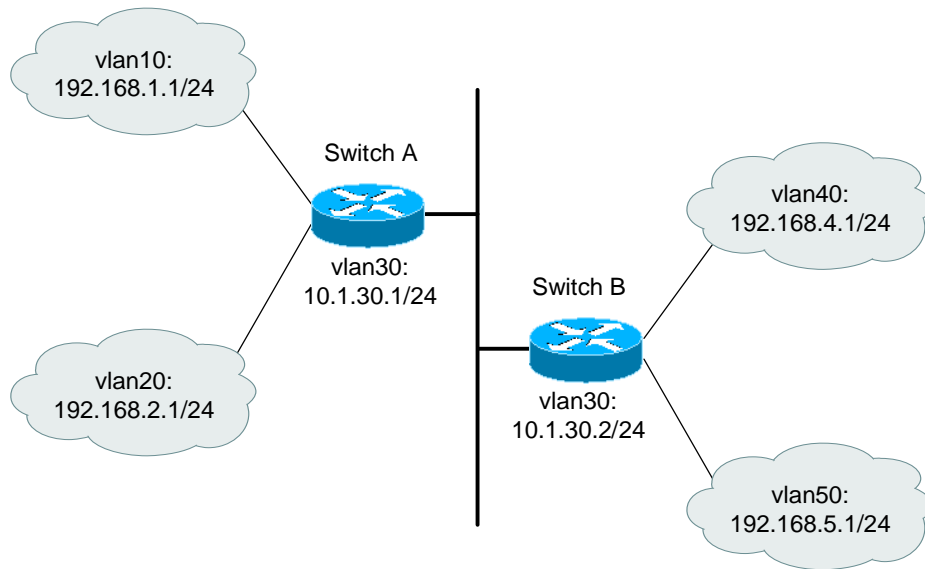


그림 7-1 RIP 를 설정한 네트워크 예제 설정 및 구성도

Switch A	Switch B
vlan10 192.168.1.1/24	vlan30 10.1.30.2/24
vlan20 192.168.2.1/24	vlan40 192.168.4.1/24
vlan30 10.1.30.1/24	vlan50 192.168.5.1/24

설정된 각 인터페이스에 RIP 프로토콜을 활성화 시키기 위해 다음의 명령을 이용한다.

Switch A 설정

```
Switch A(config)# router rip
Switch A(config-router)# network 192.168.1.1/24
Switch A(config-router)# network 192.168.2.1/24
Switch A(config-router)# network 10.1.30.1/24
Switch A(config-router)# end
Switch A# show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

C>* 10.1.30.0/24 is directly connected, vlan30
C>* 192.168.1.0/24 is directly connected, vlan10
C>* 192.168.2.0/24 is directly connected, vlan20
R> 192.168.4.0/24 [120/1] via 10.1.30.2, vlan30, 00:01:42
R>* 192.168.5.0/24 [120/1] via 10.1.30.2, vlan30, 00:01:42
Switch A#
```

Switch B 설정

```
Switch B(config)# router rip
Switch B(config-router)# network 192.168.4.1/24
Switch B(config-router)# network 192.168.5.1/24
Switch B(config-router)# network 10.1.30.2/24
Switch B(config-router)# end
Switch B# show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

C>* 10.1.30.0/24 is directly connected, vlan30
R>* 192.168.1.0/24 [120/1] via 10.1.30.1, vlan30, 00:02:13
R>* 192.168.2.0/24 [120/1] via 10.1.30.1, vlan30, 00:02:13
C>* 192.168.4.0/24 is directly connected, vlan40
C>* 192.168.5.0/24 is directly connected, vlan50
Switch B#
```

7.3.2. Offset-list 설정

이제 **offset-list** 를 이용하여 스위치 A 로 들어오는 모든 **incoming RIP** 루트의 **metric** 값을 2 증가 시켜 보자.

```
Switch A(config)# router rip
Switch A(config-router)# offset-list 4 in 2
Switch A(config-router)# exit
Switch A(config)# access-list 4 permit any
Switch A(config)# end
Switch A# show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

C>* 10.1.30.0/24 is directly connected, vlan30
C>* 192.168.1.0/24 is directly connected, valn10
C>* 192.168.2.0/24 is directly connected, vlan20
R> 192.168.4.0/24 [120/3] via 10.1.30.2, vlan30, 00:06:26
R>* 192.168.5.0/24 [120/3] via 10.1.30.2, vlan30, 00:29:04
Switch A#
```

위에서 보듯이 192.168.4.0 과 192.168.5.0 의 **metric** 값이 3 으로 증가 되었음을 알 수 있다. 물론 **distribute-list** 와 같이 **outgoing** 도 설정이 가능하다.

7.3.3. Passive-interface 설정

이 명령을 스위치의 특정 인터페이스에 적용시키면 해당 인터페이스는 **outgoing** 되는 경로를 광고하지 않는다. 예를 들면 예제 네트워크에서 스위치 A 의 **vlan30** 에 **passive-interface** 를 설정하면 스위치 A 는 모든 경로를 받지만 스위치 B 는 스위치 A 가 **vlan30** 에서 보내주는 모든 경로를 **update** 받지 못한다.

```
Switch A(config)# router rip
Switch A(config-router)# passive-interface vlan30
Switch A(config-router)# end
Switch A# show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info
```

```
C>* 10.1.30.0/24 is directly connected, vlan30
C>* 192.168.1.0/24 is directly connected, vlan10
C>* 192.168.2.0/24 is directly connected, vlan20
R> 192.168.4.0/24 [130/1] via 10.1.30.2, vlan30, 00:14:28
R>* 192.168.5.0/24 [120/1] via 10.1.30.2, vlan30, 00:37:06
Switch A#
```

```
Switch B# show ip route database
```

```
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
```

```
O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```
> - selected route, * - FIB route, p - stale info
```

```
C>* 10.1.30.0/24 is directly connected, vlan30
C>* 192.168.4.0/24 is directly connected, vlan40
C>* 192.168.5.0/24 is directly connected, vlan50
Switch B#
```

8

OSPF

본 장에서는 E7500 Series 스위치에서 사용 되는 OSPF 라우팅 프로토콜에 대해서 기술한다. OSPF 라우팅 프로토콜은 RFC 2328 에 서술되어 있다.

8.1. OSPF 개요

OSPF 는 하나의 IP 도메인 (Autonomous System, AS)에 속하는 라우터들 간에 라우팅 정보를 분배하는 link-state 라우팅 프로토콜의 일종이다. Link-state 라우팅 프로토콜에서는 각 라우터가 autonomous system 의 토폴로지에 대한 데이터베이스를 유지한다. 그리하여 각 라우터는 모두 동일한 데이터베이스를 가지게 된다.

Link-state DB (LSDB)로부터 각 라우터는 자신을 루트로 하는 최단 경로의 트리를 생성하게 된다. 이 최단 경로 트리는 AS 내의 각 목적지에 대한 경로를 제공한다. 하나의 목적지에 대하여 비용이 동일한 여러 경로가 있으면, 트래픽은 이 경로들로 분배 된다. 경로의 비용은 하나의 metric 에 의해 표현 된다.

8.1.1. Link-state Database

초기화 시, 각 라우터는 자신의 인터페이스 각각에 대한 link state advertisement (LSA)를 전송한다. LSA는 각 라우터에 의해서 수집되며 각 라우터의 LSDB에 들어가게 된다. OSPF는 라우터간에 LSA를 분배하기 위해서 flooding 알고리즘을 사용한다. 라우팅 정보의 변화는 네트워크의 모든 라우터들에게 전송된다.. 하나의 area 내의 모든 라우터들은 정확히 동일한 LSDB를 가진다. 다음 <표 8-1>는 LSA type number를 나타낸다.

표 8-1. LSA Type number

Type Number	Description
1	Router link
2	Network link
3	Summary link
4	AS summary link
5	AS external link
7	NSSA external link

8.1.2. Areas

OSPF에서는 네트워크의 각 부분들이 하나의 area들로 뭉쳐질 수 있다. 한 area 내에서의 토폴로지는 autonomous system 내의 나머지 area와 분리되어 감추어진다. 이 정보를 감추는 것은 LSA 트래픽의 상당한 감소를 가능하게 하며, 또한 LSDB를 유지하기 위해 필요한 계산을 감소시킨다. Area 내에서의 라우팅은 그 area 내의 토폴로지에 의해서만 결정된다.

OSPF에서는 다음과 같은 세가지 종류의 라우터를 정의한다.

- ✓ **Internal Router (IR)**
라우터의 모든 인터페이스가 동일한 area 내에 포함되는 라우터.
- ✓ **Area Border Router (ABR)**
여러 area에 인터페이스를 가지고 있는 라우터. 다른 ABR들과 summary advertisement를 교환하는 역할을 담당한다.
- ✓ **Autonomous System Border Router (ASBR)**
OSPF와 다른 라우팅 프로토콜, 또는 다른 Autonomous System과의 게이트웨이의 역할을 담당하는 라우터.

AREA 0

하나 이상의 area를 포함하고 있는 OSPF 네트워크는 백본(backbone)이라 불리는 area 0로 설정된 area를 반드시 가지고 있어야 한다. Autonomous system의 모든 area들은 반드시 백본에 연결이 되어야 한다. 네트워크를 설계할 때, area 0로 시작하여 다른 area들을 확장 시켜 나가야 한다.

백본은 ABR 들 사이에 **summary information** 이 교환될 수 있도록 한다. 모든 ABR 들은 다른 모든 ABR 로부터의 **summary** 정보를 듣는다. ABR 은 수집된 **advertisement** 를 살펴보아서 자신이 속한 **area** 외부의 모든 네트워크까지의 **distance** 의 그림을 구성하며 각각의 **advertising** 라우터들에 백본 **distance** 를 더한다.

Stub areas

OSPF 에서는 특정 **area** 가 **stub area** 의 형태로 될 수 있다. **stub area** 는 단 하나의 다른 **area** 에 연결된다. **Stub area** 를 연결하는 **area** 는 백본 **area** 일수도 있다. 외부 라우트 정보는 **stub area** 로는 분배되지 않는다. **Stub area** 는 OSPF 라우터의 메모리와 계산을 줄이기 위하여 사용한다.

Virtual links

백본과 직접 연결을 가지고 있지 않는 **area** 를 추가해야 하는 상황에서는 **virtual link** 가 사용된다. **Virtual link** 는 백본과 연결된 **area** 와 백본과 연결이 되지 않는 **area** 사이의 논리적인 경로를 제공한다. **Virtual link** 는 공통의 **area** 를 가지는 두 **ABR** 사이에 설정되어야 하며, 이중 하나의 **ABR** 은 백본과 연결되어 있어야 한다.

8.1.3. Route Redistribution

RIP 와 OSPF 는 스위치에서 동시에 사용될 수 있다. 라우트 재분배는 두 라우팅 프로토콜 사이에서 서로 라우팅 정보를 교환하는 것이다.

**Notice**

비록 RIP 과 OSPF 프로토콜이 동시에 스위치에서 동작할 수 있다 하더라도, 하나의 VLAN 에 두 프로토콜을 동시에 적용하지 않는다.

8.2. OSPF 설정

OSPF 라우팅 프로토콜을 사용하려면, OSPF 를 활성화 시켜 주어야 한다. 그 절차는 다음과 같다.

(1) Config 모드에서 `ospf` 모드로 진입한다.

```
router ospf [process-id]
```

(2) OSPF 프로토콜을 활성화 시킬 네트워크와 이것이 속할 `area`를 지정한다.

```
network (ip-address/M | ip-address wildcard-mask) area (area-id | area-address)
```

이렇게 하여 OSPF 를 활성화 시킨 후에는 다음에 설명되는 명령들을 이용하여 운용자의 요구와 필요에 맞게 프로토콜을 사용할 수 있다.

8.2.1. OSPF interface parameters

필요하면 OSPF 인터페이스의 특성을 변경할 수 있지만 모든 특성을 변경할 수 있는 것은 아니다. 어떤 OSPF 인자들은 네트워크에 있는 모든 라우터에서 동일한 값으로 설정해야 한다. 이런 인자들은 `ip ospf hello-interval`, `ip ospf dead-interval`, `ip ospf authentication-key` 명령어로 설정할 수 있다. 따라서 이런 OSPF 인자들을 변경할 때에는 네트워크에 있는 모든 라우터의 인터페이스 인자를 모두 변경해야 한다.

인터페이스 인자의 값을 변경하려면, 다음 명령어를 `interface configuration mode` 에서 입력해야 한다.

표 8-2. OSPF interface parameter CLI

명령어	설명
Router (config-if) # <code>ip ospf cost cost</code>	OSPF interface 에서 송신하는 packet 의 cost 를 설정한다.
Router (config-if) # <code>ip ospf retransmit-interval seconds</code>	OSPF interface 의 LSA 재전송 시간을 설정한다.
Router (config-if) # <code>ip ospf transmit-delay seconds</code>	OSPF interface 에서 전송 시 필요한 예상 시간을 설정한다.
Router (config-if) # <code>ip ospf priority number-value</code>	OSPF designated router 를 선출 할 때 사용되는 priority 를 설정한다.
Router (config-if) # <code>ip ospf hello-interval seconds</code>	OSPF interface 에서 송신하는 hello packet 의 주기를 설정한다.
Router (config-if) # <code>ip ospf dead-interval seconds</code>	OSPF hello packet 을 받지 못하면 OSPF router 를 down 시키는데, 이 때 OSPF router 를 down 시키기 전 기다려야 하는 시간을 설정한다.
Router (config-if) # <code>ip ospf authentication-key key</code>	OSPF simple password authentication 을 사용하는 network 세그먼트에서 사용하는 password 를 설정한다.
Router (config-if) # <code>ip ospf message-digest-key key-id md5 key</code>	OSPF MD5 authentication 을 사용할 때 key-id 와 key 값을 설정한다.

Router (config-if) # ip ospf authentication {message-digest null}	Authentication type 을 설정한다.
--	-----------------------------

8.2.2. Different Physical Networks

OSPF 여러 가지 매체에 따른 세 가지 default network type 이 존재한다.

- (3) Broadcast networks (Ethernet, Token Ring, FDDI)
- (4) Nonbroadcast multi-access(NBMA) networks (Switched Multimegabit Data Service(SMDS), Frame Relay, X.25)
- (5) Point-to-Point networks (High-Level Data Link Control(HDLC), PPP)

OSPF Network type

Default media type 과 관계없이 OSPF 네트워크를 broadcast 나 NBMA 로 설정 할 수 있다. 예를 들어 broadcast 네트워크를 NBMA 네트워크인 것처럼 설정 하거나, NBMA 네트워크를 broadcast 네트워크로 설정 할 수 있다.

OSPF point-to-multipoint 인터페이스는 한 개 이상의 neighbor 를 갖는 numbered point-to-point 인터페이스로 정의 된다. OSPF point-to-multipoint 네트워크는 NBMA/point-to-point 네트워크보다 다음과 같은 이점을 갖는다.

- (6) Point-to-multipoint 는 neighbor 설정이 필요 없고, DR 선출을 안하기 때문에 설정이 쉽다.
- (7) Full meshed topology 가 필요 없기 때문에 비용이 적다
- (8) VC(virtual circuit) failure 이벤트에도 연결을 계속 유지하기 때문에 더 reliable 하다.

OSPF network type 을 설정하려면 다음 명령어를 interface configuration mode 에서 입력하면 된다.

표 8-3. OSPF network type CLI

명령어	설명
Router (config-if) # ip ospf network {broadcast non-broadcast {point-to-multipoint [non-broadcast] point-to-point}}	OSPF interface 의 OSPF network type 을 설정한다.

Point-to-Multipoint, Broadcast Networks

Point-to-multipoint broadcast 네트워크에서는 neighbor 설정이 필요 없다. 하지만, 해당 neighbor 로의 cost 를 변경하고 싶으면 **neighbor** 명령을 사용하여 설정 할 수 있다. OSPF Hello, LS Update, LS acknowledgment 메시지는 multicast 로 전송된다. Cost 는 **ip ospf cost** 명령으로 설정하지만, 실제로 neighbor 마다 대역폭이 다를 경우 **neighbor** 명령을 사용하여 서로 다른 cost 를 설정 할 수 있다.

OSPF 인터페이스를 point-to-multipoint broadcast 네트워크로 설정하고 각각의 neighbor cost 를 설정

하려면 interface configuration mode 에서 다음과 같이 입력 하면 된다.

표 8-4. P-to-Multipoint Network, Broadcast Network 설정

	명령어	설명
Step 1	Router (config-if) # ip ospf network point-to-multipoint	Interface 를 Point-to-multipoint broadcast network type 으로 설정 한다.
Step 2	Router (config-if) # exit	Global configuration mode 로 변경한다.
Step 3	Router (config) # router ospf process-id	Router configuration mode 로 변경한다.
Step 4	Router (config-router) # neighbor ip-address cost number	특정 neighbor 의 cost 를 설정한다.

Nonbroadcast Networks

OSPF 네트워크에는 많은 라우터들이 존재 할 수 있기 때문에 DR(designated router) 선출이 필요하다. 만약 broadcast capability 가 설정되어 있지 않으면 DR 선출을 위한 특별한 인자 설정이 필요하다.

이와 같은 인자는 스스로 DR/BDR(backup DR)이 되기 적합한 라우터(nonzero priority 를 갖는 라우터)에만 설정이 필요하다.

Nonbroadcast 네트워크의 라우터 설정을 하려면 router configuration mode 에서 다음 명령을 사용한다.

표 8-5. Non broadcast network CLI

명령어	설명
Router (config-router) # neighbor ip-address [priority number] [poll-interval seconds]	Nonbroadcast network 의 router 를 연결한다.

Point-to-multipoint nonbroadcast 네트워크에서 neighbors 를 식별하기 위해 router configuration mode 에서 **neighbor** 명령을 사용한다.

Broadcast 를 지원하지 않는 매체에서 인터페이스를 point-to-multipoint 로 설정하려면, 다음과 같은 순서로 명령어를 입력한다.

표 8-6. Non broadcast network 설정

	명령어	설명
Step 1	Router (config-if) # ip ospf network point-to-multipoint non-broadcast	Interface 를 Point-to-multipoint nonbroadcast network type 으로 설정 한다.
Step 2	Router (config-if) # exit	Global configuration mode 로 변경한다.
Step 3	Router (config) # router ospf process-id	Router configuration mode 로 변경한다.
Step 4	Router (config-router) # neighbor ip-address [cost number]	Neighbor 와 neighbor 의 cost 를 설정한다.

8.2.3. OSPF Area parameters

OSPF 에는 설정 가능한 area 인자들이 존재한다. 이와 같은 area 인자에는 stub area 설정, 인증 설정, default summary route 에 대한 cost 설정 등이 있다. 인증 설정은 비밀 번호를 설정하여 인증되지 않은 라우터의 area 접근을 차단 할 수 있다. Stub area 설정은 area 로의 외부 라우트의 유입을 막지만 그 대신에 area 로 ABR 라우터가 생성한 default external route 를 전송한다. **no-summary** keyword 를 사용하면 summary route 를 차단하여 area 로 유입되는 라우트의 개수를 더 줄일 수 있다.

OSPF area 인자를 설정하려면 router configuration mode 에서 다음의 명령어를 사용하면 된다.

표 8-7. OSPF area parameter CLI

명령어	설명
Router (config-router) # area area-id authentication	OSPF area 에 authentication 을 설정한다.
Router (config-router) # area area-id authentication message-digest	OSPF area 에 MD5 authentication 을 설정한다.
Router (config-router) # area area-id stub	Stub area 를 설정한다.
Router (config-router) # area area-id default-cost cost	Stub area 를 위한 default summary route 의 cost 를 설정한다.

8.2.4. OSPF NSSA

OSPF not-so-stubby area(NSSA) 는 RFC 3101 에 설명 되어 있다.

NSSA 이전에는 corporate site border router 와 remote router 사이의 연결을 OSPF stub area 설정을 할 수 없었다. remote route site 에 대한 route 를 stub area 로 재분배가 허용되지 않았기 때문이다. NSSA 는 corporate router 와 remote router 사이를 stub area 로 설정하여 OSPF 기능을 확장시킨다.

OSPF stub area 와 마찬가지로 NSSA area 도 Type 5 LSAs 의 유입을 허용할 수 없다. NSSA area 로의 라우트 재분배는 특별한 종류의 LSAs(Type 7 LSAs)만 허용된다. Type 7 LSAs 는 NSSA area 에서만 존재해야 한다. NSSA autonomous system boundary router(ASBR)은 라우트 재분배를 위해 type 7 LSAs 를 생성하고 NSSA area border router(ABR)은 type 7 LSAs 를 type 5 LSAs 로 변형하여 모든 OSPF 라우팅 도메인으로 flooding 한다.

아래 그림에서 OSPF Area 1 이 stub area 로 설정되어 있다. Stub area 에서는 라우트 재분배가 허용되지 않기 때문에 ISIS 라우트는 OSPF 라우팅 도메인으로 전달 될 수 없다. 하지만, OSPF Area 1 을 NSSA 로 설정하면 NSSA ASBR 은 Type 7 LSAs 를 생성하여 ISIS 라우트를 OSPF NSSA 로 flooding 할 수 있다.

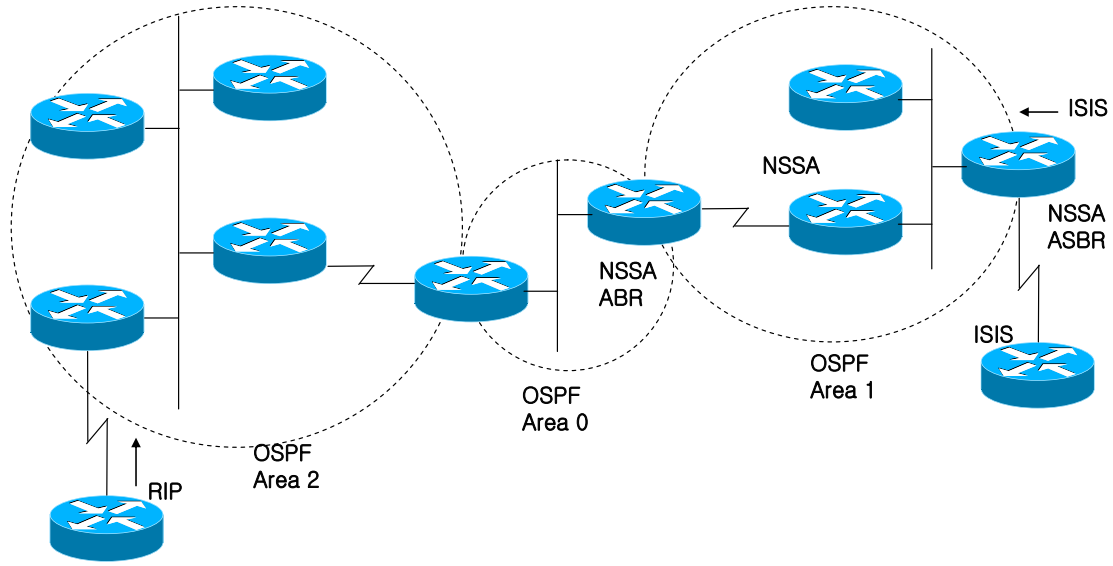


그림 8-1. OSPF Network

NSSA 는 stub area 의 확장이기 때문에 RIP 로부터 재분배된 라우트는 OSPF Area 1 로 유입 되지 않는다. Type 5 LSAs 를 유입하지 않는 Stub area 의 성질을 여전히 유지 하는 것이다.

OSPF NSSA 를 설정하려면 router configuration mode 에서 다음 명령을 사용한다.

표 8-8. OSPF NSSA CLI

명령어	설명
Router (config-router) # area area-id nssa [no-redistribution] [default-information-originate]	NSSA 를 설정한다.

8.2.5. OSPF Area Route summarization

라우트 축약(route summarization)은 advertise 된 라우트를 통합 하는 기능이다. 이 기능을 설정하면 ABR 라우터는 다른 area 로 하나의 축약된 라우트만 advertise 한다. OSPF 에서 ABR 라우터는 한 area 에 있는 네트워크를 다른 area 로 전달하는 역할을 한다. 만약 area 에 수 많은 네트워크가 존재하면 ABR 라우터에서 각 라우트를 포함하는 축약 라우트(일정한 범위의 라우트)를 advertise 하도록 설정하여 유입되는 라우트의 개수를 줄일 수 있다.

Summary address range 를 설정하려면 router configuration mode 에서 다음의 명령어를 사용한다.

표 8-9. OSPF area route summarization CLI

명령어	설명
-----	----

Router (config-router) # area <i>area-id</i> range <i>ip-address mask</i> [advertise not-advertise] [cost <i>cost</i>]	Summary route advertise 할 <i>address range</i> 를 설정 한다.
---	---

8.2.6. Redistributed Routes 의 Route Summarization

다른 라우팅 프로토콜로부터 라우트가 재분배될 때, 각각의 라우트는 Type 5 AS-External LSA 로 분배 된다. 하지만 **summary-address** 명령으로 재분배되는 모든 라우트를 포함하는 하나의 라우트로 축약할 수 있다.

모든 재분배되는 라우트를 하나의 라우트로 축약하려면 **router configuration mode** 에서 다음의 명령어를 사용한다.

표 8-10. External Route summarization CLI

명령어	설명
Router (config-router) # summary-address { <i>ip-address/prefix</i> } [not-advertise] [tag <i>tag</i>]	한 개의 라우트로 전송될 재분배 라우트를 포함하는 <i>address</i> 를 설정한다.

8.2.7. Virtual Links

OSPF 에서는 모든 **area** 는 백본 **area** 에 연결되어 있어야 한다. 만약 백본 **area** 로의 연결이 끊어지면 **virtual link** 를 설정 할 수 있다. **Virtual link** 의 두 종단은 **ABR** 라우터이고 두 라우터에서 모두 설정 되어야 한다. 또한 두 라우터는 모두 같은 **area**(transit **area**)에 있어야 하며, **stub area** 에서는 **virtual link** 를 설정 할 수 없다.

Virtual link 를 설정하려면 **router configuration mode** 에서 다음의 명령어를 사용한다.

표 8-11. OSPF virtual link CLI

명령어	설명
Router (config-router) # area <i>area-id</i> virtual-link <i>router-id</i> [authentication [message-digest null]] [hello-interval <i>seconds</i>] [retransmit-interval <i>seconds</i>] [transmit-delay <i>seconds</i>] [dead-interval <i>seconds</i>] [[authentication-key <i>key</i>] [message-digest-key <i>key-id md5 key</i>]]	Virtual link 을 설정한다.

8.2.8. Generating a Default Route

ASBR 라우터가 **OSPF** 라우팅 도메인으로 디폴트 라우트를 생성하도록 할 수 있다. 라우트 재분배 설정을 통해 라우터를 **ASBR** 라우터가 되도록 할 수 있지만, 기본적으로 **ASBR** 라우터는 디폴트 라우트

를 생성하지 않는다.

ASBR 이 디폴트 라우트를 생성하게 하려면 `router configuration mode` 에서 다음 명령어를 사용한다.

표 8-12. OSPF default route CLI

명령어	설명
Router (config-router) # default-information originate [always] [metric <i>metric-value</i>] [metric-type <i>type-value</i>] [route-map <i>map-name</i>]	ASBR 이 OSPF routing domain 에 default route 를 생성하게 한다.

8.2.9. Router ID Choice with a Loopback Interface

OSPF 는 인터페이스에 설정된 IP 주소 중에서 가장 큰 값을 라우터 ID 로 사용한다. 만약 loopback 인터페이스에 IP 주소가 설정 되어 있으면, 다른 인터페이스에 가장 큰 값을 갖는 IP 주소가 할당 되어 있어도 loopback 인터페이스 중 가장 큰 값의 IP 주소를 라우터 ID 로 사용한다.

Loopback 인터페이스에 IP address 를 할당하려면 다음과 같은 순서로 명령어를 입력한다.

표 8-13. Loopback interface 설정

	명령어	설명
Step 1	Router (config-if) # interface Loopback 0	Loopback interface 를 생성한다.
Step 2	Router (config-if) # ip address ip-address/prefix	Interface 에 IP address 를 할당 한다.

8.2.10. Default metric

OSPF 는 인터페이스의 대역폭에 따라 OSPF metric 을 다르게 계산한다. OSPF 에서 OSPF metric 은 reference-bandwidth 를 인터페이스의 대역폭으로 나눈 값을 사용한다. 인터페이스의 대역폭은 interface configuration mode 에서 **bandwidth** 명령어로 변경할 수 있다.

reference-bandwidth 를 변경하려면 `router configuration mode` 에서 다음 명령어를 사용한다.

표 8-14. Reference bandwidth CLI

명령어	설명
Router (config-router) # auto-cost reference-bandwidth ref-bw	reference-bandwidth 를 변경한다.

8.2.11. OSPF administrative Distance

Administrative Distance 는 routing information source 의 신뢰도를 나타내며, 0~255 로 표시된다. 일반적으로 큰 값이 낮은 신뢰도를 의미 한다. 255 의 administrative distance 값은 routing information source 를 신뢰할 수 없다는 의미이고 해당 route 는 무시 된다.

OSPF 는 intra-area, inter-area, external 이렇게 세 가지의 administrative distance 를 사용하고 각각의 default 값은 110 이다.

OSPF distance 를 변경하려면 router configuration mode 에서 다음 명령어를 사용한다.

표 8-15. OSPF distance CLI

명령어	설명
Router (config-router) # distance ospf {[intra-area <i>dist1</i>] [inter-area <i>dist2</i>] [external <i>dist3</i>]}	OSPF distance 를 변경한다.

8.2.12. Passive interface

passive-interface 명령은 특정 인터페이스로의 Hello 메시지 전송은 제한하지만 수신은 가능하도록 설정한다.

단 방향 인터페이스를 설정하려면 router configuration mode 에서 다음 명령어를 사용한다.

표 8-16. OSPF passive interface CLI

명령어	설명
Router (config-router) # passive-interface <i>interface-name</i>	Interface 를 통해 송신하는 hello packets 을 제한한다.

8.2.13. Route Calculation Timers

OSPF 는 네트워크 형상 변화가 발생할 때마다 SPF(shortest path first) 계산을 한다. 빈번한 SPF 계산을 방지하기 위해 형상 변화가 발생한 시각과 SPF 계산 시작 시각 사이의 지연 시간을 설정할 수 있다.

SPF 지연 시간을 설정하려면 router configuration mode 에서 다음 명령어를 사용한다.

표 8-17. OSPF SPF timer CLI

명령어	설명
Router (config-router) # timers throttle spf spf-start spf-hold spf-max-wait	SPF 계산 시간을 변경한다.

8.2.14. Logging Neighbors Going Up/Down

OSPF 는 neighbor Up/Down 이벤트에 대해 시스템 메시지를 발생시킨다. Neighbor 의 상태 변화에 대해 자세한 시스템 메시지 발생을 원한다면, **detail** 키워드를 사용한다.

neighbor UP/Down 이벤트에 대한 시스템 메시지 발생을 제한 하려면, router configuration mode 에서 no 키워드와 함께 다음 명령어를 사용한다.

표 8-18. OSPF adjacency LOG CLI

명령어	설명
Router (config-router) # log-adjacency-changes [detail]	OSPF neighbor UP/Down 에 대한 시스템 메시지를 발생한다.

8.2.15. Blocking LSA Flooding

OSPF 는 새로운 LSA 를 수신하면 수신한 인터페이스를 제외한 인터페이스로 LSA 를 flooding 한다. 하지만 이런 동작은 대역폭 낭비와 CPU 과부하를 발생시킬 수도 있다. **database-filter** 명령어를 사용하면 특정 인터페이스로의 LSA flooding 을 제한 할 수 있다.

Broadcast, non-broadcast, point-to-point 네트워크에서 OSPF LSA flooding 을 제한 하려면, interface configuration mode 에서 다음의 명령어를 사용한다.

표 8-19. Block LSA CLI

명령어	설명
Router (config-router) # ip ospf database-filter all out	Interface 의 LSA flooding 을 제한 한다.

8.2.16. Ignoring MOSPF LSA Packets

E7500 Series 스위치는 LSA Type 6 Multicast OSPF (MOSPF)를 지원하지 않기 때문에, 이 LSA 를 수신하면 시스템 메시지를 발생시킨다. 다수의 MOSPF LSA 를 수신하면 다량의 시스템 메시지가 발생하게 되는데, 시스템 메시지를 발생시키지 않으려면 이 기능을 사용한다.

LSA Type 6 패킷을 수신했을 때 시스템 메시지를 발생 하지 않게 하려면 `router configuration mode` 에서 다음의 명령어를 사용한다.

표 8-20. Ignore MOSPF LSA CLI

명령어	설명
Router (config-router) # <code>ignore lsa mospf</code>	MOSPF LSA packet 을 수신했을 때 시스템 메시지를 발생하지 않는다.

8.2.17. Monitoring and Maintaining OSPF

OSPF 라우팅 테이블, 데이터베이스, 그리고 이웃한 라우터의 연결 상태에 대한 정보를 조회 할 수 있다. 이러한 정보는 네트워크의 문제를 해결하거나 스위치의 자원 관리에 대한 참고 자료로 활용 할 수 있다.

다양한 OSPF 정보를 조회하려면 EXEC mode 에서 다음의 명령어를 사용한다.

표 8-21. Monitoring OSPF CLI

명령어	설명
Router # <code>show ip ospf [process-id]</code>	OSPF routing process 정보를 조회한다.
Router # <code>show ip ospf border-routers</code>	ABR/ASBR 에 대한 모든 routing table 을 조회한다.
Router # <code>show ip ospf [process-id] database</code>	OSPF database 를 조회한다.
Router # <code>show ip ospf [process-id] database [database-summary]</code>	
Router # <code>show ip ospf [process-id] database [router] [self-originate]</code>	
Router # <code>show ip ospf [process-id] database [router] [adv-router [ip-address]]</code>	
Router # <code>show ip ospf [process-id] database [router] [link-state-id]</code>	
Router # <code>show ip ospf [process-id] database [network] [link-state-id]</code>	
Router # <code>show ip ospf [process-id] database [summary] [link-state-id]</code>	
Router # <code>show ip ospf [process-id] database [asbr-summary] [link-state-id]</code>	
Router # <code>show ip ospf [process-id] database [external] [link-state-id]</code>	

Router # show ip ospf [<i>process-id</i>] database [<i>nssa-external</i>] [<i>link-state-id</i>]	
Router # show ip ospf [<i>process-id</i>] database [<i>opaque-link</i>] [<i>link-state-id</i>]	
Router # show ip ospf [<i>process-id</i>] database [<i>opaque-area</i>] [<i>link-state-id</i>]	
Router # show ip ospf [<i>process-id</i>] database [<i>opaque-as</i>] [<i>link-state-id</i>]	
Router # show ip ospf flood-list [<i>interface-name</i>]	Flooding 될 모든 LSAs 를 조회한다.
Router # show ip ospf interface [<i>interface-name</i>]	OSPF interface 정보를 조회한다.
Router # show ip ospf neighbor [<i>neighbor-id</i>] [<i>detail</i>]	OSPF neighbor 정보를 조회한다.
Router # show ip ospf [<i>process-id</i>] summary-address	Redistribution 정보에 관한 모든 summary address 정보를 조회한다.
show ip ospf [<i>process-id</i>] traffic	OSPF traffic 통계 정보를 조회한다.
show ip ospf [<i>process-id</i>] virtual-links	OSPF virtual link 정보를 조회한다.

OSPF 프로세스를 다시 시작 하려면 EXEC mode 에서 다음의 명령어를 사용한다.

표 8-22. Maintaining OSPF CLI

명령어	설명
Router # clear ip ospf [<i>process-id</i>] { process redistribution counters traffic }	OSPF process/counters/redistribution/traffic 을 재 시작 한다.

9

라우팅 프로토콜
BGP

본 장에서는 E7500 series 스위치에서 사용 가능한 IP 유니캐스트 라우팅 프로토콜들 중에서 BGP 에 대해서 기술한다.

9.1. BGP 개요

BGP 는 서로 다른 관리 도메인(Autonomous System : AS) 간에 라우팅 정보를 주고 받을 수 있도록 해 주는 프로토콜로서 RIP 와 OSPF 와는 달리 한 도메인 내에서의 라우팅이 아닌 도메인 간의 라우팅을 담당한다. E7500 SERIES 스위치에서는 BGP-4 를 지원하고 있다.

9.2. BGP 설정

BGP 의 구성은 크게 기본구성(basic configuration)과 고급구성(advanced configuration)으로 나누어 볼 수 있다. BGP 프로토콜을 사용하기 위해서는 우선 다음과 같은 구성을 기본적으로 하여야 한다.

- ✓ BGP 프로토콜의 활성화
- ✓ BGP neighbor 라우터 설정

9.1.1. BGP 프로토콜의 활성화

BGP 프로토콜을 사용하기 위해서는 RIP 와 OSPF 에서처럼 BGP 프로토콜의 활성화 단계가 선행 되어야 한다. 그 단계는 다음과 같다.

- 1) BGP 라우터 설정 모드로의 진입

```
router bgp <1-4294967295>
```

끝의 숫자는 AS 넘버를 가리킨다. AS 번호는 Autonomous System 번호로 BGP 네트워크를 구분하기 위해 사용되며, 망 운영자에 의해 할당된다.

- 2) BGP 네트워크를 지정하고 BGP 라우팅 테이블에 등록한다.

```
network A.B.C.D/M
```

BGP 를 통해 알려 줄 네트워크를 지정한다.

9.1.2. Neighbor 설정

BGP 라우팅 정보를 교환하기 위해 TCP 연결을 설정한 두 개의 라우터는 peer 혹은 neighbor(이하 네이버)라 불리며, 반드시 네이버 설정이 되어 있어야 한다. 이러한 네이버에는 동일한 AS 에 속한 네이버(iBGP Peer)와 다른 AS 에 속한 네이버(eBGP Peer)로 구분된다. 동일 AS 에 속한 네이버들은 직접 연결 되어 있을 필요는 없고 내부 라우팅 프로토콜(IGP, 예로 RIP 혹은 OSPF 등)로 경로 설정이 되어 있으면 된다. 그러나 다른 AS 에 속한 네이버와는 물리적으로 연결이 설정 되어 동일한 서브넷에 속해 있어야 한다.

이러한 `bgp neighbor` 를 설정하기 위해서는 다음의 명령을 사용한다.

```
neighbor ip-address remote-as number
```

이렇게 `bgp` 를 활성화 시키고 네이버 설정이 이루어 지면 기본적인 BGP 프로토콜이 동작하게 된다. 여기에 망 운용자는 다음에 설명하는 항목들을 선택적으로 설정할 수 있다.

- 1) 필터링 기능
- 2) BGP Attribute 설정
- 3) Routing policy 변경
- 4) 기타 기능

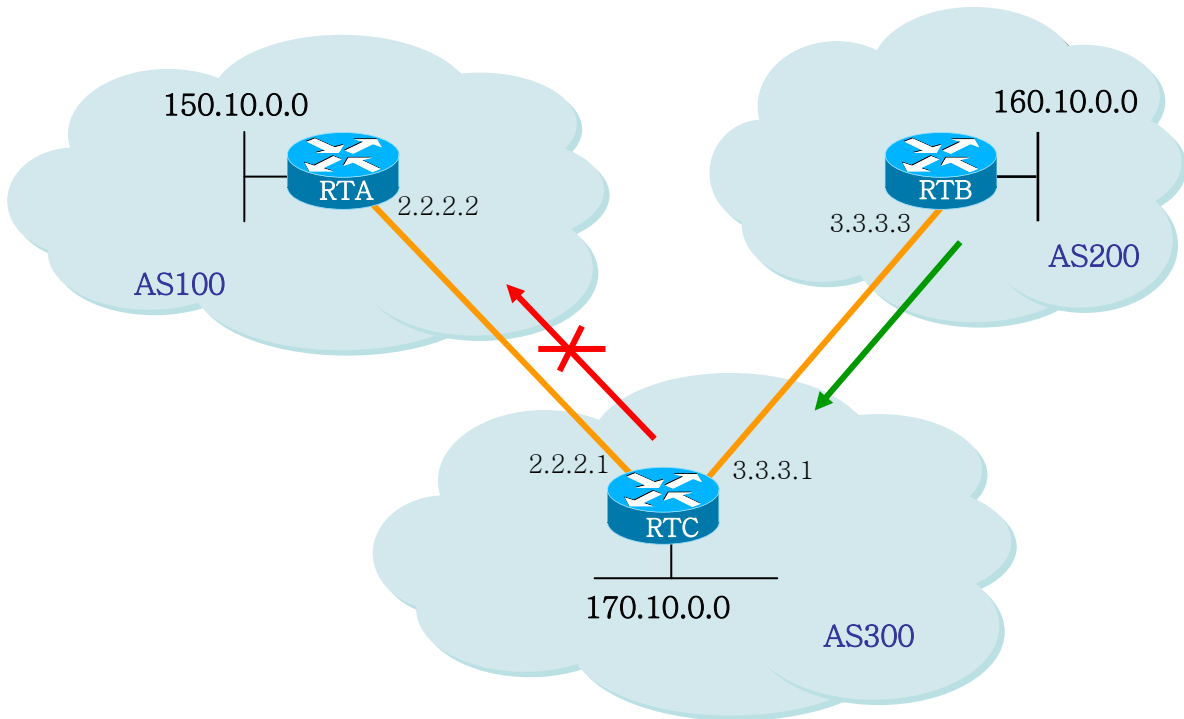
9.1.3. BGP 필터링 기능

BGP update 를 송수신 하는 것은 여러 개의 필터링 방식에 의해 조절할 수 있다. 이러한 필터링 방식에는 route filtering, path filtering, community filtering 이 있다. 이 모든 방법은 동일한 효과를 얻는다. 다만 특정한 네트워크 구성에 따라 적절한 방법을 선택하면 된다.

Route Filtering

라우터가 습득하거나 선전하는 라우팅 정보를 제한하기 위해, 특정 네이버로 가거나 오는 라우팅 업데이트에 기반하여 BGP 를 필터링 할 수 있다. 이를 위해, Access-list 가 정의되어 특정 네이버로의 입출력 업데이트에 적용된다. 이를 위해 다음의 명령을 사용한다.

neighbor {ip-address|peer-group-name} distribute-list access-list-number {in|out}



1. 그림

위 그림에서 RTB 는 네트워크 160.10.0.0 을 생성하고 RTC 로 그 정보를 보낸다. 만일 RTC 가 이 정보를 AS 100 으로 전달하지 않기로 하는 경우, 이 정보의 업데이트를 필터링 하기 위해 access-list 를 적용하여 RTA 로의 연결에 이것을 적용한다. 이것의 구성을 살펴보면 다음과 같다.

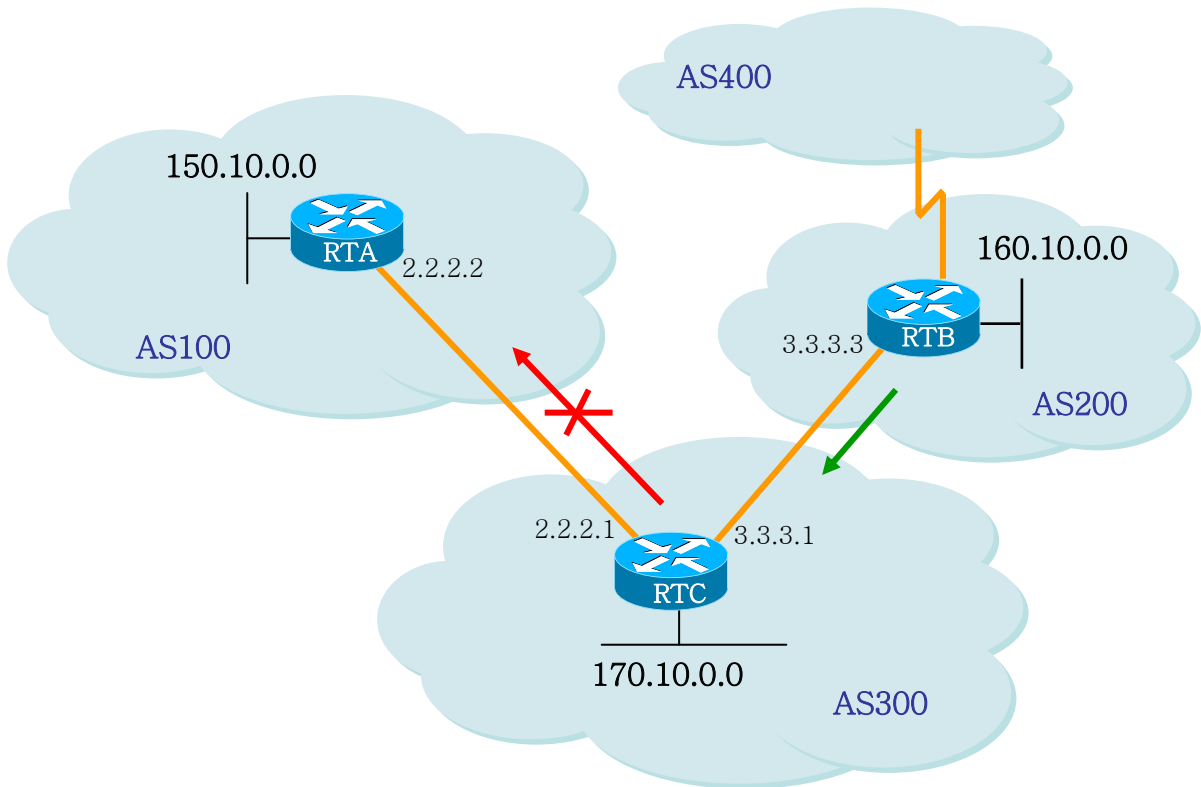
```

/*-- RTC --*/
!
router bgp 300
 network 170.10.0.0
 neighbor 3.3.3.3 remote-as 200
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 distribute-list 1 out
!
access-list 1 deny 160.10.0.0 0.0.255.255
access-list 1 permit 0.0.0.0 255.255.255.255
!-- filter out all routing updates about 160.10.x.x
!
    
```

Path Filtering

또 한가지의 필터링 방식으로, BGP AS path information 에 기반하여 입력과 출력쪽 모두에 access-list 를 설정할 수 있다. 다음 그림의 네트워크 구성도에서, AS 200 에서 생성된 업데이트가 AS 100 으로 가는 것을 막기 위해, RTC 에 access-list 를 정의함으로써, 160.10.0.0 에 대한 정보가 AS100 으로 가는 것을 막을 수 있다. 이를 위해 다음의 명령을 사용한다.

```
ip as-path access-list access-list-number {permit|deny} as-regular-expression
neighbor {ip-address|peer-group-name} filter-list access-list-number {in|out}
```



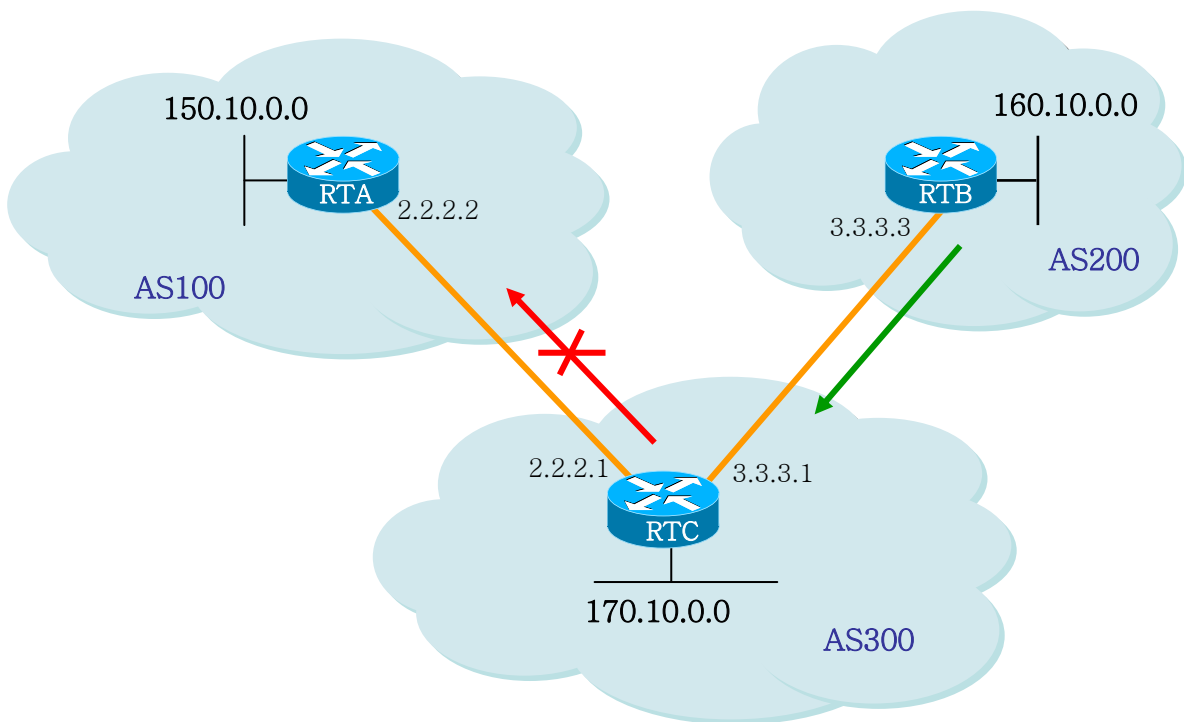
다음의 구성은 위 그림의 RTC 가 RTA 로 160.10.0.0 의 업데이트를 하는 것을 path filtering 을 사용하여 수행하는 구성을 보여준다.

```
/*-- RTC --*/
!
router bgp 300
 neighbor 3.3.3.3 remote-as 200
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 filter-list 1 out
```

```
!-- the 1 is the access list number below
!
ip as-path access-list 1 deny ^200$
ip as-path access-list 1 permit .*
!
```

Community Filtering

Community 는 여러 개의 destination 을 특정 그룹으로 community 화 하여, 이 community 에 routing decision 을 적용하기 위해 사용된다.



위 그림에서, RTC 가 자신의 eBGP peer 로 RTB 가 보내는 라우트들을 업데이트 하지 않도록, RTB 에 community attribute 를 설정하는 예가 다음에 나와 있다. 이를 위해 'no-export' community attribute 가 사용된다.

```
/*-- RTB --*/
router bgp 200
 network 160.10.0.0
 neighbor 3.3.3.1 remote-as 300
 neighbor 3.3.3.1 send-community
 neighbor 3.3.3.1 route-map setcommunity out
!
route-map setcommunity
```

```
match ip address 1
set community no-export
access-list 1 permit 0.0.0.0 255.255.255.255
!
```

시스코 라우터의 경우는 이러한 **attribute** 를 **RTC** 로 보내기 위해 **neighbor send-community** 명령을 사용해야 하나, **E7500 series** 에서는 이 명령이 **default enable** 되어 있다. 그래서 위의 구성에서 실제로는 'neighbor 3.3.3.1 send-community' 명령어는 삭제 되어도 된다. 다만 이것을 **disable** 시키기 위해서는 'no neighbor 3.3.3.1 send-community'를 명시해야 한다.

이렇게 하여 **RTC** 가 **no-export attribute** 를 가진 **update** 를 얻는 경우, **RTC** 는 이 정보들을 자신의 인접 네이바인 **RTA** 로 전달하지 않는다.

다음의 예에서는, **RTB** 가 **community attribute** 에 100, 200 을 추가하는 경우를 보여준다. 이 값 100, 200 은 **RTC** 로 보내지기 전에 현존하는 **community value** 에 덧붙여 질 것이다. 만일 **additive** 명령어가 없는 경우는 기존의 **community value** 를 100 200 로 대체하게 된다.

```
/*-- RTB --*/
!
router bgp 200
 network 160.10.0.0
 neighbor 3.3.3.1 remote-as 300
 neighbor 3.3.3.1 route-map setcommunity out
!
route-map setcommunity
 match ip address 2
 set community 100 200 additive
!
access-list 2 permit 0.0.0.0 255.255.255.255
```

community list 는, 서로 다른 **community number** 의 리스트들에 기반하여 **attribute** 들을 세팅하거나 필터링하도록 하기 위해 **route map** 의 **match** 문에 사용하게 되는 일종의 **community** 들의 그룹을 지칭한다.

```
ip community-list community-list-number {permit|deny} community-number
```

예로 다음의 **route-map** 을 정의할 수 있다.

```
!
route-map match-on-community
 match community 10
  !-- 10 is the community-list number
 set weight 20
 ip community-list 10 permit 200 300
  !-- 200 300 is the community number
!
```

이 `route-map` 을 사용하여 특정 `bgp route` 업데이트시에 이 `community value` 에 기반하여 `metric` 값이나 `weight` 가 같은 특정 파라미터들을 필터링 하거나 변경할 수 있다. 앞의 예에서, `RTB` 는 `RTC` 로 `community 100, 200` 을 가진 업데이트를 보내고 있었는데, 만일 `RTC` 가 이 값에 기반하여 `weight` 값을 세팅하고자 하는 경우 다음과 같은 구성을 할 수 있다.

```
/*-- RTC --*/
!
router bgp 300
 neighbor 3.3.3.3 remote-as 200
 neighbor 3.3.3.3 route-map check-community in
!
route-map check-community permit 10
 match community 1
 set weight 20
!
route-map check-community permit 20
 match community 2 exact
 set weight 10
!
route-map check-community permit 30
 match community 3
!
ip community-list 1 permit 100
ip community-list 2 permit 200
ip community-list 3 permit internet
!
```

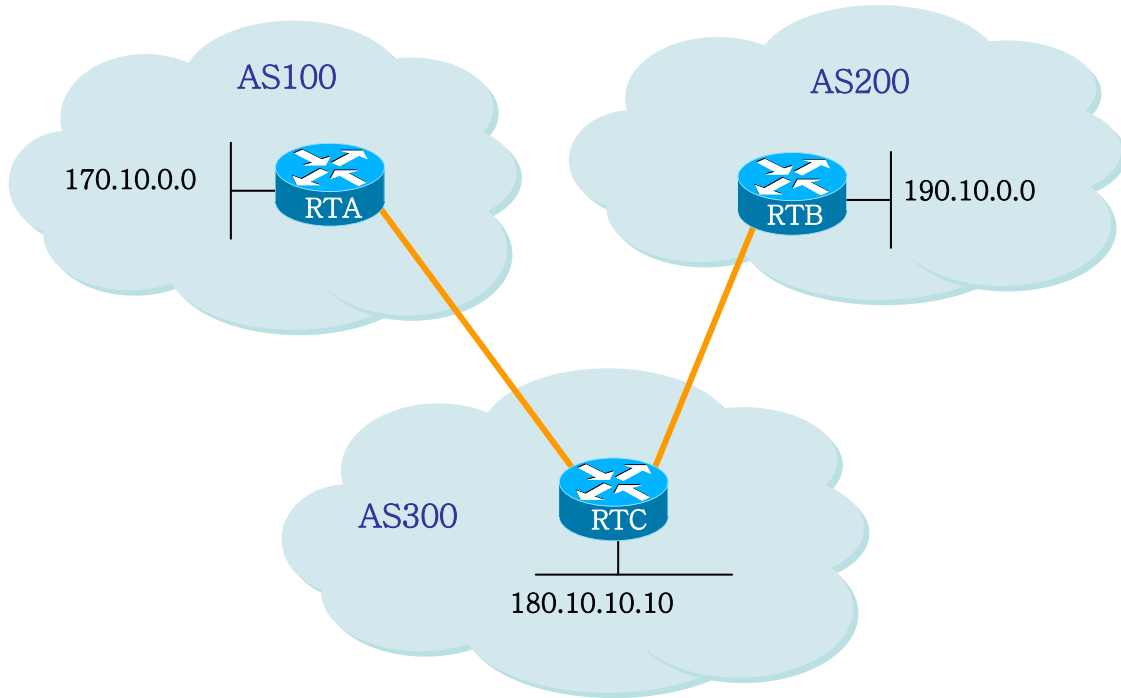
이 구성에서, `community attribute` 로 100을 가진 라우트는 리스트 1에 매치될 것이고 `set` 설정에 의해서 `weight` 값이 20으로 세팅된다. `Community` 값으로 200만을 가진 라우트는 리스트 2에 매치되어 `weight` 값 10을 갖게 된다. 키워드 `exact` 는 `community` 가 200만을 가지고 있어야 됨을 의미한다. 마지막 `community list` 는 그 외의 업데이트가 `drop` 되지 않도록 하기 위해 사용된다. 왜냐하면, 매치가 되지 않는 것들은 디폴트로 `drop` 되기 때문이다. 키워드 `internet` 은 모든 라우트들이 `internet community` 의 멤버들이기 때문에 모든 라우트들을 의미한다.

9.1.4. BGP Attribute 설정

BGP 에 사용되는 `attribute` 들에는 다음과 같은 것들이 있다.

- ✓ **As-path attribute**
- ✓ **Origin attribute**
- ✓ **Nexthop attribute**
- ✓ **Local Preference attribute**
- ✓ **Metric attribute**
- ✓ **Community attribute**
- ✓ **Weight attribute**

As_path Attribute



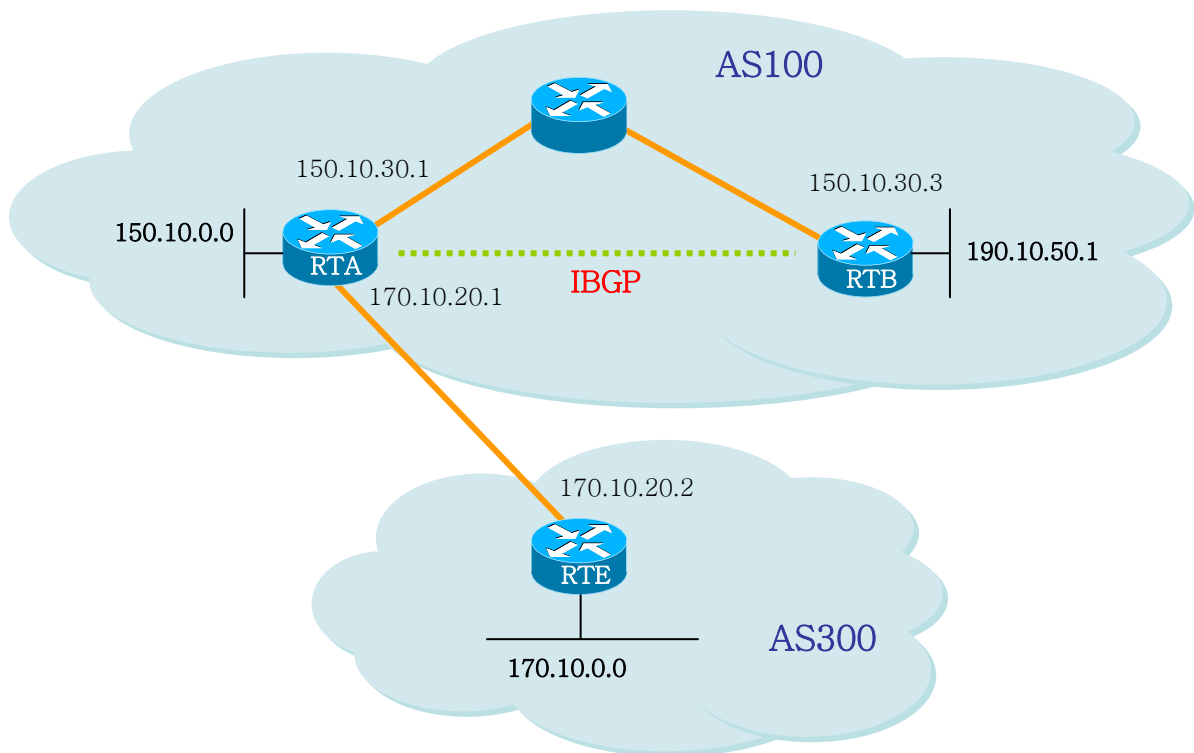
하나의 라우트가 하나의 AS 를 지나갈 때, 이 AS 의 번호가 해당 라우트의 업데이트에 추가된다. **AS_path** attribute 는 하나의 라우트가 특정 목적지에 도달하기 위해 지나온 AS 번호들의 리스트를 가리킨다. **AS-SET** 은 하나의 라우트가 지나온 모든 AS 들의 집합을 가리킨다. 위 그림에서 네트워크 190.10.0.0 은 AS200 에 있는 RTB 에 의해 알려진다. 이 라우트가 AS 300 을 지나갈 때 RTC 는 자신의 AS 번호 300 을 이 라우트의 **as-path** 에 덧붙인다. 그래서 190.10.0.0 라우트가 RTA 에 도달시 RTA 는 그것에 추가된 2 개의 AS 번호인 200 과 300 을 보게 될 것이다. 그래서 RTA 에 있어서 190.10.0.0 에 도달하기 위한 경로는 (300, 200)이 된다.

170.10.0.0 과 180.10.0.0 에 대해서도 마찬가지로 경우가 성립한다. RTB 는 170.10.0.0 에 도달하기 위해 AS300 과 AS100 을 지나가야 한다. RTC 는 190.10.0.0 에 도달하기 위해 AS 200 을 지나야 하고, 170.10.0.0 에 도달하기 위해서는 AS 100 을 지나야 한다.

Origin Attribute

이것은 패스 정보의 기원을 정의하는 attribute 이다. 이것에는 3 가지 값이 있다.

- ✓ **IGP**: NLRI(Network Layer Reachability Information)가 생성 AS의 내부에 있다. 이것은 보통 `bgp network` 명령을 사용하거나 IGP 정보가 BGP로 `redistribute` 될 때에 해당하고, 이 패스 정보의 origin은 IGP가 되고, BGP 테이블에 “i” 로 나타난다.
- ✓ **EGP**: NLRI는 BGP를 통해 습득된다. 이것은 BGP 테이블에 “e”로 표시된다.
- ✓ **INCOMPLETE**: NLRI 가 unknown이거나 기타의 방법으로 습득된다. 보통 `static route`를 BGP로 `redistribute` 할 때이다. 이것은 BGP 테이블에 “?”로 표시된다.



```
/*-- RTA --*/
!
router bgp 100
 network 150.10.0.0
 redistribute static
 neighbor 150.10.30.3 remote-as 100
 neighbor 170.10.20.2 remote-as 300
!
ip route 190.10.0.0/24 null
!

/*-- RTB --*/
!
router bgp 100
 network 190.10.50.0
 neighbor 150.10.30.1 remote-as 100
!
```

```
/*-- RTE --*/  
!  
router bgp 300  
  network 170.10.0.0  
  neighbor 170.10.20.1 remote-as 100  
!
```

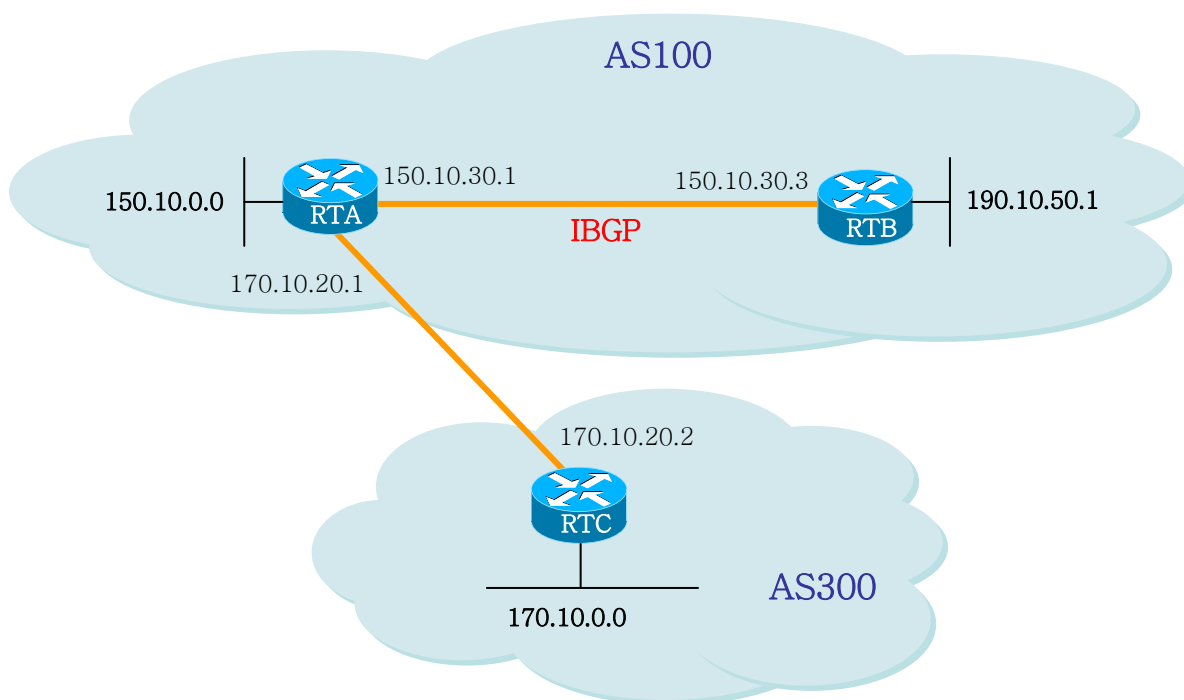
위 그림의 구성에서,

- RTA는 170.10.0.0에 300 i 를 통해 도달된다.
(이것은 다음의 AS 패스가 300이고 이 라우트의 origin이 IGP임을 의미한다.)
- RTA는 190.10.50.0에 i 를 통해 도달된다.
(이것은 다음의 AS 패스가 100이고 이 라우트의 origin이 IGP임을 의미한다.)
- RTE는 150.10.0.0에 100 i 를 통해 도달된다.
(이것은 다음의 AS 패스가 100이고 이 라우트의 origin이 IGP임을 의미한다.)
- RTE는 190.10.0.0에 100 ? 를 통해 도달된다.
(이것은 다음의 AS 패스가 100이고 이 라우트의 origin이 incomplete임을 의미한다.)

BGP Nexthop Attribute

`nexthop attribute` 은 특정 목적지에 도달하기 위해 사용될 `nexthop IP address` 를 가리킨다. EBGP의 경우, 이 `nexthop` 은 언제나 네이버 명령에서 지정된 네이버의 IP 주소이다. 다음 그림에서, RTC는 RTA로 170.10.0.0의 정보를 전달시 벡스트 홉을 170.10.20.2로 보내고, RTA는 RTC로 150.10.0.0을 전달시 벡스트 홉을 170.10.20.1로 보낸다. IBGP 경우, EBGP가 전달하는 벡스트 홉은 IBGP에서는 그대로 전달되어야 한다고 프로토콜에 규정되어 있다. 이 규정으로 인하여, RTA는 170.10.0.0을 자신의 IBGP peer인 RTB로 전달시 벡스트 홉을 170.10.20.2로 보낸다. 따라서 RTB의 경우, 170.10.0.0에 도달하기 위한 벡스트 홉은 150.10.30.1이 아닌 170.10.20.2이다.

