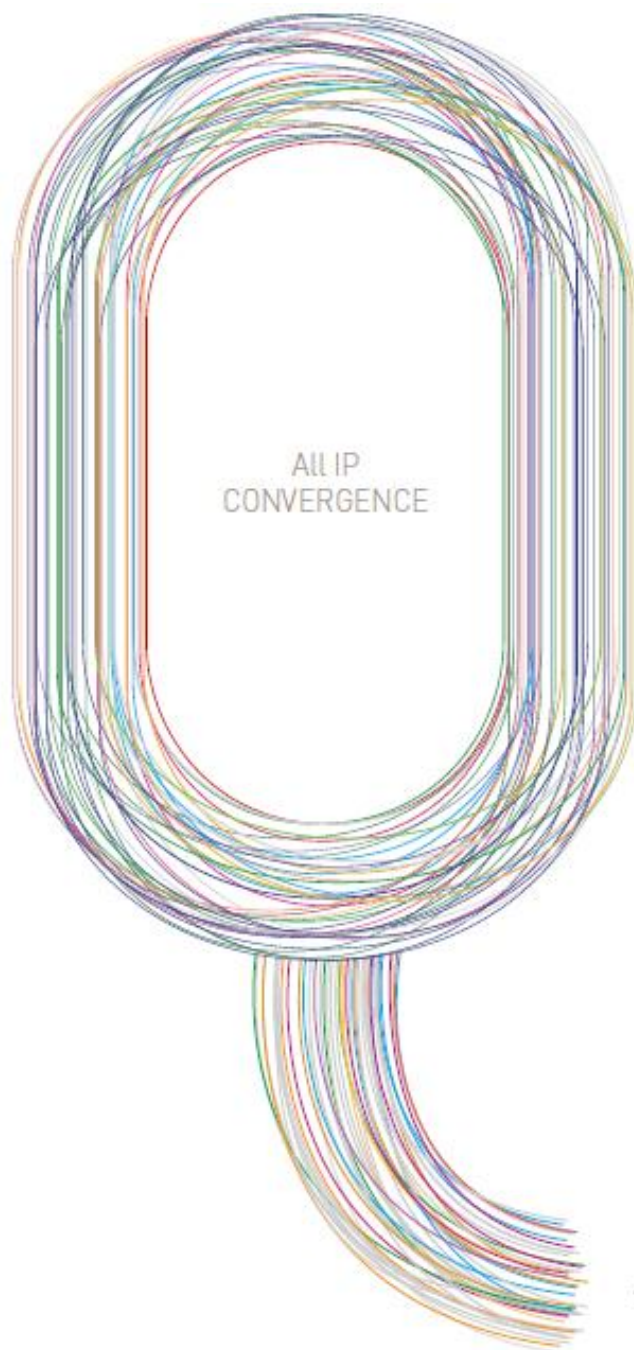


# U9200 Series GPON OLT Common User Guide



Published: Sep 2010

ubiQuoss

## 목차

목차 .....	2
표 목차 .....	15
그림 목차 .....	18
1. 서문 .....	20
1.1. 개요 .....	20
1.2. 적용 규칙 .....	21
1.3. 관련 문서 .....	22
2. 스위치 시작하기 .....	23
2.1. 편집 및 도움말 기능 .....	23
2.1.1. 명령어 문법의 이해 .....	23
2.1.2. 명령어 문법 도움말(Command Syntax Helper) .....	24
2.1.3. 단축 명령어 입력 .....	26
2.1.4. 명령어 심볼 .....	27
2.1.5. 명령어 라인 편집 키 및 도움말 .....	28
2.2. 스위치 명령어 모드 .....	28
2.3. U9200 SERIES 스위치 가동 .....	30
2.4. 사용자 인터페이스 .....	30
2.4.1. 콘솔 연결 .....	30
2.4.2. Telnet 연결 .....	31
2.4.3. SNMP Network Manager 를 통한 연결 .....	31
2.5. 계정 관리 및 인증 .....	32
2.5.1. 사용자 추가 및 삭제 .....	32
2.5.1.1. 사용자 추가 및 삭제 .....	33
2.5.2. 패스워드 설정 .....	33
2.5.2.1. Privileged 모드 패스워드 설정 .....	34
2.5.2.2. 패스워드 encryption 설정 .....	34
2.5.3. 인증 방법 설정 .....	35
2.5.4. 스위치에 login 시 인증 방법 설정 .....	35
2.5.4.1. 사용자 인증 설정 .....	35
2.5.5. privileged mode 진입시 인증 방법 설정 .....	36
2.5.5.1. privileged mode 사용자 인증 설정 .....	37
2.5.6. 권한 부여 .....	37

2.5.6.1.	사용자 권한 부여 .....	37
2.5.6.2.	명령어 권한 허가 .....	38
2.5.7.	계정 관리 .....	39
2.5.7.1.	세션 관리 .....	39
2.5.7.2.	명령어 관리 .....	40
2.5.8.	인증 서버 설정 .....	40
2.6.	HOSTNAME 설정 .....	42
2.7.	SNMP(SIMPLE NETWORK MANAGEMENT PROTOCOL).....	43
2.7.1.	SNMP Community 설정 .....	44
2.7.2.	SNMP Trap 설정 .....	45
2.7.3.	SNMP 패킷의 출발지 IP 설정 .....	46
2.7.4.	SNMP Trap enterprise - oid 설정 .....	46
2.7.5.	시스템 담당자 설정 .....	46
2.7.6.	시스템 구축 위치 설정 .....	46
2.8.	ACL(ACCESS CONTROL LIST).....	47
2.8.1.	액세스 리스트 생성 규칙.....	47
2.8.2.	표준 IP 액세스 리스트 설정 .....	47
2.8.2.1.	모든 액세스 허용 .....	47
2.8.2.2.	모든 액세스 거부 .....	48
2.8.2.3.	특정 호스트에서의 액세스만 허용 .....	48
2.8.2.4.	특정 네트워크에서의 액세스만 허용 .....	48
2.8.2.5.	특정 네트워크에서의 액세스만 거부 .....	48
2.8.3.	Telnet 연결에 액세스 리스트 설정 .....	49
2.9.	NTP 설정 .....	49
2.9.1.	NTP 개요.....	49
2.9.2.	NTP client mode 설정 .....	49
2.9.3.	NTP Server mode 설정 .....	49
2.9.4.	NTP time zone 설정 .....	50
2.9.5.	NTP summer time 설정 .....	50
2.9.6.	NTP 기타 명령어.....	50
2.9.7.	NTP 설정 예제 .....	50
3.	인터페이스 환경 설정 .....	52
3.1.	개요 .....	52
3.2.	공통 명령어 .....	52
3.2.1.	Interface name .....	53
3.2.2.	Interface id .....	53
3.2.3.	Interface 모드 프롬프트 .....	53
3.2.4.	Description 명령어 .....	53
3.3.	인터페이스 정보 및 상태 조회 .....	54
3.3.1.	show interface 명령어 .....	54
3.3.2.	show port status 명령어 .....	55
3.3.3.	show switchport 명령어 .....	55

3.4.	물리적 포트 환경 설정 .....	56
3.4.1.	Shutdown .....	57
3.4.2.	Block .....	57
3.4.3.	Speed an duplex .....	57
3.4.4.	Media Type .....	58
3.5.	STORM CONTROL .....	58
3.6.	PORT MIRRORING .....	59
3.7.	2 계층 인터페이스 환경 설정 .....	59
3.7.1.	VLAN Trunking .....	60
3.7.2.	2 계층 인터페이스 모드 .....	60
3.7.3.	2 계층 인터페이스 기본 설정 값 .....	60
3.7.4.	2 계층 인터페이스 설정/해제 .....	60
3.7.5.	Trunk port 설정 .....	61
3.7.6.	Access port 설정 .....	61
3.8.	PORT GROUP .....	62
3.8.1.	Port group 개요 .....	62
3.8.2.	Port group configuration .....	62
3.9.	MAC FILTERING .....	63
3.9.1.	MAC Filtering 개요 .....	63
3.9.2.	MAC Filtering 설정 .....	63
3.10.	CPU LOAD 에 따른 MAC FILTERING .....	63
3.10.1.	CPU Load 에 따른 MAC Filtering 개요 .....	63
3.10.2.	CPU Load 에 따른 MAC Filtering 설정 .....	63
3.11.	SWITCHING DATABASE MANAGER .....	64
3.11.1.	SDM 개요 .....	64
3.11.2.	SDM 설정 .....	64
3.12.	TRAFFIC-CONTROL .....	65
3.12.1.	Traffic-control 개요 .....	65
3.12.2.	Traffic-control 설정 .....	65
3.13.	포트 버퍼 설정 .....	66
3.14.	LLCF (LINK LOSS CARRY FORWARD) .....	66
4.	가상 랜(VLAN) .....	68
4.1.	VLAN 개관 .....	68
4.1.1.	VLAN 정의 .....	69
4.1.2.	VLAN 의 장점 .....	69
4.2.	VLAN 의 유형 .....	70
4.2.1.	포트 기반 VLAN(Port-Based VLANs) .....	70
4.2.1.1.	포트 기반 VLAN 으로 스위치 묶기 .....	70
4.2.2.	태그 VLAN(Tagged VLANs) .....	72
4.2.2.1.	태그 VLAN 의 사용(Uses of Tagged VLANs) .....	72
4.2.2.2.	VLAN 태그의 할당(Assigning a VLAN Tag) .....	73
4.2.3.	포트 기반 VLAN 과 태그 VLAN 의 혼합 .....	75



4.3.	VLAN 구성 .....	75
4.3.1.	VLAN ID .....	75
4.3.2.	Default VLAN .....	75
4.3.3.	Native VLAN .....	75
4.4.	VLAN 설정 .....	76
4.4.1.	VLAN 설정 명령 .....	76
4.5.	VLAN 설정 예제 .....	77
4.6.	VLAN 설정 정보 확인 .....	80
4.7.	802.1QINQ .....	81
4.8.	PRIVATE EDGE VLAN .....	83
4.9.	비정상적 MAC 차단기능 .....	85
<b>5.</b>	<b>IP 환경 설정 .....</b>	<b>86</b>
5.1.	개요 .....	86
5.2.	네트워크 인터페이스에 IP 주소 할당 .....	86
5.3.	ARP(ADDRESS RESOLUTION PROTOCOL) .....	88
5.4.	STATIC ROUTES 설정 .....	88
5.5.	IP 설정 예제 .....	89
<b>6.</b>	<b>DHCP .....</b>	<b>93</b>
6.1.	DHCP SERVER 기능 및 설정 .....	93
6.1.1.	DHCP Server 기능 개요 .....	93
6.1.1.1.	DHCP Server 의 Address 할당 방법 .....	93
6.1.1.2.	U9200 Series 스위치를 DHCP Server 로 사용 .....	94
6.1.1.3.	U9200 Series 스위치를 DHCP relay agent 로 사용 .....	95
6.1.1.4.	DHCP Server 의 장점 .....	96
6.1.2.	DHCP Address Pool .....	96
6.1.3.	DHCP Network Pool 설정 .....	96
6.1.3.1.	DHCP Network Pool 이름 설정 및 DHCP 설정 모드 진입 .....	96
6.1.3.2.	DHCP 서브넷 및 Network 마스크 설정 .....	97
6.1.3.3.	Network Pool 에서 할당 할 IP Address 범위 설정 .....	97
6.1.3.4.	DHCP Server 부트 파일 설정 .....	98
6.1.3.5.	Client 를 위한 기본 라우터 설정 .....	98
6.1.3.6.	Client 를 위한 DNS IP Server 설정 .....	99
6.1.3.7.	Client 를 위한 도메인 이름 설정 .....	100
6.1.3.8.	네트워크 Pool 을 위한 그룹 설정 .....	100
6.1.3.9.	Address 임대 기간 설정 .....	101
6.1.3.10.	Client 를 위한 NetBios WINS IP Server 설정 .....	101
6.1.3.11.	Client 를 위한 NetBIOS 노드 타입 설정 .....	102
6.1.4.	DHCP Host Pool 설정 .....	103
6.1.4.1.	DHCP Host Pool 이름 설정 및 DHCP 설정 모드 진입 .....	103
6.1.4.2.	DHCP 수동 바인딩을 위한 Client 설정 .....	104
6.1.5.	기타 Global 명령어 .....	105
6.1.6.	Premier DHCP Server 기능 활성화 .....	106

6.2.	DHCP RELAY 기능 및 설정 .....	106
6.2.1.	DHCP Relay 기능 개요 .....	106
6.2.2.	Premier DHCP relay 기능 활성화 .....	107
6.2.3.	DHCP relay agent 에서 서버 설정 .....	108
6.2.4.	DHCP relay information option(OPTION82) 설정 .....	109
6.2.4.1.	DHCP relay information option 기능의 활성화 .....	109
6.2.4.2.	Relay information option 재중계 정책 설정 .....	110
6.2.5.	DHCP Smart Relay 설정 .....	111
6.2.6.	DHCP Relay Verify MAC-Address 설정 .....	112
6.2.7.	DHCP relay server-id-relay 설정 .....	113
6.3.	DHCP SNOOPING 기능 .....	114
6.3.1.	DHCP Snooping 기능 개요 .....	114
6.3.1.1.	Trust and Untrust Source .....	115
6.3.1.2.	DHCP Snooping Binding Database .....	115
6.3.1.3.	Packet Validation .....	115
6.3.1.4.	Packet Rate-limit .....	115
6.3.2.	DHCP Snooping 기능의 활성화 .....	115
6.3.3.	DHCP Snooping Vlan 설정 .....	116
6.3.4.	DHCP Snooping information option(OPTION82) 설정 .....	116
6.3.4.1.	DHCP Snooping information option 기능의 활성화 .....	117
6.3.4.2.	DHCP Snooping information option 재중계 정책 설정 .....	117
6.3.5.	DHCP Snooping Trust Port 설정 .....	118
6.3.6.	DHCP Snooping max-entry 설정 .....	119
6.3.7.	DHCP Snooping Entry Time 설정 .....	119
6.3.8.	DHCP Snooping Rate-Limit 설정 .....	120
6.3.9.	DHCP Snooping Verify MAC-Address 설정 .....	121
6.3.10.	DHCP Snooping Manual Binding 설정 .....	121
6.4.	DHCP SERVER 모니터링 및 관리 .....	122
6.4.1.	DHCP Server Pool 정보 조회 .....	122
6.4.2.	DHCP Server 바인딩 정보 조회 .....	122
6.4.3.	DHCP Server 통계 정보 조회 .....	123
6.4.4.	DHCP Server 충돌 정보 조회 .....	123
6.4.5.	DHCP Server 변수 초기화 명령어 .....	123
6.4.6.	DHCP Server 디버그 명령어 .....	123
6.5.	DHCP RELAY 모니터링 및 관리 .....	123
6.6.	DHCP SNOOPING 모니터링 및 관리 .....	124
6.7.	DHCP 설정 예제 .....	124
6.7.1.	DHCP Network Pool 설정 예제 .....	124
6.7.2.	DHCP Host Pool 설정 예제 .....	125
6.7.3.	DHCP Server 모니터링 및 관리 예제 .....	126
6.7.4.	DHCP Relay Agent 설정 .....	128
7.	RIP .....	130

7.1.	INFORMATION ABOUT RIP .....	130
7.2.	HOW TO CONFIGURE RIP .....	130
7.2.1.	Enabling RIP .....	131
7.2.2.	Allowing Unicast updates for RIP .....	131
7.2.3.	Passive interface .....	131
7.2.4.	Applying Offsets to Routing metrics.....	132
7.2.5.	Adjusting Timers .....	132
7.2.6.	Specifying a RIP Version .....	132
7.2.7.	Applying Distance .....	133
7.2.8.	Enabling Split Horizon .....	134
7.3.	CONFIGURATION EXAMPLES FOR RIP .....	134
7.3.1.	RIP 구성.....	134
7.3.2.	Offset-list 설정.....	137
7.3.3.	Passive-interface 설정 .....	137
<b>8.</b>	<b>OSPF.....</b>	<b>139</b>
8.1.	OSPF 개요 .....	139
8.1.1.	Link-state Database .....	140
8.1.2.	Areas.....	140
8.1.3.	AREA 0 .....	140
8.1.4.	Stub areas.....	141
8.1.5.	Virtual links.....	141
8.1.6.	Route Redistribution .....	141
8.2.	OSPF 설정 .....	142
8.2.1.	OSPF interface parameters.....	142
8.2.2.	Different Physical Networks.....	143
8.2.3.	OSPF Area parameters .....	145
8.2.4.	OSPF NSSA .....	145
8.2.5.	OSPF Area Route summarization .....	146
8.2.6.	Redistributed Routes 의 Route Summarization.....	147
8.2.7.	Virtual Links .....	147
8.2.8.	Generating a Default Route.....	147
8.2.9.	Default metric.....	148
8.2.10.	OSPF administrative Distance .....	148
8.2.11.	Passive interface .....	149
8.2.12.	Route Calculation Timers.....	149
8.2.13.	Logging Neighbors Going Up/Down .....	149
8.2.14.	Blocking LSA Flooding .....	150
8.2.15.	Ignoring MOSPF LSA Packets.....	150
8.2.16.	Monitoring and Maintaining OSPF.....	150
<b>9.</b>	<b>BGP.....</b>	<b>153</b>
9.1.	BGP 개요 .....	153
9.2.	BGP 설정 .....	153
9.1.1.	BGP 프로토콜의 활성화 .....	153

9.2.1.	<i>Neighbor 설정</i>	155
9.2.2.	<i>BGP 필터링 기능</i>	155
9.2.2.1.	Route Filtering	156
9.2.2.2.	Path Filtering	157
9.2.2.3.	Community Filtering	158
9.2.2.4.	BGP Attribute 설정	160
9.2.2.5.	As_path Attribute	161
9.2.2.6.	Origin Attribute	162
9.2.2.7.	BGP Nexthop Attribute	163
9.2.2.8.	BGP Nexthop (Multiple access networks)	165
9.2.2.9.	BGP Nexthop (NBMA)	166
9.2.2.10.	Next-hop-self	166
9.2.2.11.	Local Preference Attribute	167
9.2.2.12.	Metric Attribute	169
9.2.2.13.	Community Attribute	171
9.2.2.14.	Weight Attribute	172
9.1.2.	<i>Routing Policy 변경</i>	174
9.1.3.	<i>BGP Peer Groups</i>	175
9.1.4.	<i>BGP Multipath</i>	177
9.1.5.	<i>BGP graceful-restart</i>	179
9.1.6.	<i>BGP default-metric</i>	180
9.1.7.	<i>BGP redistribute-internal</i>	180
9.1.8.	<i>BGP Password encryption</i>	180
9.1.9.	<i>BGP disable-adj-out</i>	180
9.1.10.	<i>Use of set as-path prepend Command</i>	181
9.3.	ROUTE FLAP DAMPENING	181
<b>10.</b>	<b>IGMP SNOOPING</b>	<b>183</b>
10.1.	IGMP SNOOPING 개요	183
10.2.	IGMP SNOOPING 설정	183
10.2.1.	<i>Enable IGMP Snooping on a VLAN</i>	184
10.2.2.	<i>Configure IGMP Snooping Functionality</i>	184
10.2.2.1.	IGMP Report-Suppression	185
10.2.2.2.	IGMP Fast-Leave	186
10.2.2.3.	IGMP Mrouter-Port	187
10.2.2.4.	IGMP Access-Group	187
10.2.2.5.	IGMP Group-Limit	189
10.3.	DISPLAY SYSTEM AND NETWORK STATISTICS	190
<b>11.</b>	<b>IP 멀티캐스트 라우팅</b>	<b>191</b>
11.1.	IP 멀티캐스트 라우팅 개요	191
11.2.	IGMP 개요	192
11.3.	PIM-SM 개요	192
11.4.	IP 멀티캐스트 라우팅 설정	193
11.4.1.	<i>Enable IP 멀티캐스트 라우팅</i>	193
11.4.2.	<i>Enable IGMP-TRAP on an interface</i>	193
11.4.3.	<i>Enable PIM on an interface</i>	193

11.4.4.	Enable IGMP on an interface.....	194
11.4.5.	Configure IGMP Functionality.....	195
11.4.5.1.	IGMP Access Group.....	195
11.4.5.2.	IGMP filter-receive-query.....	195
11.4.5.3.	IGMP Query Transmit Interval.....	196
11.4.5.4.	IGMP Leave Timeout.....	197
11.4.5.5.	IGMP Member checking interval.....	197
11.4.5.6.	IGMP Querier Timeout.....	198
11.4.5.7.	IGMP Maximum Query Response Time.....	198
11.4.5.8.	IGMP query-based-port.....	199
<b>12.</b>	<b>시스템 및 통계 모니터링.....</b>	<b>200</b>
12.1.	상태 모니터링.....	200
12.2.	시스템 임계치 설정.....	201
12.2.1.	온도 설정.....	201
12.2.2.	Cpu usage 설정.....	202
12.2.3.	Memory Usage 설정.....	202
12.2.4.	Application memory 사용 display.....	202
12.3.	포트 통계.....	203
12.4.	RMON (REMOTE MONITORING).....	206
12.4.1.	RMON 개요.....	206
12.4.2.	RMON 의 Alarm 과 Event 그룹 설정.....	208
12.5.	LOGGING.....	211
12.5.1.	시스템 로그 메시지 내용.....	212
12.5.2.	디폴트 Logging 설정 값.....	213
12.5.3.	Logging 설정 예.....	213
12.6.	sFLOW.....	214
12.6.1.	sFlow agent.....	215
12.6.2.	sFlow collector.....	216
12.6.2.1.	sflowtool 설정.....	216
12.6.2.2.	sFlowTrend 설정.....	217
12.6.3.	sFlow Network 구성.....	218
12.6.3.1.	sFlow sampling 시험.....	218
<b>13.</b>	<b>STP(SPANNING TREE PROTOCOL).....</b>	<b>221</b>
13.1.	UNDERSTANDING SPANNING-TREE FEATURES.....	222
13.1.1.	STP Overview.....	222
13.1.2.	Bridge Protocol Data Units.....	222
13.1.3.	Election of Root Switch.....	223
13.1.4.	Bridge ID, Switch Priority, and Extended System ID.....	224
13.1.5.	Spanning-Tree Timers.....	224
13.1.6.	Creating the Spanning-Tree Topology.....	225
13.1.7.	Spanning-Tree Interface States.....	225
13.2.	UNDERSTANDING RSTP.....	229
13.2.1.	RSTP Overview.....	229
13.2.2.	Port Roles and the Active Topology.....	229

13.2.3.	Rapid Convergence .....	230
13.2.4.	Bridge Protocol Data Unit Format and Processing .....	231
13.3.	UNDERSTANDING MSTP .....	232
13.3.1.	MST 영역 .....	233
13.3.2.	IST, CST 및 CIST .....	233
13.4.	CONFIGURING SPANNING-TREE FEATURES .....	234
13.4.1.	Default STP Configuration .....	235
13.4.2.	STP Configuration Guidelines .....	235
13.4.3.	Enabling STP .....	235
13.4.4.	Enable STP in not default Bridge .....	237
13.4.5.	Configuring the Port Priority .....	238
13.4.6.	Configuring the Path Cost .....	240
13.4.7.	Configuring the Switch Priority of a VLAN .....	242
13.4.8.	Configuring the Hello Time .....	245
13.4.9.	Configuring the Forwarding-Delay Time for a VLAN .....	246
13.4.10.	Configuring the Maximum-Aging Time for a VLAN .....	249
13.4.11.	Changing the Max-hops for switch .....	250
13.4.12.	Changing the Spanning-Tree mode for switch .....	251
13.4.13.	Configuring portfast for switch .....	253
13.4.14.	Changing transmit-holdcount for switch .....	255
13.4.15.	Changing Cisco-interoperability for switch .....	256
13.4.16.	Configuring autoedge for port .....	256
13.4.17.	Configuring the Port as Edge Port .....	257
13.4.18.	Specifying the Link Type to Ensure Rapid Transitions .....	259
13.4.19.	Configuring force-version for port .....	259
13.4.20.	Configuring root guard for port .....	261
13.4.21.	Configuring hello-time for port .....	262
13.4.22.	Configuring portfast for port .....	262
13.4.23.	Configuring transmit-holdcount for port .....	263
13.4.24.	Configuring restricted-role for port .....	263
13.4.25.	Configuring restricted-tcn for port .....	264
13.5.	CONFIGURING MSTP FEATURES .....	265
13.5.1.	Instance 생성 및 VLAN 연결 .....	265
13.5.2.	instance and port configuration .....	267
13.5.3.	Setting region and revision number for MST .....	271
13.5.4.	Pathcost for MSTP .....	272
13.6.	DISPLAYING THE SPANNING-TREE STATUS .....	272
13.7.	CONFIGURING BRIDGE MAC FORWARDING .....	274
13.8.	SELF-LOOP DETECTION .....	276
13.8.1.	Understanding Self-loop Detection .....	277
13.8.2.	Configuring Self-loop Detection .....	278
13.8.2.1.	Enabling Self-loop Detection .....	278
13.8.2.2.	Changing The Service Status of Port .....	281
13.8.2.3.	Disabling Self-loop Detection .....	281
13.8.3.	Displaying Self-loop Status .....	283
14.	BFD .....	285

14.1.	UNDERSTANDING BFD .....	286
14.1.1.	BFD Operation .....	286
14.1.2.	Benefits of using BFD for Failure Detection .....	287
14.1.3.	BFD Session Type .....	287
14.1.4.	BFD Version Interoperability .....	288
14.2.	BFD RESTRICTIONS .....	288
14.3.	DEFAULT BFD CONFIGURATION .....	288
14.4.	CONFIGURING BFD .....	290
14.4.1.	Configuring BFD session parameters on the interface .....	290
14.4.2.	Configuring multi-hop BFD session parameters .....	291
14.4.3.	Configuring BFD support for BGP .....	291
14.4.4.	Configuring BFD support for OSPF .....	292
14.4.5.	Configuring BFD support for Static routing .....	293
14.4.6.	Configuring Passive Mode on the Interface .....	294
14.4.7.	Configuring BFD Echo Mode .....	295
14.4.8.	Configuring BFD slow timer .....	296
14.4.9.	Displaying BFD information .....	296
14.5.	BFD CONFIGURATION SAMPLES .....	296
14.5.1.	Sample One: Configuring BFD in an OSPF Network .....	297
14.5.2.	Sample Two: Configuring BFD in an BGP Network .....	299
14.5.3.	Sample Three: Configuring BFD for static routing .....	301
<b>15.</b>	<b>LACP .....</b>	<b>304</b>
15.1.	UNDERSTANDING LINK AGGREGATION CONTROL PROTOCOL .....	304
15.1.1.	LACP Modes .....	304
15.1.2.	LACP Parameters .....	305
15.2.	CONFIGURING 802.3AD LINK AGGREGATION CONTROL PROTOCOL .....	306
15.2.1.	Specifying the System Priority .....	306
15.2.2.	Specifying the Port Priority .....	306
15.2.3.	Specifying an Administrative Key Value .....	307
15.2.4.	Specifying the Timeout Value .....	308
15.2.5.	Changing the LACP Mode .....	308
15.2.6.	Clearing LACP Statistics .....	309
15.3.	DISPLAYING 802.3AD STATISTICS AND STATUS .....	309
<b>16.</b>	<b>IP-OPTION .....</b>	<b>310</b>
16.1.	IP OPTOIN 개요 .....	310
16.2.	IP OPTOIN 명령어 .....	310
<b>17.</b>	<b>VRRP .....</b>	<b>313</b>
17.1.	INFORMATION ABOUT VRRP .....	313
17.1.1.	VRRP Operation .....	313
17.1.2.	VRRP Benefits .....	315
17.1.3.	Multiple Virtual Router Support .....	316
17.1.4.	VRRP Router Priority and Preemption .....	316
17.1.5.	VRRP Advertisements .....	317
17.1.6.	VRRP Object Tracking .....	317



17.2.	HOW TO CONFIGURE VRRP .....	317
17.2.1.	Enabling VRRP .....	317
17.2.2.	Disabling VRRP on an Interface .....	318
17.2.3.	Configuring VRRP Object Tracking.....	319
17.3.	CONFIGURATION EXAMPLES FOR VRRP .....	320
17.3.1.	Configuring VRRP: Example.....	320
17.3.2.	VRRP Object Tracking: Example .....	321
17.3.3.	VRRP Object Tracking Verification: Example.....	321
17.3.4.	Disabling a VRRP Group on an Interface: Example .....	322
<b>18.</b>	<b>SETTING TIME AND CALENDAR .....</b>	<b>323</b>
18.1.	UNDERSTANDING TIME SOURCES .....	323
18.1.1.	Network Time Protocol.....	323
18.1.2.	Hardware Clock.....	324
18.2.	CONFIGURING NTP .....	324
18.2.1.	Configuring Poll-Based NTP Associations.....	324
18.2.2.	Configuring NTP Authentication.....	325
18.2.3.	Configuring the Source IP Address for NTP Packets.....	326
18.2.4.	Configuring the System as an Authoritative NTP Server .....	326
18.2.5.	Updating the Hardware Clock .....	326
18.3.	CONFIGURING TIME AND DATE MANUALLY .....	326
18.3.1.	Configuring the Time Zone.....	327
18.3.2.	Configuring Summer Time (Daylight Savings Time).....	327
18.3.3.	Manually Setting the Software Clock .....	327
18.4.	USING THE HARDWARE CLOCK.....	328
18.4.1.	Setting the Hardware Clock .....	328
18.4.2.	Setting the Software Clock from the Hardware Clock.....	328
18.4.3.	Setting the Hardware Clock from the Software Clock.....	329
18.5.	MONITORING TIME AND CALENDAR SERVICES .....	329
18.6.	CONFIGURATION EXAMPLES .....	329
18.6.1.	Clock, Calendar, and NTP Configuration Examples .....	329
<b>19.</b>	<b>DYNAMIC ARP INSPECTION .....</b>	<b>330</b>
19.1.	UNDERSTANDING DAI .....	330
19.1.1.	Understanding ARP.....	331
19.1.2.	Understanding ARP Spoofing Attacks.....	331
19.1.3.	Understanding DAI and ARP Spoofing Attacks.....	332
19.1.4.	Interface Trust States and Network Security.....	333
19.1.5.	Rate Limiting of ARP Packets .....	335
19.1.6.	Relative Priority of ARP ACLs and DHCP Snooping Entries .....	335
19.1.7.	Logging of Dropped Packets.....	335
19.2.	DEFAULT DAI CONFIGURATION .....	336
19.3.	DAI CONFIGURATION GUIDELINES AND RESTRICTIONS.....	336
19.4.	CONFIGURING DAI.....	337
19.4.1.	Enabling DAI on VLANs.....	337
19.4.2.	Configuring the DAI Interface Trust State .....	339
19.4.3.	Applying ARP ACLs for DAI Filtering .....	339

19.4.4.	Configuring ARP Packet Rate Limiting .....	340
19.4.5.	Enabling DAI Error-Disabled Recovery.....	342
19.4.6.	Enabling Additional Validation.....	342
19.4.7.	Configuring DAI Logging.....	345
19.4.8.	DAI Logging Overview .....	345
19.4.9.	Configuring the DAI Logging Buffer Size .....	345
19.4.10.	Configuring the DAI Logging System Messages .....	346
19.4.11.	Configuring the DAI Log Filtering.....	346
19.4.12.	Displaying DAI Information .....	347
19.5.	DAI CONFIGURATION SAMPLES .....	348
19.5.1.	Sample: Interoperate with DHCP Relay.....	348
<b>20.</b>	<b>QOS 및 ACL.....</b>	<b>351</b>
20.1.	QOS.....	351
20.1.1.	전역 설정.....	351
20.1.2.	TX Scheduling 설정.....	351
20.1.3.	Port trust 모드 .....	353
20.1.4.	DSCP 변환 map 설정.....	354
20.1.4.1.	DSCP to queue 설정 .....	354
20.1.4.2.	DSCP to COS 설정 .....	355
20.1.4.3.	DSCP to DSCP 설정 .....	356
20.1.5.	COS 변환 map 설정.....	357
20.1.5.1.	COS to queue 설정 .....	357
20.1.5.2.	COS to DSCP 설정.....	357
20.1.5.3.	COS to COS 설정.....	358
20.2.	ACL 설정 .....	359
20.2.1.	Standard IP ACL.....	359
20.2.2.	Extended IP ACL.....	360
20.2.3.	MAC ACL .....	362
20.2.4.	ACL 의 인터페이스 적용 .....	363
20.3.	SERVICE-POLICY 설정.....	363
20.3.1.	Class-map .....	364
20.3.2.	Policy-map .....	365
20.3.3.	Service-policy.....	367
20.4.	COPP .....	367
20.4.1.	Service-policy on COPP.....	368
20.4.2.	Rate-limit on COPP.....	368
<b>21.</b>	<b>UTILITIES.....</b>	<b>370</b>
21.1.	개 요.....	370
21.2.	상태 DUMP 명령 .....	370
21.2.1.	명령어.....	370
21.3.	COMMAND HISTORY 기능 .....	372
21.4.	OUTPUT POST PROCESSING .....	372
21.4.1.	output post processing 개요.....	372

21.4.2.	<i>output post processing 예제</i> .....	373
21.5.	DDM (DIGITAL DIAGNOSTIC MONITORING) .....	374
21.5.1.	<i>GBIC DDM Monitoring</i> .....	374
<b>22.</b>	<b>환경설정 저장 및 소프트웨어 업그레이드</b> .....	<b>375</b>
22.1.	파일 시스템 .....	375
22.2.	IMAGE/CONFIGURATION/BSP DOWN/UP LOAD .....	378
22.2.1.	<i>FTP 를 통한 Down/Up Load</i> .....	378
22.2.2.	<i>TFTP 를 통한 Down/Up Load</i> .....	379
22.3.	CONFIGURATION 파일 관리 .....	381
22.3.1.	<i>Configuration 파일 저장</i> .....	381
22.3.2.	<i>Configuration 파일 삭제</i> .....	382
22.4.	BOOT MODE 설정 및 시스템 재시동 .....	383
22.4.1.	<i>Boot Mode 설정</i> .....	383
22.4.2.	<i>시스템 재시동</i> .....	383
<b>23.</b>	<b>GPON</b> .....	<b>386</b>
23.1.	GPON OVERVIEW .....	387
23.2.	OLT/ ONT MANAGEMENT .....	388
23.2.1.	<i>PON OLT, PORT 의 상태 설정 / 조회</i> .....	388
23.2.2.	<i>ONU/ONT 의 상태 설정 / 조회</i> .....	390
23.2.3.	<i>Registering/Retrieving ONTs</i> .....	391
23.2.4.	<i>ONU/ONT 의 정보 변경 및 삭제</i> .....	392
23.2.5.	<i>Clearing and viewing ONU/ONT unadmin-list</i> .....	393
23.2.6.	<i>Removing information of ONU/ONTs not in use automatically</i> .....	393
23.2.7.	<i>ONU/ONT equip-id 인증 기능 : equip-id 등록/삭제 및 조회</i> .....	394
23.2.8.	<i>ONU/ONT equip-id 인증 기능 : 기능 운용 Description</i> .....	396
23.2.9.	<i>Creating vlan mapping table (QinQ)</i> .....	397
23.3.	PON CONFIGURATION .....	397
23.3.1.	<i>PON OLT Configuration</i> .....	397
23.3.1.1.	<i>Creating and applying OLT Service Profile</i> .....	398
23.3.1.2.	<i>Creating OLT Policy-map</i> .....	398
23.3.1.3.	<i>Creating OLT Bridge-map</i> .....	400
23.3.1.4.	<i>Creating OLT Igmp-map</i> .....	401
23.3.2.	<i>PON ONU Configuration</i> .....	403
23.3.2.1.	<i>Creating and removing ONU Sla-map</i> .....	404
23.3.2.2.	<i>Creating or removing ONU Bridge-map</i> .....	405
23.3.2.3.	<i>Creating/Removing ONU Multicast-map</i> .....	408
23.3.2.4.	<i>ONU default service-policy 의 설정 및 조회</i> .....	409
23.3.2.5.	<i>Creating, retrieving, and removing ONU service-policy</i> .....	409
23.4.	MANAGING ONTs WITH FAULTY OPTIC MODULE .....	410
23.4.1.	<i>광모듈 불량 ONU/ONT 자동 shutdown</i> .....	410
23.4.2.	<i>ONT 광모듈 tx-power 제한</i> .....	410
23.5.	FIRMWARE UPGRADE .....	411
23.5.1.	<i>OLT firmware upgrade</i> .....	411

23.5.2.	ONT/ONU firmware upgrade (manual-upgrade).....	413
23.5.3.	ONT/ONU firmware upgrade (auto-upgrade) .....	414

## 표 목차

---

표 1-1.	문자 표시 규칙 .....	21
표 1-2.	알림 및 경고 아이콘 .....	21
표 2-1.	명령어 구문 심볼 .....	27
표 2-2.	명령어 라인 편집 명령 및 도움말 기능 .....	28
표 2-3.	스위치 명령어 모드 .....	29
표 2-4.	스위치의 명령어 모드 사이의 이동 .....	29
표 2-5.	스위치의 사용자 추가 및 삭제 명령어 .....	32
표 2-6.	스위치의 ENABLE 패스워드 설정 명령어 .....	34
표 2-7.	사용자 인증 설정 명령어 .....	35
표 2-8.	PRIVILEGED MODE 사용자 인증 설정 명령어 .....	36
표 2-9.	사용자 권한 부여 설정 명령어 .....	37
표 2-10.	명령어 모드 권한 설정 명령어 .....	38
표 2-11.	명령어 권한허가 설정 명령어 .....	38
표 2-12.	세션 관리 설정 명령어 .....	39
표 2-13.	명령어 관리 설정 명령어 .....	40
표 2-14.	RADIUS 서버 설정 명령어 .....	40
표 2-15.	TACACS+ 서버 설정 명령어 .....	42
표 2-16.	HOSTNAME 설정 명령어 .....	43
표 2-17.	SNMP 환경 설정 명령 .....	43
표 2-18.	액세스 리스트 설정 명령 .....	47
표 3-1.	U9200 SERIES 스위치가 지원하는 인터페이스 .....	52
표 3-2.	공통 명령어 .....	52
표 3-3.	INTERFACE NAME .....	53
표 3-4.	INTERFACE ID 및 지원 범위 .....	53
표 3-5.	인터페이스 정보 및 상태 관련 명령어 .....	54
표 3-6.	물리적 포트 환경 설정 명령어 .....	56
표 3-7.	MEDIA-TYPE 설정 명령어 .....	58
표 3-8.	2 계층 인터페이스 기본 설정 값 .....	60
표 3-9.	2 계층 인터페이스 설정 및 해제 명령어 .....	60
표 3-10.	TRUNK PORT 설정 명령어 .....	61
표 3-11.	ACCESS PORT 설정 명령어 .....	62
표 3-12.	포트 그룹 설정 명령어 .....	62

표 3-13. 3 계층 인터페이스 환경 설정 명령어 .....	63
표 3-14. CPU-MAC-FILTER 관련 명령어 .....	63
표 3-15. SDM 관련 명령어 .....	65
표 3-16. TRAFFIC-CONTROL 설정 명령어 .....	65
표 3-17. TRAFFIC-CONTROL 설정 명령어 .....	66
표 3-18. LLCF MODE 별 동작 .....	66
표 3-19. LLCF 설정 명령어 .....	67
표 4-1. VLAN 설정 명령어 .....	77
표 4-2. 802.1 QINQ 명령어 사용법 테이블 .....	81
표 4-3. PRIVATE EDGE VLAN 설정표 .....	84
표 4-4. 비정상 MAC 차단 명령어 .....	85
표 5-1. 사용 가능한 IP 주소 .....	86
표 5-2. IP 주소 할당 명령어 .....	87
표 5-3. ARP 환경 설정을 위한 명령어 .....	88
표 5-4. STATIC ROUTE 경로 설정 명령어 .....	88
표 5-5. 동적 라우팅 프로토콜의 DEFAULT ADMINISTRATIVE DISTANCES .....	89
표 8-1. LSA TYPE NUMBER .....	140
표 8-2. OSPF INTERFACE PARAMETER CLI .....	142
표 8-3. OSPF NETWORK TYPE CLI .....	143
표 8-4. P-TO-MULTIPOINT NETWORK, BROADCAST NETWORK 설정 .....	144
표 8-5. NON BROADCAST NETWORK CLI .....	144
표 8-6. NON BROADCAST NETWORK 설정 .....	144
표 8-7. OSPF AREA PARAMETER CLI .....	145
표 8-8. OSPF NSSA CLI .....	146
표 8-9. OSPF AREA ROUTE SUMMARIZATION CLI .....	146
표 8-10. EXTERNAL ROUTE SUMMARIZATION CLI .....	147
표 8-11. OSPF VIRTUAL LINK CLI .....	147
표 8-12. OSPF DEFAULT ROUTE CLI .....	148
표 8-13. LOOPBACK INTERFACE 설정 .....	148
표 8-14. REFERENCE BANDWIDTH CLI .....	148
표 8-15. OSPF DISTANCE CLI .....	149
표 8-16. OSPF PASSIVE INTERFACE CLI .....	149
표 8-17. OSPF SPF TIMER CLI .....	149
표 8-18. OSPF ADJACENCY LOG CLI .....	150
표 8-19. BLOCK LSA CLI .....	150
표 8-20. IGNORE MOSPF LSA CLI .....	150
표 8-21. MONITORING OSPF CLI .....	151
표 8-22. MAINTAINING OSPF CLI .....	152
표 9-1. ROUTE DAMPENING 에 사용되는 용어 .....	182
표 11-1. 멀티캐스트 프로토콜 .....	192
표 12-1. 상태 모니터링 명령어 .....	201

표 12-2. 온도 설정 관련 명령어 .....	201
표 12-3. CPU USAGE THRESHOLD 관련 명령어 .....	202
표 12-4. MEMORY USAGE 관련 명령어 .....	202
표 12-5. MEMORY DISPLAY 관련 명령어 .....	202
표 12-6. 포트 통계 조회 명령들 .....	204
표 12-7. 포트 통계 설정 명령 .....	205
표 12-8. 포트 통계 초기화 명령 .....	206
표 12-9. RMON 항목 .....	207
표 12-10. RMON ALARM AND EVENT 설정 명령 .....	208
표 12-11. RMON HISTORY 설정 및 STATISTICS 명령 .....	210
표 12-12. U9200 SERIES 스위치의 로그 레벨 .....	212
표 12-13. 시스템 로그 기본 설정 값 .....	213
표 12-14. 시스템 메시지 로깅 환경 설정 명령 .....	213
표 13-1 SWITCH PRIORITY VALUE AND EXTENDED SYSTEM ID .....	224
표 13-2 SPANNING-TREE TIMERS .....	225
표 13-3 PORT STATE COMPARISON .....	230
표 13-4. RSTP BPDU FLAGS .....	232
표 13-5. DEFAULT STP CONFIGURATION .....	235
표 20-1. QOS 전역 설정 명령어 .....	351
표 20-2. TX-SCHEDULING MAP 설정 명령어 .....	353
표 20-3. TX-SCHEDULING 설정 명령어 .....	353
표 20-4. PORT TRUST 설정 명령어 .....	354
표 20-5. DSCP-QUEUE MAP 설정 명령어 .....	355
표 20-6. DSCP-COS MAP 설정 명령어 .....	356
표 20-7. DSCP-MUTATION MAP 설정 명령어 .....	356
표 20-8. COS-QUEUE MAP 설정 명령어 .....	357
표 20-9. COS-DSCP MAP 설정 명령어 .....	358
표 20-10. COS-MUTATION MAP 설정 명령어 .....	358
표 20-11. STANDARD IP ACL 설정 명령어 .....	359
표 20-12. EXTENDED IP ACL 설정 명령어 .....	361
표 20-13. STANDARD IP ACL 설정 명령어 .....	362
표 20-14. ACL의 인터페이스 적용 설정 명령어 .....	363
표 20-15. CLASS-MAP 설정 명령어 .....	364
표 20-16. CLASS-MAP 설정 명령어 .....	366
표 20-17. SERVICE-POLICY 설정 명령어 .....	367
표 20-18. SERVICE-POLICY의 CONTROL-PLANE 적용 설정 명령어 .....	368
표 20-19. RATE-LIMIT의 CONTROL-PLANE 적용 설정 명령어 .....	368
표 22-1. 파일 관리를 위한 명령어 .....	376
표 22-2. FTP를 통한 Down/Up Load 명령어 .....	378
표 22-3. TFTP를 통한 Down/Up Load 명령어 .....	380
표 22-4. CONFIGURATION MANAGEMENT 명령어 .....	381

표 22-5. BOOT MODE 설정 및 시스템 재 시동 명령어 .....	383
표 22-6. BOOT MODE 설정 및 시스템 재 시동 명령어 .....	383

## 그림 목차

그림 2-1. U9200 SERIES 스위치와 운영 단말 연결.....	31
그림 4-1. U9200 SERIES 스위치의 포트 기반 VLAN 구성 예 .....	70
그림 4-2. 두 스위치에 걸쳐서 설정된 단일 포트 기반 VLAN.....	71
그림 4-3. 두 스위치에 걸쳐서 설정된 두 개의 포트 기반 VLAN.....	72
그림 4-4. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 물리적 다이어그램.....	74
그림 4-5. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 논리적 다이어그램.....	74
그림 4-6. NATIVE VLAN.....	76
그림 4-7. VLAN 설정 예제 – TAGGED AND UNTAGGED VLAN .....	79
그림 4-8. 802.1 QINQ 설정 .....	82
그림 5-1. 네트워크 설정 예 – 복수 IP ADDRESS.....	90
그림 5-2. 네트워크 설정 예 – STATIC ROUTE.....	91
그림 6-1. U9200 SERIES 스위치를 DHCP SERVER 로 사용 .....	94
그림 6-2. DHCP RELAY AGENT로서 DHCP SERVER의 메시지 전달 .....	95
그림 6-3. DHCP RELAY AGENT로서 DHCP SERVER의 메시지 전달.....	107
그림 6-4. DHCP RELAY OPTION82 .....	109
그림 6-5. DHCP SMART-RELAY 동작 절차 .....	111
그림 6-6. DHCP RELAY SERVER-ID-RELAY 동작 절차 .....	113
그림 7-1. RIP를 설정한 네트워크 예제 설정 및 구성도 .....	135
그림 8-1. OSPF NETWORK.....	146
그림 11-1. 여러 목적지에 트래픽을 전달하는 방법을 제공하는 멀티캐스팅 .....	191
그림 12-1. RMON MANAGER와 RMON PROBE .....	207
그림 13-1. SPANNING-TREE TOPOLOGY .....	225
그림 13-2. SPANNING-TREE INTERFACE STATES .....	226
그림 13-3. PROPOSAL AND AGREEMENT HANDSHAKING FOR RAPID CONVERGENCE .....	231
그림 13-4. VLAN에 대한 LOAD BALANCE.....	233
그림 13-5. CST, IST, CIST.....	234
그림 13-6. CST에서 인식하는 네트워크.....	234
그림 13-7. RESTRICTED-TCN.....	265
그림 13-8. SELF-LOOP 발생 환경 .....	278
그림 14-1 ESTABLISHING A BFD NEIGHBOR RELATIONSHIP.....	286
그림 14-2 TEARING DOWN AN OSPF NEIGHBOR RELATIONSHIP .....	287
그림 14-3 BFD SINGLE HOP SESSION .....	287



그림 14-4 BFD MULTHOP SESSION .....	288
그림 17-1 BASIC VRRP TOPOLOGY .....	314
그림 17-2 LOAD SHARING AND REDUNDANCY VRRP TOPOLOGY .....	315
그림 20-1. POLICY-MAP 의 계층도 .....	366

# 1

## 서문

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

### 1.1. 개요

본 가이드는 U9200 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**

U9200 Series 스위치 하드웨어의 설치 및 초기 설정과 관련된 정보는 각 시스템의 하드웨어 설치 가이드를 참고하기 바란다.



## 1.2. 적용 규칙

다음의 <표 1-1>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"> <li>명령 수행 등의 결과로 운영 단말에 표현되는 정보</li> <li>CLI 명령어 문법</li> </ul>
<b>Screen displays bold</b>	<ul style="list-style-type: none"> <li>운영자가 운영 단말에 직접 입력한 명령어</li> </ul>
[Key] 입력	<ul style="list-style-type: none"> <li>키보드의 키 입력을 나타내는 경우 [Enter] 또는 [Ctrl]과 같이 대괄호와 함께 사용</li> <li>둘 이상의 키를 동시에 입력하는 경우 [Ctrl] + [z]와 같이 키를 “+”로 연결하여 표현</li> </ul>
<i>이탤릭체</i>	<ul style="list-style-type: none"> <li>강조하는 부분이나 문장에서 새로 정의될 때 사용</li> <li>시스템 명령어 문법에서 사용자가 입력해야 하는 파라미터</li> </ul>

표 1-2. 알림 및 경고 아이콘

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

## 1.3. 관련 문서

U9200 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"> <li>■ 스위치 하드웨어 설치</li> <li>■ 초기 운용 환경 설정</li> </ul>
<i>User Guide</i>	<ul style="list-style-type: none"> <li>■ 서비스 제공을 위한 운용 환경 설정</li> <li>■ 시스템 운용 관리 및 유지보수</li> <li>■ 문제 해결(Trouble shooting)</li> </ul>



### Notice

U9200 Series 스위치를 포함한 (주)유비쿼스 네트워크의 제품에 대한 최신 문서 및 관련 정보들은 홈페이지(<http://www.ubiquoss.com>)를 통하여 다운로드 받거나 서비스를 요청할 수 있다.

## 2

U9200 Series  
스위치 시작하기

본 장은 다음과 같이 시스템 운영자가 U9200 Series 3 계층 스위치의 운용 환경을 설정하고 처음 다루기 시작할 때 필요한 정보를 제공한다.

- 편집 및 도움말 기능
- 스위치 명령어 모드의 이해
- 스위치 가동
- U9200 Series 스위치 사용자 인터페이스
- 스위치 로그인과 패스워드의 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

본 장은 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 ↵
% Command incomplete.
Switch #
```

### 2.1.2. 명령어 문법 도움말(Command Syntax Helper)

U9200 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. U9200 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.

전체 도움말 기능을 show 명령어를 통하여 보면 다음과 같다. show 명령어 다음에 공백 문자와 함께 ‘?’를 입력하면 운영자가 입력 할 수 있는 파라미터 및 값의 리스트가 출력된다. 그리고 다시 “u U9200 Series# show” 프롬프트 상태에서 커서가 깜박이면서 운영자의 입력을 대기한다. 운영자 입력에서 ‘?’는 화면에 표시되지 않는다.

```
Switch# show ?
  arp                Display ARP table entries
  authentication     Authentication configurations parameters
```

---

boot	When system booting, physical port shutdown or not
clock	show current system's time
config	Show config file information
config-list	display config file list
cpu	CPU information
cpu-filter	CPU Filter
cpu-mac-filter	MAC Blocking Table based on CPU load
cpu-packet-counter	CPU packet-counter
cpuload	CPU load information
debugging	Debugging functions
dump	dump-traffic
dump-file	tcpdump log file
environment	Temperature and FAN status information
flash:	display information about flash file system
flow	flow-rule
flow-rule	flow-rule
history	Show all contents of command history buffers
hostkeepalive	Check the keepalive for the specific host
inet-service	Display enabled internet services
interface	Interface status and configuration
ip	IP information
lacp	Port group information
license	Set enhanced software feature license
llcf-group	Link Loss Carry Forward group
logging	Show all contents of logging buffers
loop-detect	Enable self-loop detection
mac	Display MAC address table entries
mac-address-table	Display MAC address table entries
mac-count	MAC count configuration
mac-threshold	MaxMac Threshold information
max-hosts	MAC count (max-hosts) configuration
memory	Memory statistics
mirroring	Port mirroring configuration
mode	command mode
ntop	NTOP Web service
ntp	show current ntp status
policy	Policy Map Table
policy-map	Policy Map Table
port	Port status and configuration
port-group	Port-group configuration
port-mib	Port-Mib Count
private-edge-vlan	Private edge vlan configuration
privilege	Display your current level of privilege
processes	Active process statistics
qos	Qos configuration
rate-limit	Display rate-limit control parameters
rmon	Remote Monitoring
route-map	route-map information
running-config	Current operating configuration
sdm	Show SDM configuration
self-loop-detection	Enable self-loop detection
service-policy	service-policy information

---



---

sflow	sFlow
snmp	display snmp configuration
spanning-tree	Spanning tree topology
startup-config	Show startup config file information
switchport	Switching port configuration
syslog	syslog
system	Display the system information
tc-table	traffic-conditioner-table
tech-support	Display general information about the switch
temperature	Temperature and Threshold information
track	Tracking information
uptime	Display elapsed time since boot
users	Display information about terminal lines
version	Display the system version
vlan	VLAN information
vrrp	Virtual Router Redundancy Protocol (VRRP)
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?
      pdp          Global PDP configuration subcommands
      port         Display port configuration
      port-group   Port group information
Switch# show p_
```

---

### 2.1.3. 단축 명령어 입력

U9200 Series 스위치의 CLI 는 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 **U9200 Series** 스위치가 명령어를 구분하여 인식할 수 있도록 충분히 입력해야 한다. "% Ambiguous command."라는 메시지를 받을 때가 있다. 이것은 해당 모드에 입력한 문자와 **Prefix** 가 같은 하나 이상의 명령어가 있음을 의미한다.

```
Switch# show i
% Ambiguous command.
```

```
Switch# show i ?
ip                IP information
logging           Show all contents of logging buffers
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"> <li>명령어 문법에서 하나의 변수 또는 값을 의미한다. 이렇게 표현된 파라미터는 반드시 입력을 해야 한다.</li> <li>예를 들어, 다음과 같은 명령어가 있을 때  <code>access-list &lt;1-99&gt; (deny permit) address</code>                      표준 IP access control list 번호는 &lt;1-99&gt; 사이의 값으로 반드시 입력해야 한다.                 </li> </ul>
{ }:	Braces	<ul style="list-style-type: none"> <li>명령어 문법에서 사용되는 파라미터 또는 값의 리스트</li> <li>시스템 운영자는 리스트에 포함된 항목 중에서 최소한 하나 이상을 입력해야 한다.</li> <li>예를 들어, 다음과 같은 명령어가 있을 때  <code>router {rip ospf}</code>                      시스템 운영자는 라우팅 프로토콜로서 RIP 또는 OSPF 중의 하나를 반드시 명시해야 한다.                 </li> </ul>
[]:	Square brackets	<ul style="list-style-type: none"> <li>명령어 문법에서 사용되는 파라미터 또는 값의 리스트</li> <li>시스템 운영자는 리스트에 포함된 항목 중에서 필요한 항목을 선택적으로 입력한다. 경우에 따라서는 하나도 입력을 하지 않을 수도 있다.</li> <li>예를 들어, 다음과 같은 명령어가 있을 때  <code>show interface [ifname]</code>                      인터페이스의 이름을 정의하지 않을 수도 있다.                 </li> </ul>
:	Vertical bar	<ul style="list-style-type: none"> <li>파라미터 리스트에서 상호 배타적인 항목들을 표현</li> </ul>
<i>Italic 체</i>		<ul style="list-style-type: none"> <li>입력할 변수들</li> </ul>
<b>Bold 체</b>		<ul style="list-style-type: none"> <li>운영자가 입력해야 하는 명령어</li> </ul>

심볼	이름	설명
A.B.C.D		■ IP 주소 또는 서브넷 마스크를 의미
A.B.C.D/M		■ IP prefix 를 의미 (예. 192.168.0.0/24)

### 2.1.5. 명령어 라인 편집 키 및 도움말

U9200 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]	■ 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"> <li>■ 명령어의 일부분을 치고 [tab]을 치면 그 prompt 에서 같은 prefix 를 가진 명령어가 여러 개 있을 경우 리스트를 표시</li> <li>■ 한 개의 명령어만 있을 경우 명령어 나머지 부분을 완성</li> </ul>
[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"> <li>■ prompt 상에서 사용 가능한 명령어의 리스트와 설명을 표시</li> <li>■ 명령어 다음에 '?'를 쳤을 경우, 해당 명령어 다음에 입력해야 할 파라미터 리스트를 표시</li> <li>■ 부분적인 명령어에 바로 붙여서 '?'를 입력했을 경우 같은 prefix 를 가진 명령어의 리스트를 표시</li> </ul>
Return 또는 Spacebar 또는 Q	<ul style="list-style-type: none"> <li>■ -- More -- 에서 Return 키를 누르면 다음 한 line 이 표시</li> <li>■ Spacebar 를 누르면 다음 페이지가 표시되며, Q 를 누르면 종료하고 prompt 상태로 전환</li> </ul>

## 2.2. 스위치 명령어 모드

U9200 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-gil) # 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 U9200 Series 스위치의 이름을 호스트 이름으로 사용한다. 본 가이드에서는 'Switch' 프롬프트를 공통의 호스트 이름으로서 사용한다.

시스템 운영자는 U9200 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	■ User 모드에서 Privileged 모드로 이동 ■ Privileged 모드의 패스워드를 입력할 필요
disable	■ Privileged 모드에서 User 모드로 이동
configure terminal	■ Privileged 모드에서 Config 모드로 이동
interface ifname	■ Config 모드에서 Interface 모드로 이동
router {rip ospf}	■ Config 모드에서 Router 모드로 이동
exit	■ 이전의 모드로 이동
end	■ 어느 모드에서든 Privileged 모드로 이동 ■ User 모드에서는 이동하지 않는다.
ip dhcp network-pool name ip dhcp host-pool name	■ Config 모드에서 DHCP pool 설정 모드로 이동

## 2.3. U9200 Series 스위치 가동

U9200 Series 스위치는 처음 가동될 때, 자체 테스트를 실행하고 플래시 메모리로부터 OS image를 찾아서 메모리에 로드 하여 시스템을 시작한다. 시스템 부팅이 완료되면 플래시 메모리에 저장되어 있는 이전 환경 설정 값(startup-config)을 로딩한다.

**Notice**

U9200 Series 스위치는 시스템 안정성을 위하여 Primary 및 Secondary 등 두 개의 OS image를 관리한다. 기본적으로 Primary OS image가 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 U9200 Series 스위치가 제공하는 별도의 콘솔 포트를 통하여 직접 접속하는 것이다(*Out-of-band management*).

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

운영자는 아래의 방법을 사용하여 U9200 Series 스위치를 관리할 수 있다.

- 콘솔 포트에 터미널을 연결해서 CLI 접속.
- TCP/IP 기반 네트워크에서 Telnet 연결을 사용하여 CLI 접속.
- SNMP Network Manager를 통해서 관리.

U9200 Series 스위치는 운영 관리를 위하여 다음과 같이 동시 접속 연결을 지원한다.

- 1 개의 콘솔 연결
- 최대 10 개의 telnet 연결

### 2.4.1. 콘솔 연결

시스템에 내장된 CLI는 RJ-45 형태의 이더넷 포트를 통하여 접속이 가능하다. 이를 위하여 운영 단말(또는 terminal emulation 소프트웨어가 탑재된 워크스테이션)은 9핀, RS-232 DB9 포트를 지원해야 한다. 콘솔 포트는 U9200 Series 스위치의 경우 후면의 SGIM(Switching, Gigabit ethernet I/O & Management Module) 모듈에 탑재된다.

그림 2-1>과 같이 U9200 Series 스위치가 제공하는 콘솔 포트에 운영 단말을 연결한다. 일단 연결이 설정되면, 프롬프트가 나오고 로그인 프로세스를 수행한다.

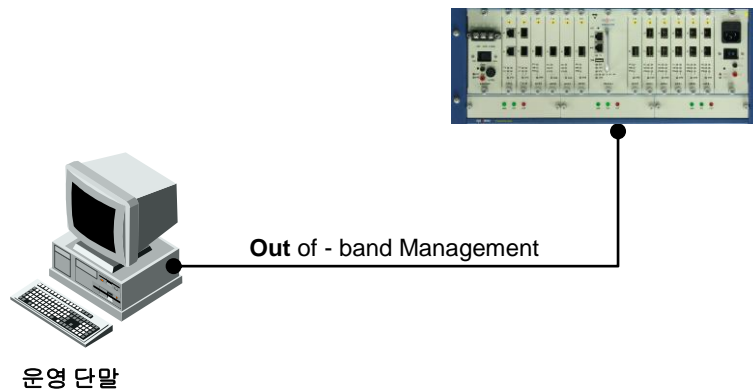


그림 2-1. U9200 Series 스위치와 운영 단말 연결



**Notice**

운영 단말의 설정 방법 및 콘솔 포트 핀 설정은 U9200 Series 스위치 하드웨어 설치 가이드를 참조하기 바란다.

## 2.4.2. Telnet 연결

시스템 운영자는 TCP/IP 및 telnet 접속 기능을 가지고 있는 워크스테이션을 통하여 U9200 Series 스위치에 접속할 수 있다. Telnet 을 사용하기 위하여, 운영자는 ID 및 비밀번호를 설정하여야 하며, 스위치는 적어도 하나 이상의 IP 주소를 가지고 있어야 한다.

```
telnet {<ipaddress> | <hostname>} [<port_number>]
```

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

또한 시스템 보안을 위하여 액세스 리스트를 사용하여 telnet 에 연결하는 사용자를 제한할 수 있다. 이는 <2.13. ACL(Access Control List)>절을 참조하라.

## 2.4.3. SNMP Network Manager 를 통한 연결

Simple Network Management Protocol (SNMP)를 지원하는 어떠한 네트워크 관리기(Network Manager)를 통해서도 U9200 Series 스위치를 관리할 수 있다.



**Notice**

SNMP 에 대한 추가적인 정보는 <2.7. SNMP>절을 참조하라.

## 2.5. 계정 관리 및 인증

### 2.5.1. 사용자 추가 및 삭제

시스템 운영자는 콘솔 포트나 telnet 을 통해서 스위치에 로그인 할 수 있다. 로그인을 위해서 사용자 등록이 필요하다. U9200 series 스위치는 사용자를 추가, 삭제 할 수 있고 각각의 사용자에게 대해 패스워드와 권한, session timeout 시간, Access List 를 지정할 수 있다.

사용자 권한은 privilege level 로 표현된다. privilege level 은 15 인 경우와 아닌 경우로만 구분하고, 0 에서 14 사이의 privilege level 간의 구분은 사용하지 않는다. privilege level 이 15 인 사용자는 enable mode 로 들어갈 수 있고, 그 외의 privilege level 을 갖는 사용자는 Privileged mode 로 들어갈 수 없다. 새로운 사용자를 등록하면 privilege level 이 1 인 사용자로 등록된다.



#### Notice

Access List 에 대한 추가적인 정보는 < [2.11. ACL](#) > 절을 참조하라

표 2-5. 스위치의 사용자 추가 및 삭제 명령어

명령어	설명	모드
username <i>userID</i> nopassword	<ul style="list-style-type: none"> <li>■ <i>userID</i> 생성</li> <li>■ password 가 없다</li> </ul>	Config
username <i>userID</i> password <i>password</i> username <i>userID</i> password 0 <i>password</i>	<ul style="list-style-type: none"> <li>■ <i>userID</i> 생성</li> <li>■ 암호화되지 않은 password 를 입력 받는다</li> </ul>	Config
username <i>userID</i> password 7 <i>password</i>	<ul style="list-style-type: none"> <li>■ <i>userID</i> 생성</li> <li>■ 암호화된 password 를 입력 받는다</li> </ul>	Config
username <i>userID</i> privilege <0-15> nopassword	<ul style="list-style-type: none"> <li>■ <i>userID</i> 생성</li> <li>■ password 가 없다</li> <li>■ privilege 15 이면 가장 높은 privilege(privileged mode 진입허용)를 갖는다.</li> </ul>	Config
username <i>userID</i> privilege <0-15> password <i>password</i> username <i>userID</i> privilege <0-15> password 0 <i>password</i>	<ul style="list-style-type: none"> <li>■ <i>userID</i> 생성</li> <li>■ privilege 15 이면 가장 높은 privilege(privileged mode 진입허용)를 갖는다.</li> <li>■ 암호화되지 않은 password 를 입력 받는다</li> </ul>	Config
username <i>userID</i> privilege <0-15> password 7 <i>password</i>	<ul style="list-style-type: none"> <li>■ <i>userID</i> 생성</li> <li>■ privilege 15 이면 가장 높은 privilege(privileged mode 진입허용)를 갖는다.</li> </ul>	Config



	■ 암호화된 password 를 입력 받는다	
username <i>userID</i> timeout <0-600>	■ user 별 session timeout 시간(분) 설정(default 20 분)	Config
no username <i>userID</i> timeout	■ user 별 session timeout 시간(분) 삭제 ■ 초기 session timeout 시간(20 분)으로 되돌린다.	Config
username <i>userID</i> access- class <1-99>	■ 해당 user 에 Access List 를 적용 ■ <i>access-list-num</i> : <1-99> 이며, standard ip access list 를 의미	Config
no username <i>userID</i> access-class	■ 해당 user 에 적용된 Access List 를 해제.	Config
no username <i>userID</i>	■ userID 삭제 ■ userID 가 root 이면 삭제되지 않고 password 가 default password 로 바뀐다.	Config

### 2.5.1.1. 사용자 추가 및 삭제

```
Switch# configure terminal
Switch# configure terminal
Switch(config)# username lns nopassword
Switch(config)# username test password test
Switch(config)# username admin privilege 15 password admin
Switch(config)# username admin timeout 50
Switch(config)# end
Switch # show running-config
!
service password-encryption
!
username root timeout 0
username lns nopassword
username test password 7 xx1LtDbOY4/E
username admin privilege 15 password 7 xxiz1FI3TBLPs
username admin timeout 50
!
Switch#
```

### 2.5.2. 패스워드 설정

U9200 series 스위치는 시스템 보안을 위해 다음과 같은 2 개의 패스워드를 사용한다.

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

표 2-6. 스위치의 Enable 비밀번호 설정 명령어

명령어	설명	모드
<code>enable password password</code>	■ Privileged 모드 패스워드를 지정	Config
<code>no enable password</code>	■ Privileged 모드 패스워드를 삭제	Config
<code>service password- encryption</code>	■ password encryption mode 를 설정	Config
<code>no service password- encryption</code>	■ password encryption mode 를 삭제	Config



**Notice**

사용자 비밀번호 설정명령은 <[2.5.1. 사용자 추가 및 삭제](#)>를 참고하라

### 2.5.2.1. Privileged 모드 패스워드 설정

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

### 2.5.2.2. 패스워드 encryption 설정

위의 예에서 보듯이 패스워드 설정 후 `show running-config` 명령으로 설정된 패스워드를 볼 수 있다. 이를 방지하기 위하여 U9200 Series 스위치는 패스워드 encryption 모드 설정을 지원한다.

```
Switch# configure terminal
Switch(config)# service password-encryption
Switch(config)# end
Switch# show running-config
!
enable password 7 xxEp88GxHJIgc
username lns nopassword
username test password 7 XX1LtDbOY4/E
username admin privilege 15 password 7 xxiz1FI3TBLPs
!
Switch#
```

### 2.5.3. 인증 방법 설정

### 2.5.4. 스위치에 login 시 인증 방법 설정

U9200 series 스위치는 시스템에 접속하는 사용자에게 인증 방법을 다양하게 설정할 수 있다. 일반적으로 스위치에 등록되어 있는 사용자의 ID와 패스워드를 사용하여 접속 권한이 주어지지만, 사용자 인증 프로토콜인 RADIUS와 TACACS+등을 이용하도록 설정하면 각각의 서버가 가지고 있는 데이터베이스에 기록된 사용자 정보를 사용하여 접속 권한이 주어진다.

표 2-7. 사용자 인증 설정 명령어

명령어	설명	모드
authentication login authen-type chap	■ tacacs server를 사용하여 인증할 경우 password를 chap 방식으로 암호화하여 전송한다.	Config
no authentication login authen-type	■ tacacs server를 사용하여 인증할 경우 password를 암호화하지 않는다.	Config
authentication login enable (local   radius   tacacs)	■ 사용할 인증방식(local, radius, tacacs)을 선택한다. ■ 여러 가지 인증방식을 선택할 수 있다.	Config
no authentication login enable (radius   tacacs)	■ 사용하도록 설정된 인증방식을 사용하지 않도록 설정한다. ■ local 인증방식은 항상 사용한다.	Config
authentication login primary (local   radius   tacacs)	■ 우선적으로 인증 받을 인증방식을 설정한다.	Config
no authentication login primary (local   radius   tacacs)	■ 우선적으로 인증 받도록 설정한 인증방식을 해제한다.	Config
authentication login template-user userID	■ radius나 tacacs로 인증 받은 경우 Dummy user를 지정할 수 있다. ■ 지정하는 Dummy user는 local database에 등록되어 있어야 한다.	Config
no authentication login template-user	■ 설정한 Dummy user를 해제한다.	Config
show authentication login	■ 인증방식의 순서와 사용여부를 보여준다	Privileged

#### 2.5.4.1. 사용자 인증 설정

U9200 series 스위치는 사용자 인증 방법으로 기존의 스위치에 등록되어 있는 사용자 ID와 패스워드를 사용하여 접속 권한 여부를 확인하는 방법과 RADIUS 서버를 이용하는 방법, TACACS+ 서버를 이용하는 방법이 있다. 이 3가지 방법을 선택적으로 사용하거나 모두 사용하도록 설정할 수 있다. 한가지 이상의 방법을 사용할 경우 먼저 우선순위가 높은 인증 방식으로 인증을 시도한다. local

database 를 사용하여 인증하는 경우, local database 에서 등록되지 않은 사용자로 인증을 시도하면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 ID 와 패스워드를 다시 요청한다. RADIUS 나 TACACS+ 서버를 사용하여 인증하는 경우, 서버와 통신을 하지 못해 인증을 시도할 수 없으면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 ID 와 패스워드를 다시 요청한다.

```
Switch# configure terminal
Switch(config)# authentication login enable radius
Switch(config)# authentication login enable tacacs
Switch(config)# authentication login primary radius
Switch(config)# authentication login primary tacacs
Switch(config)# end
Switch # show authentication login
precedence      method      status
-----
first           tacacs      enable
second          radius      enable
third           local       enable

Switch#
```

## 2.5.5. privileged mode 진입시 인증 방법 설정

U9200 series 스위치는 privileged mode 로 들어올 때 사용자에게 인증 방법을 다양하게 설정할 수 있다. 일반적으로는 스위치에 등록되어 있는 enable 패스워드를 사용하여 접속 권한이 주어지지만, 사용자 인증 프로토콜인 TACACS+를 이용하도록 설정하면 각각의 서버가 가지고 있는 데이터베이스에 기록된 정보를 사용하여 접속 권한이 주어진다.

표 2-8. privileged mode 사용자 인증 설정 명령어

명령어	설명	모드
authentication enable enable (local   tacacs)	<ul style="list-style-type: none"> <li>■ 사용할 인증방식(local, tacacs)을 선택한다.</li> <li>■ 여러 가지 인증방식을 선택할 수 있다.</li> </ul>	Config
no authentication enable enable (tacacs)	<ul style="list-style-type: none"> <li>■ 사용하도록 설정된 인증방식을 사용하지 않도록 설정한다.</li> <li>■ local 인증방식은 항상 사용한다.</li> </ul>	Config
authentication enable primary (local   tacacs)	<ul style="list-style-type: none"> <li>■ 우선적으로 인증 받을 인증방식을 설정한다.</li> </ul>	Config
no authentication enable primary (local   tacacs)	<ul style="list-style-type: none"> <li>■ 우선적으로 인증 받도록 설정한 인증방식을 해제한다.</li> </ul>	Config

---

show authentication enable      ■ 인증방식의 순서와 사용여부를 보여준다      Privileged

---

### 2.5.5.1. privileged mode 사용자 인증 설정

U9200 series 스위치는 privileged mode 로 들어올 때 사용자 인증 방법으로 기존의 스위치에 등록되어 있는 **enable** 패스워드를 사용하여 접속 권한 여부를 확인하는 방법과 **TACACS+** 서버를 이용하는 방법이 있다. 이 2 가지 방법을 선택적으로 사용하거나 모두 사용하도록 설정할 수 있다.

한가지 이상의 방법을 사용할 경우 먼저 우선순위가 높은 인증 방식으로 인증을 시도한다. local database 를 사용하여 인증하는 경우, local database 에서 등록되지 않은 사용자로 인증을 시도하면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 **enable** 패스워드를 다시 요청한다. **TACACS+** 서버를 사용하여 인증하는 경우, 서버와 통신을 하지 못해 인증을 시도할 수 없으면 다음 우선순위를 갖는 인증 방식으로 인증을 시도하고, 인증에 실패하면 **enable** 패스워드를 다시 요청한다.

---

```
Switch# configure terminal
Switch(config)# authentication enable enable tacacs
Switch(config)# authentication enable primary tacacs
Switch(config)# end
Switch # show authentication enable
precedence      method      status
-----
first           tacacs      enable
second          local       enable

Switch#
```

---

## 2.5.6. 권한 부여

### 2.5.6.1. 사용자 권한 부여

U9200 series 스위치는 시스템에 접속하는 사용자에게 대한 권한 부여 방법을 다양하게 설정할 수 있다. 일반적으로는 스위치에 등록되어 있는 사용자의 **privilege level** 을 따르지만, 사용자 인증 프로토콜인 **RADIUS** 와 **TACACS+** 등을 이용하여 login 한 경우 각각의 서버가 가지고 있는 데이터베이스에 기록된 사용자 정보를 사용하여 **privilege level** 이 주어진다.

표 2-9. 사용자 권한 부여 설정 명령어

명령어	설명	모드
authorization exec (tacacs   radius)	<ul style="list-style-type: none"> <li>■ <b>tacacs</b> 또는 <b>radius</b> 서버를 통하여 인증 받은 경우 해당 서버에서 <b>privilege level</b> 을 얻어온다.</li> <li>■ <b>local</b> 방식은 항상 사용한다.</li> </ul>	Config
no authorization exec	<ul style="list-style-type: none"> <li>■ <b>tacacs</b> 또는 <b>radius</b> 서버에서 <b>privilege level</b></li> </ul>	Config

(tacacs | radius)

을 얻어오지 않도록 한다.

- local 방식은 항상 사용한다.

## 사용자 권한 부여 설정

U9200 series 스위치는 사용자 권한 부여 방법으로 기존의 스위치에 등록되어 있는 사용자 privilege 를 받는 방법과 RADIUS 서버를 이용하는 방법, TACACS+ 서버를 이용하는 방법이 있다. 이 3 가지 방법을 선택적으로 사용하거나 모두 사용하도록 설정할 수 있다

한가지 이상의 방법을 사용할 경우 우선순위는 <2.5.3.1. 스위치에 login 시 인증 방법 설정>의 우선순위를 따른다.

```
Switch# configure terminal
Switch(config)# authorization exec radius
Switch(config)# authorization exec tacacs
Switch(config)#
```

### 2.5.6.2. 명령어 권한 허가

U9200 series 스위치는 명령어 실행 전에 TACACS+ 서버로 권한 허가를 요청 할 수 있다.

표 2-10. 명령어 모드 권한 설정 명령어

명령어	설명	모드
privilege (user-mode   privileged-mode   config-mode   interface-mode   router-mode   dhcp-mode) level <0-15>	<ul style="list-style-type: none"> <li>■ 해당 모드에서 실행되는 명령어의 privilege level 을 변경한다.</li> <li>■ &lt;0-15&gt; : 명령어의 privilege level 을 의미.</li> </ul>	Config
no privilege (user-mode   privileged-mode   config-mode   interface-mode   router-mode   dhcp-mode) level	<ul style="list-style-type: none"> <li>■ 해당 모드에서 실행되는 명령어의 privilege level 을 기본값으로 복원한다.</li> </ul>	Config
show mode privilege	<ul style="list-style-type: none"> <li>■ 명령어 모드 별로 설정된 privilege level 을 보여준다.</li> </ul>	Privileged

표 2-11. 명령어 권한허가 설정 명령어

명령어	설명	모드
authorization commands <0-15> tacacs	<ul style="list-style-type: none"> <li>■ 해당 privilege level 을 갖는 명령어를 실행하기 전에 tacacs+ 서버에 권한 허가를 요청하</li> </ul>	Config

	도록 설정한다.	
	■ <0-15> : 명령어의 privilege level 을 의미.	
no authorization commands	■ tacacs+ 서버에 권한 허가를 요청하지 않도	Config
<0-15> tacacs	록 설정한다.	
	■ <0-15> : 명령어의 privilege level 을 의미.	

## 명령어 권한 허가 설정

U9200 series 스위치는 명령어 권한 허가 방법으로 TACACS+ 서버를 이용한다.

명령어 모드 별로 privilege level 을 부여하고, 부여한 privilege level 별로 권한 허가 요청 여부를 설정한다.

```
Switch# configure terminal
Switch(config)# privilege user-mode level 2
Switch(config)# authorization commands 2 tacacs
Switch(config)# end
Switch # show mode privilege
COMMAND-MODE          LEVEL
=====
user-mode              2
privileged-mode        10
config-mode            15
interface-mode         15
router-mode            15
dhcp-mode              15
Switch#
```

## 2.5.7. 계정 관리

### 2.5.7.1. 세션 관리

U9200 series 스위치는 TACACS+ 서버에 시스템 접속 내역을 기록할 수 있다.

표 2-12. 세션 관리 설정 명령어

명령어	설명	모드
accounting exec (start-stop   stop-only) tacacs	<ul style="list-style-type: none"> <li>■ 시스템 접속 내역을 tacacs+ 서버에 기록한다.</li> <li>■ start-stop : 세션 시작과 끝을 모두 기록</li> <li>■ stop-only : 세션 끝만 기록.</li> </ul>	Config
no accounting exec	■ tacacs 시스템 접속 내역을 tacacs+ 서버	Config

에 기록하지 않는다.

## 세션 관리 설정

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

### 2.5.7.2. 명령어 관리

U9200 series 스위치는 TACACS+ 서버에 명령어 실행 내역을 기록할 수 있다.

표 2-13. 명령어 관리 설정 명령어

명령어	설명	모드
accounting commands <0-15> stop-only tacacs	<ul style="list-style-type: none"> <li>해당 privilege level 을 갖는 명령어의 실행 내역을 tacacs+ 서버에 기록 한다.</li> <li>&lt;0-15&gt; : 명령어의 privilege level 를 의미.</li> </ul>	Config
no accounting commands <0-15>	<ul style="list-style-type: none"> <li>해당 privilege level 을 갖는 명령어의 실행 내역을 tacacs+ 서버에 기록하지 않는다.</li> <li>&lt;0-15&gt; : 명령어의 privilege level 를 의미.</li> </ul>	Config

## 명령어 관리 설정

```
Switch# configure terminal
Switch(config)# accounting commands 15 stop-only tacacs
Switch(config)#
```

### 2.5.8. 인증 서버 설정

표 2-14. RADIUS 서버 설정 명령어

명령어	설명	모드
radius-server host A.B.C.D	radius-server 설정한다.	Config
no radius-server host A.B.C.D	설정된 radius-server 삭제한다.	Config



radius-server host A.B.C.D key encryption-key	<ul style="list-style-type: none"> <li>radius-server 설정한다.</li> <li>해당 server 에 접속할 때 사용하는 encryption key 를 설정한다.</li> </ul>	Config
radius-server host A.B.C.D auth-port <0-65536>	<ul style="list-style-type: none"> <li>radius-server 설정한다.</li> <li>해당 server 에 접속할 때 사용하는 auth-port 를 설정한다.</li> </ul>	Config
no radius-server host A.B.C.D auth-port	<ul style="list-style-type: none"> <li>해당 server 에 접속할 때 사용하는 auth-port 를 삭제한다.(삭제되면 default auth-port 를 사용한다.)</li> </ul>	Config
radius-server host A.B.C.D auth-port <0-65536> key encryption-key	<ul style="list-style-type: none"> <li>radius-server 설정한다.</li> <li>해당 server 에 접속할 때 사용하는 auth-port 를 설정한다.</li> <li>해당 server 에 접속할 때 사용하는 encryption key 를 설정한다.</li> </ul>	Config
radius-server key encryption-key	<ul style="list-style-type: none"> <li>radius-server 에 접속할 때 사용하는 general key 설정한다.</li> <li>server 에 key 가 지정되지 않으면 이 general key 를 사용한다.</li> </ul>	Config
no radius-server key	<ul style="list-style-type: none"> <li>설정된 general key 를 삭제한다.</li> </ul>	Config
radius-server retransmit <1-5>	<ul style="list-style-type: none"> <li>radius-server 에 접속할 때의 재시도 횟수를 설정한다.</li> </ul>	Config
no radius-server retransmit	<ul style="list-style-type: none"> <li>설정된 재시도 횟수를 삭제한다.(default 3 회)</li> </ul>	Config
radius-server timeout <1- 1000>	<ul style="list-style-type: none"> <li>응답 패킷을 받아야 하는 시간을 지정한다.</li> </ul>	Config
no radius-server timeout	<ul style="list-style-type: none"> <li>설정된 timeout 시간을 삭제한다.(default 5 초)</li> </ul>	Config

## RADIUS 서버 설정

여러 개의 RADIUS 서버를 설정 할 수 있다. 먼저 설정된 서버와 통신을 하지 못해 인증을 시도할 수 없으면 다음 서버로 인증을 시도한다.

```
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#
```

표 2-15. TACACS+ 서버 설정 명령어

명령어	설명	모드
tacacs-server host A.B.C.D key encryption-key	<ul style="list-style-type: none"> <li>■ tacacs -server 설정한다.</li> <li>■ 해당 server 에 접속할 때 사용하는 encryption key 를 설정한다.</li> </ul>	Config
no tacacs-server host A.B.C.D	<ul style="list-style-type: none"> <li>■ 설정된 tacacs -server 삭제한다.</li> </ul>	Config
tacacs-server host A.B.C.D timeout <1-1000> key encryption-key	<ul style="list-style-type: none"> <li>■ tacacs -server 설정한다.</li> <li>■ 응답 패킷을 받아야 하는 시간 timeout 을 지정한다.</li> <li>■ 해당 server 에 접속할 때 사용하는 encryption key 를 설정한다</li> </ul>	Config
tacacs-server host A.B.C.D timeout <1-1000>	<ul style="list-style-type: none"> <li>■ tacacs -server 설정한다.</li> <li>■ 응답 패킷을 받아야 하는 시간 timeout 을 지정한다.</li> </ul>	Config

## TACACS+ 서버 설정

여러 개의 TACACS+ 서버를 설정 할 수 있다. 먼저 설정된 서버와 통신을 하지 못해 인증을 시도할 수 없으면 다음 서버로 인증을 시도한다.

```
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#
```

## 2.6. Hostname 설정

Hostname 은 운영 시 시스템을 구별하기 위해 사용될 수 있으며 따라서 콘솔/Telnet 화면의 프롬프트

는 **hostname** 과 현재 명령어 모드의 조합으로 이루어져 있다. U9200 Series 스위치는 default 로 시스템의 모델명을 **hostname** 으로 사용하며 운영자가 이를 변경할 수 있다.

표 2-16. Hostname 설정 명령어

명령어	설명	모드
<code>hostname string</code>	■ Hostname 을 변경	Config
<code>no hostname</code>	■ Hostname 을 default 값으로 변경	Config

Hostname 을 설정 및 변경하는 절차는 다음과 같다.

```
Switch# configure terminal
Switch(config)# hostname P9000
P9000(config)# end
P9000#

P9000# configure terminal
P9000(config)# no hostname
Switch(config)# end
Switch#
```

## 2.7. SNMP(Simple Network Management Protocol)

SNMP Network Manager 는 Management Information Base(MIB)을 제공하는 스위치를 관리할 수 있다. 각각의 Network Manager 는 관리의 편의를 위해서 사용자 인터페이스를 제공한다. SNMP manager 로 U9200 Series 스위치를 관리하고자 할 때는 스위치의 환경 설정이 필요하다.

또한 SNMP 에이전트를 접근하기 위해서는 스위치에 하나 이상의 IP 주소 설정이 필요하다. IP 주소의 설정은 “P9000 Series\_User Guide\_제 05 장\_IP 환경 설정” 문서를 참고하라.

표 2-17. SNMP 환경 설정 명령

명령어	설명	모드
<code>snmp-server contact string</code>	■ System contact 정보를 변경	Config
<code>snmp-server location string</code>	■ System location 정보를 변경	Config
<code>snmp-server community string</code> [ro rw] [host A.B.C.D/M]   [access-class <1-99>]]	■ SNMP community 를 설정 ■ ro : read only ■ rw : read write ■ A.B.C.D/M : host IP address / prefix length ■ <1-99> : standard IP access-list	Config
<code>no snmp-server community string</code>	■ SNMP Community 를 삭제	Config
<code>snmp-server enable traps</code>	■ SNMP Trap 을 Trap-Host 에게 전송하도록	Config

<code>[notification-type]</code> <code>[notification-option]</code>	<p>설정</p> <ul style="list-style-type: none"> <li>■ <code>notification-type</code>: trap 그룹 (config, environ, multicast, other, perform, resource, security, snmp)</li> <li>■ <code>notification-option</code>: 각 trap 그룹에 속한 개별 trap 항목</li> </ul>	
<code>no snmp-server enable traps</code>	■ SNMP Trap 을 Trap-Host 에게 전송하지 않도록 설정	Config
<code>snmp-server trap-host A.B.C.D community string</code>	■ SNMP Trap Host 와 trap 을 전송할 때 사용할 community 를 설정	Config
<code>no snmp-server trap-host A.B.C.D</code>	■ SNMP Trap Host 를 삭제	Config
<code>snmp-server agent-address A.B.C.D</code>	■ 스위치에서 전송하는 snmp 패킷의 출발지 IP 를 지정	Config
<code>no snmp-server agent-address</code>	■ 스위치에서 전송하는 snmp 패킷의 출발지 IP 를 지정하지 않음	Config
<code>snmp-server trap-enterprise-oid lnsNotificationMIB</code>	■ SNMP Trap 의 enterprise OID 를 lnsNotificationMIB 으로 설정	Config
<code>no snmp-server trap-enterprise-oid</code>	■ SNMP Trap 의 enterprise OID 를 개별 trap 항목으로 설정	Config
<code>snmp-server trap-version 2</code>	■ SNMPv2 Trap 을 전송하도록 설정	Config
<code>no snmp-server trap-version</code>	■ SNMPv1 Trap 을 전송하도록 설정	Config
<code>show snmp [trap]</code>	<ul style="list-style-type: none"> <li>■ snmp 설정을 출력</li> <li>■ trap: snmp trap 설정 출력</li> </ul>	Privileged



#### Notice

U9200 Series 에서 '`show snmp [trap]`' 명령을 지원하지 않는 스위치가 있을 수 있다.

### 2.7.1. SNMP Community 설정

Community string 은 시스템과 원격 Network Manager 사이의 간단한 상호 인증 기능을 제공한다. U9200 Series 스위치는 두 가지 형태의 community string 을 지원한다.

- Read community strings
  - 시스템에 읽기 전용(read-only)으로 접속
  - 기본 읽기 전용 설정은 public
- Read-write community strings
  - 시스템에 읽기 및 쓰기(read and write) 접속
  - 기본 읽기 및 쓰기 설정은 private

```
Switch# configure terminal
```

```
Switch(config)# snmp-server community public ro
Switch(config)# snmp-server community private rw
Switch(config)# snmp-server community lns1 ro host 192.168.0.0/24
Switch(config)# snmp-server community lns2 rw access-class 99
Switch(config)# end
Switch# show running-config
!
snmp-server community public ro
snmp-server community private rw
snmp-server community lns1 ro host 192.168.0.0/24
snmp-server community lns2 rw access-class 99
!
Switch#
```

**Notice**access-class 설정은 < [2.9.ACL](#) >절을 참고하라

## 2.7.2. SNMP Trap 설정

하나 이상의 네트워크 관리 단말이 인증된 **trap receiver** 로서 설정될 수 있다. U9200 Series 스위치는 모든 **trap receiver** 에게 **SNMP trap** 을 전송한다.

```
Switch# configure terminal
Switch#(config)# snmp-server trap-version 2
Switch#(config)# snmp-server enable traps
Switch#(config)# snmp-server trap-host 192.168.0.3 community public
Switch#(config)# end
Switch# show running-config
!
snmp-server community public ro
snmp-server trap-host 192.168.123.100 community hepark
snmp-server trap-host 192.168.0.3 community public
snmp-server enable traps config slotAdd slotDel GBICAdd GBICDel powerStatus
fanStatus selfLoopDetect fanActivateStatus fanModuleEquipStatus
snmp-server enable traps environ tempUpRise tempUpFall tempLowRise tempLowFall
snmp-server enable traps other change setResponse
snmp-server enable traps perform rmonRise rmonFall bpsRise bpsFall ppsRise
ppsFall sysMacRise sysMacFall cpuMacFilter
snmp-server enable traps resource cpuUsageRise cpuUsageFall memUsageRise
memUsageFall
snmp-server enable traps security remoteConnect
snmp-server enable traps snmp coldStart warmStart linkDown linkUp authFail
snmp-server enable traps multicast snoop snoopVlan proxyReport proxyReportVlan
pimNeighborLoss
!
Switch#
```



#### Notice

U9200 Series 에서 지원하는 SNMP Trap 은 모든 스위치를 포괄한다.  
'snmp-server enable traps' 명령으로 모든 SNMP Trap 을 설정  
할 경우 현재 스위치에서 지원하지 않는 SNMP Trap 의 내용도  
running-config 에 포함될 수 있다.

### 2.7.3. SNMP 패킷의 출발지 IP 설정

스위치에서 하나 이상의 Network Manager 로 SNMP Packet 을 전송할 때, 전송되는 SNMP 패킷  
의 출발지 IP 를 특정 Local IP address 로 설정할 수 있다.

```
Switch# configure terminal
Switch(config)# snmp-server agent-address 210.48.148.125
Switch(config)# end
Switch# show running-config
!
snmp-server agent-address 210.48.148.125
!
Switch#
```

### 2.7.4. SNMP Trap enterprise - oid 설정

SNMP Trap 은 개별 Trap 항목 또는 전체 Trap 을 포괄하는 항목 정보를 enterprise-oid 를 통해  
전달한다.

```
Switch# configure terminal
Switch(config)# snmp-server trap-enterprise-oid lnsNotificationMIB
Switch(config)# end
Switch# show running-config
!
snmp-server trap-enterprise-oid lnsNotificationMIB
!
Switch#
```

### 2.7.5. 시스템 담당자 설정

시스템을 관리하는 책임을 가지는 사람을 등록할 수 있다.

```
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#
```

### 2.7.6. 시스템 구축 위치 설정

```
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#
```

## 2.8. 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 라우터를 통해 전달되는 패킷을 허용하거나 거부하기 위해 사용할 수도 있고 Telnet(vty)이나 SNMP를 통한 라우터의 접속에도 적용할 수 있다.

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

표 2-18. 액세스 리스트 설정 명령

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

### 2.8.1. 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.

### 2.8.2. 표준 IP 액세스 리스트 설정

#### 2.8.2.1. 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
!
```

### 2.8.2.2. 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
!
```

---

### 2.8.2.3. 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
!
```

---

### 2.8.2.4. 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
!
```

---

### 2.8.2.5. 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
!
```

---



### 2.8.3. Telnet 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, telnet 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#
```

## 2.9. NTP 설정

### 2.9.1. 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.

### 2.9.2. NTP client mode 설정

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

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

### 2.9.3. NTP Server mode 설정

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

명령어	설명
<b>ntp master stratum &lt;1-15&gt;</b>	■ NTP master 로 동작하도록 한다.
<b>no ntp master</b>	■ NTP master 로서의 동작을 멈춘다.

## 2.9.4. NTP time zone 설정

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

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

## 2.9.5. NTP summer time 설정

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

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

## 2.9.6. NTP 기타 명령어

명령어	설명
<b>ntp poll-interval number &lt;4-17&gt;</b>	■ 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.
<b>show ntp</b>	■ NTP 에 대한 사항을 보여준다.

## 2.9.7. 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 #
```

---

# 3

## 인터페이스 환경 설정

### 3.1. 개요

U9200 Series 스위치가 지원하는 인터페이스는 다음과 같다.

표 3-1. U9200 Series 스위치가 지원하는 인터페이스

구분	종류
Physical interfaces	<ul style="list-style-type: none"> <li>■ Gigabit Ethernet <ul style="list-style-type: none"> <li>• 100Base-TX</li> <li>• 100Base-FX</li> <li>• 1000Base-T</li> <li>• 1000Base-X</li> </ul> </li> </ul>
PON interface	■ GE-PON
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
-----	----

<b>interface</b> <i>ifname</i>	<ul style="list-style-type: none"> <li>Interface 모드로 진입.</li> <li><i>ifname</i>: 환경을 설정할 특정 인터페이스의 이름.</li> </ul>
<b>Description</b> <i>string</i>	<ul style="list-style-type: none"> <li>Interface comment</li> <li><i>string</i>: 인터페이스에 대한 주석으로 80 자 이내의 문자열</li> </ul>

### 3.2.1. Interface name

U9200 Series 에서는 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
PON interface	GEAPON	"pon" + slot_id + "/" + port_id	pon1/1
Port-group interface	Port group	"po" + port-group id	po1
VLAN interface	VLAN	"vlan" + vlan id	vlan10
Loopback interface	Loopback	"lo" + id	lo0
Management interface	Fast Ethernet	"eth" + id	eth0

\

### 3.2.2. Interface id

Interface name은interface type과id로 구성되며 <표 4>는 interface id의 표기 방법과 지원하는 범위를 보여준다.

표 3-4. Interface ID 및 지원 범위

Interface Type	ID 구성	ID Range	Name(예)
Gigabit ethernet	slot id/port id	slot id:1~12, port id: 1-2	gi1/1, gi12/2
GEAPON	slot id/port id	slot id:1~12, port id: 1-2	pon1/1, pon12/2
Port group	port-group id	1 – 30	po1, po30
VLAN	vlan id	1 – 4094	vlan1, vlan4094
LoopBack	interface id	0 – 3	lo0, lo3
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-gi1/1) #
```

### 3.2.4. Description 명령어

각 인터페이스에 대한 설명을 추가한다. 이는 단지 운영자의 기억을 돕기 위한 comment에 불과

하며 **show interfaces** 명령을 사용하면 그 결과를 볼 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
<b>show interface</b> [ifname]	■ interface 의 status, configuration 출력	Privileged
<b>show port status</b>	■ 모든 physical interface 의 status 출력	Privileged
<b>show switchport</b>	■ physical/port-group interface 의 switchport 정보 출력	Privileged

#### 3.3.1. show interface 명령어

인터페이스의 환경 설정(configuration) 정보, 링크 상태(link status) 및 인터페이스 관련 통계를 보고자 할 경우 사용한다. **show interface** 명령은 정의되어 있는 모든 인터페이스에 대한 정보를 출력한다. GBIC interface의 경우 DDM기능을 지원한다면 현재 GBIC의 Diagnostic정보를 볼 수 있다. (DDM기능에 대한 자세한 설명은 15장의 4절을 참조하도록 한다.)

```
Switch# show interface
gil is down
  type 1000Base-GBIC,LC, 10,000M, 1,490nm
  gbic inserted
    vendor EZCONN
    part name ETB43341-8LNT
    Rev No Info
    SN R00169
    Date 061218
  gbic diagnostic
    temperature 47.0 'C    vcc 3.25 Volt
    rx power -inf dBm    tx power -6.10 dBm
    bias    14.1 mA
  no auto-negotiation
  speed set 1G
  duplex set full
  vlan ingress check enabled

Last clearing of counters 00:03:54
1 minutes input rate 0 bytes/sec, 0 packets/sec
1 minutes output rate 0 bytes/sec, 0 packets/sec
  0 packets input, 0 bytes
  Received 0 broadcasts, 0 multicasts
  0 CRC, 0 oversize, 0 dropped
```

0 packets output, 0 bytes  
Sent 0 broadcasts, 0 multicasts

### 3.3.2. show port status 명령어

모든 물리적 포트의 link 상태, shutdown 상태, Auto Negotiation mode, 현재 speed/duplex mode, flow control, Mdx 설정 및 interface type이 출력된다.

Switch# **show port status**

ifname	type	combo	admin	oper	block	nego	set-speed	cur-speed	flow-ctl	link-cnt
gi1	GE	.	.	down	.	manual	1G /full	.	.	0
gi2	GE	.	.	down	.	manual	1G /full	.	.	0
gi3	GE	.	.	down	.	manual	1G /full	.	.	0
gi4	GE	.	.	down	.	manual	1G /full	.	.	0
gi5	GE	.	.	down	.	manual	1G /full	.	.	0
gi6	GE	.	.	down	.	manual	1G /full	.	.	0
gi7	GE	.	.	down	.	manual	1G /full	.	.	0
gi8	GE	.	.	down	.	manual	1G /full	.	.	0
gi9	GE	.	.	down	.	manual	1G /full	.	.	0
gi10	GE	.	.	down	.	manual	1G /full	.	.	0
gi11	GE	.	.	down	.	manual	1G /full	.	.	0
gi12	GE	.	.	down	.	manual	1G /full	.	.	0
gi13	GE	.	.	down	.	manual	1G /full	.	.	0
gi14	GE	.	.	down	.	manual	1G /full	.	.	0
gi15	GE	.	.	down	.	manual	1G /full	.	.	0
gi16	GE	.	.	down	.	manual	1G /full	.	.	0
gi17	GE	.	.	down	.	manual	1G /full	.	.	0
gi18	GE	.	.	down	.	manual	1G /full	.	.	0
gi19	GE	.	.	down	.	manual	1G /full	.	.	0
gi20	GE	.	.	down	.	manual	1G /full	.	.	0
gi21	GE-T	RJ45	.	up	.	auto	auto/auto 100 /full	.	.	7
gi22	GE-T	RJ45	.	up	.	auto	auto/auto 100 /full	.	.	7
gi23	GE-T	RJ45	.	down	.	auto	auto/auto	.	.	0
gi24	GE-T	RJ45	.	up	.	auto	auto/auto 1G /full	.	.	0
gi25	10GE	.	.	down	.	manual	10G /full	.	.	0
gi26	10GE	.	.	down	.	manual	10G /full	.	.	0



#### Notice

이후부터 각 설정 사례에 대한 CLI 캡처 화면은 **Premier 8624XG** 중심으로 했으므로 타 장비 셋팅시 변경되는 부분에 대해서는 인터페이스 아이디 <표-4>를 참고하여 적용하기 바란다.

### 3.3.3. show switchport 명령어

Switchport란 2계층 스위칭 모드로 동작하는 port 및 port-group을 말한다. **Show switchport**

명령어는 물리적 포트 및 port-group의 switchport 정보가 출력된다. Switchport 정보에는 mode, native 및 tagged vlan list 등이 포함된다.

```
Switch# show switchport
U : untagged packet drop
IFNAME    SWMODE N-VLAN TAGGED-VLAN-LIST
-----
gi1       access    1
gi2       access    1
gi3       access    1
gi4       access    1
gi5       access    1
gi6       access    1
gi7       access    1
gi8       access    1
gi9       access    1
gi10      access    1
gi11      access    1
gi12      access    1
gi13      access    1
gi14      access    1
gi15      access    1
gi16      access    1
gi17      access    1
gi18      access    1
gi19      access    1
gi20      access    1
gi21      access    21
gi22      access    22
gi23      access    23
gi24      none       .
gi25      access    1
gi26      access    1
po1       access    100
```



**Notice**

U 로 표시되는 경우는 해당 인터페이스에서 **untagged-packet-drop** 을 설정했을 경우이다. 이 명령을 통해 **trunk** 포트에서 **untagged-packet** 을 **drop** 시킬 수 있다.

### 3.4. 물리적 포트 환경 설정

물리적 포트(physical port)의 환경 설정에 사용되는 명령어는 <표3-6>과 같다.

표 3-6. 물리적 포트 환경 설정 명령어

명령어	설명	모드
-----	----	----



<b>shutdown</b>	■ 물리적 포트를 disable/enable	interface
<b>no shutdown</b>		
<b>auto-negotiation</b>	■ Enable/Disable speed auto-	Interface
<b>no auto-negotiation</b>	negotiation.	
<b>speed (10 100 1000)</b>	■ speed 설정	interface
<b>speed auto</b>		
<b>duplex (full-duplex half-duplex)</b>	■ duplex mode 설정	interface
<b>duplex auto</b>		
<b>flow-control</b>	■ flow-control 설정/해제	interface
<b>no flow-control</b>		

### 3.4.1. Shutdown

물리적 포트를 disable시킨다.

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

```
Switch# configure terminal
Switch(config) #
Switch(config) # interface gil
Switch(config-if-gil/1) # shutdown          <- disable port
Switch(config-if-gil/1) # no shutdown       <- enable port
```

### 3.4.2. Block

해당 포트를 block 시킨다. 이 경우 상대방과의 link 는 살아 있으나, 트래픽이 흐르지 않는다.

```
Switch# configure terminal
Switch(config) #
Switch(config) # interface gil
Switch(config-if-gil/1) # block             <- block port
Switch(config-if-gil/1) # no block          <- unblock port
```

### 3.4.3. Speed an duplex

U9200 Series에서 각 interface 지원하는 speed는 다음과 같다.

Type	auto-negotiation	speed	duplex
100Base-TX	on	10/100/auto	full/half/auto
	off	10/100	full/half
100Base-FX	off	100	full
1000Base-T	on	10/100/1000/auto	full/half/auto
	off	10/100/1000	full
1000Base-X	on	1000	full
	off	1000	full
10000Base-X	off	10000	full

speed, duplex 설정시 다음 사항을 주의하라.

- 100Base-FX 의 경우 speed 설정은 없다.

- 1000Base-X 의 경우 speed 설정은 없고 단지 auto-negotiation off/off 만 설정가능하며 auto-negotiation on 시 광케이블이 하나만 단절되어도 양쪽에 모두 link down 이 감지된다. (remote fault 감지)
- 만약에 양쪽이 auto-negotiation 을 지원하면, auto-nego 를 권장한다. 단, 한쪽이라도 auto 모드를 지원하지 않으면 양쪽 모두 manual 로 사용한다.

### 3.4.4. Media Type

U9200 Series 의 gi21, gi22, gi23, gi24 포트들은 RJ45 와 SFP 을 지원하는 Combo 포트이다. Combo 포트의 media type 을 결정하기 위해, 각 인터페이스 모드에서 media-type 명령어를 사용한다. 물리적 포트의 media type 을 확인하려면 show port status 명령어를 사용한다. Combo 포트의 디폴트 media type 은 RJ45 이다.

표 3-7. media-type 설정 명령어

명령어	설명	모드
<b>media-type type</b>	■ Combo 포트의 media type 을 type (rj45   sfp) 으로 변경	interface
<b>no media-type</b>	■ Combo 포트의 media type 을 디폴트 type 인 rj45 로 변경	interface

```

Switch# configure terminal
Switch(config)#
Switch(config)# interface gi21
Switch(config-if-gi2/1)# media-type sfp      <- sfp mode
Switch(config-if-gi2/1)# no media-type      <- rj45 mode

```

## 3.5. Storm Control

Storm Control이란 broadcast/multicast/unicast storm으로 인한 시스템의 과부하를 방지하기 위하여 브로드캐스트/멀티캐스트/유니캐스트 트래픽이 시스템에 유입되는 것을 제한하는 기능을 말한다. Broadcast/multicast/unicast storm은 broadcast/multicast/unicast 패킷이 서브넷에 flooding되어 과다한 트래픽으로 인한 네트워크의 성능을 저하시키는 현상을 말하며 프로토콜 스택 구현상의 오류나 네트워크 환경 설정의 오류가 이런 현상을 유발시킬 수 있다. U9200 Series는 input port의 broadcast/multicast/unicast packet을 양을 측정하여 이를 설정된 threshold와 비교 그 이상의 브로드캐스트/멀티캐스트/유니캐스트 트래픽은 시스템에 유입시키지 않고 폐기한다.

명령어	설명	모드
<b>storm-control level value</b>	■ Storm Control 의 레벨을 총 Bandwidth 의 퍼센트로 설정	interface

<b>no storm-control</b>	<ul style="list-style-type: none"> <li>Storm Control 해제</li> </ul>	interface
<b>storm-control broadcast</b>	<ul style="list-style-type: none"> <li>Storm Control 대상에 Broadcast packet 를 포함</li> </ul>	interface
<b>no storm-control broadcast</b>	<ul style="list-style-type: none"> <li>Storm Control 대상에서 Broadcast packet 를 제거</li> </ul>	interface
<b>storm-control multicast</b>	<ul style="list-style-type: none"> <li>Storm Control 시 Multicast packet 를 포함</li> </ul>	interface
<b>no storm-control multicast</b>	<ul style="list-style-type: none"> <li>Storm Control 대상에서 Broadcast packet 를 제거</li> </ul>	interface
<b>storm-control unicast</b>	<ul style="list-style-type: none"> <li>Storm Control 시 Unicast packet 를 포함</li> </ul>	interface
<b>no storm-control unicast</b>	<ul style="list-style-type: none"> <li>Storm Control 대상에 Unicast Packet 를 제거</li> </ul>	interface

## 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.

U9200 Series는rx, tx 트래픽을 각각 여러 소스 포트로부터1개의 port 혹은 cpu로mirroring할 수 있다.

명령어	설명	모드
<b>mirroring rx-target ifname &lt;0-7&gt;</b>	<ul style="list-style-type: none"> <li>입력 패킷이 mirroring 될 port 를 지정</li> </ul>	config
<b>mirroring tx-target ifname &lt;0-7&gt;</b>	<ul style="list-style-type: none"> <li>출력 패킷이 mirroring 될 port 를 지정</li> </ul>	config
<b>mirroring rx-target cpu</b>	<ul style="list-style-type: none"> <li>입력되는 패킷을 cpu 로 mirroring</li> </ul>	config
<b>mirroring tx-target cpu</b>	<ul style="list-style-type: none"> <li>출력되는 패킷을 cpu 로 mirroring</li> </ul>	config
<b>mirroring rx-traffic</b>	<ul style="list-style-type: none"> <li>해당 포트의 입력 패킷을 mirroring 하도록 설정</li> </ul>	interface
<b>mirroring tx-traffic</b>	<ul style="list-style-type: none"> <li>해당 포트의 출력 패킷을 mirroring 하도록 설정</li> </ul>	interface



**Notice** 위의 **mirroring rx-target cpu** 기능을 응용하여 특정 **physical** 인터페이스에 들어오는 패킷을 **cpu** 로 **mirroring** 설정 후, “**tcpdump -i cpu0**” command 를 이용하여 인입되는 패킷을 분석할 수 있다.

## 3.7. 2 계층 인터페이스 환경 설정

2계층 인터페이스는2계층 스위칭 모드(IEEE 802.3 Bridged VLAN)로 동작하는 인터페이스로서 U9200 Series 스위치에서는 물리적 포트와 port-group interface가 이 모드로 동작한다.

이 절에서는2계층 인터페이스의 설명과 물리적 포트와 port-group을2계층 인터페이스로 설정 하는 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.

U9200 Series 스위치는 모든 이더넷 인터페이스에 802.1Q trunking encapsulation을 지원하며 single ethernet interface 또는 port-trunk interface에 trunk를 설정할 수 있다.

### 3.7.2. 2 계층 인터페이스 모드

U9200 Series 스위치가 지원하는 2계층 인터페이스 모드에는 다음과 같이 trunk 모드와 access 모드가 있다.

표 7. U9200 Series 스위치가 지원하는 2 계층 인터페이스 모드

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

### 3.7.3. 2 계층 인터페이스 기본 설정 값

U9200 Series 스위치는 물리적 포트 또는 port-group이 layer2 interface로 설정될 때 다음과 같은 기본(default) 설정 값을 가진다.

표 3-8. 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

2계층 인터페이스로 설정 및 해제하기 위한 명령어는 다음과 같다.

표 3-9. 2 계층 인터페이스 설정 및 해제 명령어

명령어	설명	모드
<b>switchport</b>	Layer2 interface 설정	interface
<b>no switchport</b>	Layer2 interface 해제	interface

인터페이스가 최초로 2계층 인터페이스로 설정되면 2계층 인터페이스 기본 설정 값을 가지게 되며 2계층 인터페이스 설정이 해제되면 VLAN 설정 값은 모두 해제된다. 2계층 인터페이스 해제는 물리적 포트를 port-grouping하고자 할 때 적용한다.



**Notice** U9200 Series 스위치의 초기 설정은 모든 물리적 포트가 2 계층 인터페이스로 되어 있다.

### 3.7.5. Trunk port 설정

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

표 3-10. Trunk port 설정 명령어

명령어	설명	모드
<b>switchport mode trunk</b>	■ trunk mode 설정	interface
<b>switchport trunk native &lt;1-4094&gt;</b>	■ trunk port native VLAN 설정	interface
<b>no switchport trunk native</b>	■ trunk port native VLAN 을 default 로 설정	interface
<b>switchport trunk add &lt;2-4094&gt;</b>	■ trunk port tagged VLAN 등록	interface
<b>switchport trunk remove &lt;2-4094&gt;</b>	■ trunk port tagged VLAN 삭제	interface
<b>switchport trunk remove all</b>		

다음은 물리적 포트를 2 계층 트렁크 포트로 설정하는 예이다.

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1/1)# switchport ! layer2 interface set
Switch(config-if-gi1/1)# switchport mode trunk ! trunk port set
Switch(config-if-gi1/1)# switchport trunk native 2 ! native vlan set
Switch(config-if-gi1/1)# switchport trunk add 3 ! tagged vlan 등록
Switch(config-if-gi1/1)# switchport trunk add 4
Switch(config-if-gi1/1)# end
```

다음은 port-group 인터페이스를 2 계층 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 2 계층 access port로 설정하기 위한 명령어는 다음과 같다.

표 3-11. Access port 설정 명령어

명령어	설명	모드
<b>switchport mode access</b>	■ access mode 설정	interface
<b>switchport access vlan &lt;1-4094&gt;</b>	■ native vlan 설정	interface
<b>no switchport access vlan</b>	■ native vlan 을 default 로 set(VLAN 1)	interface

다음은 물리적 포트를 2계층 access port로 설정하는 예이다.

```
Switch# configure terminal
Switch(config)# interface gil
Switch(config-if-gil/1)# switchport ! layer2 interface set
Switch(config-if-gil/1)# switchport mode access ! access port set
Switch(config-if-gil/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 mode access ! access port set
Switch(config-if-po2)# switchport access vlan 5 ! native vlan set
```

## 3.8. Port group

### 3.8.1. Port group 개요

Port group이란 여러 물리적 포트를 하나의 logical group으로 묶어서 대역폭을 확장하고 링크 이중화를 확보하기 위해 사용한다. U9200 Series 스위치에서 port group 인터페이스는 2계층 인터페이스로 사용될 수 있다.

U9200 Series 스위치의 모델별 설정 가능한 port group 수는 다음과 같다.

모델	port group 수	그룹 당 최대 port
P8600 Series	30	8

### 3.8.2. Port group configuration

Port group 설정을 위한 명령어는 다음과 같다.

표 3-12. 포트 그룹 설정 명령어

명령어	설명	모드
<b>port-group ifname protocol none</b>	■ static port group 을 생성한다.	config
<b>port-group ifname protocol lacp</b>	■ LACP 로 동작하는 port group 을 생성한다.	config
<b>no port-group ifname</b>	■ port-group 을 삭제한다	config
<b>port-group lb-mode layer2</b>	■ load-balance 시 MAC 주소를 참조.	config

<b>port-group lb-mode layer3</b>	■ load-balance 시 ip field 를 참조.	config
<b>port-group lb-mode layer4</b>	■ load-balance 시 tcp/udp port 참조	config
<b>port-group ifname</b>	■ port group 설정	Interface *
<b>no port-group</b>	■ port group 해제	
<b>show port-group</b>	■ port group 설정 출력	Privileged

## 3.9. MAC Filtering

### 3.9.1. MAC Filtering 개요

L2 Switching시 특정 MAC Address에 대한 traffic을 차단하기 위해 MAC Filtering 기능을 사용한다. MAC Filtering은VLAN별로 설정 가능하다.

### 3.9.2. MAC Filtering 설정

MAC Filtering 설정을 위한 기본 명령어는 다음과 같다.

표 3-13. 3 계층 인터페이스 환경 설정 명령어

명령어	설명	모드
<b>mac-filter vlan-id mac-addr (all-drop   dst-drop   trap)</b>	■ MAC Filter add	config
<b>no mac-filter vlan-id mac-addr</b>	■ MAC Filter delete	config

## 3.10. CPU Load 에 따른 MAC Filtering

### 3.10.1. CPU Load 에 따른 MAC Filtering 개요

8600 Series에서 현재 CPU상태에 따라서 설정된 VLAN에 MAC Filtering 기능을 수행할 수 있다. 이로 인해서 특정 Rate가 넘는 Source MAC에 대해서 지정된 시간만큼 트래픽을 허용하지 않는다. 따라서 특정 트래픽이 과도한 Rate를 점유하는 등의 비정상적인 행동에 대해서 사전에 미리 차단할 수 있게 된다.

### 3.10.2. CPU Load 에 따른 MAC Filtering 설정

표 3-14. CPU-MAC-FILTER 관련 명령어

명령어	설명	모드
<b>cpu-mac-filter</b>	■ 특정 vlan 에 대해서 cpu-mac-filter 기능을 Enable 시킨다.	interface
<b>cpu-mac-filter (broadcast multicast)</b>	■ 특정 vlan 에 대해서 broadcast/multicast 패킷에 대한 cpu-mac-filter 기능을 Enable 시킨다.	Interface
<b>no cpu-mac-filter</b>	■ 특정 vlan 에 대해서 cpu-mac-filter 기능을	Interface



<b>no cpu-mac-filter (broadcast multicast)</b>	<ul style="list-style-type: none"> <li>■ 특정 vlan 에 대해서 broadcast/multicast 패킷에 대한 cpu-mac-filter 기능을 Disable 시킨다.</li> </ul>	Interface
<b>cpu-mac-filter cpu-load &lt;1-99&gt;</b>	<ul style="list-style-type: none"> <li>■ MAC-filtering 을 적용시킬 CPU Load threshold 를 설정한다.</li> </ul>	config
<b>no cpu-mac-filter cpu-load</b>	<ul style="list-style-type: none"> <li>■ MAC-filtering 을 적용시킬 CPU Load threshold 를 default 로 설정한다.</li> </ul>	config
<b>cpu-mac-filter packet-threshold &lt;1-5000&gt;</b>	<ul style="list-style-type: none"> <li>■ MAC-filtering 을 적용시킬 MAC 에 대한 Threshold Rate 를 설정한다.</li> </ul>	config
<b>no cpu-mac-filter packet-threshold</b>	<ul style="list-style-type: none"> <li>■ MAC-filtering 을 적용시킬 MAC 에 대한 Threshold Rate 를 default 로 설정한다.</li> </ul>	config
<b>cpu-mac-filter duration &lt;1-1440&gt;</b>	<ul style="list-style-type: none"> <li>■ MAC-filtering 을 적용시킬 blocking duration time 에 대해서 분단위로 설정한다.</li> </ul>	config
<b>no cpu-mac-filter duration</b>	<ul style="list-style-type: none"> <li>■ MAC-filtering 을 적용시킬 blocking duration time 에 대해서 default 로 설정한다.</li> </ul>	config
<b>clear cpu-mac-filter &lt;1-4094&gt;</b>	<ul style="list-style-type: none"> <li>■ Cpu-mac-filter 가 설정된 vlan Interface 에 대한 Filtering 정보를 초기화 시킨다.</li> </ul>	privileged
<b>show cpu-mac-filter information</b>	<ul style="list-style-type: none"> <li>■ Cpu-mac-filter 의 설정정보 및 설정된 Interface 에 대해서 보여준다.</li> </ul>	privileged
<b>show cpu-mac-filter table</b>	<ul style="list-style-type: none"> <li>■ 현재 mac-filtering 이 적용된 source mac 에 대한 정보를 보여준다.</li> </ul>	privileged

CPU-MAC-FILTERING 을 특정 VLAN 에서 Enable 할 경우에 Default 값으로 설정된 파라미터 값에 의해서 동작하게 된다. 이 값을 변경할 경우에는 위의 테이블에서 설명한 것과 같이 config 모드에서 blocking duration time 과 packet threshold 및 cpu load 에 대해서 설정할 수 있다. 설정된 정보는 show cpu-mac-filter information 을 통해 확인할 수 있으며, Filtering 되고 있는 source mac 에 대한 정보는 show cpu-mac-filter table 을 통해 확인할 수 있다.

## 3.11. Switching Database Manager

### 3.11.1. SDM 개요

TCAM은 8600 Series에서 고속으로 Forwarding Table Lookup하기 위한 특별한 메모리로 볼 수 있고, Switching Database Manager (SDM)은 Ternary Content Addressable Memory (TCAM)에 저장되어 지는 Layer2와 Layer3의 Switching Information에 대해서 관리하는 역할을 한다. 이 장에서는 TCAM의 자원을 효과적으로 관리하기 위한 SDM의 설정 방법에 대해서 알아본다.

### 3.11.2. SDM 설정

8600Series에서는 4 종류의 SDM 모드를 지원하며, 각 모드는 각각의 특별한 Forwarding Entry 에 더 많은 Memory 를 할당 하게 된다. 예를 들어 “qos mode”의 경우는 Traffic Conditioner 를 통해 전달되는 Entry 에 더 많은 Memory 를 할당 하게 되고, “route mode”의 경우는 Next Hop 을 통해 전달되는



Entry 에 더 많은 Memory 를 할당 하게 된다. 특히 “sram mode”의 경우는 routing entry 를 통해 전달 되는 mode 를 줄임으로써 자원의 소요를 가장 적게 하였다. 설정된 SDM 모드는 다음 부팅 시 적용된다. 다음은 SDM 에서 사용되는 명령어에 대해서 설명해 놓았다.

표 3-15. SDM 관련 명령어

명령어	설명	모드
<b>show sdm prefer</b>	■ 부팅시 적용된 SDM mode 의 정보 출력	privileged
<b>show sdm prefer {default   arp   qos   route   sram}</b>	■ 각 모드의 SDM 정보 출력	privileged
<b>sdm prefer {default   arp   qos   route   sram}</b>	■ 각 모드로 SDM 설정	config

## 3.12. Traffic-control

### 3.12.1. Traffic-control 개요

특정 포트에서 과다한 트래픽이 유입되는 것을 방지하기 위한 방지 장치이다. 정해진 트래픽 이상의 트래픽이 유입되면 해당 포트의 트래픽을 차단한다. 트래픽 양이 정해진 양 이하로 줄어 들게 되면 정상 상태로 복귀한다.

### 3.12.2. Traffic-control 설정

Traffic-control 설정을 위한 기본 명령어는 다음과 같다

표 3-16. traffic-control 설정 명령어

명령어	설명	모드
<b>traffic-control &lt;10-1400000&gt; &lt;10-1400000&gt;</b>	해당 포트의 트래픽을 pps 단위로 설정한다.	interface
<b>traffic-control &lt;10-1400000&gt; &lt;10-1400000&gt; alarm-only</b>	해당 포트의 트래픽을 pps 단위로 설정하며, 정해진 트래픽 이상의 트래픽이 유입되면, 해당 포트의 트래픽을 차단하지 않고 syslog 와 snmp-trap 만을 발생한다.	interface
<b>no traffic-control</b>	해당 포트의 pps 트래픽 제한을 해제한다.	interface
<b>show port traffic-control</b>	해당 포트의 traffic-control 정보를 출력한다.	privileged

### 3.13. 포트 버퍼 설정

특정 인터페이스의 출력 포트의 포트 및 각 queue 에서 저장할 수 있는 packet 수를 조정 한다. 포트 설정의 경우 Fastethernet 포트에만 적용된다. giga 에서 fast-ethernet 을 트래픽일 전송하는 경우 이 값이 작은 경우 packet 손실이 발생할 수 있으며, 이 값을 크게 하면 손실을 줄일 수 있다. 반대로 이 값을 크게 하는 경우 qos 적용시 high priority queue 트래픽에 손실이 발생 할 수 있다. 이 명령의 no 형태를 사용하여 설정을 해제 할 수 있다.

표 3-17. traffic-control 설정 명령어

명령어	설명	모드
<b>tx-buffer (1G  10G) &lt;64-510&gt;</b> <b>&lt;64-510&gt;</b>	1G/10G 인터페이스의 출력 포트에서 저장할 수 있는 버퍼의 최대값과 디스크립터의 최대값을 조정한다. 디폴트 버퍼 최대값과 디스크립터 최대값은 각각 400 이다.	privileged
<b>no tx-buffer (1G 10G)</b>	1G/10G 인터페이스의 버퍼 최대값과 디스크립터 최대값을 디폴트인 400 으로 설정한다.	privileged

### 3.14. LLCF (Link Loss Carry Forward)

U9200 Series 의 LLCF 기능은 LLCF Group 으로 관리하며, 물리적 포트는 하나의 LLCF Group 의 Uplink 멤버 또는 Downlink 멤버가 될 수 있다. LLCF Group 은 각 Group 에 설정된 모드(Uplink mode, Downlink mode, Bi-Direction mode)에 따라서 멤버들의 링크 업/다운을 관리한다.

표 3-18. LLCF mode 별 동작

LLCF Group mode	Case	Action
<b>Uplink mode</b>	Group 의 모든 Downlink 멤버들이 링크 다운되었을 때	Group 의 모든 Uplink 멤버들을 링크 다운 시킨다.
	Group 의 Downlink 멤버가 링크 업 되었을 때	LLCF 기능으로 링크 다운된 Uplink 멤버들을 링크 업 시킨다.
<b>Downlink mode</b>	Group 의 모든 Uplink 멤버들이 링크 다운되었을 때	Group 의 모든 Downlink 멤버들을 링크 다운시킨다.

	Group의 Uplink 멤버들이 링크 업 되었을 때	LLCF 기능으로 링크 다운된 Downlink 멤버들을 링크 업 시킨다.
<b>Bi-Direction mode</b>	Uplink mode + Downlink mode	

표 3-19. LLCF 설정 명령어

명령어	설명	모드
<b>llcf-group group-id enable</b>	group-id을 갖는 LLCF Group을 enable 한다. 8600 Series는 최대 12개의 Group을 지원한다.	config
<b>llcf-group group-id disable</b>	group-id을 갖는 LLCF Group을 disable 한다.	config
<b>llcf-group group-id set-mode mode</b>	group-id을 갖는 LLCF Group을 mode로 설정한다.	config
<b>llcf-group group-id uplink</b>	해당 포트를 group-id을 갖는 LLCF Group의 uplink 멤버로 등록한다.	interface
<b>llcf-group group-id downlink</b>	해당 포트를 group-id을 갖는 LLCF Group의 downlink 멤버로 등록한다.	interface
<b>no llcf-group</b>	해당 포트를 소속된 LLCF Group에서 제거한다.	interface
<b>show llcf-group</b>	LLCF Group과 멤버 포트의 관계를 출력한다.	privileged

## 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 구분되어진다.

### 4.1.1. 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.

### 4.1.2. 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

U9200 Series 스위치는 최대 4094 개의 VLAN 을 지원한다. VLAN 은 다음의 기준에 따라 생성된다:

- 물리적 포트(Physical port)
- 802.1Q 태그(tag)
- 상기 기준들의 결합

### 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 Premier 8700 Series 스위치에서 1, 2, 3, 4 포트는 VLAN A 의 **access** 포트이고 9, 10, 11, 12 포트는 VLAN B 의 **access** 포트에 할당된다. 그리고 5, 6, 7, 8, 17, 18, 19, 20 포트는 VLAN C 의 **access** 포트에 정의한다.

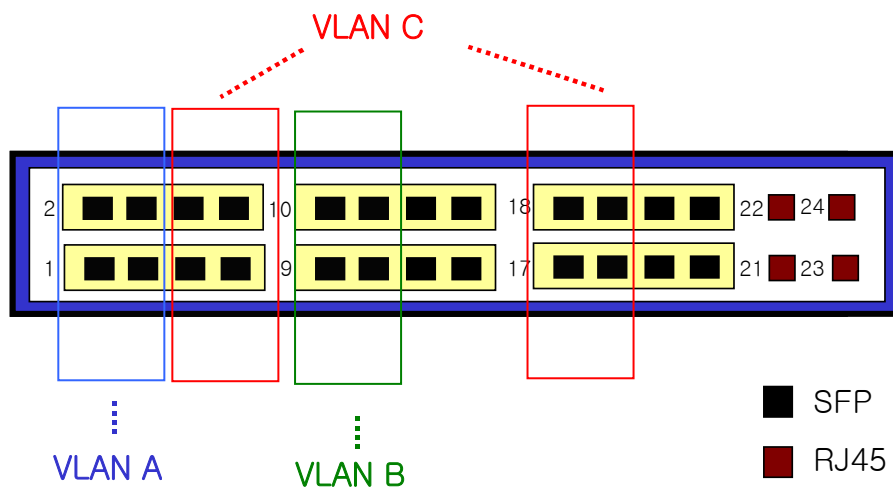


그림 4-1. U9200 Series 스위치의 포트 기반 VLAN 구성 예

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.

#### 4.2.1.1. 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 VLAN에 할당된 access 포트 중 하나씩을 사용하여 두 스위치를 케이블로 연결한다. 여러 개의 VLAN을 연결하려면, 각각의 VLAN마다 케이블로 스위치를 연결해야 한다.

<그림 2>는 서로 다른 2개의 U9200 series 스위치를 하나의 VLAN으로 묶는 방법을 보여준다. 먼저 스위치 1의 4개의 포트는 VLAN A로 포함되도록 할당되어 있다. 또한 스위치 2의 4개 포트도 VLAN A의 access 포트에 할당되어 있다. 두 스위치는 <그림 2>와 같이 상호 연결하여 하나의 브로드캐스트 도메인을 형성한다.

SWITCH 1

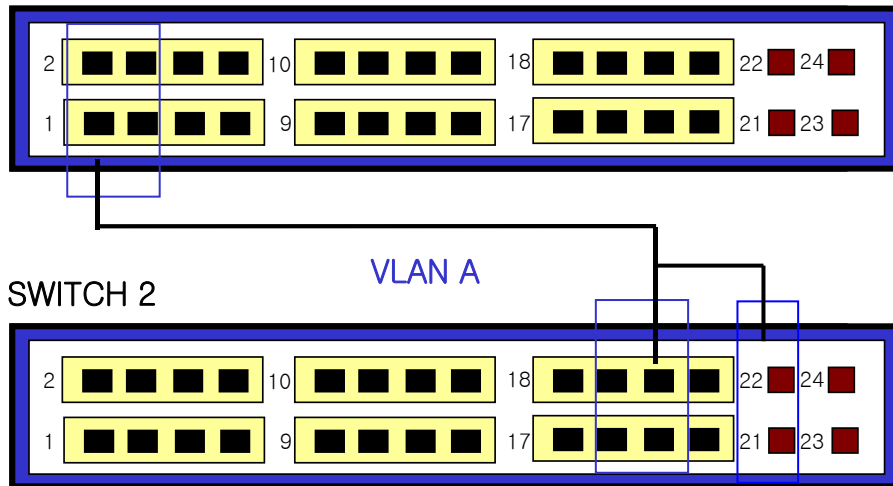


그림 4-2. 두 스위치에 걸쳐서 설정된 단일 포트 기반 VLAN

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

<그림 4-3>은 두 개의 U9200 Series 스위치에 걸쳐서 설정되는 두 개의 VLAN을 보여준다. 스위치 1에서 포트 1, 2, 3, 4 포트는 VLAN A의 access 포트이고 11, 12, 13, 14까지의 포트는 VLAN B의 access 포트에 할당되어 있다.

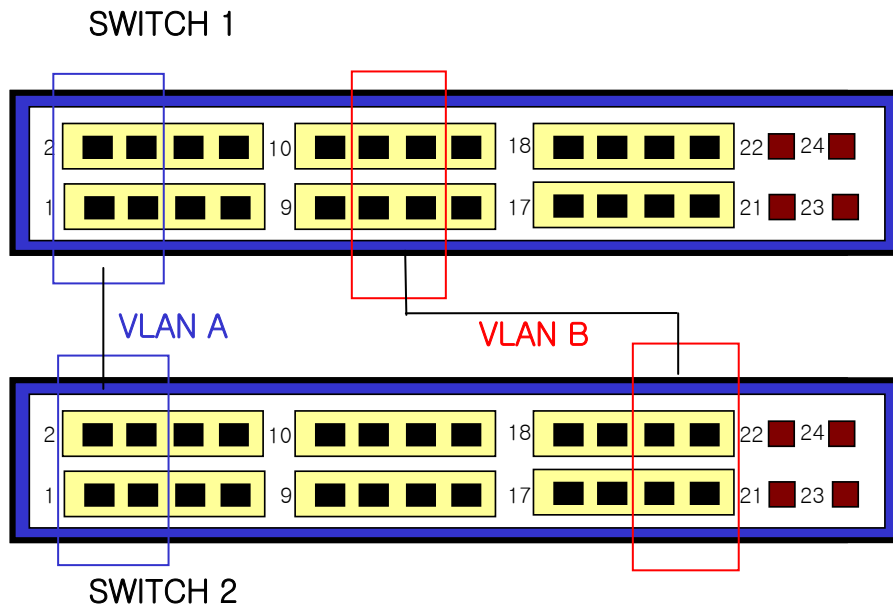


그림 4-3. 두 스위치에 걸쳐서 설정된 두 개의 포트 기반 VLAN

VLAN A는 스위치 1의 포트 1과 스위치 2의 포트 2의 연결을 통해 스위치 1과 스위치 2를 묶는다. VLAN B는 스위치 1의 포트 11과 스위치 2의 포트 22 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.

### 4.2.2.1. 태그 VLAN의 사용(Uses of Tagged VLANs)

태그는 여러 스위치를 묶는 VLAN을 생성하기 위해 가장 일반적으로 사용되는 방법이다. 태그를 사용하면, 여러 개의 VLAN이 하나 이상의 트렁크를 사용하여 프레임을 송수신할 수 있다.

<그림 4-3>에서 설명한 것처럼 포트 기반 VLAN에서는 각 VLAN 별로 하나의 포트를 할당하여 두 스



위치를 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.

#### 4.2.2.2. VLAN 태그의 할당(Assigning a VLAN Tag)

각 VLAN 은 생성할 때 VLANid 를 할당 받는다. 포트가 태그 VLAN 의 트렁크 포트에 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. 포트에 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 포트에 그 VLAN 의 태그 프레임이 수신되면, 프레임은 폐기된다. 예를 들어 VLANid 가 10, 20 의 멤버인 포트에 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.

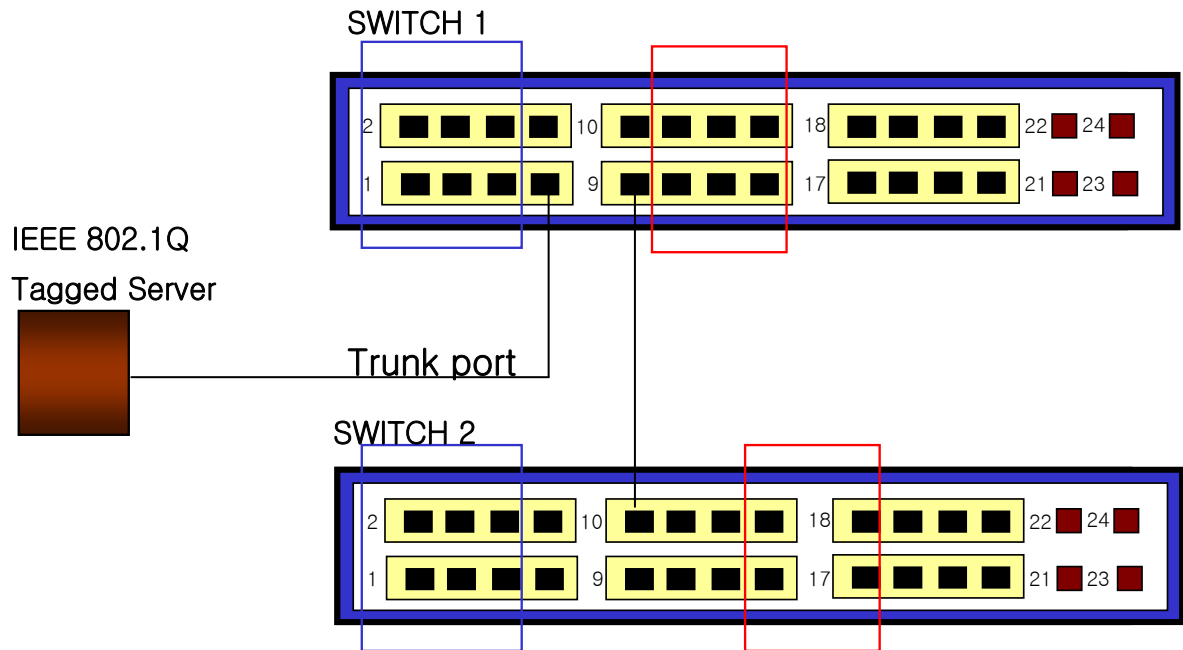


그림 4-4. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 물리적 다이어그램

<그림 4-5>는 동일한 네트워크의 논리적인 다이어그램을 보여준다.

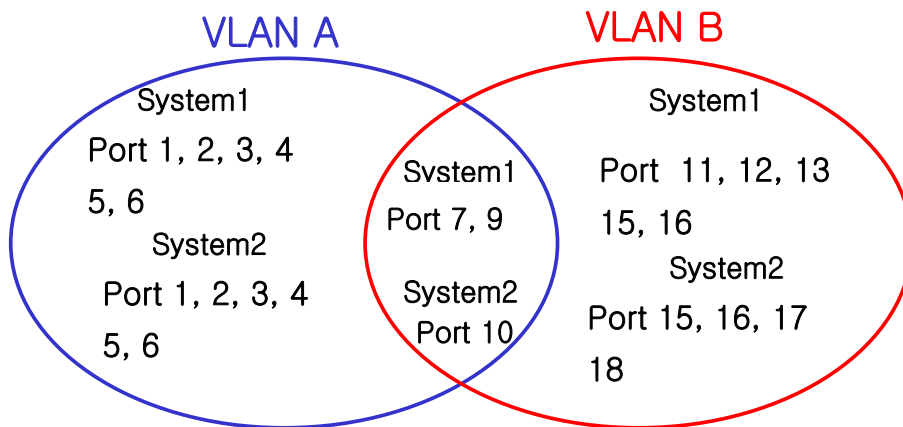


그림 4-5. 태그가 붙은 프레임과 태그가 붙지 않은 프레임의 논리적 다이어그램

<그림 4-4>와 <그림 4-5>에서:

- 각 스위치의 트렁크 포트(Tagged ports)는 VLAN A와 VLAN B의 트래픽을 전송한다.
- 각 스위치의 트렁크 포트는 태그가 붙은 프레임을 전송한다.
- 시스템 1의 포트 7와 연결된 서버는 802.1Q 태그를 지원하는 네트워크 인터페이스 카드를 장

착하고 있으며 VLAN A와 VLAN B의 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 VLAN과 태그 VLAN의 혼합

한 스위치에서 포트 기반 VLAN과 태그 VLAN을 혼합해서 사용할 수 있다. 한 포트가 속하는 포트 기반 VLAN은 오직 하나라는 조건 아래서 포트는 여러 VLAN의 멤버가 될 수 있다. 즉, 포트는 동시에 하나의 포트 기반 VLAN과 여러 개의 태그 VLAN의 멤버가 될 수 있다.

## 4.3. VLAN 구성

### 4.3.1. VLAN ID

VLAN을 식별하기 위한 VLAN id의 값으로 1부터 4,094 사이의 숫자를 사용할 수 있다. 스위치가 초기화되었을 때 기본적으로 하나의 VLAN이 생성되어 있으며(*default VLAN*), 이 VLAN이 VLAN id의 값으로 1을 사용한다. 따라서 새로 만들어지는 VLAN은 VLAN id의 값으로 1을 사용할 수 없다.

VLAN id는 태그 VLAN의 멤버인 포트가 트렁크 모드에서 동작할 때 프레임에 붙이는 태그로 사용된다. VLAN id를 잘못 설정했을 경우에 원하지 않는 VLAN으로의 프레임 송신이 발생할 수 있으므로, 전체 네트워크 구성을 잘 고려하여 VLAN id를 결정해야 한다.

### 4.3.2. Default VLAN

스위치에는 다음과 같은 특성을 가지는 default VLAN이 설정되어 있다.

- Default VLAN은 VLANid 값으로 1을 사용한다.
- Default VLAN은 태그를 사용하지 않는다.
- 스위치 초기 상태에서 모든 포트는 native VLAN으로 default VLAN이 설정되어 있다.