이를 위해 RTB는 IGP를 통해 170.10.20.2에 도달할 수 있도록 조치가 취해져야 한다. 그렇지 않으면 RTB는 170.10.0.0으로 향하는 패킷들을 버리게 된다.



```
/*-- RTA --*/
!
router bgp 100
 network 150.10.0.0
 neighbor 170.10.20.2 remote-as 300
 neighbor 150.10.30.3 remote-as 100
!

/*-- RTB --*/
!
router bgp 100
 neighbor 150.10.30.1 remote-as 100
!
```

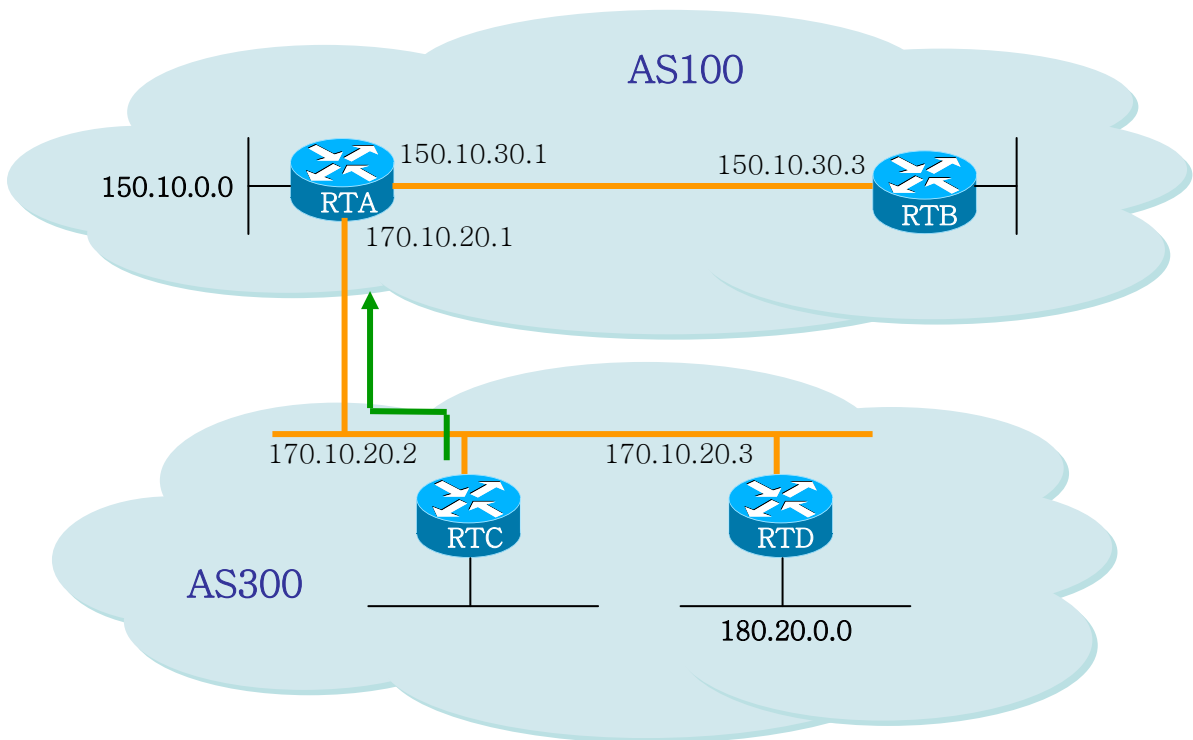
```

/*-- RTC --*/
!
router bgp 300
 network 170.10.0.0
 neighbor 170.10.20.1 remote-as 100
!
    
```

- RTC는 RTA로 170.10.0.0을 전달시 넥스트 홉이 170.10.20.2가 된다.
- RTA가 RTB로 170.10.0.0을 전달시 넥스트 홉이 170.10.20.2가 된다.

멀티액세스 네트워크와 NBMA 망에서는 특별한 주의가 요구되는데 다음에 설명한다.

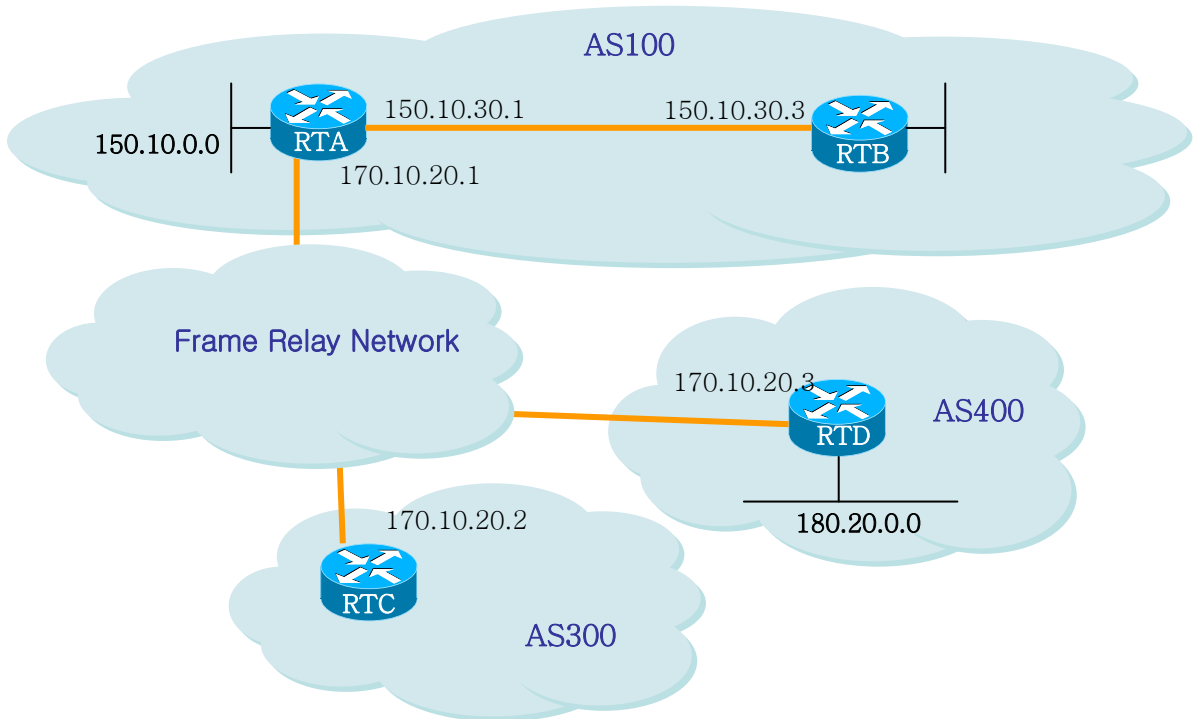
BGP Nexthop (Multiple access networks)



위 그림에서 AS 300에 있는 RTC와 RTD는 OSPF를 돌리고 있다고 가정한다. RTC는 RTA와 EBGP 연결을 설정한다. RTC는 170.10.20.3을 통하여 180.20.0.0 망에 도달할 수 있다. RTC가 180.20.0.0 정보를 RTA로 BGP 업데이트를 통해 전송 시, 넥스트 홉으로 자신의 IP인 170.10.20.2가 아닌 170.10.20.3을 사용한다. 이는 RTA, RTC, RTD 간의 망이 멀티액세스 망이고 RTA가 180.20.0.0에 도달하기 위해 RTC를 거치는 과정을 거치기 보다는 RTD를 바로 넥스트 홉으로 사용하는 것이 더 합리적이기 때문이다.

만일 RTA, RTC, RTD 에 공통인 미디어가 멀티액세스가 아니라. NBMA 인 경우는 더욱 복잡한 현상이 발생한다.

BGP Nexthop (NBMA)



위 그림에서 보듯이 공통 미디어가 Frame Relay 같은 NBMA 망이라면 앞의 경우와 같은 행동을 하게 된다. 즉 RTC 는 RTA 로 180.20.0.0 의 정보를 전달 시 넥스트 홉으로 170.10.20.3 을 사용한다. 문제는 RTA 가 RTD 로 직접적인 PVC 를 갖고 있지 않아서, 넥스트 홉에 도달할 수 없는 경우이다. 이 경우 라우팅은 실패하게 된다. 이 상황을 위해 next-hop-self 명령이 고안 되었다.

Next-hop-self

next-hop-self 명령은 프로토콜이 넥스트 홉을 지정하게 하지 않고, 지정된 IP 를 강제적으로 넥스트 홉으로 사용할 수 있게 해준다. 이 명령의 구문은 다음과 같다.

```
neighbor {ip-address|peer-group-name} next-hop-self
```

앞의 예와 같은 경우, 다음의 구성으로 문제를 해결할 수 있다.

```
/*-- RTC --*/
!
router bgp 300
```

```
neighbor 170.10.20.1 remote-as 100
neighbor 170.10.20.1 next-hop-self
!
```

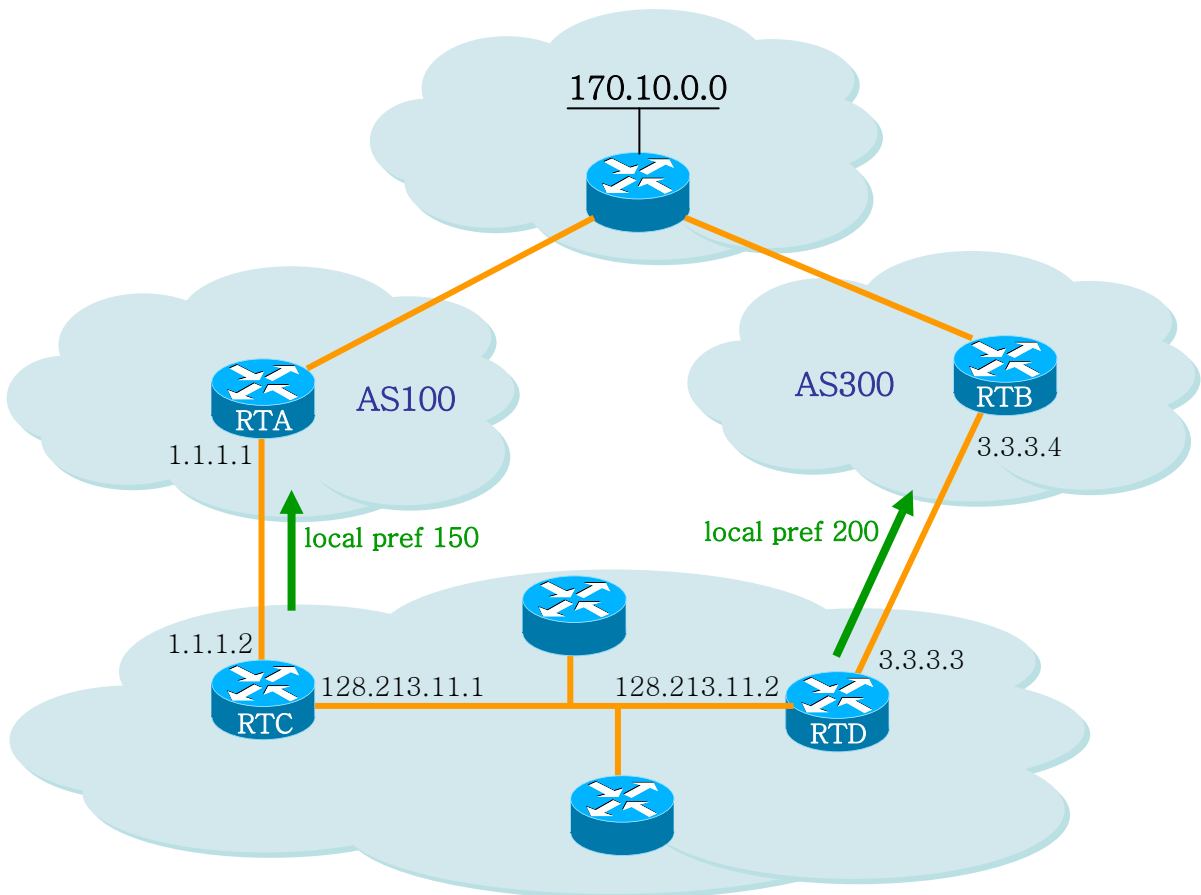
RTC 는 180.20.0.0 를 nextHop = 170.10.20.2 로 전송한다.

Local Preference Attribute

Local preference 는 특정 네트워크에 도달하기 위해 해당 AS 를 빠져나가는데 어떤 패스를 선호할 지를 AS 에게 알려준다. 더 높은 값을 지닌 local preference 를 가진 패스가 더 선호된다. 디폴트 값은 100 이다. 로컬 라우터에만 적용되는 weight attribute 와 달리, local preference 는 동일 AS 내에 있는 라우터들 간에 교환되는 attribute 이다.

local preference 는 **bgp default local-preference <value>** 명령이나 라우트 맵을 통해 세팅되는데, 다음에 그 예를 보여준다.

bgp default local-preference 명령은 동일 AS 내의 피어 라우터로 나가는 업데이트 시의 local preference 값을 모두 바꾼다. 아래 예제 그림에서, AS256 은 서로 다른 2 개의 AS 로부터 170.10.0.0 에 대한 업데이트를 받는다. local preference 는 동일 네트워크에 도달하기 위해 AS256 을 빠져 나가는 방법을 결정하는데 도움을 준다. 그림에서 RTD 가 선호되는 출구점(exit point) 이라고 가정할 때, 다음의 구성은 AS 300 에서 오는 업데이트에 대한 local preference 값을 200 으로 세팅하고 AS100 에서 오는 업데이트는 150 으로 세팅한다.



```
/*-- RTC --*/
!
router bgp 256
  bgp default local-preference 150
  neighbor 1.1.1.1 remote-as 100
  neighbor 128.213.11.2 remote-as 256
!

/*-- RTD --*/
!
router bgp 256
  bgp default local-preference 200
  neighbor 3.3.3.4 remote-as 300
  neighbor 128.213.11.1 remote-as 256
!
```

위 구성에서 RTC는 모든 업데이트의 **local preference**를 150으로 세팅하며, RTD는 모든 업데이트의 **local preference**를 200으로 세팅한다. **local preference**는 AS256 내에서 교환되기 때문에, RTC와 RTD는 네트워크 170.10.0.0 정보가 AS100 보다는 AS300에서 오는 정보가 더 높은 **local preference**를 갖는다고 인식하게 된다. 그래서 170.10.0.0으로 지정된 AS256 내의 모든 트래픽은 RTD로 보내진다.

이와는 달리 라우트 맵을 사용하여 더 많은 융통성을 제공할 수 있다. 위 예에서, RTD가 수신하는 모든 업데이트는 **local preference** 200으로 세팅된다. 이것은 바람직하지 않을 수 있다. 아래 구성에서 보여지는 것처럼 특정 업데이트는 특정 **local preference**로 세팅할 필요가 있을 때 라우트 맵을 사용한다.

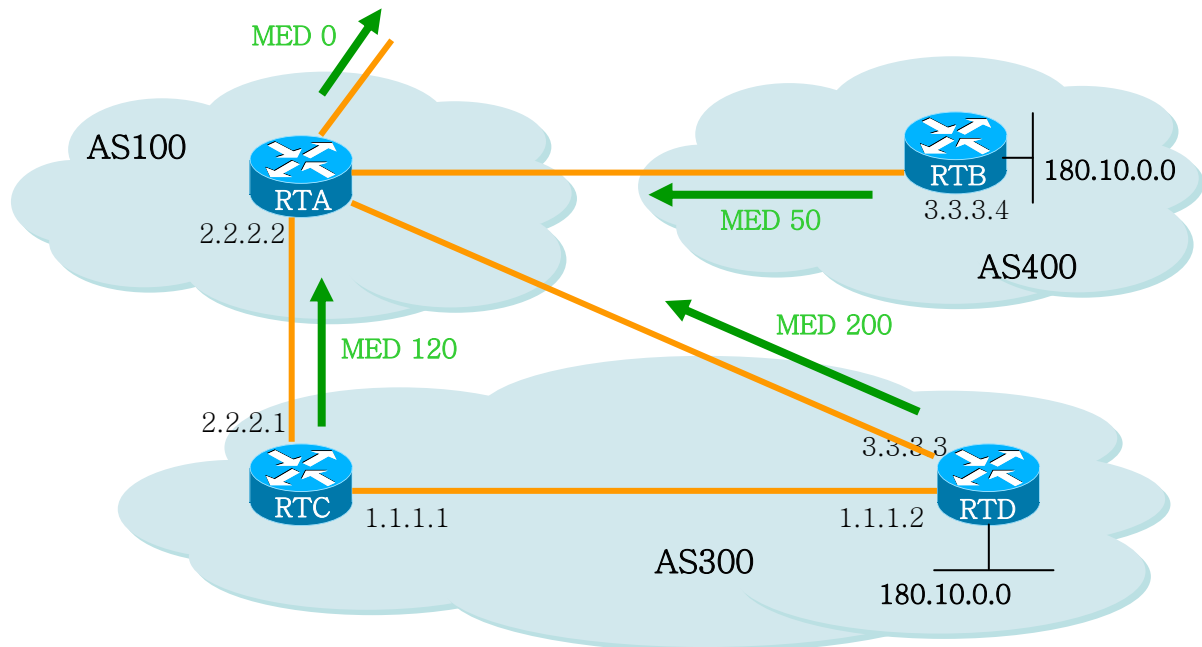
```
/*-- RTD --*/
!
router bgp 256
  neighbor 3.3.3.4 remote-as 300
  neighbor 3.3.3.4 route-map setlocalin in
  neighbor 128.213.11.1 remote-as 256
!
ip as-path access-list 7 permit ^300$
!
route-map setlocalin permit 10
  match as-path 7
  set local-preference 200
!
route-map setlocalin permit 20
  set local-preference 150
!
```

이 구성을 통해, AS300에서 오는 업데이트는 **local preference** 200으로 세팅되고, AS34로부터 오는 다른 업데이트들은 **local preference** 150으로 세팅된다.

Metric Attribute

metric attribute 는 Multi_exit_discriminator(MED)로도 불려지는데, 특정 AS 로 향하는 패스에 대한 선호정보를 외부 네이버에 제공한다. 특정 AS 로의 진입점이 다수 존재시, 그 AS 내의 라우트로 도달하기 위해 어떤 지점을 선택할 지에 대해 타 AS 에 영향을 줄 수 있는 동적인 방법이다. 더 낮은 값을 지닌 경로가 선택된다.

local preference 와 달리, metric 은 AS 들 간에 교환된다. 이 메트릭 값은 하나의 AS 로 전달되지만, 그 AS 를 떠나지는 않는다. 특정 메트릭 값을 지닌 업데이트가 AS 에 들어 왔을 때, 그 메트릭 값은 그 AS 내에서의 경로 선택에 사용된다. 동일한 업데이트 정보가 또 다른 AS 로 전달될 시, 이 메트릭 값은 0 으로 세팅되어 전달된다. 디폴트 값은 0 이다. 다른 특별한 지정이 없는 경우, 동일 AS 상에 있는 네이버들로부터 온 경로에 대해서만 메트릭 값을 비교한다. 서로 다른 AS 에 있는 네이버들로부터 온 메트릭을 비교하기 위해서는 "bgp always-compare-med" 라는 특별한 구성 명령을 필요로 한다.



위 그림에서, AS100 은 3 개의 서로 다른 라우터 RTC, RTD, RTB 를 통해서 180.10.0.0 의 네트워크 정보를 얻고 있다. RTC 와 RTD 는 AS300 에 있고, RTB 는 AS400 에 있다.

RTC 로부터 오는 메트릭 값을 120 으로 세팅하고 RTD 로부터 오는 메트릭 값은 200 으로 RTB 로부터 오는 메트릭 값은 50 으로 세팅 되어 있는 것으로 가정하자. 디폴트로, 라우터는 동일 AS 에 있는 네이버들로부터 오는 메트릭만을 비교한다. 그래서 RTA 는 RTC 와 RTD 로부터 오는 메트릭 만을 비교할 수 있어서 RTC 를 베스트 넥스트 홉으로 선택한다. 왜냐하면 120 이 200 보다 작기 때문이다. RTA 가 RTB 로부터 메트릭 50 을 지닌 정보를 수신 시, RTA 는 이것을 120 과 비교할 수 없다. 왜냐하면 RTC 와 RTB 는 서로 다른 AS 에 있기 때문이다(RTA 는 다른 attribute 들에 기반하여 경로 선택을 한다.).

RTA 가 이 메트릭을 비교할 수 있기 위해서는 RTA 에 **bgp always-compare-med** 명령을 추가한다. 아래에 그 구성이 나와있다.

```
/*-- RTA --*/
!
router bgp 100
 neighbor 2.2.2.1 remote-as 300
 neighbor 3.3.3.3 remote-as 300
 neighbor 4.4.4.3 remote-as 400
!
/*-- RTB --*/
!
router bgp 400
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 route-map setmetricout out
!
route-map setmetricout permit 10
 set metric 50
!

/*-- RTC --*/
!
router bgp 300
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 route-map setmetricout out
 neighbor 1.1.1.2 remote-as 300
!
route-map setmetricout permit 10
 set metric 120
!

/*-- RTD --*/
!
router bgp 300
 neighbor 3.3.3.2 remote-as 100
 neighbor 3.3.3.2 route-map setmetricout out
 neighbor 1.1.1.1 remote-as 300
!
route-map setmetricout permit 10
 set metric 200
!
```

위 구성에서, RTA 는 RTC 를 백스트 홉으로 선택한다. (다른 모든 attribute 들이 동일하다고 가정시). RTB 가 메트릭 비교에 포함되기 위해서는 RTA 를 다음과 같이 구성한다.

```
/*-- RTA --*/
!
router bgp 100
 bgp always-compare-med
 neighbor 2.2.2.1 remote-as 300
 neighbor 3.3.3.3 remote-as 300
 neighbor 4.4.4.3 remote-as 400
```

!

이 경우 RTA는 180.10.0.0에 도달하기 위한 최적의 넥스트 홉으로 RTB를 선택한다.

default-metric number 명령을 사용하여 BGP로 라우트를 **redistribute** 하면서 메트릭 값을 세팅할 수도 있다. 위 예에서 RTB가 스테틱 정보를 **redistribute** 한다고 가정할 경우의 구성은 다음과 같다.

```
/*-- RTB --*/
!
router bgp 400
 redistribute static
 default-metric 50
!
ip route 180.10.0.0 255.255.0.0 null 0
!
!-- Causes RTB to send out 180.10.0.0 with a metric of 50
```

Community Attribute

community attribute는 0에서 4,294,967,200까지의 값을 갖는 optional, transitive attribute이다. community attribute는 여러 개의 목적지들을 특정 community로 그룹화하는 방법인데, 이렇게 그룹화된 커뮤니티에 라우팅 결정(accept, prefer, redistribute 등)을 적용 가능하게 된다.

community attribute를 세팅하기 위해 라우트 맵을 사용할 수 있다. 라우트 맵의 세팅 명령은 다음의 구문을 갖는다.

```
set community community-number [additive]
```

몇 개의 미리 정의된 잘 알려진 커뮤니티들(community-number)로는 다음이 있다.

- **no-export** (Do not advertise to EBGp peers)
- **no-advertise** (Do not advertise this route to any peer)
- **internet** (Advertise this route to the internet community, any router belongs to it)

커뮤니티가 세팅되는 라우트 맵의 예로 다음이 있다.

```
route-map communitymap
 match ip address 1
 set community no-advertise
```

또는

```
route-map setcommunity
 match as-path 1
 set community 200 additive
```

만일 **additive** 키워드가 세팅되지 않은 경우, 200이 기존에 존재하는 커뮤니티 값을 대체한다.

Additive 키워드를 사용하는 경우, 200 이 기존 커뮤니티에 추가된다. 본 시스템에서는 community attribute 를 세팅하면, 이 attribute 는 디폴트로 네이버로 전달된다. 시스코의 경우는 다음의 명령을 사용해야 전달이 된다.

```
neighbor {ip-address|peer-group-name} send-community
```

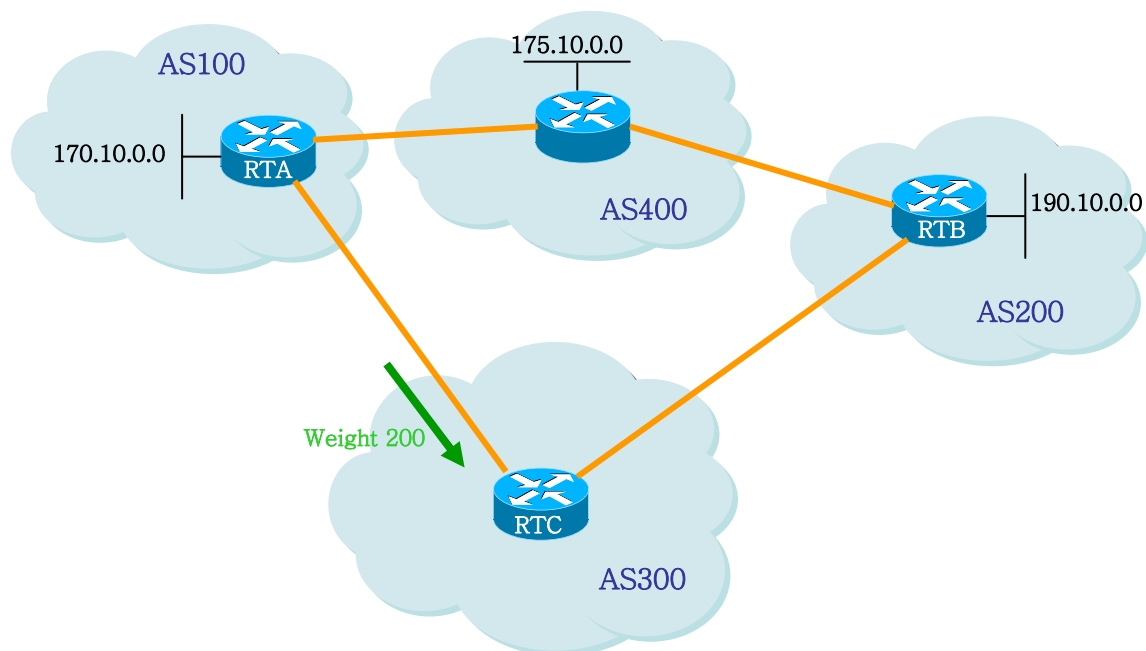
```
/*-- RTA --*/
!
router bgp 100
 neighbor 3.3.3.3 remote-as 300
 neighbor 3.3.3.3 send-community
 neighbor 3.3.3.3 route-map setcommunity out
!
```

앞서 설명한것처럼 neighbor send-community 가 디폴트로 활성화 되어 있어 'neighbor 3.3.3.3 send-community' 명령은 필요치 않다.

Weight Attribute

이 값은 해당 라우터에만 적용된다. 즉, 특정 라우터에만 의미 있는 값이고 다른 라우터로 전달되지 않는다. 이 값은 0 에서 65535 범위 값을 가지며, 자신이 생성한 경로에 대해서는 디폴트로 32768 을 할당한다. 다른 경로들은 0 값을 갖는다.

동일 목적지로 다수의 라우트가 존재시 더 높은 weight 값을 지닌 라우트가 선택된다.



위 그림에서, RTA 는 네트워크 175.10.0.0 에 대한 정보를 AS4 에서 얻었고, 이 정보를 RTC 로 전달한다. RTB 또한 네트워크 175.10.0.0 에 대한 정보를 AS4 에서 얻었고, 이 정보를 RTC 로 전달한다. 이제

RTC 는 네트워크 175.10.0.0 에 도달하는 2 가지 경로를 얻었고 어느 쪽으로 가야할 지를 선택해야 한다. 만일 RTC 에서, RTA 로부터 오는 정보에 RTB 에서 오는 정보 보다 더 높은 **weight** 값을 주면, RTC 는 네트워크 175.10.0.0 에 도달하기 위한 넥스트 홉으로 RTA 를 선택하도록 할 수 있다. 이것은 여러 가지 방법을 이용하여 수행할 수 있다.

- Using the **neighbor** command: **neighbor {ip-address|peer-group} weight weight.**
- Using AS path access-lists: **ip as-path access-list access-list-number {permit|deny} as-regular-expression neighbor ip-address filter-list access-list-number weight weight.**
- Using route-maps.

동일 목적지로의 다수 경로가 존재시, 더 높은 **weight** 값을 가진 경로가 선택된다. 위의 예제에서 RTA 를 넥스트 홉으로 선택하기 위한 구성을 3 가지 방법을 이용하여 구성하였다.

neighbor weight 명령어 사용

```
/*-- RTC --*/
!
router bgp 300
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 weight 200
 !-- route to 175.10.0.0 from RTA has 200 weight
 neighbor 2.2.2.2 remote-as 200
 neighbor 2.2.2.2 weight 100
 !-- route to 175.10.0.0 from RTB will have 100 weight
!
```

IP as-path 와 filter-list 사용

```
/*-- RTC --*/
!
router bgp 300
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 filter-list 5 weight 200
 neighbor 2.2.2.2 remote-as 200
 neighbor 2.2.2.2 filter-list 6 weight 100
!
ip as-path access-list 5 permit ^100$
 !-- this only permits path 100
ip as-path access-list 6 permit ^200$
!
```

라우트 맵 사용

```
/*-- RTC --*/
!
router bgp 300
```

```
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 route-map setweightin in
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 route-map setweightin in
!
ip as-path access-list 5 permit ^100$
!
route-map setweightin permit 10
  match as-path 5
  set weight 200
  !-- anything that applies to access-list 5, such as packets from AS100, have
  weight 200
!
route-map setweightin permit 20
  set weight 100
  !-- anything else would have weight 100
!
```

9.1.5. Routing Policy 변경

Routing policy 라 함은 네이버 라우터와 라우팅 정보를 주고 받을 때 **route-map**, **filter-list**, **prefix-list** 등을 이용하여 받아들일 정보와 제공할 정보에 대한 취사 선택을 할 수 있도록 해주는 것이다. BGP 에서는 이러한 **routing policy** 가 변경되는 경우, 기존 정책을 따르는 라우팅 정보를 삭제하거나 원 경로를 복구하여 새로운 정책에 맞는 라우팅 정보를 갖게 된다.

BGP 라우터가 새로운 정책 **policy** 에 맞는 정보를 받아들이도록 하려면, **inbound reset** 을 설정하여주고, 새로운 정보 제공의 경우에는 **outbound reset** 을 설정한다. 새로운 정책에 맞추어 새로운 정보를 제공하면 네이버 라우터들도 새로운 정보를 받아들인다.

만일 사용자의 망에 위치한 BGP 라우터와 네이버 라우터 모두가 **route refresh capability** 기능을 지원하는 경우라면 **inbound reset** 을 이용하여 라우팅 정보를 갱신할 수 있다. 이 방법을 이용한 라우터 재 설정은 다음과 같은 장점이 있다.

- ✓ 관리자의 추가 설정 동작이 필요 없다.
- ✓ 라우팅 정보 변경에 따른 추가의 메모리 사용이 없다.

네이버 라우터가 **route refresh capability** 기능을 지원하는지 확인 하려면 다음의 명령을 사용한다.

```
neighbor capability route-refresh
```

이 명령을 사용하면, 네이버 라우터에 **route refresh capability** 기능을 알려주고 네이버 라우터도 이 기능을 지원하는 경우, “**Received route refresh capability from peer**” 메시지가 출력된다.

만일 모든 BGP 라우터가 **route refresh capability** 기능을 지원한다면, 사용자는 **soft reset** 을 이용하여

이전에 보낸 경로 정보를 받아 볼 수 있다. 새로운 정책에 부합하는 라우팅 정보를 설정하려면 다음과 같은 명령을 사용한다.

```
clear ip bgp [* | AS | address] soft in
```

반면에 **outbound reset** 기능은 별도의 사전 설정을 필요로 하지 않고, **soft** 라는 명령어를 사용하여 라우팅 정보를 다시 전송할 수 있는데 이 경우 다음의 명령을 사용한다.

```
clear ip bgp [* | AS | address] soft out
```

관리자가 변경된 라우팅 정책을 초기 상태로 복구시에는 **route refresh capability** 기능을 사용한다. 이 기능을 사용하면 각각의 변경된 내용을 하나씩 삭제하지 않아도 된다.

route refresh capability 기능을 지원하지 않는 장비의 경우에는 **neighbor soft-reconfiguration** 명령어를 사용하여 기존에 주고 받던 라우팅 정보를 삭제해야 한다. 그러나 이것은 네트워크에 문제가 발생할 수 있는 소지가 있으므로 가능한 사용하지 않는 것이 좋다.

BGP 정보를 재설정하지 않고 새로운 정보를 생성하려면 라우팅 정보를 선별적으로 처리하지 않고 **BGP** 네트워크로 들어오는 모든 정보를 저장해야 한다. 이 방법은 메모리 부하를 야기 시키기 때문에 가능한 사용하지 않는 것이 좋다. 그러나 변경된 정보를 제공하는 것은 메모리를 요구하지 않는다. **BGP** 라우터가 새로운 변경된 정보를 전달하면 연쇄적으로 네이버 라우터들이 변경된 정보를 받아들 이게 된다.

설정된 **routing policy** 를 이용하여 **BGP** 설정을 바꾸기 위한 절차는 다음과 같다.

- 1) **BGP** 라우터를 재설정 한 후, 네이버 라우터가 보내온 모든 정보를 저장하도록 설정한다. 이 시점부터 **BGP** 라우터에 들어오는 모든 정보는 저장된다.

```
neighbor ip-address soft-reconfiguration inbound
```

- 2) 저장된 정보를 이용하여 새롭게 변경된 정보를 테이블에 등록한다.

```
clear ip bgp [* | AS | address] soft in
```

라우팅 테이블과 **bgp** 네이버 라우터를 통해 라우팅 정보가 제대로 변경 되었는지 확인하려면 다음의 명령을 사용한다.

```
show ip bgp neighbors ip-address [advertised-routes|received-routes|routes]
```

9.1.6. BGP Peer Groups

동일한 업데이트 **policy** 가 적용되는 **BGP** 네이버들의 그룹을 의미한다. 업데이트 폴리시는 주로 라

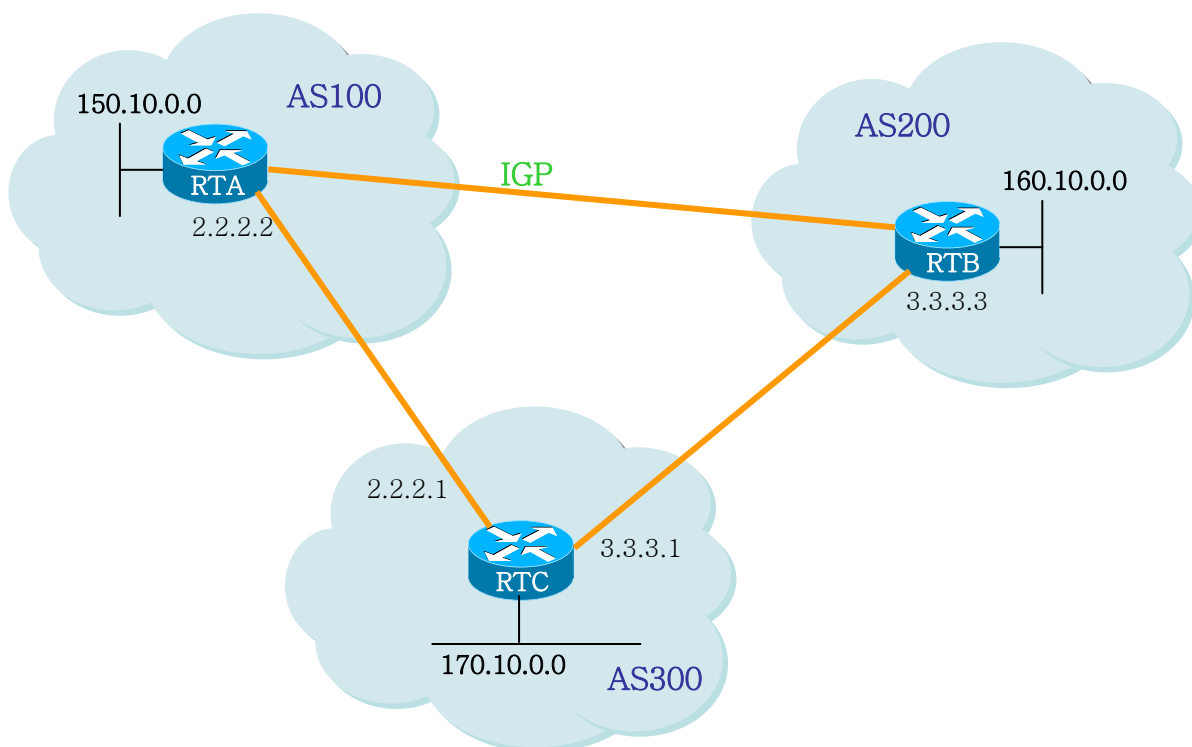
우트 맵, distribute-list, filter-list 에 의해 적용된다. 각각의 별도 네이버에 동일한 폴리스를 정의하는 대신에, Peer group name 을 정의하여 그 피어 그룹에 이러한 폴리스들을 적용한다.

피어 그룹의 멤버들은 그 피어 그룹의 configuration option 모두를 계승한다. 멤버들은 또한 출력 업데이트에 영향을 미치지 않는 옵션이라면 새로운 옵션들을 정의하여 피어 그룹의 옵션을 오버라이드 할 수 있다. 그러나 inbound 쪽에만 옵션들을 오버라이드 할 수 있음을 명심해야 한다.

피어 그룹의 정의를 위해 다음이 사용된다.

neighbor peer-group-name peer-group

BGP backdoor



위의 그림에서 RTA 와 RTC 는 EBGP 로 연결되어 있고, RTB 와 RTC 간에도 EBGP 연결이 되어있다. RTA 와 RTB 는 IGP 프로토콜(OSPF, RIP 등)을 돌리고 있다. EBGP 업데이트는 IGP distance 값보다 작은 20 의 distance 값을 갖는다. 참고로 RIP 경우는 디폴트 distance 값이 120 이고, OSPF 는 110 의 값을 갖는다.

RTA 는 두 개의 라우팅 프로토콜을 통해 160.10.0.0 에 대한 업데이트 정보를 수신한다. 이 중 하나는 distance 값 20 을 갖는 EBGP, 다른 하나는 distance 값이 20 보다 큰 값을 갖는 IGP 정보이다.

디폴트로, BGP 는 다음의 distance 값을 갖지만 다음의 distance command 에 의해 변경될 수 있다.

```
distance bgp external-distance internal-distance local-distance
external-distance:20
```



```
internal-distance:200
```

```
local-distance:200
```

RTA 는 더 낮은 **distance** 값을 지닌 **RTC** 를 통해 받은 **EBGP** 업데이트 정보를 선택한다. 만일 **RTA** 가 **160.10.0.0** 에 대한 정보를 **RTB** 를 통해(즉, **IGP** 를 통해) 받기를 원한다면, 두 가지 행동을 취할 수 있다.

- ✓ **EBGP**의 **external distance** 값이나 **IGP**의 **external distance** 값을 바꾼다.(바람직하지 않음)
- ✓ **BGP backdoor** 사용

이처럼 **BGP backdoor** 는 **IGP** 라우트를 선호 라우트로 만들어 준다. 이를 위해 다음의 명령을 사용한다.

```
network address backdoor
```

지정되는 주소 값은 **IGP** 를 통해 수신하고자 하는 네트워크 주소이다. **BGP** 의 경우, 이 네트워크는 **BGP** 업데이트에서 전달되지 않는다는 점을 제외하면 로컬로 할당된 네트워크처럼 취급된다.

```
/*-- RTA --*/
!
router ospf
!
router bgp 100
  neighbor 2.2.2.1 remote-as 300
  network 160.10.0.0 backdoor
!
```

네트워크 **160.10.0.0** 은 로컬 엔트리로 취급되지만, 보통의 네트워크 엔트리처럼 전달되지는 않는다. **RTA** 는 **distance** 값 110 을 가진 **OSPF** 를 통해 **RTB** 로부터 **160.10.0.0** 에 대한 정보를 취득한다. 그리고 동시에 **distance** 값 20 을 지닌 **EBGP** 를 통해 **RTC** 로부터도 취득한다. 보통은 **EBGP** 가 선호되지만 **backdoor** 명령 때문에 **OSPF** 정보가 선택된다.

9.1.7. BGP Multipath

BGP Multipath 는 동일한 목적지에 대해서 여러 **BGP** 경로를 갖는 것을 허락한다. 이 경로들은 **Load Sharing** 을 위해서 **best path** 와 함께 라우팅 테이블에 설정된다. **BGP Multipath** 는 **best path** 를 선정하는데 영향을 주지 않는다. 예를 들어서, 라우터는 **Multi-Path** 중에서 하나를 **best path** 로서 지정한다. 그리고 그 **best path** 를 **neighbors** 에게 **advertise** 한다.

Multipath 의 후보가 되기 위해서, 동일한 목적지를 갖는 **path** 들은 **best path** 와 다음의 조건들이 동일해야 한다.

```
Weight
Local preference
AS-PATH length
```

Origin
MED

One of these:

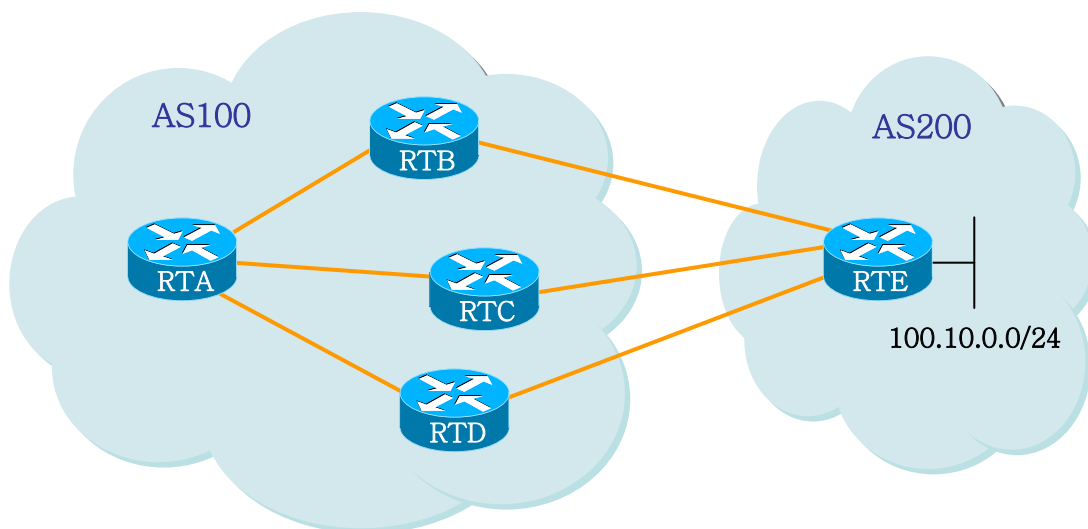
- Neighboring AS or sub-AS (before the addition of the eIBGP Multipath feature)
- AS-PATH (after the addition of the eIBGP Multipath feature)

몇몇 BGP Multipath 특징들은 multipath 후보들에 추가적인 요구사항이 있다.
다음은 eBGP multipath에 대한 추가적인 요구사항이다.

- ✓ 그 경로는 external or confederation-external neighbor로부터 배워야 한다.
- ✓ BGP nexthop에 대한 IGP metric은 best path의 IGP metric과 동일해야 한다.

다음은 iBGP multipath에 대한 추가적인 요구사항이다.

- ✓ 그 경로는 internal neighbor로부터 배워야 한다.
- ✓ BGP nexthop에 대한 IGP metric은 best path의 IGP metric과 동일해야 한다.



위의 그림에서 RTA는 네트워크 100.1.1.0/24를 RTB, RTC, RTD로부터 받게 된다. 라우터는 디폴트로 multipath 기능이 disable 되어 있다. 따라서 multipath 기능을 사용하기 위해서 다음의 명령어를 사용한다.

maximum-path [ibgp] number

Multipath 기능을 사용하기 위해 RTA에서 다음과 같이 설정을 한다.

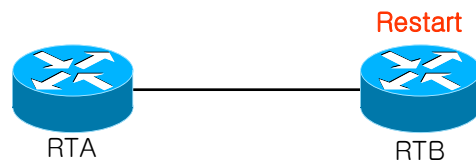
```

/*-- RTA --*/
!
router bgp 100
 maximum-paths ibgp 3
 neighbor 10.1.1.1 remote-as 200 /* RTB */
 neighbor 20.1.1.1 remote-as 200 /* RTC */
 neighbor 30.1.1.1 remote-as 200 /* RTD */
!
    
```

9.1.8. BGP graceful-restart

보통, 어떤 라우터의 BGP가 restart 했을 때, 그 BGP와 연결된 모든 BGP Peer들은 session이 down되었다가 다시 up되는 것을 감지한다. 이러한 “down/up”은 “routing flap”을 초래하고, BGP route의 재계산을 야기시킨다. 또한, “routing flaps”은 일시적으로 forwarding black hole과 forwarding loop을 발생시킬 수 있다. 이러한 것들로 인해, 전체 네트워크의 성능에 부정적인 영향을 끼치게 된다.

BGP graceful restart는 BGP restart에 의해서 야기되는 부정적인 영향들을 최소화시키는 것들을 돕는 메커니즘이다. 이 메커니즘은 BGP가 restart하는 동안, BGP speaker가 forwarding state를 보존시키도록 한다.



위 그림은 RTB가 BGP restart를 하고 RTA가 BGP graceful-restart를 처리하도록 한다. BGP graceful-restart는 default로 disable되어 있다. 따라서 이 기능을 사용하기 위해서 다음의 명령어를 설정해야 한다. stalepath-time은 Local BGP가 restarting Peer에 대해, stale-path를 hole하고 있는 최대 시간이다. stalepath-time에 명시된 시간 동안 restarting Peer가 route를 update하지 않으면 stale path는 지워진다.

```
bgp graceful-restart [stalepath-time seconds]
```

BGP graceful-restart 기능을 사용하기 위해 RTA에서 다음과 같이 설정을 한다.

```
/*-- RTA --*/
!
router bgp 100
  bgp graceful-restart stalepath-time 200
  neighbor 10.1.1.1 remote-as 200 /* RTB */
!
```

9.1.9. BGP default-metric

default metric은 incompatible metric과 함께 재분배 되는 라우트들의 문제를 해결하기 위해 사용된다. 이 값은 MED(Multi Exit Discriminator)으로써 best path selection 을 계산하는데 영향을 준다. MED는 Local AS에서만 처리되는 non-transitive 값이다. 따라서 External AS에는 이 값이 전달되지 않는다.

다음은 이 기능이 설정 되지 않았을 때, 기본적인 metric 설정을 나타낸다.

- 재분배된 IGP 라우트의 metric 은 interior BGP metric 과 동일하게 설정된다.
- 재분배된 connected 와 static 라우트의 metric 은 0 으로 설정된다.
- 그리고 이 기능이 설정되었을 때 재분배된 connected 라우트의 metric 은 0 으로 설정된다.

이 기능을 사용하기 위해서 다음의 명령어를 설정해야 한다.

```
default-metric number
```

9.1.10. BGP redistribute-internal

OSPF, RIP와 같은 IGP에서 redistribute bgp 가 설정되어있는 경우 iBGP로 얻은 route 가 같은 IGP인 OSPF나 RIP에 redistribute이 되어 loop 이 발생할 수 있게 된다.. 이러한 상황을 방지하기 위해 default 로 redistribute bgp 가 설정되어 있어도 iBGP route은 redistribute을 하지 않도록 한다.

강제적으로 iBGP route가 redistribute 되기를 원하는 경우 이 명령어를 사용한다.

```
bgp redistribute-internal
```

9.1.11. BGP Password encryption

neighbor에 password를 지정하여, TCP 연결에 대한 인증 기능을 사용할 수 있다.

Password가 일치하면, neighbor 사이에 TCP session이 연결 되고 메시지 통신을 하게 된다.

```
neighbor ip-address password KEY  
neighbor ip-address password 0 KEY  
neighbor ip-address password 7 KEY
```

neighbor의 password는 encryption가능하며, 암호화 전에 설정된 password의 level은 0이고, 암호 후에 7로 변경 된다.

단, 사용자가 암호화 전에 password를 level 7로 설정할 수는 없다.

9.1.12. BGP disable-adj-out

E7500 SERIES은 기본적으로 out bound table을 유지하지 않는다. 이것은 메모리의 overhead를 줄이기 위한 정책이다. 만약 이 기능을 사용하지 않기 위해서는 Config Mode에서 다음의 명령어를 입력해야 한다.

```
no bgp disable-adj-out
```

Notice Out bound table 을 유지하지 않을 때, “show ip bgp neighbors *ip-address* advertised-routes” 명령어는 사용할 수 없다.

9.1.13. Use of set as-path prepend Command

어떤 상황에서는 BGP decision process를 조절하기 위해 경로 정보를 조정해야만 할 때가 있다. 이를 위해 라우트 맵과 함께 사용되는 명령은 다음과 같다.

```
set as-path prepend <As-path#><As-path#> ...
```

9.3. Route Flap Dampening

route dampening 은 라우트 플래핑과 네트워크 상의 오실레이션에 의해 야기되는 불안정성을 최소화하고자 하는 메커니즘이다. 이를 위해 부적절하게 동작하는 라우트들을 정의하는 원칙이 정의된다. 플래핑 하는 라우트는 각 플랩마다 패널티 값(디폴트 1000)을 얻는다. 이렇게 축적된 패널티 값이 미리 정의된 “suppress-limit” 값을 넘으면, 이 라우트의 전달은 중지된다. 이 패널티 값은 미리 정의된 “half-time”에 도달하면 절반씩 감소되는데, 5 초마다 절반씩 감소된다. 감소된 패널티 값이 미리 정의된 “reuse-limit” 값 이하에 도달하면, 이 라우트는 다시 전달된다.

IBGP 를 통해 습득된 외부 라우트들은 dampening 되지 않음을 유의해야 한다. 그리고 dampening 정보는 패널티 값이 “reuse-limit” 값의 절반 이하가 될 때까지는 계속해서 라우터에 유지가 된다.

초기에 route dampening 은 디폴트로 오프상태이다. 다음의 명령들이 route dampening 을 조절하는데 사용된다.

- **bgp dampening** (will turn on dampening)
- **no bgp dampening** (will turn off dampening)
- **bgp dampening <half-life-time>** (will change the half-life-time)

동시에 모든 파라미터들을 바꾸는 명령은,

- **bgp dampening <half-life-time> <reuse> <suppress> <maximum-suppress-time>**
- **<half-life-time>** (range is 1-45 min, current default is 15 min)
- **<reuse-value>** (range is 1-20000, default is 750)

- <suppress-value> (range is 1-20000, default is 2000)
- <max-suppress-time> (maximum duration a route can be suppressed, range is 1-255, default is 4 times half-life-time)

다음은 route dampening 에 사용되는 용어를 정리하였다.

표 9-1. route dampening 에 사용되는 용어

항목	내용
History state	해당 route 에 대한 best path 를 갖고 있지는 않지만, 여전히 해당 라우트 플래핑에 대한 정보는 존재하는 상태
Damp state	패널티 값이 한계치를 초과 한 상태로 네이버에게 정보 전달이 안된다.
Penalty	라우트 플래핑이 발생시 마다 이 라우트에 부과되는 점수로 디폴트 값이 1000 이다. 이 점수는 누적되고, 한계치(suppress limit)가 초과되면 상태가 'history'에서 'damp' 상태로 변한다
Suppress limit	route 에 부과되는 패널티 값의 한계치로 디폴트 2000 이다
Half-life-time	route 에 부과된 패널티 값은 half-life-time 에 설정된 시간(디폴트 15 분)이 지나면 반으로 줄어드는데, 이러한 감소는 5 초마다 행해진다.
Reuse-limit	플래핑에 부과된 패널티 값이 줄어 들어서 이 값을 밑돌게 되면 무효화된 경로는 복구된다. 해당 라우트가 다시 BGP 테이블에 복구되어 전달되어진다. 디폴트 값은 750 이고, 경로 무효화를 해제하는 절차는 10 초마다 수행된다
Maximum suppress limit	라우트가 무효화될 수 있는 최대 시간이고, 기본 값은 half-lif-time 의 4 배이다.

10

IGMP Snooping

본 장에서는 IGMP Snooping 설정에 대해 설명한다.

10.1. IGMP Snooping 개요

일반적으로 Multicast Traffic 은 Unknown MAC address 나 Broadcast Frame 으로 처리되어 VLAN interface 에 속한 모든 Member interface 로 flooding 된다.

IGMP Snooping 은 VLAN interface 내의 모든 Member interface 로 Multicast Traffic 을 Forwarding 하지 않고, Multicast Traffic 을 Forwarding 할 Member interface 들을 dynamic 하게 추가/삭제함으로써 Network 의 Bandwidth 를 효율적으로 사용할 수 있도록 해준다. IGMP Snooping 을 적용하면 IGMP Host 와 Multicast Router 간의 IGMP 메시지들을 snooping 하여, Multicast Group 과 VLAN interface 의 어느 Member interface 인지 에 대한 정보를 얻어낸다.

IGMP Snooping 의 절차에 대해서 간략히 설명하면 다음과 같다. 특정 Multicast Group 에 대한 IGMP Join 메시지를 받으면, 해당 IGMP Host 가 연결된 VLAN interface 의 member interface 를 Multicast Forwarding Table Entry 에 추가한다. 그 IGMP Host 로부터 IGMP Leave 메시지를 받으면 반대로 그 IGMP Host 와 연결된 VLAN interface 의 member interface 를 Multicast Forwarding Table Entry 에서 제거한다. 또한, Multicast Router 로부터 수신되는 IGMP Query 메시지를 VLAN interface 내의 모든 member interface 로 Forwarding 한 후, IGMP Join 메시지를 받지 못해서 Update 되지 않은 Multicast Forwarding Table 의 member 들은 삭제된다.

10.2. IGMP Snooping 설정

IGMP Snooping 은 기본적으로 multicast-routing 이 Global 하게 enable 되어 있어야 동작한다.

10.2.1. Enable IGMP Snooping on a VLAN

IGMP Snooping 은 VLAN 별로 설정할 수 있으며, 다음의 명령을 interface configuration mode 에서 사용한다.

명령어	설명
ip igmp snooping	해당 VLAN 에 IGMP Snooping 을 enable 한다.
no ip igmp snooping	해당 VLAN 에 IGMP Snooping 을 disable 한다.

```

Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp snooping
Router(config-if-Vlan22)# end
Router# show ip igmp interface
.....
Interface Vlan22 (Index 2022)
  IGMP Enabled, Active, Non-Querier, Version 2 (default)
  Internet address is 220.1.1.222
  IGMP interface has 10 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP querying router is 0.0.0.0
  IGMP query interval is 125 seconds
  IGMP querier timeout is 262 seconds
  IGMP max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
.....
Router#

```


10.2.2. Configure IGMP Snooping Functionality

다양한 IGMP Snooping 기능들을 설정하기 위해서, 다음에 나오는 작업들을 수행한다.

10.2.2.1. IGMP Report-Suppression

특정 VLAN Interface 에 IGMP Snooping 을 적용하면, IGMP Report-suppression 은 기본적으로 Enable 된 상태이며, IGMP Membership 마다 하나의 IGMP Report 만 Multicast Router 로 Forwarding 된다. IGMP Report-suppression 을 Disable 하면, 수신하는 모든 IGMP Report 들을 Multicast Router 로 Forwarding 한다.

이 기능은 IGMPv1 및 IGMPv2 메시지에 한해서 적용되며, 아래의 명령을 interface configuration mode 에서 실행한다.

명령	설명
ip igmp snooping report-suppression	VLAN interface 에 IGMP report-suppression 을 설정한다.
no ip igmp snooping report-suppression	VLAN interface 에 설정된 IGMP report-suppression 을 해제한다.

```
Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# no ip igmp snooping report-suppression
Router(config-if-Vlan22)# end
Router# show ip igmp interface
.....
Interface Vlan22 (Index 2022)
  IGMP Enabled, Active, Non-Querier, Version 2 (default)
  Internet address is 220.1.1.222
  IGMP interface has 10 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP querying router is 0.0.0.0
  IGMP query interval is 125 seconds
  IGMP querier timeout is 262 seconds
  IGMP max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is disabled
.....
```

Router#

10.2.2.2. IGMP Fast-Leave

IGMP Fast-Leave 기능을 enable 하면 호스트로부터 IGMPv2 Leave 메시지를 받았을 때 해당 VLAN의 Membership interface 를 Multicast forwarding table 에서 즉시 제거한다.

IGMP Fast-Leave 기능은 VLAN interface 의 각 포트에 호스트가 하나인 경우에만 사용하여야 한다. 만약, 포트에 여러 호스트가 속해 있는 경우에 이 기능을 사용하면, IGMPv2 Leave 메시지를 보내지 않은 호스트들도 일정시간 동안 Leave 가 된 멀티캐스트 그룹에 대한 트래픽을 받지 못하게 되는 경우가 발생하게 된다. 또한, 이 기능은 모든 호스트들이 Leave 메시지가 지원되는 IGMPv2 를 사용하는 경우에만 유효하다.

명령	설명
ip igmp snooping fast-leave	해당 VLAN 에 fast-leave 기능을 설정한다.
no ip igmp snooping fast-leave	해당 VLAN 에 설정된 fast-leave 를 해제한다.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp snooping fast-leave
Router(config-if-Vlan22)# end
Router# show ip igmp interface
.....
Interface Vlan22 (Index 2022)
  IGMP Enabled, Active, Non-Querier, Version 2 (default)
  Internet address is 220.1.1.222
  IGMP interface has 10 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP querying router is 0.0.0.0
  IGMP query interval is 125 seconds
  IGMP querier timeout is 262 seconds
  IGMP max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is enabled on this interface
  IGMP Snooping fast-leave is enabled
```

```

IGMP Snooping querier is not enabled
IGMP Snooping report suppression is enabled
.....
Router#
    
```

10.2.2.3. IGMP Mrouter-Port

VLAN interface 내의 Mrouter Port 를 제외한 모든 Member port 로부터 수신되는 Multicast Traffic 들과 IGMP 메시지들은 Multicast Router 로 전달되어야 한다. 따라서, Multicast Router 와 연결된 VLAN Interface 의 Mrouter Port 는 모든 Multicast Forwarding Table Entry 의 Traffic forwarding port 로 추가 된다.

기본적으로 IGMP Snooping 은 IGMP 메시지를 Snooping 하여 Multicast Router 와 연결된 Mrouter Port 를 감지한다.

새로운 Multicast Forwarding Table Entry 가 생성될 때마다 Mrouter port 는 항상 traffic forwarding port 로 등록되며, Multicast Traffic 뿐만 아니라 IGMP Host 에서 전송하는 IGMP 메시지도 Forwarding 된다.

Multicast Router Port 를 Static 하게 설정하기 위해서는 다음의 명령을 interface configuration mode 에서 수행한다.

명령어	설명
ip igmp snooping mrouter interface IFNAME	해당 VLAN 에 mrouter port 를 수동으로 설정한다. IFNAME 은 이미 VLAN 내의 Member-Port 여야 한다.
no ip igmp snooping mrouter interface IFNAME	해당 VLAN 에 설정된 mrouter port 를 해제한다.

```

Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp snooping mrouter interface gi2/2/5
Router(config-if-Vlan22)# end
Router# show ip igmp snooping mrouter vlan22
VLAN Interface
22 Giga2/2/5

Router#
    
```

10.2.2.4. IGMP Access-Group

IGMP Snooping 은 특정 인터페이스에서 수신되는 IGMP Host 들의 특정 그룹을 제한할 수 있다.

IGMP Host 의 멀티캐스트 그룹을 제한하기 위해서는 아래의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip igmp snooping access-group <access-list>	해당 포트에 수신되는 호스트들의 멀티캐스트 그룹에 대한 등록을 제한한다.
no ip igmp snooping access-group <access-list>	해당 포트에 수신되는 제한된 호스트들의 멀티캐스트 그룹에 대한 등록을 해제한다.

```
Router# configure terminal
Router(config)# access-list 10 permit 225.1.1.1
Router(config)# access-list 10 deny any
Router(config)# interface gi3/1/2
Router(config-if-Giga3/1/2)# ip igmp snooping access-group 10
Router(config-if-Giga3/1/2)# end
Router#
```

해당 인터페이스가 여러 VLAN interface 의 member 인 경우, 특정 VLAN interface 에서만 IGMP Host 들의 멀티캐스트 그룹을 제한할 수 있으며 아래의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip igmp snooping access-group <access-list> vlan <vlan-id>	지정된 VLAN Interface 의 member interface 로 수신되는 IGMP Host 들의 멀티캐스트 그룹에 대한 등록을 제한한다.
no ip igmp snooping access-group <access-list> vlan <vlan-id>	지정된 VLAN Interface 의 member interface 로 수신되는 IGMP Host 들의 제한된 멀티캐스트 그룹에 대한 등록을 해제한다.

```
Router# configure terminal
Router(config)# access-list 10 permit 225.1.1.1
Router(config)# access-list 10 deny any
Router(config)# interface gi3/1/2
Router(config-if-Giga3/1/2)# ip igmp snooping access-group 10 vlan 22
Router(config-if-Giga3/1/2)# end
```

```
Router#
```

10.2.2.5. IGMP Group-Limit

IGMP Snooping 은 각각의 interface 별로 Multicast Group 의 개수를 제한할 수 있다.

Multicast Group 의 개수를 제한하기 위해서는 다음의 명령을 interface configuration mode 에서 수행한다.

명령어	설명
ip igmp snooping limit <count>	해당 포트에 수신되는 Multicast Group 의 개수를 제한한다.
ip igmp snooping limit <count> except <access-list>	해당 포트에 수신되는 Multicast Group 의 개수를 제한한다. 제한하지 않을 Group 은 access-list 로 만들어 지정한다.
no ip igmp snooping limit <count>	해당 포트에 설정된 Multicast Group 의 개수 제한을 해제한다.

```
Router# configure terminal
Router(config)# interface gi3/1/2
Router(config-if-Giga3/1/2)# ip igmp snooping limit 10
Router(config-if-Giga3/1/2)# end
Router#
```

해당 인터페이스가 여러 VLAN interface 의 member 인 경우, 특정 VLAN interface 에서만 Multicast Group 의 개수를 제한할 수 있으며 아래의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip igmp snooping limit <count> vlan <vlan-id>	해당 포트에서 해당 VLAN 으로 수신되는 Multicast Group 의 개수를 제한한다.
ip igmp snooping limit <count> vlan <vlan-id> except <access-list>	해당 포트에서 해당 VLAN 으로 수신되는 Multicast Group 의 개수를 제한한다. 제한하지 않을 Group 은 access-list 로 만들어 지정한다.
no ip igmp snooping limit <count> vlan <vlan-id>	해당 포트에서 해당 VLAN 으로 수신되는 Multicast Group 의 개수 제한을 해제한다.

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)# interface gi3/1/2  
Router(config-if-Giga3/1/2)# ip igmp snooping limit 10 vlan 22  
Router(config-if-Giga3/1/2)# end  
Router#
```

10.3. Display System and Network Statistics

표 10-1. IGMP Snooping 관련 모니터링 명령어

명령어	설명
show ip igmp snooping mrouter <IFNAME>	해당 VLAN 에 대한 mrouter port 를 보여준다.
show ip igmp snooping statistics	IGMP snooping 의 통계 정보를 보여준다

11

IP 멀티캐스트 라우팅

본 장에서는 IP 멀티캐스트 라우팅의 구성요소와 IP 멀티캐스트 라우팅 설정에 대해 설명한다.

11.1. IP 멀티캐스트 라우팅 개요

IP 멀티캐스팅은 하나의 IP 호스트가 여러 IP 호스트들로 구성된 하나의 그룹으로 패킷을 전송할 수 있게 하는 기능이다. 이 호스트들의 그룹은 로컬 네트워크에 있는 장비들, 사설 망 내에 있는 장비들, 또는 로컬 네트워크 바깥의 장비들을 포함할 수 있다. 트래픽을 생성하는 호스트에서는 트래픽을 받고자하는 호스트들에 대해 각각의 패킷을 전송하는 것이 아니라 하나의 패킷만을 그 그룹으로 전송하는 것이다.

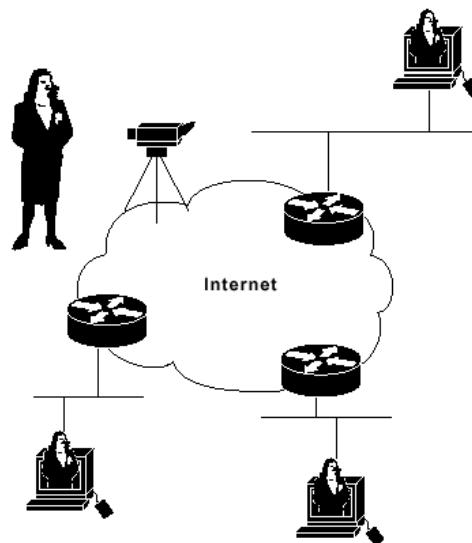


그림 11-1. 여러 목적지에 트래픽을 전달하는 방법을 제공하는 멀티캐스팅

여러 멀티캐스트 라우팅 프로토콜들은 멀티캐스트 그룹을 발견하고 각 그룹에 대한 경로를 생성하기 위해 사용된다. 예를 들면, Protocol-Independent Multicast (PIM), Distance-Vector Multicast Routing Protocol(DVMRP), Multicast Open Shortest Path First (MOSPF)와 같은 것들이 있다. 다음 <표-1 >은 각 프로토콜의 유니캐스트에 대한 요구 사항과 flooding 알고리즘을 요약한 것이다.

표 11-1. 멀티캐스트 프로토콜

프로토콜	유니캐스트 프로토콜	flooding 알고리즘
PIM-dense mode	Any	Reverse path flooding (RPF)
PIM-sparse mode	Any	RPF
DVMRP	Internal	RPF
MOSPF	OSPF	Shortest-path first

11.2. IGMP 개요

IGMP는 IP 호스트가 IP 멀티캐스트 그룹 멤버십을 라우터에 등록하기 위해 사용되는 프로토콜이다. 라우터는 등록된 그룹의 멤버십 상태를 갱신하기 위하여 주기적으로 멤버십 질의를 한다. IP 호스트가 질의에 응답을 하면 그 그룹의 등록은 유지된다.

IP 멀티캐스트에서 사용되는 멀티캐스트 그룹 주소로 class D IP 주소가 사용되며 IGMPv2는 RFC1112에 정의되어 있다.

11.3. PIM-SM 개요

PIM-SM은 다수의 멀티캐스트 데이터 스트림에 대해서 비교적 적은 수의 LAN들을 연결하기 위해 최적화된 멀티캐스트 라우팅 프로토콜이다. PIM-SM은 Rendezvous Point를 정의하는데 이것은 멀티캐스트 패킷의 라우팅을 편리하게 하기 위한 등록점으로 사용된다.

특정 멀티캐스트 서버가 인접한 멀티캐스트 라우터로 멀티캐스트 패킷을 전송하면, 인접한 멀티캐스트 라우터는 이 멀티캐스트 패킷을 rendezvous point로 보낸다. 멀티캐스트 패킷을 수신하고자 하는 멀티캐스트 라우터는 rendezvous point로부터 해당 멀티캐스트 패킷을 수신하여 호스트로 전송하게 된다.

PIM-SM v2는 PIM-SM v1에 대해 다음과 같은 개선점이 포함되었다.

- ✓ bootstrap router (BSR)은 fault-tolerant한, 자동적인 RP discovery와 distribution 메커니즘을

제공한다. 그러므로, 라우터들은 별도의 설정이 없이도 동적으로 **group-to-RP** 매핑을 할 수가 있다.

- ✓ PIM Join/Prune 메시지에 여러 **address family** 에 대한 유연한 인코딩이 가능하다.
- ✓ PIM 패킷은 더 이상 IGMP 패킷에 포함되지 않는다.

PIM-SM 은 PIM-SM 도메인의 모든 라우터들에 대한 각 그룹 **prefix** 에 대한 **RP-set** 정보를 발견하고 이를 공고하기 위하여 **BSR** 을 사용한다.