### 4.3.3. Native VLAN

각 물리적 포트는 PVID(Port VLAN ID)를 가지고 있다. 모든 802.1Q 포트에는 자신의 native VLAN ID가 PVID의 값으로 할당된다. 태그가 붙지 않은 모든 프레임은 PVID 값이 나타내는 VLAN으로 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 PVID가 붙은 프레임이 공존하는 것이 허용되므로, VLAN

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

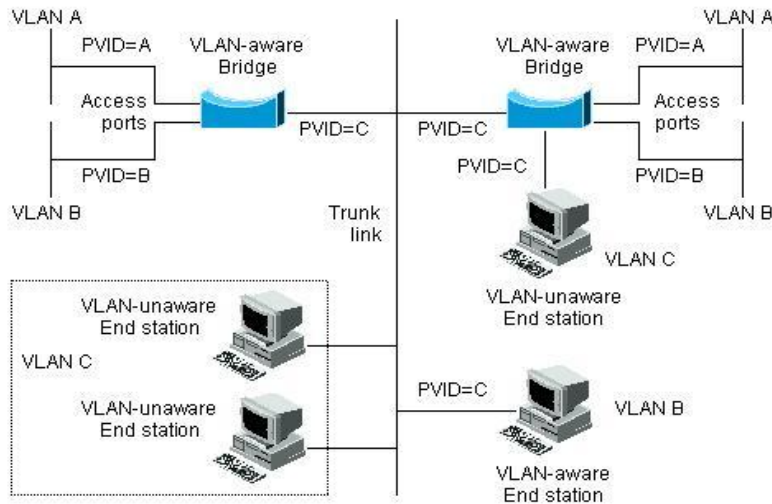


그림 4-6. Native VLAN

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 U9200 Series 스위치에 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 <i>vlanid</i></code>	<ul style="list-style-type: none"> <li>VLAN 과 관련된 값들을 생성, 삭제, 변경한다.</li> <li>1 은 default VLAN 의 값으로 사용</li> <li><i>vlanid</i> : 2 부터 4094 사이의 값을 사용한다.</li> </ul>	config
<code>switchport mode {access trunk}</code>	<ul style="list-style-type: none"> <li>포트의 VLAN 타입을 설정한다.</li> <li>access – 포트를 access 모드(포트 기반 VLAN)로 설정한다. 설정된 포트는 태그가 붙지 않은 프레임을 송수신하는 단일 VLAN 의 인터페이스로 동작한다.</li> <li>trunk – 포트를 트렁크(태그 VLAN)로 설정한다. 설정된 포트는 태그가 붙은 프레임을 송수신한다.</li> </ul>	Interface
<code>switchport access vlan <i>vlanid</i></code>	<ul style="list-style-type: none"> <li>포트를 VLAN 의 access 포트로 설정한다.</li> <li>모드가 access 로 설정되면, 설정된 포트는 VLAN 의 멤버 포트로 동작한다.</li> <li><i>vlanid</i> : 1 부터 4094 사이의 값을 사용한다.</li> </ul>	Interface
<code>switchport trunk add <i>vlanid</i></code>	<ul style="list-style-type: none"> <li>포트를 VLAN 의 트렁크 포트로 설정한다.</li> <li>포트를 여러 VLAN 의 트렁크 포트로 설정하려면, 각 VLAN 에 대해 이 명령을 반복 사용한다.</li> <li><i>vlanid</i> : 2 부터 4094 사이의 값을 사용한다.</li> <li>Default VLAN(VLANid=1)은 포트 기반 VLAN 으로 사용</li> </ul>	Interface
<code>switchport trunk native <i>vlanid</i></code>	<ul style="list-style-type: none"> <li>포트가 802.1Q 트렁크 모드, 즉 태그 VLAN 의 트렁크 포트일 때, 태그가 붙지 않고 송수신되는 트래픽을 위한 native VLAN 을 설정한다.</li> <li>native VLAN 을 설정하지 않으면 default VLAN(VLANid = 1)이 native VLAN 으로 설정</li> <li><i>vlanid</i> : 1 부터 4094 사이의 값을 사용한다.</li> </ul>	Interface
<code>switchport trunk remove {<i>vlanid</i> all}</code>	<ul style="list-style-type: none"> <li>포트를 명시한 VLAN 의 멤버에서 제외시킨다.</li> <li><i>vlanid</i> : 2 부터 4094 사이의 값을 사용한다.</li> <li>all : 모든 VLAN 으로부터 멤버에서 제외</li> </ul>	Interface
<code>(no) untagged-packet-drop</code>	<ul style="list-style-type: none"> <li>포트가 802.1Q 트렁크 모드, 즉 태그 VLAN 의 트렁크 포트일 때, 태그가 없는 packet 은 drop 시키는 기능이다. No 를 통해서 해제 가능하다.</li> </ul>	Interface

## 4.5. VLAN 설정 예제

다음의 예제에서는 VLANid 가 1000 을 생성하고, VLAN 에 IP 주소 132.15.121.1 을 할당하고, 포트 2 와 포트 4 를 VLAN 에 할당한다.

---

```
Switch(config)# vlan 1000
Switch(config)# interface vlan1000
Switch(config-if-vlan1000)# ip address 132.15.121.1/24
Switch(config-if-vlan1000)# interface gi2
Switch(config-if-gi2)# switchport mode access
Switch(config-if-gi2)# switchport access vlan 1000
Switch(config-if-gi2)# interface gi4
Switch(config-if-gi4)# switchport mode access
Switch(config-if-gi4)# switchport access vlan 1000
```

---

다음의 예제에서는 태그 기반 Vlanid 로 2000 을 할당하고, 포트 1 과 포트 2 을 트렁크 포트에 VLAN 에 추가한다.

---

```
Switch(config)# vlan 2000
Switch(config)# interface gi1
Switch(config-if-gi1)# switchport mode trunk
Switch(config-if-gi1)# switchport trunk add 2000
Switch(config-if-gi1)# interface gi2
Switch(config-if-gi2)# switchport mode trunk
Switch(config-if-gi2)# switchport trunk add 2000
```

---

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.

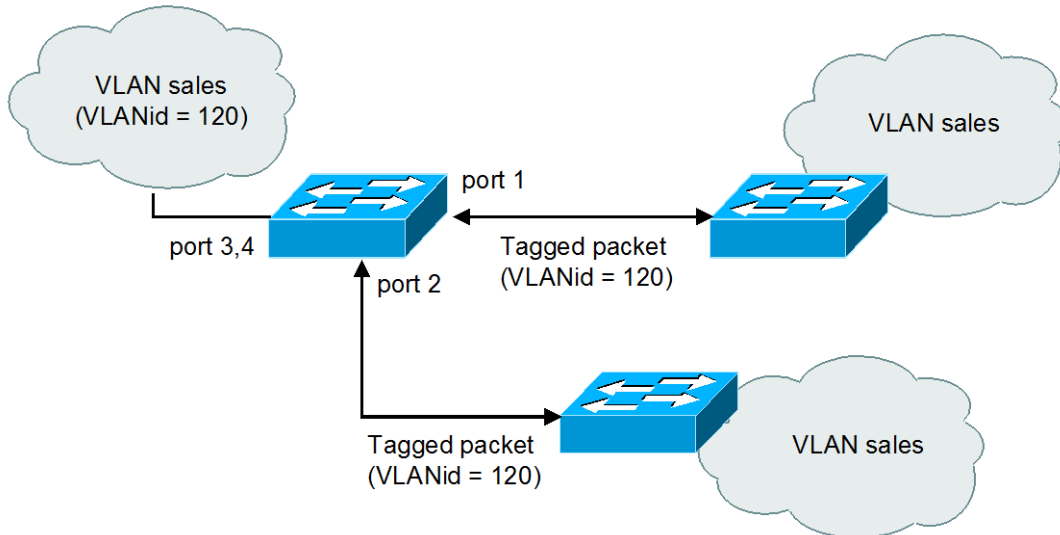


그림 4-7. VLAN 설정 예제 – Tagged and Untagged VLAN

```
Switch(config)# vlan 120
Switch(config)# interface gi1
Switch(config-if-gi1)# switchport mode trunk
Switch(config-if-gi1)# switchport trunk add 120
Switch(config-if-gi1)# interface gi2
Switch(config-if-gi2)# switchport mode trunk
Switch(config-if-gi2)# switchport trunk add 120
Switch(config-if-gi2)# interface gi3
Switch(config-if-gi3)# switchport access vlan 120
Switch(config-if-gi3)# interface gi4
Switch(config-if-gi4)# switchport access vlan 120
```

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.

```
Switch(config)# vlan 200
Switch(config)# vlan 400
Switch(config)# interface gi1
Switch(config-if-gi1)# switchport mode trunk
Switch(config-if-gi1)# switchport trunk native 200
Switch(config-if-gi1)# switchport trunk add 400
```

포트 gi1 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"> <li>■ VLAN 와 관련된 다음의 요약 정보를 출력한다. <ul style="list-style-type: none"> <li>• VLANid</li> <li>• 멤버 포트</li> </ul> </li> </ul>	Privileged

```
Switch# show vlans
```

```
VLAN MEMBER-LIST
```

```
-----
1 gi2    gi4    gi6    gi7    gi8    gi9    gi10   gi11   gi12   gi13
  gi14   gi15   gi16   gi17   gi18   gi19   gi20   gi24   gi25   gi26
2 gi1    gi3    gi5
11 gi21
13 gi22
15 gi23
-----
```

```
Switch#
```



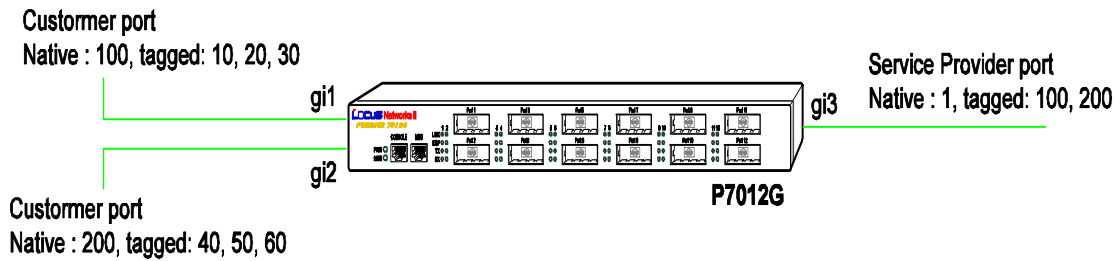
## 4.7. 802.1QinQ

QinQ 는 802.1Q 네트워크에서 금지되어 있다. 그 이유는 802.1Q 는 오직 4094 VLAN ID 들을 제공 하기 때문이다. 이 금지의 해결책으로 두 개의 1Q 레이어 사이에 802.1 QinQ 를 삽입하는 형식으로 발전하게 되었다. 802.1QinQ 는 서비스 제공 VLAN ID 와 서비스를 받는 VLAN ID 로 나누어 진다. 서비스를 받는 VLAN ID 는 서비스를 제공받는 트래픽이 지시하는 원래 VLAN ID 이다. 그리고 서비스 제공하는 VLAN ID 는 서비스 제공자들을 위해 추가하는 VLAN ID 이다.

1. 전체 시스템에 QinQ를 적용하기 위한 결정을 내린다. 이것을 적용하기 위해서는 사용자 포트 트래픽의 마지막에 4바이트에 추가를 한다.
2. Service Provider Ethertype: Set up ethertype of an outer tag (디폴트 값 0x8100).
3. Service Provider VLAN ID: Use the native VLAN ID value of customer port for outer tag VLAN ID
4. 포트모드: Q in Q를 적용하기 위해서는 각 포트마다 모드 세팅을 하는 것은 필요하다. 포트모드는 사용자포트에 outer tag를 추가해야 하고 서비스를 제공하는 포트는 outer tag를 제거 해야 한다.

표 4-2. 802.1 QinQ 명령어 사용법 테이블

명령어	설명	모드
(no) encapsulation q-in-q	QinQ enable / disable를 설정한다.	Config
(no) q-in-q tunneling ethertype VALUE	outer tag 의 ether type 설정한다. ether type 을 설정하지 않았을 경우에는 디폴트 값으로 0x8100을 사용한다.	Config
encapsulation q-in-q (default customer core)	포트 모드를 설정한다. default : 0x8100. core : ethertype으로 outer tag를 추가 customer : 사용자 포트 타입 설정	Interface



Example gi1 → gi3

DA	SA	Ether Type	Tag	Ether Type	Tag	Len/Etype	Data	FCS
		0x8101	100	0x8100	10	-	-	-

그림 4-8. 802.1 QinQ 설정

```
Switch# configure terminal
Switch(config)# vlan 10,20,30,40,50,60,100,200
Switch(config)# interface gi1
Switch(config-if-gi1)# switchport access vlan 100
Switch(config-if-gi1)# interface gi2
Switch(config-if-gi2)# switchport access vlan 200
Switch(config-if-gi2)# int gi1
Switch(config-if-gi1)# switchport mode trunk
Switch(config-if-gi1)# switchport trunk add 10,20,30
Switch(config-if-gi1)# int gi2
Switch(config-if-gi2)# switchport mode trunk
Switch(config-if-gi2)# switchport trunk add 40,50,60
Switch(config-if-gi2)# int gi3
Switch(config-if-gi3)# switchport mode trunk
Switch(config-if-gi3)# switchport trunk add 100,200
Switch(config-if-gi3)# end
```

```
Switch# show switchport
U : untagged packet drop
```

```
-----
IFNAME    SWMODE  N-VLAN  TAGGED-VLAN-LIST
-----
gi1       trunk   100     10    20    30
gi2       trunk   200     40    50    60
gi3       trunk    1      100   200
.
```

```
-----
total 12 interfaces listed
```

```
Switch# configure terminal
Switch(config)# encapsulation q-in-q
Switch(config)# interface gi1
Switch(config-if-gi1)# encapsulation q-in-q customer
Switch(config-if-gi1)# interface gi2
Switch(config-if-gi2)# encapsulation q-in-q customer
Switch(config-if-gi2)# interface gi3
Switch(config-if-gi3)# encapsulation q-in-q core (in case ethertype changed, or
encapsulation q-in-q default)
Switch(config)# q-in-q tunneling ethertype 0x8101
Switch(config)#
```

## 4.8. Private Edge VLAN

Private edge VLAN은 하나의 세그먼트 즉 VLAN 내에 존재하는 포트들이지만 허용된 포트간에만 통신을 할 수 있고, 나머지 포트들간에는 layer 2 상에서 통신을 차단시키는 기술이다. 다시 말하면 vlan 안에 다시 vlan을 나누는 개념이라고 보면 된다. 따라서 Private Edge VLAN은 스위치에 있는 지역성이 중요하다. 그리고 서로 다른 스위치간에 보호되고 있는 두 포트 사이의 독립이다. 보호되는 포트는 다른 포트에게 어떠한 트래픽(유니캐스트, 멀티캐스트, 브로드캐스트)도 발생시키지 않으며 동일 스위치에서 다른 포트들 역시 보호되는 포트에게는 어떠한 트래픽도 발생시키지 않는다.

L2에서 보호되어 있는 포트들에게는 트래픽을 전달할 수 없고, 모든 트래픽은 L3 장치를 통해서만 보호되는 포트들간에 통신을 할 수 있다.

Premier 8624 에서 private edge VLAN 간의 업 링크 설정을 위한 두 가지 방법:

- IFNAME

업 링크를 포트네임으로 지정(ex. gi1, gi2, po1...)

- VLANID

STP/RSTP 를 사용하고 있는 네트워크에서는 STP 와 RSTP 를 위한 root port 업 링크를 설정 해야 한다. 이 경우에는 uplink 를 변경하는 것이 가능하다.

표 4-3. Private Edge VLAN 설정표

명령어	설명	모드
(no) private-edge-vlan	Private-edge-vlan을 설정/해제한다.	Config
(no) private-edge-vlan IFNAME	특정 인터페이스에 private edge vlan의 uplink로 설정할 IFNAME을 입력한다.	Interface
(no) private-edge-vlan stp-root-port VLANID	특정 인터페이스에 private edge vlan의 uplink를 VLANID의 root 포트로 설정한다.	Interface
Show private-edge-vlan	Private-edge-vlan의 설정 정보를 조회한다.	Privileged

[ 예제1 ]

보호되는 포트는 gi2, gi3이며 업 링크는 gi1이다. 보호되는 포트들간의 트래픽은 허용하지 않고 오직 gi1의 트래픽만 허용한다.

```
Switch# configure terminal
Switch(config)# private-edge-vlan
Switch(config)# interface gi2
Switch(config-if-gi2)# private-edge-vlan gi1
Switch(config-if-gi2)# interface gi3
Switch(config-if-gi3)# private-edge-vlan gi1
```

[ 예제2 ]

보호되는 포트는 g1, po1, po2 이다. STP에서의 업 링크 설정은 동일한 VLAN1로 한다. 이 경우 STP의 VLAN1의 루트 포트는 “po2”가된다. 만약 src/dest private-edge-vlan 포트가 동일하다면 “\*”를 표시하고 그리고 STP의 변화된 포트만을 저장한다.

```
Switch# configure terminal
Switch(config)# int po1
Switch(config-if-po1)# private-edge-vlan stp-root-port 1
Switch(config-if-po1)# int po2
Switch(config-if-po2)# private-edge-vlan stp-root-port 1
Switch(config-if-po2)# int gi1
Switch(config-if-gi1)# private-edge-vlan stp-root-port 1
Switch(config-if-gi1)# end

Switch# show private-edge-vlan
Private Edge Vlan Mode : enabled
Static Private Edge Vlans: none
STP-ROOT-PORT Private Edge Vlans
Target Switch Port: STP Root of vlan 1: po2
Members: gi1      po1      *po2
          - (*): Temp Member
```

## 4.9. 비정상적 MAC 차단기능

다음의 명령어를 이용하여 비정상적인 MAC 주소를 가지는 패킷을 차단 혹은 cpu 로 trap 시킬 수 있다.

표 4-4. 비정상 MAC 차단 명령어

명령어	설명	모드
(no) broadcast-source-mac-drop	Source MAC address가 broadcast MAC address인 패킷을 차단하는 것을 설정 /해제 한다.	Interface
(no) gw-source-mac-drop	Source MAC address가 장비 자신인 MAC address인 패킷을 차단하는 것을 설정/ 해제 한다.	Interface
(no) null-source-mac-drop	Source MAC address가 모두 '0'인 MAC address인 패킷을 차단하는 것을 설정/ 해제 한다.	Interface
(no) self-dest-mac-trapcpu	Destination MAC address가 장비 자신인 MAC address인 패킷을 CPU로 Trap하는 것을 설정/해제 한다.	Interface

## 5

## IP 환경 설정

## 5.1. 개요

본 장에서는 IP 주소를 설정하는 방법을 설명한다.

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

U9200 Series 스위치는 다음의 인터페이스에 IP 를 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	예약
	1.0.0.0 ~ 126.0.0.0	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.

U9200 Series 스위치는 하나의 인터페이스에 복수의 IP 주소를 할당하는 기능을 지원한다. U9200 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
-----	----

`ip address ipaddress/prefixlen` ■ 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.

표 5-3. ARP 환경 설정을 위한 명령어

명령어	설명	모드
<code>show arp</code>	■ ARP 테이블의 엔트리를 출력한다.	Privileged
<code>show arp IFNAME</code>	■ ARP 테이블의 내용을 <code>vlan</code> 혹은 <code>port</code> 별로 조회한다.	Privileged
<code>show arp static</code>	■ “arp” 명령어를 통해 <code>static</code> 으로 설정한 엔트리를 출력한다.	Privileged
<code>show arp dhcp-unbinding</code>	■ Dhcp 에 의해 unbinding 된 arp 엔트리만을 출력한다.	Privileged
<code>arp ip-address mac-address vlan- name port-name</code>	<ul style="list-style-type: none"> <li>■ ARP 테이블에 static ARP 엔트리를 설정</li> <li>■ Ip-address: ARP 엔트리의 IP 주소를 나타낸다;</li> <li>■ Mac-address : ARP 엔트리의 48bit Ethernet 주소를 나타낸다.</li> <li>■ vlan-name : ARP 의 목적지 IP interface 의 이름을 나타낸다.</li> <li>■ Port-name: ip interface (즉 VLAN)의 member port 중 ARP 의 목적지 physical port name 을 나타낸다.</li> </ul>	config

## 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
-----	----



```
ip route {destination-  
prefix mask | destination-  
ipaddress/mask} {gateway-  
ipaddress | null0}  
[distance-value]
```

- **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 hops 을 더 이상 찾을 수 없을 때에도 **static route** 는 IP 라우팅 테이블에서 삭제된다.

**static route** 정보를 확인하려면 **privileged** 모드에서 다음의 명령을 사용하라.

명령	목적
<b>show ip route static</b>	■ 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-if-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.

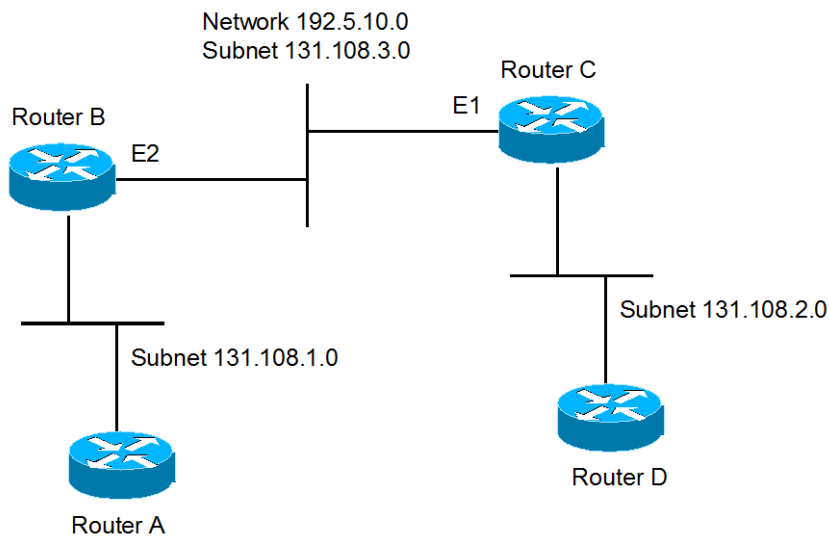


그림 5-1. 네트워크 설정 예 - 복수 IP address

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

다음의 예제들은 ARP 테이블의 내용을 확인하는 예제이다.

```
Switch# show arp
Flags>> R: reachable P: permanent K: H/W only B: dhcp unbind drop
-----
IP Address      MAC Address      Interface  PORT      RefCnt  Flags
```

10.1.2.254	0007.7089.1123	vlan2	gi1	1	R
10.1.11.46	0006.2bfc.146e	vlan11	gi7	1	R
10.1.13.1	0001.0281.f775	vlan13	gi2	1	R
10.1.13.190	0000.f083.f6d4	vlan13	gi6	1	K

다음의 명령은 ARP 테이블에 static ARP 엔트리를 등록한다.

```
Switch(config)# arp 142.10.52.196 0010.073c.0514 vlan1 gi2
Switch# show arp
```

IP Address	MAC Address	Interface	PORT	RefCnt	Flags
142.10.52.196	0010.073c.0514	vlan1	gi2	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.

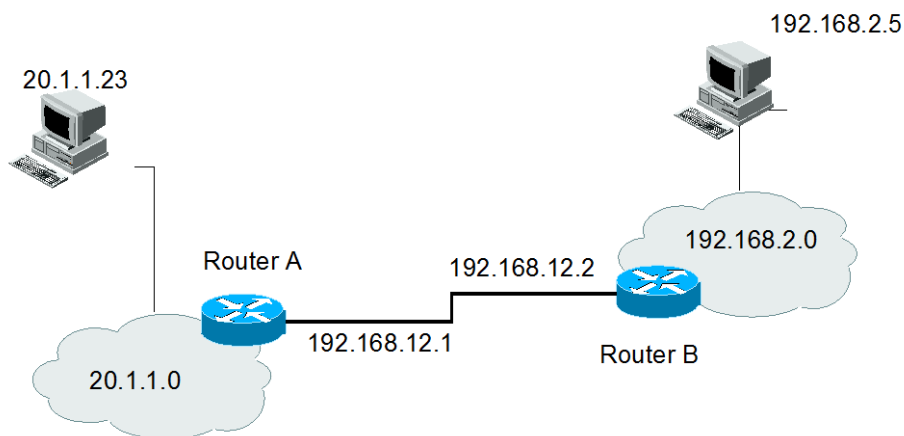


그림 5-2. 네트워크 설정 예 - Static route

#### 라우터 A 설정

```
Switch(config)# ip route 192.168.2.0/24 192.168.12.2
Switch# show ip route static database
Codes: K - kernel route, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area,
```

---

```

E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2,
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, > - selected route, * - FIB route
S>* 192.168.2.0/24 [1/0] via 192.168.12.2 vlan2
Switch#

```

### 라우터 B 설정

```

Switch(config)# ip route 20.1.1.0/8 192.168.12.1
Switch# show ip route static database
Codes: K - kernel route, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area,
E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2,
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
S 20.1.1.0/8 [1/0] via 192.168.12.1 vlan2
Switch#

```

---

## 6

## DHCP

## 6.1. DHCP Server 기능 및 설정

### 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.

Premier DHCP 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.

#### 6.1.1.1. 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)

#### 6.1.1.2. U9200 Series 스위치를 DHCP Server 로 사용

<그림 6-1>는 DHCP Client 가 DHCP Server(U9200 Series 스위치)에게 IP Address 를 요구했을 때의 기본 절차이다.

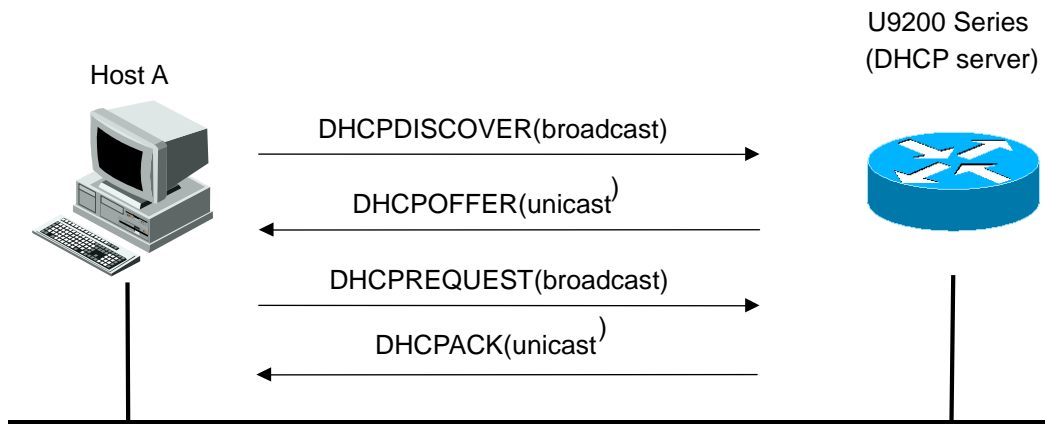


그림 6-1. U9200 Series 스위치를 DHCP Server 로 사용

- 4) Client Host A 는 브로드캐스트 메시지 *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 메시지 *DHCPOFFER* 를 사용하여 전송한다.



#### Notice

DHCP Client 는 하나 이상의 DHCP Server 로부터 *DHCPOFFER* 메시지를 받을 수 있다. Client 는 일반적으로 가장 먼저 수신된 하나의 메시지만 수용한다. 하지만 DHCP Server 의 IP Address 제공 메시지인 *DHCPOFFER* 메시지를 수신했다고 해서 DHCP Server 가 Address 할당을 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 메시지 *DHCPREQUEST* 를 사용하여 전송한다.
- 7) DHCP Server 는 Client 에게 유니 캐스트 메시지 *DHCPACK* 를 전송함으로써 IP Address 가

Client 에게 할당되었음을 확인한다.



**Notice**

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

### 6.1.1.3. U9200 Series 스위치를 DHCP relay agent 로 사용

그림 6-2>는 Premier DHCP Server 가 DHCP relay agent 로서 다른 Network 의 DHCP Server 로 DHCP Client 의 요구 메시지를 전달하는 절차이다.

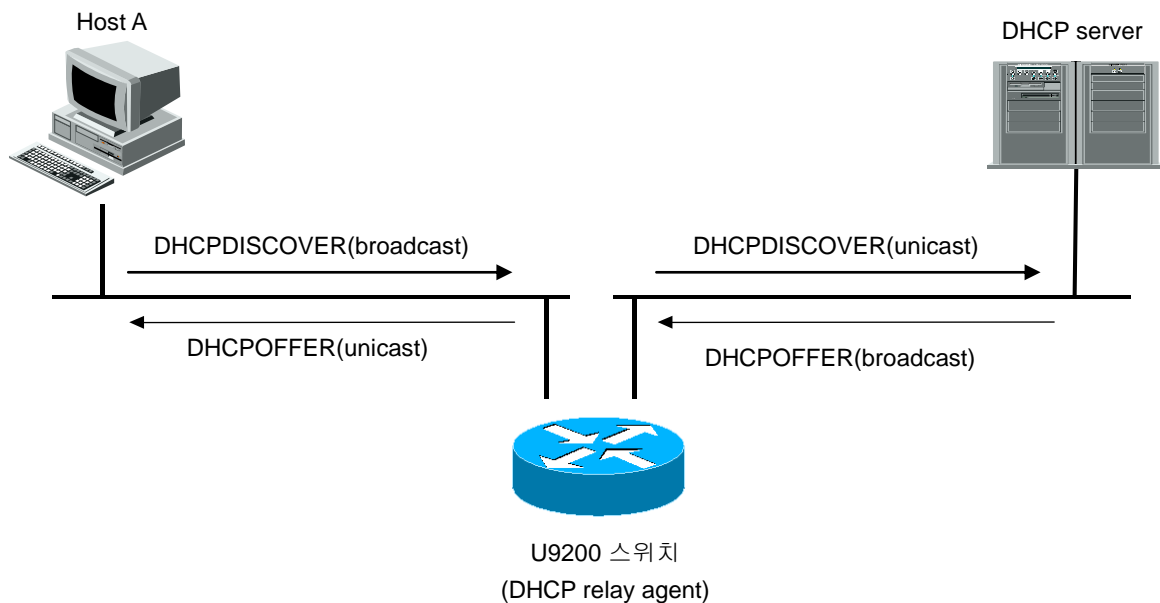


그림 6-2. DHCP relay agent 로서 DHCP Server 의 메시지 전달

DHCP Client 는 브로드캐스트 메시지 *DHCPDISCOVER* 를 Server 에게 전송한다.

- 8) Premier DHCP Server 가 Client 의 요구를 만족시킬 수 없다면, 운영자가 설정한 DHCP Server 로 유니 캐스트 메시지 *DHCPDISCOVER* 메시지를 사용하여 요구를 전달한다.
- 9) DHCP relay agent 로부터 메시지를 수신한 DHCP Server 는 Client 를 위한 IP Address, 기본 라우터 등의 정보를 유니 캐스트 메시지 *DHCPOFFER* 를 사용하여 DHCP relay agent 에게 전송한다.
- 10) DHCP relay agent 는 수신한 *DHCPOFFER* 메시지를 Client 에게 전송한다.
- 11) DHCP Server 와 Client 사이의 *DHCPREQUEST* 와 *DHCPACK* 메시지도 동일한 과정으로 DHCP

relay agent 에 의해 전달된다.

#### 6.1.1.4. DHCP Server 의 장점

Premier DHCP 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 최소화할 수 있으며, 비기술적인 사용자들에 의한 확산이 쉽다.
- 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 Address Pool

Premier DHCP 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 그룹으로 구성하면, 서로 다른 서브넷 간에 IP Pool 을 공유할 수 있습니다.
- Host Pool – manual allocation 을 위한 Pool 을 구성하며, 하나의 Host Pool 에는 공통 정보를 갖는 여러 개의 Host 를 설정할 수 있다.

#### 6.1.3. DHCP Network Pool 설정

상징적인 문자열(예를 들어 “ubiquoss”) 또는 정수(예를 들어 0)를 이름으로 사용하여 DHCP 네트워킹 Pool 을 설정할 수 있다. 또한 DHCP 네트워킹 Pool 설정은 IP Network Address, 기본 라우터 등의 파라미터를 설정할 수 있는 DHCP 네트워킹 Pool 설정 모드로 진입한다. DHCP 네트워킹 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.

##### 6.1.3.1. DHCP Network Pool 이름 설정 및 DHCP 설정 모드 진입

DHCP 네트워킹 Pool 이름을 설정하거나 DHCP Pool 설정 모드로 진입하기 위해 Global 모드에서 다음 명령을 사용한다.



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

다음의 예제는 DHCP Network Pool 이름을 ‘network\_pool1’ 로 설정하는 예제이다. DHCP Network Pool Name 의 최대 길이는 ‘31’자 이다.

```
Switch# configure terminal
Switch(config)# ip dhcp network-pool network_pool1
Switch(config-dhcp)# exit
Switch# show running-config
. . .
!
ip dhcp network-pool network_pool1
!
. . .
```

### 6.1.3.2. 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 모드에서 다음의 명령을 사용한다.

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

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

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

### 6.1.3.3. 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
<code>range lowest-address</code>	<ul style="list-style-type: none"> <li>■ 서브넷에서 클라이언트들에게 할당할 Address 범위를 지정한다.</li> </ul>

*highest-address*

- 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.

```
Switch# configure terminal
Switch(config)# ip dhcp network-pool network_pool1
Switch(config-dhcp)# range 100.0.0.1 100.0.0.100
Switch# show running-config
. . .
!
ip dhcp network-pool network_pool1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
!
. . .
```

#### 6.1.3.4. DHCP Server 부트 파일 설정

부트 파일은 Client 를 위한 부트 이미지를 저장하기 위해 사용된다. 일반적으로 부트 이미지는 Client 가 로딩하기위한 운영 시스템이다. DHCP Client 를 위한 부트 파일을 명시하기 위해 DHCP 네트워크 Pool 설정 모드에서 다음의 명령을 사용한다.

명령어	설명
<i>bootfile filename</i>	■ 부트 이미지로 사용될 파일의 이름을 명시

다음의 예제는 DHCP Server 부트 파일을 'p8xg.r100' 로 설정하는 예제이다. DHCP Server 부트 파일의, 최대 길이는 '31'자 이다.

```
Switch# configure terminal
Switch(config)# ip dhcp network-pool network_pool1
Switch(config-dhcp)# bootfile p8xg.r100
Switch(config-dhcp)# exit
Switch# show running-config
. . .
!
ip dhcp network-pool network_pool1
bootfile p8xg.r100
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
!
. . .
```

#### 6.1.3.5. Client 를 위한 기본 라우터 설정

DHCP Client 가 부팅된 후, Client 는 자신의 기본 라우터로 패킷을 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 모드에서 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.

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

#### 6.1.3.6. 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 모드에서 다음의 명령을 사용한다.

명령	설정
<code>dns-server address1 address2 address3</code>	■ 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.

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

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

### 6.1.3.7. 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 모드에서 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.

```
Switch# configure terminal
Switch(config)# ip dhcp network-pool network_pool1
Switch(config-dhcp)# domain-name ubiquoss.com
Switch(config-dhcp)# exit
Switch# show running-config
. . .
!
ip dhcp network-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
!
...
```

### 6.1.3.8. 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 <i>group-name</i>	■ 그룹 이름을 명시



#### Notice

하나의 VLAN 에 여러 개의 IP 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.

```
Switch# configure terminal
Switch(config)# ip dhcp network-pool network_pool1
Switch(config-dhcp)# group ubiquoss_pool
Switch(config-dhcp)# exit
Switch# show running-config
. . .
```

```
!
ip dhcp network-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
!
...
```

#### 6.1.3.9. Address 임대 기간 설정

기본적으로 DHCP Server 에 의해 할당된 각각의 IP Address 는 한 시간동안 임대된다. IP Address 의 할당 기간을 변경하기 위해서 DHCP Address Pool 모드에서 다음의 명령을 사용한다.

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

다음의 예제는 Address 임대 기간은 '20' 분으로 설정하는 예제이다.

```
Switch(config)# ip dhcp network-pool network_pool1
Switch(config-dhcp)# lease 0 0 20
Switch(config-dhcp)# exit
Switch# show running-config
. . .
!
ip dhcp network-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
!
...
```

#### 6.1.3.10. Client 를 위한 NetBios WINS IP Server 설정

WINS(Windows Internet Naming Service)는 일반적인 Network 그룹 내에서 Microsoft DHCP Client 가 Host 이름을 IP Address 를 변환하기 위해 사용하는 이름 해석 서비스이다. Microsoft DHCP Client 가

이용할 수 있는 NetBIOS WINS Server 를 설정하기 위해, DHCP 네트워크 Pool 설정 모드에서 다음의 명령을 사용한다.

명령어	설명
<code>netbios-name-server address</code>	■ Microsoft DHCP Client 가 이용할 수 있는 NetBIOS WINS Server 의 IP Address 를 설정

다음의 예제는 DHCP Server 에서 Client 를 위한 NetBios WINS Server 를 210.0.0.1 로 설정하는 예제이다.

```
Switch# configure terminal
Switch(config)# ip dhcp network-pool network_pool1
Switch(config-dhcp)# netbios-name-server 210.0.0.1
Switch(config-dhcp)# exit
Switch# show running-config
. . .
!
ip dhcp network-pool network_pool1
dns-server 200.0.0.1 200.0.0.2
domain-name ubiquoss.com
default-router 100.0.0.1
netbios-name-server 210.0.0.1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
group ubiquoss_pool
!
...
```

#### 6.1.3.11. Client 를 위한 NetBIOS 노드 타입 설정

Microsoft DHCP Client 를 위한 NetBIOS 노드 타입은 다음의 네 가지 중 하나이다. : broadcast, peer-to-peer, mixed, hybrid. Microsoft DHCP Client 를 위한 NetBIOS 노드 타입을 설정하기 위해 DHCP 네트워크 Pool 설정 모드에서 다음의 명령을 사용한다.

명령어	설명
<code>netbios-node-type type</code>	■ Microsoft DHCP Client 의 NetBIOS 노드 타입을 명시

다음의 예제는 DHCP Server 에서 Client 를 위한 NetBios 노드 Type 을 'p-node'로 설정하는 예제이다.

```
Switch# configure terminal
Switch(config)# ip dhcp network-pool network_pool1
Switch(config-dhcp)# netbios-node-type p-node
Switch(config-dhcp)# exit
Switch# show running-config
. . .
!
ip dhcp network-pool network_pool1
dns-server 200.0.0.1 200.0.0.2
```

```
domain-name ubiquoss.com
default-router 100.0.0.1
netbios-name-server 210.0.0.1
netbios-node-type p-node
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
group ubiquoss_pool
!
...
```

### 6.1.4. 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 모드로 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.

#### 6.1.4.1. DHCP Host Pool 이름 설정 및 DHCP 설정 모드 진입

DHCP Host Pool 이름을 설정하거나 DHCP Pool 설정 모드로 진입하기 위해 Global 모드에서 다음 명령을 사용한다.

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

다음의 예제는 DHCP Host Pool 이름을 ‘host\_pool1’로 설정하는 예제이다. DHCP Host Pool Name 의 최대 길이는 ‘31’자 이다.

```
Switch# configure terminal
Switch(config)# ip dhcp host-pool host_pool1
Switch(config-dhcp)# exit
Switch# show running-config
. . .
!
ip dhcp host-pool network_pool1
!
. . .
```

표 2. Host Pool 설정 명령어

명령어	설명
<code>bootfile filename</code>	■ 부트 이미지로 사용될 파일의 이름을 명시
<code>default-router address</code>	■ DHCP Client 를 위한 기본 라우터의 IP Address 를 명시
<code>dns-server address1 address2 address3</code>	■ DHCP Client 가 이용할 수 있는 DNS Server 의 IP Address 를 설정 ■ DHCP Client 하나의 IP Address 만 요구하지만, 명령 라인에 서 최대 3 개의 IP Address 를 설정할 수 있다.
<code>domain-name domain</code>	■ Client 를 위한 도메인 이름을 명시
<code>netbios-name-server address</code>	■ Microsoft DHCP Client 가 이용할 수 있는 NetBIOS WINS Server 의 IP Address 를 설정
<code>netbios-node-type type</code>	■ Microsoft DHCP Client 의 NetBIOS 노드 타입을 명시
<code>network ipaddr/prefix-len</code>	■ 하나의 Host Pool 내에서 설정할 수동 바인딩 IP 의 네트워크



**Notice**

Host Pool 설정 명령어는 Network Pool 설정 명령어와 설정 방법이 동일하다.



**Notice**

하나의 Host Pool 에 설정될 수동 바인딩 리스트는 `network` 명령어로 설정된 범위 내에서 할당 가능하다.

#### 6.1.4.2. DHCP 수동 바인딩을 위한 Client 설정

Host Pool 내에 수동 바인딩을 제공할 Client 들을 생성한다.

명령어	설명
<code>host ip-address netmask</code>	■ Client 에게 할당할 IP Address 와 제공할 Network 마스크 를 설정한다. ■ “config-dhcp-host#” 프롬프트로 식별되는 DHCP gHost 설정 모드로 진입

표 3. 수동 바인딩 명령어

명령어	설명
<code>hardware-address hardware-address</code>	■ Client 의 하드웨어 Address 를 명시
<code>client-name name</code>	■ 선택적으로 수행되며 표준 ASCII 문자를 사용하여 Client 의 이름을 명시



- Client 이름은 도메인 이름을 포함하지 않는다. 예로 mars 는 mars.ubiquoss.com 으로 명시하지 않는다.

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.

```
Switch# configure terminal
Switch(config)# ip dhcp host-pool host_pool1
Switch(config-dhcp)# network 110.0.0.0/24
Switch(config-dhcp)# host 110.0.0.1 255.255.255.0
Switch(config-dhcp-host)# hardware-address 00:11:22:33:44:55
Switch(config-dhcp-host)# exit
Switch# show running-config
. . .
!
ip dhcp host-pool host_pool1
network 110.0.0.0/24
host 110.0.0.1 255.255.255.0
hardware-address 0011.2233.4455
!
```

## 6.1.5. 기타 Global 명령어

표 4. Global 명령어 리스트

명령어	설명
ip dhcp default-lease {days [hours] [minutes]   infinite}	<ul style="list-style-type: none"> <li>■ 임대 기간을 명시</li> <li>■ 기본값은 한 시간으로 설정</li> <li>■ infinite: Host 에게 영구적으로 IP Address 를 임대하는 자동 할당방식으로 설정. Premier 스위치는 1 시간을 기본 값으로 갖는다.</li> <li>■ DHCP Pool 내에 Lease time 이 설정된 경우, Pool 내의 Lease time 이 default-lease time 보다 우선한다.</li> </ul>
ip dhcp max-lease {days [hours] [minutes]   infinite}	<ul style="list-style-type: none"> <li>■ 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.</li> </ul>
ip dhcp unbindig-user drop	<ul style="list-style-type: none"> <li>■ Premier 스위치로부터 IP 를 할당 받지 않은 사용자들이 스위치를 통해 서비스를 받으려고 시도할 경우 해당 패킷을 폐 기할 수 있는 기능을 지원한다.</li> </ul>
ip dhcp unbindig-user drop delay	<ul style="list-style-type: none"> <li>■ DHCP Server Daemon start 또는 새로운 Network-pool 추가 시, 기존 DHCP Client 의 서비스 연속성을 보장하기</li> </ul>

위해 unbinding-user drop 기능을 일정시간(default : 30 분) 지연시킨다.

다음의 예제는 default-lease time 을 '30'분, max-lease time 을 '2'일, unbinding-user drop 기능을 '1' 시간 지연시키는 예제이다.

```
Switch(config)# ip dhcp default-lease 0 0 30
Switch(config)# ip dhcp max-lease 0 2
Switch(config)# ip dhcp unbinding-user drop delay 0 0 1
Switch# sh running-config
!
. . .
ip dhcp unbinding-user drop delay 0 0 1
ip dhcp max-lease 0 2
ip dhcp default-lease 0 0 30
. . .
!
```

### 6.1.6. Premier DHCP Server 기능 활성화

기본적으로 스위치의 DHCP Server 기능은 비활성화 되어 있다. global 설정 모드에서 다음의 명령을 사용하여 DHCP Server 기능을 활성화 시킬 수 있다.

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

다음의 예제는 DHCP Server 기능을 활성화 시킨다.

```
Switch# configure terminal
Switch(config)# service dhcp server
Switch# sh running-config
!
. . .
service dhcp server
. . .
!
```

## 6.2. DHCP Relay 기능 및 설정

### 6.2.1. DHCP Relay 기능 개요

- DHCP Relay 는 DHCP Server 가 없는 네트워크로부터 다른 네트워크에 존재하는 1 개 이상의 DHCP Server 에게 DHCP 또는 BOOTP 패킷을 중계해주는 프로토콜이다.

다음은 U9200 스위치가 DHCP Relay Agent 로서 DHCP 클라이언트의 IP 요청 메시지를 DHCP Server 로 전달하는 절차이다.

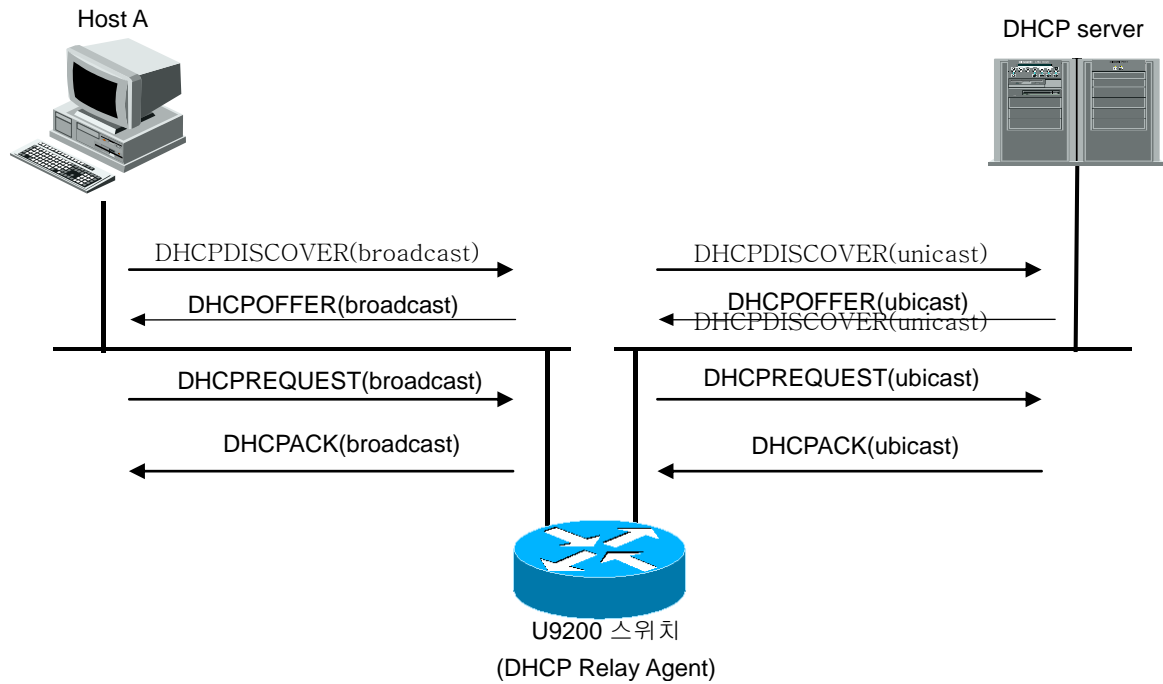


그림 6-3. DHCP Relay Agent로서 DHCP Server의 메시지 전달

- 12) DHCP 클라이언트는 IP를 요청하기 위해 DHCPDISCOVER 메시지를 Broadcast 전송한다.
- 13) DHCP Relay Agent는 DHCP 클라이언트의 IP 요청 메시지를 수신하여 DHCP Server에게 해당 메시지를 Unicast로 전달한다.
- 14) DHCP Relay Agent로부터 메시지를 수신한 DHCP Server는 클라이언트를 위한 IP 주소, 기본 라우터 등의 정보를 가진 DHCPOFFER를 Unicast로 DHCP Relay Agent에게 전송한다.
- 15) DHCP Relay Agent는 수신한 DHCPOFFER 메시지를 클라이언트에게 Broadcast 전송한다.
- 16) DHCP Server와 클라이언트 사이의 DHCPREQUEST와 DHCPACK 메시지도 동일한 과정으로 DHCP relay agent에 의해 전달된다.

### 6.2.2. Premier DHCP relay 기능 활성화

기본적으로 스위치의 DHCP relay 기능은 비활성화되어 있다. global 설정 모드에서 다음의 명령을 사용하여 DHCP relay 기능을 활성화시킬 수 있다.

명령	설명
<code>service dhcp relay</code>	<ul style="list-style-type: none"> <li>스위치의 DHCP relay 기능을 활성화</li> <li>DHCP 릴레이 기능을 비활성화하려면, 이 명령의 no 형태를 사용</li> </ul>

다음의 예제는 DHCP Relay 기능을 활성화하는 예제이다.

```
Switch# configure terminal
Switch(config)# service dhcp relay
Switch(config)# exit
Switch# 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 서버 설정

DHCP relay agent 에서 DHCP Server 를 설정하기 위해서는 Global 설정 모드에서 다음의 명령을 사용한다.

명령어	설명
<b>ip dhcp-server address</b>	<ul style="list-style-type: none"> <li>DHCP relay agent 가 DHCP 요청 패킷을 중계할 때 DHCP Server 의 IP 주소를 설정</li> <li>DHCP Server 의 삭제는 이 명령의 <b>no</b> 형태를 사용</li> </ul>



**Notice** U9200 series 의 DHCP relay Agent 는 helper-address 를 최대 20 개까지 설정 가능하다.

다음의 예제는 DHCP Relay Agent 에서 Server 주소를 지정하는 예제이다.

```
Switch# configure terminal
Switch(config)# ip dhcp helper-address 192.168.0.254
Switch(config)# exit
Switch#
Switch#
Switch# 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
```

---

#### 6.2.4. DHCP relay information option(OPTION82) 설정

Premier DHCP relay agent 는 DHCP 클라이언트로부터의 DHCP request 를 DHCP server 로 중계할 때, Premier DHCP relay agent 자체와 클라이언트가 연결된 Interface 정보를 포함할 수 있도록 DHCP relay information option 기능을 제공한다. DHCP Server 는 Option82 정보를 보고 IP 할당 및 Host Config 제공 정책을 정할 수 있다. 예를 들어 DHCP Server 는 특정 스위치의 특정 포트에 MAC(a)를 가진 Host 가 Binding 되어 있다면, 동일 스위치의 동일 포트에서 MAC(b)를 가진 Host 의 IP 요청 메시지는 무시할 수 있다.

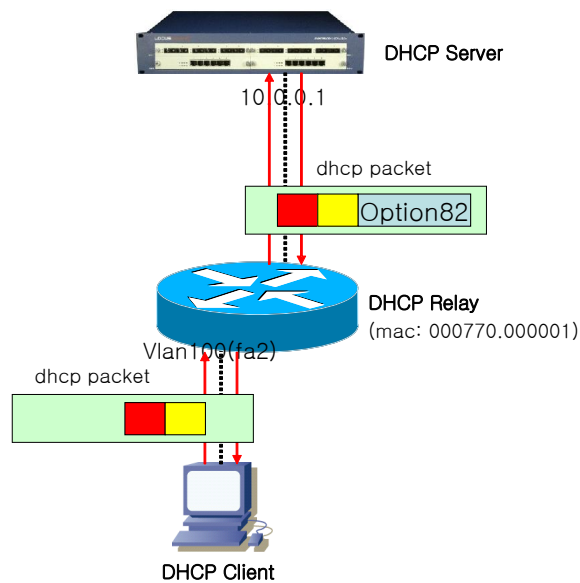


그림 6-4. DHCP Relay Option82

위 그림에서 처럼 DHCP Option82 는 DHCP Relay 와 DHCP Server 사이에서만 사용된다. DHCP Relay 는 DHCP Client 가 전송한 패킷을 DHCP Server 로 포워딩 할 때 DHCP Option82 를 추가하며, DHCP Server 가 전송한 패킷을 DHCP Client 에게 포워딩 할 때 DHCP Option82 를 제거한다.

##### 6.2.4.1. DHCP relay information option 기능의 활성화

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

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

다음은 DHCP Relay 의 Option82 기능을 활성화 시키는 예제이다.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# exit
Switch#
Switch# 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 information 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
```

#### 6.2.4.2. Relay information option 재중계 정책 설정

기본적으로, U9200 시리즈의 재중계 정책은 DHCP 클라이언트로부터 수신한 패킷 내에 기존의 relay information 을 Premier 스위치의 relay information 으로 대체한다. Premier 스위치의 기본 정책을 변경하기 원한다면, Global 모드에서 다음의 명령을 사용한다.

명령어	설명
<b>ip dhcp relay information policy {drop keep replace}</b>	<ul style="list-style-type: none"> <li>■ 기본 값은 replace 이다.</li> <li>■ drop : relay information 이 삽입되어 있는 패킷은 폐기한다.</li> <li>■ keep : 기존의 relay information 을 유지하며, 기존의 relay information 이 없으면 switch 의 relay information 을 더한다.</li> <li>■ replace : 기존의 relay information 을 Premier switch 의 relay information 으로 대체한다.</li> </ul>

다음의 예제는 DHCP Relay Information Option 재중계 설정을 Drop 으로 설정한다.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information policy drop
Switch(config)# exit
Switch# 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 information 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

DHCP Smart-relay 기능은 DHCP Relay Agent 가 Request 패킷을 DHCP Server 에게 3 회 재 전송 이 후에도 Reply 패킷을 수신하지 못한 경우 DHCP Packet 의 giaddr 를 동일 인터페이스의 또 다른 IP Address 로 변경하는 기능이다.

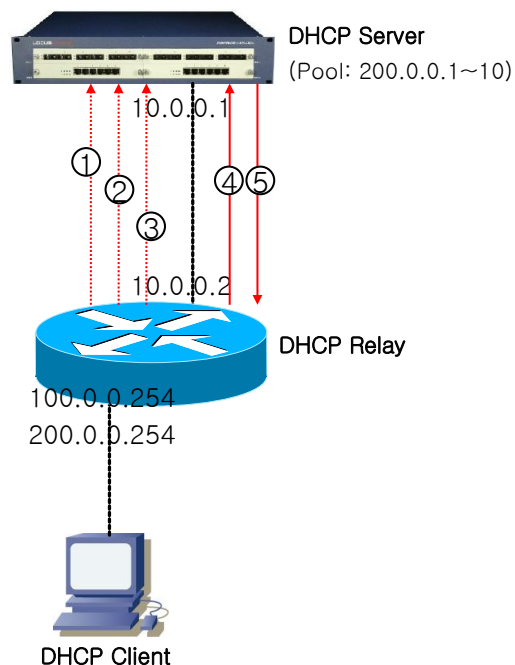


그림 6-5. DHCP Smart-Relay 동작 절차

- 17) DHCP Client로부터 IP 요청 패킷을 수신한 DHCP Relay 는 giaddr 에 '100.0.0.254'를 삽입하여 '1' 번 패킷을 DHCP Server 에게 포워딩 한다. DHCP Server 는 이 패킷의 giaddr 를 보고 자신의

Pool 영역이 아니므로 해당 패킷을 Drop 한다.

- 18) Reply 패킷을 받지 못한 DHCP Client 는 다시 한번 IP 를 요청한다. 이 패킷을 수신한 Relay Agent 는 해당 DHCP Client 에 대한 IP 요청 Retry Count 를 증가시킨다.
- 19) IP 요청 Retry Count 가 3 회이면('4' 번 패킷), DHCP Relay 는 giaddr 를 '200.0.0.254'로 변경한다. DHCP Server 는 이 패킷의 giaddr 를 보고 자신의 Pool 영역에 있으므로 Reply 패킷을 Relay Agent 에게 전송한다.

명령어	설명
<b>ip dhcp smart-relay</b>	<ul style="list-style-type: none"> <li>■ DHCP smart-relay 기능을 활성화</li> <li>■ 기본적으로, 이 특성은 비활성화 되어 있다.</li> </ul>

다음의 예제는 DHCP Smart-Relay 기능을 활성화 시킨다.

```
Switch# configure terminal
Switch(config)#
Switch(config)# ip dhcp smart-relay
Switch(config)# exit
Switch#
Switch#
Switch# 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 : Enabled
Insertion of option 82    : Enabled
DHCP relay information 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 Verify MAC-Address 설정

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

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

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

```
Switch# configure terminal
```



```
Switch(config)# no ip dhcp relay verify mac-address
Switch(config)# exit
Switch# 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 information 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 relay server-id-relay 설정

Premier DHCP relay agent 에서 DHCP Server 를 여러 개 설정했을 때, DHCP relay agent 는 DHCP Client 가 선택한 DHCP Server 에게만 DHCP Request 를 전송하기 위해 DHCP relay server-id-relay 기능을 제공한다.

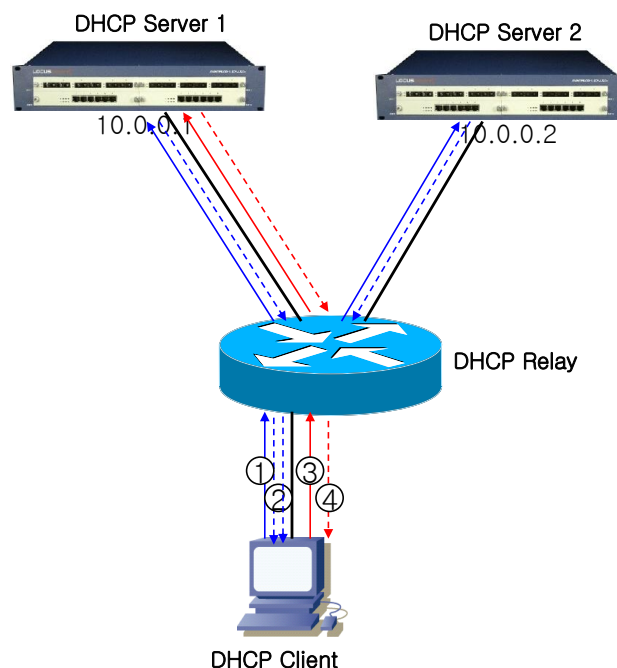


그림 6-6. DHCP Relay Server-Id-Relay 동작 절차

- 20) DHCP Client 로부터 DHCPDISCOVER 패킷을 받은 DHCP Relay Agent 는 자신에게 등록된 DHCP Server 1, DHCP Server 2 에게 패킷을 각각 포워딩한다.
- 21) DHCP Server 1 과 DHCP Server 2 는 DHCPDISCOVER 패킷을 받고 각각 DHCPOFFER 패킷으

로 Reply 한다. DHCPOFFER 패킷에는 DHCP Server Identifier Option Filed 에 Server IP 주소가 삽입되어 있다.

- 22) DHCP Client 는 DHCP Server 1 과 DHCP Server 2 로부터 DHCPOFFER 패킷을 받고 이 중에 하나를 선택하여(ex. DHCP Server 1) DHCPREQUEST 패킷을 전송한다. DHCPREQUEST 패킷에도 DHCP Server Identifier Option 이 있다.
- 23) DHCPREQUEST 패킷을 수신한 DHCP Relay Agent 는 DHCPREQUEST 의 Server Identifier Option 을 보고 DHCP Server 1 에게만 DHCPREQUEST 패킷을 전송한다. 만약 DHCP Server Selection 기능이 활성화 되어 있지 않으면 DHCP Relay Agent 는 자신에게 등록된 모든 DHCP Server 에게 패킷을 전송한다.

명령	설명
ip dhcp relay server-id-relay	<ul style="list-style-type: none"> <li>■ DHCP relay server-id-relay 기능을 활성화</li> <li>■ 기본적으로 이 특성은 비 활성화 되어 있다.</li> </ul>

다음의 예제는 DHCP Relay Server-Id-Relay 기능을 설정한다.

```
Switch# configure terminal
Switch(config)# ip dhcp relay server-id-relay
<cr>
Switch(config)# ip dhcp relay server-id-relay
Switch(config)# exit
Switch#
Switch# show ip dhcp relay

DHCP relay                : Enabled
DHCP Smart Relay feature  : Enabled
DHCP Smart Relay retry count : 3
DHCP server-id based relay : Enabled
Verification of MAC address : Enabled
Insertion of option 82    : Enabled
DHCP relay information 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
```

## 6.3. DHCP Snooping 기능

### 6.3.1. DHCP Snooping 기능 개요

DHCP Snooping 은 hosts 와 DHCP Server 사이에서 hosts 로 받은 DHCP Discover Message 에 대한 유효성을 검사하고, 동일한 hosts 로부터의 DHCP Message 에 대해 Rate-limit 를 수행하며, Option82 정보를 추가/삭제하며, hosts 에 대한 정보 Lease IP Address, Mac Address, hosts 가 연결된 Interface 정보등을 포함하는 DHCP Snooping binding database 를 생성하고, 유지 및 관리한다.

DHCP Snooping 은 Vlan 단위로 동작하며, 기본적으로 모든 Vlan 에서 inactive 상태이다.

### 6.3.1.1. Trust and Untrust Source

DHCP Snooping 은 traffic sources 가 trusted 인지 untrusted 인지 구분한다. untrusted sources 는 traffic 공격 또는 다른 적대적인 행동을 할지 모른다. 그러한 공격을 막기 위해, DHCP Snooping 은 untrusted source 로부터 message 를 필터링 할 수 있다.

### 6.3.1.2. DHCP Snooping Binding Database

DHCP Snooping은 DHCP Message를 가로 채 정보를 사용하여 database를 동적으로 만들고 유지한다. Database는 DHCP Snooping이 활성화 되어 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 message 는 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 패킷을 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 모드에서 다음의 명령어를 사용하여 DHCP Snooping 기능을 활성화 시킬 수 있다.

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

다음의 예제는 DHCP Snooping 기능을 활성화 하는 예제이다.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping
Switch(config)# exit
Switch# show ip dhcp snooping
Switch 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 패킷을 Snooping 할 Vlan 을 설정한다. 설정된 Vlan 이외의 Vlan 을 통과하는 DHCP 패킷은 Snooping 되지 않는다.

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



#### Notice

DHCP Snooping 을 DHCP Relay 와 함께 사용할 경우, DHCP Relay 가 패킷을 포워딩 하게 된다.



#### Notice

DHCP Snooping 을 DHCP Relay 와 함께 사용할 경우, DHCP Server 와 DHCP Client 양 쪽 Vlan 모두 Snooping vlan 으로 지정해야 한다.

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

```
Switch# configure terminal
Switch(config)#
Switch(config)#
Switch(config)# ip dhcp snooping vlan 1
Switch(config)# exit
Switch# show ip dhcp snooping
Switch 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 클라이언트로부터의 DHCP request 를 Snooping 할 때, DHCP 클라이언트

가 연결된 Interface 및 장비에 대한 정보를 포함할 수 있도록 DHCP Snooping information option 기능을 제공한다.

#### 6.3.4.1. DHCP Snooping information option 기능의 활성화

Premier DHCP Snooping 에서 information option 기능을 활성화시키기 위해서는 다음의 명령을 사용한다.

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

다음의 예제는 DHCP Snooping Information Option 기능을 활성화 시킨다.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping information option
Switch(config)# exit
Switch# show ip dhcp snooping
Switch 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
```

#### 6.3.4.2. DHCP Snooping information option 재중계 정책 설정

기본적으로, U9200 스위치의 DHCP Snooping information 정책은 DHCP 클라이언트로부터 수신한 패킷 내에 information Option 정보가 있으면 패킷을 Drop 시킨다. U9200 스위치의 기본 정책을 변경하기 원한다면, Global 모드에서 다음의 명령을 사용한다.

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

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

```
Switch# configure terminal
Switch(config)# ip dhcp snooping information policy keep
```

```
Switch(config)# exit
Switch#
Switch# show ip dhcp snooping
Switch 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 패킷이 Trust Port 로만 포워딩 된다.

명령어	설명
<b>ip dhcp snooping trust</b>	<ul style="list-style-type: none"> <li>지정된 포트를 Trust Port 로 설정한다. Trust Port 에서 수신한 DHCP 패킷은 Validation check 하지 않는다.</li> <li>Host 로부터의 Request 패킷이 Trust Port 로만 포워딩된다.</li> <li>기본적으로, 모든 포트는 untrust 포트이다.</li> </ul>

다음의 예제는 포트 'fa1'을 Trust Port 로 설정한다.

```
Switch(config)# interface fa1
Switch(config-if-fa1)# ip dhcp snooping trust
Switch(config-if-fa1)# end
Switch# show ip dhcp snooping interface
```

Interface	Trust State	Max Entry
fa1	Trusted	2000 0
fa2	Untrusted	2000 1
fa3	Untrusted	2000 2
fa4	Untrusted	2000 3
fa5	Untrusted	2000 4
fa6	Untrusted	2000 5
fa7	Untrusted	2000 6
fa8	Untrusted	2000 7
fa9	Untrusted	2000 8
fa10	Untrusted	2000 9
fa11	Untrusted	2000 10
fa12	Untrusted	2000 11
fa13	Untrusted	2000 12
fa14	Untrusted	2000 13
fa15	Untrusted	2000 14
fa16	Untrusted	2000 15
fa17	Untrusted	2000 16

gil	Untrusted	2000	17
-----	-----------	------	----

### 6.3.6. DHCP Snooping max-entry 설정

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

명령어	설명
<b>ip dhcp snooping max-entry</b>	<ul style="list-style-type: none"> <li>포트별로 DHCP Snooping max-entry 개수를 설정한다. 단, valid(현재 IP 를 사용중인)한 entry 는 Max entry 개수를 초과하여도 삭제하지 않는다.</li> <li>기본적으로, 포트별 Max-entry 개수는 2000 개이다.</li> </ul>

다음은 예제는 'fa1'의 DHCP Snooping Max-Entry 를 '100'개로 설정한다.

```
Switch# configure terminal
Switch(config)# interface fa1
Switch(config-if-fa1)# ip dhcp snooping max-entry 100
Switch(config-if-fa1)# end
Switch# show ip dhcp snooping interface
```

Interface	Trust State	Max Entry
fa1	Trusted	100 0
fa2	Untrusted	2000 1
fa3	Untrusted	2000 2
fa4	Untrusted	2000 3
fa5	Untrusted	2000 4
fa6	Untrusted	2000 5
fa7	Untrusted	2000 6
fa8	Untrusted	2000 7
fa9	Untrusted	2000 8
fa10	Untrusted	2000 9
fa11	Untrusted	2000 10
fa12	Untrusted	2000 11
fa13	Untrusted	2000 12
fa14	Untrusted	2000 13
fa15	Untrusted	2000 14
fa16	Untrusted	2000 15
fa17	Untrusted	2000 16
gil	Untrusted	2000 17

```
Switch#
```

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

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

```
Switch# configure terminal
Switch(config)# ip dhcp snooping entry-time
    <5-65535> Minutes
Switch(config)# ip dhcp snooping entry-time 10
Switch(config)# ex
Switch# sh ip dhcp snooping
Switch 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
<b>ip dhcp snooping rate-limit</b>	<ul style="list-style-type: none"> <li>매 1 초당 동일한 DHCP Client 로부터 Packet type 이 같은 DHCP Packet 의 허용 개수를 설정한다.</li> <li>기본적으로, 초당 2 개의 패킷을 허용한다.</li> </ul>

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

```
Switch# configure terminal
Switch(config)# ip dhcp snooping rate-limit
    <1-100> DHCP Packet rate-limit in pps
Switch(config)# ip dhcp snooping rate-limit 100
Switch(config)# end
Switch#
Switch# show ip dhcp snooping
Switch 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 패킷을 Drop 시키기 위해 다음 명령어를 사용한다.

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

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

```
Switch# configure terminal
Switch(config)# no ip dhcp snooping verify mac-address
Switch(config)# exit
Switch# show ip dhcp snooping
Switch 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
<b>ip dhcp snooping binding <i>H.H.H</i> vlan &lt;1-4094&gt; <i>A.B.C.D</i> interface <i>IFNAME</i></b>	<ul style="list-style-type: none"> <li>MAC-Address 가 <i>H.H.H</i>인 DHCP Client 를 지정된 Interface 에서 IP <i>A.B.C.D</i> 를 사용하며, lease time 은 Infinite 이다.</li> </ul>

다음의 예제는 MAC 이 1111.2222.3333 인 가입자가, Vlan 1 의 fa2 포트에 연결되어 IP 100.0.0.10 을 사용하는 예제이다.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping binding 1111.2222.3333 vlan 1 100.0.0.10
interface fa2
Switch(config)# exit
Switch#
Switch# 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)	Vlan	Interface
1111.2222.3333	100.0.0.10	Manual	Infinite	1	fa2
total 4 bindings found					

## 6.4. DHCP Server 모니터링 및 관리

### 6.4.1. DHCP Server Pool 정보 조회

DHCP Server 에 생성된 DHCP Address Pool 정보를 조회하려면, privileged EXEC 모드에서 다음의 명령을 사용한다.

명령	목적
<b>show ip dhcp pool</b>	■ DHCP Server 의 DHCP Address Pool 정보를 출력
<b>show ip dhcp pool network-pool [name]</b>	■ DHCP Server 의 Network Pool 내의 정보 출력
<b>show ip dhcp pool host-pool [name]</b>	■ DHCP Server 의 Host Pool 내의 정보 출력

### 6.4.2. DHCP Server 바인딩 정보 조회

DHCP Server 에서 Client 에게 제공한 Address 의 바인딩 정보를 조회하려면, privileged EXEC 모드에서 다음의 명령을 사용한다.

명령	목적
<b>show ip dhcp binding</b>	■ DHCP Server 에 생성된 모든 바인딩을 출력
<b>show ip dhcp binding detail</b>	■ DHCP Server 에 생성된 모든 바인딩을 좀 더 상세한 형태로 출력
<b>show ip dhcp binding network-pool {address  name}</b>	<ul style="list-style-type: none"> <li>■ DHCP Server 에 생성된 바인딩 정보 중 네트워크 Pool 에 속하는 바인딩 정보를 출력</li> <li>■ address : Address 에 해당하는 바인딩 정보 출력</li> <li>■ name : 이름에 해당하는 Network Pool 내의 모든 바인딩 정보 출력</li> </ul>
<b>show ip dhcp binding host-pool {address name}</b>	<ul style="list-style-type: none"> <li>■ DHCP Server 에 생성된 바인딩 정보 중 Host Pool 에 속하는 바인딩 정보를 출력</li> <li>■ address : Address 에 해당하는 바인딩 정보 출력</li> <li>■ name : 이름에 해당하는 Host Pool 내의 모든 바인딩 정보 출력</li> </ul>

### 6.4.3. DHCP Server 통계 정보 조회

명령	목적
<code>show ip dhcp server statistics</code>	<ul style="list-style-type: none"> <li>Server 의 통계와 송수신한 메시지와 관련된 카운터 정보를 출력</li> </ul>

### 6.4.4. DHCP Server 충돌 정보 조회

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

### 6.4.5. DHCP Server 변수 초기화 명령어

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

### 6.4.6. DHCP Server 디버그 명령어

명령어	설명
<code>debug ip dhcp server {events packets}</code>	<ul style="list-style-type: none"> <li>DHCP Server 의 디버깅 기능을 활성화</li> </ul>

## 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"> <li>DHCP Server 의 목록을 출력</li> </ul>
<code>show ip dhcp relay information option</code>	<ul style="list-style-type: none"> <li>DHCP relay information option 의 활성화 및 재중계 정책을 출력</li> </ul>
<code>show ip dhcp relay statistics</code>	<ul style="list-style-type: none"> <li>relay 의 통계와 송수신한 메시지와 관련된 카운터 정보를 출력</li> </ul>
<code>debug ip dhcp relay {events packets}</code>	<ul style="list-style-type: none"> <li>DHCP relay 의 디버깅 기능을 활성화</li> </ul>

## 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.

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

---

```
Switch(config)# configure terminal
Switch(config)# ip dhcp network-pool sales1
Switch(config-dhcp)# dns-server 1.2.3.4 1.2.3.5
Switch(config-dhcp)# lease 0 12
Switch(config-dhcp)# network 192.168.2.0/24
Switch(config-dhcp)# default-router 192.168.2.1
Switch(config-dhcp)# range 192.168.2.10 192.168.2.240
Switch(config-dhcp)# group vlan10
Switch(config-dhcp)# exit
Switch(config)# ip dhcp network-pool sales2
Switch(config-dhcp)# dns-server 1.2.3.4 1.2.3.5
Switch(config-dhcp)# lease 0 12
Switch(config-dhcp)# network 192.168.3.0/24
Switch(config-dhcp)# default-router 192.168.3.1
Switch(config-dhcp)# range 192.168.3.10 192.168.3.50
Switch(config-dhcp)# range 192.168.3.100 192.168.3.230
Switch(config-dhcp)# group vlan10
Switch(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, 00:01:02:94:77:d8, 00:01:02:94:77:d9 인 Client 에게 192.168.4.114, 192.168.4.115, 192.168.4.116 의 IP Address 와 255.255.255.0 의 Network 마스크가 할당된다. 수동 바인딩으로 할당된 IP Address 는 영구적으로 사용된다.

---

```
Switch(config)# ip dhcp host-pool mars
Switch(config-dhcp)# network 192.168.4.0/24
Switch(config-dhcp)# default-router 192.168.4.1
Switch(config-dhcp)# dns-server 192.168.4.10 192.168.4.11
Switch(config-dhcp)# domain-name ubiquoss.com
Switch(config-dhcp)# host 192.168.4.114 255.255.255.0
Switch(config-dhcp-host)# hardware-address 00:01:02:94:77:d7
Switch(config-dhcp-host)# exit
Switch(config-dhcp)# host 192.168.4.115 255.255.255.0
Switch(config-dhcp-host)# hardware-address 00:01:02:94:77:d8
Switch(config-dhcp-host)# exit
Switch(config-dhcp)# host 192.168.4.116 255.255.255.0
Switch(config-dhcp-host)# hardware-address 00:01:02:94:77:d9
```

---



**Notice**

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

### 6.7.3. DHCP Server 모니터링 및 관리 예제

다음의 예제는 DHCP Server 에 생성된 DHCP Address Pool 정보를 출력한다.

```
Switch# show ip dhcp pool
```

Pool Name	Type	IP address	Total	Used	Usage
mars	Host	192.168.4.115/24	1	1	100%
mars	Host	192.168.4.116/24	1	1	100%
mars	Host	192.168.4.117/24	1	1	100%
marketing	Network	192.168.1.0/24	172	0	0%
sales1	Network	192.168.2.0/24	231	0	0%
sales2	Network	192.168.3.0/24	172	0	0%

```
Switch# show ip dhcp pool network-pool sales1
```

```
Address pool Name      Sales
Type                   Network
Default router         192.168.2.1
Lease                  0 days, 12 hours, 0 minutes
DNS server              1.2.3.4    1.2.3.5
Network                192.168.2.0    255.255.255.0
Range (s)
                       192.168.2.10 ~ 192.168.2.240
group                  vlan10
```

```
Switch# show ip dhcp pool host-pool mars
```

```
Address pool Name      Sales
Type                   Host
Lease                  infinite
Default router         192.168.4.1
DNS server              192.168.4.10 192.168.4.11
Domain name            ubiquoss.com
Network                192.168.4.0/24

Host                   192.168.4.114      255.255.255.0
Hardware address       00:01:02:94:77:d7

Host                   192.168.4.115      255.255.255.0
Hardware address       00:01:02:94:77:d8

Host                   192.168.4.116      255.255.255.0
Hardware address       00:01:02:94:77:d9
```



#### Notice

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

다음의 예제는 DHCP Server 가 Client 에게 할당한 IP Address 를 보여준다.

```
Switch# show ip dhcp binding
```

IP address	Hardware address	Lease expiration	Type
192.168.4.114	00:01:02:94:77:d7	Infinite	Manual
192.168.3.10	02:c7:f8:00:04:22	Wed Mar 12 06:27:39 2003	Automatic

다음의 예제는 DHCP Server 가 Client 에게 할당한 IP Address 를 자세히 보여준다.

```
Switch(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
```

다음의 예제는 Client에게 이미 바인딩된 IP Address를 DHCP Server가 사용할 수 있도록(다른 Client의 IP Address로 사용하도록 시도), DHCP Server의 바인딩 정보를 삭제한다.

```

Switch(Config)# clear ip dhcp binding 192.168.3.10
Switch(Config)# show ip dhcp binding

```

IP address	Hardware address	Lease expiration	Type
192.168.4.114	00:01:02:94:77:d7	Infinit	Maunal

다음의 예제는 DHCP Server의 통계자료를 보여준다.

```

Switch# 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 설정한다. Client의 요구를 만족시키는 DHCP Address Pool이 없을 경우에 스위치는 다른 서브 Network에 위치한 DHCP Server로 Client의 요구를 전달한다.



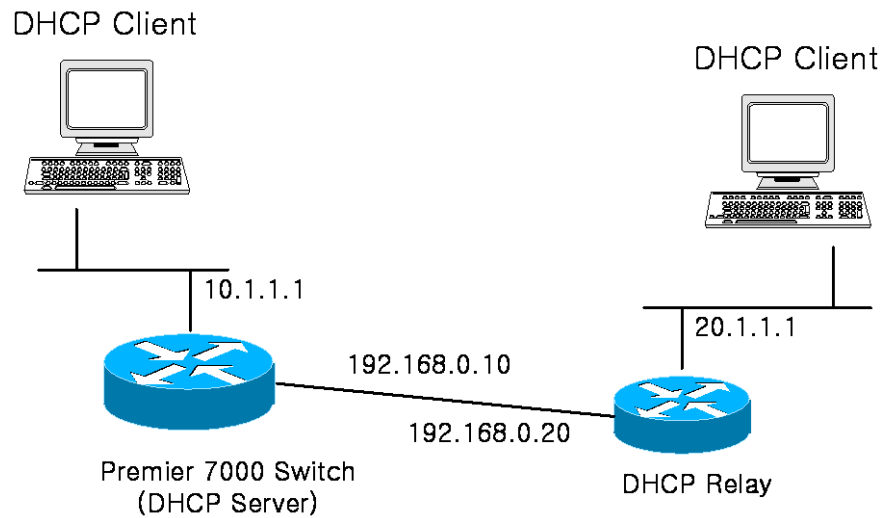


그림 3. 예제 Network – DHCP Relay agent 환경 설정

```
Switch(config)# configure terminal
Switch(config)# ip dhcp-server 10.1.1.2
Switch(config)# service dhcp relay
Switch (config)# end
Switch# show ip dhcp helper-address
Server's IP address : 10.1.1.2
Switch#
Switch# 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 메시지를 전달하려  
면, 해당 Network 에 대한 라우팅 경로 정보가 설정되어 있어야 한다.

# 7

## RIP

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

### 7.1. Information about RIP

RIP 는 오래되었지만 여전히 작은 네트워크에서 사용되는 interior gateway protocol 이다. RIP 는 고전적인 distance-vector 방식의 라우팅 프로토콜이다.

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

RIP 에서 사용하는 metric 은 hop count 이다. Hop count 는 라우트까지 지나는 라우터의 수이다. Connected 네트워크는 0 의 metric 값을 가지고 도달 불가능한 라우트의 metric 은 16 값을 가진다, 이처럼 작은 metric 범위를 사용하기 때문에 큰 네트워크를 위한 라우팅 프로토콜로는 부적합하다.

스위치는 다른 장비로부터의 update 를 통하여 default 네트워크를 수신할 수도 있고 default 네트워크를 생성할 수도 있다. 이러한 경우에, default 네트워크는 RIP 와 다른 RIP neighbor 를 통하여 advertisement 된다.

### 7.2. How to Configure RIP

RIP 를 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 Distance
- Enabling Split Horizon

### 7.2.1. Enabling RIP

RIP 를 동작시키려면 다음과 같이 설정하면 된다.

	Command or Action	Purpose
Step 1	<b>Configure terminal</b>  예제: Switch# <b>configure terminal</b>	Global configuration 모드로 진입한다
Step 2	<b>router rip</b>  예제: Switch(config)# <b>router rip</b>	RIP 라우팅 설정 모드로 진입한다.
Step 3	<b>network ip-address/prefix-len</b>  예제: Switch(config-router)# <b>network 33.1.1.0/24</b>	RIP 를 통하여 다른 라우터에게 광고하려는 네트워크를 지정한다.
Step 4	<b>end</b>  예제: Switch(config-router)# <b>end</b>	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
<b>neighbor ip-address</b>  예제: Switch(config-router)# <b>neighbor 3.3.3.2</b>	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

Passive interface 를 설정한다.

예제:

Switch(config-router)# **passive-interface** gi2/1

## 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 라우팅 metric 에 offset 을 적용한다.

예제:

Switch (router-config)# **offset-list** aa in 5 gi2/1

## 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

라우팅 프로토콜 타이머값을 조정한다.

예제:

Switch(config-router)# **timer basic** 30 120 120

## 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)# **ip rip send version 1**  
Switch(config-if-Giga2/1)# **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)# **ip rip receive version 1**  
Switch(config-if-Giga2/1)# **ip rip receive version 2**  
Switch(config-if-Giga2/1)# **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**

Administrative distance 값을 변경한다.

예제:

Switch(config-router)# **distance 90 10.1.1.1/24**

## 7.2.8. 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]

Split horizon poisoned 를 enable 한다.

예제:

```
Switch(config-if-Giga2/1)# ip rip split-horizon
poisoned
```

## 7.3. Configuration Examples for RIP

### 7.3.1. RIP 구성

그림 7-1 과 같은 네트워크 구성도를 통하여 RIP 프로토콜의 구성 예를 살펴본다.

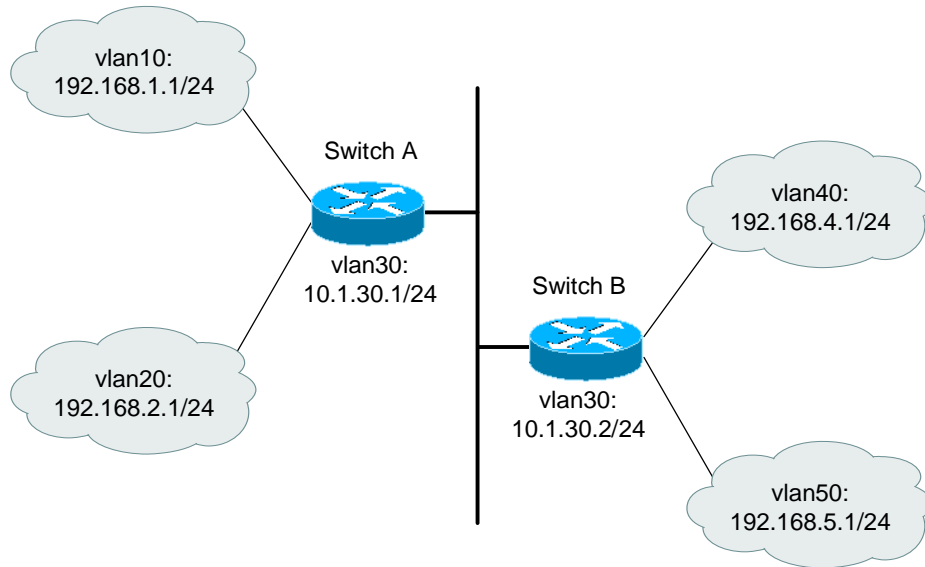


그림 7-1. RIP 를 설정한 네트워크 예제 설정 및 구성도

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 U9200 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. LSA 는 각 라우터에 의해서 수집되며 각 라우터의 LSDB 에 들어가게 된다. OSPF 는 라우터간에 LSA 를 분배하기 위해서 flooding 알고리즘을 사용한다. 라우팅 정보의 변화는 네트워크의 모든 라우터들에게 전송 된다.. 하나의 area 내의 모든 라우터들은 정확히 동일한 LSDB 를 가진다. 다음 <표 8-1>는 LSA type number 를 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

OSPF 에서는 네트워크의 각 부분들이 하나의 area 들로 뭉쳐질 수 있다. 한 area 내에서의 토폴로지는 autonomous system 내의 나머지 area 와 분리되어 감추어 진다. 이 정보를 감추는 것은 LSA 트래픽의 상당한 감소를 가능하게 하며, 또한 LSDB 를 유지하기 위해 필요한 계산을 감소시킨다. Area 내에서의 라우팅은 그 area 내의 토폴로지에 의해서만 결정된다.

OSPF 에서는 다음과 같은 세가지 종류의 라우터를 정의한다.

- ✓ **Internal Router (IR)**  
라우터의 모든 인터페이스가 동일한 area 내에 포함되는 라우터.
- ✓ **Area Border Router (ABR)**  
여러 area 에 인터페이스를 가지고 있는 라우터. 다른 ABR 들과 summary advertisement 를 교환하는 역할을 담당한다.
- ✓ **Autonomous System Border Router (ASBR)**  
OSPF 와 다른 라우팅 프로토콜, 또는 다른 Autonomous System 과의 게이트웨이의 역할을 담당하는 라우터.

### 8.1.3. AREA 0

하나 이상의 area 를 포함하고 있는 OSPF 네트워크는 백본(backbone)이라 불리는 area 0 로 설정된 area 를 반드시 가지고 있어야 한다. Autonomous system 의 모든 area 들은 반드시 백본에 연결이 되어야 한다. 네트워크를 설계할 때, area 0 로 시작하여 다른 area 들을 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.

#### 8.1.4. Stub areas

OSPF에서는 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.

#### 8.1.5. 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.

#### 8.1.6. 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 area를 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) # <b>ip ospf cost</b> cost	OSPF interface 에서 송신하는 packet 의 cost 를 설정한다.
Router (config-if) # <b>ip ospf retransmit-interval</b> seconds	OSPF interface 의 LSA 재전송 시간을 설정한다.
Router (config-if) # <b>ip ospf transmit-delay</b> seconds	OSPF interface 에서 전송 시 필요한 예상 시간을 설정한다.
Router (config-if) # <b>ip ospf priority</b> number-value	OSPF designated router 를 선출 할 때 사용되는 priority 를 설정한다.
Router (config-if) # <b>ip ospf hello-interval</b> seconds	OSPF interface 에서 송신하는 hello packet 의 주기를 설정한다.
Router (config-if) # <b>ip ospf dead-interval</b> seconds	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) # <b>ip ospf authentication-key</b> key	OSPF simple password authentication 을 사용하는 network 세그먼트에서 사용하는 password 를 설정한다.
Router (config-if) # <b>ip ospf message-digest-key</b> key-id md5 key	OSPF MD5 authentication 을 사용할 때 key-id 와 key 값을 설정한다.
Router (config-if) # <b>ip ospf authentication</b> {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 이 점을 갖는다.

- (6) Point-to-multipoint 는 neighbor 설정이 필요 없고, DR 선출을 안 하기 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) # <b>ip ospf network {broadcast   non-broadcast   {point-to-multipoint [non-broadcast]   point-to-point}}</b>	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 설정하려면 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) # <b>ip ospf network point-to-multipoint</b>	Interface 를 Point-to-multipoint broadcast network type 으로 설정 한다.
Step 2	Router (config-if) # <b>exit</b>	Global configuration mode 로 변경한다.
Step 3	Router (config) # <b>router ospf process-id</b>	Router configuration mode 로 변경한다.
Step 4	Router (config-router) # <b>neighbor ip-address cost number</b>	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) # <b>neighbor ip-address [priority number] [poll-interval seconds]</b>	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) # <b>ip ospf network point-to-multipoint non-broadcast</b>	Interface 를 Point-to-multipoint nonbroadcast network type 으로 설정 한다.
Step 2	Router (config-if) # <b>exit</b>	Global configuration mode 로 변경한다.
Step 3	Router (config) # <b>router ospf process-id</b>	Router configuration mode 로 변경한다.
Step 4	Router (config-router) # <b>neighbor ip-address [cost number]</b>	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) # <b>area area-id authentication</b>	OSPF area 에 authentication 을 설정한다.
Router (config-router) # <b>area area-id authentication message-digest</b>	OSPF area 에 MD5 authentication 을 설정한다.
Router (config-router) # <b>area area-id stub</b>	Stub area 를 설정한다.
Router (config-router) # <b>area area-id default-cost cost</b>	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.

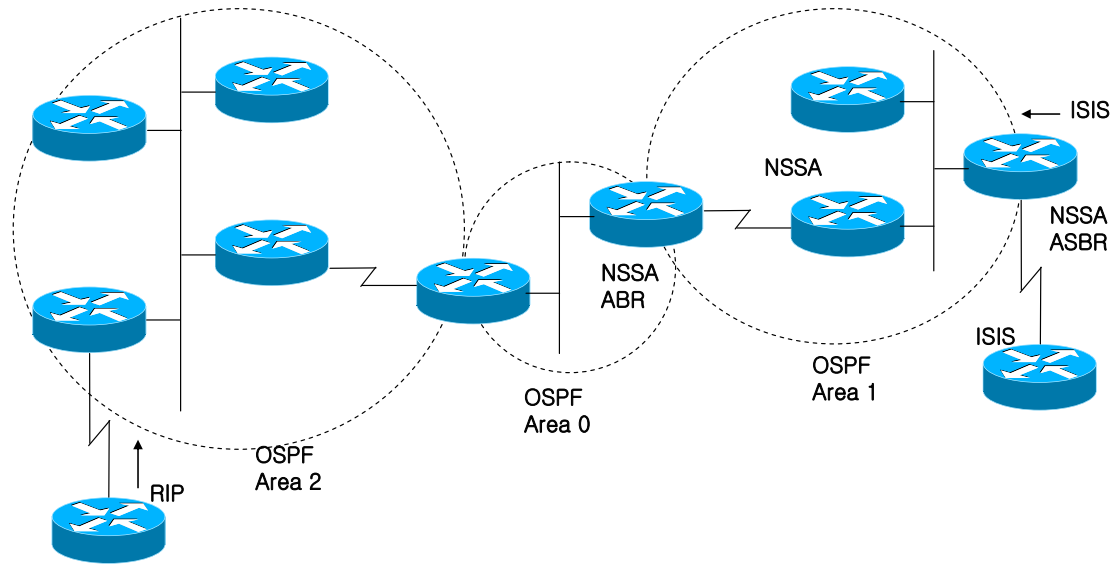


그림 8-1. OSPF Network

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) # <b>area area-id nssa</b> [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) # <b>area</b> <i>area-id</i> <b>range</b> <i>ip-address mask</i> [ <b>advertise</b>   <b>not-advertise</b> ] [ <b>cost</b> <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) # <b>summary-address</b> { <i>ip-address/prefix</i> } [ <b>not-advertise</b> ] [ <b>tag</b> <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) # <b>area</b> <i>area-id</i> <b>virtual-link</b> <i>router-id</i> [ <b>authentication</b> [ <b>message-digest</b>   <b>null</b> ]] [ <b>hello-interval</b> <i>seconds</i> ] [ <b>retransmit-interval</b> <i>seconds</i> ] [ <b>transmit-delay</b> <i>seconds</i> ] [ <b>dead-interval</b> <i>seconds</i> ] [[ <b>authentication-key</b> <i>key</i> ]   [ <b>message-digest-key</b> <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 라우트를 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) # <b>default-information originate</b> [ <b>always</b> ] [ <b>metric</b> <i>metric-value</i> ] [ <b>metric-type</b> <i>type-value</i> ] [ <b>route-map</b> <i>map-name</i> ]	ASBR 이 OSPF routing domain 에 default route 를 생성하게 한다.

#### 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) # <b>interface Loopback 0</b>	Loopback interface 를 생성한다.
Step 2	Router (config-if) # <b>ip address</b> <i>ip-address/prefix</i>	Interface 에 IP address 를 할당 한다.

### 8.2.9. 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) # <b>auto-cost reference-bandwidth</b> <i>ref-bw</i>	reference-bandwidth 를 변경한다.

### 8.2.10. 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) # <b>distance ospf</b> {[intra-area dist1] [inter-area dist2] [external dist3]}	OSPF distance 를 변경한다.

### 8.2.11. 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) # <b>passive-interface</b> interface-name	Interface 를 통해 송신하는 hello packets 을 제한한다.

### 8.2.12. 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) # <b>timers throttle spf</b> spf-start spf-hold spf-max-wait	SPF 계산 시간을 변경한다.

### 8.2.13. 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) # <b>log-adjacency-changes [detail]</b>	OSPF neighbor UP/Down 에 대한 시스템 메시지를 발생한다.

### 8.2.14. 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) # <b>ip ospf database-filter all out</b>	Interface 의 LSA flooding 을 제한 한다.

### 8.2.15. Ignoring MOSPF LSA Packets

U9200 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) # <b>ignore lsa mospf</b>	MOSPF LSA packet 을 수신했을 때 시스템 메시지를 발생하지 않는다.

### 8.2.16. Monitoring and Maintaining OSPF

OSPF 라우팅 테이블, 데이터베이스, 그리고 이웃한 라우터의 연결 상태에 대한 정보를 조회 할 수 있

다. 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 # <b>show ip ospf</b> [process-id]	OSPF routing process 정보를 조회한다.
Router # <b>show ip ospf border-routers</b>	ABR/ASBR 에 대한 모든 routing table 을 조회한다.
Router # <b>show ip ospf</b> [process-id] <b>database</b>	OSPF database 를 조회한다.
Router # <b>show ip ospf</b> [process-id] <b>database</b> [database-summary]	
Router # <b>show ip ospf</b> [process-id] <b>database</b> [router] [self-originate]	
Router # <b>show ip ospf</b> [process-id] <b>database</b> [router] [adv-router [ip-address]]	
Router # <b>show ip ospf</b> [process-id] <b>database</b> [router] [link-state-id]	
Router # <b>show ip ospf</b> [process-id] <b>database</b> [network] [link-state-id]	
Router # <b>show ip ospf</b> [process-id] <b>database</b> [summary] [link-state-id]	
Router # <b>show ip ospf</b> [process-id] <b>database</b> [asbr-summary] [link-state-id]	
Router # <b>show ip ospf</b> [process-id] <b>database</b> [external] [link-state-id]	
Router # <b>show ip ospf</b> [process-id] <b>database</b> [nssa-external] [link-state-id]	
Router # <b>show ip ospf</b> [process-id] <b>database</b> [opaque-link] [link-state-id]	
Router # <b>show ip ospf</b> [process-id] <b>database</b> [opaque-area] [link-state-id]	
Router # <b>show ip ospf</b> [process-id] <b>database</b> [opaque-as] [link-state-id]	
Router # <b>show ip ospf flood-list</b> [interface-name]	Flooding 될 모든 LSAs 를 조회한다.
Router # <b>show ip ospf interface</b> [interface-name]	OSPF interface 정보를 조회한다.
Router # <b>show ip ospf neighbor</b> [neighbor-id] [detail]	OSPF neighbor 정보를 조회한다.
Router # <b>show ip ospf</b> [process-id] <b>summary-address</b>	Redistribution 정보에 관한 모든 summary address 정보를 조회한다.
<b>show ip ospf</b> [process-id] <b>traffic</b>	OSPF traffic 통계 정보를 조회한다.

<b>show ip ospf [process-id] virtual-links</b>	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 # <b>clear ip ospf [process-id] {process   redistribution   counters   traffic}</b>	OSPF process/counters/redistribution/traffic 을 재 시작 한다.



## 9

## BGP

본 장에서는 U9200 series 스위치에서 사용 가능한 IP 유니캐스트 라우팅 프로토콜들 중에서 BGP에 대해서 기술한다.

## 9.1. BGP 개요

BGP는 서로 다른 관리 도메인(Autonomous System : AS) 간에 라우팅 정보를 주고 받을 수 있도록 해주는 프로토콜로서 RIP와 OSPF와는 달리 한 도메인 내에서의 라우팅이 아닌 도메인 간의 라우팅을 담당한다. U9200 SERIES 스위치에서는 BGP-4를 지원하고 있다.

## 9.2. BGP 설정

BGP의 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 RIP와 OSPF에서처럼 BGP 프로토콜의 활성화 단계가 선행되어야 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.

### 9.2.1. 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 AS에 속한 네이버(**iBGP Peer**)와 다른 AS에 속한 네이버(**eBGP Peer**)로 구분된다. 동일 AS에 속한 네이버들은 직접 연결되어 있을 필요는 없고 내부 라우팅 프로토콜(IGP, 예로 **RIP** 혹은 **OSPF** 등)로 경로 설정이 되어 있으면 된다. 그러나 다른 AS에 속한 네이버와는 물리적으로 연결이 설정되어 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 이루어지면 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

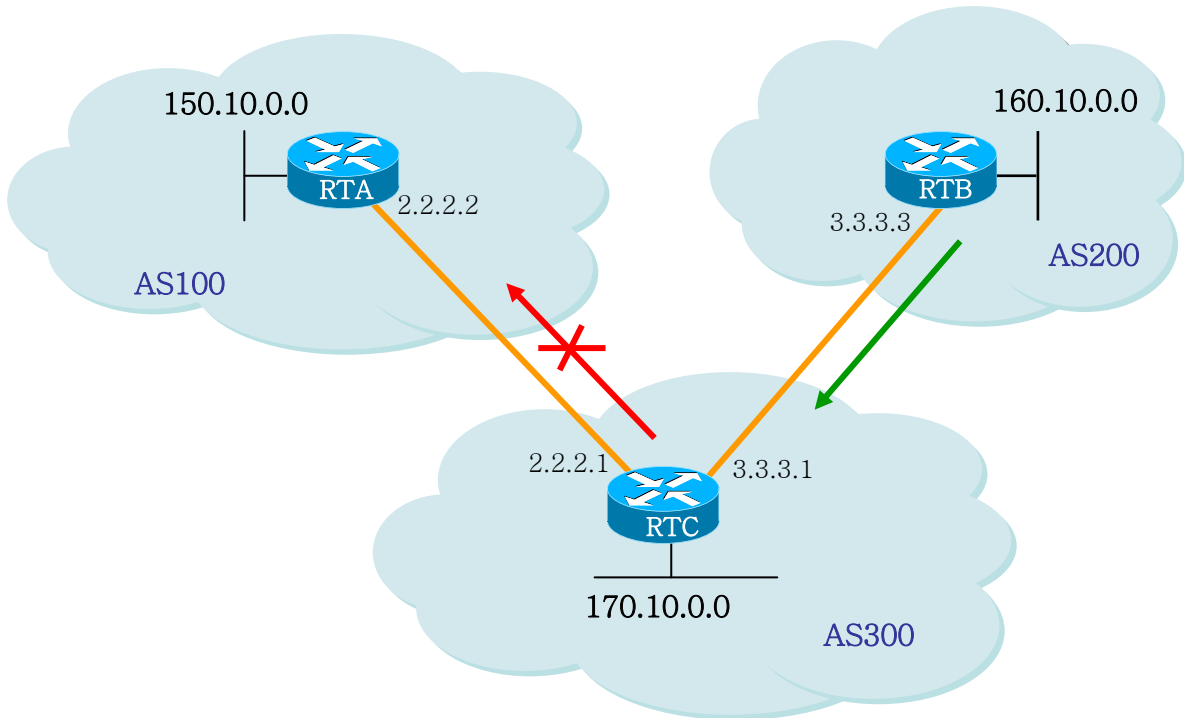
### 9.2.2. BGP 필터링 기능

**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.

### 9.2.2.1. 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}**



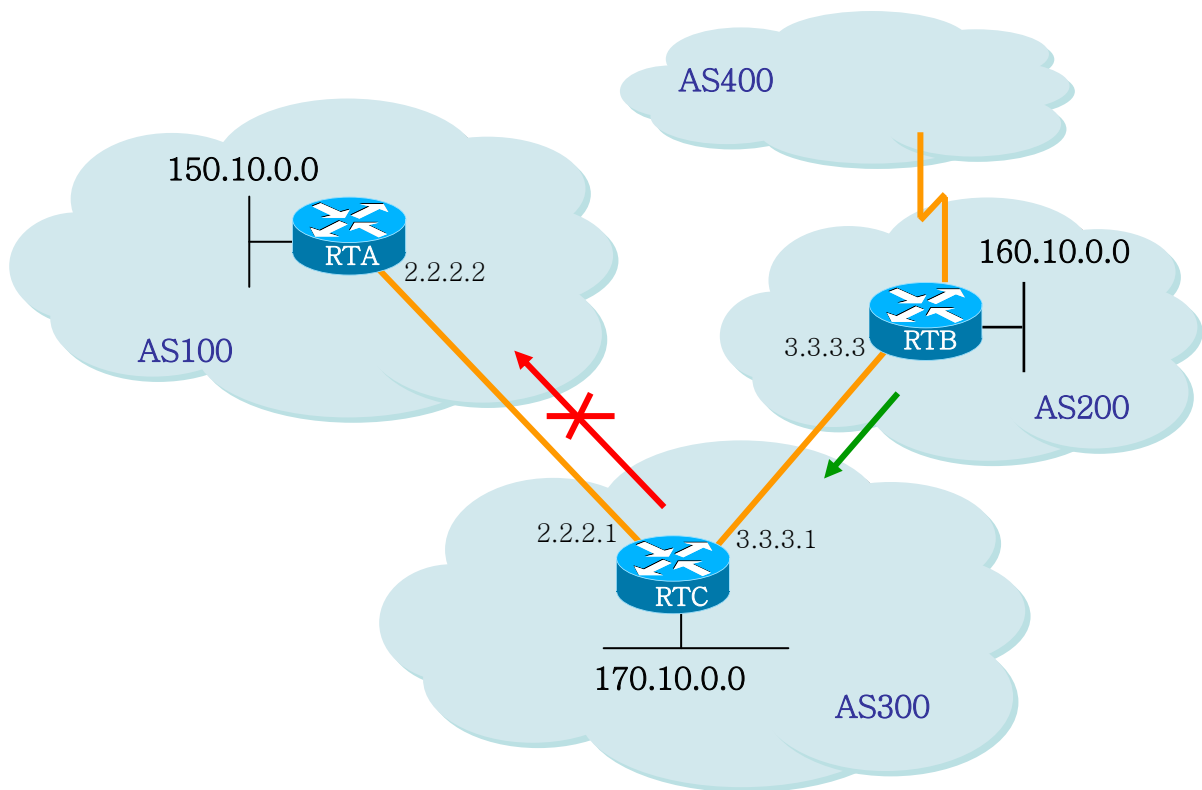
위 그림에서 RTB 는 네트워크 160.10.0.0 을 생성하고 RTC 로 그 정보를 보낸다. 만일 RTC 가 이 정보를 AS 100 으로 전달하지 않기로 하는 경우, 이 정보의 업데이트를 필터링 하기 위해 **access-list** 를 적용하여 RTA 로의 연결에 이것을 적용한다. 이것의 구성을 살펴보면 다음과 같다.

```
/*-- 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
!
```

### 9.2.2.2. 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}
```



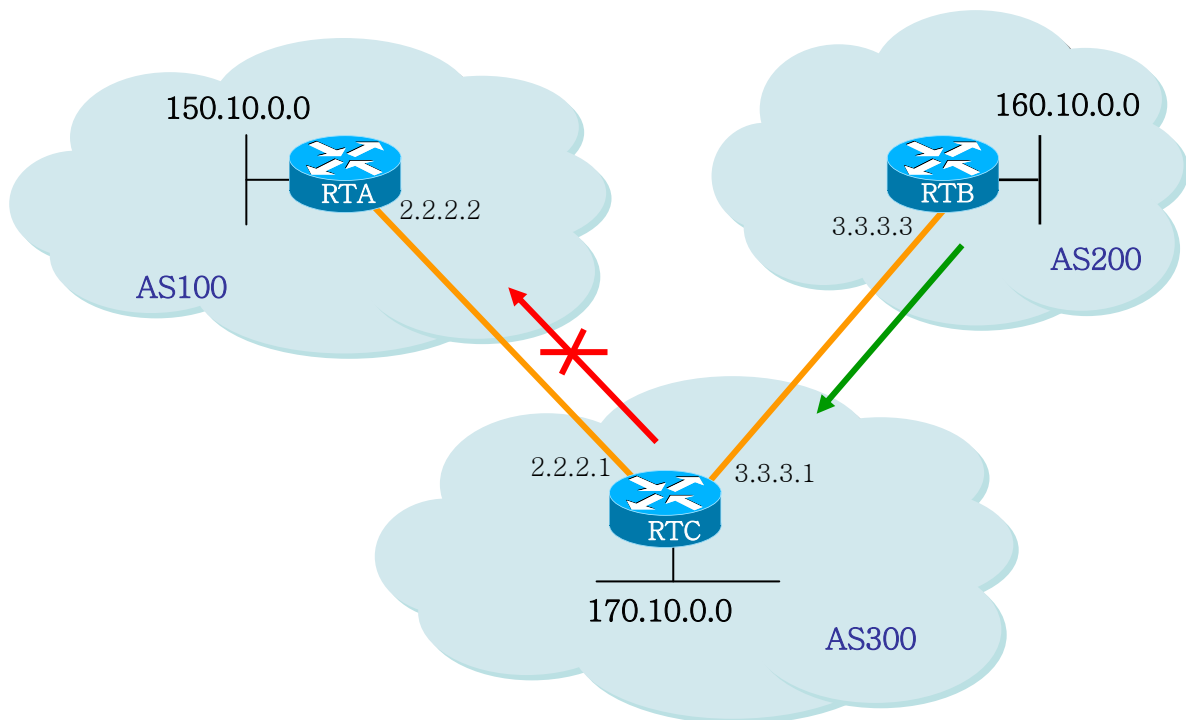
다음의 구성은 위 그림의 RTC 가 RTA 로 160.10.0.0 의 업데이트를 하는 것을 path filtering 을 사용하여 수행하는 구성을 보여준다.

```
/*-- 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 .*
!
```

### 9.2.2.3. 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, **U9200 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 100 을 가진 라우트는 리스트 1 에 매치될 것이고 **set** 설정에 의해서 **weight** 값이 20 으로 세팅된다. **Community** 값으로 200 만을 가진 라우트는 리스트 2 에 매치되어 **weight** 값 10 을 갖게 된다. 키워드 **exact** 는 **community** 가 200 만을 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.

#### 9.2.2.4. BGP Attribute 설정

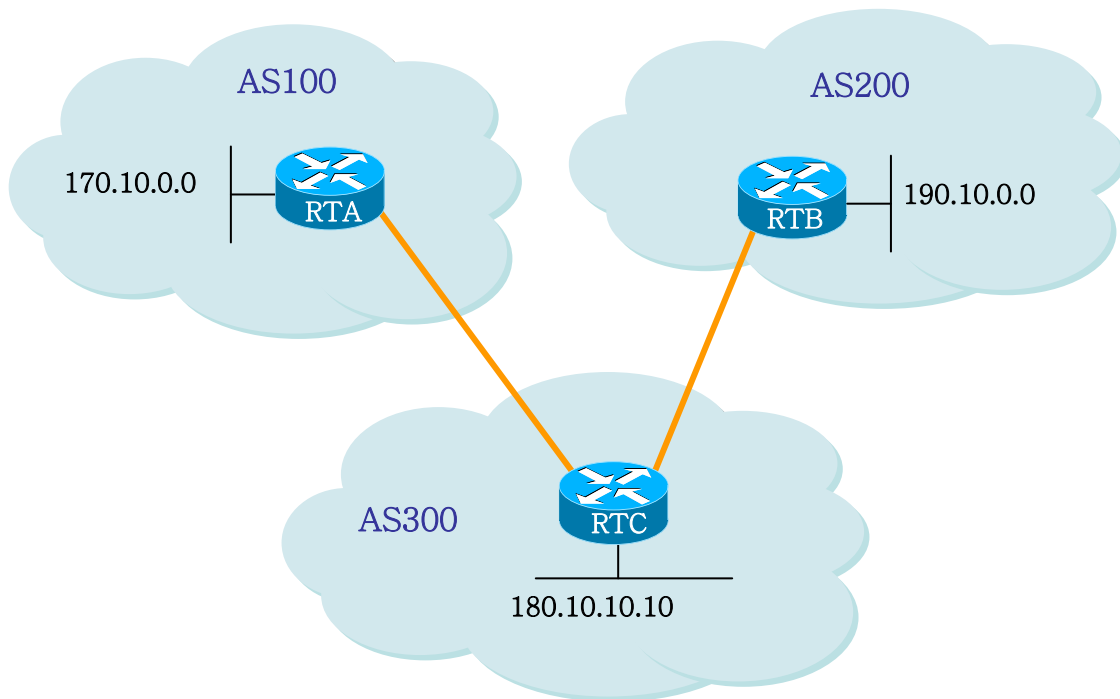
BGP 에 사용되는 **attribute** 들에는 다음과 같은 것들이 있다.

- ✓ **As-path attribute**
- ✓ **Origin attribute**
- ✓ **Nexthop attribute**
- ✓ **Local Preference attribute**



- ✓ Metric attribute
- ✓ Community attribute
- ✓ Weight attribute

#### 9.2.2.5. As\_path Attribute



하나의 라우트가 하나의 AS 를 지나갈 때, 이 AS 의 번호가 해당 라우트의 업데이트에 추가된다.

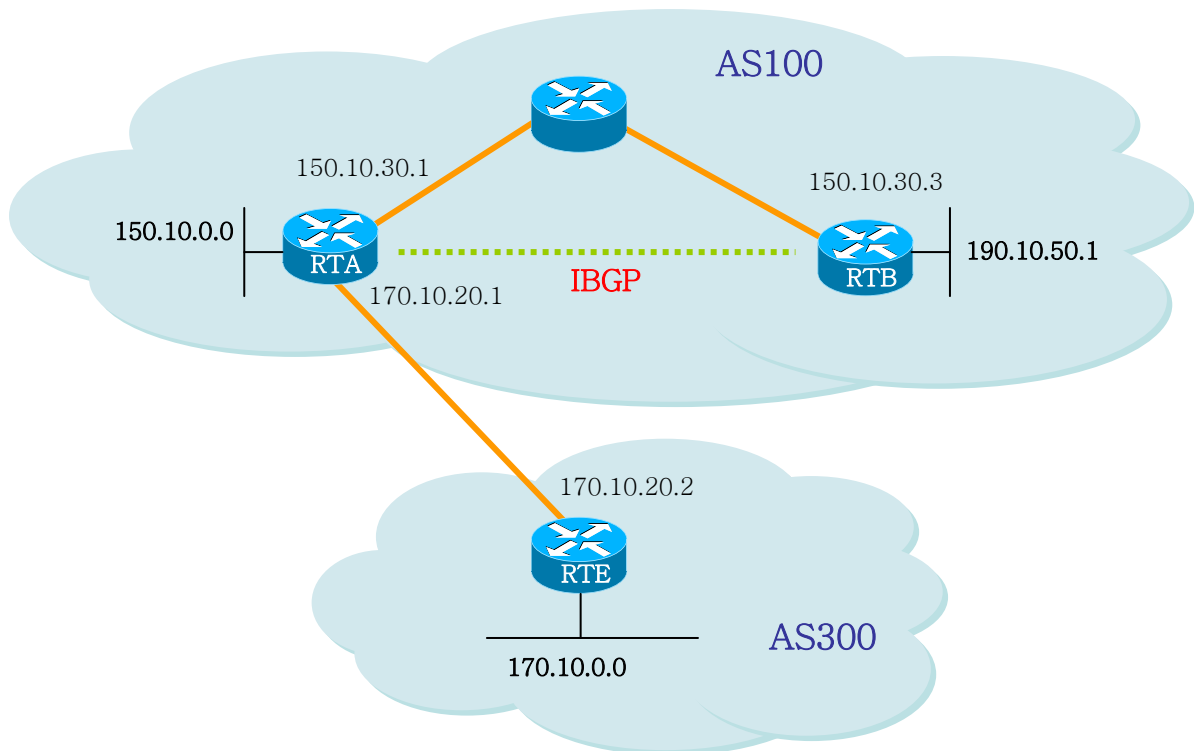
**AS\_path** attribute 는 하나의 라우트가 특정 목적지에 도달하기 위해 지나온 AS 번호들의 리스트를 가리킨다. **AS-SET** 은 하나의 라우트가 지나온 모든 AS 들의 집합을 가리킨다. 위 그림에서 네트워크 190.10.0.0 은 AS200 에 있는 RTB 에 의해 알려진다. 이 라우트가 AS 300 을 지나갈 때 RTC 는 자신의 AS 번호 300 을 이 라우트의 **as-path** 에 덧붙인다. 그래서 190.10.0.0 라우트가 RTA 에 도달시 RTA 는 그것에 추가된 2 개의 AS 번호인 200 과 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.

### 9.2.2.6. 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
!
```

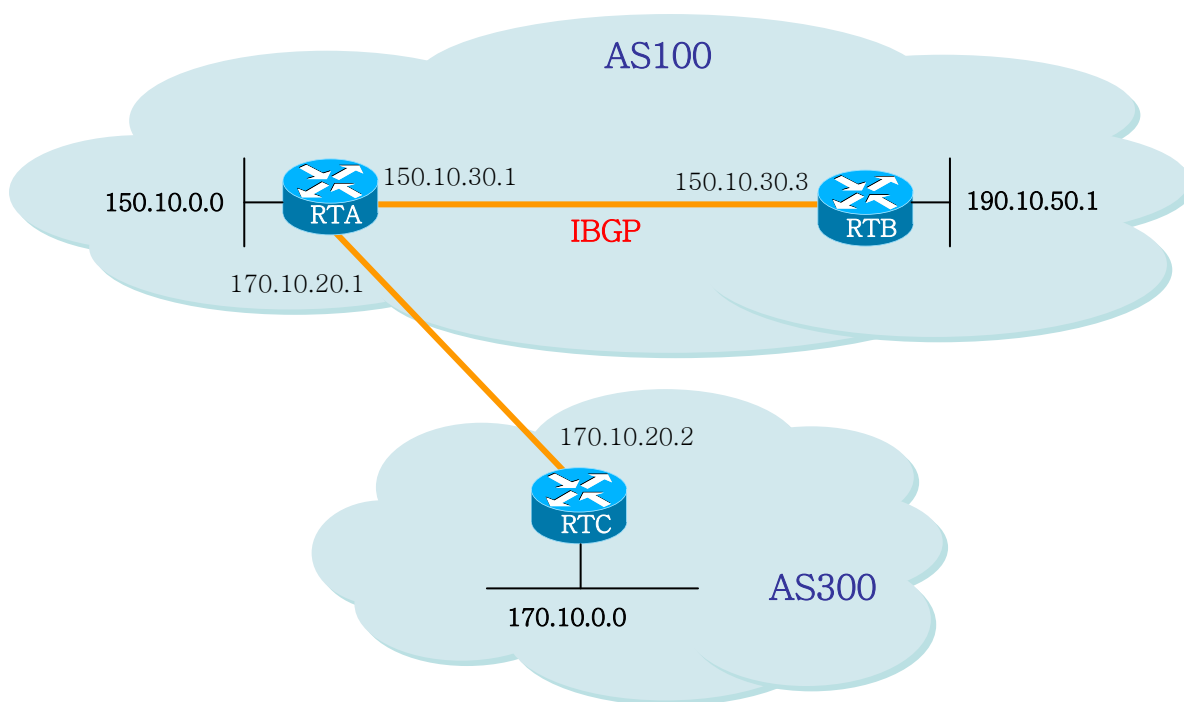
위 그림의 구성에서,

- 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.)

### 9.2.2.7. BGP Nexthop Attribute

nexthop attribute 은 특정 목적지에 도달하기 위해 사용될 nexthop IP address 를 가리킨다. EBGP 의 경우, 이 nexthop 은 언제나 네이버 명령에서 지정된 네이버의 IP 주소이다. 다음 그림에서, RTC 는 RTA 로 170.10.0.0 의 정보를 전달시 넥스트 홉을 170.10.20.2 로 보내고, RTA 는 RTC 로 150.10.0.0 을 전달시 넥스트 홉을 170.10.20.1 로 보낸다. IBGP 경우, EBGP 가 전달하는 넥스트 홉은 IBGP 에서 는 그대로 전달되어야 한다고 프로토콜에 규정되어 있다. 이 규정으로 인하여, RTA 는 170.10.0.0 을 자신의 IBGP peer 인 RTB 로 전달시 넥스트 홉을 170.10.20.2 로 보낸다. 따라서 RTB 의 경우, 170.10.0.0 에 도달하기 위한 넥스트 홉은 150.10.30.1 이 아닌 170.10.20.2 이다.

이를 위해 RTB 는 IGP 를 통해 170.10.20.2 에 도달할 수 있도록 조치가 취해져야 한다. 그렇지 않으면 RTB 는 170.10.0.0 으로 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
!

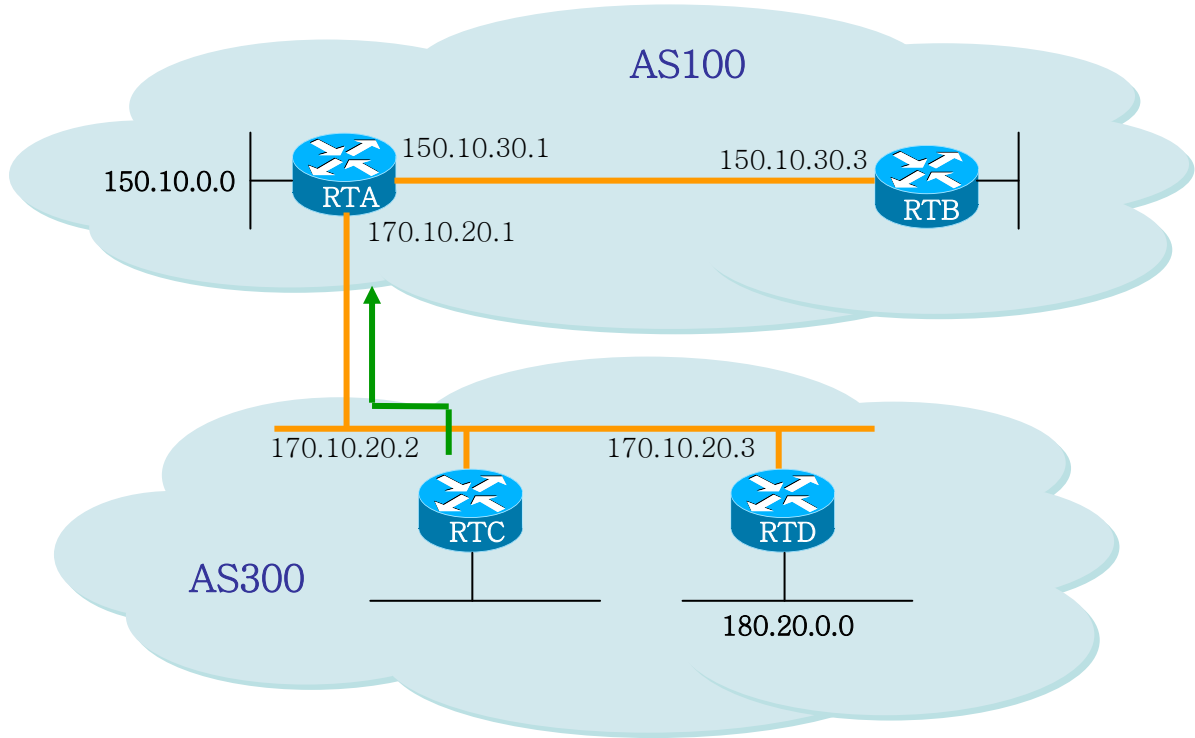
/*-- RTC --*/
!
router bgp 300
 network 170.10.0.0
 neighbor 170.10.20.1 remote-as 100
!

```

- 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.

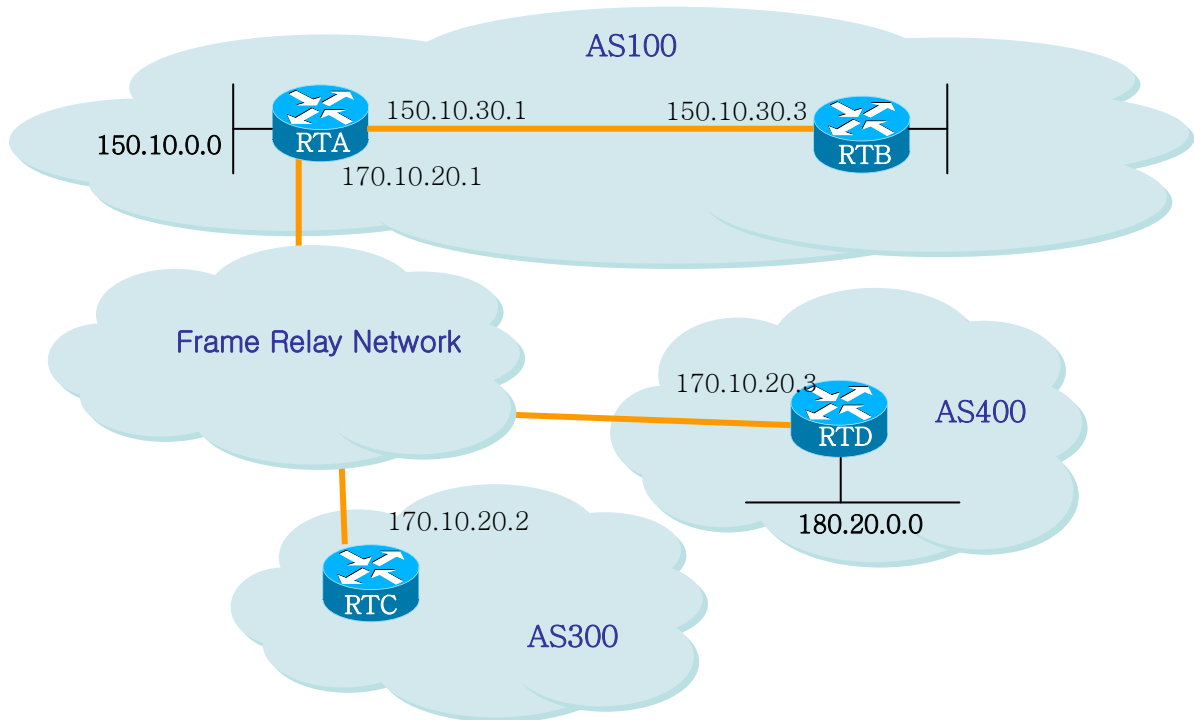
### 9.2.2.8. BGP Nexthop (Multiple access networks)



위 그림에서 AS 300 에 있는 RTC 와 RTD 는 OSPF 를 돌리고 있다고 가정한다. RTC 는 RTA 와 EBGP 연결을 설정한다. RTC 는 170.10.20.3 을 통하여 180.20.0.0 망에 도달할 수 있다. RTC 가 180.20.0.0 정보를 RTA 로 BGP 업데이트를 통해 전송 시, 넥스트 홉으로 자신의 IP 인 170.10.20.2 가 아닌 170.10.20.3 을 사용한다. 이는 RTA, RTC, RTD 간의 망이 멀티액세스 망이고 RTA 가 180.20.0.0 에 도달하기 위해 RTC 를 거치는 과정을 거치기 보다는 RTD 를 바로 넥스트 홉으로 사용하는 것이 더 합리적이기 때문이다.

만일 RTA, RTC, RTD 에 공통인 미디어가 멀티액세스가 아니라. NBMA 인 경우는 더욱 복잡한 현상이 발생한다.

### 9.2.2.9. 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.

### 9.2.2.10. 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
!
```

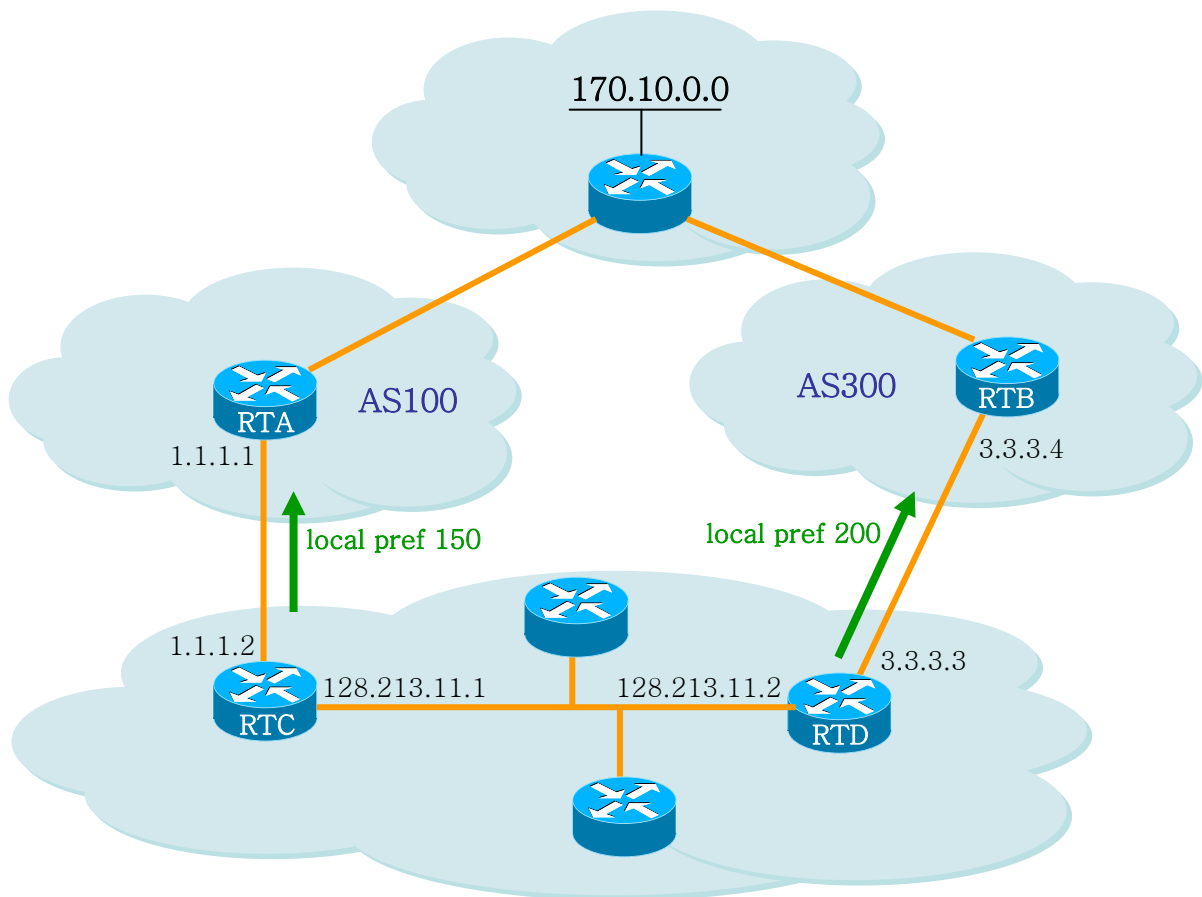
RTC 는 180.20.0.0 를 nextHop = 170.10.20.2 로 전송한다.

### 9.2.2.11. 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
!
```

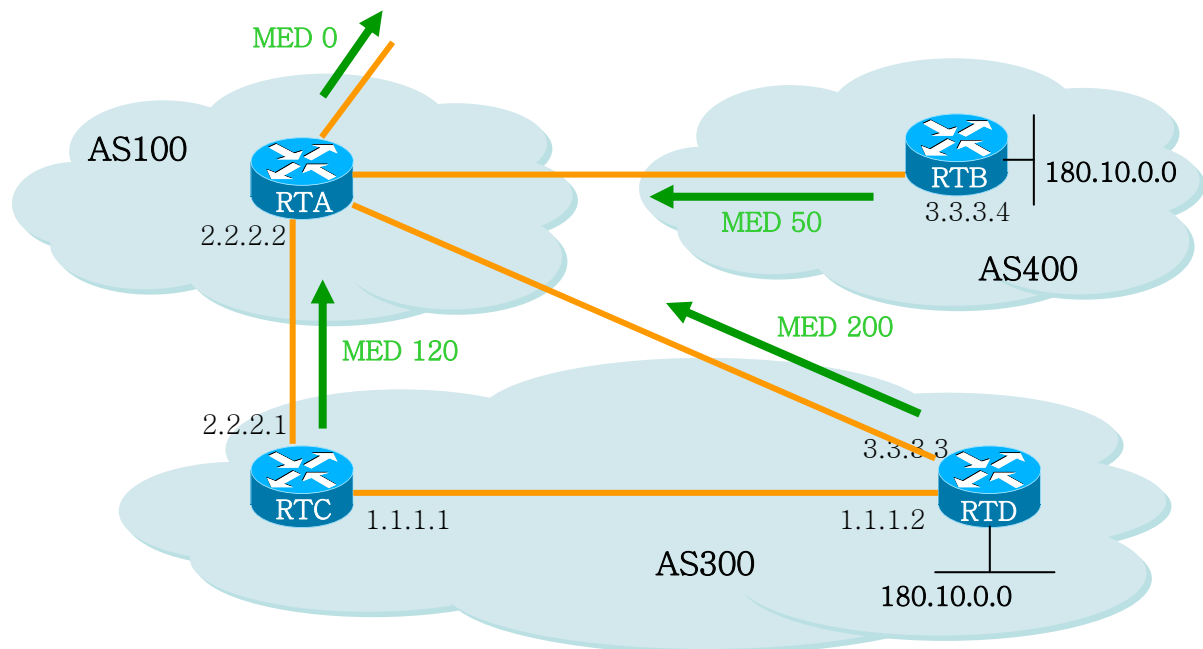
이 구성을 통해, AS300에서 오는 업데이트는 **local preference** 200으로 세팅되고, AS34로부터 오는 다른 업데이트들은 **local preference** 150으로 세팅된다.



### 9.2.2.12. 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.

RTC로부터 오는 메트릭 값을 120 으로 세팅하고 RTD로부터 오는 메트릭 값은 200 으로 RTB로부터 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 RTD로부터 오는 메트릭 만을 비교할 수 있어서 RTC 를 베스트 넥스트 홉으로 선택한다. 왜냐하면 120 이 200 보다 작기 때문이다. RTA 가 RTB로부터 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, RTA는 RTC를 베스트 홉으로 선택한다. (다른 모든 attribute들이 동일하다고 가정시). RTB가 메트릭 비교에 포함되기 위해서는 RTA를 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 RTA 는 180.10.0.0 에 도달하기 위한 최적의 넥스트 홉으로 RTB 를 선택한다.

**default-metric number** 명령을 사용하여 BGP 로 라우트를 **redistribute** 하면서 메트릭 값을 세팅할 수도 있다. 위 예에서 RTB 가 스태틱 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
```

### 9.2.2.13. Community Attribute

community attribute 는 0 에서 4,294,967,200 까지의 값을 갖는 optional, transitive attribute 이다. community attribute 는 여러 개의 목적지들을 특정 community 로 그룹화하는 방법인데, 이렇게 그룹화된 커뮤니티에 라우팅 결정(accept, prefer, redistribute 등)을 적용 가능하게 된다.

community attribute 를 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 세팅 되지 않은 경우, 200 이 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
```

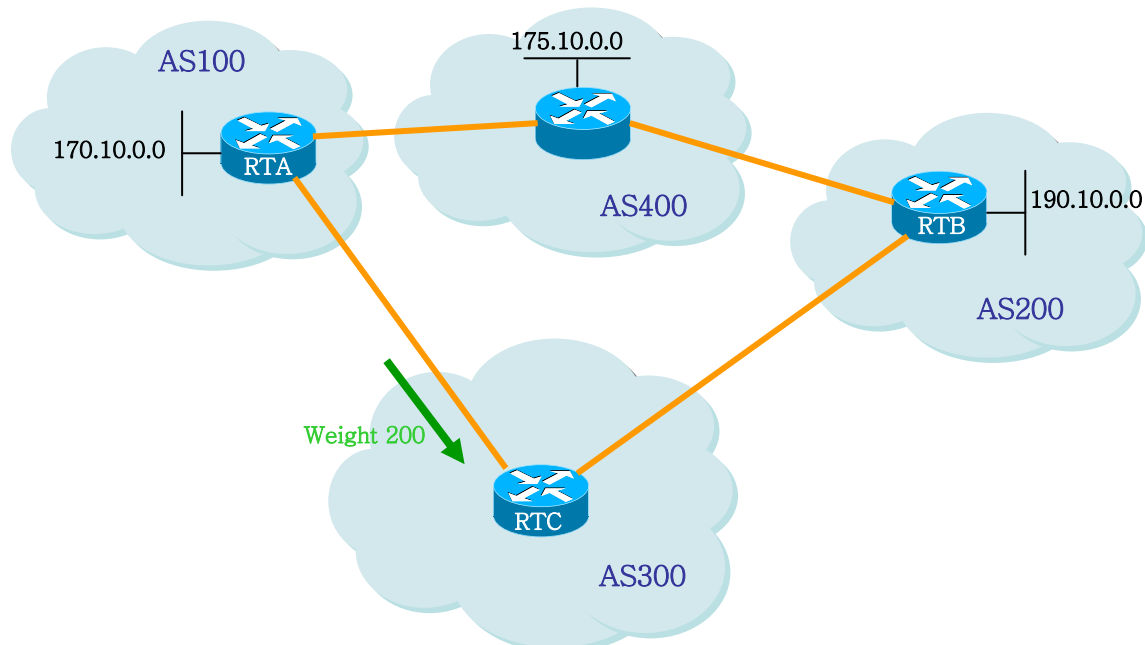
```
/*-- RTA --*/
!
router bgp 100
 neighbor 3.3.3.3 remote-as 300
 neighbor 3.3.3.3 send-community
 neighbor 3.3.3.3 route-map setcommunity out
!
```

앞서 설명한것처럼 **neighbor send-community** 가 디폴트로 활성화 되어 있어 'neighbor 3.3.3.3 send-community' 명령은 필요치 않다.

#### 9.2.2.14. 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 한

다. 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
!
```

### 9.1.2. Routing Policy 변경

Routing policy 라 함은 네이버 라우터와 라우팅 정보를 주고 받을 때 **route-map**, **filter-list**, **prefix-list** 등을 이용하여 받아들이고 정보와 제공할 정보에 대한 취사 선택을 할 수 있도록 해주는 것이다. BGP 에서 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 복구 시에는 **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 받아들여지게 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]
```

### 9.1.3. BGP Peer Groups

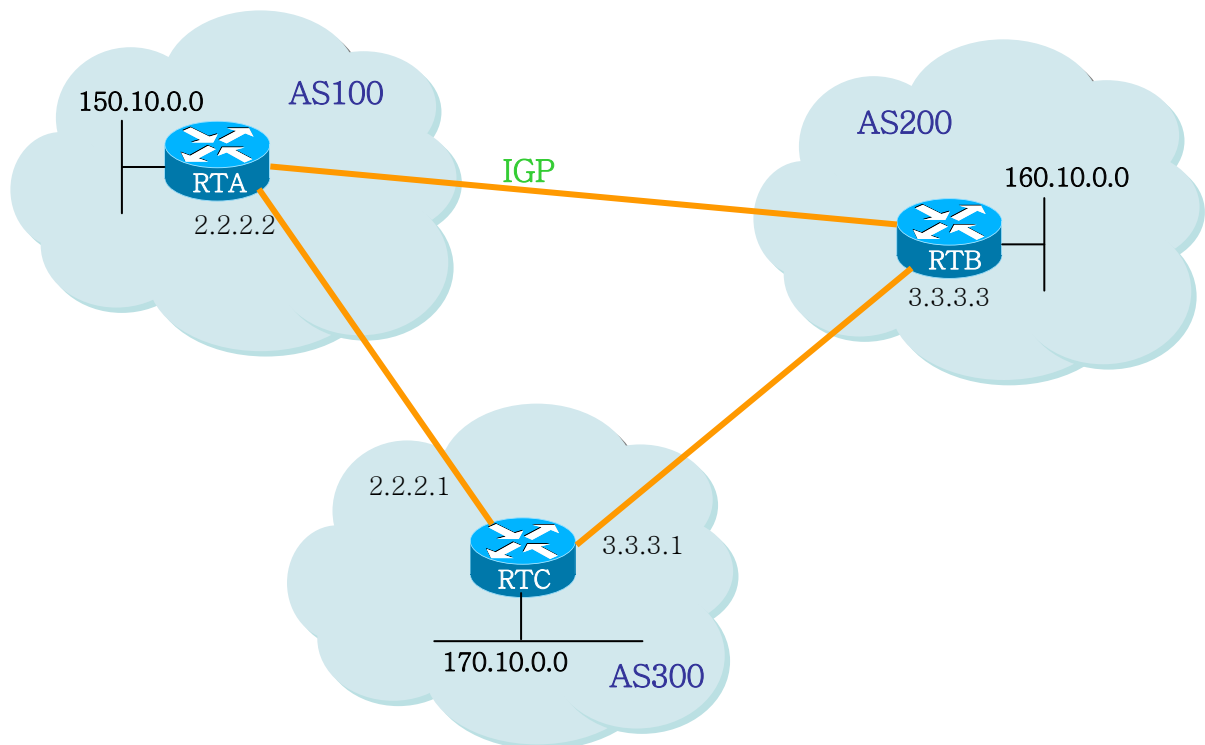
동일한 업데이트 **policy** 가 적용되는 BGP 네이버들의 그룹을 의미한다. 업데이트 폴리시는 주로 라우트 맵, **distribute-list**, **filter-list** 에 의해 적용된다. 각각의 별도 네이버에 동일한 폴리시를 정의하는 대신에, **Peer group name** 을 정의하여 그 피어 그룹에 이러한 폴리시들을 적용한다.

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 RTA와 RTC는 EBGP로 연결되어 있고, RTB와 RTC 간에도 EBGP 연결이 되어있다. RTA와 RTB는 IGP 프로토콜(OSPF, RIP 등)을 돌리고 있다. EBGP 업데이트는 IGP distance 값보다 작은 20의 distance 값을 갖는다. 참고로 RIP 경우는 디폴트 distance 값이 120이고, OSPF는 110의 값을 갖는다.

RTA는 두 개의 라우팅 프로토콜을 통해 160.10.0.0에 대한 업데이트 정보를 수신한다. 이 중 하나는 distance 값 20을 갖는 EBGP, 다른 하나는 distance 값이 20보다 큰 값을 갖는 IGP 정보이다.

디폴트로, BGP는 다음의 distance 값을 갖지만 다음의 distance command에 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 전달되지 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.