“Single point of failure”를 방지하기 위하여, PIM-SM 도메인 내에 여러 **candidate BSR** 를 설정할 수 있다. BSR 은 candidate BSR 들 중에서 자동적으로 선출된다. **bootstrap** 메시지를 이용하여 가장 우선순위가 높은 BSR 를 알아낸다. BSR 로 선출된 라우터는 PIM 도메인 내의 모든 라우터들에게 자신이 BSR 임을 알린다

Candidate RP 로 설정된 라우터들은 자신이 맡을 **group** 의 범위를 BSR 에게 유니캐스트로 알린다. BSR 은 bootstrap 메시지에 이 정보를 포함시키고 도메인 내의 모든 PIM 라우터들에 이 메시지를 전송한다. 이 정보를 바탕으로 모든 라우터는 특정 멀티캐스트 그룹에 대한 **RP** 를 알아낼 수 있게 된다. 라우터가 bootstrap 메시지를 받는 한, 라우터는 현재의 **RP map** 을 가지게 되는 것이다.

11.4. IP 멀티캐스트 라우팅 설정

11.4.1. Enable IP 멀티캐스트 라우팅

기본적으로 멀티캐스트 패킷을 포워딩하기 위해서는 IP 멀티캐스트 라우팅이 설정되어야 한다. 다음의 명령을 **global configuration mode** 에서 사용한다.

명령어	설명
ip multicast-routing	Multicast Routing 을 위한 IGMP, IGMP Snooping, PIM-SM 을 enable 시킨다.
no ip multicast-routing	Multicast Routing 을 위한 IGMP, IGMP Snooping, PIM-SM 을 disable 시킨다.

```
Router# configure terminal
Router(config)# ip multicast-routing
Router(config)#
```

11.4.2. Enable IGMP and PIM on an interface

특정 인터페이스에서 IGMP 와 PIM-SM 의 실행을 위해서는 반드시 해당 인터페이스에 PIM Sparse-Mode 를 enable 해야 한다. 해당 인터페이스에서 IGMP 와 PIM Sparse-Mode 를 enable 하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip pim sparse-mode	해당 인터페이스의 PIM Sparse-Mode 를 enable 한다.
no ip pim sparse-mode	해당 인터페이스의 PIM Sparse-Mode 를 Disable 한다.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1/1
Router(config-if-Giga2/1/1)# ip pim sparse-mode
Router(config-if-Giga2/1/1)# end
Router# show ip pim sparse-mode interface
Address          Interface  VIFindex  Ver/   Nbr    Query  DR    DR
                  Mode      Count    Intvl  Prior
2.1.1.1          Giga2/1/1  0         v2/S   0      30     1     2.1.1.1
Router#
Router# show ip igmp interface
Interface Giga2/1/1 (Index 1211)
  IGMP Active, Querier, Version 2 (default)
  Internet address is 2.1.1.1
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP query interval is 125 seconds
  IGMP querier timeout is 262 seconds
  IGMP max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is not enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
Router#
```

11.4.3. Configure Multicast Functionality

Multicast의 다양한 특성들에 대해 설정하기 위해서는 다음에 나오는 작업들을 수행한다.

11.4.3.1. Router-Guard IP Multicast

Router-Guard IP Multicast는 가입자 Network으로 지정된 인터페이스로 수신되는 Multicast Control Packet들 중에서 Multicast Router에서 발생할 수 있는 packet들을 차단하고 통계한다.

Router-Guard IP Multicast는 아래와 같은 multicast control packet들을 차단한다.

- IGMP Query Message
- PIM Message
- DVMRP Message

Router-Guard IP Multicast 기능을 설정하기 위해서는 아래의 명령을 interface configuration mode에서 실행한다.

명령어	설명
router-guard ip multicast	해당 인터페이스에 Router-Guard IP Multicast 기능을 설정한다.
router-guard ip multicast vlan <1-4093>	VLAN의 특정 Member 인터페이스만 Router-Guard IP Multicast 기능을 설정한다.
no router-guard ip multicast	설정된 인터페이스의 Router-Guard IP Multicast 기능을 해제한다.
no router-guard ip multicast vlan <1-4093>	설정된 VLAN의 특정 Member 인터페이스의 Router-Guard IP Multicast 기능을 설정한다.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 3/1/3
Router(config-if-Giga3/1/3)# router-guard ip multicast
Router(config-if-Giga3/1/3)# interface GigabitEthernet 2/1/2
Router(config-if-Giga2/1/2)# router-guard ip multicast vlan 22
Router(config-if-Giga2/1/2)# end
Router# show router-guard ip multicast

Globally enabled on interface gi3.1.3
Drop statistics
  IGMP Queries      : 0
  PIM Messages      : 0
  DVMRP Messages    : 0
  Invalid Messages  : 0

Enabled on interface gi2.1.2, vlan22
```

```
Drop statistics
  IGMP Queries      : 0
  PIM Messages      : 0
  DVMRP Messages    : 0
  Invalid Messages  : 0
Router#
```

11.4.3.2. Multicast Traffic Forwarding-TTL-Limit

Multicast Router 에서 관리되는 Multicast Traffic Forwarding 은 RPF interface 로부터 수신된 multicast traffic 을 downstream interface 로 전달하면서 TTL 을 1 씩 감소하며, 감소된 TTL 이 0 인 경우 drop 한다.

Multicast Router 에서 forwarding 되는 multicast traffic 의 TTL 에 대해서 특정 TTL 값을 지정하여 그 값 이하의 TTL 을 가진 multicast traffic 이 RPF interface 로부터 incoming 되었을 때 forwarding 하지 않도록 설정할 수 있다.

Multicast Traffic 에 대해서 forwarding 을 하지 못하도록 하기 위해서는 TTL 을 RPF Interface 에 적용해야 한다.

Multicast Traffic Forwarding 에 대한 TTL 을 설정하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip multicast ttl-threshold <1-255>	Multicast Traffic 에 대해서 TTL 제한을 적용한다.
no ip multicast ttl-threshold	적용된 Multicast Traffic 에 대한 TTL 제한을 해제한다.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 3/1/3
Router(config-if-Giga3/1/3)# ip multicast ttl-threshold 10
Router(config-if-Giga3/1/3)# end
```

11.4.3.3. Static Multicast Route Path

PIM 은 Unicast Routing Table 을 기반으로 동작한다. 하지만 Network 의 환경이나 라우터의 운용에 따라서 특정한 RP 또는 Source 에 대한 Route Path 를 Unicast Routing Table 보다 우선하는 Multicast Route Path 를 Static 하게 적용할 수 있다.

적용된 Multicast Route Path 는 PIM 에서만 유효한 경로이며, Unicast Routing Path 보다 항상 우선하

여 적용된다.

Static Multicast Route Path 를 설정하기 위해서는 아래의 명령을 global configuration mode 에서 실행한다.

명령어	설명
ip mroute <i>A.B.C.D/M [A.B.C.D bgp isis ospf rip static]</i> <i>A.B.C.D</i>	Static Multicast Route Path 를 지정한다.
no ip mroute <i>A.B.C.D [bgp isis ospf rip static]</i>	지정된 Static Multicast Route Path 를 해제한다.

```
Router# configure terminal
Router(config)# ip mroute 100.1.1.1/32 static 20.1.1.2
Router(config)# exit
Router#
```

11.4.3.4. Global Multicast Group-Limit

특정 group 들에 대해서 허용할지 제한할지 결정할 수 있는 global multicast group range 를 설정할 수 있다. 설정된 global multicast group range 는 라우터의 IGMP, PIM 등 모든 multicast protocol 에 동시에 적용된다.

global multicast group range 를 설정하기 위해서는 아래의 명령을 global configuration mode 에서 실행한다.

명령어	설명
ip multicast group-range <i>access-list</i>	Multicast group range 를 설정한다.
no ip multicast group-range	설정된 multicast group range 를 해제한다.

```
Router# configure terminal
Router(config)# access-list 20 permit 224.1.1.0 0.0.0.255
Router(config)# access-list 20 deny any
Router(config)# ip multicast group-range 20
Router(config)# exit
Router#
```

11.4.3.5. Multicast Load-Split

PIM Router 는 SPT 에 대해서 Metric 이 동일한 RPF interface 가 하나이상 존재할 수 있다. 이와 같이 특정 Source 에 대한 RPF Interface 가 여러 개가 존재하는 경우, PIM 은 (S, G) entry 의 Hash function 의해서 결정된 Hash 값에 따라서 Upstream Interface 를 선택하고 Multicast Traffic 의 수신을 분산시킬 수 있다. 이러한 load-split 기능은 load-balance 와는 다른 개념이지만 다양하고 많은 수의 multicast entry 를 처리함에 있어서 (S, G) entry 별로 다른 RPF interface 를 가지는 것은 특정 Interface 하나만을 사용하는 것 보다 RPF Interface 에 가중되는 Network Bandwidth 의 효율을 높일 수 있다.

Multicast Load-Split 기능을 설정하기 위해서는 아래의 명령을 global configuration mode 에서 실행한다.

명령어	설명
ip multicast multipath	Multicast load-split 기능을 설정한다.
no ip multicast multipath	설정된 Multicast load-split 기능을 해제한다.

```
Router# configure terminal
Router(config)# ip multicast multipath
Router(config)# exit
Router#
```

11.4.3.6. Multicast Route-Limit

Multicast Router 는 시스템에서 사용할 수 있는 Multicast Routing Entry 의 최대 수를 제한 할 수 있다. Multicast Routing Entry 의 수의 제한하기 위해서는 아래의 명령을 global configuration mode 에서 실행한다.

명령어	설명
ip multicast route-limit <1-2147483647> [<1-2147483647>]	Multicast routing entry 의 수를 제한한다. (Default : 1000 개)
no ip multicast route-limit	제한된 Multicast routing entry 의 수를 해제한다.

```
Router# configure terminal
Router(config)# ip multicast route-limit 10000 9000
Router(config)# exit
Router# show ip mroute sparse count

IP Multicast Statistics
Total 0 routes using 0 bytes memory
```

Route limit/Route threshold: 10000/9000

```
Total NOCACHE/WRONGVIF/WHOLEPKT rcv from fwd: 0/0/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 0/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK rcv/Reg NACK rcv/Reg pkt sent: 0/0/0
Next stats poll: 00:00:19

Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts
Fwd msg counts: WRONGVIF/WHOLEPKT rcv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK rcv/Reg NACK rcv/Reg pkt sent

Router#
```

11.4.4. Configure IGMP Functionality

IGMP의 다양한 특성들에 대해 설정하기 위해서는 다음에 나오는 작업들을 수행한다.

11.4.4.1. IGMP Version

Network 별로 수행되는 IGMP Querier의 IGMP Version은 Default IGMPv2로 동작되며, IGMP Version을 변경하기 위해서는 아래의 명령을 interface configuration mode에서 실행한다.

명령어	설명
ip igmp version <1-3>	해당 인터페이스의 IGMP Version을 설정한다. (Default:2)
no ip igmp version	설정된 해당 인터페이스의 IGMP Version을 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1/1
Router(config-if-Giga2/1/1)# ip igmp version 3
Router(config-if-Giga2/1/1)# end
Router# show ip igmp interface
IGMP Enabled, Active, Querier, Configured for version 3
  Internet address is 2.1.1.1
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP query interval is 125 seconds
  IGMP querier timeout is 262 seconds
  IGMP max query response time is 25 seconds
```

```
Last member query response interval is 1000 milliseconds
Group Membership interval is 275 seconds
IGMP Snooping is not enabled on this interface
IGMP Snooping fast-leave is not enabled
IGMP Snooping querier is not enabled
IGMP Snooping report suppression is enabled
Router#
```

11.4.4.2. IGMP Access-Group

멀티캐스트 라우터는 Network Host 들이 가입한 멀티캐스트 그룹들을 알아내기 위해 IGMP Query 메시지를 주기적으로 전송하며, Network Host 들은 멀티캐스트 멤버로 라우터에 등록되기 위해서 IGMP Report 메시지를 멀티캐스트 라우터로 전송한다. 멀티캐스트 라우터는 인터페이스에서 수신되는 Network Host 들의 특정 그룹의 등록을 차단하여 멀티캐스트 서비스를 제한할 수 있다.

특정 멀티캐스트 그룹의 접근을 제한하기 위해서는 인터페이스에서 아래의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip igmp access-group access-list	해당 인터페이스에서 수신되는 호스트들의 멀티캐스트 그룹에 대한 등록을 제한한다.
no ip igmp access-group	해당 인터페이스에서 수신되는 제한된 호스트들의 멀티캐스트 그룹에 대한 등록을 해제한다.

```
Router# configure terminal
Router(config)# access-list 1 deny 225.1.1.0 0.0.0.255
Router(config)# interface GigabitEthernet 2/1/1
Router(config-if-Giga2/1/1)# ip igmp access-group 1
Router(config-if-Giga2/1/1)# end
```

11.4.4.3. IGMP Query-Interval

멀티캐스트 라우터는 Multicast Membership 관리를 위해서 주기적으로 IGMP Query 메시지를 전송한다.

멀티캐스트 라우터들은 설정된 각각의 Network 에서 IGMP Query 메시지를 전송하기 위한 IGMP Querier 를 선출하며, IP 주소의 값이 가장 작은 라우터가 선출된다. 선출된 IGMP Querier 는 Network 상의 모든 호스트들에게 IGMP Query 메시지를 주기적으로 전송할 책임이 있다.

디폴트로 IGMP Querier 는 호스트와 네트워크의 IGMP 오버헤드를 낮게 유지하기 위하여 IGMP Query 메시지를 125 초마다 보낸다. 이 메시지의 전송 간격을 변경하려면, 다음의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip igmp query-interval <1-18000>	IGMP Querier 가 주기적으로 IGMP Query 메시지를 전송하는 간격을 설정 (Default : 125 초)
no ip igmp query-interval	설정된 IGMP Query Interval 을 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1/1
Router(config-if-Giga2/1/1)# ip igmp query-interval 60
Router(config-if-Giga2/1/1)# end
Router# show ip igmp interface
Interface Giga2/1/1 (Index 1211)
  IGMP Enabled, Active, Querier, Version 2 (default)
  Internet address is 2.1.1.1
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP query interval is 60 seconds
  IGMP querier timeout is 262 seconds
  IGMP max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is not enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
Router#
```

11.4.4.4. IGMP Last-Member-Query-Count

IGMP Querier 는 Host 로부터 특정 Multicast Group 에 대해 탈퇴하는 IGMP Leave 메시지를 수신한 경우, 탈퇴를 원하는 Host 가 포함된 Network 에 동일 Multicast Group 의 가입 Host 가 있는지 확인하기 위해서 IGMP Group-Specific Query 를 발생한다.

IGMP Querier 는 Group-Specific Query 에 대해서 아무런 응답이 없는 경우, 더 이상 해당 Multicast Group 의 가입 Host 가 없다고 판단하고 Multicast Membership 을 삭제한다.

IGMP Last-member-query-count 는 IGMP Querier 가 탈퇴한 Multicast Group 의 또다른 Host 를 찾기

위해서 발생하는 IGMP Group-Specific Query 의 발생 횟수를 지정한다.

IGMP Last-member-query-count 의 설정을 위해서는 interface configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip igmp last-member-query-count <2-7>	IGMP Group-Specific Query 발생 횟수를 지정한다. (Default : 2 회)
no ip igmp last-member-query-count	지정된 IGMP Group-Specific Query 발생 횟수를 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1/1
Router(config-if-Giga2/1/1)# ip igmp last-member-query-count 3
Router(config-if-Giga2/1/1)# end
```

11.4.4.5. IGMP Last-Member-Query-Interval

특정 Multicast Group Membership 에서 탈퇴를 원하는 Host 가 있는 경우, IGMP Querier 는 IGMP Group-Specific Query 를 발생함으로 동일 Multicast Group Membership 의 가입을 원하는 다른 Host 를 찾는다. IGMP Group-Specific Query 는 지정된 IGMP Last-member-query-count 의 횟수와, 지정된 IGMP Last-member-query-interval 의 주기로 발생된다.

IGMP Last-member-query-interval 의 지정은 ms 단위로 적용하며, 설정을 위해서는 interface configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip igmp last-member-query-interval <1000-25500>	IGMP Last-member-query-interval 을 지정한다. (Default : 1000ms)
no ip igmp last-member-query-interval	설정된 IGMP Last-member-query-interval 을 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1/1
Router(config-if-Giga2/1/1)# ip igmp last-member-query-interval 2000
Router(config-if-Giga2/1/1)# end
Router# show ip igmp interface
Interface Giga2/1/1 (Index 1211)
  IGMP Enabled, Active, Querier, Version 2 (default)
```

```

Internet address is 2.1.1.1
IGMP interface has 0 group-record states
IGMP activity: 0 joins, 0 leaves
IGMP query interval is 125 seconds
IGMP querier timeout is 262 seconds
IGMP max query response time is 25 seconds
Last member query response interval is 2000 milliseconds
Group Membership interval is 275 seconds
IGMP Snooping is not enabled on this interface
IGMP Snooping fast-leave is not enabled
IGMP Snooping querier is not enabled
IGMP Snooping report suppression is enabled
Router#
    
```

11.4.4.6. IGMP Immediate-Leave

IGMP Querier 는 IGMP Immediate-leave 가 설정된 인터페이스에서 Multicast Membership 탈퇴를 원하는 IGMP Leave 메시지를 수신하면 동일 Multicast Membership 에 가입을 원하는 다른 Host 의 유무를 검사하지 않고 즉시 삭제한다.

IGMP Immediate-leave 를 설정하기 위해서는 interface configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip igmp immediate-leave group-list access-list	해당 interface 에 IGMP immediate-leave 를 설정한다.
no ip igmp immediate-leave	해당 interface 에 설정된 IGMP immediate-leave 를 제한다.

```

Router# configure terminal
Router(config)# access-list 2 permit 225.1.1.0 0.0.0.255
Router(config)# interface GigabitEthernet 2/1/1
Router(config-if-Giga2/1/1)# ip igmp immediate-leave group-list 2
Router(config-if-Giga2/1/1)# end
    
```

11.4.4.7. IGMP Group Limit

IGMP Querier 는 Multicast Membership 에 가입되는 Host 들의 Multicast Group 개수를 인터페이스별로 제한할 수 있다.

IGMP Group Limit 을 설정하기 위해서는 interface configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip igmp limit <1-2097152>	해당 interface 에 IGMP Group Limit 를 설정한다. (Default : 무제한)
no ip igmp limit	해당 interface 에 설정된 IGMP Group Limit 를 해제한다.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1/1
Router(config-if-Giga2/1/1)# ip igmp limit 100
Router(config-if-Giga2/1/1)# end
```

11.4.4.8. IGMP Global Limit

IGMP Querier 는 Multicast Membership Group 에 가입되는 Host 들의 관리를 인터페이스별로 관리한다. Multicast Router 는 IGMP Querier 가 관리하는 전체 인터페이스에서 가입된 Multicast Membership Group 의 총 개수를 제한할 수 있다.

IGMP Global Group Limit 을 설정하기 위해서는 global configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip igmp limit <1-2097152>	Global 로 IGMP Group Limit 를 설정한다. (Default : 무제한)
no ip igmp limit	Global 로 설정된 IGMP Group Limit 를 해제한다.

```
Router# configure terminal
Router(config)# ip igmp limit 100
Router(config)# end
```

11.4.4.9. IGMP Minimum-Version

IGMP Querier 가 수신되는 IGMP 메시지의 Version 을 제한할 수 있다. IGMP Minimum-Version 을 2 로 설정한 경우, 수신되는 IGMPv1 메시지는 제한되며 IGMPv2, IGMPv3 메시지는 허용된다. IGMPv3 메시지의 경우에는 설정된 인터페이스의 IGMP Version 에 의해서 처리유무가 결정된다.

IGMP Minimum-Version 을 설정하기 위해서는 interface configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip igmp minimum-version <2/3>	해당 interface 에 IGMP minimum-version 을 설정한다.
no ip igmp minimum-version	해당 interface 에 설정된 IGMP minimum-version 을 해제한다.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1/1
Router(config-if-Giga2/1/1)# ip igmp minimum-version 2
Router(config-if-Giga2/1/1)# end
```

11.4.4.10. IGMP Querier-Timeout

서브넷의 Multicast Membership 관리를 지속적으로 유지하기 위해서 동일 서브넷에 여러 개의 Multicast Router 를 배치할 수 있다. 하나의 서브넷은 하나의 IGMP Querier 만을 선출하며, 선출된 IGMP Querier 는 주기적으로 IGMP Query 메시지를 발생시킨다.

IGMP Non-Querier 인 Multicast Router 는 지정된 Querier Timeout 동안 IGMP Querier 로부터 IGMP Query 메시지를 수신하지 못하면, Multicast Membership 관리를 위해서 IGMP Querier 의 역할을 수행하게 된다. 이 특징은 IGMPv2 인 경우에만 허용된다.

IGMP Querier-Timeout 을 설정하기 위해서는 interface configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip igmp querier-timeout <60-300>	IGMP Querier timeout 을 지정한다. (Default : 262 초)
no ip igmp querier-timeout	설정된 IGMP Querier timeout 을 기본값으로 설정한다.

```

Router# configure terminal
Router(config)# interface GigabitEthernet 2/1/1
Router(config-if-Giga2/1/1)# ip igmp querier-timeout 300
Router(config-if-Giga2/1/1)# end
Router# show ip igmp interface
Interface Giga2/1/1 (Index 1211)
  IGMP Enabled, Active, Querier, Version 2 (default)
  Internet address is 2.1.1.1
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP query interval is 125 seconds
  IGMP querier timeout is 300 seconds
  IGMP max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is not enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
Router#

```

11.4.4.11. IGMP Query-Max-Response-Time

IGMP Querier 인 Multicast Router 는 주기적으로 발생하는 IGMP Query 메시지의 Max Response Time 을 조절하여 Host 들에서 발생하는 IGMP Report 메시지들을 지정된 Max Response Time 시간 내에 분산시킬 수 있다.

IGMP Query Max-Response-Time 을 설정하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip igmp query-max-response-time <1-240>	max-response-time 을 지정한다. (Default : 25 초)
no ip igmp query-max-response-time	설정된 max-response-time 을 기본값으로 설정한다.

```

Router# configure terminal
Router(config)# interface GigabitEthernet 2/1/1
Router(config-if-Giga2/1/1)# ip igmp query-max-response-time 10
Router(config-if-Giga2/1/1)# end
Router# show ip igmp interface

```

```

Interface Giga2/1/1 (Index 1211)
  IGMP Enabled, Active, Querier, Version 2 (default)
  Internet address is 2.1.1.1
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP query interval is 125 seconds
  IGMP querier timeout is 262 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is not enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
Router#
    
```

11.4.4.12. IGMP Rate

Multicast Router 는 CPU 로 incoming 되는 IGMP Packet 에 대해서 PPS 로 제한할 수 있다. 설정된 IGMP Rate 를 초과하는 IGMP Packet 은 CPU 에서 Drop 처리 된다.

IGMP Packet 을 PPS 로 제한하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip igmp rate <500-6000>	IGMP Rate 를 pps 단위로 설정한다.
no ip igmp query-max-response-time	설정된 IGMP Rate 를 해제한다.

```

Router# configure terminal
Router(config)# interface GigabitEthernet 2/1/1
Router(config-if-Giga2/1/1)# ip igmp rate 100
Router(config-if-Giga2/1/1)# end
Router# show ip igmp rate-limit statistics

IGMP Message Ratelimit (pps) for IP Multicast
Ifname      Incoming rate  Rate-limit  Permit  Drop  Rx-Total
-----+-----+-----+-----+-----+-----+
gi2.1.1           0           100         0        0        0
0
Router#
    
```

11.4.4.13. IGMP Robustness-Variable

IGMP Robustness-Variable 은 IGMP Subnet 에서 발생될 수 있는 IGMP packet 의 손실을 예상하여 적당한 IGMP Membership 의 Expire Timeout 값을 Tuning 할 수 있는 설정이다. 따라서, IGMP Subnet 이 매우 좋지 않은 환경인 경우, IGMP packet 의 손실이 예상되기 때문에 Robustness Variable 의 값을 크게 설정하여 IGMP Membership 의 유지를 Tuning 할 수 있다.

IGMP Robustness-Variable 을 설정하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip igmp robustness-variable <2-7>	IGMP Robustness Variable 을 설정한다. (Default: 2)
no ip igmp query-max-response-time	설정된 IGMP Robustness Variable 을 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1/1
Router(config-if-Giga2/1/1)# ip igmp robustness-variable 5
Router(config-if-Giga2/1/1)# end
Router# show ip igmp interface
Interface Giga2/1/1 (Index 1211)
  IGMP Enabled, Active, Querier, Version 2 (default)
  Internet address is 2.1.1.1
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP query interval is 125 seconds
  IGMP querier timeout is 637 seconds
  IGMP max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 650 seconds
  IGMP Snooping is not enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
Router#
```

11.4.4.14. IGMP Static-Group

IGMP Static-Group 은 특정 IGMP Subnet 에서 IGMP Group Membership 에 Static 하게 Expire 되지 않은 Host 가 Join 되어 있다고 설정하는 것이다. 따라서, IGMP Querier 는 IGMP Static-Group 이 설정

된 해당 Interface 를 IGMP Leave 메시지를 받더라도 계속하여 Join 상태를 유지한다.

IGMP Static-Group 을 다양하게 설정하기 위해서 IGMP Class-Map 을 이용한다.

IGMP Class-Map 을 생성하기 위해서는 다음의 명령을 global configuration mode 에서 실행한다.

명령어	설명
class-map type multicast-flows name	IGMP Class-Map 을 생성한다.
no class-map type multicast-flows	생성된 IGMP Class-Map 을 삭제한다.

생성된 IGMP Class-Map 에서는 아래의 명령을 class-map mode 에서 설정할 수 있다.

명령어	설명
group A.B.C.D	하나의 IGMPv2 Group (*, G)을 지정한다.
group A.B.C.D source A.B.C.D	하나의 IGMPv3 Group 과 Source (S, G)를 지정한다.
group A.B.C.D to A.B.C.D	여러 개의 IGMPv2 Group (*, Gn)을 지정한다.
group A.B.C.D to A.B.C.D source A.B.C.D	여러 개의 IGMPv3 Group 과 하나의 Source(S, Gn)를 지정한다.
no group A.B.C.D	지정된 IGMPv2 Group (*, G)을 해제한다.
no group A.B.C.D source A.B.C.D	지정된 IGMPv3 Group 과 Source (S, G)을 해제한다.
no group A.B.C.D to A.B.C.D	지정된 여러 개의 IGMPv2 Group (*, Gn)을 해제한다.
no group A.B.C.D to A.B.C.D source A.B.C.D	지정된 여러 개의 IGMPv3 Group 과 하나의 Source(S, Gn)를 해제한다.

IGMP Class-Map 에서 지정할 수 있는 source 의 설정은 IGMPv3 인 경우에만 유효하다.

```

Router# configure terminal
Router(config)# class-map type multicast-flows igmp_static
Router(config-mcast-flows-cmap)# group 225.1.1.1 to 225.1.1.10
Router(config-mcast-flows-cmap)# group 225.1.2.1
Router(config-mcast-flows-cmap)# end
Router# show ip igmp static-group class-map

Class-map igmp_static
  description : -
  Group address range 225.1.1.1 to 225.1.1.10
  Group address 225.1.2.1
Router#
    
```

IGMP Static-Group 을 설정하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
ip igmp static-group A.B.C.D	IGMP Class-Map 을 사용하지 않고 IGMPv2 Static-Group 을 설정한다.
ip igmp static-group A.B.C.D interface IFNAME	IGMP Snooping 이 설정된 VLAN interface 인 경우, IGMPv2 Static-Group 의 설정시 VLAN interface 의 member port 를 지정한다.
ip igmp static-group A.B.C.D source A.B.C.D	IGMP Class-Map 을 사용하지 않고 IGMPv3 Static-Group 를 설정한다.
ip igmp static-group A.B.C.D source A.B.C.D interface IFNAME	IGMP Snooping 이 설정된 VLAN interface 인 경우, IGMPv3 Static-Group 의 설정시 VLAN interface 의 member port 를 지정한다.
ip igmp static-group class-map name	IGMP Class-Map 을 사용하여 IGMP Class-Map 에서 지정된 Group 정보를 사용하여 Static-Group 을 설정한다.
no ip igmp static-group A.B.C.D	설정된 IGMPv2 Static-Group 을 해제한다.
no ip igmp static-group A.B.C.D interface IFNAME	IGMP Snooping 이 설정된 VLAN interface 에 설정된 IGMPv2 Static-Group 을 해제한다.
no ip igmp static-group A.B.C.D source A.B.C.D	설정된 IGMPv3 static-group 을 해제한다.
no ip igmp static-group A.B.C.D source A.B.C.D interface IFNAME	IGMP Snooping 이 설정된 VLAN interface 에 설정된 IGMPv3 Static-Group 을 해제한다.
no ip igmp static-group class-map name	설정된 IGMP Class-Map 의 Static-Group 을 해제한다.

```

Router# configure terminal
Router(config)# interface GigabitEthernet 2/1/1
Router(config-if-Giga2/1/1)# ip igmp static-group igmp_static
Router(config-if-Giga2/1/1)# end
Router# show ip igmp group
IGMP Connected Group Membership
Group Address      Interface          Uptime    Expires    Last Reporter
225.1.1.1          Giga2/1/1         00:01:42  static    0.0.0.0
225.1.1.2          Giga2/1/1         00:01:42  static    0.0.0.0
225.1.1.3          Giga2/1/1         00:01:42  static    0.0.0.0
225.1.1.4          Giga2/1/1         00:01:42  static    0.0.0.0
225.1.1.5          Giga2/1/1         00:01:42  static    0.0.0.0
225.1.1.6          Giga2/1/1         00:01:42  static    0.0.0.0
    
```

```

225.1.1.7      Giga2/1/1      00:01:42      static 0.0.0.0
225.1.1.8      Giga2/1/1      00:01:42      static 0.0.0.0
225.1.1.9      Giga2/1/1      00:01:42      static 0.0.0.0
225.1.1.10     Giga2/1/1      00:01:42      static 0.0.0.0
225.1.2.1      Giga2/1/1      00:01:42      static 0.0.0.0
Router# show ip igmp static-group class-map interface gi2/1/1

Giga2/1/1
Class-map attached : igmp_static
  Group address range 225.1.1.1 to 225.1.1.10
  Group address 225.1.2.1
Router#
    
```

11.4.4.15. IGMP SSM-MAP

IGMPv2 는 특정 Group 으로 IGMP Join 이 이루어짐으로 PIM Router 는 PIM domain 에서 공유된 RP 의 RPF Tree 를 통해서 해당 Group 의 Traffic 을 수신할 수 있다. 하지만, 해당 Group 의 Multicast Traffic 을 전송하는 Source 를 PIM Router 가 알고 있다면, PIM domain 에서 공유한 RP 의 RPF Tree 를 사용하지 않고 Multicast Traffic 을 전송하는 Source 의 Short-Path-Tree 로 직접 PIM Join 을 할 수 있다.

IGMPv3 의 경우에는 IGMP Join 메시지에 특정 Group 의 Multicast Traffic 을 발생하는 Source 를 지정 할 수 있기 때문에 PIM 의 Source-Specific-Multicast (SSM)의 기능을 사용할 수 있다.

IGMPv2 의 경우에는 IGMP join 메시지에 특정 Group 만을 지원하기 때문에 IGMP SSM-MAP 기능을 통하여 PIM SSM 기능을 사용해야 한다.

PIM SSM 기능은 Default 로 Enable 되어 있으며 PIM SSM 기능을 Disable 하기 위해서는 global configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
no ip igmp ssm-map enable	SSM-MAP 기능을 Disable 한다.
ip igmp ssm-map enable	SSM-MAP 기능을 Enable 한다.

```

Router# configure terminal
Router(config)# no ip igmp ssm-map enable
Router(config)# exit
Router# show ip igmp ssm-map
SSM Mapping : Disabled
Database    : None configured
Router#
Router# configure terminal
Router(config)# ip igmp ssm-map enable
    
```

```
Router(config)# exit
Router# show ip igmp ssm-map
SSM Mapping : Enabled
Database    : None configured
```

IGMPv2 로 Join 되는 Group 은 IGMP SSM-MAP 의 Database 에서 지정한 Group 과 mapping 하여 지정된 source 를 SSM 으로 처리한다.

IGMP SSM-MAP 의 Database 를 생성하기 위해서는 global configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip igmp ssm-map static access-list A.B.C.D	Access-list 를 사용하여 ssm-map database 를 추가한다.
no ip igmp ssm-map static access-list A.B.C.D	Access-list 를 사용하여 추가된 ssm-map database 를 삭제한다.

```
Router# configure terminal
Router(config)# access-list 20 permit 224.1.1.0 0.0.0.255
Router(config)# access-list 21 permit 224.1.3.0 0.0.0.255
Router(config)# ip igmp ssm-map static 20 179.1.1.200
Router(config)# ip igmp ssm-map static 21 179.1.1.201
Router(config)# exit
Router# show ip igmp ssm-map
SSM Mapping : Enabled
Database    : Static mappings configured
Router#
Router# show ip igmp ssm-map 224.1.1.1
Group address: 224.1.1.1
Database    : Static
Source list : 179.1.1.200
Router#
Router# show ip igmp ssm-map 224.1.2.1

Can't resolve 224.1.2.1 to source-mapping

Router#
Router# show ip igmp ssm-map 224.1.3.1
Group address: 224.1.3.1
Database    : Static
Source list : 179.1.1.201
Router#
```

11.4.5. Configure PIM-SM Functionality

Protocol Independent Multicast (PIM)의 다양한 특성들에 대해 설정하기 위해서는 다음에 나오는 작업들을 수행한다.

11.4.5.1. PIM Hello-Interval

PIM은 주기적으로 Hello 메시지를 전송하며, PIM Hello 메시지의 주기를 설정하기 위해서는 다음의 명령을 interface configuration mode에서 실행한다

명령어	설명
ip pim hello-interval < 1-65535>	Hello 메시지의 전송간격을 설정한다. (Default : 30s)
no ip pim hello-interval	설정된 Hello 메시지의 전송간격을 기본값으로 설정한다.

```

Router# configure terminal
Router(config)# interface GigabitEthernet 3/1/3
Router(config-if-Giga3/1/3)# ip pim hello-interval 60
Router(config-if-Giga3/1/3)# end
Router# show ip pim sparse-mode interface
Address          Interface  VIFindex Ver/   Nbr   Query  DR   DR
                  Mode     Count  Intvl Prior
3.1.1.222        Giga3/1/3  0       v2/S  0     60    1   3.1.1.222
Router#
    
```

11.4.5.2. PIM Hello-Holdtime

PIM은 주기적으로 Hello 메시지를 전송하며, PIM Hello 메시지를 수신하는 Neighbor는 PIM Hello 메시지에서 지정한 Holdtime 시간만큼 PIM Hello 메시지를 전송한 Neighbor를 유지해야 한다.

PIM Hello-Holdtime의 값을 변경하기 위해서는 다음의 명령을 interface configuration mode에서 실행한다

명령어	설명
ip pim hello-holdtime < 1-65535>	Hello 메시지의 holdtime을 설정한다. (Default : 105s)
no ip pim hello-interval	설정된 Hello 메시지의 holdtime을 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 3/1/3
Router(config-if-Giga3/1/3)# ip pim hello-holdtime 120
Router(config-if-Giga3/1/3)# end
```

11.4.5.3. PIM DR-Priority

PIM 은 주기적으로 Hello 메시지를 전송하며, PIM Hello 메시지를 수신하는 Neighbor 는 PIM Hello 메시지에서 지정한 DR-Priority 에 의해서 해당 인터페이스의 DR 을 Selection 한다.

DR 을 선택할 때, 아래와 같은 조건들이 적용된다.

- 인터페이스에 설정된 DR Priority 와 Neighbor 의 DR Priority 를 비교하여 Highest DR Priority 값을 가지면 DR Router 가 된다.
- 인터페이스에 모두 동일한 DR Priority 를 가지는 경우에는 Highest IP address 가 DR Router 가 된다.
- DR Priority 값을 포함하지 않은 PIM Hello 메시지를 수신한 경우, Highest priority 를 가진 것으로 간주하고 DR 로 해당 Neighbor 가 선택된다.
- DR Priority 값을 포함하지 않은 Neighbor 가 다수인 경우에는 그 Neighbor 들 중에서 Highest IP address 가 DR Router 로 선택된다.

PIM Hello 의 DR Priority 값을 변경하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다

명령어	설명
ip pim dr-priority <0-4294967294 >	Hello 메시지의 DR Priority 를 설정한다. (Default : 1)
no ip pim hello-interval	설정된 Hello 메시지의 holdtime 을 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 3/1/3
Router(config-if-Giga3/1/3)# ip pim dr-priority 10
Router(config-if-Giga3/1/3)# end
Router# show ip pim sparse-mode interface
Address          Interface  VIFindex Ver/   Nbr   Query  DR   DR
                  Mode     Count  Intvl Prior
3.1.3.222        Giga3/1/3  0      v2/S  0     60    10  3.1.3.222
Router#
```

11.4.5.4. PIM Propagation-Delay

Multi-Access Network 의 환경에서 하나의 특정 PIM Neighbor 가 더 이상 Multicast Traffic 을 원하지 않는 경우 PIM Prune 을 Upstream Router 로 전송하며, Upstream Router 는 해당 Multi-Access Network 에서 또다른 PIM Router 가 동일한 Multicast Traffic 을 계속 받기를 원할 수 있기 때문에 Prune 처리를 지정된 시간만큼 지연한다. Prune 처리가 지연된 Multicast Traffic 을 계속 수신하기를 원하는 PIM Router 가 있다면 Upstream Router 가 Multicast Traffic 을 계속 Forwarding 할 수 있도록 Prune 처리가 지연된 시간 이내에 Upstream Router 로 PIM Join 을 전송해야 한다.

이러한 Multi-Access Network 의 Multicast Traffic Forwarding 에서 PIM Prune 처리 지연을 위해서 PIM Router 는 PIM Hello 메시지에 propagation delay 를 포함하여 전송한다. PIM Hello 메시지의 propagation delay 를 변경하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다

명령어	설명
ip pim propagation-delay <1000-5000>	PIM Hello 메시지의 propagation delay 를 설정한다. (Default: 1000ms)
no ip pim propagation-delay	설정된 PIM Hello 메시지의 propagation delay 를 해제한다.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 3/1/3
Router(config-if-Giga3/1/3)# ip pim propagation-delay 5000
Router(config-if-Giga3/1/3)# end
Router# show ip pim sparse-mode interface detail
Giga3/1/3 (vif 0):
  Address 3.1.3.222, DR 3.1.3.222
  Hello period 30 seconds, Next Hello in 23 seconds
  Triggered Hello period 5 seconds
  Propagation delay is 1000 milli-seconds
  Configured Propagation-delay 5000 milli-seconds
  Generation ID : 795759275
  Neighbors:

Router#
```

11.4.5.5. PIM Exclude-Genid

PIM 은 주기적으로 Hello 메시지를 전송하며, PIM Hello 메시지는 Generation ID 를 포함할 수 있다. PIM Router 는 특정 Network 의 동일한 Neighbor 로부터 다른 Generation ID 를 가지는 PIM Hello 메시지가 수신되면 해당 Neighbor 가 Start 되었거나 Restart 되었음을 인지하고 RP 정보 또는 PIM RPF 등을 갱신하는 PIM Neighbor Discovery 를 수행한다.

PIM Hello 메시지를 전송할 때, Generation ID 를 포함하지 않도록 설정하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다

명령어	설명
ip pim exclude-genid	PIM hello 메시지에 Generation ID 를 포함하지 않고 전송하도록 설정한다.
no ip pim exclude-genid	exclude-genid 설정을 해제한다.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 3/1/3
Router(config-if-Giga3/1/3)# ip pim exclude-genid
Router(config-if-Giga3/1/3)# end
Router#
```

11.4.5.6. PIM Neighbor-Filter

PIM 은 주기적으로 Hello 메시지를 전송하며, PIM Hello 메시지를 수신하는 Neighbor 는 PIM Hello 메시지를 통하여 해당 Network 의 DR 을 선택한다.

특정 PIM Neighbor 를 제한해야 될 필요가 있는 경우 다음의 명령을 interface configuration mode 에서 실행한다

명령어	설명
ip pim neighbor-filter access-list	PIM neighbor 차단을 설정한다.
no ip pim neighbor-filter access-list	설정된 PIM neighbor 차단을 해제한다.

```
Router# configure terminal
Router(config)# access-list 3 permit 3.1.3.1
Router(config)# interface GigabitEthernet 3/1/3
Router(config-if-Giga3/1/3)# ip pim neighbor-filter 3
Router(config-if-Giga3/1/3)# end
```

11.4.5.7. PIM BSR-Border

Bootstrap Router (BSR)는 주기적인 간격마다 Network 에 배치된 RP 들의 정보를 모은 Bootstrap 메시지를 발생한다. 특정 인터페이스에서 BSR Border 를 설정하면 Bootstrap 메시지의 송수신이 제한됨으로 서로 다른 PIM Domain 을 구성할 수 있다.

BSR Border 를 설정하기 위해서는 다음의 명령을 **interface configuration mode** 에서 실행한다

명령어	설명
ip pim bsr-border	해당 인터페이스로의 BSR 메시지 송수신을 차단한다.
no ip pim bsr-border	설정된 인터페이스의 BSR 메시지 송수신 차단을 해제한다.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 3/1/3
Router(config-if-Giga3/1/3)# ip pim bsr-border
Router(config-if-Giga3/1/3)# end
```

11.4.5.8. PIM JP-Timer

Multicast Router 는 Multicast Traffic Forwarding 을 유지하기 위해서 PIM JoinPrune 메시지를 정기적으로 SPT 또는 RPT 의 Routing Path 에 있는 Upstream Multicast Router 로 전송한다.

PIM JoinPrune 메시지의 전송 주기의 기본값은 60 초이며, PIM JoinPrune 메시지의 전송 주기를 변경하기 위해서는 다음의 명령을 **global configuration mode** 에서 실행한다

명령어	설명
ip pim jp-timer <1-65535>	PIM JoinPrune 메시지의 전송주기를 설정한다. (Default : 60 초)
no ip pim jp-timer	설정된 PIM JoinPrune 메시지의 전송주기를 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# ip pim jp-timer 120
Router(config)# exit
```

11.4.5.9. PIM Access-Group

Multicast Router 는 정기적인 PIM Join 메시지를 수신하여 Multicast Traffic Forwarding 을 유지한다. 서비스를 원하지 않은 Multicast Group 으로 PIM Join 이 수신된 경우에는 이를 제한할 수 있다.

특정한 Multicast Group 으로의 PIM Join 을 제한하고자 할 때에는 다음의 명령을 interface configuration mode 에서 실행한다

명령어	설명
ip multicast boundary access-list	Access-List 에서 지정된 Group 으로의 PIM Join 을 제한한다.
no ip multicast boundary access-list	제한된 PIM Join 을 해제한다.

```
Router# configure terminal
Router(config)# access-list 3 deny 224.1.1.0 0.0.0.255
Router(config)# interface GigabitEthernet 3/1/3
Router(config-if-Giga3/1/3)# ip multicast boundary 3
Router(config-if-Giga3/1/3)# end
```

11.4.5.10. PIM Accept-Register

RP 로 운용중인 Multicast Router 는 PIM Domain 에 속한 1st-Hop Multicast Router 로부터 PIM Register 메시지를 수신하여 Multicast Source Entry 를 관리한다.

Multicast Router 는 수신되는 특정 Source 의 PIM Register 메시지를 제한하기 위해서는 다음의 명령을 global configuration mode 에서 수행한다.

명령어	설명
ip pim accept-register list access-list	수신되는 PIM Register 메시지의 source 를 제한한다.
no ip pim register-filter-group	수신되는 PIM Register 메시지의 제한된 source 를 해제한다.

```
Router# configure terminal
Router(config)# access-list 30 permit 100.1.1.0 0.0.0.255
Router(config)# access-list 30 deny any
Router(config)# ip pim accept-register list 30
Router(config)# exit
```

11.4.5.11. PIM SPT-Threshold

Multicast Router 가 IGMP Host 에 대한 IGMP Membership 을 유지하는 경우, 이 Multicast Router 를 Last-Hop Router 라고 한다. Last-Hop Router 는 RP Tree 로부터 수신되는 Multicast Traffic 에 대해서 해당 Traffic 의 Source 로 향하는 가장 빠른 경로인 Shortest-Path-Tree 로 Traffic 을 받을 수 있도록

SPT 전환을 할 수 있다.

PIM SPT-Threshold 를 설정하기 위해서는 다음의 명령을 global configuration mode 에서 수행한다.

명령어	설명
ip pim spt-threshold [group-list access-list]	PIM SPT Threshold 를 설정한다.
no ip pim spt-threshold [group-list access-list]	설정된 PIM SPT Threshold 를 해제한다.

```
Router# configure terminal
Router(config)# ip pim spt-threshold
Router(config)# exit
```

11.4.5.12. PIM Cisco-Register-Checksum

멀티캐스트 Originator 로부터 전송된 Multicast Packet 을 수신한 First-Hop 에 위치한 라우터는 RP 로 해당 Packet 을 PIM Register 메시지 내에 포함하여 unicast routing 을 통하여 전달한다. 이 PIM Register 메시지를 수신한 RP 는 메시지 내에 포함된 Multicast Packet 을 Multicast Routing Entry 로 forwarding 한다.

RFC 표준에 의하면, PIM-SM Register 메시지의 Checksum 은 Header 부분만 계산되지만, CISCO 라우터의 경우 Register 메시지 전체가 계산된다.

따라서 CISCO 라우터와 호환하기 위해서는 반드시 Checksum 의 계산은 메시지 전체가 되어야 한다.

Cisco Register-Checksum 을 설정하기 위해서는 다음의 명령을 global configuration mode 에서 실행한다

명령어	설명
ip pim cisco-register-checksum	모든 Group 에 대해서 Cisco 라우터와 호환하도록 설정한다.
ip pim cisco-register-checksum group-list access-list	Access-list 에서 지정된 Group 에 대해서 Cisco 라우터와 호환하도록 설정한다.
no ip pim cisco-register-checksum	모든 Group 에 대해서 설정된 register-checksum 을 해제한다.
no ip pim cisco-register-checksum group-list access-list	Access-list 에서 지정된 Group 에 대해서 설정된 register-checksum 을 해제한다.

```
Router# configure terminal
Router(config)# ip pim cisco-register-checksum
Router(config)# exit
```

```
Router# configure terminal
Router(config)# access-list 11 permit 224.1.1.0 0.0.0.255
Router(config)# ip pim cisco-register-checksum group-list 11
Router(config)# exit
```

11.4.5.13. PIM BSR-Candidate

Multicast Router 가 BSR Candidate 로 동작하기 위해서는 PIM Domain 에 포함되어 있어야 한다. Multicast Router 를 BSR Candidate 로 설정하기 위해서는 global configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip pim bsr-candidate <i>ifname</i> [<i>hash-mask-length</i>] [<i>priority</i>]	Multicast Router 가 BSR candidate 로 동작하도록 설정한다.
no ip pim bsr-candidate [<i>ifname</i>]	설정된 BSR candidate 를 해제한다.

```
Router# configure terminal
Router(config)# ip pim bsr-candidate lo0
Router(config)# exit
Router# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.1.222
  Uptime:      00:02:32, BSR Priority: 64, Hash mask length: 10
  Next bootstrap message in 00:00:24
  Role: Candidate BSR
  State: Elected BSR
Router#
```

```
Router# configure terminal
Router(config)# ip pim bsr-candidate lo0 24 128
Router(config)# exit
Router# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
```

```
This system is the Bootstrap Router (BSR)
BSR address: 172.16.1.222
Uptime:      00:05:01, BSR Priority: 128, Hash mask length: 24
Next bootstrap message in 00:00:59
Role: Candidate BSR
State: Elected BSR
Router#
```

11.4.5.14. **PIM RP-Candidate**

Multicast Router 가 RP Candidate 로 동작하기 위해서는 PIM Domain 에 포함되어 있어야 한다. RP Candidate 는 전체 IP 멀티캐스트 주소 공간, 또는 일부분에 대해서 서비스를 할 수 있다. Candidate RP 는 주기적으로 Candidate RP Advertisement 메시지를 Bootstrap Router (BSR)에게 전송한다.

Multicast Router 를 RP Candidate 로 설정하기 위해서는 global configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip pim rp-candidate ifname	Default value 로 Candidate RP 가 동작하도록 설정한다.
ip pim rp-candidate ifname priority <0-255>	지정된 priority 를 가지는 Candidate RP 가 동작하도록 설정한다.
ip pim rp-candidate ifname priority <0-255> interval <1-16383>	지정된 priority 를 가지고 지정된 RP Advertisement 메시지를 주기적으로 전송하는 Candidate RP 가 동작하도록 설정한다.
ip pim rp-candidate ifname priority <0-255> interval <1-16383> group-list access-list	지정된 priority 를 가지고 지정된 Group 에 대해서만 지정된 RP Advertisement 메시지를 주기적으로 전송하는 Candidate RP 가 동작하도록 설정한다.
no ip pim rp-candidate [ifname]	설정된 Candidate RP 동작을 해제한다.

```
Router# configure terminal
Router(config)# ip pim bsr-candidate lo0
Router(config)# ip pim rp-candidate lo0
Router(config)# exit
Router# show ip pim sparse-mode bsr-router
This system is the Bootstrap Router (BSR)
BSR address: 172.16.1.222
Uptime:      00:03:56, BSR Priority: 64, Hash mask length: 10
Next bootstrap message in 00:00:07
```

```

Role: Candidate BSR
State: Elected BSR

Candidate RP: 172.16.1.222 (Loopback0)
  Advertisement interval 60 seconds
  Next C-RP advertisement in 00:00:36
Router#
Router# show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
  RP: 172.16.1.222
    Info source: 172.16.1.222, via bootstrap, priority 192
    Uptime: 00:00:08, expires: 00:02:24
Router#
    
```

11.4.5.15. PIM RP-Address

RP Candidate 와 BSR Candidate 를 운용할 수 없는 Network 의 환경에서 특정 멀티캐스트 라우터를 RP 로 Static 하게 지정하고자 할 때 설정할 수 있다.

설정된 Static RP 의 정보는 Bootstrap 메시지에 의해서 Dynamic 하게 Learning 되는 RP Candidate 보다 우선순위가 낮으며, Learning 된 RP Candidate 보다 우선순위를 높게 하려면 RP-Address Override 를 설정해야 한다.

Multicast Router 에 Static RP 의 정보를 설정하기 위해서는 global configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
ip pim rp-address A.B.C.D [access-list] [override]	Multicast Router 에 Static RP 를 설정한다.
no ip pim rp-address A.B.C.D [access-list]	설정된 Static RP 정보를 해제한다.

```

Router# configure terminal
Router(config)# ip pim rp-address 172.16.0.1
Router(config)# exit
Router# show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4, Static
  RP: 172.16.0.1
    Uptime: 00:00:37
Router#
    
```

11.4.5.16. PIM Register-Source

1st-Hop Router 에서 RP 로 PIM Register 를 전송할 때, PIM Register Packet 의 IP Source 를 Static 하게 지정하여 전송할 수 있다. PIM Register-Source 를 설정하기 위해서는 다음의 명령을 global configuration mode 에서 실행한다.

명령어	설명
ip pim register-source [ifname A.B.C.D]	PIM Register-Source 를 지정한다.
no ip pim rp-address A.B.C.D [access-list]	지정된 PIM Register-Source 를 해제한다.

```
Router# configure terminal
Router(config)# ip pim register-source lo0
Router(config)# exit
Router#
```

11.4.5.17. PIM SSM

PIM SSM 을 설정하면 설정된 SSM 의 Group range 에 포함되는 Group 에 대해서는 RPT 기능이 제한되며, SPT 기능만 제공된다.

SSM 의 Group Range 를 설정하기 위해서는 다음의 명령을 global configuration mode 에서 실행한다.

명령어	설명
ip pim ssm default	PIM SSM 에 대해서 Default Group range(232/8)를 적용한다.
ip pim ssm range access-list	PIM SSM 에 대해서 Access-List 에서 지정한 Group Range 로 적용한다.
no ip pim ssm	적용된 PIM SSM Group range 를 해제한다.

```
Router# configure terminal
Router(config)# ip pim ssm default
Router(config)# access-list 10 permit 224.1.1.0 0.0.0.255
Router(config)# ip pim ssm range 10
Router(config)# exit
Router#
```

11.4.6. Display System and Network Statistics

표 11-2 IP 멀티캐스트 라우팅 관련 모니터링 명령어

명령어	설명
show ip igmp groups	호스트들이 가입한 멀티캐스트 그룹들을 보여준다.
show ip igmp interface	인터페이스들의 멀티캐스트와 관련된 정보들을 보여준다.
show ip igmp rate-limit statistics	rate-limit 이 설정된 인터페이스의 멀티캐스트 packet 통계를 보여준다.
show ip igmp ssm-map	ssm-map 의 설정 상태를 보여준다.
show ip igmp static-group class-map	static group 을 지정하기 위한 class-map 의 설정 상태를 보여준다.
show ip mcache	멀티캐스트 라우팅 캐쉬 내용을 보여준다.
show ip mroute	멀티캐스트 라우팅 테이블의 내용을 보여준다.
show ip mvif	멀티캐스트 인터페이스의 정보를 보여준다.
show ip pim sparse-mode anycast-rp	PIM anycast RP 에 대한 정보를 보여준다.
show ip pim bsr-router	BSR 라우터에 대한 정보를 보여준다.
show ip pim sparse-mode interface	PIM 이 설정된 인터페이스에 대한 정보를 보여준다.
show ip pim sparse-mode local-members	PIM local membership 정보를 보여준다.
show ip pim sparse-mode mroute	PIM 에서 관리하는 멀티캐스트 라우팅 테이블의 내용을 보여준다
show ip pim neighbor	PIM neighbor 들을 보여준다.
show ip pim rp	RP 에 대한 정보를 보여준다.
show ip pim rp-hash	RP-HASH 에 대한 정보를 보여준다.
show ip rpf	RPF 에 대한 정보를 보여준다.
show ip rpf event	수신한 RPF 이벤트 대한 정보를 보여준다.

12

시스템 및 통계 모니터링

본 장은 현재 운영중인 E7500 Series 스위치의 시스템 및 통계 모니터링 기능에 대해 설명한다.

- 시스템 상태 모니터링
- 인터페이스 통계
- Logging 설정
- RMON (Remote Monitoring)
- 임계치 설정

E7500 Series 스위치가 제공하는 통계 정보는 시스템 운영자가 현재 네트워크의 운영 상태를 즉시 파악할 수 있도록 한다. 주기적으로 통계 데이터를 관리하면 향후 흐름을 예측하고, 문제가 발생하기 전에 미리 조치를 취할 수 있다.

12.1. 상태 모니터링

상태 관리 기능은 스위치에 대한 정보를 제공한다. E7500 Series 스위치는 **show** 명령의 서브 명령을 통하여 다양한 상태 정보를 운영자 화면을 통하여 제공한다.

표 12-1. 상태 모니터링 명령어

명령어	설명	모드
show logging	시스템이 현재 관리하고 있는 로그를 보여 준다.	Privileged
show memory usage	현재 시스템의 메모리 사용 상태를 보여 준다.	Privileged
show cpu usage	현재 CPU 점유율을 보여 준다.	Privileged
show environment [cooling temperature status]	시스템의 파워, FAN, 온도에 대한 환경 정보를 출력한다. <ul style="list-style-type: none"> ■ cooling: FAN 정보 ■ temperature: 온도 정보 ■ status: 파워, FAN, 온도의 상태 정보 출력 	Privileged
show environment alarm [status]	시스템 환경 정보에 대한 알람 이력을 출력한다. <ul style="list-style-type: none"> ■ status: 알람 이력 출력 	Privileged
show version	시스템의 버전 정보를 보여 준다.	Privileged

12.2. 시스템 임계치 설정

E7500 Series 스위치는 시스템 모듈 온도, CPU 및 메모리 사용률 등에 대해 임계치(threshold)를 설정할 수 있다. 임계치는 상한 임계치와 하한 임계치로 설정할 수 있으며, 설정한 범위를 벗어나는 경우 syslog 및 SNMP 트랩을 발생시킬 수 있다.

12.2.1. 온도 설정

시스템의 각 모듈에 대해 온도의 상한 및 하한 임계치를 설정할 수 있다. 임계치 범위를 벗어나는 경우 알람이 발생하며 발생한 알람에 대한 이력을 관리를 할 수 있다.

표 12-2. 온도 설정 관련 명령어

명령어	설명	모드
facility-alarm temperature major value minor value	모든 모듈에 대해 온도 임계치(major/ minor)를 설정한다.	Config
facility-alarm temperature {pfe-module sfe-module <1-6>} major value minor value	각 PFE, SFE 모듈에 온도 임계치 (major/ minor)를 설정한다.	Config
no facility-alarm temperature [pfe-module sfe-module <1-6>]	온도 임계치를 기본값으로 설정한다.	Config
show environment alarm thresholds	파워, FAN, 온도의 알람 임계치 정보를 출력한다.	Privileged
clear facility-alarm [major minor]	알람 이력을 삭제한다.	Privileged

아래 예제는 SFP module 1 에 대해 major 및 minor 온도 임계치를 설정하였다.

```
Switch# configure terminal
Switch(config)# facility-alarm temperature sfp-module 1 major 65 minor
45
Switch(config)# exit
Switch# show environment alarm thresholds
```

-- 생략 --

```
SFE module 1 temperature 42.5'C
  threshold #1 for SFE module 1 temperature:
    (sensor value >= 65'C) is system major alarm
  threshold #2 for SFE module 1 temperature:
    (sensor value >= 45'C) is system minor alarm
SFE module 2 temperature 35.5'C
  threshold #1 for SFE module 2 temperature:
    (sensor value >= 70'C) is system major alarm
  threshold #2 for SFE module 2 temperature:
    (sensor value >= 60'C) is system minor alarm
PFE module 1 temperature 47.0'C
  threshold #1 for PFE module 1 temperature:
    (sensor value >= 65'C) is system major alarm
  threshold #2 for PFE module 1 temperature:
    (sensor value >= 50'C) is system minor alarm
```

12.2.2. Cpu usage 설정

장비에 CPU 사용율에 대한 임계치를 설정하고, 임계치 초과시 syslog 와 SNMP 트랩으로 이를 알린다.

표 12-3. CPU usage threshold 관련 명령어

명령어	설명	모드
cpu usage threshold low <30-100> high <40-100>	CPU usage 의 임계치를 설정하는 명령어이다. CPU 사용률이 임계치 보다 높아지거나 (high) 다시 낮아지면(low) syslog 를 발생한다.	Config
cpu usage time-period (<300> <5> <60>)	CPU 사용률(average) 기준이 되는 시간을 설정한다.	Config
snmp-server enable traps resource cpu-load-monitor	CPU 사용률이 임계치보다 높아지거나(high) 다시 낮아지면(low) snmp trap 을 발생 한다.	Config
show cpu usage	현재의 CPU usage 를 조회한다.	Privileged

12.2.3. Memory Usage 설정

장비에 memory 에 대한 임계치를 설정하고, 사용 가능한 memory 의 사용 가능한 양이 임계치 보다 낮아지면 syslog 와 SNMP 트랩으로 이를 알린다.

표 12-4. Memory usage 관련 명령어

명령어	설명	모드
<code>memory free low-watermark</code> <code><10-70></code>	사용 가능한 memory 량의 임계치를 설정하는 명령어이다. 사용 가능한 memory 가 임계치 보다 낮아지거나 다시 높아지면 syslog 를 발생한다.	Config
<code>snmp-server enable traps</code> <code>resource memory-free-monitor</code>	사용 가능한 memory 가 임계치 보다 낮아지거나 다시 높아지면 SNMP 트랩을 발생한다.	Config
<code>show memory usage</code>	현재의 memory usage 를 조회한다.	Privileged

12.2.4. Application memory 사용 display

각 application 들이 사용하는 memory 관련 정보를 보여주기 위해 다음과 같은 명령을 사용한다

표 12-5. Memory display 관련 명령어

명령어	설명	모드
<code>show memory</code> <code>(bfd bgp imi mstp nsm ospf pimd rip)</code>	각 application 의 memory 사용정보 를 조회한다.	Privileged

12.3. 포트 통계

E7500 Series 스위치는 각 포트의 통계 정보를 제공한다. 포트 통계를 보기 위해서는 다음의 명령을 사용한다.

```
show interface [ifname]
```

E7500 Series 스위치는 운용자에게 아래와 같은 포트 통계 정보를 제공한다.

- **Received Packet Count (Rx Pkt Count)** – The total number of good packets that have been received by the port.
- **Received Byte Count (Rx Byte Count)** – The total number of bytes that were received by the port, including bad or lost frames. This number includes bytes contained in the Frame Check Sequence (FCS), but excludes bytes in the preamble.

- **Transmit Packet Count (Tx Pkt Count)** – The number of packets that have been successfully transmitted by the port.
- **Transmit Byte Count (Tx Byte Count)** – The total number of data bytes successfully transmitted by the port.
- **Received Broadcast (Rx Bcast)** – The total number of frames received by the port that are addressed to a broadcast address.
- **Received Multicast (Rx Mcast)** – The total number of frames received by the port that are addressed to a multicast address.
- **Transmit Collisions (Tx Coll)** – The total number of collisions seen by the port, regardless of whether a device connected to the port participated in any of the collisions.
- **Received Bad CRC Frames (RX CRC)** – The total number of frames received by the port that were of the correct length, but contained a bad FCS value.
- **Receive Oversize Frames (RX Oversize)** – The total number of good frames received by the ports that were of greater than the supported maximum length of 1,522 bytes.
- **Receive Dropped Frames (Rx Drop)** – The total number of dropped frames due to lack of system resources.

다음은 **show interface** 명령으로 통계 데이터를 포함한 포트 정보를 출력하였다.

```
Switch# show interface GigabitEthernet 2/1/11

Giga2/1/11 is up, line protocol is up (connected)
Hardware is Ethernet, address is 0007.709e.2914 (bia 0007.709e.2914)
index 1111 metric 1 mtu 1500 arp ageing timeout 7200
Full-duplex, A-1000Mb/s, media type is 1000BaseLX
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
Bandwidth 1g
inet 3.44.1.230/24 broadcast 3.44.1.255
VRRP Master of : VRRP is not configured on this interface.
Last clearing of "show interface" counters never
60 seconds input rate 88 bits/sec, 0 packets/sec
60 seconds output rate 72 bits/sec, 0 packets/sec
L2/L3 in Switched: ucast 30 pkt - mcast 20,532 pkt
L2/L3 out Switched: ucast 36 pkt - mcast 20,871 pkt
20,565 packets input, 1,782,898 bytes
Received 3 broadcast pkt (20,532 multicast pkt)
0 CRC, 0 oversized, 0 dropped
20,918 packets output, 1,790,946 bytes
0 collisions
0 late collisions, 0 deferred
```

표 12-6. 포트 통계 조회 명령들

명령어	설명	모드
show port counter [detail]	아래 항목에 대해 모든 인터페이스의 누적 통계 정보를 출력한다. <ul style="list-style-type: none"> ■ I-Kbps/ O-Kbps ■ InOctets/ OutOctets ■ InPkts/ OutPkts 	Privileged
show port statistics {all IFNAME}	아래 항목에 대해 인터페이스의 누적 통계 정보를 5 초/1 분/5 분 단위로 출력한다. <ul style="list-style-type: none"> ■ TX: bits/s, pkts/s ■ RX: bits/s, pkts/s 	Privileged
show port statistics avg type [IFNAME]	트래픽 타입 기반의 항목에 대해 인터페이스의 평균 통계 정보를 5 초/1 분/5 분 단위로 출력한다. <ul style="list-style-type: none"> ■ TX: Unicast/Multicast/Broadcast s ■ RX: Unicast/Multicast/Broadcast 	Privileged
show port statistics interface [IFNAME]	아래 항목에 대한 인터페이스의 통계 정보를 출력한다. <ul style="list-style-type: none"> ■ InOctets/ OutOctets ■ InUcastPkts/ OutUcastPkts ■ InMcastPkts/ OutMcastPkts ■ InBcastPkts/ OutBcastPkts ■ IflInDiscards ■ IflInErrors 	Privileged
show port-mib IFNAME	해당 인터페이스의 현재 통계와 누적 통계 정보를 상세하게 출력한다.	Privileged
show interface counters [module <1-6>]	아래 항목에 대해 인터페이스의 누적 통계 정보를 출력한다. module 옵션은 개별 모듈 정보를 출력한다. <ul style="list-style-type: none"> ■ InOctets/ OutOctets ■ InUcastPkts/ OutUcastPkts ■ InMcastPkts/ OutMcastPkts ■ InBcastPkts/ OutBcastPkts 	Privileged
show interface counters errors [module <1-6>]	인터페이스에서 발생한 누적 에러 통계 정보를 출력한다. module 옵션은 개별 모듈 정보를 출력한다.	Privileged

다음은 **show interface counter** 명령을 이용하여 전체 포트의 누적 통계 정보를 출력한 내용이다.

```
Switch# show interface counters
```

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
Te1/1/1	0	0	0	0
Te1/1/2	0	0	0	0
Te1/2/1	0	0	0	0
Te1/2/2	0	0	0	0
Gi2/1/1	0	0	0	0
Gi2/1/2	0	0	0	0

Gi2/1/3	0	0	0	0
Gi2/1/4	0	0	0	0
Gi2/1/5	0	0	0	0
Gi2/1/6	0	0	0	0
Gi2/1/7	0	0	0	0
Gi2/1/8	0	0	0	0
Gi2/1/9	0	0	0	0
Gi2/1/10	0	0	0	0
Gi2/1/11	1,873,636	30	21,577	3
Gi2/1/12	0	0	0	0
Gi2/2/1	32,567,322	437,460	22,565	4
Gi2/2/2	13,388,018	29	21,094	180,777
Gi2/2/3	0	0	0	0
Gi2/2/4	0	0	0	0
Gi2/2/5	14,986,518	37	21,454	205,155
Gi2/2/6	14,985,892	582	20,922	205,139
Gi2/2/7	1,857,912	578	20,932	8
Gi2/2/8	13,638,481	164,376	20,932	3
Gi2/2/9	0	0	0	0
Gi2/2/10	0	0	0	0
Gi2/2/11	1,976,170	50	22,893	7
Gi2/2/12	0	0	0	0
Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
-----	-----	-----	-----	-----
Te1/1/1	0	0	0	0
Te1/1/2	0	0	0	0
Te1/2/1	0	0	0	0
Te1/2/2	0	0	0	0
Gi2/1/1	0	0	0	0
Gi2/1/2	0	0	0	0
Gi2/1/3	0	0	0	0
Gi2/1/4	0	0	0	0
Gi2/1/5	0	0	0	0
Gi2/1/6	0	0	0	0
Gi2/1/7	0	0	0	0
Gi2/1/8	0	0	0	0
Gi2/1/9	0	0	0	0
Gi2/1/10	0	0	0	0
Gi2/1/11	1,880,754	36	21,917	11
Gi2/1/12	0	0	0	0
Gi2/2/1	33,315,630	447,667	22,561	23
Gi2/2/2	1,871,404	114	21,409	6
Gi2/2/3	0	0	0	0
Gi2/2/4	0	0	0	0
Gi2/2/5	6,656,196	68,438	21,465	76
Gi2/2/6	1,868,632	450	21,082	53
Gi2/2/7	3,665,906	455	21,089	28,122
Gi2/2/8	17,120,726	216,612	21,086	36
Gi2/2/9	0	0	0	0
Gi2/2/10	0	0	0	0
Gi2/2/11	2,014,134	59	22,900	12

Gi2/2/12	0	0	0	0
----------	---	---	---	---

다음은 **show port statistics** 명령을 이용하여 특정 포트의 5 초/1 분/5 분 통계 정보를 출력한 내용이다.

```
Switch# show port statistics gi2/1/11

Last clearing of counters 55:03:45
=====
Port                               TX|                               RX
          bits/s          pkts/s|          bits/s          pkts/s
-----
Gi2/1/11 -----
  5 sec.           264           0           296           0
  1 min.            88           0           96           0
  5 min.            72           0           72           0
=====
```

인터페이스의 통계 정보는 현재 값을 나타내는 평균 값과 누적 값으로 보여진다. 아래 명령을 사용하여 인터페이스의 평균 통계 정보를 갱신하는 시간 설정을 바꾸거나 해당 인터페이스에 대해 일정 기간 동안 High/Low threshold 값을 설정하여 모니터링 할 수 있다. .

표 12-7. 포트 통계 설정 명령

명령어	설명	모드
load-interval <i>interval</i>	인터페이스의 평균 통계 정보를 갱신하는 시간을 설정한다.	interface
no load-interval	인터페이스의 평균 통계 정보를 갱신하는 시간을 기본 값으로 변경한다.	interface
input-load-monitor <i>interval low-threshold high-threshold</i>	해당 인터페이스에 대해 일정한 시간 동안 low 및 high 임계 값을 설정하여 수신 트래픽이 해당 임계 값을 벗어나는 경우를 모니터링 할 수 있다.	interface
no input-load-monitor	해당 인터페이스에 대한 모니터링 설정을 해제한다.	interface
show port input-load-monitor	인터페이스에 대한 모니터링 설정을 출력한다.	interface

다음 명령은 포트 통계에 대해 누적 값을 초기화시키는 명령어이다.

표 12-8. 포트 통계 초기화 명령

명령어	설명	모드
clear counters	모든 인터페이스의 통계 누적 값을 초기화한다.	privileged
clear counters <i>IFNAME</i>	특정 인터페이스의 통계 누적 값을 초기화한다.	privileged



Notice SNMP 로 출력되는 값은 **clear counter** 명령으로 초기화되지 않는다.

12.4. RMON (Remote MONitoring)

시스템 운영자는 E7500 Series 스위치가 제공하는 RMON(Remote Monitoring) 기능을 사용하여, 시스템을 보다 효율적으로 운영하고 네트워크의 로드를 줄일 수 있다. 다음 절에서는 RMON 개념 및 E7500 Series 스위치가 지원하는 RMON 기능에 대하여 자세히 설명한다.

12.4.1. RMON 개요

RMON은 IETF(Internet Engineering Task Force)의 RFC 1271와 RFC 1757에 정의되어 있는 국제 표준 규격으로 시스템 운영자가 네트워크를 원격으로 관리하는 기능을 제공한다. 일반적으로 RMON은 다음의 두 가지 구성 요소를 가진다.

- **RMON probe**
 - 원격으로 제어되면서 지속적으로 LAN 세그먼트 또는 VLAN의 통계 정보를 수집하는 지능형 디바이스 또는 소프트웨어 에이전트
 - 수집한 정보를 운영자의 요구가 있을 때 또는 미리 정의한 환경에 따라서 자동으로 관리 호스트에게 전송
- **RMON Manager**
 - RMON probe와 통신하면서 통계 정보를 수집
 - 반드시 RMON probe와 동일한 네트워크에 있을 필요는 없으며, RMON probe를 in-band 또는 out-of-band 연결을 통하여 제어

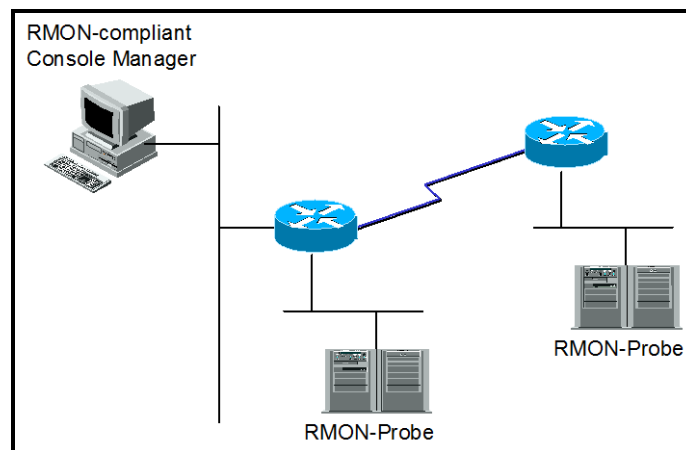


그림 12-1. RMON Manager와 RMON Probe

기존의 SNMP MIBs이 SNMP agent가 탑재된 장비 자체를 관리 대상으로 보고 있는데 반하여 RMON

MIBs는 관리 대상을 장비에 연결된 LAN 세그먼트로 한다. 즉 LAN 세그먼트의 전체 발생 트래픽, 세그먼트에 연결된 각 호스트의 트래픽, 호스트들 사이의 트래픽 발생 현황을 알려준다.

RMON Agent는 전체 통계 데이터, 이력 데이터, 호스트 관련 데이터, 호스트 매트릭스와 사전에 문제 예측 및 제거를 위해서 특정 패킷을 필터링하는 기능과 임계 값을 설정하여 이에 도달하면 자동으로 알려주는 경보 기능 및 사건 발생 기능을 보유하고 있어야 한다.

E7500 Series 스위치에서는 <오류! 참조 원본을 찾을 수 없습니다.8>에서 정의한 RMON의 9개 그룹 중 통계, 이력, 알람, 이벤트 그룹만을 지원한다. RMON은 디폴트로 모든 설정이 disabled이다.

표 12-9. RMON 항목

항목	설명
통계	<ul style="list-style-type: none"> 한 세그먼트에서 발생한 패킷/바이트 수, 브로드캐스트/멀티캐스트 수, 충돌 수 및 패킷 길이별 수 그리고 각종 오류(fragment, CRC Alignment, 길이 미달, 길이 초과 등)에 대한 통계를 제공.
이력	<ul style="list-style-type: none"> 관리자가 설정한 시간 간격 내에 발생한 각종 트래픽 및 오류에 대한 정보를 제공 기본적으로 단기/장기적으로 간격을 설정 가능하고 1-3600 초를 간격으로 제한 이 자료를 통해 시간대별 이용 현황 및 다른 세그먼트와 비교 가능
경보	<ul style="list-style-type: none"> 주기적으로 특정한 값을 체크 해 기준치에 도달하면 관리자에 보고하고 대리인이 자신의 기록을 보유 기준치는 절대값 및 상대값으로 정할 수 있고 지속적인 경보 발생을 막기 위해서 상/하한치를 설정해서 넘나드는 경우에만 경보가 발생.
호스트	<ul style="list-style-type: none"> 세그먼트에 연결된 각 장비가 발생시킨 트래픽, 오류 수를 호스트별로 관리
상위 n 개의 호스트	<ul style="list-style-type: none"> 위 호스트 테이블에 발견될 호스트 중에서 일정시간 동안 가장 많은 트래픽을 발생시킨 호스트 검색 관리자는 원하는 종류의 자료와 시간 간격 및 원하는 호스트의 개수를 설정해서 정보를 수집
트래픽 매트릭스	<ul style="list-style-type: none"> 데이터 링크 계층, 즉 MAC 어드레스를 기준으로 두 호스트간에 발생한 트래픽 및 오류에 대한 정보를 수집 이 정보를 이용해서 특정 호스트에 가장 많은 이용자가 누구인지를 어느 정도는 판별 가능함 다른 세그먼트에 있는 호스트가 가장 많이 이용했다면 이것은 주로 라우터를 통과함으로써 실제 이용자는 알 수 없음.
필터	<ul style="list-style-type: none"> 관리자가 특정한 패킷의 동향을 감시하기 위해서 이용
패킷 수집	<ul style="list-style-type: none"> 세그먼트에 발생한 패킷을 수집해서 관리자가 분석.
사건	<ul style="list-style-type: none"> 특정한 사건이 발생하면 그 기록을 보관하고 관리자에게 경고 메시지를

전송. 트랩 발생 및 기록보관은 선택적임.

12.4.2. RMON 의 Alarm 과 Event 그룹 설정.

사용자는 CLI 또는 SNMP 관리자에 의해서 RMON 을 설정할 수 있다.

표 12-10. RMON Alarm and Event 설정 명령

명령어	설명	모드
<code>rmon alarm <i>index variable interval seconds</i> {absolute delta} rising-threshold <i>value event num</i> falling-threshold <i>value event num</i> [owner <i>string</i>]</code>	RMON alarm 을 추가한다. <ul style="list-style-type: none"> ▪ <i>Index</i>: Alarm 인덱스 ▪ <i>Variable</i>: Alarm 발생 대상으로 SNMP mib 인스턴스를 지정 ▪ <i>Interval</i>: 샘플링 시간 간격 (단위: 초). ▪ <i>Absolute</i>: 샘플링 되는 alarm value 에 대해 절대값을 관찰하도록 설정 ▪ <i>Delta</i>: 샘플링 되는 alarm value 에 대해 현재 값과 이전 값의 차이를 관찰하도록 설정 ▪ <i>Rising-threshold, falling-threshold value</i>: alarm 을 발생시킬 설정 값 ▪ <i>event</i>: Delta 나 absolute 로 샘플링 되는 alarm value 가 rising-threshold 또는 falling - threshold 값에 도달했을 때 각각 해당 Event 가 발생하도록 설정 ▪ <i>owner</i>: Alarm 의 owner 를 등록 	Config
<code>rmon event <i>index</i> [log] [trap <i>community</i>] [description <i>string</i>] [owner <i>string</i>]</code>	RMON event 를 추가한다. <ul style="list-style-type: none"> ▪ <i>Index</i>: Event 인덱스 ▪ <i>log</i>: Event 가 발생한 경우 log 를 생성하도록 설정 ▪ <i>trap</i>: Event 가 발생한 경우 설정한 community 와 함께 trap 을 전송하도록 설정 ▪ <i>owner</i>: Event 의 owner 를 등록 ▪ <i>description</i>: Event 에 대한 설명을 등록 	Config
<code>no rmon alarm <i>alarm-index</i></code>	설정된 RMON alarm 설정을 삭제한다.	Config
<code>no rmon event <i>event-index</i></code>	설정된 RMON event 설정을 삭제한다	Config
<code>show rmon alarms</code>	RMON alarm 정보 출력한다.	Privileged
<code>show rmon events</code>	RMON event 정보 출력한다.	Privileged

아래 예제는 GigabitEthernet 2/2/8 에 대해 rmon alarm 을 설정하였다. GigabitEthernet 2/2/8 의 inOctets 값을 30 초마다 샘플링하며 rising-threshold 및 falling-threshold 를 벗어나면 각 설정된 event 를 발생시키도록 한다. Rmon alarm 을 설정할 때 아래와 같이 event 및 stats 을 먼저 설정 해야 한다.

```
Switch# configure terminal
Switch(config)# rmon event 1 log trap rmon_test description RisingAlarm
Switch(config)# rmon event 2 log trap rmon_test description
FallingAlarm
Switch(config)# interface GigabitEthernet 2/2/8
Switch(config-if-Giga2/2/8)# rmon collection stats 1
Switch(config)# rmon alarm 1 etherStatsEntry.4.1158 interval 30
absolute rising-threshold 2000000 event 1 falling-threshold 1000000
event 2
Switch(config)# exit
Switch# show rmon alarm
Alarm 1 is active, owned by RMON_SNMP
  Monitors etherStatsOctets.1158 every 30 second(s)
  Taking Absolute samples, last value was 00
  Rising threshold is 2000000, assigned to event 1
  Falling threshold is 1000000, assigned to event 2
  On startup enable rising or falling alarm alarmRisingThreshold : 15
alarmFallingThreshold : 0
alarmRisingEventIndex : 1
alarmFallingEventIndex : 1
alarmOwner : hong
Switch# show rmon event
  event Index = 1
    Description RisingAlarm
    Event type Log & Trap
    Event community name rmon_test
    Last Time Sent = 5774:38:20
    Owner RMON_SNMP

  event Index = 2
    Description FallingAlarm
    Event type Log & Trap
    Event community name rmon_test
    Last Time Sent = 00:00:00
    Owner RMON_SNMP
Switch# show rmon statistics
Collection 1 on Giga2/2/8 is active, and owned by RMON_SNMP,
Monitors ifEntry.1.1158 which has
Received 014354459 octets, 0195285 packets,
  03 broadcast and 021164 multicast packets,
  00 undersized and 00 oversized packets,
  00 fragments and 00 jabbers,
  00 CRC alignment errors and 00 collisions.
# of dropped packet events (due to lack of resources): 00
# of packets received of length (in octets):
64: 01585, 65-127: 0440336, 128-255: 0308
256-511: 04, 512-1023: 00, 1024-1518: 00
```

표 12-11. RMON History 설정 및 statistics 명령

명령어	설명	모드
rmon collection stats <i>index</i> [owner <i>string</i>]	물리적 인터페이스의 통계 값을 수집한다. <ul style="list-style-type: none"> ▪ <i>Index</i>: etherStats 인덱스, 	Interface
rmon collection history <i>index</i> [buckets <i>number</i>] [interval <i>seconds</i>] [owner <i>string</i>]	물리적 인터페이스에 대하여 이력을 수집한 다. <ul style="list-style-type: none"> ▪ <i>Index</i>: History 인덱스, ▪ <i>buckets</i>: 수집할 이력의 수 ▪ <i>Interval</i>: 이력 수집 간격 (단위: 초) ▪ <i>owner</i>: History의 owner를 등록. 	Interface
no rmon collection stats <i>index</i>	물리적 인터페이스의 통계 값을 수집하지 않 도록 설정한다.	Interface
no rmon collection history <i>index</i>	물리적 인터페이스의 이력을 수집하지 않도 록 설정한다.	Interface
show rmon history	RMON history 정보를 출력한다.	Privileged
show rmon statistics	RMON statistics 정보를 출력한다.	Privileged
rmon clear counters	해당 인터페이스의 statistics 값을 초기화한 다.	Interface

아래 예제는 GigabitEthernet 2/2/8에 대해 10초마다 최대 30개의 bucket을 이용해 RMON 이력을 수집하도록 설정한다.

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet 2/2/8
Switch(config-if-Giga2/2/8)# rmon collection stats 1
Switch(config-if-Giga2/2/8)# rmon collection history 1 buckets 30
interval 10
Switch(config-if-Giga2/2/8)# exit
Switch(config)#exit
Switch# show rmon history
Entry 1 is active, and owned by RMON_SNMP
Monitors ifIndex 1158 every 10 second(s)
Requested # of time intervals, ie buckets, is 30,
Sample # 1 began measuring Received 14953616 octets, 203700
packets,
3 broadcast and 21362 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
# of dropped packet events is 0
Sample # 2 began measuring Received 14956451 octets, 203740
packets,
3 broadcast and 21363 multicast packets,
```

```

0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
# of dropped packet events is 0
Sample # 3 began measuring   Received 14959509 octets, 203783
packets,
3 broadcast and 21364 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
# of dropped packet events is 0

```

12.5. Logging

E7500 Series 스위치 로그는 모든 환경 설정 정보와 경보 발생 정보를 보여 준다. 시스템 메시지 로깅 소프트웨어는 스위치의 메모리에 로그 메시지를 저장하며, 다른 디바이스로 메시지를 보낼 수 있다. 시스템 메시지 로깅 기능은 다음을 지원한다.

- 사용자에게 수집할 로깅 타입을 선택할 수 있도록 한다.
- 사용자에게 수집한 로깅을 보낼 디바이스를 선택할 수 있도록 한다.

E7500 Series 스위치는 기본적으로 내부 버퍼와 시스템 콘솔에 디버그 레벨의 로그를 저장하고 보낸다. 사용자는 CLI를 사용하여 로깅되는 시스템 메시지를 제어할 수 있다. 최대 약 1000 개의 로그 메시지를 시스템 버퍼에 저장한다. 시스템 운영자는 시스템 메시지를 Telnet 이나 콘솔을 통해서, 또는 syslog server 의 로그를 봄으로써 원격으로 모니터 할 수 있다.

E7500 Series 스위치는 0-7 까지의 Severity 레벨을 가지고 있다.

표 12-12. E7500 Series 스위치의 로그 레벨

Severity 레벨	설명
Emergencies (0)	시스템 사용 불가.
Alerts (1)	즉각적인 조치가 필요한 상태
Critical (2)	Critical 상태.
Errors (3)	에러 메시지.
Warnings (4)	경고 메시지.
Notifications (5)	정상적인 상태지만 중요한 정보.
Informational (6)	사용자에게 제공하는 정보 메시지.

Debugging (7) 디버깅 메시지.

12.5.1. 시스템 로그 메시지 내용

E7500 Series 스위치의 시스템 로그 메시지는 다음과 같은 내용을 제공한다.

- **Timestamp**
 - Timestamp 는 이벤트가 발생한 월, 날짜, 연도 및 구체적인 시간 정보를 Month Day HH:MM: SS 와 같이 기록한다.
- **Severity level**
 - <표 12>에서 정의한 E7500 Series 의 로그 메시지의 레벨
 - 0-7 까지의 숫자
- **Log description**
 - 발생한 이벤트에 대한 상세한 정보를 포함하는 텍스트 문자열

다음은 시스템 부팅 시의 로그 메시지 이다.

```
May 6 11:53:48 [5] %REMOTE-CONNECT: login from console as lns
May 6 11:54:01 [5] IFM-NOTICE: Rate limit ra creation
May 7 02:10:24 [5] %REMOTE-CONNECT: login from console as lns
May 7 02:10:40 [5] IFM-NOTICE: Flow xx classified
May 7 02:10:48 [5] IFM-NOTICE: Flow xx match rate 10
May 7 05:17:56 [5] %REMOTE-CONNECT: login from console as lns
May 7 05:23:10 [5] IFM-NOTICE: Service pa add interface fa1
```

12.5.2. 디폴트 Logging 설정 값.

표 12-13. 시스템 로그 기본 설정 값

설정 파라미터	기본 설정 값
콘솔로의 로깅 출력	disable
Telnet 세션으로의 로깅 출력	disable.
로깅 버퍼 사이즈	1MB
Time-Stamp 출력	enabled
Logging Server	disabled
Syslog server IP address	None configured
Server facility	LOCAL7
Server severity	Warnings(4)
콘솔의 Severity	Debuggings(7)
Telnet 의 Severity	info (6)

표 12-14. 시스템 메시지 로깅 환경 설정 명령

명령어	설명
logging console {<0-7> alerts critical debugging emergencies errors informations notifications warnings}	콘솔로의 로깅 출력 여부 설정 및 환경 설정.
logging facility {auth cron daemon kernel local0 local1 local2 local3 local4 local5 local6 local7 lpr mail news syslog user uucp}	syslog 메시지를 보낼 Facility parameter 를 설정.
logging A.B.C.D	syslog 메시지를 외부 syslog 서버 에 보낼지 설정
logging monitor alerts critical debugging emergencies errors informations notifications warnings}	현 세션으로의 로깅 출력 여부 설 정.
logging source-ip A.B.C.D	syslog packet 의 source ip 를 설정
logging trap alerts critical debugging emergencies errors informations notifications warnings}	syslog server 의 logging level 설정
show logging	로깅 버퍼 출력 및 로깅 설정 확인.

12.5.3. Logging 설정 예.

Console 로 접속한 경우 Log level notice(5) 이하의 log message 만을 console 로 출력하고자 할 때 다음과 같이 설정한다. console 로 log message 출력을 중단하고자 할 경우 “no logging console” command 를 사용한다.

```
Switch# configure terminal
Switch(config)# logging console notifications
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# no logging console
Switch(config)#
```

Telnet 으로 접속한 경우 Log level warn(4) 이하의 log message 만을 telnet session 에 출력하고자 할 때 다음과 같이 설정한다. Telnet session 으로 log message 출력을 중단하고자 할 경우 “logging session disable” command 를 사용한다.

```
Switch#
Switch# configure terminal
Switch(config)# logging monitor warnings
Switch(config)# end
Switch#
Switch# configure terminal
```



```
Switch(config)# no logging session  
Switch(config)#
```

Log server 100.10.1.1 에 이 switch 에서 발생하는 log 중 Log level err(5) 이하의 log message 를 보내고자 할 경우 다음과 같이 설정한다. log server 로 log message 보내는 것을 중단하고자 할 경우 “no logging A.B.C.D” command 를 사용한다.

```
Switch# configure terminal  
Switch(config)# logging 100.10.1.1  
Switch(config)# logging trap errors  
Switch(config)# end  
Switch#  
Switch# configure terminal  
Switch(config)# no logging 100.10.1.1  
Switch(config)#
```

13

STP(Spanning Tree Protocol)

이 장에서는 Spanning Tree Protocol(STP)과 Rapid Spanning Tree Protocol(RSTP), Multiple Spanning Tree(MSTP), Rapid Per Vlan Spanning Tree Plus (RPVST+)를 설정하는 방법과 Bridge에서의 프레임 전송에 대해 설명한다.

**Note**

이 장에서 사용되는 명령의 완전한 형식 및 사용법은 `command reference` 를 참고하라.

이 장은 다음의 절들로 구성된다:

- Understanding Spanning-Tree Features
- Understanding RSTP
- Understanding MSTP
- Understanding RPVST+
- Configuring Spanning-Tree Features
- Displaying the Spanning-Tree Status
- Configuring Bridge Mac Forwarding

13.1. Understanding Spanning-Tree Features

이 절에서는 다음의 STP 기능에 대해 설명한다:

- STP Overview
- Supported Spanning-Tree Instances
- Bridge Protocol Data Units
- Election of the Root Switch
- Bridge ID, Switch Priority, and Extended System ID
- Spanning-Tree Timers
- Creating the Spanning-Tree Topology
- Spanning-Tree Interface State

13.1.1. STP Overview

STP는 네트워크에서 루프를 방지하고 경로의 이중화를 제공하는 Layer 2 링크 관리 프로토콜이다. Layer 2 이더넷(Ethernet) 네트워크가 정상적으로 동작하려면, 임의의 두 단말 사이에는 오직 하나의 활성 경로만 존재해야 한다. Spanning-tree의 동작은 종단 단말(end station)들에 대해 투명하기 때문에, 종단 단말들은 단일 LAN에 연결되었는지 여러 개의 조각으로 구성된 switched LAN에 연결되었는지 감지할 수 없다.

고장에 견고한 네트워크 형상을 구성하려면, 네트워크의 모든 노드들 사이에는 루프가 없어야 한다. Spanning-tree 알고리즘은 switched Layer 2 네트워크를 통해 루프가 없는 최적의 경로를 계산한다. 스위치는 주기적으로 bridge protocol data unit(BPDU)라 불리는 spanning-tree 프레임을 송수신한다. 스위치는 이 프레임들을 forward 하지 않고, 루프가 없는 경로를 생성하기 위해 사용한다.

두 종단 단말 사이에 여러 개의 활성화된 경로가 존재하면 네트워크에 루프가 발생한다. 네트워크에 루프가 존재한다면 종단 단말은 중복된 프레임을 수신할 것이다. 스위치에서는 한 종단 단말의 MAC 주소가 여러 개의 Layer 2 인터페이스에 등록된다. 이런 상황은 네트워크를 불안정하게 만든다.

Spanning tree는 Layer 2 네트워크에서 root 스위치와 root 스위치로부터 모든 스위치까지 루프가 없는 경로를 가진 tree를 정의한다. Spanning tree는 중복된 데이터 경로를 standby(blocked) 상태로 만든다. 중복된 경로가 존재하는 네트워크에 고장이 발생하면, spanning-tree 알고리즘은 spanning-tree 형상을 새로 계산하고 standby 경로를 활성화시킨다.

스위치의 두 인터페이스가 루프의 일부라면, spanning-tree port priority와 path cost 설정이 인터페이스의 forwarding 상태와 blocking 상태를 결정한다. port priority 값은 네트워크에서 인터페이스의 위치와 트래픽을 위해 얼마나 잘 위치하고 있는가를 나타낸다. path cost 값은 매체의 속도를 나타낸다.

13.1.2. Bridge Protocol Data Units

다음의 요소들에 의해 spanning-tree의 안정된 active 형상이 결정된다:

- 각 VLAN과 연관된 유일한 BridgeID(스위치 priority와 MAC 주소)
- root 스위치로의 spanning-tree path cost
- 각 Layer 2 인터페이스에 할당된 포트 식별자(포트 priority와 포트 번호)

스위치에 전원이 들어왔을 때, 스위치는 root 스위치처럼 동작한다. 각 스위치는 자신의 모든 포트에 configuration BPDU를 전송한다. 스위치들은 BPDU를 서로 교환하고 BPDU로 spanning-tree 형상을 계산한다. 각 configuration BPDU는 다음의 정보를 포함한다:

- root 스위치의 BridgeID
- root까지의 spanning-tree path cost
- BPDU를 전송하는 스위치의 BridgeID
- Message age
- BPDU를 전송하는 스위치의 인터페이스 식별자

- hello, forward-delay, max-age 프로토콜 타이머의 값

스위치가 자신보다 우월한 정보(낮은 BridgeID, 낮은 path cost, 등등)를 가진 BPDU 를 수신했을 경우, 그 정보를 BPDU 를 수신한 포트에 저장한다. BPDU 를 수신한 포트가 root 포트라면, 스위치는 메시지를 갱신해서 자신의 designated LAN 으로 전달한다.

스위치가 현재 포트의 정보보다 열등한 정보를 포함한 BPDU 를 수신하면 그 BPDU 를 버린다. 스위치가 designated LAN 으로부터 열등한 메시지를 수신했다면, 포트에 저장된 정보로 갱신된 BPDU 를 LAN 으로 전송한다. 이런 방식으로 열등한 정보는 버려지고 우월한 정보가 네트워크에 전파된다.

다음은 BPDU 교환으로 인한 결과이다:

- 네트워크의 한 스위치가 root 스위치로 선택된다.
- Root 스위치를 제외한 각 스위치에서 root 포트가 선택된다. 이 포트는 스위치가 root 스위치로 패킷을 전송할 때 최적의 경로(가장 낮은 비용)를 제공한다.
- 각 스위치는 path cost를 기반으로 root 스위치까지의 최단 거리를 계산한다.
- 각각의 LAN을 위한 designated 스위치가 결정된다. designated 스위치는 LAN에서 root 스위치로 패킷을 전달할 때 가장 낮은 path cost를 제공한다. LAN과 연결된 designated 스위치의 포트를 designated 포트라 부른다.
- Spanning-tree 에 포함되는 인터페이스들이 결정된다. root 포트와 designated 포트는 forwarding 상태에 놓인다.
- Spanning-tree에 포함되지 않는 모든 인터페이스들은 blocked 된다.

13.1.3. Election of Root Switch

Layer 2 네트워크의 spanning tree 에 참여하는 모든 스위치는 BPDU 의 교환을 통해 다른 스위치들에 관한 정보를 모은다. 이러한 메시지의 교환은 다음의 행위를 야기한다:

- 각 spanning-tree instance에 대한 유일한 root 스위치 선출
- 모든 switched LAN 조각을 위한 designated 포트 결정
- 중복된 링크로 연결된 Layer 2 인터페이스의 차단에 의한 switched 네트워크의 루프 제거

각 VLAN 에서 가장 높은 스위치 priority(작은 숫자 값을 가진)를 가진 스위치가 root 스위치로 결정된다. 모든 스위치가 default priority(32768)로 설정되었다면, VLAN 에서 가장 낮은 MAC 주소를 가진 스위치가 root 스위치가 된다. 스위치 priority 는 BridgeID 의 최상위 비트에 포함된다.

스위치의 스위치 priority 의 값을 변경함으로써 그 스위치가 root 스위치가 될 가능성을 변경할 수 있다. 스위치 priority 를 큰 값으로 설정하면 가능성이 낮아지고, 작은 값으로 설정하면 가능성이 높아진다.

Root 스위치는 switched 네트워크에서 spanning-tree 형상의 논리적인 중심이다. Switched 네트워크에서 root 스위치로 달을 필요가 없는 경로들은 spanning-tree blocking 상태가 된다.

BPDU 는 BPDU 를 전송하는 스위치와 포트, 스위치의 MAC 주소, 스위치 priority, port priority, path cost 등의 정보를 포함한다. Spanning tree 는 이 정보를 사용하여 root 스위치와 root 포트, designated 포트를 결정한다.

13.1.4. Bridge ID, Switch Priority, and Extended System ID

IEEE 802.1D 표준에 따르면 각 스위치는 root 스위치를 선택하기 위해 사용되는 유일한 브리지 식별자(BridgeID)를 가진다. 각 VLAN 은 논리적으로 서로 다른 브리지로 간주되므로 스위치는 VLAN 별로 서로 다른 BridgeID 를 가질 수 있다. 스위치는 8 바이트의 BridgeID 를 가진다; 최상위 2 바이트는 스위치 priority 로 사용되고, 나머지 6 바이트는 스위치의 MAC 주소이다.

Premier 8700 Series 스위치는 802.1T spanning-tree extensions 를 지원한다. 표와 같이 스위치 priority 로 사용되던 2 바이트가 4 비트 priority 값과 VLAN ID 와 동일한 12 비트 extended system ID 값으로 재할당 되었다.

Switch Priority Value				Extended System ID(Set Equal to the VLAN ID)											
Bit16	Bit15	Bit14	Bit13	Bit12	Bit11	Bit10	Bit9	Bit8	Bit7	Bit6	Bit5	Bit 4	Bit3	Bit2	Bit1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

표 13-1 Switch Priority Value and Extended System ID

Spanning tree 는 extended system ID 와 스위치 priority, 그리고 MAC 주소로 BridgeID 를 만든다.

13.1.5. Spanning-Tree Timers

표는 spanning-tree 의 성능에 영향을 미치는 타이머들을 나타낸다.

Variable	Description
Hello timer	스위치가 다른 스위치로 얼마나 자주 hello 메시지를 전송할 것인가를 결정한다.
Forward-delay timer	인터페이스가 forwarding 상태가 되기 전에 listening 과 learning 상태에서 각각 얼마나 머물 것인가를 결정한다.
Maximum-age timer	인터페이스로 수신한 프로토콜 정보를 얼마 동안 저장할 것인가를 결정한다.

표 13-2 Spanning-Tree Timers

13.1.6. Creating the Spanning-Tree Topology

그림에서 모든 스위치들의 스위치 priority 가 default(32768)이고 스위치 A 가 가장 낮은 MAC 주소를 가진다고 가정하면 스위치 A 가 root 스위치가 된다. 하지만, forwarding 인터페이스의 개수 혹은 link-type 때문에 스위치 A 는 이상적인 root 스위치가 아니다. Root 스위치로 만들려는 스위치의 priority 를

증가시킴으로써(낮은 숫자 값을 사용), spanning-tree 의 형상을 재계산하여 이상적인 스위치를 root 로 만들 수 있다.

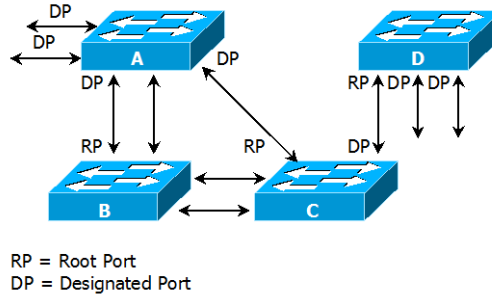


그림 13-1 Spanning-Tree Topology

default 인자를 기반으로 spanning-tree 형상을 계산하면, 시작 단말과 목적지 단말 사이의 경로는 이상적이지 않다. 예로, root 포트보다 높은 포트 번호를 가진 인터페이스에 연결된 고속의 링크는 스위치의 root 포트 변경을 야기할 수 있다. 목표는 가장 빠른 링크를 root 포트로 만드는 것이다.

예를 들어 스위치 B 의 한 포트가 기가비트 이더넷 링크이고, 스위치 B 의 다른 포트(10/100 링크)가 현재 root 포트라고 가정하자. 네트워크 트래픽이 기가비트 이더넷 링크를 통해 전달되는 것이 더 효과적이다. 기가비트 이더넷 인터페이스의 port priority 를 root 포트보다 더 높은 priority(낮은 숫자 값)를 가지도록 변경함으로써, 기가비트 이더넷 인터페이스를 새로운 root 포트로 만들 수 있다.

13.1.7. Spanning-Tree Interface States

프로토콜 정보가 switched LAN 을 통해 전달될 때 전파지연이 발생한다. 그 결과 다른 시각, 다른 장소에서 switched LAN 의 형상변화가 발생한다. Spanning-tree 에 참여하지 않는 Layer 2 인터페이스가 바로 forwarding 상태가 된다면 일시적인 데이터 루프가 발생할 수 있다. 그러므로 스위치는 프레임을 forwarding 하기 전에 switched LAN 을 통해 전파되는 새로운 형상 정보를 기다려야 한다.

Spanning tree 가 활성화된 스위치의 각 Layer 2 인터페이스는 다음 상태 중 하나이다:

- Blocking - 인터페이스는 프레임을 forwarding 하지 않는다.
- Listening - 인터페이스가 프레임을 forwarding 해야 한다고 결정되었을 때, blocking state 다음의 천이 상태.
- Learning - 인터페이스가 프레임을 forwarding 하기 위해 준비한다. MAC learning이 수행된다.
- Forwarding - 인터페이스가 프레임을 forward 한다.
- Disabled - 포트가 shutdown 상태이거나 포트에 링크가 없거나, 포트에 실행중인 spanning-tree instance가 없기 때문에 인터페이스는 spanning tree에 참여하지 않는다.

인터페이스들은 다음의 상태로 이동한다:

- 초기상태에서 blocking 상태로
- blocking 상태에서 listening 혹은 disabled 상태로

- listening 상태에서 learning 혹은 disabled 상태로
- learning 상태에서 forwarding 혹은 disabled 상태로
- forwarding 상태에서 disabled 상태로

다음의 그림은 인터페이스의 상태천이를 보여준다.

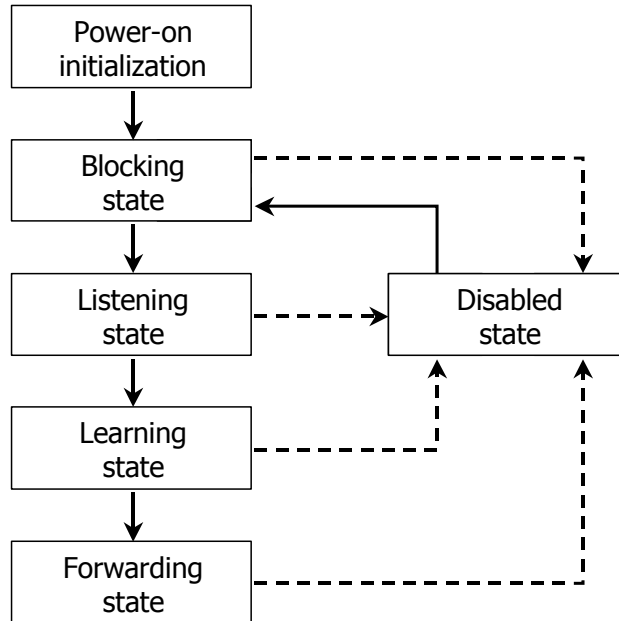


그림 13-2 Spanning-Tree Interface States

STP 가 활성화 되었을 때, 스위치의 모든 인터페이스는 blocking 상태가 되고 listening 과 learning 의 일시적인 상태를 지난다. 안정화된 spanning tree 에서 각 인터페이스는 forwarding 혹은 blocking 상태로 설정된다.

Spanning-tree 알고리즘이 Layer 2 인터페이스를 forwarding 상태로 만들기로 결정했다면 다음의 과정이 발생한다:

1. 인터페이스가 forwarding 상태가 되어야 한다는 프로토콜 정보를 수신하면 인터페이스는 listening 상태가 된다.
2. forward-delay 타이머가 만료되었을 때, spanning tree는 인터페이스를 learning 상태로 만들고 forward-delay 타이머를 재설정한다.
3. learning 상태에서, 인터페이스는 종단 단말의 MAC learning은 수행하면서 프레임의 forwarding은 차단한다.
4. forward-delay 타이머가 만료되면, spanning tree는 인터페이스를 forwarding 상태로 만들고, learning 과 프레임의 forwarding이 모두 가능하다.

Blocking State

Blocking state 의 Layer 2 인터페이스는 프레임을 forwarding 하지 않는다. 스위치는 초기화 후에 스위치의 각 인터페이스로 BPDU 를 전송한다. 스위치는 다른 스위치와 BPDU 를 교환할 때까지 자신이 root 스위치 인 것처럼 동작한다. 이러한 BPDU 의 교환은 네트워크의 한 스위치를 root 스위치로 결정한다.

네트워크에 오직 하나의 스위치만 있다면 스위치 간의 BPDU 교환은 발생하지 않으며, forward-delay 타이머는 종료되면 인터페이스는 listening 상태에 놓인다. 인터페이스는 스위치 초기화 후에 항상 blocking 상태로 설정된다.

인터페이스는 blocking 상태에서 다음과 같이 동작한다:

- 포트로 수신된 프레임을 폐기한다
- forwarding을 위해 다른 인터페이스로부터 스위칭된 프레임들을 폐기한다
- 주소를 learning 하지 않는다
- BPDU를 수신한다

Listening State

listening state 는 blocking 상태 다음의 천이 상태이다. 인터페이스가 프레임을 forwarding 해야 한다고 결정되면, 인터페이스는 listening 상태가 된다.

인터페이스는 listening 상태에서 다음과 같이 동작한다:

- 포트로 수신된 프레임을 폐기한다
- forwarding을 위해 다른 인터페이스로부터 스위칭된 프레임들을 폐기한다
- 주소를 learning 하지 않는다
- BPDU를 수신한다

Learning State

learning 상태의 Layer 2 인터페이스는 프레임 forwarding 을 준비한다. 인터페이스는 listening 상태에서 learning 상태로 들어간다.

인터페이스는 learning 상태에서 다음과 같이 동작한다:

- 포트로 수신된 프레임을 폐기한다
- forwarding을 위해 다른 인터페이스로부터 스위칭된 프레임들을 폐기한다
- 주소를 learning 한다
- BPDU를 수신한다

Forwarding State

forwarding 상태의 Layer 2 인터페이스는 프레임을 forward 한다. 인터페이스는 learning 상태에서 forwarding 상태로 들어간다.

인터페이스는 forwarding 상태에서 다음과 같이 동작한다:

- 포트로 수신된 프레임들을 forward 한다
- 다른 인터페이스로부터 스위칭된 프레임들을 forward 한다
- 주소를 learning 한다
- BPDU를 수신한다

Disable State

disabled 상태의 Layer 2 인터페이스는 프레임 forwarding 이나 spanning tree 에 참여하지 않는다.

disable 된 인터페이스는 다음과 같이 동작한다:

- 포트로 수신된 프레임을 폐기한다
- forwarding을 위해 다른 인터페이스로부터 스위칭된 프레임들을

- 폐기한다
- 주소를 learning 하지 않는다
- BPDU를 수신하지 않는다.

13.2. Understanding RSTP

RSTP는 point-to-point 연결에 대해 spanning tree의 빠른 복구를 제공하는 장점을 가진다. Spanning tree의 재구성은 1초(802.1D spanning tree의 default 설정에서 최대 50초가 소요되는 것과는 대조적으로) 이내에 완료된다. 이것은 음성과 영상과 같은 지연에 민감한 트래픽을 전송하는 네트워크에 유효하다.

이 절은 RSTP가 어떻게 동작하는 지를 설명한다:

- RSTP Overview
- Port Roles and the Active Topology
- Rapid Convergence
- Bridge Protocol Data Unit Format and Processing

13.1.8. RSTP Overview

RSTP는 스위치, 스위치 포트 혹은 LAN에 장애가 발생했을 경우, 재빠른 연결의 복구(약 1초 이내)를 제공한다. 새로운 root 포트로 선택된 포트는 바로 forwarding 상태로 천이할 수 있고, 스위치 사이의 명시적인 acknowledgement를 통해 designated 포트도 forwarding 상태로 바로 천이할 수 있다.

13.1.9. Port Roles and the Active Topology

RSTP는 active 형상을 결정하기 위한 port role을 할당함으로써 spanning tree의 빠른 복구를 제공한다. RSTP는 STP처럼 가장 높은 스위치 priority(가장 낮은 priority 값)를 가진 스위치를 root 스위치로 선택한다. 그리고 RSTP는 각각의 포트에 다음과 같은 port role을 할당한다:

- Root port – 스위치가 root 스위치로 패킷을 forward 할 때 최적의 경로(가장 낮은 cost)를 제공한다.
- Designated port – designated 스위치와 연결되어, LAN에서 root 스위치로 패킷을 forward 할 때 가장 낮은 비용을 제공한다. LAN과 연결되어 있는 designated 스위치의 포트를 designated port라 부른다.
- Alternate port – 현재 root 포트가 제공하는 root 스위치로의 대체 경로를 제공한다.
- Backup port – spanning tree의 앞쪽으로 향한 designated 포트에 의해 제공되는 경로의 backup으로 동작한다. Backup 포트는 두 포트가 point-to-point 링크로 loopback으로 연결되었거나 스위치가 공유 LAN 조각에 대해 둘 이상의 연결이 있을 경우에만 존재한다.

- Disabled port – spanning tree의 동작에서 아무런 역할도 가지지 않는다.

root 혹은 designated 포트 역할을 가진 포트는 active 형상에 포함된다. alternate 혹은 backup 포트 역할을 가진 포트는 active 형상에서 제외된다.

네트워크 전체가 일관된 port role 을 가진 안정된 형상에서, RSTP 는 모든 root 포트와 designated 포트가 바로 forwarding 상태로 천이하는 것을 보장한다. 반면 모든 alternate 포트와 backup 포트는 항상 discarding 상태(802.1D의 blocking 과 동등한 상태)에 놓인다. 포트의 상태는 forwarding 과 learning 과정의 동작을 제어한다. 다음의 표는 802.1D 와 RSTP 의 포트 상태를 비교한다.

Operational Status	STP Port State	RSTP Port State	Is Port Included in the Active Topology?
Enabled	Blocking	Discarding	No
Enabled	Listening	Discarding	No
Enabled	Learning	Learning	Yes
Enabled	Forwarding	Forwarding	Yes
Disabled	Disabled	Discarding	No

표 13-3 Port State Comparison

STP 구현과의 일관성을 위해, 이 문서에서는 포트 상태에서 *discarding* 대신 *blocking* 을 사용한다. Designated port 는 listening 상태에서 시작한다.

13.1.10. Rapid Convergence

RSTP 는 다음과 같은 스위치, 포트 혹은 LAN 의 장애에 대해 빠른 연결의 복구를 제공한다. edge 포트와 새로운 root 포트, 그리고 point-to-point 링크로 연결된 포트에 대해 빠른 복구를 제공한다:

- Edge ports – RSTP 스위치에서 포트를 edge 포트로 설정하면, edge 포트는 forwarding 상태로 바로 천이한다. edge 포트는 STP에서 PortFast가 설정된 포트와 동일하고, 하나의 종단 단말과 연결된 포트에만 설정해야 한다.
- Root ports – RSTP가 새로운 root 포트를 선택하면, 이전의 root 포트는 block 상태가 되고, 새로운 root 포트는 바로 forwarding 상태가 된다.
- Point-to-point links – 포트를 다른 포트와 point-to-point 링크로 연결한다면, 로컬 포트는 designated 포트가 되고 루프를 제거하기 위해 다른 포트와 proposal-agreement 교환을 통한 빠른 천이를 협상한다.

다음 그림에서, 스위치 A 는 스위치 B 와 point-to-point 링크로 연결되어 있고 모든 포트는 blocking 상태이다. 스위치 A 의 priority 가 스위치 B 의 priority 보다 낮은 수의 값을 가진다고 가정하자. 스위치 A 는 proposal 메시지(proposal flag 가 설정된 BPDU)를 스위치 B 로 전송하고 자신을 designated 스위치로 제안한다.

스위치 B 는 proposal 메시지를 수신한 후에, proposal 메시지를 수신한 포트를 새로운 root 포트로 선택하고, 모든 non-edge 포트를 blocking 상태로 설정하고, agreement 메시지(agreement flag 를 설정한 BPDU)를 새로운 root 포트를 통해 전송한다.

스위치 B 의 agreement 메시지를 수신한 후에, 스위치 A 는 자신의 designated 포트를 forwarding 상태로 천이한다. 스위치 B 가 자신의 모든 non-edge port 를 block 시키고, 스위치 A 와 스위치 B 사이는 point-to-point 링크로 연결되었기 때문에 네트워크에 루프가 발생하지 않는다.

스위치 C 가 스위치 B 와 연결될 때, 유사한 협상 메시지가 교환된다. 스위치 C 는 스위치 B 와 연결된 포트를 root 포트로 선택하고, 두 스위치의 두 포트는 forwarding 상태로 천이한다. 협상 과정에서 하나 이상의 스위치가 active 형상에 참여한다. 네트워크의 복구에서 이런 proposal-agreement 협상은 spanning tree 의 root 에서 앞 방향으로 진행된다.

스위치는 포트의 duplex 모드로 link-type 을 결정한다: full-duplex 포트는 point-to-point 연결로 고려되고; half-duplex 포트는 공유 연결로 고려된다. interface configuration 명령 spanning-tree link-type 명령으로 duplex 모드에 의해 결정되는 default 설정을 변경할 수 있다.

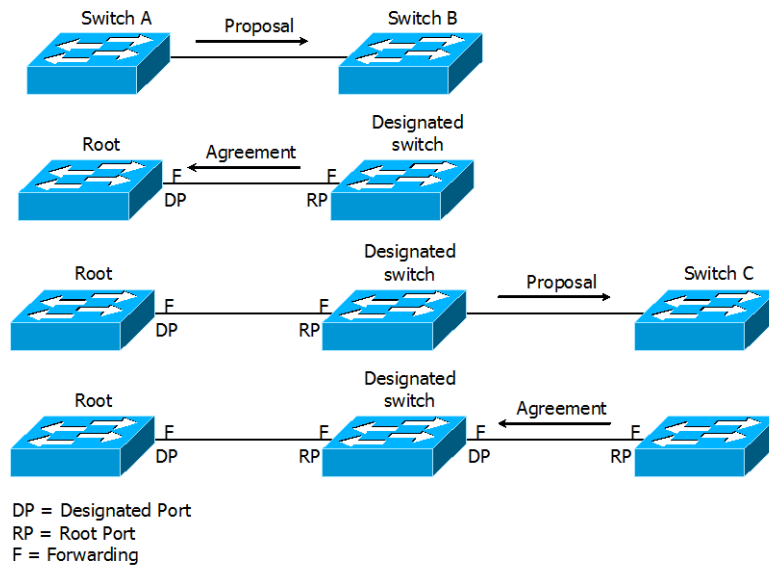


그림 13-3 Proposal and Agreement Handshaking for Rapid Convergence

13.1.11. Bridge Protocol Data Unit Format and Processing

protocol version 필드의 값이 2 로 설정되는 것을 제외하고 RSTP BPDU 의 형식은 IEEE 802.1D BPDU 형식과 같다. 새로운 1 바이트 version 1 Length 필드는 0 으로 설정된다; 이는 version 1 프로토콜 정보를 포함하지 않는다는 의미이다. 다음의 표는 RSTP flag 필드를 보여준다.

표 4 RSTP BPDU Flags

Bit	Function
0	Topology change (TC)
1	Proposal
2-3:	Port role:
00	Unknown
01	Alternate port
10	Root port
11	Designated port
4	Learning
5	Forwarding
6	Agreement
7	Topology change acknowledgement (TCA)

자신을 LAN 의 designated 스위치로 제안하려는 스위치는 RSTP BPDU 의 proposal flag 를 설정해서 전송한다. proposal 메시지의 port role 은 항상 designated 포트로 설정된다.

다른 스위치에 의한 제안을 받아들이는 스위치는 RSTP BPDU 의 agreement flag 를 설정해서 전송한다. agreement 메시지의 port role 은 항상 root port 로 설정된다.

RSTP 는 독립적인 topology change notification (TCN) BPDU 를 사용하지 않는다. topology change 를 알리기 위해 RSTP BPDU flag 의 topology change (TC) flag 를 사용한다. 하지만 802.1D 스위치와의 연동을 위해 TCN BPDU 를 생성하고 처리한다.

전송하는 포트의 상태에 따라 learning 과 forwarding flag 가 설정된다.

13.3. Understanding MSTP

MSTP (Multiple Spanning Tree Protocol)은 IEEE 802.1s 에 정의된 프로토콜이며, 복수개의 VLAN 을 하나의 그룹으로 묶어 스페닝 트리를 동작시킨다. MSTP 에서는 인스턴스라고 하는 VLAN 그룹당 하나의 스페닝 트리가 동작하므로 많은 수의 스페닝 트리를 계산할 필요가 없어 스위치의 부하를 줄인다. 예를 들어, 2000 개의 VLAN 을 사용하는 네트워크에서 PVST 를 사용하면 스위치들이 2000 개의 스페닝 트리를 계산해야 한다. 그러나 MSTP 를 사용하여 2000 개의 VLAN 을 2 개의 그룹으로 나눈다면 스페닝 트리는 2 개만 사용하게 된다 뿐만 아니라 MSTP 가 동작하면 BPDU 전송량도 획기적으로 줄어든다. 이처럼 MSTP 를 사용하여 스페닝 트리의 수를 줄일 수 있는 것은 대부분의 스위치 네트워크에서 밀의 그림에서 나타내듯 로드 밸런싱 시킬 수 있는 경로 수만큼의 스페닝 트리만 필요하기 때문이다.

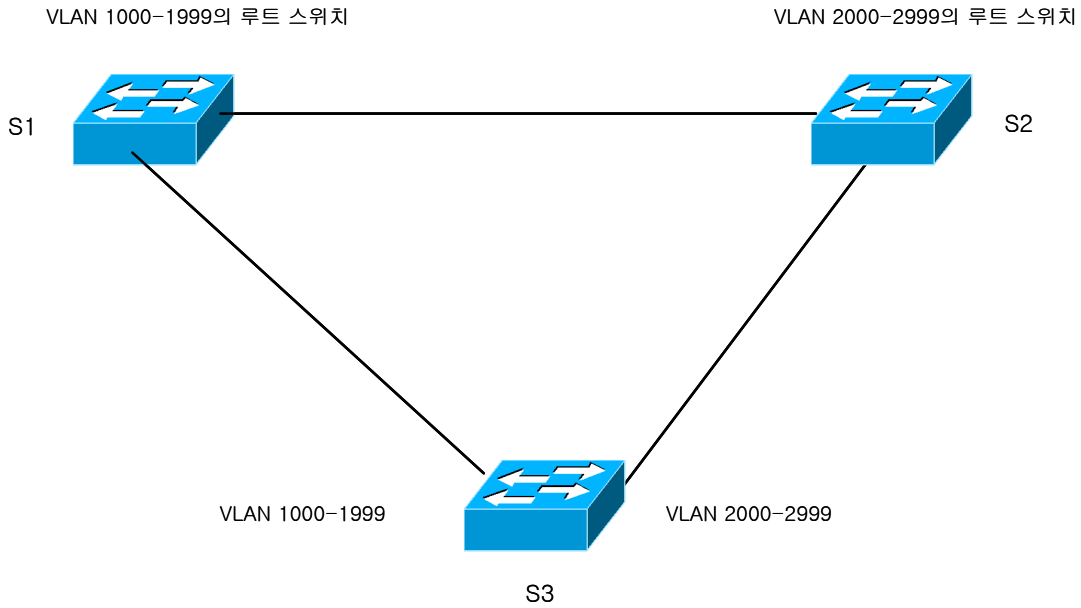


그림 13-4 VLAN 에 대한 load balance

즉, 스위치 S3 에서 사용되는 VLAN 이 1000-2999 까지 2000 개라 하여도 스페닝 트리가 2 개만 동작하면 S1, S2 로 로드 밸런싱 시킬 수 있다.

13.1.12. MST 영역

동일한 MST 설정값을 가진 스위치의 집합을 하나의 MST 영역 (region)이라고 한다. MST 설정값 중에서 MST name, MST revision 및 instance 의 VLAN list 값이 일치하는 스위치들을 동일한 MST 영역에 있다고 한다.

13.1.13. IST, CST 및 CIST

MSTP 에서는 2 가지 종류의 스페닝 트리가 사용된다. 하나의 MST 영역내에서는 IST (Internal Spanning Tree)가 동작 한다. 동일 MST 영역에서 모두 63 개의 스페닝 트리를 동작시킬 수 있다. 각각의 스페닝 트리 인스턴스에 0 에서 63 까지의 번호를 사용할 수 있으며, 이중에서 인스턴스 0 을 IST 라고 한다. MST 에서는 IST 만 BPDU 를 송수신 한다. 따라서 다른 인스턴스의 스페닝 트리 정보가 모두 IST 의 BPDU 에 포함되어 있으며, 스위치가 처리해야 하는 BPDU 의 수가 더욱 줄어든다. MST 영역을 포함한 전체 스위치 네트워크에서 공통으로 CIST (common and Internal Spanning Tree)가 동작한다. CIST 는 IST 와 CST 의 집합이다. IEEE 802.1Q 에서는 복수개의 VLAN 이 존재해도 스페닝 트리는 하나만 동작하며, 이 스페닝 트리를 CST (common Spanning Tree)라고 한다. IST, CST 및 CIST 의 관계를 그림으로 나타내면 다음과 같다

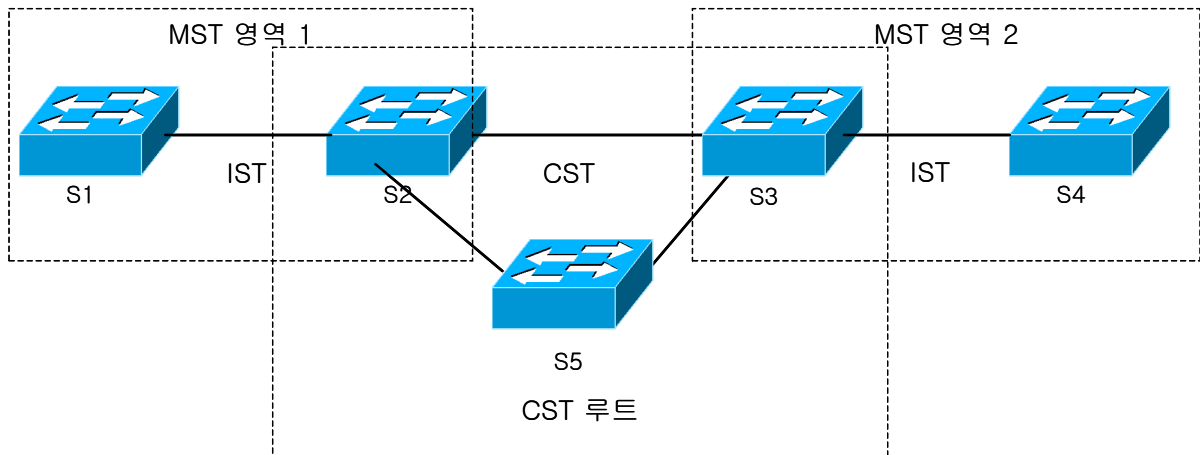


그림 13-5 CST, IST, CIST

MST 영역이 다르면 IST도 서로 별개로 동작한다. 서로 다른 MST 영역 사이에는 IST가 아닌 CST가 동작한다. 따라서 그림에서 스위치 S1, S2의 MST 영역이 스위치 S3, S4와 서로 다르므로 각각의 MST 영역에서 동작하는 IST는 별개로 동작하며, 두 영역을 연결하는 스위치 S2와 S3 사이에는 CST가 동작한다. 각 MST 영역내에서 CST 루트 스위치까지의 경로값, 브리지 ID, 포트 ID 값이 가장 작은 스위치를 IST master라고 한다. 위의 그림처럼 S5가 CST 루트 스위치라면 S2와 S3이 각각의 MST 영역에서 IST master 스위치로 동작한다. CST 루트 스위치가 MST 영역 밖에 있다면, IST 마스터는 항상 CST와 MST의 경계상에 있게 된다. 만약 스위치 네트워크가 하나의 MST 영역으로 구성된 경우에는 동일한 스위치가 CST 루트와 IST 마스터로 동작한다. CST는 서로 다른 MST 영역간 뿐만 아니라 802.1D로 동작하는 스위치 사이 또는 MST와 802.1D 스위치 사이에서도 동작한다. CST의 관점에서 하나의 MST 영역 전체를 하나의 스위치로 간주한다. 따라서 위와 같은 네트워크를 CST에서는 다음 그림과 같이 인식한다.

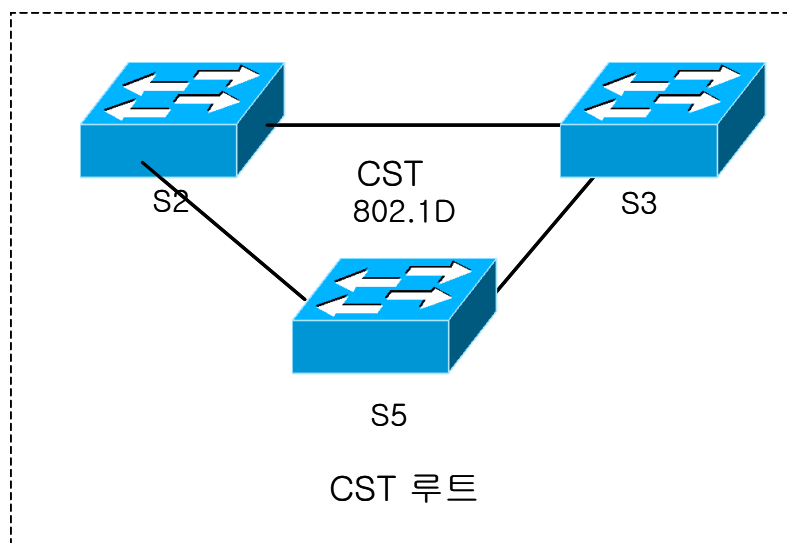


그림 13-6 CST에서 인식하는 네트워크

13.4. Understanding RPVST+

VLAN trunk 에 관한 표준인 IEEE 802.1Q 는 trunk 에 허용된 모든 VLAN 에 대해 오직 하나의 spanning-tree instance 만 요구하고 있다. 그리고 기존의 PVST (Per Vlan Spanning-Tree)의 경우 각 VLAN 별로 spanning-tree instance 를 제공 하지만 IEEE 802.1D 와는 다른 frame 포맷을 사용하기 때문에 연동 되지 않는다. RPVST+ (Rapid Per Vlan Spanning-tree plus)는 이러한 문제를 해결하기 위해서 VLAN trunk 에서 BPDU 를 전송 할 때 0100.0CCC.CCCD 의 Multicast MAC 주소를 이용한다. VLAN ID 가 1 이고 native 인 경우 untagged 로 전송되고 VLAN ID 가 1 이 아닌 native 의 경우 tagged 로 전송된다. 이를 통해 VLAN trunk 의 각 vlan 마다 존재하는 spanning-tree instance 가 IEEE 802.1Q 만을 지원하는 스위치를 지나도 BPDU 를 올바르게 전송 할 수 있다.

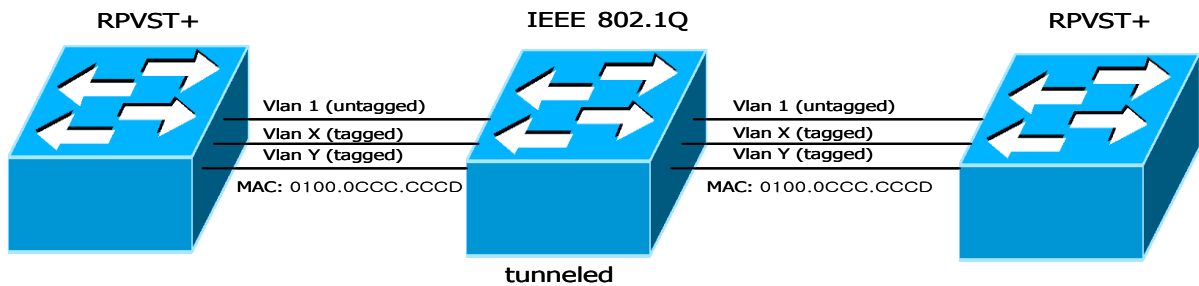


그림 13-7 PVST+ switch 와 IEEE 802.1Q 연동

13.5. Configuring Spanning-Tree Features

이 절에서는 spanning-tree 를 설정하는 방법에 대해 설명한다. Spanning-tree 의 설정 방법은 mode 에 따라 차이가 있다. RSTP 와 STP 의 경우 같은 방법으로 설정되고 MSTP, RPVST+의 경우 다른 설정방법을 갖는다.

13.1.14. Default STP Configuration

다음의 표는 STP의 default 설정을 보여준다.

표 5 Default STP Configuration

Feature	Default Setting
Enable state	모든 bridge에 대해 비활성 되어 있음. 기본적으로 RSTP 모드가 설정되어 있는 상황에서 disable로 되어있어서 enable시킬 경우 RSTP가 시작됨
Spanning-tree mode	IEEE 802.1w RSTP.
System priority	32768.
Spanning-tree port priority (configurable on a per-port)	128.
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	10000 Mbps: 2. 1000 Mbps: 4. 100 Mbps: 19. 10 Mbps: 100.
Hello time	2 초.
Forward-delay time	15 초.
Maximum-aging time	20 초.

13.1.15. STP Configuration Guidelines

E7500 Series는 PVST를 지원하지 않는다. 그래서 Bridge에 1개의 spanning-tree가 구동되고 여기에 붙어 있는 VLAN은 어떠한 영향을 미치지 않는다. 대신에 bridge마다 spanning-tree를 구동할 수 있고 bridge는 256개까지 생성 가능하다. VLAN은 1개의 Bridge에만 속할 수 있고 trunk VLAN의 경우는 default Bridge에만 속하게 되어있다. Trunk VLAN에서 spanning-tree를 구동할 경우 전체 VLAN에 1개의 spanning-tree가 구동되도록 하거나 RPVST+ 모드에서 각 VLAN별로 spanning-tree를 구동할 수 있다.

13.1.16. Enabling STP

E7500 Series에서 처음에 STP는 동작하지 않는다. 네트워크에 루프가 존재할 가능성이 있다면 STP를 활성화 시키도록 한다. STP를 활성화 시키면 기본적으로 RSTP가 구동 된다.



Caution STP 가 비활성 되어있고 형상에 루프가 존재한다면, 과도한 트래픽과 무한의 패킷 중첩이 발생하여 네트워크의 성능을 감소시킨다.

STP 를 활성화시키려면 privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	spanning-tree enable	Default Bridge 에 대해 STP 를 구동한다
Step3	end	privileged EXEC 모드로 변경한다.
Step4	show spanning-tree	설정 내용을 확인한다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

STP 를 비활성 하려면, global configuration 명령 **spanning-tree shutdown bridge-forward** 를 사용한다.

다음은 STP 를 활성화하고 비활성화하는 예를 보여준다

```
Switch#
Switch# configure terminal
Switch(config)# spanning-tree enable
Switch(config)#
Switch(config)# end
Switch#
Switch# show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
  Root ID   Priority   32768
    Address 00077074ff01
  This bridge is the root
  Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec

  Bridge ID Priority   32768
    Address 00077074ff01
  Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec
  Aging Time 300

Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga6/1/2   Disb BLK 4      128.610 Shared

Switch#
Switch# configure terminal
```

```
Switch(config)# spanning-tree shutdown bridge-forward
Switch(config)# end
Switch# show spanning-tree
Spanning tree instance(s) does not exist

Switch#
```

13.1.17. Enable STP in not default Bridge

E7500 Series 는 Bridge 별로 spanning-tree 를 운영할 수 있다. Bridge 를 생성하고 여기에 spanning-tree 로 동작되길 원하는 interface 를 포함 시킨 후 해당 Bridge 의 spanning-tree 를 활성화 시키면 된다.



Note

Bridge 에 spanning-tree 를 구동하기 위해 포함 시키는 interface 는 직접 Bridge 에 넣을 수 없고 VLAN 에 넣은 후 그 VLAN 을 Bridge 에 넣어야 한다.

Default Bridge 이외의 Bridge 의 STP 기능을 활성화 시키려면, privileged EXEC 모드에서부터 다음의 과정을 거친다:

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	Bridge <1-256> protocol vlan-bridge	Bridge 를 생성한다.
Step3	bridge <1-256> spanning- tree enable	Bridge 의 STP 를 enable 한다.
Step4	Bridge-group <1-256>	Vlan 을 Bridge 에 포함시킨다.
Step5	copy running-config startup- config	(옵션) 설정을 configuration 파일에 저장한다.

Default Bridge이외의 Bridge의 STP기능을 비활성화 하려면, global configuration 명령 **bridge shutdown <1-256> bridge-forward** 명령을 사용하라. Bridge를 삭제 하기 위해서는 **no bridge <1-256>** 명령을 사용한다.

```
Switch#
Switch# show spanning-tree

Spanning tree instance(s) does not exist

Switch# configure terminal
```

```
Switch(config) Bridge 1 protocol vlan-bridge
Switch(config) Bridge 1 spanning-tree enable
Switch(config)# interface Vlan100
Switch (config-if-Vlan100)#bridge-group 1
Switch(config)# end
Switch# show running-config
!
bridge 1 protocol vlan-bridge
bridge 1 spanning-tree enable
!
Switch#
Switch# configure terminal
Switch(config)# bridge shutdown 1 bridge-forward
Switch(config)# no bridge 1
Switch(config)# end
Switch# show running-config
!
!
Switch#
```

13.1.18. Configuring the Port Priority

루프가 발생하면 spanning tree 는 포트의 priority 를 사용하여 forwarding 상태의 인터페이스를 결정한다. 먼저 선택될 인터페이스에는 높은 priority 의 값(낮은 수)을, 나중에 선택될 인터페이스에는 낮은 priority 의 값(높은 수)를 할당할 수 있다. 모든 인터페이스가 같은 priority 값을 가진다면, spanning tree 는 낮은 인터페이스 번호를 가진 인터페이스를 forwarding 상태로 만들고 다른 인터페이스들은 block 시킨다.

인터페이스의 priority 를 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	interface <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹이다.
Step3	spanning-tree port-priority <i>priority</i>	인터페이스의 포트 priority 를 설정한다. ● <i>priority</i> 의 범위는 0~240 사이의 16의 배수이다. default는 128 이다. 낮은 수가 높은 priority를 의미한다. 유효한 값은 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224와 240이다. 이 외의 다른 값들은 거부된다.
Step4	end	privileged EXEC 모드로 변경한다.

Step5	show spanning-tree	설정 내용을 확인한다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

인터페이스의 default 설정으로 복구하려면, interface configuration 명령 **no spanning-tree priority** 를 사용한다. Default Bridge가 아닌 경우에는 spanning-tree 대신 **bridge <1-256>** 을 사용한다.