#### 9.1.4. 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:

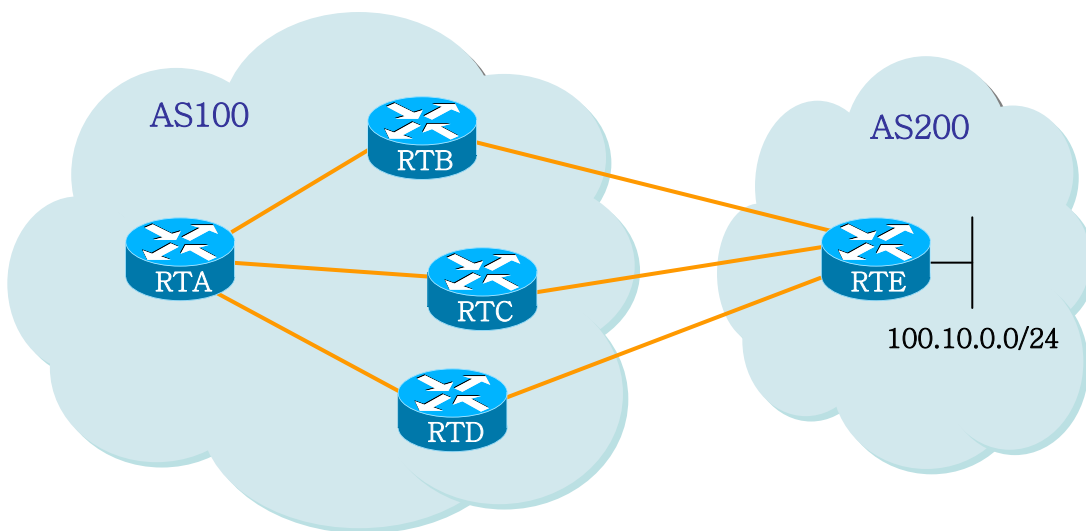
Neighboring AS or sub-AS (before the addition of the eBGP Multipath feature)  
AS-PATH (after the addition of the eBGP Multipath feature)

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 disable되어 있다. 따라서 multipath 기능을 사용하기 위해서 다음의 명령어를 사용한다.

**maximum-path [ibgp] number**

Multipath 기능을 사용하기 위해 RTA에서 다음과 같이 설정을 한다.

```

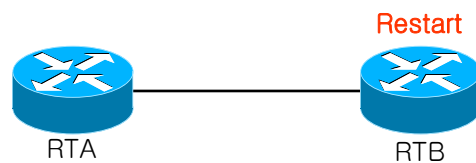
/*-- RTA --*/
!
router bgp 100
 maximum-paths ibgp 3
 neighbor 10.1.1.1 remote-as 200 /* RTB */
 neighbor 20.1.1.1 remote-as 200 /* RTC */
 neighbor 30.1.1.1 remote-as 200 /* RTD */
!

```

### 9.1.5. 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 */
!
  
```

### 9.1.6. 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
```

### 9.1.7. 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
```

### 9.1.8. 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.

### 9.1.9. BGP disable-adj-out

U9200 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.

### 9.1.10. Use of set as-path prepend Command

어떤 상황에서는 BGP decision process를 조절하기 위해 경로 정보를 조정해야만 할때가 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 최소화 하고자 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
<b>History state</b>	해당 route 에 대한 best path 를 갖고 있지는 않지만, 여전히 해당 라우트 플래핑에 대한 정보는 존재하는 상태
<b>Damp state</b>	패널티 값이 한계치를 초과 한 상태로 네이버에게 정보 전달이 안된다.
<b>Penalty</b>	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
<b>Suppress limit</b>	route 에 부과되는 패널티 값의 한계치로 디폴트 2000 이다
<b>Half-life-time</b>	route 에 부과된 패널티 값은 half-life-time 에 설정된 시간(디폴트 15 분)이 지나면 반으로 줄어드는데, 이러한 감소는 5 초마다 행해진다.
<b>Reuse-limit</b>	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
<b>Maximum suppress limit</b>	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
<b>ip igmp snooping</b>	해당 VLAN 에 IGMP Snooping 을 enable 한다.
<b>no ip igmp snooping</b>	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
<b>ip igmp snooping report-suppression</b>	VLAN interface 에 IGMP report-suppression 을 설정한다.
<b>no ip igmp snooping report-suppression</b>	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 responsetime 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
<b>ip igmp snooping fast-leave</b>	해당 VLAN 에 fast-leave 기능을 설정한다.
<b>no ip igmp snooping fast-leave</b>	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
<b>ip igmp snooping mrouter interface IFNAME</b>	해당 VLAN 에 mrouter port 를 수동으로 설정한다. IFNAME 은 이미 VLAN 내의 Member-Port 여야 한다.
<b>no ip igmp snooping mrouter interface IFNAME</b>	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 Host의 멀티캐스트 그룹을 제한하기 위해서는 아래의 명령을 interface configuration mode에서 실행한다.

명령어	설명
<b>ip igmp snooping access-group &lt;access-list&gt;</b>	해당 포트에 수신되는 호스트들의 멀티캐스트 그룹에 대한 등록을 제한한다.
<b>no ip igmp snooping access-group &lt;access-list&gt;</b>	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 interface의 member인 경우, 특정 VLAN interface에서만 IGMP Host들의 멀티캐스트 그룹을 제한할 수 있으며 아래의 명령을 interface configuration mode에서 실행한다.

명령어	설명
<b>ip igmp snooping access-group &lt;access-list&gt; vlan &lt;vlan-id&gt;</b>	지정된 VLAN Interface의 member interface로 수신되는 IGMP Host들의 멀티캐스트 그룹에 대한 등록을 제한한다.
<b>no ip igmp snooping access-group &lt;access-list&gt; vlan &lt;vlan-id&gt;</b>	지정된 VLAN Interface의 member interface로 수신되는 IGMP Host들의 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
<b>ip igmp snooping limit &lt;count&gt;</b>	해당 포트에 수신되는 Multicast Group 의 개수를 제한한다.
<b>ip igmp snooping limit &lt;count&gt; except &lt;access-list&gt;</b>	해당 포트에 수신되는 Multicast Group 의 개수를 제한한다. 제한하지 않을 Group 은 access-list 로 만들어 지정한다.
<b>no ip igmp snooping limit &lt;count&gt;</b>	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
<b>ip igmp snooping limit &lt;count&gt; vlan &lt;vlan-id&gt;</b>	해당 포트에서 해당 VLAN 으로 수신되는 Multicast Group 의 개수를 제한한다.
<b>ip igmp snooping limit &lt;count&gt; vlan &lt;vlan-id&gt; except &lt;access-list&gt;</b>	해당 포트에서 해당 VLAN 으로 수신되는 Multicast Group 의 개수를 제한한다. 제한하지 않을 Group 은 access-list 로 만들어 지정한다.
<b>no ip igmp snooping limit &lt;count&gt; vlan &lt;vlan-id&gt;</b>	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 1 IGMP Snooping 관련 모니터링 명령어

명령어	설명
<b>show ip igmp snooping mrouter &lt;IFNAME&gt;</b>	해당 VLAN 에 대한 mrouter port 를 보여준다.
<b>show ip igmp snooping statistics</b>	IGMP snooping 의 통계 정보를 보여준다

# 11

## IP 멀티캐스트 라우팅

본 장에서는 IP 멀티캐스트 라우팅의 구성요소와 U9200 Series 스위치에서의 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, 사설망내에 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.

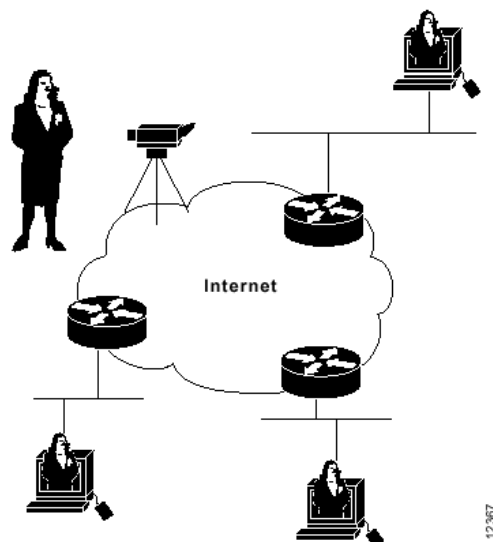


그림 11-1. 여러 목적지에 트래픽을 전달하는 방법을 제공하는 멀티캐스팅

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.



## 11.4. IP 멀티캐스트 라우팅 설정

### 11.4.1. Enable IP 멀티캐스트 라우팅

기본적으로 멀티캐스트 패킷을 포워딩하기 위해서는 IP 멀티캐스트 라우팅이 **enable** 되어야 한다. 다음의 명령을 global configuration mode 에서 사용한다.

명령어	설명
<b>ip multicast-routing igmp-querier</b>	Multicast Routing 을 위한 IGMP Host Membership 관리를 위해서 IGMP Querier 를 enable 한다.
<b>no ip multicast-routing igmp-querier</b>	IGMP Querier 를 Disable 한다.
<b>ip multicast-routing pim-sm</b>	Multicast Routing 을 위해서 PIM-SM 을 enable 한다.
<b>no ip multicast-routing pim-sm</b>	PIM-SM 을 Disable 한다.

```
Router# configure terminal
Router(config)# ip multicast-routing pim-sm
Router(config)# ip multicast-routing igmp-querier
```

### 11.4.2. Enable IGMP-TRAP on an interface

라우터에서 IGMP Querier 를 활성화할 때에는 IGMP packet 들을 수신할 수 있도록 각 port interface 에서 IGMP-TRAP 을 반드시 enable 해야 한다.

명령어	설명
<b>igmp-trap</b>	해당 인터페이스에 igmp-trap 를 enable 한다.
<b>no igmp-trap</b>	igmp-trap 를 Disable 한다.

```
Router# configure terminal
Router(config)# interface gil
Router(config-if-gil)# igmp-trap
```

### 11.4.3. Enable PIM on an interface

PIM-SM 의 실행을 위해서는 해당 인터페이스에 PIM Flag 가 반드시 **enable** 되어있어야 한다. 인터페이스에서 PIM Flag 를 enable 하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
<b>ip pim</b>	해당 인터페이스에 PIM Flag 를 enable 한다.
<b>no ip pim</b>	PIM Flag 를 Disable 한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim
Router# show ip pim interface
```

Address	Interface	Status	Version/Mode	Nbr Count	JP Intvl	MCache Intvl	CISCO ChkSum	PRI	DR
10.1.1.254	vlan11	DOWN	v2/Sparse	0	60	110	OFF	1	10.1.1.254

```
total : 1
```

#### 11.4.4. Enable IGMP on an interface

IGMP Querier 의 실행을 위해서는 해당 인터페이스에 IGMP Flag 가 반드시 enable 되어 있어야 한다. 인터페이스에서 IGMP Flag 를 enable 하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
<b>ip igmp</b>	해당 인터페이스에 IGMP Flag 를 enable 한다.
<b>no ip igmp</b>	IGMP Flag 를 Disable 한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip igmp
Router# show ip igmp interface
```

```
Name : vlan1
IGMP is enabled on interface.
  IGMP version is 2.
  IGMP leave-timeout is 5 seconds.
  IGMP member-checking-interval is 2 seconds.
  IGMP querier-timeout is 132 seconds.
  IGMP query-interval is 60 seconds.
  IGMP query-max-response-time is 25 seconds.
  Internet address is 10.1.1.254, subnet mask is 255.255.255.0.
Quering Router(10.1.1.254)
```

## 11.4.5. Configure IGMP Functionality

IGMP의 다양한 특성들에 대해 설정하기 위해서는 다음에 나오는 작업들을 수행한다.

### 11.4.5.1. IGMP Access Group

멀티캐스트 라우터는 이 라우터가 부착된 네트워크의 호스트들이 가입한 멀티캐스트 그룹들을 알아내기 위해 IGMP host-query 메시지를 주기적으로 전송한다. 이후, 라우터는 해당 멀티캐스트 그룹을 목적으로 하는 모든 패킷들이 오면 이를 이 그룹의 멤버들에게 포워딩한다. 인터페이스에 의해 서비스되는 서브넷의 호스트들이 가입할 수 있는 멀티캐스트 그룹을 제한하기 위한 각 인터페이스에 필터를 설정할 수 있다.

인터페이스에서 특정 멀티캐스트 그룹의 접근을 필터링하기 위해서는 아래의 명령을 interface configuration mode에서 실행한다.

명령어	설명
<b>ip igmp access-group</b> <i>access-list-number</i>	해당 인터페이스에 의해 서비스되는 서브넷의 호스트들이 가입할 수 있는 멀티캐스트 그룹 제어
<b>no ip igmp access-group</b>	해당 인터페이스에 설정된 그룹제어를 해제한다.

```
Router# configure terminal
Router(config)# access-list 1 deny 239.0.0.0 255.0.0.0
Router(config)# interface vlan1
Router(config-if-vlan1)# ip igmp access-group 1
```

### 11.4.5.2. IGMP filter-receive-query

멀티캐스트 라우터는 query message를 수신하면 querier selection을 수행한다. 가입자 VLAN에서 query message가 수신되어도 querier selection을 수행한다. 가입자 VLAN의 라우터가 querier로 선출되는 것을 제한하기 위해 query message를 차단할 수 있다.

가입자 VLAN에서 수신되는 query message를 차단하기 위해서는 아래의 명령을 global configuration mode에서 실행한다.

명령어	설명
<b>ip igmp filter-receive-query</b>	가입자 VLAN에서 수신되는 query message를 차단한다.

<b>no ip igmp filter-receive-query</b>	filter-receive-query 를 해제한다.
--	------------------------------

```
Router# configure terminal
Router(config)# ip igmp filter-receive-query
Router(config)#
```

#### 11.4.5.3. IGMP Query Transmit Interval

멀티캐스트 라우터는 Multicast Membership 관리를 위해서 주기적으로 IGMP Query 메시지를 전송한다. 이 메시지는 TTL을 1로 하며, all-system-group-address인 224.0.0.1로 보내진다.

멀티캐스트 라우터들은 LAN (서브넷)을 위한 IGMP Query 메시지를 전송하기 위한 IGMP Querier router를 선출하는데, IP 주소의 값이 가장 작은 라우터가 선출되게 된다. 선출된 Querier Router는 LAN 상의 모든 호스트들에게 IGMP Query 메시지를 전송할 책임이 있으며, 또한 RP 라우터에게 PIM Register와 PIM Join 메시지를 전송한다.

디폴트로 IGMP Querier Router는 호스트와 네트워크의 IGMP 오버헤드를 낮게 유지하기 위하여 IGMP host-query 메시지를 125초마다 보낸다. 이 메시지의 전송 간격을 변경하려면, 다음의 명령을 interface configuration mode에서 실행한다.

명령어	설명
<b>ip igmp query-interval seconds</b>	IGMP Querier Router가 IGMP Query 메시지를 전송하는 간격을 설정 (Default : 125 초)
<b>no ip igmp query-interval</b>	설정된 IGMP Query Interval을 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip igmp query-interval 60
```

#### 11.4.5.4. IGMP Leave Timeout

IGMP Querier Router 는 Host 로부터 특정 Multicast Group 에 대해 탈퇴하는 IGMP Leave 메시지를 수신한 경우, Host 가 포함된 해당 VLAN 에 또다른 Multicast Group 에 가입된 Host 가 있는지 Multicast Membership 을 Checking 하게 된다.

해당 VLAN 의 Membership 을 Checking 한 후, Multicast Group 에 대한 Member 가 더 이상 존재하지 않으면, Multicast Membership 에서 삭제된다.

디폴트로 Multicast Membership Checking 시간은 260 초이다.

IGMP Querier Router 가 사용하는 IGMP 의 Leave-timeout 을 변경하기 위해서는 interface configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
<b>ip igmp leave-timeout seconds</b>	IGMP member leave timeout 설정한다. (Default:260 초)
<b>no ip igmp leave-timeout</b>	설정된 IGMP Leave Timeout 을 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip igmp leave-timeout 30
```

#### 11.4.5.5. IGMP Member checking interval

IGMP Querier Router 는 Host 로부터 특정 Multicast Group 에 대해 탈퇴하는 IGMP Leave 메시지를 수신한 경우, Host 가 포함된 해당 VLAN 에 또다른 Multicast Group 에 가입된 Host 가 있는지 Multicast Membership 을 Checking 하게 된다.

Multicast Membership 을 Checking 하기 위해서 전송되는 IGMP Query 메시지는 TTL 을 1 로 하며, all-system-group-address 인 224.0.0.1 로 보내진다.

설정된 Member Checking Interval 은 IGMP Specific-Query Message 에 포함된 Max-Response-Time 으로 사용된다. Member Checking Interval 이 설정되지 않은 경우, IGMP Specific-Query Message 에 포함된 Max-Response-Time 은 Default “1”초이다.

디폴트로 Specific IGMP Query 메시지를 전송하는 주기는 2 초이며, member-checking-interval 을 변경하기 위해서는 interface configuration mode 에서 다음의 명령을 실행한다.

명령어	설명
-----	----

<b>ip igmp member-checking-interval</b> <i>seconds</i>	IGMP member checking interval 을 지정한다. (Default : 2 초)
<b>no ip igmp member-checking-interval</b>	설정된 IGMP member checking interval 을 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip igmp member-checking-interval 1
```

#### 11.4.5.6. IGMP Querier Timeout

서브넷에 있는 IGMP Querier Router 의 동작이 멈추면, 서브넷의 또다른 멀티캐스트 라우터가 해당 인터페이스의 IGMP Querier Router 가 되어 서브넷의 Multicast Membership 관리는 지속적으로 유지된다.

IGMP Non-Querier Router 는 지정된 Querier Timeout 동안 IGMP Querier Router 로부터 IGMP Query 메시지를 수신하지 못하면, Multicast Membership 관리를 위해서 IGMP Querier 의 역할을 수행하게 된다. 이 특징은 IGMPv2 인 경우에만 허용된다.

디폴트로 멀티캐스트 라우터는 **ip igmp query-interval** 에 의해 설정된 query interval value 의 2 배를 기다린다.

명령어	설명
<b>ip igmp querier-timeout</b> <i>seconds</i>	IGMP Querier timeout 을 지정한다. (Default : 255 초)
<b>no ip igmp querier-timeout</b>	설정된 IGMP Querier timeout 을 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip igmp querier-timeout 300
```

#### 11.4.5.7. IGMP Maximum Query Response Time

디폴트로 IGMP 에 Query 메시지에 의해 통지되는 maximum query response time 은 10 초이다. 이 값

의 변경은 라우터가 IGMPv2 를 사용하고 있는 경우에만 가능하다. Host 는 IGMP query message 를 수신하면 query message 에 설정된 maximum query response time 값 이내의 임의의 시간에 report message 를 전송하게 된다. 이를 통하여 IGMP report 가 분산되어 전달되는 효과를 얻게 되는 것이다. 또한 이 값을 조절하여 Sub-Network 의 multicast traffic 의 flooding 을 tuning 할 수 있다. 설정된 Query-Response-Time 은 IGMP General Query 의 Max-Response-Time 으로만 사용된다.

이 Maximum Query Response Time 의 설정 범위는 1 ~ 25 초이며, Maximum query response time 을 변경하기 위해서는 다음의 명령을 interface configuration mode 에서 실행한다.

명령어	설명
<b>ip igmp query-max-response-time seconds</b>	IGMP query 에 공시되는 maximum-query-response-time 을 지정한다. (Default : 10 초)
<b>no ip igmp query-max-reposnse-time</b>	설정된 query-max-response-time 을 기본값으로 설정한다.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip igmp query-max-response-time 5
```

#### 11.4.5.8. IGMP query-based-port

Port 별로 수신되는 Leave 에 대한 Group Specific Query 메시지를 VLAN 의 전체 Port 로 전송하지 않고, Leave 된 Port 로만 전송되도록 하기 위해서는 다음의 명령을 global configuration mode 에서 실행한다.

명령어	설명
<b>ip igmp query-based-port</b>	Group Specific Query 를 해당 port 로만 전송하도록 설정한다.
<b>no ip igmp query-based-port</b>	query-based-port 설정을 해제한다.

```
Router# configure terminal
Router(config)# ip igmp query-based-port
Router(config)#
```

# 12

## 시스템 및 통계 모니터링

본 장은 현재 운영중인 U9200 Series 스위치의 시스템 및 통계 모니터링 기능에 대해 설명한다.

- 시스템 상태 모니터링
- 인터페이스 통계
- Logging 설정
- RMON (Remote Monitoring)
- 임계치 설정

U9200 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. U9200 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 scu]	시스템의 파워, FAN, 온도에 대한 환경 정보를 출력한다. <ul style="list-style-type: none"> <li>cooling: FAN 정보</li> <li>temperature: 온도 정보</li> <li>status: 파워, FAN, 온도의 상태 정보 출력</li> <li>scu: SCU 현재 voltage 정보</li> </ul>	Privileged
show version	시스템의 버전 정보를 보여 준다.	Privileged

## 12.2. 시스템 임계치 설정

U9200 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 온도의 상한 및 하한 임계치를 설정할 수 있다.

표 12-2. 온도 설정 관련 명령어

명령어	설명	모드
temperature threshold HIGHVAL LOWVAL	온도의 임계치를 설정하는 명령어로 임계치를 초과하면 syslog 와 snmp trap 을 발생한다.	Config
show environment temperature	현재의 온도와 임계치를 조회하며 FAN 을 지원하는 모델의 경우 FAN 의 상태도 조회 가능하다.	Privileged

아래 예제는 시스템에 대한 온도 임계치를 설정하였다.

```
Switch# configure terminal
Switch(config)# temperature threshold 80 20
Switch(config)# exit
Switch# show environment temperature
```

Temperature : 74.2 (°C)  
Threshold : High 80 (°C) Low 20 (°C)

### 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
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
memory free low-watermark <10-70>	사용 가능한 memory 량의 임계치를 설정하는 명령어이다. 사용 가능한 memory 가 임계치 보다 낮아지거나 다시 높아지면 syslog 를 발생한다.	Config
show memory usage	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
show memory (bfd bgp imi mstp nsm ospf pimd rip)	각 application 의 memory 사용정보 를 조회한다.	Privileged

## 12.3. 포트 통계

U9200 Series 스위치는 각 포트의 통계 정보를 제공한다. 포트 통계를 보기 위해서는 다음의 명령을 사용한다.

```
show interface [ifname]
```

U9200 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 5/1
```

```
Giga5/1 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"> <li>■ I-Kbps/ O-Kbps</li> <li>■ InOctets/ OutOctets</li> <li>■ InPkts/ OutPkts</li> </ul>	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"> <li>■ TX: bits/s, pkts/s</li> <li>■ RX: bits/s, pkts/s</li> </ul>	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"> <li>■ TX: Unicast/Multicast/Broadcast s</li> <li>■ RX: Unicast/Multicast/Broadcast</li> </ul>	Privileged
show port statistics interface [IFNAME]	아래 항목에 대한 인터페이스의 통계 정보를 출력한다. <ul style="list-style-type: none"> <li>■ InOctets/ OutOctets</li> <li>■ InUcastPkts/ OutUcastPkts</li> <li>■ InMcastPkts/ OutMcastPkts</li> <li>■ InBcastPkts/ OutBcastPkts</li> <li>■ IfInDiscards</li> <li>■ IfInErrors</li> </ul>	Privileged
show port-mib IFNAME	해당 인터페이스의 현재 통계와 누적 통계 정보를 상세하게 출력한다.	Privileged
show interface counters	아래 항목에 대해 인터페이스의 누적 통계 정보를 출력한다. <ul style="list-style-type: none"> <li>■ InOctets/ OutOctets</li> <li>■ InUcastPkts/ OutUcastPkts</li> <li>■ InMcastPkts/ OutMcastPkts</li> <li>■ InBcastPkts/ OutBcastPkts</li> </ul>	Privileged
show interface counters errors	인터페이스에서 발생한 누적 에러 통계 정보를 출력한다	Privileged

다음은 **show interface counter** 명령을 이용하여 전체 포트의 누적 통계 정보를 출력한 내용이다.

```
Router#show interface counters
```

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
-----	-----	-----	-----	-----
Gi5/1	0	0	0	0
Gi5/2	0	0	0	0
Gi5/3	0	0	0	0
Gi5/4	0	0	0	0
Gi5/5	0	0	0	0
Gi5/6	0	0	0	0
Gi5/7	2,560	0	20	0
Gi5/8	2,560	0	20	0

Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
-----	-----	-----	-----	-----
Gi5/1	0	0	0	0
Gi5/2	0	0	0	0
Gi5/3	0	0	0	0
Gi5/4	0	0	0	0
Gi5/5	37,466	0	305	0
Gi5/6	37,220	0	303	0
Gi5/7	36,974	0	301	0
Gi5/8	36,605	0	298	0

```
Router#
```

다음은 **show port statistics** 명령을 이용하여 특정 포트의 5 초/1 분/5 분 통계 정보를 출력한 내용이다.

```
Router#show port statistics gi5/5
```

```
Last clearing of counters 00:14:24
```

Port	bits/s	Tx  pkts/s	bits/s	Rx pkts/s
-----	-----	-----	-----	-----
Gi5/5	-----	-----	-----	-----
5 sec.	392	0	0	0
1 min.	488	0	0	0
5 min.	488	0	0	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</i> <i>low-threshold high-threshold</i>	해당 인터페이스에 대해 일정한 시간 동안 <b>low</b> 및 <b>high</b> 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 U9200 Series 스위치가 제공하는 RMON(Remote Monitoring) 기능을 사용하여, 시스템을 보다 효율적으로 운영하고 네트워크의 로드를 줄일 수 있다. 다음 절에서는 RMON 개념 및 U9200 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

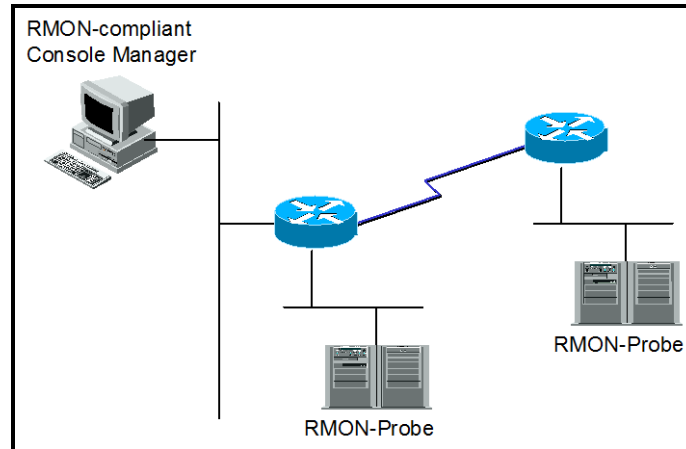


그림 12-1. RMON Manager 와 RMON Probe

기존의 SNMP MIBs 이 SNMP agent 가 탑재된 장비 자체를 관리 대상으로 보고 있는데 반하여 RMON MIBs 는 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 Agent 는 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.

U9200 Series 스위치에서는 <표 9>에서 정의한 RMON 의 9 개 그룹 중 통계, 이력, 알람, 이벤트 그룹 만을 지원한다. RMON 은 디폴트로 모든 설정이 disabled 이다.

표 12-9. RMON 항목

항목	설명
통계	<ul style="list-style-type: none"> <li>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.</li> </ul>
이력	<ul style="list-style-type: none"> <li>관리자가 설정한 시간 간격 내에 발생한 각종 트래픽 및 오류에 대한 정보를 제공</li> <li>기본적으로 단기/장기적으로 간격을 설정 가능하고 1-3600 초를 간격으로 제한</li> <li>이 자료를 통해 시간대별 이용 현황 및 다른 세그먼트와 비교 가능</li> </ul>
경보	<ul style="list-style-type: none"> <li>주기적으로 특정한 값을 체크 해 기준치에 도달하면 관리자에 보고하고 대리인이 자신의 기록을 보유</li> <li>기준치는 절대값 및 상대값으로 정할 수 있고 지속적인 경보 발생을 막기 위해서 상/하한치를 설정해서 넘나드는 경우에만 경보가 발생.</li> </ul>

호스트	<ul style="list-style-type: none"> <li>세그먼트에 연결된 각 장비가 발생시킨 트래픽, 오류 수를 호스트별로 관리</li> </ul>
상위 n 개의 호스트	<ul style="list-style-type: none"> <li>위 호스트 테이블에 발견될 호스트 중에서 일정시간 동안 가장 많은 트래픽을 발생시킨 호스트 검색</li> <li>관리자는 원하는 종류의 자료와 시간 간격 및 원하는 호스트의 개수를 설정해서 정보를 수집</li> </ul>
트래픽 메트릭스	<ul style="list-style-type: none"> <li>데이터 링크 계층, 즉 MAC 어드레스를 기준으로 두 호스트간에 발생한 트래픽 및 오류에 대한 정보를 수집</li> <li>이 정보를 이용해서 특정 호스트에 가장 많은 이용자가 누구인지를 어느 정도는 판별 가능함</li> <li>다른 세그먼트에 있는 호스트가 가장 많이 이용했다면 이것은 주로 라우터를 통과함으로써 실제 이용자는 알 수 없음.</li> </ul>
필터	<ul style="list-style-type: none"> <li>관리자가 특정한 패킷의 동향을 감시하기 위해서 이용</li> </ul>
패킷 수집	<ul style="list-style-type: none"> <li>세그먼트에 발생한 패킷을 수집해서 관리자가 분석.</li> </ul>
사건	<ul style="list-style-type: none"> <li>특정한 사건이 발생하면 그 기록을 보관하고 관리자에게 경고 메시지를 전송. 트랩 발생 및 기록보관은 선택적임.</li> </ul>

## 12.4.2. RMON의 Alarm과 Event 그룹 설정.

사용자는 CLI 또는 SNMP 관리자에 의해서 RMON을 설정할 수 있다.

표 12-10. RMON Alarm and Event 설정 명령

명령어	설명	모드
<code>rmon alarm index variable interval seconds {absolute   delta} rising-threshold value event num falling-threshold value event num [owner string]</code>	RMON alarm을 추가한다. <ul style="list-style-type: none"> <li><b>Index:</b> Alarm 인덱스</li> <li><b>Variable:</b> Alarm 발생 대상으로 SNMP mib 인스턴스를 지정</li> <li><b>Interval:</b> 샘플링 시간 간격 (단위: 초).</li> <li><b>Absolute:</b> 샘플링 되는 alarm value에 대해 절대값을 관찰하도록 설정</li> <li><b>Delta:</b> 샘플링 되는 alarm value에 대해 현재 값과 이전 값의 차이를 관찰하도록 설정</li> <li><b>Rising-threshold, falling-threshold value:</b> alarm을 발생시킬 설정 값</li> <li><b>event:</b> Delta나 absolute로 샘플링 되는 alarm value가 rising-threshold 또는 falling - threshold 값에 도달했을 때 각각 해당 Event가 발생하도록 설정</li> <li><b>owner:</b> Alarm의 owner를 등록</li> </ul>	Config
<code>rmon event index</code>	RMON event를 추가한다.	Config



[log]	■ <i>Index</i> : Event 인덱스	
[trap <i>community</i> ]	■ log: Event 가 발생한 경우 log 를 생성하도록 설정	
[description <i>string</i> ]	■ trap: Event 가 발생한 경우 설정한 <i>community</i> 와 함께 trap 을 전송하도록 설정	
[owner <i>string</i> ]	■ owner: Event 의 owner 를 등록	
	■ description: Event 에 대한 설명을 등록	
no rmon alarm <i>alarm-index</i>	설정된 RMON alarm 설정을 삭제한다.	Config
no rmon event <i>event-index</i>	설정된 RMON event 설정을 삭제한다	Config
show rmon alarms	RMON alarm 정보 출력한다.	Privileged
show rmon events	RMON event 정보 출력한다.	Privileged

아래 예제는 GigabitEthernet 2/2 에 대해 rmon alarm 을 설정하였다. GigabitEthernet 2/2 의 inOctets 값을 30 초마다 샘플링하며 rising-threshold 및 falling-threshold 를 벗어나면 각 설정된 event 를 발생 시키도록 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
Switch(config-if-Giga2/2)# 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 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. ■ <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 수집한다. ■ <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 않도록 설정한다.	Interface
no rmon collection history <i>index</i>	물리적 인터페이스의 이력을 수집하지 않도록 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 초기화한다.	Interface

아래 예제는 GigabitEthernet 2/2에 대해 10초마다 최대 30개의 bucket을 이용해 RMON 이력을 수

집하도록 설정한다.

---

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet 2/2
Switch(config-if-Giga2/2)# rmon collection stats 1
Switch(config-if-Giga2/2)# rmon collection history 1 buckets 30
interval 10
Switch(config-if-Giga2/2)# 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

U9200 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.

U9200 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 메시

지를 시스템 버퍼에 저장한다. 시스템 운영자는 시스템 메시지를 **Telnet** 이나 콘솔을 통해서, 또는 **syslog server** 의 로그를 봄으로써 원격으로 모니터 할 수 있다.

U9200 Series 스위치는 0-7 까지의 **Severity** 레벨을 가지고 있다.

표 12-12. U9200 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

U9200 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 U9200 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
<code>logging console {&lt;0-7&gt;  alerts critical debugging emergencies errors  informations notifications warnings}</code>	콘솔로의 로깅 출력 여부 설정 및 환경 설정.
<code>logging facility {auth cron daemon kernel local0  local1 local2 local3 local4 local5  local6 local7 lpr mail news syslog  user uucp}</code>	syslog 메시지를 보낼 Facility parameter 를 설정.
<code>logging A.B.C.D</code>	syslog 메시지를 외부 syslog 서버 에 보낼지 설정
<code>logging monitor  alerts critical debugging emergencies errors  informations notifications warnings}</code>	현 세션으로의 로깅 출력 여부 설 정.
<code>logging source-ip A.B.C.D</code>	syslog packet 의 source ip 를 설정
<code>logging trap  alerts critical debugging emergencies errors  informations notifications warnings}</code>	syslog server 의 logging level 설정
<code>show logging</code>	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 다

음과 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.

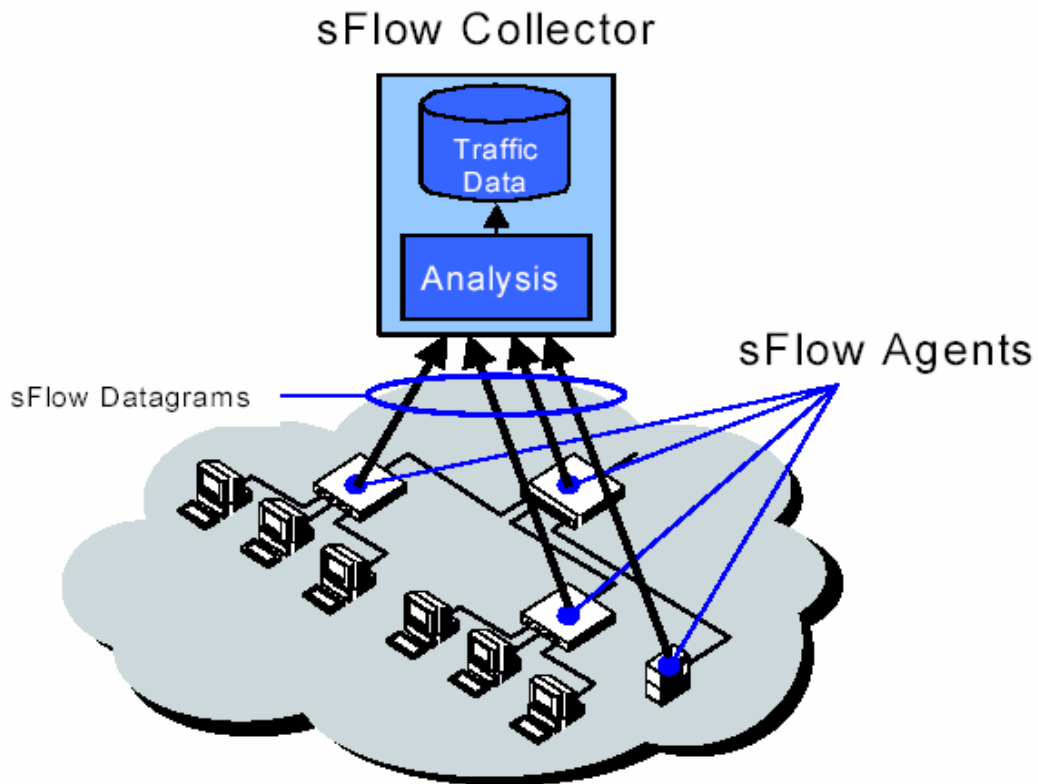
```
Switch#
Switch# configure terminal
Switch(config)# logging monitor warnings
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# no logging session
Switch(config)#
```

Log server 100.10.1.1 에 이 switch 에서 발생하는 log 중 Log level err(5) 이하의 log message 를 보내 고자 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)#
```

## 12.6. sFlow

본 U9200 Series 스위치에서는 각 interface 의 Traffic flow 별 모니터링과 statistics 에 대한 정보를 수집하기 위해 sFlow 를 지원한다. U9200 Series 에서 sFlow 를 지원하는 interface 의 범위는 physical port 에 한한다. sFlow 는 switch 또는 router 에 있는 상태 및 통계 정보를 수집해 주는 sFlow agent 와 이 정보를 sorting 하여 운영자에게 보여주는 sFlow collector 가 있다. 아래는 sFlow 개념에 대해 설명한 그림이다.



■ 그림 2. sFlow 개념도(sFlow agent 와 collector)

### 12.6.1. sFlow agent

여기서는 sFlow agent 와 관련된 기능 및 명령어에 대해서 소개한다. 이와 관련된 명령어는 크게 agent 및 collector IP 설정, flow sampling rate, counter(statistics) polling interval, sflow forward, service sflow 로 나뉜다. Agent IP 는 sFlow collector 로 샘플링 정보를 보낼 때 샘플링 패킷에 삽입되며, sFlow collector 는 샘플링 패킷에 삽입된 Agent IP 를 지정해야 한다. sFlow 는 패킷 기반의 Flow sampling 과 시간 기반의 counter(statistics) sampling 으로 나뉜다. flow sampling rate 는 Interface 에 통과하는 패킷 중, 몇 번째 패킷마다 패킷을 샘플링 할지 결정하며, counter polling interval 은 Interface statistics 를 몇 초마다 sampling 할지 결정한다. sflow forward 라는 명령어으로써 sampling 할 물리적 인터페이스(ex, gi1)를 결정하며 최대 4 개의 인터페이스를 설정할 수 있다. service sflow 라는 명령어으로써 sflow service 를 시작하게 된다.

표 33. sFlow 관련 명령어

명령어	설명	모드
<b>show sflow</b>	sflow 설정과 관련된 명령어를 보여준다	Privileged
<b>service sflow</b>	sampling 이 enable 된 interface 의 flow sampling 및 statistics sampling 을 시작하게 된다. Disable 은 no 형태를 취한다.	Config
<b>sflow forwarding</b>	해당 interface 를 통과하는 패킷에 대해서 sampling 을 할 것인지 설정한다. Disable 은 no 형태를 취한다.	Interface

<b>sflow sample</b> <10-65530>	Interface 를 통과하는 패킷 중 몇 패킷마다 을 sampling 을 취할지를 설정한다. no 형태로 Default 값을 취한다.	Interfac, Config
<b>sflow polling-interval</b> <20-120>	몇 초마다 statistics sample 을 sampling 할지 결정한다.	Config
<b>sflow agent</b> A.B.C.D	sflow agent 의 ip address 를 설정한다. No 형태로 Default 값을 취한다	Config
<b>sflow destination</b> A.B.C.D	sflow collector 의 ip address 를 설정한다. No 형태로 Default 값을 취한다	Config

## 12.6.2. sFlow collector

여기서는 sFlow collector 와 관련된 기능 및 설정에 대해서 소개 한다. sFlow collector 는 switch 또는 router 와 별개로 Linux 및 Window 시스템에 설치되어 sFlow Agent 가 송신한 sampling 패킷을 분석 후, 통계 수치를 운영자에게 보여준다. sFlow collector 에는 sampling 패킷의 통계값을 텍스트 형태로 보여주는 sflowtool 과 그래픽 형태로 보여주는 sFlowTrend, Inmon Traffic Server 등이 있다. 이 중 공개 버전인 sflowtool 과 sFlowTrend 는 Inmon corporation 홈페이지 <http://www.inmon.com/index.htm> 에서 무료로 다운 받을 수 있다. 다음은 sflowtool 과 sFlowTrend 설정에 대한 설명이다.

### 12.6.2.1. sflowtool 설정

1) port 6343으로 수신된 sFlow sampling packet을 출력한다.

```
[Ins:/home/Ins] sflowtool -p 6343
startDatagram =====
datagramSourceIP 192.168.0.212
datagramSize 144
unixSecondsUTC 1136381882
datagramVersion 5
agentSubId 0
agent 192.168.0.212
packetSequenceNo 9512
sysUpTime 190157000
samplesInPacket 1
startSample -----
sampleType_tag 0:2
sampleType COUNTERSSAMPLE
.....
endSample -----
endDatagram =====
```



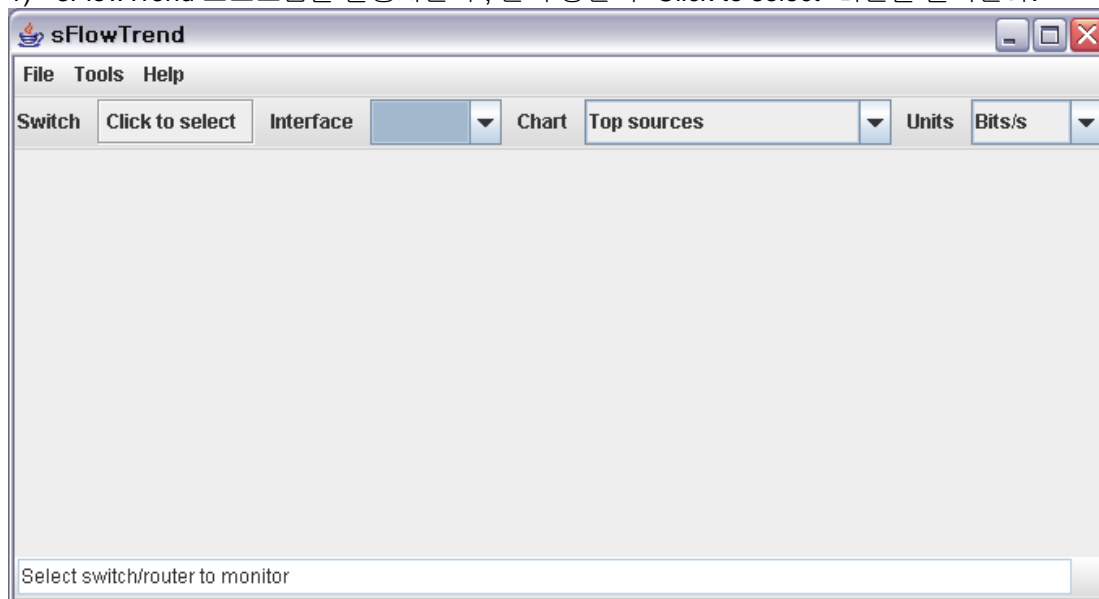
2) sFlow sampling packet을 line 단위로 출력한다.

[Ins:/home/Ins] **sflowtool -l**

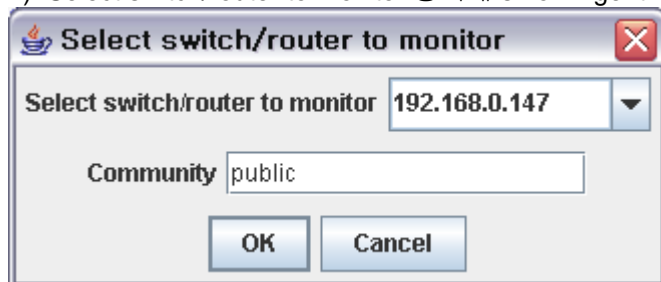
```
CNTR,10.0.0.254,17,6,100000000,0,2147483648,175283006,136405187,2578019,297011,0,3,0,0,0,
0,0
,0,0,1
FLOW,10.0.0.254,0,0,00902773db08,001083265e00,0x0800,0,0,10.0.0.1,10.0.0.254,17,0x00,64,356
9
0,161,0x00,143,125,80
```

### 12.6.2.2. sFlowTrend 설정

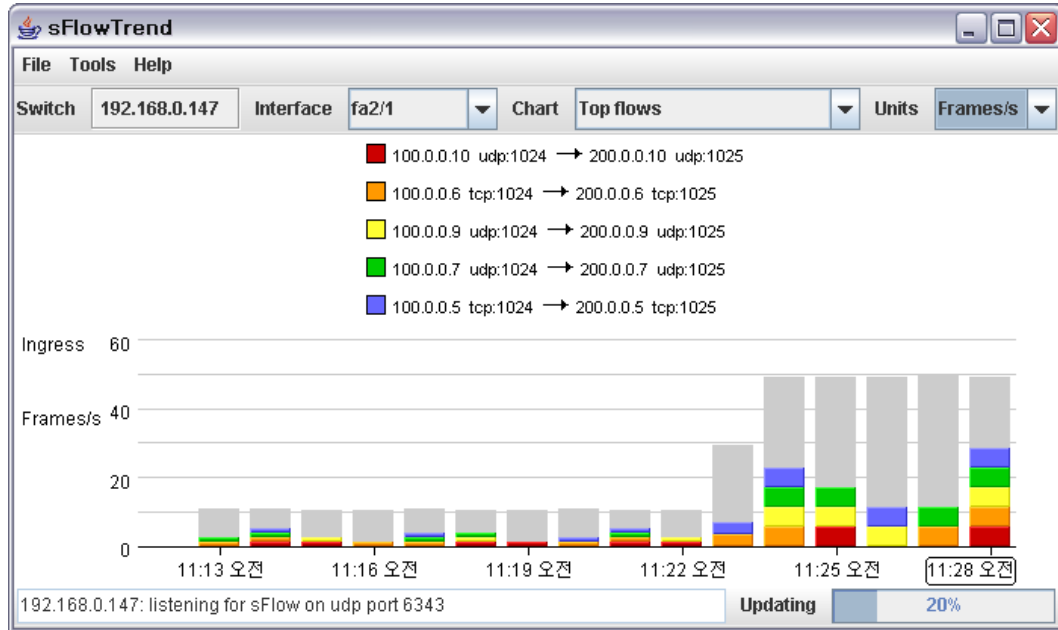
1) sFlowTrend 프로그램을 실행시킨 후, 왼쪽 상단의 “Click to select” 버튼을 클릭한다.



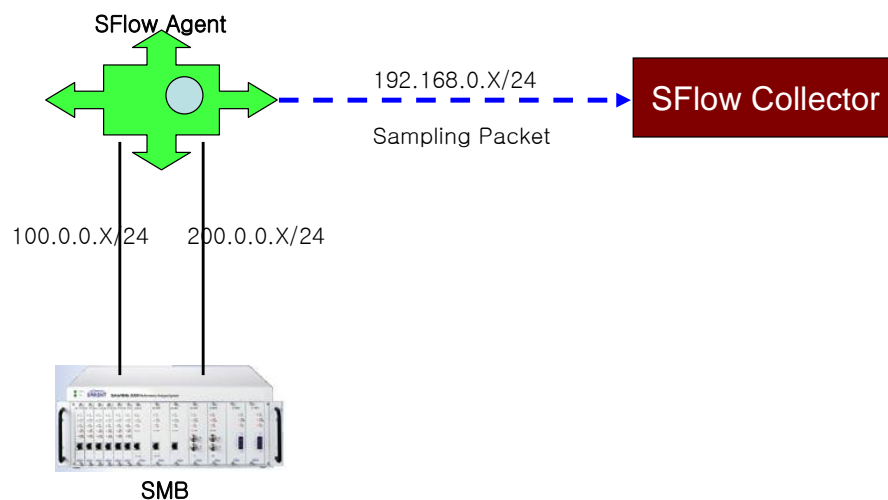
2) Select switch/router to monitor 항목에 sFlow Agent의 IP Address를 입력한다.



3) sFlowTrend가 sampling 정보를 얻어오면 Interface, Chart(Utilization, Counters, Top flows . . .), Units 항목에서 운영자가 확인하고자 하는 항목을 선택한다.



### 12.6.3. sFlow Network 구성



■ 그림 3. sFlow 를 설정한 네트워크 예제 설정 및 구성도

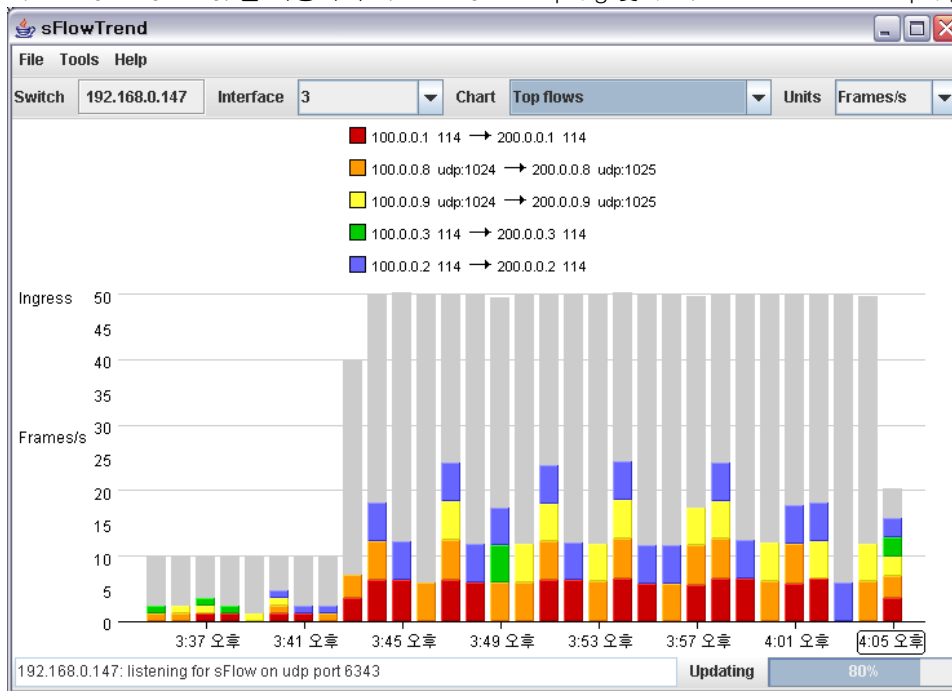
#### 12.6.3.1. sFlow sampling 시험

sFlow sampling 에는 트랙픽 flow sampling 과 Interface statistics sampling 이 있다. 위의 그림에서 설정한 sFlow 네트워크 구성도에서 sFlow collector 를 통하여 sampling 결과를 확인한다.

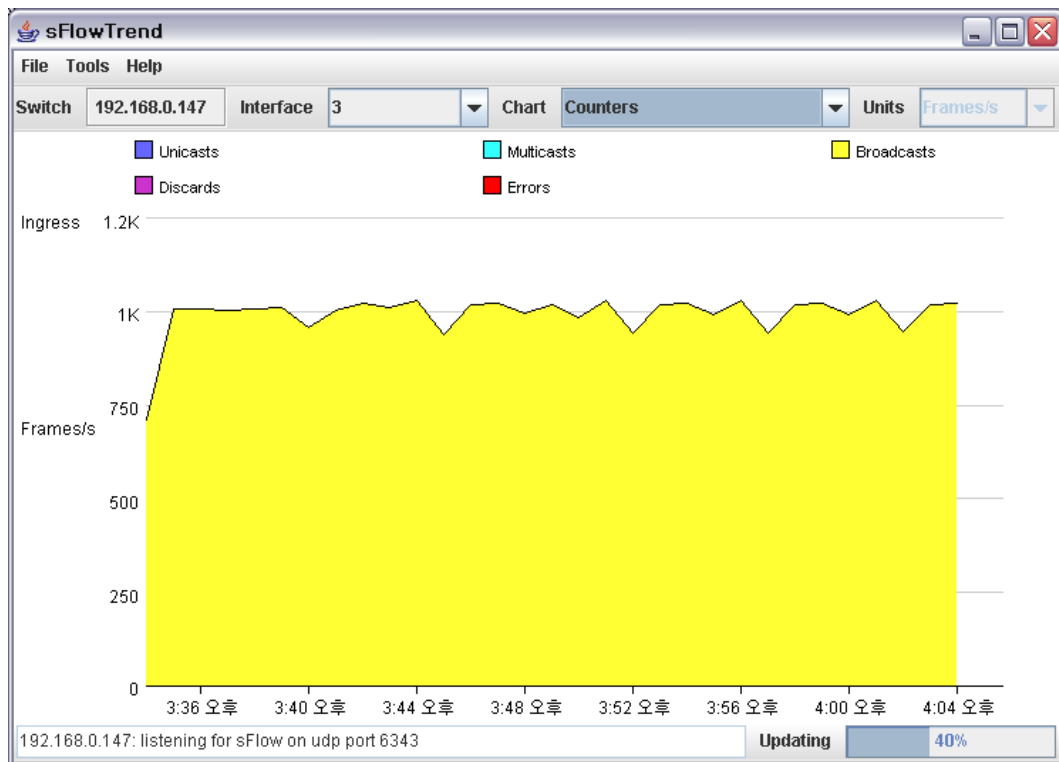
1. SMB 를 사용하여 다양한 flow(TCP, UDP, IP, 여러개의 IP Address)별 트래픽을 생성하여, Sflow Agent 에게 송신한다.
2. Sflow Agent 에서 SMB 와 연결된 포트의 트래픽을 샘플링하고, 이 트래픽을 SFlow Collector 에게 전송하기 위하여 SFlow Collector 와 SFlow Agent 의 IP Address 를 설정한다. SFlow Service 를 활성화 시킨다.

```
Switch(config)# interface gi1
Switch(config-if-Giga5/1)# sflow forwarding
Switch(config-if-Giga5/1)# exit
Switch(config)# sflow agent 192.168.0.147
Switch(config)# sflow destination 192.168.0.200
Switch(config)# service sflow
```

3. SFlow Collector 을 사용하여 Traffic flow sampling 및 Interface statistics sampling 을 확인한다.



※ Traffic flow sampling



※ Interface statistics sampling

## 13

## STP(Spanning Tree Protocol) & SLD(Self-loop Detection)

이 장에서는 Spanning Tree Protocol(STP)과 Rapid Spanning Tree Protocol(RSTP), Multiple Spanning Tree(MSTP)를 설정하는 방법과 Bridge 에서의 프레임 전송에 대해 설명한다.

**Notice**

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
- 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 BPDU 를 전송한다. 스위치들은 BPDU 를 서로 교환하고 BPDU 로 spanning-tree 형상을 계산한다. 각 configuration BPDU 는 다음의 정보를 포함한다:

- root 스위치의 BridgeID
- root 까지의 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 가

진 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	Bit4	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.

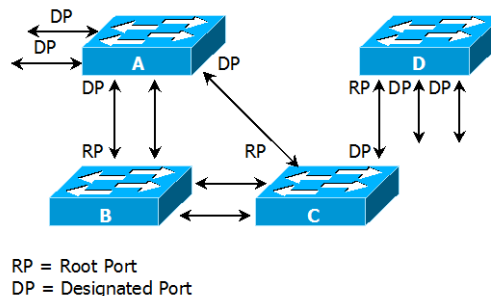


그림 13-1. Spanning-Tree Topology

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 forwarding하지 않는다.
- Listening - 인터페이스가 프레임을 forwarding해야 한다고 결정되었을 때, blocking state

다음의 천이 상태.

- Learning - 인터페이스가 프레임을 forwarding하기 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.

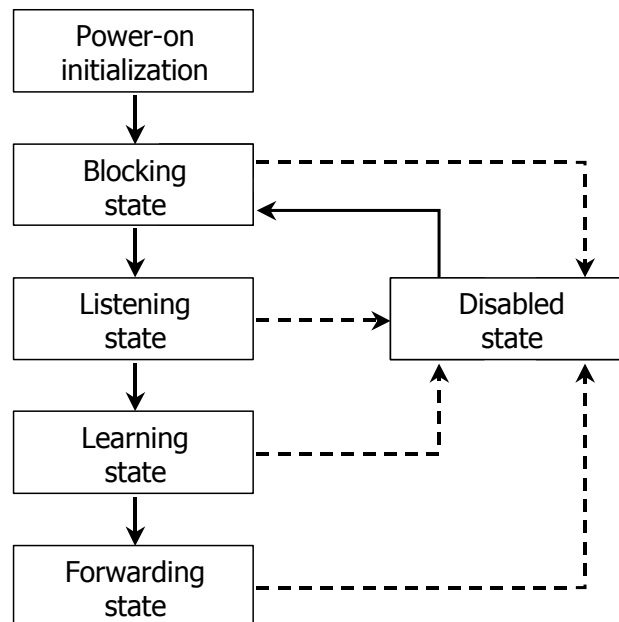


그림 13-2. Spanning-Tree Interface States

STP가 활성화 되었을 때, 스위치의 모든 인터페이스는 blocking 상태가 되고 listening과 learning의 일시적인 상태를 지난다. 안정화된 spanning tree에서 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 중단 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 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 동작하는지를 설명한다:

- RSTP Overview
- Port Roles and the Active Topology
- Rapid Convergence
- Bridge Protocol Data Unit Format and Processing

### 13.2.1. 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.

### 13.2.2. 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 forward할 때 최적의 경로(가장 낮은 cost)를 제공한다.
- Designated port – designated 스위치와 연결되어, LAN에서 root 스위치로 패킷을 forward할 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 role을 가진 안정된 형상에서, RSTP는 모든 root 포트와 designated 포트가 바로 forwarding 상태로 천이하는 것을 보장한다. 반면 모든 alternate 포트와 backup 포트는

항상 discarding 상태(802.1D의 blocking과 동등한 상태)에 놓인다. 포트의 상태는 forwarding과 learning 과정의 동작을 제어한다. 다음의 표는 802.1D와 RSTP의 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 port는 listening 상태에서 시작한다.

### 13.2.3. Rapid Convergence

RSTP는 다음과 같은 스위치, 포트 혹은 LAN의 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 A는 스위치 B와 point-to-point 링크로 연결되어 있고 모든 포트는 blocking 상태이다. 스위치 A의 priority가 스위치 B의 priority보다 낮은 수의 값을 가진다고 가정하자. 스위치 A는 proposal 메시지(proposal flag가 설정된 BPDU)를 스위치 B로 전송하고 자신을 designated 스위치로 제안한다.

스위치 B는 proposal 메시지를 수신한 후에, proposal 메시지를 수신한 포트를 새로운 root 포트에 선택하고, 모든 non-edge 포트를 blocking 상태로 설정하고, agreement 메시지(agreement flag를 설정한 BPDU)를 새로운 root 포트를 통해 전송한다.

스위치 B의 agreement 메시지를 수신한 후에, 스위치 A는 자신의 designated 포트를 forwarding 상태로 천이한다. 스위치 B가 자신의 모든 non-edge port를 block시키고, 스위치 A와 스위치 B 사이는 point-to-point 링크로 연결되었기 때문에 네트워크에 루프가 발생하지 않는다.

스위치 C가 스위치 B와 연결될 때, 유사한 협상 메시지가 교환된다. 스위치 C는 스위치 B와 연결된 포트를 root 포트에 선택하고, 두 스위치의 두 포트는 forwarding 상태로 천이한다.

다. 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.

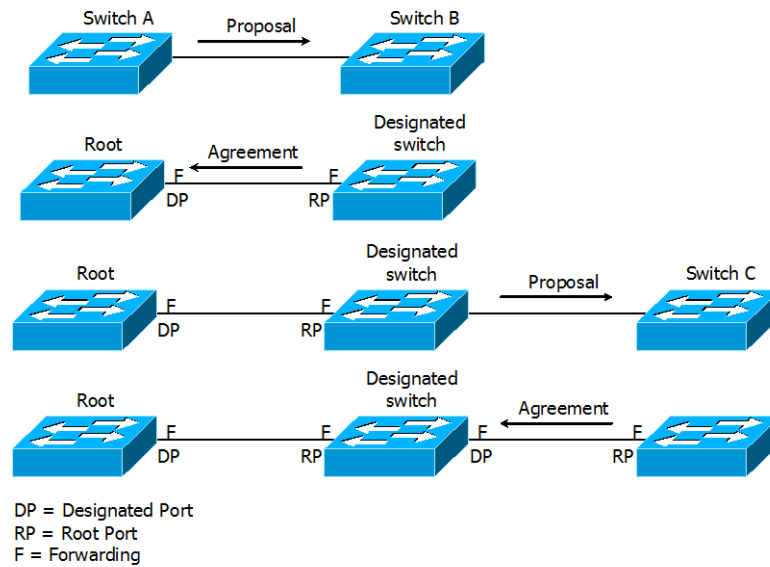


그림 13-3. Proposal and Agreement Handshaking for Rapid Convergence

#### 13.2.4. 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 13-4. 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 밑의 그림에서 나타내듯 로드 밸런싱 시킬 수 있는 경로 수만큼의 스페닝 트리만 필요하기 때문이다.



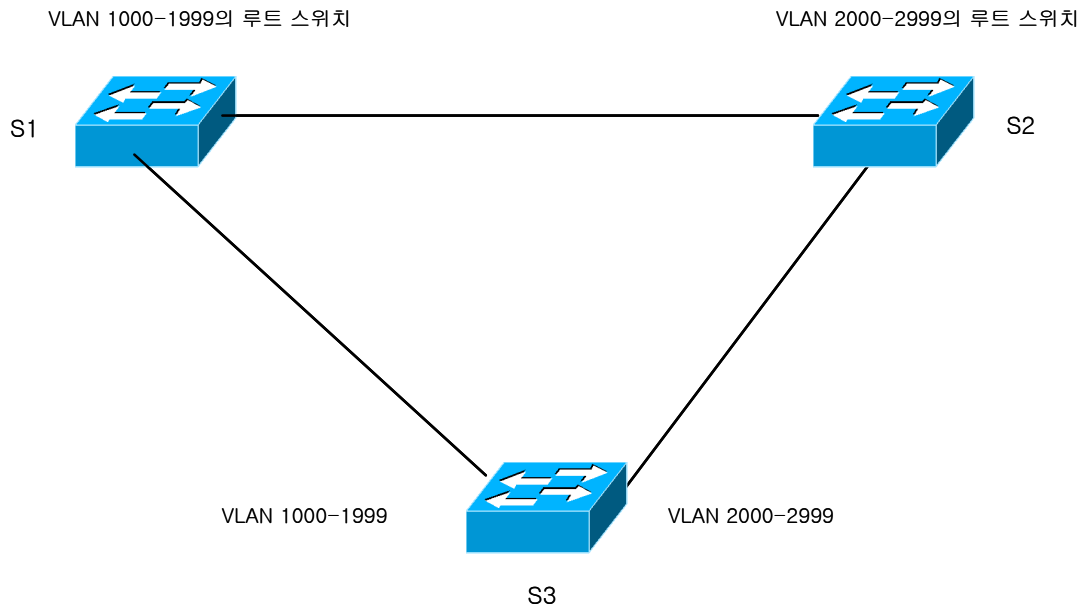


그림 13-4. VLAN 에 대한 load balance

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.

### 13.3.1. 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.

### 13.3.2. 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

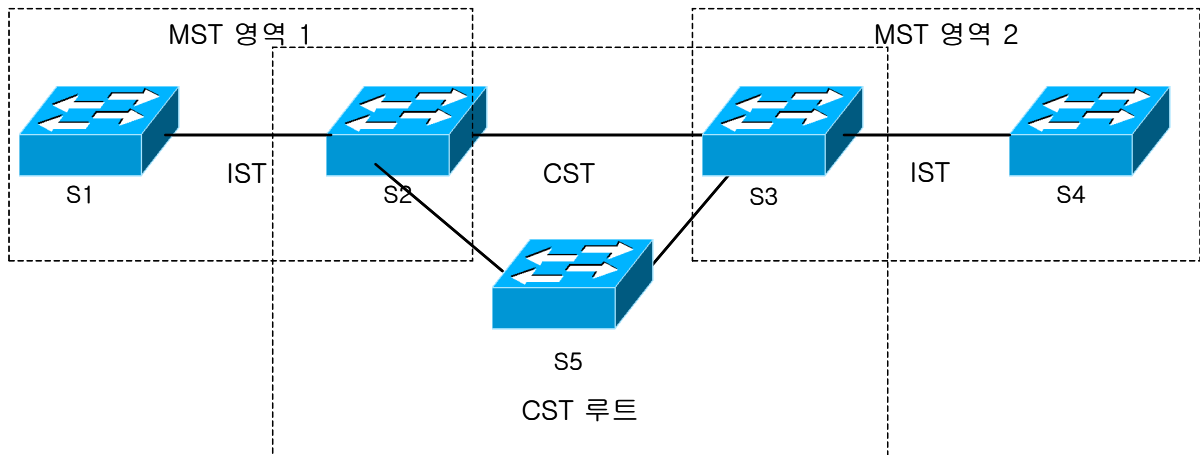


그림 13-5. CST, IST, CIST

MST 영역이 다르면 IST 도 서로 별개로 동작한다. 서로 다른 MST 영역 사이에는 IST 가 아닌 CST 가 동작한다. 따라서 그림에서 스위치 S1, S2 의 MST 영역이 스위치 S3, S4 와 서로 다르므로 각각의 MST 영역에서 동작하는 IST 는 별개로 동작하며, 두 영역을 연결하는 스위치 S2 와 S3 사이에는 CST 가 동작한다. 각 MST 영역내에서 CST 루트 스위치까지의 경로값, 브리지 ID, 포트 ID 값이 가장 작은 스위치를 IST master 라고 한다. 위의 그림처럼 S5 가 CST 루트 스위치라면 S2 와 S3 이 각각의 MST 영역에서 IST master 스위치로 동작한다. CST 루트 스위치가 MST 영역 밖에 있다면, IST 마스터는 항상 CST 와 MST 의 경계상에 있게 된다. 만약 스위치 네트워크가 하나의 MST 영역으로 구성된 경우에는 동일한 스위치가 CST 루트와 IST 마스터로 동작한다. CST 는 서로 다른 MST 영역간 뿐만 아니라 802.1D 로 동작하는 스위치 사이 또는 MST 와 802.1D 스위치 사이에서도 동작한다. CST 의 관점에서 하나의 MST 영역 전체를 하나의 스위치로 간주한다. 따라서 위와 같은 네트워크를 CST 에서는 다음 그림과 같이 인식한다.

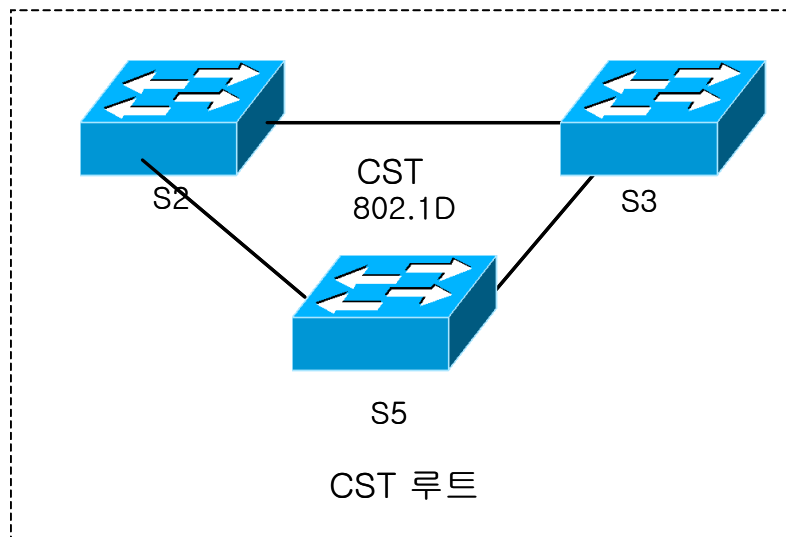


그림 13-6. CST 에서 인식하는 네트워크

## 13.4. 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 의 경우 다른 설정방법을 갖는다.

### 13.4.1. Default STP Configuration

다음의 표는 STP 의 default 설정을 보여준다.

표 13-5. Default STP Configuration

Feature	Default Setting
Enable state	모든 bridge 에 대해 비활성 되어 있음. 기본적으로 RSTP 모드가 설정되어 있는 상황에서 disable 로 되어있어서 enable 시킬 경우 RSTP 가 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.

### 13.4.2. STP Configuration Guidelines

U9264 Series 는 PVST 를 지원하지 않는다. 그래서 Bridge 에 1 개의 spanning-tree 가 구동되고 여기에 붙어 있는 VLAN 은 어떠한 영향을 미치지 않는다. 대신에 bridge 마다 spanning-tree 를 구동할 수 있고 bridge 는 256 개까지 생성 가능하다. VLAN 은 1 개의 Bridge 에만 속할 수 있고 trunk VLAN 의 경우는 default Bridge 에만 속하게 되어있다. Trunk VLAN 에서 spanning-tree 를 구동 할 경우 전체 VLAN 에 1 개의 spanning-tree 가 구동되도록 한다.

### 13.4.3. Enabling STP

U9264 Series 에서 처음에 STP 는 동작하지 않는다. 네트워크에 루프가 존재할 가능성이 있다면 STP 를 활성화 시키도록 한다. STP 를 활성화 시키면 기본적으로 RSTP 가 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	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>spanning-tree enable</b>	Default Bridge 에 대해 STP 를 구동한다
Step3	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step4	<b>show spanning-tree</b>	설정 내용을 확인한다.
Step5	<b>copy running-config startup-config</b>	(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)# exit
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 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority   32768
    Address   00077074ff01
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
    Aging Time 300

Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga5/3/2   Disb BLK 4      128.610 Shared

Switch#
Switch# configure terminal
```

```
Switch(config)# spanning-tree shutdown bridge-forward
Switch(config)# exit
Switch# show spanning-tree
Spanning tree instance(s) does not exist

Switch#
```

### 13.4.4. Enable STP in not default Bridge

U9264 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.