```
shu#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID   Priority   32768
Address   00077074ff01
This bridge is the root
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority   32768
Address   00077074ff01
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300

Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga6/1/1   Disb BLK 4      128.611 Shared

shu # configure terminal
shu(config)#int GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#spanning-tree port-priority 0
shu(config-if-Giga6/1/1)#end
shu # show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID   Priority   32768
Address   00077074ff01
This bridge is the root
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority   32768
Address   00077074ff01
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300

Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga6/1/1   Disb BLK 4      0.611 Shared

shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#no spanning-tree port-priority
shu(config-if-Giga6/1/1)#end
shu#show spanning-tree
```

```

Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID Priority 32768
      Address 00077074ff01
      This bridge is the root
      Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority 32768
      Address 00077074ff01
      Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec
      Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
-----
Giga6/1/1 Disb BLK 4 128.611 Shared

shu#
    
```

13.1.19. Configuring the Path Cost

spanning-tree 의 path cost 의 default 값은 인터페이스의 속도로부터 결정된다. 루프가 발생하면 spanning tree 는 포트의 cost 를 사용하여 forwarding 상태의 인터페이스를 결정한다. 먼저 선택될 인터페이스에는 낮은 cost 값을, 나중에 선택될 인터페이스에는 높은 cost 값을 할당할 수 있다. 모든 인터페이스가 같은 cost 값을 가진다면, spanning tree 는 낮은 인터페이스 번호를 가진 인터페이스를 forwarding 상태로 만들고 다른 인터페이스들은 block 시킨다.



Note

port group 일 경우 path cost 의 값을 인터페이스의 속도로부터 결정할 수 없다: 각각의 멤버 포트가 서로 다른 속도를 가질 수 있다. 따라서 port group 에 대해서는 수동으로 path cost 를 설정해서 사용하라.

인터페이스의 path cost 를 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	interface interface-id	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹이다.
Step3	spanning-tree path-cost cost	cost 를 설정한다. 루프가 발생했을 때 forwarding 상태의 포트를 결정하기 위해 spanning tree 는 path cost 를 사용한다. path cost 값이 낮을 수록 고속의 전송이 가능함을 의미한다. ● cost 의 범위는 1~200000000 이다. default 값은 인터페이스의 전송속도로부터 결정된다.
Step4	end	privileged EXEC 모드로 변경한다.
Step5	show spanning-tree	설정 내용을 확인한다.

Step6 **copy running-config startup-config** (옵션) 설정을 configuration 파일에 저장한다.

인터페이스의 default 설정으로 복구하려면, interface configuration 명령 **no spanning-tree path-cost** 를 사용한다. Default Bridge가 아닌 경우에는 spanning-tree 대신 **bridge <1-256>** 을 사용한다.

```
shu#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID   Priority   32768
Address   00077074ff01
This bridge is the root
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority   32768
Address   00077074ff01
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Giga6/1/1	Disb	BLK	4	128.611	Shared

```
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#spanning-tree path-cost 10
shu(config-if-Giga6/1/1)#end
shu#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID   Priority   32768
Address   00077074ff01
This bridge is the root
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority   32768
Address   00077074ff01
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Giga6/1/1	Disb	BLK	10	128.611	Shared

```
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#no spanning-tree path-cost
shu(config-if-Giga6/1/1)#end
shu#sh spanning-tree
```

```

Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority 32768
Address 00077074ff01
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
-----
Giga6/1/1 Disb BLK 4 128.611 Shared

shu#
    
```

13.1.20. Configuring the Switch Priority of a VLAN

스위치가 root 스위치가 될 가능성을 높이기 위해 스위치 priority 를 변경할 수 있다.

VLAN 에 대한 스위치 priority 를 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	spanning-tree priority <i>priority</i>	<ul style="list-style-type: none"> <i>priority</i> 의 범위는 0~61440 사이의 4096의 배수이다. default는 32768 이다. 낮은 수일수록 root 스위치로 선택될 가능성이 높다. 유효한 priority 값은 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344과 61440 이다. 다른 값들은 거부된다.
Step3	end	privileged EXEC 모드로 변경한다.
Step4	show spanning	설정 내용을 확인한다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

스위치의 default 설정으로 복구하려면, global configuration 명령 **no spanning-tree priority** 명령을 사용하라. . Default Bridge가 아닌 경우에는 spanning-tree 대신 **bridge <1-256>** 을 사용한다.

```

shu#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority 32768
    
```

```
Address 00077074ff01
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Giga6/1/1	Disb	BLK	4	128.611		Shared

```
shu#
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#spanning-tree priority 4096
shu(config)#end
shu#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID Priority 4096
Address 00077074ff01
This bridge is the root
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec
```

```
Bridge ID Priority 4096
Address 00077074ff01
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Giga6/1/1	Disb	BLK	4	128.611		Shared

```
shu#conf t
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#no spanning-tree priority
shu(config)#end
shu#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec
```

```
Bridge ID Priority 32768
Address 00077074ff01
Hello Time 1 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Giga6/1/1	Disb	BLK	4	128.611		Shared


```
shu#
```

13.1.21. Configuring the Hello Time

hello time 을 변경함으로써 root 스위치가 전송하는 configuration BPDU 의 주기를 설정할 수 있다.

hello time 을 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	spanning-tree hello-time seconds	hello time 은 root 스위치가 configuration 메시지를 전송하는 주기이다. 이 메시지는 스위치가 살아있음을 의미한다. • seconds 의 범위는 1~10 이다. default 는 2 이다.
Step3	end	privileged EXEC 모드로 변경한다.
Step4	show spanning-tree	설정 내용을 확인한다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

스위치의 default 설정으로 복구하려면, global configuration 명령 **no spanning-tree hello-time** 명령을 사용하라. Default Bridge가 아닌 경우에는 spanning-tree 대신 **bridge <1-256>** 을 사용한다.

```
shu#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID   Priority   32768
Address   00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority   32768
Address   00077074ff01
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300

Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga6/1/1   Disb BLK 4      128.611 Shared

shu#
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#spanning-tree hello-time 9
shu(config)#end
shu#show spanning-tree
detail interface mst rpvtst+
shu#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 9 sec Max Age 20 sec Foward Delay 15 sec
```

```
Bridge ID Priority 32768
Address 00077074ff01
Hello Time 9 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
Giga6/1/1 Disb BLK 4 128.611 Shared
```

```
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#no spanning-tree hello-time
shu(config)#end
shu#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
```

```
Bridge ID Priority 32768
Address 00077074ff01
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
Giga6/1/1 Disb BLK 4 128.611 Shared
```

```
shu#
```

13.1.22. Configuring the Forwarding-Delay Time for a VLAN

VLAN 의 forwarding-delay time 을 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	spanning-tree forward-time seconds	forward delay 는 포트가 spanning-tree 의 listening 혹은 learning 상태에서 forwarding 상태로 천이하기 위해 기다리는 시간이다.

	● <i>seconds</i> 의 범위는 4~30 이다. default는 15 이다.
Step3	end privileged EXEC 모드로 변경한다.
Step4	show spanning-tree 설정 내용을 확인한다.
Step5	copy running-config startup-config (옵션) 설정을 configuration 파일에 저장한다.

스위치의 default 설정으로 복구하려면, global configuration 명령 **no spanning-tree forward-time** 명령을 사용하라. Default Bridge가 아닌 경우에는 **spanning-tree** 대신 **bridge <1-256>** 을 사용한다.

```

shu#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID   Priority   32768
Address   00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority   32768
Address   00077074ff01
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300

Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga6/1/1   Disb BLK 4      128.611 Shared

shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#spanning-tree forward-time 20
shu(config)#end
shu#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID   Priority   32768
Address   00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Foward Delay 20 sec

Bridge ID Priority   32768
Address   00077074ff01
Hello Time 2 sec Max Age 20 sec Foward Delay 20 sec
Aging Time 300

Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga6/1/1   Disb BLK 4      128.611 Shared

shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#no spanning-tree forward-time
    
```

```

shu(config)#end
shu#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID   Priority   32768
        Address   00077074ff01
        This bridge is the root
        Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority   32768
        Address   00077074ff01
        Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
        Aging Time 300

Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga6/1/1   Disb BLK 4      128.611 Shared

shu#
    
```

13.1.23. Configuring the Maximum-Aging Time for a VLAN

maximum-aging time 을 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	spanning-tree max-age seconds	maximum-aging time 을 설정한다. maximum-aging time 은 스위치가 재구성을 하기 전에 spanning-tree 정보를 수신하지 않고 기다리는 최대 시간이다. ● seconds 의 범위는 6~40 이다. default는 20 이다.
Step3	end	privileged EXEC 모드로 변경한다.
Step4	show spanning-tree	설정 내용을 확인한다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

스위치의 default 설정으로 복구하려면, global configuration 명령 **no spanning-tree max-age** 명령 을 사용하라. Default Bridge가 아닌 경우에는 spanning-tree 대신 **bridge <1-256>** 을 사용한다.

```

shu#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID   Priority   32768
        Address   00077074ff01
        This bridge is the root
        Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority   32768
        Address   00077074ff01
    
```

```
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

```
Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga6/1/1   Disb BLK 4    128.611 Shared
```

```
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#spanning-tree max-age 15
shu(config)#end
shu#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 15 sec Foward Delay 15 sec
```

```
Bridge ID Priority 32768
Address 00077074ff01
Hello Time 2 sec Max Age 15 sec Foward Delay 15 sec
Aging Time 300
```

```
Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga6/1/1   Disb BLK 4    128.611 Shared
```

```
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#no spanning-tree max-age
shu(config)#end
shu#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
```

```
Bridge ID Priority 32768
Address 00077074ff01
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

```
Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga6/1/1   Disb BLK 4    128.611 Shared
```

```
shu#
```

13.1.24. Changing the Spanning-Tree mode for switch

E7500 Series 는 STP, RSTP, MSTP, RPVST+ mode 를 지원하고 mode 가 정해지면 모든 Bridge 는 정해진 mode 로 변경 되고 disable 상태로 변한다.

스위치의 spanning-tree 모드를 변경하려면, privileged EXEC 모드부터 다음의 과정을 거친다

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	spanning-tree mode {rstp stp mstp rpvst+}	스위치의 spanning-tree 모드를 변경한다.
Step3	end	privileged EXEC 모드로 변경한다.
Step4	show running-config	설정 내용을 확인한다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

```
shu#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
```

```
Bridge ID Priority 32768
Address 00077074ff01
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
Giga6/1/1 Disb BLK 4 128.611 Shared
```

```
shu#configure terminal
```

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

```
shu(config)#spanning-tree mode stp-vlan-bridge
```

```
shu(config)#end
```

```
shu(config)#spanning-tree enable
```

```
shu(config)#end
```

```
shu#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled stp-vlan-bridge
Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
```

```
Bridge ID Priority 32768
Address 00077074ff01
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
```

Aging Time 300

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Giga6/1/1	Disb	DIS	4	128.611		Shared

```
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#spanning-tree mode mstp
shu(config)#spanning-tree enable
shu(config)#end
shu#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled mstp
Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority 32768
Address 00077074ff01
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Giga6/1/1	Disb	BLK	20000	128.611		Shared

```
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#spanning-tree mode rpvst+
shu(config)#spanning-tree enable
shu(config)#end
shu#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rpvst+
Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority 32768
Address 00077074ff01
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Giga6/1/1	Disb	BLK	4	128.611		Shared

```
shu#
```

13.1.25. Configuring the Port as Edge Port

RSTP 를 사용할 때, 단일 호스트와 연결된 포트에 대해서 edge port 로 설정한다. 만약 포트를 edge 포트로 설정하지 않으면, 그 포트는 forwarding 상태로 천이하는데 2 x Forward Time 이 소요된다.



Note 단말과 연결된 포트에 대해서는 반드시 edge port 로 설정해야 한다. 그렇지 않으면, 네트워크의 STP 형상에 변화가 발생할 때 단말이 연결된 포트의 STP 상태도 영향을 받게된다.

포트를 edge port 로 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	Interface <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹이다.
Step2	spanning-tree edgeport	포트를 edge port로 설정한다.
Step3	end	privileged EXEC 모드로 변경한다.
Step4	show running-config	설정 내용을 확인한다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

스위치의 default 설정으로 복구하려면, interface configuration 명령 **no spanning-tree edgeport** 명령을 사용하라.

```
shu#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID   Priority   32768
Address   00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority   32768
Address   00077074ff01
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300

Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga6/1/1   Disb BLK 4      128.611 Shared

shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#spanning-tree edgeport
shu(config-if-Giga6/1/1)#end
shu#show spanning-tree
```



```
Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
```

```
Bridge ID Priority 32768
Address 00077074ff01
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
Giga6/1/1 Disb BLK 4 128.611 Shared edge port
```

```
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#no spanning-tree edgeport
shu(config-if-Giga6/1/1)#end
shu#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
```

```
Bridge ID Priority 32768
Address 00077074ff01
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
Giga6/1/1 Disb BLK 4 128.611 Shared
```

```
shu#
```

13.1.26. Specifying the Link Type to Ensure Rapid Transitions

포트를 다른 포트와 point-to-point 링크로 연결한다면, 로컬 포트는 designated 포트가 된다.

기본적으로 link-type 은 인터페이스의 duplex 모드에 의해 결정된다: full-duplex 포트는 point-to-point 연결로 간주되고; half-duplex 모드는 공유 연결로 간주된다. 물리적으로 point-to-point 로 상대 스위치의 포트와 연결된 half-duplex 링크를 가지고 있다면, link-type 의 default 설정을 변경함으로써 forwarding 상태로의 빠른 천이를 가능하게 할 수 있다.



Note port group 의 경우 duplex 모드로부터 링크의 종류를 판단할 수 없다: 각각의 멤버 포트가 서로 다른 duplex 모드를 가질 수 있다. 따라서 port group 에 대해서는 수동으로 링크 종류를 설정해서 사용하라.

default link-type 를 변경하려면, privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	interface <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	spanning-tree link-type point-to-point	포트의 링크 종류를 point-to-point 로 설정한다.
Step4	end	privileged EXEC 모드로 변경한다.
Step5	show running-config	설정 내용을 확인한다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

default 설정으로 복구하려면, interface configuration 명령 **no spanning-tree link-type** 명령을 사용한다.

13.6. Configuring MSTP Features

이 절에서는 multiple spanning-tree(MSTP)를 설정하는 방법에 대해 설명한다. MSTP 의 경우 instance 별로 spanning-tree 가 구성 되기 때문에 instance 를 생성하고 여기에 VLAN 을 포함시키는 부분과 STP 나 RSTP 와 같이 hello time, port priority 등을 설정하는 부분으로 나뉜다.

13.1.27. Instance 생성 및 VLAN 연결

Instance 를 생성하고 여기에 VLAN 을 넣기 위해서는 privileged EXEC 모드에서부터 다음의 과정을 거친다

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	Spanning-tree configuration mst	Instance 를 생성하고 vlan 과 연결시키기 위해 mst configuration 모드로 진입한다.
Step3	instance <i>instance-id</i> vlan <i>vlan-id</i>	Instance id 를 생성하고 여기에 vlan-id 에 있는 vlan 을 포함시킨다
Step4	exit	Global configuration 모드로 진입한다.
Step5	interface <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로

		진입한다.
Step6	Spanning-tree instance <i>instance-id</i>	Instance 에 해당 포트를 넣는다
Step7	end	privileged EXEC 모드로 변경한다.
Step8	show running-config	설정 내용을 확인한다.
Step9	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

생성되어 있는 instance 를 삭제할 경우에는 **no instance** *instance-id* 명령을 사용하라.

```

shu#show spanning-tree mst configuration

name [Default]
Revision 0 Instances configured 0

% Instance VLAN
% 0: 2-3, 100
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#spanning-tree mst configuration
shu(config-mst)#instance 1 vlan 2
shu(config-mst)#exit
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#spanning-tree instance 1
shu(config-if-Giga6/1/1)#end
shu#show spanning-tree mst configuration

name [Default]
Revision 0 Instances configured 0

% Instance VLAN
% 0: 3, 100
% 1: 2
shu# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#spanning-tree mst configuration
shu(config-mst)#no instance 1 vlan 2
shu(config-mst)#end
shu#show spanning-tree mst configuration
name [Default]
Revision 0 Instances configured 0

```

```
% Instance      VLAN
% 0:            2-3, 100
shu#
```

13.1.28. instance and port configuration

MSTP 에서는 각 instance 마다 spanning-tree 가 동작하기 때문에 instance 별로 priority 를 설정한다. 여기서 사용되는 명령어 들은 STP, RSTP 에서 사용되는 명령어에 instance 가 붙어서 사용된다. Instance 에 priority 를 설정하기 위해서는 privileged EXEC 모드에서부터 다음의 과정을 거친다

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	Spanning-tree instance <i>instance-id priority priority</i>	Instance 에 priority 를 설정한다
Step3	end	privileged EXEC 모드로 변경한다.
Step4	show running-config	설정 내용을 확인한다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

default 값으로 복구하려면 **no spanning-tree instance instance-id priority** 명령을 사용한다.

```
shu#show spanning-tree mst
##### MST1  vlans mapped:2
Bridge   address 0007.7074.ff01 priority   32768 (32768 sysid 0)
Root     this switch for the CIST
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role  Sts Cost   Prio.Nbr Type
-----
-----
Giga6/1/1     Disb  BLK 20000  128.611 Shared

shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#spanning-tree instance 1 priority 4096
shu(config)#end
shu#show spanning-tree mst
##### MST1  vlans mapped:2
Bridge   address 0007.7074.ff01 priority   4096 (4096 sysid 0)
Root     this switch for the CIST
```

```

Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role   Sts Cost   Prio.Nbr Type
-----
-----
Giga6/1/1     Disb   BLK 20000 128.611 Shared

shu#
    
```

port 에 관한 설정도 마찬가지로 **instance *instance-id***가 추가 된다.

port 의 **priority** 값을 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	interface <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	Spanning-tree instance <i>instance-id</i> priority <i>priority</i>	port 에 priority 를 설정한다
Step4	end	privileged EXEC 모드로 변경한다.
Step5	show running-config	설정 내용을 확인한다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

default 값으로 복구하려면 **no spanning-tree instance *instance-id* priority** 명령을 사용한다.

```

shu#show spanning-tree mst
#### MST1   vlans mapped:2
Bridge     address 0007.7074.ff01 priority    32768 (32768 sysid 0)
Root      this switch for the CIST
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role   Sts Cost   Prio.Nbr Type
-----
-----
Giga6/1/1     Disb   BLK 20000 128.611 Shared

shu#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
    
```

```

shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#spanning-tree instance 1 priority 0
shu(config-if-Giga6/1/1)#end
shu#show spanning-tree mst
##### MST1   vlans mapped:2
Bridge    address 0007.7074.ff01  priority    32768 (32768 sysid 0)
Root      this switch for the CIST
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role   Sts Cost   Prio.Nbr Type
-----
-----
Giga6/1/1     Disb   BLK 20000   0.611 Shared

shu#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#no spanning-tree instance 1 priority
shu(config-if-Giga6/1/1)#end
shu#show spanning-tree mst
##### MST1   vlans mapped:2
Bridge    address 0007.7074.ff01  priority    32768 (32768 sysid 0)
Root      this switch for the CIST
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role   Sts Cost   Prio.Nbr Type
-----
-----
Giga6/1/1     Disb   BLK 20000  128.611 Shared

shu#

```

port 의 path cost 값을 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	interface interface-id	설정할 인터페이스를 명시하여 interface configuration 모드로

		진입한다.
Step3	Spanning-tree instance <i>instance-id path-cost path-cost</i>	port 에 path cost 를 설정한다
Step4	end	privileged EXEC 모드로 변경한다.
Step5	show running-config	설정 내용을 확인한다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

default 값으로 복구하려면 **no spanning-tree instance *instance-id* path-cost** 명령을 사용한다.

```

shu#show spanning-tree mst
##### MST1   vlans mapped:2
Bridge   address 0007.7074.ff01 priority   32768 (32768 sysid 0)
Root     this switch for the CIST
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role   Sts Cost   Prio.Nbr Type
-----
-----
Giga6/1/1      Disb   BLK 20000  128.611 Shared

shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#spanning-tree instance 1 path-cost 1
shu(config-if-Giga6/1/1)#end
shu#show spanning-tree mst
##### MST1   vlans mapped:2
Bridge   address 0007.7074.ff01 priority   32768 (32768 sysid 0)
Root     this switch for the CIST
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role   Sts Cost   Prio.Nbr Type
-----
-----
Giga6/1/1      Disb   BLK 1     128.611 Shared

shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

```

```

shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#no spanning-tree instance 1 path-cost
shu(config-if-Giga6/1/1)#end
shu#show spanning-tree mst
##### MST1   vlans mapped:2
Bridge      address 0007.7074.ff01  priority    32768 (32768 sysid 0)
Root        this switch for the CIST
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface    Role   Sts Cost   Prio.Nbr Type
-----
-----
Giga6/1/1    Disb   BLK 20000  128.611 Shared

shu#
    
```



Note

MSTP 에서 instance 와 port 에 설정을 하기 위해서는 instance 생성이 먼저 이루어 져야 한다.

13.7. Configuring RPVST+ Features

이 절에서는 rapid per vlan spanning-tree plus (RPVST+)를 설정하는 방법에 대해 설명한다. RPVST+ 모드를 설정하면 기존에 있던 vlan 이 trunk vlan 으로 변환된다. 그래서 trunk VLAN 별로 spanning-tree 가 구성 되기 때문에 VLAN 하는 부분과 STP 나 RSTP 와 같이 hello time, port priority 등을 설정하는 부분으로 나뉜다.

13.1.29. VLAN 생성

VLAN 을 생성 위해서는 privileged EXEC 모드에서부터 다음의 과정을 거친다

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	Spanning-tree configuration rpvst+	VLAN 를 생성하기 위해 rpvst+ configuration 모드로 진입한다.
Step3	vlan <i>vlan-id</i>	vlan-id 에 해당하는 vlan 을 생성시킨다
Step4	exit	Global configuration 모드로 진입한다.
Step5	interface <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로

		진입한다.
Step6	Spanning-tree vlan <i>vlan-id</i>	VLAN 에 해당 포트를 넣는다
Step7	end	privileged EXEC 모드로 변경한다.
Step8	show running-config	설정 내용을 확인한다.
Step9	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

생성되어 있는 instance 를 삭제할 경우에는 **no vlan** *vlan-id* 명령을 사용하라.

```
shu#
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#spanning-tree rpvt+ configuration
shu(config-rpvst+)#vlan 2
shu(config-rpvst+)#exit
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#spanning-tree vlan 2
shu(config-if-Giga6/1/1)#end
shu#show spanning-tree rpvt+
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20
% Default: CIST Root Id 800000077074ff01
% Default: CIST Bridge Id 800000077074ff01
% 0: 0 topology change(s) - last topology change Thu Jan 1 00:00:00 1970

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec
%
% Instance      VLAN
% 0:            1, 3, 100
% 1:            2
shu#
```

13.1.30. VLAN and port configuration

RPVST+에서는 각 VLAN 마다 spanning-tree 가 동작하기 때문에 VLAN 별로 priority 를 설정한다. 여기서 사용되는 명령어 들은 STP, RSTP 에서 사용되는 명령어에 vlan 이 붙어서 사용된다.

vlan 에 priority 를 설정하기 위해서는 privileged EXEC 모드에서부터 다음의 과정을 거친다

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	Spanning-tree vlan <i>vlan-id</i> priority <i>priority</i>	VLAN 에 priority 를 설정한다
Step3	end	privileged EXEC 모드로 변경한다.
Step4	show running-config	설정 내용을 확인한다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

default 값으로 복구하려면 **no spanning-tree vlan *vlan-id* priority** 명령을 사용한다.

```

shu#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 0: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 0: MSTI Root Id 100200077074ff01
% 0: MSTI Bridge Id 100200077074ff01
% Giga6/1/1: Port 611 - Id 8263 - Role Disabled - State Discarding
% Giga6/1/1: Designated Internal Path Cost 0 - Designated Port Id 0
% Giga6/1/1: Configured Internal Path Cost 4
% Giga6/1/1: Configured CST External Path cost 4
% Giga6/1/1: CST Priority 128 - MSTI Priority 128
% Giga6/1/1: Designated Root 000000077074ff01
% Giga6/1/1: Designated Bridge 000000077074ff01
% Giga6/1/1: Message Age 0 - Max Age 0
% Giga6/1/1: Hello Time 0 - Forward Delay 0
% Giga6/1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%

shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#spanning-tree vlan 2 priority 4096
shu(config)#end
shu#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 0: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 4096
% 0: MSTI Root Id 100200077074ff01
% 0: MSTI Bridge Id 100200077074ff01
% Giga6/1/1: Port 611 - Id 8263 - Role Disabled - State Discarding
% Giga6/1/1: Designated Internal Path Cost 0 - Designated Port Id 0
% Giga6/1/1: Configured Internal Path Cost 4

```

```

% Giga6/1/1: Configured CST External Path cost 4
% Giga6/1/1: CST Priority 128 - MSTI Priority 128
% Giga6/1/1: Designated Root 000000077074ff01
% Giga6/1/1: Designated Bridge 000000077074ff01
% Giga6/1/1: Message Age 0 - Max Age 0
% Giga6/1/1: Hello Time 0 - Forward Delay 0
% Giga6/1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#no spanning-tree vlan 2 priority
shu(config)#end
shu#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 0: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 0: MSTI Root Id 100200077074ff01
% 0: MSTI Bridge Id 100200077074ff01
% Giga6/1/1: Port 611 - Id 8263 - Role Disabled - State Discarding
% Giga6/1/1: Designated Internal Path Cost 0 - Designated Port Id 0
% Giga6/1/1: Configured Internal Path Cost 4
% Giga6/1/1: Configured CST External Path cost 4
% Giga6/1/1: CST Priority 128 - MSTI Priority 128
% Giga6/1/1: Designated Root 000000077074ff01
% Giga6/1/1: Designated Bridge 000000077074ff01
% Giga6/1/1: Message Age 0 - Max Age 0
% Giga6/1/1: Hello Time 0 - Forward Delay 0
% Giga6/1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
shu#
    
```

port 에 관한 설정도 마찬가지로 **vlan** *vlan-id* 가 추가 된다.

port 의 priority 값을 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	interface <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	Spanning-tree vlan <i>vlan-id</i> priority <i>priority</i>	port 에 priority 를 설정한다

Step4	end	privileged EXEC 모드로 변경한다.
Step5	show running-config	설정 내용을 확인한다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

default 값으로 복구하려면 **no spanning-tree vlan *vlan-id* priority** 명령을 사용한다.

```

shu#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 0: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 4096
% 0: MSTI Root Id 100200077074ff01
% 0: MSTI Bridge Id 100200077074ff01
% Giga6/1/1: Port 611 - Id 8263 - Role Disabled - State Discarding
% Giga6/1/1: Designated Internal Path Cost 0 - Designated Port Id 0
% Giga6/1/1: Configured Internal Path Cost 4
% Giga6/1/1: Configured CST External Path cost 4
% Giga6/1/1: CST Priority 128 - MSTI Priority 128
% Giga6/1/1: Designated Root 000000077074ff01
% Giga6/1/1: Designated Bridge 000000077074ff01
% Giga6/1/1: Message Age 0 - Max Age 0
% Giga6/1/1: Hello Time 0 - Forward Delay 0
% Giga6/1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#spanning-tree vlan 2 priority 0
shu(config-if-Giga6/1/1)#end
shu#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 0: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 4096
% 0: MSTI Root Id 100200077074ff01
% 0: MSTI Bridge Id 100200077074ff01
% Giga6/1/1: Port 611 - Id 8263 - Role Disabled - State Discarding
% Giga6/1/1: Designated Internal Path Cost 0 - Designated Port Id 0
% Giga6/1/1: Configured Internal Path Cost 4
% Giga6/1/1: Configured CST External Path cost 4
% Giga6/1/1: CST Priority 128 - MSTI Priority 0
% Giga6/1/1: Designated Root 000000077074ff01
% Giga6/1/1: Designated Bridge 000000077074ff01
% Giga6/1/1: Message Age 0 - Max Age 0
% Giga6/1/1: Hello Time 0 - Forward Delay 0

```

```

% Giga6/1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%

%

shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#no spanning-tree vlan 2 priority
shu(config-if-Giga6/1/1)#end
shu#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 0: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 4096
% 0: MSTI Root Id 100200077074ff01
% 0: MSTI Bridge Id 100200077074ff01
% Giga6/1/1: Port 611 - Id 8263 - Role Disabled - State Discarding
% Giga6/1/1: Designated Internal Path Cost 0 - Designated Port Id 0
% Giga6/1/1: Configured Internal Path Cost 4
% Giga6/1/1: Configured CST External Path cost 4
% Giga6/1/1: CST Priority 128 - MSTI Priority 128
% Giga6/1/1: Designated Root 000000077074ff01
% Giga6/1/1: Designated Bridge 000000077074ff01
% Giga6/1/1: Message Age 0 - Max Age 0
% Giga6/1/1: Hello Time 0 - Forward Delay 0
% Giga6/1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%

shu#
    
```

port 의 path cost 값을 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	interface <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	Spanning-tree vlan <i>vlan-id</i> path-cost <i>path-cost</i>	port 에 path cost 를 설정한다
Step4	end	privileged EXEC 모드로 변경한다.
Step5	show running-config	설정 내용을 확인한다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

default 값으로 복구하려면 **no spanning-tree vlan *vlan-id* priority** 명령을 사용한다.

```
shu#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 0: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 4096
% 0: MSTI Root Id 100200077074ff01
% 0: MSTI Bridge Id 100200077074ff01
% Giga6/1/1: Port 611 - Id 8263 - Role Disabled - State Discarding
% Giga6/1/1: Designated Internal Path Cost 0 - Designated Port Id 0
% Giga6/1/1: Configured Internal Path Cost 4
% Giga6/1/1: Configured CST External Path cost 4
% Giga6/1/1: CST Priority 128 - MSTI Priority 128
% Giga6/1/1: Designated Root 000000077074ff01
% Giga6/1/1: Designated Bridge 000000077074ff01
% Giga6/1/1: Message Age 0 - Max Age 0
% Giga6/1/1: Hello Time 0 - Forward Delay 0
% Giga6/1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#spanning-tree vlan 2 path-cost 1
shu(config-if-Giga6/1/1)#end
shu#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 0: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 4096
% 0: MSTI Root Id 100200077074ff01
% 0: MSTI Bridge Id 100200077074ff01
% Giga6/1/1: Port 611 - Id 8263 - Role Disabled - State Discarding
% Giga6/1/1: Designated Internal Path Cost 0 - Designated Port Id 0
% Giga6/1/1: Configured Internal Path Cost 1
% Giga6/1/1: Configured CST External Path cost 4
% Giga6/1/1: CST Priority 128 - MSTI Priority 0
% Giga6/1/1: Designated Root 000000077074ff01
% Giga6/1/1: Designated Bridge 000000077074ff01
% Giga6/1/1: Message Age 0 - Max Age 0
% Giga6/1/1: Hello Time 0 - Forward Delay 0
% Giga6/1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
%
shu#configure terminal
```

```

Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#interface GigabitEthernet 6/1/1
shu(config-if-Giga6/1/1)#no spanning-tree vlan 2 path-cost
shu(config-if-Giga6/1/1)#end
shu#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 0: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 4096
% 0: MSTI Root Id 100200077074ff01
% 0: MSTI Bridge Id 100200077074ff01
% Giga6/1/1: Port 611 - Id 8263 - Role Disabled - State Discarding
% Giga6/1/1: Designated Internal Path Cost 0 - Designated Port Id 0
% Giga6/1/1: Configured Internal Path Cost 4
% Giga6/1/1: Configured CST External Path cost 4
% Giga6/1/1: CST Priority 128 - MSTI Priority 128
% Giga6/1/1: Designated Root 000000077074ff01
% Giga6/1/1: Designated Bridge 000000077074ff01
% Giga6/1/1: Message Age 0 - Max Age 0
% Giga6/1/1: Hello Time 0 - Forward Delay 0
% Giga6/1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
shu#

```

**Note**

RPVST+에서 VLAN 와 port 에 설정을 하기 위해서는 VLAN 생성이 먼저 이루어져야 한다.

13.8. Displaying the Spanning-Tree Status

spanning-tree 상태를 조회하려면, 다음 표에 명시된 privileged EXEC 명령 중 하나를 사용하라:

Command	Purpose
<code>show spanning-tree</code>	전체 인터페이스의 spanning-tree 정보를 출력한다.
<code>show spanning-tree interface <i>interface-id</i></code>	특정 인터페이스의 spanning-tree 정보를 출력한다.
<code>show spanning-tree detail</code>	포트 상태를 자세하게 보여준다.

privileged EXEC 명령 `show spanning-tree` 명령의 다른 키워드에 관한 정보는 command reference를 참고하라.

```
shu#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
```

```
Bridge ID Priority 32768
Address 00077074ff01
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Giga6/1/1	Disb	BLK	4	128.611	Shared

```
shu#show spanning-tree interface gi6/1/1
```

```
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20
% Default: Root Id 800000077074ff01
% Default: Bridge Id 800000077074ff01
% Default: last topology change Thu Jan 1 00:00:00 1970
% 0: 0 topology change(s) - last topology change Thu Jan 1 00:00:00 1970

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec
% Giga6/1/1: Port 611 - Id 8263 - Role Disabled - State Discarding
% Giga6/1/1: Designated Path Cost 0
% Giga6/1/1: Configured Path Cost 4 - Add type Explicit ref count 1
% Giga6/1/1: Designated Port Id 0 - Priority 128 -
% Giga6/1/1: Root 000000077074ff01
% Giga6/1/1: Designated Bridge 000000077074ff01
% Giga6/1/1: Message Age 0 - Max Age 0
% Giga6/1/1: Hello Time 0 - Forward Delay 0
% Giga6/1/1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
% Giga6/1/1: forward-transitions 0
% Giga6/1/1: Version Rapid Spanning Tree Protocol - Received None - Send STP
% Giga6/1/1: No portfast configured - Current portfast off
% Giga6/1/1: portfast bpdu-guard default - Current portfast bpdu-guard off
```



```

% Giga6/1/1: portfast bpd-filter default - Current portfast bpd-filter off
% Giga6/1/1: no root guard configured - Current root guard off
% Giga6/1/1: Configured Link Type point-to-point - Current shared
%
%
shu#show spanning-tree detail

Default is executing the rstp-vlan-bridgecompatible Spanning Tree protocol
Bridge Identifier has priority 8000 address 00077074ff01
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag not set, detected flag not set
Number of topology changes 0 last change occurred Thu Jan 1 00:00:00 1970
Times: hold 6, topology change 0, notification 5
      hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 25, notification 0, aging 300
Port 611 (Giga6/1/1) of Default is Discarding
Port path cost 0 Port priority 128, 128.611.
Designated root has priority 1280, address 0007.7074.ff01
Designated bridge has priority 8000, address 0007.7074.ff01
Designated port id is 0, designated path cost 4 Hello is not pending
Number of transitions to forwarding state: 0
Link type is Shared
BPDU: sent 0

shu#

```

13.9. Configuring Bridge MAC Forwarding

Layer 2 이더넷(Ethernet) 네트워크가 정상적으로 동작하려면 프레임에 있는 MAC 주소를 MAC address table 에 있는 주소와 비교해서 해당 interface 로 전송해야 한다. 그러기 위해서는 Bridge 의 MAC address table 이 설정이 되어야 하고 이를 MAC learning 이라 한다. MAC learning 은 장비 에 들어온 프레임을 검사해서 설정하는 동적 방법과 관리자가 직접 입력하는 정적 방법이 있다.

MAC learning 을 하기 위해서 Config 모드에서 다음 명령을 수행한다

Command	Purpose
spanning-tree acquire	Default Bridge 의 MAC learning 을 동적으로 하도록 설정한다. (default 로 enable 되어있다)
no spanning-tree acquire	Default Bridge 의 MAC learning 을 동적으로 하지 않도록

	설정한다.
bridge <1-256> acquire	Default Bridge 가 아닌 Bridge 의 MAC learning 을 동적으로 하도록 설정한다. (default 로 enable 되어있다)
no bridge <1-256> acquire	Default Bridge 가 아닌 Bridge 의 MAC learning 을 동적으로 하지 않도록 설정한다.
mac-address-table static MAC (forward discard) IFNAME	해당 Bridge 에 MAC 주소를 IFNAME interface 로 forwarding 하거나 discard 한다
no mac-address-table static MAC (forward discard) IFNAME	MAC 주소에 해당하는 forwarding entry 를 삭제 한다

Default Bridge 가 아닌 경우에는 **bridge <1-256> mac-address-table static MAC (forward|discard) IFNAME** 명령을 사용한다.

다음은 정적으로 MAC learning 을 하는 예시이다.

```

shu#configure terminal
shu(config)#mac-address-table static 1111.1111.1111 forward gi6/1/1
shu(config)#end
shu#show mac-address-table

vlan  mac address  type  fwd      ports
-----+-----+-----+-----+-----
      1 1111.1111.1111  static  1 Gi6/1/1
shu(config)#no mac-address-table static 1111.1111.1111 forward gi6/1/1
shu(config)#end
shu#show mac-address-table

vlan  mac address  type  fwd      ports
-----+-----+-----+-----+-----
No entries present.
shu#
    
```

E7500 series 는 MAC address table 에서 동적인 entry 와 정적 entry 를 삭제하는 설정을 할 수 있다.

Command	Purpose
clear mac-address-table (dynamic multicast static)	해당 Bridge 에 정적, 동적, multicast MAC 주소 entry 를 삭제한다.
clear mac-address-table (static multicast dynamic) (address MACADDR interface IFNAME vlan VID)	해당 Bridge 에있는 Vlan 이나 물리적 포트의 정적, 동적, multicast MAC 주소 entry 를 삭제한다.

Default Bridge 가 아닌 경우에는 **clear mac-address-table (dynamic|multicast|static) (address MACADDR | interface IFNAME | vlan VID) bridge <1-256>** 명령을 사용한다.

다음은 정적 MAC 주소 entry 를 삭제하는 예시이다.

```

shu#show mac-address-table

vlan  mac address  type  fwd      ports
-----+-----+-----+-----+-----
      1 1111.1111.1111  static  1 Gi6/1/1
shu#clear mac-address-table static
shu#show mac-address-table

vlan  mac address  type  fwd      ports
-----+-----+-----+-----+-----

No entries present.

shu#
    
```

MAC 주소 entry 를 조회 하기 위해 다음과 같은 명령을 Exec 모드에서 수행한다.

Command	Purpose
show mac-address-table	MAC address table 정보를 보여준다.
show mac-address-table (static dynamic multicast) vlan <1-4094>	MAC address table 정보를 정적, 동적, multicast, vlan 에 대해서 보여준다
show mac-address-table count (module <1-6> vlan <1-4094>)	MAC address table 에서 정적 동적 multicast 주소의 개수를 보여준다

14

BFD

(Bidirectional Forwarding Detection)

이 장에서는 BFD(Bidirectional Forwarding Detection)를 설정하는 방법에 대해 설명한다. BFD는 포워딩 경로의 장애를 빨리 감지하기 위한 목적으로 설계된 프로토콜이다. BFD는 사용하는 네트워크 종류와 형태 그리고 라우팅 프로토콜의 영향을 받지 않고 독립적으로 동작한다.

이 장은 다음과 같은 내용으로 구성된다:

- BFD에 대한 이해 (Understanding BFD)
- BFD 제약 사항 (Restrictions BFD Configuration)
- BFD 기본 설정 (Default BFD Configuration)
- BFD 설정 (Configuring BFD)
- BFD 설정 예제 (BFD Configuration Samples)

14.1. Understanding BFD

14.1.1. BFD Operation

BFD는 두 라우터 사이의 포워딩 경로 장애와 인터페이스, 데이터 링크 그리고 포워딩 계층의 장애를 빠르게 감지할 수 있다. E7500 시리즈 스위치는 두 시스템이 임의로 BFD 컨트롤 메시지를 교환하는 BFD 비동기 모드(asynchronous mode)를 지원한다. BFD 세션을 생성하기 위해서는 두 시스템 모두 BFD를 설정해야 한다. 라우팅 프로토콜에 의해 BFD 세션이 생성되면 두 라우터 사이의 협상에 의해 BFD 전송 주기가 결정되고, 두 라우터(BFD peer)는 주기적으로 BFD 컨트롤 메시지를 전송한다.

BFD는 물리 매체의 종류, 인캡슐레이션(encapsulations), 네트워크 형상 그리고 라우팅 프로토콜(BGP, OSPF)의 종류와 무관하게 BFD 시스템 간의 신속한 장애 감지가 가능하다. BFD는 장애를 감지하면 라우팅 프로토콜에게 알려주고, 라우팅 프로토콜은 라우팅 테이블을 재계산을 빨리 수행할 수 있

기 때문에 네트워크 전체의 라우팅 테이블 변경 시간을 단축할 수 있다. 그림 1은 두 개의 라우터로 구성된 간단한 네트워크를 보여주며, 각 라우터에는 OSPF와 BFD가 동작하고 있다. OSPF가 neighbor를 발견했을 때(1), OSPF는 BFD 프로세스에게 BFD 세션을 생성하기 위한 요청을 한다(2). 그러면 OSPF neighbor와 같이 BFD 세션도 생성된다.

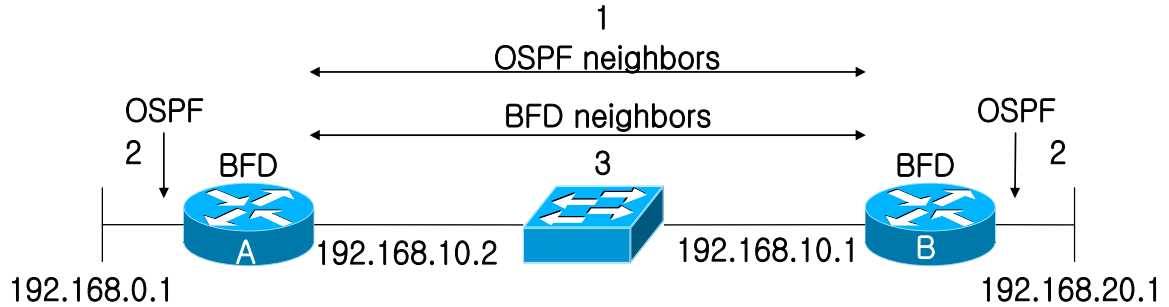


그림 14-1 Establishing a BFD neighbor relationship

그림 2는 네트워크에서 링크 장애가 발생했을 때의 상황을 나타낸다(1). OSPF neighbor와 BFD 세션이 다운 되면(2), BFD는 OSPF 프로세스에게 BFD peer와의 통신이 불가능하다고 통지한다(3). OSPF 프로세스는 OSPF neighbor 관계를 끊는다(4). 만약 다른 경로가 있으면 라우터는 즉시 라우팅 테이블을 재계산 한다.

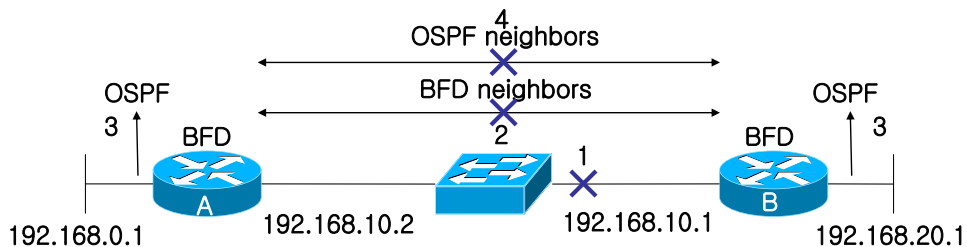


그림 14-2 Tearing down an OSPF neighbor relationship

14.1.2. Benefits of using BFD for Failure Detection

BFD는 OSPF와 같은 라우팅 프로토콜에 장애 감지 메커니즘을 제공할 수 있다. 라우팅 프로토콜에서 BFD를 사용하면 다음과 같은 장점이 있다:

- OSPF에서 타이머 시간을 최대한 줄이면 1~2초 이내의 장애 감지가 가능하지만, BFD는 1초 이내로 장애를 감지할 수 있다.
- BFD는 특정 라우팅 프로토콜을 고려해서 설계된 것이 아니기 때문에 다양한 라우팅 프로토콜의 장애 감지 메커니즘으로 사용할 수 있다.

14.1.3. BFD Session Type

BFD 는 네트워크 구성에 따라 BFD single hop 세션과 BFD multihop 세션을 사용한다.

BFD single hop 세션은 물리적으로 직접 연결된 두 장비 사이의 BFD 연결에 사용된다. 다음의 그림은 BFD single hop 이 사용되는 구성을 나타낸다. 그림처럼 두 장비는 특정 인터페이스를 통해 직접 연결되므로 BFD single hop 세션은 이 인터페이스를 통해서만 생성된다. E7500 시리즈 스위치에서는 **bfd interval** 명령으로 인터페이스에 BFD 세션 파라미터를 설정해야만 BFD single hop 세션이 생성된다.

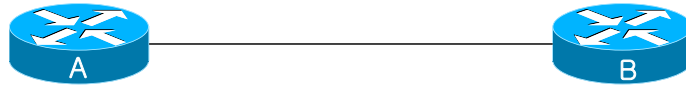


그림 14-3 BFD single hop session

BFD multihop 세션은 두 시스템 사이의 연결 경로가 임의적일 때 사용된다. 다음의 그림처럼 두 장비 사이의 통신의 라우팅 테이블에 따라 달라진다. 그러므로 BFD multihop 세션은 특정 인터페이스에 종속되지 않는다. BFD multihop 세션은 인터페이스의 BFD 세션 파라미터 설정과 상관없이 생성할 수 있다. BFD multihop 세션의 파라미터는 **bfd multihop-peer** 명령으로 설정할 수 있다.

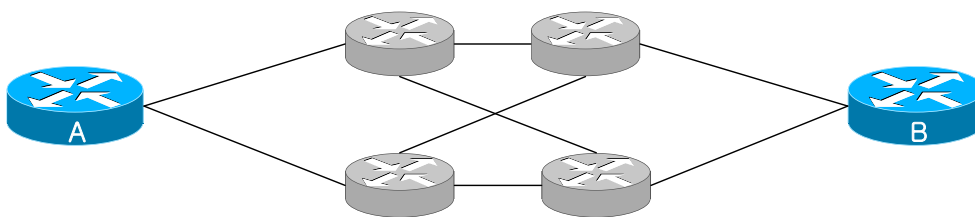


그림 14-4 BFD multihop session

14.1.4. BFD Version Interoperability

E7500 시리즈 스위치는 BFD 버전 1 뿐만 아니라 버전 0 도 지원한다. 모든 BFD 세션은 버전 1 으로 생성되지만 버전 0 와 상호 연동이 가능하다. 시스템은 자동으로 BFD 버전을 감지해서 연동하는 장비와 공통으로 사용할 수 있는 가장 높은 버전으로 BFD 세션이 동작한다. 예를 들어, 한 시스템이 버전 0 를

사용하고 있고 나머지 시스템들은 버전 1 을 사용하고 있다면, 모든 시스템들이 버전 0 를 사용하게 된다. **show bfd neighbor [details]** 명령으로 BFD 세션이 사용하고 있는 버전을 확인할 수 있다.

14.2. BFD Restrictions

E7500 시리즈 스위치의 BFD는 다음과 같은 제약사항이 있다:

- ✓ 현재 BFD 구현에서는 비동기 모드만 지원한다. 비동기 모드에서는 어떤 BFD peer 라도 BFD 세션을 시작 할 수 있다.
- ✓ 현재 BFD 는 BGP 와 OSPF 그리고 정적 라우팅(static routing)을 지원한다.
- ✓ 최대 128 개의 BFD 세션을 생성할 수 있다. 128 개 이상의 세션을 생성하려 하면 다음과 같은 메시지가 출력된다.

%BFD-5-SESSIONLIMIT: Attempt to exceed session limit of 128 neighbors.

- ✓ 모든 BFD 기능은 제어 계층(control plane)에서 제공된다. 따라서 CPU 사용률이 높아지면 패킷 손실에 의한 장애 인식 가능성이 높아진다. 이런 경우에는 Required minimum receive interval 을 적절한 값으로 조절해야 한다.

14.3. Default BFD Configuration

다음의 표는 기본 BFD 설정을 보여준다.

Feature	Default Setting
BFD	모든 인터페이스에 대해 비활성 상태이다.
Interface passive mode	모든 인터페이스들은 Active mode 이다.
BFD Echo packet reception	비활성 상태이다
BFD Echo mode	사용하지 않는다
Desired transmit interval	750 밀리 초 (Multihop 세션)
Required minimum receive interval	500 밀리 초 (Multihop 세션)
Multiplier	3 (Multihop 세션)
BFD Slow-timer	1000 밀리 초.

Desired transmit interval, Required minimum receive interval 그리고 Multiplier 는 중요한 BFD 세션 파라미터들이다. BFD single hop 세션을 생성하려면 **bfd interval** 명령으로 이 파라미터 값을 직접 설정해야 한다. BFD multihop 세션에 대한 **bfd multihop-peer** 설정이 없으면 표에 명시된 값이 사용된다.

14.4. Configuring BFD

이 절에서는 다음과 같은 BFD 설정 방법에 대해 설명한다:

- Configuring BFD session parameters on the interface
- Configuring BFD multi-hop session parameters
- Configuring BFD support for BGP
- Configuring BFD support for OSPF
- Configuring BFD support for static routing
- Configuring Passive Mode on the Interface
- Configuring BFD slow timer
- Configuring BFD echo mode
- Monitoring and Troubleshooting BFD

14.4.1. Configuring BFD session parameters on the interface

다음의 과정은 인터페이스에 BFD 세션 파라미터를 설정하는 방법이다.

	Command or Action	Purpose
Step 1	configure terminal 예제: Switch# configure terminal	Global configure 모드로 진입한다
Step 2	interface interface-name 예제: Switch(config)# interface gi2/2/1	Interface configuration 모드로 진입한다.
Step 3	ip address ip-address/prefix-length 예제: Switch(config-if-Giga2/2/1)# ip address 33.1.1.1/24	인터페이스에 IP 주소를 설정한다.
Step 4	bfd interval minlliseconds min_rx milliseconds multiplier interval-multiplier 예제: Switch(config-if-Giga2/2/1)# bfd interval 750 min_rx 500 multiplier 3	인터페이스에 BFD 파라미터를 설정한다.
Step 5	end 예제: Switch(config-if-Giga2/2/1)# end	privileged EXEC 모드로 돌아간다



Note single-hop BFD 세션을 생성하기 위해서는 반드시 **bfd interval** 명령으로 관련된 인터페이스에 BFD 파라미터를 설정해야 한다.

14.4.2. Configuring multi-hop BFD session parameters

BFD multihop 세션의 BFD 세션 파라미터는 BFD peer 별로 설정해야 한다. 다음은 BFD multihop 세션의 파라미터를 설정하는 방법이다.

	Command or Action	Purpose
Step 1	configure terminal 예제: Switch# configure terminal	Global configure 모드로 진입한다
Step 2	bfd multihop-peer A.B.C.D interval minliseconds min_rx milliseconds multiplier interval-multiplier 예제: Switch(config)# bfd multihop-peer 10.1.1.1 interval 750 min_rx 500 multiplier 3	Multi-hop BFD 세션의 BFD 파라미터를 설정한다.
Step 3	End 예제: Switch(config)# end	privileged EXEC 모드로 돌아간다

14.4.3. Configuring BFD support for BGP

BGP 에서 BFD 를 설정하는 방법은 다음과 같다.

	Command or Action	Purpose
Step 1	configure terminal 예제: Switch# configure terminal	Global configure 모드로 진입한다
Step 2	router bgp as-tag 예제: Switch(config)# router bgp 100	BGP 라우팅 설정 모드로 진입한다.
Step 3	neighbor ip-address fall-over bfd 예제: Switch(config-router)# neighbor 3.3.3.2 fall-over bfd	BGP neighbor 와의 연결상태 검사에 BFD 를 사용하도록 설정한다.

Step 4	end 예제: Switch(config-router)# end	Privileged EXEC 모드로 돌아간다.
--------	--	---------------------------

14.4.4. Configuring BFD support for OSPF

다음의 두 가지 방법으로 OSPF 에서 BFD 를 사용하도록 설정할 수 있다.

- OSPF 라우팅 설정 모드에서 **bfd all-interface** 명령으로 OSPF virtual link 를 제외한 모든 OSPF 인터페이스에 대해 BFD 세션을 생성할 수 있다.
- 인터페이스 모드에서 **ip ospf bfd** 명령으로 OSPF 의 특정 인터페이스에 대해 BFD 세션을 생성할 수 있다.

Configuring BFD support for OSPF for all interface

모든 OSPF 인터페이스에 대해 BFD 세션을 생성할 수 있도록 설정하려면 다음의 작업을 수행하면 된다.

	Command or Action	Purpose
Step 1	configure terminal 예제: Switch# configure terminal	Global configure 모드로 진입한다
Step 2	router ospf process-id 예제: Switch(config)# router ospf 10	OSPF 라우팅 설정 모드로 진입한다.
Step 3	bfd all-interfaces 예제: Switch(config-router)# bfd all-interface	모든 OSPF 인터페이스에 대해 BFD 세션을 생성할 수 있도록 설정한다.
Step 4	exit 예제: Switch(config-router)# exit	global configuration 모드로 되돌아 간다.
Step 5	interface type number 예제: Switch(config)# interface gi2/1/1	Interface configuration 모드로 진입한다.
Step 6	bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier	OSPF 인터페이스에 BFD 세션 파라미터 값을 설정한다.

	<p>예제: Switch(config-if-Giga2/2/1)# bfd interval 750 min_rx 500 min 3</p>	BFD 세션을 사용할 모든 OSPF 인터페이스에 대해 bfd interval 설정을 해야 한다.
Step 7	<p>interface <i>type number</i></p> <p>예제: Switch(config)# interface gi2/2/1</p>	(Option) Interface configuration 모드로 진입한다.
Step 8	<p>ip ospf bfd [disable]</p> <p>예제: Switch(config-if-Giga2/2/1)# ip ospf bfd disable</p>	(Option) 특정 OSPF 인터페이스에 대해서는 BFD 세션이 생성되지 않도록 설정한다. Note disable keyword 는 bfd all-interface 명령이 수행 되어 BFD 가 enable 된 인터페이스에서만 사용해야 한다.
Step 9	<p>end</p> <p>예제: Switch(config-if-Giga2/2/1)# end</p>	Privileged EXEC 모드로 되돌아 간다.

Configure BFD Support for OSPF for One or More Interface

다음은 특정 OSPF 인터페이스에 대해 BFD 세션이 생성되도록 설정하는 방법이다.

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>예제: Switch# configure terminal</p>	Global configure 모드로 진입한다
Step 2	<p>interface <i>type number</i></p> <p>예제: Switch(config)# interface gi2/1/1</p>	Interface configuration 모드로 진입한다.
Step 3	<p>bfd interval <i>minlliseconds</i> min_rx <i>milliseconds</i> multiplier <i>interval-multiplier</i></p> <p>예제: Switch(config-if-Giga2/2/1)# bfd interval 750 min_rx 500 multiplier 3</p>	인터페이스에 BFD 파라미터를 설정한다.
Step 4	<p>ip ospf bfd [disable]</p> <p>예제: Switch(config-if-Giga2/1/1)# ip ospf bfd</p>	이 OSPF 인터페이스를 통해 BFD 세션이 생성될 수 있도록 설정한다.
Step 5	<p>end</p> <p>예제:</p>	Privileged EXEC 모드로 되돌아 간다.

```
Switch(config-if-Giga2/1/1)# end
```

14.4.5. Configuring BFD support for Static routing

정적 라우팅(static routing)에서는 정적 라우트의 게이트웨이를 BFD peer 로 설정한다. 다음은 정적 라우팅에서 BFD 를 설정하는 방법이다.

	Command or Action	Purpose
Step 1	configure terminal 예제: Switch# configure terminal	Global configure 모드로 진입한다
Step 2	interface interface-name 예제: Switch(config)# interface gi2/2/1	Interface configuration 모드로 진입한다.
Step 3	ip address ip-address/prefix-length 예제: Switch(config-if-Giga2/2/1)# ip address 1.1.1.1/24	인터페이스에 IP 주소를 설정한다.
Step 4	bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier 예제: Switch(config-if-Giga2/2/1)# bfd interval 750 min_rx 500 min 3	인터페이스에 BFD 세션 파라미터 값을 설정한다.
Step 5	Exit 예제: Switch(config-if-Giga2/2/1)# exit	Global configuration 모드로 돌아간다
Step 6	ip route A.B.C.D/M gateway-addr 예제: Switch(config)# ip route 7.0.0.0/8 1.1.1.254	정적 라우트를 설정한다.
Step 7	ip route static bfd IFNAME gateway-addr 예제: Switch(config)# ip route static bfd gi2/2/1 1.1.1.254	정적 라우트의 BFD neighbor 를 지정한다. 정적라우트의 게이트웨이가 연결된 인터페이스와 게이트웨이의 IP 주소를 명시한다.
Step 8	end 예제: Switch(config)# end	Privileged EXEC 모드로 되돌아 간다.

14.4.6. Configuring Passive Mode on the Interface

BFD 수동 모드(passive mode)는 다른 BFD neighbor로부터 BFD 컨트롤 패킷을 수신한 후부터 BFD 컨트롤 패킷을 전송하기 시작한다. 즉, 먼저 BFD 컨트롤 패킷을 전송하지 않는다. BFD를 수동 모드로 동작시키려면 다음의 순서대로 인터페이스를 설정하면 된다.

네트워크의 모든 라우터를 BFD 수동 모드로 설정하면 BFD가 동작하지 않는다. 적어도 하나의 시스템의 BFD는 능동 모드(active mode)로 동작해야 한다.

	Command or Action	Purpose
Step 1	configure terminal 예제: Switch# configure terminal	Global configure 모드로 진입한다
Step 2	interface interface-name 예제: Switch(config)# interface gi2/2/1	Interface configuration 모드로 진입한다.
Step 3	bfd passive 예제: Switch(config-if-Giga2/2/1)# bfd passive	인터페이스를 BFD 수동 모드로 설정한다.
Step 4	end 예제: Switch(config-if-Giga2/2/1)# end	privileged EXEC 모드로 돌아간다

14.4.7. Configuring BFD Echo Mode

BFD echo 모드에서 BFD echo 패킷을 수신한 시스템은 이 패킷을 전송한 시스템으로 되돌려 보낸다. BFD Echo 패킷을 사용할 경우 BFD 컨트롤 패킷의 전송 주기가 길어진다. 따라서 BFD neighbor들 사이에서 송수신되는 BFD 컨트롤 패킷의 수를 감소시킬 수 있다. BFD echo 모드는 비활성화 되어 있다.

	Command or Action	Purpose
Step 1	configure terminal 예제: Switch# configure terminal	Global configure 모드로 진입한다
Step 2	bfd echo [accept send]	BFD echo 모드를 enable 한다.

	<p>예제: Switch(config)# bfd echo</p>	<p>- accept 키워드는 Echo packet 을 receive 할 때 사용 - send 키워드는 Echo packet 을 send 할 때 사용</p>
Step 3	<p>end</p> <p>예제: Switch(config)# end</p>	<p>Priviledged EXEC 모드로 되돌아 간다.</p>

14.4.8. Configuring BFD slow timer

BFD neighbor 가 서로 상대방을 인식하지 못한 상태 (BFD 상태가 Up 이 아닌 상태)에서는 BFD 쿼트를 패킷을 **bfd interval** 로 설정한 주기로 전송하는 것이 무의미하다. BFD 세션의 상태가 Up 이 아닐 때 BFD 쿼트를 패킷의 전송주기를 설정하려면 **bfd slow-timer** 명령을 사용하면 된다.

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>예제: Switch# configure terminal</p>	<p>Global configure 모드로 진입한다</p>
Step 2	<p>bfd slow-timer milliseconds</p> <p>예제: Switch(config)# bfd slow-timer 2000</p>	<p>BFD slow timer 를 설정한다.</p>
Step 3	<p>end</p> <p>예제: Switch(config)# end</p>	<p>Privileged EXEC 모드로 돌아간다.</p>

14.4.9. Displaying BFD information

	Command or Action	Purpose
Step 1	<p>show bfd neighbor [detail]</p> <p>예제: Switch# show bfd neighbor details</p>	<p>(option) BFD adjacency database 를 보여준다. - detail 키워드는 모든 BFD 프로토콜 파라미터와 타이머를 보여준다.</p>
Step 2	<p>debug bfd [echo event fsm loopback neighbor nsm packet]</p> <p>예제:</p>	<p>(Option) BFD 와 관련된 debugging 정보를 보여준다.</p>

```
Switch# debug bfd packet
```

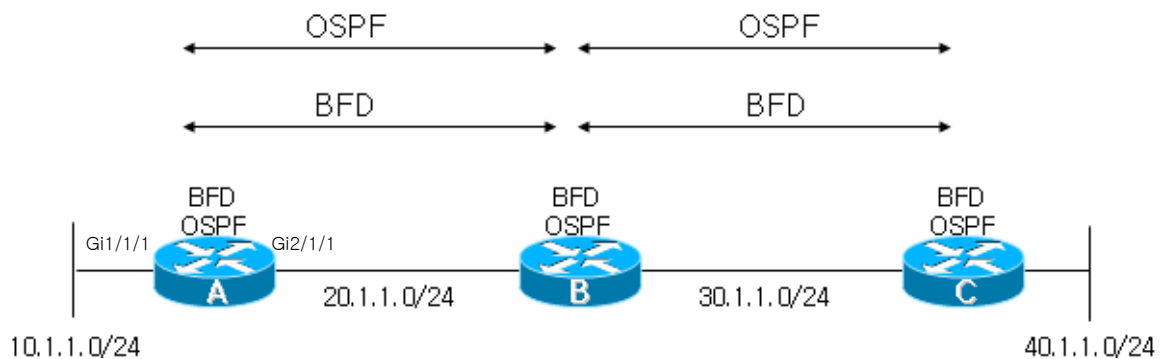
14.5. BFD Configuration Samples

이 절은 다음과 같은 예제들을 포함한다:

- Sample One: Configuring BFD in an OSPF Network
- Sample Two: Configuring BFD in an BGP Network
- Sample Three: Configuring BFD for static routing

14.5.1. Sample One: Configuring BFD in an OSPF Network

이 예제는 OSPF 네트워크에서 BFD 를 사용하는 방법을 설명한다. 다음과 같은 네트워크 구성을 가정 하자:



OSPF 는 OSPF 인터페이스에 대해 BFD 를 설정해야 한다. OSPF 인터페이스에 BFD 를 설정하는 방법은 다음과 같다:

- ✓ OSPF 의 모든 인터페이스에서 BFD 를 사용하도록 설정
- ✓ 특정 OSPF 인터페이스에서 선택적으로 BFD 를 사용하도록 설정

1. Configuring BFD Support for OSPF for All Interfaces

OSPF 의 모든 인터페이스에서 BFD 를 사용하려면 다음과 같이 설정한다.

Step 1 OSPF 를 설정한다.

```
Switch_A# configure terminal
Switch_A(config)# router ospf 100
Switch_A(config-router)# network 10.1.1.0/24 area0
Switch_A(config-router)# network 20.1.1.0/24 area0
```

Step 2 BFD 세션 파라미터를 설정한다.

```
Switch_A# configure terminal
Switch_A(config)# interface gi2/1/1
Switch_A(config-if-Giga2/1/1)# bfd interval 300 min_rx 300 multiplier 3
```

Step 3 OSPF 의 모든 인터페이스가 BFD 를 사용하도록 설정한다.

```
Switch_A# configure terminal
Switch_A(config)# router ospf
Switch_A(config-router)# bfd all-interfaces
```

Step 4 OSPF neighbor 가 연결되지 않는 인터페이스로는 BFD 세션이 생성되지 않도록 설정한다.

```
Switch_A# configure terminal
Switch_A(config)# interface gi1/1/1
Switch_A(config-if-Giga1/1/1)# ip ospf bfd disable
```

Step 5 BFD peer 의 상태를 확인한다.

```
Switch_A# show bfd neighbors
```

**Note**

bfd all-interfaces 가 설정된 상태에서 OSPF 의 특정 인터페이스에서만 BFD 를 사용하지 않으려면, interface command 명령 **ip ospf bfd disable** 을 사용한다.

스위치의 설정을 조회하면 다음과 같다.

```
!
interface Giga1/1/1
 ip address 10.1.1.1/24
 ip ospf bfd diable
!
interface Giga2/1/1
 ip address 20.1.1.1/24
 bfd interval 300 min_rx 300 multiplier 3
!
router ospf 100
 network 10.1.1.0/24 area0
 network 20.1.1.0/24 area0
 bfd all-interfaces
!
```

2. Configuring BFD Support for OSPF for One or More Interfaces

특정 OSPF 인터페이스에서 BFD 를 사용하려면 다음과 같이 설정한다.

Step 1 OSPF 를 설정한다.

```
Switch_A# configure terminal
Switch_A(config)# router ospf 100
Switch_A(config-router)# network 10.1.1.0/24 area0
Switch_A(config-router)# network 20.1.1.0/24 area0
```

Step 2 Single hop BGP session 을 enable 하고, bfd session parameter 를 설정한다.

```
Switch_A# configure terminal
Switch_A(config)# interface gi2/1/1
Switch_A(config-if-Giga2/1/1)# bfd interval 300 min_rx 300 multiplier 3
```

Step 3 특정 OSPF 인터페이스에 대해 BFD 를 사용하도록 설정한다.

```
Switch_A# configure terminal
Switch_A(config)# interface gi2/1/1
Switch_A(config-if-Giga2/1/1)# ip ospf bfd
```

Step 4 BFD peer 의 상태를 확인한다.

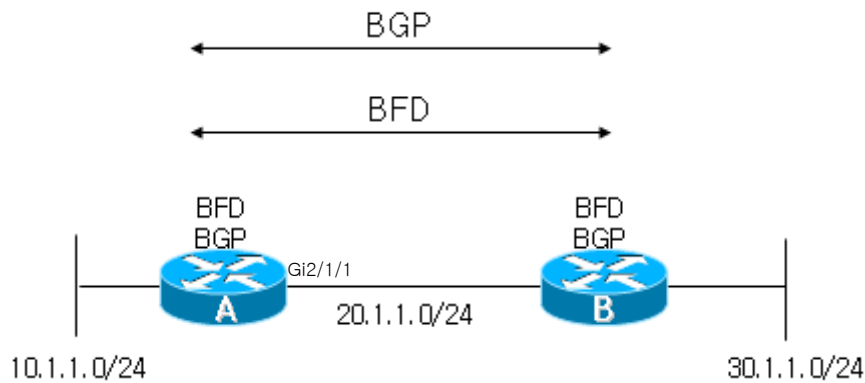
```
Switch_A# show bfd neighbors
```

스위치의 설정을 조회하면 다음과 같다.

```
!
interface Giga2/1/1
ip address 20.1.1.1/24
ip ospf bfd
bfd interval 300 min_rx 300 multiplier 3
!
router ospf 100
network 10.1.1.0/24 area0
network 20.1.1.0/24 area0
!
```

14.5.2. Sample Two: Configuring BFD in an BGP Network

이 예제는 BGP 네트워크에서 BFD 를 사용하는 방법을 설명한다. 다음과 같은 네트워크 구성을 가정하자:



BGP 는 각 BGP neighbor 별로 BFD 를 사용하도록 설정해야 한다. BGP neighbor 에 BGP 를 설정하고 BFD 세션 parameter 를 설정 하는 방법은 다음의 두 경우에 따라 달라진다:

- ✓ External BGP 이고 물리적으로 직접 연결된 경우
- ✓ Multihop-External BGP 인 경우와 Internal BGP 인 경우

1. Configuring BFD Support for connected external BGP

BGP 에서 특정 BGP peer 에 대해 BFD 를 사용하려면 다음과 같이 설정한다.

Step 1 BGP 를 설정한다.

```
Switch_A# configure terminal
Switch_A(config)# router bgp 80
Switch_A(config-router)# neighbor 20.1.1.81 remote-as 81
```

Step 2 BGP 가 특정 neighbor 와의 세션에 BFD 를 사용하도록 설정한다.

```
Switch_A# configure terminal
Switch_A(config)# router bgp 80
Switch_A(config-router)# neighbor 20.1.1.81 fall-over bfd
```

Step 3 Single hop BGP 세션을 enable 하고, bfd 세션 parameter 를 설정한다.

```
Switch_A# configure terminal
Switch_A(config)# interface gi2/1/1
Switch_A(config-if-Giga2/1/1)# bfd interval 300 min_rx 300 multiplier 3
```

Step 4 BFD peer 의 상태를 확인한다.

```
Switch_A# show bfd neighbors
```

스위치의 설정을 조회하면 다음과 같다.

```
!  
interface Giga2/1/1  
 ip address 20.1.1.1/24  
 bfd interval 300 min_rx 300 multiplier 3  
!  
router bgp 80  
 neighbor 20.1.1.81 remote-as 81  
 neighbor 20.1.1.81 fall-over bfd  
!
```

2. Configuring BFD Support for Internal BGP

Internal BGP 에서 BFD 를 사용하려면 다음과 같이 설정한다.

Step 1 Internal BGP 를 설정한다.

```
Switch_A# configure terminal  
Switch_A(config)# router bgp 80  
Switch_A(config-router)# neighbor 20.1.1.81 remote-as 80
```

Step 2 BGP 가 특정 neighbor 와의 세션에 BFD 를 사용하도록 설정한다.

```
Switch_A# configure terminal  
Switch_A(config)# router bgp 80  
Switch_A(config-router)# neighbor 20.1.1.81 fall-over bfd
```

Step 3 Multihop bfd 세션 parameter 를 설정한다.

(Option)

```
Switch_A# configure terminal  
Switch_A(config)# bfd multihop-peer 20.1.1.81 interval 900 min_rx 500 multiplier 3
```

Step 4 BFD peer 의 상태를 확인한다.

```
Switch_A# show bfd neighbors
```

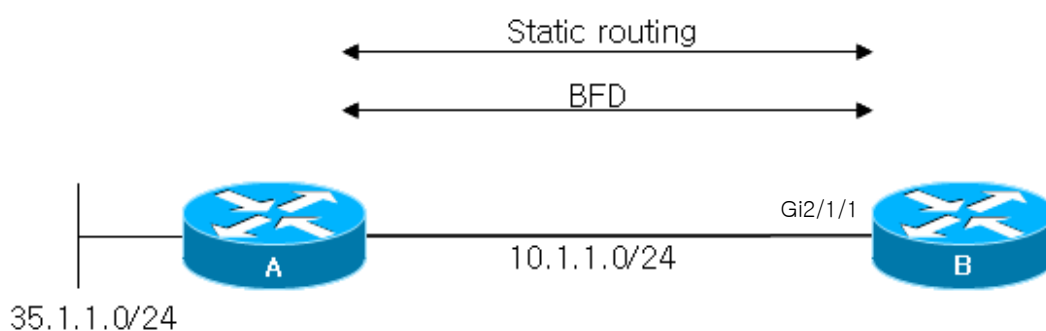
스위치의 설정을 조회하면 다음과 같다.

```
!  
interface Giga2/1/1  
 ip address 20.1.1.1/24  
!  
bfd multihop-peer 20.1.1.81 interval 900 min_rx 500 multiplier 3  
!  
router bgp 80  
 neighbor 20.1.1.81 remote-as 80
```

```
neighbor 20.1.1.81 fall-over bfd
!
```

14.5.3. Sample Three: Configuring BFD for static routing

이 예제는 정적 라우팅을 사용하는 네트워크에서 BFD를 사용하는 방법을 설명한다. 다음과 같은 네트워크 구성을 가정하자:



특정 static route 로의 next-hop 이 실제로 active 한 상태인지를 확인하기 위하여 BFD 를 사용하려면 다음과 같이 설정한다.

Step 1 **Static route** 를 설정한다.

```
Switch_B# configure terminal
Switch_B(config)# ip route 35.1.1.0/24 10.1.1.254
```

Step 2 **Single hop BGP session** 을 enable 하고, **bfd session parameter** 를 설정한다.

```
Switch_B# configure terminal
Switch_B(config)# interface gi2/1/1
Switch_B(config-if-Giga2/1/1)# bfd interval 300 min_rx 300 multiplier 3
```

Step 3 **Static route** 의 next-hop 과의 failure detection 위해 BFD 를 사용 하도록 설정한다.

```
Switch_B# configure terminal
Switch_B(config)# ip route static bfd gi2/1/1 10.1.1.254
```

Step 4 **BFD peer** 의 상태를 확인한다.

```
Switch_B# show bfd neighbors
```

**Note**

BFD 세션이 UP 상태가 되기 위해서는 Switch A 에도 Switch B 와 연결된 인터페이스에 BFD 가 설정되어야 한다.

Switch_B 의 설정을 조회하면 다음과 같다.

```
!  
interface Giga2/1/1  
 ip address 10.1.1.1/24  
 bfd interval 300 min_rx 300 multiplier 3  
!  
ip route 35.1.1.0/24 10.1.1.254  
ip route static bfd gi2/1/1 10.1.1.254  
!
```

15

Link Aggregation Control Protocol

이 장에서는 port-group을 구성하기 위해 스위치에 IEEE 802.3ad Link Aggregation Control Protocol(LACP)를 설정하는 방법을 설명한다.

**Note**

이 장에서 사용되는 명령어에 대한 문법과 사용방법에 관한 정보는 **command reference** 를 참조하라.

이 장은 다음의 절로 구성된다:

- Understanding the Link Aggregation Control Protocol
- Configuring 802.3ad Link Aggregation Control Protocol and static link aggregation
- Displaying 802.3ad Statistics and Status

15.1. Understanding Link Aggregation Control Protocol

Link Aggregation Control Protocol (LACP) is part of an IEEE specification (802.3ad) that allows you to bundle several physical ports together to form a single logical channel. LACP allows a switch to negotiate an automatic bundle by sending LACP packets to the peer. Link Aggregation Control Protocol (LACP)는 IEEE 802.3ad 에 기술 되어 있는 프로토콜로 여러 개의 물리적 interface 를 하나의 logical interface 로 묶어서 사용할 수 있게 해준다. 상대편 장비와 연결된 interface 에서 서로 LACP 패킷 (LACPDU)을 주고 받으며 해당 interface 가 logical interface 에 포함되는 여부를 판단한다.

이 절에서는 다음 항목을 설명한다:

- LACP 동작 원리
- LACP Modes
- LACP Parameters

15.1.1. LACP 동작 원리

LACP 는 연결된 두 장비 모두 설정이 되어 있어서 LACPDU 를 주고 받으며 interface 의 상태를 정하고 Link Aggregation 을 결정한다. LACP 가 설정된 interface 는 LACPDU 를 통해 여러 상태를 지나게 되고 두 장비가 서로 조건이 맞을 경우 Link Aggregation 이 일어난다. LACP 가 설정이 되면 logical interface 가 생성 된다. LACPDU 를 받은 interface 는 연결된 장비가 LACP 가 설정 되어 있다는 것을 파악한 후 자신의 LACPDU 전송 주기를 확인하고 그에 맞게 LACPDU 를 전송한다. 그리고 LACPDU 를 통해 받은 정보와 interface 가 가지고 있는 정보가 일치하는 지를 확인하고 일치 할 경우 logical interface 에 해당 물리적 interface 를 연결한다.

15.1.2. LACPDU 구성

LACPDU 는 전송하는 interface 의 정보와 상대방의 정보를 가진다. 이 정보들을 이용해서 각 interface 에서 정보를 저장하고 이 값을 다음에 도착하는 LACPDU 와 비교한다. 다음 표는 LACPDU 에 포함되는 정보들을 나타낸다.

field	description
Actor_System_Priority	장비에 설정된 priority
Actor_System	장비의 MAC 값과 priority 로 만든 ID
Actor_Key	logical interface 의 ID
Actor_Port_Priority	Port 의 priority
Actor_Port	Port 의 index
Actor_State	Port 의 상태를 bit 으로 나타낸 값
Partner_System_Priority	상대편 장비의 system priority
Partner_System	상대편 장비의 system ID
Partner_Key	상대편 장비의 logical interface 의 ID
Partner_Port_Priority	상대편 Port 의 priority
Partner_Port	상대편 Port 의 index
Partner_State	상대편 Port 의 상태

표 15-1 LACPDU 에 포함되는 정보

15.1.3. LACP Modes

E7500 series 는 port group 을 수동으로 구성할 수 있고, IEEE 802.3ad LACP(Link Aggregation Control Protocol)를 사용하여 자동으로 구성할 수도 있다.

LACP 로 port group 을 구성하려면, active 나 passive 모드를 사용하면 된다. 적어도 링크의 한쪽은 active 모드로 설정되어 있어야 한다. Passive 모드의 포트는 LACP 패킷을 먼저 전송하지 않고 LACP 패킷을 수신했을 경우에 LACP 패킷을 전송하기 시작한다.

LACP 에서 가능한 모드

Mode	Description
on	LACP 에 의해 포트 그룹이 생성되지 않고 static 한 포트 그룹이 생성된다.
passive	포트를 passive 협상 모드로 설정한다. Passive 모드의 포트는 먼저 LACP 패킷을 전송하여 협상을 시작하지 않고, LACP 패킷을 수신했을 때 응답만 한다.
active	포트를 active 협상 모드로 설정한다. Active 모드의 포트는 LACP 패킷을 전송함으로써 협상을 시작한다.

15.1.4. LACP Parameters

LACP 의 설정에 사용되는 인자들은 다음과 같다:

- System Priority
LACP 가 동작하는 각 스위치에는 자동으로 혹은 CLI 를 통해서 system priority 를 할당해야 한다. System priority 는 스위치의 MAC 주소와 같이 사용되어 system ID 를 구성하고, 다른 시스템과의 협상에 사용된다.
- Port Priority
스위치의 각 포트에는 자동으로 혹은 CLI 를 통해서 port priority 를 할당해야 한다. Port priority 는 포트 번호와 함께 port identifier 를 구성한다. Port priority 는 하드웨어의 제약 때문에 적합한 모든 포트가 통합될 수 없을 때, standby 모드로 만들 포트를 결정하기 위해 사용된다.
- Administrative key
 - 스위치의 각 포트는 그 포트의 성질에 따라 자동으로 administrative key 값을 할당 받는다. Administrative key를 결정하는 성질은 bandwidth, vlan id, duplex, mtu 등이 있고 이 값이 같은 경우에만 같은 logical interface에 속할 수 있다.

LACP 가 활성화되면, LACP 는 항상 통합 가능한 최대 개수의 포트를 통합하려 시도한다. 만약 통합 가능한 모든 포트들을 통합할 수 없다면, 통합되지 않은 모든 포트들은 hot standby 상태에 놓이게 되며 통합된 다른 포트에 고장이 발생했을 경우에만 사용된다.

15.2. Configuring 802.3ad Link Aggregation Control Protocol and Static Link Aggregation

이 절에서는 LACP 로 port group 을 구성하는 방법을 설명한다:

- Specifying the System Priority
- Specifying the Port Priority
- Specifying an Administrative Key Value
- Specifying the Timeout Value
- Configuration LACP and static port group
- Clearing LACP Statistics

15.2.1. Specifying the System Priority

System priority 의 값은 1 과 65535 사이의 정수 값이어야 한다. 숫자가 클수록 낮은 우선순위를 나타낸다. default priority 는 32768 이다.

LACP System priority 를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	lACP system-priority <i>priority</i>	system priority 를 설정한다.
Step3	end	privileged EXEC 모드로 변경한다.
Step4	show lACP sys-id	설정 내용을 확인한다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

설정한 system priority 를 default 설정으로 복구하려면 global configuration 명령 **no lACP system-priority** 를 사용하라

다음은 system priority 를 20000 으로 설정하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# lACP system-priority 20000
Switch(config)# end
```

15.2.2. Specifying the Port Priority

Port priority 의 값은 1 과 65535 사이의 정수 값이어야 한다. 숫자가 클수록 낮은 우선순위를 나타낸다. default priority 는 32768 이다.

Port priority 를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	interface <i>interface-id</i>	LACP 를 port priority 를 설정하려는 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	lcp port-priority <i>priority</i>	port priority 를 설정한다.
Step4	end	privileged EXEC 모드로 변경한다.
Step5	show running-config	설정 내용을 확인한다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

설정한 port priority 를 default 설정으로 복구하려면 interface configuration 명령 **no lcp port-priority** 를 사용하라

다음은 인터페이스 gi1 의 port-priority 를 10 으로 설정하는 예이다:

```
Switch# configure terminal
Switch(config)# interface Giga6/1/1
Switch(config-if-Giga6/1/1)# lcp port-priority 10
Switch(config)# end
```

15.2.3. Specifying the Timeout Value

포트별로 LACPDU 의 전송 주기를 설정할 수 있다. 전송주기는 short (1 초)나 long (30 초)으로 설정할 수 있다.



Note **lcp timeout** 명령은 설정하는 스위치가 아닌 상대 스위치의 LACPDU 전송 주기에 영향을 미친다.

LACPDU 의 전송 주기를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	interface <i>interface-id</i>	LACPDU 전송주기를 설정하려는 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	lcp timeout {short long}	LACPDU 전송주기를 설정한다.

Step4	end	privileged EXEC 모드로 변경한다.
Step5	show running-config	설정 내용을 확인한다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

설정된 LACPDU 전송주기를 default 로 복구하려면, interface configuration 명령 **no lacp timeout** 을 사용하라.

다음은 인터페이스 gi1 과 연결된 상태 시스템의 LACPDU 전송주기를 short 로 설정하는 예이다:

```
Switch# configure terminal
Switch(config)# interface Giga6/1/1
Switch(config-if- Giga6/1/1)# lacp timeout short
Switch(config)# end
```

15.2.4. Configuration LACP and static port group

인터페이스에서 LACP 를 설정할 수 있다.

LACP 모드를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	interface <i>interface-id</i>	LACP 모드를 설정하려는 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	Channel-group <i>po-id</i> mode {active on passive}	Port group 모드를 설정한다. Active 와 Passive 는 LACP mode 이고 on 은 static port group 이다.
Step4	end	privileged EXEC 모드로 변경한다.
Step5	show running-config	설정 내용을 확인한다.
Step6	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

다음은 인터페이스 Giga6/1/1 를 port-group 1 의 멤버로 등록 하는 예이다.

```
Switch# configure terminal
Switch(config)# interface Giga6/1/1
Switch(config-if- Giga6/1/1)# channel-group 1 mode active
Switch(config)# end
```

LACP 에 의해서가 아닌 static 으로 port-group 을 생성 할 경우는 다음과 같다

```
Switch# configure terminal
Switch(config)# interface Giga6/1/1
Switch(config-if- Giga6/1/1)# channel-group 1 mode on
Switch(config)# end
```

15.2.5. Clearing LACP Statistics

LACP의 통계 정보를 삭제하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	clear lacp [aggregator-id] counters	해당 port group의 LACP 통계 정보를 삭제한다.
Step2	show lacp counters	변경 내용을 확인한다.

다음은 port group 1의 LACP를 통계정보를 삭제하는 예이다:

```
Switch# clear lacp 1 counters
```

15.3. Displaying 802.3ad Statistics and Status

E7500 series는 모든 포트 그룹에 대한 정보를 확인하는 여러 명령어를 제공한다.

Command	Purpose
show etherchannel	port group의 ID 연결된 포트의 수 등 전반적인 정보를 제공.
show etherchannel summary	Port group과 연결된 포트의 정보를 간결하게 제공
show etherchannel detail	Port group과 연결된 포트의 정보를 자세하게 제공

다음은 static한 port group이 설정된 정보를 확인하는 예이다

```
shu#show etherchannel
Channel-group listing:
-----

Group: 1
-----
Group state = L2
Ports: 1 Max Maxports = 8
Port-channels: 1 Max Port-channels = 8
Protocol= -

shu#show etherchannel summary
Flags: D - down      P - bundled in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3     S - Layer2
       U - in use     f - failed to allocate aggregator

       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
Number of channel-groups in use: 1
Number of aggregators:          1
```

```

Group Port-channel Protocol Ports
-----+-----+-----+-----
1 Po1(SD) - Gi6/1/1(D)

shu#show etherchannel detail
Channel-group listing:
-----

Group: 1
-----
Group state = L2
Ports: 1 Max Maxports = 8
Port-channels: 1 Max Port-channels = 8
Protocol= -
Ports in the group:
-----
Port: Gi6/1/1
-----

Port state = Down Not-in-Bndl
Channel group = 1 Mode = On Gcchange = -
Port-channel = NULL GC = - Pseudo port-channel= Port-chan
nel1
Port index = 0 Load = 0x00
Protocol = -

Age of the port in the current state: 0d:16h44m24s

Port-channels in the group:
-----
Port-channel: Port-channel1
-----
Age of the Port-channel = 0d:0h0m18s
Number of ports = 0
GC = 0x00000000 HotStandBy port= null
Port state = Down Ag-Not-Inuse
Protocol = -
shu#

```

모든 포트 그룹에 대한 LACP 통계를 조회하려면, privileged EXEC 명령 **show lacp counters** 를 사용하라.

특정 포트 그룹에 대한 LACP 통계를 조회하려면, privileged EXEC 명령 **show lacp aggregator-id counters** 를 사용하라.

스위치의 LACP 프로토콜 정보와 상태를 조회하려면, privileged EXEC 명령 **show lacp internal** 을 사용하라. 상대 시스템의 LACP 프로토콜 정보와 상태를 조회하려면, privileged EXEC 명령 **show lacp neighbor** 을 사용하라.

출력 결과물의 항목에 대한 상세정보는 [command reference](#) 를 참고하라.

16

IP-OPTION

16.1. IP OPTOIN 개요

IP OPTION 기능은 linux kernel 에서 제공하는 /proc/sys/net/ipv4 아래의 parameter 들 중 attack 방지와 관련된 parameter 들을 설정/해제 가능 하도록 하여주는 기능이다

16.2. IP OPTOIN 명령어

IP OPTION 명령어로 설정 가능한 parameter 들은 다음과 같다.

표 18.1 IP OPTION 명령어

명령어	설명	모드
ip option icmp-drop icmp-type (any <0-255> echo-reqeust echo-reply) length <1-65535>	ICMP 패킷 차단을 위한 icmp-type 및 패킷 사이즈를 설정한다.	Config
no ip option icmp-drop	ICMP 패킷 차단 설정을 해제한다.	Config
ip icmp-ttl-exceed-send	TTL Exceed ICMP 에러 전송을 허용 또는 차단한다. Default) send	Config
no ip icmp-ttl-exceed-send	TTL Exceed ICMP 에러 전송 설정을 해제한다.	Config
ip option icmp-unreachable-send	ICMP unreachable 에러 전송을 허용 또는 차단한다. Default) send	Config
no ip option icmp-unreachable-send	ICMP unreachable 에러 전송 설정을 해제한다.	Config
ip option ip_default_ttl VALUE	Default TTL 크기를 설정한다. Default) 64	Config

no ip option ip_default_ttl	Default TTL 크기 설정을 기본값으로 변경한다.	Config
ip option ipfrag_time VALUE	메모리에서 IP fragment 를 유지하는 시간을 설정한다. Default) 30	Config
no ip option ipfrag_time	메모리에서 IP fragment 를 유지하는 시간을 기본값으로 변경한다.	Config
ip option tcp-conn-rate-limit profile-id <1-128> (any PORT) period <1-3600> count <1-65535>	TCP connection rate-limit profile 을 추가한다. TCP 목적지 포트에 대해 period 이내에 count 이상 TCP 연결을 시도하는 경우 로깅 및 차단할 수 있다.	Config
no ip option tcp-conn-rate-limit profile-id <1-128>	Profile-id 에 해당하는 TCP connection rate-limit profile 을 삭제한다.	Config
ip option tcp_fin_timeout VALUE	FIN-WAIT-2 상태의 소켓 유지 시간을 설정한다. Default) 60	Config
no ip option tcp_fin_timeout	FIN-WAIT-2 상태의 소켓 유지 시간을 기본값으로 변경한다.	Config
ip option tcp_keepalive_probes VALUE	연결이 끊어졌다고 여길 때까지 발생 시킬 keepalive probe 메시지 수를 설정한다. Default) 9	Config
no ip option tcp_keepalive_probes	Keepalive probe 메시지 수를 기본값으로 변경한다.	Config
ip option tcp_keepalive_time VALUE	Keepalive 가 활성화되었을 경우 keepalive 메시지 전송 시간을 설정을 설정한다. Default) 7200	Config
no ip option tcp_keepalive_time	Keepalive 메시지 전송 시간을 기본값으로 변경한다.	Config
ip option tcp_max_syn_backlog VALUE	TCP syn backlog queue 의 최대치 설정이다. Default) 1024	Config
no ip option tcp_max_syn_backlog	TCP syn backlog queue 의 최대치 설정을 기본값으로 변경한다.	Config
ip option tcp_max_tw_buckets VALUE	Timewait 소켓의 수를 설정한다. Default) 18700	Config
no ip option tcp_max_tw_buckets	Timewait 소켓의 수를 기본값으로 변경한다.	Config
ip option tcp_retries1 VALUE	의심스러운 TCP session 에 대한 재전송 횟수를 설정한다. Default) 3	Config
no ip option tcp_retries1	의심스러운 TCP session 에 대한 재전송 횟수를 기본값으로 변경한다.	Config
ip option tcp_retries2 VALUE	종단전 재전송 횟수를 설정한다.	Config

	Default)15	
no ip option tcp_retries2	중단전 재전송 횟수를 기본값으로 변경한다.	Config
ip option tcp_syn_retries <i>VALUE</i>	활성 TCP 연결에서 재전송을 위해 지정한 시간만큼 지난 뒤에 초기화 SYN 패킷을 보낸다. Default) 5	Config
no ip option tcp_syn_retries	TCP syn 재 전송 횟수를 기본값으로 변경한다.	Config
ip option tcp_syncookies (default disable enable)	Syn flood attack 방어를 위해 설정한다. Default) enable	Config
ip option telnet-acl access-group <1-99>	Telnet 접속을 access-group 에 대해 허용 및 차단하도록 설정한다.	Config
no ip option telnet-acl access-group <1-99>	Access-group 에 의한 telnet 접속 제한 설정을 해제한다.	Config

17

VRRP

(Virtual Router Redundancy Protocol)

VRRP (Virtual Router Redundancy Protocol)는 같은 LAN에 속한 여러 대의 라우터를 하나의 그룹으로 묶어 하나의 가상 IP 주소를 부여하고, 그 중 한 라우터를 마스터로 선출하는 프로토콜이다. VRRP 프로토콜에 의해 같은 그룹에 속한 라우터 중 하나의 라우터만 마스터로 동작하고 나머지 라우터들은 마스터로 지정된 라우터의 장애에 대비해 백업 라우터로 동작한다. 마스터로 지정된 라우터에 장애가 발생하면 VRRP 그룹 내의 백업 라우터 중 하나가 자동으로 마스터로 전환된다.

17.1. Information about VRRP

17.1.1. VRRP Operation

LAN에 연결된 호스트는 외부의 호스트와 통신하기 위해 여러 가지 방법으로 디폴트 게이트웨이 (first hop router)를 선택한다. 호스트는 동적 절차나 수동 설정을 통해 디폴트 게이트웨이를 결정한다. 다음은 동적으로 라우터를 결정하는 방법들이다:

- Proxy ARP – 호스트는 자신의 목적지의 물리 주소를 알기 위해 Address Resolution Protocol (ARP)를 사용하고, 라우터는 자신의 MAC 주소를 사용해서 ARP request에 응답한다.
- Routing protocol – 호스트는 동적 라우팅 프로토콜의 업데이트 정보를 이용해서 자신의 라우팅 테이블을 구축한다.
- IRDP (ICMP Router Discovery Protocol) 클라이언트 – 호스트는 Internet Control Message Protocol (ICMP) router discover 클라이언트를 실행한다.

동적 프로토콜을 사용하면 호스트에 대한 설정이 필요하고 프로토콜 동작에 따른 오버헤드가 발생하는 단점이 있다. 또한 라우터에 장애가 발생했을 때, 다른 라우터로의 절체가 느려질 수 있다.

동적 프로토콜을 사용하지 않고 호스트에서 디폴트 라우터를 수동으로 설정할 수도 있다. 이 방법은 호스트를 설정하는 방법도 쉽고 동작도 간단하다. 그러나 설정된 디폴트 게이트웨이에 장애가 발생하

면, 호스트는 더 이상 외부 네트워크와 통신할 수 없다.

VRRP 는 디폴트 라우터를 수동으로 설정하는 방법의 문제를 해결할 수 있다. VRRP 는 여러 개의 라우터를 하나의 그룹으로 묶어 가상 라우터(virtual router)를 만든다. LAN 에 연결된 호스트들은 이 가상 라우터를 자신의 디폴트 게이트웨이로 설정한다. 라우터가 그룹으로 묶인 가상 라우터를 VRRP 그룹이라고 표현하기도 한다.

그림 1 은 VRRP 가 설정된 LAN 형상을 나타낸다. 이 예에서 라우터 A, B 그리고 C 는 가상 라우터를 구성하도록 VRRP 가 실행되는 VRRP 라우터이다. 가상 라우터의 IP 주소는 라우터 A 의 IP 주소 (10.0.0.1)과 동일하게 설정한다.

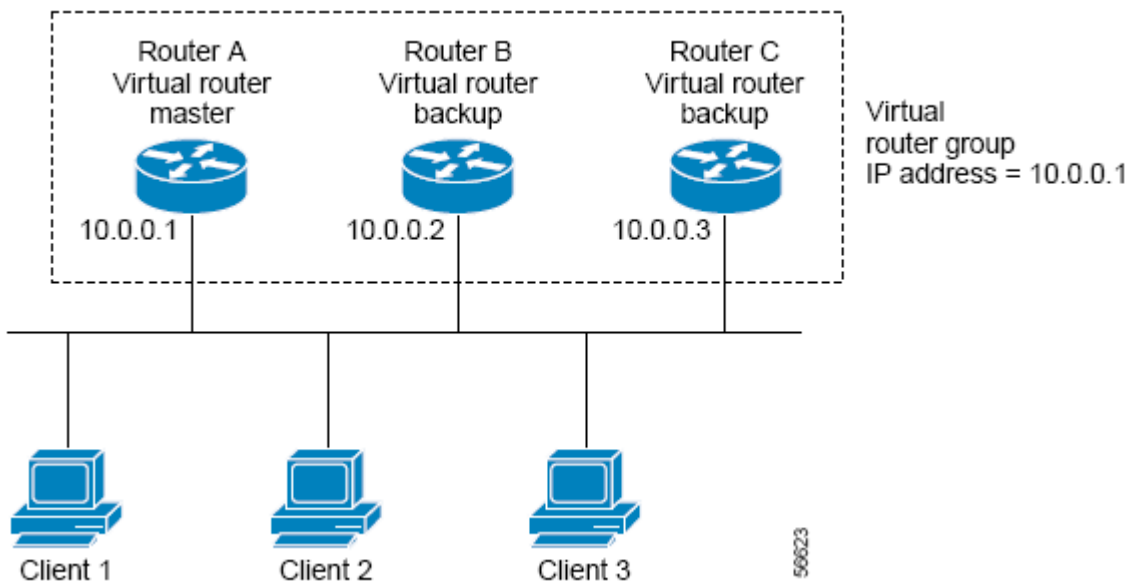


그림 17-1 Basic VRRP Topology

가상 라우터가 라우터 A 의 인터페이스에 할당된 IP 주소를 사용하기 때문에, 라우터 A 가 가상 라우터의 마스터 역할을 담당하고 IP 주소의 소유주라 부른다. 라우터 A 는 마스터로써 가상 라우터의 IP 주소를 제어하고, 이 IP 주소로 전달된 패킷의 포워딩을 담당한다. 클라이언트들은 디폴트 게이트웨이의 IP 주소를 가상 라우터의 IP 주소인 10.0.0.1 로 설정한다.

라우터 B 와 C 는 백업 가상 라우터로 동작한다. 만약 마스터 가상 라우터에 장애가 발생하면, 백업 라우터 중에서 가장 높은 우선 순위를 가진 라우터가 마스터가 되어 LAN 에 연결된 호스트들에게 계속 서비스를 제공한다. 라우터 A 가 장애로부터 복구되면, 라우터 A 가 가상 라우터의 IP 주소 소유주이기 때문에 마스터가 된다.

그림 2 는 라우터 A 와 B 가 트래픽을 공유하도록 VRRP 를 설정한 예를 보여준다. 라우터 A 와 B 는 서로에 대한 백업 라우터로 동작한다.

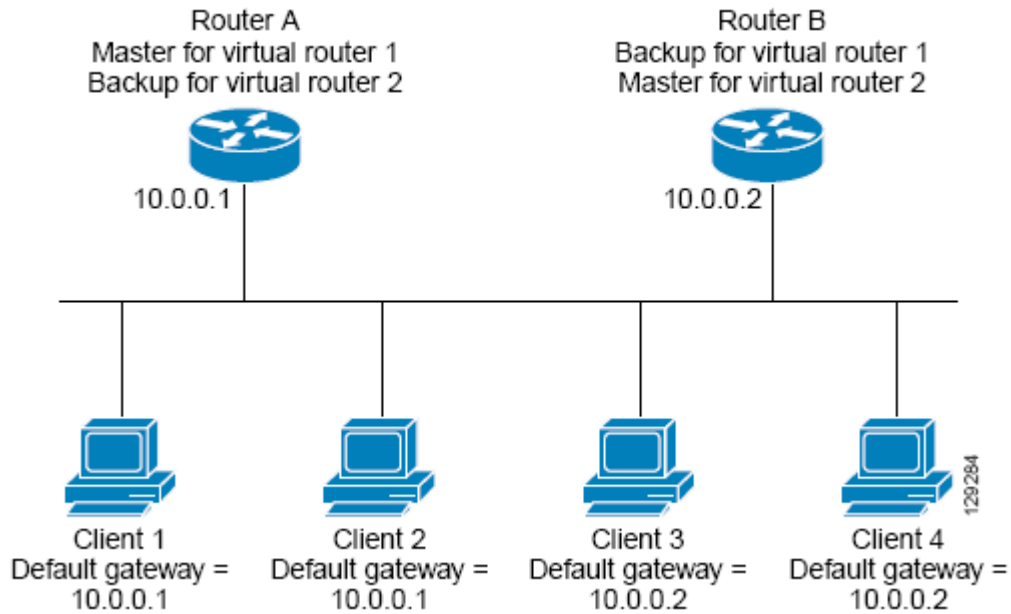


그림 17-2 Load Sharing and Redundancy VRRP Topology

이 형상에서 두 개의 가상 라우터가 설정된다. 가상 라우터 1에서 라우터 A가 IP 주소 10.0.0.1의 소유주이자 마스터 가상 라우터이며, 라우터 B는 라우터 A에 대한 백업 가상 라우터이다. 클라이언트 1과 2는 디폴트 게이트웨이의 IP 주소로 10.0.0.1을 사용한다.

가상 라우터 2에서 라우터 B가 IP 주소 10.0.0.2의 소유주이자 마스터 가상 라우터이며, 라우터 A는 라우터 B에 대한 백업 가상 라우터이다. 클라이언트 3과 4는 디폴트 게이트웨이의 IP 주소로 10.0.0.2를 사용한다.

17.1.2. VRRP Benefits

Redundancy

VRRP는 여러 개의 라우터를 디폴트 게이트웨이로 사용할 수 있게 해준다. 이것은 네트워크의 단일 지점 장애에 대한 위험을 낮춰준다.

Load Sharing

LAN 클라이언트로부터의 트래픽이 여러 라우터에게로 분산되도록 VRRP를 설정할 수 있다. 이렇게 함으로써 트래픽에 대한 부담을 여러 라우터들에게 분산시킬 수 있다.

Multiple Virtual Routers

VRRP는 인터페이스 당 최대 255개의 가상 라우터 (VRRP 그룹)을 지원한다. 다수의 가상 라우터를 지원함으로써 이중화와 트래픽 부하 분산이 가능하다.

Preemption

VRRP의 이중화 방법은 높은 우선 순위의 라우터가 사용 가능하게 되었을 때, 현재의 마스터를 대신

해서 마스터가 되는 것을 허용한다.

Advertisement Protocol

VRRP 는 전용의 멀티캐스트 주소 (224.0.0.18)를 사용해서 VRRP 메시지를 전송한다. IANA 는 VRRP 에게 IP 프로토콜 번호 112 를 할당한다.

VRRP circuit fail-over

VRRP circuit fail-over 은 인터페이스의 상태에 따라 VRRP 우선 순위를 변경해서, 최적의 VRRP 라우터가 마스터 가상 라우터가 될수 있도록 지원한다.

17.1.3. Multiple Virtual Router Support

라우터의 물리 인터페이스에 최대 255 개의 가상 라우터를 설정할 수 있다. 라우터가 지원할 수 있는 실제 가상 라우터의 개수는 다음의 요인에 영향을 받는다:

- 라우터의 프로세스 능력
- 라우터의 메모리 용량
- 라우터의 인터페이스가 제공할 수 있는 최대 MAC 주소 개수

17.1.4. VRRP Router Priority and Preemption

VRRP 에서 VRRP 라우터 우선 순위가 가장 중요한 요소이다. 마스터 가상 라우터에 장애가 발생했을 때, 우선 순위로써 VRRP 라우터의 역할을 결정한다.

만약 VRRP 라우터가 가상 라우터의 IP 주소를 자신의 물리 인터페이스의 IP 주소로 가지고 있다면, 이 라우터는 마스터 가상 라우터로 동작한다.

또한 우선 순위는 마스터 가상 라우터에 장애가 발생했을 때, 백업 가상 라우터로 동작중인 VRRP 라우터 중에서 마스터 가상 라우터를 선출하는 기준이 된다. **priority** 명령을 사용해서 백업 가상 라우터의 우선 순위를 1 ~ 254 범위로 설정할 수 있다.

예를 들어, LAN 에서 마스터 가상 라우터인 라우터 A 에 장애가 발생했다면, 선출 프로세스는 백업 가상 라우터 B 와 C 중에서 마스터를 선출해야 한다. 라우터 B 와 C 의 우선 순위가 각각 101 과 100 으로 설정되어 있다면, 라우터 B 의 우선 순위가 더 높으므로 라우터 B 가 마스터 가상 라우터가 된다. 만약 라우터 B 와 C 의 우선 순위가 똑같이 100 으로 설정되었다면, 높은 IP 주소를 가진 백업 가상 라우터가 마스터 가상 라우터로 선출 된다.

높은 우선 순위의 백업 가상 라우터가 마스터 가상 라우터가 될 수 있도록 현재의 마스터 라우터를 대체할 수 있는 방법(preemptive scheme)을 제공한다. **preempt-mode false** 명령을 사용해서 이러한 기능을 사용하지 않을 수 있다. 선점(preemption)이 비활성화 되면, 마스터 가상 라우터가 된 백업 가상 라우터는 원래의 마스터 가상 라우터가 복구되어 마스터가 될 때까지 계속 마스터의 역할을 수행한다.

17.1.5. VRRP Advertisements

마스터 가상 라우터는 같은 그룹의 다른 VRRP 라우터에게 VRRP advertisement 메시지를 전송한다. VRRP Advertisement 메시지는 마스터 가상 라우터의 우선 순위와 상태 정보가 포함된다. VRRP advertisement 메시지는 IP 패킷으로 만들어져서, VRRP 그룹에 할당된 IPv4 멀티캐스트 주소로 전송된다. 전송 주기를 설정하지 않았을 경우 매 1 초마다 전송되며, 전송 주기는 변경이 가능하다.

17.1.6. VRRP Circuit failover

VRRP의 circuit failover 기능은 인터페이스의 상태를 감시한다. 감시할 인터페이스는 **circuit-failover** 명령으로 설정할 수 있다. VRRP는 추적하는 인터페이스의 상태에 따라 가상 라우터의 우선 순위 값을 감소 시키거나 증가 시킨다.

17.2. How to Configure VRRP

이 장에서는 다음과 같은 절차를 설명한다:

- Enabling VRRP
- Disabling VRRP
- Customizing VRRP
- Configuring VRRP circuit fail-over

17.2.1. Enabling VRRP

VRRP를 작동시키려면 다음의 작업을 수행한다.

	Command or Action	Purpose
Step 1	configure terminal 예제: Switch# configure terminal	Global configure 모드로 진입한다
Step 2	interface interface-name 예제: Switch(config)# interface gi2/2/10	Interface configuration 모드로 진입한다.
Step 3	ip address ip-address/prefix-length 예제: Switch(config-if-Gi2/2/10)# ip address 33.1.1.1/24	인터페이스에 IP 주소를 설정한다.

Step 4	router vrrp <i>virtual-ID interface-name</i> 예제: Switch(config)# router vrrp 3 gi2/2/10	Router configuration 모드로 진입한다.
Step 5	virtual-ip <i>ip-address</i> 예제: Switch(config-router)# virtual-ip 33.1.1.1	인터페이스에 VRRP 를 작동시키고 virtual-ip 를 설정한다. 주의: VRRP 그룹의 모든 라우터들은 같은가 가상 IP 주소로 설정해야 한다. 다른 IP 주소가 설정되면, VRRP 그룹의 라우터들은 서로 통신을 할 수 없게 되고, 잘못 설정된 라우터는 자신이 마스터로 동작한다.
Step 6	enable 예제: Switch(config-router)# enable	vrrp session 을 enable
Step 7	End 예제: Switch(config-router)# end	privileged EXEC 모드로 돌아간다
Step 8	show vrrp 예제: Switch# show vrrp	(옵션) 라우터의 VRRP 그룹의 상태 정보를 조회한다.
Step 9	show vrrp <i>virtual-ID interface-name</i> 예제: Switch# show vrrp gi2/2/10	(옵션) 특정 인터페이스에 설정된 VRRP 그룹의 정보를 조회한다.

17.2.2. Disabling VRRP on an Interface

인터페이스의 VRRP 를 중단시킴으로써 VRRP 설정은 유지하고 프로토콜 동작만 중지하는 것이 가능하다. **show running-config** 명령으로 조회했을 때, VRRP 그룹의 설정 상태와 VRRP 가 동작하는지 중단되었는지를 확인할 수 있다.

	Command or Action	Purpose
Step 1	configure terminal 예제: Switch# configure terminal	Global configure 모드로 진입한다
Step 2	router vrrp <i>virtual-ID interface-name</i> 예제: Switch(config)# router vrrp 3 gi2/2/10	Router configuration 모드로 진입한다.

Step 3 disable 예제: Switch(config-router)# disable	특정 vrrp session 을 중단한다.
---	-------------------------

17.2.3. Customizing VRRP

VRRP 를 customize 하기 위한 옵션을 설정하려면 다음의 작업을 수행하라.

	Command or Action	Purpose
Step 1	configure terminal 예제: Switch# configure terminal	Global configure 모드로 진입한다
Step 2	router vrrp virtual-ID interface-name 예제: Switch(config)# router vrrp 3 gi2/2/10	Router configuration 모드로 진입한다.
Step 3	advertisement-interval interval 예제: Switch(config-router)# advertisement-interval 3	VRRP 마스터가 전송하는 VRRP advertiment 를 전송 주기를 설정한다. - default 1 초 Note 같은 VRRP 그룹에 속한 라우터들은 같은 전송 주기로 설정해야 한다.
Step 4	preempt-mode [true false] 예제: Switch(config-router)# preempt-mode true	현재 가상 마스터 라우터보다 우선 순위가 높은 라우터가 마스터가 될수 있도록 허용할 것인 가를 설정한다.
Step 5	priority level 예제: Switch(config-router)# priority 200	VRRP 의 우선 순위 값을 설정한다. - default 는 100

17.2.4. Configuring VRRP circuit failover

VRRP circuit failover 를 설정하려면 다음의 작업을 수행하라. 이 명령어로 설정된 인터페이스가 다운 되면, VRRP 는 지정한 값만큼 라우터의 우선 순위 값을 감소 시킨다.

VRRP 그룹이 IP 주소의 소유주라면, VRRP 그룹의 우선 순위는 255 로 고정되고 circuit failover 명령을 통해 우선 순위가 변경되지 않는다.

	Command or Action	Purpose
Step 1	configure terminal 예제: Switch# configure terminal	Global configure 모드로 진입한다
Step 2	router vrrp virtual-ID interface-name 예제: Switch(config)# router vrrp 1 gi2/2/1	Router configuration 모드로 진입한다.
Step 3	circuit-failover interface-name PriorityDelta 예제: Switch(config-router)# circuit-failover gi1/1/1 10	인터페이스의 상태가 VRRP 그룹의 우선 순위에 영향을 미치는 인터페이스를 설정하고 우선 순위 값을 감소시킬 값을 설정한다.
Step 4	show vrrp 예제: Switch# show vrrp	(옵션) 라우터의 VRRP 그룹의 상태 정보를 조회한다.

17.3. Configuration Examples for VRRP

17.3.1. Configuring VRRP: Example

다음의 예제에서 스위치 A와 스위치 B는 3개의 VRRP 그룹에 포함된다. 각 그룹의 설정은 다음과 같다:

- Group 1:
 - 가상 IP 주소는 10.1.0.10
 - 스위치 A가 우선 순위 값 120으로 이 그룹의 마스터가 된다
 - Advertising 주기는 3초이다.
 - Preemption이 활성화되어 있다.
- Group 5:
 - 스위치 B가 우선 순위 값 200으로 이 그룹의 마스터가 된다.
 - Advertising 주기는 10초이다.
 - Perrmption이 활성화되어 있다.
- Group 100:
 - 스위치 A가 가장 높은 IP 주소 (10.1.0.2)를 가지고 있기 때문에, 이 그룹의 마스터가 된다.
 - Advertising 주기는 default 1초이다.
 - Preemption이 비활성화되어 있다.

Router A
router vrrp 1 vlan1


```
virtual-ip 10.1.0.10 backup
advertisement-interval 3
priority 120
router vrrp 5 vlan1
virtual-ip 10.1.0.50 backup
advertisement-interval 10
router vrrp 100 vlan1
virtual-ip 10.1.0.100 backup
preempt-mode false
```

Router B

```
router vrrp 1 vlan1
virtual-ip 10.1.0.10 backup
advertisement-interval 3
router vrrp 5 vlan1
virtual-ip 10.1.0.50 backup
priority 200
advertisement-interval 10
router vrrp 100 vlan1
virtual-ip 10.1.0.100 backup
preempt-mode false
```

17.3.2. VRRP circuit failover: Example

다음의 예제에서, 인터페이스 `vlan10`의 link 상태를 추적하도록 설정된다. 인터페이스 `vlan1`의 VRRP는 인터페이스 `vlan10`의 프로토콜 상태 변환에 대한 정보를 전달 받는다. 인터페이스 `vlan10`의 link 상태가 `down`이 되면, VRRP 그룹의 우선 순위 값이 15만큼 감소한다.

```
router vrrp 3 vlan1
virtual-ip 33.1.1.1 backup
priority 120
circuit-failover vlan10 15
```

17.3.3. VRRP Circuit fail-over Verification: Example

다음의 예제는 “VRRP circuit failover: Example” 절에서의 설정을 확인한다:

```
Switch# show vrrp
Address family IPv4
State is Master
Virtual IP address is 33.1.1.1 (Not-owner)
Virtual MAC address is 0000.5e00.0101
```

Advertisement interval is 1 sec
Preemption is enabled
Priority is 120, Current priority is 120
Master Router is 33.1.1.3 (), priority is 120
Master Advertisement interval is 1 sec
Master Down interval is 4 sec
Circuit failover interface vlan10, Priority Delta 15, Status UP

17.3.4. Disabling a VRRP Group on an Interface: Example

다음의 예는 인터페이스 VRRP 그룹의 설정을 유지하면서 인터페이스 vlan1 의 VRRP 그룹을 중지시키는 방법을 보여준다:

```
router vrrp 3 vlan1
  virtual-ip 33.1.1.1 backup
  priority 120
  disable
```

18

Setting Time and Calendar

E7500 시리즈 스위치는 **time-of-day** 서비스를 제공한다. 이 서비스는 여러 장비들이 같은 시각으로 동기화를 맞추거나, 다른 시스템에 시간 서비스를 제공할 수 있도록 스위치가 정확한 현재 시간을 유지하도록 한다.

18.1. Understanding Time Sources

E7500 시리즈 스위치는 두 개의 클락(clock)을 가진다. 하나는 배터리에 의해 유지되는 하드웨어 클락 (“calendar” CLI 명령 참조)이고 나머지 하나는 소프트웨어 클락 (“clock” CLI 명령 참조)이다. 이 두개의 클락은 각각 관리된다.

시스템이 사용하는 기본 시간 소스는 소프트웨어 클락이다. 소프트웨어 클락은 시스템 시작 후부터 현재 시각을 유지한다. 소프트웨어 클락은 여러 가지 소스로부터 설정할 수 있고, 다양한 방법을 통해 다른 시스템으로 전달된다. 소프트웨어 클락은 시스템이 초기화되거나 리부트 될 때 하드웨어 클락을 사용해서 초기화된다. 그리고 나서 다음의 소스들을 사용해서 변경할 수 있다:

- Network Time Protocol (NTP)
- 수동 설정 (하드웨어 클락 사용)

소프트웨어 클락은 내부적으로 Coordinated Universal Time (UTC), 또는 Greenwich Mean Time (GMT) 기반으로 시간 정보를 관리한다. 장비가 사용되는 지역의 시간 정보를 반영할 수 있도록 지역 시간대 (time zone)과 서머 타임 (daylight savings time)을 설정할 수 있다.

18.1.1. Network Time Protocol

NTP는 네트워크에 연결된 장비들의 시간 동기화를 위해 설계된 프로토콜이다. NTP는 IP/UDP 서비스를 이용해서 동작한다. RFC1305에 NTP 버전 3에 대해 정의되어 있다.

NTP 네트워크는 타임 서버(time server)에 연결된 라디오 클락(radio clock) 또는 원자 클락 (atomic

clock)과 같은 권위있는 타임 소스(authoritative time source)로부터 시간 정보를 획득한다. NTP 는 이 시간 정보를 네트워크를 통해 분배한다. NTP 는 두 시스템 사이에 밀리초 단위의 시간 동기화를 맞추는데 분당 하나의 패킷을 사용할 정도로 매우 효과적인 프로토콜이다.

NTP 는 권위있는 타임 소스로까지 얼마나 많은 NTP “hops”이 존재하는 지를 나타내는 “stratum”이란 개념을 사용한다. 일반적으로 “stratum 1” 타임 서버에는 권위있는 타임 소스가 직접 연결 되어 있다. “stratum 2” 타임 서버는 “stratum 1” 타임 서버로부터 NTP 를 통해 시간 정보를 수신한다. NTP 는 사용할 수 있는 타임 서버중 가장 작은 stratum 을 가진 타임 서버를 자신의 시간 소스로 선택한다.

NTP 는 의심스러운 시간 정보로 동기화를 하지 않기 위해 다음 두 가지 방법을 제공한다.

- NTP 는 자신을 소스로 동기화한 장비와는 동기화하지 않는다.
- NTP 는 여러 장비에서 얻은 시간을 비교하고 다른 것과 큰 시간차를 보이는 장비와는 stratum 이 작아도 동기화하지 않는다.

18.1.2. Hardware Clock

E7500 시리즈 스위치는 시스템이 재시작되거나 전원이 꺼지더라도 현재 시각을 유지할 수 있도록 배터리에 의해 유지되는 하드웨어 클락을 가진다. 하드웨어 클락은 시스템이 시작할 때 소프트웨어 클락을 초기화하는데 사용된다.

18.2. Configuring NTP

이 장에서는 시스템에서 NTP 를 사용할 수 있도록 다음과 같은 절차에 대해 설명한다:

- Configuring Poll-Based NTP Associations
- Configuring NTP Authentication
- Configuring the Source IP Address for NTP Packets
- Configuring the System as an Authoritative NTP Server
- Updating the Hardware Clock

18.2.1. Configuring Poll-Based NTP Associations

NTP 를 사용하는 네트워크 장비는 시간 소스와 동기화를 맞추는데 여러 가지 동작 모드를 제공한다. 장비가 네트워크로부터 시간 정보를 획득하는 방법으로는 호스트 서버에게 시간 정보를 요청(poll-based association)하거나 브로드 캐스트되는 NTP 정보를 청취하는 두 가지 방법이 있다. 이 장에서는 서버에게 요청하는 모드에 대해 설명한다.

다음은 가장 많이 사용되는 서버 요청 모드이다:

- Client mode

- Symmetric active mode

Client 와 Symmetric active 모드는 NTP 에 높은 수준의 시간 정밀도가 요구될 때 사용된다.

클라이언트 모드에서 장비는 현재 시간 정보를 얻기 위해 설정된 시간 서버들을 조사한다. 장비는 조사된 여러 개의 시간 서버들 중 하나를 선택해서 시간 동기를 맞춘다. 이 경우 장비와 시간 서버는 클라이언트-서버 관계를 맺고 있기 때문에, 장비는 다른 클라이언트 장비가 보낸 시간 정보는 사용하지 않는다. 이 모드는 다른 로컬 클라이언트에게로 시간 정보를 제공할 필요가 없는 시스템에 유용하다. 클라이언트 모드에서 시간 동기를 맞추고 싶은 시간 서버를 명시하기 위해 **ntp server** 명령을 사용하면 된다.

Symmetric active 모드에서 장비는 현재 시간 정보를 얻기 위해 설정된 시간 서버들을 조사하고, 로컬 호스트에게는 시간 정보를 제공한다. 이 모드는 **peer-to-peer** 관계이기 때문에 장비는 자신이 통신하는 로컬 네트워크 장비의 시간 정보도 함께 저장한다. 이 모드는 복잡한 네트워크 경로를 통해 연결된 상호 중복된 서버가 존재할 경우에 사용되어야 한다. 대부분의 **stratum 1** 과 **stratum 2** 서버는 이런 형태의 네트워크 설정을 사용한다. Symmetric active 모드를 사용하려면 **ntp peer** 명령을 사용하라.

NTP 의 동작 모드를 결정하는 것은 장비의 역할 (서버 또는 클라이언트)과 **stratum 1** 서버 설정에 의존적이다.

Command	Purpose
Switch(config)# ntp server <i>ip-address</i>	Client 모드로 NTP 설정
Switch(config)# ntp peer <i>ip-address</i>	Symmetric active 모드로 NTP 설정

18.2.2. Configuring NTP Authentication

암호화된 NTP 인증은 인증 키와 NTP 패킷의 정보를 사용하기 전에 신뢰할 수 있는 장비로부터 전송된 패킷인지를 검사하는 인증 절차를 사용한다.

인증 절차는 NTP 패킷이 생성되는 순간부터 시작된다. MD5 message digest 알고리즘에 의해 암호화된 체크섬(checksum) 키가 생성되고 NTP 패킷에 포함되어 클라이언트에게 전송된다. 패킷을 수신한 클라이언트는 패킷의 암호화된 체크섬 키를 해독한 후 자신의 **trusted** 키와 비교한다. 패킷이 유효한 인증 키를 포함하고 있다면 클라이언트는 이 패킷의 시간 정보를 허용한다. 클라이언트와 일치하는 인증 키를 포함하고 있지 않는 NTP 패킷은 폐기된다.

NTP 인증이 올바르게 설정된 후부터 장비는 오직 신뢰할 수 있는 시간 소스와 시간을 동기화 시킨다. 장비에서 암호화된 NTP 패킷을 송수신하게 하려면, 글로벌 설정 모드에서 다음의 명령을 사용하라:

	Command or Action	Purpose
Step 1	Switch(config)# ntp authenticate	NTP의 인증 기능을 활성화 시킨다.
Step 2	Switch(config)# ntp authentication-key <i>key-number</i> md5 <i>value</i>	인증 키를 정의한다. 각 키는 키 번호와 종류 그리고 값을 가진다. 현재 지원되는 키 종류는 MD5이다.
Step 3	Switch(config)# ntp trusted-key <i>key-number</i>	신뢰하는 인증 키를 정의한다. 만약 인증키가 신뢰하는 키라면, 시스템은 NTP 패킷에 이 키를 사용하는 시스템과 시간 동기를 시도한다.
Step 4	Switch(config)# ntp server <i>ip-address</i> key <i>key-number</i>	소프트웨어 클락이 NTP 타임 서버와 동기화 되도록 허용한다.

18.2.3. Configuring the Source IP Address for NTP Packets

시스템이 NTP 패킷을 전송할 때, NTP 패킷의 소스 IP 주소는 NTP 패킷을 전송하는 인터페이스의 주소로 설정된다. NTP 패킷의 소스 IP 주소로 특정 인터페이스의 IP 주소를 사용하고 싶다면 글로벌 설정 모드에서 다음의 명령을 사용하라:

Command	Purpose
Switch(config)# ntp source <i>interface</i>	IP 주소를 빌려올 인터페이스를 지정한다.

18.2.4. Configuring the System as an Authoritative NTP Server

시스템이 외부의 시간 소스와 동기화가 되지 않더라도 시스템을 NTP 서버로 사용하려면 글로벌 설정 모드에서 다음의 명령을 수행하라:

Command	Purpose
Switch(config)# ntp master [<i>stratum</i>]	시스템을 NTP 서버로 설정한다.

E7500 시리즈 스위치는 **stratum 1** 서비스를 지원한다. 하지만 장비 내부에 연결 가능한 라디오 혹은 원자 클락이 존재하지는 않으므로 E7500 시리즈 스위치를 **stratum 1**로 설정하는 것은 권장하지 않는다.

18.2.5. Updating the Hardware Clock

하드웨어 클락이 가진 장비에서, 소프트웨어 클락으로 하드웨어 클락이 주기적으로 업데이트 하도록 설정할 수 있다. NTP로 설정되는 소프트웨어 클락이 하드웨어 클락보다 더 정확하기 때문에 NTP를 사용하는 장비에서는 이렇게 설정하는 것이 바람직하다.

하드웨어 클락을 NTP 시각과 동기화시키려면 글로벌 설정 모드에서 다음의 명령을 사용하라:

Command	Purpose
Switch(config)# ntp update-calendar	시스템의 하드웨어 클락을 주기적으로 소프트웨어 클락으로 업데이트 하도록 설정한다.

18.3. Configuring Time and Date Manually

사용 가능한 타임 소스가 없다면, 시스템이 시작된 후에 현재 시각을 직접 설정할 수 있다.

18.3.1. Configuring the Time Zone

시간대 정보를 설정하려면 글로벌 설정 모드에서 다음의 명령을 사용하라:

Command	Purpose
Switch(config)# clock timezone zone hours-offset [minutes-offset]	시간대를 설정한다. 인자 zone 은 시간대의 이름을 표시한다 (보통 표준 시간대 이름을 사용). 인자 hours-offset 은 UTC 와의 시차를 명시한다. 인자 minutes-offset 은 UTC 와의 분차를 명시한다.

18.3.2. Configuring Summer Time (Daylight Savings Time)

매년 특정 날짜에 시작되고 끝나는 서머 타임 (daylight savings time)을 설정하려면 글로벌 설정 모드에서 다음의 명령을 사용하라:

Command	Purpose
Switch(config)# clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]	반복되는 서머타임의 시작과 끝을 설정. 인자 offset 은 서머 타임 동안 추가되는 분을 표시한다.

서머 타임이 매년 동일하게 반복되지 않는다면, 글로벌 설정 모드에서 다음의 명령으로 다음 서머타임이 시작되는 정확한 날짜를 설정할 수 있다:

Command	Purpose
Switch(config)# clock summer-time zone date month date year hh:mm month date year hh:mm [offset]	특정 서머타임의 시작과 끝을 설정. 인자 offset 은 서머 타임 동안 추가되는 분을 표시한다.

또는	
Switch(config)# clock summer-time zone date date onth date year hh:mm date month year hh:mm [offset]	

18.3.3. Manually Setting the Software Clock

일반적으로 시스템이 NTP 와 같은 유효한 시간 메카니즘에 의해 시간 동기화가 이루어지거나, 시스템이 하드웨어 클락을 가지고 있다면 소프트웨어 클락을 설정할 필요가 없다. 만약 사용가능한 시간 소스가 없다면 이 명령을 사용하라. 이 명령으로 설정되는 시간은 시간대의 영향을 받는다. 소프트웨어 클락을 직접 설정하려면, EXEC 모드에서 다음의 명령을 사용하라:

Command	Purpose
Switch# clock set <i>hh:mm:ss day month year</i>	소프트웨어 클락 설정.
또는	
Switch# clock set <i>hh:mm:ss month day year</i>	

18.4. Using the Hardware Clock

E7500 시리즈 스위치는 소프트웨어 기반의 클락과는 독립된 하드웨어 기반의 클락을 추가로 가지고 있다. 하드웨어 클락은 충전이 가능한 배터리를 가진 칩(chip)으로 장비가 리부트 되더라도 시각 정보를 유지할 수 있다.

소프트웨어 클락은 정확한 시각 정보를 유지하기 위해 네트워크의 권위있는 타임 소스로부터의 시간 업데이트 정보를 수신해야 한다. 그리고 시스템이 동작중인 동안 소프트웨어 클락은 하드웨어 클락을 주기적으로 업데이트 해줘야 한다.

하드웨어 클락을 설정하기 위해 다음의 작업을 할 수 있다:

- Setting the Hardware Clock
- Setting the Software Clock from the Hardware Clock
- Setting the Hardware Clock from the Software Clock

18.4.1. Setting the Hardware Clock

하드웨어 클락은 소프트웨어 클락과 별도로 시간을 관리한다. 하드웨어 클락은 시스템이 재시작되거나 전원이 꺼진 상태에서도 계속 동작한다. 일반적으로 하드웨어 클락은 시스템이 설치될 때 한 번만 설정하면 된다.

믿을 수 있는 외부 시간 소스를 사용하고 있다면 하드웨어 클락을 직접 설정하지 않도록 한다. 시간 동기화는 NTP 를 이용해서 이뤄질 것이다.

만약 사용할 수 있는 외부 시간 소스가 없다면 하드웨어 클락을 설정하기 위해 EXEC 모드에서 다음의 명령을 사용하라:

Command	Purpose
Switch# calendar set <i>hh:mm:ss day month year</i>	하드웨어 클락 설정.
또는	
Switch# calendar set <i>hh:mm:ss month day year</i>	

18.4.2. Setting the Software Clock from the Hardware Clock

새로운 하드웨어 클락 설정으로 소프트웨어 클락을 설정하려면, EXEC 모드에서 다음의 명령을 상용하라:

Command	Purpose
Switch# clock read-calendar	하드웨어 클락으로 소프트웨어 클락 설정.

18.4.3. Setting the Hardware Clock from the Software Clock

새로운 소프트웨어 클락 설정으로 하드웨어 클락을 설정하려면, EXEC 모드에서 다음의 명령을 사용하라:

Command	Purpose
Switch# clock update-calendar	소프트웨어 클락으로 하드웨어 클락 설정.

18.5. Monitoring Time and Calendar Services

클락, 카렌더 그리고 NTP 정보를 조회하려면 다음의 명령들을 사용하라.

Command	Purpose
Switch# show calendar	현재 하드웨어 클락 조회
Switch# show clock	현재 소프트웨어 클락 조회
Switch# show ntp associations [detail]	NTP association 상태 조회
Switch# show ntp status	NTP 상태 조회

18.6. Configuration Examples

18.6.1. Clock, Calendar, and NTP Configuration Examples

다음 예에서 하드웨어 클락을 가진 스위치는 두 개의 다른 시스템과 서버 관계를 가지고 있고, 주기적으로 하드웨어 클락을 업데이트 한다.

```
clock timezone KST 9
ntp update-calendar
ntp server 192.168.13.57
ntp server 192.168.11.58
```

19

Dynamic ARP Inspection

문서버전 History

E7500-DAI-2

마지막 수정 날짜: 2010-02-17

적용가능 장비: E7500 series

이 장에서는 ARP 패킷을 검사하는 dynamic Address Resolution Protocol (ARP) inspection (DAI) 기능에 대한 설정 방법을 설명한다.



Note

이 장에서 사용되는 명령어에 대한 문법과 사용 방법에 관한 상세한 정보는 **command reference** 를 참조하라.

이 장은 다음과 같은 내용으로 이루어져 있다:

- DAI에 대한 이해 (Understanding DAI)
- DAI 기본 설정 (Default DAI Configuration)
- DAI 설정 지침과 제약 사항 (DAI Configuration Guidelines and Restrictions)
- DAI 설정 (Configuring DAI)
- DAI 설정 예제 (DAI Configuration Samples)

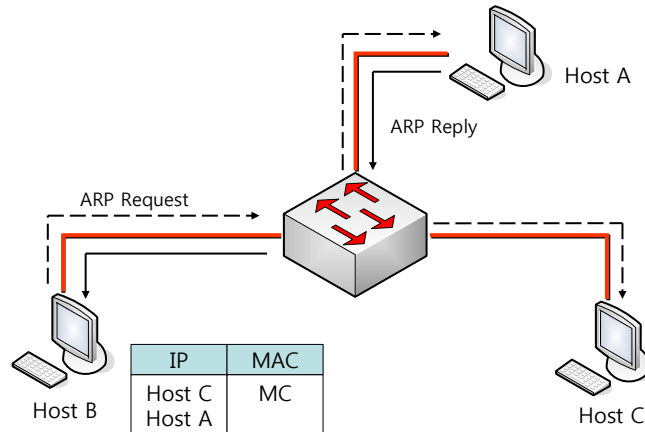
19.1. Understanding DAI

이 절에서는 DAI 에 대한 설명과 DAI 기능을 사용해서 ARP spoofing 공격 ^{attack} 을 방어하는 방법에 대해 설명한다. 이 절은 다음과 같은 내용으로 이루어져 있다:

- Understanding ARP
- Understanding ARP Spoofing Attacks
- Understanding DAI and ARP Spoofing Attacks
- Interface Trust States and Network Security
- Rate Limiting of ARP Packets
- Relative Priority of ARP ACLs and DHCP Snooping Entries
- Logging of Dropped Packets

19.1.1. Understanding ARP

ARP 는 IP 주소와 MAC 주소를 매핑 ^{mapping} 해서 Layer 2 브로드캐스트 ^{broadcast} 도메인에서 IP 통신이 가능하게 한다. 예를 들어, 호스트 B 가 호스트 A 로 정보를 전송하려고 하는데 호스트 B 의 ARP 테이블에 호스트 A 에 대한 MAC 주소가 등록되어 있지 않다고 가정하자.

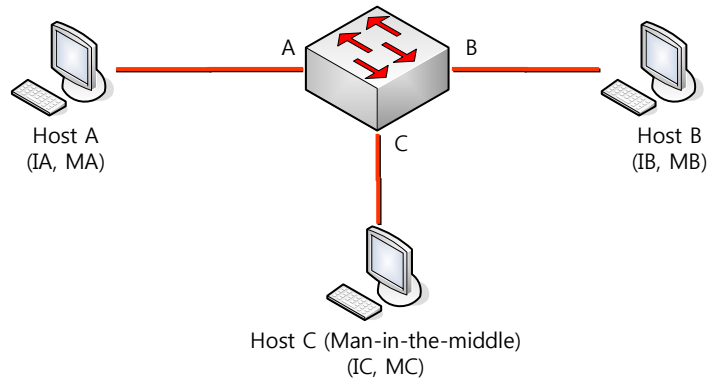


호스트 B 는 호스트 A 의 IP 주소에 대응하는 MAC 주소를 알아내기 위해서, 브로드캐스트 도메인 내부의 모든 호스트들에게 브로드캐스트 메시지 (ARP request)를 전송한다. 브로드캐스트 도메인 내부의 모든 호스트들은 호스트 B 가 전송한 ARP request 를 수신하고, 호스트 A 는 자신의 MAC 주소를 응답한다.

19.1.2. Understanding ARP Spoofing Attacks

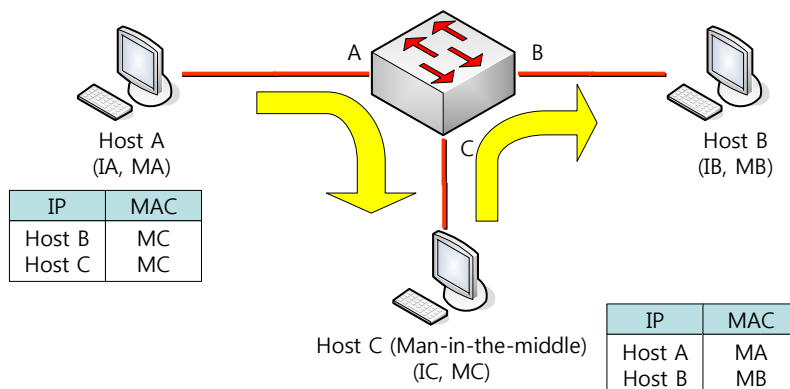
ARP 는 ARP request 를 수신하지 않은 호스트가 전송한 gratuitous reply 로 ARP 테이블이 변경되는 것을 허용한다. 이로 인해 ARP spoofing 공격과 ARP cache poisoning 이 발생할 수 있다. 공격 이후에는 공격 당한 장비의 모든 트래픽은 공격자의 컴퓨터를 통해 라우터, 스위치 또는 호스트로 전달된다.

ARP spoofing 공격은 Layer 2 네트워크에 연결된 호스트, 스위치, 라우터의 ARP 캐시 ^{cache} 을 조작한다. 그리고 다른 호스트로 전달되어야 할 트래픽을 가로챈다. 다음의 그림은 ARP cache poisoning 의 예를 보여준다.



호스트 A, B, C 는 각각 스위치의 인터페이스 A, B, C 에 연결되어 있으며, 모두 같은 서브넷에 위치한다. IP 주소와 MAC 주소를 괄호 안에 나타내었다: 예를 들어, 호스트 A 는 IP 주소 IA 와 MAC 주소 MA 를 사용한다. 호스트 A 가 IP 계층에서 호스트 B 와 통신할 필요가 있을 때, IP 주소 IB 와 연관된 MAC 주소를 알기 위해 ARP request 를 브로드캐스트로 전송한다. 스위치와 호스트 B 는 이 ARP request 를 수신하면, IP 주소 IA 와 MAC 주소 MA 를 가진 호스트의 ARP 캐시를 갱신한다: 예를 들어, IP 주소 IA 는 MAC 주소 MA 에 매핑되어 있다. 호스트 B 가 응답하면, 스위치와 호스트 A 는 IP 주소 IB 와 MAC 주소 MB 를 가진 호스트의 ARP 캐시를 갱신한다.

호스트 C 는 IP 주소 IA (또는 IB)에 대한 MAC 주소로 MC 를 사용하는 ARP response 를 브로드캐스트함으로써 스위치, 호스트 A, 호스트 B 의 ARP 캐시를 오염시킬 수 있다. ARP 캐시가 오염된 호스트들은 IA 또는 IB 로 향하는 트래픽의 목적지 MAC 주소로 MC 를 사용하게 된다. 이것은 호스트 C 가 트래픽을 가로챈다는 것을 의미한다. 호스트 C 는 IA, IB 와 연관된 진짜 MAC 주소를 알고 있기 때문에, 올바른 MAC 주소를 목적지 MAC 주소로 사용해서 가로챈 트래픽을 원래 호스트들에게로 포워딩 forwarding 한다. 호스트 C 는 호스트 A 와 호스트 B 의 트래픽 사이에 자신을 집어 넣게 되고, 이런 현상을 *man-in-the middle attack* 이라 한다.