#### Notice

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 <1-255> protocol vlan-bridge	Bridge 를 생성한다.
Step3	bridge <1-255> spanning-tree enable	Bridge 의 STP 를 enable 한다.
Step4	Bridge-group <1-255>	Vlan 을 Bridge 에 포함시킨다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

Default Bridge 이외의 Bridge 의 STP 기능을 비활성화 하려면, global configuration 명령 **bridge shutdown <1-255> bridge-forward** 명령을 사용하라. Bridge 를 삭제 하기 위해서는 **no bridge <1-255>** 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)# exit
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)# exit
Switch# show running-config
!
!
Switch#
```

### 13.4.5. 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)을 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	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>interface</b> <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹이다.
Step3	<b>spanning-tree</b> <b>port-priority</b> <i>priority</i>	인터페이스의 포트 priority 를 설정한다. <ul style="list-style-type: none"> <li><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.</li> </ul>

Step4	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step5	<b>show spanning-tree</b>	설정 내용을 확인한다.
Step6	<b>copy running-config startup-config</b>	(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 <1-255>** 을 사용한다.

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 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
-----		
Giga5/3	Disb BLK 4	128.138 Shared
Switch # configure terminal		
Switch(config)#int GigabitEthernet 5/3		
Switch(config-if-Giga5/3)# <b>spanning-tree port-priority 0</b>		
Switch(config-if-Giga5/3)#exit		
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 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
-----		
Giga5/3	Disb BLK 4	0.138 Shared
Switch#configure terminal		
Switch(config)#interface GigabitEthernet 5/3		
Switch(config-if-Giga5/3)# <b>no spanning-tree port-priority</b>		
Switch(config-if-Giga5/3)#exit		

```
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 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768
Address 00077074ff01
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
-----
Giga5/3 Disb BLK 4 128.138 Shared

Switch#
```

### 13.4.6. 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.



**Notice** 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	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>interface</b> <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹이다.
Step3	<b>spanning-tree path-cost</b> <i>cost</i>	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. ● <i>cost</i> 의 범위는 1~200000000 이다. default 값은 인터페이스의 전송속도로부터 결정된다.
Step4	<b>exit</b>	privileged EXEC 모드로 변경한다.



Step5	<b>show spanning-tree</b>	설정 내용을 확인한다.
Step6	<b>copy running-config startup-config</b>	(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 <1-255>** 을 사용한다.

```
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 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
-----
Giga5/3    Disb BLK 4      128.138 Shared

Switch#configure terminal

Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#spanning-tree path-cost 10
Switch(config-if-Giga5/3)#exit
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 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
-----
Giga5/3    Disb BLK 10      128.138 Shared

Switch#configure terminal

Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#no spanning-tree path-cost
Switch(config-if-Giga5/3)#exit
```

```
Switch#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 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority   32768
        Address    00077074ff01
        Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
        Aging Time 300

Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga5/3     Disb BLK 4      128.138 Shared

Switch#
```

### 13.4.7. 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	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>spanning-tree priority <i>priority</i></b>	<ul style="list-style-type: none"> <li><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.</li> </ul>
Step3	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step4	<b>show spanning</b>	설정 내용을 확인한다.
Step5	<b>copy running-config startup-config</b>	(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 <1-255>** 을 사용한다.

```
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 2 sec Max Age 20 sec Forward 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
Giga5/3	Disb	BLK	4	128.138	Shared

```
Switch#
Switch#configure terminal
```

```
Switch(config)#spanning-tree priority 4096
Switch(config)#exit
Switch#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 2 sec Max Age 20 sec Foward Delay 15 sec
```

```
Bridge ID Priority 4096
Address 00077074ff01
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Giga5/3	Disb	BLK	4	128.138	Shared

```
Switch#conf t
```

```
Switch(config)#no spanning-tree priority
Switch(config)#exit
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 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
Giga5/3	Disb	BLK	4	128.138	Shared

Switch#

### 13.4.8. 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	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>spanning-tree hello-time</b> <i>seconds</i>	hello time 은 root 스위치가 configuration 메시지를 전송하는 주기이다. 이 메시지는 스위치가 살아있음을 의미한다. • <i>seconds</i> 의 범위는 1~10 이다. default 는 2 이다.
Step3	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step4	<b>show spanning-tree</b>	설정 내용을 확인한다.
Step5	<b>copy running-config startup-config</b>	(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 <1-255>** 을 사용한다.

```
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 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority   32768
Address   00077074ff01
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga5/3    Disb BLK 4      128.138 Shared

Switch#
Switch#configure terminal

Switch(config)#spanning-tree hello-time 9
Switch(config)#exit
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 9 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32768
Address 00077074ff01
Hello Time 9 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
Giga5/3 Disb BLK 4 128.138 Shared
```

```
Switch#configure terminal
```

```
Switch(config)#no spanning-tree hello-time
Switch(config)#exit
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 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32768
Address 00077074ff01
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
Giga5/3 Disb BLK 4 128.138 Shared
```

```
Switch#
```

### 13.4.9. Configuring the Forwarding-Delay Time for a VLAN

VLAN 의 forwarding-delay time 을 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>spanning-tree forward-time seconds</b>	forward delay 는 포트가 spanning-tree 의 listening 혹은 learning 상태에서 forwarding 상태로 천이하기 위해 기다리는 시간이다. ● seconds 의 범위는 4~30 이다. default는 15 이다.
Step3	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step4	<b>show spanning-tree</b>	설정 내용을 확인한다.
Step5	<b>copy running-config startup-config</b>	(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 <1-255>** 을 사용한다.

```
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 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority   32768
Address   00077074ff01
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

```
Interface   Role Sts Cost    Prio.Nbr Type
-----
```

```
Giga5/3    Disb BLK 4      128.138 Shared
```

```
Switch#configure terminal
```

```
Switch(config)#spanning-tree forward-time 20
```

```
Switch(config)#exit
```

```
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 2 sec Max Age 20 sec Forward Delay 20 sec
```

```
Bridge ID Priority   32768
Address   00077074ff01
Hello Time 2 sec Max Age 20 sec Forward Delay 20 sec
Aging Time 300
```

```
Interface   Role Sts Cost    Prio.Nbr Type
-----
```

```
Giga5/3    Disb BLK 4      128.138 Shared
```

```
Switch#configure terminal
```

```
Switch(config)#no spanning-tree forward-time
```

```
Switch(config)#exit
```

```
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 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
Giga5/3	Disb	BLK	4	128.138	Shared

Switch#



### 13.4.10. Configuring the Maximum-Aging Time for a VLAN

maximum-aging time 을 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>spanning-tree max-age</b> <i>seconds</i>	maximum-aging time 을 설정한다. maximum-aging time 은 스위치가 재구성을 하기 전에 spanning-tree 정보를 수신하지 않고 기다리는 최대 시간이다. ● <i>seconds</i> 의 범위는 6~40 이다. default는 20 이다.
Step3	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step4	<b>show spanning-tree</b>	설정 내용을 확인한다.
Step5	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

스위치의 default 설정으로 복구하려면, global configuration 명령 **no spanning-tree max-age** 명령을 사용하라. Default Bridge가 아닌 경우에는 spanning-tree 대신 **bridge <1-255>** 을 사용한다.

```
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 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32768
```

```
Address 00077074ff01
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----
```

```
Giga5/3 Disb BLK 4 128.138 Shared
```

```
Switch#configure terminal
```

```
Switch(config)#spanning-tree max-age 15
```

```
Switch(config)#exit
```

```
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 2 sec Max Age 15 sec Forward 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
-----
Giga5/3     Disb BLK 4      128.138 Shared

Switch#configure terminal

Switch(config)#no spanning-tree max-age
Switch(config)#exit
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 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
-----
Giga5/3     Disb BLK 4      128.138 Shared

Switch#

```

### 13.4.11. Changing the Max-hops for switch

MSTP mode 는 max age 와 forward delay 를 사용하는 대신 IP 의 TTL 과 같은 역할을 하는 hop count 를 이용한다.

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>Spanning-tree max-hops <i>count</i></b>	스위치의 max-hop 을 변경한다.
Step3	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step4	<b>show running-config</b>	설정 내용을 확인한다.
Step5	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

```

Switch(config)#spanning-tree max-hops 10
Switch(config)#do show spa mst
#### MST1    vlans mapped:20,70
Bridge      address 0007.70de.ad99 priority    32768 (32768 sysid 0)

```

```

Root      address 0007.709e.12fd priority    8000 (8000 sysid 0)
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 10
Interface      Role  Sts Cost    Prio.Nbr Type
-----
-----

Giga5/3      Mstr   FWD 20000   128.138 P2p
Giga5/4      Altn   BLK 20000   128.139 P2p

Switch(config)#no spanning-tree max-hops
Switch(config)#do show spa mst
#### MST1   vlans mapped:20,70
Bridge      address 0007.70de.ad99 priority    32768 (32768 sysid 0)
Root      address 0007.709e.12fd priority    8000 (8000 sysid 0)
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
-----
-----

Giga5/3      Mstr   FWD 20000   128.138 P2p
Giga5/4      Altn   BLK 20000   128.139 P2p

```

### 13.4.12. Changing the Spanning-Tree mode for switch

U9264 Series 는 STP, RSTP, MSTP 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

Step1	Command	Purpose
	configure terminal	Global configuration 모드로 진입한다.

Step2	<code>spanning-tree mode {stp rstp mstp  provider-mstp provider-rstp  stp-vlan-bridge rstp-vlan-bridge}</code>	스위치의 spanning-tree 모드를 변경한다.
Step3	<code>exit</code>	privileged EXEC 모드로 변경한다.
Step4	<code>show running-config</code>	설정 내용을 확인한다.
Step5	<code>copy running-config startup-config</code>	(옵션) 설정을 configuration 파일에 저장한다.

```
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 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority   32768
Address   00077074ff01
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

```
Interface   Role Sts Cost      Prio.Nbr Type
-----
Giga5/3     Disb BLK 4       128.138 Shared
```

```
Switch#configure terminal
```

```
Switch(config)#spanning-tree mode stp-vlan-bridge
```

```
Switch(config)#exit
```

```
Switch(config)#spanning-tree enable
```

```
Switch(config)#exit
```

```
Switch#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 Forward Delay 15 sec
```

```
Bridge ID Priority   32768
Address   00077074ff01
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

```
Interface   Role Sts Cost      Prio.Nbr Type
-----
Giga5/3     Disb DIS 4       128.138 Shared
```

```
Switch#configure terminal
```

```
Switch(config)#spanning-tree mode mstp
```

```
Switch(config)#spanning-tree enable
Switch(config)#exit
Switch#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 Forward Delay 15 sec

Bridge ID Priority   32768
Address   00077074ff01
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga5/3     Disb BLK 20000   128.138 Shared
```

### 13.4.13. Configuring portfast for switch

Switch 의 모든 port 들에 bpdu-filter 와 bpdu-guard 를 설정할 수 있다. Bpdu-filter 는 해당 port 로 유입되는 bpdu 를 차단하는 것이고, bpdu-guard 는 해당 port 로 bpdu 유입시 port 를 block state 로 전환하는 것이다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	spanning-tree portfast {bpdu-filter bpdu-guard }	모든 port 에 portfast 설정을 적용한다.
Step3	exit	privileged EXEC 모드로 변경한다.
Step4	show running-config	설정 내용을 확인한다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

```
Switch(config)#do show spa inter gi5/3
Default: Bridge up - Spanning Tree Enabled
Default: Root Path Cost 4 - Root Port 138 - Bridge Priority 32768
Default: Forward Delay 15 - Hello Time 2 - Max Age 20
Default: Root Id 80000007709e12fd
Default: Bridge Id 8000000770dead99
Default: last topology change Tue Jan 13 23:32:51 1970
0: 2 topology change(s) - last topology change Tue Jan 13 23:32:51 1970

Default: portfast bpdu-filter disabled
```

```

Default: portfast bpdu-guard disabled
Default: portfast errdisable timeout disabled
Default: portfast errdisable timeout interval 300 sec
Giga5/3: Port 138 - Id 808a - Role Rootport - State Forwarding
Giga5/3: Designated Path Cost 0
Giga5/3: Configured Path Cost 4 - Add type Explicit ref count 1
Giga5/3: Designated Port Id 8001 - Priority 128 -
Giga5/3: Root 80000007709e12fd
Giga5/3: Designated Bridge 80000007709e12fd
Giga5/3: Message Age 0 - Max Age 20
Giga5/3: Hello Time 2 - Forward Delay 15
Giga5/3: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change timer 0
Giga5/3: forward-transitions 1
Giga5/3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
Giga5/3: No portfast configured - Current portfast off
Giga5/3: portfast bpdu-guard default - Current portfast bpdu-guard off
Giga5/3: portfast bpdu-filter default - Current portfast bpdu-filter off
Giga5/3: no root guard configured - Current root guard off
Giga5/3: Configured Link Type point-to-point - Current point-to-point

```

```
Switch(config)#spanning-tree portfast bpdu-filter
```

```
Switch(config)#do show spa inter gi5/3
```

```

Default: Bridge up - Spanning Tree Enabled
Default: Root Path Cost 4 - Root Port 138 - Bridge Priority 32768
Default: Forward Delay 15 - Hello Time 2 - Max Age 20
Default: Root Id 80000007709e12fd
Default: Bridge Id 8000000770dead99
Default: last topology change Tue Jan 13 23:32:51 1970
0: 2 topology change(s) - last topology change Tue Jan 13 23:32:51 1970

```

```
Default: portfast bpdu-filter enabled
```

```
Default: portfast bpdu-guard disabled
```

```
Default: portfast errdisable timeout disabled
```

```
Default: portfast errdisable timeout interval 300 sec
```

```

Giga5/3: Port 138 - Id 808a - Role Rootport - State Forwarding
Giga5/3: Designated Path Cost 0
Giga5/3: Configured Path Cost 4 - Add type Explicit ref count 1
Giga5/3: Designated Port Id 8001 - Priority 128 -
Giga5/3: Root 80000007709e12fd
Giga5/3: Designated Bridge 80000007709e12fd

```

```
Giga5/3: Message Age 0 - Max Age 20
Giga5/3: Hello Time 2 - Forward Delay 15
Giga5/3: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change timer 0
Giga5/3: forward-transitions 1
Giga5/3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
Giga5/3: No portfast configured - Current portfast off
Giga5/3: portfast bpdu-guard default - Current portfast bpdu-guard off
Giga5/3: portfast bpdu-filter default - Current portfast bpdu-filter on
Giga5/3: no root guard configured - Current root guard off
Giga5/3: Configured Link Type point-to-point - Current point-to-point
```



**Notice**

bpdu-guard 나 bpdu-filter 를 설정하기 전에 portfast 를 먼저 설정해야 한다.

### 13.4.14. Changing transmit-holdcount for switch

Maximum transmit rate(default : 3sec) 동안 전송할 수 있는 BPDU 의 수를 제한하는데 이 값을 transmit-holdcount 에 저장한다. (default : 6)

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>spanning-tree</b> <b>transmit-holdcount</b> <i>holdcount</i>	Transmit-holdcount 를 변경한다.
Step3	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step4	<b>show running-config</b>	설정 내용을 확인한다.
Step5	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

```
#### MST1 vlans mapped:70
Bridge address 0007.70de.ad99 priority 32768 (32768 sysid 0)
Root address 0007.709e.12fd priority 8000 (8000 sysid 0)
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
-----
Giga5/3 Mstr FWD 20000 128.138 P2p
Giga5/4 Altn BLK 20000 128.139 P2p
```

```
U9200_112(config)#no spanning-tree transmit-holdcount
U9200_112(config)#do show spa mst
#### MST1    vlans mapped:70
Bridge      address 0007.70de.ad99 priority    32768 (32768 sysid 0)
Root        address 0007.709e.12fd priority    8000 (8000 sysid 0)
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 10
Configured hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role    Sts Cost    Prio.Nbr Type
-----
Giga5/3        Mstr    FWD 20000    128.138 P2p
Giga5/4        Altn    BLK 20000    128.139 P2p
```

### 13.4.15. Changing Cisco-interoperability for switch

Cisco 에서 규정한 BPDU 는 표준 BPDU 와 specification 이 차이가 있기 때문에 그에 따른 호환성이 있어야 한다. (default : enable)

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	spanning-tree cisco-interoperability {enable disable}	cisco 와의 호환성 가능 여부를 설정한다
Step3	exit	privileged EXEC 모드로 변경한다.
Step4	show running-config	설정 내용을 확인한다.
Step5	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

### 13.4.16. Configuring autoedge for port

Port 에 연결되는 device 가 edge 인지 아닌지를 자동으로 판별하도록 설정할 수 있다.

autoedge 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 autoedge	Port에 autoedge를 설정한다.
Step3	exit	privileged EXEC 모드로 변경한다.



Step4	<code>show running-config</code>	설정 내용을 확인한다.
Step5	<code>copy running-config startup-config</code>	(옵션) 설정을 configuration 파일에 저장한다.

### 13.4.17. 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.



#### Notice

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	<code>configure terminal</code>	Global configuration 모드로 진입한다.
Step2	<code>Interface interface-id</code>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹이다.
Step2	<code>spanning-tree edgeport</code>	포트를 edge port로 설정한다.
Step3	<code>exit</code>	privileged EXEC 모드로 변경한다.
Step4	<code>show running-config</code>	설정 내용을 확인한다.
Step5	<code>copy running-config startup-config</code>	(옵션) 설정을 configuration 파일에 저장한다.

스위치의 default 설정으로 복구하려면, interface configuration 명령 `no spanning-tree edgeport` 명령을 사용하라.

```
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 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32768
```

```
Address 00077074ff01
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----
Giga5/3   Disb BLK 4       128.138 Shared
```

```
Switch#configure terminal
```

```
Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#spanning-tree edgeport
Switch(config-if-Giga5/3)#exit
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 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
-----
Giga5/3     Disb BLK 4       128.138 Shared edge port
```

```
Switch#configure terminal
```

```
Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#no spanning-tree edgeport
Switch(config-if-Giga5/3)#exit
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 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
-----
Giga5/3     Disb BLK 4       128.138 Shared
```

```
Switch#
```

### 13.4.18. 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.



#### Notice

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	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>interface</b> <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	<b>spanning-tree link-type point-to-point</b>	포트의 링크 종류를 point-to-point 로 설정한다.
Step4	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step5	<b>show running-config</b>	설정 내용을 확인한다.
Step6	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

default 설정으로 복구하려면, interface configuration 명령 **no spanning-tree link-type** 명령을 사용한다.

### 13.4.19. Configuring force-version for port

STP compatibility 를 위해 RSTP 나 MSTP 는 port 에 version 을 설정하여 해당 version 의 STP mode 로 작동하도록 할 수 있다.

Port 에 force-version 을 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>Interface</b> <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹이다.
Step2	<b>spanning-tree force-version</b> <i>version</i>	포트에 force-version을 설정한다. (0 : STP, 2 : RSTP, 3 : MSTP)

Step3	<code>exit</code>	privileged EXEC 모드로 변경한다.
Step4	<code>show running-config</code>	설정 내용을 확인한다.
Step5	<code>copy running-config startup-config</code>	(옵션) 설정을 configuration 파일에 저장한다.

```

Default: Bridge up - Spanning Tree Enabled
Default: Root Path Cost 4 - Root Port 138 - Bridge Priority 32768
Default: Forward Delay 15 - Hello Time 2 - Max Age 20
Default: Root Id 80000007709e12fd
Default: Bridge Id 8000000770dead99
Default: last topology change Wed Jan 14 12:07:59 1970
0: 2 topology change(s) - last topology change Wed Jan 14 12:07:59 1970

Default: portfast bpdu-filter disabled
Default: portfast bpdu-guard disabled
Default: portfast errdisable timeout disabled
Default: portfast errdisable timeout interval 300 sec
Giga5/3: Port 138 - Id 808a - Role Rootport - State Forwarding
Giga5/3: Designated Path Cost 0
Giga5/3: Configured Path Cost 4 - Add type Explicit ref count 1
Giga5/3: Designated Port Id 8001 - Priority 128 -
Giga5/3: Root 80000007709e12fd
Giga5/3: Designated Bridge 80000007709e12fd
Giga5/3: Message Age 0 - Max Age 20
Giga5/3: Hello Time 2 - Forward Delay 15
Giga5/3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer 0
Giga5/3: forward-transitions 1
Giga5/3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
Giga5/3: No portfast configured - Current portfast off
Giga5/3: portfast bpdu-guard default - Current portfast bpdu-guard off
Giga5/3: portfast bpdu-filter default - Current portfast bpdu-filter off
Giga5/3: no root guard configured - Current root guard off
Giga5/3: Configured Link Type point-to-point - Current point-to-point

Switch(config)#inter gi5/3
Switch(config-if-Giga5/3)#spanning-tree force-version 0
Switch(config-if-Giga5/3)#do show spa inter gi5/3
Default: Bridge up - Spanning Tree Enabled
Default: Root Path Cost 4 - Root Port 139 - Bridge Priority 32768

```

```

Default: Forward Delay 15 – Hello Time 2 – Max Age 20
Default: Root Id 80000007709e12fd
Default: Bridge Id 8000000770dead99
Default: last topology change Wed Jan 14 12:09:00 1970
0: 3 topology change(s) – last topology change Wed Jan 14 12:09:00 1970

Default: portfast bpdu-filter disabled
Default: portfast bpdu-guard disabled
Default: portfast errdisable timeout disabled
Default: portfast errdisable timeout interval 300 sec
Giga5/3: Port 138 – Id 808a – Role Designated – State Discarding
Giga5/3: Designated Path Cost 4
Giga5/3: Configured Path Cost 4 – Add type Explicit ref count 1
Giga5/3: Designated Port Id 808a – Priority 128 –
Giga5/3: Root 80000007709e12fd
Giga5/3: Designated Bridge 8000000770dead99
Giga5/3: Message Age 1 – Max Age 20
Giga5/3: Hello Time 2 – Forward Delay 15
Giga5/3: Forward Timer 14 – Msg Age Timer 0 – Hello Timer 0 – topo change timer 34
Giga5/3: forward-transitions 1
Giga5/3: Version Spanning Tree Protocol – Received None – Send STP
Giga5/3: No portfast configured – Current portfast off
Giga5/3: portfast bpdu-guard default – Current portfast bpdu-guard off
Giga5/3: portfast bpdu-filter default – Current portfast bpdu-filter off
Giga5/3: no root guard configured – Current root guard off
Giga5/3: Configured Link Type point-to-point – Current point-to-point

```

### 13.4.20. Configuring root guard for port

해당 port 로 연결되어 있는 Switch 가 root switch 가 되는 것을 방지하는 기술이다. Root guard 가 설정되어 있으면, superior BPDU 가 전달되어도 무시한다. MSTP 에서만 적용된다.

Port 에 root guard 를 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>Interface</b> <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹이다.

Step2	<b>spanning-tree guard root</b>	포트에 root guard를 설정한다.
Step3	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step4	<b>show running-config</b>	설정 내용을 확인한다.
Step5	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

```
Giga5/3 of MST1 is Rootport Forwarding
Edge port: no (default) port guard : none (default)
Link type: point-to-point (auto) bpdu filter :disable (disable)
bpdu guard:disable (disable)
Bpdus send 0
Instance Role Sts Cost Prio.Nbr Vlans mapped
-----
1 Root FWD 20000 128.138
70
%
Switch#con t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#inter gi5/3
Switch(config-if-Giga5/3)#spanning-tree guard root
Switch(config-if-Giga5/3)#do show spa mst inter gi5/3
Giga5/3 of MST1 is Designated root-inconsistent
Edge port: no (default) port guard : root (root)
Link type: point-to-point (auto) bpdu filter :disable (disable)
bpdu guard:disable (disable)
Bpdus send 0
Instance Role Sts Cost Prio.Nbr Vlans mapped
-----
1 Desg RIT 20000 128.138
70
```

### 13.4.21. Configuring hello-time for port

Switch 별로 정하는 hello-time 을 port 별로 설정할 수 있다. 방법은 interface mode 로 진입한다는 점을 제외하고는 switch 의 설정법과 동일하다.

### 13.4.22. Configuring portfast for port

Switch 별로 portfast 를 port 별로 설정할 수 있다. 방법은 interface mode 로 진입한다는 점을 제외하고는 switch 의 설정법과 동일하다.

### 13.4.23. Configuring transmit-holdcount for port

Switch 별로 transmit-holdcount 를 port 별로 설정할 수 있다. 방법은 interface mode 로 진입한다는 점을 제외하고는 switch 의 설정법과 동일하다.

### 13.4.24. Configuring restricted-role for port

MSTP mode 에서 해당 port 가 root port 가 되지 못하도록 하는 기능이다.

포트를 restricted-role 로 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>Interface</b> <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹이다.
Step2	<b>spanning-tree restricted-role</b>	포트를 restricted-role로 설정한다.
Step3	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step4	<b>show running-config</b>	설정 내용을 확인한다.
Step5	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

```

U9200_112(config)#inter gi5/3
U9200_112(config-if-Giga5/3)#spanning-tree restricted-role
U9200_112(config-if-Giga5/3)#do show spa

Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID   Priority   32768
Address   0007709e12fd
Cost      4
Port      139 (Giga5/4)
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority   32768
Address   000770dead99
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300

Interface   Role Sts Cost   Prio.Nbr Type

```

```

-----
Giga5/3    Altn BLK 4    128.138 P2p
Giga5/4    Root FWD 4    128.139 P2p

U9200_112(config-if-Giga5/3)#no spanning-tree restricted-role
U9200_112(config-if-Giga5/3)#do show spa

Root ID    Priority    32768
Address    0007709e12fd
Cost       20000
Port       138 (Giga5/3)
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID   Priority    32768
Address     000770dead99
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300

Interface   Role Sts Cost    Prio.Nbr Type
-----
Giga5/3     Root FWD 4    128.138 P2p
Giga5/4     Altn BLK 4    128.139 P2p

```

### 13.4.25. Configuring restricted-tcn for port

해당 port 가 tcn BPDU 를 받지 못하도록 설정할 수 있다.

포트를 restricted-role 로 설정하려면, privileged EXEC 모드부터 다음의 과정을 거친다:

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>Interface</b> <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다. 유효한 인터페이스는 물리적 인터페이스와 포트 그룹이다.
Step2	<b>spanning-tree restricted-tcn</b>	포트를 restricted-tcn로 설정한다.
Step3	<b>exit</b>	privileged EXEC 모드로 변경한다.



Step4	<code>show running-config</code>	설정 내용을 확인한다.
Step5	<code>copy running-config startup-config</code>	(옵션) 설정을 configuration 파일에 저장한다.

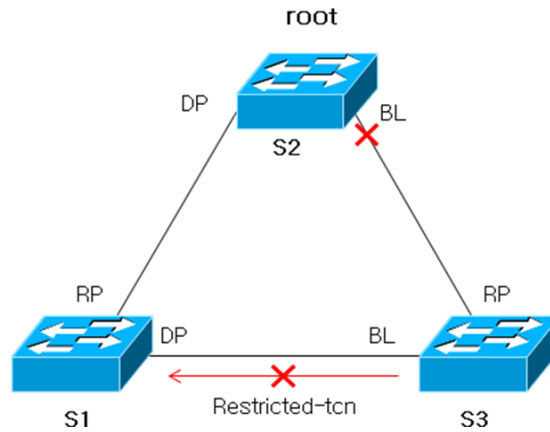


그림 13-7. restricted-tcn

## 13.5. 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 포함 시키는 부분과 STP 나 RSTP 와 같이 hello time, port priority 등을 설정하는 부분으로 나뉜다.

### 13.5.1. Instance 생성 및 VLAN 연결

Instance 를 생성하고 여기에 VLAN 을 넣기 위해서는 privileged EXEC 모드에서부터 다음의 과정을 거친다

	Command	Purpose
Step1	<code>configure terminal</code>	Global configuration 모드로 진입한다.
Step2	<code>Spanning-tree mst configuration</code>	Instance 를 생성하고 vlan 과 연결시키기 위해 mst configuration 모드로 진입한다.
Step3	<code>instance instance-id vlan vlan-id</code>	Instance id 를 생성하고 여기에 vlan-id 에 있는 vlan 을 포함시킨다
Step4	<code>exit</code>	Global configuration 모드로 진입한다.
Step5	<code>interface interface-id</code>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step6	<code>Spanning-tree instance instance-id</code>	Instance 에 해당 포트를 넣는다

Step7	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step8	<b>show running-config</b>	설정 내용을 확인한다.
Step9	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

생성되어 있는 instance 를 삭제할 경우에는 **no instance *instance-id*** 명령을 사용하라.

```
Switch#show spanning-tree mst configuration

name      [Default]
Revision  0    Instances configured 0

% Instance      VLAN
% 0:            2-3, 100
Switch#configure terminal

Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance 1 vlan 2
Switch(config-mst)#exit
Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#spanning-tree instance 1
Switch(config-if-Giga5/3)#exit
Switch#show spanning-tree mst configuration

name      [Default]
Revision  0    Instances configured 0

% Instance      VLAN
% 0:            3, 100
% 1:            2
Switch# configure terminal

Switch(config)#spanning-tree mst configuration
Switch(config-mst)#no instance 1 vlan 2
Switch(config-mst)#exit
Switch#show spanning-tree mst configuration
name      [Default]
Revision  0    Instances configured 0

% Instance      VLAN
% 0:            2-3, 100
```

Switch#

### 13.5.2. instance and port configuration

MSTP에서는 각 instance마다 spanning-tree가 동작하기 때문에 instance별로 priority를 설정한다. 여기서 사용되는 명령어들은 STP, RSTP에서 사용되는 명령어에 instance가 붙어서 사용된다. Instance에 priority를 설정하기 위해서는 privileged EXEC 모드에서부터 다음의 과정을 거친다

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>Spanning-tree instance</b> <i>instance-id priority priority</i>	Instance에 priority를 설정한다
Step3	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step4	<b>show running-config</b>	설정 내용을 확인한다.
Step5	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

default 값으로 복구하려면 **no spanning-tree instance *instance-id* priority** 명령을 사용한다.

```
Switch#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
-----
Giga5/3      Disb    BLK 20000   128.138 Shared

Switch#configure terminal

Switch(config)#spanning-tree instance 1 priority 4096
Switch(config)#exit
Switch#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
-----	-----	-----	-----	-----
Giga5/3	Disb	BLK 20000	128.138	Shared
Switch#				

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	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>interface</b> <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	<b>Spanning-tree instance</b> <i>instance-id priority priority</i>	port 에 priority 를 설정한다
Step4	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step5	<b>show running-config</b>	설정 내용을 확인한다.
Step6	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

default 값으로 복구하려면 **no spanning-tree instance** *instance-id priority* 명령을 사용한다.

```
Switch#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
-----
Giga5/3      Disb    BLK 20000    128.138 Shared

Switch#configure terminal

Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#spanning-tree instance 1 priority 0
```

```
Switch(config-if-Giga5/3)#exit
Switch#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
-----
Giga5/3        Disb    BLK 20000    0.138 Shared

Switch#configure terminal

Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#no spanning-tree instance 1 priority
Switch(config-if-Giga5/3)#exit
Switch#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
-----
Giga5/3        Disb    BLK 20000   128.138 Shared

Switch#
```

port 의 path cost 값을 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>interface</b> <i>interface-id</i>	설정할 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	<b>Spanning-tree</b> <b>instance</b>	port 에 path cost 를 설정한다

	<i>instance-id</i> <b>path-cost</b> <i>path-cost</i>	
Step4	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step5	<b>show running-config</b>	설정 내용을 확인한다.
Step6	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

default 값으로 복구하려면 **no spanning-tree instance** *instance-id* **path-cost** 명령을 사용한다.

```
Switch#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
-----
Giga5/3      Disb    BLK 20000   128.138 Shared

Switch#configure terminal

Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#spanning-tree instance 1 path-cost 1
Switch(config-if-Giga5/3)#exit
Switch#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
-----
Giga5/3      Disb    BLK 1       128.138 Shared

Switch#configure terminal

Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#no spanning-tree instance 1 path-cost
```

```
Switch(config-if-Giga5/3)#exit
Switch#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
-----
-----
Giga5/3        Disb    BLK 20000  128.138 Shared

Switch#
```



#### Notice

MSTP 에서 instance 와 port 에 설정을 하기 위해서는 instance 생성이 먼저 이루어 져야 한다.

### 13.5.3. Setting region and revision number for MST

동일한 MST 에 존재하는 Switch 들은 동일한 MST configuration 을 유지해야 한다. Region 와 revision number 는 MST configuration 에 포함되는 값들이다.

Region 과 revision number 를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	configure terminal	Global configuration 모드로 진입한다.
Step2	spanning-tree mst configuration	mst configuration 모드로 진입한다.
Step3	Region <i>NAME</i>	Region name 을 설정한다.
Step4	Revision <i>number</i>	Revision number 를 설정한다.
Step5	exit	privileged EXEC 모드로 변경한다.
Step6	show running-config	설정 내용을 확인한다.
Step7	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

```
name [Default]
Revision 0    Instances configured 2
```

Instance VLAN

0 1-69, 71-4000  
1 70

SWITCH(config-mst)#region TEST  
SWITCH(config-mst)#revision 100  
SWITCH(config-mst)#do show spa mst conf  
name [TEST]  
Revision 100 Instances configured 2

Instance VLAN

0 1-69, 71-4000  
1 70

### 13.5.4. Pathcost for MSTP

MSTP 에서의 Path cost 값은 아래와 같이 명시되어 있다.

speed	Path cost
10M	2000000
100M	200000
1G	20000
10G	2000

## 13.6. Displaying the Spanning-Tree Status

spanning-tree 상태를 조회하려면, 다음 표에 명시된 privileged EXEC 명령 중 하나를 사용하라:

Command	Purpose
show spanning-tree	전체 인터페이스의 spanning-tree 정보를 출력한다.
show spanning-tree interface <i>interface-id</i>	특정 인터페이스의 spanning-tree 정보를 출력한다.
show spanning-tree detail	포트 상태를 자세하게 보여준다.

privileged EXEC 명령 show spanning-tree 명령의 다른 키워드에 관한 정보는 command



reference를 참고하라.

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 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
-----					
Giga5/3	Disb	BLK	4	128.138	Shared

Interface Role Sts Cost Prio.Nbr Type

-----

Giga5/3 Disb BLK 4 128.138 Shared

Switch#**show spanning-tree interface gi5/3**

% 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

% Giga5/3: Port 138 – Id 8263 – Role Disabled – State Discarding

% Giga5/3: Designated Path Cost 0

% Giga5/3: Configured Path Cost 4 – Add type Explicit ref count 1

% Giga5/3: Designated Port Id 0 – Priority 128 –

% Giga5/3: Root 000000077074ff01

% Giga5/3: Designated Bridge 000000077074ff01

% Giga5/3: Message Age 0 – Max Age 0

% Giga5/3: Hello Time 0 – Forward Delay 0

% Giga5/3: Forward Timer 0 – Msg Age Timer 0 – Hello Timer 0 – topo change timer 0

% Giga5/3: forward-transitions 0

```
% Giga5/3: Version Rapid Spanning Tree Protocol - Received None - Sexit STP
% Giga5/3: No portfast configured - Current portfast off
% Giga5/3: portfast bpdu-guard default - Current portfast bpdu-guard off
% Giga5/3: portfast bpdu-filter default - Current portfast bpdu-filter off
% Giga5/3: no root guard configured - Current root guard off
% Giga5/3: Configured Link Type point-to-point - Current shared
%
%
```

Switch#**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 138 (Giga5/3) of Default is Discarding
Port path cost 0 Port priority 128, 128.138.
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
```

Switch#



#### Notice

MSTP 에서 “show spanning-tree interface IFNAME”은 작동하지 않는다.

## 13.7. Configuring Bridge MAC Forwarding

Layer 2 이더넷(Ethernet) 네트워크가 정상적으로 동작하려면 프레임에 있는 MAC 주소를 MAC address table에 있는 주소와 비교해서 해당 interface로 전송해야 한다. 그러기 위해서는 Bridge의 MAC address table이 설정이 되어야 하고 이를 MAC learning이라 한다. MAC learning은 장비에 들어온 프레임을 검사해서 설정하는 동적 방법과 관리자가 직접 입력하는 정적 방법이 있다.

MAC learning을 하기 위해서 Config 모드에서 다음 명령을 수행한다

Command	Purpose
<b>spanning-tree acquire</b>	Default Bridge 의 MAC learning 을 동적으로 하도록 설정한다. (default 로 enable 되어있다)
<b>no spanning-tree acquire</b>	Default Bridge 의 MAC learning 을 동적으로 하지 않도록 설정한다.
<b>bridge &lt;1-255&gt; acquire</b>	Default Bridge 가 아닌 Bridge 의 MAC learning 을 동적으로 하도록 설정한다. (default 로 enable 되어있다)
<b>no bridge &lt;1-255&gt; acquire</b>	Default Bridge 가 아닌 Bridge 의 MAC learning 을 동적으로 하지 않도록 설정한다.
<b>mac-address-table static MAC (forward discard) IFNAME</b>	해당 Bridge 에 MAC 주소를 IFNAME interface 로 forwarding 하거나 discard 한다
<b>no mac-address-table static MAC (forward discard) IFNAME</b>	MAC 주소에 해당하는 forwarding entry 를 삭제 한다

Default Bridge 가 아닌 경우에는 **bridge <1-255> mac-address-table static MAC (forward|discard) IFNAME** 명령을 사용한다.

다음은 정적으로 MAC learning 을 하는 예시이다.

```
Switch#configure terminal
Switch(config)#mac-address-table static 1111.1111.1111 forward gi5/3
Switch(config)#exit
Switch#show mac-address-table

vlan  mac address  type  fwd      ports
-----+-----+-----+-----+-----
      1 1111.1111.1111  static  1 Gi5/3
Switch(config)#no mac-address-table static 1111.1111.1111 forward gi5/3
Switch(config)#exit
Switch#show mac-address-table

vlan  mac address  type  fwd      ports
-----+-----+-----+-----+-----
No entries present.
Switch#
```

U9264 series 는 MAC address table 에서 동적인 entry 와 정적 entry 를 삭제하는 설정을 할 수 있다.

Command	Purpose
<b>clear mac-address-table (dynamic multicast static)</b>	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 <1-255> 명령을 사용한다.

다음은 정적 MAC 주소 entry 를 삭제하는 예시이다.

Switch#show mac-address-table	
vlan	mac address type fwd ports
-----+	-----+
1	1111.1111.1111 static 1 Gi5/3
Switch#clear mac-address-table static	
Switch#show mac-address-table	
vlan	mac address type fwd ports
-----+	-----+
No entries present.	
Switch#	

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

## 13.8. Self-loop Detection

자신이 전송한 패킷이 되돌아 오는 현상을 감지하는 self-loop 감지 기능을 설정하는 방법을 설명한다.

### 13.8.1. Understanding Self-loop Detection

사용자의 스위치에 이중 경로가 존재하지 않아도 네트워크 구성이나 스위치에 연결된 케이블의 상태 등에 따라 loop 가 발생할 수 있다.

스위치가 자신의 한 포트로 전송한 패킷이 다시 그 포트로 되돌아왔을 때, 이런 현상을 self-loop 이라 한다. 다음의 그림은 self-loop 이 발생한 환경에 대한 예제이다.

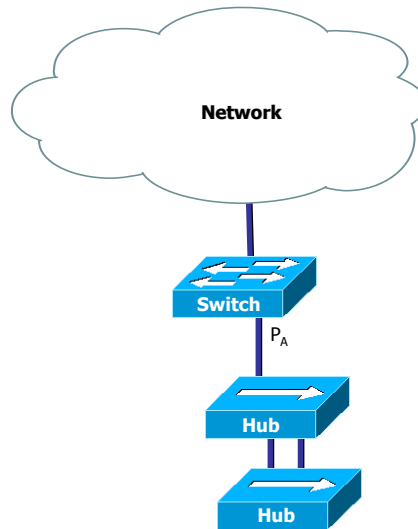


그림 13-8. self-loop 발생 환경

그림에서 두 hub 사이에 이중 경로에 의한 loop 이 존재한다. STP 가 활성화 되지 않은 상태이기 때문에 hub 사이의 loop 은 제거되지 않으며 network 의 불안정을 초래하게 된다. 이 경우 스위치가 포트 PA 를 통해 전송한 패킷은 다시 PA 로 수신된다. 스위치에 self-loop 감지 기능이 활성화되어 있다면, 포트 PA 에 self-loop 이 있다는 것을 감지하고 포트 PA 를 서비스 불가능 상태 (Administrative disable)로 만들어 스위치와 포트 PA 와 연결되지 않은 다른 네트워크를 보호하게 된다. 포트 PA 에 연결된 장비와 네트워크에 여전히 loop 은 존재한다(네트워크에서 완전한 loop 의 제거를 원한다면 STP 를 사용하라).

## 13.8.2. Configuring Self-loop Detection

이 절에서는 스위치에 self-loop 감지 기능을 설정하는 방법을 설명한다:

- Enabling Self-loop Detection
- Changing The Service Status of Port

### 13.8.2.1. Enabling Self-loop Detection

Self-loop 감지 기능은 스위치의 각 포트 별로 기능의 활성화가 가능하다. 또는 Port 의 range 선택 상태에서도 활성화가 가능하다. default 는 self-loop 감지 기능이 비활성화 되어 있다.

Self-loop 감지 기능이 활성화 된 후 이 기능에 의하여 port 가 shutdown 상태가 되면 설정된 limit time 이 지난 후 자동으로 no shutdown 상태로 바뀐다. Limit time 의 default 값은 5 분이고, 분 단위로 0 부터 1440 까지 지정할 수 있으며 0 으로 설정하면 수동으로 no shutdown 하기 전까지

port 가 shutdown 상태로 있다.



**Notice**

P8600에서는 기존의 SLD와는 다르게 Self-loop 감지하고자 하는 포트가 속한 vlan에 self-loop-detection을 활성화한 이후에 실제 Self-loop 감지하고자 하는 포트에 self-loop-detection을 활성화해야 SLD가 정상적으로 동작한다.

Self-loop 감지 기능을 활성화하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	<b>Configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>interface</b> <i>vlan-name</i>	Self-loop을 걸고자 하는 포트가 속한 vlan
Step3	<b>self-loop-detection</b>	해당 vlan에 Self-loop 감지 기능을 활성화한다.
Step4	<b>interface</b> <i>interface-name</i>	Interface configuration 모드로 진입한다.
Step5a	<b>self-loop-detection</b>	Self-loop 감지 기능을 활성화한다. Self loop에 의해 shutdown되면 5 minutes 후에 자동으로 no shutdown한다.
Step5b	<b>self-loop-detection limit_time</b> <i>&lt;0-1440&gt;</i>	Self-loop 감지 기능을 활성화한다. Self loop에 의해 shutdown되면 설정된 minutes 후에 자동으로 no shutdown한다.
Step6	<b>exit</b>	privileged EXEC 모드로 변경한다.
Step7a	<b>show running-config</b>	설정 내용을 확인한다.
Step7b	<b>show self-loop-detection</b>	Self-loop 설정 내용을 확인한다.
Step7c	<b>show loop-detect</b>	Self-loop 설정 내용을 확인한다.
Step8	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

다음은 포트 gi1 에 self-loop 감지 기능을 default limit time 으로 활성화 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if-vlan1)# self-loop-detection
Switch(config-if-vlan1)# interface gi1
Switch(config-if-gi1)# self-loop-detection
Switch(config-if-gi1)# exit
Switch# show self-loop-detection
```

ifname	ld	link	shutdown	set_time	remain_time	count	last-occur
gi1	set	up	.	5 min	.	0	.
gi2	.	down	.	.	.	0	.
gi3	.	down	.	.	.	0	.
gi4	.	down	.	.	.	0	.
gi5	.	up	.	.	.	0	.
.....							
gi25	.	down	.	.	.	0	.
gi26	.	down	.	.	.	0	.

Switch#



### 13.8.2.2. Changing The Service Status of Port

Self-loop 감지 기능에 의해 서비스 불가능 상태가 된 포트가 limit time 이 0 으로 설정된 상태라면 수동으로만 서비스 가능 상태로 만들 수 있다.

포트를 서비스 가능 상태로 만들려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	Configure terminal	Global configuration 모드로 진입한다.
Step2	interface <i>interface-name</i>	Interface configuration 모드로 진입한다.
Step3	no shutdown	포트를 서비스 가능 상태로 만든다.
Step4	exit	privileged EXEC 모드로 변경한다.
Step5	show port status	포트의 상태정보를 확인한다.

### 13.8.2.3. Disabling Self-loop Detection

Self-loop 감지 기능은 스위치의 각 포트 별로 또는 Port 의 range 선택 상태에서 기능의 비활성화가 가능하다.

만약 비활성화할 Port 가 Self-loop 감지기능에 의해 자동으로 shutdown 된 상태라면 no shutdown 으로 설정 후 Self-loop 감지 기능을 비활성화 한다.

Self-loop 감지 기능을 비활성화 하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	Configure terminal	Global configuration 모드로 진입한다.
Step2	interface <i>interface-name</i>	Interface configuration 모드로 진입한다.
Step3a	no self-loop-detection	Self-loop 감지 기능을 비활성화 한다. Self loop 에 의해 shutdown 되면 5 minutes 후에 자동으로 no shutdown 한다.
Step4	interface <i>vlna-name</i>	vlan configuration 모드로 진입한다.
Step5a	no self-loop-detection	Self-loop 감지 기능을 비활성화 한다.
Step6	exit	privileged EXEC 모드로 변경한다.
Step7a	show running-config	설정 내용을 확인한다.
Step7b	show self-loop-detection	Self-loop 설정 내용을 확인한다.
Step8	copy running-config startup-config	(옵션) 설정을 configuration 파일에 저장한다.

다음은 포트 gi1 에 self-loop 감지 기능을 비 활성화 하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if-vlan1)# self-loop-detection
Switch(config-if-vlan1)# interface gi1
```

```
Switch(config-if-gi1)# no self-loop-detection
```

```
Switch(config-if-gi1)# exit
```

```
Switch# show self-loop-detection
```

```
-----
ifname  Id  link  shutdown set_time remain_time count    last-occur
-----
gi1     .   up    .         .         .         0       .
gi2     .   down  .         .         .         0       .
gi3     .   down  .         .         .         0       .
gi4     .   down  .         .         .         0       .
gi5     .   up    .         .         .         0       .
.....
gi25    .   down  .         .         .         0       .
gi26    .   down  .         .         .         0       .
Switch#
```

### 13.8.3. Displaying Self-loop Status

포트의 self-loop 감지 기능 설정 상태를 조회하려면, privileged EXEC 명령 **show running-config** 나 **show self-loop-detection** 을 사용하라.

**show self-loop-detection** 에서

- ifname : Interface name (Port name)
- Id : self-loop-detection 설정 (set)
- link : link 의 상태 (up, down)
- shutdown : SLD 에 의한 shutdown (block)
- set\_time : SLD 에 의한 limit time (minutes). 만약 0 min 이라면 SLD 에 의해 shutdown 된 후, 수동으로 해당 Port 를 no shutdown 하기 전까지 계속 shutdown 상태로 있게 된다.
- remain\_time : SLD 에 의한 shutdown 시 정상으로 복귀되기 까지 남은 시간 (minute:second)
- count : SLD 에 의한 shutdown 횟수
- last-occur : 마지막으로 SLD 에 의해 shutdown 된 시간

다음 예는 Port gi5 에 SLD 가 default time 인 5 분으로 설정되어 있는 것을 보여준다. Port gi5 는 May 29 04:48:39 2006 에 SLD 에 의해 self loop 이 감지되어 shutdown 된 적이 한번 있었다는 것을 알 수 있다.

Switch# **show running-config**

```
!
interface gi5
  self-loop-detection
!
interface vlan1
  self-loop-detection
  ip address 100.1.1.1/24
!
```

Switch#

Switch# **show self-loop-detection**

ifname	ld	link	shutdown	set_time	remain_time	count	last-occur
gi1	.	down	.	.	.	0	.
gi2	.	up	.	.	.	0	.
gi3	.	down	.	.	.	0	.
gi4	.	down	.	.	.	0	.
gi5	set	up	block	5 min	.	1	SEP 04:48:39 2010
gi6	.	down	.	.	.	0	.
gi7	.	down	.	.	.	0	.
gi8	.	down	.	.	.	0	.

Switch#

# 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. U9200 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 있기 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.

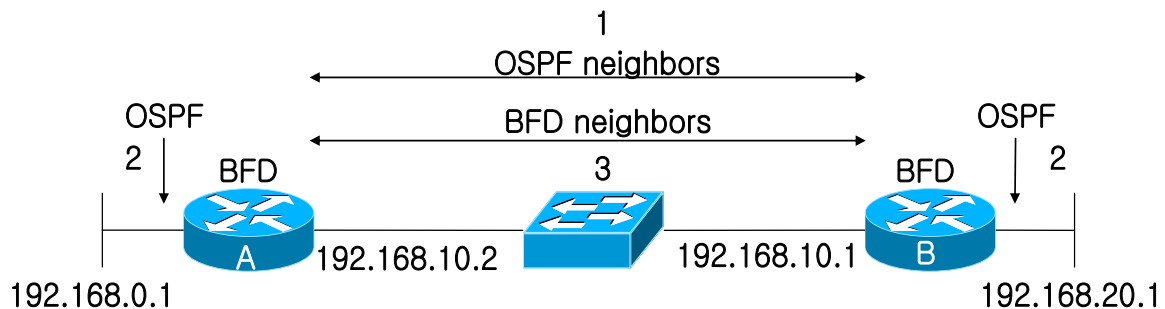


그림 14-1 Establishing a BFD neighbor relationship

그림 14-2는 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.

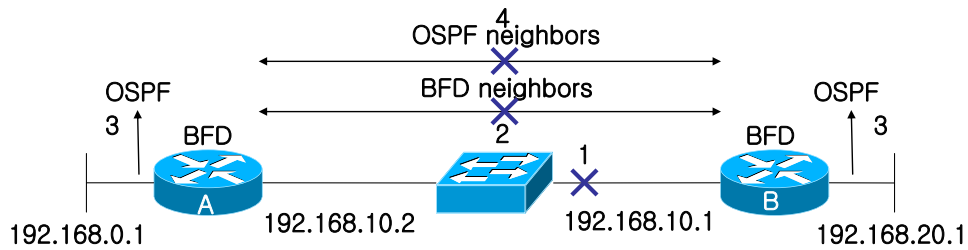


그림 14-2 Tearing down an OSPF neighbor relationship

### 14.1.2. Benefits of using BFD for Failure Detection

BFD 는 OSPF 와 같은 라우팅 프로토콜에 장애 감지 메커니즘을 제공할 수 있다. 라우팅 프로토콜에서 BFD 를 사용하면 다음과 같은 장점이 있다:

- OSPF 에서 타이머 시간을 최대한 줄이면 1~2 초 이내의 장애 감지가 가능하지만, BFD 는 1 초 이내로 장애를 감지할 수 있다.
- BFD 는 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. U9200 시리즈 스위치에서는 **bfd interval** 명령으로 인터페이스에 BFD 세션 파라미터를 설정해야만 BFD single hop 세션이 생성된다.

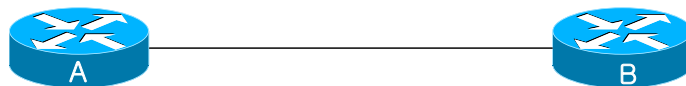


그림 14-3 BFD single hop session

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 있

다. BFD multihop 세션의 파라미터는 **bfd multihop-peer** 명령으로 설정할 수 있다.

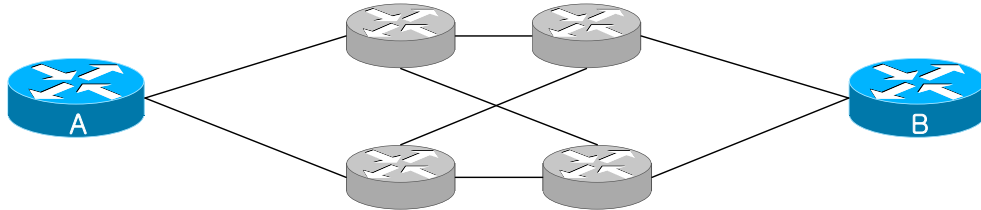


그림 14-4 BFD multihop session

#### 14.1.4. BFD Version Interoperability

U9200 시리즈 스위치는 BFD 버전 1 뿐만 아니라 버전 0도 지원한다. 모든 BFD 세션은 버전 1으로 생성되지만 버전 0와 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 0를 사용하고 있고 나머지 시스템들은 버전 1을 사용하고 있다면, 모든 시스템들이 버전 0를 사용하게 된다. **show bfd neighbor [details]** 명령으로 BFD 세션이 사용하고 있는 버전을 확인할 수 있다.

## 14.2. BFD Restrictions

U9200 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	<b>configure terminal</b>  예제: Switch# <b>configure terminal</b>	Global configure 모드로 진입한다
Step 2	<b>interface interface-name</b>  예제: Switch(config)# <b>interface gi2/2/1</b>	Interface configuration 모드로 진입한다.
Step 3	<b>ip address ip-address/prefix-length</b>  예제: Switch(config-if-Giga2/2/1)# <b>ip address 33.1.1.1/24</b>	인터페이스에 IP 주소를 설정한다.
Step 4	<b>bfd interval minlliseconds min_rx milliseconds multiplier interval-multiplier</b>  예제: Switch(config-if-Giga2/2/1)# <b>bfd interval 750 min_rx 500 multiplier 3</b>	인터페이스에 BFD 파라미터를 설정한다.
Step 5	<b>end</b>  예제: Switch(config-if-Giga2/2/1)# <b>end</b>	privileged EXEC 모드로 돌아간다



#### Notice

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	<b>configure terminal</b>  예제: Switch# <b>configure terminal</b>	Global configure 모드로 진입한다
Step 2	<b>bfd multihop-peer A.B.C.D interval minlliseconds min_rx milliseconds multiplier interval-multiplier</b>  예제: Switch(config)# <b>bfd multihop-peer 10.1.1.1 interval 750 min_rx 500 multiplier 3</b>	Multi-hop BFD 세션의 BFD 파라미터를 설정한다.
Step 3	<b>End</b>  예제: Switch(config)# <b>end</b>	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	<b>configure terminal</b>  예제: Switch# <b>configure terminal</b>	Global configure 모드로 진입한다
Step 2	<b>router bgp as-tag</b>  예제: Switch(config)# <b>router bgp 100</b>	BGP 라우팅 설정 모드로 진입한다.
Step 3	<b>neighbor ip-address fall-over bfd</b>  예제: Switch(config-router)# <b>neighbor 3.3.3.2 fall-over bfd</b>	BGP neighbor 와의 연결상태 검사에 BFD 를 사용하도록 설정한다.
Step 4	<b>end</b>  예제: Switch(config-router)# <b>end</b>	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	<b>configure terminal</b>  예제: Switch# <b>configure terminal</b>	Global configure 모드로 진입한다
Step 2	<b>router ospf process-id</b>  예제: Switch(config)# <b>router ospf 10</b>	OSPF 라우팅 설정 모드로 진입한다.
Step 3	<b>bfd all-interfaces</b>  예제: Switch(config-router)# <b>bfd all-interface</b>	모든 OSPF 인터페이스에 대해 BFD 세션을 생성할 수 있도록 설정한다.
Step 4	<b>exit</b>  예제: Switch(config-router)# <b>exit</b>	global configuration 모드로 되돌아 간다.
Step 5	<b>interface type number</b>  예제: Switch(config)# <b>interface gi2/1/1</b>	Interface configuration 모드로 진입한다.
Step 6	<b>bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier</b>  예제: Switch(config-if-Giga2/2/1)# <b>bfd interval 750 min_rx 500 min 3</b>	OSPF 인터페이스에 BFD 세션 파라미터 값을 설정한다.  BFD 세션을 사용할 모든 OSPF 인터페이스에 대해 <b>bfd interval</b> 설정을 해야 한다.
Step 7	<b>interface type number</b>  예제:	(Option) Interface configuration 모드로 진입한다.

Step 8	Switch(config)# <b>interface gi2/2/1</b>	
	<b>ip ospf bfd [disable]</b>  예제: Switch(config-if-Giga2/2/1)# <b>ip ospf bfd disable</b>	(Option) 특정 OSPF 인터페이스에 대해서는 BFD 세션이 생성되지 않도록 설정한다.  <b>Note</b> <b>disable</b> keyword 는 <b>bfd all-interface</b> 명령이 수행 되어 BFD 가 <b>enable</b> 된 인터페이스에서만 사용해야 한다.
Step 9	<b>end</b>	Privileged EXEC 모드로 되돌아 간다.
	예제: Switch(config-if-Giga2/2/1)# <b>end</b>	

### 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	<b>configure terminal</b>	Global configure 모드로 진입한다
	예제: Switch# <b>configure terminal</b>	
Step 2	<b>interface type number</b>	Interface configuration 모드로 진입한다.
	예제: Switch(config)# <b>interface gi2/1/1</b>	
Step 3	<b>bfd interval minlliseconds min_rx milliseconds multiplier interval-multiplier</b>	인터페이스에 BFD 파라미터를 설정한다.
	예제: Switch(config-if-Giga2/2/1)# <b>bfd interval 750 min_rx 500 multiplier 3</b>	
Step 4	<b>ip ospf bfd [disable]</b>	이 OSPF 인터페이스를 통해 BFD 세션이 생성될 수 있도록 설정한다.
	예제: Switch(config-if-Giga2/1/1)# <b>ip ospf bfd</b>	
Step 5	<b>end</b>	Privileged EXEC 모드로 되돌아 간다.
	예제: Switch(config-if-Giga2/1/1)# <b>end</b>	

### 14.4.5. Configuring BFD support for Static routing

정적 라우팅(static routing)에서는 정적 라우트의 게이트웨이를 BFD peer 로 설정한다. 다음은 정적 라

우팅에서 BFD 를 설정하는 방법이다.

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  예제: Switch# <b>configure terminal</b>	Global configure 모드로 진입한다
Step 2	<b>interface interface-name</b>  예제: Switch(config)# <b>interface gi2/2/1</b>	Interface configuration 모드로 진입한다.
Step 3	<b>ip address ip-address/prefix-length</b>  예제: Switch(config-if-Giga2/2/1)# <b>ip address 1.1.1.1/24</b>	인터페이스에 IP 주소를 설정한다.
Step 4	<b>bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier</b>  예제: Switch(config-if-Giga2/2/1)# <b>bfd interval 750 min_rx 500 min 3</b>	인터페이스에 BFD 세션 파라미터 값을 설정한다.
Step 5	<b>Exit</b>  예제: Switch(config-if-Giga2/2/1)# <b>exit</b>	Global configuration 모드로 돌아간다
Step 6	<b>ip route A.B.C.D/M gateway-addr</b>  예제: Switch(config)# <b>ip route 7.0.0.0/8 1.1.1.254</b>	정적 라우트를 설정한다.
Step 7	<b>ip route static bfd IFNAME gateway-addr</b>  예제: Switch(config)# <b>ip route static bfd gi2/2/1 1.1.1.254</b>	정적 라우트의 BFD neighbor 를 지정한다. 정적라우트의 게이트웨이가 연결된 인터페이스와 게이트웨이의 IP 주소를 명시한다.
Step 8	<b>end</b>  예제: Switch(config)# <b>end</b>	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. BFD 를 수동 모드로 동작시키려면 다음의 순서대로 인터페이스를 설정하면 된다.

네트워크의 모든 라우터를 BFD 수동 모드로 설정하면 BFD 가 동작하지 않는다. 적어도 하나의 시스

템의 BFD 는 능동 모드(active mode)로 동작해야 한다.

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  예제: Switch# <b>configure terminal</b>	Global configure 모드로 진입한다
Step 2	<b>interface interface-name</b>  예제: Switch(config)# <b>interface gi2/2/1</b>	Interface configuration 모드로 진입한다.
Step 3	<b>bfd passive</b>  예제: Switch(config-if-Giga2/2/1)# <b>bfd passive</b>	인터페이스를 BFD 수동 모드로 설정한다.
Step 4	<b>end</b>  예제: Switch(config-if-Giga2/2/1)# <b>end</b>	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 neighbor 들 사이에서 송수신되는 BFD 컨트롤 패킷의 수를 감소 시킬 수 있다. BFD echo 모드는 비활성화 되어 있다.

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  예제: Switch# <b>configure terminal</b>	Global configure 모드로 진입한다
Step 2	<b>bfd echo [accept   send]</b>  예제: Switch(config)# <b>bfd echo</b>	BFD echo 모드를 enable 한다.  - <b>accept</b> 키워드는 Echo packet 을 receive 할 때 사용 - <b>send</b> 키워드는 Echo packet 을 send 할 때 사용
Step 3	<b>end</b>  예제: Switch(config)# <b>end</b>	Privileged EXEC 모드로 되돌아 간다.

### 14.4.8. Configuring BFD slow timer

BFD neighbor 가 서로 상대방을 인식하지 못한 상태 (BFD 상태가 Up 이 아닌 상태)에서는 BFD 컨트롤 패킷을 **bfd interval** 로 설정한 주기로 전송하는 것이 무의미하다. BFD 세션의 상태가 Up 이 아닐 때 BFD 컨트롤 패킷의 전송주기를 설정하려면 **bfd slow-timer** 명령을 사용하면 된다.

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  예제: Switch# <b>configure terminal</b>	Global configure 모드로 진입한다
Step 2	<b>bfd slow-timer</b> <i>milliseconds</i>  예제: Switch(config)# <b>bfd slow-timer 2000</b>	BFD slow timer 를 설정한다.
Step 3	<b>end</b>  예제: Switch(config)# <b>end</b>	Privileged EXEC 모드로 돌아간다.

### 14.4.9. Displaying BFD information

	Command or Action	Purpose
Step 1	<b>show bfd neighbor</b> [detail]  예제: Switch# <b>show bfd neighbor details</b>	(option) BFD adjacency database 를 보여준다.  - <b>detail</b> 키워드는 모든 BFD 프로토콜 파라미터와 타이머를 보여준다.
Step 2	<b>debug bfd</b> [echo event fsm loopback neighbor nsm packet]  예제: Switch# <b>debug bfd packet</b>	(Option) BFD 와 관련된 debugging 정보를 보여준다.

## 14.5. BFD Configuration Samples

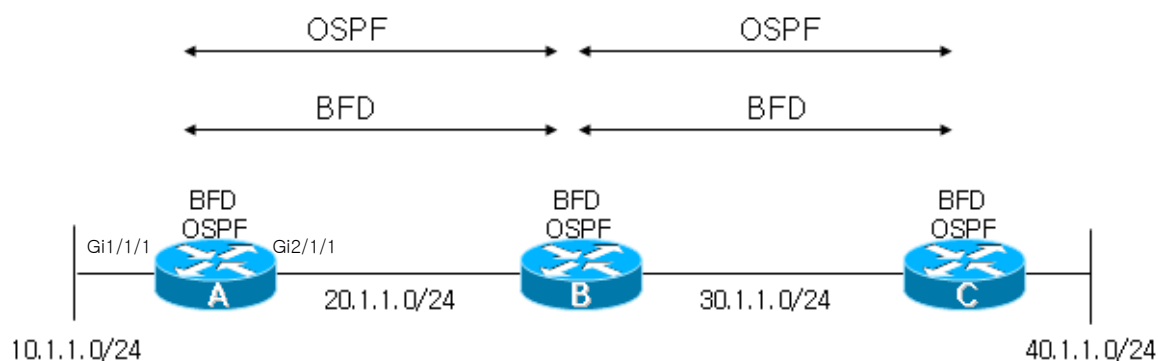
이 절은 다음과 같은 예제들을 포함한다:

- 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 BFD를 사용하는 방법을 설명한다. 다음과 같은 네트워크 구성을 가정하자:



OSPF는 OSPF 인터페이스에 대해 BFD를 설정해야 한다. OSPF 인터페이스에 BFD를 설정하는 방법은 다음과 같다:

- ✓ OSPF의 모든 인터페이스에서 BFD를 사용하도록 설정
- ✓ 특정 OSPF 인터페이스에서 선택적으로 BFD를 사용하도록 설정

#### 1. Configuring BFD Support for OSPF for All Interfaces

OSPF의 모든 인터페이스에서 BFD를 사용하려면 다음과 같이 설정한다.

Step 1 OSPF를 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 OSPF의 모든 인터페이스가 BFD를 사용하도록 설정한다.

```
Switch_A# configure terminal
Switch_A(config)# router ospf
Switch_A(config-router)# bfd all-interfaces
```

Step 4 OSPF neighbor가 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**



**Notice**

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.

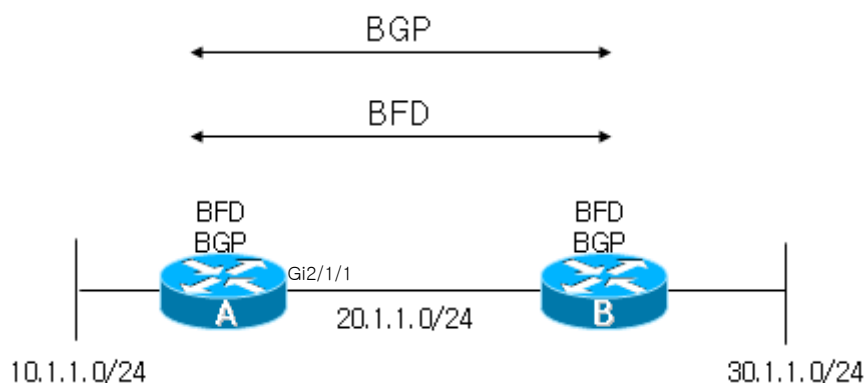
```
Switch_A# show bfd neighbors
```

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
```

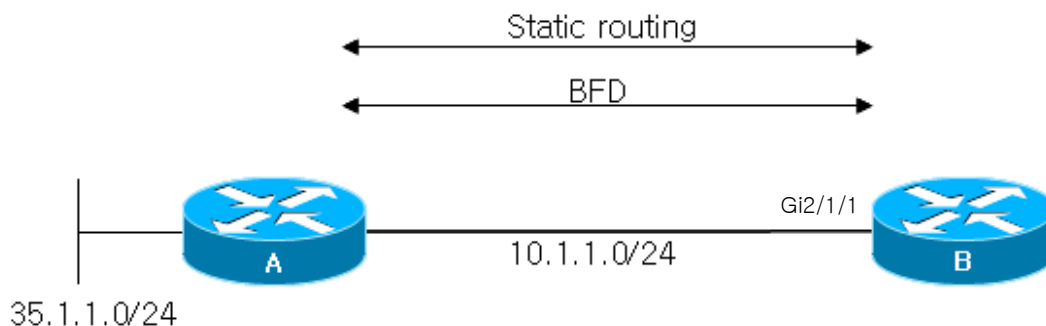
스위치의 설정을 조회하면 다음과 같다.

```
!
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 BFD 를 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
```



**Notice**

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.

**Notice**

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
- Displaying 802.3ad Statistics and Status

## 15.1. Understanding Link Aggregation Control Protocol

이 절에서는 다음 항목을 설명한다:

- LACP Modes
- LACP Parameters

### 15.1.1. LACP Modes

U9200 Series switch 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
off	LACP 에 의해 포트가 포트 그룹으로 구성되지 않도록 한다
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.

## 15.1.2. 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 포트에는 자동 혹은 CLI 통해서 administrative key 값을 할당해야 한다. 포트가 다른 포트와 통합될 수 있는 능력은 administrative key 에 의해 정의 된다. 다른 포트와 통합될 수 있는 포트의 능력은 다음의 요소에 의해 결정된다:
  - 전송률(data rate), duplex 모드, point-to-point 혹은 공유 매체와 같은 포트의 물리적 특성
  - 설정 제약

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

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
- Changing the LACP Mode
- 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
<b>Step1</b>	<b>configure terminal</b>	Global configuration 모드로 진입한다.
<b>Step2</b>	<b>lacp system-priority <i>priority</i></b>	system priority 를 설정한다.
<b>Step3</b>	<b>end</b>	privileged EXEC 모드로 변경한다.
<b>Step4</b>	<b>show lacp sys-id</b>	설정 내용을 확인한다.
<b>Step5</b>	<b>copy running-config startup-config</b>	(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	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>interface</b> <i>interface-id</i>	LACP 를 port priority 를 설정하려는 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	<b>lacp port-priority</b> <i>priority</i>	port priority 를 설정한다.
Step4	<b>end</b>	privileged EXEC 모드로 변경한다.
Step5	<b>show running-config</b>	설정 내용을 확인한다.
Step6	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

설정한 port priority 를 default 설정으로 복구하려면 interface configuration 명령 **no lacp port-priority** 를 사용하라

다음은 인터페이스 gi1 의 port-priority 를 10 으로 설정하는 예이다:

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# lacp port-priority 10
Switch(config)# end
```

### 15.2.3. Specifying an Administrative Key Value

포트나 시스템의 administrative key 값을 설정할 수 있다. admin-key 값을 설정하지 않는다면 자동으로 값이 설정된다. 두 경우 모두 유효한 admin-key 값의 범위는 1~1024 이다.

administrative key 값을 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>interface</b> <i>interface-id</i>	administrative key 를 설정하려는 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	<b>lacp admin-key</b> <i>key</i>	administrative key 를 설정한다.
Step4	<b>end</b>	privileged EXEC 모드로 변경한다.
Step5	<b>show running-config</b>	설정 내용을 확인한다.
Step6	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

인터페이스에 자동으로 administrative key 값을 할당하려면, interface configuration 명령 **no lacp admin-key** 를 사용하라.