19.1.3. Understanding DAI and ARP Spoofing Attacks

DAI 는 ARP 패킷을 검사하는 보안 기능이다. DAI 는 유효하지 않은 IP-to-MAC 주소 binding 을 가진 ARP 패킷을 로깅 ^{logging} 하고, 폐기 ^{drop} 한다. 이 기능은 main-in-the-middle attack 으로부터 네트워크를 보호한다.

DAI 는 ARP 테이블이 오직 유효한 ARP request 와 response 에 의해 변경되도록 동작한다. DAI 기능이 활성화된 스위치는 다음과 같이 동작한다:

- untrusted 포트로 수신한 모든 ARP 패킷을 검사한다.
- 자신의 ARP 캐시를 변경하기 전에, 수신한 패킷이 유효한 IP-to-MAC 주소 binding 을 가지고 있는지 검사한다.
- 유효하지 않은 ARP 패킷을 폐기한다.

DAI 는 ARP 패킷의 유효성을 검사할 때, 신뢰할 수 있는 데이터베이스 ^{database} 인 DHCP snooping binding 데이터베이스에 저장된 IP-to-MAC 주소 binding 을 사용한다.

**Note**

스위치와 VLAN 에 DHCP snooping 이 활성화 되어 있을 때, DHCP snooping 에 의해 DHCP snooping binding 데이터베이스가 생성된다.

ARP 패킷을 수신한 인터페이스의 특성에 따라 스위치는 다음과 같이 동작한다:

- trusted 인터페이스로 수신한 ARP 패킷은 검사하지 않는다.
- untrusted 인터페이스에 대해서는 오직 유효한 패킷만 허용한다.

DAI 는 정적으로 할당된 IP 주소를 가진 호스트에 대해서는 운용자가 정의한 ARP access control lists (ACLs)를 사용할 수도 있다. 스위치는 폐기된 패킷에 대해 로그를 남길 수도 있다.

또한 다음과 같은 경우 DAI 가 ARP 패킷을 폐기하도록 설정할 수도 있다:

- 패킷의 IP 주소가 유효하지 않다 – 예를 들어, 0.0.0.0, 255.255.255.255 또는 IP 멀티캐스트 주소.
- ARP 패킷의 body 에 포함된 MAC 주소와 Ethernet 헤더의 주소가 일치하지 않는다.

19.1.4. Interface Trust States and Network Security

DAI 는 스위치의 각 인터페이스에 대한 trust 상태 ^{state} 정보를 유지하고 있다. Trusted 인터페이스를 통해 수신한 패킷에 대해서는 어떤 DAI 검사도 수행하지 않는다. 반면, Untrusted 인터페이스를 통해 수신한 패킷은 DAI 의 검사를 받는다.

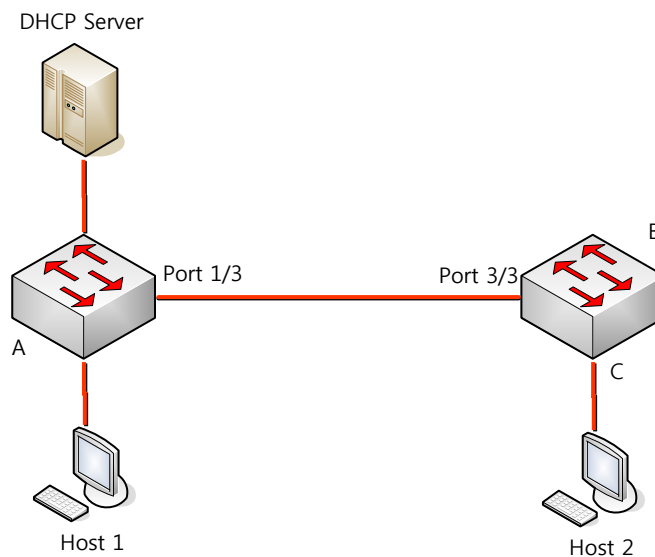
전형적인 네트워크 구성에서, 호스트와 연결된 스위치 포트를 untrusted 로 설정하고 스위치에 연결된 포트는 trusted 로 설정한다. 이런 설정에서, 이 스위치를 통해 네트워크로 유입되는 모든 ARP 패

킷은 보안검사를 받게 된다. VLAN 이나 네트워크의 다른 장소에서 더 이상의 유효성 검사가 필요하지는 않다. trust 설정은 인터페이스 설정 명령인 **ip arp inspection trust** 를 사용하면 된다.



Caution 네트워크 보안을 위해 스위치가 모든 ARP 패킷을 검사하도록 하려면, 특별한 기능이 필요하다. 즉, DAI 가 스위치의 포워딩 엔진 forwarding engine 을 통해 포워딩되는 유니캐스트 ARP 패킷도 검사할 수 있도록 스위치의 CPU 로 trap 할 수 있어야 한다.
유니캐스트 ARP 패킷을 검사하도록 설정하는 방법은 19.4.1 절에서 설명하도록 하겠다.

다음 그림에서 스위치 A 와 스위치 B 에서 호스트 1 과 호스트 2 를 포함하는 VLAN 에 대해 DAI 가 실행 중이라고 가정하자. 호스트 1 과 호스트 2 가 스위치 A 와 연결된 DHCP 서버 server 로부터 IP 주소를 할당 받았다면, 오직 스위치 A 는 호스트 1 에 대한 IP-to-MAC 주소 매핑을 가지고 있다. 그러므로, 스위치 A 와 스위치 B 사이의 인터페이스가 untrusted 라면, 호스트 1 이 전송한 ARP 패킷은 스위치 B 에서 폐기된다. 즉, 호스트 1 과 호스트 2 는 통신을 할 수 없게 된다.



인터페이스를 trusted 로 설정했을 때, 신뢰할 수 없는 장비가 존재한다면 네트워크 보안에 허점이 발생한다. 스위치 A 에서 DAI 를 실행하고 있지 않으면, 호스트 1 은 스위치 B (그리고 스위치 사이의 인터페이스가 trusted 로 설정되어 있다면 호스트 2 까지)의 ARP 캐시를 오염시킬 수 있다. 이런 현상은 스위치 B 에서 DAI 를 실행시키더라도 발생한다.

DAI 가 실행 중인 스위치는 연결된 호스트가 네트워크의 다른 호스트들의 ARP 캐시를 오염시키는 행위를 방지한다. 그러나, DAI 는 DAI 가 실행 중인 다른 네트워크의 호스트의 ARP 캐시를 오염시키는 것을 방지하지는 못한다.

이 경우에 DAI 를 실행 중인 스위치에서는 DAI 를 실행시키지 않는 스위치와 연결된 인터페이스를 untrusted 로 설정하라. 그리고 DAI 가 설정되지 않는 스위치로부터의 packet 을 검사하기 위해 DAI

를 실행중인 스위치에서 ARP ACLs 를 설정하라. 이런 설정이 불가능하다면, Layer 3 에서 DAI 를 사용중인 스위치와 사용하지 않는 스위치를 분리해야 한다.

**Note**

E7500 series 는 DAI 가 모든 ARP 패킷을 검사하는 네트워크를 보호 기능을 제공한다.

19.1.5. Rate Limiting of ARP Packets

DAI 기능이 활성화된 스위치는 CPU 로 유입되는 ARP 패킷의 rate 를 제한한다. 디폴트로 untrusted 인터페이스에 대해서 초당 15 개 (15 pps)의 ARP 패킷만 허용되며, trusted 인터페이스의 rate 는 제한하지 않는다. 인터페이스 설정 명령 `ip arp inspection limit` 를 사용해서 설정을 변경할 수 있다.

특정 포트를 통해 CPU 로 유입되는 ARP 패킷의 rate 가 설정한 값을 초과하면, 스위치는 이 포트로 수신한 모든 ARP 패킷을 폐기한다. 사용자가 설정을 변경할 때까지 이 상태가 유지된다. 인터페이스 설정 명령 `ip arp inspection limit auto-recovery` 를 사용하면, 일정 시간이 경과한 후 포트를 자동으로 서비스 가능 상태로 만들 수 있다.

**Note**

ARP 패킷의 rate limit 는 CPU 에서 software 로 처리되기 때문에, Denial-of-Service (DoS) 공격에 대해 큰 효과를 기대할 수 없다.

19.1.6. Relative Priority of ARP ACLs and DHCP Snooping Entries

DAI 는 IP-to-MAC 주소 매핑을 검사할 때, DHCP snooping binding 데이터베이스를 사용한다.

ARP ACLs 은 DHCP snooping binding 데이터베이스보다 먼저 검사에 사용된다. 스위치는 `ip arp inspection filter` 명령으로 설정이 되었을 경우에만 ACLs 을 사용한다. 스위치는 먼저 사용자가 설정한 ARP ACLs 로 ARP 패킷을 검사한다. 만약 ARP 패킷이 ARP ACLs 의 deny 조건과 일치하면, DHCP snooping 에 의해 유효한 binding 이 존재하더라도 그 패킷은 폐기된다.

19.1.7. Logging of Dropped Packets

스위치는 폐기할 패킷에 대한 정보를 로그 버퍼에 저장하고, 설정된 발생률에 맞춰 시스템 메시지를 생성한다. 메시지가 생성되면 관련된 정보는 로그 버퍼에서 삭제된다. 각각의 로그에는 flow 정보 (수신한 VLAN, port 번호, source 와 destination IP 주소, source 와 destination MAC 주소)가 포함된다.

Global 설정 명령 `ip arp inspection log-buffer` 로 버퍼의 크기를 설정할 수 있으며, 단위 시간 동안

필요한 로그의 개수를 설정해서 시스템 메시지의 생성량을 조절할 수 있다. 그리고, Global 설정 명령 `ip arp inspection vlan logging` 으로 로그할 패킷의 종류를 지정할 수도 있다.

19.2. Default DAI Configuration

다음의 표는 default DAI 설정을 보여준다.

Feature	Default Setting
DAI	모든 VLAN에 대해 비활성 상태이다.
Interface trust state	모든 인터페이스들은 untrusted 상태이다.
Rate limit of incoming ARP packets	초당 15개의 새로운 호스트가 등록되는 Layer 2 네트워크라 가정하고, untrusted 인터페이스에 대해 15 pps로 설정된다. Trusted 인터페이스에 대해서는 rate를 제한하지 않는다. burst interval은 1초이다. 인터페이스의 rate limit 기능은 disable되어 있다.
ARP ACLs for non-DHCP environments	ARP ACLs은 정의되어 있지 않다.
Validation checks	어떤 검사도 수행하지 않는다.
Log buffer	DAI가 활성화되면, deny되거나 drop되는 모든 ARP 패킷 정보가 로깅된다. log entry의 개수는 32개. 생성되는 시스템 메시지의 개수는 초당 5개. logging-rate 주기는 1초.
Per-VLAN logging	deny되거나 drop되는 모든 ARP 패킷이 로깅된다.

19.3. DAI Configuration Guidelines and Restrictions

DAI를 설정할 때, 다음의 사항을 준수하라:

- ✓ DAI는 기본적으로 스위치 자신의 ARP 테이블만 보호한다. 네트워크를 보호하기 위해서는 모든 ARP 패킷을 CPU로 trap할 수 있는 기능이 필요하다.
- ✓ DAI는 입구 보안^{ingress security} 기능이다; 출구 검사^{egress check}에 사용하지 마라.
- ✓ DAI는 DAI를 지원하지 않는 스위치에 연결된 호스트에 대해서는 효과적이지 않다. man-in-the-middle attack은 단일 Layer 2 브로드캐스트 도메인에 제한되기 때문에, DAI를 사용하는 도메인을 그렇지 않은 도메인으로부터 분리하라. 이것은 DAI가 활성화된 도메인에 위치한 호스트의 ARP 테이블을 보호해준다.

- ✓ DAI는 유입된 ARP request와 ARP response 패킷의 IP-to-MAC 주소 binding을 검사하기 위해 DHCP snooping binding 데이터베이스를 사용한다. 동적으로 할당되는 IP 주소에 대한 ARP 패킷을 허용하기 위해서는 반드시 DHCP snooping을 활성화시켜라.
- ✓ DHCP snooping이 비활성 상태이거나 DHCP 환경이 아니라면, 패킷을 permit하거나 deny 하기 위해 ARP ACL을 사용하라.
- ✓ 포트의 특성을 고려해서 ARP 패킷의 rate를 설정하라.

19.4. Configuring DAI

이 절에서는 DAI 를 설정하는 방법에 대해 설명한다:

- Enabling DAI on VLANs (필수)
- Configuring the DAI Interface Trust State (옵션)
- Applying ARP ACLs for DAI Filtering (옵션)
- Configuring ARP Packet Rate Limiting (옵션)
- Enabling DAI Error-Disabled Recovery (옵션)
- Enabling Additional Validation (옵션)
- Configuring DAI Logging (옵션)
- Displaying DAI Information

19.4.1. Enabling DAI on VLANs

VLAN 에 DAI 를 enable 하면, 스위치는 해당 VLAN 을 통해 수신한 다음과 같은 ARP 패킷들을 검사한다:

- 브로드캐스트되는 ARP 패킷
- 스위치의 MAC 주소를 요청하는 ARP request 패킷
- 스위치가 요청한 ARP request 에 대한 응답 패킷
- 단말들 사이에 송수신되는 모든 unicast ARP 패킷

이 패킷들을 검사해서, 유효한 패킷에 대해서만 응답하고 ARP 테이블을 변경한다.

VLAN 에 DAI 를 enable 하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# configure terminal	global 설정 모드로 진입한다.
Switch(config)# ip arp inspection vlan <i>vlan-id</i>	VLAN 에 DAI 를 enable 한다.
Switch(config)# no ip arp inspection vlan <i>vlan-id</i>	VLAN 에 DAI 를 disable 한다.
Switch# show ip arp inspection	설정을 확인한다.



Note VLAN 에 DAI 를 enable 하면, 해당 VLAN 을 통해 송수신 되는 모든 ARP 패킷을 검사한다. 다시 말해, 스위치의 ARP 캐시와 네트워크가 함께 보호된다.

다음의 예는 VLAN 200 에 DAI 를 enable 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 200
```

다음의 예는 설정을 확인하는 방법을 보여준다:

```
Switch# show ip arp inspection
DHCP Snoop Bootstrap      : Disabled
Source MAC Validation     : Disabled
Destination MAC Validation : Disabled
IP Address Validation     : Disabled
ARP Field Validation      : Disabled
```

Vlan	Config	Operation	ACL Match	Static ACL	ACL Log	DHCP Log
200	Enabled	Active+		No	Deny	Deny

유니캐스트 ARP 패킷에 대해 DAI 기능을 사용하도록 할려면 class-map 과 policy-map 을 사용하여 ARP 패킷을 CPU 로 trap 되도록 해야한다.

다음은 Vlan200 에서 수신한 ARP 패킷을 CPU 로 trap 되도록 설정하는 예제이다.

```
Switch(config)#class-map arp_trap_class
Switch(config-cmap)#match ethertype 0806
Switch(config-cmap)#end
Switch#show class-map
```

```
CLASS-MAP-NAME: arp_trap_class (match-all)
Match Ethertype: 0806
```

```
Switch#config terminal
Switch(config)#policy-map arp_trap_map
Switch(config-pmap)#class arp_trap_class
Switch(config-pmap-c)#trap-cpu
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#int vlan200
Switch(config-if-vlan200)#service-policy input dhcp_user_map
```

```
Switch#show policy-map
```

```
POLICY-MAP-NAME: arp_trap_map
State: attached
```

```
CLASS-MAP-NAME: arp_trap_class (match-all)
Trap-cpu
```

```
Switch#show service-policy
```

```
Interface Vlan200 : input dhcp_user_map
```

19.4.2. Configuring the DAI Interface Trust State

스위치는 trusted 인터페이스로부터 수신한 ARP 패킷은 검사하지 않는다.

Untrusted 인터페이스를 통해 수신한 ARP 패킷은 유효한 IP-to-MAC 주소 매핑을 가지고 있는지 검사된다. 스위치는 유효하지 않은 패킷은 폐기하고, **ip arp inspection vlan logging** 설정에 따라 로그 버퍼에 패킷 로그를 저장한다.

인터페이스의 trust 상태를 설정하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# configure terminal	global 설정 모드로 진입한다.
Switch(config)# interface ifname	다른 스위치와 연결된 인터페이스를 명시하고, 인터페이스 설정 모드로 진입한다.
Switch(config-if-Giga1/1/1)# ip arp inspection trust	스위치와 연결된 인터페이스를 trusted 로 설정한다. (default: untrusted)
Switch(config-if-Giga1/1/1)# no ip arp inspection trust	스위치와 연결된 인터페이스를 untrusted 로 설정한다.
Switch(config-if-Giga1/1/1)# end	Enable 모드로 돌아간다.
Switch# show ip arp inspection interfaces	설정을 확인한다.

다음의 예는 Gigabit 포트 1 을 trusted 로 설정하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# interface gi1/1/1
Switch(config-if-Giga1/1/1)# ip arp inspection trust
Switch(config-if-Giga1/1/1)# end
Switch# show ip arp inspection interfaces
Interface      Trust State  Rate (pps)  Burst Interval  Auto Recovery
-----
Giga1/1/1     Trusted      None        1               Disabled
```

19.4.3. Applying ARP ACLs for DAI Filtering

ARP ACL 을 사용하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# configure terminal	global 설정로 진입한다.
Switch(config)# ip arp inspection filter <i>arp_acl_name</i> vlan <i>vlan-id</i> [static]	VLAN 에 ARP ACL 을 적용한다.
Switch(config)# end	Enable 모드로 돌아간다.
Switch# show ip arp inspection	설정을 확인한다.

ARP ACL 을 적용할 때, 다음의 사항에 유의하라:

- ARP ACL 의 implicit deny 를 explicit deny 처럼 다루고 ACL 의 어떤 조건과도 일치하지 않는 패킷을 폐기하려면, **static** 키워드를 사용하라. 이 경우에 DHCP binding 은 사용되지 않는다.
static 키워드를 사용하지 않으면, ACL 에 일치하는 조건이 없는 패킷에 대해서는 DHCP binding 을 사용해서 패킷을 permit 할 것인지 deny 할 것인지를 결정한다.
- IP-to-MAC 주소 매핑을 포함하고 있는 ARP 패킷만 ACL 로 검사한다. Access list 가 permit 하는 패킷들만 permit 된다.

다음의 예는 이름이 example_arp_acl 인 ARP ACL 을 VLAN 200 에 적용하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# ip arp inspection filter example_arp_acl vlan 200
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap      : Disabled
Source MAC Validation     : Disabled
Destination MAC Validation : Disabled
IP Address Validation     : Disabled
ARP Field Validation      : Disabled
```

Vlan	Config	Operation	ACL Match	Static ACL	ACL Log	DHCP Log
200	Enabled	Active	example_arp_acl	No	Deny	Deny

19.4.4. Configuring ARP Packet Rate Limiting

DAI 가 활성화 되면 스위치는 모든 ARP 에 대해 유효성 검사를 하고, 이로 인해 스위치는 ARP 패킷의 DoS 공격에 취약해진다. 스위치의 CPU 에서 ARP 패킷의 rate 를 제한함으로써 CPU 의 부하를 감소시킬 수 있다.



Note DAI 가 제공하는 ARP rate limit 는 소프트웨어 기능이기 때문에, 스위치의 CPU 사용률을 직접적으로 감소시킬 수는 없다. 하지만 DAI 가 처리하는 ARP 패킷의 양을 조절함으로써, DAI 에 의한 CPU 사용률을 낮출 수는 있다.

포트에 대해 ARP 패킷에 대한 rate limit 를 설정하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# configure terminal	global 설정으로 진입한다.
Switch(config)# interface ifname	다른 스위치와 연결된 인터페이스를 명시하고, 인터페이스 설정 모드로 진입한다.
Switch(config-if-Giga1/1/1)# ip arp inspection limit {rate pps [burst interval seconds] none}	(옵션) ARP packet rate limit 를 설정한다.
Switch(config-if-Giga1/1/1)# no ip arp inspection limit	default 설정으로 복원한다.
Switch(config-if-Giga1/1/1)# ip arp inspection limit enable	인터페이스의 ARP rate limit 기능을 enable 시킨다.
Switch(config-if-Giga1/1/1)# no ip arp inspection limit enable	인터페이스의 ARP rate limit 기능을 disable 시킨다.
Switch(config)# end	Enable 모드로 돌아간다.
Switch# show ip arp inspection interfaces	설정을 확인한다.

ARP packet rate limit 를 설정할 때, 다음의 사항에 유의하라:

- 디폴트로 untrusted 인터페이스에 대해서는 15 pps (packet per second), trusted 인터페이스에 대해서는 rate 를 제한하지 않는다.
- **rate pps** 로 초당 처리할 수 있는 상한을 설정한다. 범위는 0 부터 2048 이다.
- **rate none** 키워드는 수신되는 ARP 패킷의 rate 에 제한을 하지 않음을 명시한다.
- (옵션) **burst interval seconds** (default 는 1)는, ARP 패킷의 rate 가 상한을 초과하는지 관측하는 시간이다. 즉, **rate** 로 설정한 값을 **burst interval** 초 동안 초과할 때 해당 포트로 유입되는 ARP 패킷을 제한한다. 값의 범위는 1 ~ 15 이다.
- 유입되는 ARP 패킷의 rate 가 설정 값을 초과하면, 스위치는 해당 포트에 수신한 모든 ARP 패킷을 폐기한다. 운영자가 설정을 변경할 때까지 이 상태가 유지된다.
- 인터페이스의 rate-limit 값을 변경하지 않고, 인터페이스의 trust 상태를 변경해도 인터페이스에 대한 rate-limit 의 default 값이 변경된다. rate-limit 값을 변경한 후에는, trust 상태를 변경하더라도 설정한 값이 그대로 보존된다. 인터페이스 설정 명령 **no ip arp inspection limit** 을 사용하면, 인터페이스의 rate-limit 값은 default 값으로 복원된다.
- **ip arp inspection limit enable** 명령을 설정해야, ARP 패킷 rate limit 가 동작한다.

다음은 gi1/1/1 에 ARP packet rate limit 를 설정하는 예이다:

```
Switch# configure terminal
```

```
Switch(config)# interface gi1/1/1
Switch(config-if-Giga1/1/1)# ip arp inspection limit rate 20 burst interval 2
Switch(config-if-Giga1/1/1)# ip arp inspection limit enable
Switch(config-if-Giga1/1/1)# end
Switch# show ip arp inspection interfaces
```

Interface	Trust State	Rate (pps)	Burst Interval	Auto Recovery
Giga1/1/1	Untrusted	20	2	Disabled

19.4.5. Enabling DAI Error-Disabled Recovery

ARP 패킷에 대한 rate limit 때문에, ARP 패킷의 수신에 제한된 포트를 자동으로 복구하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# configure terminal	global 설정 모드로 진입한다.
Switch(config)# interface ifname	다른 스위치와 연결된 인터페이스를 명시하고, 인터페이스 설정 모드로 진입한다.
Switch(config-if-Giga1/1/1)# ip arp inspection limit auto-recovery seconds	(옵션) 자동 복구 기능을 활성화 시킨다.
Switch(config)# no ip arp inspection limit auto-recovery	자동 복구 기능을 해제한다.
Switch(config)# end	Enable 모드로 돌아간다.
Switch# show ip arp inspection interfaces	설정을 확인한다.

다음은 인터페이스 gi1/1/1 이 ARP rate limit 에 의해 ARP 패킷 수신에 차단되었을 경우, 10 초 후에 자동으로 복구되도록 설정하는 예이다:

```
Switch# configure terminal
Switch(config)# interface gi1/1/2
Switch(config-if-Giga1/1/1)# ip arp inspection limit auto-recovery 10
Switch(config-if-Giga1/1/1)# ip arp inspection limit enable
Switch(config-if-Giga1/1/1)# end
Switch# show ip arp inspection interfaces
```

Interface	Trust State	Rate (pps)	Burst Interval	Auto Recovery
gi1/1/1	Untrusted	20	2	10
gi1/1/2	Untrusted	15	1	Disabled

19.4.6. Enabling Additional Validation

DAI 로 ARP 패킷의 destination MAC 주소, sender 와 target IP 주소, source MAC 주소에 대한 유효성 검사를 할 수 있다.

IP 주소 또는 MAC 주소에 대한 유효성 검사를 하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# configure terminal	global 설정 모드로 진입한다.
Switch(config)# ip arp inspection validate {dst-mac ip src-mac}	(옵션) 추가적인 유효성 검사를 enable 한다. (default: none)
Switch(config)# no ip arp inspection validate {dst-mac ip src-mac}	추가적인 유효성 검사를 disable 한다.
Switch(config)# end	Enable 모드로 돌아간다.
Switch# show ip arp inspection	설정을 확인한다.

추가적인 유효성 검사를 enable 하려면, 다음의 사항에 유의하라:

- 다음의 키워드 중 적어도 하나를 사용해야 한다.
- 각 **ip arp inspection validate** 명령은 이전의 명령을 삭제한다. 만약, **ip arp inspection validate** 명령으로 **src-mac** 와 **dst-mac** 검사를 enable 하고, 두 번째 **ip arp inspection validate** 명령으로 **ip** 검사만을 enable 했다면, **src-mac** 와 **dst-mac** 검사는 disable 되고 **ip** 검사만이 enable 된다.
- 추가적인 유효성 검사는 다음과 같다:
 - **dst-mac** – ARP response 패킷에 대해 Ethernet 헤더의 destination MAC 주소와 ARP body의 target MAC 주소를 비교한다.
 - **ip** – ARP body의 유효하지 않은 IP 주소를 검사한다. 0.0.0.0 또는 255.255.255.255 또는 멀티캐스트 IP 주소는 폐기된다. ARP request의 sender IP 주소, ARP response의 sender/target IP 주소를 검사한다
 - **src-mac** – 모든 ARP 패킷에 대해 Ethernet 헤더의 source MAC 주소와 ARP body의 sender MAC 주소를 비교한다.

다음의 예는 src-mac 에 대한 추가적인 유효성 검사를 enable 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate src-mac
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap      : Disabled
Source MAC Validation      : Enabled
Destination MAC Validation : Disabled
IP Address Validation      : Disabled
ARP Field Validation       : Disabled
```


Vlan	Config	Operation	ACL Match	Static ACL	ACL Log	DHCP Log
200	Enabled	Active		No	Deny	Deny

다음의 예는 dst-mac 에 대한 추가적인 유효성 검사를 enable 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate dst-mac
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap      : Disabled
Source MAC Validation     : Disabled
Destination MAC Validation : Enabled
IP Address Validation     : Disabled
ARP Field Validation      : Disabled
```

Vlan	Config	Operation	ACL Match	Static ACL	ACL Log	DHCP Log
200	Enabled	Active		No	Deny	Deny

다음의 예는 ip 에 대한 추가적인 유효성 검사를 enable 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate ip
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap      : Disabled
Source MAC Validation     : Disabled
Destination MAC Validation : Disabled
IP Address Validation     : Enabled
ARP Field Validation      : Disabled
```

Vlan	Config	Operation	ACL Match	Static ACL	ACL Log	DHCP Log
200	Enabled	Active		No	Deny	Deny

다음의 예는 src-mac 과 dst-mac 에 대한 추가적인 유효성 검사를 enable 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate dst-mac src-mac
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap      : Disabled
Source MAC Validation     : Enabled
Destination MAC Validation : Enabled
IP Address Validation     : Disabled
ARP Field Validation      : Disabled
```

Vlan	Config	Operation	ACL Match	Static ACL	ACL Log	DHCP Log
200	Enabled	Active		No	Deny	Deny

19.4.7. Configuring DAI Logging

이 절에서는 DAI의 로깅(logging)에 대해 설명한다:

- DAI Logging Overview
- Configuring the DAI Logging Buffer Size
- Configuring the DAI Logging System Messages
- Configuring DAI Log Filtering

19.4.7.1. DAI Logging Overview

스위치는 폐기할 패킷에 대한 정보를 로그 버퍼에 저장하고, 설정된 발생률에 맞춰 시스템 메시지를 생성한다. 메시지가 생성되면 관련된 정보는 로그 버퍼에서 삭제된다. 각각의 로그에는 flow 정보(수신한 VLAN, port 번호, source와 destination IP 주소, source와 destination MAC 주소)가 포함된다.

하나의 로그 버퍼 entry는 하나 이상의 패킷에 대한 정보를 표시할 수 있다. 예를 들어, 같은 VLAN에서 같은 ARP 인자(parameter)를 가진 패킷을 동일한 인터페이스를 통해 많이 수신한다면, DAI는 이 패킷에 대한 로그 버퍼 entry를 하나 생성하고, 하나의 시스템 메시지를 생성한다.

19.4.7.2. Configuring the DAI Logging Buffer Size

DAI 로그 버퍼의 크기를 설정하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# configure terminal	global 설정 모드로 진입한다.

Switch(config)# ip arp inspection log-buffer entries <i>number</i>	DAI의 로그 버퍼 크기를 설정한다. (범위는 0 ~ 1024).
Switch(config)# no ip arp inspection log-buffer entries	default 버퍼 크기로 복원한다. (32)
Switch(config)# end	Enable 모드로 돌아간다.
Switch# show ip arp inspection log	설정을 확인한다.

다음의 예는 DAI의 로그 버퍼 크기를 64 개로 설정한다:

```
Switch# configure terminal
Switch(config)# ip arp inspection log-buffer entries 64
Switch(config)# end
Switch# show ip arp inspection log
Total Log Buffer Size: 32
Syslog rate : 5 entries per 1 seconds.
No entries in log buffer.
```

19.4.7.3. Configuring the DAI Logging System Messages

DAI가 생성하는 로그 메시지를 설정하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# configure terminal	global 설정 모드로 진입한다.
Switch(config)# ip arp inspection log-buffer logs <i>number_of_messages</i> interval <i>length_in_seconds</i>	DAI 로그 버퍼를 설정한다.
Switch(config)# no ip arp inspection log-buffer logs	default 로 복원한다.
Switch(config)# end	Enable 모드로 돌아간다.
Switch# show ip arp inspection log	설정을 확인한다.

DAI의 로깅 시스템 메시지를 설정하려면, 다음의 사항에 유의하라:

- **logs** *number_of_messages* (default 는 5) 에서, 값의 범위는 0 ~ 1024 이다. 0 으로 설정하면 로그 메시지가 생성되지 않는다.
- **interval** *length_in_seconds* (default 는 1) 에서, 값의 범위는 0 ~ 86400 초 (1 일)이다. 0 으로 설정하면, 로그 메시지가 바로 생성된다 (즉, 로그 버퍼는 항상 비어있다).
- 시스템 로그 메시지는 *length_in_seconds* 초당 *number_of_messages* 의 비율로 생성된다.

다음의 예는 매 2 초마다 12 개의 DAI 로그 메시지를 생성하도록 설정한다:

```
Switch# configure terminal
```

```
Switch(config)# ip arp inspection log-buffer logs 12 interval 2
Switch(config)# end
Switch# show ip arp inspection log
Total Log Buffer Size: 32
Syslog rate : 12 entries per 2 seconds.
No entries in log buffer.
```

19.4.7.4. Configuring the DAI Log Filtering

ARP 패킷을 검사한 후, 그 결과에 대한 시스템 메시지를 선택적으로 생성할 수 있다.

DAI의 log filtering 기능을 설정하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# configure terminal	global 설정 모드로 진입한다.
Switch(config)# ip arp inspection vlan <i>vlan-id</i> { acl-match { matchlog none } dhcp- bindings { all none permit }}	각 VLAN에 대해 log filtering을 설정한다.
Switch(config)# end	Enable 모드로 돌아간다.
Switch# show running-config	설정을 확인한다.

DAI의 로깅 시스템 메시지를 설정하려면, 다음과 같은 사항에 유의하라:

- Default로 모든 deny되는 패킷은 로깅된다.
- **acl-match matchlog** — ACL 설정을 기반으로 로깅한다. 이 명령에 **matchlog** 키워드를 명시했고, ARP access-list 설정의 **permit** 또는 **deny** 명령에 **log** 키워드가 사용되었다면, ACL에 의해 permit되거나 deny되는 ARP 패킷들이 로깅된다.
- **acl-match none** — ACL과 일치하는 패킷에 대해 로깅하지 않는다.
- **dhcp-bindings all** — DHCP binding과 일치하는 모든 패킷들을 로깅한다.
- **dhcp-bindings none** — DHCP binding과 일치하는 패킷들을 로깅하지 않는다.
- **dhcp-bindings permit** — DHCP binding에 의해 허용된 패킷들을 로깅한다.

다음의 예는 VLAN 200에 대해 ACL과 일치하는 패킷에 대한 로그 메시지를 생성하지 않도록 설정한다:

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 200 logging acl-match none
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap      : Disabled
Source MAC Validation     : Disabled
Destination MAC Validation : Disabled
IP Address Validation     : Disabled
```

ARP Field Validation : Disabled

Vlan	Config	Operation	ACL Match	Static ACL	ACL Log	DHCP Log
200	Enabled	Active		No	None	Deny

19.4.8. Displaying DAI Information

DAI의 정보를 조회하려면, 다음의 명령을 사용하라:

Command	Description
show arp access-list	ARP ACL에 대한 정보를 출력한다.
show ip arp inspection interfaces	인터페이스의 trust 상태 정보를 출력한다.
show ip arp inspection vlan [vlan-id]	VLAN에 대한 DAI 설정과 동작 상태 정보를 출력한다.
show ip arp inspection arp-rate	인터페이스의 ARP 패킷 수신 rate 정보를 출력한다.

DAI 통계정보를 조회하거나 초기화하려면, 다음의 명령을 사용하라:

Command	Description
clear ip arp inspection statistics	DAI 통계 정보를 초기화 한다.
show ip arp inspection statistics [vlan vlan-id]	DAI가 처리한 ARP 패킷에 대한 통계정보를 출력한다.

DAI logging 정보를 조회하거나 초기화하려면, 다음의 명령을 사용하라:

Command	Description
clear ip arp inspection log	DAI 로그 버퍼를 초기화 한다.
show ip arp inspection log	DAI 로그 버퍼의 설정과 로그 버퍼의 내용을 출력한다.

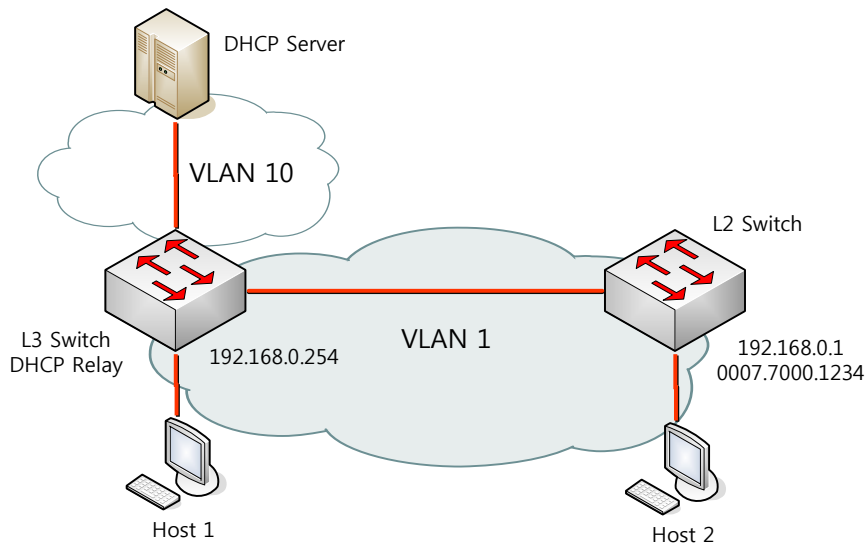
19.5. DAI Configuration Samples

이 절은 다음과 같은 예제들을 포함한다:

- Sample One: Interoperate with DHCP Relay
- Sample Two: Interoperate with DHCP Server

19.5.1. Sample: Interoperate with DHCP Relay

이 예제는 DHCP relay 기능을 사용하는 스위치에 DAI 를 설정하는 방법을 설명한다. 다음의 그림처럼 네트워크가 구성되어 있다고 가정하자:



L3 스위치는 VLAN 10 을 통해 DHCP 서버로 DHCP 메시지를 중계하며, 호스트 또는 L2 스위치가 연결된다. L3 스위치에 연결된 L2 스위치는 고정 IP 주소를 사용한다. 호스트 1 과 호스트 2 는 DHCP 를 통해 IP 주소를 할당 받는다. 그리고 모든 스위치와 호스트들은 VLAN 1 에 위치한다.



Note 이런 구성에서 DAI 는 IP-to-MAC binding 정보를 전적으로 DHCP snooping binding 정보에 의존한다. DHCP snooping 설정은 DHCP snooping 매뉴얼을 참고하라.

DHCP relay 로 사용되는 스위치에서 DAI 기능을 사용하려면, 다음과 같이 설정한다:

Step 1 DHCP relay 기능을 활성화 시킨다.

```
Switch# configure terminal
Switch(config)# ip dhcp helper-address 10.1.1.1
Switch(config)# service dhcp relay
```

Step 2 DHCP 로 IP 를 할당 받는 호스트의 IP-to-MAC binding 정보를 구축하기 위해, DHCP server 와의 통신에 사용되는 인터페이스 VLAN 10 과 호스트가 연결된 인터페이스 VLAN 1 에 DHCP snooping 을 활성화 시킨다.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 1
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping
```

Step 3 고정 IP 를 사용하는 스위치의 ARP 패킷을 허용하기 위해 ARP ACL 을 설정한다.

```
Switch# configure terminal
Switch(config)# arp access-list permit-switch
Switch(config-arp-nacl)# permit ip host 192.168.0.1 mac host 0007.7000.1234
Switch(config-arp-nacl)# exit
Switch(config)# ip arp inspection filter permit-switch vlan 1
Switch(config)# end
```

올바르게 설정되었는지 확인한다.

```
Switch# show ip arp inspection vlan 1
```

Step 4 호스트가 연결된 VLAN 1 에 DAI 를 활성화 시킨다.

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 1
Switch(config)# end
```

올바르게 설정되었는지 확인한다.

```
Switch# show ip arp inspection vlan 1
```

L3 스위치의 설정을 조회하면 다음과 같다.

```
!
arp access-list permit-switch
  permit ip host 192.168.0.1 mac host 0007.7000.1234
!
ip arp inspection vlan 1
ip arp inspection filter permit-switch vlan 1
!
ip dhcp helper-address 10.1.1.1
service dhcp relay
!
ip dhcp snooping vlan 1
ip dhcp snooping vlan 10
ip dhcp snooping
!
```

20

Netflow

20.1. Netflow overview

20.1.1. Netflow 소개

Netflow 기능은 network 를 사용하는 network application(eg. ftp / http / IPTV 등)별로 network traffic 의 사용규모와 시간등의 data 를 수집하고 배포하는 기능이다. 구체적으로 다음과 같은 용도로 사용될 수 있다.

- Network Monitoring - Netflow 는 real time 에 근접한 시간차로 network switch / router 를 통과 하는 traffic 의 data 를 배포할수 있고 배포된 Netflow data 를 사용하는 응용프로그램은 traffic pattern 을 표, 그래프등으로 사용자에게 보여줄 수 있다.
- Application Monitoring and Profiling - Netflow data 는 개개 network application 별로 사용중인 network 자원 사용량의 변화를 시간순서로 묘사할 수 있다. 이러한 특성은 새로운 service 를 계획하거나 network 자원(ex. switch/router 등의 배치), application 자원(ex. WEB server 의 배치규모)을 고객의 요구에 맞춰서 배치하는데에 사용할 수 있다.
- User Monitoring and Profiling - Netflow 를 사용하여 customer 또는 user 가 사용하는 network 와 application 자원에 대한 구체적인 정보를 획득할수 있다. 이러한 정보는 network 와 application 자원의 배치를 결정하는데에 사용될 수 있고, 잠재적인 보안 위협요소에 대한 발견과 해결에도 사용될 수 있다.
- Network Planning - Netflow 를 사용하면 network 를 흐르는 traffic 에 대한 장기간의 data 를 얻을수 있고, 이런 장기적인 data 는 network 규모가 성장하는 것을 추적하고 예측하는데에 유용하다. 이는 routing 장비의 숫자, 장비내 port/interface 의 성능또는 개수등 network infrastructure 에 대한 upgrade 를 계획하는데에 사용될 수있다.
- Accounting/Billing - 상세한 자원사용 통계를 제공하기위해 Netflow 를 사용하면 IP, TCP/UDP port, bytes, packets 등의 항목별로 계측이 가능하다. ISP 는 이러한 통계를 사용하여 일일사용시간, bandwidth 사용, 사용 application 등을 근거로하는 과금측정을 할 수 있다.

20.2. Netflow overview

20.2.1. Netflow 소개

Netflow 기능은 network 를 사용하는 network application(eg. ftp / http / IPTV 등)별로 network traffic 의 사용규모와 시간등의 data 를 수집하고 배포하는 기능이다. 구체적으로 다음과 같은 용도로 사용될 수 있다.

- Network Monitoring - Netflow 는 real time 에 근접한 시간차로 network switch / router 를 통과 하는 traffic 의 data 를 배포할수 있고 배포된 Netflow data 를 사용하는 응용프로그램은 traffic pattern 을 표, 그래프등으로 사용자에게 보여줄 수 있다.
- Application Monitoring and Profiling - Netflow data 는 개개 network application 별로 사용중인 network 자원 사용량의 변화를 시간순서로 묘사할 수 있다. 이러한 특성은 새로운 service 를 계획하거나 network 자원(ex. switch/router 등의 배치), application 자원(ex. WEB server 의 배치규모)을 고객의 요구에 맞춰서 배치하는데에 사용할 수 있다.
- User Monitoring and Profiling - Netflow 를 사용하여 customer 또는 user 가 사용하는 network 와 application 자원에 대한 구체적인 정보를 획득할수 있다. 이러한 정보는 network 와 application 자원의 배치를 결정하는데에 사용될 수 있고, 잠재적인 보안 위협요소에 대한 발견과 해결에도 사용될 수 있다.
- Network Planning - Netflow 를 사용하면 network 를 흐르는 traffic 에 대한 장기간의 data 를 얻을수 있고, 이런 장기적인 data 는 network 규모가 성장하는 것을 추적하고 예측하는데에 유용하다. 이는 routing 장비의 숫자, 장비내 port/interface 의 성능또는 개수등 network infrastructure 에 대한 upgrade 를 계획하는데에 사용될 수있다.
- Accounting/Billing - 상세한 자원사용 통계를 제공하기위해 Netflow 를 사용하면 IP, TCP/UDP port, bytes, packets 등의 항목별로 계측이 가능하다. ISP 는 이러한 통계를 사용하여 일일사용시간, bandwidth 사용, 사용 application 등을 근거로하는 과금측정을 할 수 있다.

20.2.2. Netflow deployment

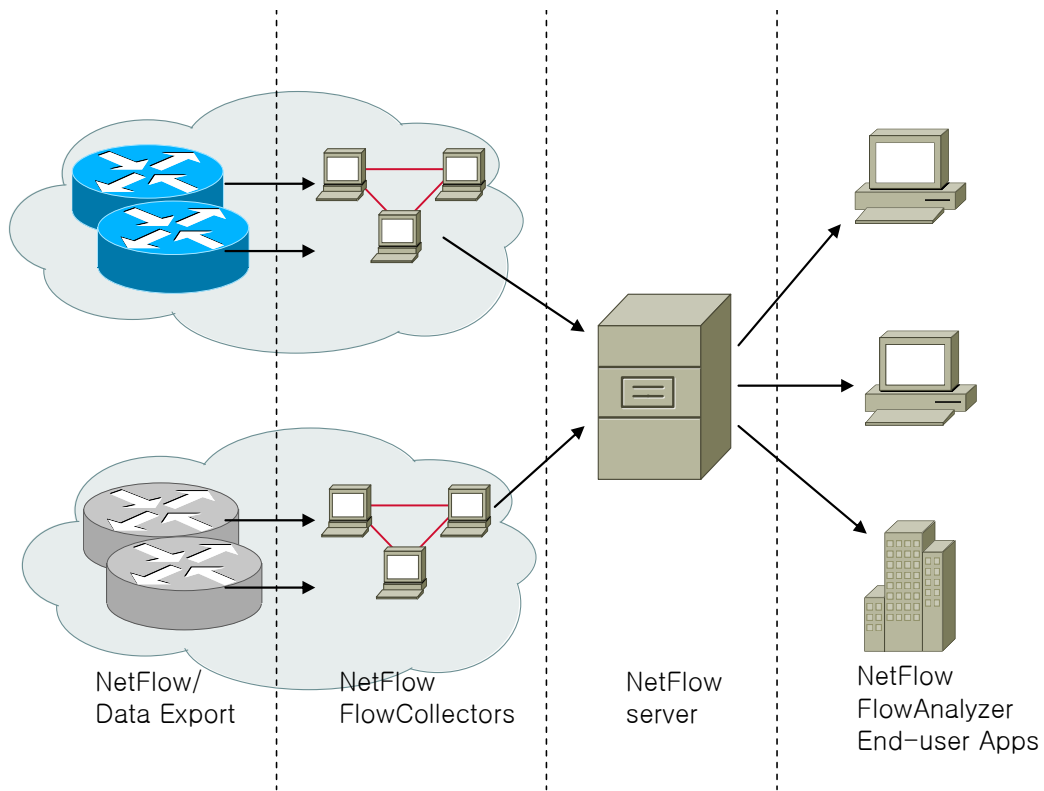


그림 20-1 Netflow deployment

Netflow 는 실제 배치시 다음의 세가지 구성 요소를 필요로 한다.

- **Netflow Exporter:** Netflow data 를 수집하고 이를 collector 로 전송한다. 그림에서 *Netflow Data Export* 로 표시된 항목이며 주로 *routing device* 가 이 역할을 맡지만 *network application server* 에 직접배치하기도 한다.
- **Netflow Collector:** Exporter 로부터 전송받은 Netflow data 를 수신하여 물리적인 저장장치에 저장하거나 또다른 collector 또는 Netflow Analyzer 로 전송한다. 그림에서 *Netflow Flow Collectors, Netflow Server* 로 표시된 항목이다.
- **Netflow Analyzer:** Collector 가 저장한 data 를 가공하여 사용자가 볼수있게한다.

20.2.3. Netflow flow

일정시간동안 수집된 특정한 IP packet 들의 집합을 flow(또는 IP flow)라 정의한다. flow 는 packet 의 IP, UDP/TCP Port 등의 요소로 구분될 수 있으며 같은 flow 에 속한 IP packet 들은 서로간에 공통적인 요소를 가진다. Netflow exporter 는 flow 의 생성/삭제/검색을 통해 Netflow data 를 관리하고 Netflow collector 로 전송한다.

flow 는 Netflow exporter 에서 생성된 이후 폐기될 수 있으며 폐기된 flow 에 한해 Netflow collector 로 전송된다. flow 는 다음과 같은 경우 Netflow exporter 로부터 폐기된다.

- exporter 가 flow 가 끝났음을 (즉 더이상 이 flow 에 해당하는 packet 이 수집되지않을 것을) 감지 할수 있을때. 예를 들자면 TCP packet 의 FIN 또는 RST bit 를 통해 TCP connection 이 종료되었음을 감지했을때 이에 해당되는 flow 가 끝났다고 판단하여 flow 를 폐기한다.
- flow 가 일정시간동안 inactive 되었을때 (즉 일정시간동안 flow 에 해당하는 packet 이 수집되지않을때)
- flow 가 일정시간이상 지속되었을때 (즉 일정시간이상 flow 에 해당하는 packet 이 계속 수집되었을때)
- Netflow exporter 의 한계상 더이상 flow 를 유지할수 없을때. 예를 들자면 Netflow exporter 시스템의 memory 가 부족하거나 byte 또는 packet 수를 세는 counter 의 표현한계에 도달했을 때.

20.2.4. Netflow packet

Netflow 는 version 에 따라 Netflow exporter 에서 Netflow collector 로 Netflow data 를 전송하는 packet 의 format 이 다르다. 여기서는 E7500 에서 Netflow V5 의 전송 format 을 소개한다.

IP header
UDP header
Netflow header
Flow record
Flow record
...
Flow record

그림 20-2 Netflow V5 packet format

Netflow V5 는 UDP 를 전송 protocol 로 사용하며 header field 이후로 Netflow collector 로 전송될 flow(flow record)가 삽입된다. 각 flow record 는 다음과 같은 내용을 가지고 있다.

source IP
destination IP
next hop IP
flow 를 RX 하는 interface 의 SNMP index

flow 를 TX 하는 interface 의 SNMP index
flow 의 누적 packet 수
flow 의 누적 byte 수
flow 생성시간
마지막으로 flow 에 해당하는 packet 을 받은시간
TCP/UDP source port
TCP/UDP destination port
TCP flag
IP Protocol type
IP TOS(TypeOfService)
source AS 번호
destination AS 번호
source address pfeix mask bits
destination address pfeix mask bits

표 20-1 Netflow V5 record 내용

20.3. E7500 Netflow

20.3.1. requirement 및 특성

E7500 의 Netflow 기능은 Netflow processing engine(이하 NP)를 장착해야만 사용할 수 있다. NP 는 routing 과정에 개입하지 않으며 E7500 의 routing engine(이하 PFE)과는 분리되어있다. 따라서 Netflow 기능을 enable 하는것이 routing 될 packet 의 drop 으로 이어지지는 않는다.

20.3.2. flow 생성

NP 는 PFE 을 통해 routing 된 packet 을 수집하여 flow 로 분류하고 이를 flow table 에 저장한다. E7500 Netflow 는 수집한 packet 을 flow 로 분류하기 위해 packet 에서 다음의 5 가지 field 를 검사한다.

- source IP
- destination IP
- source PORT
- destination PORT
- IP header 의 protocol field

위 5 가지 field 를 key field 라 하고 key field 가 같은 packet 은 동일한 flow 로 분류된다. E7500 Netflow 는 transport layer protol 로 UDP/TCP/ICMP 를 지원한다 ICMP 의 경우 source/destination PORT 대신 ICMP type 을 사용하여 packet 이 속한 flow 를 구분하며 그외의 transport layer protocol 의 경우 PORT 를 사용하지 않고 flow 를 구분한다.

20.3.3. flow 폐기

NP 는 주기적으로 flow table 을 점검하여 폐기되어야할 flow 를 검사하며 폐기된 flow 에 한해 Netflow

collector 로 전송될 수 있으며 Netflow data 를 전송할 collector 가 없을경우 폐기된 flow 는 바로 삭제된다. 다음의 경우에 NP 는 flow 를 폐기한다.

- long aging time 이 지났을 경우, long aging time 은 flow 가 flow table 에 존재할 수 있는 최대 시간을 의미한다.
- normal aging time 이 지났을 경우, normal aging time 은 flow 가 update 되지않고(즉 flow 에 해당하는 packet 을 NP 가 더이상 수집할 수 없을때) flow table 에 존재할 수 있는 최대시간을 의미한다.
- TCP flow 의 경우 TCP connection 이 끊겼을때.
- flow 의 누적 byte 수가 2G 를 넘을때



Notice

Netflow v5 packet 의 dOctet 이 4byte 이므로 이를 사용하여 표현할 수 있는 정수 최대값:4giga byte 가 되기전에 flow 가 폐기되어야 한다.

20.3.4. 제한사항

E7500 Netflow 는 다음과 같은 제한사항을 가진다.

- PFE 를 통해 routing 된 packet 에 한해서만 수집할 수 있다.
- IPv4 packet 만 수집할 수 있다.
- interface 에서 TX 되는 packet 은 수집할 수 없다.
- Netflow collector 로 통계 data 전송시 Netflow v5 protocol 만을 지원한다.
- Netflow 기능 enable 시 port mirroring 기능은 사용할 수 없다.

20.3.5. E7500 Default Netflow configuration

항목	Default
PFE 에서 routing 된 IP traffic 통계 data 수집	Disable
Sampled Netflow	1Gigabit module: Disable
	10Gigabit module : 1/30
Netflow collector 로 통계 data 를 전송	Disabled

20.4. Netflow traffic 통계 data 수집설정

20.4.1. Netflow traffic 통계 data 수집설정 명령어 요약

명령어	설명
mls netflow	IP traffic 통계 data 수집 enable
ip flow ingress	interface 를 통해 RX 되는 IP packet 에 대한 통계 data 수집 enable

mls aging	flow 의 aging out 시간을 설정
flow-sampler module	각 module 별로 sampling rate 를 설정.

20.4.2. Netflow traffic 통계 data 수집 enable

명령어	설명
Router(config)# mls netflow	IP traffic 통계 data 수집 enable
Router(config)# no mls netflow	IP traffic 통계 data 수집 disable
Router(config-if-<interface>)# ip flow ingress	interface 에서 IP traffic 통계 data 수집 enable
Router(config-if-<interface>)# no ip flow ingress	interface 에서 IP traffic 통계 data 수집 disable

E7500 에서 IP traffic 통계 data 를 수집하려면 'mls netflow'명령을 사용하여 Netflow 기능을 enable 하는 것 이외에도 수집할 traffic 의 ingress 방향 interface 에서 'ip flow ingress'명령을 사용하여 NP 가 이 interface 를 통해 RX 되는 packet 을 볼수있게 설정해야 한다.

E7500 Netflow 는 PFE 를 통해 routing 되는 packet 에 대해서만 통계 data 를 수집할 수 있으므로 'ip flow ingress' 명령은 IP 가 설정된 interface 에서만 사용되어야 한다.

20.4.3. Flow aging out 시간 설정

flow 숫자가 NP 가 관리할 수 없을 정도로 늘어나는 것을 막고 flow 의 누적 byte 값과 같이 NP 가 표현할 수 있는 한계가 있는 통계값이 한계치 이상으로 늘어나는 것을 막기 위해 flow 는 생성되고 일정시간 후에는 폐기되어야 하며 폐기된 flow 는 Netflow collector 로 전송될 수 있고 NP 로부터 삭제될 수 있다. aging out 시간은 NP 가 flow 의 폐기여부를 결정하는데 사용되며 다음의 두가지 종류가 있다.

종류	설명
normal	normal aging out 시간동안 flow 에 속하는 packet 을 NP 가 보지못하면 이 flow 는 폐기된다.
long	long aging out 시간 이상 NP 에 존재한 flow 는 폐기된다.

long aging out 이 normal aging out 보다 우선된다. 즉 normal aging out 시간이 지나지 않았더라도 long aging out 시간이 지났다면 flow 는 폐기된다.

aging out 을 설정하기 위해 다음의 명령을 사용한다.

명령어	설명
Router(config)# mls aging {long 64-1920 normal 32-4092}	flow 의 aging out 시간을 설정 long aging default: 1920 초 normal aging default: 600 초
Router(config)# no mls aging {long normal}	flow 의 aging out 시간을 default 값으로 되돌린다.

NP의 성능상 한계때문에 flow가 aging out된 후로 NP가 실제로 flow를 폐기하게 될때까지의 시간은 약간의 오차가 있으며 최대 10초의 오차값을 가진다.

aging out 시간 설정 상태를 조회하기 위해 아래의 명령을 사용할 수 있다.

명령어	설명
Router# show mls netflow aging	flow의 aging out 시간을 표시

```
Router#show mls netflow aging
                enable  timeout  packet threshold
                -----  -
normal aging    true     600      N/A
long aging      true     1920    N/A
```

20.4.4. 최대 flow 개수 지정

NP가 저장하고 있는 flow 수에는 제한이 있다. 사용자가 설정한 flow 수 이상으로는 flow가 생성되지 않으며 NP에서 수집된 packet은 즉시버려진다.

명령어	설명
Router(config) # mls netflow maximum-flows <1024-524288>	최대 flow 개수를 설정 default는 524288 개이다.
Router(config) # no mls netflow maximum-flows	최대 flow 개수를 default로 되돌린다.

20.4.5. Sampled Netflow 기능 설정

수십만개의 flow가 높은 rate으로 forwarding되는 장비에서 interface로 들어오는 packet을 특정 flow로 분류하고 flow별로 aging out 여부를 주기적으로 check하는것은 상당히 부하가 큰작업이다. E7500은 통계 data를 수집하는 NP와 packet forwarding을 처리하는 PFE가 분리되어있어 통계 data수집의 부하가 큰 traffic을 수집하는것이 forwarding되어야 할 packet의 drop으로 이어지지는 않지만, NP에서는 많은 수의 packet이 통계 data에 반영되지 못하고 무작위적으로 drop되므로 통계 data가 traffic의 양상을 정확히 반영하지 못하게 된다.

E7500 Netflow는 module별로 module에 속한 interface로 들어오는 packet N개중 하나만 선택하는 방식으로 interface로 들어오는 packet중 일부에 대해서만 통계 data를 수집하도록 할 수 있다.이 경우 일정한 비율로 packet이 NP의 통계 data에 반영되므로 통계 data가 실제 traffic의 양상을 반영할 수 있다.

명령어	설명
Router(config) # flow-sampler module <module 번호> mode random one-out-of <1-2047>	module별로 sampling rate을 설정한다. module 번호: sampling rate를 지정할 모듈의 번호 1Gigabit module default sampint rate: 1/1

	10Gigabit module default sampint rate: 1/30
Router(config) # no flow-sampler module <module 번호>	module 별 sampling rate 를 default 로 되돌린다.

20.5. Netflow traffic 통계 data 조회

20.5.1. Netflow traffic 통계 data 조회 명령어 요약

명령어	설명
show mls netflow ip	flow 를 조회
show mls netflow ip count	flow 숫자를 조회
clear mls netflow ip	flow 를 즉시 폐기

20.5.2. flow 조회 명령

명령어	설명
show mls netflow ip [detail] [nowrap] [LINE]	NP 내의 폐기되지 않은 flow 를 조회한다. detail: 다음의 추가적인 정보를 표시한다. <ul style="list-style-type: none"> ● output interface (SNMP interface index) ● source/destination AS number ● next hop address ● source/destination MASK ● TCP FIN/RST flag nowrap: 정보출력시 자동 줄바꿈을 하지않는다. LINE: bpf filter, tcpdump 에서 사용하는 bpf filter syntax 를 명시하면 filter 에 match 되는 flow 만 출력할 수있다. (자세한 bpf filter 문법은 tcpdump 매뉴얼을 참조)
show mls netflow ip [detail] [nowrap] [LINE]	NP 내의 폐기되지 않은 flow 의 숫자를 조회한다. LINE: bpf filter, tcpdump 에서 사용하는 bpf filter syntax 를 명시하면 filter 에 match 되는 flow 의 숫자만 센다.

20.2.1.2->10.2.1.2 UDP (1000 -> 1003~1007) 5 개의 flow 에 대한 조회화면이다.

```
Router# show mls netflow ip
DstIP      SrcIP      Prot:SrcPort:DstPort  Src i/f
-----
Pkts      Bytes      Age  LastSeen
-----
20.2.1.2  10.2.1.2   udp :1000 :1003  1101
920752    47879104  63   2010-02-08T14:08:11
```



```

20.2.1.2 10.2.1.2 udp :1000 :1004 1101
921432 47914464 63 2010-02-08T14:08:11
20.2.1.2 10.2.1.2 udp :1000 :1005 1101
921957 47941764 63 2010-02-08T14:08:11
20.2.1.2 10.2.1.2 udp :1000 :1006 1101
922770 47984040 63 2010-02-08T14:08:12
20.2.1.2 10.2.1.2 udp :1000 :1007 1101
923127 48002604 63 2010-02-08T14:08:12
    
```

```

Router# show mls netflow ip detail
DstIP      SrcIP      Prot:SrcPort:DstPort  Src i/f
-----
Pkts      Bytes     Age  LastSeen
-----
Out i/f    Src AS Dst AS Nh Addr      Src Mask Dst Mask FIN/RST
-----+-----+-----+-----+-----+-----+-----+
20.2.1.2  10.2.1.2  udp :1000 :1003 1101
108269    5629988  7   2010-02-08T14:09:26
1102      0 0 0.0.0.0  16 16 0
20.2.1.2  10.2.1.2  udp :1000 :1004 1101
108950    5665400  7   2010-02-08T14:09:26
1102      0 0 0.0.0.0  16 16 0
20.2.1.2  10.2.1.2  udp :1000 :1005 1101
109474    5692648  7   2010-02-08T14:09:26
1102      0 0 0.0.0.0  16 16 0
20.2.1.2  10.2.1.2  udp :1000 :1006 1101
110263    5733676  7   2010-02-08T14:09:26
1102      0 0 0.0.0.0  16 16 0
20.2.1.2  10.2.1.2  udp :1000 :1007 1101
110624    5752448  7   2010-02-08T14:09:26
1102      0 0 0.0.0.0  16 16 0
    
```

destination port 1005 인 flow 만 표시하게 하였다.

```

Router# show mls netflow ip detail dst port 1005
DstIP      SrcIP      Prot:SrcPort:DstPort  Src i/f
-----
Pkts      Bytes     Age  LastSeen
-----
Out i/f    Src AS Dst AS Nh Addr      Src Mask Dst Mask FIN/RST
-----+-----+-----+-----+-----+-----+
20.2.1.2  10.2.1.2  udp :1000 :1005 1101
205363    10678876 14  2010-02-08T14:12:48
1102      0 0 0.0.0.0  16 16 0
    
```

flow 숫자를 조회하는 예이다

```

Router# show mls netflow ip count
Number of shortcuts = 5
    
```

```
Router# show mls netflow ip count dst port 1005
Number of shortcuts = 1
```

20.5.3. flow 폐기명령

명령어	설명
Router# clear mls netflow ip	전체 flow 를 즉시 폐기

20.6. Netflow traffic 통계 data 전송 설정

flow 가 폐기되고 통계 data 를 전송할 Netflow collector 가 설정되어있다면 flow 는 Netflow collector 로 전송된다. E7500 은 Netflow v5 packet 을 전송에 사용한다.

20.6.1. Netflow traffic 통계 data 전송설정 명령어 요약

명령어	설명
mls nde sender	Netflow traffic 통계 data 전송 enable
ip flow-export destination	Netflow collector 를 설정
ip flow-export source	통계 data 전송시 사용할 source interface 지정.

20.6.2. Netflow traffic 통계 data 전송 enable

명령어	설명
Router(config)# mls nde sender	Netflow traffic 통계 data 전송 enable
Router(config)# no mls sender	Netflow traffic 통계 data 전송 disable

20.6.3. Netflow traffic 통계 data 전송대상 설정

명령어	설명
Router(config)# ip flow-export destination A.B.C.D <1-65535>	Netflow traffic 통계 data 를 전송받을 Netflow collector 의 IP, UDP PORT 를 설정한다. 최대 2 개까지 설정할 수 있다.
Router(config)# no ip flow-export destination A.B.C.D <1-65535>	Netflow collector 를 통계 data 전송대상에서 제외

20.6.4. 통계 data 전송시 사용할 source interface 지정

E7500 Netflow 는 보안을 위해 통계 data 를 전송하는 interface 를 변경할 수 있다.

명령어	설명
-----	----

Router(config)# ip flow-export source <i>IFNAME</i>	Netflow traffic 통계 data 를 전송하는 packet 의 source IP 를 지정된 interface 의 IP 로 변경한다.
Router(config)# no ip flow-export source	Netflow traffic 통계 data 를 전송하는 packet 의 source IP 로 Netflow collector 와 연결된 interface 의 IP 를 사용하도록 한다.

20.6.5. Netflow traffic 통계 data 전송설정 조회

명령어	설명
Router(config)# show mls nde	Netflow traffic 통계 data 전송설정 조회

```
Router#show mls nde
Netflow Data Export enabled
Exporting flows to 30.2.1.2 (55555) 40.2.1.2 (33333)
Exporting flows from Loopback0
Version: 5
Total Netflow Data Export Packets are:
    8 packets, 10 records
Total Netflow Data Export Send Errors:
    0 packets, 0 records dropped
Total Netflow Data Export Packets are:
    8 packets, 10 records
Total Netflow Data Export Send Errors:
    0 packets, 0 records dropped
```

21

QoS 및 ACL

본 장은 현재 운영중인 E7500 Series 스위치의 QoS (Quality of Service) 설정 및 ACL (access-list) 설정에 대해서 다룬다.

21.1. QoS

21.1.1. 전역 설정

본 장비의 qos 에 대한 전역 설정을 활성화 시키는 명령어는 다음과 같다.

표 21-1. QoS 전역 설정 명령어

명령어	설명	모드
mls qos	QoS 전역 설정을 활성화 한다.	Config
no mls qos	QoS 전역 설정을 비활성화 한다.	Config
show mls qos	QoS 전역 설정 상태를 조회한다	Exec

E7500 장비의 QoS 관련 설정은 위의 전역 설정이 되어 있다는 것을 기본 전제하에 동작한다. Mls qos 가 활성화 되어 있지 않은 경우 대부분의 QoS 관련 명령어는 설정이 불가능하다.

21.1.2. TX Scheduling 설정

E7500 Series 스위치에서는 Scheduling 을 위해 SPQ (Strict Priority Queue) Method 와 WRR (Weighted Round Robin) Method 를 제공하며 디폴트는 SPQ 이다. 이 둘은 서로 혼재해서 사용하는 것이 가능하며, 2 개의 WRR 그룹을 가져서 이들 사이에서의 우선 순위도 가진다.

이 장비에서 제공되는 WRR 은 정확하게는 SDWRR (Shaped Deficit Weighted Round Robin) Method

이다. DWRR 은 일반 WRR 에서 quota 관리를 더 해주는 방식으로 동작하며, 이를 통해서 꾸준히 들어 오는 트래픽과, burst 하게 몰려 들어 오는 트래픽의 데이터량을 조절해주는 기능을 포함한다. SDWRR 은 여기에 데이터의 흐름에 latency 를 줄이기 위한 shaping 기능이 포함된다. 5:3 비율로 2 개의 queue 에 weight 가 주어졌다고 할 때, WRR (혹은 DWRR) 은 1,1,1,1,1,0,0,0, 1,1,1,1,1,0,0,0 순서로 queue 배분이 이루어진다면, SDWRR 를 쓰는 경우에는 1,0,1,0,1,0,1,1, 1,0,1,0,1,0,1,1 순서로 queue 배분이 이루어지면서 weight 에 따라 패킷양을 조절함과 동시에 트래픽의 latency 도 줄이도록 노력한다.

각 포트는 모두 8 개의 queue 를 가지고 있으며 7 번 큐가 가장 높은 우선순위를 가지고, 0 번 큐가 가장 낮은 우선 순위를 가진다.

Queue 7	SPQ
Queue 6	SPQ
Queue 5	WRR group 1 (50)
Queue 4	WRR group 1 (30)
Queue 3	WRR group 1 (20)
Queue 2	WRR group 2 (60)
Queue 1	WRR group 2 (40)
Queue 0	SPQ

위의 표는 큐 별 스케줄링에 대해서 한가지 예시를 적용한 것이다.

- Q7 과 Q6 은 SPQ 로 설정되었다. Q7 은 가장 높은 우선순위이며 동시에 SPQ 이므로, 모든 트래픽중 가장 높은 우선순위로 처리된다. 그다음으로 Q6 이 처리된다.
- Q5,4,3 은 WRR group 1 으로 설정되어 있으며 각각의 weight 은 50:30:20 으로 분배되었다. WRR group 1 은 SPQ 보다 우선순위가 낮지만, WRR group 2 보다는 높으며 이 둘 사이에는 SPQ 와 마찬가지로 절대적인 우선순위 차이를 가진다.
- Q2,1 은 WRR group 2 로 설정되어 있으며, 이 둘 사이에는 60:40 의 weight 배분을 가진다. WRR group 2 는 위의 모든 큐에서 데이터가 처리된 후에나 처리된다.
- Q0 은 SPQ 로 선언되었지만, 제일 낮은 우선순위를 가진다, Q7~1 의 모든 큐가 처리되어야만 Q0 이 동작한다.