다음은 인터페이스 gi1 의 administrative key 를 10 으로 설정하는 예이다:

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# lacp admin-key 10
Switch(config)# end
```

## 15.2.4. Specifying the Timeout Value

포트별로 LACPDU의 전송 주기를 설정할 수 있다. 전송 주기는 short (1 초)나 long (30 초)으로 설정할 수 있다.



**Notice** **lacp timeout** 명령은 설정하는 스위치가 아닌 상대 스위치의 LACPDU 전송 주기에 영향을 미친다.

LACPDU의 전송 주기를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>interface</b> <i>interface-id</i>	LACPDU 전송주기를 설정하려는 인터페이스를 명시하여 interface configuration 모드로 진입한다.
Step3	<b>lacp timeout</b> {short long}	LACPDU 전송주기를 설정한다.
Step4	<b>end</b>	privileged EXEC 모드로 변경한다.
Step5	<b>show running-config</b>	설정 내용을 확인한다.
Step6	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

설정된 LACPDU 전송주기를 default로 복구하려면, interface configuration 명령 **no lacp timeout**을 사용하라.

다음은 인터페이스 gi1과 연결된 상태 시스템의 LACPDU 전송주기를 short로 설정하는 예이다:

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# lacp timeout short
Switch(config)# end
```

## 15.2.5. Changing the LACP Mode

인터페이스의 LACP 동작 모드를 설정할 수 있다.

LACP 모드를 설정하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	<b>configure terminal</b>	Global configuration 모드로 진입한다.
Step2	<b>interface</b> <i>interface-id</i>	LACP 모드를 설정하려는 인터페이스를 명시하여 interface

		configuration 모드로 진입한다.
Step3	<b>lACP mode</b> <b>{active   off   passive}</b>	LACP 모드를 설정한다.
Step4	<b>end</b>	privileged EXEC 모드로 변경한다.
Step5	<b>show running-config</b>	설정 내용을 확인한다.
Step6	<b>copy running-config startup-config</b>	(옵션) 설정을 configuration 파일에 저장한다.

다음은 인터페이스 gi1의 LACP를 disable하는 예이다:

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# lACP mode off
Switch(config)# end
```

### 15.2.6. Clearing LACP Statistics

LACP의 통계 정보를 삭제하려면 privileged EXEC 모드에서부터 다음의 과정을 거친다.

	Command	Purpose
Step1	<b>clear lACP [aggregator-id] counters</b>	해당 port group의 LACP 통계 정보를 삭제한다.
Step2	<b>show lACP counters</b>	변경 내용을 확인한다.

다음은 port group 1의 LACP를 통계정보를 삭제하는 예이다:

```
Switch# clear lACP 1 counters
```

## 15.3. Displaying 802.3ad Statistics and Status

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**를 사용하라.

출력 결과물의 항목에 대한 상세정보는 command reference를 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 명령으로 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. <b>Default) send</b>	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. <b>Default) send</b>	Config
no ip option icmp-unreachable-send	ICMP unreachable 에러 전송 설정을 해제한다.	Config
ip option ip_default_ttl VALUE	Default TTL 크기를 설정한다. <b>Default) 64</b>	Config
no ip option ip_default_ttl	Default TTL 크기 설정을 기본값으로 변경한다.	Config

	다.	
ip option ipfrag_time <i>VALUE</i>	메모리에서 IP fragment 를 유지하는 시간을 설정한다. <b>Default) 30</b>	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  <i>PORT</i> ) period <1-3600> count <1-655535>	TCP connection rate-limit profile 을 추가한다. TCP 목적지 포트에 대해 period 이내에 count 이상 TCP 연결을 시도하는 경우 로깅 및 차단 할 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 <i>VALUE</i>	FIN-WAIT-2 상태의 소켓 유지 시간을 설정한 다. <b>Default) 60</b>	Config
no ip option tcp_fin_timeout	FIN-WAIT-2 상태의 소켓 유지 시간을 기본값 으로 변경한다.	Config
ip option tcp_keepalive_probes <i>VALUE</i>	연결이 끊어졌다고 여길 때까지 발생 시킬 keepalive probe 메시지 수를 설정한다. <b>Default) 9</b>	Config
no ip option tcp_keepalive_probes	Keepalive probe 메시지 수를 기본값으로 변 경한다.	Config
ip option tcp_keepalive_time <i>VALUE</i>	Keepalive 가 활성화되었을 경우 keepalive 메 시지 전송 시간을 설정을 설정한다. <b>Default) 7200</b>	Config
no ip option tcp_keepalive_time	Keepalive 메시지 전송 시간을 기본값으로 변 경한다.	Config
ip option tcp_max_syn_backlog <i>VALUE</i>	TCP syn backlog queue 의 최대치 설정이다. <b>Default) 1024</b>	Config
no ip option tcp_max_syn_backlog	TCP syn backlog queue 의 최대치 설정을 기 본값으로 변경한다.	Config
ip option tcp_max_tw_buckets <i>VALUE</i>	Timewait 소켓의 수를 설정한다. <b>Default) 18700</b>	Config
no ip option tcp_max_tw_buckets	Timewait 소켓의 수를 기본값으로 변경한다.	Config
ip option tcp_retries1 <i>VALUE</i>	의심스러운 TCP session 에 대한 재전송 횟수 를 설정한다. <b>Default) 3</b>	Config
no ip option tcp_retries1	의심스러운 TCP session 에 대한 재전송 횟수 를 기본값으로 변경한다.	Config
ip option tcp_retries2 <i>VALUE</i>	종단전 재전송 횟수를 설정한다. <b>Default)15</b>	Config

no ip option tcp_retries2	종단전 재전송 횟수를 기본값으로 변경한다.	Config
ip option tcp_syn_retries <i>VALUE</i>	활성 TCP 연결에서 재전송을 위해 지정한 시간만큼 지난 뒤에 초기화 <b>SYN</b> 패킷을 보낸다. <b>Default) 5</b>	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. <b>Default) enable</b>	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)

Virtual Router Redundancy Protocol (VRRP)는 LAN에서 여러 개의 접근 경로를 제공하기 위해 여러 라우터가 동일한 가상 IP 주소를 가지도록 허용하고, 그 중 한 라우터를 가상 라우터로 선출하는 프로토콜이다. VRRP 라우터는 LAN에 연결된 다른 라우터와 통신하기 위해 VRRP 프로토콜을 사용한다. VRRP 설정에서, 한 라우터가 마스터 가상 라우터로 선출되면 나머지 라우터들은 마스터 가상 라우터의 장애에 대비해 backup으로 동작한다.

## 17.1. Information About VRRP

### 17.1.1. VRRP Operation

LAN 클라이언트가 특정 목적지에 대한 first hop 라우터를 선택하는 방법은 여러 가지가 있다. 클라이언트는 동적 절차나 정적 설정을 사용할 수 있다. 동적으로 라우터를 결정하는 방법의 예는 다음과 같다:

- Proxy ARP – 클라이언트는 자신의 목적지를 알기 위해 Address Resolution Protocol (ARP)를 사용하고, 라우터는 자신의 MAC 주소를 사용해서 ARP request에 응답한다.
- Routing protocol – 클라이언트는 dynamic 라우팅 프로토콜의 업데이트 정보를 이용해서 자신의 라우팅 테이블을 구축한다.
- IRDP (ICMP Router Discovery Protocol) client – 클라이언트는 Internet Control Message Protocol (ICMP) router discover 클라이언트를 실행한다.

LAN 클라이언트에 대한 설정과 프로토콜 동작에 대한 부담이 동적 프로토콜의 단점이다. 또한 라우터에 장애가 발생했을 때, 다른 라우터로의 절체가 느려질 수 있다.

동적 프로토콜에 대한 대안은 클라이언트에 default 라우터를 정적으로 설정하는 것이다. 이 방법은 클라이언트의 설정과 동작이 간단하다. 그러나 default gateway에 장애가 발생하면, LAN 클라이언트는 외부 네트워크와의 통신이 단절된다.

VRRP는 정적 설정 문제를 해결할 수 있다. VRRP는 라우터의 그룹이 하나의 가상 라우터를 형성하

도록 한다. LAN 클라이언트는 가상 라우터를 자신의 **default gateway** 로 설정한다. 라우터의 그룹을 표현하는 가상 라우터를 **VRRP 그룹**이라고 표현하기도 한다.

그림 1 은 VRRP 가 설정된 LAN 형상을 나타낸다. 이 예제에서 라우터 **A, B** 그리고 **C** 가 가상 라우터를 구성하는 VRRP 라우터 (VRRP 를 실행하는 라우터)이다. 가상 라우터의 IP 주소는 라우터 **A** 의 IP 주소 (10.0.0.1)과 동일하게 설정한다.

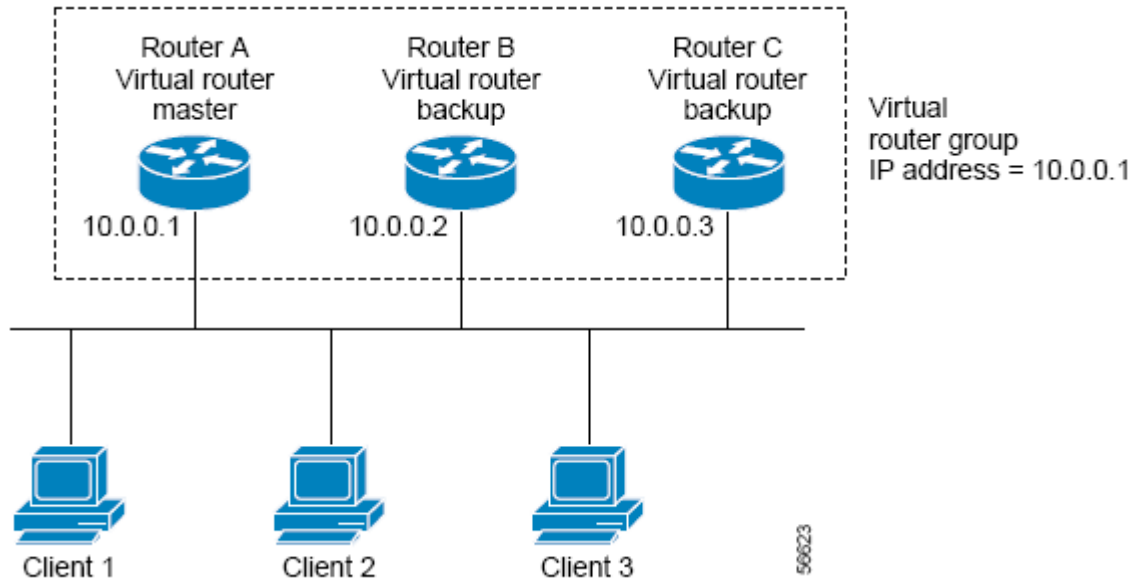


그림 17-1 Basic VRRP Topology

가상 라우터가 라우터 **A** 의 물리적 주소를 사용하기 때문에, 라우터 **A** 가 마스터 가상 라우터 의 역할을 담당하고 **IP address owner** 라 부른다. 라우터 **A** 는 마스터 가상 라우터로써 가상 라우터의 IP 주소를 제어하고, 이 IP 주소로 전달된 패킷의 포워딩을 담당한다. Client 1 부터 3 은 **default gateway** 의 IP 주소를 10.0.0.1 로 설정한다.

라우터 **B** 와 **C** 는 백업 가상 라우터로 동작한다. 만약 마스터 가상 라우터에 장애가 발생하면, 높은 우선 순위를 가진 라우터가 마스터 가상 라우터가 되어 LAN 호스트들에게 계속 서비스를 제공한다. 라우터 **A** 가 복구되면, 다시 마스터 가상 라우터가 된다.

그림 2 는 라우터 **A** 와 **B** 가 트래픽을 공유하도록 VRRP 를 설정한 예를 보여준다. 라우터 **A** 와 **B** 는 서로에 대한 백업 가상 라우터로 동작한다.

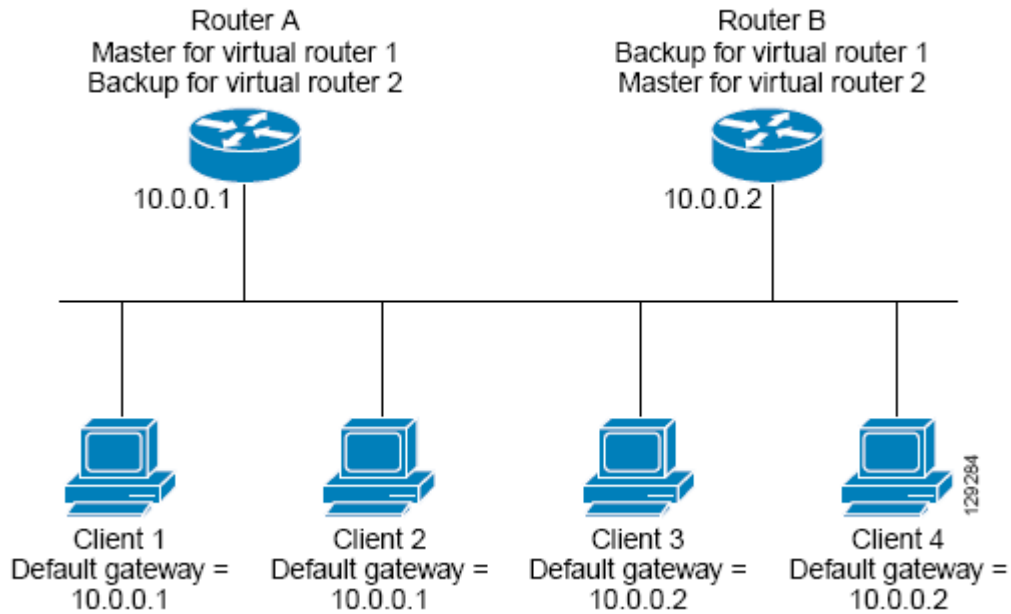


그림 17-2 Load Sharing and Redundancy VRRP Topology

이 형상에서 두 개의 가상 라우터가 설정된다. 가상 라우터 1에서 라우터 A가 IP 주소 10.0.0.1의 주인이자 마스터 가상 라우터이며, 라우터 B는 라우터 A에 대한 백업 가상 라우터이다. 클라이언트 1과 2는 default gateway의 IP 주소로 10.0.0.1을 사용한다.

가상 라우터 2에서 라우터 B가 IP 주소 10.0.0.2의 주인이자 마스터 가상 라우터이며, 라우터 A는 라우터 B에 대한 백업 가상 라우터이다. 클라이언트 3과 4는 default gateway의 IP 주소로 10.0.0.2를 사용한다.

## 17.1.2. VRRP Benefits

### Redundancy

VRRP는 default gateway 라우터로 여러 개의 라우터를 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 최대 255개의 가상 라우터 (VRRP 그룹)을 지원한다. 다수의 가상 라우터를 지원함으로써 LAN 구성에서 redundancy와 load sharing의 지원이 가능하다.

### Preemption

VRRP의 redundancy scheme은 높은 우선 순위의 라우터가 사용 가능하게 되었을 때, 백업 가상 라우터를 대신해서 마스터 가상 라우터가 되는 것을 허용한다.

### Advertisement Protocol

VRRP 는 전용의 Internet Assigned Numbers Authority (IANA) 표준 멀티캐스트 주소 (224.0.0.18)를 VRRP advertisement 에 사용한다. IANA 는 VRRP 에게 IP 프로토콜 번호 112 를 할당한다.

### VRRP Object Tracking

VRRP object tracking 은 인터페이스 또는 IP route 의 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 이중화 기능에서 중요한 요소는 VRRP 라우터 우선 순위이다. 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. **vrrp 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 **preemptive scheme** 가 적용 된다. **no vrrp preempt** 명령을 사용해서 **preemptive scheme** 를 중지시킬 수 있다. 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 를 전송한다. Advertisement 에는 마스터 가상 라우터의 우선 순위와 상태 정보가 포함된다. VRRP advertisement 는 IP 패킷으로 만들어져서, VRRP 그룹에 할당된 IPv4 멀티캐스트 주소로 전송된다. Default 로 매 1 초마다 advertisement 가 전송되며, 전송 주기는 설정 가능하다.

### 17.1.6. VRRP Object Tracking

Object tracking 은 인터페이스의 line-protocol 상태와 같은 객체를 생성하고 모니터링하며, 제거를 관리하는 독립된 프로세스이다. VRRP 와 같은 클라이언트는 상태의 변화를 알고 싶은 객체를 등록한다.

추적할 객체는 tracking comman-line-interface (CLI)에 의해 유일한 번호를 할당 받는다. VRRP 와 같은 클라이언트 프로세스는 이 번호를 사용해서 추적할 객체를 명시한다.

Tracking 프로세스는 주기적으로 객체의 상태를 검사하고 상태 값의 변화를 클라이언트에게 알려준다. 객체의 상태 값은 up 또는 down 으로 표시된다.

Tracking 프로세스를 통해 VRRP 는 모든 객체의 상태 변화를 추적할 수 있다. Tracking 프로세스는 인터페이스의 line protocol 상태, route 의 도달 가능성 등 각 객체의 상태 추적 기능을 제공한다.

각 VRRP 그룹은 VRRP 라우터의 우선 순위에 영향을 미치는 여러 객체를 추적할 수 있다. 추적할 객체 번호를 명시하면 VRRP 는 그 객체의 상태 변화를 감지하게 된다. VRRP 는 추적하는 객체의 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 on an Interface
- Configuring VRRP Object Tracking

### 17.2.1. Enabling VRRP

VRRP 를 작동시키려면 다음의 작업을 수행한다.

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  예제: Switch# <b>configure terminal</b>	Global configure 모드로 진입한다

Step 2	<b>interface</b> <i>interface-name</i>  예제: Switch(config)# <b>interface</b> <b>vlan1</b>	Interface configuration 모드로 진입한다.
Step 3	<b>ip address</b> <i>ip-address/prefix-length</i>  예제: Switch(config-if-vlan1)# <b>ip address</b> <b>172.16.6.5/24</b>	인터페이스에 IP 주소를 설정한다.
Step 4	<b>vrrp group</b> <b>ip address</b> <i>ip-address</i>  예제: Switch(config-if-vlan1)# <b>vrrp 10 ip 172.16.6.5</b>	인터페이스에 VRRP 를 작동시킨다.  <b>주의:</b> VRRP 그룹의 모든 라우터들은 같은 IP 주소로 설정해야 한다. 다른 IP 주소가 설정되면, VRRP 그룹의 라우터들은 서로 통신을 할 수 없게 되고, 잘못 설정된 라우터는 자신이 마스터로 동작한다.
Step 5	<b>end</b>  예제: Switch(config-if-vlan1)# <b>end</b>	privileged EXEC 모드로 돌아간다
Step 6	<b>show vrrp</b> [ <b>brief</b>   <b>group</b> ]  예제: Switch# <b>show vrrp 10</b>	(옵션) 라우터의 VRRP 그룹의 상태 정보를 조회한다.
Step 7	<b>show vrrp interface</b> <i>interface-name</i> [ <b>brief</b> ]  예제: Switch# <b>show vrrp interface</b> <b>vlan1</b>	(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	<b>configure terminal</b>  예제: Switch# <b>configure terminal</b>	Global configure 모드로 진입한다
Step 2	<b>interface</b> <i>interface-name</i>	Interface configuration 모드로 진입한다.

	예제: Switch(config)# <b>interface vlan1</b>	
Step 3	<b>ip address</b> <i>ip-address/prefix-length</i>  예제: Switch(config-if-vlan1)# <b>ip address 172.16.6.5/24</b>	인터페이스에 IP 주소를 설정한다.
Step 4	<b>vrrp group shutdown</b>  예제: Switch(config-if-vlan1)# <b>vrrp 10 shutdown</b>	인터페이스의 VRRP 를 중단시킨다.  주의: VRRP 설정은 유지한채 VRRP 를 중단시킬 수 있다.

### 17.2.3. Configuring VRRP Object Tracking

VRRP object tracking을 설정하려면 다음의 작업을 수행하라.

VRRP 그룹이 IP 주소의 소유주라면, VRRP 그룹의 우선 순위는 255 로 고정되고 object tracking 을 통해 우선 순위가 변경되지 않는다.

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  예제: Switch# <b>configure terminal</b>	Global configure 모드로 진입한다
Step 2	<b>track</b> <i>object-number</i> <b>interface</b> <i>interface-name</i> { <b>line-protocol</b>   <b>ip routing</b> }  예제: Switch(config)# <b>track 2 interface vlan1 line-protocol</b>	인터페이스의 상태가 VRRP 그룹의 우선 순위 에 영향을 미치는 인터페이스를 설정한다. - 이 명령으로 인터페이스를 설정하고 <b>vrrp track</b> 명령에서는 대응되는 object 번호가 사용된다. - <b>line-protocol</b> 키워드는 인터페이스의 상태가 up 인가를 추적한다. <b>ip routing</b> 키워드는 IP 주소가 설정되었고 인터페이스의 상태가 up 인가를 검사한다. - <b>track ip route</b> 명령을 사용해서 특정 IP route 의 도달성을 검사할 수도 있다.
Step 3	<b>interface</b> <i>interface-name</i>  예제: Switch(config)# <b>interface vlan10</b>	Interface configuration 모드로 진입한다.
Step 4	<b>ip address</b> <i>ip-address/prefix-length</i>  예제: Switch(config-if-vlan10)# <b>ip address 10.0.1.1/24</b>	인터페이스에 IP 주소를 설정한다.

Step 5	<b>vrrp group ip address</b> <i>ip-address</i>  예제: Switch(config-if-vlan10)# <b>vrrp 10 ip 10.0.1.20</b>	인터페이스에 VRRP 를 작동시키고 가상 라우터의 IP 주소를 설정한다.
Step 6	<b>vrrp group priority</b> <i>leve</i>  예제: Switch(config-if-vlan10)# <b>vrrp 10 priority 120</b>	VRRP 라우터의 우선 순위를 설정한다.
Step 7	<b>vrrp group track</b> <i>object-number</i> [ <b>decrement</b> <i>priority</i> ]  예제: Switch(config-if-vlan10)# <b>vrrp 10 track 2 decrement 15</b>	VRRP 가 object 의 상태를 추적하도록 설정한다.

## 17.3. Configuration Examples for VRRP

### 17.3.1. Configuring VRRP: Example

다음의 예제에서 스위치 A 와 스위치 B 는 3 개의 VRRP 그룹에 포함된다.

각 그룹의 설정은 다음과 같다:

- Group 1:
  - 가상 IP 주소는 10.1.0.10
  - 스위치 A 가 우선 순위 값 120 으로 이 그룹의 마스터가 된다
  - Advertising 주기는 3 초이다.
  - Preemption 이 활성화 되어 있다.
- Group 5:
  - 스위치 B 가 우선 순위 값 200 으로 이 그룹의 마스터가 된다.
  - Advertising 주기는 30 초이다.
  - Perrmption 이 활성화 되어 있다.
- Group 100:
  - 스위치 A 가 가장 높은 IP 주소 (10.1.0.2)를 가지고 있기 때문에, 이 그룹의 마스터가 된다.
  - Advertising 주기는 default 1 초이다.
  - Preemption 이 비활성화 되어 있다.

#### Router A

```
interface vlan1
  ip address 10.1.0.2/8
  vrrp 1 priority 120
  vrrp 1 timers advertise 3
  vrrp 1 ip 10.1.0.10
  vrrp 5 timer advertise 30
  vrrp 5 ip 10.1.0.50
  no vrrp 100 preempt
```



```
vrrp 100 ip 10.1.0.100
```

### Router B

```
interface vlan1
  ip address 10.1.0.1/8
  vrrp 1 timers advertise 3
  vrrp 1 ip 10.1.0.10
  vrrp 5 priority 200
  vrrp 5 timer advertise 30
  vrrp 5 ip 10.1.0.50
  no vrrp 100 preempt
  vrrp 100 ip 10.1.0.100
```

## 17.3.2. VRRP Object Tracking: Example

다음의 예제에서, 인터페이스 `vlan10`의 `line protocol` 상태를 추적하도록 `tracking` 프로세스가 설정된다. 인터페이스 `vlan1`의 VRRP는 인터페이스 `vlan10`의 프로토콜 상태 변환에 대한 정보를 전달받을 수 있도록 `tracking` 프로세스에 등록한다. 인터페이스 `vlan10`의 `line protocol` 상태가 `down`이 되면, VRRP 그룹의 우선 순위 값이 15만큼 감소한다.

```
track 1 interface vlan10 line-protocol
!
interface vlan1
  ip address 10.0.0.2/8
  vrrp 1 ip 10.0.0.3
  vrrp 1 priority 120
  vrrp 1 track 1 decrement 15
```

## 17.3.3. VRRP Object Tracking Verification: Example

다음의 예제는 “VRRP Object Tracking: Example” 절에서의 설정을 확인한다:

```
Switch# show vrrp
```

```
vlan1 – Group 1
  State is Master
  Virtual IP address is 10.0.0.3
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1 sec
  Preemption is enabled
  Priority is 105
  Track object 1 state Down decrement 15
  Master Router is 10.0.0.2 (local) priority is 105
  Master Advertisement interval is 1 sec
  Master Down interval is 3.531 sec
```

Switch# **show track**

Track 1

Interface vlan10 line-protocol

Line protocol is Down (hw down)

1 change, last change 00:06:53

Tracked by:

VRRP vlan1 1

### 17.3.4. Disabling a VRRP Group on an Interface: Example

다음의 예는 인터페이스 VRRP 그룹의 설정을 유지하면서 인터페이스 vlan1의 VRRP 그룹을 중지시키는 방법을 보여준다:

```
interface vlan1
```

```
ip address 10.24.1.1/24
```

```
vrrp1 ip 10.24.1.254
```

```
vrrp 1 shutdown
```

## 18

## Setting Time and Calendar

U9200 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

U9200 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 두 개의 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. NTP는 이 시간 정보를 네트워크를 통해 분배한다. NTP는 두 시스템 사이에 밀리초 단위의 시간 동기화를 맞추

는데 분당 하나의 패킷을 사용할 정도로 매우 효과적인 프로토콜이다.

NTP는 권위있는 타임 소스로까지 얼마나 많은 NTP “hops”이 존재하는지를 나타내는 “stratum”이란 개념을 사용한다. 일반적으로 “stratum 1” 타임 서버에는 권위있는 타임 소스가 직접 연결되어 있다. “stratum 2” 타임 서버는 “stratum 1” 타임 서버로부터 NTP를 통해 시간 정보를 수신한다. NTP는 사용할 수 있는 타임 서버중 가장 작은 stratum을 가진 타임 서버를 자신의 시간 소스로 선택한다.

NTP는 의심스러운 시간 정보로 동기화를 하지 않기 위해 다음 두 가지 방법을 제공한다.

- NTP는 자신을 소스로 동기화한 장비와는 동기화하지 않는다.
- NTP는 여러 장비에서 얻은 시간을 비교하고 다른 것과 큰 시간차를 보이는 장비와는 stratum이 작아도 동기화하지 않는다.

### 18.1.2. Hardware Clock

U9200 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 NTP를 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

NTP를 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

Client와 Symmetric active 모드는 NTP에 높은 수준의 시간 정밀도가 요구될 때 사용된다.

클라이언트 모드에서 장비는 현재 시간 정보를 얻기 위해 설정된 시간 서버들을 조사한다. 장비는 조

사된 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)# <b>ntp server</b> <i>ip-adress</i>	Client 모드로 NTP 설정
Switch(config)# <b>ntp peer</b> <i>ip-adress</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)# <b>ntp authenticate</b>	<b>NTP</b> 의 인증 기능을 활성화 시킨다.
Step 2	Switch(config)# <b>ntp authentication-key</b> <i>key-number</i> <b>md5</b> <i>value</i>	인증 키를 정의한다. 각 키는 키 번호와 종류 그리고 값을 가진다. 현재 지원되는 키 종류는 <b>MD5</b> 이다.
Step 3	Switch(config)# <b>ntp trusted-key</b> <i>key-number</i>	신뢰하는 인증 키를 정의한다. 만약 인증키가 신뢰하는 키라면, 시스템은 <b>NTP</b>

Step 4		패킷에 이 키를 사용하는 시스템과 시간 동기를 시도한다.
	Switch(config)# <b>ntp server</b> <i>ip-address</i> <b>key</b> <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)# <b>ntp source</b> <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)# <b>ntp master</b> [ <i>stratum</i> ]	시스템을 NTP 서버로 설정한다.

U9200 시리즈 스위치는 **stratum 1** 서비스를 지원한다. 하지만 장비 내부에 연결 가능한 라디오 혹은 원자 클락이 존재하지는 않으므로 U9200 시리즈 스위치를 **stratum 1** 로 설정하는 것은 권장하지 않는다.

### 18.2.5. Updating the Hardware Clock

하드웨어 클락을 가진 장비에서, 소프트웨어 클락으로 하드웨어 클락을 주기적으로 업데이트 하도록 설정할 수 있다. NTP 로 설정되는 소프트웨어 클락이 하드웨어 클락보다 더 정확하기 때문에 NTP 를 사용하는 장비에서는 이렇게 설정하는 것이 바람직하다.

하드웨어 클락을 NTP 시각과 동기화시키려면 글로벌 설정 모드에서 다음의 명령을 사용하라:

Command	Purpose
Switch(config)# <b>ntp update-calendar</b>	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)# <b>clock timezone</b> zone hours-offset [minutes-offset]	시간대를 설정한다. 인자 <b>zone</b> 은 시간대의 이름을 표시한다 (보통 표준 시간대 이름을 사용). 인자 <b>hours-offset</b> 은 UTC 와의 시차를 명시한다. 인자 <b>minutes-offset</b> 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)# <b>clock summer-time</b> zone <b>recurring</b> [week day month hh:mm week day month hh:mm [offset]]	반복되는 서머타임의 시작과 끝을 설정. 인자 <b>offset</b> 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)# <b>clock summer-time</b> zone <b>date</b> month date year hh:mm month date year hh:mm [offset]	특정 서머타임의 시작과 끝을 설정. 인자 <b>offset</b> 은 서머 타임 동안 추가되는 분을 표시한다.
또는	
Switch(config)# <b>clock summer-time</b> zone <b>date</b> 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# <b>clock set</b> <i>hh:mm:ss day month year</i>	소프트웨어 클럭 설정.
또는	
Switch# <b>clock set</b> <i>hh:mm:ss month day year</i>	

## 18.4. Using the Hardware Clock

U9200 시리즈 스위치는 소프트웨어 기반의 클럭과는 독립된 하드웨어 기반의 클럭을 추가로 가지고 있다. 하드웨어 클럭은 충전이 가능한 배터리를 가진 칩(chip)으로 장비가 리부트 되더라도 시각 정보를 유지할 수 있다.

소프트웨어 클럭은 정확한 시각 정보를 유지하기 위해 네트워크의 권위있는 타임 소스로부터의 시간 업데이트 정보를 수신해야 한다. 그리고 시스템이 동작중인 동안 소프트웨어 클럭은 하드웨어 클럭을 주기적으로 업데이트 해줘야 한다.

하드웨어 클럭을 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 클럭은 소프트웨어 클럭과 별도로 시간을 관리한다. 하드웨어 클럭은 시스템이 재시작되거나 전원이 꺼진 상태에서도 계속 동작한다. 일반적으로 하드웨어 클럭은 시스템이 설치될 때 한 번만 설정하면 된다.

믿을 수 있는 외부 시간 소스를 사용하고 있다면 하드웨어 클럭을 직접 설정하지 않도록 한다. 시간 동기화는 NTP 를 이용해서 이뤄질 것이다.

만약 사용할 수 있는 외부 시간 소스가 없다면 하드웨어 클럭을 설정하기 위해 EXEC 모드에서 다음의 명령을 사용하라:

Command	Purpose
Switch# <b>calendar set</b> <i>hh:mm:ss day month year</i>	하드웨어 클럭 설정.
또는	
Switch# <b>calendar set</b> <i>hh:mm:ss month day year</i>	

### 18.4.2. Setting the Software Clock from the Hardware Clock

새로운 하드웨어 클럭 설정으로 소프트웨어 클럭을 설정하려면, EXEC 모드에서 다음의 명령을 사용



하라:

Command	Purpose
Switch# <b>clock read-calendar</b>	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# <b>clock update-calendar</b>	소프트웨어 클락으로 하드웨어 클락 설정.

## 18.5. Monitoring Time and Calendar Services

클락, 카렌더 그리고 NTP 정보를 조회하려면 다음의 명령들을 사용하라.

Command	Purpose
Switch# <b>show calendar</b>	현재 하드웨어 클락 조회
Switch# <b>show clock</b>	현재 소프트웨어 클락 조회
Switch# <b>show ntp associations [detail]</b>	NTP association 상태 조회
Switch# <b>show ntp status</b>	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

U9200-DAI-2

마지막 수정 날짜: 2010-02-17

적용가능 장비: U9200 series

이 장에서는 ARP 패킷을 검사하는 dynamic Address Resolution Protocol (ARP) inspection (DAI) 기능에 대한 설정 방법을 설명한다.

**Notice**

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)

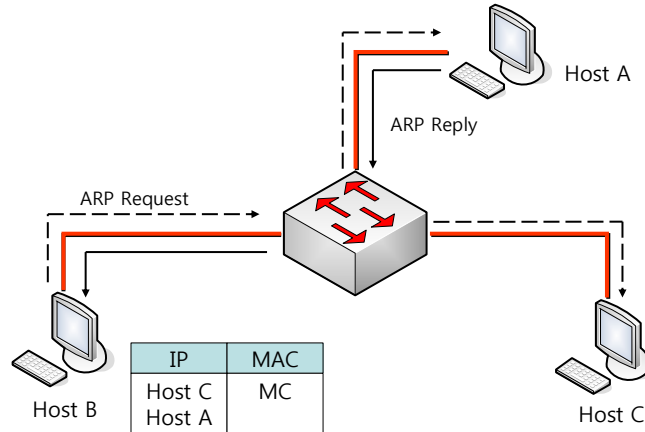
## 19.1. Understanding DAI

이 절에서는 DAI 에 대한 설명과 DAI 기능을 사용해서 ARP spoofing 공격<sup>attack</sup> 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 <sup>mapping</sup> 해서 Layer 2 브로드캐스트 <sup>broadcast</sup> 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.

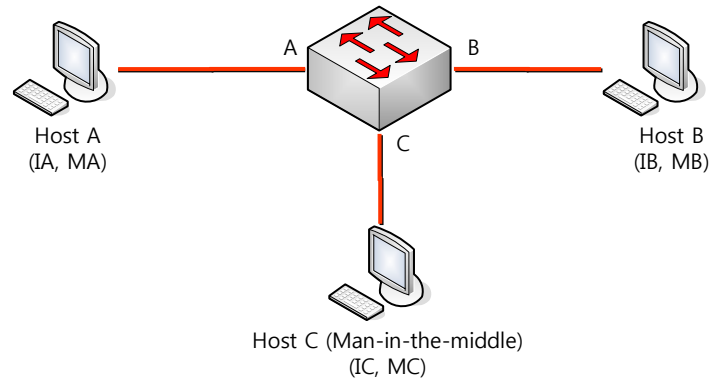


호스트 B 는 호스트 A 의 IP 주소에 대응하는 MAC 주소를 알아내기 위해서, 브로드캐스트 도메인 내부의 모든 호스트들에게 브로드캐스트 메시지 (ARP request)를 전송한다. 브로드캐스트 도메인 내부의 모든 호스트들은 호스트 B 가 전송한 ARP request 를 수신하고, 호스트 A 는 자신의 MAC 주소를 응답한다.

### 19.1.2. Understanding ARP Spoofing Attacks

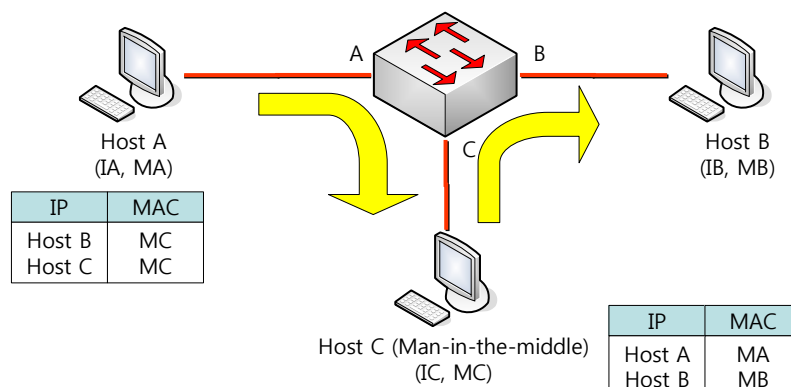
ARP 는 ARP request 를 수신하지 않은 호스트가 전송한 gratuitous reply 로 ARP 테이블이 변경되는 것을 허용한다. 이로 인해 ARP spoofing 공격과 ARP cache poisoning 이 발생할 수 있다. 공격 이후에는 공격 당한 장비의 모든 트래픽은 공격자의 컴퓨터를 통해 라우터, 스위치 또는 호스트로 전달된다.

ARP spoofing 공격은 Layer 2 네트워크에 연결된 호스트, 스위치, 라우터의 ARP 캐시 <sup>cache</sup> 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 형상을 *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 가

진 ARP 패킷을 로깅 <sup>logging</sup> 하고, 폐기 <sup>drop</sup> 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 <sup>database</sup> 인 DHCP snooping binding 데이터베이스에 저장된 IP-to-MAC 주소 binding 을 사용한다.



#### Notice

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 운영자가 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 <sup>state</sup> 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 패킷은 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.

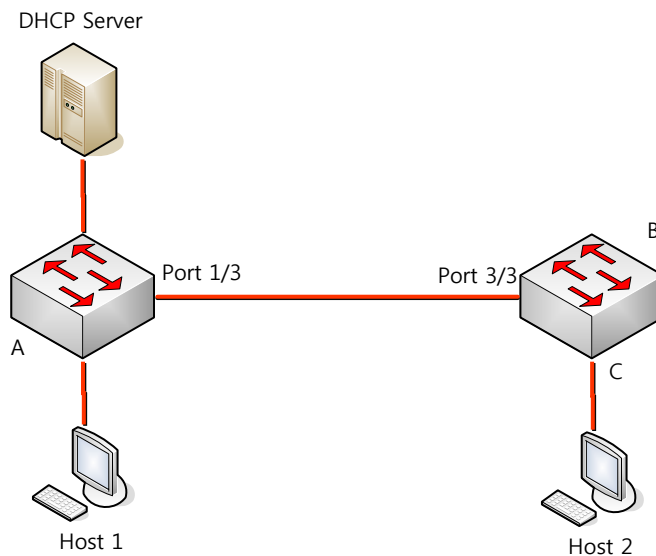


### Caution

네트워크 보안을 위해 스위치가 모든 ARP 패킷을 검사하도록 하려면, 특별한 기능이 필요하다. 즉, DAI 가 스위치의 포워딩 엔진 <sup>forwarding engine</sup> 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 <sup>server</sup> 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 실행 중인 스위치에서 ARP ACLs 를 설정하라. 이런 설정이 불가능하다면, Layer 3 에서 DAI 를 사용 중인 스위치와 사용하지 않는 스위치를 분리해야 한다.

**Notice**

U9200 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.

**Notice**

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 VLAN 에 대해 비활성 상태이다.
Interface trust state	모든 인터페이스들은 untrusted 상태이다.
Rate limit of incoming ARP packets	초당 15 개의 새로운 호스트가 등록되는 Layer 2 네트워크라 가정하고, untrusted 인터페이스에 대해 15 pps 로 설정된다. Trusted 인터페이스에 대해서는 rate 를 제한하지 않는다. burst interval 은 1 초이다. 인터페이스의 rate limit 기능은 disable 되어 있다.
ARP ACLs for non-DHCP environments	ARP ACLs 은 정의되어 있지 않다.
Validation checks	어떤 검사도 수행하지 않는다.
Log buffer	DAI 가 활성화되면, deny 되거나 drop 되는 모든 ARP 패킷 정보가 로깅된다. log entry 의 개수는 32 개. 생성되는 시스템 메시지의 개수는 초당 5 개. logging-rate 주기는 1 초.
Per-VLAN logging	deny 되거나 drop 되는 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<sup>Ingress security</sup> 기능이다; 출구 검사<sup>Egress check</sup>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# <b>configure terminal</b>	global 설정 모드로 진입한다.
Switch(config)# <b>ip arp inspection vlan</b> <i>vlan-id</i>	VLAN 에 DAI 를 enable 한다.
Switch(config)# <b>no ip arp inspection vlan</b> <i>vlan-id</i>	VLAN 에 DAI 를 disable 한다.
Switch# <b>show ip arp inspection</b>	설정을 확인한다.



#### Notice

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 arp_trap_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# <b>configure terminal</b>	global 설정 모드로 진입한다.
Switch(config)# <b>interface ifname</b>	다른 스위치와 연결된 인터페이스를 명시하고, 인터페이스 설정 모드로 진입한다.
Switch(config-if-Giga1/1)# <b>ip arp inspection trust</b>	스위치와 연결된 인터페이스를 trusted 로 설정한다. (default: untrusted)
Switch(config-if-Giga1/1)# <b>no ip arp inspection trust</b>	스위치와 연결된 인터페이스를 untrusted 로 설정한다.
Switch(config-if-Giga1/1)# <b>end</b>	Enable 모드로 돌아간다.
Switch# <b>show ip arp inspection interfaces</b>	설정을 확인한다.

다음의 예는 Gigabit 포트 1/1 을 trusted 로 설정하는 방법을 보여준다:

```
Switch# configure terminal
Switch(config)# interface gi1/1
Switch(config-if-Giga1/1)# ip arp inspection trust
Switch(config-if-Giga1/1)# end
Switch# show ip arp inspection interfaces
Interface           Trust State  Rate (pps)  Burst Interval  Auto Recovery
-----
Giga1/1             Trusted      None        1              Disabled
```

## 19.4.3. Applying ARP ACLs for DAI Filtering

ARP ACL 을 사용하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# <b>configure terminal</b>	global 설정으로 진입한다.
Switch(config)# <b>ip arp inspection filter arp_acl_name vlan vlan-id [static]</b>	VLAN 에 ARP ACL 을 적용한다.

Switch(config)# <b>end</b>	Enable 모드로 돌아간다.
Switch# <b>show ip arp inspection</b>	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.



##### Notice

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# <b>configure terminal</b>	global 설정으로 진입한다.
Switch(config)# <b>interface</b> <i>ifname</i>	다른 스위치와 연결된 인터페이스를 명시하고, 인터페이스 설정 모드로 진입한다.
Switch(config-if-Giga1/1)# <b>ip arp inspection limit {rate pps [burst interval seconds]   none}</b> Switch(config-if-Giga1/1)# <b>no ip arp inspection limit</b>	(옵션) ARP packet rate limit 를 설정한다.  default 설정으로 복원한다.
Switch(config-if-Giga1/1)# <b>ip arp inspection limit enable</b> Switch(config-if-Giga1/1)# <b>no ip arp inspection limit enable</b>	인터페이스의 ARP rate limit 기능을 enable 시킨다. 인터페이스의 ARP rate limit 기능을 disable 시킨다.
Switch(config)# <b>end</b>	Enable 모드로 돌아간다.
Switch# <b>show ip arp inspection interfaces</b>	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 포트로 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 에 ARP packet rate limit 를 설정하는 예이다:

```
Switch# configure terminal
Switch(config)# interface gi1/1
Switch(config-if-Giga1/1)# ip arp inspection limit rate 20 burst interval 2
Switch(config-if-Giga1/1)# ip arp inspection limit enable
Switch(config-if-Giga1/1)# end
Switch# show ip arp inspection interfaces
```

Interface	Trust State	Rate (pps)	Burst Interval	Auto Recovery
-----	-----	-----	-----	-----

Giga1/1      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# <b>configure terminal</b>	global 설정 모드로 진입한다.
Switch(config)# <b>interface ifname</b>	다른 스위치와 연결된 인터페이스를 명시하고, 인터페이스 설정 모드로 진입한다.
Switch(config-if-Giga1/1)# <b>ip arp inspection limit auto-recovery seconds</b>	(옵션) 자동 복구 기능을 활성화 시킨다.
Switch(config)# <b>no ip arp inspection limit auto-recovery</b>	자동 복구 기능을 해제한다.
Switch(config)# <b>end</b>	Enable 모드로 돌아간다.
Switch# <b>show ip arp inspection interfaces</b>	설정을 확인한다.

다음은 인터페이스 gi1/1 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
Switch(config-if-Giga1/1)# ip arp inspection limit auto-recovery 10
Switch(config-if-Giga1/1)# ip arp inspection limit enable
Switch(config-if-Giga1/1)# end
Switch# show ip arp inspection interfaces
```

Interface	Trust State	Rate (pps)	Burst Interval	Auto Recovery
gi1/1	Untrusted	20	2	10
gi1/2	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# <b>configure terminal</b>	global 설정 모드로 진입한다.
Switch(config)# <b>ip arp inspection validate</b>	(옵션) 추가적인 유효성 검사를 enable 한다.

{dst-mac   ip   src-mac} Switch(config)# no ip arp inspection validate {dst-mac   ip   src-mac}	(default: none) 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

### 19.4.8. 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.

### 19.4.9. Configuring the DAI Logging Buffer Size

DAI 로그 버퍼의 크기를 설정하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# <b>configure terminal</b>	global 설정 모드로 진입한다.
Switch(config)# <b>ip arp inspection log-buffer entries number</b>	DAI의 로그 버퍼 크기를 설정한다. (범위는 0 ~ 1024).
Switch(config)# <b>no ip arp inspection log-buffer entries</b>	default 버퍼 크기로 복원한다. (32)
Switch(config)# <b>end</b>	Enable 모드로 돌아간다.
Switch# <b>show ip arp inspection log</b>	설정을 확인한다.

다음의 예는 DAI의 로그 버퍼 크기를 64개로 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.
```

## 19.4.10. Configuring the DAI Logging System Messages

DAI 가 생성하는 로그 메시지를 설정하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# <b>configure terminal</b>	global 설정 모드로 진입한다.
Switch(config)# <b>ip arp inspection log-buffer logs <i>number_of_messges</i> interval <i>length_in_seconds</i></b>	DAI 로그 버퍼를 설정한다.
Switch(config)# <b>no ip arp inspection log-buffer logs</b>	default 로 복원한다.
Switch(config)# <b>end</b>	Enable 모드로 돌아간다.
Switch# <b>show ip arp inspection log</b>	설정을 확인한다.

DAI 의 로깅 시스템 메시지를 설정하려면, 다음의 사항에 유의하라:

- **logs *number\_of\_messges*** (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.
```

## 19.4.11. Configuring the DAI Log Filtering

ARP 패킷을 검사한 후, 그 결과에 대한 시스템 메시지를 선택적으로 생성할 수 있다.

DAI 의 log filtering 기능을 설정하려면, 다음의 작업을 수행하라:

Command	Purpose
Switch# <b>configure terminal</b>	global 설정 모드로 진입한다.
Switch(config)# <b>ip arp inspection vlan</b> <i>vlan-id</i> { <b>acl-match</b> { <b>matchlog</b>   <b>none</b> }   <b>dhcp-bindings</b> { <b>all</b>   <b>none</b>   <b>permit</b> }}	각 VLAN에 대해 log filtering을 설정한다.
Switch(config)# <b>end</b>	Enable 모드로 돌아간다.
Switch# <b>show running-config</b>	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

## 19.4.12. Displaying DAI Information

DAI의 정보를 조회하려면, 다음의 명령을 사용하라:

Command	Description
---------	-------------

show arp access-list	ARP ACL 에 대한 정보를 출력한다.
show ip arp inspection interfaces	인터페이스의 trust 상태 정보를 출력한다.
show ip arp inspection vlan [vlan-id]	VLAN 에 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]	DAI 가 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.

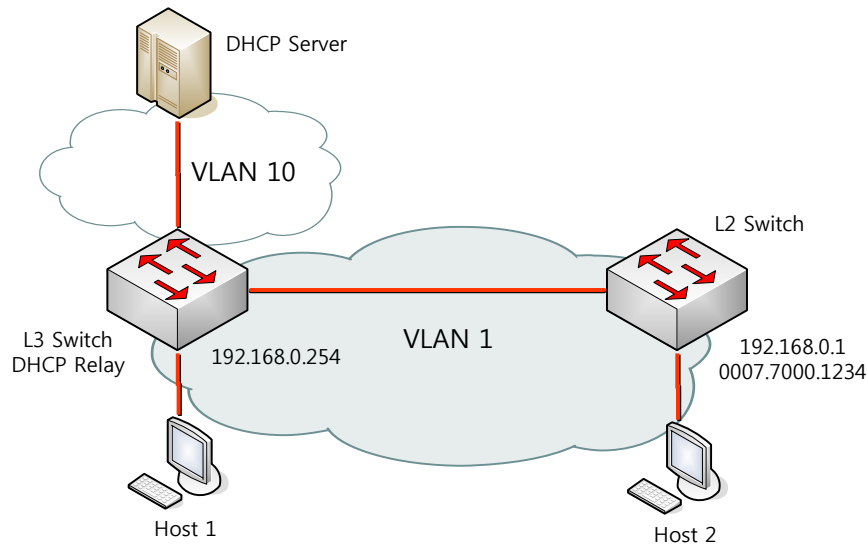
## 19.5. DAI Configuration Samples

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.



#### Notice

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

## QoS 및 ACL

본 장은 현재 운영중인 U9200 Series 스위치의 QoS (Quality of Service) 설정 및 ACL (access-list) 설정에 대해서 다룬다.

### 20.1. QoS

#### 20.1.1. 전역 설정

본 장비의 qos 에 대한 전역 설정을 활성화 시키는 명령어는 다음과 같다.

표 20-1. QoS 전역 설정 명령어

명령어	설명	모드
<b>mls qos</b>	QoS 전역 설정을 활성화 한다.	Config
<b>no mls qos</b>	QoS 전역 설정을 비활성화 한다.	Config
<b>show mls qos</b>	QoS 전역 설정 상태를 조회한다	Exec

U9200 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.

#### 20.1.2. TX Scheduling 설정

U9200 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 방식으로 동작하며, 모듈당 7 개 의 map 을 적용해서 사용할 수 있다. 실제로는 총 8 개의 map 을 설정할 수 있으나, 0 번은 default SPQ 로 사용되며 변경이 불가능하므로, 운용자가 설정할 수 있는 것은 7 개



이다.

표 20-2. Tx-scheduling map 설정 명령어

명령어	설명	모드
<b>mls qos map tx-scheduling NAME queueing-method &lt;0-7&gt; (strict wrr1 wrr2)</b>	해당 이름을 가지는 mapping table 의 n 번째 큐에 대한 queueing-method 를 설정한다. 해당 이름을 가지는 mapping table 이 없는 경우에는 새로 생성한다.	Config
<b>mls qos map tx-scheduling NAME queueing-method &lt;0-7&gt; (wrr1 wrr2) &lt;1-100&gt;</b>	wrr1 또는 wrr2 를 설정할 경우는 wrr weight 를 동시에 설정이 가능하다. Weight 값이 주어지지 않으면 1 로 설정된다.	Config
<b>mls qos map tx-scheduling NAME wrr-weight &lt;0-7&gt; &lt;1-100&gt;</b>	Wrr 로 설정된 큐의 weight 를 설정한다.	Config
<b>no mls qos map tx-scheduling NAME queueing-method &lt;0-7&gt;</b>	해당 큐의 queueing-method 를 해제한다. 해제할 경우 디폴트인 strict 로 바뀐다.	Config
<b>no mls qos map tx-scheduling NAME wrr-weight &lt;0-7&gt;</b>	Wrr 로 설정된 큐의 weight 를 해제한다. 디폴트인 1 로 설정된다.	Config
<b>no mls qos map tx-scheduling NAME</b>	해당 이름을 가지는 mapping table 을 삭제한다.	Config
<b>show mls qos map tx-scheduling</b>	Tx-scheduling 설정 정보를 보여준다.	Exec

위와 같이 만들어진 tx-scheduling 에 대한 mapping table 을 원하는 포트에 다음과 같이 설정하여 사용한다.

표 20-3. Tx-scheduling 설정 명령어

명령어	설명	모드
<b>mls qos tx-scheduling NAME</b>	해당 이름을 가지는 mapping table 을 해당 포트 인터페이스에 설정한다.	interface
<b>no mls qos tx-scheduling NAME</b>	해당 이름을 가지는 mapping table 을 해당 포트 인터페이스에서 해제한다.	interface

### 20.1.3. Port trust 모드

포트에 인입되는 트래픽에 대해서 QOS 를 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 없

는 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 20-4. port trust 설정 명령어

명령어	설명	모드
<b>mls qos trust (cos dscp both)</b>	해당 포트 인터페이스에 trust mode 를 설정한다.	interface
<b>no mls qos trust</b>	해당 포트 인터페이스에 trust mode 를 해제한다. 이 경우 none 으로 설정된다.	interface
<b>mls qos cos &lt;0-7&gt;</b>	포트의 디폴트 cos 값을 설정	interface
<b>no mls qos cos</b>	포트의 디폴트 cos 값 설정을 해제함.	interface

## 20.1.4. 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

### 20.1.4.1. 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    1    1
1 :      1    1    1    1    1    1    2    2    2    2
2 :      2    2    2    2    3    3    3    3    3    3
3 :      3    3    4    4    4    4    4    4    4    4
4 :      5    5    5    5    5    5    5    5    6    6
5 :      6    6    6    6    6    6    7    7    7    7
6 :      7    7    7    7
```

표 20-5. dscp-queue map 설정 명령어

명령어	설명	모드
<b>mls qos map dscp-queue &lt;0-63&gt; ... &lt;0-63&gt; to &lt;0-7&gt;</b>	Dscp-queue map 을 설정한다.	config
<b>no mls qos map dscp-queue</b>	Dscp-queue map 을 초기화 한다..	config
<b>show mls qos map dscp-queue</b>	현재 dscp-queue map 설정을 보여준다.	Exec

#### 20.1.4.2. 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    1    1
1 :      1    1    1    1    1    1    2    2    2    2
2 :      2    2    2    2    3    3    3    3    3    3
3 :      3    3    4    4    4    4    4    4    4    4
4 :      5    5    5    5    5    5    5    5    6    6
5 :      6    6    6    6    6    6    7    7    7    7
6 :      7    7    7    7
```

표 20-6. dscp-cos map 설정 명령어

명령어	설명	모드
<b>mls qos map dscp-cos &lt;0-63&gt; ... &lt;0-63&gt; to &lt;0-7&gt;</b>	Dscp-cos map 을 설정한다.	config
<b>no mls qos map dscp-cos</b>	Dscp-cos map 을 초기화 한다..	config
<b>mls qos dscp-cos</b>	해당 포트 인터페이스에 dscp-cos marking 을 수행하도록 설정한다.	interface
<b>no mls qos dscp-cos</b>	해당 포트 인터페이스에 dscp-cos marking 을 수행하지 않도록 설정한다.	interface
<b>show mls qos map dscp-cos</b>	현재 dscp-cos map 설정을 보여준다.	Exec

#### 20.1.4.3. 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 20-7. dscp-mutation map 설정 명령어

명령어	설명	모드
<b>mls qos map dscp-mutation &lt;0-63&gt; ... &lt;0-63&gt; to &lt;0-63&gt;</b>	Dscp-mutation map 을 설정한다.	config
<b>no mls qos map dscp-mutation</b>	Dscp-mutation map 을 초기화 한다..	config
<b>mls qos dscp-mutation</b>	해당 포트 인터페이스에 dscp remarking 을 수행하도록 설정한다.	interface
<b>no mls qos dscp-mutation</b>	해당 포트 인터페이스에 dscp remarking 을 수행하지 않도록 설정한다.	interface

show mls qos map dscp-mutation	현재 dscp-mutation map 설정을 보여준다.	Exec
--------------------------------	--------------------------------	------

### 20.1.5. 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

#### 20.1.5.1. 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 20-8. 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

#### 20.1.5.2. 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 20-9. cos-dscp map 설정 명령어

명령어	설명	모드
<b>mls qos map cos-dscp &lt;0-7&gt; &lt;0-63&gt;</b>	Cos-dscp map 을 설정한다.	config
<b>no mls qos map cos-dscp</b>	Cos-Dscp map 을 초기화 한다..	config
<b>mls qos cos-dscp</b>	해당 포트 인터페이스에 cos-dscp marking 을 수행하도록 설정한다.	interface
<b>no mls qos cos-dscp</b>	해당 포트 인터페이스에 cos-dscp marking 을 수행하지 않도록 설정한다.	interface
<b>show mls qos map cos-dscp</b>	현재 cos-dscp map 설정을 보여준다.	Exec

### 20.1.5.3. 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 20-10. cos-mutation map 설정 명령어

명령어	설명	모드
<b>mls qos map cos-mutation &lt;0-7&gt; &lt;0-7&gt;</b>	Cos-mutation map 을 설정한다.	config
<b>no mls qos map cos-mutation</b>	Cos-mutation map 을 초기화 한다..	config
<b>mls qos cos-mutation</b>	해당 포트 인터페이스에 cosremarking 을 수행하도록 설정한다.	interface
<b>no mls qos cos-mutation</b>	해당 포트 인터페이스에 cos remarking 을 수행	interface

	하지 않도록 설정한다.	
<b>show mls qos map cos-mutation</b>	현재 cos-mutation map 설정을 보여준다.	Exec

## 20.2. ACL 설정

U9200 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.

### 20.2.1. 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 20-11. standard IP ACL 설정 명령어

명령어	설명	모드
<b>access-list &lt;1-99&gt; (permit deny) SRC_IP_ADDRESS</b>	Standard IP ACL 을 설정한다.	config
<b>no access-list &lt;1-99&gt; (permit deny) SRC_IP_ADDRESS</b>	Standard IP ACL 을 해제한다.	config
<b>no access-list &lt;1-99&gt;</b>	해당 이름(번호)를 가지는 ACL 전부를 삭제한다.	config
<b>access-list &lt;1-99&gt; remark LINE</b>	해당 ACL 에 대한 설명을 추가한다.	config

<b>access-list &lt;1300-1999&gt; (permit deny) SRC_IP_ADDRESS</b>	Expanded range 의 Standard IP ACL 을 설정한다.	config
<b>no access-list &lt;1300-1999&gt; (permit deny) SRC_IP_ADDRESS</b>	Expanded range 의 Standard IP ACL 을 해제한다.	config
<b>no access-list &lt;1300-1999&gt;</b>	해당 번호를 가지는 ACL 전부를 삭제한다.	config
<b>access-list &lt;1300-1999&gt; remark LINE</b>	해당 ACL 에 대한 설명을 추가한다.	config
<b>access-list standard WORD (permit deny) SRC_IP_ADDRESS</b>	Named Standard IP ACL 을 설정한다.	config
<b>no access-list standard WORD (permit deny) SRC_IP_ADDRESS</b>	Named Standard IP ACL 을 해제한다.	config
<b>no access-list standard WORD</b>	해당 이름을 가지는 ACL 전부를 삭제한다.	config
<b>access-list WORD remark LINE</b>	해당 ACL 에 대한 설명을 추가한다.	config
<b>Show access-list</b>	ACL 설정을 조회한다	Exed

위 명령어중에서 **SRC\_IP\_ADDRESS** 는 다음과 같은 방법으로 설정할 수 있다.

<b>A.B.C.D A.B.C.D</b>	IP 대역을 wildcard 형태로 설정이 가능하다. 일반적인 IP 설정과는 반대로 <b>masking</b> 되는 부분이 <b>0</b> 이다.
<b>host A.B.C.D</b>	단 하나의 IP 주소만을 가르킬때는 <b>host prefix</b> 를 붙여서 사용한다.
<b>A.B.C.D</b>	하나의 IP 만 주어진 경우는 <b>host A.B.C.D</b> 과 동일하게 처리된다.
<b>any</b>	모든 IP 주소를 지정하는 경우는 <b>any</b> 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.

## 20.2.2. 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 20-12. extended IP ACL 설정 명령어

명령어	설명	모드
<b>access-list &lt;100-199&gt; (permit deny) &lt;0-255&gt; icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS</b>	Extended IP ACL 을 설정한다.	config
<b>access-list &lt;100-199&gt; (permit deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE</b>	ICMP type 의 Extended IP ACL 을 설정한다.	config
<b>access-list &lt;100-199&gt; (permit deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE</b>	IGMP type 의 Extended IP ACL 을 설정한다.	config
<b>access-list &lt;100-199&gt; (permit deny) (tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS eq &lt;0-65536&gt;</b>	TCP / UDP type 의 Extended IP ACL 을 설정한다.	config
<b>no access-list &lt;100-199&gt; (permit deny) &lt;0-255&gt; icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS</b>	Extended IP ACL 을 해제한다.	config
<b>no access-list &lt;100-199&gt;</b>	해당 이름(번호)를 가지는 ACL 전부를 삭제한다.	config
<b>access-list &lt;100-199&gt; remark LINE</b>	해당 ACL 에 대한 설명을 추가한다.	config
<b>access-list &lt;2000-2699&gt; (permit deny) &lt;0-255&gt; icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS</b>	Expanded range 의 Extended IP ACL 을 설정한다.	config
<b>access-list &lt;2000-2699&gt; (permit deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE</b>	ICMP type 의 Expanded range 의 Extended IP ACL 을 설정한다.	config
<b>access-list &lt;2000-2699&gt; (permit deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE</b>	IGMP type 의 Expanded range 의 Extended IP ACL 을 설정한다.	config
<b>access-list &lt;2000-2699&gt; (permit deny) (tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS eq &lt;0-65536&gt;</b>	TCP / UDP type 의 Expanded range 의 Extended IP ACL 을 설정한다.	config
<b>no access-list &lt;2000-2699&gt; (permit deny) &lt;0-255&gt; icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS</b>	Extended IP ACL 을 해제한다.	config
<b>no access-list &lt;2000-2699&gt;</b>	해당 이름(번호)를 가지는 ACL 전부를 삭제한다.	config
<b>access-list &lt;2000-2699&gt; remark LINE</b>	해당 ACL 에 대한 설명을 추가한다.	config
<b>access-list extended WORD (permit deny) &lt;0-255&gt; icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS</b>	Named Extended IP ACL 을 설정한다.	config
<b>access-list extended WORD (permit deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE</b>	ICMP type 의 Extended IP ACL 을 설정한다.	config
<b>access-list extended WORD (permit deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE</b>	IGMP type 의 Extended IP ACL 을 설정한다.	config

<b>no access-list extended WORD (permit deny)</b> <b>(&lt;0-255&gt; icmp igmp ip ospf pim tcp udp)</b> <b>SRC_IP_ADDRESS DST_IP_ADDRESS</b>	Named Extended IP ACL 을 해제한다.	config
<b>no access-list extended WORD</b>	해당 이름을 가지는 ACL 전부를 삭제한다.	config
<b>access-list WORD remark LINE</b>	해당 ACL 에 대한 설명을 추가한다.	config
<b>Show access-list</b>	ACL 설정을 조회한다	Exec

위 명령어중에서 **SRC\_IP\_ADDRESS** 와 **DST\_IP\_ADDRESS** 다음과 같은 방법으로 설정할 수 있다.

<b>A.B.C.D A.B.C.D</b>	IP 대역을 wildcard 형태로 설정이 가능하다. 일반적인 IP 설정과는 반대로 masking 되는 부분이 0 이다.
<b>host A.B.C.D</b>	단 하나의 IP 주소만을 가르킬때는 host prefix 를 붙여서 사용한다.
<b>any</b>	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.

### 20.2.3. 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 20-13. standard IP ACL 설정 명령어

명령어	설명	모드
<b>mac-access-list &lt;1100-1199&gt; (permit deny)</b> <b>SRC_MAC_ADDRESS DST_MAC_ADDRESS</b> <b>&lt;1-8&gt;</b>	MAC ACL 을 설정한다.	config
<b>no mac-access-list &lt;1100-1199&gt; (permit deny)</b> <b>SRC_MAC_ADDRESS DST_MAC_ADDRESS</b> <b>&lt;1-8&gt;</b>	MAC ACL 을 해제한다.	config
<b>no mac-access-list &lt;1100-1199&gt;</b>	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.

#### 20.2.4. 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 20-14. ACL 의 인터페이스 적용 설정 명령어

명령어	설명	모드
ip access-group { <1-199>   <1300>2699>   WORD ) } {in out}	해당 인터페이스에 acl 을 설정한다.	Interface
no ip access-group { <1-199>   <1300>2699>   WORD ) } {in out}	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.

### 20.3. 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 수 도 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.

### 20.3.1. Class-map

Class-map 은 패킷을 분류하기 위한 목적으로 생성된다. 패킷의 분류는 기본적으로 **ACL** 을 사용하여 할수 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 20-15. Class-map 설정 명령어

명령어	설명	모드
<b>class-map WORD</b>	AND 연산으로 분류하는 Class-map 을 생성하고 해당 노드로 이동한다.	Config
<b>class-map match-all WORD</b>	AND 연산으로 분류하는 Class-map 을 생성하고 해당 노드로 이동한다.	Config
<b>class-map match-any WORD</b>	OR 연산으로 분류하는 Class-map 을 생성하고 해당 노드로 이동한다.	Config
<b>no class-map WORD</b>	Class-map 을 삭제한다..	Config
<b>match access-group NAME</b>	ACL 을 이용한 분류 조건을 설정한다.	cmap
<b>match cos &lt;0-7&gt;</b>	Cos 을 이용한 분류 조건을 설정한다.	cmap

<b>match ethertype WORD</b>	Ethertype 을 이용한 분류 조건을 설정한다.	cmap
<b>match ip-dscp &lt;0-63&gt;</b>	Dscp 을 이용한 분류 조건을 설정한다.	cmap
<b>match ip-precedence &lt;0-7&gt;</b>	Ip-precedence 을 이용한 분류 조건을 설정한다.	cmap
<b>match layer4 {source-port destination-port} &lt;1-65536&gt;</b>	L4 port 을 이용한 분류 조건을 설정한다.	cmap
<b>match mpls exp-bit topmost &lt;0-7&gt;</b>	Mpls flag 을 이용한 분류 조건을 설정한다.	cmap
<b>match tcp-control VALUE</b>	Tcp-control 을 이용한 분류 조건을 설정한다.	cmap
<b>match vlan &lt;1-4095&gt;</b>	VLAN 을 이용한 분류 조건을 설정한다.	cmap



**Notice** Ethertype 의 분류는 4 자리 hexadecimal 로 분류한다. 예를 들어 ARP 타 입인 경우 0806 으로 지칭하면 된다.



**Notice** Tcp-control 을 6 자리 2 진수로 분류한다. 예를 들어 5 번째 자리인 SYN flag 를 보고자 할때는 000010 으로 선언하면 된다.

## 20.3.2. 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.

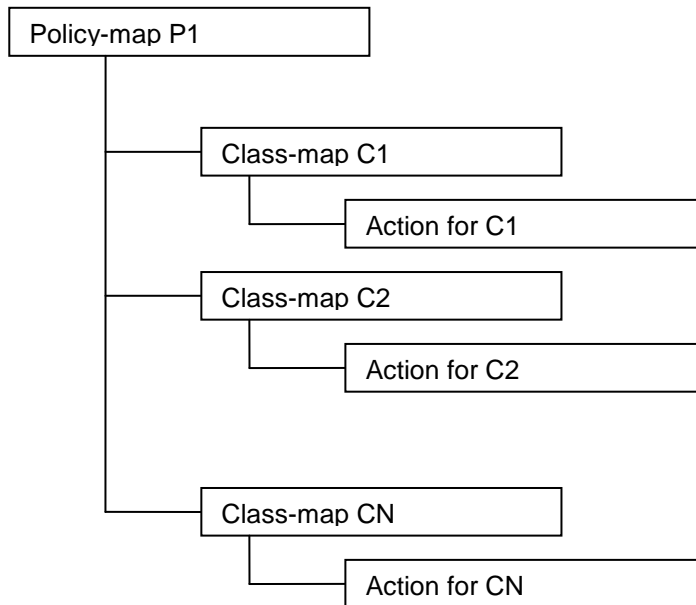


그림 20-1. policy-map 의 계층도

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 20-16. Class-map 설정 명령어

명령어	설명	모드
<b>policy-map NAME</b>	해당 이름의 policy-map 을 생성하고 해당 노드로 이동한다.	Config
<b>no policy-map NAME</b>	해당 이름의 policy-map 을 삭제한다..	Config
<b>class NAME</b>	Class-map 의 동작을 지정하는 sub node 로 이동한다	pmap
<b>no class NAME</b>	해당 class-map 동작 설정을 삭제한다.	pmap
<b>drop</b>	해당 class-map 으로 분류된 트래픽을 drop 한다.	pmap-c
<b>set cos &lt;0-7&gt;</b>	Cos marking 설정	pmap-c
<b>set drop-precedence &lt;0-2&gt;</b>	Drop precedence 설정	pmap-c
<b>set ip-dscp &lt;0-63&gt;</b>	Dscp marking 설정	pmap-c
<b>set ip-precedence &lt;0-7&gt;</b>	Ip precedence (tos) 설정	pmap-c
<b>set queueing &lt;0-7&gt;</b>	Queueing 설정	pmap-c
<b>police &lt;1-10000000&gt; &lt;1-10000000&gt; exceed-action drop</b>	Rate-limit 설정	pmap-c

<b>police aggregate NAME</b>	Aggregated rate-limit 설정	pmap-c
<b>nexthop A.B.C.D { priority &lt;1-8&gt;   }</b>	PBR nexthop 설정 및 nexthop priority 설정	pmap-c
<b>netflow</b>	Netflow 설정	pmap-c
<b>redirect IFNAME</b>	Redirect 설정	pmap-c
<b>mirror</b>	Mirror 설정	pmap-c
<b>trap-cpu { high-priority  }</b>	CPU trap 설정	pmap-c

### 20.3.3. 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 20-17. service-policy 설정 명령어

명령어	설명	모드
<b>service-policy { input   output } NAME</b>	해당 이름의 policy-map 을 인터페이스에 적용한다.	interface
<b>no service-policy { input   output } NAME</b>	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 방향으로 service-policy 와 ACL 을 동시에 적용하여 사용하는 것이 가능하다, output 방향으로 둘중 하나만 설정이 가능하다.

## 20.4. 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.



### 20.4.1. Service-policy on COPP

Control Plane 에 service-policy 를 적용해서 CPU 로 유입되는 트래픽에 대해 Policing 을 수행할 수 있다.

표 20-18. service-policy 의 control-plane 적용 설정 명령어

명령어	설명	모드
<b>control-plane</b>	Control-plane 모드로 진입한다	configure
<b>service-policy input NAME</b>	해당 이름의 policy-map 을 control-plane 에 적용한다.	Control-plane
<b>no service-policy input NAME</b>	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.

### 20.4.2. Rate-limit on COPP

CPU 로 유입되는 특정 트래픽에 대해서 rate-limit 을 설정 할 수 있다.

표 20-19. rate-limit 의 control-plane 적용 설정 명령어

명령어	설명	모드
<b>rate-limit arp-reply &lt;1-1000000&gt; &lt;0-7&gt;</b>	CPU 로 유입되는 트래픽 중 arp-reply 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
<b>rate-limit arp-request &lt;1-1000000&gt; &lt;0-7&gt;</b>	CPU 로 유입되는 트래픽 중 arp-request 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
<b>rate-limit igmp &lt;1-1000000&gt; &lt;0-7&gt;</b>	CPU 로 유입되는 트래픽 중 igmp 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
<b>rate-limit ip-control-over-multicast &lt;1-1000000&gt; &lt;0-7&gt;</b>	CPU 로 유입되는 트래픽 중 ip-control 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
<b>rate-limit ipv6-neib-sol &lt;1-1000000&gt; &lt;0-7&gt;</b>	CPU 로 유입되는 트래픽 중 ipv6 ns 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
<b>rate-limit l4-port (both tcp udp) (both multicast unicast) &lt;1-65535&gt; &lt;1-65535&gt; &lt;1-1000000&gt; &lt;0-7&gt;</b>	CPU 로 유입되는 트래픽 중 L4 트래픽에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
<b>rate-limit mld &lt;1-1000000&gt; &lt;0-7&gt;</b>	CPU 로 유입되는 트래픽 중 mld 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
<b>rate-limit multicast &lt;1-1000000&gt; &lt;0-7&gt;</b>	CPU 로 유입되는 트래픽 중 multicast 에 대해	Control-



	서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	plane
<b>rate-limit protocol &lt;1-255&gt; &lt;1-1000000&gt; &lt;0-7&gt;</b>	CPU 로 유입되는 트래픽 중 특정 protocol 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
<b>rate-limit ripv1 &lt;1-1000000&gt; &lt;0-7&gt;</b>	CPU 로 유입되는 트래픽 중 rip(version 1) 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
<b>rate-limit tcp-syn &lt;1-1000000&gt; &lt;0-7&gt;</b>	CPU 로 유입되는 트래픽 중 tcp-syn 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane
<b>rate-limit udp-broadcast &lt;1-1000000&gt; &lt;0-7&gt;</b>	CPU 로 유입되는 트래픽 중 udp broadcast 에 대해서 허용되는 트래픽의 양(PPS)과 queue 를 선택한다	Control-plane

# 21

## Utilities

### 21.1. 개 요

본 장에서는 시스템 운영에 필요한 기타 기능들에 대해 설명하도록 한다.

### 21.2. 상태 dump 명령

#### 21.2.1. 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          : U9200
SERIAL-NO           :
System MAC-ADDRESS: 00:07:70:74:ff:01
```

```
--- Display the system version ---
-----
```

```
Ubiquoss Switch Operating System Software
U9200 Software (U9200), Version 1.1.0
Technical Support: http://www.ubiquoss.com
Copyright (c) 2001-2010 by Ubiquoss Inc.
```

```
BOOTLDR: U9200 Software (u92h_bsp.r005), Version 1.3.5
```

```
Router uptime is 6 minutes
Time since Router switched to active is 4 minutes
System restarted at 1970:01:01-00:08:59
System image file is "tftp://192.168.0.9/u92h.r110_ssj"
```

```
If you require further assistance please contact us by sending email to
spot.team@ubiquoss.com.
```

```
Router Router processor with RouterM bytes of memory.
Processor board ID
460EX CPU at 1000Mhz, Rev 24.162 (pvr 1302 18a2), 1024KB L2 Cache
Last reset from h/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 ---
-----
```

...

## 21.3. Command history 기능

운용자에 의해 수행된 명령어를 명령어를 실행한 시간순서 또는 실행한 시간의 역순으로 출력하는 기능이다. 이 기능을 사용하여 운용자가 실행한 명령의 조회가 가능하며 시스템 오동작시 원인 규명 및 복원이 편리하게 된다.

표 1. command history 조회 및 설정 명령어

명령어	설명	모드
<b>show history</b>	■ 실행된 명령어들을 조회한다.	Privileged
<b>show history back</b>	■ 실행된 명령어들을 시간의 역순으로 조회한다.	Privileged
<b>show history detail</b>	■ 명령을 실행한 시간/user/접속 IP 를 추가적으로 표시한다.	Privileged

같은 명령어를 반복하여 입력하는 경우는 한번만 저장된다.

## 21.4. Output Post Processing

### 21.4.1. 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 일반적이거나, 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
<b>  include WORD</b>	■ 특정 단어를 포함하는 문자열을 출력한다.
<b>  exclude WORD</b>	■ 특정 단어를 포함하지 않는 문자열을 출력한다.
<b>  begin WORD</b>	■ 특정 단어를 포함하는 문자열부터 그 이후에 나오는 모든 라인을 출력한다.

## 21.4.2. 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.

---

```
Switch#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
```

---

## 21.5. DDM (Digital Diagnostic Monitoring)

EU9200 은 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

### 21.5.1. 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).

Optical  Optical
Temperature Voltage Current Tx Power Rx Power
Port (Celsius) (Volts) (mA) (dBm) (dBm)
-----
Gi2/3 42.6 3.32 17.4 -7.7 -40.0 --
Gi2/4 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
.....
```

## 22

## 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. U9200 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)

## 22.1. 파일 시스템

U9200 Series 스위치는 OS image 파일 저장 및 환경 설정의 저장을 위해 기본적으로 Flash 파일 시스템을 구축하고 USB 를 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 시스템은 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 22-1. 파일 관리를 위한 명령어

명령어	설명	모드
show flash:	Flash 파일의 상태를 보여준다.	Privileged
show usbflash: <0-9>	USB 메모리의 상태를 보여준다.	Privileged
dir (usbflash:  flash:) (<0-9> ) directory	해당 파일 시스템의 상태를 보여준다	Privileged
erase (flash: ) filename	Flash 메모리에 저장된 파일을 삭제한다.	Privileged
erase (usbflash:) (<0-9> ) filename	CF 메모리, USB 메모리에 있는 파일을 삭제한다	Privileged
rename (usbflash: flash:) (<0-9> ) filename (usbflash: flash:) (<0-9> ) change	파일의 이름 및 파일 시스템의 위치를 변경한다.	Privileged

다음은 U9200 Series 스위치에서 File System의 정보를 보는 예시이다. 파일 이름과 파일 사이즈, 그리고 현재(B) 및 다음 부팅 모드(\*)에 대한 정보와 함께 그 파일의 종류를 표시한다.

```
Router#show flash:

-length-  -----type/info-----  CN path
1260      text file                      -- dconfig
616       text file                      B* igmp_cpuha
3571      text file                      -- econfig
1893      text file                      -- igmp_mvlan_final
2048      text file                      -- igmp_cpuha_bk
50274956 [U9200] 1.1.0                  -- u92h.r110
59537056 [U9200] 1.1.1                  -- u92h.r111
1196      text file                      -- lacp_test

19060 Kbytes available (112012 Kbytes used, 86% used)

Router#
```

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#
```

## 22.2. Image/Configuration/BSP Down/Up Load

U9200 Series 스위치는 운영하면서 필요한 OS Image, Configuration 파일 및 Bootloader에 대해서 FTP 또는 TFTP를 이용해서 다운로드 또는 업로드 할 수 있다. 이는 새로운 파일을 Flash 파일에 저장하거나, 적용으로 사용될 수도 있고, 운용상 필요한 Backup을 FTP/TFTP 서버에 할 수 있다. 또한 새로운 BSP 파일을 다운로드 하여 적용할 수 있다. 이 장에서는 어떻게 FTP/TFTP를 통해서 파일을 다운로드 또는 업로드 하는지 설명한다. 아래에서 기술한 running-config 및 startup-config에 대한 설명은 <[14.3 Configuration 파일 관리](#)>를 참조하라.



**Warning** 업그레이드할 Image의 선택은 시스템 모델과 버전에 따라 상당히 주의를 요하므로 당사의 지시 사항을 따르기 바란다.



**Warning** FTP/TFTP를 통해 적용되는 configuration은 현재 시스템의 configuration에 추가되거나 변경된다. 즉 현재 시스템의 configuration이 완전히 없어지고 다운로드 되는 configuration으로 완전히 바뀌지는 않는다.

### 22.2.1. FTP를 통한 Down/Up Load

아래는 FTP를 이용한 파일 다운로드 또는 업로드 방법에 대한 명령어에 대해서 표로 설명해 놓았다.

표 22-2. FTP를 통한 Down/Up Load 명령어

명령어	설명	모드
copy ftp: (usbflash: disk1: flash:) (<0-9> )	FTP 서버에 있는 OS Image 파일을 Flash, USB, CF에 저장한다.	Privileged
copy (usbflash: disk1: flash:) (<0-9> ) ftp	Flash, USB, CF에 있는 OS Image 파일을 FTP 서버에 저장한다.	Privileged
copy ftp: config-file	FTP 서버에 있는 Configuration 파일을 Flash에 저장한다.	Privileged
copy ftp: running-config	FTP 서버에 있는 Configuration 파일을 현재의 running-config로 적용시킨다.	Privileged
copy running-config (usbflash: disk1: flash:) (<0-9> ) filename	Running-config를 해당 파일 시스템에 filename으로 저장한다	Privileged
copy running-config ftp:	시스템에서 운용중인 현재 running-config를 FTP 서버에 저장한다.	Privileged
copy ftp: bootloader	FTP 서버에 있는 BSP 파일을 Flash에 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.

## 22.2.2. TFTP 를 통한 Down/Up Load

아래는 TFTP 를 이용한 파일 다운 방법에 대한 명령어에 대해서 표로 설명해 놓았다.

표 22-3. 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)
```

## 22.3. Configuration 파일 관리

환경 설정은 시스템 운영자가 U9200 Series 스위치를 운영하면서 설정된 다양한 파라미터의 집합이다. U9200 Series 스위치에서 사용하는 Configuration에는 startup-config와 running-config가 있다. Flash 메모리에 저장되어 스위치 초기 구동 시 로딩되는 Configuration을 startup-config라고 하며, DRAM 내에서 구동하는 환경설정 값을 running-config라고 한다. 여기서는 Configuration File Management에 필요한 저장, 삭제 및 다운로드 방법을 설명한다.

표 22-4. Configuration Management 명령어

명령어	설명	모드
show startup-config	Flashes, USB, CF 메모리 중 Booting configuration으로 설정된 파일의 정보를 보여준다.	Privileged
show running-config	현재의 환경 설정 정보를 보여준다.	Privileged
copy running-config startup-config	현재 시스템에서 운용중인 Running configuration 파일을 startup 파일로 저장한다.	Privileged
erase startup-config	현재 설정된 startup configuration 파일을 지운다.	Privileged

### 22.3.1. 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 configuration를 보여주는 명령어와 현재의 running-config를 startup-config로 저장하는 명령어에 대한 예를 보여 준다.

```
Switch# show running-config
!
no service dhcp
!
no logging console
!
ip domain-lookup
!
spanning-tree mode rstp-vlan-bridge
... <생략> ....
SWITCH#
SWITCH# copy running-config startup-config
Overwrite 'system.cfg'? [yes/no] y
SWITCH# show startup-config
!
no service dhcp
```

```
!  
no logging console  
!  
ip domain-lookup  
!  
spanning-tree mode rstp-vlan-bridge  
... <생략> ....  
SWITCH#
```

### 22.3.2. Configuration 파일 삭제

U9200 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
```

## 22.4. Boot Mode 설정 및 시스템 재시동

U9200 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 22-5. Boot Mode 설정 및 시스템 재 시동 명령어

명령어	설명	모드
boot system flash <i>filename</i>	다음 부팅 시 적용될 OS Image 를 설정한다.	Privileged
boot system tftp <i>filename</i> A.B.C.D	다음 부팅 시 적용될 OS Image 를 tftp booting 으 로 한다.	Privileged
boot config <i>filename</i>	다음 부팅 시 적용될 Configuration 파일을 설정한 다.	Privileged
reload	시스템을 재 시동 시킨다.	Privileged

### 22.4.1. Boot Mode 설정

U9200 Series 스위치에서 OS Image 와 configuration 파일에 대해서 다음 Boot Mode 를 설정할 때에는 다음과 같은 주의가 필요하다. **boot flash** 명령어를 실행할 때에는 U9200 Series 스위치에서 사용할 수 있는 OS Image 파일에 대해서만 적용하도록 해야 하며, 또 **boot config** 명령어를 시행할 때에는 U9200 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 u92h.r111
Switch#
Switch# boot config lns.cfg
Switch#
```

### 22.4.2. 시스템 재시동

U9200 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 22-6. Boot Mode 설정 및 시스템 재 시동 명령어

명령어	설명	모드
reload	시스템을 즉시 재 시작한다.	Privileged
reload	시스템 재 시작을 예약한다.	Privileged

<code>{in time at time [day] [month]} [reason]</code>	<ul style="list-style-type: none"> <li>▪ <b>in</b>: 설정한 시간(time)후에 시스템이 재 시작됨</li> <li>▪ <b>at</b>: 설정한 시각에 시스템이 재 시작됨</li> <li>▪ <b>time</b>: HH:MM 형식으로 설정 가능</li> <li>▪ <b>day</b>: 1일부터 31일까지 설정 가능</li> <li>▪ <b>month</b>: 1월부터 12월까지 설정 가능 (ex. Jan or January)</li> <li>▪ <b>reason</b>: 시스템 재 시작 이유를 등록</li> </ul>
<code>reload cancel</code>	시스템 재 시작 예약을 취소한다. 시스템 재 시작 Privileged 의 취소 내용은 모든 터미널로 출력된다.
<code>show reload</code>	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 UTC Thu Sep 14 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 강제적으로 재시동 시켜서는 안 된다.

---

# 23

## GPON

This chapter describes how to configure GPON parts of U9200 switch. This chapter consists of the following sections.

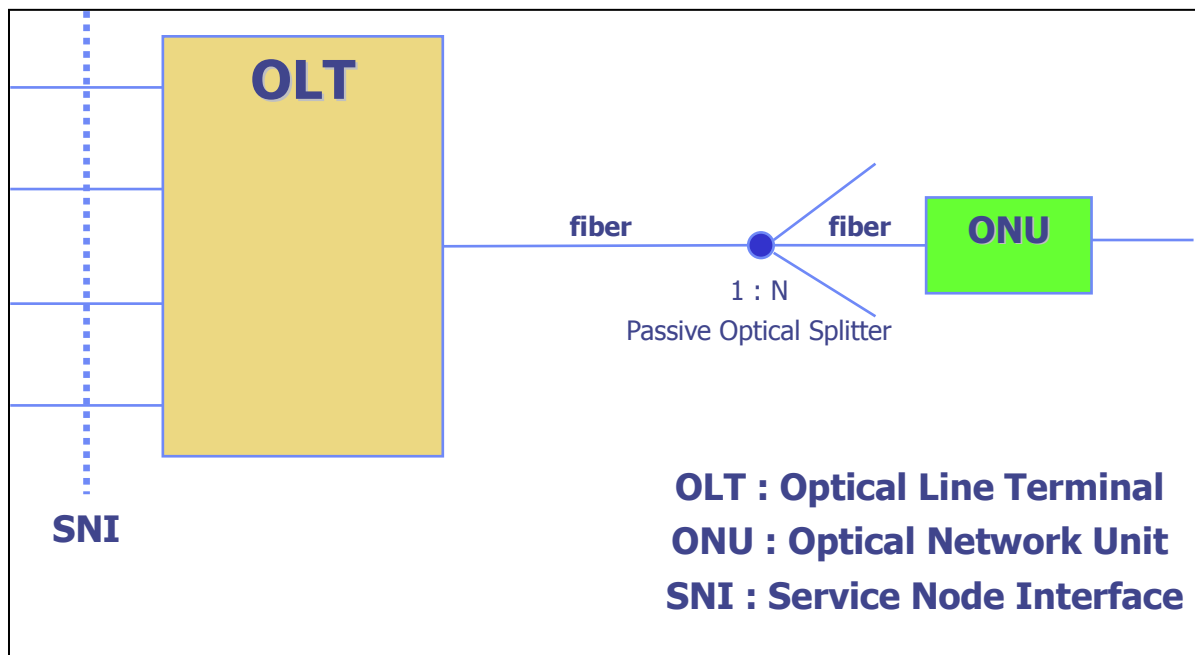
- GPON Overview
- OLT Management
- ONU/ONT Management
- GPON Function Configuration

**Notice**

이 장에서 사용되는 CLI Command 의 상세한 사용방법은 **command reference** 를 참고하십시오.

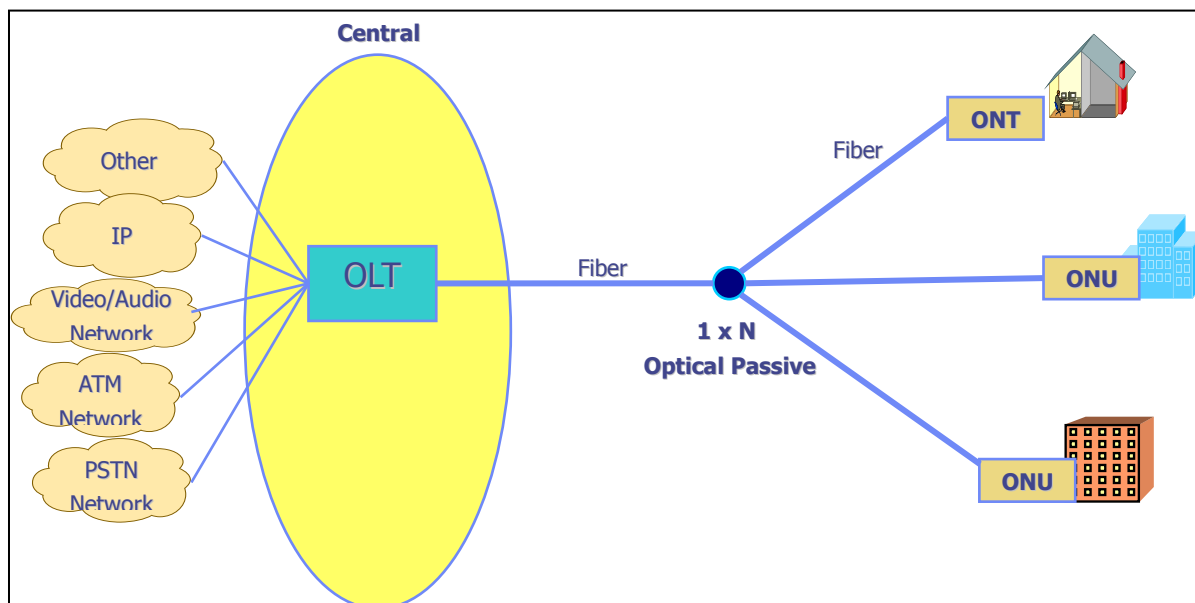
## 23.1. GPON Overview

PON(Passive Optical Network) is a technology that allows to connect an OLT(Optical Line Termination) to multiple ONUs(Optical Network Unit) or ONTs(Optical Network Termination) over passive optical network.



### 【 PON Structure】

PON allows to save the network rollout cost by providing Point-to-Multipoints access so that many subscribers can share the total bandwidth using passive optical splitters. Moreover, passive splitters provide advantages in operating the network in the field since they do not require power feed.



### 【 GPON Structure】

GPON 은 PON 종류의 하나로써 일반적인 망구조는 OLT 를 전화국사 또는 서비스제공지에 설치하고 다수의 ONU 나 가입자의 ONT 를 1:N 으로 연결합니다.

전송방식은 하향(Downstream) 전송은 Broadcast 방식으로 상향(Upstream) 전송은 TDMA(Time Division Multiple Access) 방식을 사용합니다.

하향 전송시 각 패킷들은 광분배기에서 데이터가 동일하게 나누어져 각 ONU 로 전달 되어 집니다. 각 ONU 는 자신에 해당되는 패킷만 받아들이고 다른 ONU 에 해당하는 패킷들은 모두 버리게 됩니다.

상향 전송시 광분배기 특성으로 인해 ONU/ONT 가 전송한 패킷은 다른 ONU(ONT)로 향하지 않습니다. 각 ONU 의 패킷들은 하나의 Fiber 를 공유하기 때문에 패킷간 충돌이 일어나지 않도록 해야 합니다. 그래서 TDMA 방식을 사용하여 ONU/ONT 는 OLT 가 할당한 Time Slot 동안 상향으로 데이터를 전송할 수 있습니다.

## 23.2. OLT/ ONT Management

이 절에서는 OLT 설정에 대한 지침과 OLT / ONT 관리 방법에 대해서 Description 합니다.

### 23.2.1. PON OLT, PORT 의 상태 설정 / 조회

PON의 중요한 역할을 담당하는 PIU interface 카드에 대해서 Administrative State를 설정하는 방법입니다. GPON\_MODE에서 수행되며, CONFIG\_MODE에서 'gpon' Command를 수행하면 됩니다. Factory Default 상태의 system의 PON의 PORT의 상태가 'enable' 상태로 되어 있으며 변경 및 조회하는 명령은 다음과 같습니다.

Command	Description	Mode
<b>show gpon topology olt</b>	OLT 의 모든 pon 상태 출력	Enable
<b>show gpon topology onu IF_NAME</b>	ONU/ONT 의 상태 정보 출력	Enable
<b>show gpon onu information IF_NAME</b>	ONU/ONT 의 상태 정보 출력	Enable
<b>show gpon onu detailed-information IF_NAME</b>	ONU/ONT 의 상세 상태 정보 출력	Enable
<b>[no] shutdown port IF_NAME</b>	PON port 의 administrative 상태를 [disable] enable 상태로 변경 IF_NAME : slot/port	Config-gpon
<b>reset olt IF_NAME</b>	- OLT device reset	Config-gpon

```
U9200#show gpon topology olt
```

```
PON NETWORK OLT TOPOLOGY INFORMATION
```

OLT	ADMIN	OPER	MODE	IPC STATE
1/1	ENABLE	UP	MIXED	UP
1/2	ENABLE	UP	MIXED	UP
1/3	ENABLE	UP	MIXED	UP
1/4	ENABLE	UP	MIXED	UP
1/5	ENABLE	UP	MIXED	UP
1/6	ENABLE	UP	MIXED	UP
1/7	ENABLE	UP	MIXED	UP
1/8	ENABLE	UP	MIXED	UP

```
U9200#show gpon topology onu 1/1
```

```
PON NETWORK ONU TOPOLOGY FOR OLT(1/1) INFORMATION
```

IF_NAME	MAC ADDR LOCATION	ADMIN	OPER (DOWN DUR)	ONU TYPE	DISTANCE
1/1-1	5542.5153.7012.002e	ENABLE	UP	UBQS_601A	73 m
1/1-2	5542.5153.7002.101a	ENABLE	UP	UBQS_601A	73 m

```
U9200#show gpon onu information 1/1
```

OLT	ONU	STATUS	Serial No. (LOCATION)	Rx Power	Distance	Equip-id
1/1	1	Activate	5542.5153.7012.002e	-19.00	0.074km	UBQS_601A
1/1	2	Activate	5542.5153.7002.101a	-19.00	0.073km	UBQS_601A

```
U9200#show gpon onu detailed-information 1/1-1
```

```
-- GPON ONU DETAILED INFORMATION --
```

```
OLT : 1/1, ONU : 1
```

```

Activation Link Status      : Activate
Onu Serial Number          : 5542.5153.7012.002e
Onu Equip-id               : UBQS_601A
Onu Rx Power               : -19.00 dbm
Onu Distance               : 0.074 km
Onu Equalization Delay     : 266579
Onu Upstream FEC State     : Disable
Onu List of Alloc Id       : 640, 0
OMCI Port Id               : 0
Onu Encryption Key         : 00000000000000000000000000000000
Onu Host Name              :
Onu MAC Address            : 0007.7012.002e

```

```
U9200#
```



**Notice**

Shutdown port 를 할 경우 해당 port 의 모든 Link 가 down 됩니다.

### 23.2.2. ONU/ONT 의 상태 설정 / 조회

사용자는 다음 Command를 실행하여 OLT 에 등록된 ONU/ONT 의 pon port, user port 상태를 제어하거나 ONU/ONT를 reset 할 수 있습니다.

Command	Description	Mode
<b>[no] shutdown onu IF_NAME</b>	- ONU/ONT pon admin state 설정	Config-gpon
<b>onu uni-status IF_NAME (enable   disable)</b>	- ONT uni port admin state 설정 IF_NAME : Slot/Port-Onu/Uni	Config-gpon
<b>onu mib-upload limitation IF_NAME (enable   disable)</b>	- ONT/ONU 의 mib-upload 실행여부 결정 - enable : 동일 ONT 가 재등록 되는 경우 mib-upload 를 재실행하지 않음. - disable : 동일 ONT 가 재등록되더라도 mib-upload 를 실행함.	config-gpon
<b>deactivate onu IF_NAME</b>	- ONT/ONU deactivate 실행.	config-gpon
<b>reset onu IF_NAME</b>	- ONT/ONU reset 실행.	config-gpon

### 23.2.3. Registering/Retrieving ONTs

All the ONUs/ONTs physically connected to the OLT are automatically registered to the OLT in specific Index assigned by the OLT by the activation procedures. 다음 Command 는 자동 등록이 아닌 사용자가 원하는 인덱스로 ONU/ONT 를 등록시키기 위해 사용됩니다. GPON\_MODE 에서 수행됩니다.

등록하고자 하는 ONU/ONT 의 interface 이름, serial number, 위치정보 등을 입력합니다.

Command	Description	Mode
<b>Topology onu IF_NAME serial SERIAL_NUMBER loc LINE</b>	ONU/ONT 를 system 의 자원으로 등록 - IF_NAME : Index(slot/port-onu) - SERIAL_NUMBER : xxxx.xxxx.xxxx.xxxx - LINE : 위치 정보 문자열	Config-gpon
<b>show gpon onu information IF_NAME</b>	ONU 의 등록상태 조회 - IF_NAME : OLT Index (slot/port)	Enable

```

U9200#conf t
Enter configuration commands, one per line. End with CNTL/Z.
U9200(config)#gpon
U9200(config-gpon)#topology onu 1/1-1 serial 5542.5153.7012.002e loc GPON ONT
U9200(config-gpon)#end
U9200#show gpon onu information 1/1
-----
OLT | ONU | STATUS | Serial No. | Rx Power | Distance | Equip-id
      |      |         | (LOCATION)  |           |           |
-----
1/1  |  1  | Inactive| 5542.5153.7012.002e | 0.00 | 0.000km |
      |      |         | GPON ONT
-----
U9200#

```

## 23.2.4. ONU/ONT의 정보 변경 및 삭제

ONU/ONT의 변경 및 삭제를 하기 위해 GPON\_MODE에서 다음 Command를 실행해야 합니다. 삭제된 ONU/ONT는 unadmin-list에 등록되어 unadmin-list를 clear할 때까지 해당 ONU/ONT는 재등록되지 않습니다.

Command	Description	Mode
<b>no topology onu IF_NAME</b>	- 등록된 ONU/ONT의 삭제	Config-
<b>edit-onu loc IF_NAME LINE</b>	- 등록된 ONU/ONT의 위치 정보 변경	gpon
<b>onu-auto-remove-timer &lt;1-100&gt;</b>	- 사용하지 않는 ONU/ONT의 자동삭제 - 최소 1 일에서 최대 100 일까지 설정	Config- gpon
<b>show pon topology onu IF_NAME</b>	-ONU의 등록상태 출력 IF_NAME : OLT Index(slot/port)	Enable
<b>show gpon unadmin-onu-list IF_NAME</b>	- 삭제되어 unadmin-list에 등록된 ONU 조회	

```

U9200#conf t
U9200(config)#gpon
U9200(config-gpon)#edit-onu loc 1/1-1 UBIQUOSS
U9200(config-gpon)#end
U9200#show gpon onu information 1/1
-----
  OLT  | ONU | STATUS |      Serial No.      | Rx Power | Distance |      Equip-id
      (LOCATION)
-----
  1/1  |  1  | Activate| 5542.5153.7012.002e |   -19.00 |  0.073km | UBQS_601A
      UBIQUOSS
-----

U9200#conf t
U9200(config)#gpon
U9200(config-gpon)#no topology onu 1/1-1
U9200(config-gpon)#end
U9200#show gpon onu information 1/1
-----
  OLT  | ONU | STATUS |      Serial No.      | Rx Power | Distance |      Equip-id
      (LOCATION)
-----
-----

U9200#show gpon unadmin-onu-list 1/1
-- GPON UNADMIN ONU LIST : 1/1 --
=====
  IDX  | SERIAL-NUMBER | REASON      | EQUIP-ID
-----
  [ 1 ] | 5542.5153.7012.002e | DEREGISTERED | UBQS_601A
=====
U9200#

```



### 23.2.5. Clearing and viewing ONU/ONT unadmin-list

"no topology onu IF\_NAME" 명령을 실행하여 ONU/ONT 를 삭제할 경우 해당 ONU/ONT 정보는 unadmin-list 에 등록됩니다. unadmin-list 에 등록된 ONU/ONT 는 OLT 에 재등록되지 않으므로 등록시키기 위해서는 unadmin-list clear 를 실행해야 합니다.

Command	Description	Mode
<b>clear gpon unadmin-onu-list IF_NAME serial SERIAL_NUMBER</b>	OLT port 내 특정 serial-number 에 대해서 unadmin-list 를 clear 합니다.	Config-gpon
<b>clear gpon unadmin-onu-list IF_NAME all</b>	OLT port 내 모든 serial-number 에 대해서 unadmin-list 를 clear 합니다.	Config-gpon
<b>clear gpon unadmin-onu-list all</b>	system 전체에 대해서 unadmin-list 를 clear 합니다.	Config-gpon
<b>show gpon onu information IF_NAME</b>	ONU 등록 상태 조회	enable
<b>show gpon unadmin-onu-list IF_NAME</b>	ONU unadmin-list 조회	enable

### 23.2.6. Removing information of ONU/ONTs not in use automatically

This function is to remove the information of ONU/ONT in link DOWN state automatically. The time information of DOWN 상태가 유지되고 있는 시간 정보는 'show gpon topology onu IF\_NAME' Command로 조회합니다.

Command	Description	Mode
<b>onu-auto-remove-timer &lt;1-100&gt;</b>	- 사용하지 않는 ONU/ONT 의 자동삭제 - 최소 1 일에서 최대 100 일까지 설정	Config-gpon
<b>no onu-auto-remove-timer</b>	- onu-auto-remove-timer 기능을 비활성화합니다.	Config-gpon
<b>show gpon onu-auto-remove-timer</b>	- onu-auto-remove-timer 설정상태 확인	Enable

### 23.2.7. ONU/ONT equip-id 인증 기능 : equip-id 등록/삭제 및 조회

U9200 system 에서는 인증되지 않은 ONU/ONT 의 등록을 제한하기 위해 equip-id 인증 기능을 제공합니다. OLT 에 ONT 연결 시 authenticated equip-id 로 등록된 equip-id 를 사용하는 ONU/ONT 만 OLT 에 정상 등록되며, authenticated equip-id 로 등록되지 않은 equip-id 를 가진 ONU/ONT 는 OLT 에 의해 등록이 제한되고 해당 ONU/ONT 는 unadmin-list 에 등록됩니다. 사용자는 다음 Command 를 실행하여 authenticated equip-id 를 등록하거나 삭제할 수 있습니다.

Command	Description	Mode
<b>authenticated-equip-id add</b> <i>EQUIP-ID</i> <i>DESCRIPTION</i>	authenticated equip-id 를 등록합니다.	Config-gpon
<b>authenticated-equip-id delete</b> <i>EQUIP-ID</i>	authenticated equip-id 를 삭제합니다. 기본으로 제공되는 default equip-id 는 삭제할 수 없습니다.	Config-gpon
<b>show gpon authenticated-equip-id</b>	authenticated equip-id 를 조회합니다.	enable

```

U9200#show gpon onu-auto-remove-timer

ONU AUTO REMOVE TIMER : disable
U9200#
U9200#conf t
Enter configuration commands, one per line. End with CNTL/Z.
U9200(config)#gpon
U9200(config-gpon)#onu-auto-remove-timer 100
U9200(config-gpon)#end
U9200#
U9200#show gpon onu-auto-remove-timer

ONU AUTO REMOVE TIMER : 100 days
U9200#
U9200#
U9200#show gpon topology onu 4/1
PON NETWORK ONU TOPOLOGY FOR OLT(4/1) INFORMATION
=====
IF_NAME      MAC ADDR      ADMIN    OPER      ONU TYPE      DISTANCE
  LOCATION
-----
4/1-1        504d.4353.d562.808f  ENABLE   CABLE DOWN  UBQS_601A      72 m
              (2190 sec)
=====
U9200#

```

```
U9200#show gpon onu information 1/1
```

```
-----
OLT | ONU | STATUS | Serial No. | Rx Power | Distance | Equip-id
      (LOCATION)
-----
```

```
U9200#
```

```
U9200#show gpon unadmin-onu-list 1/1
```

```
-- GPON UNADMIN ONU LIST : 1/1 --
```

```
=====
IDX | SERIAL-NUMBER | REASON | EQUIP-ID
-----
[ 1] | 5542.5153.7012.002e | DEREGISTERED | UBQS_601A
=====
```

```
U9200#
```

```
U9200#clear gpon unadmin-onu-list 1/1 serial 5542.5153.7012.002e
```

```
U9200#show gpon onu information 1/1
```

```
-----
OLT | ONU | STATUS | Serial No. | Rx Power | Distance | Equip-id
      (LOCATION)
-----
```

```
1/1 | 1 | Activate | 5542.5153.7012.002e | -19.00 | 0.073km | UBQS_601A
-----
```

```
U9200#
```

```
U9200#show gpon authenticated-equip-id
-- GPON AUTHENTICATED EQUIP_ID LIST --
=====
  IDX |      EQUIP-ID      |      DESCRIPTION
-----
[ 1 ] | UBQS_ONU           | (D) ubiquoss ONU
[ 2 ] | UBQS_601A          | (D) ubiquoss 1port ONT
-----
                                (D) : default equip-id
=====
U9200#conf t
U9200(config)#gpon
U9200(config-gpon)#authenticated-equip-id add UBQS_601B ubiquoss ONT
U9200(config-gpon)#end
U9200#show gpon authenticated-equip-id
-- GPON AUTHENTICATED EQUIP_ID LIST --
=====
  IDX |      EQUIP-ID      |      DESCRIPTION
-----
[ 1 ] | UBQS_ONU           | (D) ubiquoss ONU
[ 2 ] | UBQS_601A          | (D) ubiquoss 1port ONT
[ 3 ] | UBQS_601B          | ubiquoss ONT
-----
                                (D) : default equip-id
=====
U9200#
```

### 23.2.8. ONU/ONT equip-id 인증 기능 : 기능 운용 Description

인증되지 않은 equip-id 를 가진 ONU/ONT 가 OLT 에 등록을 시도할 경우, OLT 는 등록을 제한하기위해 아래와 같이 해당 ONT 의 serial number 를 unadmin-list 에 등록한 뒤 ONT 를 emergency-stop 상태로 변경합니다.

```
U9200#show gpon authenticated-equip-id
-- GPON AUTHENTICATED EQUIP_ID LIST --
=====
  IDX |      EQUIP-ID      |      DESCRIPTION
-----
[ 1 ] | UBQS_ONU           | (D) ubiquoss ONU
[ 2 ] | UBQS_601A          | (D) ubiquoss 1port ONT
-----
                                (D) : default equip-id
=====
U9200#
U9200#show gpon unadmin-onu-list 1/1
-- GPON UNADMIN ONU LIST : 1/1 --
=====
  IDX |      SERIAL-NUMBER      |      REASON      |      EQUIP-ID
-----
[ 1 ] | 4451.9245.5e27.3128    | UNAUTHENTICATED  | U014PL-102
-----
U9200#
```

equip-id 인증기능에 의해 block 된 ONU/ONT를 정상 등록시키기 위해서는 해당 ONU/ONT의 equip-

id를 authenticated equip-id로 등록한 뒤 clear gpon unadmin-list 명령을 실행합니다.

```
U9200#conf t
U9200(config)#gpon
U9200(config-gpon)#authenticated-equip-id add U014PL-102
U9200(config-gpon)#end
U9200#
U9200#clear gpon unadmin-onu-list 1/1 serial 4451.9245.5e27.3128
U9200#
U9200#show gpon onu information 1/1
-----
  OLT   | ONU | STATUS |      Serial No.      | Rx Power | Distance |      Equip-id
          |      |         | (LOCATION)             |           |           |
-----
  1/1   |  3  | Activate| 4451.9245.5e27.3128 |    19.00 | 0.071km | U014PL-102
-----
U9200#
```

### 23.2.9. Creating vlan mapping table (QinQ)

OLT - ONT 간 QinQ 기능을 지원하기 위해 vlan mapping table을 생성합니다.

Command	Description	Mode
<b>vlan mapping IF_NAME &lt;1-4&gt; s-vlan &lt;1-4095&gt; c-vlan &lt;1-4095&gt;</b>	vlan mapping table 을 생성합니다. QinQ 동작 시 해당 table 을 참조하여 s-vlan 및 c-vlan 을 구성합니다.	Config-gpon
<b>show gpon vlan mapping onu</b>	vlan mapping table 을 조회합니다.	enable

## 23.3. PON Configuration

This section lists the commands used to configure PON OLT and ONU and shows the exemplary use of the commands.

PON 설정은 기본적으로 Service Profile을 작성하고 이를 interface에 적용하는 방식을 따릅니다. OLT와 ONU Service Profile 작성 및 적용 Command는 각각 GPON\_MODE의 Sub-mode인 OLT\_QOS\_MODE와 ONU\_QOS\_MODE에서 수행됩니다.

### 23.3.1. PON OLT Configuration

OLT Service Profile은 Policy-map, Bridge-map, Igmp-map 으로 구성됩니다.

Policy-map은 각종 alarm 설정 항목으로 구성되며, Bridge-map은 Bridging Configuration 설정으로

구성됩니다. Igmp-map은 OLT에서 제공하는 igmp 기능관련 설정항목으로 구성됩니다.  
system의 초기 설정은 'oltProfile'이라는 Service Profile로 설정되어 있으며, 이는 Policy-map으로 'oltPmap'를 Bridge-map으로 'oltBmap'을, 그리고 Igmp-map으로 'oltImap'을 포함합니다.

Command	Description	Mode
olt-qos	OLT Service Profile 작성 Mode 로 변경	Config-gpon

### 23.3.1.1. Creating and applying OLT Service Profile

OLT Service Profile을 작성하려면 우선 Policy-map, Bridge-map, Igmp-map을 먼저 작성해야 합니다.  
Service Profile 작성 및 삭제, 그리고 OLT port interface에의 적용 Command는 아래와 같습니다.

Command	Description	Mode
<b>service-map PROFILE_NAME policy-map POLICY_NAME bridge-map BRIDGE_NAME igmp-map IGMP_NAME</b>	OLT Service Profile 작성 - PROFILE_NAME : Service Profile Name - POLICY_NAME : Policy-map Name - BRIDGE_NAME : Bridge-map Name - IGMP_NAME : Igmp-map Name	Config-gpon-oltqos
<b>no service-map PROFILE_NAME</b>	OLT Service Profile 삭제 Default Profile(oltProfile)과 현재 interface 에 적용 중인 Profile 은 삭제 불가	Config-gpon-oltqos

Command	Description	Mode
<b>no policy-map MAP_NAME</b>	OLT Policy-map 삭제 - 현재 사용중인 map 은 삭제 불가	Config-gpon-oltqos
<b>no bridge-map MAP_NAME</b>	OLT Bridge-map 삭제 - 현재 사용중인 map 은 삭제 불가	Config-gpon-oltqos
<b>service-policy IF_NAME service-map PROFILE_NAME</b>	IF_NAME : OLT Port interface Name PROFILE_NAME : OLT Service Profile Name	Config-gpon-oltqos
<b>show pon service-map olt (PROFILE_NAME )</b>	OLT Service Profile List 조회 또는 특정 Service Profile 의 내용 조회	enable
<b>Show pon service-policy olt (IF_NAME )</b>	OLT Port Interface 에 현재 적용된 Service Profile 조회	enable

### 23.3.1.2. Creating OLT Policy-map

OLT Policy-map은 OLT Port의 alarm 설정으로 구성됩니다. OLT\_QOS\_MODE에서 'policy-map' Command를 이용하여 OLT\_PMAP\_MODE로 전환하여 작성합니다.

Command	Description	Mode
olt-qos	OLT Service Profile 작성 Mode 로 변경	Config-gpon
policy-map MAP_NAME	Policy-map 작성 Mode 로 변경	Config-gpon-

		oltqos
<b>alarm ( dowi   rdii   loami   lcdgi ) ( enable   disable )</b>	dowi : ONU transmission is received at an expected place within the virtual frame rdii : RDI fields asserted loami : Three consecutive PLOAM message is lost lcdgi : GEM fragment delineation is lost	Config-gpon-oltqos-pmap
<b>alarm ( loai   pee   loki   tiwi   tia ) ( enable   disable )</b>	loai : OLT does not receive any acknowledgement pee : OLT receives the PEE from the ONU loki : Key transmission message is failed tiwi : Drift of ONU transmission exceed the threshold tia : ONU turns on its laser at a time assigned to another ONU	Config-gpon-oltqos-pmap
<b>alarm sdi ( enable &lt;4-9&gt;   disable )</b>	sdi : Upstream BER is $\geq 10^{-x}$ - Range of x is 4 to 9	Config-gpon-oltqos-pmap
<b>alarm sfi ( enable &lt;3-8&gt;   disable )</b>	sfi : Upstream BER is $\geq 10^{-y}$ - Range of y is 3 to 8	Config-gpon-oltqos-pmap

Command	Description	Mode
<b>Map-end</b>	Policy-map 작성 완료 및 상위 Mode 로 전환(이 Command 를 입력하지 않으면 map 은 생성되지 않으므로 작성 후 항상 이 Command 를 입력하여 상위 Mode 로 전환해야 합니다.)	Config-gpon-oltqos-pmap
<b>Show pon policy-map olt (MAP_NAME )</b>	OLT Policy-map List 조회 또는 특정 Policy-map 상세 정보 조회	enable

### 23.3.1.3. Creating OLT Bridge-map

OLT Bridge-map은 OLT port의 Bridge 관련 설정을 포함합니다. OLT\_QOS\_MODE에서 'bridge-map' Command를 이용하여 OLT\_BMAP\_MODE로 전환하여 작성합니다.

Command	Description	Mode
<b>olt-qos</b>	OLT Service Profile 작성 Mode 로 변경	Config-gpon
<b>bridge-map MAP_NAME</b>	Bridge-map 작성 Mode 로 변경	Config-gpon-oltqos
<b>address-table s-vlan (none   &lt;1-4095&gt;) (forwarding-mode (1:1   N:1)   (use-s-vlan (on   off)   (use-c-vlan (on   off)   (use-priority (on   off)   (discard-unknown (on   off)  </b>	s-vlan : service vlan id 를 설정. forwarding-mode : OLT forwarding-mode 를 설정. 1:1 은 VLAN base, N:1 은 mac base 로 동작합니다. use-c-vlan : client vlan 사용여부를 설정. use-priority : use-priority 사용여부를 설정. discard-unknown : un 트래픽에 대한 discard 여부를 설정.	Config-gpon-oltqos-bmap
<b>bridgeconfig (remove-when-aged (on   off)   (discard-unlearned-sa (on   off)   (learned-entry-age-limit &lt;5-17280&gt;  </b>	remove-when-aged : entry 삭제 설정 discard-unlearned-sa : unlearned source address 에 대한 discard 여부 설정 learned-entry-age-limit : aging time 설정	Config-gpon-oltqos-bmap
<b>bridgeconfig vlan priority-mapping (upstream   downstream) &lt;0-7&gt; &lt;0-7&gt; &lt;0-7&gt; &lt;0-7&gt; &lt;0-7&gt; &lt;0-7&gt; &lt;0-7&gt;</b>	upstream/downstream 의 priority-mapping 값을 설정함.	Config-gpon-oltqos-bmap
<b>bridgeconfig vlan 1:1 &lt;0-4094&gt;</b>	vlan 1:1 mode 설정	Config-gpon-oltqos-bmap
<b>vlan downlink s-vlan (none   &lt;1-4095&gt;) (double-tag-handling (on   off)   (vlan-priority-handling (on   off)  </b>	vlan downlink 설정 double-tag-handling : double tagging 설정 vlan-priority-handling : priority handling 설정	Config-gpon-oltqos-bmap



Command	Description	Mode
Map-end	Bridge-map 작성 완료 및 상위 Mode 로 전환(이 Command 를 입력하지 않으면 map 은 생성되지 않으므로 작성 후 항상 이 Command 를 입력하여 상위 Mode 로 전환해야 합니다.)	Config-pon-oltqos-bmap
Show pon bridge-map olt (MAP_NAME )	OLT Bridge-map List 조회 또는 특정 Bridge-map 상세 정보 조회	enable

#### 23.3.1.4. Creating OLT Igmp-map

OLT Igmp-map includes the configurations related with igmp protocol of OLT ports. OLT\_QOS\_MODE에서 'igmp-map' Command를 이용하여 OLT\_IMAP\_MODE로 전환하여 작성합니다.

Command	Description	Mode
olt-qos	OLT Service Profile 작성 Mode 로 변경	Config-gpon
bridge-map MAP_NAME	Bridge-map 작성 Mode 로 변경	Config-gpon-oltqos
(no) ip igmp discard-untagged	untagged frame 에 대한 discard 설정	Config-gpon-oltqos-imap
(no) ip igmp ignore-vlan	VLAN tag 에 대한 discard 설정	Config-gpon-oltqos-imap
ip igmp last-member-query-count <1-8> no ip igmp last-member-query-count	last-member-query-count 설정	Config-gpon-oltqos-imap
ip igmp last-member-query-interval <1-255> no ip igmp last-member-query-interval	last-member-query-interval 설정	Config-gpon-oltqos-imap
ip igmp query-interval <1-18000> no ip igmp query-interval	query-interval 설정	Config-gpon-oltqos-imap
ip igmp ra-option no ip igmp ra-option	IGMP Strict RA Option Validation 설정	Config-gpon-oltqos-imap
ip igmp robustness-variable <1-8> no ip igmp robustness-variable	Robustness counter 설정	Config-gpon-oltqos-imap
ip igmp snooping fast-leave no ip igmp snooping fast-leave	igmp snooping fast-leave 설정	Config-gpon-oltqos-imap
ip igmp version <1-3> no ip igmp version	igmp version 설정	Config-gpon-oltqos-imap
ip igmp mode (disable   snoop   proxy)	igmp mode 설정	Config-gpon-oltqos-imap

<b>ip igmp vlan-select (inner   outer)</b>	double tag frame 수신 시 inner or outer tag 선택 설정	Config-gpon-oltqos-imap
--	--	-------------------------

Command	Description	Mode
<b>Map-end</b>	Igmp-map 작성 완료 및 상위 Mode 로 전환(이 Command 를 입력하지 않으면 map 은 생성되지 않으므로 작성 후 항상 이 Command 를 입력하여 상위 Mode 로 전환해야 합니다.)	Config-pon-oltqos-imap
<b>Show pon igmp-map olt (MAP_NAME )</b>	OLT igmp-map List 조회 또는 특정 igmp-map 상세 정보 조회	enable

## 23.3.2. PON ONU Configuration

ONT Service Profile consists of Sla-map, Bridge-map, and Multicast-map.

Sla-map은 은 Link에 대한 SLA 설정으로 구성되며, Bridge-map은 Bridging Configuration 을 설정합니다. Multicast-map은 Multicast service 관련 파라미터 설정을 포함하고 있습니다.

Sla-map, Bridge-map, Multicast-map 은 service-policy를 구성하는 요소로써, service-policy는 현재 등록되어 있는 ONT에 적용된 service profile 입니다.

system 내에는 ONT equip-id 에 맞는 default service policy가 설정이 되어 있어서 ONT가 등록이 될 때 해당 ONT에 맞는 default service-policy가 자동으로 설정이 됩니다.

또한 Sla-map, Bridge-map, Multicast-map을 각각 개별적으로 해당 ONT에 설정할 수도 있습니다. 운용자에 의해 설정된 service-policy는 default service-policy 에 우선하여 적용됩니다.

현재 equip-id에 따른 Default service-policy는 아래와 같습니다. Default service-policy 는 CLI를 통해 추가가 가능합니다.

equip-id	sla-map	bridge-map	multicast-map
UBQS_ONU	ubqs1000	hybridBmap	mcastMap-noSnoop
UBQS_601A	ubqs1000	ont1PortBmap	mcastMap-snoop
H645A	ubqs1000	ont1PortBmap	mcastMap-snoop

ONU Service Profile 작성은 GPON\_MODE의 Sub-mode인 ONU\_QOS\_MODE에서 수행합니다.

Command	Description	Mode
onu-qos	ONU Service Profile 작성 Mode 로 변경	Config-gpon-onuqos

### 23.3.2.1. Creating and removing ONU Sla-map

ONU Sla-map includes configuration of SLA for ONU Link. ONU\_QOS\_MODE에서 'sla-map' Command를 이용하여 ONU\_SMAP\_MODE로 전환하여 작성합니다.

Command	Description	Mode
<b>onu-qos</b>	ONU Service Profile 작성 Mode 로 변경	Config-gpon
<b>sla-map MAP_NAME</b>	sla-map 작성 Mode 로 변경	Config-gpon- onuqos
<b>upstream sla &lt;1-4&gt; (data   voip) (nsr   type0   type1) &lt;1-1244&gt; &lt;0-15&gt; &lt;1-1244&gt; &lt;0-15&gt;</b>	ONU Link 의 Upstream SLA 설정 - tcont <1-4> : SLA 를 설정할 tcont id 선택 - (data   voip) : service type 선택 - (nsr   type0   type1) : status-report type 선택 - Guaranteed bandwidth : <1-1244> - Fine Guaranteed bandwidth : <0-15> - Best Effort bandwidth : <1-1244> - Fine Best Effort bandwidth : <1-1244>	Config-pon- onuqos-smap
<b>downstream policing &lt;1-4&gt; &lt;1-2500&gt; &lt;1-2500&gt;</b>	ONU Link 의 Downstream policing 설정 - tcont <1-4> : policing 을 설정할 tcont id 선택 - Committed Bandwidth in Mbps : <1-2500> - Excess Bandwidth in Mbps : <1-2500>	Config-pon- onuqos-smap
<b>show gpon sla-map onu (MAP_NAME  )</b>	ONU Sla-map List 조회 또는 특정 Sla-map 상세 정보 조회	enable

### 23.3.2.2. Creating or removing ONU Bridge-map

ONU Bridge-map은 User Port와 Link의 Bridge 관련 설정과 bridge 관련 OMCI ME 설정, 그리고 encryption 및 fec 설정 등을 포함합니다.

ONU\_QOS\_MODE에서 'bridge-map' Command를 이용하여 ONU\_BMAP\_MODE로 전환하여 작성합니다.

Command	Description	Mode
<b>onu-qos</b>	ONU Service Profile 작성 Mode 로 변경	Config-gpon
<b>bridge-map MAP_NAME base-map MAP_NAME</b>	ONU bridge-map 생성 - default bridge-map 을 base-map 으로 지정하여 기존 map 내용을 복사하여 생성합니다. default map 만 base-map 으로 지정할 수 있으므로 운용 시 적절한 default map 을 선택합니다.	Config-gpon-onuqos
<b>primary-vid enable PRIMARY_VID_LIST</b>	OLT - ONT 간 primary-vid tag 설정 (1~4094) OLT 는 ONT 로부터 수신되는 frame 중 설정된 primary-vid tag 의 frame 만을 허용합니다. 최대 20 개까지 설정이 가능합니다.	Config-gpon-onuqos-bmap
<b>primary-vid disable</b>	OLT - ONT 간 primary-vid tag 를 설정하지 않습니다. OLT 는 ONT 로부터 수신되는 모든 tag 를 허용합니다.	Config-gpon-onuqos-bmap
<b>mapper &lt;1-4&gt;</b>	802.1p mapper service profile 설정 - 802.1p mapper service profile 설정을 위해 mapper mode 로 진입합니다. - mapper 는 최대 4 개까지 생성할 수 있습니다.	Config-gpon-onuqos-bmap
<b>gemport count (1   2   4)</b>	mapper 에 연결되어 사용할 gem-port 의 갯수를 설정합니다.	Config-gpon-onuqos-bmap-mapper
<b>gem-port-mapping &lt;1-4&gt; tcont &lt;1-4&gt;</b>	gem-port 별로 연결할 tcont id 를 지정합니다.	Config-gpon-onuqos-bmap-mapper
<b>default-pbit-marking (enable   disable)</b>	모든 frame 에 대해서 pbit 을 default 값으로 변경할지 여부를 설정합니다.	Config-gpon-onuqos-bmap-mapper
<b>default-cos &lt;0-7&gt;</b>	default-pbit-marking 이 활성화된 경우 사용되는 default pbit 값입니다.	Config-gpon-onuqos-bmap-mapper
<b>unmarked-frame-option (0   1)</b>	unmarked-frame-option 을 설정합니다. - 0 : Convert from DSCP to 802.1p - 1 : Tag frame to a certain value	Config-gpon-onuqos-bmap-mapper
<b>bridge &lt;1-4&gt;</b>	MAC bridge service profile 설정 - MAC bridge service profile 설정을 위해 bridge mode 로 진입합니다.	Config-gpon-onuqos-bmap
<b>mac-learning</b>	Learning ind 설정 - bridge learning function 을 활성화하거나 비활성화합니다.	Config-gpon-onuqos-bmap - bridge

U9200 Series User Guide

<b>&lt;1-4095&gt; &lt;0-7&gt; (&lt;1-4095&gt; &lt;0-7&gt; &lt;1-4095&gt; &lt;0-7&gt; (&lt;1-4095&gt; &lt;0-7&gt; &lt;1-4095&gt; &lt;0-7&gt;))))))))))</b>		
<b>bind &lt;1-4&gt; tcont &lt;1-4&gt; mapper &lt;1-4&gt; bridge &lt;1-4&gt;</b>	tcont - mapper -bridge - uni 연결을 설정합니다. 해당 uni 의 트래픽이 해당 tcont 으로 처리됩니다.	Config-gpon-onuqos-bmap - bridge
<b>bridgemode &lt;1-4&gt; vlan-mapping (1:1   N:1 limit &lt;0-126&gt;)</b>	ONT 의 bridgemode 를 설정합니다. N:1 선택 시 mac-limit 을 설정합니다.	Config-gpon-onuqos-bmap - bridge
<b>encryption (enable   disable)</b>	encryption 사용여부를 설정합니다.	Config-gpon-onuqos-bmap - bridge
<b>fec upstream (enable   disable)</b>	fec 사용여부를 설정합니다.	Config-gpon-onuqos-bmap - bridge
<b>Show gpon bridge-map onu (MAP_NAME )</b>	ONU Bridge-map List 조회 또는 특정 Bridge-map 상세 정보 조회	enable

### 23.3.2.3. Creating/Removing ONU Multicast-map

ONU Multicast-map includes configurations related with Multicast service of ONU.

ONU\_QOS\_MODE에서 'multicast-map' Command를 이용하여 ONU\_MCASTMAP\_MODE로 전환하여 작성합니다.

Command	Description	Mode
<b>onu-qos</b>	ONU Service Profile 작성 Mode 로 변경	Config-gpon
<b>multicast -map MAP_NAME</b>	multicast -map 작성 Mode 로 변경	Config-gpon-onuqos
<b>group-range start A.B.C.D end A.B.C.D</b>	multicast group range 를 설정합니다.	Config-gpon- onuqos
<b>igmp snoop version &lt;1-3&gt; no igmp snoop version</b>	igmp snoop version 을 설정합니다. 'no' 명령 실행 시 기본값인 version 2 로 설정됩니다.	Config-gpon-onuqos- mcastmap
<b>(no) igmp snoop fast-leave</b>	igmp snoop fast-leave 를 활성화하거나 비활성화합니다.	Config-gpon-onuqos- mcastmap
<b>igmp snoop max-groups eth &lt;1-4&gt; &lt;0-1000&gt; no igmp snoop max-groups eth &lt;1-4&gt;</b>	user port 별 max group 을 설정합니다. 'no' 명령 실행 시 group 수를 최대로 설정합니다. (제한을 해제합니다)	Config-gpon-onuqos- mcastmap
<b>(no) igmp snoop</b>	igmp snooping 을 활성화합니다.	Config-gpon-onuqos- mcastmap
<b>Map-end</b>	Igmp-map 작성 완료 및 상위 Mode 로 전환 (이 Command 를 입력하지 않으면 map 은 생성되지 않으므로 작성 후 항상 이 Command 를 입력하여 상위 Mode 로 전환해야 합니다.)	Config-gpon-onuqos- mcastmap
<b>Show gpon multicast-map onu (MAP_NAME )</b>	ONU Igmp-map List 조회 또는 특정 Igmp-map 상세 정보 조회	enable



#### 23.3.2.4. ONU default service-policy 의 설정 및 조회

ONU default service-policy를 설정하면 ONT가 등록이 될 때 해당 ONT의 equip-id 에 맞는 Default profile이 자동으로 설정이 됩니다.

Command	Description	Mode
<b>default service-policy EQUIP_ID bridge-map MAP_NAME sla-map MAP_NAME (multicast-map MAP_NAME)</b>	ONU Default service-policy 설정 SLA_NAME : Sla-map Name BRIDGE_NAME : Bridge-map Name IGMP_NAME : Igmp-map Name	Config-gpon-onuqos
<b>show gpon default service-policy onu</b>	ONU default Service-policy 조회	enable

#### 23.3.2.5. Creating, retrieving, and removing ONU service-policy

Command	Description	Mode
<b>service-policy IFNAME BRIDGE_MAP SLA_MAP (mcast-map MAP_NAME ) (vlan-tag &lt;0-4095&gt; &lt;0-4095&gt; &lt;0-4095&gt; &lt;0-4095&gt; )</b>	ONU service-policy 설정 IFNAME : Interface Name BRIDGE_MAP : Bridge-map Name SLA_MAP : Sla-map Name MCAST_MAP : multicast-map Name vlan-tag : ONT bridge-map 설정 중 vlan-tagging-operation-config 에 적용되는 upstream tag 설정입니다. 양쪽에 모두 설정이 존재할 경우 bridge-map 설정에 우선하여 적용됩니다. multicast map 과 vlan tag 설정은 옵션 항목입니다. (mcast-map 설정을 입력하지 않으면 igmp snoop 이 동작하지 않습니다.)	Config-gpon-onuqos
<b>no service-policy IFNAME</b>	ONU 에 적용된 service-policy 를 삭제 - 운영중인 ONU 에 적용된 profile 은 삭제 불가	Config-gpon-onuqos
<b>show pon service-policy onu IFNAME</b>	ONU 에 적용된 service-policy 를 조회	enable

## 23.4. Managing ONTs with Faulty Optic Module

### 23.4.1. 광모듈 불량 ONU/ONT 자동 shutdown

광모듈 불량인 ONT를 검출 하여 해당 ONT를 자동 shutdown 시키는 기능을 제공합니다.

Command	Description	Mode
<b>ldshutdown (enable   disable)</b>	LD shutdown 기능 활성화/비활성화 설정	Config-gpon
<b>show gpon ldshutdown</b>	LD shutdown 기능 상태조회	enable

### 23.4.2. ONT 광모듈 tx-power 제한

This function is to limit tx-power of optic modules of ONT for specific time period.

Command	Description	Mode
<b>ldshutdown onu IF_NAME &lt;0-65535&gt;</b>	IF_NAME : slot/port-onuld <0-65535> : tx-power 를 제한할 시간(sec) 설정. (0 : permanently)	Config-gpon

## 23.5. Firmware upgrade

### 23.5.1. OLT firmware upgrade

This function is to upgrade firmware of OLT PON chip using tftp.

Command	Description	Mode
<b>software download olt (address IF_NAME ) FILENAME (A.B.C.D )</b>	OLT 펌웨어를 업그레이드합니다.  <b>address</b> : slot/port 형식으로 입력하되, 슬롯 당 2 개의 pon chip 을 사용하므로 port 번호는 1 또는 5 를 입력합니다. (port 1, 2, 3, 4 번은 port 번호 1 로 입력, port 5, 6, 7, 8 번은 port 번호 5 로 입력) 여러 개의 address 를 업그레이드할 경우 range interface 로 입력할 수 있습니다. 예) 1/1 과 1/5 와 2/1 : 1/1~2/1 또는 1/1,1/5,2,1 의 형식으로 입력가능. <b>address</b> 를 입력하지 않을 경우 전체 slot 에 대해 업그레이드를 진행합니다. <b>FILENAME</b> : 업그레이드할 펌웨어의 파일명을 입력합니다. <b>(A.B.C.D )</b> : tftp 서버 주소를 입력합니다. 주소를 입력하지 않을 경우 장비의 flash 내에서 펌웨어 파일을 찾아 업그레이드를 진행합니다. (flash 에 파일이 없을 경우 업그레이드 종료) <b>업그레이드 진행확인</b> : enable Mode 에서 terminal monitor 를 입력한 뒤 업그레이드를 진행합니다. 업그레이드 종료 시 'completed' 로그가 출력되며, 업그레이드가 완료된 pon chip 은 자동으로 reload 됩니다.	Config-gpon
<b>show gpon software olt</b>	OLT 펌웨어 버전정보를 조회합니다.	enable

--> 4 번 슬롯 두번째 pon chip 에 대해서 OLT 펌웨어 다운로드 실행

```
U9200#show gpon software olt
```

```
=====
DEV_NAME          F/W VER      H/W VER
-----
4/1                2.1.5.2      5211 2
4/2                2.1.4.4      5211 2
-----
Host Version :   1.2.50
=====
```

```
U9200#
```

```
U9200#configure terminal
```

```
U9200(config)#gpon
```

```
U9200(config-gpon)#software download olt address 4/5 PAS5211_v2_1_build_5_2.bin 192.168.0.9
```

```
U9200(config-gpon)#Jan  1 02:15:53 [5] OLT IMAGE UPGRADE STATUS: transfered Slot 4 Port 0 with
pmc/PAS5211_v2_1_build_5_2.bin image
```

```
U9200(config-gpon)#Jan  1 02:16:10 [5] OLT IMAGE UPGRADE STATUS: completed Slot 4 Port 0 with
pmc/PAS5211_v2_1_build_5_2.bin image
```

```
U9200(config-gpon)#
```

```
U9200(config-gpon)#end
```

```
U9200#show gpon software olt
```

```
=====
DEV_NAME          F/W VER      H/W VER
-----
4/1                2.1.5.2      5211 2
4/2                2.1.5.2      5211 2
-----
Host Version :   1.2.50
=====
```

```
U9200#
```

## 23.5.2. ONT/ONU firmware upgrade (manual-upgrade)

This function is to upgrade the firmware of ONT/ONU PON chip using tftp.

Command	Description	Mode
<b>software download onu (address IF_NAME ) (image-id &lt;0-1&gt;) FILENAME (A.B.C.D )</b>	<p>ONT/ONU 펌웨어를 업그레이드합니다.</p> <p><b>address</b> : slot/port-onu 의 형식으로 입력합니다. 여러 개의 address 를 업그레이드할 경우 range interface 로 입력할 수 있습니다. 예) ONT 1/1-1 과 1/1-2 와 1/1-3 : 1/1-1~1/1-3 또는 1/1-1,1/1-2,1/1-3 의 형식으로 입력가능.</p> <p>address 를 입력하지 않을 경우 전체 ONT 에 대해 업그레이드를 진행합니다.</p> <p><b>image-id &lt;0-1&gt;</b> : gpon ONT/ONU 는 dual image 구조를 지원합니다. 업그레이드할 image 의 번호를 입력합니다.</p> <p><b>FILENAME</b> : 업그레이드할 펌웨어의 파일명을 입력합니다.</p> <p><b>(A.B.C.D )</b> : tftp 서버 주소를 입력합니다. 주소를 입력하지 않을 경우 장비의 flash 내에서 펌웨어 파일을 찾아 업그레이드를 진행합니다. (flash 에 파일이 없을 경우 업그레이드 종료)</p> <p><b>업그레이드 진행확인</b> : enable Mode 에서 terminal monitor 를 입력한 뒤 업그레이드를 진행합니다. 업그레이드 종료 시 'completed' 로그가 출력되며, 펌웨어 적용을 위해서는 해당 ONT 를 reload 해야 합니다. (software activate Command 사용)</p>	Config-gpon
<b>software commit onu IF_NAME &lt;0-1&gt;</b>	<p>다음 부팅에 사용될 image-id 에 대해 commit 을 실행합니다. ONT OFF/ON 시 commit 된 펌웨어로 부팅되지는 않습니다. (software activate 실행 시에만 다른 펌웨어로 변경됨.)</p>	Config-gpon
<b>software activate onu IF_NAME &lt;0-1&gt;</b>	<p>ONT software 를 reload 하고 선택한 image-id 로 부팅합니다.</p>	Config-gpon
<b>show gpon software onu IF_NAME</b>	<p>ONT/ONU 펌웨어 버전정보를 조회합니다.</p>	enable

### 23.5.3. ONT/ONU firmware upgrade (auto-upgrade)

U9264 supports auto-upgrade of ONT/ONU pon chip.

auto-upgrade unlikely manual-upgrade does not perform download by each interface. 각 ONT 의 펌웨어를 flash 에 업로드한 뒤 auto-download 를 start 하면 OLT 에 등록되어 있는 모든 ONT 에 대해 자동으로 업그레이드를 진행합니다.

Command	Description	Mode
<b>software add onu FILENAME A.B.C.D</b>	tftp 서버로부터 펌웨어를 flash 에 업로드합니다. 최대 10 개의 펌웨어를 업로드할 수 있습니다.	Config-gpon
<b>software remove onu FILENAME</b> <b>software remove onu all</b>	flash 에 존재하는 auto-upgrade 용 펌웨어를 삭제합니다.	Config-gpon
<b>software auto-download onu start</b> <b>(autoReset (time &lt;0-23&gt; ))  </b> <b>manualReset)</b>	auto-download 기능을 활성화합니다. <b>autoReset</b> : upgrade 가 완료된 ONT 에 대해서 강제로 reload 를 실행합니다. <b>time (0-23)</b> : autoReset 을 실행할 시간을 설정합니다. (0 시~23 시, 정시 기준) <b>manualReset</b> : upgrade 가 완료된 ONT 에 대해서 autoReset 을 진행하지 않습니다. CLI 를 통해 reload 를 진행해야 업그레이드한 펌웨어가 적용됩니다.	Config-gpon
<b>software auto-download onu stop</b>	auto-download 기능을 비활성화합니다.	Config-gpon
<b>show gpon software auto-download</b> <b>status SLOT</b>	auto-download 진행상태를 확인합니다. 펌웨어 목록도 확인할 수 있습니다.	enable