Notice

2 개의 WRR group 을 섞어서 사용하거나 (예: Q5 와 Q2 에 WRR1 을 설정하고, Q4 와 Q1 에 WRR2 를 설정하여 사용하는 경우) WRR group 사이 또는 더 낮은 큐에 SPQ 를 사용하는 것은 권장사항이 아니며, 이렇게 설정할 경우에 스케줄링 동작에 대해서는 설정과 다르게 동작할 수 있다.

본 장비에서는 스케줄링 설정은 tx-scheduling 이라는 mapping table 을 생성한 뒤, 포트에 적용하는 방

식으로 동작하며, 모듈당 7개의 map을 적용해서 사용할 수 있다. 실제로는 총 8개의 map을 설정할 수 있으나, 0번은 default SPQ로 사용되며 변경이 불가능하므로, 운용자가 설정할 수 있는 것은 7개이다.

표 21-2. Tx-scheduling map 설정 명령어

명령어	설명	모드
mls qos map tx-scheduling NAME queueing-method <0-7> (strict wrr1 wrr2)	해당 이름을 가지는 mapping table의 n번째 큐에 대한 queueing-method를 설정한다. 해당 이름을 가지는 mapping table이 없는 경우에는 새로 생성한다.	Config
mls qos map tx-scheduling NAME queueing-method <0-7> (wrr1 wrr2) <1-100>	wrr1 또는 wrr2를 설정할 경우는 wrr weight를 동시에 설정이 가능하다. Weight 값이 주어지지 않으면 1로 설정된다.	Config
mls qos map tx-scheduling NAME wrr-weight <0-7> <1-100>	Wrr로 설정된 큐의 weight를 설정한다.	Config
no mls qos map tx-scheduling NAME queueing-method <0-7>	해당 큐의 queueing-method를 해제한다. 해제할 경우 디폴트인 strict로 바뀐다.	Config
no mls qos map tx-scheduling NAME wrr-weight <0-7>	Wrr로 설정된 큐의 weight를 해제한다. 디폴트인 1로 설정된다.	Config
no mls qos map tx-scheduling NAME	해당 이름을 가지는 mapping table을 삭제한다.	Config
show mls qos map tx-scheduling	Tx-scheduling 설정 정보를 보여준다.	Exec

위와 같이 만들어진 tx-scheduling에 대한 mapping table을 원하는 포트에 다음과 같이 설정하여 사용한다.

표 21-3. Tx-scheduling 설정 명령어

명령어	설명	모드
mls qos tx-scheduling NAME	해당 이름을 가지는 mapping table을 해당 포트 인터페이스에 설정한다.	interface
no mls qos tx-scheduling NAME	해당 이름을 가지는 mapping table을 해당 포트 인터페이스에서 해제한다.	interface

21.1.3. Port trust 모드

포트에 인입되는 트래픽에 대해서 QOS를 수행하기 위해서는 패킷의 COS 또는 DSCP 값을 확인한 뒤, 이를 바탕으로 패킷의 우선 순위를 정하게 되어 있다. 하지만, 인입되는 트래픽의 COS 또는 DSCP 값이 믿을 수 있는지를 결정해 주어야 한다.

아무런 설정이 없는 경우에는 COS 또는 DSCP 값을 참조하지 않으며, 이 경우에는 포트에 설정된 default COS 값을 이용하여 동작하게 되어 있다. 참고로 이 default COS 값은 COS 또는 DSCP 가 없는 패킷 (예:untagged packet) 에 대한 기본 동작을 정의하는 용도로도 사용된다.

Trust mode 는 COS 또는 DSCP 에 대해서 설정할 수 있으며, 둘 다 설정할 수도 있고, 둘 다 설정하지 않을 수도 있다.

- trust DSCP (또는 BOTH) 모드이며, 패킷에 DSCP 값이 있다면 이를 이용한다.
- trust COS (또는 BOTH) 모드이며, 패킷에 COS 값이 있다면 이를 이용한다.
- trust COS (또는 BOTH) 모드이며, 패킷에 COS 값이 없다면, 포트에 설정된 default COS 값을 이용한다.
- 그 외의 경우에는 default COS 값을 이용한다.

Trust DSCP 모드이며, 패킷에 DSCP 값이 있는 경우라면, 해당 패킷은 DSCP 를 바탕으로 QOS 가 진행되며, 그렇지 않은 경우는 COS 를 바탕으로 QOS 가 진행된다.

표 21-4. port trust 설정 명령어

명령어	설명	모드
mls qos trust (cos dscp both)	해당 포트 인터페이스에 trust mode 를 설정한다.	interface
no mls qos trust	해당 포트 인터페이스에 trust mode 를 해제한다. 이 경우 none 으로 설정된다.	interface
mls qos cos <0-7>	포트의 디폴트 cos 값을 설정	interface
no mls qos cos	포트의 디폴트 cos 값 설정을 해제함.	interface

21.1.4. DSCP 변환 map 설정

Trust DSCP 모드에 의해서 해당 패킷이 DSCP 를 기준으로 동작하게 될 경우, 이 패킷은 다음과 같이 동작한다.

- DSCP 값에 따른 queueing 동작
- DSCP 값에 따른 COS marking(or remarking) 동작
- DSCP 값에 따른 DSCP remarking 동작

21.1.4.1. DSCP to queue 설정

DSCP 값에 따라 해당 패킷은 queueing 동작을 수행하는데, 이는 enable/disable 설정이 없이 항상 동작한다. 이 동작에 필요한 DSCP-queue map 값은 전역 설정으로 유지된다.

```
Switch#show mls qos map dscp-queue
DSCP-TO-QUEUE MAP
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 0 0 0 0 0 0 0 0 0 1 1
1 : 1 1 1 1 1 1 2 2 2 2 2
2 : 2 2 2 2 3 3 3 3 3 3 3
3 : 3 3 4 4 4 4 4 4 4 4 4
4 : 5 5 5 5 5 5 5 5 5 6 6
5 : 6 6 6 6 6 6 7 7 7 7 7
6 : 7 7 7 7
```

표 21-5. dscp-queue map 설정 명령어

명령어	설명	모드
mls qos map dscp-queue <0-63> ... <0-63> to <0-7>	Dscp-queue map 을 설정한다.	config
no mls qos map dscp-queue	Dscp-queue map 을 초기화 한다..	config
show mls qos map dscp-queue	현재 dscp-queue map 설정을 보여준다.	Exec

21.1.4.2. DSCP to COS 설정

DSCP 값에 따라 해당 패킷은 COS marking (or remarking) 동작을 수행할 수 있다. 이는 포트 인터페이스 별로 enable/disable 설정이 가능하며, 디폴트는 disable 이다. 이 동작에 필요한 DSCP to COS map 값은 전역 설정으로 유지된다.

```
Switch#show mls qos map dscp-cos
DSCP-TO-COS MAP
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 0 0 0 0 0 0 0 0 0 1 1
1 : 1 1 1 1 1 1 2 2 2 2 2
2 : 2 2 2 2 3 3 3 3 3 3 3
3 : 3 3 4 4 4 4 4 4 4 4 4
4 : 5 5 5 5 5 5 5 5 5 6 6
5 : 6 6 6 6 6 6 7 7 7 7 7
6 : 7 7 7 7
```


표 21-6. dscp-cos map 설정 명령어

명령어	설명	모드
mls qos map dscp-cos <0-63> ... <0-63> to <0-7>	Dscp-cos map 을 설정한다.	config
no mls qos map dscp-cos	Dscp-cos map 을 초기화 한다..	config
mls qos dscp-cos	해당 포트 인터페이스에 dscp-cos marking 을 수행하도록 설정한다.	interface
no mls qos dscp-cos	해당 포트 인터페이스에 dscp-cos marking 을 수행하지 않도록 설정한다.	interface
show mls qos map dscp-cos	현재 dscp-cos map 설정을 보여준다.	Exec

21.1.4.3. DSCP to DSCP 설정

DSCP 값에 따라 해당 패킷은 DSCP remarking 동작을 수행할 수 있다. 이는 자기 자신의 DSCP 값을 변경한다는 의미에서 mutation 이란 표현을 사용한다. 이는 포트 인터페이스 별로 enable/disable 설정이 가능하며, 디폴트는 disable 이다. 이 동작에 필요한 DSCP to DSCP map 값은 전역 설정으로 유지된다. 디폴트는 1:1 이 기본이므로, 의미 있게 사용하기 위해서는 map 을 변경후에 포트 인터페이스에 적용해야 한다.

```
Switch#show mls qos map dscp-mutation
DSCP MUTATION MAP
  d1 :   d2  0   1   2   3   4   5   6   7   8   9
-----
  0 :       0   1   2   3   4   5   6   7   8   9
  1 :      10  11  12  13  14  15  16  17  18  19
  2 :      20  21  22  23  24  25  26  27  28  29
  3 :      30  31  32  33  34  35  36  37  38  39
  4 :      40  41  42  43  44  45  46  47  48  49
  5 :      50  51  52  53  54  55  56  57  58  59
  6 :      60  61  62  63
```

표 21-7. dscp-mutation map 설정 명령어

명령어	설명	모드
mls qos map dscp-mutation <0-63> ... <0-63> to <0-63>	Dscp-mutation map 을 설정한다.	config
no mls qos map dscp-mutation	Dscp-mutation map 을 초기화 한다..	config
mls qos dscp-mutation	해당 포트 인터페이스에 dscp remarking 을 수행하도록 설정한다.	interface
no mls qos dscp-mutation	해당 포트 인터페이스에 dscp remarking 을 수행하지 않도록 설정한다.	interface
show mls qos map dscp-mutation	현재 dscp-mutation map 설정을 보여준다.	Exec

21.1.5. COS 변환 map 설정

Trust COS 모드에 의해서 해당 패킷이 COS 를 기준으로 동작하게 될 경우, DSCP 와 비슷하게 이 패킷은 다음과 같이 동작한다.

- COS 값에 따른 queueing 동작
- COS 값에 따른 DSCP marking(or remarking) 동작
- COS 값에 따른 COS remarking 동작

21.1.5.1. COS to queue 설정

COS 값에 따라 해당 패킷은 queueing 동작을 수행하는데, 이는 enable/disable 설정이 없이 항상 동작한다. 이 동작에 필요한 COS-queue map 값은 전역 설정으로 유지된다.

```
Switch#show mls qos map cos-queue
COS-TO-QUEUE MAP
COS : 0 1 2 3 4 5 6 7
-----
Queue: 2 1 0 3 4 5 6 7
```

표 21-8. cos-queue map 설정 명령어

명령어	설명	모드
mls qos map cos-queue <0-7> <0-7>	Cos-queue map 을 설정한다.	config
no mls qos map cos-queue	Cos-queue map 을 초기화 한다..	config
show mls qos map cos-queue	현재 cos-queue map 설정을 보여준다.	Exec

21.1.5.2. COS to DSCP 설정

COS 값에 따라 해당 패킷은 DSCP marking (or remarking) 동작을 수행할 수 있다. 이는 포트 인터페이스 별로 enable/disable 설정이 가능하며, 디폴트는 disable 이다. 이 동작에 필요한 COS to DSCP map 값은 전역 설정으로 유지된다.

```
Switch# show mls qos map cos-dscp
COS-TO-DSCP MAP
COS : 0 1 2 3 4 5 6 7
-----
DSCP: 0 8 16 24 32 40 48 56
```

표 21-9. cos-dscp map 설정 명령어

명령어	설명	모드
mls qos map cos-dscp <0-7> <0-63>	Cos-dscp map 을 설정한다.	config
no mls qos map cos-dscp	Cos-Dscp map 을 초기화 한다..	config
mls qos cos-dscp	해당 포트 인터페이스에 cos-dscp marking 을 수행하도록 설정한다.	interface
no mls qos cos-dscp	해당 포트 인터페이스에 cos-dscp marking 을 수행하지 않도록 설정한다.	interface
show mls qos map cos-dscp	현재 cos-dscp map 설정을 보여준다.	Exec

21.1.5.3. COS to COS 설정

COS 값에 따라 해당 패킷은 COS remarking 동작을 수행할 수 있다. 이는 자기 자신의 COS 값을 변경한다는 의미에서 mutation 이란 표현을 사용한다. 이는 포트 인터페이스 별로 enable/disable 설정이 가능하며, 디폴트는 disable 이다. 이 동작에 필요한 DSCP to DSCP map 값은 전역 설정으로 유지된다. 디폴트는 1:1 이 기본이므로, 의미 있게 사용하기 위해서는 map 을 변경후에 포트 인터페이스에 적용해야 한다.

```
Switch#show mls qos map cos-mutation
COS MUTATION MAP
  In COS   :   0   1   2   3   4   5   6   7
  -----
  Out cos  :   0   1   2   3   4   5   6   7
```

표 21-10. cos-mutation map 설정 명령어

명령어	설명	모드
mls qos map cos-mutation <0-7> <0-7>	Cos-mutation map 을 설정한다.	config
no mls qos map cos-mutation	Cos-mutation map 을 초기화 한다..	config
mls qos cos-mutation	해당 포트 인터페이스에 cosremarking 을 수행하도록 설정한다.	interface
no mls qos cos-mutation	해당 포트 인터페이스에 cos remarking 을 수행하지 않도록 설정한다.	interface
show mls qos map cos-mutation	현재 cos-mutation map 설정을 보여준다.	Exec

21.2. ACL 설정

E7500 장비는 다양한 ACL 설정이 가능하며 이를 이용해서, 쉽게 허용하고자 하는 패킷과 그렇지 않는 패킷을 구분할 수 있다.

본 장비에서 제공되는 ACL 은 크게 분류하여 **standard IP ACL**, **extended IP ACL**, **MAC ACL** 로 구분할 수 있다.

Standard IP ACL 은 source IP 로만 패킷을 구분한다. Standard IP ACL 을 위해서는 <1-99>, <1300-1999> 의 번호 대역이 할당되어 있으며, 그 외 번호가 아닌 이름으로도 생성하는 것이 가능하다.

Extended IP ACL 은 source IP, destination IP, protocol type 을 이용해서 패킷을 구분할 수 있다. 또한, TCP, UDP 패킷인 경우는 L4 src 및 dst port 를 이용해서 구분하는 것도 가능하며, ICMP 패킷의 경우는 icmp-type 을, IGMP 패킷인 경우는 igmp-type 을 이용해서 구분하는 것도 가능하다. <100-199> <2000-2699> 의 번호 대역이 할당되어 있으며, 그 외 번호가 아닌 이름으로도 생성하는 것이 가능하다.

MAC ACL 은 mac 주소를 이용해서 패킷을 구분하며, mac-access-list 라는 명령어로 분리 되어 있다. MAC ACL 용으로는 <1100-1199> 의 번호 대역이 할당되어 있다.

21.2.1. Standard IP ACL

Standard IP ACL 은 패킷의 source IP 로 패킷을 분류한다. 하나의 번호 또는 이름에 여러 개의 access-list 가 연결될 수 있으며, 개별의 조건마다 permit 또는 deny 동작을 수행할 수 있다.

Standard IP ACL 은 원래 <1-99> 의 99 개의 ACL 을 설정할 수 있도록 할당되었는데, 필요한 ACL 의 개수가 늘어나면서 <1300-1999> 의 700 개의 expanded 영역이 추가되었다. 또한, 문자로 이름을 정해서 사용할 수 있게 되면서 거의 무제한의 ACL 을 추가하는 것이 가능하다.

표 21-11. standard IP ACL 설정 명령어

명령어	설명	모드
access-list <1-99> (permit deny) SRC_IP_ADDRESS	Standard IP ACL 을 설정한다.	config
no access-list <1-99> (permit deny) SRC_IP_ADDRESS	Standard IP ACL 을 해제한다.	config
no access-list <1-99>	해당 이름(번호)를 가지는 ACL 전부를 삭제한다.	config
access-list <1-99> remark LINE	해당 ACL 에 대한 설명을 추가한다.	config
access-list <1300-1999> (permit deny) SRC_IP_ADDRESS	Expanded range 의 Standard IP ACL 을 설정한다.	config
no access-list <1300-1999> (permit deny)	Expanded range 의 Standard IP ACL 을 해제한다.	config

SRC_IP_ADDRESS	다.	
no access-list <1300-1999>	해당 번호를 가지는 ACL 전부를 삭제한다.	config
access-list <1300-1999> remark LINE	해당 ACL 에 대한 설명을 추가한다.	config
access-list standard WORD (permit deny) SRC_IP_ADDRESS	Named Standard IP ACL 을 설정한다.	config
no access-list standard WORD (permit deny) SRC_IP_ADDRESS	Named Standard IP ACL 을 해제한다.	config
no access-list standard WORD	해당 이름을 가지는 ACL 전부를 삭제한다.	config
access-list WORD remark LINE	해당 ACL 에 대한 설명을 추가한다.	config
Show access-list	ACL 설정을 조회한다	Exed

위 명령어중에서 **SRC_IP_ADDRESS** 는 다음과 같은 방법으로 설정할 수 있다.

A.B.C.D A.B.C.D	IP 대역을 wildcard 형태로 설정이 가능하다. 일반적인 IP 설정과는 반대로 masking 되는 부분이 0 이다.
host A.B.C.D	단 하나의 IP 주소만을 가르킬때는 host prefix 를 붙여서 사용한다.
A.B.C.D	하나의 IP 만 주어진 경우는 host A.B.C.D 과 동일하게 처리된다.
any	모든 IP 주소를 지정하는 경우는 any 를 사용한다.



Notice

일반적으로 IP 대역을 의미할 경우 10.1.1.0/24 와 같은 표현은 10.1.1.0 255.255.255.0 과 동일한 의미를 가지며 이는 10.1.1.0 ~ 10.1.1.255 의 IP 구간을 의미한다.
하지만, ACL 설정에서는 wildcard 는 이와 반대로 설정되며 10.1.1.0 ~ 10.1.1.255 IP 구간을 지정하기 위해서는 10.1.1.0 0.0.0.255 로 지정해야 한다.

21.2.2. Extended IP ACL

Standard IP ACL 이 src ip 주소만으로 패킷을 구분하는데 반해, extended ip acl 을 src ip 와 dest ip 를 모두 사용한다. 뿐만 아니라 protocol type 을 이용해서 패킷을 구분할 수 있다. 또한, TCP, UDP 패킷인 경우는 L4 src 및 dst port 를 이용해서 구분하는 것도 가능하며, ICMP 패킷의 경우는 icmp-type 을, IGMP 패킷인 경우는 igmp-type 을 이용해서 구분하는 것도 가능하다.

Extended IP ACL 은 원래 <100-199> 의 100 개의 ACL 을 설정할 수 있도록 할당되었는데, 필요한 ACL 의 개수가 늘어나면서 <2000-2699> 의 700 개의 expanded 영역이 추가되었다. 또한, standard IP ACL 과 마찬가지로 문자로 이름을 정해서 사용할 수 있게 되면서 거의 무제한의 ACL 을 추가하는 것이 가능하다.

표 21-12. extended IP ACL 설정 명령어

명령어	설명	모드
access-list <100-199> (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Extended IP ACL 을 설정한다.	config
access-list <100-199> (permit deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE	ICMP type 의 Extended IP ACL 을 설정한다.	config
access-list <100-199> (permit deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE	IGMP type 의 Extended IP ACL 을 설정한다.	config
access-list <100-199> (permit deny) (tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS eq <0-65536>	TCP / UDP type 의 Extended IP ACL 을 설정한다.	config
no access-list <100-199> (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Extended IP ACL 을 해제한다.	config
no access-list <100-199>	해당 이름(번호)를 가지는 ACL 전부를 삭제한다.	config
access-list <100-199> remark LINE	해당 ACL 에 대한 설명을 추가한다.	config
access-list <2000-2699> (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Expanded range 의 Extended IP ACL 을 설정한다.	config
access-list <2000-2699> (permit deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE	ICMP type 의 Expanded range 의 Extended IP ACL 을 설정한다.	config
access-list <2000-2699> (permit deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE	IGMP type 의 Expanded range 의 Extended IP ACL 을 설정한다.	config
access-list <2000-2699> (permit deny) (tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS eq <0-65536>	TCP / UDP type 의 Expanded range 의 Extended IP ACL 을 설정한다.	config
no access-list <2000-2699> (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Extended IP ACL 을 해제한다.	config
no access-list <2000-2699>	해당 이름(번호)를 가지는 ACL 전부를 삭제한다.	config
access-list <2000-2699> remark LINE	해당 ACL 에 대한 설명을 추가한다.	config
access-list extended WORD (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Named Extended IP ACL 을 설정한다.	config
access-list extended WORD (permit deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE	ICMP type 의 Extended IP ACL 을 설정한다.	config
access-list extended WORD (permit deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE	IGMP type 의 Extended IP ACL 을 설정한다.	config
no access-list extended WORD (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp)	Named Extended IP ACL 을 해제한다.	config

SRC_IP_ADDRESS DST_IP_ADDRESS		
no access-list extended WORD	해당 이름을 가지는 ACL 전부를 삭제한다.	config
access-list WORD remark LINE	해당 ACL 에 대한 설명을 추가한다.	config
Show access-list	ACL 설정을 조회한다	Exec

위 명령어중에서 **SRC_IP_ADDRESS** 와 **DST_IP_ADDRESS** 다음과 같은 방법으로 설정할 수 있다.

A.B.C.D A.B.C.D	IP 대역을 wildcard 형태로 설정이 가능하다. 일반적인 IP 설정과는 반대로 masking 되는 부분이 0 이다.
host A.B.C.D	단 하나의 IP 주소만을 가르킬때는 host prefix 를 붙여서 사용한다.
any	모든 IP 주소를 지정하는 경우는 any 를 사용한다.



Notice A.B.C.D 는 명령어 상의 혼돈을 피하기 위해서 extended IP ACL 에서는 지원하지 않으며, 단일 IP 을 지정하는 경우는 host A.B.C.D 를 사용한다.



Notice 일반적으로 IP 대역을 의미할 경우 10.1.1.0/24 와 같은 표현은 10.1.1.0 255.255.255.0 과 동일한 의미를 가지며 이는 10.1.1.0 ~ 10.1.1.255 의 IP 구간을 의미한다.
하지만, ACL 설정에서는 wildcard 는 이와 반대로 설정되며 10.1.1.0 ~ 10.1.1.255 IP 구간을 지정하기 위해서는 10.1.1.0 0.0.0.255 로 지정해야 한다.

21.2.3. MAC ACL

MAC 주소를 이용하여 패킷을 구분하는 것이 가능하다. MAC ACL 은 원래 <1100-1199> 의 ACL 번호가 할당되어 있다. MAC ACL 은 IP ACL 과 달리 mac-access-list 라는 명령어를 사용한다.

표 21-13. standard IP ACL 설정 명령어

명령어	설명	모드
mac-access-list <1100-1199> (permit deny) SRC_MAC_ADDRESS DST_MAC_ADDRESS <1-8>	MAC ACL 을 설정한다.	config
no mac-access-list <1100-1199> (permit deny) SRC_MAC_ADDRESS DST_MAC_ADDRESS <1-8>	MAC ACL 을 해제한다.	config
no mac-access-list <1100-1199>	해당 이름(번호)를 가지는 ACL 전부를 삭제한다.	
Show mac-access-list	MAC ACL 설정 상태를 조회한다.	Exec

위 명령어중에서 **SRC_MAC_ADDRESS** 와 **DST_MAC_ADDRESS** 다음과 같은 방법으로 설정할 수 있다. 단 SRC_MAC 과 DST_MAC 둘다 any 가 될 수는 없다.

H.H.H H.H.H	MAC 대역을 wildcard 형태로 설정이 가능하다..
any	모든 MAC 주소를 지정하는 경우는 any 를 사용한다.

21.2.4. ACL 의 인터페이스 적용

위와 같이 설정된 ACL 은 다음과 같이 인터페이스에 적용이 가능하다. 여기서 인터페이스는 다음 VLAN 인터페이스를 의미하며, router port 로 지정된 포트 인터페이스에도 적용이 가능하다.

Input 방향과 output 방향에 걸 수 있으며, 해당 인터페이스로 들어 오는 또는 나가는 패킷에 대해서 ACL 을 설정할 수 있다.

표 21-14. ACL 의 인터페이스 적용 설정 명령어

명령어	설명	모드
<code>ip access-group { <1-199> <1300>2699> WORD } {in out}</code>	해당 인터페이스에 acl 을 설정한다.	Interface
<code>no ip access-group { <1-199> <1300>2699> WORD } {in out}</code>	해당 인터페이스에 acl 을 해제한다.	Interface



Notice Router port 란 no switchport 상태인 port 를 의미한다.



Notice Service-policy 는 ACL 과 합쳐서 최대 input 방향으로 16000 개, output 방향으로 4000 개의 rule 을 설정할 수 있다.



Notice Input 방향으로는 service-policy 와 ACL 을 동시에 적용하여 사용하는 것이 가능하다, output 방향으로는 둘중 하나만 설정이 가능하다.

21.3. Service-policy 설정

단순한 ACL 설정 이외에 더 복잡한 형태의 QOS 설정을 위해서는 class-map 과 policy-map 을 이용해서 다양한 형태의 rule 과 action 을 설정하는 것이 가능하다. Class-map 에서는 ACL 또는 특정한 패킷의 성질을 이용해서 패킷을 분류하고, policy-map 에서는 이렇게 분류된 패킷에 특정한 동작을 수행할 수 있도록 해준다.

Class-map 에서는 ACL 을 통한 패킷 분류 뿐만 아니라 ethertype, cos, vlan, protocol, dscp, ip-precedence(TOS), I4 port, tcp flag, mpls flag 등 다양한 방법으로 패킷을 분류하는 것이 가능하다. Class-map 은 ACL 을 이용할 수 있을 뿐만 아니라, AND OR 조합으로 ACL 과 다른 항목을 조합하여 사용하는 것도 가능하다.

이러한 class-map 으로 분류된 트래픽은 기본적인 permit / drop 동작이외에도 queueing, cos marking / remarking, dscp marking / remarking, rate-limit 등의 동작을 수행하는 것이 가능하다. 또한 nexthop 을 연동하여 PBR (Policy based routing) 이 가능하게 할 수 있다. QOS 와 상관 없지만, trap-cpu, mirror, redirect, netflow 등의 동작을 수행하게 하여 장비 운용에 필요한 다양한 동작을 수행토록 할 수도 있다.

이렇게 선언된 policy-map 은 service-policy 라는 명령을 통해서 vlan 인터페이스 또는 router port interface 에 input 또는 output 방향에 적용하여 사용할 수 있다.

21.3.1. Class-map

Class-map 은 패킷을 분류하기 위한 목적으로 생성된다. 패킷의 분류는 기본적으로 ACL 을 사용하여 할 수 있으며, 그외에도 ethertype, cos, vlan, protocol, dscp, ip-precedence(TOS), I4 port, tcp flag, mpls flag 등 다양한 방법으로 패킷을 분류하는 것이 가능하다.

ACL 은 ip acl 과 mac-acl 을 모두 사용가능하지만, 1 개의 ACL 만 연동할 수 있다. 1 개의 ACL 이 가질 수 있는 세부 항목의 최대 개수는 1000 개이며, 1000 개 이상의 ACL 을 적용하고자 하면, 여러 개의 ACL 로 분리 한뒤 class-map 도 각각 따라 만들어 연동해 주어야 한다.

ACL 을 비롯한 다른 분류 조건은 기본적으로 AND 연산을 수행하는데, 예를 들어 ACL 과 DSCP 를 같이 설정하면, 두개의 조건이 모두 해당되는 패킷만 분류 할 수 있다. Class-map 을 선언할 때 match-any 옵션을 명시적으로 선언 하는 경우는 OR 연산을 수행하여, 둘중 하나만 만족하더라도 패킷이 분류 된다.

표 21-15. Class-map 설정 명령어

명령어	설명	모드
class-map WORD	AND 연산으로 분류하는 Class-map 을 생성하고 해당 노드로 이동한다.	Config

class-map match-all WORD	AND 연산으로 분류하는 Class-map 을 생성하고 해당 노드로 이동한다.	Config
class-map match-any WORD	OR 연산으로 분류하는 Class-map 을 생성하고 해당 노드로 이동한다.	Config
no class-map WORD	Class-map 을 삭제한다..	Config
match access-group NAME	ACL 을 이용한 분류 조건을 설정한다.	cmap
match cos <0-7>	Cos 을 이용한 분류 조건을 설정한다.	cmap
match ethertype WORD	Ethertype 을 이용한 분류 조건을 설정한다.	cmap
match ip-dscp <0-63>	Dscp 을 이용한 분류 조건을 설정한다.	cmap
match ip-precedence <0-7>	Ip-precedence 을 이용한 분류 조건을 설정한다.	cmap
match layer4 {source-port destination-port} <1-65536>	L4 port 을 이용한 분류 조건을 설정한다.	cmap
match mpls exp-bit topmost <0-7>	Mpls flag 을 이용한 분류 조건을 설정한다.	cmap
match tcp-control VALUE	Tcp-control 을 이용한 분류 조건을 설정한다.	cmap
match vlan <1-4095>	VLAN 을 이용한 분류 조건을 설정한다.	cmap



Notice Ethertype 의 분류는 4 자리 hexadecimal 로 분류한다. 예를 들어 ARP 타 입인 경우 0806 으로 지중하면 된다.



Notice Tcp-control 을 6 자리 2 진수로 분류한다. 예를 들어 5 번째 자리인 SYN flag 를 보고자 할때는 000010 으로 선언하면 된다.

21.3.2. Policy-map

Class-map 으로 분류된 트래픽은 기본적인 permit / drop 동작이외에도 queueing, cos marking / remarking, dscp marking / remarking, rate-limit 등의 동작을 수행하는 것이 가능하다. 또한 nexthop 을 연동하여 PBR (Policy based routing) 이 가능하게 할 수 있다. QOS 와 상관 없지만, trap-cpu, mirror, redirect, netflow 등의 동작을 수행하게 하여 장비 운용에 필요한 다양한 동작을 수행토록 할 수도 있다.

하나의 policy-map 에는 최대 100 개의 class-map 에 대해서 동작을 지정하는 것이 가능하다. Class-map 당 1000 개의 항목을 가지는 ACL 이 사용될 수 있기에, 이론상 10 만개의 ACL 항목을 하나의 policy-map 에서 제어가 가능하지만, 실제 H/W 의 제약으로 이렇게 많은 수를 rule 을 사용할 수는 없다.

각 class-map 별로 패킷에 대한 동작을 수행할 수 있는데, 다음과 같은 것들을 지정할 수 있으며, 동작의 조건에 따라 중복 적용도 가능하다. 예를 들어 하나의 class-map 에 대해서 queueing 7 을 주며, cos marking 6 을 하고, dscp marking 54 를 동시에 수행하도록 할 수도 있다. 동작의 특성상 drop 같은 경우는 다른 동작과 중복되지 않는다.

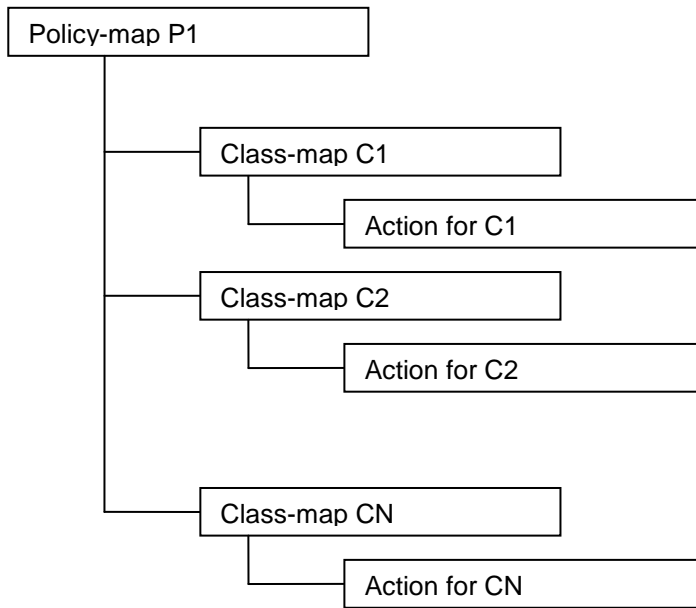


그림 21-1. policy-map 의 계층도

Marking 과 remarking 은 별다른 구분없이 사용되는데, 들어오는 패킷에 해당 필드가 없으면 자동으로 marking 을 수행하고, 해당 필드가 있으면 remarking 으로 동작한다. Trap-cpu, mirror, redirect, netflow 등의 동작은 QOS 와는 직접적인 상관은 없지만, class-map 과 policy-map 을 이용해서 제어하는 것이 가능하다.

표 21-16. Class-map 설정 명령어

명령어	설명	모드
policy-map NAME	해당 이름의 policy-map 을 생성하고 해당 노드로 이동한다.	Config
no policy-map NAME	해당 이름의 policy-map 을 삭제한다..	Config
class NAME	Class-map 의 동작을 지정하는 sub node 로 이동한다	pmap
no class NAME	해당 class-map 동작 설정을 삭제한다.	pmap
drop	해당 class-map 으로 분류된 트래픽을 drop 한다.	pmap-c
set cos <0-7>	Cos marking 설정	pmap-c
set drop-precedence <0-2>	Drop precedence 설정	pmap-c
set ip-dscp <0-63>	Dscp marking 설정	pmap-c
set ip-precedence <0-7>	Ip precedence (tos) 설정	pmap-c
set queueing <0-7>	Queueing 설정	pmap-c
police <1-10000000> <1-10000000> exceed-action drop	Rate-limit 설정	pmap-c

police aggregate NAME	Aggregated rate-limit 설정	pmap-c
nexthop A.B.C.D { priority <1-8> }	PBR nexthop 설정 및 nexthop priority 설정	pmap-c
netflow	Netflow 설정	pmap-c
redirect IFNAME	Redirect 설정	pmap-c
mirror	Mirror 설정	pmap-c
trap-cpu { high-priority }	CPU trap 설정	pmap-c

21.3.3. Service-policy

위와 같은 방법으로 설정된 policy-map 은 vlan interface 또는 router port interface 에 적용이 가능하다. ACL 과 마찬가지로 input 과 output 방향에 설정할 수 있다. 단, output 방향으로는 service-policy 와 ACL 중 하나만 설정이 가능하며, input 방향은 두가지 설정을 동시에 적용이 가능하다.

표 21-17. service-policy 설정 명령어

명령어	설명	모드
service-policy { input output } NAME	해당 이름의 policy-map 을 인터페이스에 적용한다.	interface
no service-policy { input output } NAME	해당 이름의 policy-map 을 인터페이스에서 삭제한다.	interface



Notice Router port 란 no switchport 상태인 port 를 의미한다.



Notice Service-policy 는 ACL 과 합쳐서 최대 input 방향으로 16000 개, output 방향으로 4000 개의 rule 을 설정할 수 있다.



Notice Input 방향으로는 service-policy 와 ACL 을 동시에 적용하여 사용하는 것이 가능하다, output 방향으로는 둘중 하나만 설정이 가능하다.

21.4. COPP

COPP 는 Control Plane Policing 라는 의미로 CPU 로 유입되는 트래픽에 대한 rate-limit 및 QOS 정책을 적용하는 것을 의미한다. CPU 에는 프로토콜에 관련된 다양한 제어 패킷이 유입되는데, 특정한 패킷이 과도하게 유입되는 경우에는 CPU 의 성능 문제가 발생할 수 있으며, 더 중요한 우선순위를 가지는 다른 프로토콜 패킷이 처리되지 않을 수 있는 문제를 야기할 수 있다. 그러므로, 패킷별 우선순위 설정 및 rate-limit 설정을 통해 트래픽을 정리해주는 기능이 필요하다.

21.4.1. Service-policy on COPP

Control Plane 에 service-policy 를 적용해서 CPU 로 유입되는 트래픽에 대해 Policing 을 수행할 수 있다.

표 21-18. service-policy 의 control-plane 적용 설정 명령어

명령어	설명	모드
control-plane	Control-plane 모드로 진입한다	configure
service-policy input NAME	해당 이름의 policy-map 을 control-plane 에 적용한다.	Control-plane
no service-policy input NAME	해당 이름의 policy-map 을 control-plane 에 적용을 해지한다.	Control-plane



Notice Control-plane 에서 Service-policy 가 사용되는 경우에는 policy-map 에서 설정하는 동작 중 **police, drop, set queueing** 의 동작만 수행이 된다.

21.4.2. Rate-limit on COPP

CPU 로 유입되는 특정 트래픽에 대해서 rate-limit 을 설정 할 수 있다.

표 21-19. rate-limit 의 control-plane 적용 설정 명령어

명령어	설명	모드
rate-limit arp-reply <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 arp-reply 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit arp-request <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 arp-request 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit igmp <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 igmp 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit ip-control-over-multicast <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 ip-control 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit ipv6-neib-sol <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 ipv6 ns 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit l4-port (both tcp udp) (both multicast unicast) <1-65535> <1-65535> <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 L4 트래픽에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit mld <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 mld 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane

rate-limit multicast <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 multicast 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit protocol <1-255> <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 특정 protocol 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit ripv1 <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 rip(version 1) 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit tcp-syn <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 tcp-syn 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
rate-limit udp-broadcast <1-1000000> <0-7>	CPU 로 유입되는 트래픽 중 udp broadcast 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane

22

Utilities

22.1. 개요

본 장에서는 시스템 운영에 필요한 기타 기능들에 대해 설명하도록 한다.

22.2. 상태 dump 명령

22.2.1. 명령어

각 모듈들(시스템 환경, MULTICAST, 라우팅, 드라이버 등)의 시스템 로깅 메시지를 dump 하기 위한 목적으로 "show tech-support" 명령을 사용한다.

show tech-support

시스템 운영 시 문제가 발생했을 경우, 기존에는 여러 명령을 입력하여 모듈들의 동작 상태를 확인해야 하는 번거로움이 있었지만, 이 명령을 사용함으로써, 미리 정의해 놓은 모듈들의 주요 명령들이 수행되어 그 결과 메시지가 출력되기 때문에, 각 모듈 담당자들이 이 메시지를 통해 좀 더 빠르게 확인할 수 있다.

출력 메시지는 페이지가 되지 않기 때문에, 출력 메시지는 명령의 수행이 끝날 때까지 출력된다. 이 명령의 수행 도중에, 출력을 멈추기 위해서는 **Ctrl+C** 를 입력하여 중단시켜야 한다.

다음의 예를 살펴보도록 하자.

Show tech 명령의 수행은 CPU 에 상당한 부하를 가하기 때문에, 처리시간도 길다. CPU 가 100% 지속됨에 따라 라우팅 끊김 현상이 발생할 수 있기 때문에, 다음과 같이 운용자에게 다시 한번 명령을 수행할 것인지에 대한 confirm 을 요청한다.

```
Switch# show tech-support
```

```
--- Display the system information ---
```

```
-----
```

```
MODEL-NAME       : E7508
SERIAL-NO        : P00M0000000A
System MAC-ADDRESS: 00:07:70:74:ff:01
```

```
--- Display the system version ---
```

```
-----
```

```
Ubiquoss Switch Operating System Software
E7508 Software (E7500-PFE), Version 1.3.7
Technical Support: http://www.ubiquoss.com
Copyright (c) 2001-2010 by Ubiquoss Inc.
```

```
BOOTLDR: E7500 Software (e_project_boot_r017.bin_os), Version 0.1.7
```

```
shu uptime is 5 hours, 11 minutes
Time since shu switched to active is 5 hours, 10 minutes
System restarted at 09:15:11 UTC Thu Feb 18 2010
System image file is "tftp://10.1.13.4/evol.r137"
```

```
If you require further assistance please contact us by sending email to
spot.team@ubiquoss.com.
```

```
Freescale MPC8641HPCN processor with 2048M bytes of memory.
Processor board ID P00M0000000A
7448 CPU at 1000Mhz, Rev 0.2 (pvr 8004 0202), 1024KB L2 Cache
Last reset from s/w reset
131072K bytes of Flash internal SIMM (Sector size 256K).
```

```
--- Show current system's time ---
```

```
-----
```

```
14:26:50 UTC Thu Feb 18 2010
```

```
--- Display elapsed time since boot ---
```

```
-----
```

```
0 days, 5 hours, 11 mins, 39 secs since boot
```



```
--- CPU information ---
```

```
-----
```

```
...
```

22.3. Command history 기능

운영자에 의해 수행된 명령어를 명령어를 실행한 시간순서 또는 실행한 시간의 역순으로 출력하는 기능이다. 이 기능을 사용하여 운영자가 실행한 명령의 조회가 가능하며 시스템 오동작시 원인 규명 및 복원이 편리하게 된다.

표 1. command history 조회 및 설정 명령어

명령어	설명	모드
show history	■ 실행된 명령어들을 조회한다.	Privileged
show history back	■ 실행된 명령어들을 시간의 역순으로 조회한다.	Privileged
show history detail	■ 명령을 실행한 시간/user/접속 IP 를 추가적으로 표시한다.	Privileged

같은 명령어를 반복하여 입력하는 경우는 한번만 저장된다.

22.4. Output Post Processing

22.4.1. output post processing 개요

장비의 현재 상태 또는 설정을 보는 명령어는 대부분 **show** 로 시작한다. **show** 명령은 대부분 한 화면에 보기 편하게 정리해서 보여주는 것이 일반적이나, 그 내용이 방대한 경우도 상당히 많다.

예를 들면, **show mac-address-table** 명령의 경우 수천 라인의 정보가 보여 질 수 있으며, **show interface** 명령의 경우에도 상당히 많은 분량의 내용이 출력된다. 출력되는 내용이 많을 경우, 이 내용 중에서 원하는 부분을 찾는 것은 쉽지 않다. 이럴 때 본 장비에서 지원하는 **output post processing** 기능을 사용하면 편리하다.

일반적으로 유닉스에서 **pipe** 라고 부르는 기능과 비슷하며, 본 장비에서는 3 가지의 미리 정의된 **output post processing** 을 지원한다. **Output post processing** 기능을 사용하기 위해서는 **show** 명령 이후 **bar (|)** 를 이어 붙이고, 다음의 명령어를 사용하면 된다.

명령어	설명
include WORD	■ 특정 단어를 포함하는 문자열을 출력한다.
exclude WORD	■ 특정 단어를 포함하지 않는 문자열을 출력한다.
begin WORD	■ 특정 단어를 포함하는 문자열부터 그 이후에 나오는 모든 라인을 출력한다.

22.4.2. output post processing 예제

show mac-address-table 명령은 상당한 양의 결과를 출력하는데, 그 중 원하는 부분이 포함된 mac 주소만 출력하고자 할 때는 **include** 를 사용한다.

```
Switch#
Switch# show run | inc service
service password-encryption
service dhcp
```

show ip interface 명령은 상당한 양의 결과를 출력하는데, 그 중 특정 vlan 인터페이스 이후의 결과만을 원할 때는 **begin** 을 사용한다.

```
E7508_236#show ip interface | begin Vlan1

...skipping
Vlan1 is up, line protocol is up
  Internet protocol processing disabled
  IP Flow switching is disabled
Vlan33 is administratively down, line protocol is down
  Internet address is 20.1.3.2/24
  Broadcast address is 20.1.3.255
  MTU is 1500 bytes
  Ingress service-policy is not set.
  Egress service-policy is not set.
  IP Flow switching is disabled
Vlan200 is down, line protocol is down
  Internet address is 200.1.1.236/24
  Broadcast address is 200.1.1.255
  MTU is 1500 bytes
  Ingress service-policy is not set.
  Egress service-policy is not set.
  IP Flow switching is disabled
```

22.4.3. DDM (Digital Diagnostic Monitoring)

E7508 는 DDM 을 지원하는 GBIC 의 상태를 상세하게 사용자에게 보여주는 명령어를 지원한다. Monitoring 항목은 다음과 같다.

항목	설명
온도	GBIC Port 온도
전압	GBIC Port 전압
전류	GBIC Port 전류
RxPower	GBIC Port 광 입력 세기
TxPower	GBIC Port 광 출력 세기

22.4.4. GBIC DDM Monitoring

DDM 을 지원하는 gbic 에 한해 다음 명령어를 사용하여 gbic 의 현재 상태를 확인할 수 있다.

명령어	Mode	설명
show interface transceiver	Privileged	DDM 을 지원하는 gbic 의 상태를 확인한다.

```
Switch# show interface transceiver
If device is externally calibrated, only calibrated values are printed.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).

Port          Temperature Voltage Current   Optical   Optical
(Celsius)    (Volts)  (mA)     (dBm)     (dBm)
-----
Gi2/1/3       42.6      3.32     17.4      -7.7      -40.0 --
Gi2/1/4       41.5      3.32     15.5      -6.7      -40.0 --
.....
....
gi3 gbic ddm          50.6'C          3.5 V          14.0 mA          -6.08 dBm          -40.00
dBm
Normal          Normal          Normal          Alarm(L)
Alarm(L)
(warn) 100.0 -10.0  4.0  1.0  131.0  0.0  8.00  0.00  8.00
0.00
(alarm) 100.0 -10.0  4.0  1.0  131.0  0.0  8.00  0.00  8.00
0.00
.....
.... gi1/2 .
Normal          Normal          Normal          Normal          Normal
(warn) 128.0 -128.0  6.6  0.0  131.0  0.0  8.20 -40.00  8.00 -40.00
(alarm) 128.0 -128.0  6.6  0.0  131.0  0.0  8.20 -40.00  8.00 -40.00
.....
```

23

환경설정 저장 및 소프트웨어 업그레이드

본 장에서는 시스템의 Flash File System 의 관리 방안 및 USB, Compact Flash(CF) File System 의 사용에 대해서 설명한다. E7500 series 에서 제공하는 File System 은 시스템 OS Image 와 Configuration 파일을 저장하는 장소로 주로 사용되며, 부팅 시 여기에 저장된 OS Image 와 Configuration 파일을 시스템이 Loading 하게 된다. 이 장에서는 기본적인 File System 운용에 필요한 명령어와 OS Image 와 Configuration File Management 에 필요한 명령어 및 부팅 모드 설정에 필요한 명령어 등을 중심으로 설명한다.

(주. 본 매뉴얼에서 설명된 기능은 당사의 사정에 의해 변경될 수 있다)

23.1. 파일 시스템

E7500 Series 스위치는 OS image 파일 저장 및 환경 설정의 저장을 위해 기본적으로 Flash 파일 시스템을 구축하고 USB, Compact Flash 등을 지원한다. 이 장에서 본 제품의 여러 파일 시스템에 대해 설명한다.

Flash 파일 시스템은 OS image 파일과 장비의 설정을 파일로 저장하기 위해 사용한다. 각 파일은 Flash 메모리의 영역에서 기록되고, 저장할 때 또는 **rename** 명령어로 저장이름을 설정할 수 있다. 또한 사용자의 요구사항에 따라 이미 Flash File System 에 저장된 파일을 **erase** 명령어로 지울 수 있다. 단 지우거나 변경할 파일이 다음 부팅 때 사용될 OS image 또는 설정 파일인지 주의해야 한다. Flash 파일 시스템과는 다르게 USB 파일 시스템과 CF 파일 시스템은 장비에 탈 부착이 가능하고 장비에 연결되어 있는 경우 Flash 파일 시스템과 같이 OS image 파일과 장비 설정 파일을 저장하고 여러 명령들을 통해서 파일들의 관리가 가능하다.

시스템 파일 관리를 위한 기본 명령어는 다음과 같다.

표 23-1. 파일 관리를 위한 명령어

명령어	설명	모드
show flash:	Flash 파일의 상태를 보여준다.	Privileged
show (usbflash: disk1:) (<0-9>)	CF 메모리, USB 메모리에 의 상태를 보여준다.	Privileged
dir (usbflash: disk1: flash:)	해당 파일 시스템의 상태를 보여준다	Privileged
erase (flash:)filename	Flash 메모리에 저장된 파일을 삭제한다.	Privileged
erase (disk1: usbflash:) (<0-9>) filename	CF 메모리, USB 메모리에 있는 파일을 삭제한다	Privileged
rename (usbflash: disk1: flash:) (<0-9>) filename (usbflash: disk1: flash:) (<0-9>) change	파일의 이름 및 파일 시스템의 위치를 변경한다.	Privileged

다음은 E7500 Series 스위치에서 File System 의 정보를 보는 예시이다. 파일 이름과 파일 사이즈, 그리고 현재(B) 및 다음 부팅 모드(*)에 대한 정보와 함께 그 파일의 종류를 표시한다.

```
Switch# show flash:

-length- -----type/info----- CN path
1155631 text file -- aaa
...
2216 text file -- tmp.cfg
12678220 [NP]1.2.4 -- Eoct.R124
12683172 [NP]1.2.5 -- Eoct.R125
...

11480 Kbytes available (119592 Kbytes used, 92% used)
```

```
Switch# show disk1:

-----filename----- -----type/info----- CN -length-
acl_15k text file -- 732508160
osfp_ecmp text file -- 731899904
...

1474004 Kbytes available (2147920 Kbytes, 28 % used)
```

다음은 USB 메모리에 있는 파일을 지우는 예시이다.

```
shu#show usbflash:

-----filename----- -----type/info----- CN -length-
1.avi                  binary data file           -- 732508160
2.avi                  binary data file           -- 731899904
.....

1474004 Kbytes available (2147920 Kbytes, 28 % used)

shu#erase usbflash: 1.avi
shu#show usbflash:

-----filename----- -----type/info----- CN -length-
2.avi                  binary data file           -- 731899904
.....

2189344 Kbytes available (1432580 Kbytes, 19 % used)

shu#
```

23.2. Image/Configuration/BSP Down/Up Load

E7500 Series 스위치는 운영하면서 필요한 OS Image, Configuration 파일 및 Bootloader 에 대해서 FTP 또는 TFTP 를 이용해서 다운로드 또는 업로드 할 수 있다. 이는 새로운 파일을 Flash 파일에 저장하거나, 적용으로 사용될 수도 있고, 운용상 필요한 Backup 을 FTP/TFTP 서버에 할 수 있다. 또한 새로운 BSP 파일을 다운로드 하여 적용할 수 있다. 이 장에서는 어떻게 FTP/TFTP 를 통해서 파일을 다운로드 또는 업로드 하는지 설명한다. 아래에서 기술한 running-config 및 startup-config 에 대한 설명은 <[14.3 Configuration 파일 관리](#)>를 참조하라.



Warning 업그레이드할 Image 의 선택은 시스템 모델과 버전에 따라 상당히 주의가 요구하므로 당사의 지시 사항을 따르기 바란다.



Warning FTP/TFTP 를 통해 적용되는 configuration 은 현재 시스템의 configuration 에 추가되거나 변경된다. 즉 현재 시스템의 configuration 이 완전히 없어지고 다운로드 되는 configuration 으로 완전히 바뀌지는 않는다.

23.2.1. FTP 를 통한 Down/Up Load

아래는 FTP 를 이용한 파일 다운로드 또는 업로드 방법에 대한 명령어에 대해서 표로 설명해 놓았다.

표 23-2. FTP 를 통한 Down/Up Load 명령어

명령어	설명	모드
copy ftp: (usbflash: disk1: flash:) (<0-9>)	FTP 서버에 있는 OS Image 파일을 Flash, USB, CF 에 저장한다.	Privileged
copy (usbflash: disk1: flash:) (<0-9>) ftp	Flash, USB, CF 에 있는 OS Image 파일을 FTP 서버에 저장한다.	Privileged
copy ftp: config-file	FTP 서버에 있는 Configuration 파일을 Flash 에 저장한다.	Privileged
copy ftp: running-config	FTP 서버에 있는 Configuration 파일을 현재의 running-config 로 적용시킨다.	Privileged
copy running-config (usbflash: disk1: flash:) (<0-9>) filename	Running-config 를 해당 파일 시스템에 filename 으로 저장한다	Privileged
copy running-config ftp:	시스템에서 운용중인 현재 running-config 를 FTP 서버에 저장한다.	Privileged

copy ftp: bootloader FTP 서버에 있는 BSP 파일을 Flash 에 저장한다. Privileged

아래는 FTP 를 이용한 파일 다운 방법에 대한 예를 보여준다.

```
Switch# copy ftp: flash
IP address of remote host ? 10.1.13.4
User ID ? evolution
Password ?
Source file name ? 0621
Destination file name ? 0621
Warning: There is a file already existing with this name
Do you want to over-write [yes/no]? y
Over-writing 0621 file to flash memory
(생략)
```

```
Switch# copy ftp bootloader
IP address of remote host ? 192.168.0.1
User ID ? lns
Password ?
Source file name ? E7xg.bsp
Bootloader key (0xaabb) ? 0x860011
FTP:: 10.1.13.4//E7xg.bsp --> bootloader
Continue [yes/no]? yes
(생략)
```

다음은 현재 config 를 USB 메모리에 저장하는 명령의 예시이다.

```
shu#copy running-config usbflash: evol.cfg
shu#show usbflash:

-----filename-----type/info----- CN -length-
2.avi          binary data file      -- 731899904
evol.cfg      text file              --   7131
.....
2189336 Kbytes available (1432588 Kbytes, 19 % used)

shu#
```



Warning Bootloader 적용 시의 key 값은 보안을 위해 사전에 협의 후 배포한다.

23.2.2. TFTP 를 통한 Down/Up Load

아래는 TFTP 를 이용한 파일 다운 방법에 대한 명령어에 대해서 표로 설명해 놓았다.

표 23-3. TFTP 를 통한 Down/Up Load 명령어

명령어	설명	모드
copy tftp: (usbflash: disk1: flash:) (<0-9>)	TFTP 서버에 있는 OS Image 파일을 Flash, USB, CF 에 저장한다.	Privileged
copy (usbflash: disk1: flash:) (<0-9>) tftp:	Flash 에 있는 OS Image 파일을 TFTP 서버에 저장한다.	Privileged
copy tftp: config-file	TFTP 서버에 있는 Configuration 파일을 Flash 에 저장한다.	Privileged
copy tftp: running-config	TFTP 서버에 있는 Configuration 파일을 현재의 running-config 로 적용시킨다.	Privileged
copy running-config tftp:	시스템에서 운용중인 현재 running-config 를 TFTP 서버에 저장한다.	Privileged
copy tftp: bootloader	TFTP 서버에 있는 BSP 파일을 Flash 에 저장한다.	Privileged

아래는 TFTP 서버에서 파일을 다운로드 하는 방법에 대한 예를 보여준다.

```
shu#copy tftp: usbflash:
IP address of remote host ? 10.1.13.4
Source file name ? evol.r137
Destination file name ? evol.r137

TFTP::10.1.13.4//evol.r137 --> usbflash: 0 [evol.r137]
Proceed [yes/no]? y
```

```
Switch# copy tftp bootloader
IP address of remote host ? 10.1.13.4
Source file name ? E7x.bsp
Bootloader key (0xaabb) ? 0x860011

TFTP:: 10.1.13.4// E7x.bsp --> bootloader
Proceed [yes/no]? yes
(생략)
```

23.3. Configuration 파일 관리

환경 설정은 시스템 운영자가 E7500 Series 스위치를 운영하면서 설정된 다양한 파라미터의 집합이다. E7500 Series 스위치에서 사용하는 Configuration에는 `startup-config`와 `running-config`가 있다. Flash 메모리에 저장되어 스위치 초기 구동 시 로딩되는 Configuration을 `startup-config`라고 하며, DRAM 내에서 구동하는 환경설정 값을 `running-config`라고 한다. 여기서는 Configuration File Management에 필요한 저장, 삭제 및 다운로드 방법을 설명한다.

표 23-4. Configuration Management 명령어

명령어	설명	모드
<code>show startup-config</code>	Flashes, USB, CF 메모리 중 Booting configuration으로 설정된 파일의 정보를 보여준다.	Privileged
<code>show running-config</code>	현재의 환경 설정 정보를 보여준다.	Privileged
<code>copy running-config startup-config</code>	현재 시스템에서 운용중인 Running configuration 파일을 <code>startup</code> 파일로 저장한다.	Privileged
<code>erase startup-config</code>	현재 설정된 <code>startup configuration</code> 파일을 지운다.	Privileged

23.3.1. Configuration 파일 저장

시스템 운영자가 환경 설정을 변경하면 새로운 설정은 DRAM에 저장된다. DRAM에 저장된 설정 정보는 시스템 재 부팅 시 유지되지 않는다. 따라서 설정 정보를 시스템 재 부팅 시에도 계속 유지하기 위해서는 설정 정보 파일을 Flash 메모리에 저장해야 한다. 다음은 현재의 `running configuration`를 보여주는 명령어와 현재의 `running-config`를 `startup-config`로 저장하는 명령어에 대한 예를 보여 준다.

```
Switch# show running-config
!
interface Giga6/1/1
  no switchport
  ip address 192.168.51.1/24
  ... <생략> ....
SWITCH#
SWITCH# copy running-config startup-config
Overwrite 'system.cfg'? [yes/no] y
SWITCH# show startup-config
!
interface Giga6/1/1
  no switchport
  ip address 192.168.51.1/24
```

```
... <생략> ....
```

```
SWITCH#
```

23.3.2. Configuration 파일 삭제

E7500 Series 스위치는 시스템 재시동 시 Flash 메모리에 저장되어 있는 **startup-config** 를 재 로딩한다. 만약 현재 저장되어 있는 **configuration** 파일을 삭제하고 다른 파일로 시스템을 사용하고자 한다면 다음 예에서 보여주는 것처럼 **startup-config** 를 지우고 다른 파일로 설정 후 재 부팅하면 된다.

```
SWITCH# erase flash: System1.cfg  
Warning: System1.cfg is booting config file  
Do you want to erase it [yes/no]? y  
SWITCH# boot config System2.cfg  
SWITCH# reload
```

23.4. SFE/NETFLOW 소프트웨어 관리

E7500 Series 스위치는 SFE 및 NETFLOW의 flash에 각각의 module이 구동하는데 필요한 소프트웨어를 저장할 수 있다. 여기서는 SFE/NETFLOW의 소프트웨어들을 조회/추가/삭제하는 명령에 대하여 설명한다.

표 23-5. SFE/NETFLOW 소프트웨어 관리 명령어

명령어	설명	모드
show flash: module (<1-6>)	SFE module의 파일 정보를 보여준다.	Privileged
show flash: netflow	netflow의 파일 정보를 보여준다.	Privileged
copy flash: module	flash의 파일을 SFE module에 추가한다.	Privileged
copy flash: netflow	flash의 파일을 net flow에 추가한다.	Privileged
erase flash: module <1-6> filename	SFE module의 파일을 삭제한다.	Privileged
erase flash: netflow filename	netflow module의 파일을 삭제한다.	Privileged

23.4.1. SFE/NETFLOW 소프트웨어 조회

SFE Module의 flash에 존재하는 파일의 정보는 전체 혹은 module ID를 지정하여 조회가 가능하며, 그 예제는 다음과 같다.

```
Switch#show flash: module

Module 1 Flash Information :

-length- -----type/info----- CN path
19775     executable binary file      -- pss_misc_5836
4470825   [SFE] 0.0.1                      B* evolsfe.r101
4476230   [SFE] 1.0.9                        -- evolsfe.r109

6312 Kbytes available (9432 Kbytes used)
... <생략> ...

% failed connect to module 5
% failed connect to module 6

Switch#show flash: module 1

Module 1 Flash Information :

-length- -----type/info----- CN path
19775     executable binary file      -- pss_misc_5836
4470825   [SFE] 0.0.1                      B* evolsfe.r101
4476230   [SFE] 1.0.9                        -- evolsfe.r109
```

```
6312 Kbytes available (9432 Kbytes used)
```



Notice 장착되지 않은 module 에 대한 조회는 “%failed connect to module” 메시지가 출력된다.

NETFLOW 의 파일 정보를 조회하는 예는 다음과 같다

```
Switch#show flash: netflow

NetFlow Flash Information :

-length- -----type/info----- CN path
11640516 [NP]1.2.1                      B* Eoct.R121

19524 Kbytes available (12604 Kbytes used)
```

23.4.2. SFE/NETFLOW 소프트웨어 추가

PFE 의 flash 에는 SFE 및 NETFLOW 의 구동에 필요한 소프트웨어를 저장할 수 있다. 이 저장된 소프트웨어를 SFE 및 NETFLOW 에 추가하는 방법은 다음과 같다.

```
Switch#copy flash: module
filename to write on SFE ? evolsfe.r105
SFE Module id(1~6) ? 1

Send: -> Module 1//evolsfe.r105
Proceed [yes/no]? y
..... < 생략 > .....

Switch#show flash: module 1

Module 1 Flash Information :

-length- -----type/info----- CN path
19775     executable binary file      -- pss_misc_5836
4470825   [SFE] 0.0.1                      B* evolsfe.r101
4476721  [SFE] 1.0.5                       -- evolsfe.r105
4476230   [SFE] 1.0.9                      -- evolsfe.r109

1416 Kbytes available (14328 Kbytes used)
```

```
Switch#copy flash: netflow
filename to write on Netflow ? Eoct.R105

Send: -> Netflow Module//Eoct.R105
```

```
Proceed [yes/no]? y
..... < 선택 > .....

Switch#show flash: netflow

NetFlow Flash Information :

-length- -----type/info----- CN path
11421604 [netflow]1.0.5           -- Eoct.R105
11640516 [NP]1.2.1               B* Eoct.R121

8176 Kbytes available (23952 Kbytes used)
```

23.4.3. SFE/NETFLOW 소프트웨어 삭제

SFE/NETFLOW의 메모리에 존재하는 소프트웨어의 삭제하는 예제는 다음과 같다.

```
Switch#show flash: module 1

Module 1 Flash Information :

-length- -----type/info----- CN path
19775     executable binary file     -- pss_misc_5836
4470825   [SFE] 0.0.1                 B* evolsfe.r101
4476721  [SFE] 1.0.5                 -- evolsfe.r105
4476230   [SFE] 1.0.9                 -- evolsfe.r109

1416 Kbytes available (14328 Kbytes used)

Switch#erase flash: module 1 evolsfe.r105
Switch#show flash: module 1

Module 1 Flash Information :

-length- -----type/info----- CN path
19775     executable binary file     -- pss_misc_5836
4470825   [SFE] 0.0.1                 B* evolsfe.r101
4476230   [SFE] 1.0.9                 -- evolsfe.r109

6236 Kbytes available (9508 Kbytes used)
```

```
Switch#show flash: netflow

NetFlow Flash Information :

-length- -----type/info----- CN path
11421604 [netflow]1.0.5           -- Eoct.R105
11640516 [NP]1.2.1               B* Eoct.R121
```

```
8176 Kbytes available (23952 Kbytes used)
```

```
Switch#erase flash: netflow Eoct.R105
```

```
Switch#show flash: netflow
```

```
NetFlow Flash Information :
```

```
-length- -----type/info----- CN path  
11640516 [NP]1.2.1 B* Eoct.R121
```

```
19428 Kbytes available (12700 Kbytes used)
```

23.5. Boot Mode 설정 및 시스템 재시동

E7500 Series 스위치는 운영하면서 필요한 OS Image 와 configuration 파일에 대해서 다음 부팅 파일로 설정할 수 있다. 이렇게 설정된 OS Image 와 configuration 파일은 시스템의 재 시동 시 적용되므로 각별한 주의가 필요하다. 아래에서는 OS Image 와 configuration 파일에 대해서 어떻게 다음 부팅 모드로 설정하는지와 시스템 재 시동 방법에 대해서 설명해 놓았다.

표 23-6. Boot Mode 설정 및 시스템 재 시동 명령어

명령어	설명	모드
<code>boot system flash filename</code>	다음 부팅 시 적용될 OS Image 를 설정한다.	Privileged
<code>boot system tftp filename A.B.C.D</code>	다음 부팅 시 적용될 OS Image 를 tftp booting 으 로 한다.	Privileged
<code>boot config filename</code>	다음 부팅 시 적용될 Configuration 파일을 설정한 다.	Privileged
<code>reload</code>	시스템을 재 시동 시킨다.	Privileged

23.5.1. Boot Mode 설정

E7500 Series 스위치에서 OS Image 와 configuration 파일에 대해서 다음 Boot Mode 를 설정할 때에는 다음과 같은 주의가 필요하다. **boot flash** 명령어를 실행할 때에는 E7500 Series 스위치에서 사용할 수 있는 OS Image 파일에 대해서만 적용하도록 해야 하며, 또 **boot config** 명령어를 시행할 때에는 E7500 Series 스위치에서 사용할 수 있는 configuration 파일에 대해서만 적용하도록 해야 된다. 그리고 현재 Flash File System 에 있는 파일에 대해서만 적용하도록 하여야 한다.

```
Switch#
Switch# boot system flash p8xg.r090
Switch#
Switch# boot config lns.cfg
Switch#
```

23.5.2. 시스템 재시동

E7500 Series 스위치의 전원 On/Off 또는 **reload** 명령으로 시스템 재 시작이 가능하다. 또한 **reload** 명령의 **in** 또는 **at** 서브 명령으로 시스템 재 시작에 대한 예약도 가능하다. 만일 **reload at** 명령으로 시스템 재 시작을 예약한다면 **show clock** 명령의 현재 시간을 참조하여 설정해야 한다.

표 23-7. Boot Mode 설정 및 시스템 재 시동 명령어

명령어	설명	모드
reload	시스템을 즉시 재 시작한다.	Privileged
reload {in time at time [day][month]} [reason]	<p>시스템 재 시작을 예약한다.</p> <ul style="list-style-type: none"> ▪ in: 설정한 시간(time)후에 시스템이 재 시작됨 ▪ at: 설정한 시각에 시스템이 재 시작됨 ▪ time: HH:MM 형식으로 설정 가능 ▪ day: 1일부터 31일까지 설정 가능 ▪ month: 1월부터 12월까지 설정 가능 (ex. Jan or January) ▪ reason: 시스템 재 시작 이유를 등록 	Privileged
reload cancel	시스템 재 시작 예약을 취소한다. 시스템 재 시작의 취소 내용은 모든 터미널로 출력된다.	Privileged
show reload	시스템 재 시작 예약 내용을 출력한다.	Privileged

아래 예제는 **reload at** 명령으로 시스템 재 시작을 예약하는 설정하고 **reload cancel** 명령으로 예약을 취소하는 설정이다.

```
Switch# show clock
23:52:01 KST Thu Feb 18 2010
Switch# reload at 13:00 19 Feb For reload test

System configuration has been modified. Save? [y/n]: y
Building configuration...
[OK]
Reload scheduled for 13:00:00 KST Fri Feb 19 2010 in ( 13 hours 7 minutes )
Reload Reason: For reload test

continue to reboot ? [yes/no]: y

Switch# show reload
Reload scheduled for 13:00:00 KST Fri Feb 19 2010 in ( 13 hours 7 minutes 28
seconds ) on vty/0 (10.1.20.99)
Reload reason: For reload test
Switch#
Switch# reload cancel

***
*** --- SHUTDOWN ABORTED ---
***

Switch# show reload
No reload is scheduled.
Switch#
```



Warning 시스템의 재 시작 전에는 반드시 현재의 **configuration** 을 Flash 메모리에 저장하도록 한다. **Config** 모드로 진입한 후 **reload** 명령을 실행하면 아래와 같은 설정 저장 여부를 항상 확인한다.

```
System configuration has been modified. Save? [y/n]: y
```



Warning 시스템이 **Flash File System** 에 파일을 저장하고 있을 때는 시스템을 강제로 재시동 시켜서는 안 된다.